



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**
 - Programs 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

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 accorgete che non state più "memorizzando" le password (quindi non potrete scordarle). E avrete, nello stesso tempo, la garanzia di averle differenziate.

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:



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.

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 Thailandia. 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 si-

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".



curi 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,

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.



CHIAVI DUPLICABILI

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 le 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.

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 riuscire a fare breccia. ♦

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

Worst Passwords of 2013

The 2013 list of worst passwords, influenced by findings from the SplashData, shows the importance of not using passwords in the application or website being accessed.

1. 1234567890
2. 12345678
3. 1234567
4. qwerty
5. 123456
6. 123456789
7. 1234567890
8. 12345678901
9. 123456789012
10. 1234567890123

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.



Cosa ti serve

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



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.

Un controllo dettagliato

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



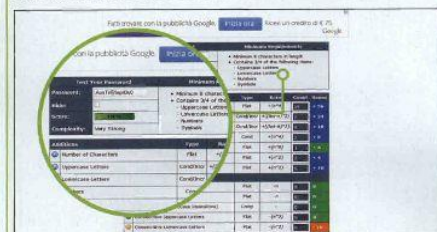
1 Guarda quello che scrivi

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.



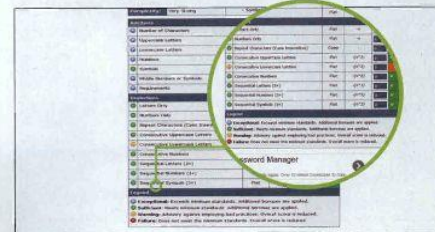
2 Il primo tentativo

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 hai 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 **Additions** 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.



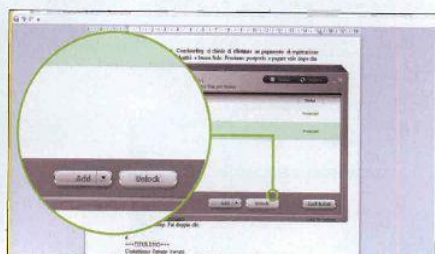
4 Prima li vedevi, ora non ci sono più!

I file e le cartelle che hai aggiunto a Protect Folder sembrano 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 opportunamente 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

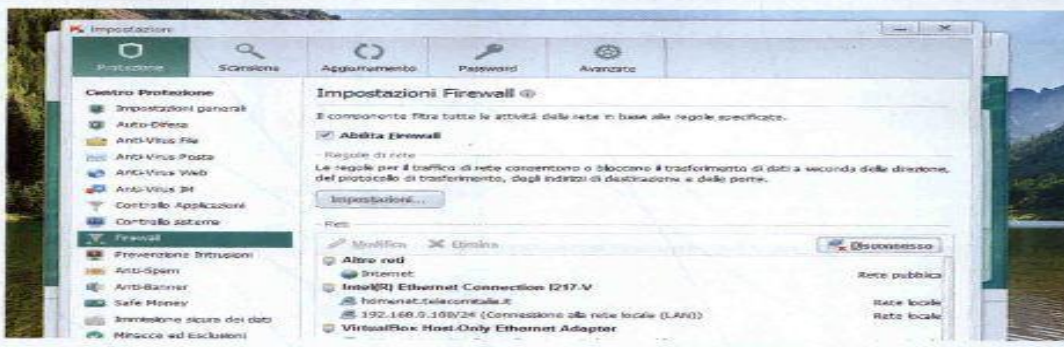
ha bisogno di collegare nessun cavo. Basta che si apposti nelle vicinanze, rilevi la rete con un dispositivo mobile e si metta all'opera per superare le difese. La prima cosa da fare è quindi occultare la visibilità della WLAN (Wireless LAN). In pratica, il nome con cui etichettiamo la rete, chiamato 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.



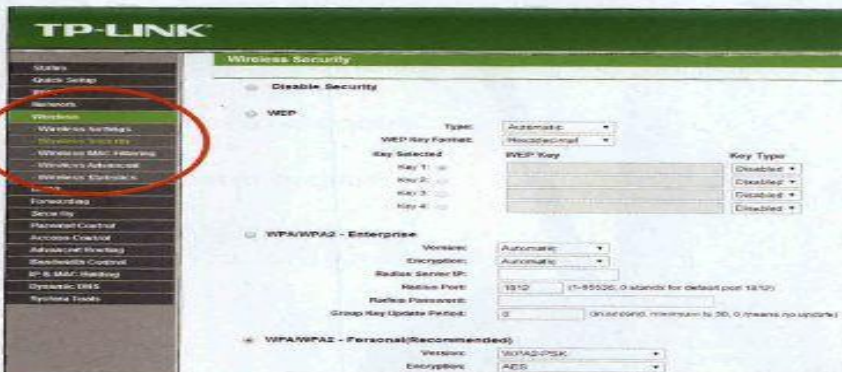
una scansione alla ricerca delle Wi-Fi. Se lo nascondiamo, evitiamo che qualcuno possa accorgersi casualmente della presenza di una rete in zona. Ecco come procedere: nel pannello di gestione del router, andate alla ricerca della voce "Wireless Network Name" e impostate un nome a vostro piacere con cui sarà identificata la WLAN. A questo punto, togliete il segno di spunta da "Enable SSID Broadcast". Anche se esistono stratagemmi piuttosto semplici per avviare 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.

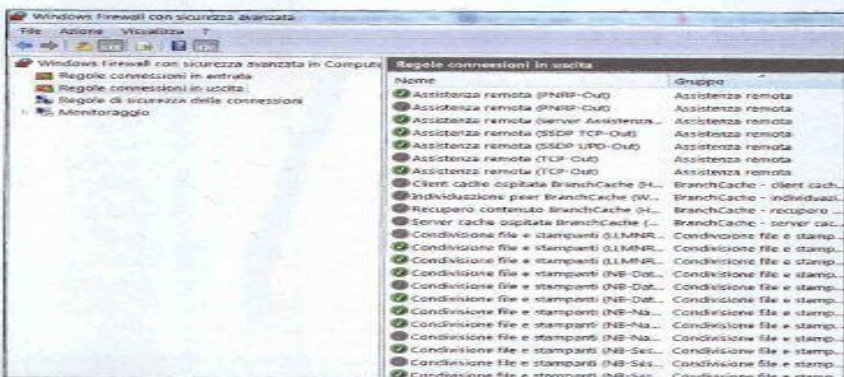
Comunicazioni blindate

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 dati 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'ulteriore 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

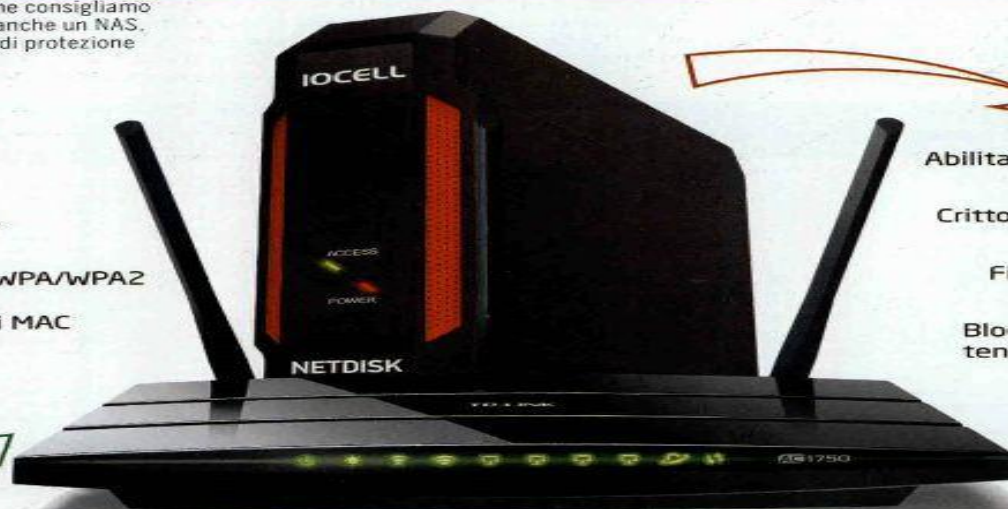
Arriviamo dunque al firewall, l'elemento dedicato alla sicurezza per eccellenza. È grazie a esso se la maggior parte dei tentativi di accesso fraudolento alla rete vengono respinti al mittente. Ogni router ne integra uno e, a differenza di quello del singolo PC, questo sovrintende alla protezione di 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 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.

► 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, permettiamo di criptare i documenti contenuti nei dischi fissi installati al loro interno. È quindi opportuno abilitare questa funzione, mettendosi così al riparo non

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.

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

Gestione Modem

Accesso

Gestione Autenticazione Utente

Attenzione: Ti consigliamo di configurare una password di accesso al modem per aumentare il livello di sicurezza della rete e dei dispositivi collegati. Una volta impostata, la password sarà richiesta ad ogni successivo accesso al modem.

☒ ATTIVA
☐ DISATTIVA

La password deve contenere almeno un carattere di ciascuno dei seguenti insiemi:
 [0 - 9], [a - z], [A - Z].

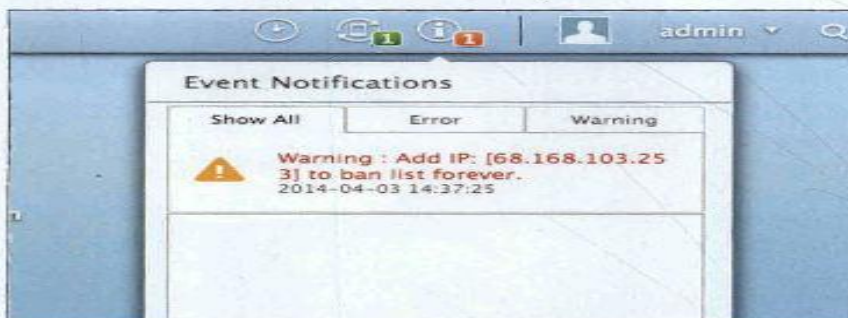
Imposta Password: [4 - 8 caratteri]
 Ripeti Password: [4 - 8 caratteri]

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.

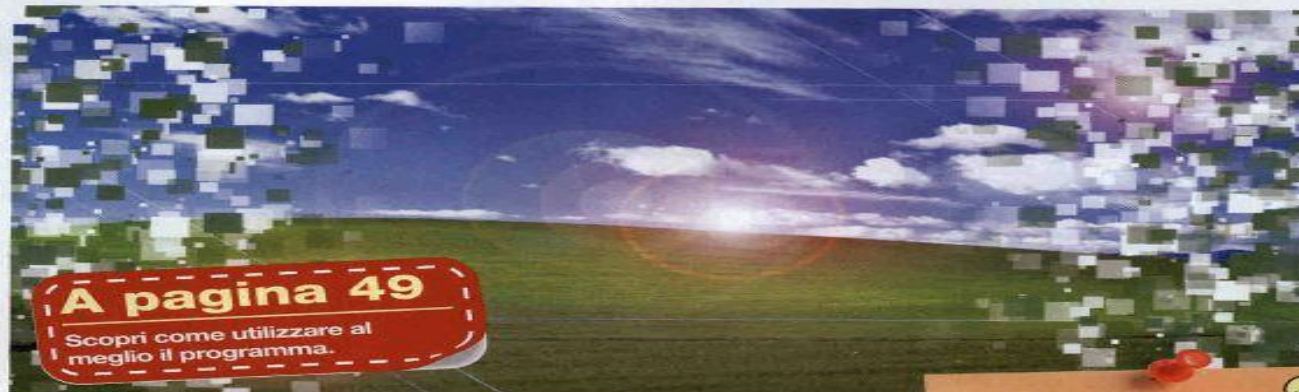
Dovremmo già saperlo, ma nel caso lo ricordiamo: dall'8 aprile, il colosso di Redmond ha terminato il supporto per Windows XP, cui verranno a mancare tutti gli aggiornamenti e l'assistenza di cui un sistema Microsoft gode fin dalla nascita. Usarlo come opzione principale diventa quindi rischioso, ma ciò non impedisce di riportarlo in vita su Windows 7 o 8 con la virtualizzazione. Vediamo come fare.

■ Imbrogliamo XP

Virtualizzare un sistema operativo significa utilizzarlo all'interno di un altro programma, così che condivide le risorse presenti con il sistema principale. In altre parole, per utilizzare Windows XP all'interno di 8, ci avvaliamo di una macchina virtuale che induce XP a credere di essere installato su di un vero e proprio PC. In realtà, sta girando dentro un'applicazione che emula le periferiche hardware come se fossero reali. Il sistema continuerà a rilevare RAM, disco fisso, processore e unità ottiche, senza sapere che sono virtuali, funzionando quindi come di consueto. In definitiva, utilizzare XP con questa modalità ci mette al riparo da notevoli insidie. In primis, qualsiasi virus contratto su di una macchina virtuale vi rimane confinato. In secondo luogo perché possiamo utilizzarlo solo quando serve e come alternativa al sistema principale.

■ La lista della spesa

A parole, un concetto come quello sopra espresso potrebbe sembrare complicato. Il solo pensiero di inserire un sistema operativo dentro l'altro dà l'idea



A pagina 49

Scopri come utilizzare al meglio il programma.

Windows XP in sicurezza

Anche se Microsoft ha interrotto il supporto per il vecchio sistema operativo, possiamo continuare a usarlo senza correre rischi.

di un processo al di fuori delle competenze di molti. Eppure non è così, poiché con appositi programmi come **VirtualBox**, la virtualizzazione è semplice come fare clic su di un'icona. Tutto quello di cui abbiamo bisogno, oltre all'applicazione che possiamo scaricare da **www.virtualbox.org**, è il CD originale di Windows XP con regolare licenza d'uso. Come utilizzare il programma e gestire tutto nel migliore dei modi, oltre a vederlo nel tutorial a pagina 49, lo approfondiremo di seguito.

■ I preparativi

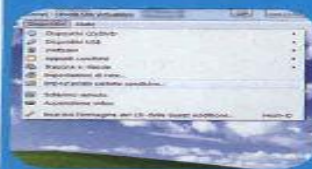
Prima di addentrarci nell'uso di VirtualBox, dobbiamo lavorare per qualche minuto sul CD di Windows XP. Per virtualizzare un sistema, infatti, non è possibile inserire il disco nell'unità ottica e avviare la procedura d'installazione come faremmo normalmente. È invece necessario creare una copia virtuale del disco di XP, che prende il nome di **immagine ISO**. In pratica, si tratta di un'istantanea del CD con tutto ciò che contiene. Farlo è davvero semplice

Da sapere!

Tutti i programmi per la masterizzazione sono in grado di produrre immagini ISO su CD e DVD. È un formato molto comodo, che ci evita di dover aggiornare manualmente i file che vogliamo includere nel supporto di memorizzazione.

e basta un qualsiasi programma per la masterizzazione gratuito come **CDBurnerXP**, **https://cdburnerxp.se**. Inserendo il disco di XP nel masterizzatore del nostro computer e avviando poi CDBurnerXP, non dovremo far altro che selezionare l'opzione che permette di creare l'immagine dal contenuto. Al termine della procedura, che dura solo pochi minuti, verrà generato un file con estensione **.ISO**, che per VirtualBox corrisponderà al CD d'installazione del sistema operativo.

Il consiglio veloce



Impostazioni cartelle a forma di cartella con un più (+) sovrainciso, quindi scegliamo la directory da condividere su Windows 8.

Per generare un ponte tra il sistema operativo principale e quello ospite, possiamo creare una rete virtuale. Sarà così possibile passare i file dall'uno all'altro con un semplice copia e incolla. Nella finestra di Windows XP, nella parte superiore, facciamo clic sul menu **Dispositivi di VirtualBox**, quindi proseguiamo con **condivise**. Selezioniamo l'icona a forma di cartella con un più (+) sovrainciso, quindi scegliamo la directory da condividere su Windows 8.



XP e Linux insieme su Windows 7

No, non si tratta di un'illusione ottica, ma di una delle tante magie di cui è capace VirtualBox con le sue formidabili macchine virtuali.

Un'occhiata a VirtualBox

Ecco il programma che permette di usare XP in una finestra, come qualsiasi altra applicazione.

Il menu

Il pulsante Nuova consente di avviare la procedura guidata per la creazione di una macchina virtuale, mentre Impostazioni di accedere alla sua configurazione. Mostra scompare e viene sostituito con Avvia quando è spenta.

La lista

Qui è dove troviamo le icone che riiepilogano le macchine virtuali con i rispettivi sistemi operativi installati. In questo esempio, possiamo ben vedere come sia possibile far coesistere sistemi Linux con Windows XP.

Le specifiche

In questa sezione vengono riiepilogate tutte le specifiche hardware della macchina virtuale. Così come in un vero e proprio computer, anche il nostro "falso" PC mostra le impostazioni di Rete, delle porte USB, dei dischi fissi e molto altro.

Il sistema virtualizzato

Ecco Windows XP contenuto in una tradizionale finestra al pari di qualsiasi altro programma in esecuzione sul sistema operativo principale. Mouse e tastiera si interfacciano automaticamente ogni volta che passiamo il cursore sopra il riquadro ed eseguiamo un clic.



Creiamo la macchina

A questo punto è venuto il momento di prendere confidenza con VirtualBox, che si dimostra fin da subito un programma piuttosto intuitivo. L'interfaccia grafica è suddivisa in tre sezioni principali: a destra troveremo le icone che permettono di avviare i sistemi operativi virtualizzati. Infatti, così come XP, niente vieta di far girare anche altre versioni di Windows o addirittura di Linux utilizzando lo stesso programma. A sinistra, invece, troviamo la finestra che riiepiloga la configurazione della macchina e quindi ci informa sull'hardware virtualizzato che andremo poi a scegliere. La parte superiore è dedicata alle funzioni principali, su cui dobbiamo concentrarci

per creare il nostro "falso" PC con Windows XP. Per iniziare, basta premere sul pulsante **Nuova** e seguire le istruzioni a schermo che ci guidano in un passo-passo semplice e veloce, al termine del quale avremo scelto le principali caratteristiche del nostro computer virtuale, tra cui il quantitativo di RAM e la capienza del disco fisso. Il primo passaggio è probabilmente il più importante e consiste nell'informare VirtualBox su quale sistema operativo intendiamo virtualizzare. Scrivendo semplicemente Windows XP, nei passi successivi non dovremo neppure preoccuparci di modificare le impostazioni predefinite, perché verranno automaticamente regolate per far funzionare a dovere il sistema.

Se abbiamo Windows 7, per usare XP su una macchina virtuale, basta scaricare XP Mode dal sito Microsoft e avviarlo.

Pronti alla partenza

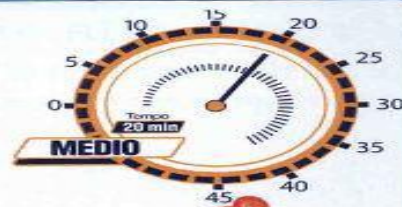
Terminata la creazione della macchina virtuale, vedremo comparire la sua icona nel menu a destra nell'interfaccia di VirtualBox. A questo punto, non dobbiamo fare altro che selezionarla con un clic e premere il pulsante **Impostazioni**. Infatti, è venuto il momento di aggiungere l'immagine ISO del CD di Windows XP nel lettore virtuale che farà partire l'installazione. Spostandoci tra i vari

menu, ecco che troviamo quello di nostro interesse, vale a dire **Archiviazione**. Qui sono riiepilogate le unità di memorizzazione che la macchina virtuale utilizza. Noi dovremo solo aggiungere, sotto la voce **Controller IDE**, l'immagine ISO creata in precedenza. Non resta che avviare la macchina e godersi l'installazione di XP, che terminerà con il sistema operativo pronto all'uso in una finestra di Windows 8. ♦

Utilizzare Windows XP a richiesta, così come facciamo con un comune programma, è un grande vantaggio. Sia perché non dobbiamo dedicargli un computer, né tanto meno utilizzarlo come sistema principale dopo che Microsoft ne ha cessato il supporto. Vediamo quindi come installarlo su **VirtualBox**, un'applicazione capace di creare macchine virtuali, che permettono di utilizzare qualsiasi sistema operativo con pochi e semplici clic. Non dobbiamo né formattare, né compiere complessi passaggi per far convivere più versioni di Windows sullo stesso disco. Tutto quello di cui abbiamo bisogno è un'immagine ISO. Per saperne di più, leggi l'articolo a pagina 26.

Windows XP torna in vita

Con VirtualBox usiamo l'ormai vetusto sistema operativo come se fosse un normale programma.



Cosa ti serve

- ✓ **CD DI WINDOWS XP** naturalmente originale
- ✓ **CDBURNER XP** per creare l'immagine ISO
- ✓ **VIRTUALBOX** per virtualizzare il sistema

Crea l'immagine ISO

Usa **CDBurnerXP** per comprimere il contenuto del CD di Windows in un solo file.



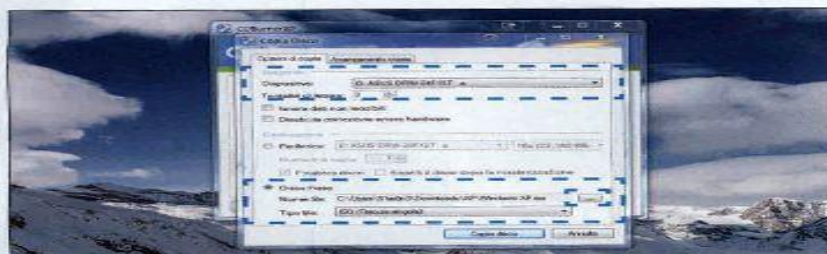
1 Procurati il programma

Punta il browser all'indirizzo <https://cdburnerxp.se/it/home> e scarica **CDBurnerXP**. Una volta fatto, installalo seguendo la procedura guidata e poi avvialo.



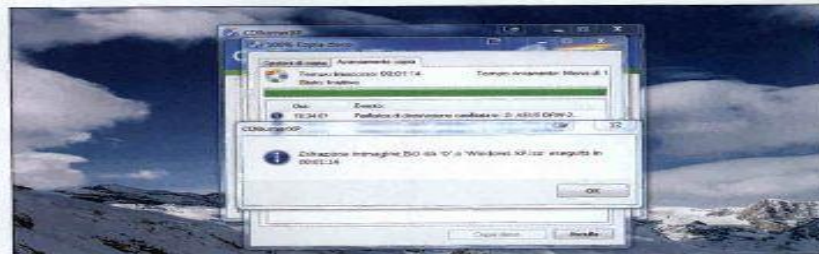
2 Interfaccia semplice e intuitiva

La prima finestra di CDBurnerXP permette di selezionare rapidamente il tipo di attività che vuoi compiere. Inserisci il CD di Windows XP nel lettore, quindi seleziona la voce **Copia disco**.



3 Configura sorgente e destinazione

In **Sorgente**, scegli il masterizzatore. Spunta la voce **Disco fisso** e fai clic sui **tre punti (...)**, quindi scegli il nome dell'immagine. In **Tipo file** seleziona **ISO (Traccia singola)** e premi **Copia disco**.

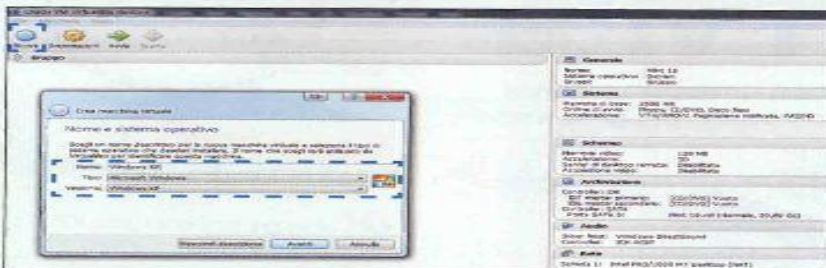


4 Ecco fatto! L'ISO è completa

La procedura di creazione dell'immagine ISO dura soltanto qualche minuto, al termine della quale verrai informato della sua corretta esecuzione.

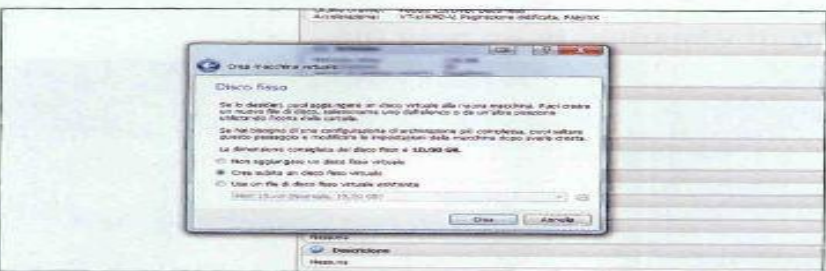
Pronto alla virtualizzazione

È venuto il momento di usare VirtualBox e lanciare Windows XP.



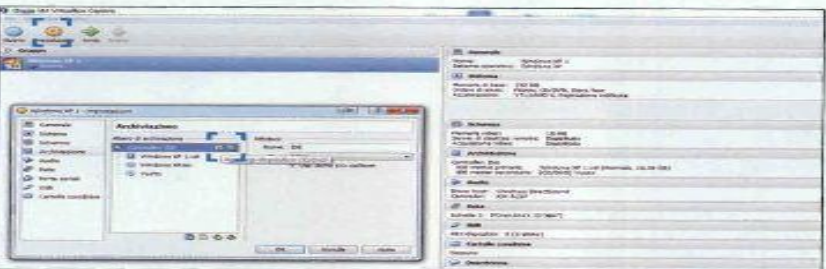
1 Basta solo il nome

Collegati a www.virtualbox.org, quindi scarica il software. Avvialo e fai clic su **Nuova**. Alla voce **Nome**, scrivi Windows XP. Non è necessario aggiungere altro. Basta fare clic su **Avanti**.



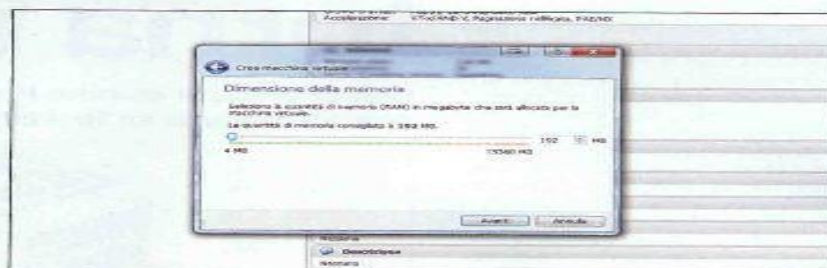
3 Il turno del disco fisso

I passi successivi ti portano a specificare alcune opzioni relative al disco fisso virtuale. Lascia invariato quanto ti propone VirtualBox e fai clic su **Crea**.



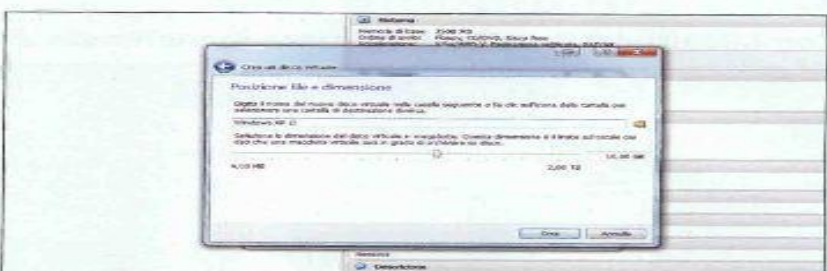
5 Aggiungi l'immagine ISO

Terminata la procedura di creazione del PC virtuale, seleziona dal menu a sinistra e vai in **Impostazioni>Archiviazione**. Fai clic sul + accanto a **Controller IDE** e scegli l'immagine ISO del CD di XP.



2 È il momento della RAM

A questo punto ti verrà chiesto quanta memoria RAM vuoi assegnare alla macchina virtuale. Puoi lasciare invariato il valore proposto da VirtualBox, poiché è già ottimizzato per far funzionare XP.



4 Scegli le dimensioni

Come per la RAM, anche per il disco fisso virtuale puoi scegliere la quantità di spazio. Anche qui, puoi lasciare il valore invariato. Se ne hai necessità, però, niente impedisce di aumentarlo a piacere.



6 Non ti resta che installare XP

Fai clic sull'icona **Avvia** nella barra superiore di VirtualBox. In poco più di due secondi si aprirà la procedura d'installazione di XP, al termine della quale avrai il sistema operativo a disposizione.

Due milioni di password rubate da un solo virus

(07/12/2013)



- Due milioni di password rubate da Facebook e Twitter non sono tante sul miliardo di utenti che li utilizzano ma il fatto che un solo programma sia riuscito a farlo rende la faccenda ben più interessante. Partito il 21 ottobre, l'attacco è valso un bottino di un milione e mezzo di credenziali per l'accesso ai siti, 320 mila account email, 41 mila accessi all'FTP e tremila accessi al remote desktop, il controllo a distanza di un computer da parte di un altro terminale. Oltre ai due social network risultano colpiti anche Gmail, Yahoo e LinkedIn, in pratica la nostra vita in Rete.

VIRUS GLOBALE - La portata è stata globale con ben 92 Paesi colpiti tra cui l'Italia ma va detto però che ad essere assaltati sono stati soprattutto gli account coperti da password deboli e scontate come «123456», «123456789», «1234», e, incredibilmente, la parola «password». A livello geografico la nazione più colpita sono stati i Paesi Bassi seguiti da Thailandia, Germania, Singapore e Indonesia. L'Italia fortunatamente non compare tra i primi dieci che vedono la presenza anche di Stati Uniti, Siria, Iran e Libano anche se la localizzazione è difficoltosa. Probabilmente i computer di questi Paesi sono serviti solo da ponte per la diffusione del virus con un sistema di rimpalli continui che fa perdere le tracce dei computer infetti.

..... segue



- **BUSTE PAGA RUBATE**- A prescindere dai privati cittadini, la vittima più illustre di questo attacco è stata la Automatic Data Processing (ADP), azienda statunitense che fornisce software gestionali per la contabilità alle imprese. Al momento le sono state sottratte oltre ottomila credenziali di accesso che vengono usate dalle risorse umane per gestire i pagamenti dei propri dipendenti. Come afferma John Miller di Trustwave, i responsabili dell'attacco potrebbero essere stati in grado di modificare gli stipendi dei dipendenti, tagliarli o aumentarli a loro discrezione.

CAMBIARE PASSWORD - Per correre ai ripari Facebook, LinkedIn e Twitter hanno chiesto agli utenti colpiti di resettare le password mentre Miller consiglia di aggiornare il proprio antivirus e di scaricare le ultime versioni del browser, di tutti i programmi Adobe installati e di Java. E magari, aggiungiamo noi, scegliere una password degna di questo nome

19/05/2014 – Retata globale di hacker, trasformavano i pc in zombie

Perquisiti e denunciati 13 "hacker" (come sono stati definiti, ma sarebbero 'cracker') che hanno messo su una rete di zombie, vale a dire una serie di pc infetti da malware utilizzati in remoto per attacchi informatici come la sottrazione di informazioni e dati sensibili. Accesso abusivo a sistema informatico, detenzione abusiva di codici di accesso, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico e intercettazione di comunicazioni telematiche sono i reati contestati.

La polizia postale, in collaborazione con Fbi e Europol, si è mossa tra Roma, Firenze, Napoli, Palermo, Catania, Milano, Venezia, Trento e Trieste, con il diretto coinvolgimento delle sezioni di Latina, Messina, Vicenza, Bergamo, Enna, Bolzano, Gorizia e Frosinone.

Gli indagati, infatti, si sarebbero procurati un malware denominato 'BlackShades', questo software viene venduto in internet e pubblicizzato come prodotto che consente di avere il controllo dei pc di una rete, con lo scopo di facilitare l'attività di amministrazione. In realtà, oltre alle funzioni lecite, il programma, che può essere reso invisibile agli antivirus tramite cifratura, dà la possibilità di acquisire il pieno controllo dei pc di ignari utenti, attivarne le webcam, i microfoni fino ad intercettare ciò che viene digitato sulle tastiere attraverso tecniche di keylogging, realizzando in tal modo vere e proprie botnet, ovvero reti di computer 'zombie' controllate da un amministratore occulto, il 'Botmaster', utilizzate per effettuare attacchi informatici di varia natura.



08/06/2014 – Polizia postale e Fbi smantellano rete hacker

Un'operazione congiunta di Polizia postale e Fbi ha portato allo smantellamento di una Botnet, ossia una rete di pc 'zombie', in grado di infettare ben 500mila-1 milione di computer nel mondo, 10mila in Italia. Si stima un danno economico nell'ordine di 100 milioni di euro.

Il nome dato all'operazione è 'GameOver Zeus', dal virus Informatico utilizzato per infettare i computer delle vittime. Questo malware, che rientra nella categoria dei cosiddetti trojan bancari, permetteva il totale controllo da remoto della macchina infetta consentendo all'attaccante di carpire informazioni sensibili quali ad esempio le credenziali per l'autenticazione a servizi di banking online o per lanciare attacchi di tipo DDoS (Distributed Denial of Service). Zeus era anche utilizzato per installare un programma malevolo in grado di criptare i dati presenti sui pc delle vittime alle quali veniva poi richiesto il pagamento di un riscatto per la decrittazione.

In Italia sono stati individuati oltre 160 nodi trust della rete, mentre il numero di pc infettati si stima intorno alle 10.000 unità. Oltre a Italia e Stati Uniti, l'operazione – coordinata dalla Procura della Repubblica di Roma - ha visto coinvolte le polizie di Ucraina, Regno Unito, Germania, Giappone, Francia, Olanda e Canada



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 coordinate 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.



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;
- Ransomware 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 usa 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
- Se hai un PC con Windows hai gli **aggiornamenti automatici già attivi**: se possibile, abilitali anche per gli altri programmi che usi

... Aggiorna in particolare il tuo programma per navigare su Internet (Browser)



- **Il Browser è la tua nave** per navigare su Internet, assicurati che sia la più sicura possibile, e mantienila sempre **aggiornata**
- Se hai un PC con Windows e usi Internet Explorer come tuo browser preferito, assicurati di aver scaricato e installato la sua **ultima versione**, sempre **gratuita**

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)

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

Microsoft®
Security Essentials

- 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**

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!



La nostra
vita
nel mondo
fisico

La nostra
vita nel
mondo
virtuale

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 E' VIETATO AI MINORI DI 13 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



- ▶ Adescamento
- ▶ Attenzione alle amicizie
- ▶ Furto di credenziali per l'accesso e furto di identità
- ▶ Sostituzione di persona
- ▶ Diffamazione
- ▶ 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
- ▶ Rivelazione di segreti

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

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 che commette reati**

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

Minore vittima

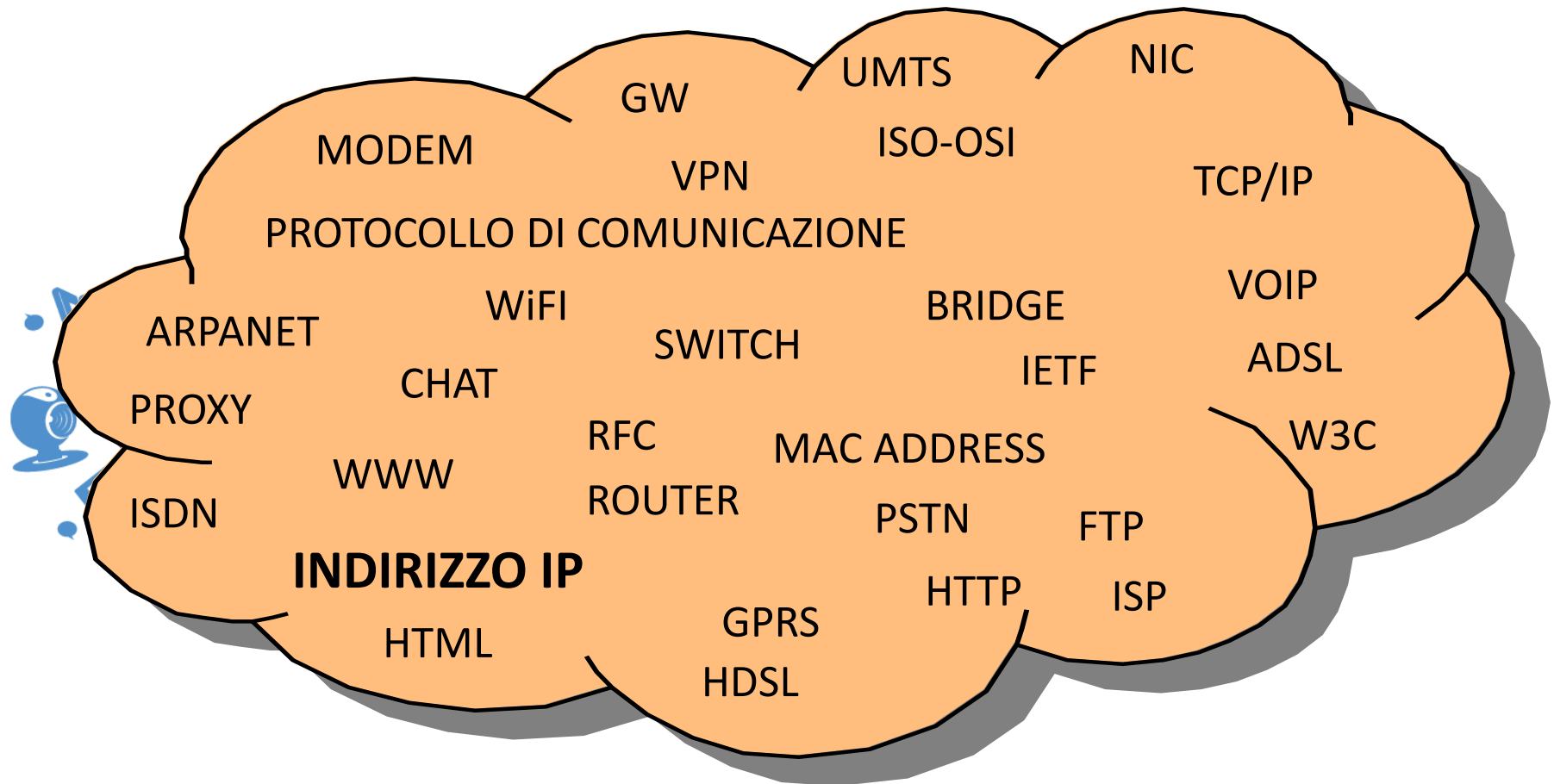
- Adescamento - Scherzo che degenera
- Cyber bullismo - Stalking
- Minacce - Molestie
- Diffamazione - Ingiurie
- Calunnie - Furto di identità
- Accesso abusivo - Danneggiamento

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

Notizia Ansa del 24/05/2014

Adescava ragazzine sul web, denunciato insegnante di 51 anni



Un insegnante di 51 anni di Enna che adescava minorenni a Catania promettendo l'inserimento nel mondo della moda in cambio delle loro attenzioni è stato denunciato dalla polizia postale alla Procura.

Secondo l'accusa, l'uomo sarebbe entrato in contatto, **con un falso profilo di Facebook**, con una tredicenne millantando conoscenze nel mondo della fotografia e della moda con le quali poteva rendere ricca e famosa l'adolescente in cambio delle sue attenzioni. Si era dichiarato disponibile a regalarle "vestiti, scarpe e cose belle", aggiungendo che per una ragazza

come lei poteva "fare pazzie".

Anche un'altra ragazza, amica della vittima, era stata contattata con identiche modalità sul social network.

L'insegnante era anche riuscito a conoscere la minorenne direttamente, pedinandola e fermandola nelle vicinanze di casa, in una zona centrale di Catania, per farle dei complimenti. La ragazzina impaurita per le proposte dell'adescatore e per i suoi pedinamenti aveva avvertito i genitori che hanno denunciato i fatti alla Polizia Postale di Catania. Le indagini hanno consentito di risalire all'uomo indagato, interessato da perquisizioni domiciliare e informatica disposte dalla Procura Distrettuale, nel corso delle quali hanno

trovato conferma le ipotesi investigative degli inquirenti. Sono in corso attività tecniche per comprendere se altri Minorenni siano stati adescati

01/10/2014

In tribunale è stata ascoltata la ragazza, che ha compiuto diciotto anni e abita in un'altra provincia. Alle domande del PM, la ragazzina ha detto di essersi fidanzata virtualmente via Facebook con un diciottenne. Solo quando lo ha incontrato a Marina di Massa, dove si trovava in vacanza con la famiglia, aveva scoperto che in realtà il suo fidanzato virtuale aveva molti anni più di lei. La giovane ha quindi raccontato di essere salita con lui in macchina per paura che pubblicasse le foto osé che gli aveva inviato e che l'uomo aveva preteso un rapporto sessuale. Poi, nonostante lo spavento, la decisione di sporgere denuncia.

ROMA, RAGAZZA DI 15 ANNI VIOLENTATA DA UOMO CONOSCIUTO IN CHAT

25/11/2014

Una ragazza di quindici anni è stata violentata da un 44enne conosciuto in chat.

L'uomo è stato arrestato per violenza sessuale aggravata.

La ragazza si è spacciata per una diciottenne nella chat dove ha conosciuto l'uomo che ha abusato di lei, con il quale, dopo un certo periodo di tempo, si è scambiata anche il numero di cellulare.

Quarantaquattro anni, residente nella zona dei Castelli Romani, l'uomo ha convinto la ragazza a incontrarsi vicino alla Stazione Termini. Poi l'ha invitata ad andare a casa sua per "parlare un po'", ma appena giunti nell'abitazione le ha fatto spegnere il cellulare e contro la sua volontà e l'ha violentata più di una volta.

Incapace di reagire, la ragazza è stata liberata quando sua madre, Preoccupata per le sorti della figlia che non era rincasata, ha chiesto aiuto alla sorella, la zia della 15enne. Quest'ultima è riuscita ad ottenere il numero di telefono del 44enne dall'amica del cuore della nipote: lo ha contattato e ha minacciato di rivolgersi alle forze dell'ordine se non avesse immediatamente detto dove era la 15enne. A quel punto è riuscita a ottenere un appuntamento al quale l'uomo si è presentato con la ragazza riconsegnandola alla zia.

Visibilmente scossa, la giovane non ha voluto confidare alla zia quanto successo ma appena arrivati a casa è scoppiata in lacrime e ha raccontato quanto le era accaduto. La ragazza è stata poi accompagnata in ospedale dove i medici l'hanno visitata e dimessa con una prognosi di alcuni giorni a seguito di alcune escoriazioni riscontrate su varie parti del corpo. La conseguente denuncia negli uffici di polizia del Commissariato di Tivoli, ha fatto scattare subito le indagini.

L'uomo, che dai primi accertamenti abita nella zona di Marino, non è stato reperito in quella che doveva essere la sua dimora. Ma poco più tardi, a seguito di ulteriori verifiche, è stato intercettato vicino all'attività lavorativa della sua attuale compagna e lì bloccato ed arrestato.



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 avvicinare 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».



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 messaggi privati molto in voga tra gli adolescenti. Una situazione che ovviamente ha prodotto nella ragazzina uno 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.



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.



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.



"Se mi posti ti cancello", la web serie contro i pericoli della Rete

29 settembre 2014

“Se mi posti ti cancello”. Non è una minaccia scritta su un social network, magari in un momento di rabbia, ma la webserie disponibile da oggi in esclusiva nella sezione on demand del sito di Mtv. Obiettivo numero uno: aiutare i ragazzi, e specialmente i giovanissimi, a un uso corretto della Rete. Non solo. Perché per combattere i mille pericoli che si annidano sul web (dal cyberbullismo al digital divide) sono gli stessi ragazzi a insegnare ai loro coetanei, rigorosamente via video, come difendersi.

Il progetto, realizzato del Safer Internet Centre Italia, Generazioni Connesse (Sic), coordinato dal Ministero dell'Istruzione e CO-

finanziato dalla Commissione Europea, ha visto la partecipazione anche di numerose associazioni come l'Autorità Garante per l'Infanzia e l'Adolescenza, Polizia di Stato, Save the Children Italia, Telefono Azzurro, Cooperativa E.D.I. e Movimento Difesa del Cittadino.

La serie, che parte oggi con la prima puntata, prende ispirazione dagli oltre 300 video inviati dai ragazzi tra gli 11 e 16 anni che hanno aderito alla Campagna "Se mi posti ti cancello" lanciata da Generazioni Connesse lo scorso febbraio. Cinque i video vincitori, che saranno trasmessi ogni lunedì fino al 27 ottobre. Voce narrante degli episodi, che partono da esperienze realmente vissute dai protagonisti, RichardHTT, webstar di Youtube, che lancia i suoi video sui temi delle puntate in modo alquanto ironico, ma senza tralasciare messaggi di tipo educativo. La serie vedrà anche la partecipazione dell'attrice e comica Alessandra Faiella, nel ruolo di madre di Laura.

Ogni puntata, realizzata con il contributo degli stessi autori dei video selezionati, è dedicata a un tema diverso: cyberbullismo, sexting, esposizione ai media, sessualita' online e digital divide (i materiali sono disponibili anche sul sito www.generazioniconnesse.it/webserie).

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 crittate, 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.



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.

■ 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 HyperText 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 reindirizzati 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

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

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.

■ 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, maschererà l'indirizzo IP con cui ci colleghiamo e, quando possibile, tenta di farci passare in automatico dalla navigazione in HTTP a HTTPS. ♦

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.

Connessi e sicuri

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



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.



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.



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.



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.

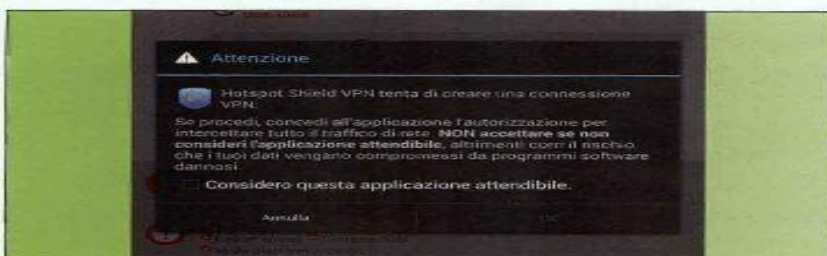
Proteggi il tuo dispositivo mobile

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



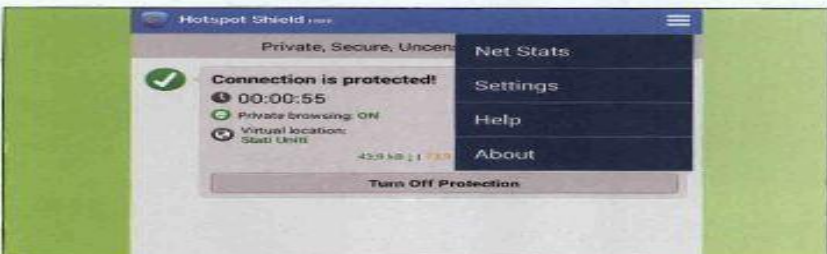
1 Scarica l'App mobile

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.



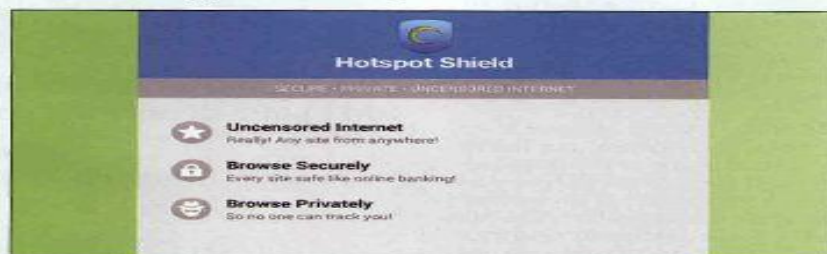
3 Conferma la creazione della VPN

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**.



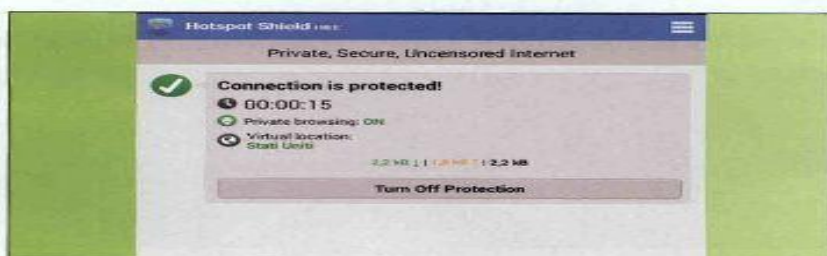
5 Accedi alle opzioni

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.



2 Si attiva in una mossa

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



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**.



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



- **Attivate il GPS solo per le app necessarie:** con pochissime eccezioni, serve soltanto ai pubblicitari ed agli stalker per pedinarvi e localizzarvi meglio. E consuma batteria. Usatelo soltanto per le app di navigazione o per localizzare uno smartphone/tablet smarrito.
- **Controllate spesso che siano disattivati il roaming voce/dati:** altrimenti la bolletta rischia di essere salatissima.
- **Crakkare o fare *jailbreak* per mettere app a scrocco è stupido, non è *cool*;** vuol dire che siete taccagni
- **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



- **Non installate app senza un buon motivo:** le app inutili fanno perdere tempo, rallentano il funzionamento e spesso rubano dati personali o password o mandano sms/mms a pagamento.
- **Occhio agli acquisti in-app:** magari il giochino è gratis, ma gli accessori si pagano. Il fatto che basti fare clic o toccare OK non significa che non siano soldi veri. Disattivate gli acquisti in-app.
- **Specialmente se usate Android, installate un antivirus:** per esempio quello di Sophos.
- **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.
- **Usate nomi falsi per gli account di qualunque app o servizio “social”:** non mettete mai nome e cognome, diventa troppo facile trovarvi per qualunque rompicatole.



- **Non parlate/chattate con gli sconosciuti:** là fuori ci sono truffatori e molestatori senza scrupoli, e sono molto abili. Vi agiranno, 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 simili:** 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 lasciate incustodito il vostro smartphone/tablet:** costa ed i ladri lo smerciano facilmente. Contiene tutti i vostri dati personali, che fanno gola anche ai vostri compagni di scuola. Tenetelo sempre addosso o al sicuro e bloccato con un pin.
- **Tutto quello che è gratis si paga:** non come soldi, ma sotto forma di ficcanasceria. WhatsApp si legge tutti i numeri della vostra rubrica telefonica, per esempio. Se giocate a Candy Crush, l'app vi userà per farsi pubblicità avvisando tutti i vostri amici che ci state giocando (magari in un momento in cui non dovrete).
- **Non fate agli altri quello che non vorreste che gli altri facessero a voi:** è facile prendere in giro qualcuno anche pesantemente o insultarlo al riparo dello schermo. Ma è anche molto vigliacco.



- **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.***

Essere consapevole delle informazioni che stai condividendo, scoprire come controllarle e avere la possibilità di trovare le risposte di cui hai bisogno sono elementi essenziali per garantire un'esperienza online positiva. Anche se Facebook offre una [serie di strumenti](#) pensati proprio per questo, vogliamo aiutarti a capire quali altre risorse hai a disposizione per migliorare la tua vita online, - non solo la tua esperienza su Facebook.

CONSAPEVOLEZZA: cosa sono i dati personali, come vengono condivisi, perché è importante sapere come vengono utilizzati i tuoi dati

CONTROLLO: come faccio a controllare quello che condivido, che scelte posso fare, dove posso trovare maggiori informazioni

PROTEZIONE: chi mi protegge, cosa devo chiedere, dove posso ricevere assistenza

