OUCH! | Gennaio 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Tablet e sicurezza

Introduzione

I tablet sono strumenti comodo ed efficace per comunicare con gli altri, per acquistare online, guardare film, giocare e per una miriade di altre attività. Poiché il vostro tablet diventerà molto probabilmente una parte importante della vostra vita, sostituendo spesso il vostro computer, vi presentiamo alcuni suggerimenti che dovreste seguire per proteggere sia il dispositivo sia le informazioni in esso contenute.

L'autore di questo numero

Lori Rosenberg ha maturato una grande esperienza nello sviluppo di strumenti di formazione e training per dipendenti aziendali e clienti, grazie alla sua passione nel trovare sempre metodi nuovi e coinvolgenti per condividere la conoscenza. Potete seguirla su Twitter: **@InfoSecLori**.

Rendere sicuro il tablet

Sarete sopresi dal sapere che il rischio maggiore per il vostro tablet non sono gli hacker, ma siete voi. È molto più probabile che venga perso, dimenticato o sottratto piuttosto che venga compromesso da un hacker. Il primo passo per fare in modo di proteggere il tablet è di abilitare il blocco dello schermo. Questo significa che ogni volta che vorrete usarlo, dovrete prima sbloccarlo con una password, un segno di sblocco o con la vostra impronta digitale. In questo modo anche se verrà perso o sottratto, nessuno vi potrà accedere, proteggendo così tutte le informazioni personali, le app e qualsiasi cosa in esso conservata. Una volte che avrete attivato il blocco dello schermo dovreste seguire alcuni accorgimenti ulteriori:

1. installate o attivate il software per il tracciamento remoto del tablet via Internet, in modo che se andasse smarrito o venisse sottratto, potrete potenzialmente collegarvi ad esso via Internet, individuandone la localizzazione, oppure, nel caso peggiore, cancellando da remoto ogni informazione conservata al suo interno;
2. aggiornate il dispositivo e attivate gli aggiornamenti automatici in modo che sia sempre disponibile l'ultima versione del sistema operativo. I criminali informatici sono sempre alla ricerca di nuove vulnerabilità del software: di conseguenza i produttori rilasciano costantemente nuovi aggiornamenti e patch per porvi rimedio. Grazie alla versione più aggiornata del sistema operativo e delle app, renderete la vita più difficile a chi vuole compromettere il vostro tablet;
3. fate attenzione quando configurate il tablet per la prima volta, specialmente per quanto concerne le opzioni di privacy: uno dei problemi più importanti è infatti la possibilità di essere tracciati e far conoscere la propria posizione. Vi raccomandiamo di disabilitare il tracciamento della localizzazione geografica per qualsiasi cosa, abilitandolo esclusivamente per le

Tablet e sicurezza

app per cui pensiate vi sia realmente bisogno, ad esempio per il navigatore o per i programmi di ricerca dei ristoranti nelle vicinanze. Per la maggior parte delle app invece non è assolutamente necessario;

4. la maggior parte delle app memorizza le vostre informazioni sul cloud, per cui dovreste capire dove risiedono i vostri dati e con che livello di sicurezza sono conservati. Non vorreste mai che le vostre foto private venissero divulgate su Internet in modo che il mondo intero le potesse vedere, conoscendone anche la posizione geografica. Disabilitate per default ogni condivisione di informazioni sul cloud e abilitatela solo quando volete davvero condividere qualcosa di specifico;
5. j tablet sincronizzano le vostre app con altri device, come il vostro smartphone o il laptop. Questa funzione può essere estremamente utile, ma fate attenzione a quali app la permettete. Se avete attivato la sincronizzazione, non sorprendetevi del fatto che i siti che visitate e le tab che create nel browser sul vostro tablet appariranno anche sul vostro PC.

Il miglior modo per rendere sicuro il tablet è abilitare il blocco dello schermo, rivedere le impostazioni di privacy e mantenerlo sempre aggiornato.

Come gestire la sicurezza

Una volta che il vostro tablet è stato messo in sicurezza, sicuramente vorrete mantenerla costantemente. Ecco alcuni accorgimenti per impostarla in modo adeguato:

- non effettuate il jailbreak o il rooting del tablet, operazione che scavalcherebbe e renderebbe inutili molte misure di sicurezza e renderebbe il dispositivo più vulnerabile ad attacchi;
- scaricate solo app di cui avete realmente bisogno e solo da fonti affidabili. Per l'iPad, scaricate app solo da iTunes, poiché vengono analizzate da Apple prima che possano essere rese disponibili. Per i dispositivi Android vi raccomandiamo di scaricare solo da Google Play mentre per i tablet Amazon, solo all'Amazon App Store. Sebbene possiate scaricare app anche da altri siti, sappiate che esse non sono sottoposte ad alcun esame di sicurezza e potrebbero quindi essere infette da malware. Vi racomandiamo infine di cancellare un'app una volta che non ne fate più uso;

Tablet e sicurezza

- quando installate una nuova app, assicuratevi di configurare le opzioni di privacy, così come avete fatto quando avete configurato inizialmente il tablet. Fate attenzione alle funzioni a cui può avere accesso un app: chiedetevi, ad esempio, se una nuova app deve avere veramente accesso ai vostri contatti o alla vostra posizione geografica. Se i permessi richiesti non vi lasciano tranquilli, cercate un'altra app che soddisfi le vostre esigenze. Ricontrollate regolarmente i permessi per verificare che non siano stati modificati.

Il vostro tablet è uno strumento molto potente e vogliamo che lo usiate nel modo migliore. Ricordandovi questi semplici passi, potrete mantenerlo costantemente sicuro.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito

http://www.securingthehuman.org

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Usare le app in modo sicuro:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201501_it.pdf
Le passphrase:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_it.pdf
Usare il Cloud in modo sicuro:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_it.pdf
Lo smaltimento dei dispositivi mobili:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201406_it.pdf

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis