OUCH! | Febbraio 2017

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Sicurezza in viaggio

Introduzione

È possibile usare la tecnologia al meglio in ogni momento, anche quando viaggiamo. In questa newsletter illustreremo come potete collegarvi a Internet e usare i vostri dispositivi in modo sicuro anche durante i viaggi.

L'autore di questo numero

Mark Williams è Enterprise Security Architect presso la BlueCross Blueshield del Tennessee. È anche istruttore SANS e presidente del capitolo ISSA di Chattanooga. Nella sua vita ha viaggiato molto e conosce molto bene le problematiche legate all'uso dei dispositivi durante i viaggi.

Controlli preventivi

Sebbene la vostra rete al lavoro o a casa possa considerarsi sicura, quando viaggiate dovete pensare che ogni rete a cui vi collegate non può essere degna della vostra fiducia. Non potete sapere chi altri vi si è collegato e cosa stia facendo. Ecco alcuni semplici passi da seguire per proteggere voi e i vostri dati anche quando viaggiate.

- L'informazione più sicura è quella che non avete con voi. Identificate quali dati non vi servono sui dispositivi che state portando con voi e rimuoveteli. Questo ridurrà significativamente il danno nei caso i dispositivi vadano persi, vi vengano sottratti o sequestrati in dogana. Se viaggiate per lavoro chiedete al vostro responsabile se l'azienda mette a disposizione dei dispositivi usati specificamente per lavorare durante i viaggi.
- Bloccate il dispositivo mobile o il laptop con una password forte o un passcode. In questo modo, se dovesse essere perso o sottratto, gli estranei non potranno accedere alle informazioni in esso conservate. Attivate o installate la crittografia del disco (full disk encryption) sui dispositivi. Per molti dispositivi mobili, viene attivata quando usate il blocco dello schermo.
- Installate o attivate la funzione per tracciare remotamente dove si trova il vostro dispositivo ed effettuare la cancellazione remota, nel caso non sia più in vostro possesso.
- Aggiornate il dispositivo, le applicazioni e il software anti-virus prima di partire, in modo da avere installate le ultime versioni disponibili. Molti attacchi prendono di mira i dispositivi con software non aggiornato.
- Effettuate un salvataggio completo di tutti i dispositivi. In questo modo, se dovesse succeder loro qualcosa mentre viaggiate, avete comunque tutti i vostri dati originali in un luogo sicuro.

Sicurezza in viaggio

- Per i viaggi internazionali, verificate quale tipo di servizio mette a disposizione il vostro fornitore telefonico. Spesso vengono addebitate tariffe alte per l'utilizzo del collegamento dati, per cui dovreste disattivare la funzione dati in queste situazioni o comprare una SIM locale prepagata.

Per essere più sicuro durante i viaggi proteggi i tuoi dispositivi prima di partire, tienili sempre sotto controllo e usa connessioni protette da crittografia.

Dispositivi persi o sottratti

Una volta che iniziate il vostro viaggio, assicuratevi della sicurezza fisica dei dispositivi. Non lasciateli mai nell'auto, in posizione visibile, poiché un ladro potrebbe rompere un finestrino per impossessarsene facilmente. Sebbene il crimine sia un rischio, secondo una recente indagine condotta da Verizon, la probabilità di perdere un dispositivo è di 100 volte superiore a quella di vederselo sottrarre. Controllate attentamente di avere con voi i vostri dispositivi quando viaggiate, ad esempio, dopo la perquisizione all'aeroporto, quando lasciate un taxi o un ristorante, quando fate il check out in hotel o scendete dall'aereo. Controllate sempre la tasca posteriore del sedile!

Accesso WiFi

Avere accesso a Internet quando si viaggia significa spesso utilizzare i punti di accesso WiFi pubblici, disponibili in hotel, caffetterie o aeroporti. Questi punti di accesso presentano però due problemi: non potete aver fiducia in chi li li ha messi a disposizione e nemmeno potete sapere chi vi è connesso. Per tale motivo essi sono da considerare insicuri, ed è per questo che prima di viaggiare dovete prendere le precauzioni illustrate in precedenza. Il WI-Fi, inoltre, utilizza le onde radio, il che significa che chiunque fisicamente nelle vostre vicinanza può potenzialmente intercettare e monitorare le comunicazioni. Per questo motivo, se usate il WiFi pubblico dovete assicurarvi che le comunicazioni siano protette da crittografia. Ad esempio, quando vi connettete utilizzando il browser, verificate che i siti che visitate siano cifrati: potete assicurarvi di ciò osservando la presenza dell'indirizzo https:// (attenzione alla "s" finale) o l'immagine del lucchetto chiuso di fianco alla barra dell'indirizzo. Oppure potreste avere a disposizione una VPN (Virtual Private Network) in grado di cifrare tutte le vostre attività online. Potrebbe essere stata configurata al lavoro, ma ne esistono anche per uso privato, a pagamento. Se pensate che non ci siano reti WiFi di cui poter aver fiducia, usate il tethering del vostro smartphone. Fate attenzione , però, che i costi

Sicurezza in viaggio

della connettività dati, in roaming, possono essere molto elevati. Controllate prima di partire la tariffa dati internazionale del luogo in cui vi recherete.

Computer nei luoghi pubblici

Se dovete collegarvi a servizi “sensibili” (e-banking, email, ecc) non usate computer pubblici, disponibili negli hotel o nelle caffetterie, perché non potete sapere chi abbia utilizzato quel computer prima di voi: potrebbe essere stato infettato deliberatamente o involontariamente. Quando possibile, usate solo dispositivi che controllate e di cui avete fiducia. I computer pubblici sono utilizzabili per informazioni pubbliche, come il le previsioni del tempo o le news. Collegarsi ad un account, come Gmail ad esempio, è un invito per gli hacker che potrebbero starvi ad osservare.

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
securingthehuman.sans.org/ouch/archives

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

Le Passphrase:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_it.pdf
Salvataggi e ripristino:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_it.pdf
Il Malware:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_it.pdf
La crittografia:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201606_it.pdf

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