Navigare sicuri sul Web

Miotti Stefano

volontario per la «Sicurezza in Rete»

incontra le classi di seconda media

della scuola media Moroni di Vigodarzere (Pd)

La ricetta per la Sicurezza su Internet = Essere al Sicuro + Agire in modo Sicuro

Su Internet,

come nella vita di ogni giorno, serve…

… rendere sicuri i nostri computer nello stesso modo in cui chiudiamo le porte e le finestre quando usciamo di casa

… conoscere i pericoli che possono anche nascondersi su Internet e agire con comportamenti sicuri

Minacce alla sicurezza del PC

Virus/Worm

Programmi Software progettati per invadere il vostro computer e copiare, danneggiare o cancellare i vostri dati

Trojan Horses

Virus che finge di essere un programma utile ma che invece distrugge dati e danneggia il vostro computer

Spyware/Adware

Software che spia e tiene traccia delle vostre attività online o manda pop up pubblicitari senza fine

Le password più popolari del 2022: un incubo senza fine

Se le password peggiori del 2019 erano un autentico orrore, le **password più popolari del 2020 / 2021 e del 2022** rappresentano un'ulteriore conferma del fatto che la sicurezza informatica è un obiettivo a lunghissimo termine. Forse persino impossibile da raggiungere.

Anche nel 2022, come nel 2021 e negli anni prima ancora, **le password più comuni sono quelle che si *crackano* nel giro qualche secondo** o anche in meno tempo. A mettere insieme la lista aggiornata è NordPass, società non a caso specializzata nella gestione sicura e multi-piattaforma di password a prova di hacker.

Secondo NordPass, il trittico delle password più usate nell'anno che volge al termine include *123456*, *123456789* e *picture1*, con le prime due a crescere in popolarità e la terza come nuova entry. La **colonna infame delle password del 2022** comprende poi la mitica *password* (una frazione di secondo per il crack), *12345678*, *111111* e altre mostruosità assortite a seguire.

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213
11. ↑ (12)	1234567	165,909	Less than a second	2,516,606

Come creare una password sicura in 5 mosse

1 - Scegliete un nome legato alla vostra vita. Per esempio, un protagonista dei cartoni animati dell'infanzia, la vostra squadra del cuore, oppure il nome del vostro partner. Nel nostro esempio scegliamo "**sampei**"

2 - Trasformate alcune lettere in numeri. "**5ampe1**"

3 - Aggiungete in testa o in coda un numero facile da ricordare, come l'anno di nascita di un figlio. "**5ampe185**"

4 - Aggiungete un carattere speciale in testa o in coda. "**5ampe185_**"

5 - Ultima mossa: dopo il carattere speciale, **aggiungete una lettera** (magari MAIUSCOLA) legata al servizio da proteggere con password. "**5ampe185_E**" sarà la password delle email, "**5ampe185_B**" sarà della banca e così via.

È importante che non riveliate a nessuno le vostre regole. Il metodo è semplice: richiede un po' di utilizzo, come **imparare le tabelline**. Ma dopo poco tempo vi accorgerete che non state più "memorizzando" le password (quindi non potrete scordarle). E avrete, nello stesso tempo, la garanzia di averle differenziate.

A pagina 57
Password infallibili e protezione per i tuoi file.

Password banali? Guai a te!

Da una ricerca di Splashdata sono emerse le password più gettonate del 2013: un vero campionario di ingenuità e palese banalità.

Password: la parola d'accesso a un account o un servizio, ma anche la vera trappola della Rete, una trappola che noi stessi approntiamo e in cui, spesso, cadiamo. Sono moltissime la password banali impostate ogni giorno in tutto il mondo e, fin troppo di frequente, l'uso di una di queste parole chiave create senza accortezza può portarci a perdere dati vitali, se non direttamente dei soldi, a vedere un nostro profilo hackerato e a dover correre ai ripari quando ormai il danno è stato fatto. Per pigrizia, mancanza di conoscenza o per semplice disattenzione, moltissime persone scelgono termini banali, sequenze di lettere e numeri facilmente intuibili e si espongono così a gravissimi rischi.

Una situazione preoccupante

Splashdata, azienda produttrice di applicazioni e programmi per smartphone, ha pubblicato i risultati della sua ricerca annuale sulle password più comuni usate in Rete. Il quadro che ne esce è desolante: gli utenti medi sono senza alcun dubbio degli sprovveduti. Se i dati degli internauti fossero soldi e gioielli e le password delle casseforti, probabilmente sarebbero di cartone e forse neanche chiuse. Il fatto è che, mediamente, quando si deve scegliere una parola in codice per tutelare un account, l'operazione viene svolta controvoglia e senza prendere in considerazione le regole di sicurezza più elementari. Il risultato è che le password più comuni appartengono a due categorie: sequenze di lettere o numeri organizzate solo secondo la loro disposizione sulla tastiera, oppure parole assolutamente banali e quindi individuabili da un programma per violare le password con estrema facilità. Esiste anche una terza categoria, non presente in questo elenco di 25 termini, semplicemente perché costituita da parole che variano da persona a persona, ma che sono altrettanto facili da individuare per un malintenzionato che studi la nostra vita virtuale: date e nomi per noi significativi.

La nostra vita in una parola

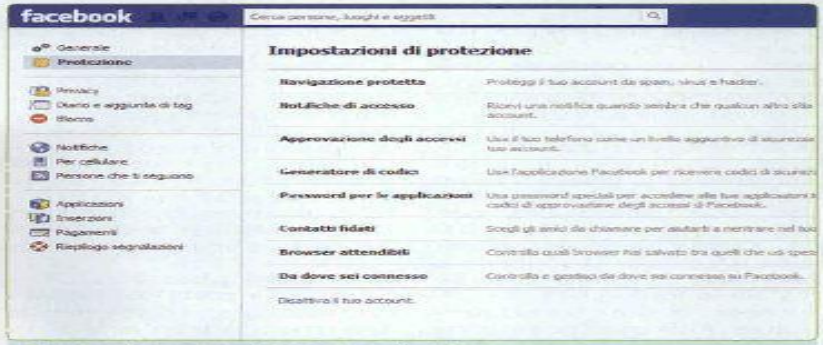
Viene da chiedersi quali siano le password che seguono. Dopo quel livello, si tratta di parole sempre meno frequenti, termini specifici relativi alla vita delle persone: sono nomi di amici, parenti e animali con numeri e date, luoghi, squadre sportive, titoli di film o di personaggi. Apparentemente sembrerebbero soluzioni sicure.

Le 25 parole più usate

Secondo SplashData, gran parte degli utenti è priva di fantasia e di cautela.

Dalla più frequente alla più rara, ecco le 25 password più usate: 123456, password, 12345678, qwerty, abc123, 123456789, 111111, 1234567, iloveyou, adobe123, 123123, admin, 1234567890, letmein, photoshop, 1234, monkey, shadow, sunshine, 12345, password1, princess, azerty, trustno1, 000000.

Come si può constatare la situazione è agghiacciante: vuol dire che al momento di creare la password, letteralmente migliaia di utenti si sono limitati a premere i numeri del tastierino in sequenza lineare. Per non parlare dell'intramontabile password "password". Alzi la mano chi non l'ha mai usata!



Facebook è potenzialmente a rischio

Per la sicurezza di Facebook non basta scegliere una password robusta: le Impostazioni di protezione, che si raggiungono dall'icona a forma di lucchetto in alto a destra, permettono di stabilire chi ha accesso alle nostre informazioni.

Tuttavia, come vedremo, prestano il fianco agli attacchi più determinati.

Un furto impensabile

Sono molti i modi per sottrarre le password: usando dei keylogger, tramite attacchi di phishing oppure con i cosiddetti attacchi "Forza bruta", che provano tutte le combinazioni alfanumeriche, o ancora "Dizionario", dove vengono testate tutte le parole di uso comune. Proprio con questi due attacchi, usati per "indovinare" la password, a fine 2013 sono state sottratte parole chiave da circa 326.000 account di Facebook, 60.000 profili di Google, 59.000 identità su Yahoo e 22.000 accessi a Twitter negli Stati Uniti, in Germania, a Singapore e in Tailandia. Dopo un'indagine, gli esperti di sicurezza delle aziende coinvolte si sono dichiarati assolutamente basiti: le password sottratte erano semplicissime, a livello di "123".

Che cos'è "l'ingegneria sociale"?

Potremmo pensare, ingenuamente, che nessuno indovinerà mai che la nostra password sia costituita dal nome del nostro cane e dalla data del giorno in cui è entrato in famiglia! Oppure, potremmo sentirci sicuri a usare come chiave d'accesso le date di compleanno di nostra madre e di nostra figlia, usando il nome del mese al posto del numero, per rappresentarlo. Normalmente sarebbe vero. Tuttavia, uno dei metodi più usati è quello della Social Engineering, ormai tradotto con l'errata formula "Ingegneria Sociale". Si tratta di una pratica, più che di una tecnica, con la quale chi vuole forzare un sistema informatico, studia la vita della sua vittima. Ci si spinge a livelli incredibili, come controllare il profilo di Facebook raccogliendo i dati, annotando i soprannomi usati, controllando gli amici e i parenti. In alcuni casi si arriva anche a rovistare nell'immondizia, soprattutto quella cartacea: uno dei motivi per cui molte aziende tendono a distruggere i documenti. Prima o poi, i dati che usiamo per proteggere il nostro profilo, potrebbero comparire in un'email, una conversazione, un post. E se qualcuno è davvero determinato, potrebbe usarli contro di noi e riuscirà a fare breccia.

Il WOPR e la Forza Bruta
In questa famosa scena del film Wargames - Giochi di guerra, vediamo il computer Joshua che cerca di trovare i codici di lancio dei missili atomici con un attacco "Forza bruta".

Cosa significa?

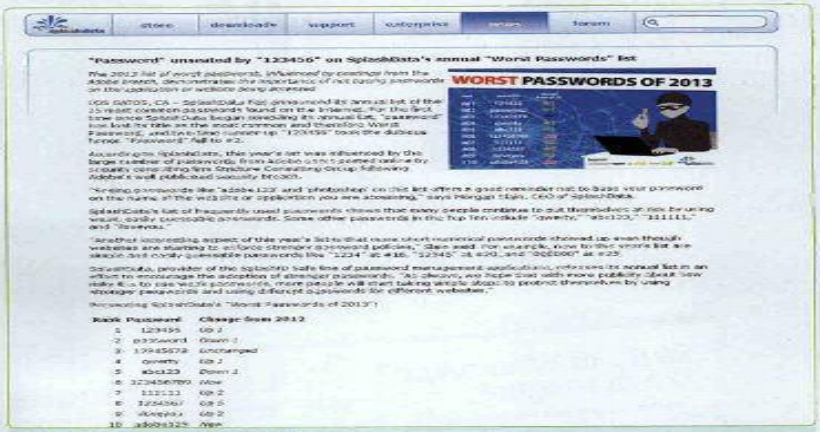
Ci sono alcuni termini che non sono di dominio comune. Vi spieghiamo cosa vogliono dire.

Attacco "Dizionario". Tecnica usata per accedere a sezioni protette da password e codici di accesso, che si basa sul provare sistematicamente tutte la parole di un dizionario linguistico con l'intento di trovare una password costituita da un termine di uso comune.
Attacco "Forza bruta". Tecnica usata per accedere a sezioni protette da password e codici di accesso, che si basa sulla prova sistematica di tutte le possibili combinazioni alfanumeriche, una volta conosciuti i campi da riempire e il numero di "cifre" che il codice deve contenere.
Azerty. Termine che identifica le tastiere che presentano in sequenza i tasti A, Z, E, R, T e Y, sono le tastiere usate prevalentemente nei Paesi di lingua francese
Hackerato. Letteralmente: "che ha subito l'attacco di un hacker", nel senso che è stato violato e modificato.
Keylogger. Programma che legge e registra tutto quello che viene digitato su di una tastiera, usato dai pirati per carpire dati e password
Ingegneria sociale. Tecnica di raccolta delle informazioni personali di un soggetto in modo da carpire o dedurre password, login e codici di accesso attraverso il controllo delle attività online e della vita reale.
Qwerty. Termine che identifica le tastiere che presentano in sequenza i tasti Q, W, E, R, T e Y, sono le tastiere "tradizionali" utilizzate in Italia.

5 trucchi per chiavi sicure

Sebbene non esistano password perfette, con un po' di astuzia possiamo proteggerci bene.

Ecco come fare per essere sicuri di non avere password a rischio:
- Usiamo lettere minuscole, maiuscole e numeri per comporre una password di almeno otto lettere.
- Se il servizio lo consente, usiamo anche punteggiatura e simboli come "&", "$" e "@".
- Usiamo una parola che non sia presente in un dizionario.
- Evitiamo parole facili da indovinare, anche se non presenti in un dizionario, come cognomi di cantanti, titoli di canzoni o di film.
- Evitiamo come la peste date di compleanno, festività, momenti importanti della nostra vita e cose deducibili da qualcuno che ci conosca.



Venticinque fallimenti
La pagina con i risultati della ricerca annuale di SplashData, **splashdata.com/press/worstpasswords2013.htm**, mostra l'elenco delle password più comuni... e banali!

Due servizi preziosi

La sicurezza dei dati è fondamentale: usiamo una buona password oppure nascondiamo le cartelle.

Tutto dipende dalla sicurezza delle nostre password e dalla capacità di impedire ai malintenzionati l'accesso al computer: le informazioni sensibili, i dati di lavoro e finanziari, la nostra vita privata e i contatti. Le password di per sé sono vulnerabili: numeri, lettere, simboli, possono essere combinati in un numero finito di variabili. Vediamo insieme due interessanti servizi. Con il primo valutiamo la sicurezza delle nostre password, mentre con il secondo proteggiamo i dati e le cartelle, rendendoli invisibili.

Collaudo di sicurezza

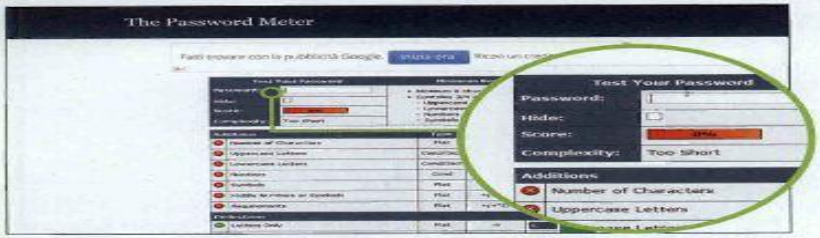
Se andiamo all'indirizzo **http://www.passwordmeter.com** possiamo sfruttare un simpatico servizio online per testare la sicurezza della nostra password. Il principio è immediato: una parola chiave costituita da lettere che formino un termine di uso comune è molto vulnerabile, a differenza di una sequenza casuale di simboli, lettere e numeri. Il servizio valuta la resistenza di una password con un punteggio percentuale e ci mostra i suoi punti forti e i difetti. Per saperne di più leggi l'articolo a pag. 30.

Cosa ti serve

- **CONNESSIONE A INTERNET** un collegamento attivo
- **UNA PASSWORD** per poterla collaudare
- **LINGUA INGLESE** il servizio non è tradotto

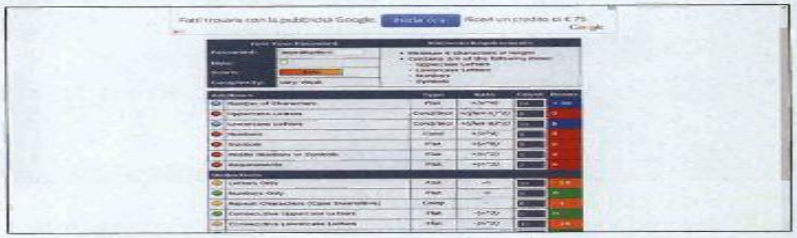
Un controllo dettagliato

La procedura è semplice: scrivi la tua password e lascia che il servizio la valuti.



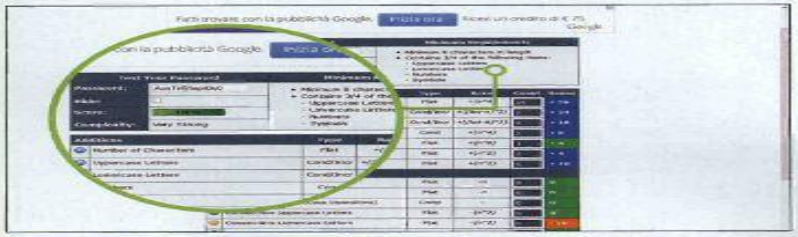
1 Guarda quello che scrivi

Quando visiti il servizio, prima di cominciare a scrivere la password, togli il segno di spunta alla voce "Hide", ossia "nascondi". In questo modo potrai osservare come i diversi simboli incidano sulla sicurezza.



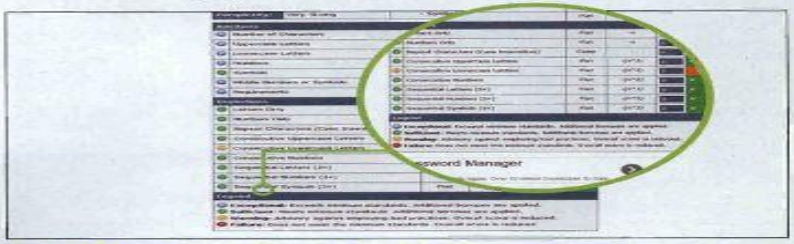
2 Il primo tentativo

Ora componi una password o inseriscine una che già utilizzi, noterai come il suo punteggio di sicurezza si modifica e potrai consultare i campi per vedere dove ha dei punti deboli.



3 Consigli importanti

Segui i consigli presentati nel riquadro in alto a destra: almeno otto caratteri, almeno tre su quattro tra lettere maiuscole, minuscole, simboli, numeri. Riprova e guarda come cambia il punteggio.



4 Cosa significano i punteggi

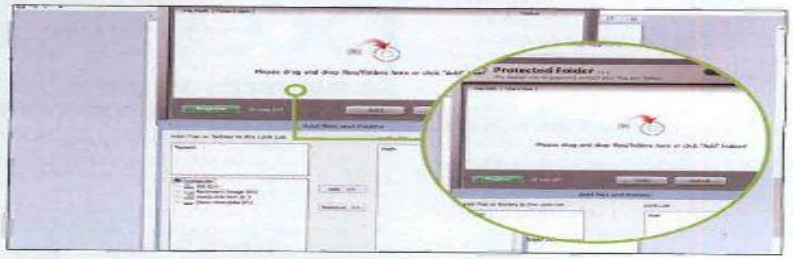
Nella parte inferiore della pagina puoi consultare una legenda dei simboli. Puoi notare anche come vengano conteggiati i punteggi di sicurezza della tua password osservando i campi **Addictions** e **Deductions**.

Se non le trovano... sono al sicuro

Protect Folder di Softonic, su http://password-folder.softonic.it, "nasconde" le cartelle.

1 Crea una nuova password

Il primo passo è quello di creare la tua password. Dopo aver avviato la procedura di installazione, il programma ti chiederà di inserire per due volte la password di accesso. Successivamente, scrivi un suggerimento per ritrovarla.

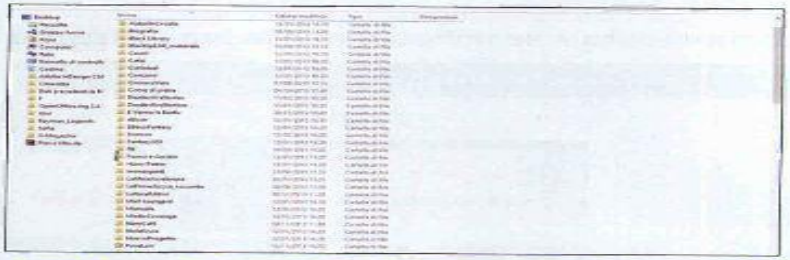


2 Uno spazio invisibile ai curiosi

Per nascondere file e cartelle, il programma ti crea uno spazio "segreto" raggiungibile solo da chi possiede la password. Trascina al suo interno i dati da nascondere, oppure premi il tasto Add e cercali uno a uno.

3 Scegli i file da proteggere

Una volta selezionati e aggiunti alla cartella nascosta tutti i file o le cartelle che desideri celare, fai clic sulla voce **Lock & Exit**, in basso a destra. A questo punto potrai chiudere la cartella e uscire dal programma.

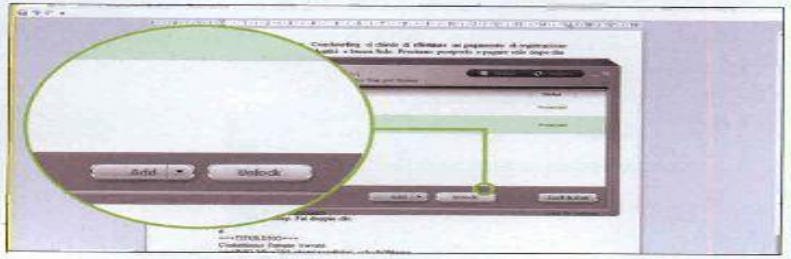


4 Prima li vedevi, ora non ci sono più!

I file e le cartelle che hai aggiunto a Protect Folder sembreranno effettivamente scomparsi, quasi per miracolo, dalla loro posizione originaria. In realtà, per fortuna, sono stati solamente nascosti dal programma.

5 Tranquillo, in realtà sono lì

Se hai bisogno di accedere a una delle cartelle che hai nascosto, dovrai aprire il programma. Tra le opzioni di installazione avrai quella di posizionare l'icona di Protect Folder sulla Scrivania. Fai doppio clic sull'icona.



6 Con due clic tutto torna a posto

Inserisci la password per aprire Protect Folder. A questo punto, seleziona la cartella o i file che vuoi "liberare". Per sbloccarli, fai clic sul comando Unlock e li vedrai ricomparire nella loro posizione originaria.

La rete in sicurezza

Rendiamo la vita difficile ai malintenzionati che tentano di accedere alla nostra LAN. Impariamo a chiuderli fuori dalla porta configurando a dovere il router, il NAS e i servizi cloud.

Ci hanno appena attivato la tanto attesa ADSL, abbiamo anche acquistato un nuovo modem-router Wi-Fi. Lo colleghiamo, tutto funziona a dovere e sedendo davanti al PC siamo convinti che sia tutto a posto. Ebbene no, purtroppo non è così, perché manca l'aspetto più importante: la sicurezza della rete locale. Il router, infatti, è il cuore di tutta l'infrastruttura domestica e, se non opportunatamente configurato nella protezione delle trasmissioni, rischia di diventare il principale tallone d'Achille di un apparato altrimenti perfetto. Vediamo quindi come difenderci nel migliore dei modi, blindando a doppia mandata la Wireless LAN.

L'importanza del router

Una rete locale, indipendentemente dal fatto che sfrutti un collegamento via cavo o Wi-Fi, è un'infrastruttura costituita da una serie di componenti: modem, router e unità collegate (computer, smartphone, tablet, Smart TV, NAS e via dicendo). Il primo si occupa di ricevere la linea tramite il segnale ADSL e stabilisce fisicamente la connessione con il Web. Il router, che viene collegato al modem tramite un cavo di rete, è il dispositivo in assoluto più importante. Il suo compito, infatti, è duplice: ricevere la connessione Internet dal modem, rigirandola ai PC connessi alla LAN e al contempo fare in modo che i vari apparecchi dialoghino tra loro, scambiandosi file, informazioni e quant'altro. In pratica, il router può essere definito come il centro di smistamento posto a barriera tra la rete domestica e Internet. Se un malintenzionato riesce a superare le difese poste da questo dispositivo, potenzialmente può accedere a tutte le unità collegate. È questo il motivo per cui i router integrano una serie di funzioni dedicate alla sicurezza e a cui dobbiamo prestare tutta la nostra attenzione ben prima di iniziare a navigare.

Nascosta è meglio

Visto che oramai il Wi-Fi è ampiamente diffuso, prendiamo in considerazione l'idea di configurare una rete senza fili. Questo standard, però, è il più pericoloso da usare. Infatti, chiunque sia intenzionato ad accedere indebitamente non ha bisogno di collegare nessun cavo. Basta che si apposti nelle vicinanze, rilevi la rete con un dispositivo mobile e si metta all'opera per superare le difese. La prima cosa da fare è quindi occultare la visibilità della WLAN (Wireless-LAN). In pratica, il nome con cui etichettiamo la rete, chiamato SSID (Service Set Identifier), non deve più comparire nel rilevamento automatico dei dispositivi che compiono

Prima di leggere l'articolo...

In queste pagine, tra le altre cose, parliamo di come configurare le opzioni di sicurezza di un router. Per applicare i nostri consigli, dovrete accedere al pannello di gestione del dispositivo, immettendo il suo IP nella barra degli indirizzi del browser. In base alla marca e al modello, le voci possono cambiare, ma le opzioni rimangono sostanzialmente le stesse. Noi ci riferiremo alle diciture inglesi, poiché la maggior parte di questi dispositivi sfrutta pannelli di controllo in lingua straniera. Ciononostante, non sarà difficile accomunare i nomi anglosassoni alla nostra lingua madre. Se vi sorgessero dubbi, potete controllare il manuale del router che avete acquistato. Sempre a questo proposito, se avete in dotazione un modello fornito dal provider, spesso vi sono alcune funzionalità bloccate, non disponibili o non accessibili dal pannello Web. In linea generale consigliamo sempre di acquistare un router di terze parti, da collegare poi al dispositivo in comodato d'uso. In questo modo potrete avere pieno controllo su ogni opzione.

Due è meglio di uno

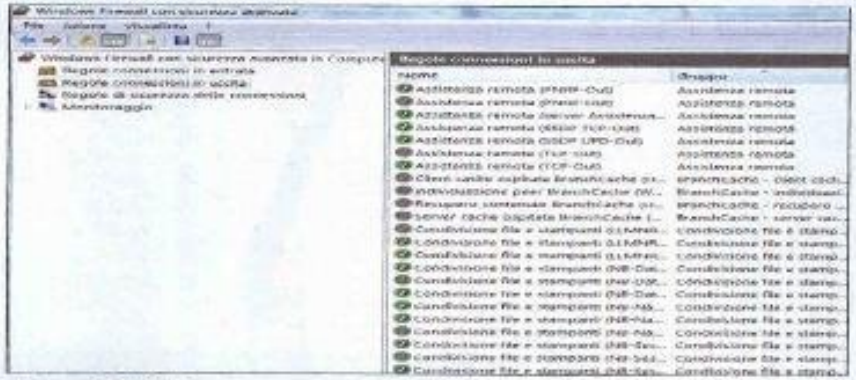
Quando si parla di firewall hardware ci si riferisce a quello del router, *mentre* con la dicitura software si indicano i programmi installati nel PC. La differenza è sostanziale e dipende dalla natura stessa del firewall. Nel primo caso, infatti, siamo di fronte a un modulo integrato direttamente nel router, che sovrintende alla sicurezza di tutta la rete. Nel secondo, invece, si tratta un'applicazione che può essere singola, come Windows Firewall o Look 'n' Stop, oppure inserita all'interno di suite per la sicurezza come Norton Internet Security o Kaspersky Pure. Nonostante a molti possa sembrare ridondante, installare sia un firewall software sia hardware ha i suoi vantaggi. A meno di configurazioni particolari, di solito non si verificano incompatibilità o problematiche. In compenso si ha la sicurezza di avere una doppia protezione. Se poi vi collegate con un portatile tramite una chiavetta Internet, allora diventa indispensabile avere il firewall software, in quanto non si è protetti da alcun dispositivo hardware.

una scansione alla ricerca delle Wi-Fi. Se lo nascondiamo, evitiamo che qualcuno possa accorgersi casualmente della presenza di una rete in zona. Ecco come procedere: nel pannello di gestione del router, andate alla ricerca della voce "Wireless Network Name" e impostate un nome a vostro piacere con cui sarà identificata la WLAN. A questo punto, togliete il segno di spunta da "Enable SSID Broadcast". Anche se esistono stratagemmi piuttosto semplici per ovviare a questa impostazione, ciò non toglie che sia sempre una pratica da attuare. Un altro sistema per rendere più difficile l'accesso alla rete da parte di un malintenzionato è modificare il suo IP. I router, infatti, vengono configurati con impostazioni predefinite in modo da usare indirizzi tipo "192.168.0.1", "192.168.1.1" o "192.168.2.1". Chiunque abbia un minimo di conoscenza riguardante le reti informatiche, inizierà proprio da questi numeri a cercare un ingresso. Per questo motivo vale la pena modificarli a piacere. Le possibilità sono infinite e dipende dalla fantasia nel trovare una combinazione numerica opportuna. Nel pannello di configurazione del router, dovrete solo cercare la voce "IP Address" nel menu LAN.

Comunicazioni blindate

Proseguiamo con uno degli aspetti più importanti concernenti la sicurezza: la crittografia della rete. Gli standard WEP, WPA e WPA2 di cui probabilmente avrete già sentito parlare, si riferiscono proprio a quest'argomento. Attivandoli, siamo sicuri che qualsiasi dato in transito sulla Wi-Fi sia illeggibile a chiunque non possieda le credenziali di accesso. Infatti bisogna considerare che le reti senza fili sono basate sull'uso delle onde radio. Queste si espandono in ogni direzione dal punto in cui vengono emesse e possono essere captate da chiunque abbia un apparato ricevente. Se le informazioni contenute in queste onde non sono criptate, chi le riceve può leggerle senza problemi. Nel caso di una rete Wi-Fi, i dati di cui parliamo possono essere molto sensibili: password, email, comunicazioni private e molto altro. WEP ha purtroppo riscontrato dei limiti operativi che possono essere sfruttati per bypassarlo. WPA e WPA2 sono quindi da preferirsi. Se con i router che acquistiamo è necessario abilitare questi standard manualmente, nei dispositivi che ci vengono forniti dal provider sono spesso già operativi. C'è però un problema da non

Quando possibile, attiviamo sempre lo standard crittografico WPA2 anziché WEP! È molto più affidabile e sicuro. Troviamo le opzioni nel pannello di configurazione del router sotto la voce "Wireless security".



Il firewall di Windows, a cominciare da quello di Seven, è diventato molto più affidabile delle versioni precedenti. Dal pannello "Impostazioni avanzate" è possibile modificare le regole delle connessioni in entrata e in uscita.

Nelle opzioni di sicurezza del NAS troviamo una funzione che permette di abilitare o disabilitare l'accesso a determinati indirizzi IP. Configuriamola per diminuire al minimo la possibilità di ingressi non autorizzati.

La funzione di protezione degli accessi alla rete aumenta la protezione del NAS. Basta selezionare il protocollo e le rispettive opzioni, per definire delle regole oltre le quali un IP viene bloccato.

sottovalutare: le chiavi di accesso predefinite possono essere scoperte facilmente con i giusti software. Per questo è sempre opportuno modificarle con dei valori scelti a caso. Un'ottima chiave di cifratura è composta da almeno dodici caratteri alfanumerici, con maiuscole e minuscole incluse. Anche in questo caso, troviamo tutte le voci di cui abbiamo bisogno nel pannello "Wireless Security del router".

Zona a traffico limitato

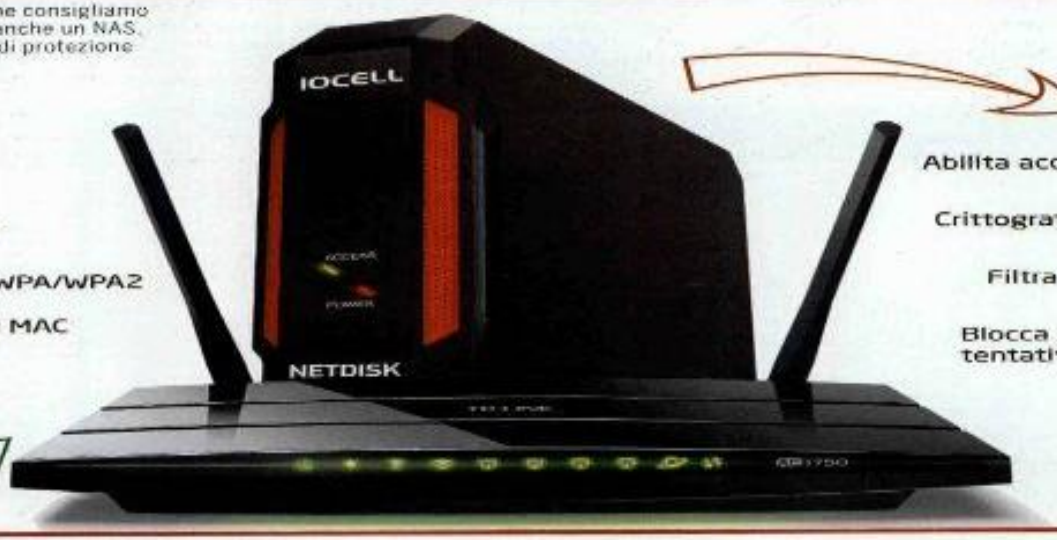
Supponiamo che un hacker davvero bravo sia riuscito a scoprire la chiave di accesso WPA alla rete. Teoricamente dovrebbe essere in grado di entrare senza problemi. In pratica, però, possiamo mettere un'ulteriora barriera che gli impedirà di andare oltre. Stiamo parlando del filtraggio dell'identificativo MAC, un codice univoco che identifica ogni dispositivo di rete. È una specie di numero di telaio, che permette di risalire al modulo di ricezione utilizzato, tra cui le schede che installiamo nel PC, i dongle USB e i moduli presenti in tablet e smartphone. Ogni router permette infatti di filtrare i MAC e consente di scegliere se dare l'accesso o meno a determinati identificativi. Per fare un paragone calzante, potremmo definire questo sistema simile alla presenza di un poliziotto che fa entrare in una determinata zona solo i mezzi con le targhe autorizzate. Dando accesso solo ai dispositivi conosciuti, evitiamo che chiunque abbia altri computer, smartphone o tablet entri alla rete indebitamente.

Il muro di fuoco

Arriviamo dunque al firewall, l'elemento dedicato alla sicurezza per eccellenza. È grazie a esso se la maggior parte dei tentativi di accesso fraudolento alla rete vengono rispediti al mittente. Ogni router ne integra uno e, a differenza di quello del singolo PC, questo sovrintende alla protezione di tutta l'infrastruttura. Per tale motivo è sempre importante assicurarsi di averlo attivato. Nel pannello di configurazione troviamo diverse voci, molte delle quali non sono immediatamente comprensibili. Infatti, si riferiscono ai

Sicurezza in pillole

In verde i parametri di sicurezza che consigliamo di configurare sul router. Se avete anche un NAS, impostate su quest'ultimo i criteri di protezione indicati in rosso.



ROUTER

- Occulta il SSID
- Modifica IP del router
- Attiva la crittografia WPA/WPA2
- Abilita il filtraggio dei MAC e il firewall

NAS

- Abilita accesso protetto
- Crittografa i dischi fissi
- Filtra gli indirizzi IP
- Blocca gli IP dopo tot tentativi di accesso

comportamenti che il firewall deve tenere in occasione di determinate situazioni. Possiamo fare in modo che un IP che tenta un accesso per un certo numero di volte venga bloccato preventivamente. E ancora evitiamo di essere sottoposti a un "flood", ovvero a una valanga di pacchetti inviati per paralizzare l'intera rete. Dopo aver impostato un numero massimo di dati ricevibili, nel caso in cui venga superato, il firewall blocca la ricezione mantenendoci così al sicuro. Un altro attacco, da cui è possibile difendersi abilitando la corretta voce nel pannello di configurazione, è il "DoS" ossia il "Denial of Service". Anche in questo caso si tratta di un'azione dolosa, che consiste nell'esaurire tutte le risorse della rete per bloccarla. Viene quindi inondata da una serie di richieste fino a quando non collassa.

La password è sotto il router

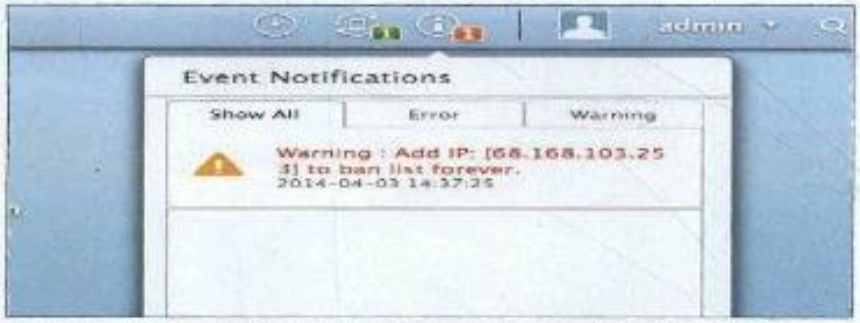
Il pannello di controllo del router è bloccato da una procedura di login. Bisogna quindi farsi riconoscere inserendo nome utente e password. Queste credenziali, almeno per il primo accesso, sono impostate in modo predefinito dal produttore. Per sapere quali sono, controllate il manuale d'istruzioni o in alternativa sotto il router, dove solitamente vengono riportate su un'etichetta. Una volta entrati, ricordatevi di modificarle immediatamente. Altrimenti rischiate che chiunque acceda alla rete locale possa modificare indebitamente le impostazioni del router.

Proteggiamo il NAS

Come anticipato, il router permette di mantenere al sicuro l'intera rete locale e quindi tutti i dispositivi collegati. Tra loro ci sono i NAS, che solitamente contengono la maggior parte dei nostri dati, mettendoli a disposizione di tutti gli apparecchi che ne fanno richiesta. Questi dispositivi di rete devono essere ulteriormente protetti. A tal proposito, permettono di criptare i documenti contenuti nei dischi fissi installati al loro interno. È quindi opportuno abilitare questa funzione, mettendosi così al riparo non solo da accessi non autorizzati, ma perfino da possibili furti di dati. Come per il router, per entrare nel pannello di configurazione del NAS è necessario abilitare nome utente e password. In tal modo, evitate che chiunque possa modificare le impostazioni senza autorizzazione. Nel menu Protezione presente in molti server di questo tipo, potete filtrare le connessioni in ingresso. Inserendo l'IP del computer o del dispositivo autorizzato ad accedere ai dati del NAS, terrete fuori dalla porta i malintenzionati. Sempre in questo comparto, la funzione Protezione accesso alla rete consente di specificare il comportamento del dispositivo nel caso avvengano determinate circostanze. Infatti, abbiamo a disposizione una serie di protocolli (SSH, HTTP, FTP e così via) su cui può avvenire il trasferimento di dati. Supponiamo quindi di voler impostare un blocco di sicurezza per chi tenta di accedere indebitamente attraverso FTP. Basta spuntare la giusta voce, scegliere un periodo di tempo entro il quale un IP può tentare di collegarsi e nel caso non riesca per un tot di volte, viene bloccato.

Al sicuro sulle nuvole

I dati non si trovano più solo nei dischi fissi, ma sempre più spesso nella famosa nuvola, il cloud. Per evitare accessi fraudolenti, dobbiamo quindi porre ancora più attenzione. I servizi online forniscono i più alti standard di sicurezza, ma l'attenzione alle politiche di riconoscimento degli account è affar nostro. Impostando una password debole o non attivando gli appositi protocolli di blocco, rischiamo che chiunque possa curiosare facilmente tra i documenti archiviati nella nuvola. A questo proposito, servizi come Dropbox, Onedrive di Microsoft e Google Drive hanno implementato la verifica in due passaggi. Si tratta di un sistema che prevede, oltre alla tradizionale password, l'immissione di un altro codice numerico inviato tramite SMS, via posta elettronica o fornito mediante un'app specifica per dispositivi mobile. In questo modo, se un hacker scopre la chiave di accesso principale, non potrà entrare a meno che sia in possesso del nostro smartphone o riesca a leggere le email che riceviamo. Per attivare questa funzione, è sufficiente seguire le istruzioni sul sito del servizio cloud utilizzato.



L'indirizzo IP 68.168.103.25 ha tentato di accedere più volte al nostro NAS. È stato quindi bloccato a tempo indeterminato per prevenire il perpetrarsi dell'attacco.

L'accesso a Google account e allo spazio cloud di Google Drive, può avvenire tramite la verifica in due passaggi. Nel nostro caso abbiamo scelto di ricevere il codice supplementare tramite l'app Google Authenticator.

Scopri chi spia il tuo computer

La tua rete di casa ti sembra più lenta del solito? Forse non è il caso di prendersela con il gestore del servizio. Qualcuno potrebbe essersi intrufolato al suo interno per navigare e scaricare usando la tua banda. Questo è solo uno dei segnali che fanno suonare un campanello d'allarme e devono farci correre immediatamente ai ripari

Tutti ormai abbiamo uno smartphone e la maggior parte di noi, a casa, possiede anche una connessione senza fili. Ci sarà certamente capitato di notare che, quando usciamo dall'appartamento, il nostro segnale Wi-Fi spesso risulta ancora raggiungibile e il telefono continua a navigare, sfruttando la Rete domestica. Lo stesso vale per gli appartamenti confinanti con il nostro. D'altronde, se a casa nostra, oltre alla rete wireless che ci appartiene, vediamo anche quelle dei vicini, è naturale che accada pure il contrario. Ma questo che cosa significa? Quando una rete è visibile chiunque può tentare di bucarla e qualcuno ci riesce pure. Purtroppo, il fatto di avere impostato una password non ci mette al riparo dai pirati informatici. Leggiamo ogni giorno di attacchi fatti a colossi che spendono in sicurezza decine di migliaia di euro e non per questo possono dirsi completamente al sicuro...

Conoscere i rischi

Con questo non vogliamo assolutamente fare del terrorismo giornalistico: bisogna essere consapevoli dei rischi che corriamo e armarsi al meglio, per alzare il più possibile il nostro livello di sicurezza. A quali pericoli andiamo incontro, se qualcuno entra nella nostra rete Wi-Fi? Il più fastidioso, benché meno pericoloso, riguarda la velocità. Se un nostro vicino decide di guardare film in 4K in streaming, usando la nostra rete, è ovvio che per noi la navigazione risulterà molto più lenta. Ma se decide di scaricare materiale pirata to o, peggio ancora, andare a visitare siti illegali che contengono, ad esempio, video pedopornografici, potremmo andare incontro a guai con la giustizia molto seri, perché il traffico, eventualmente monitorato dalle autorità, farà capo direttamente al nostro router! Inoltre, quando qualcuno accede alla nostra rete, può anche forzare dall'interno il router, i computer collegati, le webcam e le cartelle condivise. Certo, se non siamo personaggi in vista, nessuno si sognerà di venire a forzare le nostre difese. Ma siamo proprio certi che nel nostro palazzo, in quello di fronte, o nell'auto parcheggiata sotto casa, non ci sia un pirata in cerca di qualcuno su cui "fare pratica"?

Siamo abituati a pensare che gli hacker siano persone super esperte con un preciso credo politico e motivazioni ideolo-

Su internet si trovano strumenti gratis per violare anche le reti più protette

Non solo computer

Oggi i dispositivi collegati a una rete Wi-Fi sono sempre più numerosi e, di conseguenza, anche i rischi sono maggiori. **Alla nostra rete senza fili sempre più spesso, oltre a smartphone, tablet e PC, sono collegati anche smart TV e oggetti come condizionatori, videocamere per la sorveglianza e perfino giocattoli** come le Hello Barbie di Mattel, che si connettono a Internet per parlare con i nostri bimbi e che nei mesi scorsi sono state al centro di tante polemiche in tutto il mondo. La sicurezza dei nostri dati e dei nostri cari è quindi sempre più a rischio, e prestare attenzione a qualunque movimento sospetto all'interno della nostra rete non è più solo un'accortezza, ma un dovere a cui dobbiamo assolvere nel migliore dei modi.

5 PASSI PER STARE SICURI

Ecco che cosa possiamo fare per rendere più sicura la nostra rete Wi-Fi:

1. **Controlliamo tutti i dispositivi collegati al router.**
2. **Aggiorniamo sempre il firmware del router.**
3. **Scegliamo una protezione di tipo WPA2 (AES).**
4. **Usiamo una password di almeno 15 caratteri.**
5. **Inseriamo nella password numeri, lettere e simboli, ma non nomi e date di nascita.**

giche che li spingono a fare quello che fanno. La realtà è un'altra. Oggi esistono strumenti sul web che permettono a chiunque (o quasi) di violare una rete Wi-Fi. Spesso a tentare di forzare il nostro computer è soltanto un ragazzino alla ricerca di una rete gratuita per navigare. Poi, però, una volta dentro, potrebbe venirgli in mente di fare tutt'altro. Oppure il pirata potrebbe essere qualcuno che compie azioni illegali, come per esempio furti di identità o truffe e ha bisogno di cavie per portare avanti i suoi loschi affari senza che la cosa sia riconducibile a lui.

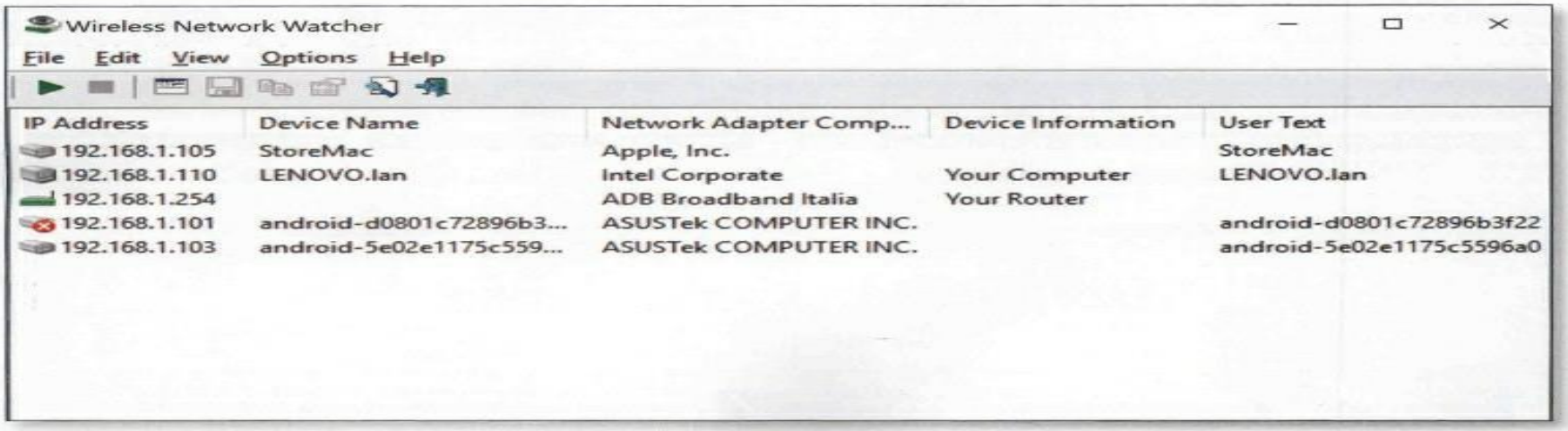
Strumenti per pirati

Alcuni strumenti per entrare illegalmente nelle reti Wi-Fi visibili, come **Crackactivator**, sono disponibili con una semplice ricerca su Google e permettono di craccare anche reti protette con codifica WEP, WPA e WPA2. Crackactivator funziona su Windows e su dispositivi Android. Gli autori del software spiegano addirittura che questo strumento è: "*Incredibilmente facile da usare*". **Programmi di questo tipo, una volta forzato l'accesso a una rete privata, sono addirittura in grado di scollegare i proprietari reali di quel router, per non rallentare il collegamento dei pirati che lo stanno usando!** Abbiamo riportato il nome di questo software per fare un esempio di cosa si può trovare, ma è importante sapere e lo ribadiamo a chiare lettere, che sconsigliamo di scaricare e utilizzare programmi simili: sono illegali ed è un reato violare una rete che non ci appartiene!

Spesso i pirati sono solo ragazzini in cerca di un collegamento a Internet

La buona notizia

Se quanto letto finora ci sta facendo venire i brividi lungo la schiena, tiriamo un sospiro di sollievo. La buona notizia è che non dobbiamo per forza considerarci esposti a queste minacce. In realtà, possiamo corazzarci anche contro simili pericoli e spesso le soluzioni sono più semplici di quanto si possa immaginare. Partiamo da un presupposto fondamentale: ogni collegamento deve passare dal router, che rappresenta il cancello d'ingresso alla rete e anche il centro di smistamento dei dispositivi collegati. Quindi qualunque computer, smartphone o tablet che si connette alla nostra rete, deve per forza passare dal router che tiene traccia di tutto. La prima cosa da fare, quindi, è accedere al nostro router e controllare che non ci siano



Controllo ai raggi X. *Il programma Wireless Network Watcher permette di controllare quali dispositivi stanno usando il nostro collegamento Wi-Fi. Facciamo dei test tutte le volte che ce ne ricordiamo e verifichiamo se nella lista appare qualche apparecchio che non ci appartiene.*

anomalie nei dispositivi collegati. Come si fa? Ogni modello ha le proprie procedure, alcuni hanno software installati in locale, altri hanno bisogno di un nome utente e una password (che ci fornisce direttamente il provider della nostra rete) e permettono di accedere in remoto al dispositivo collegandoci a un preciso indirizzo web, tipo 192.168.1.254. Una volta entrati nelle impostazioni dobbiamo ricercare una voce simile a "*Rete Utente*", "*Rete Locale*" o "*Dispositivi collegati*" per accedere alla lista completa di qualsiasi apparecchio risulti connesso al nostro router. A volte i nomi non sono chiari, ma dobbiamo capire se fra i nostri tablet, gli smartphone, i computer o la Smart Tv sia anche presente qualche dispositivo dal nome strano o che sappiamo non appartenerci. Per sicurezza, possiamo spegnere momentaneamente i dispositivi collegati, che spariranno così anche dalla lista del nostro router. Facciamolo con calma e se ci rendiamo conto che, nonostante tutto, qualche cosa risulta ancora collegata, allora molto probabilmente nella nostra rete c'è un intruso!

Prima di urlare vittoria

Prima di sentirci completamente al sicuro, dobbiamo considerare anche un altro fattore: un eventuale pirata potrebbe non essere collegato alla nostra rete al momento della nostra verifica e quindi potrebbe non apparire nella lista del router. Fortunatamente, esistono strumenti come **Wireless Network Watcher** scaricabile gratuitamente dal sito *http://bit.ly/1dfCrqY*, che ci permettono di tenere sempre sotto controllo i dispositivi connessi al nostro router. Wireless Network Watcher esamina tutto ciò che è collegato al router e ci offre anche informazioni sul produttore del dispositivo collegato, quindi per noi sarà più facile capire di cosa si tratta. Oltre a questo programma, possiamo usarne anche un altro: si chiama **GlassWire** ed è un firewall che si scarica all'indirizzo *www.glasswire.com*. La versione base è gratuita e permette di capire in maniera molto chiara in che modo è suddiviso il traffico della rete. Nella versione a pagamento è possibile impostare dei messaggi di allerta quando un nuovo dispositivo si collega al nostro router.

Per scoprire gli intrusi controlliamo tutti i dispositivi collegati al nostro router

Il modem di Fastweb. *Per accedere alle impostazioni del nostro modem ADB fornito da Fastweb, ci colleghiamo all'indirizzo: 192.160.1.254 e inseriamo nome utente e password.*

Strumenti di controllo

Un altro metodo per verificare se un intruso è all'interno della nostra rete riguarda i DNS, ovvero il sistema di server che permette di tradurre i nomi dei siti in indirizzi IP. In pratica, gli hacker che entrano nel nostro router spesso modificano i DNS in modo da farci collegare a siti falsi, spesso fonte di frodi digitali. Questa tecnica, in gergo viene chiamata **DNS hijack**. Ma cosa accade quando un router è stato infettato? Questo tipo di attacco permette ai pirati di monitorare e ridirezionare il nostro traffico web. Se il nostro router è stato sottoposto a questo tipo di violazione, tutte le volte che tenteremo di accedere al sito della nostra banca, ad esempio, verremo direzionati verso un sito finto, che all'apparenza è identico all'originale e ruberà i nostri codici di accesso. Cosa dobbiamo fare allora per capire se il nostro router è stato violato e infettato da qualche malware che ha dirottato i DNS? Possiamo sfruttare strumenti come **F-Secure Router Checker** che si trova all'indirizzo *http://bit.ly/2d7QQzu* e permette di fare una scansione rapida senza

Verifichiamo se il router è infetto

1 All'indirizzo: *http://bit.ly/2d7QQzu* troviamo uno strumento completamente gratuito fornito da F-Secure che permette di controllare se nel nostro router è stato installato un malware che modifica i server DNS.

2 Il controllo è rapido e, se tutto è a posto, restituisce un messaggio con scritto: **No issues were found**, ovvero: *non sono stati rilevati problemi*. Se viene segnalato un errore, avviamo subito un controllo con l'antivirus su tutte le macchine.

Di Luca Epifanio

I miei dati di accesso sono al sicuro?

Ecco come scoprire se le credenziali di login sono state violate e sono disponibili agli hacker.

In questi anni abbiamo assistito ad una vera e propria guerra dei dati, in cui le credenziali d'accesso rubate (nome utente, password) vengono vendute nei market illeciti online. Sempre più spesso capita di leggere che qualche grande azienda dichiari di aver subito un attacco informatico, che a volte è culminato con la sottrazione dei database delle credenziali degli utenti. È cronaca di queste settimane l'attacco informatico che ha preso di mira la compagnia aerea EasyJet, a cui sono stati sottratti i dati personali di circa nove milioni di clienti.

Ma come fanno i criminali informatici ad acquisire interi database con le credenziali? Quando viene attaccato con successo un sito Web, solitamente gli hacker fanno un *dump* del database, ovvero ne scaricano una copia esatta, per poi tentare di estrapolare le informazioni più interessanti, come appunto indirizzi email e password di accesso. A ingigantire il problema, concorre l'abitudine di molti utenti a utilizzare un'unica password per accedere a più servizi e portali, rendendo le conseguenze di tali furti virtuali una catastrofe; facendo un giro sul deep Web è facile trovare in vendita interi database di credenziali rubate. Premesso che la prima arma di difesa rimane e rimarrà sempre la consapevolezza sul tema (diversificare le password per ogni sito, sceglierne di complesse, evitare di scriverle in un file di testo, magari usare un programma di gestione delle password), alcune aziende hanno ideato tool e servizi gratuiti che permettono agli utenti di verificare se un indirizzo email risulti presente in uno di questi database. Per sapere se una credenziale d'accesso è stata compromessa si può utilizzare uno dei servizi Web che collezionano e analizzano centinaia di dump caricati dagli hacker in molteplici canali (non per forza nel Dark Web,

L'archivio del servizio Have I been pwned include oltre 9 milioni e mezzo di account compromessi

Con un database di più di nove milioni e mezzo di credenziali compromesse, Have I Been Pwned è uno dei migliori servizi per verificare l'eventuale compromissione degli indirizzi email.

Se un'email risultasse compromessa, il servizio restituirà in output le informazioni relative al data breach, come per esempio la data e il nome del servizio attaccato.

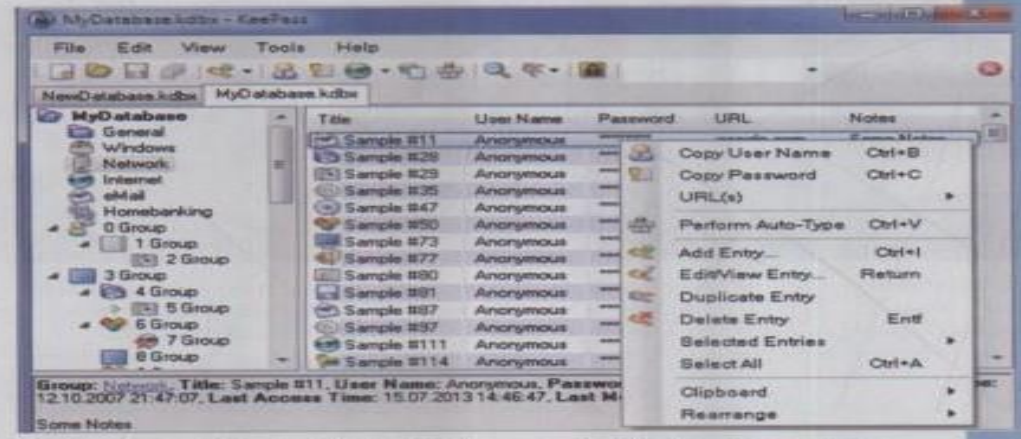
anche su Pastebin se ne trovano moltissimi). Il più noto tra i servizi di questo genere è *Have I Been Pwned?*, con un database che comprende circa 9 milioni e mezzo di account compromessi. Per utilizzarlo non serve nessun download o installazione, basta invece accedere al sito *https://haveibeenpwned.com*

Una volta inserito l'indirizzo email da verificare verrà mostrato il risultato e – in caso positivo (cioè se le informazioni risultino in uno di questi database) – il sito offrirà una serie di informazioni utili, come per esempio la data della violazione, quante credenziali sono state compromesse e altri dettagli (se disponibili) sulla tipologia dell'attacco informatico subito dal servizio. Il servizio offre anche altre funzioni interessanti, come per esempio *Notify Me* che permette di ricevere una notifica, come una sorta di newsletter, ogni volta che l'email indicata risultasse coinvolta in un nuovo data breach. Chi invece ha la necessità di monitorare tutti gli indirizzi di un'azienda, e quindi tenere sotto controllo l'intero dominio di posta aziendale, può andare su *Domain Search*; dopo aver compilato il modulo ed eseguito una verifica di sicurezza riceverà una notifica ogni volta che un'email del dominio risulti nei loro database.

Servizi come BreachAlarm offrono alle aziende la possibilità di tenere sotto controllo l'intero dominio di posta aziendale, facendo scattare una notifica via email per intervenire in maniera repentina.

Ovviamente esistono anche altri servizi altrettanto validi, come per esempio DeHashed *(www.dehashed.com)* e Avast Hack Check *(www.avast.com/hackcheck)*.

Se si considera che molti di essi poggiano su fonti diverse, potrebbe essere saggio utilizzarne e confrontarne più di uno. Tutti i servizi citati sono gratuiti, ma chi ha esigenze particolari e desidera un sistema di notifica ancora più avanzato può rivolgersi a *breachalarm.com*: oltre a offrire il check gratuito come gli altri servizi citati prima, propone diversi pacchetti a pagamento di E-mail watchdog che consentono di cui specificare più indirizzi da monitorare, sia per proteggere tutti gli account di una famiglia sia per il proprio business, con una reportistica più ricca e dettagliata e un supporto di assistenza diretto.



KeePass è un ottimo tool (gratuito) che permette di salvare le password usate per accedere ai servizi online in maniera sicura, evitando soluzioni casalinghe poco sicure per la memorizzazione delle credenziali.

Niente panico

Se si riceve una segnalazione di credenziali compromesse non bisogna entrare nel panico; invece è fondamentale prendere alcuni provvedimenti che ora vedremo nel dettaglio.
Oltre all'ovvietà di cambiare immediatamente la password, bisogna verificare in quali siti e servizi sono state utilizzare le credenziali compromesse dall'attacco, poiché spesso i criminali informatici utilizzano la tecnica del credential stuffing che consiste proprio nel tentare l'accesso su più portali utilizzando le informazioni recuperate in un attacco precedente. A tal proposito, si consiglia di utilizzare un programma di gestione delle password, così da non aver paura di inventare una password diversa per ogni servizio e fare una verifica complessiva sulle credenziali utilizzate per individuare facilmente quali servizi eventualmente condividano la stessa password. Tali servizi (che sono stati oggetto di un articolo pubblicato su numero 351 di *PC Professionale*) permettono di compilare un inventario delle credenziali in sicurezza, senza lasciarle in chiaro nel computer. Se si salva una password all'interno in un file di testo, nel caso di una compromissione del Pc è molto semplice per un malintenzionato estrapolare tutti i dati in chiaro. Al contrario, i programmi di gestione delle password utilizzano algoritmi di codifica robusti (solitamente basati sulle specifiche Rsa) che non solo salvano le password codificate nel Pc, ma consentono anche di generare combinazioni di caratteri casuali (e più sicuri) in maniera automatica, per poi effettuare il login automatico attraverso estensioni per i principali browser.
L'utilizzo di password complesse può limitare o impedire ai criminali di estrarre in chiaro le credenziali dai dump: nella stragrande maggioranza dei casi, infatti, i database rubati non contengono password in chiaro ma i loro hash (ovvero le impronte digitali generate tramite algoritmi specifici, come per esempio Md5); questi algoritmi sono costruiti per non consentire di risalire alla stringa originale partendo dall'hash, ma nel caso di password molto comuni e semplici questa impronta è già nota e quindi tramite tecniche di comparazione è piuttosto semplice decodificare la password.
Per capire meglio come funziona un hash basta collegarsi al sito *https://md5decrypt.net* e digitare per esempio *password1*, fare clic su *encrypt* e copiare l'output generato (l'hash per l'appunto). Ora si può raggiungere il sito *https://crackstation.net*, incollare l'hash e poi fare clic su *crack hashes*. Il sito verificherà la presenza dell'hash nel suo dizionario e restituirà la corrispondente password in chiaro. Questo è possibile proprio perché l'associazione univoca tra la stringa *password1* e il

Per capire come funziona un hash si possono usare diversi siti che permettono di applicare l'algoritmo md5 per la cifratura e la decifratura.

suo hash è già nota, e quindi di facile decodifica. L'ultimo suggerimento, forse il più importante, è attivare ovunque sia disponibile la 2FA (two factor authentication), ossia il secondo fattore di autenticazione; l'abbinamento tra la password e un secondo elemento (in genere un codice, ma anche un device fisico o una verifica biometrica) consente di proteggere l'accesso anche in caso di compromissione di un singolo fattore (in genere la password). Google, Facebook, Microsoft ma ormai anche siti e servizi molto più piccoli permettono di attivare questa modalità di login. Con le ultime regolamentazioni (come per esempio il Gdpr), le compagnie che subiscono furti di dati in cui è potenzialmente compromessa la privacy degli utenti sono obbligate ad avvisare i propri clienti ed emanare bollettini per informare del problema. Purtroppo, ciò non accade sempre e quindi l'impiego dei servizi di verifica rimane un valido strumento per venire a conoscenza di eventuali violazioni. Interessante, infine, è l'utilizzo di questi tool da parte dei criminali informatici che hanno come obbiettivo un utente specifico. Infatti, una volta scoperto l'indirizzo email della vittima questi servizi possono essere sfruttati come pratico database, per poi effettuare ricerche specifiche nel Dark Web e acquistare le informazioni rubate per sfruttarle nel caso in cui l'utente non abbia ancora provveduto a mettersi al sicuro. Per tale ragione, alcuni siti di verifica delle compromissioni inviano una notifica via email ogni volta che si controlla un indirizzo. •

Sempre più aziende incentivano l'uso del secondo fattore di autenticazione; se è attivo, infatti, la violazione della password non porta automaticamente alla compromissione dei dati.

Il regolamento Gdpr (General Data Protection Regulation), entrato in vigore oltre due anni fa, è molto chiaro circa le comunicazioni che le aziende devono fornire ai loro utenti in caso di data breach.

RIPRENDI IL CONTROLLO DEI TUOI DATI

Servono pochi clic per scoprire quali informazioni personali sono finite in pasto ai vari servizi Web e chiedere loro di cancellarli

Per alcune persone, **i dati sono il petrolio del futuro**. Possederli e saperli interpretare grazie a tecnologie sempre più sofisticate significa infatti conoscere le nostre abitudini, i nostri gusti e persino qualche segreto. Tutto materiale che, sfruttando l'intelligenza artificiale, può aiutare aziende e istituzioni perfino a prevedere i nostri comportamenti di consumatori e non solo. Questo spiega come mai negli ultimi anni siano nate diverse iniziative volte ad aiutarci a proteggere i nostri dati. Un esempio? **Mine** (*saymine.com*), la startup israeliana che ci permette di conoscere la nostra "impronta digitale", rintracciando tutti i servizi Web a cui abbiamo lasciato le nostre informazioni per poi, magari, dimenticarcene. Lanciata all'inizio di quest'anno, Mine utilizza l'apprendimento automatico per trovare le aziende che possiedono i nostri dati tramite una lettura veloce della nostra posta in arrivo e sfrutta la legge sul "diritto all'oblio" per chiederne la cancellazione.

La filosofia di Mine

L'algoritmo di Mine riesce a scoprire quali aziende detengono i nostri dati, leggendo l'oggetto delle email. Avete presente quei messaggi di posta nel cui oggetto c'è scritto "benvenuto nel nuovo servizio..."? Spesso queste email introduttive sono il segno che da qualche parte c'è una nostra registrazione. Mine lo sa e in linea con le normative sulla privacy GDPR (vedi qui a lato) manda alle aziende un'email nella quale chiede la cancellazione dei nostri dati, anche se in passato siamo stati noi a darglieli. Nulla di strano: se abbiamo utilizzato un servizio online è comprensibile che abbia informazioni su di noi, altrimenti non potrebbe funzionare. Ma quante volte ci siamo iscritti a un sito o abbiamo aderito a una promozione commerciale, per poi dimenticarcene? Intanto i nostri dati, a volte anche sensibili, come la data di nascita e il numero di telefono, restano lì alla mercé del sito e dei broker che li acquistano per finalità di mercato. Un settore sempre ricco. Peccato però che a guadagnarci non siamo noi.

Non solo. Spesso i dati che lasciamo distrattamente o volutamente in giro sono anche vittima di violazioni da parte di pirati informatici, che a loro volta li rivendono o possono utilizzarli per scopi illeciti. «Ogni

Per proteggere la nostra email principale, usiamo il servizio https://anonaddy.com/

DA SAPERE: IL GDPR

Il 25 maggio 2018 è divenuto applicabile in tutti gli Stati membri il Regolamento noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali. Il testo introduce molte novità a favore dei consumatori utenti. Ma per far valere i nostri diritti bisogna conoscerlo. Per chi volesse farlo, è qui: *https://bit.ly/ci208_gdpr*.

Guadagniamo dai nostri dati con Gener8

Tra le app che hanno fatto della nostra privacy la loro missione c'è **Gener8** (*gener8ads.com*). Fondata dall'ex direttore marketing della Red Bull, Sam Jones, Gener8 si basa su un componente aggiuntivo del browser (Firefox e Chrome) che ci consente di guadagnare dalle pubblicità che guardiamo online, stabilendo una relazione più equa con chi si appropria dei nostri dati. «Sempre più persone si rendono conto che i loro dati sono intrinsecamente preziosi, e desiderano una delle due cose: avere la capacità di controllarli o la capacità di guadagnarci», spiegano gli sviluppatori.

COME FUNZIONA

Registrandoci al servizio, Gener8 ci mostra annunci in base i nostri interessi e ci fa guadagnare un punto ogni volta che guardiamo un annuncio online. Questi punti in un secondo momento possono essere scambiati con prodotti, buoni Amazon o anche trasformati in donazioni di denaro in beneficenza. E il vantaggio non è solo per gli utenti. Anche le agenzie pubblicitarie in realtà ci guadagnano, visto che i loro annunci saranno guardati con attenzione: in Gran Bretagna, Gener8 ha una percentuale di clic superiore del 760% rispetto agli standard.

LA FILOSOFIA DI GENER8

«Penso che un giorno ripenseremo a questo periodo e ci chiederemo come mai è potuto accadere», ha spiegato Jones in un'intervista. «Il fatto che ci sia così tanto valore derivato dai nostri dati personali, ma non sappiamo nemmeno chi li sta raccogliendo e senza averne alcun ritorno, è ridicolo». Per sensibilizzare gli utenti di Internet, Jones ha da poco lanciato una campagna per la creazione di un "Dividendo di dati digitali", che prevede che coloro che non vogliono che le loro informazioni vengano raccolte online, possano deciderlo con un clic e che le società compensino finanziariamente le persone di cui vendono i loro dati. Per ora sembra utopia. Ma in futuro chissà...

giorno c'è una nuova violazione dei dati o uno scandalo sulla privacy. Non possiamo davvero controllarlo e prevenirlo perché la sicurezza è difficile, ma noi vi aiuteremo a conservare i dati solo dove ne avete effettivamente bisogno», spiegano quelli di Mine. La filosofia dell'applicazione Web è quella di aiutarci a diventare consapevoli di quali nostri dati girano per il Web e scegliere quali cancellare. Lo stesso fondatore di Mine, Gal Ringel, ha scoperto che 700 aziende detenevano i suoi dati e le ha ridotte a 350, limitandosi a quelle davvero indispensabili. «Se vogliamo usare la forza di Internet, non possiamo non fornire i nostri dati personali. Dunque noi di Mine non proponiamo di smettere di condividerli, ma solo di sapere quali aziende dispongono di tali informazioni e controllarle», ha spiegato in un'intervista.

Come funziona

Dal 2014, le norme sulla protezione dei dati dell'UE ci consentono di chiedere alle organizzazioni di eliminare le nostre informazioni personali, inclusi numeri di telefono, date di nascita e indirizzi email. Google è stato tra i più colpiti da questo "diritto all'oblio", con 2,4 milioni di persone che hanno inviato richieste in tal senso in quattro anni. L'app Mine funziona utilizzando quelli che in gergo si chiamano algoritmi di machine learning "non intrusivi", programmati per stanare le aziende che invadono la nostra casella di posta con promozioni o altro materiale di iscrizione. Per attivare Mine bisogna recarsi sul sito saymine.com, cliccare il pulsante **Get started** in homepage e scegliere successivamente tra tre opzioni: sapere quali aziende possiedono i nostri dati; comprendere in che modo la nostra impronta digitale ci condiziona; riprendere possesso delle informazioni. Una volta scelto, ci viene richiesto di iscriverci via Google o Microsoft, in modo che l'algoritmo possa scandagliare la nostra email su uno dei due popolari provider. Il risultato è quasi immediato e attraverso una serie di numeri in evidenza, ci mostra quante aziende possiedono i nostri dati, specificando anche a quale settore appartengono. Per approfondire e saperne di più, basta cliccare su **See my footprint**. Il risultato è sorprendente visto che Mine scava anche tra le email sepolte nell'archivio di Gmail e Hotmail.

Liberare i nostri dati

Ad analisi terminata, Mine ci presenta l'elenco delle aziende che attualmente detengono le nostre informazioni personali, proponendosi di inviare loro un'email chiedendo che i nostri preziosi dati vengano eliminati una volta e per tutte. Per attivare questo processo dobbiamo cliccare su **Take quick action**, scegliere uno ad uno i servizi e i siti a cui vogliamo togliere la podestà sui nostri dati e cliccare su **Let's reclaim**. Mine a quel punto gli invia un'email con la richiesta, come spiegato nelle FAQ (*https://bit.ly/ci208_mine*) e da quel momento in poi potremo seguire tutti gli sviluppi, collegandoci di tanto in tanto a Saymine.com.

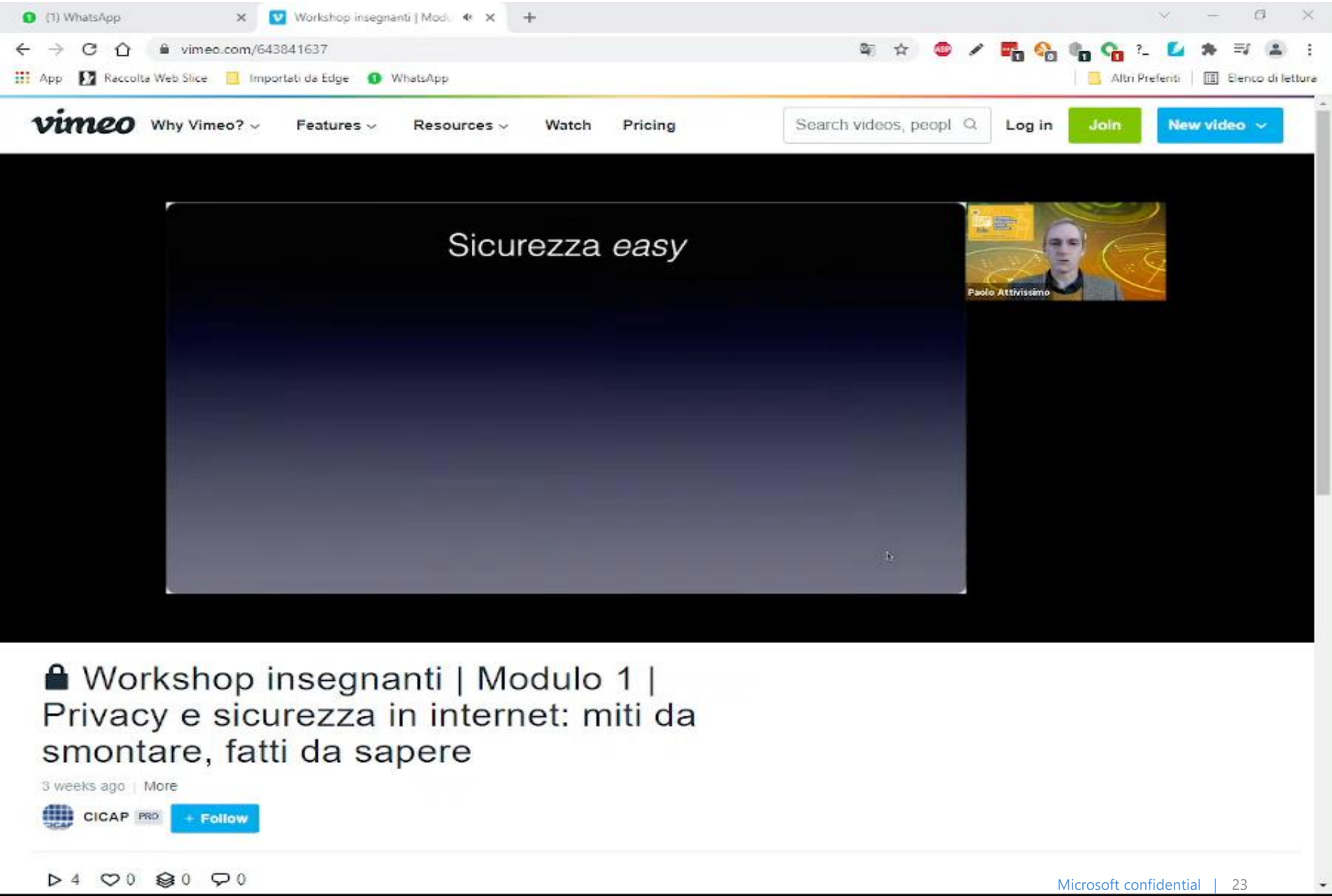
La scommessa

L'idea di Mine è davvero ambiziosa: spostare la nostra attenzione e quella delle Istituzioni dalla privacy alla proprietà dei dati.

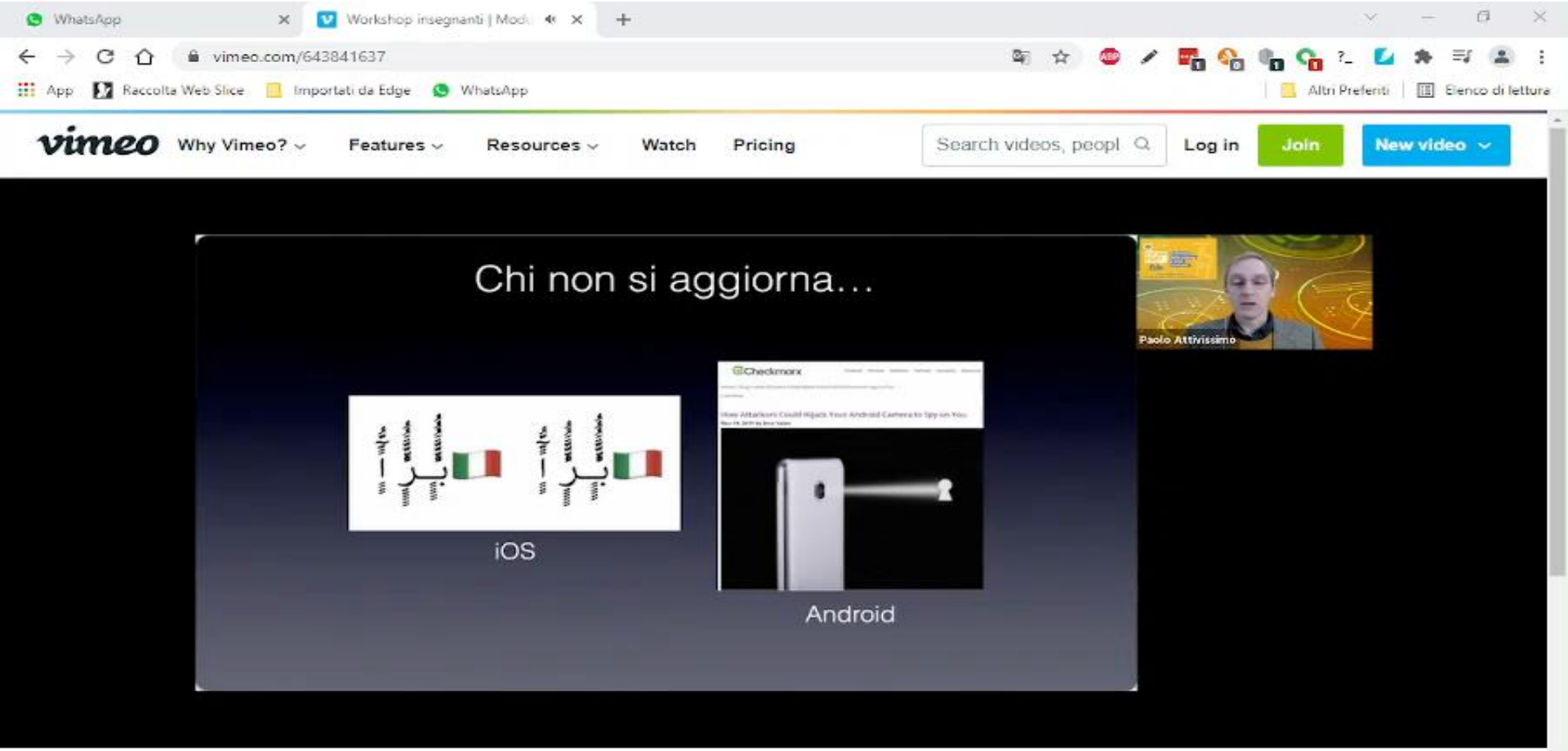
«Viviamo in un'epoca in cui le persone sono sempre più preoccupate di quanto siano diventate invadenti le app e le varie piattaforme che usiamo tutti i giorni», ha dichiarato Gal Ringel. «Pertanto, abbiamo deciso di investire i nostri sforzi nella costruzione di una soluzione in grado di offrire ai consumatori una scelta reale su chi può conservare i propri dati e su come questi possono essere utilizzati. Stiamo dando il via al futuro della proprietà dei dati».

Riassunto finale. *Ecco come appare una schermata di Mine, dopo aver analizzato la nostra email alla ricerca dei servizi che possiedono i nostri dati.*

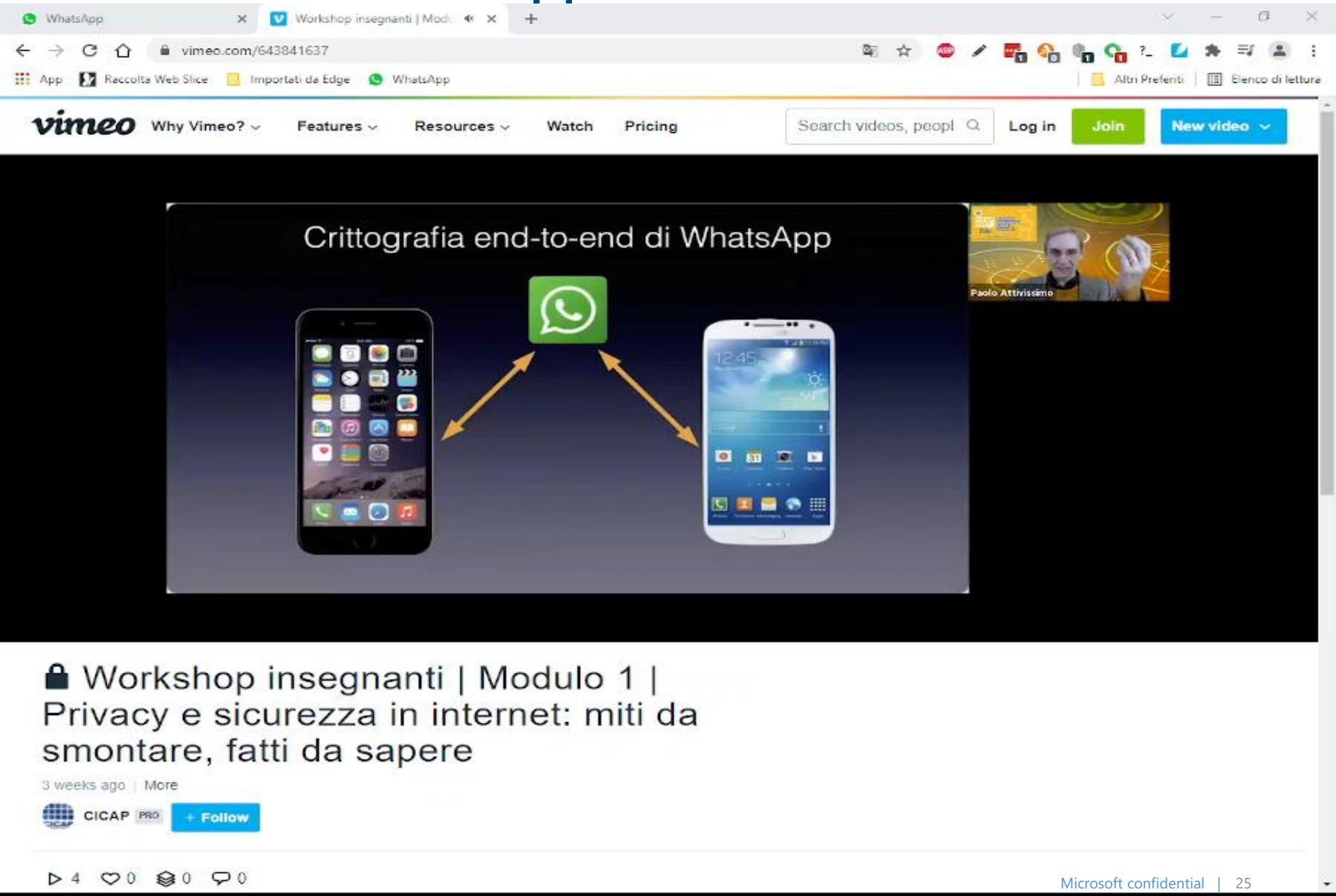
Sicurezza


(1) WhatsApp
Workshop insegnanti | Mod
vimeo.com/643841637
App
Raccolta Web Slice
Importati da Edge
WhatsApp
Altri Preferiti
Elenco di lettura
vimeo
Why Vimeo?
Features
Resources
Watch
Pricing
Search videos, peopl
Log in
Join
New video
Sicurezza easy
Paolo Attivissimo
Workshop insegnanti | Modulo 1 | Privacy e sicurezza in internet: miti da smontare, fatti da sapere
3 weeks ago
More
CICAP
PRO
+ Follow
4
0
0
0

Whatsapp e password



Whatsapp end to end



Di Dario Orlandi

SUITE DI SICUREZZA FAI-DA-TE

Oltre alla protezione contro i malware veri e propri, le moderne security suite offrono anche una miriade di altre funzioni, che spaziano dal backup dei dati alla gestione delle password. Con un po' di lavoro, però, si può ottenere gratuitamente una dotazione analoga, in alcuni casi addirittura migliore.

GARANTIRE LA SICUREZZA DEI COMPUTER, DEI FILE E DEGLI UTENTI È UNA SFIDA CONTINUA, CHE RICHIEDE UN APPROCCIO A 360 GRADI: MINACCE SEMPRE NUOVE SI AGGIUNGONO A UNA CASISTICA GIÀ AMPIA, E I SOFTWARE DI PROTEZIONE COMMERCIALI HANNO VISTO CRESCERE NEL TEMPO LA LORO DOTAZIONE NEL TENTATIVO DI COPRIRE TUTTI I PRINCIPALI FATTORI DI RISCHIO. MOLTE FUNZIONI INTEGRATE NELLE SUITE PIÙ RICCHE POSSONO PERÒ ESSERE AVVICINATE, EGUAGLIATE O ADDIRITTURA SUPERATE DA STRUMENTI E SOFTWARE SPECIFICI, SPESSO DISPONIBILI GRATUITAMENTE. NELLE PROSSIME PAGINE SCOPRIREMO QUALI PROGRAMMI AGGIUNGERE E QUALI IMPOSTAZIONI UTILIZZARE PER OTTENERE UNA DOTAZIONE SIMILE A QUELLA PROPOSTA DAI PRODOTTI DI SICUREZZA PIÙ RICCHI E COMPLETI.

In principio era l'antivirus, un software dedicato all'individuazione dei malware che verificava periodicamente la presenza di infezioni, a cui soltanto in un secondo tempo sono state aggiunte le funzioni di analisi in tempo reale che oggi costituiscono la prima linea di difesa in tutti i computer. Ma la crescita delle minacce alla sicurezza informatica e le esigenze commerciali dei produttori di soluzioni antimalware hanno portato al progressivo incremento della dotazione di funzioni e del numero di pacchetti proposti: all'antivirus è stata affiancata la security suite, che in origine includeva anche un desktop firewall (ora questa funzione è spesso affidata al sistema operativo), e poi i pacchetti completi, caratterizzati da denominazione come Total, Complete o 360, per indicare l'obbiettivo di garantire una protezione assoluta e di rispondere a tutte le esigenze di sicurezza dell'utente. La dotazione di questi prodotti non è mai stata del tutto uniforme, ma in genere erano inclusi anche strumenti di backup e funzioni di ottimizzazione delle prestazioni del computer. Nel corso degli anni la dotazione è cresciuta e si è in parte modificata; abbiamo già accennato alla progressiva sparizione dei firewall, la cui presenza è divenuta sempre meno rilevante man mano che le funzioni integrate in Windows crescevano in efficacia e popolarità: oggi solo pochissime suite continuano a proporre un firewall che si sostituisce del tutto a quello nativo. Più spesso, le funzioni del software si limitano a modificare la configurazione predefinita aggiungendo nuove regole o cambiando alcune impostazioni, e talvolta trascurano del tutto questo aspetto lasciando lavorare senza intromissioni il firewall nativo di Windows, che oggi è perfettamente in grado di garantire la protezione nella grandissima maggioranza dei casi.

Un'altra categoria di funzioni sempre meno popolare è quella dedicata all'ottimizzazione delle prestazioni del computer; da un lato, la potenza di calcolo garantita dalle architetture hardware moderne è in genere più che sufficiente per offrire un'esperienza d'uso più che soddisfacente, mentre dall'altro i reali benefici degli strumenti di ottimizzazione sono a stento misurabili, e certamente impercettibili nel lavoro quotidiano. Questo non significa, comunque, che la dotazione di queste suite sia diminuita nel corso del tempo; al contrario, il numero e la varietà degli strumenti disponibili è in continua crescita, sia perché sono nate e

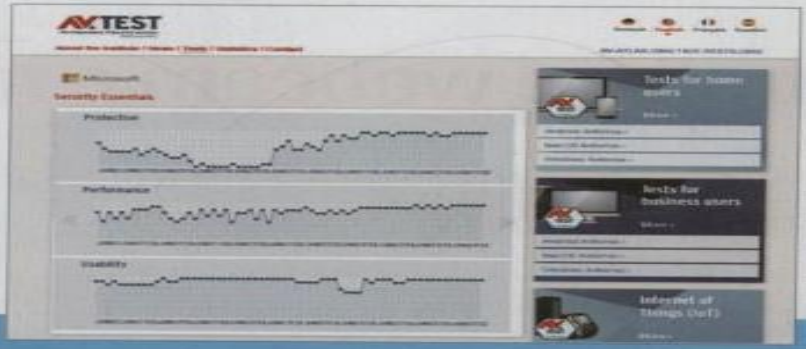
Lanciato nell'ormai lontano 2007, Norton 360 (ai tempi prodotto da Symantec) è stato uno dei primi pacchetti di sicurezza all-in-one a raggiungere il mercato.

La lista delle funzioni integrate in una suite di sicurezza moderna (nell'esempio la pagina di confronto di Kaspersky) va molto oltre la semplice individuazione e rimozione del malware.

si sono imposte nuove minacce alla sicurezza e all'integrità dei dispositivi, sia perché i produttori cercano di differenziare la loro proposta in un settore in cui la concorrenza è spietata e le alternative rimangono numerose.

Una dotazione in continua crescita

Gli esempi sono numerosissimi: innanzi tutto, l'esplosione del fenomeno ransomware ha riportato al centro dell'attenzione l'importanza delle funzioni di backup, ancora oggi l'unico reale antidoto contro questa subdola forma di attacco malware. A questo si aggiunge la sempre più frequente integrazione tra backup locale e remoto, con servizi cloud che garantiscono anche contro eventi estremi come il furto o lo smarrimento dell'hardware.



I risultati delle analisi condotte dai laboratori di ricerca indipendenti (come AV Test) sottolineano la crescita delle funzioni di sicurezza sviluppate da Microsoft e integrate per default in Windows.

Un altro aspetto che viene affrontato sempre più spesso dalle suite di sicurezza è la gestione dell'autenticazione, con strumenti di password management più o meno ricchi ed efficaci; garantire una memorizzazione sicura e un accesso rapido alle credenziali di login è infatti cruciale per proteggere l'accesso ai moltissimi dati personali che sono ormai disseminati nei più diversi siti e servizi Web. Sono preziose anche le funzioni di analisi dell'archivio, capaci di segnalare password deboli o ripetute, o ancora notificare l'utente nel malaugurato ma sempre più frequente caso in cui si venga coinvolti in qualche violazione di servizi remoti.

La fantasia degli sviluppatori si è poi sbizzarrita negli ultimi anni, con l'aggiunta di strumenti come quelli che verificano la presenza di eventuali aggiornamenti delle applicazioni installate, e magari consentono anche lo scaricamento e l'installazione automatica delle nuove release, oppure i tool che tengono sotto controllo l'utilizzo di alcune periferiche critiche (webcam e microfono) da parte delle applicazioni, o ancora funzioni capaci di individuare eventuali problemi nelle memoria di massa prima che il danno diventi irrimediabile. I lettori più attenti ed esperti però avranno già notato come la grande maggioranza di queste casistiche sia in realtà coperta, con maggiore o minore efficacia, anche da software specializzati o addirittura da funzioni e impostazioni native del sistema operativo. In alcuni casi l'implementazione offerta dalle security suite offre vantaggi significativi in termini di efficacia e semplicità d'uso, ma in molti altri invece i programmi e i servizi specializzati garantiscono maggiore potenza e flessibilità: è il caso, per esempio, dei software di backup, dei gestori di password e dei servizi Vpn.

Questo non significa, naturalmente, che il pacchetto di funzioni offerto dalle security suite commerciali sia superfluo: l'integrazione tra le diverse componenti è infatti un fattore importante per valutare questi software, che propongono una soluzione "chiavi in mano" capace di garantire un ottimo livello di sicurezza appena dopo aver completato l'installazione, senza bisogno di cercare, installare e configurare nient'altro.

Chi invece preferisce scegliere personalmente gli strumenti e le funzioni più adatte per le proprie esigenze, magari abbinandole a un antivirus gratuito (o addirittura alle sottovalutate funzioni di protezione native di Windows) potrà trovare nelle prossime pagine molti suggerimenti e indicazioni per comporre la propria suite di sicurezza personale, cucita su misura per rispondere alle necessità e preferenze personali.

Controllare webcam e microfono

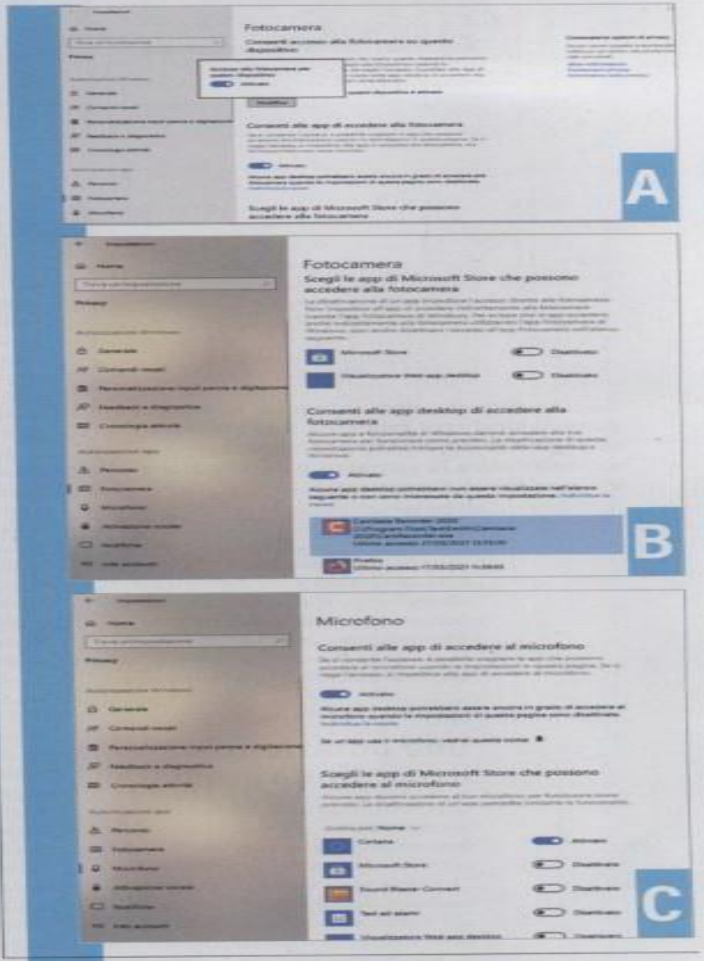
Per evitare sguardi indesiderati è opportuno tenere sotto controllo, ed eventualmente bloccare, l'accesso alle periferiche di input multimediali più diffuse.

I malware più evoluti possono compromettere i sistemi infettati in molti modi; oltre a esfiltrare file e documenti, cifrare i contenuti per chiedere un riscatto oppure registrare tutti i caratteri digitati tramite la tastiera, possono anche attivare altre periferiche che fanno ormai parte della dotazione standard dei computer, specialmente i notebook, come per esempio webcam e microfono. I timori per questo genere di attacchi hanno portato alcuni utenti a coprire la webcam con lo scotch o applicare sportellini adesivi che possono essere aperti in caso di necessità; alcuni produttori hardware hanno aggiunto ai loro computer interruttori che interrompono fisicamente la connessione elettrica tra la webcam e la scheda madre, o coperchi per oscurare l'obbiettivo e accecare quindi potenziali spettatori indesiderati.

Senza arrivare a soluzioni così estreme, molte suite di sicurezza segnalano quando un software tenta di accedere a questi dispositivi, e in molti casi permettono anche di scegliere se concedere l'autorizzazione all'accesso (per esempio nel caso di un software di comunicazione) o se invece negarla. Questi strumenti funzionano in genere molto bene e offrono un buon livello di protezione, ma opzioni simili sono integrate da qualche tempo direttamente in Windows 10: per individuarle basta aprire l'app Impostazioni e raggiungere la pagina *Privacy/Fotocamera;* in cima alla pagina una stringa segnala lo stato della periferica (normalmente *L'accesso alla fotocamera per questo dispositivo è attivato*); un clic sul pulsante *Modifica* consente di attivare o disattivare completamente il device *(figura A)*. Scorrendo la pagina verso il basso si trovano altri due switch che permettono di controllare l'accesso per le app Microsoft Store e per i tradizionali software desktop *(figura B)*. Nel caso delle app, l'autorizzazione può essere concessa oppure negata singolarmente, mentre le applicazioni win32 vengono soltanto elencate. Non è l'unico limite: Windows sottolinea che, nel caso delle applicazioni tradizionali, la protezione non sia assicurata in ogni circostanza. Alcune applicazioni potrebbero infatti installare driver proprietari per accedere direttamente all'hardware aggirando i blocchi imposti dal sistema operativo. Del tutto analoga è la pagina *Privacy/Microfono (figura C)*, che offre opzioni pressoché identiche ma è naturalmente dedicata alle periferiche di input audio.

Una piccola ma gradevole differenza riguarda la segnalazione dell'attivazione: quando un'app utilizza il microfono, infatti, il sistema mostra un'icona nell'area di notifica della barra delle applicazioni; peccato che lo stesso non avvenga nel caso della webcam.

Le funzioni di Windows 10 sono molto semplici da utilizzare e piuttosto rapide da raggiungere, ma esistono moltissime utility di terze parti che rendono la vita ancora più semplice; WebCam On-Off *(www.sordum.org/8585/webcam-on-off-v1-4/)*, per esempio, è un tool gratuito, distribuito in formato portable, che può individuare e bloccare con due clic la webcam e il microfono. Il tool supporta anche alcuni argomenti per la riga di comando, e permette quindi di creare semplici collegamenti per attivare o disattivare le periferiche con un semplice doppio clic.

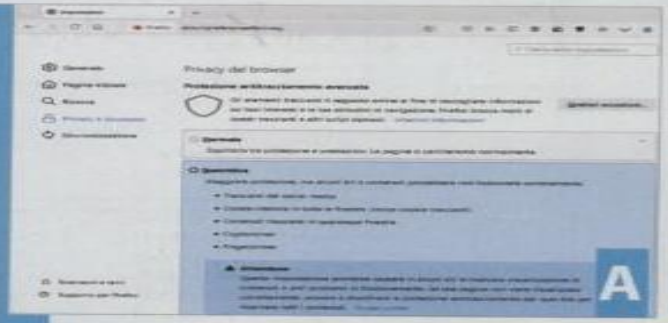


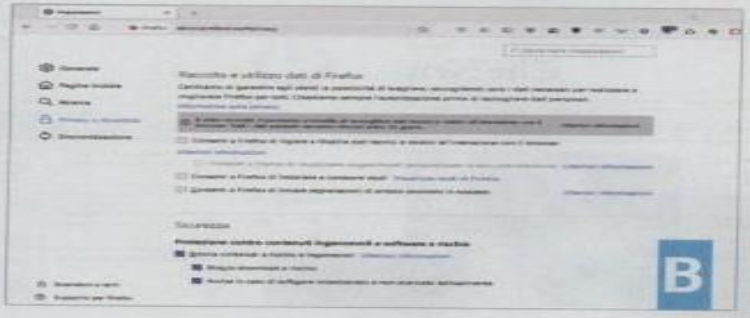
Privacy e sicurezza nella navigazione

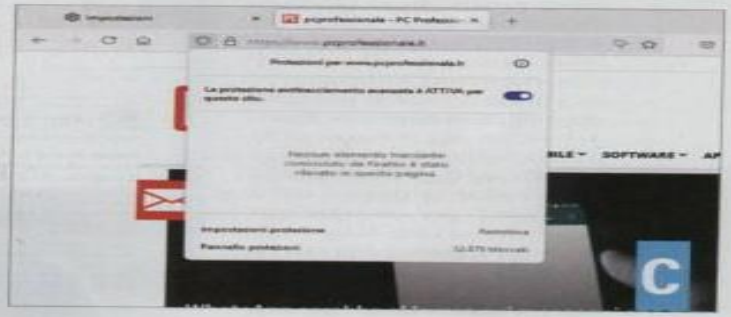
La navigazione su Internet è l'attività più frequente svolta dalla maggioranza dei possessori di Pc, ma è anche una delle più pericolose.

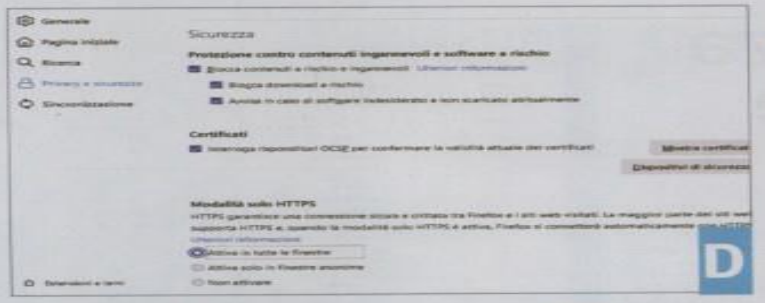
Molti antimalware includono estensioni per il browser che proteggono l'utente durante la navigazione quotidiana; anche in questo caso, gran parte delle funzioni offerte è facilmente replicabile utilizzando gli strumenti integrati direttamente nel browser (o, per lo meno, in alcuni browser) o ampliando la dotazione tramite estensioni dedicate. Il primo passo è la scelta del browser: in questo paragrafo concentreremo l'attenzione in particolare su Mozilla Firefox, che offre una dotazione di funzioni legate alla tutela della privacy particolarmente ricca e completa. Inoltre, la presenza di moltissime estensioni consente di personalizzare in profondità il suo comportamento e l'esperienza d'uso. In ogni caso, quasi tutti i browser offrono opzioni e funzioni analoghe, almeno per le configurazioni di base. Cominciamo quindi a personalizzare le impostazioni di Firefox; da qualche settimana, l'interfaccia del browser di Mozilla è stata rivista in profondità, ma le opzioni sono rimaste invariate. Aprite il browser e raggiungete la pagina delle impostazioni, facendo clic sul pulsante hamburger in alto a destra e poi selezionando la voce *Impostazioni* nel menu a discesa. Aprite la sezione *Privacy e sicurezza* (*figura A*): per prima cosa, disattivate la telemetria, scorrendo la pagina fino alla sezione *Raccolta e utilizzo dati di Firefox* (*figura B*). Si possono disattivare senza timore tutte le opzioni eventualmente attive. All'inizio della pagina si trova invece la sezione *Privacy del browser*; selezionate l'opzione *Restrittiva* per garantire una protezione anti tracciamento più aggressiva; il browser sottolinea come alcuni siti potrebbero non funzionare correttamente, ma per risolvere eventuali incompatibilità basta aggiungere il sito problematico a una specifica whitelist: è sufficiente fare clic sull'icona a forma di scudo, a sinistra dell'indirizzo della pagina aperta, e disattivare la protezione anti tracciamento tramite lo switch (*figura C*).

Per quanto riguarda la sicurezza, la relativa sezione si trova in fondo alla pagina delle impostazioni: le opzioni offerte sono poche dal punto di vista numerico, ma piuttosto efficaci e soprattutto preconfigurate quasi sempre per garantire la massima protezione (*figura D*): il browser, infatti, blocca automaticamente i contenuti rischiosi e potenzialmente ingannevoli, ne impedisce il download e avvisa se si cerca di scaricare software poco diffuso. Inoltre, utilizza il protocollo Ocsp per verifica-









re la validità dei certificati. A questo proposito, in fondo alla pagina si trova un'opzione molto interessante, quella che forza l'utilizzo delle connessioni cifrate Https (qualora siano disponibili): è utile attivarla in tutte le finestre, modificando l'impostazione predefinita.

Sempre nella pagina *Privacy e sicurezza* delle impostazioni si può trovare anche l'opzione per inviare il segnale Do Not Track; questa funzione prevede la collaborazione dei server remoti, ma in genere è ignorata dalla grande maggioranza dei sistemi di tracking; non solo: poiché è un'opzione poco diffusa, può essere utilizzata come elemento per costruire un'impronta digitale unica dell'utente a partire dalla configurazione del suo sistema. Di conseguenza, molti esperti di privacy suggeriscono ora di mantenere l'impostazione predefinita e utilizzare strumenti proattivi per bloccare il tracciamento.

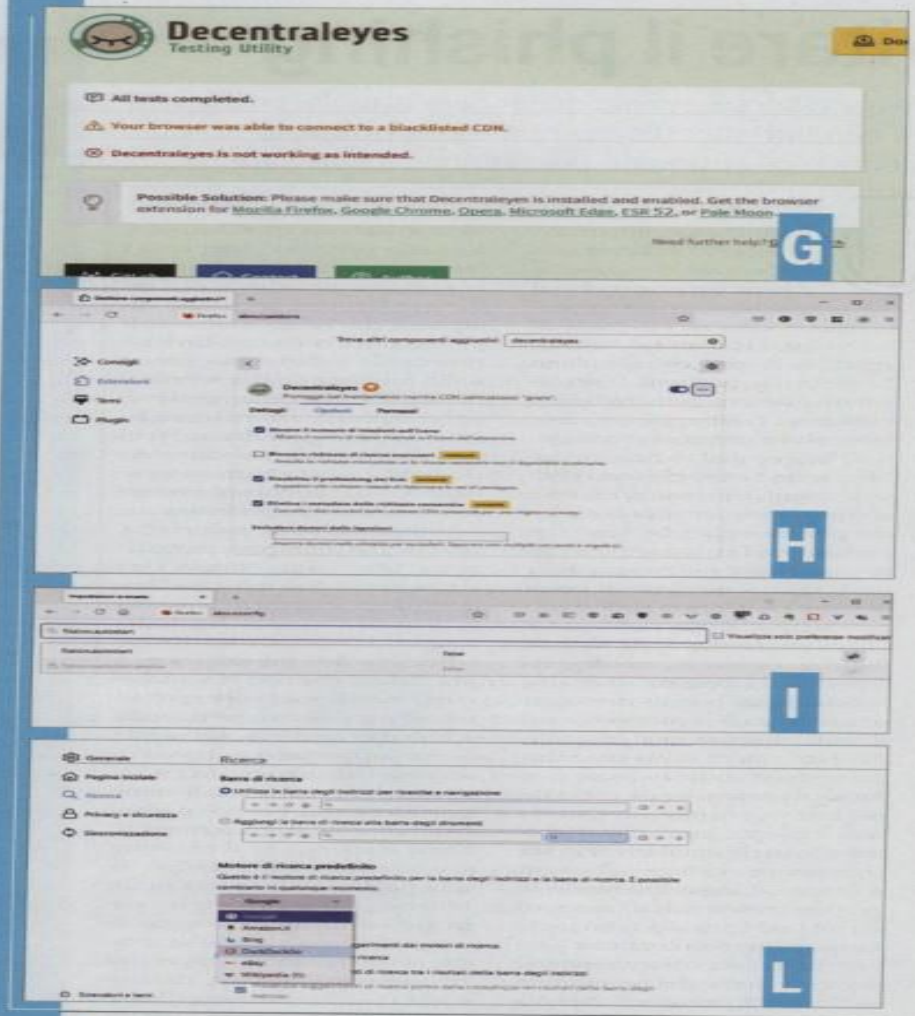
A questo proposito, una delle soluzioni più efficienti ed efficaci è uBlock Origin, un'estensione disponibile anche per molti altri browser, capace di bloccare sia le funzioni di tracciamento sia i messaggi pubblicitari; per installarla basta aprire la pagina delle estensioni (per esempio con la scorciatoia *Ctrl+Maiusc+A*), digitarne il nome nella casella di ricerca in alto a destra, selezionare il risultato desiderato e fare clic sul pulsante *Aggiungi a Firefox*. Una volta installata, l'estensione inizia subito a lavorare ed è preconfigurata in maniera piuttosto efficace. Si può comunque aprire la pagina di configurazione (basta fare clic sul pulsante aggiunto alla barra degli strumenti e poi sull'icona a forma di ingranaggi in basso a destra) per modificare qualche altra opzione: per esempio, nella scheda *Filtri di terze parti* si possono trovare altre liste interessanti (per esempio quelle destinate a specifici ambiti geografici) (*figura E*). Molto utili, e spesso trascurate, sono le opzioni offerte nel menu principale del tool (*figura F*): bisogna infatti fare clic su *Altro* per svelare alcuni pulsanti preziosi, che permettono di bloccare elementi specifici come i popup, i file multimediali di grandi dimensioni o addirittura il codice javascript.

Funzioni che in passato erano affidate a estensioni specifiche, come NoScript o HttpsAnywhere, sono oggi gestite direttamente da uBlock oppure dalle opzioni integrate nel browser; anche se le estensioni dedicate sono certamente più ricche, nella maggior parte dei casi si può evitare di appesantire il browser con l'installazione di molti strumenti di terze parti. Un tool potenzialmente piuttosto utile è invece Decentraleyes (*https://addons.mozilla.org/it/firefox/addon/decentraleyes*), un'estensione disponibile per tutti i principali browser (*figura G*) dedicata al blocco delle Cdn (Content Delivery Network), strumenti importanti per garantire l'accesso a contenuti Web in caso di traffico elevato, che però veicolano le richieste attraverso reti che possono carpire una grande quantità

di informazioni sull'utente. Molti grandi attori del Web (Google, Microsoft, Facebook e tanti altri) offrono funzioni Cdn gratuitamente (*figura H*), una proposta che potrebbe celare qualche secondo fine. Altre funzioni di protezione di Firefox, spesso ancora in fase di sviluppo, sono accessibili nella pagina delle impostazioni avanzate: per raggiungerla bisogna digitare la stringa *about:config* e poi fare clic sul pulsante *Accetta il rischio e continua*, per oltrepassare l'avviso che suggerisce di procedere con cautela nella modifica di questi parametri. Una funzione recente e molto interessante è il nuovo framework di isolamento dei siti chiamato Fission, che garantisce una maggiore separazione tra le diverse pagine aperte contemporaneamente: per attivarlo bisogna raggiungere la voce *fission.autostart* (basta digitarla nella casella di ricerca) e modificare il valore da *false* a *true* (*figura I*).

I più volenterosi possono anche disattivare il tracciamento geografico automatico tramite i server Google, digitando *geo.enable* e modificando il valore in *false*, e attivare le funzioni di offuscamento delle caratteristiche del sistema locale, che promettono di rendere la profilazione mediante impronta digitale molto più difficile; l'impostazione da modificare è *privacy.resistFingerprinting*. Queste ultime due modifiche potrebbero però avere qualche ripercussione sull'usabilità quotidiana del browser: i servizi Web potrebbero avere difficoltà a individuare correttamente la regione geografica oppure l'ora locale, causando malfunzionamenti per esempio nella gestione dei calendari.

L'ultima modifica, ma probabilmente la più importante, riguarda sia la configurazione del browser sia le abitudini dell'utente: cambiare le impostazioni, infatti, è quasi inutile se poi si continua a cadere tra le braccia dei servizi che vivono e prosperano grazie al tracciamento degli utenti, come Google oppure Facebook. Per questo è utile cambiare il motore di ricerca predefinito, scegliendo un servizio (come DuckDuckGo) più attento alla privacy dei suoi utenti: nella pagina delle impostazioni di Firefox basta raggiungere la sezione *Ricerca* e modificare la voce *Motore di ricerca predefinito* (*figura L*), scegliendo l'opzione preferita nella casella a discesa.

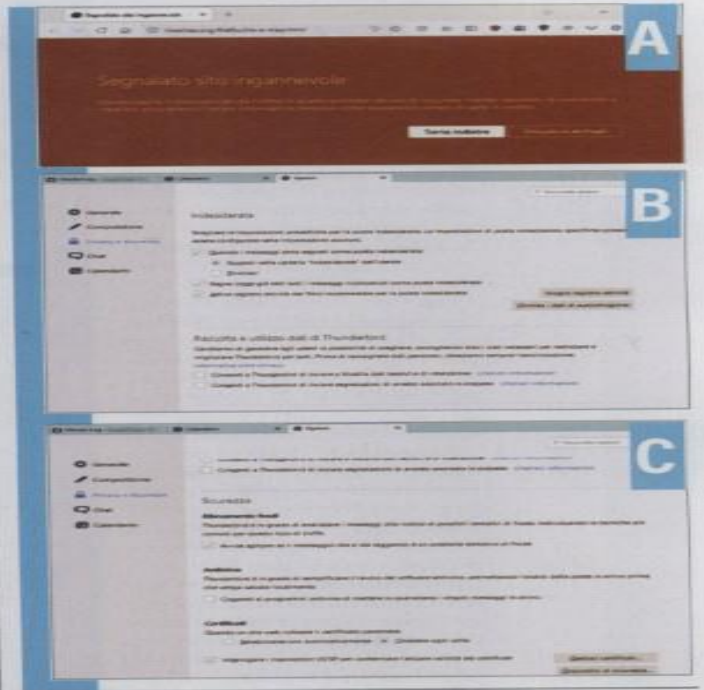


Evitare il phishing

Una minaccia tradizionale ma ancora attuale, può essere combattuta efficacemente con l'attenzione dell'utente e gli strumenti predefiniti dei software.

Un altro fattore importante e molto reclamizzato dalle suite di sicurezza è la protezione contro il phishing; evidentemente, nessun software è in grado di individuare in maniera "intelligente" le pagine che simulano l'aspetto e le funzioni di siti legittimi, e devono quindi affidarsi a soluzioni di filtraggio basate su liste e altri accorgimenti collegati all'analisi dell'indirizzo Url. Meccanismi analoghi sono però implementati in maniera nativa anche da molte applicazioni, come per esempio i browser (ne parliamo nel paragrafo dedicato alla privacy e sicurezza della navigazione) o i client di posta elettronica. L'unica differenza può riguardare la ricchezza e l'aggiornamento delle liste di indirizzi pericolosi, ma i test effettuati dai laboratori di analisi specializzati hanno mostrato una sostanziale equivalenza tra il livello di protezione garantito dai filtri offerti dalla maggior parte delle security suite e le funzioni native implementate nei browser (*figura A*). Questo non significa, però, che il phishing (ossia la simulazione di siti legittimi per indurre gli utenti a tentare il login inserendo le proprie credenziali di accesso) sia un problema del tutto risolto: questa tecnica continua a essere utilizzata correntemente, segno evidente che un numero sufficiente di navigatori abbocca ancora all'amo.

Per ridurre al minimo i rischi è opportuno innanzi tutto prestare molta attenzione: ogni volta che si apre una pagina Web in cui è presente un modulo di autenticazione è essenziale verificare che il nome di dominio corrisponda effettivamente a quello previsto (oggi tutti i browser principali evidenziano la porzione principale dell'indirizzo Url con un colore diverso) e che venga utilizzato il protocollo cifrato https. Un altro potenziale indizio può venire dalla funzione (o dal servizio) di compilazione delle password: se l'autocompilazione (che è legata a specifici indirizzi Web) non si attiva automaticamente, dovrebbe scattare un campanello d'allarme. Potrebbe essere solo una modifica perfettamente legittima alla struttura del sito, ma bisogna comunque procedere con la massima cautela. Una strategia che può mitigare l'impatto degli attacchi di phishing (e di molti altri rischi legati alla sicurezza delle password) è l'abilitazione dell'autenticazione a più fattori, che non ci stancheremo mai di suggerire specialmente per i servizi che custodiscono dati sensibili sull'utente o che supportano funzioni di acquisto (siti di commercio elettronico, servizi cruciali come provider email, per non parlare naturalmente degli account di home banking). Se il phishing si concretizza quasi sempre in una pagina Web aperta in un browser, l'attacco parte invece in genere da un messaggio di posta elettronica (anche se sempre sta diventando sempre più frequente lo Smishing, che usa come veicolo i messaggi Sms e i servizi di messaggistica istantanea). Anche su questo fronte, si possono implementare diverse strategie utili: in primo luogo, è essenziale attivare la funzione di protezione contro lo spam, che in genere integra anche regole ed euristiche pensate per individuare e filtrare automaticamente i tentativi di phishing (*figura B*). Queste funzioni sono attive quasi sempre per impostazione predefinita, ma è comunque prudente una verifica nelle impostazioni. In alcuni casi, il client potrebbe offrire anche impostazioni specifiche per individuare e contrassegnare i tentativi di frode e per interfacciarsi con i software antivirus: è il caso, per esempio, di Thunderbird, che propone queste impostazioni in fondo alla sezione *Privacy e sicurezza* nella pagina delle *Opzioni* (*figura C*). Una precauzione importante da prendere quando rimane qualche dubbio sulla legittimità di un messaggio è quella di evitare il clic diretto sul link proposto dal messaggio email.



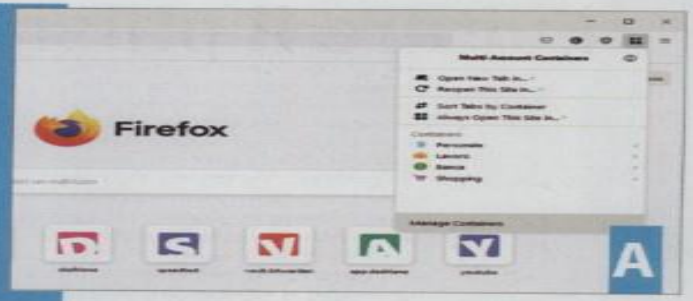
Browser sicuro per le transazioni

Un browser irrobustito con una configurazione di sicurezza più stringente e estensioni dedicate garantisce una maggiore sicurezza.

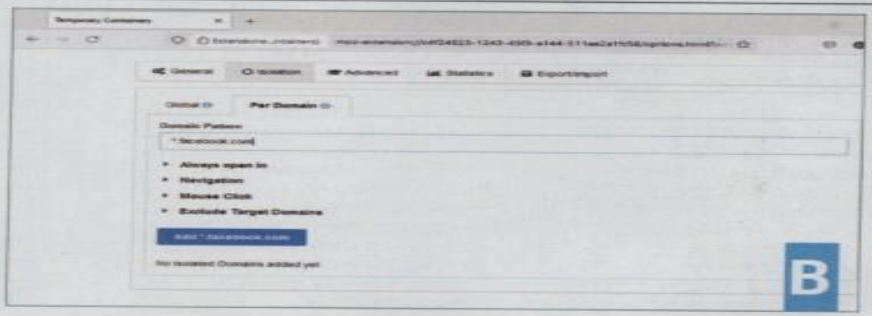
Se la sicurezza e la privacy sono importanti durante la navigazione quotidiana, diventano invece cruciali quando attraverso il browser si vogliono compiere operazioni delicate, come l'accesso a un sito di commercio elettronico, al portale della propria banca o all'estratto conto della carta di credito. Per compiere queste operazioni, molte security suite propongono uno strumento apposito, un browser dedicato capace di intervenire quando si cerca di raggiungere uno dei siti contenuti nella loro whitelist (o eventualmente aggiunto all'elenco dall'utente) per spostare la sessione in un ambiente potenzialmente più robusto e sicuro.

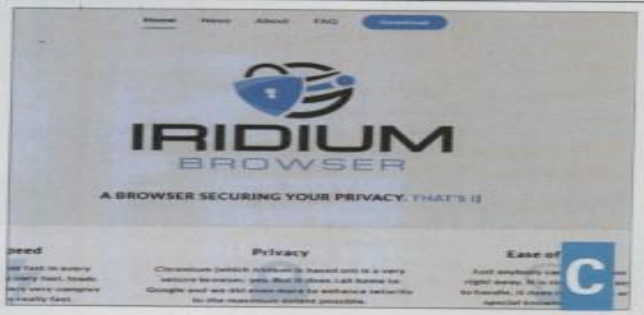
Premesso che un browser selezionato con attenzione, aggiornato e configurato opportunamente (si veda il paragrafo sulla privacy e sicurezza nella navigazione) può essere sufficiente per la grande maggioranza dei casi, questi strumenti possono offrire effettivamente qualche garanzia in più, poiché implementano in genere policy di sicurezza e configurazioni specifiche molto più stringenti, che causerebbero qualche difficoltà se utilizzate invece nella navigazione quotidiana.

Anche in questo caso, esistono strategie capaci di emulare alcune delle caratteristiche dei browser "sicuri" integrati nei prodotti di sicurezza. La soluzione più semplice e meno invasiva, dedicata agli utenti di Firefox, è sfruttare la tecnologia dei container, che permette di aprire siti Web specifici utilizzando un diverso set di credenziali, come se si trattasse di due profili distinti. Il metodo più semplice per attivare la funzione è installare le estensioni Multi Account Containers



e Temporary Containers La prima è un'estensione creata dalla stessa Mozilla Foundation che consente di creare spazi virtuali separati e isolati, per esempio dividendo la navigazione personale da quella lavorativa (*figura A*). Le diverse "personalità" sono contraddistinte da icone e sottolineate cromaticamente, rendendo piuttosto semplice l'individuazione rapida del profilo in uso. Non mancano neppure funzioni e voci di menu per aprire un collegamento o spostare una scheda attiva da un profilo all'altro. Temporary Containers, invece, estende la dotazione con strumenti per creare contenitori usa e getta, che si distruggono automaticamente alla fine della sessione di navigazione portando con sé tutte le informazioni





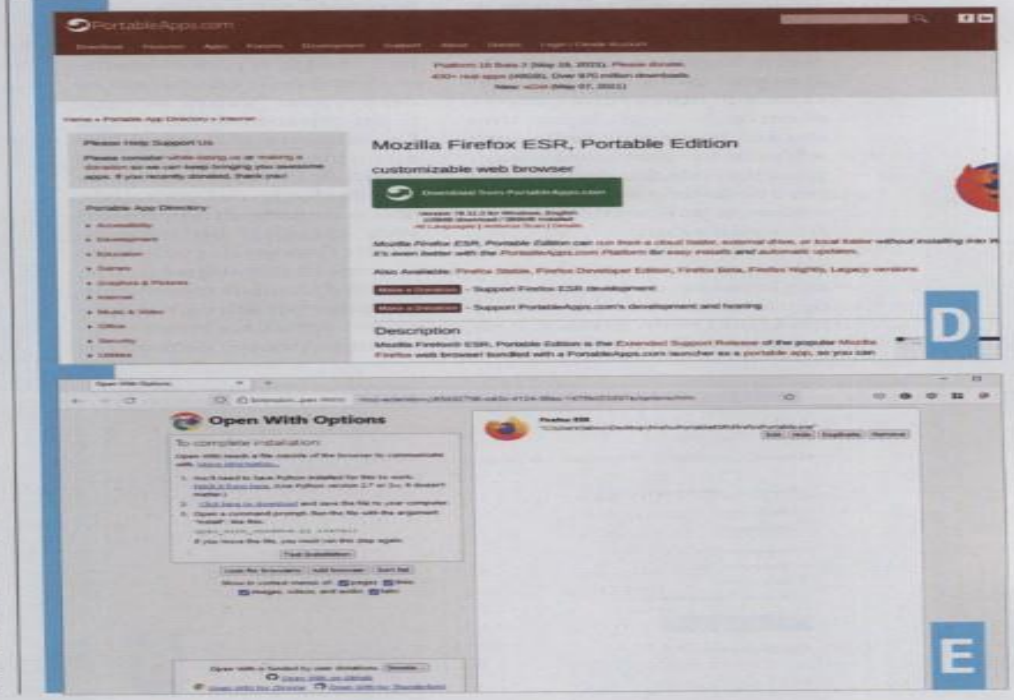
eventualmente memorizzate, come cookie e cronologia. Per automatizzare la creazione di un container temporaneo bisogna raggiungere le impostazioni dell'estensione; le opzioni sono molto ricche e richiedono qualche istante per districarsi tra i vari menu. Si può, per esempio, attivare una modalità automatica che crea un nuovo container per ogni scheda aperta, oppure decidere dopo quanto tempo eliminare le informazioni sulle sessioni chiuse (15 minuti per default).

Per collegare l'attivazione solo a specifici indirizzi Web bisogna raggiungere la sezione *Isolation*, aprire la scheda *Per Domain* e aggiungere alla lista il nome del dominio da individuare (si può anche inserire un pattern, come per esempio **.facebook.com*). Quando si cerca di raggiungere un indirizzo compreso nell'elenco, Firefox crea automaticamente un nuovo container (*figura B*).

Naturalmente, questa soluzione offre una protezione solo parziale; per ottenere una robustezza maggiore è opportuno creare una configurazione separata del browser, partendo dalle indicazioni offerte in questo stesso articolo e magari applicando impostazioni ancor più restrittive, bloccando gli script e cancellando automaticamente tutte le informazioni legate alla sessione di navigazione alla chiusura.

Esistono diversi browser alternativi, che assicurano una maggiore attenzione alla privacy e alla sicurezza dei loro utenti, ma è difficile consigliarne uno, per motivazioni di ordine diverso: innanzi tutto, se si sceglie un progetto completamente originale c'è il rischio di incontrare problemi di compatibilità con qualche sito. L'interfaccia e l'usabilità della maggior parte delle pagine Web viene infatti testata con i browser più comuni, e allontanandosi dalla massa cresce il rischio di trovarsi a utilizzare un software sicurissimo ma incompatibile. Esistono browser "irrobustiti" e basati su motori di rendering diffusi, come per esempio Iridium (*www.iridium.de*) (*figura C*); il progetto in sé è piuttosto interessante, ma passa comunque qualche settimana prima che le patch di sicurezza del progetto principale vengano integrate anche in queste varianti, con il risultato netto di esporre gli utenti a qualche rischio in più.

Una strada potrebbe essere quella di scegliere la versione portable di un browser comune (per esempio la variante Esr – con supporto esteso – di Firefox, scaricabile dalla pagina *https://portableapps.com/apps/internet/firefox-portable-esr*) (*figura D*) e aggiungervi le estensioni e le configurazioni opportune per garantire la massima sicurezza. Per passare facilmente dal browser quotidiano a quello robusto si possono utilizzare estensioni dedicate, come per esempio *Open With* per Firefox (*figura E*), che permette di configurare altri browser a cui inviare indirizzi Url e schede aperte; è però necessaria un'installazione attiva di Python, un requisito piuttosto comune nel mondo Linux che invece è molto meno frequente in ambito Windows. L'ambiente è comunque scaricabile e installabile gratuitamente, per chi volesse seguire fino in fondo questa strada.



Parental control

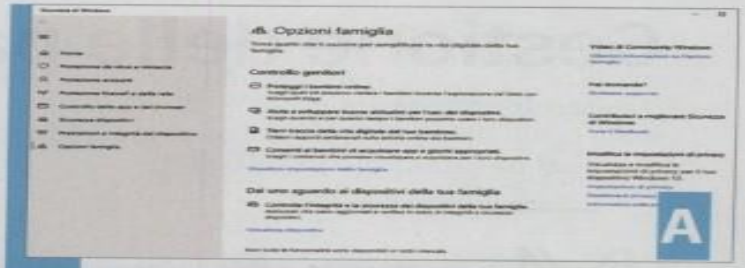
Gestire l'uso del computer da parte dei minori è un compito davvero difficile, ma Windows ha iniziato a integrare funzioni piuttosto interessanti.

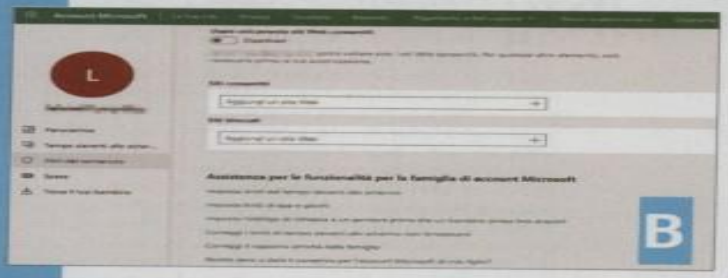
L'inclusione di strumenti di parental control nelle suite di sicurezza è da tempo oggetto di dibattito, con approcci molto vari da parte dei diversi produttori. Alcuni inseriscono queste funzioni direttamente nei pacchetti di sicurezza, specialmente nelle versioni più costose e complete, mentre altri preferiscono scorporare il prodotto per venderlo separatamente, poiché solo una parte dei clienti è interessata. A nostro parere, un prodotto di sicurezza che si proponga come soluzione "totale e completa" dovrebbe coprire anche questa esigenza.

In ogni caso, il problema della sicurezza (online e fisica) dei minori raccoglie un'attenzione e una consapevolezza crescente da parte dei genitori; questo è senz'altro un bene, poiché in passato si sono trascurati troppo a lungo, per ignoranza, sottovalutazione o semplice incompetenza tecnica, i potenziali rischi insiti nell'accesso dei minori a un universo di contatti e informazioni libere da qualsiasi controllo e vigilanza.

Il principale problema di tutti questi strumenti è la loro efficacia solo parziale: non si può pretendere che un software sia uno scudo capace di garantire contro qualsiasi contatto indesiderato, specialmente se poi si consente ai minori un accesso privo di vincoli e supervisione ai dispositivi informatici. Nonostante esistano in tutti i sistemi operativi moderni (e in molti software) strumenti e opzioni gratuite per migliorare la sicurezza dei minori in rete, i servizi di parental control commerciali hanno alcuni punti di forza difficili da eguagliare. In particolare, le soluzioni più evolute supportano tutti i principali ambienti software, desktop e mobile, e permettono quindi di creare policy che si estendono a tutti i dispositivi di ciascun utente, seguendolo negli spostamenti tra un ambiente e l'altro. La configurazione e la gestione centralizzata, spesso tramite un'interfaccia basata sul Web, sono altri vantaggi di questa organizzazione.

Chi non vuole sottoscrivere un abbonamento a un servizio di parental control commerciale ha comunque qualche freccia al suo arco; in particolare, può utilizzare le funzioni integrate in Windows 10, partendo dalla pagina *Account/Famiglia e altri utenti* dell'app Impostazioni *(figura A)*. È infatti cruciale che si crei un account separato per ciascun utente, tenendo quindi separati i documenti e le applicazioni di ognuno. Ormai da tempo, Windows 10 permette di creare nuovi utenti di tipo tradizionale *(Altri utenti)* oppure nuovi *Membri della famiglia*; ciascun utente di questo genere dev'essere collegato a un account Microsoft e può essere gestito da un'interfaccia basata sul Web che offre alcune funzioni piuttosto interessanti. Per esempio, si possono impostare limitazioni al tempo concesso davanti allo schermo, bloccare i contenuti inappropriati (in base alla fascia d'età), ricevere notifiche sulla posizione geografica e visualizzare rapporti sintetici sulle attività compiute da ciascun utente.





Queste funzioni rientrano sotto l'ombrello del servizio Microsoft Family Safety, raggiungibile anche via Web all'indirizzo *https://account.microsoft.com/family (figura B)*. Dopo aver completato l'autenticazione, si raggiunte una dashboard che consente di modificare le impostazioni di ogni membro, ad esempio limitando l'accesso ad applicazioni specifiche o filtrando i contenuti accessibili via Web. Il limite principale di questa soluzione è la copertura solo parziale, sia per quanto riguarda i sistemi operativi (il servizio è disponibile per Windows 10, Android e Xbox, lasciando invece del tutto scoperto il mondo Apple), sia soprattutto perché le funzioni di filtraggio dei contenuti sono implementate unicamente per il browser Microsoft Edge. Per garantire l'applicazione dei filtri, tutti gli altri browser sono automaticamente inseriti nella blacklist e non possono quindi essere utilizzati.

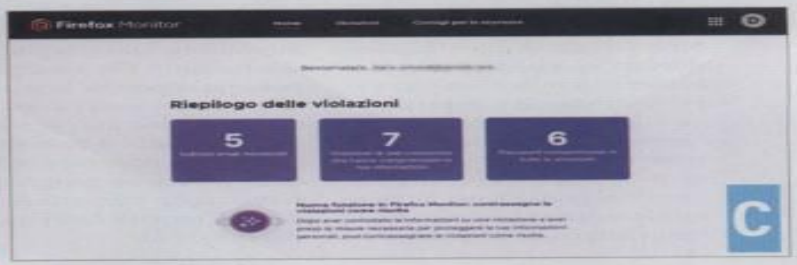
Gestione delle password

Uno strumento dedicato all'archiviazione sicura delle credenziali di login è ormai indispensabile per ogni navigatore e utente di Pc.

Mantenere l'ordine nell'archivio in continua crescita delle credenziali d'accesso ai siti Web, alle applicazioni e ai servizi è un compito quasi sempre impossibile da svolgere efficacemente in modo manuale. Una ricerca recente (commissionata però da un servizio di gestione delle password) sottolinea come un utente medio, senza allenamento specifico, possa memorizzare non più di 100 password. Secondo la nostra personale esperienza, questo numero potrebbe essere in realtà molto generoso, specialmente se si scelgono password complesse, casuali e quindi (si spera) più difficili da violare. Proprio per questo, è ormai indispensabile appoggiarsi a strumenti di memorizzazione esterni.

Molte security suite integrano funzioni di gestione delle credenziali di autenticazione, ma in questo caso chi decidesse di affidarsi invece a servizi e strumenti separati perderebbe davvero poco, e anzi in molti casi avrebbe soltanto da guadagnarci. I password manager integrati nei software di sicurezza offrono in genere un ambiente simile al resto della suite, ma dal punto di vista funzionale invece faticano a eguagliare la dotazione e l'efficacia dei migliori servizi dedicati. E se è vero che molti strumenti sono disponibili soltanto a pagamento (o con formule freemium piuttosto vincolanti), si segnalano invece diverse soluzioni efficaci, complete e gratuite. Abbiamo affrontato questo argomento diverse volte su *PC Professionale:* la comparativa più recente è stata pubblicata sul numero 351 (giugno 2020), e rimandiamo a quell'articolo per tutti gli approfondimenti. La soluzione più semplice, ma anche quella meno sicura, è utilizzare gli strumenti di sincronizzazione delle credenziali integrati direttamente nei browser. Se dal punto di vista funzionale sono molto efficaci (per lo meno finché non si passa da un browser all'altro, o si cerca di utilizzarli per le operazioni di autenticazione all'interno delle app e di altri software), i servizi integrati nel browser lasciano invece molti dubbi per quanto riguarda la sicurezza di queste importantissime informazioni personali. Per questo motivo, il nostro consiglio è quello di disattivare al più presto le funzioni "native" di gestione delle password, per affidarsi invece a un servizio o a un software specializzato.

La prima opzione da citare, la più matura ma anche la più rudimentale nell'integrazione con software e servizi di terze parti, è la famiglia di applicazioni Keepass, un progetto open source disponibile in diverse generazioni e più varianti. Quella più attiva sembra essere la versione KeepassXC (*https://keepassxc.*

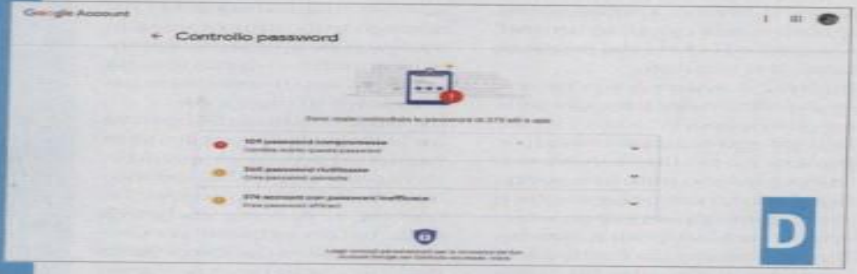


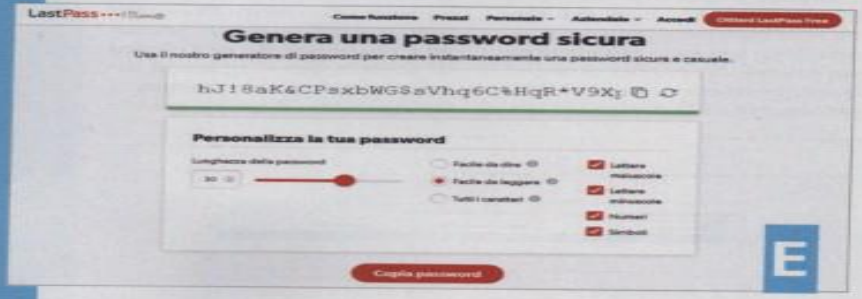
org), che offre un'ampia dotazione di funzioni e una discreta compatibilità. Questa soluzione mantiene in locale l'archivio delle credenziali, migliorandone la sicurezza ma rendendo inevitabilmente più complesse le operazioni di sincronizzazione e l'accesso da più dispositivi (bisogna lavorare di fantasia e appoggiarsi a qualche servizio di cloud storage).

Bitwarden *(https://bitwarden.com)* è invece un servizio cloud (anche se si può ospitare il server anche "on premises", su hardware personale) proposto con una formula freemium ragionevole, che consente un uso piuttosto efficace anche senza dover sottoscrivere alcun abbonamento. I prezzi sono comunque economici (10 dollari Usa all'anno per un utente premium, oppure 40 dollari per un account Family con un massimo di 6 utenti) e consentono di sfruttare tutte le funzioni avanzate, come l'autenticazione Totp, l'accesso di emergenza, il supporto a molti strumenti di autenticazione a due fattori e l'analisi dello stato di salute dell'archivio.

Per concludere questa rapida carrellata segnaliamo infine Myki *(https://myki.com)* *(figura A)*, un'interessante soluzione che non utilizza server remoti ma riesce comunque a garantire la sincronizzazione trasparente tra più dispositivi grazie all'uso intelligente dei device che più spesso sono accesi e connessi a Internet, come gli smartphone e i tablet. Anche Myki è gratuito per l'uso privato, ma alcune funzioni avanzate (per esempio i campi e le etichette personalizzate) possono essere sbloccate con acquisti in-app una tantum.

Indipendentemente dal particolare servizio di gestione delle password utilizzato, ci sono poi alcune funzioni e strumenti che possono tornare utili nel rapporto quotidiano con le informazioni di autenticazione. Innanzi tutto, è utile conoscere un servizio capace di segnalare il coinvolgimento del proprio account nelle sempre più frequenti violazioni degli archivi custoditi (male) dai più svariati siti e servizi Web: il primo punto di riferimento in questo settore è il sito *https://haveibeenpwned.com (figura B)*, che permette di verificare eventuali violazioni digitando il proprio indirizzo email o il numero di telefono (completo di prefisso internazionale). Questo sito funziona però su richiesta, e servono quindi visite periodiche per garantire un'informazione tempestiva. Per tenere sotto controllo indirizzi specifici si può invece sfruttare un tool come Firefox Monitor *(https://monitor.firefox.com)*, che si basa sullo stesso archivio di violazioni ma consente di aggiungere fino a un massimo di cinque account da monitorare *(figura C)*. Anche se non lo consigliamo in assoluto, chi utilizza il servizio di gestione delle password di Google (quello integrato in Chrome) può accedere a diverse funzioni interessanti per l'analisi del suo archivio di password: oltre a informazioni sugli account compromessi, che richiedono un intervento immediato per minimizzare i rischi, la dashboard (accessibile all'indirizzo *https://passwords.google.com/checkup*) segnala anche le password riutilizzate (che andrebbero sostituite per precauzione) e quelle inefficaci, perché troppo comuni o deboli. Pur non rappresentando un pericolo immediato, anche questi problemi andrebbero risolti quanto prima per minimizzare i rischi *(figura D)*. A questo proposito, può essere utile un servizio per creare password robuste: interessante è quello presente sul sito di Lastpass *(www.lastpass.com/it/password-generator)*, che offre un paio di opzioni interessanti per evitare i caratteri simili ed escludere quelli speciali *(figura E)*





Backup di sistema e documenti

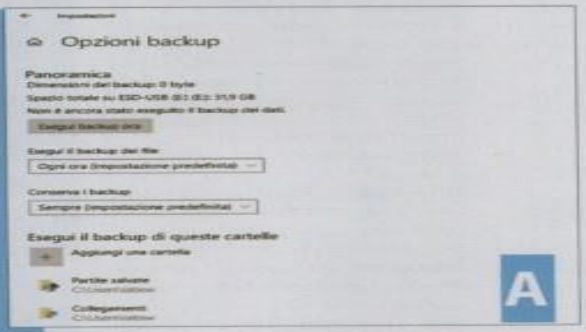
La crescita dei ransomware ha riportato al centro della scena il backup, una pratica essenziale in ambito It ma troppo spesso trascurata.

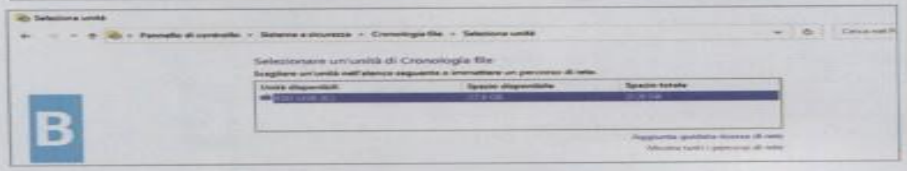
Quello del backup è un altro ambito in cui scegliere personalmente gli strumenti software offre grossi vantaggi rispetto alle funzioni integrate nelle security suite; proteggere i documenti personali e l'integrità complessiva del sistema rientra certamente nell'ambito della sicurezza, specialmente da quando l'ascesa dei ransomware ha reso la prevenzione l'unica strategia realmente efficace contro queste minacce. Nella maggioranza dei casi, però, le funzioni di backup integrate nelle security suite sono sufficienti, a volte discrete, ma quasi mai buone o ottime, specialmente se confrontate con gli strumenti e le opzioni offerte dai migliori strumenti dedicati.

Inoltre, il sistema operativo stesso offre molte funzioni utili a questo scopo: Windows 10, infatti, integra alcuni strumenti di protezione piuttosto avanzati, che richiedono però una specifica configurazione hardware e rimangono spesso sottotraccia, senza essere sfruttati a dovere.

Il primo passaggio è attivare la Cronologia file, una funzione integrata in Windows che salva automaticamente su un'unità disco separata più versioni successive di ogni documento: questo permette non soltanto di proteggere i file contro i crash, le sovrascritture e le cancellazioni accidentali, ma anche di ritornare sui propri passi in caso di modifiche errate. Come abbiamo già accennato, Cronologia file richiede una destinazione separata in cui memorizzare le versioni successive dei documenti: l'unità non deve essere dedicata unicamente a questo scopo, ma naturalmente questa funzione richiede parecchio spazio libero. Se collegare al computer un disco esterno è la soluzione più semplice, non è però l'unica: Cronologia file può infatti utilizzare come destinazione anche un percorso di rete locale. Per configurare questa funzione si può utilizzare sia la tradizionale interfaccia basata sul Pannello di controllo, sia la nuova app Impostazioni di Windows 10 (*figura A*).

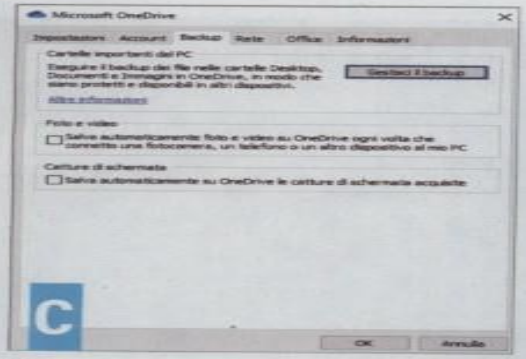
La suddivisione delle opzioni tra le due interfacce è un vero pasticcio, poiché alcune funzioni sono disponibili soltanto tramite Pannello di controllo, mentre altre sono esclusiva della nuova versione moderna. Se si passa dal Pannello di controllo (nella sezione *Sistema e sicurezza/Cronologia file*) si può trovare il collegamento *Seleziona unità* (*figura B*), nell'elenco di sinistra, per scegliere il disco di destinazione, mentre il collegamento *Aggiunta guidata risorse di rete*, in basso a destra, è perfetto per chi preferisce mantenere le informazioni di backup su un sistema separato. Questa opzione è disponibile soltanto nel Pannello di controllo, e non è invece replicata nell'app Impostazioni.

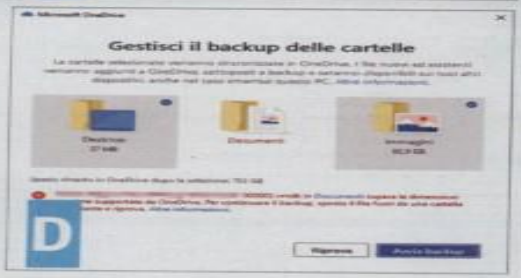


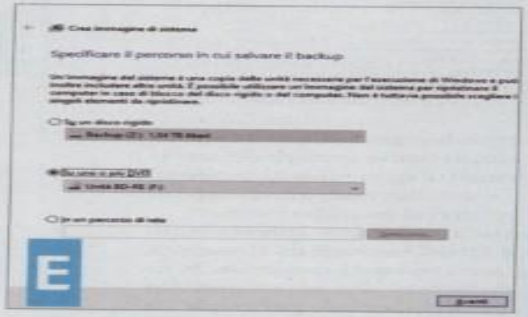


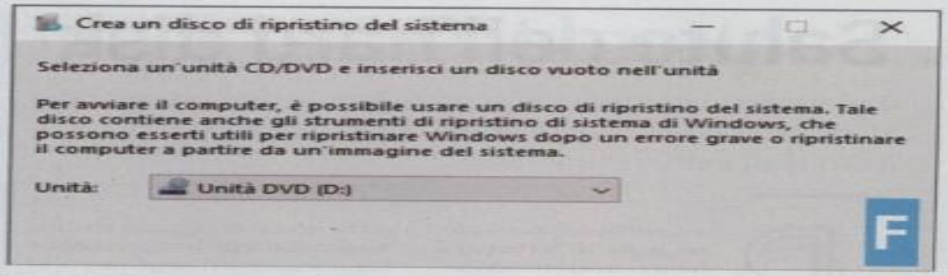
Per impostazione predefinita, Cronologia file protegge i contenuti delle cartelle personali dell'utente (Raccolte, Desktop, Contatti e Preferiti), ma si possono aggiungere anche altri percorsi locali. L'operazione deve però essere effettuata dalla nuova interfaccia; bisogna aprire le Impostazioni, raggiungere la sezione *Aggiornamento e sicurezza/Backup*, scorrere la pagina fino a *Backup con Cronologia file* e fare clic sul collegamento *Altre opzioni*. In questa pagina si trova l'elenco delle cartelle protette, che può essere ampliato facendo clic su *Aggiungi una cartella*. In modo simile, si possono anche escludere percorsi specifici per evitare il salvataggio di informazioni superflue.

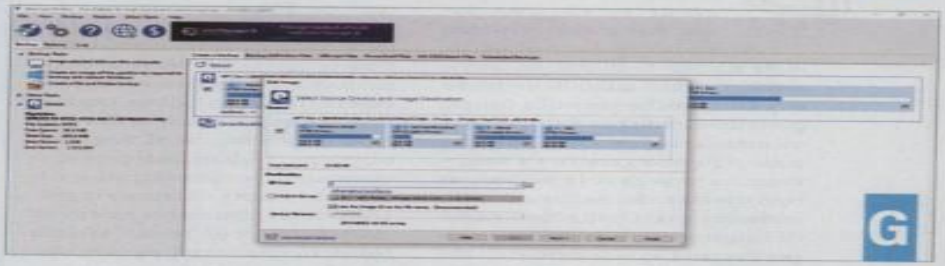
La protezione dei file tramite backup locale è la prima linea di difesa, ma certamente non l'unica. Da qualche anno, ormai, Microsoft suggerisce di abbinare il backup locale con quello remoto, grazie all'integrazione con il servizio di cloud storage OneDrive. Il client pro-











pone l'attivazione di questa funzione in diverse occasioni, ma anche chi ha declinato le offerte può facilmente tornare sui suoi passi: basta fare clic sull'icona di OneDrive, nell'area di notifica della barra delle applicazioni, selezionare *Impostazioni e guida/Impostazioni* per aprire la finestra delle opzioni (*figura C*). Al suo interno bisogna raggiungere la scheda *Backup* e poi fare clic su *Gestisci il backup* per aprire la finestra che consente di attivare le funzioni di backup automatico per il Desktop, i Documenti e le Immagini (*figura D*). Naturalmente, se il computer ospita molti documenti di grandi dimensioni lo spazio di archiviazione gratuito offerto a tutti gli utenti Microsoft (pari a 5 Gbyte) è piuttosto risicato. In questo caso, potrebbe essere utile restringere il campo a uno solo dei target supportati (per esempio i Documenti).

Windows 10 integra anche una funzione di backup dell'intero sistema, ereditata da Windows 7 e accessibile soltanto dal Pannello di controllo. Basta raggiungere la sezione *Sistema e sicurezza/Backup e ripristino (Windows 7)*, fare clic sul collegamento *Crea immagine di sistema* e impostare la destinazione, che può essere un disco rigido locale, un percorso di rete o un set di dischi ottici (*figura E*). Questa funzione ha il grande pregio di essere molto semplice e integrata direttamente nel sistema operativo, ma le opzioni disponibili sono davvero poche rispetto ai migliori software di questo settore (*figura F*). Poiché alcuni di questi software sono disponibili anche gratuitamente, il nostro consiglio è quello di utilizzare un software di terze parti (ne abbiamo parlato dettagliatamente nell'articolo sui software di backup pubblicato sul numero 360 di *PC Professionale*); in particolare, eccellente è la proposta di Macrium Reflect (*www.macrium.com*), un software di backup affidabile, potente e ricco di funzioni anche nella versione gratuita (*figura G*). L'offerta freemium esclude inevitabilmente alcune funzioni avanzate (in particolare la protezione contro il ransomware, il delta cloning e il supporto per le immagini incrementali), ma gli strumenti disponibili gratuitamente sono più che sufficienti per implementare un piano di backup personale efficace e affidabile.

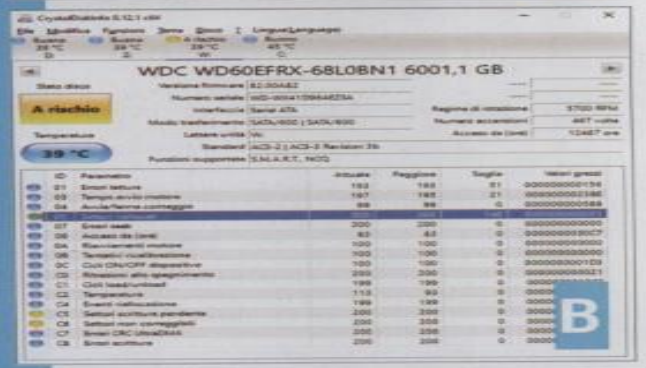
Salute dell'hard disk

Tenere sotto controllo lo stato di salute delle memorie di massa può prevenire crash disastrosi ed evitare perdite di dati irrecuperabili.

Da qualche tempo, alcune suite di sicurezza hanno iniziato a includere nella loro dotazione anche funzioni che analizzano lo stato di salute delle memorie di massa, avvisando l'utente quando un'unità mostra qualche segno di usura, probabilmente perché si sta avvicinando la fine della sua vita utile. Questo genere di informazioni non rientra nell'alveo tradizionale dei software antimalware, ma si tratta comunque di informazioni preziose, utili per l'utente a prescindere da chi le fornisce. La base di partenza in ogni caso sono i dati Smart (acronimo di *Self-Monitoring, Analysis and Reporting Technology*), informazioni diagnostiche memorizzate da tutte le unità disco ragionevolmente moderne (sia a stato solido sia a piatti magnetici) e accessibili via Api a qualsiasi software capace di supportare lo standard.

Il principale problema con questa tecnologia è che i valori cambiano radicalmente tra un produttore e l'altro, tra un modello e l'altro e a volte anche tra un esemplare e l'altro dello stesso modello (*figura A*). Per le applicazioni che leggono queste informazioni può quindi essere molto difficile ricavare con una singola lettura informazioni davvero affidabili sullo stato di salute di ogni unità; più semplice, invece, è confrontare lo stato attuale con quelli precedenti, per evidenziare tendenze specifiche come l'aumento del numero di settori riallocati oppure un degrado delle prestazioni, segnali che possono far presagire un guasto imminente. Inoltre, il protocollo Smart permette anche di eseguire routine diagnostiche di durata variabile per ricercare attivamente eventuali problemi.

Le funzioni di analisi integrate nelle security suite non sono in genere particolarmente avanzate, ma hanno il grande pregio di essere (di solito) attive per default e sempre in attesa di eventuali problemi. Se si vogliono ottenere risultati analoghi con strumenti personalizzati è necessario un po' di lavoro in più. Uno degli strumenti storici di questo settore è CrystalDiskInfo (*https://crystalmark.info/en/software/crystaldiskinfo*), scaricabile gratuitamente in diverse versioni (cambia solo l'aspetto estetico), sia in formato installabile sia come archivio portable. Il programma è compattissimo (l'eseguibile occupa meno di 3 Mbyte sull'hard disk, mentre il processo supera di poco i 5 Mbyte in memoria) e mostra in maniera piuttosto completa tutti i principali parametri di ogni unità installata (*figura B*). Come abbiamo già accennato, per ottenere la massima protezione è utile mantenere il programma sempre attivo in background, così da rilevare eventuali variazioni nei parametri misurati; per ottenere questo risultato basta selezionare *Funzioni/Esegui all'avvio di Windows* nel menu principale. Per default, il programma emette un avviso acustico in caso di problemi; si può invece configurarlo per inviare messaggi diagnostici via email (una soluzione molto utile, in particolare, per il monitoraggio remoto dei sistemi) selezionando *Funzioni/Funzioni allerta/Mail avviso*. Perché l'invio dei messaggi si completi con successo, però, bisogna richiamare la finestra di configurazione del server email (*Funzioni/Funzioni allerta/Impostazioni mail*) e inserire i dati relativi al provider Smtp.



Un'alternativa interessante è DiskCheckup di Passmark (*www.passmark.com/products/diskcheckup*), che però è gratuito soltanto per uso personale (la versione commerciale costa 27 dollari Usa). Questo programma offre un'interfaccia più semplice e intuitiva rispetto a CrystalDiskInfo e permette di avviare facilmente i test diagnostici Smart, sia quello breve sia quello esteso. Anche in questo caso, si può configurare il tool per inviare notifiche via email in caso di problemi.

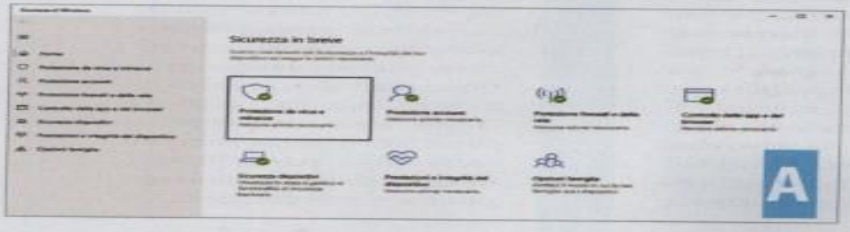
Controllo della configurazione del Pc

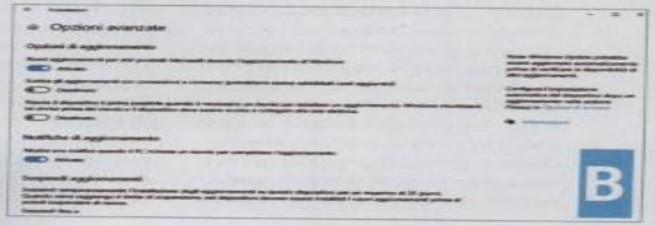
Basta un errore nella configurazione del computer o un'applicazione non aggiornata per vanificare tutte le precauzioni prese per la sicurezza del Pc.

Un settore in cui le migliori security suite offrono un vantaggio significativo rispetto a qualsiasi soluzione fai-da-te è l'analisi complessiva del livello di sicurezza garantito dal sistema in cui sono installate; ma gli strumenti predefiniti di Windows sono migliorati negli ultimi anni e offrono molte informazioni utili (se si sa dove cercare). Il punto di partenza principale è la finestra Sicurezza di Windows, che può essere richiamata con un semplice doppio clic sulla sua icona (a forma di scudo) nell'area di notifica della barra delle applicazioni (*figura A*). Se non dovesse essere disponibile (ad esempio perché si è installato un antivirus di terze parti) basta comunque digitare *sicurezza di windows* nella casella di ricerca per individuare rapidamente lo strumento. La pagina Home mostra un riepilogo del livello di protezione del sistema del tutto analogo a quelli offerti dagli antivirus di terze parti; in caso di problemi, icone colorate attireranno l'attenzione dell'utente e permetteranno di prendere gli opportuni provvedimenti per migliorare il livello di protezione. Per garantire la sicurezza del computer è essenziale assicurarsi che tutti i software installati (a partire dal sistema operativo) siano aggiornati alle versioni più recenti, e in particolare che tutte le patch di sicurezza vengano correttamente scaricate e installate non appena disponibili. È quindi opportuno raggiungere le Impostazioni, aprire la pagina *Aggiornamento e sicurezza/Windows Update*, fare clic sul pulsante *Opzioni avanzate* e verificare la configurazione, per esempio includendo gli aggiornamenti relativi ad altri prodotti Microsoft e attivando le notifiche relative alla presenza di aggiornamenti che richiedono un riavvio del computer (*figura B*).

Oltre al sistema operativo, è essenziale occuparsi anche dell'aggiornamento di tutte le applicazioni installate; questo può essere un problema banale o molto difficile da risolvere, a seconda delle proprie abitudini e dei software utilizzati. Per la minoranza che utilizza prevalentemente o esclusivamente i software scaricati dal Microsoft Store, gli aggiornamenti possono essere facilmente automatizzati: basta aprire lo Store, richiamare le *Impostazioni* dal menu associato all'icona con i tre puntini, in alto a destra, e verificare che sia attivata l'opzione *Aggiorna le app automaticamente*. Per forzare una verifica basta fare clic su *Download e aggiornamenti* (sempre nel menu principale) e poi sul pulsante *Recupera aggiornamenti*.

I problemi iniziano quando invece si installano software provenienti da altre fonti; nella migliore delle ipotesi, ogni programma integra la sua funzione di verifica e applicazione degli aggiornamenti, che in genere viene però richiamata soltanto all'esecuzione. Per evitare di dover passare in rassegna tutti i software installati alla ricerca di eventuali update, può essere utile installare uno strumento come Sumo (*https://www.kcsoftwares.com/?sumo*), che analizza la configurazione del sistema, individua la gran parte dei software installati e segnala la presenza di nuove release. Molto più efficace, ma più laboriosa da implementare, è l'installazione di un packet manager centralizzato in stile Linux; in attesa che maturi la proposta di Microsoft (Windows Package Manager, attualmente disponibile all'indirizzo *https://github.com/microsoft/winget-cli*), la soluzione più ricca ed efficace rimane Chocolatey (*https://chocolatey.org*), a cui abbiamo dedicato un approfondimento sul numero 331 di *PC Professionale*.



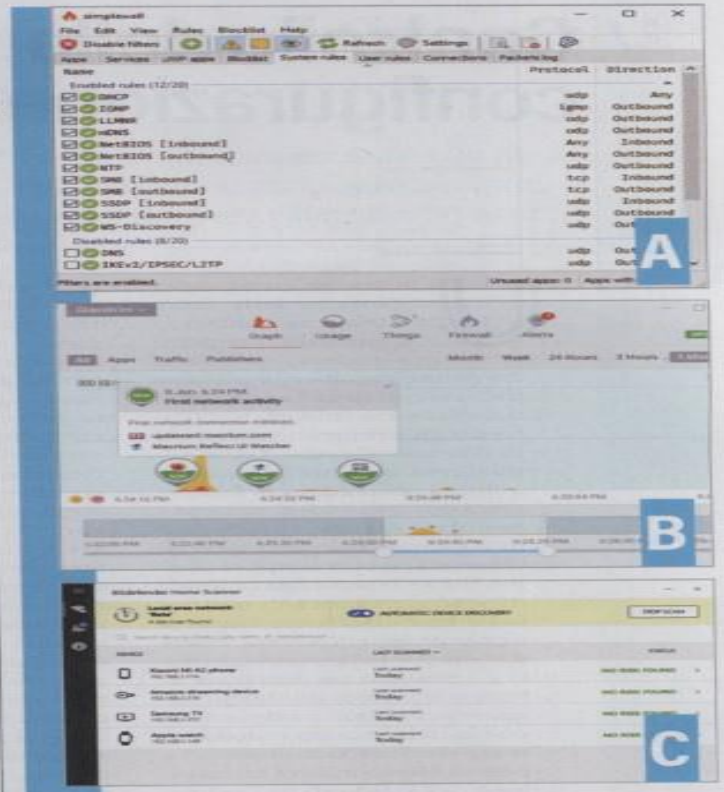


Accesso a internet e stato della rete locale

La sicurezza informatica non è più limitata al perimetro del computer, ma deve considerare anche molti altri dispositivi connessi alla rete locale.

Sempre più spesso la sicurezza informatica non inizia e finisce sui computer, ma coinvolge anche numerosissimi dispositivi di varia natura, dalle console per videogiochi ai televisori smart, dalle lampadine intelligenti agli assistenti vocali. Tenere sotto controllo il livello di sicurezza di tutti questi dispositivi può essere un vero problema, poiché nella maggior parte dei casi gli utenti comuni non hanno alcuna informazione sullo stato di ogni device e sui potenziali pericoli.

Per quanto riguarda l'analisi delle comunicazioni da e verso il computer, il firewall integrato in Windows offre da molti anni livelli di protezione e flessibilità tali che molti produttori di software di sicurezza hanno ormai rinunciato a sviluppare sostituiti, modificando invece le impostazioni e l'interfaccia delle funzioni native del sistema operativo. In effetti, l'interfaccia del firewall nativo è piuttosto complessa da utilizzare e si trova nascosta nei meandri delle opzioni di configurazione di Windows; in molti casi la configurazione predefinita è perfettamente efficace e non richiede quindi alcuna modifica, ma se invece è necessario cambiare qualche parametro o aggiungere una nuova regola potrebbe rivelarsi prezioso un software come Simplewall (*www.henrypp.org/product/simplewall*), pensato proprio per offrire un'interfaccia più semplice da utilizzare e veloce da raggiungere (*figura A*) per modificare le impostazioni di Windows. Quando invece l'oggetto delle attenzioni non è il computer ma gli altri elementi della rete locale, l'offerta si fa molto più povera: sono infatti disponibili moltissimi strumenti pensati per gli esperti e per le reti aziendali, mentre gli strumenti dedicati alle reti domestiche sono pochi e spesso poco interessanti. Un'eccezione potrebbe essere Glasswire (*www.glasswire.com*), un firewall con funzioni di analisi della rete locale caratterizzato da un'interfaccia molto gradevole, un'ottima usabilità e funzioni piuttosto complete (*figura B*). La versione gratuita soffre però di alcune limitazioni piuttosto significative, mentre quelle commerciali hanno prezzi elevati e sono proposte soltanto in abbonamento (a partire da 39 dollari Usa all'anno). Chi volesse semplicemente tenere sotto controllo lo stato della rete locale potrebbe provare Bitdefender Home Scanner (*www.bitdefender.com/solutions/home-scanner.html*), un software offerto gratuitamente dal noto produttore di soluzioni di sicurezza. Come il nome lascia chiaramente intendere, il suo scopo è analizzare la rete locale per evidenziare problemi di sicurezza o nuove connessioni potenzialmente indesiderate. Una volta completata l'installazione, il tool richiede la creazione di un account Bitdefender, dopodiché inizia ad analizzare i dispositivi connessi alla rete locale, evidenziando poi eventuali problemi (*figura C*). Durante le nostre prove, dopo qualche minuto è partita automaticamente anche l'installazione dell'antivirus Bitdefender, che abbiamo dovuto interrompere a mano. Dopo aver completato l'analisi (che potrebbe richiedere anche parecchi minuti, specialmente nel caso di reti molto popolose), il tool offre una panoramica sullo stato della sicurezza della rete; le informazioni raccolte possono essere piuttosto utili per individuare eventuali punti deboli, mentre i suggerimenti offerti lo sono molto meno: in tutti i casi, infatti, il tool ha proposto l'acquisto del Bitdefender Box, un'appliance di sicurezza da aggiungere alla rete locale.



Virtual Private Network

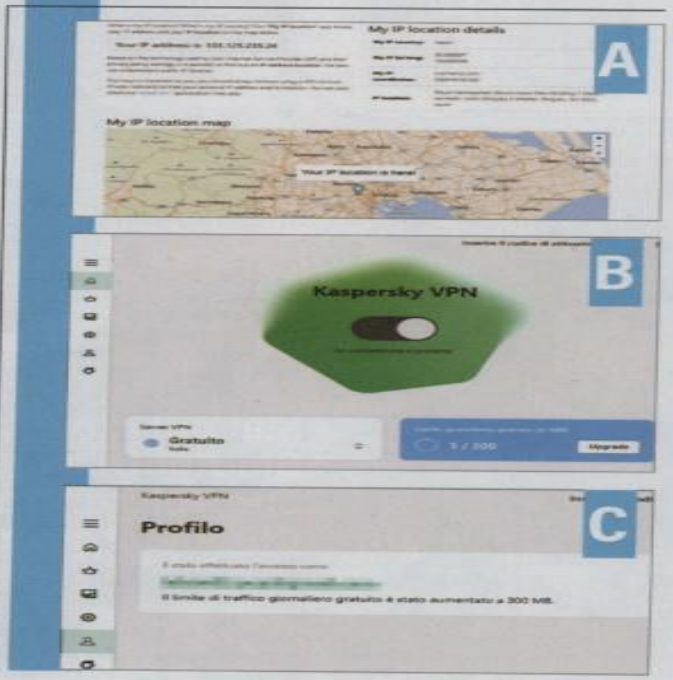
Un servizio Vpn può essere un alleato prezioso per garantire la privacy della navigazione.

Le reti Vpn possono essere utili in moltissime situazioni e rappresentano un'arma importante nell'arsenale degli strumenti di sicurezza per i computer e gli altri dispositivi informatici. Questa tecnologia consente di creare tunnel cifrati tra due punti di Internet, per instaurare una comunicazione privata e sicura anche se non ci si trova fisicamente connessi alla stessa rete locale. Le Vpn sono quindi preziose per collegarsi da casa alla rete aziendale, oppure per effettuare l'accesso ai dispositivi della Lan domestica quando ci si trova fuori case (ad esempio in viaggio).

Quando si menziona la Vpn tra le funzioni dei prodotti di sicurezza, ci si riferisce ai servizi che offrono una connessione sicura a un gran numero di server distribuiti geograficamente nel modo più uniforme possibile. Questi servizi permettono ad esempio di proteggere la propria connessione quando si usa una rete locale non affidabile (come quella di un albergo o di un locale pubblico) per effettuare operazioni delicate come l'accesso al proprio conto corrente online. Oppure possono essere utilizzate per simulare la connessione da aree geografiche diverse da quella attuale (*figura A*), ad esempio per aggirare i blocchi all'accesso ad alcuni servizi (si pensi, per esempio, ai siti e alle applicazioni di streaming video, spesso vincolate da licenze che consentono la trasmissione solo entro i confini nazionali). Infine, le Vpn possono rappresentare l'unica soluzione per connettersi liberamente a Internet e per comunicare con l'esterno per chi si trova a vivere in Paesi che censurano e controllano l'accesso alla Rete.

In questo campo, l'offerta delle principali suite di sicurezza è in realtà piuttosto deludente: anche i pacchetti più ricchi e costosi, spesso proposti con denominazioni come "total" o "complete" che lasciano presupporre una dotazione senza limitazioni, in realtà integrano soltanto versioni ridotte delle offerte Vpn illimitate, disponibili in genere solo con un abbonamento separato. Questo è un difetto grave quando si paga magari oltre 100 euro all'anno per una suite di sicurezza, ma invece è un vincolo perfettamente accettabile per chi utilizza un accesso gratuito. Diversi servizi, infatti, offrono account gratuiti con soglie di traffico giornaliero o mensile, spesso accompagnate da un limite alla velocità raggiungibile o al numero di server utilizzabili. Il primo servizio da segnalare è ProtonVPN (*https://protonvpn.com*), uno dei pochissimi a non imporre limitazioni di traffico per gli utenti gratuiti; naturalmente qualche vincolo è comunque presente, e riguarda i server raggiungibili (in sole tre nazioni invece delle 55 supportate dalla versione Plus, che costa 8 euro al mese), la velocità della comunicazione e l'assenza di alcune funzioni avanzate, come il supporto ai servizi di streaming e al traffico peer to peer o il blocco automatico delle pubblicità. Nonostante queste limitazioni, il servizio è comunque perfettamente ad+atto a proteggere le comunicazioni quando ci si trova a dover utilizzare una rete WiFi non affidabile, il caso più rilevante dal punto di vista della sicurezza.

Segnaliamo anche l'offerta di Kaspersky, che propone il servizio Secure Connection (*www.kaspersky.it/vpn-secure-connection*) con un'offerta analoga a quella inclusa nelle suite di sicurezza dell'azienda (*figura B*). Per ottenere un servizio completo e illimitato, infatti, bisogna comunque sottoscrivere un abbonamento separato, a un prezzo per la verità piuttosto conveniente: 29,99 euro all'anno per cinque dispositivi. In alternativa si può sfruttare l'accesso gratuito, con connessione automatica al server più vicino (senza quindi poter scegliere la posizione geografica di uscita su Internet) e limitato a 200 Mbyte di traffico al giorno, che possono crescere fino a 300 Mbyte creando un account gratuito My Kaspersky (*figura C*). Anche in questo caso, quindi, le funzioni più evolute dei servizi Vpn (come il mascheramento della posizione geografica) non sono disponibili, ma il limite di traffico è piuttosto generoso per chi vuole semplicemente collegarsi a Internet senza troppe preoccupazioni quando si trova fuori casa. •



Di Alfonso Maruccia

ANTIVIRUS GRATUITI

I MIGLIORI SULLA PIAZZA

Il mercato dei software antivirali offre come sempre ampie opportunità di scelta. L'antivirus continua a essere uno strumento di protezione indispensabile, ma con le soluzioni gratuite non è necessario spendere soldi per navigare in sicurezza.

PER QUEL CHE CONCERNE LA SICUREZZA INFORMATICA E I RISCHI A CUI SONO SOTTOPOSTI GLI UTENTI, LO SCENARIO TECNOLOGICO MODERNO È A DIR POCO IRRICONOSCIBILE ANCHE SOLO RISPETTO AD ALCUNI ANNI FA. OGGI I DATI RAPPRESENTANO IL BERSAGLIO PRIVILEGIATO DI CYBER-CRIMINALI IMPEGNATI A GESTIRE DELLE VERE E PROPRIE PIATTAFORME MALEVOLE, MENTRE IL MERCATO DEI MALWARE HA ABBANDONATO DEFINITIVAMENTE L'APPROCCIO DILETTANTESCO E "IDEOLOGICO" PER RAGGIUNGERE LE DIMENSIONI DI UN BUSINESS MULTI-MILIARDARIO. IL RANSOMWARE PENETRA NEI SISTEMI DI AZIENDE E SOGGETTI "SENSIBILI", PRENDE IN OSTAGGIO I FILE E POI CHIEDE IL PAGAMENTO DI UN RISCATTO IN CRIPTOMONETA PER EVITARE CONSEGUENZE POTENZIALMENTE DISASTROSE PER LE ORGANIZZAZIONI COLPITE.

In una situazione del genere, tutto lascerebbe supporre la necessità di investire ingenti risorse economiche (e non solo) per blindare le porte di accesso ai Pc domestici e alle reti aziendali. Nei casi maggiormente strutturati e nelle realtà economiche più significative ciò è certamente vero – o dovrebbe essere vero – mentre per i sistemi individuali o le reti meno complesse è ancora possibile risparmiare parecchio adottando una soluzione difensiva dal costo iniziale praticamente imbattibile: zero. Un buon antivirus gratuito, oggi come in passato, può essere un ottimo compagno di viaggio in grado di facilitare la navigazione tranquilla in Rete e nel nostro *mare magnum* digitale. Un primo scudo indispensabile da frapporre tra il Pc (o i Pc) e i pericoli provenienti da Internet, un involucro protettivo con cui tenere al riparo i dati sensibili di basso o anche medio livello da ransomware, malware, virus, falle *0-day* e altri detestabili esponenti dell'affollato bestiario cyber-criminale contemporaneo.

I molti contro di Windows Defender

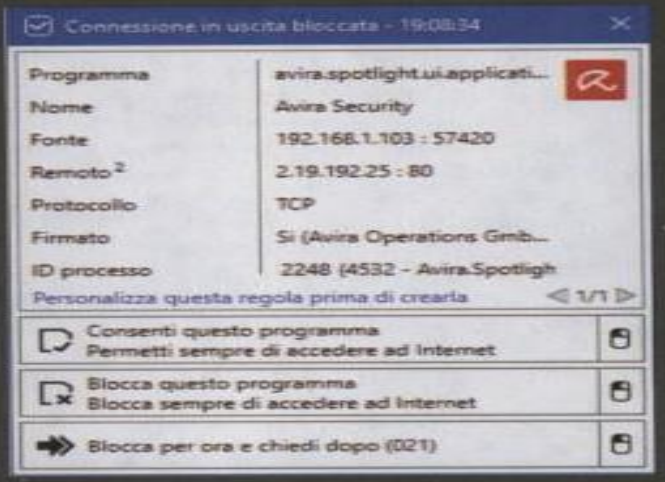
Noto inizialmente come *Microsoft AntiSpyware*, Windows Defender è diventato parte integrante dei sistemi operativi Windows a partire dal 2006, assieme a Windows Vista. Quello che in origine era uno strumento progettato esclusivamente per combattere spyware e adware si è alla fine trasformato in una soluzione antimalware a tutto tondo, ed è oggi parte integrante di Windows 10 con il nome di *Microsoft Defender Antivirus* o anche *Windows Defender Antivirus*. Defender, in buona sostanza, è l'antivirus nativo della moderna generazione di OS Windows, con buona pace delle polemiche e delle previsioni di chi, negli anni scorsi, preannunciava la morte del mercato degli antivirus commerciali a causa del nuovo (ennesimo) approccio monopolistico dell'azienda di Redmond.

Ovviamente, le cose non sono andate così e Defender non ha "ammazzato" alcunché: l'antivirus nativo di Windows offre certamente una protezione di base decente, ma l'utente medio che usa il Pc con una certa costanza farebbe bene a considerare l'adozione di una soluzione di terze parti. Gli antivirus "alternativi" sono ancora in circolazione, anzi il mercato della sicurezza è a dir poco prospero a causa delle minacce informatiche sempre più virulente, pericolose e tecnologicamente sofisticate. Secondo *AV-Test*, Windows Defender fa un lavoro "eccellente" nella protezione contro le falle 0-day e i malware più recenti (a giugno 2021), mentre *AV-Comparatives* è decisamente meno indulgente assegnando all'antivirus di Microsoft una

capacità di identificazione dei malware "offline" a dir poco mediocre (54,8%) contro una protezione online che si avvicina al 100% (test di marzo 2021). Livello di protezione a parte, Defender ha la spiccata tendenza a interferire con le attività dell'utente riconoscendo come potenzialmente "pericolosi" (e mettendo immediatamente in quarantena) programmi assolutamente legittimi, modifiche al Registro di Windows o al file *hosts* apportate manualmente dall'utente e altri file sicuri scaricati da Internet.
Nella nostra esperienza personale e nell'opinione comune di molti forum di discussione in Rete, Defender è a dir poco "impiccione" e produce con una certa regolarità un numero eccessivo di falsi positivi durante le sue scansioni in tempo reale. L'idea che, secondo Microsoft, l'uso di un antivirus esterno peggiori la sicurezza di Windows aumentando la cosiddetta "superficie di attacco" è stata poi resa obsoleta dai fatti: ormai non passa mese che Microsoft non sia costretta a correggere gravissime vulnerabilità di sicurezza in Defender, con patch correttive pensate per neutralizzare falle 0-day, bug e difetti nel codice in grado di esporre a grandissimi rischi il Pc, i dati degli utenti o Windows stesso. Non aiuta, infine, il fatto che la natura "integrata" dell'antivirus (e la conseguente "liquefazione" dell'interfaccia di controllo all'interno delle caotiche Impostazioni di Windows 10) abbia reso meno agevole l'utilizzo delle opzioni avanzate. Per tutti questi motivi, e magari perché non vogliamo dipendere dai server remoti e dagli onnipresenti servizi di Microsoft anche quando si tratta di difenderci dalle minacce informatiche e dai rischi del Web, la scelta e l'adozione in pianta stabile di un antivirus di terze parti ci offre l'opportunità concreta di migliorare la nostra vita e il nostro business digitali. Una scelta che nel corso delle

Antivirus free, ma con benefici

Come spieghiamo nel corso dell'articolo, un antivirus gratuito dotato di engine di protezione in tempo reale continua a offrire quell'indispensabile "prima linea" difensiva contro malware, ransomware e attacchi locali o provenienti da remoto. Vista la gratuità dell'offerta, è altrettanto pacifico immaginare che una protezione di buona qualità necessiti anche di qualche strumento aggiuntivo, con soluzioni in grado di migliorare e integrare la protezione di base dell'antivirus offrendo una superficie di attacco ulteriormente ridotta per gli sporchi affari di *cracker* e cyber-criminali. Ecco quali sono le altre armi di difesa che potete mettere in campo.



Windows Firewall Control è indispensabile per prendere il pieno controllo del firewall nativo di Windows. Tutte le connessioni esterne sono bloccate senza il nostro permesso.

Windows Firewall Control

Per tenere a bada i malware e assicurarsi che i criminali non trasformino la nostra postazione in un Pc zombi assimilato a una botnet, è indispensabile sfruttare a fondo la tecnologia *Windows Filtering Platform* (WFP) alla base del firewall di Windows. Una *applet* gratuita come *Windows Firewall Control* (*binisoft.org/wfc*) è in tal senso l'ideale, visto che sfrutta il suddetto firewall di base migliorandone le capacità e le possibilità di controllo da parte dell'utente. In particolare, grazie a WFC verremo allertati a ogni tentativo di accesso a Internet da parte di nuovi programmi e processi (e di Windows stesso), così da accorgerci immediatamente del fatto che un programma non identificato e potenzialmente malevolo sta cercando di "chiamare casa" per ricevere istruzioni dai server remoti in mano ai criminali (su *PC Professionale* n. 334, gennaio 2019, trovate un articolo dedicato proprio a Windows Firewall Controll).

Sandbox

WFC è utilissimo per cogliere sul fatto i tentativi di comunicazione remota sconosciuti o non autorizzati, ma la soluzione ideale sarebbe evitare del tutto l'arrivo di un malware sul sistema o la diffusione di

un'infezione a opera di un *trojan* camuffato sotto mentite spoglie. Lasciando da parte le virtual machine complete vista la loro complessità di setup e gestione, una strada intermedia tra la virtualizzazione e la censura totale è rappresentata dalla tecnologia delle *sandbox*. Una sandbox permette l'accesso in lettura dei file e delle risorse di sistema da parte dei programmi sconosciuti avviati al suo interno, ma rende le operazioni di scrittura temporanee eliminando tutte le modifiche al sistema alla chiusura. Una sandbox storica e ancora valida è ad esempio quella offerta da *Sandboxie* nella sua nuova incarnazione open source nota come *Sandboxie Plus* (*sandboxie-plus.com*), mentre le versioni Pro ed Enterprise di Windows 10 includono un piccolo ambiente virtualizzato noto come *Windows Sandbox*.

Scanner offline

La protezione di un engine antivirale in tempo reale è indispensabile, ma le buone pratiche di *opsec* consigliano di utilizzare periodicamente anche uno scanner di terze parti privo di funzionalità real-time. Sfruttando uno o più "scanner offline", infatti, avremo modo di analizzare il sistema mettendolo a confronto con un engine diverso da quello dell'antivirus installato sul Pc, così da avere una seconda (e magari terza) opinione sull'effettiva sicurezza della situazione e l'assenza di malware su disco. Moltissime società di sicurezza offrono il loro scanner offline gratuito, di seguito elenchiamo alcuni esempi da valutare per l'adozione permanente sul Pc. Con un avvertimento: uno scanner offline non è in genere in grado di aggiornarsi da solo, e va quindi sostituito con il download dell'ultima versione disponibile sul sito ufficiale:

Kaspersky Virus Removal Tool - *https://www.kaspersky.com/downloads/thank-you/free-virus-removal-tool*
Malwarebytes AdwCleaner - *https://www.malwarebytes.com/adwcleaner*
McAfee Stinger - *https://www.mcafee.com/enterprise/en-us/downloads/free-tools/stinger.html*
Microsoft Safety Scanner - *https://docs.microsoft.com/it-it/windows/security/threat-protection/intelligence/safety-scanner-download*
Panda Cloud Cleaner - *https://www.pandasecurity.com/it/homeusers/cloud-cleaner/*
Sophos Virus Removal Tool - *https://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx*

Immagini ISO avviabili

Nel peggiore dei casi, se il sistema risultasse alla fine infetto nonostante le nostre migliori intenzioni, la soluzione più pratica e sicura per cercare di riparare al danno consisterebbe nel download di un'ambiente di ripristino esterno per avviare le procedure di scansione e pulizia mentre il sistema operativo Windows è "offline". Anche in questo caso, le migliori *security enteprise* mondiali offrono diverse immagini ISO da scaricare, quindi masterizzare su Cd/Dvd oppure trasformare in unità Usb avviabili. In genere, per ogni immagine ISO vengono fornite tutte le istruzioni utili a creare il nostro disco avviabile e usare l'ambiente di ripristino appena approntato:

Avira Rescue System - *https://support.avira.com/hc/en-us/articles/360007776058-How-do-I-use-Avira-Rescue-System*
Kaspersky Rescue Disk - *https://support.kaspersky.com/14226*
Panda Cloud Cleaner Rescue ISO - *https://www.pandasecurity.com/it/support/card?id=1681*
Sophos Bootable Anti-Virus - *https://support.sophos.com/support/s/article/KB-000033800*

prossime pagine daremo per scontata, e che non ha praticamente alcuna conseguenza negativa: una volta installato il nuovo antivirus, Windows Defender disabiliterà il suo *engine* di scansione in tempo reale e non darà più fastidio. Qualora invece decidessimo di disinstallare l'AV per tornare tra le braccia di Microsoft, Defender ritornerebbe a essere la protezione antimalware predefinita del sistema.

Il focus delle recensioni

Ciascuna delle soluzioni considerate per questa prova è stata analizzata nel corso della sua intera fase di vita informatica, dall'installazione alla configurazione all'utilizzo quotidiano su un sistema portatile "live" dalle specifiche relativamente moderne (Cpu Core i7-7700HQ, Gpu Nvidia GeForce GTX 1060, 16 GB di Ram, Ssd + Hdd) per valutare il comportamento del prodotto durante la navigazione sul Web, il download e l'installazione dei programmi, il gaming, la produttività. È stata valutata anche la fase di disinstallazione, e l'eventuale presenza di "residui" indesiderati non rimossi correttamente dal sistema. Ogni antivirus è stato installato su un sistema operativo Windows 10 Home originale a 64-bit, pienamente aggiornato all'ultima major release (Windows 10 21H1) e con tutte le patch ufficiali disponibili al momento di scrivere. Per l'effettiva capacità degli antivirus di proteggere da malware e minacce informatiche faremo riferimento ai test delle organizzazioni specializzate del settore e in particolare alle comparative periodiche pubblicate dalla tedesca *AV-TEST* (*https://www.av-test.org/en/*) e dalla austriaca *AV-Comparatives* (*https://www.av-comparatives.org/consumer/*). In ogni caso, la lista dei prodotti di sicurezza testati comprende una nutrita rappresentanza di quelli che sono considerati i migliori antivirus gratuiti (e non) attualmente presenti sulla piazza.

Avast Free Antivirus

Il classico degli antivirus gratuiti offre un'ottima protezione e funzionali evolute, ma è caduto in disgrazia dalla scoperta della profilazione estesa degli utenti a scopo pubblicitario.

Forse Avast non ha inventato il modello di business "freemium" alla base degli antivirus gratuiti, una tipologia di prodotto che potremmo far risalire agli antivirus shareware distribuiti all'epoca del DOS, ma di certo la società ceca è stata in grado di trasformarlo in un successo di livello globale. Avast Antivirus può contare su oltre 400 milioni di utenti in tutto il mondo, la seconda maggiore quota di mercato nel campo delle soluzioni anti-malware, e *Avast Free Antivirus* rappresenta il primo punto di accesso di una piattaforma dalla storia recente a dir poco travagliata.

L'installazione di Avast Free Antivirus comincia in seguito al download del *Web Installer* compatto per il sistema operativo in uso (Windows ma anche Mac, Android o iOS) dal sito Web ufficiale. L'installer permette di avviare subito l'installazione oppure di personalizzare la procedura. Questa seconda opzione, caldamente consigliata in qualsiasi scenario di utilizzo, facilita la disabilitazione di quei componenti superflui o indesiderati che poco hanno a che fare con un software antivirus come *Software Updater*, *Browser Cleanup* e altri. Confermata la scelta e avviata l'installazione, bastano pochi minuti per il download e la configurazione dell'antivirus sul Pc. La schermata principale di Avast Free Antivirus ci accoglie con un messaggio rassicurante sulla protezione attiva, l'invito a una prima "scansione intelligente" e un messaggio pubblicitario nella parte bassa che ci invita ad aggiornare l'antivirus alla versione a pagamento. L'advertising per i prodotti commerciali di Avast è costante, in effetti, anche se in genere non da particolarmente fastidio e può essere del tutto trascurato.

Dopo l'installazione, la prima cosa da fare è controllare le impostazioni del nostro nuovo antivirus tramite il pulsante *Menu* in alto a destra. Le opzioni di Avast Free Antivirus sono divise in tre diverse schede: *Generali* comprende la scelta della lingua, il controllo degli aggiornamenti, le notifiche, le eccezioni dei file eseguibili da escludere dalle scansioni, la protezione dell'antivirus con una "master password", la condivisione dei dati sulle minacce individuate con Avast; la scheda *Protezione* comprende le opzioni per configurare il comportamento dell'antivirus (più o meno interattivo, più o meno automatico a seconda delle nostre preferenze) in fase di scansione, di protezione in tempo reale, con le minacce in quarantena, la scansione delle reti Wi-Fi e la protezione dai ransomware. Con *Prestazioni*, infine, possiamo configurare la *Modalità Non Disturbare* e il modulo *Software Updater* eventualmente installato assieme all'antivirus.

L'installazione di Avast Free Antivirus può avvenire in modalità automatica o personalizzata (opzione consigliata).

Dopo la configurazione, è il momento di esplorare le funzionalità di protezione disponibili con Avast Free Antivirus. Il "succo" di tali funzionalità è raggruppato nella scheda *Protezione*, accessibile dalla colonna a sinistra della finestra principale. La prima, fondamentale opzione di protezione è ovviamente quella delle *Scansioni antivirus*, con la *Scansione Intelligente* a fare bella mostra di sé nella parte alta dell'interfaccia, la creazione di un Disco di soccorso in formato ISO (o USB avviabile) per le situazioni di emergenza, e le diverse tipologie di scansione manali in basso compresa la scansione completa dei dischi, la scansione mirata, all'avvio o personalizzata. Una prima *Scansione Intelligente* richiede poco tempo e ci permette di verificare la presenza di eventuali problemi sul sistema (e non solo sui dischi), anche se il risultato finale ci è sembrato l'ennesimo invito ad acquistare la versio-

★★★☆☆

https://www.avast.com/it-it/free-antivirus-download

PRO
Protezione eccellente / Strumenti avanzati / Antivirus leggero

CONTRO
Pubblicità un po' fastidiosa / Bloatware nell'installazione / Potenziale rischio privacy

IN BREVE **Avast è da anni la soluzione antivirus gratuita per eccellenza, con un'ottima protezione e funzionalità avanzate accessibili a tutti. Però è gravissima, e senza possibilità di scusa, la violazione della privacy emersa negli anni passati.**

Personalizzando l'installazione, avremo modo di disabilitare tutti gli strumenti inutili (e indesiderati) riducendo al minimo il bloatware integrato da Avast nel suo antivirus free.

Al termine dell'installazione, Avast Free Antivirus ci accoglie con la sua caratteristica finestra con sfondo scuro, messaggi e pubblicità ovunque. Per Avast "Il computer è protetto".

ne commerciale di Avast per risolvere i presunti problemi di cui sopra. Più utile e funzionale risulta invece la scansione completa, di durata variabile in relazione ai dati presenti su disco e alla profondità dell'analisi scelta nelle impostazioni: a scansione terminata, una pratica schermata dei risultati ci darà modo di selezionare le minacce (reali o presunte in caso di falsi positivi) da "risolvere" spostando i file in quarantena oppure eliminandoli. Oltre alle scansioni, le altre funzionalità di protezione di Avast Free Antivirus permettono di abilitare o disabilitare le difese in tempo reale contro i malware, i comportamenti "sospetti" delle applicazioni, gli attacchi Web e via e-mail. Potremo altresì analizzare le minacce attualmente in quarantena, impostare le cartelle da proteggere in scrittura contro le applicazioni non attendibili (*Protezione ransomware*), avviare la scansione della rete wireless con *Wi-Fi Inspector*. Funzionalità, quest'ultima, decisamente interessante che procede all'analisi della rete Wi-Fi, i dispositivi connessi e la presenza di eventuali vulnerabilità di sicurezza. Il resto delle protezioni è accessibile solo effettuando l'upgrade alla versione a pagamento dell'antivirus, la protezione alla privacy offre la possibilità (piuttosto problematica come vedremo a breve) di proteggere i nostri account registrando un *Account Avast*, e la *Modalità Non disturbare* nella scheda *Prestazioni* permette di aggiungere e configurare le applicazioni che vogliamo eseguire a pieno schermo senza interruzioni, notifiche o fastidi di sorta. Una configurazione che è possibile effettuare anche in maniera interattiva, visto che Avast ha la tendenza a visualizzare una notifica su schermo dopo l'utilizzo di ogni applicazione "esclusiva" come videogiochi, browser e visualizzatori di immagini.

Anche nella sua versione gratuita, in buona sostanza, Avast Antivirus offre una protezione di notevole livello con strumenti dedicati (ransomware, Wi-Fi) e un engine antivirale costantemente in cima alle classifiche nei test dei laboratori specializzati. Gli ultimi test pubblicati da AV-Comparatives assegnano ad Avast il massimo livello di identificazione dei malware offline (93,4%) e online (96,3%), con percentuali altrettanto eccellenti nei test "dal vivo" (99,9%); stesso discorso per AV-TEST, che ad Avast Free Antivirus assegna quasi il massimo dei voti nella protezione contro gli attacchi 0-day (99,3%), l'identificazione del malware più diffuso e recente (100%), l'impatto ridotto sulle prestazioni del sistema e l'usabilità. Nei test effettuati sulla nostra macchina di prova, Avast si è comportato in ma-

Dalle Impostazioni, avremo modo di personalizzare il comportamento di Avast Free Antivirus e il livello di protezione o interattività del software.

Particolarmente importanti sono le opzioni di protezione e delle scansioni, per evitare effetti indesiderati come la rimozione automatica dei falsi positivi.

Per le scansioni antivirus di Avast c'è l'imbarazzo della scelta. Disponibile anche una comoda opzione per la creazione di un "disco di soccorso" per le emergenze.

Per essere così in bella mostra, la "Scansione Intelligente" di Avast sembra più un mezzo per spingere gli utenti ad acquistare l'antivirus premium che altro.

La Scansione Antivirus Completa analizza in dettaglio lo stato del sistema, dei dischi e dei file. La durata dell'analisi è variabile in proporzione al numero di file presenti sul Pc.

Al termine della scansione, Avast permette di "correggere", eliminare o mettere in quarantena le minacce o i falsi positivi identificati, agendo in blocco o singolarmente.

Wi-Fi Inspector analizza la rete wireless identificando dispositivi connessi e potenziali vulnerabilità della rete. Una funzionalità aggiuntiva molto utile e a costo zero

niera sostanzialmente egregia senza alcuna "degradazione" percepibile durante l'utilizzo quotidiano del Pc, dalle applicazioni di produttività (in prevalenza Microsoft Office) ai videogiochi. Purtroppo Avast, a nostro giudizio, non è più una società di cui ci si può fidare a occhi chiusi (trovate in queste pagine il box dedicato "Chi controlla i controllori?"). Avast Free Antivirus è certamente una soluzione antimalware valida e funzionale, ma all'utente spetta la decisione finale sulla possibilità di adottare il software in pianta stabile e configurarlo in modo da ridurre al minimo la condivisione "in chiaro" dei dati con Avast.

AVG AntiVirus Free

AVG condivide lo stesso engine antivirale di Avast (e stessi pro e contro) ma è sufficientemente diverso in alcune delle funzionalità disponibili agli utenti.

L'installazione personalizzata di AVG AntiVirus Free include meno componenti inutili rispetto ad Avast.

Come Avast, anche *AVG Technologies* è una *security enteprise* nata nell'allora Cecoslovacchia (oggi Repubblica Ceca) poco prima della dissoluzione del Muro di Berlino. Specializzata fin dall'inizio nella commercializzazione di software antivirus, la società è stata interamente acquisita da Avast nel 2016 per 1,3 miliardi di dollari. Di fatto, Avast e AVG sono oggi lo stesso antivirus con una *skin* leggermente diversa, anche se le due entità continuano a esistere come prodotti separati con un'offerta di protezione differenziata. Secondo i numeri ufficiali, i software e i servizi offerti da AVG possono contare su più di 200 milioni di utenti attivi in tutto il mondo (su Pc e mobile).

Il fatto che Avast e AVG condividano la stessa "anima" risulta evidente fin da subito, ovvero dopo il download e l'avvio dell'installer compatto di AVG AntiVirus Free dal sito ufficiale. Stesso discorso per l'installazione personalizzata, dove però emergono le prime differenze nell'offerta dei componenti aggiuntivi che è possibile selezionare/deselezionare accanto alla protezione antivirale. Anche in questo caso è altamente consigliata la disabilitazione di tool superflui come *File Shredder* e *Cleanup*. Completata l'installazione, AVG fa mostra dell'interfaccia, invero più compatta ed essenziale di Avast, del suo Antivirus gratuito. Al solito, dalla voce *Menu* in alto a destra si accede alle impostazioni del programma, con una UI sostanzialmente identica a quella di Avast con poche differenze qua e là. AVG AntiVirus Free offre una "protezione di base gratuita" che si incarica di proteggere il Pc, le applicazioni, le comunicazioni Web e le e-mail, mentre i componenti della "*Protezione completa*" necessitano dell'acquisto della suite commerciale *Internet Security*. Con un clic sulla voce *Computer* della *Protezione di base* si accede alle difese informatiche essenziali, avendo quindi la possibilità di attivare/disattivare la protezione in tempo reale, aprire la protezione contro i ransomware (identica a quella di Avast) e l'utilità *Controllo di rete* (vale a dire il *Wi-Fi Inspector* di Avast). Sempre nella protezione di base, la schermata Web e Email fornisce accesso alle protezioni contro gli attacchi da remoto e a un "Account AVG" per il monitoraggio degli account personali. Le scansioni antivirali sono accessibili dal menu a scomparsa nascosto dietro l'icona a tre punti accanto alla voce in evidenza *Esegui Scansione Intelligente*, e permettono di analizzare in profondità il sistema, file o cartelle specifici, supporti rimuovibili o di pianificare una scansione all'avvio alla caccia del codice malevolo nascosto nei "luoghi inaccessibili durante le comuni scansioni". In quest'ultimo caso AVG consiglia di installare le "definizioni antivirus specializzate" per un'analisi ancora più efficace. Come già con Avast, la *Scansione Intelligente* di AVG non sembra essere particolarmente utile all'utente ma solo all'azienda per promuovere l'acquisto della suite a pagamento Internet Security. Per contro, lo spam e i messaggi pubblicitari sono quasi inesistenti al confronto di Avast.

La vera ragion d'essere di AVG AntiVirus Free sembra in effetti essere quella di fornire una versione meno "accessoriata" del software freemium di Avast, con meno bloatware integrato in fase di installazione e alcuni

★★★

https://www.avg.com/it-it/free-antivirus-download

PRO
Protezione eccellente / Interfaccia essenziale / Antivirus leggero

CONTRO
Continui inviti all'upgrade a pagamento / Bloatware / Potenziale rischio privacy

IN BREVE AVG Antivirus offre lo stesso, eccellente livello di protezione di Avast, con meno bloatware e i medesimi, identici difetti sul fronte dei rischi per la riservatezza.

Tranne qualche differenza qua e là, il Menu e le Impostazioni di AVG sono identiche a quelle di Avast. L'engine antivirale è lo stesso.

La "Protezione di base" di AVG tiene al sicuro Pc, Web ed e-mail. Il resto è accessibile a pagamento con la suite Internet Security.

La protezione include scansioni real time, analisi del comportamento delle applicazioni, scudi contro ransomware e attacchi alla rete.

Nascoste dietro "scansione intelligente", le scansioni antimalware analizzano Pc, file e dispositivi alla caccia del software malevolo.

componenti in meno (come ad esempio la creazione di un disco ISO di soccorso). AVG e Avast hanno da tempo adottato un engine antivirale comune (quello di Avast) ma "aumentandolo" con le capacità di AVG, ed è pacifico evidenziare come i test dei laboratori specializzati assegnino esattamente gli stessi punteggi e lo stesso livello di protezione ai due antivirus. Identico è anche il discorso sulla violazione della privacy emersa con la storiaccia di Jumpshot, e nel caso di AVG si tratta di un'aggravante visto che anche prima dell'acquisizione da parte di Avast, la società era impegnata (per sua stessa ammissione) nel tracciamento dell'attività degli utenti a scopo di profitto. Disdicevole, inoltre, il comportamento della toolbar *SafeGuard* installata senza il consenso degli utenti, difficile da rimuovere e classificata (dal 2012 in poi) come un vero e proprio software indesiderato (PUP ovvero *Potentially Unwanted Program*). Quello stesso tipo di software da cui AVG dovrebbe difendere gli utenti con il suo antivirus. Come Avast, infine, la sussidiaria AVG è destinata a diventare parte integrante di un'unica offerta antivirale sotto il problematico ombrello di NortonLifeLock.

La scansione all'avvio si offre di analizzare i luoghi del Pc "inaccessibili" alle scansioni comuni, con tanto di definizioni antivirali specializzate.

Come rendere (meno) inutile Windows Defender

Nel corpo dell'articolo abbiamo accennato ai molti lati negativi che caratterizzano Windows Defender, spiegando perché un antivirus gratuito di terze parti continua a essere la scelta migliore per la sicurezza del Pc. Siamo altresì consapevoli del fatto che non sempre è possibile usare un antivirus esterno o scegliere liberamente quali software installare sul sistema. In casi del genere, Defender resta l'unica difesa contro attacchi e malware. Per tale ragione, di seguito elenchiamo alcuni dei migliori "trucchi" per rendere la nostra coabitazione con l'antimalware nativo di Windows un po' meno goffa e problematica.

Scansioni personalizzate

A eccezione degli occasionali allarmi sulla presenza di presunte minacce che poi si rivelano puntualmente essere solo dei falsi positivi, Defender se ne sta in genere per conto proprio e si limita a controllare in tempo reale la sicurezza del Pc. Qualora volessimo effettuare una scansione personalizzata di un particolare file o di una cartella, potremo seguire due strade diverse: la prima consiste nell'utilizzare il *Menu Contestuale* accessibile con un clic destro sugli oggetti da esaminare (*Analizza con Microsoft Defender*), la seconda prevede l'apertura della app *Sicurezza di Windows* tramite la ricerca della voce *Protezione da virus e minacce* sul Menu Start. Da qui potremo scegliere la voce *Opzioni di analisi*, selezionare *Analisi personalizzata* e fare clic su *Avvia analisi*: a questo punto basterà selezionare una cartella o un file per avviare la scansione. Alla fine della procedura, Defender presenterà un riassunto molto stringato sui file analizzati, l'eventuale presenza di minacce e le azioni consentite all'utente.

Configurazione avanzata

All'apparenza, Windows Defender è un software di sicurezza che offre ben poche possibilità di personalizzazione e configurazione da parte dell'utente finale. In realtà è possibile modificare radicalmente il funzionamento dell'antivirus, anche se per farlo sarebbe necessario entrare nei meandri dell'ambiente PowerShell di Windows e digitare una lunga serie di comandi testuali per cambiare ogni opzione. A facilitare tale gravoso compito arriva *ConfigureDefender*, un piccolo tool open source ospitato sui server di GitHub (*https://github.com/AndyFul/ConfigureDefender*) che in pratica converte i lunghi comandi di PowerShell in un'interfaccia grafica molto più *user-friendly*.

ConfigureDefender è un piccolo tool open source in grado di rendere più accessibile la configurazione di ogni aspetto di Microsoft Defender grazie a un'interfaccia grafica dedicata.

Grazie a ConfigureDefender potremo agilmente modificare ogni singola opzione nascosta di Defender, impostando altresì un livello di sicurezza complessivo a scelta tra Default, Alto o Massimo. Completata la personalizzazione, sarà necessario confermare la nuova configurazione con un

clic sul pulsante *Refresh* e quindi riavviare Windows per rendere effettive le modifiche.

Gestione delle minacce

Fra le tante pecche di Windows Defender c'è la scarsa, scarsissima praticità nella gestione delle minacce o dei falsi positivi individuati dall'antivirus. Anche in questo caso è possibile utilizzare un tool di terze parti, sviluppato per l'occasione dalla sempre prolifica *NirSoft*, per rendere più agevole e usabile la piattaforma di sicurezza nativa di Windows. *WinDefThreatsView*, questo il nome del tool in oggetto, è la solita applicazione portabile NirSoft che non richiede installazione sul sistema (*https://www.nirsoft.net/utils/windows_defender_threats_view.html*). Il programma visualizza un elenco di tutte le minacce fin qui individuate da Defender, e permette di effettuare diverse operazioni sui file corrispondenti compresa la cancellazione, il blocco o il permesso all'esecuzione. Particolarmente utile è poi la possibilità di selezionare più minacce contemporaneamente, effettuando operazioni in blocco piuttosto che agendo individualmente come saremmo costretti a fare dalla limitatissima interfaccia di Defender.

Scansioni da riga di comando

Per quanto sia, al solito, poco pratico da usare, Microsoft Defender include anche uno scanner da riga di comando da lanciare in una finestra del Prompt testuale di Windows 10. Qualora volessimo sentirci di nuovo come ai tempi del DOS e di McAfee VirusScan, dovremo prima di tutto aprire una finestra Admin del Prompt (*Win+R*, "cmd", *Ctrl+Shit+Invio*), quindi posizionarci nella cartella di Defender tramite il seguente comando:

```
cd c:\ProgramData\Microsoft\Windows Defender\Platform
```

A questo punto occorrerà visualizzare le diverse sottocartelle disponibili (*dir*), quindi posizionarci nella cartella con il numero di versione più recente con il comando *cd*. Nel caso del Pc usato per i test, il comando corretto è il seguente:

```
cd 4.18.2109.6-0
```

Il file eseguibile corrispondente alla versione da riga di comando di Defender si chiama *mpcmdrun.exe*, ed è possibile utilizzarlo per avviare diversi tipi di scansioni esattamente come nella versione con GUI. Segnaliamo in particolare i seguenti comandi "generalisti", rimandando alla lettura delle guida ufficiale di Microsoft ogni ulteriore approfondimento (*https://docs.microsoft.com/it-it/microsoft-365/security/defender-endpoint/command-line-arguments-microsoft-defender-antivirus?view=o365-worldwide*):

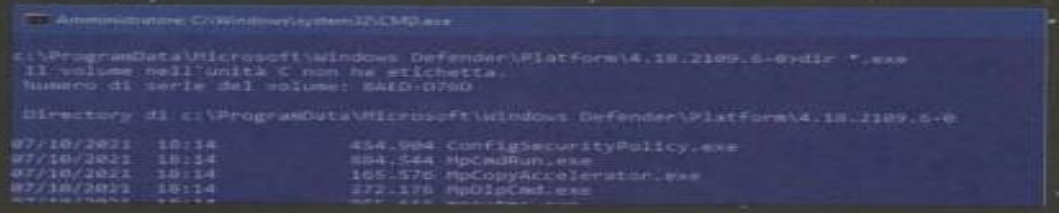
```
mpcmdrun -Scan -ScanType 1
```
effettua una scansione veloce delle zone del sistema più sensibili ai potenziali attacchi da malware (Registro, cartelle di avvio ecc.);

```
mpcmdrun -Scan -ScanType 2
```
effettua una scansione completa del sistema con conseguente dispendio di tempo in proporzione al numero di file presenti su disco;

```
mpcmdrun -Scan -ScanType -BootSectorScan -
```
effettua una scansione veloce del settore di boot del disco alla ricerca di possibili malware "invisibili";

```
mpcmdrun -Scan -ScanType 3 -File "Percorso"
```
effettua la scansione del percorso specificato dall'utente (es. *"C:\Windows\Boot"* al posto di *"Percorso"*).

WinDefThreatsView ci permette di gestire agilmente le minacce individuate da Defender, con la possibilità di agire in blocco eliminando i file eseguibili o permettendo la loro esecuzione in caso di falsi positivi.



Windows Defender ha anche una versione eseguibile da riga di comando. Diversamente dal classico McAfee VirusScan, l'integrazione con il sistema operativo è sempre la stessa.

Avira Free Security

Un tempo antivirus gratuito per eccellenza, Avira è oggi una suite di sicurezza a tutto tondo, con parecchi difetti e alcune caratteristiche discutibili.

La schermata principale di Avira Free Security offre una visione d'insieme sullo stato del sistema per la sicurezza, la privacy e le prestazioni.

Solo pochi anni or sono, la società tedesca *Avira GmbH* rappresentava la scelta di sicurezza ideale per centinaia di milioni di utenti soddisfatti grazie all'estrema popolarità di *Avira Free Antivirus*. Il software antimalware teutonico ha poi preso una piega da vera e propria "suite" trasformandosi in *Avira Free Security*, e la trasformazione è stata imposta in maniera tanto repentina all'intera base di utenza che l'insoddisfazione e le critiche continuano a circolare furenti online. Noi apparteniamo alla schiera di utenti assolutamente insoddisfatti, e il giudizio finale sulla suite Avira sarà pesantemente influenzato dalla nuova politica coercitiva (e del tutto irrispettosa delle esigenze di utilizzo personali) imposta dalla società tedesca.

Prima dei giudizi, in ogni caso, è opportuno analizzare più in dettaglio le caratteristiche e le funzionalità di Avira Free Security. La suite si installa tramite il download e l'avvio del solito *downloader* compatto, e diversamente dalla concorrenza Avira non offre alcuna possibilità di personalizzare l'installazione dei componenti disponibili. Fortunatamente, almeno per quanto riguarda l'installer attualmente scaricabile dal sito ufficiale, non è più prevista l'installazione obbligatoria, "silenziosa" e assolutamente non richiesta del browser Opera come invece è capitato a noi durante l'aggiornamento forzato da Avira Free Antivirus. Avira Free Security vuole ovviamente essere più di un antivirus, prendendosi carico della gestione della sicurezza, della privacy e delle prestazioni del sistema. La scansione "intelligente" (o "in background") accessibile dalla prima scheda di Avira Free Security è, come spesso accade in questi casi, del tutto inutile: verificando i singoli risultati tramite l'apposito pulsante, ci imbatteremo nelle indicazioni su quello che secondo Avira occorrerebbe fare per ottimizzare lo stato del sistema. Nei nostri test, in particolare, la suite ci ha consigliato di aggiornare le "app obsolete" (inclusa l'ultimissima versione di Windows 10 Home x64 installata solo qualche settimana prima), di disattivare diverse impostazioni di Windows, di cancellare centinaia di voci nel Registro di Windows e di ritardare il caricamento di tre applicazioni potenzialmente in grado di rallentare l'avvio di Windows. I "consigli" di Avira si possono insomma ignorare senza problemi, ma Avira Free Security continuerà a rimarcare la presenza di questi presunti "problemi" ogni 24 ore tramite un fastidioso "pallino" persistente nell'icona del software nell'Area di Notifica. Passando alle altre funzionalità accessibili dalla schermata principale, la scheda *Sicurezza* include le solite scansioni antivirus (completa, rapida o personalizzata), la modifica delle opzioni di protezione avanzate (tutte a pagamento a eccezione del suddetto AV), l'accesso alle presunte minacce in quarantena; la funzionalità di *Software Updater* per l'aggiornamento automatico delle applicazioni è a nostro parere da evitare come la peste, mentre *Firewall* si limita a fornire un paio di collegamenti al firewall nativo di Windows. La scheda *Privacy* comprende funzionalità altrettanto basilari e quindi per la maggior parte trascurabili, ovvero un'estensione anti-tracciamento per browser Web (molto meglio affidarsi a sistemi dedicati come *uBlock Origin* e installare il browser Mozilla Firefox), la solita VPN ultra-limitata (500 MB

★★

https://www.avira.com/it/free-security

PRO

Avira Antivirus c'è ma non si vede / Forse utile per gli utenti alle primissime armi / Non costa un centesimo

CONTRO

Funzionalità avanzate potenzialmente pericolose / Nessun controllo in fase di installazione / Avira Free Antivirus non esiste più

IN BREVE **Avira Free Security sostituisce l'antivirus gratuito di Avira con una suite graficamente pasticciata, dalle funzionalità discutibili e del tutto irrispettosa della volontà dell'utente.**

di traffico mensile e un solo punto di accesso in Italia), un gestore di password. Disponibile anche un "distruggidocumenti" per rendere inaccessibili i file cancellati, mentre con *Impostazioni di privacy* è possibile modificare diverse opzioni delle applicazioni e di Windows stesso per "migliorare la privacy del sistema" (telemetria, sensori, rete, ricerca, Store eccetera). La scheda *Prestazioni*, infine, da accesso a un clone ultra-semplificato del celeberrimo CCleaner (*Optimizer*), all'aggiornamento dei driver di sistema, la ricerca dei file duplicati e ad altri "Strumenti avanzati". Buona parte di questi strumenti fa parte del pacchetto *Avira System Speedup*, un programma esterno installato assieme ad Avira Free Security e dedicato all'ottimizzazione di Windows, dei programmi di avvio, della pulizia di file inutili e di molto altro ancora. Anche in questo caso, si tratta di un'offerta dalla qualità a dir poco discutibile (di interfaccia grafica prima ancora che di effettiva capacità di ottimizzazione) che fa il verso ai programmi di terze parti con in più lo spam per l'acquisto della versione a pagamento del programma. Anche in un pasticcio di software come Avira Free Security, in ogni caso, batte il cuore pulsante di un antivirus degno di questo nome: basta accedere alle *Opzioni di protezione* oppure avviare una scansione dalla scheda *Sicurezza*, per ritrovarsi al cospetto di un'interfaccia in stile "Windows 2000" da cui è possibile modificare in ogni minimo dettaglio il comportamento dell'engine antivirale e della protezione in tempo reale, seguire con dovizia di particolari l'andamento delle scansioni e approfondire il livello di ogni singola minaccia o consultare il rapporto finale. Lo storico e ormai famigerato Avira Free Antivirus, insomma, continua a vivere all'interno di Avira Free Security, anche se bisogna scavare un

Analizzando in dettaglio i risultati della scansione sullo sfondo, ci si accorge che le "soluzioni" di Avira Free Security non sono quasi mai ideali. E possono persino risultare dannose.

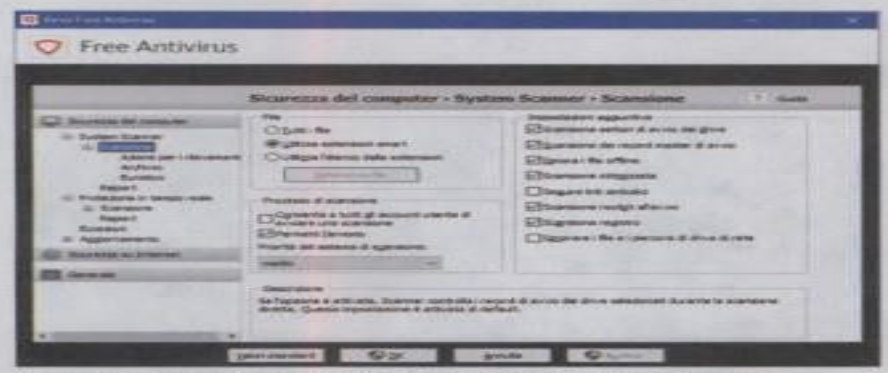
La scheda Sicurezza racchiude le difese e le diverse modalità di scansione contro i malware, la quarantena, un inutile software updater e il collegamento al firewall di Windows.

I consigli di aggiornamento di Software Updater possono essere superflui o, nel peggiore dei casi, dannosi per il software che usiamo quotidianamente o per Windows stesso. Da evitare.

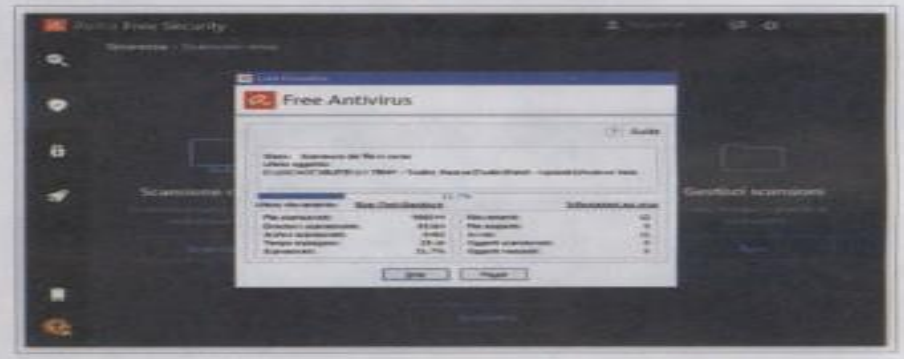
Le impostazioni della privacy consigliate da Avira Free Security modificano in modo significativo il funzionamento di Windows e dei programmi installati. E il risultato potrebbe non piacerci.

Avira Free Security vuole fornire una serie di strumenti pensati per ottimizzare le prestazioni del Pc con il minimo sforzo. Con risultati altrettanti minimi e dall'utilità marginale.

Avira System Speedup sembra un clone mal concepito di CCleaner, con qualche messaggio pubblicitario in più e l'ennesima interfaccia dedicata diversa da quella base.



Le opzioni di sicurezza di Avira Free Security tradiscono la natura caotica del software, con un'interfaccia e un livello di personalizzazione estranei al resto della suite.



Avira Free Antivirus continua a vivere come base di Avira Free Security, lo dimostra la classica finestra del "Luke Filewalker" durante le scansioni a caccia di malware.

po' per accorgersene. Stando ad AV-Comparatives, la protezione offerta da Avira (Antivirus Pro) contro le minacce in tempo reale è pari al 98,9%, mentre la capacità del tool di identificare i malware varia dal 90,3% off-line a un livello di protezione on-line del 99,98%. Altrettanto lusinghieri gli score di AV-TEST con un 100% tondo per la protezione contro gli attacchi 0-day e l'identificazione dei malware più diffusi e prevalenti. Significativo in questo caso è l'impatto misurato sulle prestazioni nella navigazione Web (-50% di velocità su un Pc "standard"), anche se le cose potrebbero variare sensibilmente nel caso dell'offerta gratuita. Nei nostri test, inoltre, Avira Free Security ha fatto segnare il degrado più evidente nelle prestazioni del sistema in fase di avvio, con un ritardo di 5-6 secondi aggiuntivi per la comparsa del Desktop di Windows rispetto ai 28-30 secondi degli antivirus concorrenti. Protezione e prestazioni a parte, Avira Free Security è una suite piena di spam e strumenti inutili o persino pericolosi, fa una gran confusione in ambito grafico utilizzando ben tre interfacce totalmente differenti (suite, antivirus, Avira System Speedup) e non la smette di annoiare l'utente con il promemoria quotidiano sulla presenza di inesistenti "problemi" sul sistema. Come Avast e AVG, infine, anche Avira è entrata a far parte della grande famiglia di NortonLifeLock in seguito all'acquisizione avvenuta nel gennaio del 2021. Diversamente dagli altri due AV gratuiti, al momento non si prevede il pensionamento forzato dell'engine antivirale di Avira in favore dell'adozione di quello di Avast. Anche se a questo punto potrebbe essere il male minore.

Bitdefender Antivirus Free Ed.

Bitdefender può vantare uno dei migliori punteggi in fatto di identificazione delle minacce, ma l'antivirus in versione free è davvero ridotto all'osso.

Le origini di Bitdefender risalgono al lontano 1990 con la creazione di *Softwin*, prima società IT nata nella Romania post-comunista a opera di Florin Talpes e consorte. La nascita ufficiale della corporation esclusivamente dedicata alle soluzioni antivirus avviene nel 2001, e da allora è stata una corsa verso il successo e le moderne dimensioni da multinazionale. Oggi gli strumenti di sicurezza di Bitdefender vengono usati in 150 diversi paesi, dice Talpes, con 500 milioni di utenti registrati e più di 1.600 dipendenti a livello globale. Una parte significativa dell'utenza ha ovviamente adottato *Bitdefender Antivirus Free Edition*, un AV dalle indubbie qualità ma anche con difetti non trascurabili per chi è abituato a "sporcarsi le mani" con opzioni e personalizzazioni varie.

Bitdefender Antivirus Free Edition si installa come al solito tramite un installer Web di piccole dimensioni e il successivo download delle centinaia di megabyte necessarie al setup. Parimenti a Kaspersky Cloud, anche l'antivirus rumeno richiede la registrazione obbligatoria di un account remoto per poter funzionare. Diversamente da Kaspersky, Bitdefender segue un approccio che definire minimalista è dire poco: un clic sull'icona bianco-rossa nell'*Area di Notifica* porta in evidenza la semplicissima finestra principale dell'antivirus, pensata per veicolare le varie notifiche di attività del programma (aggiornamenti firme virali, scansioni, identificazione malware ecc). Gli unici elementi interattivi nella finestra includono il pulsante *System Scan*, da cui far partire la scansione dell'intero sistema, il pulsante per l'aggiornamento alla versione commerciale in basso e l'icona-ingranaggio in alto a destra con cui accedere alle poche finestre informative dell'antivirus. È inoltre possibile fare clic su ogni evento elencato nella finestra principale per consultare i dettagli corrispondenti. Le finestre accessibili dall'icona-ingranaggio includono *Events*, con l'elenco di tutti gli eventi registrati durante l'attività del programma, *Quarantine* per la gestione degli oggetti in quarantena, *Exclusion* per i file e i falsi positivi da ignorare, infine *Protection* con i dettagli sulle versioni installate dell'engine antivirale e le firme virali corrispondenti. L'unica possibile modifica alla configurazione è presente in questa finestra, e permette di attivare o disattivare temporaneamente la protezione in tempo reale dell'antivirus (*Protection Shield*). Bitdefender Antivirus Free Edition è in pratica tutto qui, un tool che non si perde assolutamente in chiacchiere offrendo una protezione antimalware di base (per file e browser Web) e nessuno strumento aggiuntivo. La scansione può avvenire tramite il già citato pulsante *System Scan* dalla finestra principale, con il trascinamento di file e/o cartelle sul suddetto pulsante o tramite il menu contestuale della shell grafica di Windows (*Esplora File*). Di particolare interesse la scansione completa del sistema, un'operazione che sul Pc di prova ha richiesto poco più di una decina di minuti contro

Come ogni "buon" antivirus moderno, anche Bitdefender Antivirus Free Edition richiede la registrazione di un account per poter funzionare.

Bitdefender

★★★★★

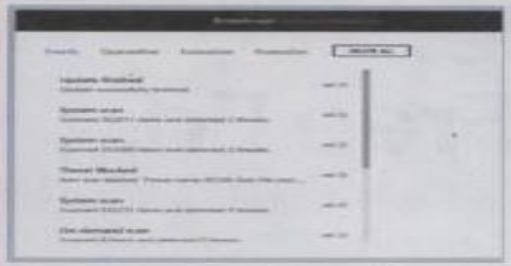
https://www.bitdefender.it/solutions/free.html

PRO
Protezione eccellente / Leggerissimo / Niente advertising compulsivo

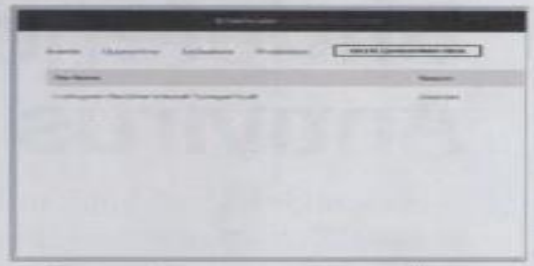
CONTRO
Configurazione estremamente limitata / Scansione di sistema insoddisfacente / Non disponibile in italiano

IN BREVE **Bitdefender Antivirus è un software antimalware potente ed estremamente essenziale. Forse troppo essenziale anche per gli utenti meno smaliziati.**

La finestra principale di Bitdefender Antivirus Free Edition comprende tutte le funzionalità essenziali del programma.



Dalla finestra Eventi è possibile tenere traccia (e approfondire) tutte le scansioni, gli aggiornamenti e gli allarmi generati dall'antivirus.



La Quarantena comprende un elenco dei file "segregati" dal resto del sistema, così da poter agire individualmente su ciascun file sospetto

i 30-50 minuti abbondanti degli antivirus trattati nelle pagine precedenti. Ulteriori scansioni successive tendono a ridurre ulteriormente i tempi, anche se i risultati finali evidenziano una certa "superficialità" dell'analisi. Al confronto con Kaspersky Security Cloud, ad esempio, Bitdefender ha ignorato completamente la scansione del nostro archivio ZIP contenente pericolosi *sample* virali di virus, worm, trojan e ogni sorta di minaccia collezionata nel corso degli ultimi anni. Né è presente, come abbiamo già visto, alcuna opzione o configurazione in grado di abilitare la scansione diretta degli archivi compressi. Non che all'antivirus rumeno faccia difetto l'efficacia nel contrasto ai malware e al crimine informatico, beninteso: nei test di laboratorio specializzati *Bitdefender Internet Security* è costantemente in cima alle classifiche dei risultati, con una protezione perfetta (100%) contro attacchi 0-day e malware più diffusi secondo AV-TEST, eccellente difesa contro gli attacchi real-world (99,9%) e per l'identificazione dei file malevoli in fase di esecuzione (96,8% off-line, 100% protezione on-line) e pochissimi falsi positivi secondo AV-Comparatives. Bitdefender Antivirus Free Edition include esattamente lo stesso livello di protezione della sua controparte commerciale, ed è forse nella sua estrema semplicità ed essenzialità che va identificato il difetto più grave di un programma che altrimenti andrebbe candidato al premio di "antivirus gratuito perfetto". Un altro aspetto problematico, anche se è oramai storia di undici anni fa, è l'incidente capitato il 20 marzo 2010 a causa di un aggiornamento bacato delle firme virali. Scaricato e installato l'update, Bitdefender aveva cominciato a classificare TUTTI i file eseguibili e le librerie dll presenti sul sistema come infetti (*Trojan.FakeAlert.5*) spostandoli in quarantena. L'update fallato è stato rimosso piuttosto in fretta, ma i problemi e i malfunzionamenti provocati sui Pc di tutto il mondo sono facilmente immaginabili anche per chi manca di fantasia.

La finestra Protezione comprende l'unica opzione modificabile dall'utente, ovvero l'attivazione o la temporanea disabilitazione della scansione in tempo reale.

La Scansione di Sistema di Bitdefender Antivirus Free è veloce, essenziale come il resto del programma e non esattamente approfondita

I risultati della scansione permettono di verificare la presenza di eventuali minacce sul sistema e di agire su ciascuna di essa.

Kaspersky Security Cloud Free

Da sempre sinonimo di sicurezza e "caccia ai malware", la russa Kaspersky offre una suite gratuita che ha alla base lo stesso engine dell'antivirus commerciale.

Kaspersky Security Cloud Free obbliga l'utente a registrare un account My Kaspersky per poter usare il programma. Nessuna eccezione.

Kaspersky è uno dei nomi più celebri nel mercato dei prodotti per la sicurezza informatica, un colosso con base a Mosca, in Russia, e 400 milioni di utenti sparsi in giro per il mondo. La *security enterprise* moscovita detiene la quota più ampia del mercato europeo, ed è particolarmente nota per le notevoli qualità del suo team di "cacciatori di malware" – oltre che per rapporti non molto chiari (e fin qui senza conferme ufficiali) con l'intelligence russa ai danni (presunti) di quella americana. Tralasciando, per ora, il capitolo spie, dell'offerta antivirus gratuita di Kaspersky possiamo prima di tutto dire che... non è un semplice antivirus. *Kaspersky Security Cloud Free* è infatti, almeno in superficie, una suite di protezione completa che ha alla sua base le indubbie qualità anti-malware di Kaspersky Anti-Virus. Diversamente da altri antivirus, Kaspersky Security Cloud Free necessita della registrazione obbligatoria di un account online "My Kaspersky" per poter funzionare correttamente. Come opportunamente sottolineato dall'installer Web in fase di download e setup, la suite gratuita include antivirus, una VPN a dir poco basilare e altri strumenti aggiuntivi. La protezione di Kaspersky Security Cloud Free ha la capacità di adattarsi allo stile di vita dell'utente, dice ancora il suddetto installer, avvisandolo e interpellandolo solo nei momenti più opportuni o quando è necessario intervenire per bloccare le minacce dirette. Dalla schermata principale possiamo accedere alla finestra delle scansioni, a quella per l'aggiornamento dei database antivirali (aggiornati in automatico di default) e agli altri componenti della suite. La fondamentale procedura di configurazione e modifica delle impostazioni di base parte con clic sulla piccola icona a forma di ingranaggio in basso a sinistra, e come al solito le impostazioni sono raggruppate in una serie di schede dedicate. Nella scheda *Protezione* troviamo tutte le opzioni per configurare antivirus, il protocollo standard AMSI (per il controllo di Kaspersky Anti-Virus da parte delle applicazioni esterne), il controllo del sistema, mentre le altre schede includono le opzioni generali, le esclusioni e la quarantena, la protezione della rete, l'interfaccia e altro ancora. Tornando alla schermata principale, Kaspersky Security Cloud Free include una funzionalità di *Protezione privacy* molto limitata e quindi del tutto trascurabile, il download della app di protezione per i dispositivi mobile, una finestra per facilitare l'avvio della VPN integrata. Chiamato piuttosto banalmente *Kaspersky VPN*, questo componente garantisce un massimo di 200 megabyte di traffico giornaliero e l'accesso anonimo a Internet tramite un singolo (e non modificabile) server dedicato presente in Italia. Per sfruttare al massimo la VPN della società moscovita, com'è prevedibile, occorre fare l'upgrade alla suite a pagamento. Dalla finestra delle *Scansioni*, vero cuore pulsante di ogni antivirus che si rispetti, possiamo avviare e configurare i diversi tipi di analisi anti-malware disponibili inclusa la scansione rapida, quella completa, la scansione selettiva, per i dispositivi rimuovibili e l'eventuale scansione sullo sfondo da attivare e configurare all'occor-

kaspersky

★★★★

https://www.kaspersky.it/free-cloud-antivirus

PRO
Protezione eccellente / Tanti strumenti aggiuntivi / VPN di base gratuita

CONTRO
Tante schermate in cui perdersi / La VPN di base è troppo limitata

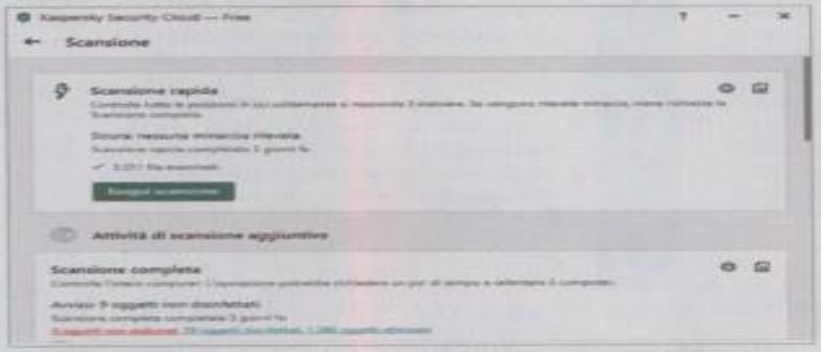
IN BREVE Kaspersky è da sempre sinonimo di protezione e sicurezza contro virus e malware, anche se la suite gratuita è come al solito ricca di inviti all'upgrade alla versione a pagamento.

renza. La scansione completa è particolarmente diligente nella sua opera di scandaglio, e richiede prevedibilmente un tempo molto più lungo rispetto alle scansioni parziali. Per quanto riguarda gli strumenti aggiuntivi accessibili tramite il pulsante *Altri strumenti* della finestra principale, Kaspersky Security Cloud Free si offre di controllare e correggere le "impostazioni vulnerabili" del sistema, un database basato sul cloud per una reazione "immediata" alle nuove minacce, un link per il download di un disco di soccorso, l'eliminazione definitiva dei file (scheda *Protezione dati*), la pulizia dei dati inutili e la risoluzione dei problemi di Windows. Tutti gli altri strumenti (controllo applicazioni, rete, backup ecc.) sono disponibili solo previo aggiornamento alla versione commerciale della suite.

Per quanto riguarda l'effettiva capacità di Kaspersky Security Cloud Free di proteggere l'utente dagli attacchi e dal codice malevolo, possiamo fare riferimento ai punteggi ottenuti da Kaspersky Internet Security nei test di laboratorio dedicati: AV-Comparatives incensa il programma con una capacità di identificazione "online" del 99,96% e un 99,5% per la protezione dagli attacchi real-world; AV-TEST riporta un punteggio perfetto (100%) nella protezione dagli attacchi 0-day e dai malware più diffusi, e un impatto limitato sulle prestazioni di sistema per i Pc sufficientemente carrozzati. Nel 2017, Kaspersky è stata accusata dal governo statunitense di collaborare direttamente con i funzionari della FSB, la principale agenzia di intelligence russa, per tenere sotto controllo i collaboratori della National Security Agency (NSA) statunitense e rubare dati confidenziali dai Pc protetti tramite Kaspersky Anti-Virus. L'azienda fondata da Eugene Kaspersky ha sempre negato ogni addebito, impegnandosi per di più in una maggiore opera di trasparenza fornendo l'accesso al suo codice sorgente per verifiche indipendenti. Parte dell'infrastruttura di protezione principale per i clienti stranieri è stata altresì spostata fuori dal territorio russo, e più precisamente in Svizzera.

La schermata principale della suite Kaspersky è stata ben strutturata e organizzata e permette di lanciare la Vpn gratuita e gli altri strumenti integrati.

Kaspersky VPN può proteggere e rendere più anonima la connessione, ma con un limite di download giornaliero piuttosto stringente.



Come da prassi, anche le Scansioni Kaspersky eseguono l'analisi dei diversi dispositivi e del sistema con vari livelli di approfondimento.

Gli strumenti aggiuntivi di Kaspersky Security Cloud Free sono quasi tutti disponibili solo nella versione a pagamento della suite.

Panda Free Antivirus

Panda ha puntato tutto sul cloud, e i risultati si vedono, mentre l'interfaccia grafica è stata progettata su temi naturali e con una chiara vocazione anti-ansiogena.

Fondata nel 1990 in Spagna, *Panda Security* è una società multinazionale impegnata nello sviluppo di soluzioni di sicurezza per i dispositivi *endpoint* – Pc, workstation e volendo anche smartphone. La corporation può vantare una particolare specializzazione nei software di protezione basati sul cloud, un tipo di tecnologia che in teoria dovrebbe garantire la sicurezza totale contro minacce note e sconosciute – almeno fino a quanto la connessione a Internet rimane stabile e funzionante per il 100% del tempo.

La vocazione al cloud è ovviamente parte anche di *Panda Free Antivirus*, l'offerta antimalware gratuita per gli utenti consumer o che comunque non hanno particolari esigenze sul fronte delle funzionalità aggiuntive. In fase di download tramite il solito *Web installer*, Panda Free Antivirus prevede l'installazione del browser Opera a meno che l'utente non disabiliti le due caselle di accettazione presenti nella finestra. A installazione completata, il programma propone la creazione del solito, ennesimo account di Rete tramite indirizzo di posta elettronica; in questo caso l'offerta si può rifiutare, ma in seguito Panda non mancherà occasione di ripresentare su schermo la finestra di accesso all'account o di limitare l'uso di alcune funzionalità aggiuntive. Caratteristica piuttosto insolita nell'ambito degli antivirus (gratuiti o meno), Panda Free Antivirus utilizzata un'interfaccia che fa ampio uso di sfondi a tema naturale e animale. Un contrasto grafico forse pensato per rendere meno ostico e allarmante l'uso del software di sicurezza da parte degli utenti più o meno inesperti. La schermata principale di Panda Free Antivirus mette in evidenza il "conto" di tutti gli oggetti analizzati a partire dalla prima installazione, con un collegamento diretto al *Riepilogo generale sulla licenza disponibile* (ovviamente gratuita), le statistiche sulla protezione e un ulteriore collegamento al rapporto completo su tutti gli eventi registrati in fase di scansione – per tutte le scansioni siano essere automatiche o a richiesta. È possibile scorrere la finestra principale di Panda per avere accesso agli strumenti aggiuntivi inclusi nel software antivirus. Dal pulsante-hamburger in alto a sinistra possiamo accedere all'account personale eventualmente registrato in precedenza, al supporto tecnico e alle impostazioni. In quest'ultimo caso, Panda Free Antivirus si discosta nettamente dal pessimo esempio di Bitdefender offrendo una serie di schermate per la configurazione della modalità multimediale / di gioco a schermo intero (attivabile o disattivabile anche dal menu contestuale dell'icona nell'*Area di Notifica*), le modalità di protezione dell'antivirus, la quarantena, il monitoraggio dei processi e degli URL e altro ancora. Tornando alla schermata principale, la prima icona a forma di lente d'ingrandimento apre prevedibilmente la finestra per le analisi antimalware. Sono disponibili le solite scansioni delle zone "critiche" (memoria Ram, processi in esecuzione eccetera), la scansione personalizzata o quella completa e approfondita di tutto il Pc. In questo caso i tempi di attesa si allungano, richiedendo sul sistema di prova un tempo leggermente più alto rispetto agli altri antivirus ma comunque al di sotto dell'ora. A fine scansione, Panda visualizza il numero totale di elementi analizzati e le minacce rilevate; visualizzando i dettagli (voce in basso a destra) è possibile avere un quadro più particolareggiato, fino a poter consultare il rapporto globale degli eventi così da agire su ogni singola minaccia identificata –

Panda Free Antivirus si offre di installare il browser Opera. Per fortuna l'offerta può essere al momento ancora rifiutata.

★★★

https://www.pandasecurity.com/it/homeusers/free-antivirus/

PRO
Protezione eccellente... se c'è il cloud / GUI piacevole / Strumenti aggiuntivi interessanti

CONTRO
Poco affidabile senza il cloud / Spam per l'apertura di un account / Troppi falsi positivi

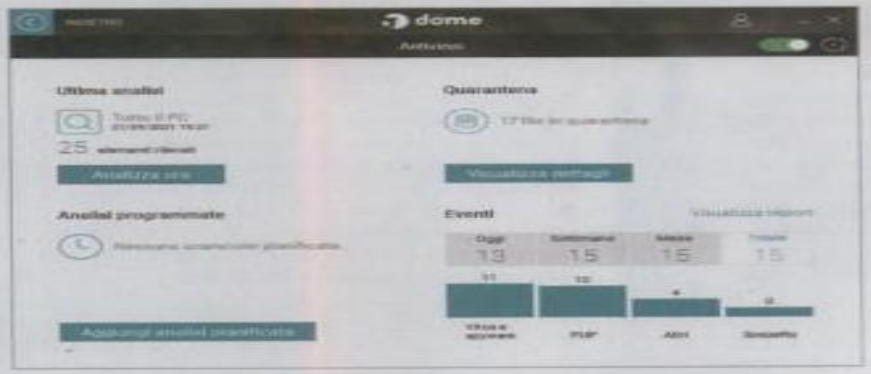
IN BREVE **Panda Free Antivirus protegge gli utenti e i dispositivi personali sfruttando la potenza del cloud. Sicuramente ha l'interfaccia più gradevole da usare nel mercato degli antivirus free.**

L'attivazione di un account remoto è opzionale, ma Panda Free Antivirus ripeterà la richiesta ad libitum se non ne registreremo uno. Nel cloud sempre e comunque.

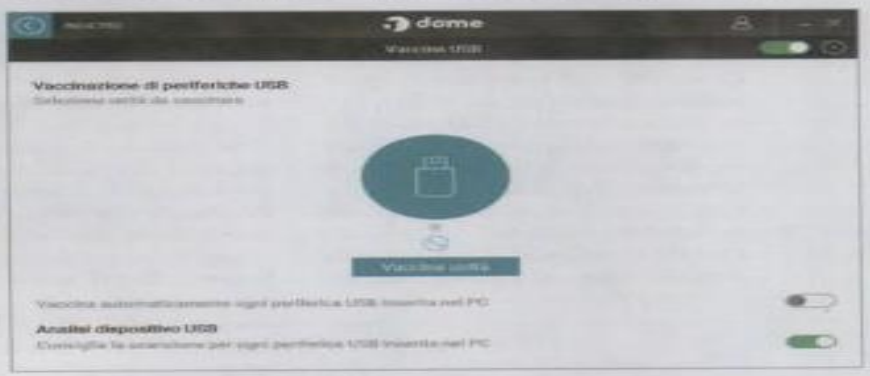
L'interfaccia grafica di Panda Free Antivirus fa ampio sfoggio di rassicuranti paesaggi naturali, animali, insetti e icone per le scansioni e le funzionalità accessorie.

La schermata delle scansioni (che Panda chiama "analisi") permette di controllare le zone critiche del Pc, l'intero sistema o anche una cartella a scelta. Con report dettagliati.

Panda Free Antivirus permette di tenere sempre sotto controllo l'andamento delle scansioni e l'identità delle singole minacce individuate. E volendo di approfondire ogni singolo evento.



La schermata Antivirus offre un riassunto onnicomprensivo delle attività del software antivirale, la quarantena, le operazioni pianificate, gli eventi e le minacce rilevate.



Vaccino USB è una delle funzioni accessorie esclusive di Panda, e dovrebbe garantire la sicurezza dei dispositivi Usb contro il malware eseguibile. Attivabile manualmente o in automatico.

ed eventualmente ripristinare i falsi positivi recuperandoli dalla quarantena. Archiviato il capitolo scansioni, è il momento di addentrarci negli altri elementi funzionali dell'interfaccia di Panda Free Antivirus. L'icona *Antivirus* visualizza la schermata corrispondente e permette di aprire velocemente la finestra della quarantena, avviare una nuova scansione, pianificare una scansione programmata, visualizzare i rapporti sugli eventi. L'icona *VPN* apre una delle funzionalità accessorie di Panda, ovvero la protezione dell'accesso a Internet tramite l'uso di un server "virtuale"; come nel caso di Kaspersky, si tratta di un'opzione estremamente limitata (150 MB di traffico al giorno) con un singolo punto di accesso presente sul territorio nazionale. Dalla schermata *Dispositivi personali* è possibile accedere velocemente al download dei software Panda per altre piattaforme (Mac, Android, iOS), o anche alla lista dei nostri dispositivi personali registrati sull'account remoto di Panda.

La seconda serie di icone della schermata principale apre le porte ad alcune funzionalità aggiuntive potenzialmente interessanti, come ad esempio un *Dark Web Scanner* per verificare la presenza della nostra e-mail in uno dei database venduti illegalmente sulla darknet di Tor (previo accesso all'account Panda), il *Monitor dei processi in memoria*, il *Kit di ripristino* con la creazione di un'unità Usb avviabile. Di particolare interesse è il *Vaccino USB*, funzionalità pensata per rendere i dispositivi Usb immuni ai malware eseguibili. In pratica, il *Vaccino USB* consiste nella neutralizzazione della funzionalità di *autorun* in modo da inibire l'esecuzione di codice potenzialmente malevolo al collegamento di una chiavetta al Pc. È possibile vaccinare a richiesta ogni singola unità Usb oppure procedere alla vaccinazione automatica di tutti i dispositivi collegati al sistema.

Panda Free Antivirus propone una soluzione antimalware che vuole essere contemporaneamente semplice e piacevole da usare, leggera e sicura, e buona parte di questi obiettivi sono raggiunti con l'implementazione della tecnologia *TruPrevent* che fa totale affidamento sugli algoritmi disponibili sui server remoti del cloud per l'identificazione proattiva delle minacce. Secondo Panda non è necessario installare pesanti aggiornamenti quotidiani per aggiungere una gran mole di nuove firme antivirali, anche se a conti fatti gli aggiornamenti automatici dell'antivirus vengono scaricati con una certa frequenza più volte al giorno. Per quanto riguarda la reale efficacia della protezione TruPrevent, invece, le promesse di Panda sembrano coincidere con i risultati dei test di laboratorio specializzati: secondo AV-Comparatives, Panda Free Antivirus offre una protezione quasi perfetta contro le minacce real-world (99,9%) e identifica quasi tutti i sample virali analizzati (99,98%) quando la connessione a Internet è disponibile e pienamente operativa. Se il cloud non è accessibile, invece, Panda raggiunge uno score estremamente mediocre (45,6%) identificando meno della metà dei sample virali scovati da Bitdefender nelle stesse condizioni operative. Estremamente alto è poi il numero di falsi positivi, il più alto (65 falsi allarmi) su 17 antivirus testati. All'utente finale spetta decidere se tali pecche risultino troppo gravi o siano solo il prezzo da pagare per un antivirus comunque efficacie (nel cloud) e graficamente piacevole da usare. ▪

Chi controlla i controllori?

NortonLifeLock

I produttori di antivirus si trovano in una posizione molto delicata, potendo entrare nelle stanze di controllo dei computer degli utenti. E qualche volta si sono approfittati della fiducia degli utenti. Come è accaduto nel 2019 e 2020 con Avast: infatti due diverse indagini hanno evidenziato la raccolta non dichiarata dei dati degli utenti – cronologia di navigazione, ricerche, "ogni singolo clic", acquisti online e altro ancora – tramite l'estensione Avast per browser e lo stesso antivirus. I dati raccolti venivano poi rivenduti ai clienti (cioè alle società pubblicitarie) tramite una società sussidiaria chiamata *Jumpshot*, azienda che è stata in seguito chiusa e liquidata completamente dopo la scoperta della gravissima violazione della privacy a opera della *security enteprise* di Praga. La profilazione nascosta degli utenti è sempre un evento spiacevole da riportare, ma quando tale business viene condotto da una società che dovrebbe proteggere i suddetti utenti da minacce, attacchi e compromissioni della riservatezza si apre una crepa nella fiducia difficile da rimarginare.

Un ultimo aspetto potenzialmente problematico arriva infine dall'acquisizione di Avast da parte di *NortonLifeLock*, operazione da 8 miliardi di dollari annunciata nell'agosto del 2021. Ad acquisizione completata, Norton (corporation fuoriuscita dal conglomerato Symantec alla fine del 2019) diverrà proprietaria di tre dei più popolari antivirus gratuiti in circolazione (Avast, AVG e Avira), e c'è già chi preconizza, in un futuro non molto lontano, la volontà dell'ex-Symantec di dismettere tutta l'offerta freemium a beneficio dei prodotti commerciali per utenti consumer. Un rischio a nostro avviso ancora marginale, visto il gravissimo danno di immagine che ne deriverebbe a livello globale, ma che va tenuto in debita considerazione per prepararsi al peggio.

Verificare le impostazioni del router

Tutti i router moderni sono dotati di firewall e meccanismi di sicurezza integrati, che in teoria dovrebbero mettere le comunicazioni di rete al riparo da malintenzionati, attacchi e pacchetti malevoli.

Controllare che alla teoria corrisponda una effettiva sicurezza pratica non è mai un esercizio superfluo.

Una delle componenti più importanti delle comunicazioni di rete è ovviamente l'infrastruttura dei server Dns, un sistema remoto che svolge il fondamentale compito di tradurre i domini alfanumerici in formato leggibile nei corrispondenti Ip numerici, necessari al trasferimento dati tramite il protocollo Tcp/Ip.

Per controllare che le impostazioni Dns del router funzionino normalmente e non siano stato manomesse, è possibile usare il test

F-SECURE ROUTER CHECKER: basta visitare il sito www.f-secure.com/it/home/free-tools/router-checker , fare clic sul pulsante *controlla il router* ed attendere il risultato del check-up automatico e verificare il risultato del test.

Microsoft dice addio a Windows Vista

Addio ad aggiornamenti e correzioni per eventuali errori o falle nella sicurezza. Come previsto da tempo, a partire da oggi, 11 aprile 2017, Microsoft non supporterà più Windows Vista. Una decisione che obbliga tutti coloro che utilizzano ancora il sistema operativo a migrare verso i successori 7, 8 e 10. Un problema però, che riguarda solo una piccolissima porzione del mercato: lo 0,75% degli utenti. I quali dovranno fare i conti con enormi rischi, in particolare per quanto riguarda la sicurezza.

Microsoft dice addio a Windows 7

WINDOWS 7 va in pensione. Da oggi, 14 gennaio 2020, il sistema Microsoft non gode più del supporto esteso. Ciò vuol dire che ogni pc dotato di questo sistema operativo d'ora in poi sarà maggiormente esposto ad attacchi informatici e virus.

Un utente di Windows 7 da oggi dovrebbe iniziare a pensare di aggiornare il proprio pc a un nuovo sistema operativo, a patto che l'hardware integrato sia adeguato. L'ideale sarebbe passare a Windows 10 sfruttando lo strumento online di Microsoft che consente lo scaricamento e l'attivazione gratuita del software. Il consiglio è di consultare prima i "requisiti minimi di sistema" richiesti e assicurarsi di disporre di una licenza ufficiale di Windows 7. L'altra opzione è quella di puntare su una delle tante distribuzioni Linux gratuite, come ad esempio Ubuntu.

La procedura per installare Windows 10, comunque, è semplice: si accede alla pagina Microsoft, si sceglie la versione (32 o 64 bit), la lingua e si scarica il file (ISO) sul pc. Dopodiché grazie allo strumento “Media Creation tool” - volendo a sua volta scaricabile da Microsoft se non presente - si seguono le istruzioni per caricare il file di installazione direttamente o su un’unità flash USB.

Computer in ostaggio: "Paga il riscatto o perdi tutti i dati"

Este, 25/06/2015

Pareva una semplice mail del corriere espresso. Un avviso che comunicava la giacenza di un pacco e che invitava ad avviare una procedura per il ritiro dello stesso. Pareva. Invece quella mail maledetta e quel clic galeotto sono costati ad Antonio Zaglia, patron della libreria Gregoriana, almeno tre giorni di ansia e quasi 2 mila euro di danno. Il libraio di Este è stato letteralmente "ostaggio" di un virus ed è riuscito ad uscire dall'incubo solo con il pagamento di un "riscatto". Robe da film e da guerre cybernetiche, ma che in realtà sono in agguato anche nei computer di casa.

L'episodio. La settimana scorsa Antonio Zaglia, titolare della nota libreria di via Cavour, ha ricevuto una mail con il logo della Sda, una delle principali azienda di spedizioni. «La mail spiegava che il corriere non aveva trovato nessuno in negozio e che quindi c'era un pacco in giacenza», spiega Zaglia. «Mi veniva dato un codice di spedizione e venivo invitato a scaricare un modulo per avviare una nuova consegna. Vuoi perché settimanalmente mi arrivano pacchi di libri con questa azienda, vuoi perché avevo dei clienti in negozio e non ero attentissimo, ho cliccato quel link e di fatto ho dato il via al disastro». Nel giro di qualche ora la maggior parte dei dati nel pc di Zaglia – ordini, contabilità, dati sensibili - sono diventati inaccessibili. Tecnicamente, criptati.

Il ricatto. «È quindi comparsa una schermata che mi intimava a versare 300 euro entro 90 ore, con tanto di countdown», continua il commerciante. «Nel caso non avessi pagato quella cifra, il "riscatto" sarebbe raddoppiato e poi, dopo altre 90 ore, ogni dato sarebbe stato definitivamente cancellato». Compresa la gravità della situazione, Zaglia si è prima rivolto alla Guardia di Finanza e quindi alla Polizia postale: i primi hanno giustamente rinviato la competenza ai secondi, i secondi hanno amaramente spiegato al libraio che c'era poco da fare e che comunque sarebbe servito del tempo. Tempo che, ovviamente, Zaglia non aveva. È quindi scattata la ricerca al consulente più afferrato in materia: tra un consiglio e l'altro, al titolare della Gregoriana non è rimasto che pagare.

Moneta virtuale. Pagare il riscatto è stato tutt'altro che facile. Per pagare i 300 euro si potevano infatti utilizzare solamente canali difficilmente rintracciabili, utilizzando i cosiddetti bitcoin, una sorta di moneta virtuale. Un bitcoin vale oggi 215,29 euro; se ne possono acquistare non più di uno al giorno, proprio per evitare pagamenti illeciti o facili estorsioni. Zaglia ha quindi dovuto attendere altre 24 ore per acquistare il secondo Bitcoin e quindi versare i 300 euro in un portafoglio di rete le cui coordinare sono state date all'ultimo. «Proprio come in un sequestro di persona», ha commentato lo scrittore Giancarlo Marinelli, tra i clienti più fedeli di Zaglia In pochi minuti tutti i file "presi in ostaggio" sono stati sbloccati e Zaglia ha potuto tirare un sospiro di sollievo. Circostanza non scontata: la letteratura web racconta infatti che molte vittime avrebbero pagato senza aver mai ottenuto la decifrazione dei propri dati.

Conto salato. Quanto è costato lo scherzetto? Oltre ai 430 euro di bitcoin, il commerciante ora dovrà resettare e ripulire i propri pc, dotarsi di software antivirus più aggiornati ed evidentemente rivolgersi a dei tecnici preparati in materia. Se a questo si aggiungono i tre giorni di lavoro persi, le ansie e i giri per la città alla ricerca di una valida soluzione, il conto supera certamente i duemila euro. E tutto per colpa di un clic sovrappensiero.

Virus Cryptocker (Mattino di Padova del 30/03/2016)

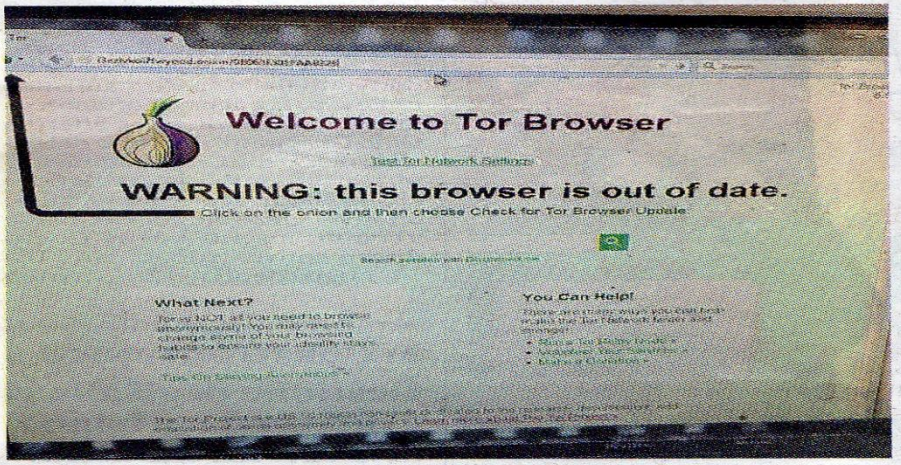
"Cryptolocker" colpisce un'azienda padovana

Apre una mail inviata dal suo stesso indirizzo e tutti i dati del suo pc scompaion e arriva la richiesta di "riscatto": imprenditrice si rivolge alle forze dell'ordine

di Elena Livieri

Il temuto virus "Cryptolocker" è arrivato anche in città. A farne le spese un'azienda padovana finita nel mirino del potente baco informatico che - arrivando sotto le mentite spoglie di normali e ami - è in grado di criptare tutti i contenuti della memoria del computer, rendendone impossibile la visione al proprietario. Salvo, ovviamente, che accetti di pagare in cambio di avere di nuovo accesso alla sua memoria. Una vera e propria forma di estorsione che corre sul web.

Nei giorni scorsi si è presentata al comando provinciale dei carabinieri la titolare di un'azienda padovana denunciando di aver ricevuto una mail sul suo pc che riportava il suo stesso indirizzo di posta elettronica, come se l'invio fosse partito da lei stessa. La donna ha commesso l'errore di aprire la mail e in quel momento il virus ha colpito. Senza pietà. Tutti i file, le icone, i dati dei clienti, ogni cosa che era contenuta nella memoria del computer è sparita. Come dissolta nel nulla. Anni di contatti e documenti polverizzati con un click.



Una delle forme in cui il virus "Cryptolocker" si manifesta sul pc

Poco dopo la seconda amara sorpresa: sul desktop del pc sono comparse alcune icone che riportavano la richiesta di un "riscatto", per una cifra di circa 1.120 euro, per rientrare in possesso dei dati volatilizzati. A quel punto l'imprenditrice ha deciso di rivolgersi alle forze dell'ordine e dai carabinieri l'indagine è stata girata alla polizia informatica che sta cercand di risalire agli autori dell'a tacco.

La raccomandazione dell forze di polizia, che stann registrando un numero cre scente di casi di estorsion tramite il viru "Cryptolocker" raccomanda no di non aprire mai le e ma sospette.

Di solito il pericoloso viru si nasconde in e mail inviat apparentemente da cono scenti, amici, familiari o co rieri - ma con diciture inusua li nel campo dell'oggetto, ta volta anche una serie di lett re e cifre - e basta aprire un a legato perché il virus intacch il sistema. E puntuale, subit dopo, arriva la richiesta di d naro affinché l'infezione ver ga rimossa e il proprietari del computer torni in posse so dei suoi dati. Una vol che "Cryptolocker" ha colp to, poi, non è affatto det che pagando gli estorsori situazione si risolva. Motiv per cui, a maggior ragione, polizia raccomanda la mass ma prudenza.

I pirati entrano nel nostro smartphone

I PERICOLI PIU' DIFFUSI:

- Spyware che controllano le nostre attività sul telefono come chiamate, email e messaggi;
- Malware in grado di trasmettere al criminale di turno i dati di accesso dei nostri account e quelli delle carte di credito;
- Virus di ogni tipo che possono trasformare il nostro telefono in un dispositivo zombie al servizio degli hacker;
- Ramsomware che criptano i nostri dati, comprese le chat o le immagini scattate dalla fotocamera del telefono e ci chiedono un riscatto per riaverli indietro.

COME PROTEGGERE IL NOSTRO TELEFONO:

- Non scarichiamo mai applicazioni di terze parti dagli store non ufficiali;
- Controlliamo quali privilegi servono per utilizzare un'app … spesso quelle dannose ci chiedono senza motivo di accedere, per es., alla rubrica, alle email od alle impostazioni del telefono;
- Quando possibile aggiorniamo il sistema operativo;
- Per maggiore sicurezza installiamo un anti-malware (Android = 360 Mobile Security, Avast Mobile Security & Antivirus, Lookout Security & Antivirus)

Capire se un telefono è infetto

In generale, un improvviso peggioramento nella durata della batteria può indicare che un'App sta lavorando senza che nessuno l'abbia avviata. Controlliamo spesso quali delle nostre App usano più energia: per farlo, con Android, basta entrare in Impostazioni – Batteria … cancelliamo tutte le piccole App troppo affamate di cui non conosciamo con certezza la provenienza e che magari non usiamo mai. A questo punto entriamo in Impostazioni – Utilizzo dei dati … quando un'App una molti dati senza un valido motivo (ad es. la torcia o la calcolatrice) c'è qualcosa che non va. In alcuni casi è la bolletta telefonica a dirci se abbiamo un malware, se scopriamo qualche voce di spesa diversa dal solito. Lo stesso può valere per le carte di credito od il conto in banca: spesso i malintenzionati, prima di sottrarci grosse somme, iniziano con piccole somme per verificare che tutto funzioni.

Aggiorna TUTTI i programmi del tuo PC…

- Installa **TUTTI gli aggiornamenti** di sicurezza non appena sono disponibili
- Assicurati di farlo **per TUTTI i programmi** presenti sul tuo PC
- Sei hai un PC con Windows hai gli **aggiornamenti automatici già attivi**: se possibile, abilitali anche per gli altri programmi che usi

SCOPRI INSIEME AI TUOI GENITORI COME al link

http://windows.microsoft.com/it-IT/windows/help/windows-update

Usa e attiva un Firewall per Internet

- **Il firewall è come un muro** intorno ad un castello, crea una barriera tra il tuo computer e Internet
- Se hai un PC con Windows, **il Firewall è già presente e attivo**: verifica solo che sia ancora abilitato (Centro di Sicurezza)

Di Alfonso Maruccia

WINDOWS FIREWALL CONTROL

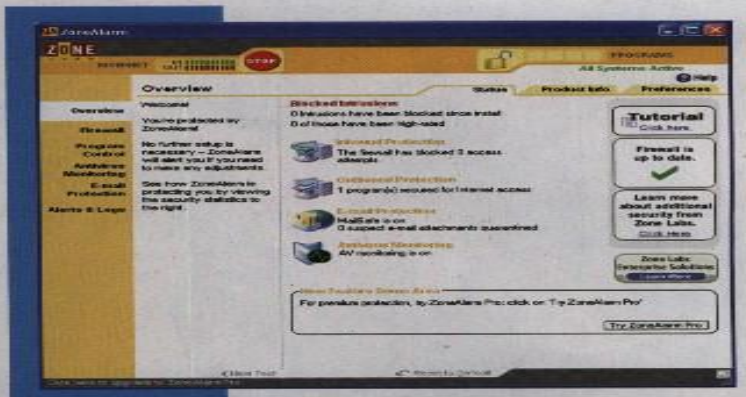
PROTEZIONE ASSOLUTA

Guida all'utilizzo dell'applicazione in grado di migliorare la gestione del firewall nativo dei sistemi operativi Microsoft. Un'utility freeware assolutamente indispensabile.

FINO A POCHI ANNI OR SONO, QUANDO INTERNET ERA ANCORA UNA TERRA DI NESSUNO IN CUI GLI ATTUALI MONOPOLI DI FATTO DEL CLOUD E DELLE "PIATTAFORME" OMNICOMPRENSIVE NON ERANO ANCORA EMERSI IN TUTTO IL LORO MONOLITICO FULGORE, GLI UTILIZZATORI DI PERSONAL COMPUTER WINDOWS ERANO OBBLIGATI A CIRCONDARSI DI SOFTWARE DI SICUREZZA DI TERZE PARTI, STRUMENTI SECONDARI, MA INDISPENSABILI A GARANTIRE UNA NAVIGAZIONE TRANQUILLA NEI MARI BURRASCOSI DELLA RETE TELEMATICA MONDIALE. UNO DEGLI ELEMENTI ESSENZIALI DI QUESTO TOOLKIT DI NAVIGAZIONE TRANQUILLA ERA IL FIREWALL DI RETE, UN TOOL IN GRADO DI TENERE FUORI DALLA PORTA (DEL MODEM) WORM E CYBER-CRIMINALI MA GENERALMENTE FORIERO DI CONFLITTI E PROBLEMI DI GESTIONE QUANDO USATO ASSIEME AI CLIENT DI FILE SHARING O AD ALTRI SOFTWARE CHE FACEVANO UN USO INTENSIVO DI INTERNET.

Nomi come *ZoneAlarm* e *Comodo Firewall* saranno certamente riconoscibili a chi ha vissuto (pericolosamente?) quell'era della telematica mondiale in ambito consumer, e altrettanto certamente evocheranno ricordi di poco piacevoli di porte che non si aprono, crash, "livelli" di apertura del firewall che non hanno gli effetti sperati rendendo l'esperienza di rete alquanto accidentata.

Oggi, nel 2018, le cose sono cambiate in un modo che non era possibile prevedere anche solo dieci anni fa: anche Windows è entrato a far parte del novero dei sistemi operativi dotati di un firewall – anzi di una "piattaforma" di filtraggio dei dati – pienamente operativo e degno di tale nome, mentre gli attori malevoli si sono evoluti di pari passo con le misure di sicurezza esplorando nuovi vettori di attacco. Il firewall di Windows è un componente essenziale del sistema, ma com'è tradizione della corporation di Redmond non include tutti gli strumenti utili a rendere l'utente pienamente padrone del suo funzionamento. Il mercato delle utility di terze parti si è ridimensionato ma è ancora piuttosto attivo e produce software come quello oggetto di questa guida: **Windows Firewall Control** (WFC) è un'applicazione progettata per estendere le funzionalità del Firewall di Windows, fornendo altresì nuove opzioni extra in grado di migliorare ulteriormente il funzionamento del suddetto firewall. WFC rientra di diritto nella categoria delle utility indispensabili per gli OS Windows, e ora che è stato acquisito da *Malwarebytes* (nel maggio del 2018) ed è disponibile a titolo assolutamente gratuito – con le funzionalità prima a pagamento sbloccate per tutti gli utenti – non esiste davvero alcuna scusa per non scaricare e installare l'applicazione.



ZoneAlarm, un nome capace di evocare ricordi non proprio piacevoli...

BREVE STORIA DEL FIREWALL

Dalle barriere fisiche contro gli incendi a quelle virtuali contro i pericoli in agguato sulla Rete.

La definizione generica più comune descrive il firewall come un sistema per la sicurezza di rete in grado di monitorare e controllare il traffico in entrata e in uscita, una barriera progettata per funzionare secondo regole di sicurezza predefinite e tradizionalmente posta a salvaguardia di una rete interna "trusted" (come ad esempio una LAN domestica) dai pericoli provenienti da una rete esterna "untrusted" come Internet.
Il termine "firewall" era in origine usato per indicare una barriera – ad esempio un muro – resistente al fuoco e usata per prevenire la diffusione di incendi in un edificio, un aereo o altri tipi di strutture. Solo negli anni '80, quindi prima che Internet divenisse di pubblico dominio, si è cominciato a usare il termine anche in ambito di sicurezza per le tecnologie di rete che andavano sostituendo i router delle origini. L'evoluzione dei firewall è passata attraverso tre diverse generazioni (filtri di pacchetti, *stateful filter*, firewall di applicazioni), mentre le due categorie in cui oggi vengono generalmente classificati i firewall sono i firewall di rete e quelli *host-based*. Nel primo caso si parla di firewall deputati al controllo delle comunicazioni fra due o più network, il secondo tipo include i firewall software pensati per girare su computer e controllare il traffico di rete da e verso queste macchine.

Il firewall di Windows è quindi un classico firewall per host, visto che ha il compito di sovraintendere le comunicazioni di rete per i Pc su cui è installato il sistema operativo Microsoft. La prima incarnazione del firewall di Windows, allora chiamata "*Internet Connection Firewall*", è arrivata assieme a Windows XP nell'ottobre del 2001 ma aveva un'utilità piuttosto limitata.
Infatti il tool era disabilitato di default per evitare problemi di compatibilità con il software dell'epoca, e solo con il debutto dell'ormai leggendario Service Pack 2 – e in seguito a incidenti di sicurezza telematica di altissimo profilo come i worm Blaster e Sasser – è stato migliorato al punto da divenire utilizzabile

Windows XP, il debutto del firewall di Redmond.

Il firewall protegge la rete interna dai pericoli esterni.

anche dall'utente comune. Il 2006 ha segnato il debutto di Windows Vista, sistema operativo spesso additato come un autentico disastro – anzi un "Vistastro" – per l'intera industria dei PC ma che ha gettato le fondamenta di tecnologie oggi molto importanti per l'ecosistema Windows. Una di queste novità tecnologiche è l'implementazione della cosiddetta *Windows Filtering Platform* (WFP), un insieme di servizi di sistema e interfacce di programmazione (API) progettate per facilitare l'interazione fra le applicazioni di terze parti e lo stack di rete di nuova generazione (IPv4/IPv6) incluso nel sistema.

La piattaforma si incarica di processare i pacchetti di dati in arrivo e in partenza da e verso la rete, gestendo altresì il filtraggio dei pacchetti indesiderati sulla base delle regole del firewall configurate dall'utente o dal sistema.

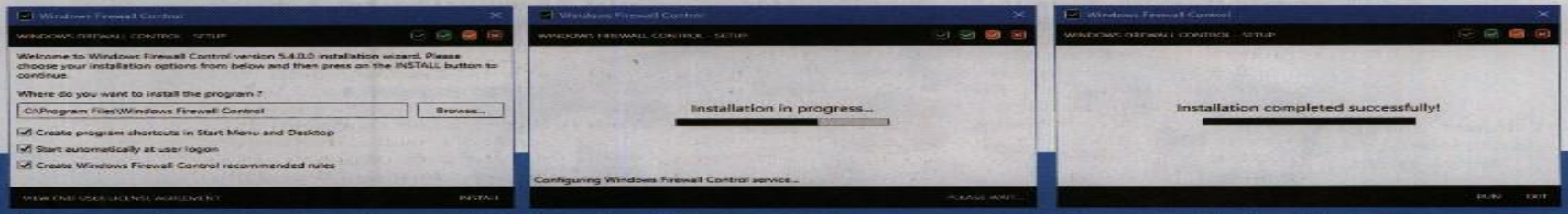
Anche il firewall di Windows 10 è basato su WFP e sui miglioramenti apportati alla piattaforma da Windows 7 (o anche Windows Server 2008 R2). Il compito di Windows Firewall Control è appunto quello di rendere *user-friendly* la gestione del firewall nativo di Windows sfruttando il filtraggio e i meccanismi di controllo della piattaforma WFP, un approccio che garantisce il massimo livello di compatibilità con le applicazioni di rete che girano sul Pc ma che soffre degli stessi limiti del firewall di Windows come vedremo in seguito.

GUIDA A WINDOWS FIREWALL CONTROL

Ecco come installare, configurare e ottimizzare il compagno ideale per il Firewall di Windows.

INSTALLAZIONE E CONFIGURAZIONE DI BASE

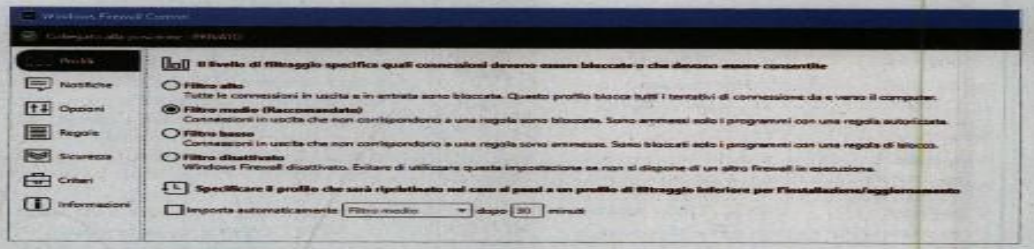
L'ultima versione di WFC è scaricabile direttamente dal sito ufficiale, su *https://www.binisoft.org/wfc*, oppure su uno dei mirror indicati dalla succitata homepage; la versione più recente del tool disponibile al momento di scrivere è la 5.4.0.0, aggiornata all'1 agosto 2018. I requisiti indispensabili per l'uso di WFC 5.4 includono .NET Framework 4.5 (già integrata su Windows 10), e un sistema operativo Windows (10, 8.1, 8, 7, Server 2016, Server 2012) a 32 o a 64-bit; il servizio di sistema di Windows Firewall (*MpsSvc*) deve essere ovviamente abilitato e in funzione, e lo stesso vale per il servizio per Client DNS (*Dnscache*). Una volta verificato tutto il necessario, è possibile procedere all'installazione lanciando l'installer *wfc5setup.exe*.



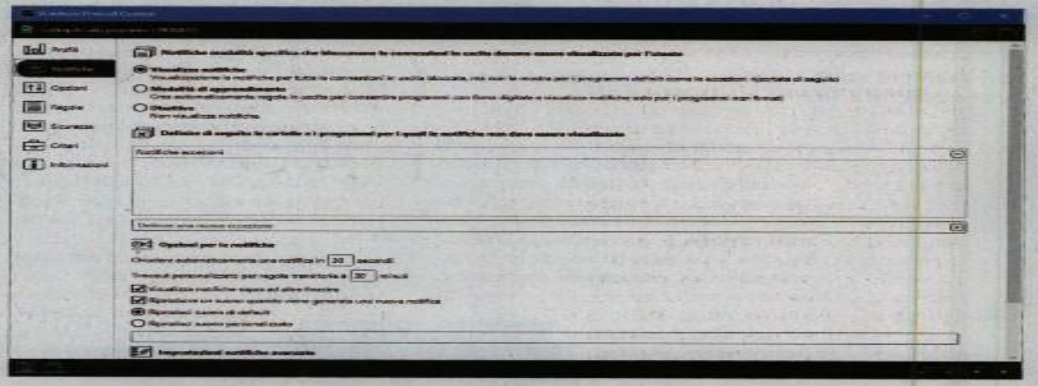
Chiara, semplice e veloce: l'installazione di Windows Firewall Control è la fase meno complicata del processo di setup del programma. Il bello viene immediatamente dopo la fine dell'installazione.

Il programma di installazione chiederà di confermare (o modificare) la cartella in cui copiare i file di WFC, permettendo altresì di creare link nel menu *Start* e sul desktop, di avviare automaticamente l'applicazione all'accesso del nostro profilo utente (opzione ALTAMENTE consigliata per usare al meglio il firewall) e di creare una serie di regole "raccomandate" per facilitare l'integrazione tra WFC e il sistema.
Dopo una breve attesa il processo di installazione sarà concluso, e si potrà cominciare a usare WFC per gestire in modo pratico ed efficiente il Firewall nativo di Windows 10. Nonostante la sua indubbia utilità, una volta installato e configurato WFC "pesa" davvero poco sul sistema con circa 6,15 megabyte di spazio occupato su disco, 15 nuove chiavi create nel Registro di Windows e un singolo servizio di sistema necessario al funzionamento del software (*wfcs*). WFC include il supporto multilingua, e volendo personalizzare ulteriormente il tool possiamo scaricare il file necessario alla traduzione in italiano dalla homepage (link veloce: *https://www.binisoft.org/get.php?translation=wfcIT.lng*); una volta scaricato, il file deve essere copiato nella cartella in cui abbiamo installato il software. Al successivo riavvio, WFC caricherà il file e risulterà quindi localizzato nella lingua del Belpaese.

Una volta attivato, WFC segnalerà la propria presenza con una nuova icona nel Systray; facendo clic sull'icona avremo accesso all'interfaccia principale del software. Per cominciare a sfruttare subito le funzionalità più utili di WFC, la prima cosa da fare è scegliere il *Profilo* con il livello di filtraggio che desideriamo imporre alle connessioni di rete: il **Filtro alto** indica un blocco totale di tutte le connessioni in entrata e in uscita, il **Filtro medio blocca le connessioni in uscita per cui non esiste una regola specifica nel firewall**,



Dalla pagina Profili è possibile impostare il livello di filtraggio con cui desideriamo gestire le connessioni di rete.

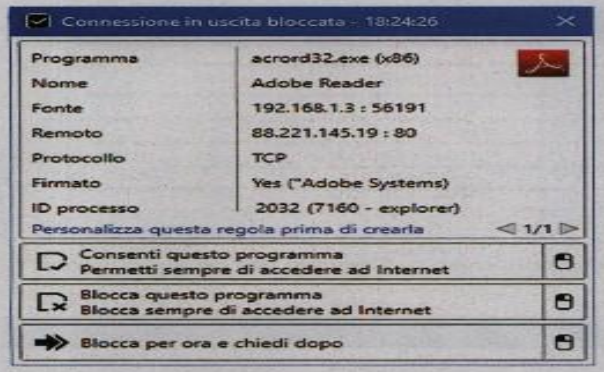


Il pannello delle Notifiche permette di impostare la funzionalità forse più importante di Windows Firewall Control, vale a dire quella delle Notifiche Interattive.

Filtro basso permette a qualsiasi connessione di passare il firewall a eccezione dei programmi per cui già esiste una regola di blocco. Con **Filtro disattivato** il Firewall di Windows viene completamente spento, ed è infine possibile specificare il passaggio automatico a un profilo specifico (scegliendo tra Filtro alto e Filtro medio) dopo X minuti. Il nostro consiglio, come pure quello di WFC, è di impostare il Filtro medio: in questo modo si otterrà il massimo livello di sicurezza con il massimo della praticità di uso del firewall di sistema.
Un'altra funzionalità indispensabile per trarre il massimo da WFC è quella delle Notifiche, da attivare nell'apposita finestra selezionando l'opzione **Visualizza notifiche**: in questo modo, a ogni connessione bloccata WFC presenterà una finestra interattiva da cui sarà possibile decidere il da farsi – se cioè continuare a bloccare la connessione o se impostare una regola di comportamento diversa.

NOTIFICHE

A conti fatti le notifiche rappresentano il "cuore" di WFC, una caratteristica che rende il tool un comprimario indispensabile per sfruttare il Firewall di Windows al meglio delle sue possibilità rimediando all'unica, grave



Un esempio delle notifiche visualizzate quando viene bloccata una connessione.

mancanza che ancora affligge il componente dell'OS Microsoft: quando un'applicazione prova ad accedere a Internet senza che in precedenza sia stata impostata una regola, il firewall di sistema blocca i pacchetti di dati corrispondenti generando un nuovo evento nel *Log* degli eventi di sicurezza. WFC è programmato per tenere sotto controllo il suddetto Log, e ogni volta che un pacchetto di dati viene dismesso dal firewall decide se visualizzare o meno una notifica di connessione bloccata.

La notifica di *Connessione in uscita bloccata* identifica il programma che ha provato ad accedere alla Rete esterna con relativo file eseguibile, l'IP di origine dell'evento e l'IP remoto che l'eseguibile stava provando a contattare, il protocollo di rete utilizzato, l'eventuale presenza di una firma digitale valida, l'ID del processo di sistema. L'utente può quindi decidere di consentire una nuova connessione del programma bloccato in modo permanente o per un periodo di tempo limitato (in quest'ultimo caso facendo clic con un tasto del mouse accanto all'opzione *Consenti questo programma*), bloccare l'accesso del programma a Internet in modo permanente o temporaneo (clic del mouse accanto a *Blocca questo programma*), bloccare l'uscita del programma dal firewall rinviando la decisione definitiva a una successiva istanza dell'evento.

In base alla decisione dell'utente, WFC creerà una regola permanente o temporanea che il firewall di Windows rispetterà da qui in poi. La notifica di connessione bloccata scompare dopo 30 secondi di attesa andata a vuoto, e permette una personalizzazione veloce della regola del firewall prima della sua creazione tramite la voce *Personalizza questa regola prima di crearla*. In precedenza le notifiche di connessione bloccata erano utilizzabili solo dagli utenti a pagamento, ma ora che WFC è disponibile in via del tutto gratuita sono utilizzabili da tutti senza limitazioni di sorta.

Il comportamento delle notifiche può poi essere modificato in dettaglio dal pannello delle *Notifiche* sull'interfaccia principale di WFC: come abbiamo già visto da questa finestra è possibile attivare la visualizzazione delle notifiche, attivare le notifiche in "modalità apprendimento" (tutti i programmi con una firma digitale valida vengono fatti passare senza blocco della connessione), disattivare le notifiche, definire una serie di cartelle e programmi per cui le notifiche non devono essere visualizzate, cambiare le temporizzazioni per la chiusura automatica delle notifiche e la durata delle regole transitorie, visualizzare le notifiche al di sopra di tutte le altre finestre o meno, riprodurre un suono in concomitanza con una nuova notifica, impostare il comportamento avanzato delle notifiche per minimizzare l'insorgere di incompatibilità o conflitti con gli altri software di sicurezza.

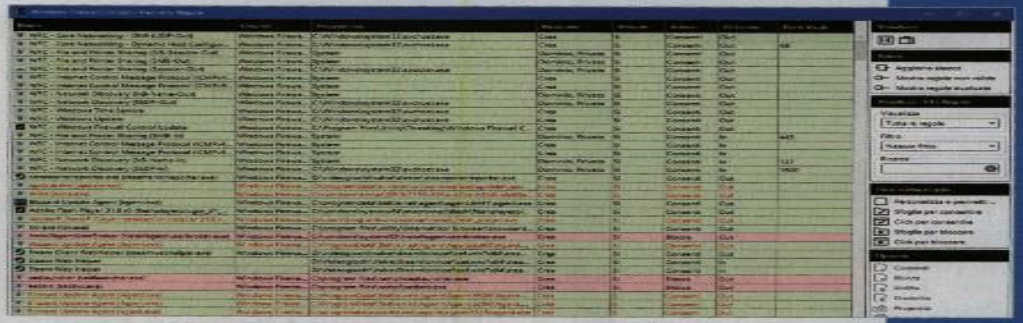
Le notifiche sono il "cuore" di WFC, una caratteristica che rende il tool indispensabile per sfruttare il Firewall di Windows al meglio

REGOLE DEL FIREWALL E LOG DELLE CONNESSIONI

Escludendo le più che indispensabili notifiche, i due pannelli di controllo più utili a "tarare" il firewall di Windows sulle nostre specifiche esigenze solo il pannello delle *Regole* e il log delle connessioni *Bloccato di recente*. È possibile accedere a questi pannelli tramite le due icone presenti in basso a sinistra sul pannello principale di WFC.

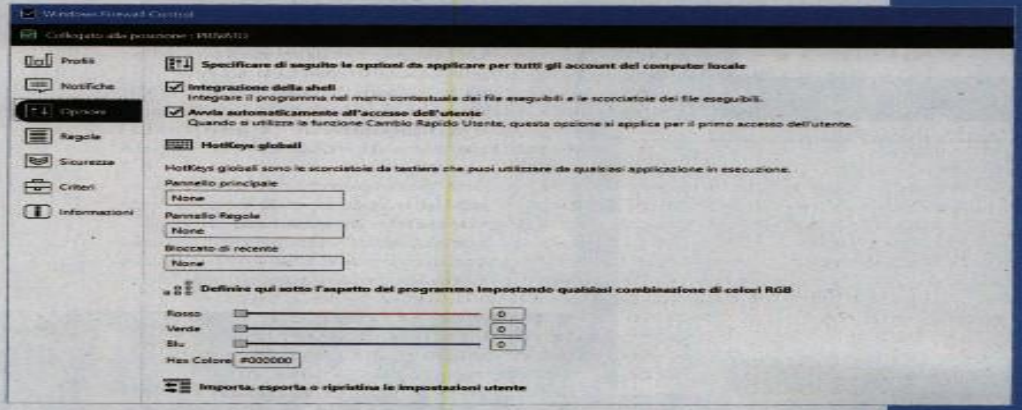
Il Pannello Regole presenta una lista ordinata cronologicamente delle regole esistenti nel firewall di Windows, con una descrizione dettagliata di tutte le informazioni utili sul programma a cui la regola fa riferimento, il gruppo a cui appartiene la regola, la posizione, lo stato di attivazione o meno della regola, la direzione delle comunicazioni (in uscita o in entrata), le porte locali, gli indirizzi remoti, il protocollo usato e molto altro ancora.

Le regole in verde sono quelle che consentono la connessione, quelle con sfondo rosato sono quelle che la bloccano e quelle in rosso fanno riferimento a programmi o eseguibili non più presenti sul sistema. Servendosi dei menù disponibili sulla destra, l'utente può effettuare una scrematura veloce delle regole visualizzando solo quelle non valide o quelle duplicate – entrambe eliminabili senza problema – cercare una regola specifica, creare manualmente una nuova regola (consigliato solo ai veri smanettoni), agire su una o più regole selezionate col mouse o con la tastiera (tramite le *Opzioni* di destra o agendo col tasto destro del mouse) consentendo la connessione, bloccandola per tutte le regole, disabilitando o abilitando le regole, creando duplicati, eliminando le regole o controllando un file sullo scanner



Dal Pannello delle Regole è possibile agire manualmente sulle regole create da Windows Firewall Control per il firewall nativo di Windows.

Le connessioni Bloccate di recente erano molto utili soprattutto quando le notifiche interattive di WFC erano a pagamento.



Il fondamentale Pannello delle Opzioni, per personalizzare il comportamento di Windows Firewall Control sul sistema Windows 10.

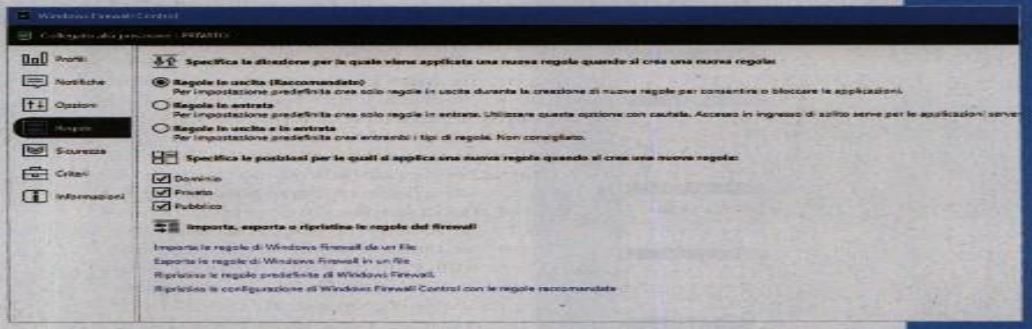
online di *VirusTotal*.

Il pannello delle connessioni *Bloccato di recente* fa esattamente quel che dice, presenta cioè la cronologia delle connessioni bloccate dal firewall di Windows nel rispetto delle regole impostate dall'utente. Si tratta di un pannello forse meno utile di quello delle regole del firewall trattato in precedenza, soprattutto se abbiamo abilitato le notifiche per le connessioni bloccate di WFC. Tuttavia avere una panoramica dettagliata delle connessioni bloccate di recente può servire a risolvere eventuali problemi con gli applicativi di rete, e anche col pannello in oggetto è possibile (con le opzioni a destra o tramite il tasto destro del mouse) filtrare la visualizzazione delle connessioni, consentire una connessione, creare regole del tutto nuove, verificare la sicurezza di file e indirizzi IP.

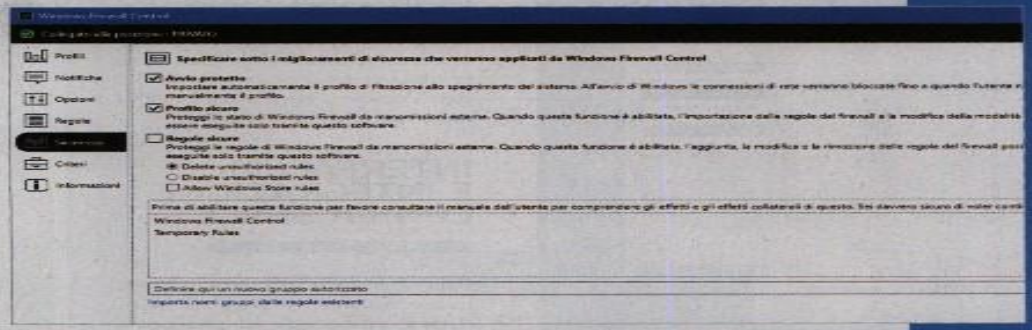
INTERFACCIA E INTEGRAZIONE CON LA SHELL

Facendo clic sull'icona di WFC presente nel Systray di Windows, si accede al pannello di controllo del software. Di Profili e Notifiche abbiamo già parlato in precedenza, quindi ora è il momento di analizzare la finestra delle *Opzioni*: abilitando l'opzione *Integrazione della shell*, WFC sarà disponibile anche nel menù contestuale (accessibile col tasto destro del mouse) per consentire o bloccare velocemente la connessione di un programma o un eseguibile a Internet; l'opzione *Avvia automaticamente all'accesso dell'utente* serve poi a garantire che WFC prenda il controllo del firewall di sistema subito dopo il logon, l'avvio o il riavvio di Windows.

Grazie alla funzionalità *HotKeys globali* è possibile impostare tre diverse scorciatoie da tastiera (del tutto opziona-



Dalla pagina delle Regole di WFC è possibile configurare la creazione delle regole del Firewall e le posizioni della rete a cui applicarle.

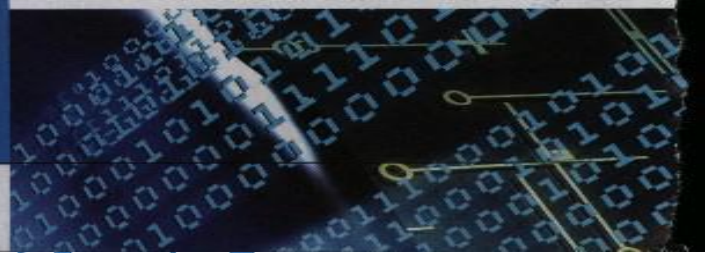


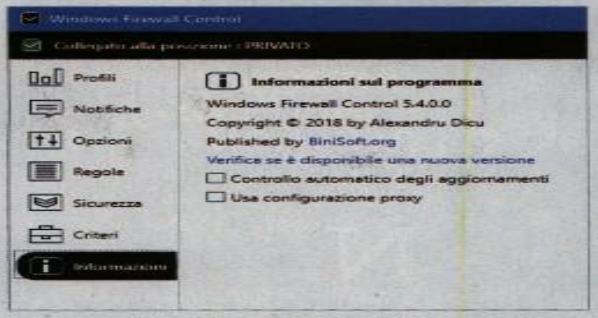
Il pannello Sicurezza include una serie di impostazioni aggiuntive in grado di rafforzare la sicurezza di WFC e del sistema.

Il pannello Criteri include i link veloci alle utilità native di Windows e gli URL dei servizi usati per i controlli di sicurezza.

li) per accedere velocemente al *Pannello principale* del software, al *Pannello Regole* del firewall e al log delle connessioni *Bloccato di recente*. Agendo sui tre slide dei colori Rosso, Verde e Blu si può modificare la tonalità cromatica dell'interfaccia, mentre con gli ultimi tre comandi presenti in basso è possibile esportare le impostazioni utente di WFC, importare le impostazioni salvate in precedenza e ripristinare tutte le impostazioni ai valori di default.

Dal pannello delle Regole è poi possibile modificare il comportamento di WFC durante la creazione delle regole del firewall, specificando cioè se si desidera creare solo regole per le connessioni in uscita, solo regole in entrata o per le connessioni in entrambe le direzioni. L'impostazione raccomandata è quella di creare solo regole in uscita, ed è quella che consigliamo di usare anche noi: Windows Firewall prevede un trattamento "speciale" per le connessioni in entrata senza l'intervento di tool esterni (vedi box di approfondimento). Le regole possono poi essere applicate alle diverse categorie di reti supportate dal firewall di sistema (*Dominio, Privata, Pubblica*) ed è consigliabile selezionare tutte e tre le opzioni disponibili. Le ultime opzioni della pagina servono a importare ed esportare le regole attuali del firewall, ripristinare le regole predefinite e ripristinare la configurazione base di WFC con le regole raccomandate.
Sul pannello *Sicurezza* è possibile impostare le opzioni di sicurezza aggiuntive di WFC, scegliendo l'*Avvio protetto* se si vuole avviare Windows 10 con tutte le connessioni di rete bloc-





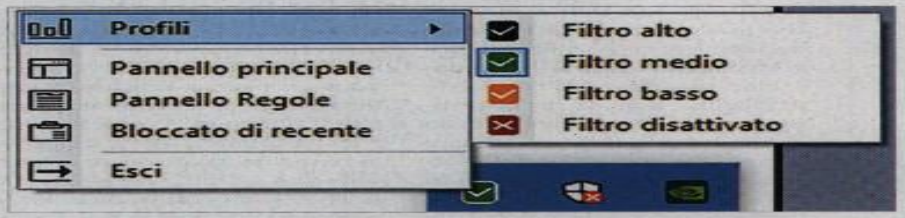
La pagina delle Informazioni su WFC con tanto di copyright, controllo update e proxy.

cate (molto utile per i paranoici o per chi non si fida più delle politiche di Microsoft), impostando il *Profilo sicuro* per inibire il controllo del firewall di Windows con applicazioni esterne che non siano WFC, abilitando le *Regole sicure* per proteggere le regole del firewall da manomissioni esterne. Quest'ultima opzione va utilizzata con molta attenzione, visto che WFC chiederà l'autorizzazione all'utente per cancellare o disabilitare le regole create da ambienti esterni a WFC. Nella maggior parte dei casi è consigliabile non servirsi delle Regole sicure per evitare problemi di incompatibilità o malfunzionamenti dei software installati.

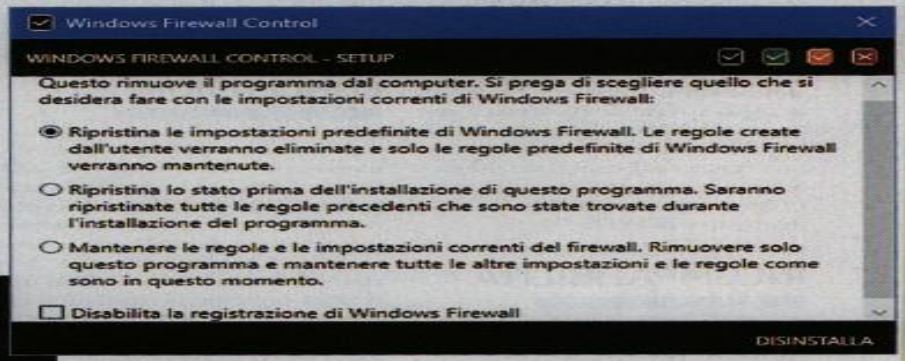
Dalla pagina dei *Criteri* (fig. 17) si può accedere velocemente alle utilità di Windows connesse al firewall di sistema, alla pagina del Visualizzatore eventi dedicata a WFC e al tool per il Monitoraggio delle risorse hardware. È poi possibile visionare o modificare gli URL usati per verificare online la reputazione di un indirizzo IP (*Ipvoid*), il controllo degli hash SHA256 (*VirusTotal*), le ricerche nel database WHOIS, le informazioni sulle porte di rete (*Grc.com*).

La pagina delle *Informazioni* è utile per verificare la versione di WFC in uso o l'eventuale disponibilità di un aggiornamento. Le due icone in alto a destra dell'interfaccia sono utili rispettivamente a proteggere la configurazione di WFC tramite l'utilizzo di una password e ad accedere al manuale del software (disponibile solo in inglese). Le quattro icone in basso a destra, invece, sono un retaggio delle vecchie versioni di WFC (dove le notifiche interattive erano riservate solo agli utenti paganti) con cui è possibile selezionare il programma (o meglio il relativo file eseguibile) per cui si vuole consentire o bloccare la connessione verso la Rete, oppure fare clic sulla finestra di un programma già attivo da bloccare o meno sul firewall. Tanto lavoro manuale che a nostro avviso non ha più molta ragion d'essere, ora che le *Notifiche* sono utilizzabili liberamente da tutti.

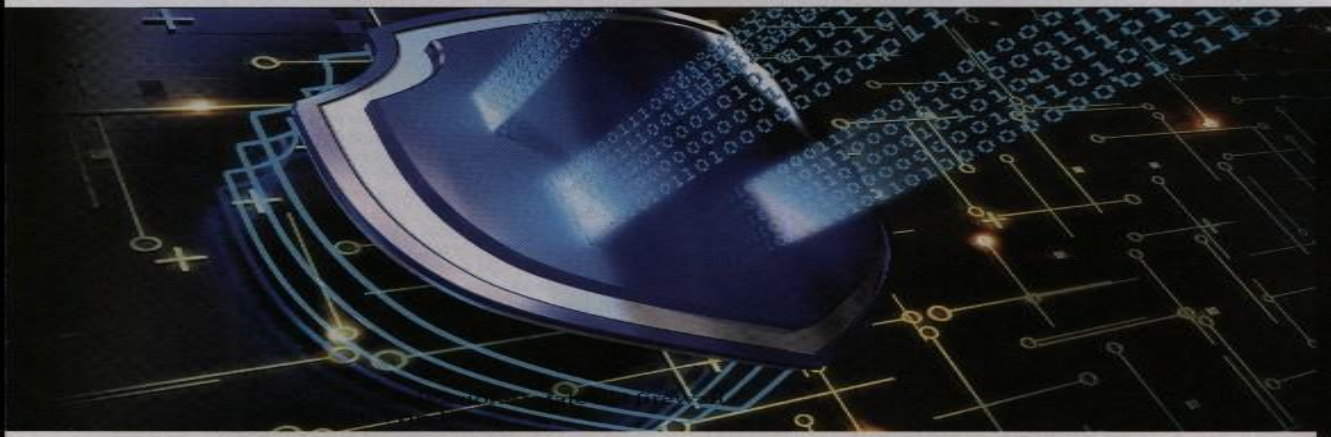
Per finire, anche l'icona di WFC nell'area di notifica del sistema operativo fornisce alcune scorciatoie alle funzionalità più utili del tool: facendo clic col tasto destro del mouse sulla suddetta icona, si potranno aprire velocemente il *Pannello Principale*, il *Pannello Regole* del firewall e la pagina delle connessioni *Bloccate di recente*, mentre un sottomenù *Profili* permetterà di impostare immediatamente il livello di filtraggio del firewall di Windows: *Filtro alto* equivale al massimo di protezione possibile (tutte le connessioni di rete sono bloccate), *Filtro disattivato* equivale alla



Le icone di WFC nell'Area di Notifica di Windows, utili per l'accesso immediato alle funzionalità indispensabili.



Quando si disinstalla WFC, occorre prestare una certa attenzione al modo in cui in seguito dovrà comportarsi il firewall di Windows.



DISINSTALLAZIONE

Vista la delicatezza del ruolo svolto una volta installato sul sistema, WFC richiede una scelta consapevole dell'utente anche qualora il suddetto utente decidesse di disinstallare il programma. Avviata la fase di disinstallazione, infatti, WFC chiede di scegliere il modo in cui gestire le regole create tramite l'uso del tool: è possibile ripristinare le impostazioni predefinite di Windows Firewall eliminando tutte le regole create dall'utente, ripristinare lo stato precedente all'installazione del programma o mantenere le regole e le impostazioni del firewall attuali. La scelta spetta ovviamente all'utente, anche se ci sentiamo di non consigliare la disinstallazione di WFC se ciò non fosse strettamente necessario. L'opzione *Disabilita la registrazione di Windows Firewall* si riferisce alla gestione del log delle connessioni bloccate, una funzionalità sostanzialmente inutile se non viene utilizzata in concomitanza con le notifiche interattive di WFC.

INCOMPATIBILITÀ

Windows Firewall Control è un software progettato per agire in stretta collaborazione con il firewall nativo di Windows, e per tale motivo soffre delle sue stesse limitazioni. Come infatti sottolineato anche dal manuale del programma, WFC e Windows Firewall sono piuttosto insofferenti se usati insieme ai proxy software, i moduli per il filtraggio dei dati Web, i driver NDIS e i moduli di filtraggio che intercettano i pacchetti di dati telematici. Il firewall di Windows vuole in pratica l'esclusiva sul filtraggio delle comunicazioni di rete, e WFC non può che seguire a ruota quando sorge qualche incompatibilità con questo o quel software.
Anche il sistema di notifiche interattive di WFC può dare origine a qualche incompatibilità, ad esempio – si legge ancora nel manuale ufficiale – con le vecchie versioni di software per la cifratura come *BoxCryptor* e *TrueCrypt*.

CONCLUSIONI

Per essere un tool di piccole dimensioni, Windows Firewall Control è in grado di offrire una "profondità" di utilizzo davvero notevole. Merito certo della stretta integrazione del tool con il firewall dell'OS Microsoft, una "bestia" silente e quasi invisibile ma sempre presente, che un software specialistico come WFC è in grado di "addomesticare" quel tanto che basta da renderla una guardiana preziosa delle nostre attività di rete – fuori e dentro Internet. •

OUTBOUND E INBOUND? PARI NON SONO

Nella sua configurazione di default e anche in quella consigliata, WFC visualizza le notifiche solo per le connessioni in uscita bloccate dal firewall di Windows. È infatti verso traffico di rete in *outbound* che l'utente deve avere il massimo dell'attenzione, poiché in quelle richieste di comunicazione con gli IP remoti potrebbe celarsi un malware che prova a "chiamare a casa" o anche un software dotato di routine sconosciute – e potenzialmente pericolose per la privacy – che richiedono l'accesso ai server esterni. Per il traffico *inbound*, invece, è lo stesso firewall di sistema a comportarsi come WFC: ogni richiesta di traffico in entrata viene bloccata, e Windows Firewall presenta una notifica nativa chiedendo all'utente se pianifica di accettare le prossime connessioni in entrata del programma appena bloccato. In condizioni normali non dovrebbe esserci necessità di una connessione inbound, ma un particolare software di terze parti potrebbe averne bisogno per funzionare correttamente. Una popolare darknet basata su Java (I2P) ha ad esempio questo genere di necessità.

Installa un Software AntiMalware (Antivirus + Antispyware) e mantienilo aggiornato

Se hai un PC con Windows ancora senza Antivirus, se vuoi puoi scaricare e installare quello **gratuito** di Microsoft

- Il software Antimalware può trovare ed eliminare i **virus** che arrivano sul tuo computer prima che facciano dei danni…
- … e può evitare che dei programmi possano **spiare quello che fai** ed eventualmente **rubarti informazioni**
- Il software antimalware, per essere efficace, deve essere sempre **aggiornato**

Spybot Identity Monitor (monitorare account ed email)

Spybot mette a disposizione uno strumento “off-line” per il controllo della sicurezza degli account di rete, un’utility che permette anche di automatizzare il check-up degli account a ogni logon.

Oltre a essere nota per la produzione di Spybot Search & Destroy, storico software di sicurezza progettato per eliminare adware e spyware dal PC, Spybot mette a disposizione degli utenti anche **un utility in grado di tenere sotto controllo la sicurezza degli account di rete**. Un tool aggiuntivo che può essere usato assieme ai servizi telematici specializzati per rendere ancora più sicura la nostra presenza on-line.

Spybot Identity Monitor (SIM), questo il nome del nuovo tool, è un software gratuito – per la precisione *donationware* – disponibile per Windows **o anche in formato “app”** per lo Store Microsoft o l’App Store per Mac. Nella sua versione Windows, SIM necessita di essere scaricato dal sito ufficiale e installato sul sistema Windows 7 o Windows 10 su cui intendiamo utilizzarlo.

Una volta avviato, SIM presenta l'interfaccia principale da cui è possibile accedere a tutte le funzionalità del software: sulla destra vengono elencati tutti gli account che intendiamo monitorare, mentre il pulsante centrale permette di accedere all'elenco degli account e serve da "allerta" nel caso in cui fossero individuate eventuali brecce di sicurezza in Rete.

Al momento SIM è in grado di controllare la presenza di un account in oltre 340 diverse brecce di rete (con più di 2 miliardi di account totali), un elenco delle quali è accessibile dal pulsante Services presente sull'interfaccia principale del software. Premendo il pulsante My Accounts, invece, si accede all'elenco degli account sotto controllo: è possibile aggiungere e-mail o username, e facendo click su ogni singolo account si accede all'elenco delle brecce di sicurezza in cui esso è eventualmente presente o alla possibilità di eliminarlo dal monitoraggio.

Accedendo al pannello delle impostazioni tramite il pulsante Settings, infine, è possibile istruire il software sul controllo automatico della sicurezza degli account a ogni logon di Windows (tramite l'Utilità di Pianificazione del sistema), sulla verifica della disponibilità di una nuova versione o sull'utilizzo (forzato o meno) di una modalità scura più riposante per gli occhi. Per il controllo delle brecce al logon è necessario eseguire SIM con i pieni privilegi di un account amministratore.

Un software come Spybot Identity Monitor può rappresentare un'importante "seconda opinione" sulla sicurezza dei nostri account di rete, uno strumento che andrebbe necessariamente utilizzato in concomitanza con i tantiservizi Webspecializzati per avere la ragionevole certezza di non essere a rischio. Se un nostro account risulta presente in un database compromesso, infine, è indispensabile provvedere al cambio immediato della password per tutti i servizi collegati.

Nuova breccia di sicurezza, miliardi di utenti (forse) a rischio

Un nuovo, massiccio archivio di credenziali di accesso compromesse circola on-line, gli hacker sono impegnati a scambiarsi le informazioni ma il rischio è probabilmente molto più basso di quanto i numeri facciano intendere.

Era solo questione di tempo, prima che hacker e cyber-criminali cominciassero a condividere gli altri archivi di credenziali di accesso compromesse emersi on-line assieme alla famigerata "Collection #1". Quegli archivi sono ora in circolazione, e **il rischio (potenziale) riguarda questa volta miliardi di utenti**.

Da Collection #1 si è ora passati alle "Collections #2-5", un *dump* contenente la bellezza di 25 miliardi di record per un totale di 845 Gigabyte di dati; stando a quanto sostengono i ricercatori, **il numero di nomi utente e password unici a rischio si attesta sui 2,2 miliardi**, mentre erano "appena" 773 milioni nella prima mega-raccolta.

Il nuovo mega-archivio di mega-brecce di sicurezza sta già facendo il giro dei soliti "circoli" del cyber-crimine, dicono gli esperti, con migliaia di download e centinaia di "seed" impegnati a condividere il pacco.

Per quanto riguarda la provenienza dei dati, invece, si ipotizza che la stragrande maggioranza delle credenziali compromesse provenga da brecce avvenute in passato, mentre una piccola parte dei dati potrebbe arrivare da violazioni di minore entità e quindi potenzialmente più pericolose per gli utenti registrati sui servizi compromessi.

Come già successo con Collection #1, insomma, il rischio che le nostre password risultino presenti negli archivi compromessi è piuttosto basso ma non va trascurato. Per verificare che i dati personali siano al sicuro, è possibile controllare l'e-mail sul servizio on-line messo a disposizione dall'Hasso Plattner Institute chiamato ***HPI Identity Leak Checker*** e già aggiornato con l'aggiunta delle Collections #2-5.

Verificare la violazione degli account

La Centrale di Analisi e Sicurezza Svizzera mette gratuitamente a disposizione degli utenti uno strumento con cui controllare l'integrità delle proprie credenziali di autenticazione, come nomi utente ed indirizzi email.

Usare il **MELANI CHECK TOOL** è facile: dopo aver raggiunto la pagine del servizio all'indirizzo www.checktool.ch, basta specificare la casella di posta elettronica od il nome utente di cui vogliamo verificare la sicurezza e premere il pulsante Check.

Il tool controllerà la presenza delle informazioni nella propria banca dati e comunicherà all'utente se le credenziali sono o meno compromesse.

I dati inseriti non vengono trasmessi a terzi ed i server sono localizzati in Svizzera.

Il tool è anche in lingua italiana.

Silver Sparrow, il virus misterioso che colpisce i Mac. E si autodistrugge

22/02/2021

I ricercatori di Malwarebytes e Red Canary l'hanno già individuato dentro circa 30mila Mac, i computer di Apple senza distinzione fra laptop e fissi. Ma è verosimile che Silver Sparrow, così l'hanno battezzato, abbia già infettato molte più macchine. Sono due gli aspetti interessanti di questo nuovo virus scovato sui pc della Mela, ritenuti a torto più sicuri degli altri: il primo è che sembra progettato per traghettare qualcosa sui computer, ma non si sa ancora cosa visto che il virus al momento è innocuo. Si limita cioè a collegarsi al server di riferimento una volta all'ora, per controllare se ci siano comandi da eseguire o pacchetti da scaricare, e poi si ritira silenziosamente. Il secondo è che parrebbe dotato di un meccanismo di autodistruzione che sarebbe in grado di rimuovere ogni traccia del suo passaggio, una volta fatto quel che dovrà fare. Il che lascia pensare al frutto di un'operazione particolarmente sofisticata, non troppo comune per questo tipo di minacce.

In un post sul blog ufficiale Red Canary fornisce ulteriori dettagli, compreso il fatto di averne scoperti diversi tipi in grado appunto di colpire non solo i Mac equipaggiati con processori Intel, tutti quelli messi in commercio fino alla rivoluzione dello scorso autunno, ma anche i nuovissimi computer dotati di piattaforma proprietaria M1 basati su architettura Arm. Un aspetto, questo, che inquieta non poco considerando appunto che sono appena stati lanciati sul mercato: sono il cuore dei nuovi Mac mini, MacBook Air e MacBook Pro (13 pollici) svelati alla fine del 2020 e sono note pochissime vulnerabilità sul loro conto. La prima era stata scoperta proprio pochi giorni fa dal ricercatore Patrick Wardle di Objective-See: si tratta di un adware installato tramite un'estensione per Safari, una variante del noto adware Pirrit per Mac.

Secondo gli esperti, Silver Sparrow potrebbe essere in fase di distribuzione e iniziare a fare il suo (sporco) lavoro solo una volta raggiunta un'"infezione" diffusa su scala internazionale e su un numero ancora più elevato di "endpoint". In ogni caso, già ora le macchine in cui è stato individuato sono installate in 153 paesi sebbene concentrate soprattutto in Canada, Francia, Germania, Regno Unito e ovviamente Stati Uniti. A quanto pare, dall'analisi del codice il virus si baserebbe sull'infrastruttura cloud di Amazon Web Services e sulla piattaforma di Akamai per la distribuzione dei contenuti. Ma il punto è proprio questo: al momento non sta distribuendo nulla e non c'è chiarezza sulla sua finalità malevola. Non c'è alcuna prova che sia stato utilizzato in qualche modo, anche se è probabile, e Apple sarebbe già corsa ai ripari, impedendone l'installazione e revocando i certificati.
Nello specifico, dopo la scoperta del malware, Apple ha revocato i certificati degli account sviluppatore utilizzati per firmare i pacchetti, impedendo l'infezione di nuovi dispositivi. Anche se non ci sono prove che suggeriscano che il malware identificato abbia fornito un payload dannoso agli utenti infetti, oltre alle protezioni hardware e software di sicurezza personalizzate, Apple fa sapere che i servizi forniscono anche un meccanismo per costanti aggiornamenti software sicuri, rafforzando le protezioni dell'ecosistema. Rimane chiaro che il Mac App Store offre una garanzia di sicurezza del software che arriva direttamente da Cupertino, mentre per il software scaricato al di fuori del Mac App Store, Apple impiega il servizio di notarizzazione direttamente da sistema operativo, per rilevare eventuale malware e bloccandolo in modo che non possa essere eseguito.

Vita reale – Vita virtuale

- La vita in Rete è piena di risorse e possibilità di conoscere persone, di partecipare e organizzare eventi e attività.
  Occorre però chiedersi: è vita vera?

- Reale e virtuale sono due mondi distinti che possono interagire in modo vantaggioso, ma vanno tenuti molto distinti

La nostra vita REALE è una sola!

Navigare, chattare, giocare su Internet possono darci l'impressione di vivere una vita VIRTUALE, diversa da quella FISICA

La VITA REALE è UNA SOLA

Noi siamo qui !!

I minori e la rete

MEGLIO UTILIZZARE INDIRIZZI E-MAIL ANONIMI

- Non inserire nome e cognome nell'indirizzo mail utilizzato
- Non dare indicazioni dell'anno di nascita
- Non dare indicazioni della città di residenza

FACEBOOK / INSTAGRAM SONO VIETATI AI MINORI DI 16 ANNI

- L'età minima è sancita dal contratto che regola il social network
- Iscrivendosi occorre inserire l'anno di nascita: non mentite!

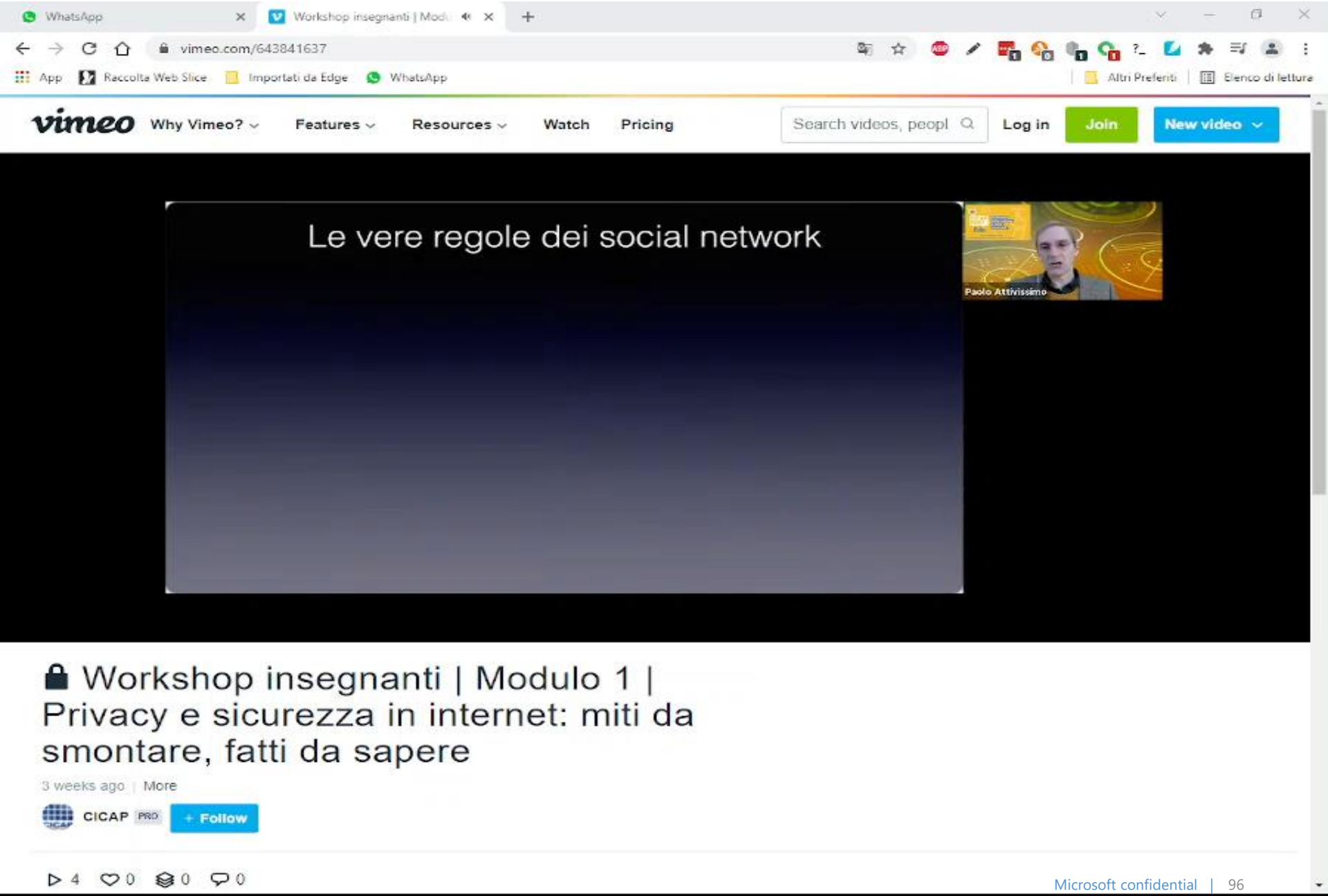
I PERICOLI DEI SOCIAL NETWORK … e se dai il telefono ad altri

- Adescamento (il reato commesso da chi, in luogo pubblico, con atti o parole, offre prestazioni sessuali a pagamento e non)
- Attenzione alle amicizie
- Furto di credenziali per l'accesso e furto di identità
- Sostituzione di persona / identità
- Diffamazione (una condotta mirante ad offendere e/o screditare la reputazione di una persona)
- Minacce
- Molestie
- Diffusione di video senza consenso
- Diffusione di immagini senza consenso

I PERICOLI DELLE CHAT

- Contatti con malintenzionati
- Chi dialoga spesso può non essere chi dice di essere
- Furto di credenziali per l’accesso e furto di identità
- Sostituzione di persona / identità
- Rivelazione di segreti

Social Network



Lavoro, attenzione alle tracce lasciate sui social: così i recruiter scoprono chi siete

ROMA - Cari ragazzi fate attenzione a cosa pubblicate sui social. E soprattutto a come lo scrivete, perché quando inviate un curriculum a un'azienda con la speranza di venir assunti il capo del personale, probabilmente, cercherà informazioni su di voi in Rete. Lo fa l'80% degli head hunter intervistati da Wyser, società internazionale di Gi Group, che si occupa di selezione di profili manageriali, senior ma anche junior. I più esperti lo sanno. Ma sapere che un recruit quando si ritrova un curriculum tra le mani o meglio sulla mail, otto volte su dieci digita il vostro nome sulla Rete è altra cosa. Cosa cerca? Un buon 45,2% si sforza di comprendere chi siete, se siete tolleranti o no, violenti o tranquilli, se la vostra apertura mentale è sufficiente per rapportarsi con culture diverse, ma anche qual è il vostro senso etico. Il restante, il 42,9%, cerca invece conferme alle vostre qualifiche. E appena il 7,1% è interessato ai vostri interessi personali come alle vostre passioni.

Il terreno di caccia più frequentato dagli head hunter è Linkedln. E sappiate che a condizionare i capi del personale non saranno le reccomendation che avete collezionato, semmai sono più interessante le vostre esperienze o i post pubblicati. E in quella che viene definita la più grande rete professionale al mondo, ordine, completezza e aggiornamento del profilo, rappresentano un plus in più. Lasciarlo invecchiare non è una buona idea. Non solo. Chi ha tra le mani il vostro curriculum può confrontare facilmente ciò che avete scritto sulla vostra lettera di presentazione e ciò che avete messo su Linkedin. E se le due cose non combaciano i capi del personale storceranno il naso.

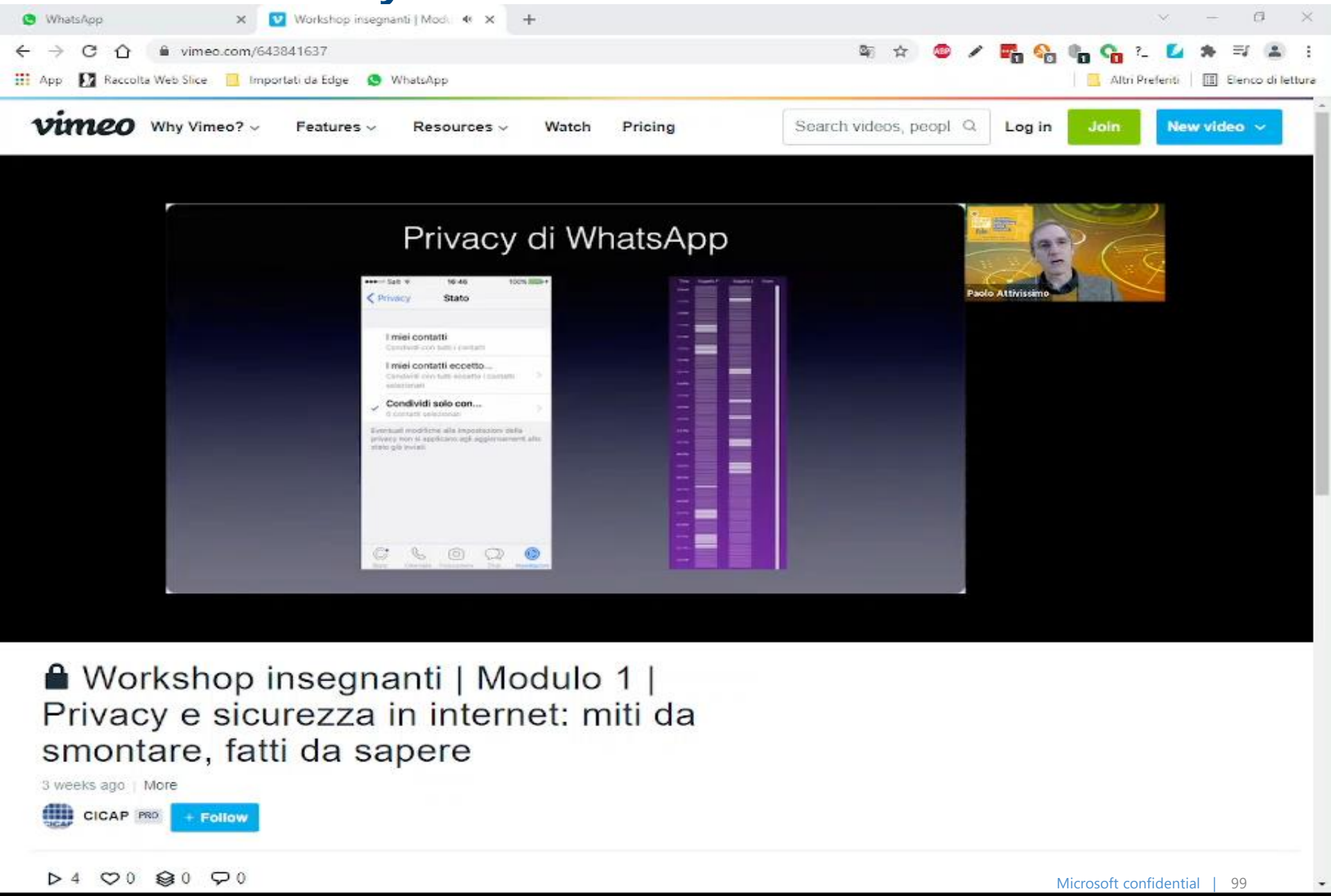
Ma è Facebook in realtà il luogo preferito dagli head hunter. E state sicuri che il vostro curriculum verrà stracciato nel 69% dei casi se i post che avete pubblicato sono offensivi o volgari. E accadrà più o meno lo stesso (40,5%), se i vostri commenti denotano un alto grado di discriminazione, non importa se a caratte sessuale, religioso o razziale. In un mondo globale in azienda vince l'inclusione, tant'è che sempre più multinazionali la inseriscono nelle linee guida. Così come la presenza di errori grammaticali o di ortografia non farà una buona impressione al vostro esaminatore (è vista male dal 35,7% dei capi del personale). D'obbligo in italiano, ma anche nelle altre lingue.

Il web dunque è diventato oltre che un canale di reclutamento anche di verifica. "Va però sottolineato - dichiara Carlo Caporale, ad di Wyser Italia - come la Rete vada utilizzata secondo le regole che vigono anche in sede di colloquio. Ciò significa che non va invasa la sfera privata del candidato, del tutto irrilevante ai fini dell'assunzione e rispettando le norme non discriminatorie previste dalla deontologia". Detto questo i cambiamenti nel mondo del lavoro e le nuove dinamiche che lo regolano hanno fatto delle soft skill le armi vincenti di manager e professionisti". E chi sui social non c'è? Per un recruiter su tre non è un buon segnale, anche se non è determinante nella scelta.

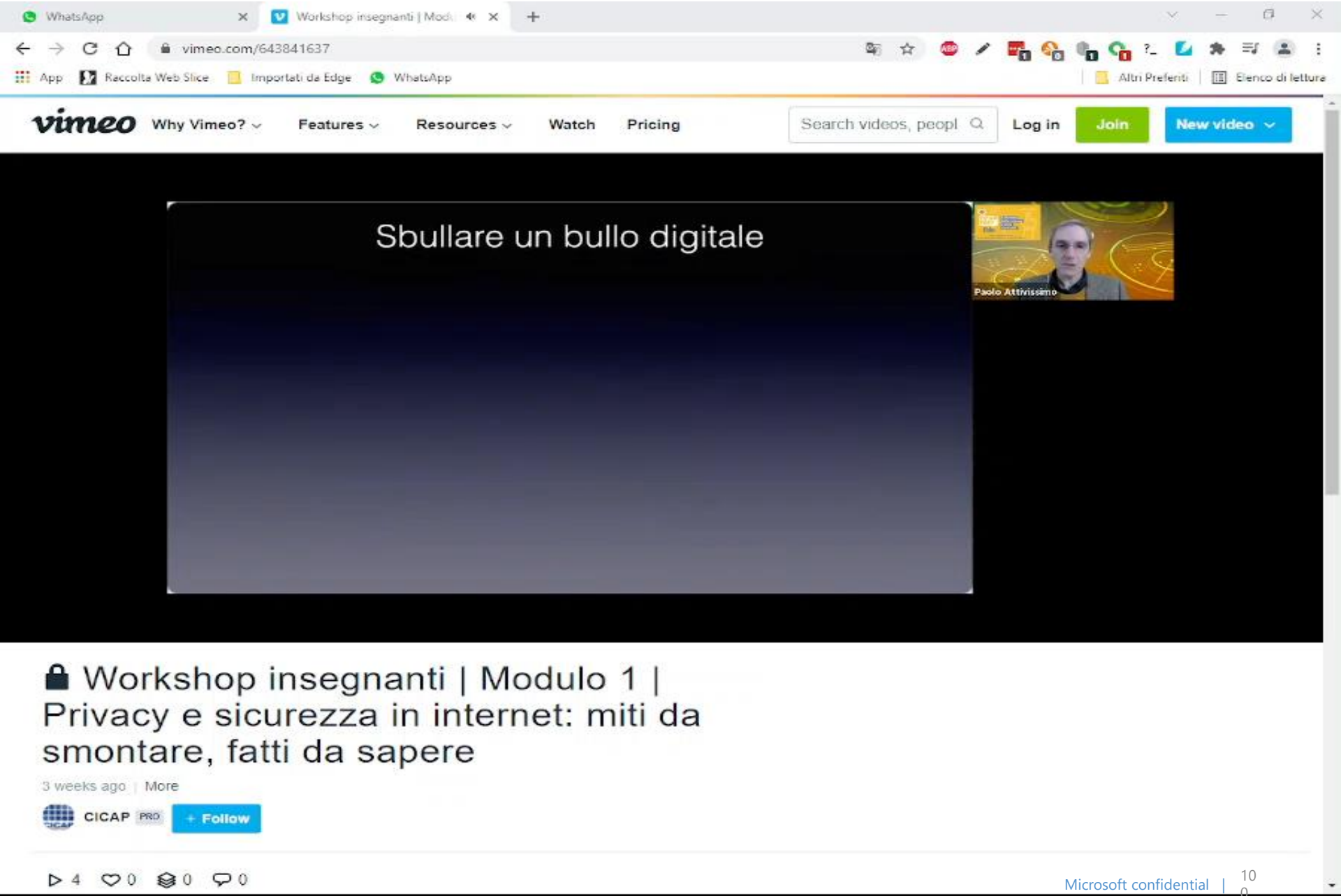
IL CYBERBULLISMO

- Azioni di bullismo “tradizionale” con fotografie e riprese pubblicate su Internet
- Violenze su compagni riprese e pubblicate su Internet
- Danneggiamenti o comportamenti irresponsabili ripresi e pubblicati su Internet
- Momenti privati e di intimità ripresi e diffusi tramite Internet o MMS
- Alterazione della percezione della gravità delle azioni

Cyberbullismo - 1



Cyberbullismo - 2



LEGGE CONTRO IL BULLISMO (Maggio 2017)

La definizione di cyberbullismo

La legge, come detto, dà per la prima volta una definizione chiara del fenomeno: «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito dei dati personali in danno di minorenni, nonché la diffusione di contenuti online il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo». Fondamentale, dal punto di vista legislativo, perché introduce la possibilità di violenza per vie telematiche.

Anche i minori possono denunciare

La legge poi introduce la possibilità di richiedere la rimozione di contenuti offensivi dalla rete e dai social network. Anche se sono esclusi soggetti come gli access provider, i cache provider e i motori di ricerca. Un diritto esteso anche ai minori, dai 14 anni in su. Al di sotto di questa soglia, necessario l'intervento dei genitori. Nel caso in cui il contenuto non venisse rimosso entro 24 ore, interviene il Garante della privacy nelle successive 48 ore. Con l'accertamento del reato, è previsto l'avvio dei una procedura di ammonimento se compiuto da un minorenne (con più di 14 anni) nei confronti di un altro minorenne. Se non si verifica reiterazione, non c'è nessuna ulteriore conseguenza al compimento della maggiore età.

In caso di episodi di bullismo via web, il questore può ammonire l'autore con un provvedimento analogo a quello adottato per lo stalking: fino a quando non sia stata presentata querela o denuncia per i reati di ingiuria, diffamazione, minaccia o trattamento illecito di dati personali commessi, mediante Internet, da minorenni sopra i 14 anni nei confronti di altro minorenne, il questore potrà convocare il minore responsabile (insieme ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale), ammonendolo oralmente ed invitandolo a tenere una condotta conforme alla legge.

Insegnanti «anti-bullo»

Una seconda parte della legge si focalizza sulla prevenzione: si vuole inserire un referente in ogni istituto scolastico che avvii corsi di formazione per gli insegnanti così che possano avere le competenze per riconoscere questo tipo di comportamenti. Al preside spetta il compito del dialogo con le famiglie degli studenti coinvolti in casi di cyberbullismo e deve anche decidere azioni educativa per chi è autore di violenza online. L'educazione si rivolge anche agli stessi studenti, con dei piani ad hoc all'interno dell'offerta formativa. Il ministero dell'Istruzione ha il compito di predisporre linee guida e di predisporre vie per insegnare ai ragazzi un uso consapevole di internet e i principi della legalità. Alle iniziative in ambito scolastico collaboreranno anche polizia postale e associazioni territoriali.

Nasce YouPol, l'app della polizia pensata per i ragazzi contro i bulli

Un'app che consente di interagire con la polizia consentendo l'invio, anche in maniera anonima, di segnalazioni riguardanti episodi di bullismo o di spaccio di droga: è "YouPol", l'applicazione per smartphone e tablet presentata questa mattina in un istituto professionale della periferia di Roma.

Un'app pensata per i più giovani

All'evento erano presenti il ministro dell'Interno Marco Minniti e il capo della Polizia Franco Gabrielli. YouPol sarà operativa da oggi a Roma, Milano e Catania, da febbraio in tutti i capoluoghi di regione e da agosto in tutte le province italiane. L'applicazione renderà possibile inviare immagini e segnalazioni direttamente alle sale operative delle Questure relative a episodi di bullismo e droga, sia di cui si è stati testimoni sia di cui si è appreso per altre vie. Sarà inoltre possibile effettuare anche una chiamata di emergenza in caso di necessità.

Gli obiettivi delle autorità

"Questa è una app amica - ha detto il ministro Minniti rivolgendosi agli studenti - è la vostra amica a cui potete rivolgervi in caso di difficoltà. Lanciate il segnale, dite che c'è bisogno di un aiuto, fatelo anche in maniera anonima se volete, ma l'unica cosa che non dovete fare è voltarvi dall'altra parte". Perché, ha aggiunto il ministro "non c'è una società libera se in quella società prevale la violenza. Noi non abbiamo bisogno di ragazzi eroi, abbiamo bisogno di persone che pensino che facendo questo stiano facendo un qualcosa che fa bene al loro essere cittadini". Con la app, ha poi garantito Franco Gabrielli, la Polizia non ha alcuna intenzione "di entrare nelle vite dei ragazzi né di diventare una sorta di Grande Fratello. La app non è uno strumento di delazione, non abbiamo bisogno di avere spioni sul territorio".

Alcuni suggerimenti 1/2

1. Ricordate che Internet è un luogo pubblico, e che i contenuti che condividete vivono di vita propria: le foto, i messaggi e le conversazioni possono essere viste anche da sconosciuti. Non postare nulla di personale o riservato e di cui ci si potrebbe pentire in futuro

2. Imparate a non condividere le informazioni personali: cognome, indirizzo, numero di telefono, foto, sono tutte informazioni personali da non divulgare a soggetti sconosciuti

3. Su Facebook, Twitter, Windows Live, Badoo, Netlog e su tutti gli altri social network controllare bene le proprie impostazioni. Chi può vedere il profilo? Chi può fare ricerche sul nome? Scoprire l'età? Chi può scrivere commenti oppure creare situazioni non controllabili?

Alcuni suggerimenti 2/2

4. Bisogna essere educati nella vita virtuale così come nella vita reale: non insultare o mettere in cattiva luce nessuno, non pubblicare contenuti privati di altre persone.

5. Se vi sentite a disagio per qualcosa: parlate e chiedete aiuto ad un adulto di cui vi fida

6. Gli amici vanno conosciuti di persona prima di diventare amici su Internet, non viceversa

7. Le persone non sempre sono chi dicono di essere: parlate con un adulto di cui vi fidate prima di incontrare qualcuno di persona conosciuto su Internet, e non fate questi incontri da soli

I REATI SU INTERNET

Minore vittima

- Adescamento
- Scherzo che degenera
- Cyber bullismo
- Stalking
- Minacce
- Molestie.
- Diffamazione
- Ingiurie
- Calunnie
- Furto di identità
- Accesso abusivo
- Danneggiamento

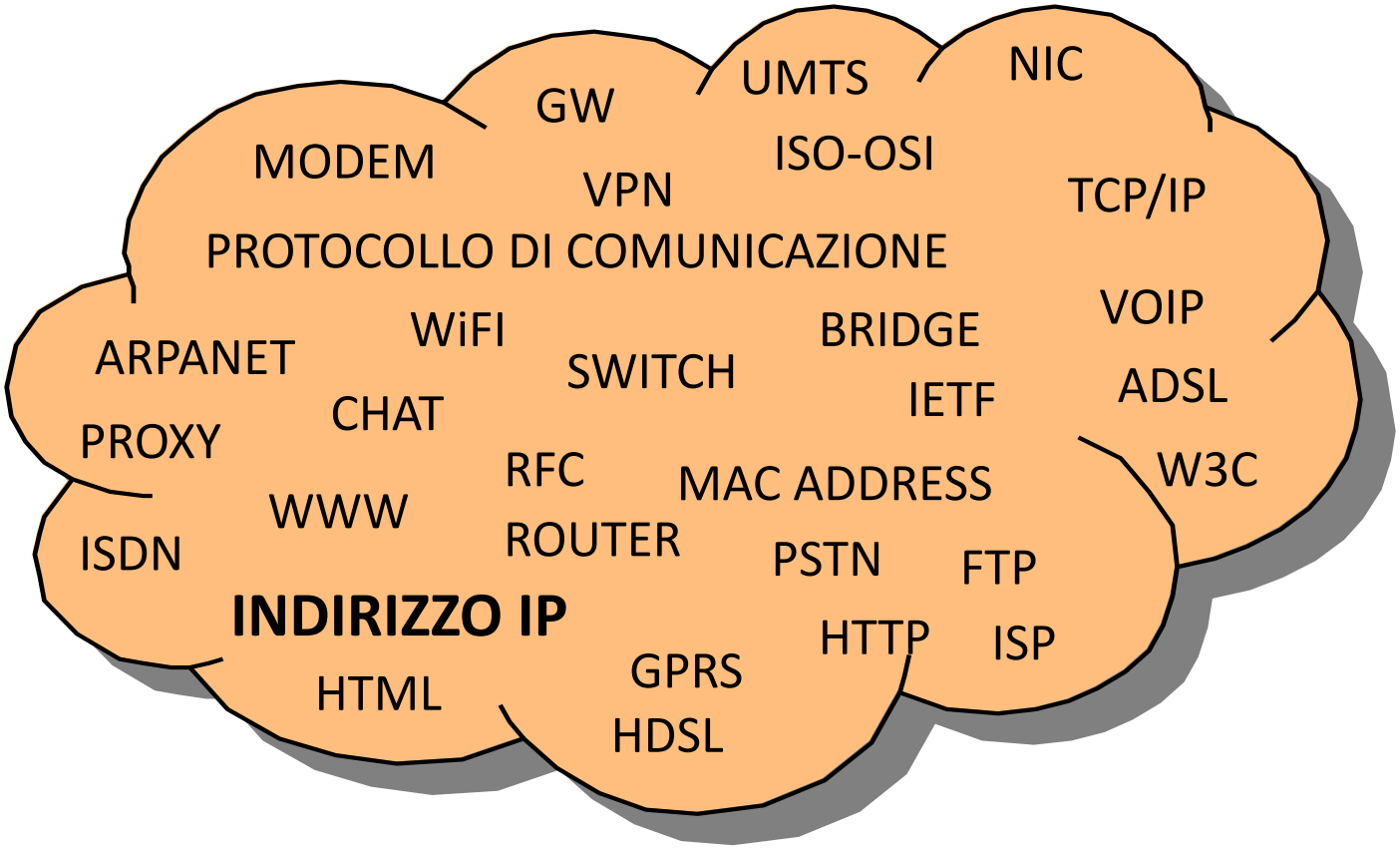
Minore che commette reati

- Scherzo che degenera
- Cyber bullismo
- Stalking
- Minacce
- Molestie
- Diffamazione
- Ingiurie
- Calunnie
- Furto di identità
- Accesso abusivo
- Danneggiamento

I REATI SU INTERNET

- Il minore di età inferiore ai 14 anni non è imputabile
- La responsabilità penale è personale (quindi il genitore non è imputabile al posto del minore)
- Per il risarcimento di eventuali danni, anche morali, il genitore è responsabile per il minore

Non esiste l'anonimato in rete!



Rintracciabilità da parte della Polizia Postale dell'indirizzo IP del pc

DEEP e DARK WEB

Il dark web (in italiano: web oscuro o rete oscura) è la terminologia che si usa per definire i contenuti del World Wide Web nelle darknet (reti oscure) che si raggiungono via Internet attraverso specifici software, configurazioni e accessi autorizzativi.

Il dark web non è raggiungibile dai classici motori di ricerca, perché si sovrappone alle normali reti e alle architetture delle reti private, rendendo molto difficile l'accesso, e permettendo cosi di nascondere e commerciare materiale illegale. All'interno del dark web si può trovare:

- condivisione di file (piratati, personali, illegali o contraffatti, etc.);
- crimini informatici (corruzione di file, frodi, etc.);
- protezione dei dissidenti da ritorsioni politiche;
- protezione della privacy dei cittadini soggetti a sorveglianza di massa;
- vendita di beni limitati su mercati darknet;
- compravendita di beni o servizi illeciti o illegali;
- fughe di notizie;
- aggiramento della censura di internet e dei sistemi di filtraggio dei contenuti o superamento di firewall.

I pericoli del Dark Web

Navigare sulla rete oscura non è illegale, ma essendo fuori da qualunque controllo, è molto semplice finire nei guai, anche per file scaricati involontariamente.

Ecco perché è un luogo, seppur virtuale, costantemente monitorato dalle Forze dell'Ordine.

Non sono inoltre da trascurare i pericoli a cui si è sottoposti quando si naviga all'interno di forum che trattano argomenti pericolosi, poiché dietro i numerosi nickname possono nascondersi i peggiori criminali, per i quali non è affatto complicato risalire all'indirizzo di casa degli altri utenti

Diffondono foto osé di coetanea: sono minori ma pagano i genitori

Sono tutti minorenni gli undici ragazzini che sono stati «condannati» a risarcire una loro coetanea per aver fatto circolare sui telefonini una sua foto nuda. Una sentenza destinata a far discutere perché con loro sono stati «sanzionati» anche i genitori, considerati co-responsabili. La sentenza è stata emessa dal giudice del tribunale di Sulmona Daniele Sodani, la cittadina abruzzese dono si sono svolti i fatti, il quale ha ritenuto responsabili i genitori per le colpe dei loro figli. L'episodio risale al 2013 quando una ragazza, all'epoca 14enne, denunciò di essere apparsa nuda su Facebook per alcune ore e poi sui telefonini di amici e conoscenti. Quello che all'inizio sembrava agli occhi dei ragazzini un semplice gioco è finito al centro di indagini giudiziarie condotte dai carabinieri di Sulmona, sollecitati dai genitori della ragazza. L'accusa: diffusione di materiale pedopornografico. All'inizio furono una trentina i ragazzi, quasi tutti minorenni, chiamati a deporre dai carabinieri.

Da questo elenco sono poi stati estrapolati gli undici ritenuti autori materiali della diffusione delle foto osé. In sede di udienza preliminare gli indagati sono stati tutti prosciolti. Non così in sede civile dove il giudice accogliendo parzialmente le richieste dei genitori che avevano avanzato un risarcimento di 650 mila euro, per danni patrimoniali e non, ha stabilito che i convenuti debbano versare, a vario titolo, la cifra in totale di oltre 100 mila euro, come danno non patrimoniale. Il giudice ha disposto che a pagare il risarcimento debbano essere i genitori degli allora minorenni perché «è in capo al genitore l'onere di provare e di dimostrare il corretto assolvimento dei propri obblighi educativi e di controllo sul figlio, solo in tal modo potendosi esonerare dalla condanna risarcitoria». Per il giudice nulla invece sarebbe stato dimostrato. Anzi sempre secondo la sentenza «i fatti esprimono, di per sé, una carenza educativa degli allora minorenni, dimostratisi in tal modo privi del necessario senso critico di una congiura capacità di discernimento e di orientamento consapevole delle proprie scelte nel rispetto e nella tutela altrui. Capacità che invece avrebbero già dovuto godere in relazione all'età posseduta. Tanto è vero che alcuni coetanei ricevuta la foto non l'hanno divulgata». Il giudice non ha risparmiato neanche i genitori della minorenne: per loro nessun risarcimento perché «non avrebbero vigilato sulla condotta imprudente della propria figlia, da cui sarebbero partite le foto osé».

Identità digitale rovinata da Google

Ci sono storie che appaiono e scompaiono tra le notizie, e che invece restano indelebilmente stampate nella mente di Cassandra, come suoi peccati; profezie che ha enunciato, ma non con abbastanza forza. Ci sono storie che per fortuna hanno un lieto fine, che tuttavia, a volerlo ben esaminare, tanto lieto non è, e che proprio per questo hanno una morale evidente. Ci sono storie che alla fine contengono anche una seconda morale, ben nascosta e ancora più importante, importante per tutti noi.
È il caso di questa notizia, apparsa per la prima volta il 21 agosto sul New York Times e immediatamente ripresa da Slashdot, e che i distrattissimi media nazionali non hanno per ora mai considerato. I fatti risalgono a febbraio, e riguardano la storia di due genitori americani il cui figlio piccolo un giorno si è ammalato, ma invece del solito mal di gola o dolore di pancia ha manifestato una preoccupante irritazione ai genitali.
Cosa avreste fatto nei loro panni? Avreste telefonato al medico. Il medico non c'era, e la segretaria, molto opportunamente, dopo essersi fatto spiegare il problema, ha suggerito di mandare una foto al dottore in modo che potesse anticipare la diagnosi. Così hanno fatto; il dottore ha prescritto un antibiotico e tutto si è risolto nel migliore dei modi. Solo dal punto di vista medico, però.

Sì, perché le foto dell'inguine e annessi del bambino sono state scattate con uno smartphone Android. Lo smartphone Android utilizzava il backup nel cloud, che Google cerca in tutti i modi di far abilitare ai propri utenti, chissà perché.

Le foto sono quindi finite nel cloud dove, nel caso non lo sapeste, sono state scansionate da un sistema di verifica di contenuti pedopornografici. I famosi "filtri dei contenuti". Chissà, forse un'Intelligenza Artificiale.

Le foto in questione apparivano tali, e quindi sono state passate a una verifica manuale. Probabilmente a un "consulente" stressatissimo in un paese remoto dove la manodopera costa poco, un poveraccio con la testa piena (per motivi "professionali") di schifezze. Il poveretto non si è accorto dell'irritazione cutanea, ha padellato la valutazione e ha fatto partire le procedure di Google del caso.

L'account è stato sospeso con una mail di comunicazione minacciosa ma generica, e una copia di tutti i dati dell'account è stata inviata alla polizia, che ha cominciato un'indagine criminale. Nel frattempo i genitori, che avevano affidato tutte le loro informazioni digitali a Google e solo a Google (madornale errore!), si sono trovati improvvisamente privati di tutta la loro vita digitale.
Dopo un mese, diciamo "per fortuna", è arrivata la comunicazione delle indagini in corso con relativa convocazione, cosa che ha finalmente permesso ai genitori di presentare le loro ragioni senza continuare a rimbalzare su muri di gomma. Si erano fatti preparare una dichiarazione del medico che ha subito convinto l'investigatore; quindi, con i tempi dovuti, supersonici rispetto a quelli italiani, è stato comunicato il non luogo a procedere.
Lieto fine? Certamente, considerando il fatto che se l'investigatore fosse stato distratto come l'impiegato di Google, i genitori potevano vedersi sottratto il figlio dai servizi sociali, e anche finire in galera, in isolamento, perché non è sano essere in mezzo ad altri detenuti con la reputazione di molestatori di bambini.
No, nessun lieto fine, solo il meno peggiore, per due buoni motivi. Il primo motivo è quello che Matteo Flora chiamerebbe in maniera asettica "danno reputazionale", cioè il fatto che la notizia è comunque trapelata, e quella successiva del non luogo a procedere non si diffonderà mai con la stessa ampiezza.
Il secondo motivo, e questa è la "morale nascosta", è che Google si è rifiutata ufficialmente e decisamente di riattivare l'account, malgrado la prova incontrovertibile che la loro segnalazione era totalmente errata. Lo scarno messaggio informava che l'account era stato permanentemente cancellato, e che il giudizio di Google è inappellabile. Interrogati nuovamente su questo punto, l'inappellabilità e la cancellazione totale dell'account sono state confermate.
Questo è tutto per quanto riguarda la cronaca. Vediamo ora la lezione da apprendere e la morale nascosta sottostante. Si tratta di un ottimo e purtroppo normale esempio di cosa gli utenti sono per le multinazionali dell'informatica. Merce da vendere, e in casi come questi "falsi positivi" dei loro filtri automatici. Mai esseri umani, men che mai clienti, figuriamoci vittime innocenti di errori. Quindi indegni di protezione, privi di diritti, "ammanettati« da decine di migliaia di parole delle condizioni d'uso sempre in continuo mutamento.
L'unica possibilità per gli incauti genitori (incauti dal punto di vista informatico, per la mancanza di backup, e per la scarsa tutela della privacy loro e del figliuolo) di riavere la propria vita digitale è stata quella di chiederlo alla polizia, che è l'unica detentrice di una copia integrale dei dati del loro account.
E sapete la buona notizia? Molto più umanamente di Google, la polizia ha assicurato che faranno tutto il possibile per aiutarli. Forse loro si sentono leggermente in colpa per aver perseguito degli innocenti. Google invece evidentemente no, malgrado un antico "Don't be evil".
Ma questo è del tutto naturale, perché le multinazionali ovviamente non hanno una coscienza. Sono esseri non umani, il cui unico scopo è pagare i dividendi agli azionisti. Fanno tanta pubblicità sui temi politically correct del momento, ma solo come investimento per le public relations; sotto sotto restano schiacciasassi, macinatori di profitti e, quando capita, di persone.

Insulti anonimi su web sono diffamazione (16/04/2014)

Gli insulti su Facebook anche se indirizzati ad una persona di cui non viene fatto il nome e letti da una cerchia ristretta di iscritti possono portare ad una condanna per diffamazione. Lo dice la Cassazione che ha rinviato a nuovo processo l'assoluzione di un maresciallo capo della Guardia di Finanza: aveva pubblicato sul social network una frase offensiva rivolta ad un collega, senza nominarlo, ed una espressione volgare rivolta alla moglie di quest'ultimo.

Per la frase incriminata, che aveva offeso la reputazione del maresciallo designato al posto suo al comando della compagnia, l'imputato era stato condannato dal tribunale militare di Roma a tre mesi di reclusione militare per diffamazione pluriaggravata.

In Appello era stato assolto per insussistenza del fatto, poiché l'identificazione della persona offesa risultava – aveva spiegato la Corte militare d'Appello di Roma – possibile soltanto da parte di una ristretta cerchia di soggetti rispetto alla generalità degli utenti del social network. Nel ricorso, il procuratore generale militare ha evidenziato come, al contrario, la pubblicazione su Facebook abbia determinato la conoscenza delle frasi offensive da parte di più "soggetti indeterminati iscritti al social network e che chiunque, collega o conoscente dell'imputato, avrebbe potuto individuare la persona offesa".

La prima sezione penale della Cassazione ha riconosciuto come la frase fosse "ampiamente accessibile", essendo indicata sul cosiddetto 'profilo'" e l'identificazione della persona offesa favorita dall'avverbio "attualmente" riferita alla funzione di comando rivestita.

Tra l'altro "il reato di diffamazione non richiede il dolo specifico" ma la "consapevolezza di pronunciare una frase lesiva dell'altrui reputazione e la volontà che la frase venga a conoscenza anche soltanto di due persone". Ad avviso della Corte, "i giudici di secondo grado non hanno adeguatamente indicato le ragioni logico-giuridiche per le quali il limitato numero delle persone in grado di identificare il soggetto passivo della frase a contenuto diffamatorio determini l'esclusione della prova della volontà dell'imputato di comunicare con più persone in grado di individuare il soggetto interessato".

A 13 anni gira un video hard con gli amici: finisce diffuso in mille cellulari

07/12/2014

- A 13 anni si lascia filmare con il telefonino mentre ha un rapporto con due ragazzini poco più grandi all'interno di un garage. Ma non immagina neanche le conseguenze che avrà su di lei quel video, fatto circolare tra migliaia di coetanei attraverso i social network. È l'incubo che sta vivendo da un mese una tredicenne, residente a Castelfranco, che ora si rifiuta di tornare alla scuola media che frequenta per la vergogna non solo di quanto ha fatto, ma anche per la consapevolezza che tutti i compagni ormai hanno visto cosa ha fatto. Ma neanche gli amici che erano con lei immaginavano che si sarebbero trovati in un guaio simile per aver fatto girare tra gli amici quelle immagini che, nel giro di pochi giorni, hanno raggiunto almeno un migliaio di telefonini non solo tra gli studenti della Castellana, ma anche del Bassanese e del Padovano. **I carabinieri di Castelfranco hanno infatti denunciato i due ragazzi che facevano sesso con la tredicenne e un terzo che faceva da palo, tutti tra i 14 e i 15 anni, per violenza sessuale e pornografia minorile.** Ma le conseguenze potrebbero non essere circoscritte solamente ai protagonisti del video. **Sono infatti in arrivo analoghe denunce per chi ha ricevuto e inviato a sua volta il video**.
- Il fatto risale ormai ad un mese fa. La tredicenne viene invitata da tre ragazzini poco più grandi all'interno di un garage di un complesso residenziale a Castelfranco. Sono le 8 di sera. Dalle prime ricostruzioni sembra che i tre, che già da tempo provavano ad approcciare la ragazzina, l'avessero convinta a seguirli. La tredicenne, non rendendosi conto delle conseguenze, ha lasciato che i tre la riprendessero con lo smartphone mentre praticava sesso orale a due ragazzi, davanti al terzo. Nel video il volto della ragazzina è chiaramente riconoscibile. E, nel giro di pochi giorni, in troppi vedono cosa è accaduto.

- I tre infatti inviano tramite WhatsApp il filmato ai loro amici, non immaginando che nel giro di poche ore sarebbe diventato virale tra tutti gli studenti della loro scuola, ma non solo. I carabinieri sospettano che almeno un migliaio di cellulari abbiano scaricato il video. E infatti le immagini del garage arrivano anche sul telefonino di un cugino della tredicenne. Questi, maggiorenne, riconosciuta la parente, avvisa immediatamente i familiari. È il padre della ragazzina a denunciare il fatto ai carabinieri e a dare il via alle indagini. Un'inchiesta estremamente delicata che svela i pericoli che si annidano nei social network se utilizzati nel modo sbagliato. In brevissimo tempo gli investigatori riescono a risalire all'identità dei tre ragazzi presenti all'interno del garage. Vengono denunciati per violenza sessuale e pornografia minorile.
- Ma non è finita. **I carabinieri dovranno anche perseguire chi ha ricevuto il video e a suo volta l'ha fatto girare inviandolo ad altri amici. Per loro l'accusa sarà di detenzione o trasmissione di materiale pedopornografico. «Questi giovani devono capire le conseguenze dei loro comportamenti», ha spiegato il capitano Salvatore Gibilisco, comandante della compagnia di Castelfranco, «pensano di non fare nulla di male, ma anche il semplice invio di un messaggio può avere conseguenze anche gravi sotto il profilo penale».**
- Ma al momento le conseguenze più pesanti, a livello psicologico, le sta subendo la tredicenne. Ora è seguita da uno psicologo e non ha più voluto tornare a scuola da quando ha saputo che tantissimi, compagni e non, avevano visto il video che la vedeva protagonista. Troppo grande la vergogna. La speranza a questo punto è che la ragazzina comprenda fino in fondo la gravità di quanto fatto e le insidie che possono nascondersi nella rete. E che analoga riflessione sia fatta da tutti quelli che hanno diffuso il video.

Minori: procura, in Liguria boom di adescamenti su WhatsApp

- L'adescamento dei minori adesso avviene anche tramite l'applicazione di messaggistica, la popolare WhatsApp. E' quanto emerge dalla procura di Genova che in questi giorni ha ricevuto numerose denunce da parte di genitori di ragazzine contattate da finti coetanei che chiedono prestazioni sessuali o foto osè.
- Il modus operandi degli 'orchi' è sempre lo stesso: la minore, sono pochi i casi in cui la vittima è un maschio, viene prima contattata su Facebook, altri social o via email. I primi contatti sono 'normali', scambi di saluti, domande sugli interessi personali. Il pedofilo, quasi sempre, si finge un coetaneo. Dopo i primi scambi di lettere virtuali, l'orco chiede il numero di telefono per poter chiacchierare tramite l'app. A quel punto le richieste diventano esplicite: prima la richiesta di foto hard e poi di incontri, in cambio di regali come cellulari o altri oggetti. L'applicazione viene scelta dai pedofili perché difficile da intercettare da parte degli inquirenti.
- La maggior parte delle volte c'è solo lo scambio di foto, e non si arriva all'incontro per paura. I casi segnalati sono arrivati dopo che i genitori hanno 'spulciato' i social dei figli scoprendo le mail e le richieste esplicite. Lo scorso anno sono state 15 le denunce arrivate al gruppo che si occupa di questo tipo di reati e che ha competenza territoriale in tutto il distretto, da Ventimiglia a Massa. Nella maggior parte dei casi, quelli per cui si è riusciti a risalire all'autore dell'adescamento, si tratta di persone già denunciate per reati dello stesso tipo.

Si lasciano a 15 anni, lui manda agli amici le foto sexy di lei

PADOVA – 16/02/2015.

Si chiama "revenge porn" (in italiano "vendetta a luci rosse"). E' un fenomeno sempre più diffuso: quando una coppia si lascia, uno dei due posta sui social network le immagini erotiche dei loro rapporti intimi come forma di "vendetta" per essere stato abbandonato o per altri rancori. E' accaduto anche nell'Alta Padovana ma stavolta la vicenda, finita dritta dritta dai carabinieri, ha per protagonisti due adolescenti di 15 anni.

Lei lo ha lasciato e lui si è vendicato inviando ai compagni di scuola la foto a seno nudo della sua ex via WhatsApp, il sistema di messaggini privati molto in voga tra gli adolescenti. Una situazione che ovviamente ha prodotto nella ragazzina una stato di prostrazione psicologica, facendola addirittura rischiare di perdere un anno a scuola.

Così la famiglia di lei ha denunciato tutto ai carabinieri ed è stata coinvolta anche la scuola per capire come gestire il caso. I militari dell'Arma hanno denunciato il ragazzo autore dell'invio della foto e del caso se ne occuperà il tribunale dei minori di Venezia.

Pedopornografia, l'arresto del 23enne è valido

VIGODARZERE (Novembre 2015).

Si è avvalso della facoltà di non rispondere davanti gip padovano Domenica Gambardella, che gli ha contestato l'accusa di detenzione di materiale pedopornografico in quantità ingente. Accanto a lui nell'interrogatorio di convalida dell'arresto il suo difensore, l'avvocato Francesco Lava. Non una parola, non una spiegazione, com'è nel suo diritto, da parte di D.G., ventitreenne residente a Tavo di Vigodarzere.

Ma negli occhi tutto lo smarrimento di un ragazzo dei suoi anni, forse scoperto in una situazione più grande di lui ma oltre i limiti della legalità. Il giudice ha convalidato il provvedimento restrittivo, pur alleggerendo la misura cautelare trasformata dagli arresti domiciliari all'obbligo di presentazione quotidiana alla polizia giudiziaria: in pratica il 23enne dovrà recarsi ogni giorno a firmare un registro nella caserma dei carabinieri. Intanto va avanti l'inchiesta padovana coordinata dal procuratore aggiunto Valeria Sanzari che ha provveduto al sequestro del materiale, migliaia fra foto e video scaricati in rete dal ragazzo.

Un materiale relativo a immagini scabrose di minorenni, che aveva fatto scattare gli arresti domiciliari giovedì mattina nel corso di una perquisizione nell'abitazione del giovane ordinata dalla procura di Roma e affidata alla Polizia postale. Polizia impegnata nell'identificazione di internauti che, navigando in rete, vanno a caccia di siti pornografici dedicati ai minorenni e "scaricano" il materiale per tenerlo per sé o per divulgarlo. In questo caso D.G. aveva "scaricato" il materiale, archiviandolo in supporti informatici.

Quando gli investigatori hanno cominciato a controllare la casa, si sono imbattuti in alcuni files vietati. E hanno sequestrato non solo il pc del giovane, ma anche quello dei genitori (talvolta in uso al figlio) con diversi hard disk.

Scambiano la foto hard della compagna: carabinieri a scuola, dieci nei guai

PADOVA (Aprile 2016).

A 14 anni è stata "prelevata" a scuola dai carabinieri e condotta prima a casa per la perquisizione della cameretta, poi in caserma per un'ora e mezza di accertamenti. A 14 anni ha inoltrato ad alcuni amici la foto di una coetanea completamente nuda e questo suo clic è diventato l'oggetto di un'indagine che coinvolge una decina di giovani. Giovani e inconsapevoli del male che può fare. Giovedì scorso sono stati tutti raggiunti dagli uomini in divisa. Questa storia lascerà ferite difficili da rimarginare.

L'indagine. Un momento di intimità concesso quando tutto va bene si è trasformato in un'arma per ferire nel momento in cui il rapporto si è incrinato. Succede spesso, ora più di prima. I social network e gli smartphone rendono tutto più veloce, abbattono i freni inibitori. Sembra tutto facile, tutto uno scherzo. Ma non è così. Lo ha scoperto, suo malgrado, una ragazza di 14 anni che abita in un paese della Bassa padovana e frequenta la prima classe in un istituto tecnico sempre in quella zona. In queste ultime settimane le sue foto nuda (una scattata davanti allo specchio) sono volate di telefonino in telefonino. Ma non c'è nulla di virtuale in tutto ciò perché le voci e le risate sono arrivate fino in paese, in classe, nei cortili dove si svolgono le ricreazioni. E quel clic su WhatsApp si è trasformato in un incubo da cui fatica a uscire. Giunta al culmine della preoccupazione si è dovuta confidare con i genitori che sono corsi a denunciare tutto ai carabinieri. È nata così un'indagine coordinata dalla Procura dei Minori che ha disposto accertamenti e perquisizioni a carico di una decina di ragazzi.

Choc a scuola. Il contesto è questo e, purtroppo, non è un caso isolato. Non è il primo e non sarà l'ultimo. Ciò che è successo dopo, però, rischia di ferire altri ragazzini. Sicuramente una dei dieci che ora sono accusati di aver diffuso il materiale hard. Sì, perché una giovane di prima superiore, studentessa in un istituto professionale di Padova, giovedì mattina si è vista raggiungere dai carabinieri nel parcheggio della scuola. Erano circa le sette e mezzo. Appena varcato l'ingresso ha notato la pattuglia dell'Arma ma non ci ha fatto troppo caso, salvo poi rendersi conto che dall'auto stava uscendo suo padre. Il genitore, su indicazione dei militari, l'ha raggiunta e invitata a salire in macchina. Tutto davanti agli occhi dei compagni di classe, quasi increduli. Durante il tragitto tra Padova e il paesino di provincia in cui abita il maresciallo le ha spiegato ciò che la Legge le contesta: aver diffuso le foto hard della coetanea. In lacrime ha assistito al momento in cui i carabinieri hanno indossato i guanti bianchi per prendere in mano il suo computer, il suo telefonino, il suo iPad. Hanno esaminato anche alcuni mozziconi di sigaretta. Poi hanno chiesto a padre e figlia di seguirli in caserma e lì sono rimasti un'ora e mezza.

Dieci nei guai. Sono dieci i giovani accusati di aver diffuso con leggerezza l'immagine della loro amica senza veli. Si conoscono quasi tutti perché a quell'età ci si vede in giro, a scuola, nella piazza del paese. Tutti giovedì mattina sono stati raggiunti dai carabinieri, chi in un modo chi nell'altro. E tutti si sono ritrovati in caserma per dare spiegazioni, rispondere a domande, consegnare i telefonini nelle mani di chi ora sta indagando. Pensavano si trattasse di una ragazzata, invece è proprio una brutta storia.

Su WhatsApp il video hard di due coppie di minorenni

(Settembre 2016).

Doveva essere un gioco tra di loro. Un video che li ritraeva in momenti di intimità, due coppie di minorenni chiuse in una stanza mentre i genitori erano fuori. Un'idea che all'inizio ha trovato tutti favorevoli, massì, resta tra di noi. Ma che è diventata un boomerang quando il filmato è stato condiviso su WhatsApp con altre compagne di scuola. A quel punto una delle minorenni coinvolte si è rivolta in lacrime alla madre ed è scattata la denuncia.

La storia è raccontata sull'*Unione Sarda* di oggi. I protagonisti sono cinque amici del Cagliaritano, due coppie più un altro ragazzino che ha realizzato il video. La serata si era svolta mesi fa a casa di uno degli adolescenti, quando i suoi genitori non c'erano. I fidanzati (probabilmente adesso ex) prima si erano chiusi in stanze separate per stare un po' da soli, dopo avevano deciso di vedersi tutti insieme e infine un quinto è entrato nella camera per filmare la scena dei quattro che si scambiavano effusioni. Doveva restare una cosa tra di loro, ma dopo poco tempo il video è arrivato sul telefonino di qualcun altro. «Ti ho vista, mi hanno mandato il filmato su WhatsApp», ha riferito l'amica di una minorenne. Di qui la denuncia.

Tra qualche giorno i tre ragazzi minorenni dovranno presentarsi davanti al giudice per le udienze preliminari per «aver utilizzato minori di 18 anni per la produzione di materiale pornografico e immagini porno che poi divulgavano». Il caso si inserisce nella scia di fatti di cronaca che hanno per oggetto il sexting, dopo il suicidio di Tiziana Cantone, la 33enne napoletana morta suicida perché esasperata dalla diffusione in Rete di un suo video privato hard.

TikTok, introduce Filtro famiglia e Gestione tempo

TikTok, l'app di destinazione per i video brevi da dispositivi mobili, **introduce due nuove funzionalità: il Filtro Famiglia**, che aiuta i genitori e in generale gli adulti responsabili di un minore, a garantire la sicurezza dei loro ragazzi quando usano TikTok, e la **Gestione del Tempo nel Feed**, un sistema unico di notifiche proattive nell'app per tenere sotto controllo il tempo passato online.

Il **Filtro Famiglia associa l'account TikTok di un adulto a quello del minore di cui è responsabile**. Una volta attivata, l'associazione permetterà all'adulto di intervenire sulle funzionalità di Controllo Applicazione, tra le quali: Gestione del Tempo che permette di impostare un tempo massimo che il minore può trascorrere ogni giorno su TikTok; i messaggi diretti che permette di limitare chi può inviare messaggi all'account associato, o di disattivarli del tutto; la modalità limitata che esclude contenuti che potrebbero non essere appropriati per tutti gli spettatori.

Perseguitava ragazzini trovati su Instagram: arrestato un 21enne a Milano

(Febbraio 2018).

Sceglieva le vittime su Instagram, ragazzini tra i 14 e i 16 anni. Passando al setaccio le foto pubblicate sul social network, prendeva informazioni sulle loro vite. Poi li tempestava di messaggi, anche più di un centinaio in qualche giorno, pieni di espliciti inviti a incontri sessuali. Un «vizio» che aveva da tempo, come lui stesso ha dichiarato agli agenti di polizia che lo hanno arrestato, nel giro di pochi minuti dalla denuncia presentata dalla madre preoccupata di uno studente di un liceo milanese. In manette è finito un 21enne di origine kossovara accusato di atti persecutori e in attesa dell'interrogatorio di convalida davanti al gip. Un «arresto lampo», concluso dagli agenti dell'ufficio prevenzione generale, guidati dal dirigente Maria Josè Falcicchia.

Tutto è iniziato due giorni fa. Il 21enne ha puntato il ragazzo che, sul profilo Instagram aveva salvato il numero di cellulare. Prima gli ha chiesto di sentirsi su Facebook e la vittima si è rifiutata. Poi lo ha contattato su Whatsapp. Nel giro di poche ore il 16enne ha capito che la situazione si stava facendo pericolosa e ha chiesto aiuto alla madre. Le ha detto di non voler andare a scuola perché, dalle foto pubblicate, quello sconosciuto aveva scoperto quale liceo frequentasse. La signora inizialmente ha provato a tranquillizzarlo e la mattina dopo lo ha accompagnato personalmente a scuola. Ma quell'uomo continuava a scrivere con un tono che si faceva sempre più insistente.

Così appena il figlio è tornato a casa, insieme si sono presentati negli uffici della questura. Mentre erano intenti a firmare la denuncia, alle 16.38 è arrivato al 16enne l'ultimo messaggio, con l'invito a presentarsi in un posto in zona Lambrate. Qualche minuto più tardi una volante era già davanti al luogo in cui si sarebbe dovuto tenere l'incontro. Una volta individuato, il 21enne è stato arrestato. Già nel 2016 aveva avuto guai di questo tipo con la giustizia. Agli agenti l'indagato ha detto: «Ho sbagliato di nuovo: è un vizio e non riesco a smettere». Il 16enne non era l'unica attuale vittima dello stalker. La polizia ha individuato già altri tre ragazzini, ma il numero è destinato a crescere in questi giorni.

Lodi, 13enne ricattata per foto intime pensa al suicidio. La polizia a scuola: denunciato un compagno

19/03/2019

La paura e la vergogna per le continue minacce del compagno di scuola l'avevano portata a progettare il suicidio. L'episodio di cyberbullismo è avvenuto in una scuola media di Lodi: venerdì scorso tre pattuglie della polizia di Stato erano intervenute a scuola per sequestrare gli smartphone di alcuni studenti nei quali si sospettava ci fossero chat e video con contenuti offensivi e lesivi della riservatezza della compagna di classe.

La vittima è una ragazzina di 13 anni presa di mira da uno studente che la minacciava di diffondere le sue foto intime se non gliene avesse mandate altre. La situazione di cyberbullismo era già stata segnalata da alcuni allievi agli insegnanti, che dopo aver tenuto lezioni a tema per contrastare il fenomeno hanno deciso di allertare la questura, quando le tensioni in classe sono culminate nel malore della studentessa.

Le indagini, condotte con il sequestro di due telefoni cellulari e colloqui con almeno una decina di studenti, hanno accertato che le fotografie della studentessa venivano fatte circolare via chat contro la sua volontà, con conseguente derisione da parte dei compagni, determinando di fatto una situazione di cyberbullismo. Uno studente di 14 anni è stato denunciato per diffusione di materiale pedopornografico. Al vaglio anche l'ipotesi di estorsione.

La ragazzina è ricoverata in pediatria, è in osservazione dopo lo shock subito. I medici incontreranno la preside per definire insieme una linea di comportamento da tenere dopo che sarà dimessa. "Si tratta di una ragazza che è sempre andata bene a scuola e non ha avuto mai alcun problema – racconta la dirigente - La nostra scuola, proprio quest'anno, si era impegnata per far conoscere agli studenti i pericoli del web, di Internet. E li aveva anche ammoniti, con lezioni tenute dalla polizia, sui risvolti penali di un uso cattivo di questi strumenti. Una situazione del genere non ce la saremmo mai aspettata".

Europol: non usate i WiFi pubblici, sono a rischio di furto di dati. Come difendersi

Troels Oerting, responsabile dell'Europol per la lotta al crimine informatico, ha messo in guardia gli internauti contro il rischio di furto di dati sensibili se usano gli accessi WiFi pubblici.

In un'intervista alla BBC, Oerting ha segnalato la crescita degli attacchi effettuati utilizzando questi accessi *"per rubare informazioni, identità o password e soldi... dovremmo insegnare agli utenti che non dovrebbero gestire informazioni sensibili quando usano un WiFi aperto non sicuro."*

Il WiFi di casa va bene, ha aggiunto, ma è meglio evitare l'accesso senza fili spesso offerto da luoghi di ristoro o locali pubblici.

La tecnica d'attacco è semplice: il criminale crea un *hotspot* WiFi che somiglia a quelli pubblici (non è difficile, basta un laptop o uno smartphone) e convince le persone a collegarsi a Internet tramite quell'hotspot. In questo modo i dati delle vittime transitano dai dispositivi del criminale che, con il software opportuno, può intercettarli e decifrarli.

L'attacco in sé non è una novità (in gergo si chiama *"man in the middle"*, letteralmente *"uomo che si mette in mezzo"*): uno dei casi più noti riguarda il Parlamento europeo, che qualche mese fa ha spento il proprio sistema WiFi pubblico dopo che un informatico ha dimostrato quanto era facile usarlo per compiere proprio questo genere d'incursione.

La difesa, per fortuna, è semplice: usare la connessione dati cellulare invece del WiFi. Purtroppo questo diventa assai costoso se si è in roaming.

In casi come questo si può usare il WiFi pubblico, avendo però l'accortezza di adottare un software di cifratura della connessione (VPN), che ha il vantaggio aggiuntivo di mascherare la reale posizione geografica e di scavalcare i filtri adottati da molti fornitori d'accesso (consentendo, per esempio, di vedere i video di Youtube che hanno restrizioni geografiche).

Alcuni nomi: Anonymizer, Avast SecureLine, TunnelBear, disponibili per Windows, Android e iOS.

La polizia postale ai ragazzi: occhio agli sticker, possono essere pericolosi

Anche uno sticker può far male. Sì, gli adesivi digitali gratuiti da creare, scaricare o condividere, tanto alla moda tra i giovanissimi in questo momento, possono a volte nascondere una lato estremamente negativo: questo strumento per le chat rischia infatti di veicolare immagini di contenuto offensivo, violento, discriminatorio, antisemita o pedopornografico. E la polizia postale lancia il suo appello ai ragazzi e non soltanto a loro ma a tutti gli utenti della messaggistica istantanea: "Postate con la testa". E' la raccomandazione che la Polizia postale rivolge a proposito di questa nuova, scivolosa frontiera. La frontiera degli stickers.

"Negli ultimi mesi - ricordano gli investigatori, impegnati un un monitoraggio continuo della rete - anche WhatsApp, sulla scia dei propri competitor, ha offerto agli utenti la possibilità di utilizzare, accanto a emoji, gif e pacchetti di stickers messi a disposizione dall'applicazione stessa, anche la possibilità di crearne di personalizzati, ricavandoli da fotografie reali, tramite diverse App gratuite, disponibili per iOS e Android, che ne consentono la modifica". Questo tipo di servizio sta spopolando soprattutto tra preadolescenti e adolescenti, "i quali, tuttavia, spesso ne fanno un uso improprio, diffondendo adesivi digitali dai contenuti illeciti (pedopornografici, xenofobi, discriminatori). Comportamenti, questi, che configurano reati gravi". A genitori ed insegnanti la Polizia postale consiglia di "sensibilizzare i ragazzi ad un uso consapevole della rete e, in particolare, dei sistemi di instant messaging (WhatsApp, Telegram, etc)", "vigilare sul materiale (video, foto, stickers) che i ragazzi condividono" e "rivolgersi alle forze dell'ordine per segnalare situazioni riconducibili a tale fenomeno".

Tre consigli preziosi anche per i ragazzi, e non meno importanti: "Non create né partecipate a 'gruppi' il cui fine è la diffusione di immagini a sfondo sessuale, razzista ed offensive nei confronti di persone diversamente abili", "non diffondete o scaricate stickers di tale contenuto" e "Se siete a conoscenza che avvengano tali 'fenomeni' tra i vostri amici, parlatene con un adulto di riferimento (genitore, docente, allenatore)".

La violazione privacy ai tempi dei gruppi WhatsApp

Se all'interno della chat collettiva si inseriscono persone che non si conoscono fra loro e che non dispongono dell'altrui contatto, l'inserimento del numero senza un autorizzazione rappresenta sempre una violazione e, quindi, un trattamento **illecito di dati personali**.

Hai costituito un gruppo chiuso su WhatsApp riunendo alcuni amici. Come sempre succede in questi casi, dall'uso si passa facilmente all'abuso. Inizialmente nato con lo scopo di tenervi in contatto, ora il gruppo è diventato ripostiglio di barzellette, video e immagini divertenti, auguri per le feste e qualche foto delle vacanze per fare un po' di invidia. Un giorno decidi di confidare un pettegolezzo particolarmente delicato sul conto di un'altra persona. Lo fai con una certa leggerezza contando sul legame che vi unisce. Non sai però che uno dei componenti del gruppo è legato a questa persona da un'amicizia ancora più forte. Così fa uno screenshot e glielo invia. Lo vieni a sapere dal diretto interessato che ti contatta in privato e ti minaccia di denunciarti per aver divulgato informazioni sensibili coperti dalla privacy. Dal canto tuo pensi di rivalerti contro chi ha fatto la spia: così gli preannunci che, se sarai querelato, agirai allo stesso modo nei suoi confronti.

I messaggi di Whatsapp, se inoltrati al numero chiuso di persone, come appunto le chat private, devono essere considerati alla stregua della **corrispondenza privata**, chiusa e inviolabile.

Pertanto chi rivela a terzi il contenuto della chat o del gruppo WhatsApp commette un reato, quello di **violazione del segreto della corrispondenza**, comportamento che è appunto punito penalmente dal Codice.

****

Negli USA non esiste l'equivalente della Legge Europea sulla Privacy (GDPR) e quindi è possibile, per Facebook / Instagram / Whatsapp / etc. utilizzare i dati / foto / video a fini diversi, come il monitoraggio delle preferenze politiche o religione od altro.

TWITTER: QUEI 140 CARATTERI SONO PER SEMPRE. TUTTI SCHEDATI DAL 2006 AD OGGI

25/11/2014

Cinguettare in libertà, ma non troppo. Un archivio pubblico, raccoglie tutti i tweet dal 2006, anno di lancio del social network, ad oggi. Miliardi e miliardi di post, un pozzo infinito nel quale orientarsi tramite varie chiavi di ricerca.

Ciò che è scritto resta, dunque, anche su Twitter dove troppo spesso si ha l'illusione di poter commentare in libertà. Lo hanno di certo pensato spesso molte star e personaggi famosi che si sono lasciati andare a post irriverenti e talvolta inopportuni. Si pensi a quello di Lady Gaga che appena atterrata a Bangkok, scrisse: "Non vedo l'ora di comprare un rolex falso". Ma anche i milioni di utenti che troppo spesso si abbandonano a commenti conditi di parolacce o insulti.

Cassazione. Diffamazione aggravata se è su bacheca di Facebook

Febbraio 2016

E' diffamazione aggravata, paragonabile a quella a mezzo stampa, anche la diffusione di un messaggio offensivo attraverso una 'bacheca' Facebook. La Cassazione stabilisce la linea dura nei casi di offesa sui social network, sottolineando che "la condotta di postare un commento" costituisce "la pubblicazione e la diffusione di esso, per la idoneità del mezzo utilizzato a determinare la circolazione del commento tra un gruppo di persone, comunque, apprezzabile per composizione numerica". La suprema corte ha per questo confermato la condanna al pagamento di una multa da 1.500 euro, emessa con rito abbreviato, di un componente in congedo del corpo militare della Croce Rossa Italiana. La persona diffamata e *apostrofata tra l'altro come 'verme' e 'parassita'* è Francesco Rocca, all'epoca commissario straordinario della Cri, oggetto delle offese in uno scambio avviato su Facebook nel dicembre 2010. Inizialmente, come denunciato da Rocca, che alla querela aveva allegato la stampa delle pagine Facebook, il dibattito riguardava scelte e iniziative da lui adottate alla guida dell'ente, ma alcuni passaggi, correlati da sue foto, avevano travalicato – come riconosciuto dal giudice di merito - il limite dell'ordinario diritto di critica, per sfociare in palese offese
del suo decoro personale. La Cassazione ha riconosciuto come le frasi quali "parassita del sistema clientelare" o "quando i cialtroni diventano parassiti", che l'istruttoria compiuta nella fase di merito ha attribuito all'imputato, siano "oggettivamente lesive della reputazione", "trasmodando in una gratuita e immotivata aggressione delle qualità personali di Rocca". E il carattere proprio di un messaggio sulla bacheca Facebook, attraverso il quale "gruppi di soggetti socializzano le rispettive esperienze di vita", è potenzialmente quello di "raggiungere un numero indeterminato di persone", e questo giustifica la condanna per diffamazione aggravata.

Foto su Facebook senza consenso: si rischia il carcere

- **Condividere contenuti, come fotografie e video, via Facebook è una delle cose che si fa più spesso**. Condivisione che spesso avviene per lo più senza l'autorizzazione del titolare dei diritti. In questi casi **è molto facile sconfinare nel penale**, si legge su laleggepertutti.it. Ad esempio si commette una violazione del diritto d'autore quando si pubblicano immagini o video realizzati da un altro soggetto che ne è l'autore e il relativo proprietario (un fotografo, un regista, un videoclip musicale appartenente alla relativa etichetta discografica, ecc.). Si commette, invece, un illecito trattamento di dati personali nell'ipotesi – più frequente – di condivisione, sul profilo Facebook, di fotografie e filmati in cui sono presenti altri soggetti senza che questi ne abbiano autorizzato la pubblicazione.
- L'**errore che si commette spesso è quello di ritenere che il consenso a farsi fotografare contenga anche il permesso alla pubblicazione del relativo scatto. Nulla di più falso**. Si può autorizzare una persona a scattare la foto, ma non è detto che ciò implichi anche assenso a farla apparire pubblicamente su Facebook. Se un nostro amico si fa fotografare insieme a noi nel corso di una scampagnata, con un gruppo di compagni, o durante una serata in discoteca, o ancora si presta a un selfie dobbiamo chiedergli una seconda autorizzazione se vogliamo postare l'immagine sul nostro profilo social.
- Quindi, **chi pubblica sul proprio (o sull'altrui) profilo Facebook la foto di un soggetto senza aver prima ottenuto da questi l'autorizzazione** (autorizzazione che può essere anche tacita, ma espressa in modo inequivoco) **commette un reato**.
- La legge sulla privacy, a riguardo, punisce con la **reclusione fino a due anni** chi esegue un illecito trattamento di dati personali tramite internet. È proprio il caso di chi pubblica la fotografia del volto di un altro soggetto senza il suo consenso. La legge richiede che lo scopo della pubblicazione sia quello di trarne profitto e di arrecare un danno alla vittima, ma questa espressione è stata interpretata in senso lato dalla giurisprudenza, secondo cui è sufficiente – ai fini del reato – un semplice fastidio o un turbamento alla vittima. Insomma, il penale scatta anche senza che vi sia un danno di natura patrimoniale.
- La **norma ha trovato ampia applicazione** in tutti i casi di diffusione non autorizzata di fotografie o video a mezzo WhatsApp, Snapchat, Facebook o Youtube. I social network, infatti, nati proprio per la condivisione dei contenuti, sono anche il terreno fertile per questo tipo di reati. Il che denota anche l'assenza di cultura giuridica – oltre che di sensibilità – da parte di questa società, affacciatasi a un mezzo pubblico con inesperienza e incapacità di comprendere le problematiche sottese ai dati altrui.
- **Quando le immagini hanno natura intima** (ad esempio, le foto ritraggono un soggetto nudo o nel compimento di un atto sessuale), **può scattare il reato più grave di stalking**, sempre che la condotta sia "idonea a determinare nella vittima un grave stato d'ansia e una incontrollabile paura che la costringe a modificare le proprie abitudini e a rivolgersi a uno psicologo". Così si è pronunciata la Cassazione di recente.
- Per **ottenere la cancellazione della fotografia** pubblicata sull'altrui profilo Facebook dobbiamo innanzitutto **diffidare il responsabile con una raccomandata a.r.** Non basta un'email o un messaggio su Facebook o su Whatsapp. Quindi potremo denunciare l'accaduto alla Polizia postale o ai Carabinieri. In alternativa potremo recarci alla procura della Repubblica e depositare la querela anche accompagnati da un avvocato. Il processo penale è volto all'applicazione della pena nei confronti del reo.
- Per **chiedere invece il risarcimento del danno** è necessario agire in via civile. Sempre in via civile è possibile ottenere dal tribunale un provvedimento di urgenza che ordini al responsabile la cancellazione della foto.
- Ricordiamo in ultimo che **chi ha prestato il consenso alla pubblicazione di una foto su Facebook può sempre revocarlo** in qualsiasi momento. In tal caso, chi ha pubblicato l'immagine è tenuto a cancellarla. Un caso paradigmatico è quello della coppia che si separa: dopo la cancellazione del matrimonio l'uno dei due può chiedere la rimozione dal profilo dell'ex di tutte le foto scattate insieme e di quelle del matrimonio (leggi Dopo la separazione vanno cancellate le foto di coppia su Facebook). È **esclusa, invece, la responsabilità di Google o di Facebook** a cui è inutile chiedere il risarcimento del danno.
- La responsabilità ricade quindi sempre sull'utente che pubblica la foto su Facebook o su qualsiasi altro sito internet. Solo a questi spetta l'obbligo di ottenere il consenso dell'avente diritto prima di pubblicare on line una fotografia o un video che lo riguardi.

Foto su Facebook, le regole per non finire nei guai

Con la diffusione di device digitali e social network è sempre più facile per gli utenti condividere le proprie foto sul web. A chi non è mai successo di uscire con gli amici, andare ad un concerto o partecipare ad un evento, scattarsi una foto e poi pubblicarla su Facebook o su Instagram?

Un'azione semplice, ormai quasi quotidiana, che spesso viene realizzata senza pensarci ma che potrebbe avere delle conseguenze negative, addirittura risvolti penalistici molto rilevanti. In proposito il portale di informazione legale 'La legge per tutti', ha spiegato quali sono i rischi cui va incontro chi pubblica una foto sul web.

- PUBBLICAZIONE FOTO: LA NORMATIVA

L' articolo 167 del codice privacy - spiega il portale di informazione legale - prevede il reato di illecita diffusione dei dati personali. Quando si verifica? La norma, in particolare, individua due diverse ipotesi:

1) Una prima condotta, punita con la reclusione da sei a diciotto mesi, si realizza in caso di trattamento illecito dei dati personali dal quale derivi un danno al titolare. Si configura un trattamento illecito ogni volta in cui manca il consenso espresso da parte del titolare dei dati personali;

2) Una diversa condotta, conseguente rispetto alla prima, punita con la reclusione da sei a ventiquattro mesi, è realizzata attraverso la comunicazione o diffusione dei dati che sono stati trattati illecitamente. Ciò che rileva è aver portato soggetti non determinati a conoscenza dei dati personali, in qualunque forma, anche attraverso la loro messa a disposizione o consultazione. Non rileva in alcun modo invece l'eventuale danno subito.

- PUBBLICAZIONE FOTO: LE REGOLE DA SEGUIRE

Quali sono quindi le regole per non finire nei guai dopo aver pubblicato una foto sui social? E' importante sapere che viene punito colui che non rispetta le disposizioni dettate in materia di trattamento dei dati personali al fine di trarre per sé o per altri un profitto o di recare un danno ad altri. Dunque un tale comportamento, per essere penalmente rilevante, deve essere caratterizzato da dolo specifico che consiste nell'aver posto in essere il comportamento con lo scopo specifico di trarre profitto o arrecare un danno ad altri.

Non è quindi prevista - si legge ancora sul portale di informazione giuridica - la reclusione per ogni violazione del trattamento dei dati personali. Ad esempio, non è sufficiente il semplice disappunto del soggetto che vede una sua foto o alcuni suoi dati personali diffusi senza aver dato il proprio consenso. Inoltre, il danno rilevante ai fini della configurabilità del reato non è soltanto quello derivato al titolare dei dati trattati, ma anche quello subito da soggetti terzi come conseguenza dell'illecito trattamento.

- PUBBLICAZIONE FOTO: SE IL SOGGETTO SONO I BAMBINI

Problematica strettamente collegata a quella appena vista, seppur diversa per quanto riguarda fondamenti e disciplina, è quella riguardante la pubblicazione di foto sui social che ritraggono bambini.

Ogni genitore ha il diritto di pubblicare una foto del proprio figlio sui social network, tuttavia è importante essere consapevoli che questo può esporre a rischi, decisamente più pericolosi, rispetto alla semplice mancanza del consenso che può verificarsi quando si tratta di foto che ritraggono persone maggiorenni.

La scelta delle amicizie virtuali, inoltre, non limita il numero delle persone che possono vedere la foto pubblicata e, una volta che il file è stato caricato sul social, è possibile salvarlo e utilizzarlo.

Storia di Andrea, sopravvissuta ai cyberbulli: “Sono loro i veri malati. Io ho scelto la vita”

Per molto tempo è stata vittima di bullismo digitale, arrivando anche a pensare al suicidio. Ora che sta bene, ha deciso di raccontare tutto in un diario dal titolo Ho scelto me

http://www.lastampa.it/2016/06/16/italia/cronache/storia-di-andrea-sopravvissuta-ai-cyberbulli-sono-loro-i-veri-malati-io-ho-scelto-la-vita-hdENW32Q4FeAltuw1DnXLI/pagina.html?utm_source=dlvr.it&utm_medium=twitter

Quel tema di un ragazzo di 12 anni che ha messo a tacere i bulli: "Sono diverso, non sbagliato"

Pubblichiamo in questa pagina il tema di Ivan (nome di fantasia) svolto in risposta alla traccia "Inventa un racconto in cui sono presenti i seguenti personaggi: una vittima, un gruppo di ragazzi prepotenti, degli spettatori, un adulto. Soffermati sui dialoghi e sugli stati d'animo dei diversi personaggi. Alla base del racconto può essere un fatto realmente accaduto o un episodio verosimile. Scegli un finale che preveda uno scioglimento positivo o una soluzione negativa". Quando la sua insegnante riconsegna i lavori (dando 10 al contenuto di Ivan, 8/9 alla forma), chiede al ragazzo se vuole leggere pubblicamente il suo, e lui lo fa. I risultati sono tangibili: alcuni ragazzini coinvolti negli episodi raccontati nel tema chiedono scusa. Anche se non tutti.

ALCUNE persone all'apparenza stanno bene, ma muoiono dentro. Io sono Ivan e ho dodici anni. Vivo in una cittadina del Centro Italia, in una famiglia modesta, ma senza amici. Fin da quando ero all'asilo non ho mai amato i giochi da maschio: calcio, carte, giochi elettronici... A me non sono mai interessati. Preferivo stare con le femmine, più interessanti, a mio parere.
Ero diverso, non sbagliato. Venivo preso in giro, deriso davanti a tutti, perfino i miei amici partecipavano, per poi chiedere pateticamente scusa. "Mamma, ma perché mi trattano così? Cos'ho che non va?!?!". "Tranquillo, amore: sono solo invidiosi!". Io non credo proprio.
Poi arrivo alle elementari, un'occasione di riscatto, lasciando il passato alle spalle. La prima cosa che i compagni notano di me è la mia voce, acuta, squillante, diversa da quella degli altri maschi. Conoscevo qualcuno, ma erano proprio quelli che mi guardavano con più disprezzo. Ero solo, di nuovo.
Successivamente lego con due bambine, diventano le mie migliori amiche. Nonostante il nostro profondo legame cerco di stare lontano da tutte e due, temevo che se mi avessero conosciuto meglio se ne sarebbero andate. Le offese si ripetono, non erano pesanti, ma era il modo in cui le dicevano che mi feriva.
Passano quattro anni e arrivo in quinta. Le prese in giro gradualmente finiscono e riesco finalmente ad entrare nel "mondo dei maschi". Francesco, Flavio, Domenico, Roberto: eravamo inseparabili. Con l'arrivo in questo nuovo "mondo" o semplicemente un "diverso punto di vista" (come diceva papà) alcune cose cambiano in me. Inizio a seguire la moda, carte e gameboy sparsi per tutta la camera. Ero felice, finalmente.
Nella classe però c'erano alcuni ragazzi più emarginati, capivo come si sentivano e cercavo di stare vicino anche a loro: Alfredo, Saverio, Livio e Mario. Purtroppo questo bellissimo anno finisce.
Iniziano le medie. C'erano tutti: Livio, Domenico ecc... Entro a testa alta, fiero dell'anno precedente. Ma magari avrei dovuto abbassarla. Ginnastica, il mio punto debole. Non essendo interessato agli sport non ne avevo mai praticato uno. "Tutti alla sbarra! Flessioni!" urla il prof di ginnastica. Fiero di me mi getto sulla sbarra, faccio più flessioni che posso. Ma poi mi fermo. Tutti mi guardano. Uno dei compagni rompe il silenzio: "Ma cosa sei? Una femminuccia?!? ". "Già: scommetto che non sai nemmeno saltare!".
Tutti ridono, mi indicano come se fossi un fenomeno da baraccone. Ero a pezzi. "Omosessuale" "Trans" , ormai era così che mi chiamavano. Inizio con l'autolesionismo, una droga potentissima di cui non puoi più fare a meno. Mi chiedo come sarebbe bere quel bicchiere di candeggina sopra la lavatrice.
Un giorno vado al mare con Domenico e Francesco. Vedo in lontananza Alfredo, Saverio e Livio con cui avevo chiuso i rapporti. Si avvicinano e mi spingono a terra, sento un calcio, poi un altro ancora, iniziano a picchiarmi. Vedo Francesco e Domenico dietro di me, pietrificati, non reagiscono semplicemente perché non vogliono vedere. Mi lasciano a terra senza nemmeno la forza di piangere. Torno a casa e mi chiudo in camera.
Accendo il telefono "Cento nuovi messaggi dal gruppo antIvan". Il gruppo l'aveva creato Alfredo, c'era tutta la scuola. Leggo solo insulti, nessuno mi difende. "Ivan" chissà se ricorderanno questo nome, una volta che non ci sarò più. Apro la finestra e mi lascio andare. È finita, finalmente in pace. Sono diverso, non sbagliato.

Treviso, a 15 anni scrive ai bulli «Non mangio più ma la vostra ignoranza mi ha reso più forte»

«Grazie per avermi lasciata da sola a raccogliere i pezzi rotti di me stessa e fatto in modo che li rimontassi a mio piacimento così da sembrare più forte; grazie perché adesso il mio fisico è cambiato. Non so se è migliorato perché ha perso quei pochi chili che avevo in più e di cui mi vergognavo, dopo tutte le vostre critiche».

« I bulli la prendevano in giro per qualche chilo di troppo e lei ha rinunciato al cibo. È l'anoressia, il riflesso della sua sofferenza.

«Per perdere tutti quei chili ho smesso di mangiare e facendo così ho rovinato il mio metabolismo, e il mio stomaco non accetta più il cibo come faceva prima».

«Grazie per avermi insegnato che nella vita non ci si deve fidare di nessuno, neanche di quelli che si pensano amici veri. Grazie anche a voi ho imparato a capire cosa significa soffrire sul serio di solitudine. Quando mi avete disintegrata all'interno e mi avete lasciata lì, da sola, ne ho approfittato per costruire più di un muro: ogni muro rappresenta la mia personalità, quello più esterno è quello più cattivo, più spesso, oscuro, che fa paura a tutti, mentre quello più interno è quello più sottile e vulnerabile».

«Voglio solo dire un altro grazie a tutti quelli privi di cuore nei miei confronti. Perché nonostante tutto, la vostra ignoranza mi ha reso più forte e ho sempre mantenuto il sorriso davanti a voi, non lasciandovela vinta».

Seviziarono un compagno di scuola: due bulli condannati a 8 anni

Due giovani residenti nel Torinese sono stati condannati a 8 anni e 6 mesi di carcere per aver seviziato un loro compagno di scuola.

Il ragazzo sottoposto alla serie di violenze all'epoca dei fatti era sedicenne, mentre i suoi due compagni di studi erano di qualche anno più grandi. Tutti e tre frequentavano un istituto professionale nella provincia torinese. Le vessazioni dei due bulli, che hanno sempre respinto le accuse, sarebbero durate quasi due anni.

Uno dei due legali di parte civile, l'avvocata Maria Giovanna Musone, commentando la decisione del tribunale ha parlato di "sentenza esemplare". I giudici hanno accolto la richiesta del pm Dionigi Tibone. Le accuse nei confronti dei due ragazzi erano stalking, violenze e lesioni. La storia risale al periodo tra il febbraio 2013 e il settembre 2014.

Fotografano i prof in aula e postano gli scatti su Instagram: 2 studenti sospesi

"Sospesi per un tempo ancora da definire": sono costati cari a due studenti che frequentano il primo anno di un istituto tecnico alcuni scatti postati su Instagram. I due hanno pubblicato sul social network centinaia di immagini dei loro professori, fotografati con i telefonini durante le lezioni.

Una palese violazione del regolamento d'istituto - è vietato utilizzare gli smartphone nelle classi - e della legge sulla privacy. Alcuni giorni fa a scuola si sono però accorti della bravata e hanno subito avvertito la preside.

È scattata così la sospensione sia nei confronti del ragazzo che aveva scattato la maggior parte delle foto, sia del complice, che lo aveva aiutato a scrivere alcuni dei testi che accompagnano le immagini.

Bullismo, il decalogo per i ragazzi

1) Rispetta: Non offendere i tuoi compagni o amici. Anche se ognuno è diverso, la prima regola è il rispetto

2) Coinvolgi: se vedi un tuo coetaneo escluso dai giochi e dalle attività che fate, coinvolgilo, anche se può sembrarti diverso

3) Dialoga: subire il bullismo fa stare male. Parlane con un adulto di cui ti fidi, con i tuoi genitori, con gli insegnanti, con il tuo medico.

4) Segnala: se sai che qualcuno subisce prepotenze, parlane subito con un adulto. Questo non vuol dire fare la spia, ma aiutare gli altri.

5) Reagisci: se gli atti di bullismo diventano violenti, se ti prendono in giro sui social network, dopo averne parlato con la tua famiglia e la scuola se gli episodi continuano rivolgiti ai centri specializzati o a Carabinieri e Polizia di Stato

6) Non isolarti: spesso il bullo provoca quando sei solo. Se stai vicino agli adulti e ai compagni che possono aiutarti, sarà difficile per lui avvicinarsi.

7) No alla violenza: se uno o più persone compiono atti ripetuti di bullismo colpendoti, con violenza difenditi, ma non diventare violento anche tu.

8) Fai buon uso dei social network: usa i social network in maniera responsabile e rispettosa per comunicare con i tuoi amici. Non 'taggare' i tuoi compagni senza aver avuto prima la loro autorizzazione, non parlare male di loro, non caricare video che potrebbero creare imbarazzo o vergogna

9) Pensa prima di agire: Cosa succede se compio quel gesto? Prima di compiere certe azioni, pensa, rifletti e poi agisci. Certe azioni se gravi comportano delle violazioni della legge e si è perseguibili

10) Sconfiggi il bullismo!

UN PERICOLO DI NOME GRAND-SHARENTING

Esporre i "figli in vetrina" è diventata una cattiva abitudine della società 2.0, un malcostume sembra colpire non solo i genitori ma anche i nonni.

Viviamo nell'era del "tutto è social". Ogni giorno siamo invasi da un numero impressionante di contenuti prodotti da aziende e personaggi famosi (gli influencer) ma anche da semplici genitori, vicini di casa e amici di vecchia data che si divertono a condividere con noi ogni istante della loro vita.
Sui social network ci sono persone che postano continuamente contenuti personali, dimenticandosi che ogni volta che si pubblica "qualcosa" si fornisce in modo consapevole (e non) informazioni che possono essere usate da malintenzionati per scopi che potremmo definire non proprio legali.
Il "grand-sharenting" nato dalla semplice fusione delle parole "share" (condividere) e "parenting" (fare i genitori), lo **sharenting** è diventato in pochissimi anni un fenomeno globale, con milioni di genitori impegnati a postare quotidianamente foto e contenuti riguardanti la vita dei propri figli, fino ad arrivare ai casi più estremi con futuri neo papà/mamme che pubblicano le immagini della prima ecografia del bimbo pur di ottenere un migliaio di "mi piace" o un buon numeri di commenti.
Purtroppo, il fenomeno dello sharenting non sembra essere limitato ai soli genitori: negli ultimi anni ha contagiato una platea più vasta, quella degli over 65. Infatti, nei paesi anglofoni è stata coniata l'espressione grandsharenting per tutti quei nonni (grandfather in inglese) che si divertono a condividere informazioni di qualsiasi tipo sui propri nipoti e figli.
Tra un decennio, il fenomeno dei furti d'identità colpirà circa due terzi dei giovani di età superiore ai 18 anni, procurando un danno quantificabile sui 800 milioni di euro all'anno: queste sono le stime previste da una ricerca condotta da una serie di istituti bancari inglesi.
Quando scattiamo una foto con il nostro smartphone o con la fotocamera digitale dobbiamo ricordarci che nelle immagini sono contenute preziose informazioni: i famosi metadati. Posizione, data e ora sono solo alcuni dei dati contenuti in queste immagini e che possono diventare pericolosi se cadono nelle mani sbagliate. Per gli hacker, infatti, è davvero facile risalire al nome di una persona, alla data di nascita e all'indirizzo di casa sfruttando i soli metadati.
Quando postiamo una foto della nostra camera da letto o del giardino di casa su Facebook o Instagram ricordiamoci che stiamo fornendo informazioni che possono essere sfruttate non solo da criminali ma anche dal Governo o dai servizi segreti, senza dimenticare i reparti marketing delle aziende che sono disposti a pagare qualsiasi cifra per entrare in possesso di tutte le informazioni che produciamo con i nostri dispositivi digitali.
Gli esperti di sicurezza online hanno condiviso una serie di consigli per tutti quei nonni affetti dalla patologia del grand-sharenting, perchè la privacy della famiglia è sacra.
Per esempio, una pessima abitudine è quella di postare foto sui social network quando si è in vacanza da qualche parte del globo o via per un viaggio di lavoro. I ladri d'appartamento non aspettano altro e molti di loro controllano abitualmente Facebook, Instagram e gli altri social media per verificare se siamo in casa oppure no.
Con Google Maps i criminali hanno l'opportunità di studiare in modo dettagliato la nostra casa, i punti di accesso e persino controllare se c'è installato un allarme o un sistema di telecamere a circuito chiuso. Pubblicando una foto del nostro salotto o di una stanza particolare possiamo attirare la loro attenzione (ci sono oggetti di valore), come dimostrano i numerosi casi di furti con protagonisti calciatori e personaggi dello spettacolo. Un consiglio utile è quello di non postare mai una foto raffigurante l'ingresso della casa o il numero civico del cancello per evitare di fornire l'indirizzo al nostro potenziale ladro.
(…continua…)

Quando pubblichiamo la foto di compleanno del nipotino evitiamo di fornire informazioni troppo dettagliate: possiamo pubblicarla la settimana successiva e senza specificare l'età del festeggiato (mai mettere o rendere visibile a tutti la propria data di nascita o quella dei famigliari!).
Quando pubblichiamo un commento sulla bacheca di un amico o di un nostro famigliare riflettiamo prima di condividere informazioni "sensibili".
Oltre a prestare attenzione al materiale che pubblichiamo abitualmente, un altro consiglio è quello di modificare le password predefinite dei dispositivi digitali/elettronici presenti nella nostra abitazione: router, altoparlanti intelligenti come Alexa o Google Home, telecamere di sicurezza e persino certi giocattoli interattivi.
Per gli hacker prendere il controllo di questi dispositivi via Internet o Bluetooth è un gioco da ragazzi, così come ascoltare e registrare le conversazioni tramite la telecamera posizionata nella camera del bambino per vedere se dorme e così via.
Non dobbiamo postare mai informazioni riguardanti gli hobby dei nostri nipoti/ figli né i loro interessi: molti pedofili e predatori sessuali non aspettano altro che avere informazioni precise per entrare in contatto con loro.
Se il nostro nipotino ha una passione per un videogioco o uno sport particolare, evitiamo di scriverlo continuamente.
Infine, prestiamo attenzione alle truffe: le persone di una certa età si mostrano sensibili a certi inganni che diventano "credibili" grazie alle informazioni che i criminali riescono a trovare online.
Ricapitolando, i social network sono una risorsa e per sfruttarla al meglio è necessario che tutta la famiglia sia sulla stessa linea d'onda.
Non ha senso che un famigliare stia attento a pubblicare certe foto se poi un altro le posta in modo indiscriminato ovunque.
Consigliamo ai nonni affetti da grand-sharenting di trasformare il proprio profilo pubblico in privato e di concordare con la propria famiglia "cosa e dove" pubblicare certi contenuti.

******

Un po' per orgoglio personale, un po' per quella voglia di essere protagonisti in quest'era social, molti genitori si divertono a condividere sui social network la vita dei propri figli. Il famoso sociologo Vanni Codeluppi l'ha ribattezzata vetrinizzazione sociale.
Il fenomeno dello sharenting è stato oggetto delle attenzioni della Commissione Europea con il recente regolamento sulla protezione dei dati personali (il famoso "General Data Protection Regulation").
La UE ha stabilito in modo chiaro e perentorio come la pubblicazione di foto/video di un minore sia soggetta alle nuove restrittive norme in tema di privacy.
Lo sharenting trasforma la vita di ogni individuo in un gigantesco archivio digitale pubblico: questo è pericoloso per la "Web reputation" dei bambini che, diventati ormai adolescenti, hanno il timore di scoprire cos'hanno condiviso i propri genitori sui social network.
In loro cresce la paura di essere giudicati negativamente dai coetanei, l'ansia di diventare potenziali vittime di cyberbullismo e la preoccupazione di avere problemi quando si troveranno a fare dei colloqui di lavoro.
Quindi, teniamolo a mente quando pubblichiamo il milionesimo post sui nostri adorati bambini.

Dispositivi smart

Sicurezza *easy*

- Evitare app di provenienza dubbia o non originale
- Scaricare solo app famose, solo dai siti sicuri, e pagarle con carte prepagate
- Usare antivirus sui computer (anche Mac)
  e sui tablet e smartphone Android
- Non "craccare" iPhone, iPad, iPod touch
- Stare aggiornati sempre
- Usare password difficili e differenti e l'autenticazione a due fattori
- Salvare una copia dei propri dati (backup)

la tua PRIVACY è a RISCHIO

anche se non usi i social

Inutile cancellarsi da Twitter o Facebook per proteggere la nostra intimità. A rivelare preziose informazioni su di noi, in modo pericolosamente inconsapevole, sono prima di tutto i nostri contatti. Alle aziende basta utilizzare gli algoritmi giusti

Oggi la tutela della privacy non è più un fatto privato ma collettivo. Non solo perché governi e organi legislativi sovranazionali (come il Parlamento europeo) si occupano e si preoccupano sempre di più dell'argomento, ma soprattutto perché per difenderci non è sufficiente cancellarsi da un social, evitare di utilizzare alcuni strumenti online o stare attenti ai permessi accordati quando comunichiamo i nostri dati. **Può bastare l'uso di qualche app sul telefono, incrociato con le attività sulle principali piattaforme social dei nostri amici, perché molto di noi sia noto a tante aziende**, che sfrutteranno le informazioni raccolte a nostra insaputa per scopi economici e talvolta non solo. A suggerirlo, dando prova concreta di quanto può accadere, è uno studio pubblicato sulla prestigiosa rivista Nature Human Behavior.

I numeri non mentono

La ricerca, condotta da un'università americana del Vermont in collaborazione con un istituto australiano di Adelaide, parla chiaro: pur eliminando correttamente tutti i nostri profili social, dati e informazioni private che ci riguardano possono finire nelle mani di chissà chi. Persino se non ci siamo mai iscritti a un solo social network in tutta la nostra vita. E questo per un motivo molto semplice: abbiamo degli amici che invece i sociali li utilizzano. Vediamo prima come si sono mossi i ricercatori per portare alla luce il problema. Hanno analizzato 30 milioni di messaggi su Twitter pubblicati da quasi 14 mila persone. Successivamente hanno selezionato in questo *mare magnum* di iscritti 927 individui con un numero di follower compreso tra 50 e 500. Poiché quello che fanno i nostri amici può essere indicativo di ciò che amiamo fare (e facciamo) noi, la presenza di post o tweet di amici fa sì che alcuni algoritmi matematici possano prevedere gli incontri e le attività future di chi non è iscritto alla piattaforma. Tra l'altro con una precisione elevata. Il modello di calcolo applicato si basa sull'entropia, ovvero sulla stima dell'incertezza di quello che una persona, pur avendo pubblicato un certo messaggio sui social, andrà a pubblicare successivamente. Più entropia significa maggiore variabilità e minore prevedibilità. Tra i risultati più interessanti di questo studio c'è il fatto che i tweet dei nostri amici possono più facilmente indicare quello che andremo a pubblicare noi più di quanto non faccia il nostro personale flusso di tweet, ma andiamo per gradi.

Gli ingredienti del calcolo

Nell'analisi dei messaggi, perché il risultato relativo al calcolo dell'entropia ottenuto fosse affidabile, sono stati valutati molti elementi, primo fra tutti la lunghezza del testo e il tipo di lin-

Quando regaliamo informazioni online diffondiamo anche quelle degli amici

PEGGIO DI UNA SPIA

Molti esperti di scienze computazionali concordano sul fatto che siamo solo all'inizio: nel prossimo futuro saranno sempre di più le informazioni che potranno essere carpite e rivelate a partire dai social network, compresi dati sensibili come l'orientamento sessuale, senza bisogno di dichiarazioni o comportamenti espliciti. A rischiare di più sono le categorie più deboli, soprattutto bambini e minori, la cui privacy potrebbe essere involontariamente violata dai genitori stessi.

Effetto farfalla. *In fondo lo potevamo immaginare. Violando la nostra privacy mettiamo a rischio quella di tutte le persone che ci sono vicine a partire dai familiari, creando conseguenze ben più grandi di quelle immaginate all'atto del consenso del trattamento dati.*

Alcuni social svelano più facilmente il luogo dove siamo, altri i nostri desideri

guaggio utilizzato. Ma anche la data, i commenti di risposta al tweet, le altre interazioni raccolte: qualcuno ha fatto un retweet copiando e pubblicando lo stesso messaggio sul proprio profilo oppure ha messo un Mi piace? Fondamentale valutare pure il tipo di relazione tra chi ha pubblicato per primo e tutti gli altri che hanno interagito. Ottenuta la stima dell'entropia, i ricercatori hanno applicato una formula complessa per valutare con quale probabilità si riesca ragionevolmente a prevedere le parole future dell'utente.

9 persone per prevedere il futuro

Passiamo alla parte più stupefacente: i risultati. L'indagine scientifica conclude che **sono sufficienti i messaggi di 8 o 9 persone in stretto contatto con un utente "bersaglio" per riuscire a prevedere in maniera molto accurata, indovinando nel 95% dei casi, il suo tweet successivo. Ma cosa c'entra chi non è iscritto a Twitter in tutto questo? Come abbiamo già accennato, con lo stesso sistema è possibile prevedere le mosse di un utente non iscritto o che ha abbandonato il social.**

Ecco come funzionerebbe la cosa. Si ricavano i nomi di tutti i contatti di una persona non iscritta a Twitter utilizzando, per esempio, le informazioni alle quali accedono molte app installate sul telefono. Tra i contatti si selezionano quelli più stretti ma anche più attivi sul social, ne bastano una decina. Poi si utilizzano gli algoritmi messi a punto nello studio per predire cosa scriverebbe la persona oggetto d'indagine se fosse su Twitter. Perché dovrebbe interessare a qualcuno? Come sottolinea in un articolo pubblicato su Science Matthew Hutson: "*le aziende hanno fatto miliardi di dollari trasformando tutto ciò che diciamo, facciamo e guardiamo online in un esperimento di profilazione dei consumatori. Recentemente, alcuni utenti ne hanno avuto abbastanza, limitando il loro uso dei social media o eliminando completamente i loro account. Ma questa non è garanzia di privacy. Se puoi essere collegato ad altri utenti, la loro attività può esporti*". E più le aziende sanno dei consumatori meglio riescono a vendere i loro prodotti. Profilare tutti, non solo quelli attivi sui social, è come vincere alla lotteria. Tra l'altro si può fare con Twitter ma anche con Facebook e probabilmente con Instagram, ma quest'ultimo va trattato diversamente, perché fornisce informazioni veicolate in modo differente.

Twitter fa male?

Pensato per informarsi sulle cose che ci interessano maggiormente e per aumentare il senso di comunità, Twitter è oggi sempre più criticato. Tra i pericoli che si corrono usandolo non c'è solo quello della rinuncia alla privacy. Si rischia di cadere nelle mani di bulli e disturbatori di ogni genere. Persino di veri e propri molestatori. Amnesty International lo ha definito "tossico per le donne".

I social sanno tutto di te

Qualcuno ha già fatto qualcosa di simile. Facebook, ad esempio, ha sfruttato le liste dei contatti dei propri utenti per creare una sorta di profili ombra "ideali", appartenenti a persone che non si trovano in Rete. I nostri tweet e post sono già stati utilizzati da centinaia di ricercatori per delineare le caratteristiche della nostra personalità, ad esempio allo scopo di capire se abbiamo tendenza alla depressione o all'aggressività, come pure per cercare di definire dai messaggi sui social se siamo persone che votano a destra oppure a sinistra e perché.

Un difetto c'è

La ricerca di cui abbiamo parlato in queste pagine stima un alto livello di capacità predittiva dei tweet futuri per chi è iscritto al social e dei tweet ipotetici per chi non è presente sulla piattaforma, considerando ugualmente importanti tutte le parole postate. Un dettaglio che potrebbe portare a errori e quindi alla raccolta di informazioni errate che di fatto non ci riguardano davvero. Peccato che nel tempo gli algoritmi predittivi sembrano destinati a diventare sempre più sofisticati, quindi sbaglieranno di meno. Pare sia solo questione di tempo.

A pagina 57
Scopri come sfruttare al meglio Hotspot Shield.

Libera l'hotspot in tutta sicurezza

I punti di accesso Wi-Fi gratuiti sono molto comodi, ma il loro uso può mettere in serio pericolo la nostra sicurezza. Vediamo perché e come evitare i rischi.

Siamo in giro, non abbiamo una connessione mobile 3G e troviamo un punto di accesso Wi-Fi che non richiede alcuna password per accedere. La prima cosa che ci viene in mente di fare è collegarci, spesso senza valutare bene i rischi. Facciamo quindi il punto della situazione e scopriamo cosa si può nascondere dietro agli hotspot liberi.

Cosa rischiamo?

Dietro a un accesso libero alla Rete possono nascondersi pericoli e insidie che minacciano la nostra sicurezza. Il problema non è tanto la password di accesso, quanto più la mancanza di crittografia della trasmissione. I così detti standard WPA e WEP, che usiamo anche nei nostri router domestici, servono a fare in modo che le informazioni in transito sulla rete siano indecifrabili a occhi indiscreti. In assenza di questi protocolli, come nel caso degli hotspot liberi, qualsiasi dato è visibile a chiunque abbia un minimo di competenza. Dobbiamo ricordare che le connessioni senza fili funzionano con le onde radio, le stesse che propagano le trasmissioni radiofoniche che ascoltiamo in auto o a casa. Come loro, le onde viaggiano in ogni direzione e, se non criptate, lasciano il contenuto perfettamente in chiaro. Ciò significa che quando ci connettiamo a un hotspot libero, le informazioni che scambiamo si propagano in ogni direzione e chiunque sia munito di un congegno per intercettarle può carpire ogni cosa: password, email, messaggi privati, dati bancari, cronologia di navigazione e altro ancora.

Attenti alle trappole

Per trarci in inganno, molti malintenzionati utilizzano gli hotspot liberi come esche. Confidando nel nostro interesse a sfruttare un collegamento alla Rete a costo zero, i più subdoli creano accessi liberi ben visibili ai passanti, nella speranza che qualcuno si colleghi. Tra gli stratagemmi più gettonati, c'è quello di rinominare la rete Wi-Fi con un identificativo che trasmetta un senso di affidabilità, riprendendo per esempio i nomi delle attività pubbliche, del comune in cui ci troviamo o di associazioni insospettabili, come quelle di volontariato o no-profit. Una volta connessi, ecco che iniziano a tracciare i nostri dati e, nella peggiore delle ipotesi, riescono perfino ad accedere alla memoria dei nostri PC, smartphone o tablet. Un altro trucco, utilizzato sempre con maggior frequenza, consiste nel falsificare la pagina di accesso a

Da sapere!

Le VPN, Virtual Private Network, sono utilizzate anche in ambito aziendale, per garantire la sicurezza delle comunicazioni tra due o più computer all'interno di una rete locale più grande. Alcuni router permettono di crearle dal pannello di configurazione.

Hotspot Shield

Inquadriamo il QR Code in alto se abbiamo un dispositivo Android, in basso per quello con iOS.

Glossario

Scopriamo i significati dei termini più importanti

- **Hotspot Wi-Fi:** letteralmente "punto caldo senza fili". Sta a indicare un accesso alla Rete tramite la tecnologia Wi-Fi aperto a chiunque. Può essere pubblico o privato. Nel primo caso si tratta di Hotspot messi a disposizione da Enti di natura governativa come Comuni, Regioni e via dicendo. Nel secondo vengono annoverati tutti quei collegamenti offerti da bar, alberghi, campeggi, centri commerciali e simili.
- **HTTPS:** acronimo di Hyper Text Transfer Protocol over Secure Socket Layer. Protocollo di sicurezza utilizzato per criptare le trasmissioni via Internet. Viene sfruttato dai siti di home banking, ma anche da Google, Facebook e Twitter.
- **VPN:** acronimo di Virtual Private Network. Rete di comunicazione privata creata ad hoc tra due o più soggetti, utile per rendere sicura la trasmissione dei dati durante l'uso di un hotspot libero.

Le cinque regole da ricordare

Non è difficile proteggersi dalle insidie che si possono nascondere dietro agli hotspot liberi. Basta avere un po' di accortezza, evitare azioni affrettate e mettere in pratica una serie di comportamenti assennati.

1. Connessione manuale
Disattiviamo sempre la ricezione del Wi-Fi quando siamo in giro e, nel caso sia attiva, selezioniamo l'opzione che evita la connessione automatica agli hotspot liberi. Se comunque stabiliamo il collegamento, usiamo sempre un software o un'App per la creazione di una VPN come HotSpot Shield.

2. Evitare i servizi di pagamento
Se siamo collegati a un hotspot libero, evitiamo sempre di usare servizi sensibili, quali l'home banking o account per la compravendita online come Amazon, eBay, PayPal o di qualsiasi altro sito del genere.

3. Niente acquisti
Durante una sessione di collegamento non crittografato, evitiamo assolutamente gli acquisti con la carta di credito e men che meno tramite il nostro conto corrente.

4. Usiamo HTTPS
Prima di collegarci a qualsiasi sito, proviamo a immettere il prefisso HTTPS al posto di HTTP nella barra di navigazione del browser. Se il primo è disponibile, possiamo sfruttare un collegamento criptato tra noi e la pagina in questione.

5. Niente condivisioni
Se stiamo usando un PC portatile con Windows, disattiviamo sempre la condivisione di file e stampanti dal pannello Centro connessioni di rete e condivisione del Pannello di controllo.

un hotspot libero, come quelli utilizzati dai pubblici uffici per offrire connettività ai turisti. In pratica, anziché collegarci attraverso il corretto canale, veniamo reinstradati verso una connessione fraudolenta, che non si limita a intercettare tutti i nostri dati, ma spesso ci reindirizza verso pagine Web piene di virus e spyware. Non solo, se stiamo usando uno smartphone, c'è perfino il rischio di vedersi addebitare costi truffaldini.

Come proteggersi

Mettersi al riparo da questi spiacevoli problemi richiede soprattutto l'uso del buon senso, unito a un pizzico di attenzione in ciò che facciamo. Per prima cosa, quando andiamo in giro con il nostro smartphone o tablet, disattiviamo il collegamento automatico alle Wi-Fi libere o, ancor meglio, disabilitiamo direttamente la ricezione. Possiamo sempre attivarla quando abbiamo intenzione di usare la Rete. In secondo luogo, se ci colleghiamo a un hotspot libero, evitiamo di usare servizi quali l'home banking o accedere ai nostri account utili per l'acquisto online, come PayPal, eBay o Amazon. Eviteremo così di utilizzare dati di accesso che potrebbero far gola a un potenziale malintenzionato che stia tracciando il nostro collegamento. Diamo uno sguardo alla barra degli indirizzi e facciamo attenzione alla presenza del prefisso **HTTPS** quando ci colleghiamo a siti in cui prevediamo di utilizzare i nostri dati personali, come Facebook o Twitter. Questa sigla, che sta a identificare l'uso del protocollo conosciuto come **HyperText Transfer Protocol over Secure Socket Layer**, significa che il collegamento con un determinato sito è protetto dalla crittografia e quindi non tracciabile. È bene però ricordare che nel caso in cui ci colleghiamo a un hotspot libero, la crittografia con HTTPS funziona solo con il sito che la usa. Se ci connettiamo a una pagina con il tradizionale HTTP, ecco che siamo di nuovo sottoposti ai rischi.

Collegandoci alla pagina www.hotspots-wifi.it localizziamo la maggior parte degli hotspot liberi in Italia.

Un aiuto più tecnico

Il miglior modo per mettersi al riparo dai problemi è unire i consigli di cui abbiamo appena parlato alla protezione che può fornirci una **VPN** o **Virtual Private Network**. Si tratta di una speciale infrastruttura di rete, che creiamo appositamente all'interno di quella dell'hotspot libero e ci permette così di sfruttare una rete virtuale criptata non intercettabile. Un programma gratuito come **Hotspot Shield**, disponibile per PC e dispositivi portatili e di cui approfondiamo il funzionamento nel tutorial a pagina 57, permette di instradare la connessione verso i propri server sicuri, evitando così di passare dal router che gestisce l'hotspot libero. Inoltre, maschera l'indirizzo IP con cui ci colleghiamo e, quando possibile, tenta di farci passare in automatico dalla navigazione in HTTP a HTTPS.

Connessi e sicuri

Usiamo Hotspot Shield per blindare il collegamento con i punti di accesso liberi che troviamo in giro.

Navigare in modo sicuro anche quando si usano hotspot pubblici senza crittografia, non è impossibile. Basta usare gli strumenti giusti, insieme al buon senso che dobbiamo avere quando sfruttiamo una connessione non nostra.

Solo pochi passi

Il metodo migliore per evitare che qualche malintenzionato si approfitti della mancanza di crittografia su un hotspot pubblico è usare una VPN, Virtual Private Network, che indica la presenza di una rete privata, in cui le informazioni sono custodite da un collegamento sicuro. Vediamo come crearla con **Hotspot Shield**. Leggi l'articolo a pagina 36.

Cosa ti serve

- ✔ **SMARTPHONE O TABLET** per Hotspot Shield mobile
- ✔ **HOTSPOT SHIELD** il programma da utilizzare

Naviga in sicurezza

Avvia Hotspot Shield sul PC e guarda le sue principali funzioni.

1 Scarica Hotspot Shield

Apri il browser e collegati all'indirizzo **www.hotspotshield.com**, quindi fai clic su **Free Download** per scaricare la versione gratuita del software.

2 Subito pronto all'azione

Dopo l'installazione, Hotspot Shield si attiva automaticamente, disponendosi nella barra di avvio rapido di Windows. Come vedi, la protezione è già in funzione.

3 Modifica la località virtuale

Facendo clic sul selettore **Virtual Location**, puoi cambiare il tuo IP e di conseguenza le indicazioni geografiche che permettono ai siti di recuperare la tua posizione.

4 Fai un test per vedere se funziona

Facendo clic sulla voce **Test**, di fianco alla barra **Virtual Location**, si apre una pagina Web che mostra come la tua connessione viene rilevata. In questo caso, è come se fossimo negli Stati Uniti.

Proteggi il tuo dispositivo mobile

Se sei in giro con smartphone o tablet, Hotspot Shield è un'App che non può mancare.

1 Scarica l'App mobile

Dallo Store del tuo dispositivo mobile, cerca l'App **Hotspot Shield VPN**. Troverai quella compatibile con il sistema utilizzato dal tuo smartphone o tablet. Infatti, è disponibile sia per Android, sia per iOS.

2 Si attiva in una mossa

Come per la versione per PC, anche quella mobile è semplice e intuitiva da usare. La prima schermata riepiloga i campi su cui andrà ad agire. Per attivarla è sufficiente premere il pulsante **Yes, protect my connection!** presente nella parte inferiore della pagina.

3 Conferma la creazione della VPN

Il sistema operativo del dispositivo mobile (nel nostro caso Android) avverte che l'applicazione sta tentando di creare una connessione VPN. Spunta la voce **Considero questa applicazione attendibile** e conferma con **OK**.

4 Collegamento blindato

La connessione adesso è sicura. Nota che la funzione **Private browsing** è attiva e l'IP che verrà rilevato dalle pagine Internet è identificabile con un indirizzo degli Stati Uniti. Per interrompere la protezione, premi **Turn Off Protection**.

5 Accedi alle opzioni

Premendo l'icona con le tre linee orizzontali, che trovi nella parte superiore destra dell'interfaccia, apri il menu delle opzioni. In **Settings** hai solo la possibilità di impostare l'avvio automatico dell'applicazione ogni volta che accendi il dispositivo.

6 Tutto sotto controllo

Premendo **Net Stats** nel menu delle opzioni, si apre la tabella riepilogativa delle connessioni attive in ingresso e in uscita. In questo caso, viene mostrato anche il nome delle altre App che stanno comunicando con l'esterno.

Miniguida all'uso dello smartphone

- **Fate un backup dei vostri dati**: se vi rubano il tablet/smartphone o se si rompe, si guasta o vi cade in acqua, e non avete una copia di scorta dei dati, tutto è perso per sempre.

- **Sappiate che siete tracciati. SEMPRE**: la Polizia o gli specialisti della Rete sanno sempre come identificarvi. Se non vi difendete, lo sapranno anche i pubblicitari ed i molestatori. Non pensate mai di essere anonimi. Non lo siete

- **Non parlate/chattate con gli sconosciuti**: là fuori ci sono truffatori e molestatori senza scrupoli, e sono molto abili. Vi agireranno, anche se voi credete di saperli riconoscere. La soluzione più semplice è non dare corda e bloccarli.

- **Non fidatevi delle promesse di privacy di Facebook, WeChat, Instagram, SnapChat e similari**: qualunque foto, una volta che l'avete messa in Rete, può essere salvata, copiata o inviata a chiunque. Qualunque messaggio, per quanto "privato", può essere intercettato, copiato e ripubblicato. Internet è piena di figuracce fatte in questo modo. Cancellare gli originali non serve a niente.

- **Ricordate che una foto messa online ci resta PER SEMPRE**: fra cinque anni, quella vostra fotografia con la bocca a sedere d'anatra, in posa *gangsta* o con la felpa di Miley Cyrus sarà imbarazzante come la t-shirt di Julio Iglesias di vostra madre. Anche se la cancellate, gli amici ne faranno copie, la vedranno i datori di lavoro ai vostri colloqui. Non fatela, che è meglio.

- Non credete a tutto quello che leggete su Internet: neanche se ve lo dicono gli amici. Probabilmente si sono fatti abbindolare anche loro da qualche storia sensazionale ma fasulla. Pensate con la vostra testa ed informatevi prima di diffondere qualunque cosa.
- Usate Internet per imparare e non solo per perdere tempo: avete a disposizione tutto il sapere dell'Umanità, avete un privilegio che nessuna generazione, prima di voi, ha mai avuto. Non sprecatevi giocando a Ruzzle.
- La gente è furba: più di quello che immaginate, più di quello che potete immaginare.

- *Non fate stupidaggini …….. e divertitevi.*

Video 1 – bullismo online

Video 2 – i pericoli delle chat

Video 3 – l’ingenuità della gente