SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Maggio 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Sicurezza e divario generazionale

Introduzione

Molti di noi si sentono a proprio agio con la tecnologia e sanno come utilizzarla in modo sicuro. Altri componenti della famiglia, però, potrebbero non avere lo stesso approccio, specialmente se non sono cresciuti usando computer e Internet. Ecco alcuni accorgimenti che potrete adottare per diminuire il divario generazionale nella vostra famiglia. Parleremo inoltre di cosa fare per rendere sicura la tecnologia per i nostri figli, anche quando hanno a che fare con essa fuori dall'ambito famigliare.

L'autore di questo numero

Brian Honan (Twitter **@brianhonan**) è un consulente indipendente nell'ambito della sicurezza: con base a Dublino, Brian è fondatore e capo del primo CERT irlandese, è Special Advisor del Cybercrime Centre dell'Europol (EC3) e professore di Information Security all'University College di Dublino. É anche autore di diversi libri e articoli per varie pubblicazioni.

Le basi

Bastano pochi accorgimenti per rendere più sicura la vita digitale di chiunque: quelli che troverete di seguito sono raccomandazioni per ogni membro della vostra famiglia. Nel caso qualcuno non fosse in grado di comprendere queste indicazioni, vi raccomandiamo di aiutarlo a capirne il contenuto e i razionali.

- **Social Engineering**. Spiegate il concetto di social engineering in termini semplici e accessibili. Truffe e frodi esistono da migliaia di anni e questo tipo di attacchi si differenzia dagli altri solo per il tipo di strumento impiegato: Internet. Fate esempi delle truffe più comuni, come le email di phishing o la chiamata da un addetto del supporto tecnico. Spiegate che non bisogna mai dare la propria password ad altre persone o permettere l'accesso remoto al proprio computer. Infine, assicuratevi che nel caso abbiano un sospetto o delle perplessità su una mail o una telefonata ricevuta, vi possono chiamare prima di dare qualsiasi informazione a sconosciuti.
- **La rete Wi-Fi di casa**: fate in modo di rendere sicura la rete Wi-Fi della loro abitazione. Come minimo, assicuratevi di cambiare la password amministrativa, di impiegare una password forte per accedere alla rete e di utilizzare la crittografia più forte per le connessioni. Potreste anche valutare di utilizzare un servizio DNS sicuro, come www.opendns.org. Servizi come questo non solo impediscono di visitare siti infetti, ma possono darvi un controllo sui siti che possono essere visitati, fattore importante soprattutto per i bambini che usano Internet.

Sicurezza e divario generazionale

- **Patch**: mantenere i sistemi sempre aggiornati è uno degli accorgimenti fondamentali per migliorare la sicurezza, con qualsiasi tecnolgia. Per questo motivo, fate in modo che tutti i dispositivi in casa, ivi inclusi i dispositivi mobili come tablet e smartphone, e le applicazioni, siano impostati per aggiornarsi sistematicamente, laddove possibile.
- **Anti-Virus**: è molto facile cliccare e installare applicazioni che probabilmente non dovremmo avere. Sebbene gli anti-virus non fermino tutto il malware, aiutano comunque a bloccare le forme più comuni di attacco. Fate quindi in modo che tutti i computer di casa e i dispositivi mobili abbiano installato un anti-virus e che sia aggiornato sistematicamente.

Le vecchie generazioni potrebbero aver bisogno del vostro aiuto per mettere in sicurezza le moderne tecnologie in casa: questo costituirà la base per la creazione di un ambiente sicuro anche per i bambini.

- **Le passwords**: password forti sono fondamentali per proteggere dispositivi, applicazioni e account online. Spiegate ai vostri famigliari come creare password forti. Le passprase sono probabilmente più semplici da usare e ricordare. Un'altra buona idea è installare un password manager e spiegar loro come funziona. Se non è possibile, insegnate loro a scrivere le password e a conservarle in un luogo sicuro a cui solo loro potranno avere accesso. Per ogni account critico sarebbe poi opportuno impiegare la verifica in due passaggi.
- **Salvataggi**: quando tutto il resto non funziona, solo i salvataggi possono aiutarvi. Fate in modo che i membri della vostra famiglia abbiano un sistema di backup funzionante.

È opportuno che voi facciate un controllo di quando in quando per verificare che questi accorgimenti siano ancora validi e implementati. Nello scenario peggiore, installate un sistema di amministrazione remota su un dispositivo, facendo in modo di renderlo sicuro con la crittografia e una password forte e univoca.

Bambini in visita

Spesso, quando i più piccoli visitano i propri parenti, non è detto che trovino sui loro computer le stesse regole che voi avete stabilito a casa vostra per proteggere la navigazione. Ecco cosa potete fare.

Sicurezza e divario generazionale

- **Regole**. Assicuratevi che se avete stabilito delle regole per la sicurezza dei vostri figli, esse siano conosciute anche dai vostri parenti. Avete ad esempio stabilito regole sul tempo massimo di gioco online o su quando possono avere accesso ai loro dispositivi mobili? Non aspettatevi che i vostri figli spieghino queste regole ad altri membri della vostra famiglia. Potreste invece creare uno schema di regole e condividerlo con i parenti che i vostri figli visitano più frequentemente.
- **Controllo**. Se i vostri figli comprendono la tecnologia meglio dei loro guardiani, potrebbero trarne vantaggio. I ragazzi potrebbero chiedere o ottenere i diritti amministrativi del computer dei nonni e disporne a piacimento, visualizzando quei siti o installando quei giochi che voi avete proibito. Spiegate ai vostri parenti che non devono dare ai vostri figli nessun altro tipo di accesso oltre a quello che voi avete stabilito.

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

Social Engineering:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_it.pdf
La sicurezza della rete di casa:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201401_it.pdf
Le passphrases:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_it.pdf
Anti-Virus:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201412_it.pdf
Proteggere le attività online dei nostri figli:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201304_it.pdf

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