OUCH! | Febbraio 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Sicurezza in viaggio

Introduzione

In questa newsletter vi illustreremo come collegarvi a Internet e lavorare in sicurezza anche durante i viaggi.

L'autore di questo numero

Steve Armstrong è Direttore Tecnico del CyberCPR presso Logically Secure, istruttore SANS certificato e autore di corsi. Potete seguirlo su Twitter come **@Nebulator** e su Google plus: **+SteveArmstrongSecurity**.

I controlli prima della partenza

Le vostre reti di casa e dell'ufficio possono considerarsi sicure, ma quando siete in viaggio dovete sempre pensare che ognuna delle reti a cui vi collegate potrebbe non esserlo. Non è possibile sapere chi altro vi sia connesso e a quali minacce potreste essere sottoposti. Per proteggere i vostri dati è quindi opportuno prendere alcune semplici precauzioni prima di partire. Cominciate qualche settimana prima con le seguenti operazioni:

- identificate, sui dispositivi che porterete con voi, quali dati non vi saranno necessari e procedete alla loro rimozione, in modo da ridurre eventuali effetti negativi dovuti a perdita, sottrazione o sequestro alla dogana del dispositivo. Se dovete viaggiare per lavoro, chiedete al vostro responsabile se l'azienda mette a disposizione dei dispositivi alternativi da usare specificamente durante i viaggi;
- in caso di viaggi all'estero, verificate quale tipo di presa di corrente viene utilizzata nella vostra nazione di destinazione: potreste aver bisogno di un adattatore per caricare i vostri dispositivi;
- verificate inoltre qual è il piano tariffario per il vostro telefono all'estero: le tariffe delle compagnie telefoniche per il collegamento dati internazionale sono spesso piuttosto costose. Potrebbe essere opportuno quindi disabilitare le funzionalità di connessione dati durante il viaggio o modificare il piano di servizio;
- installate software di tracciamento sul vostro dispositivo in modo da poter capire dove si trova, nel caso di perdita o sottrazione. Alcuni software sono anche in grado di rimuovere il contenuto del dispositivo, in caso di perdita. Molti dispositivi sono già dotati di queste funzioni, ma dovrete comunque attivarle. Ricordate che queste funzionalità richiedono un collegamento Internet per essere operative.

Il giorno prima di partire:

Sicurezza in viaggio

- aggiornate i vostri dispositivi, le applicazioni e il software anti-virus, in modo da poter disporre delle ultime versioni;
- abilitate le configurazioni di sicurezza, firewall e antivirus attivi;
- impostate una password forte su tablet, smartphone e computer. In questo modo, anche in caso di perdita, sarà più difficile, per uno sconosciuto, accedere alle vostre informazioni;
- crittografate i vostri dispositivi in modo da preservare i dati contenuti. Alcuni dispositivi, come l'iPhone, lo fanno già automaticamente quando configurate una password;
- eseguite un salvataggio completo dei dispositivi, in modo che se dovesse succeder loro qualcosa durante il viaggio, i vostri dati saranno comunque al sicuro.

Per aumentare la sicurezza durante un viaggio è necessario innanzitutto rendere sicuri i vostri dispositivi prima di partire, sia dal punto di vista fisico, sia facendo in modo di sapere dove si trovano in ogni momento, e, successivamente, proteggendo le attività online con la crittografia.

Dispositivi perduti o sottratti

Una volta iniziato il viaggio, assicuratevi della sicurezza fisica dei dispositivi: mai lasciarli in auto, alla portata dello sguardo di chiunque, poiché un criminale potrebbe facilmente rompere un finestrino e sottrarveli. Utilizzate un cavo di sicurezza (cable lock) per ancorare il laptop alla scrivania, al tavolo o a una superficie fissa. Il furto di un dispositivo costituisce un rischio, ma la sua perdita, secondo uno studio della durata di 10 anni effettuato da Verizon, ha una probabilità 15 volte superiore. Verificate sempre di avere tablet e smartphone sempre con voi quando viaggiate, ad esempio quando superate i controlli all'aeroporto, o lasciate un taxi o uscite da un ristorante, quando lasciate una camera d'albergo o prima di sbarcare da un aereo.

L'accesso Wi-Fi

Per connettervi a Internet durante un viaggio potreste ricorrere a un punto di accesso Wi-Fi pubblico, come quelli presenti in hotel, caffetterie o aeroporti. Il problema degli accessi pubblici non risiede solo nell'impossibilità di sapere come sono configurati, ma anche nella non conoscenza di chi vi si connette: essi devono essere considerati non affidabili per cui sarà necessario adottare ulteriori contromisure. Considerate inoltre che il collegamento Wi-Fi utilizza le onde radio per comunicare, per cui chiunque fisicamente vicino a voi potrebbe intercettare e monitorare le vostre comunicazioni.

Ecco perché in questi casi dovete assicurarvi che le vostre sessioni siano protette da crittografia. Ad esempio, quando vi collegate online con il browser, assicuratevi che i siti che visitate siano protetti (il loro URL inizierà con "https://"

Sicurezza in viaggio

e sarà presente l'immagine di un lucchetto chiuso). Potete utilizzare una VPN, cioè una Virtual Private Network, in modo da cifrare ogni vostra comunicazione online: nel caso non vi venga messa a disposizione dalla vostra azienda, potreste acquistare un servizio per uso personale. Se temete che non ci siano punti di accesso Wi-Fi affidabili, potete attivare le funzionalità di tethering o il router sul vostro smartphone, tenendo sempre presente che le tariffe di connessione dati internazionali potrebbero essere piuttosto costose.

Computer pubblici

Non usate mail computer pubblici, spesso presenti nelle hall degli hotel, in biblioteche o caffetterie. Non potendo sapere chi ha utilizzato il computer prima di voi, non potete essere certi che sia immune da virus e malware. Quando possibile, usate solo dispositivi sotto il vostro diretto controllo per ogni attività online. Nel caso doveste per forza usare un computer pubblico, non accedete a nessun servizio che richieda l'autenticazione con utente e password.

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

Programmi di gestione password:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_it.pdf
La verifica in due passaggi:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_it.pdf
La crittografia:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_it.pdf
Rendere sicuro il tablet:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_it.pdf

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