MOTHERBOARD
TECH BY VICE

La guida di Motherboard per non farsi hackerare

Ecco le cose principali da fare per mettere al sicuro noi stessi e i nostri dati.

Di **Lorenzo Franceschi-Bicchierai e Joseph Cox**

31 agosto 2016, 11:32am

Internet può essere un posto davvero spaventoso, dove un hacker rubano **centinaia di milioni** di **password** in un colpo solo e un altro causare, a piacere, **un blackout su vasta scala**.il futuro non promette molto meglio: **disastri reali causati da apparecchiature connesse a internet**, r**obot domestici che possono uccidere**, **portatili volanti** e **il rischio concreto che un hacker malintenzionato possa aver accesso ai tuoi dati genetici**.

La minaccia è una vostra ex che temete possa accedere al vostro account Facebook? Allora assicurarvi che non conosca la password del suddetto account Facebook, beh, potrebbe essere un buon inizio. (Non condividete mai le passowrd importanti con nessuno, non importa di chi si tratti; se condividete un account Netflix con qualcuno assicuratevi di non riutilizzare *mai* quella password altrove.) State cercando di tenere alla larga qualche truffatore opportunista, ché non riesca a raccogliere troppe informazioni personali sul vostro conto? D'accordo, fate bene attenzione a cosa pubblicate sui social. Ah, usate sempre l'autenticazione a due fattori (approfondiremo più tardi) ogni qual volta sia disponibile. Sempre.

Anche sovrastimare la propria minaccia può generare effetti paradossali, comunque: se cominciate a usare sistemi operativi personalizzati, macchine vertuali o qualsiasi tecnica avanzata dove non necessario (o senza saperle davvero usare) potreste fare qualche danno. Nel migliore dei casi operazioni semplici potrebbero diventare estremamente più lunghe; nel peggiore dei casi, invece, i vostri gadget potrebbero ipnotizzarci in un falso senso di sicurezza, mentre tralasciate le cose davvero importanti.

Con questo in mente, ecco i promessi, semplici, consigli per prevenire alcune delle più comuni minacce online.

RICORDATEVI DI AGGIORNARE LE APP

Forse la cosa più elementare e parimenti importanti che possiate fare, per proteggervi, è usare software sempre aggiornato. Questo significa utilizzare una versione aggiornata, appunto, di qualsiasi sistema operativo utiliziate e aggiornare sempre tanto le vostre app sullo smartphone, quando, in generale, i vostri software. Tenete a mente, anche, che non dovete necessariamente utilizzare l'ultima versione del vostro sistema operativo come, per esempio, Windows 10 (in certi casi alcune versioni passate di un sistema operativo continuano a ricevere supporto e aggiornamento. Purtroppo non è più il caso di **Windows XP**, no, e quindi smettetela subito di usarlo)

Prima lezione della guida di Motherboard alla sicurezza informatica: aggiornate, aggiornate, aggiornate, patchate, patchate, patchate.

Alcuni dei più comuni cyberattacchi sfruttano le vulnerabilità del software datato, che sia un browser o un lettore di PDF. Tenendo tutto aggiornato per benino abbassate di molto le vostre possibilità di essere la prossima vittima di ransomware, per esempio (una forma di hack che prevede il pagamento di un vero e proprio riscatto, entro un certo tempo, pena la salute del vostro computer o dei vostri dati)

PASSWORD

Abbiamo tutti troppe password da tenere a mente ed è proprio il motivo per cui la maggior parte delle persone riutilizza la stessa ovunque. E, **anche se apparentemente i nostri cervelli sono piuttosto efficienti a ricordare le pasword**, è quasi impossibile ricordarsi venti o più password forti, prodotte come si deve.

La buona notizia è che la soluzione al problema è già là fuori: i password manager. Un password manager è un software che genera e memorizza le password al postro vostro e sì, semplifica di molto la vita. Se usate un manager tutto ciò che dovrete ricordare è una singola password, il più complessa possibile, che sblocchi la cassaforte virtuale che contiene tutte le altre.

Intuitivamente, potreste pensare sia poco saggio salvare tutte le vostre password sul computer, per quanto complesse. E se un hacker si facesse largo? Non è certamente meglio me le tenga tutte per me, stipate nella zucca? Beh, no: il rischio che qualcuno si approfitti di una password riciclata su più siti è molto, molto più elevato che qualche hacker, dalle abilità davvero sofisticate, oltretutto, riesca a caricare un malware particolarmente sofisticato sul vostro computer e accedere al manager. Ancora, si tratta di capire cosa vi minaccia.

Quindi, per piacere, usate **uno dei molti password manager disponibili**. Non esiste un solo buon motivo per non farlo. Vi metterà più al sicuro—e noi con voi. E poi, insomma, renderà la vostra vita addirittura più confortevole.

TWO-FACTOR AUTHENTICATION

Avere un'unica password forte è un buon inizio, ma anche queste possono essere sottratte. Per questo, quantomeno per i vostri account più importanti (la vostra mail principale, Facebook e Twitter, per esempio) potreste aggiungere uno strato ulteriore di sicurezza attivando quella che è nota come 2FA, autenticazione a due fattori, o passi.

Attivandola avrete bisogno di qualcosa di più della sola password, per connettervi a questi account. Di solito, un codice numerico mandato al vostro cellulare o potrebbe essere un codice creato da qualche applicazione ad hoc (che è molto comodo quando avete urgenza di connettervi a qualcosa, ma il telefono non ha campo)

Si discute molto, ultimamente, su come i cellulari potrebbero in realtà non essere adatti alla 2FA. **Il numero telefonico dell'attivista Deray McKesson è stato dirottato**, il che signifca che l'hacker in questione aveva accesso ai codici di sicurezza a protezione dei vari account, semplicemente facendoseli spedire. E l'istituto nazionale degli standard e della tecnologia" (NIST), un ramo del governo degli Stati Uniti che compila le linee guida per ogni genere di misure, inclusa la sicurezza, ha recentemente scoraggiato l'uso della 2FA basata su SMS.

L'attacco ai danni di Deray era molto semplice e poco high tech: l'hacker è riuscito a convincere la compagnia telefonica a inviargli una copia della SIM della vittima. È difficile difendersi da questo genere di cose, oltretutto gli SMS presentano altre criticità ed esistono altri modi per ottenere quei codici dal momento che un messaggio può, in linea teorica, essere intercettato da qualcuno che faccia leva su alcune vulnerabilità nella dorsale dell'operatore che gestisce le vostre conversazioni. C'è anche la possibilità di utilizzre un IMSI-catcher, altresì noto come **Stingray**, per intercettare direttamente le comunicazioni e, ovviamente, anche i codici di verifica per l'autenticazione a due fattori.

A differenza di ottenere una nuova SIM, però, questi attacchi non sono per niente rudimentali, non solo perché richiedono strumenti costosi e specifici: proprio come lo Stingray, per esempio. Quindi, realisticamente, per la maggior parte delle persone nel mondo la 2FA via SMS è una misura sufficientemente robusta e adatta al suo compito: aggiungere un ulteriore strato di sicurezza alla propria password che potrebbe essere rubata.

Come anticipato, se il sito lo prevede e ve lo permette, utilizzare un'altra opzione di 2FA (non basate su SMS, ma su delle app di autenticazione (per esempio, **Google Authenticator**) o addirittura assicurarvi un token fisico come **Yubikey** (simili a quelli associati a molte carte di credito). Se queste opzioni sono previste vi consigliamo caldamente di adottarle, ma sarebbe davvero ingeneroso denigrare la buona 2FA via SMS, spercialmente se non siete sotto attacco.

La 2FA è un grande modo di rendere quasi impossibile al cybercriminale medio accedere ai vostri dati. Qui potete controllare tutti i siti che offrono il servizio e le guide su come attivarli.

DOs & DON'Ts

Non utilizzate Flash: Flash è storicamente uno dei software più insicuri che abbia popolato il vostro computer. Gli hacker adorano Flash perché ha più buchi di un formaggio svizzero. La buona notizia è che la gran parte del web ha mollato Flash quindi non ne avete più davvero bisogno, senza rinunciare a un'esperienza di navigazione ricca e piacevole. Quindi, sì, prendete in considerazione di esorcizzarlo dal vostro computer una volta per tutte, o almeno di modificare le impostazioni relative del vostro browser perché vi chieda conferma ogni volta che dovrete aprire un contenuto Flash.

Utilizzate un antivirus: sì, immaginiamo ne abbiate già sentito parlare. Ma resta ancora vero (generalmente). In effettii antivirus, piuttosto

ironicamente, **sono pieni di falle di sicurezza**, ma è del tutto probabile non siate così importanti da essere sotto attacco di un team di hacker nazionali e crittologi. Avere un antivirus rimane una buona idea. Resta il fatto, e non si tratta di paranoia, che nel 2016 avete bisogno di *più* di un antivirus per essere al sicuro.

Utilizzate alcuni semplici plugin di sicurezza: A volte, tutto ciò di cui ha bisogno un hacker per pwnarvi è di attirarti sul sito giusto—ovviamente farcito di malware. Per questo vale la pena usare alcuni semplici plugin come **adblockers**, che vi protegge dalla **pubblicità tossica**. (naturalmente noi di Motherboard avremmo piacere mettiate in whitelist il sito, perché i proventi pubblicitari pagano le nostre bollette)

Un altro plugin utile è **HTTPS-Everywhere**, che forza di default la connessione criptata per tutti quei siti (molti) che lo permettono. Non vi salverà se il sito che state visitando contiene malware, ma in alcuni casi, gli hacker proveranno a re-indirizzarvi su una versione falsa dello stesso sito (se ne esiste una versione criptata) e il plugin vi proteggerà dai tentativi di instrusione nella vostra connessione.

Utilizzare una VPN: se state accedendo a internet da uno spazio pubblico che sia Starbucks, l'aeroporto o addirittura **un appartamento affittato su Airbnb** state condividendo quella connessione con qualcuno che non conoscete. E se un malintenzionato è presente sul network può avere accesso ai vostri dati, compromettere la connessione o, addirittura, danneggiare il computer.

Cercate di non sovraesporvi: Le persone amano condividere sui social qualsiasi aspetto della propria vita. Ma per piacere, vi spplichiamo, non postate su Twitter una foto della vostra carta di credito o cose di questo tipo. Più in generale, è una buona idea capire che un post su un social è spesso un post che chiunque su internet può leggere, che i vostri profili sono visitabili e spesso pubblici e che con un po' di impegno potrebbe anche

scoprire l'indirizzo di casa vostra o i vostri percorsi su siti come Strava, un network per runner e ciclisti.

Le informazioni personali come il vostro indirizzo o le scuole che avete frequentato, a loro volta, possono ricondurre a un gran numero di altre informazioni tramite **ingegneria sociale**. Più informazioni personali sono in possesso dell'hacker e più è probabile riesca a ottenere l'accesso ai vostri accounts. Tenendo questo ben in mente, potreste considerare di aumentare i settaggi relativi alla privacy ovunque possibile.

Non aprite gli allegati mail a cuor leggero: per decenni, i cybercriminali hanno nascosto malware in allegati come file di testo o PDF. Gli antivirus qualche volta intercettano questo tipo di minacce, ma è molto meglio usare il semplice buon senso: non aprite allegati (né cliccate su link) di persone che non conoscete o che non stavate aspettando. E se volete proprio farlo--non potete proprio resistere--fatelo con precauzione, per esempio aprendo l'allegato all'interno di Chrome, senza scaricare effettivamente i file. Ancora meglio: salvate il file su Google Drive e poi apritelo all'interno di Drive; il motivo per cui è un'idea ancora migliore è che in questo modo il file sarà aperto da Google e non dal vostro computer.

Disabilitate le macro: un hacker può utilizzare le macro di Microsoft Office per diffondere malware nel vostro computer. È un vecchio trucco, ma sta **tornando di moda**. Disabilitatele e basta.

Fate regolari backup dei vostri file: sì, come per l'antivirus non stiamo dando un grande suggerimento, ma se siete preoccupati che un hacker possa compromettere i vostri file (per esempio in un caso di **ransomware**) ecco che averne uno o più backup diventa davvero una buona idea. Idealmente, fate i vostri backup sconnessi da internet, utilizzare hard disk esterni così che anche in caso di ransomware il contenuto dei backup non potrà fisicamente essere infettato.