SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Novembre 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Acquisti online in sicurezza

Natale sta arrivando! Prepariamoci!

Natale si sta avvicinando e presto milioni di persone in tutto il mondo partiranno alla ricerca del regalo perfetto. Molti di noi sceglieranno di fare acquisti online approfittando dei prezzi convenienti ed evitando così lunghe file e negozi affollati. Sfortunatamente, questo è anche uno dei periodi preferiti dai criminali specializzati in frodi informatiche. Questo mese vi illustreremo i pericoli degli acquisti online e i modi per proteggervi al meglio.

L'autore di questo numero

Jonathan Homer (**@JonathanLHomer**) si occupa di Cyber Security Awareness nel settore pubblico e privato. Jon è specializzato nel coinvolgere il pubblico e nell'utilizzo di tecniche di formazione d'avanguardia.

Negozi online falsi

Sebbene la maggior parte dei negozi online sia legittima, ci sono purtroppo alcune eccezioni: si tratta di siti web falsi creati ad arte da criminali copiando il look di negozi molto conosciuti o usandone il nome allo scopo di ingannare chi va alla ricerca del miglior affare possibile. Quando cercate un'offerta vantaggiosa online potreste essere diretti a uno di questi siti.

Nel momento di scegliere un sito dove acquistare un prodotto, guardate con sospetto i siti che pubblicizzano prezzi esageratamente più bassi degli altri negozi online, così come quei siti che offrono prodotti che risultano essere esauriti in ogni altro posto. Per quale motivo questi prodotti sono così economici o disponibili? Perché si tratta di prodotti contraffatti, rubati o, in qualche caso, inesistenti: qualora li compraste, molto probabilmente non ricevereste nulla. Proteggetevi seguendo i seguenti consigli.

- Verificate che il sito abbia un indirizzo email legittimo e un numero di telefono di supporto. Se avete qualche sospetto, chiamate e parlate con un addetto
- Osservate eventuali errori di grammatica e ortografia
- Se un sito è l'esatta replica di un altro sito molto conosciuto che avete già usato in passato, ma l'indirizzo o il nome sono leggermente differenti, dovete agire con cautela. Un esempio: tutti conosciamo il servizio di Amazon che risponde all'indirizzo https://www.amazon.it. Cosa pensereste di un sito che si spaccia per Amazon e che ha indirizzo http://store-amazon.com?

Acquisti online in sicurezza

- Digitate il nome del negozio o l'URL in un motore di ricerca e leggete ciò che altre persone hanno detto in proposito. Cercate i termini "truffa" o "sito falso". Una mancanza di opinioni potrebbe non costituire un buon segno perché indica che il sito web è molto recente.

Ricordate: solo perché il sito sembra professionale, non significa che sia anche legittimo. Se qualcosa del sito vi fa suonare un campanello d'allarme, esaminatelo con attenzione. Se non vi sentite a vostro agio, non usatelo. Trovate invece un sito conosciuto di cui avete fiducia: anche se non farete gli affari che vi prometteva il sito falso, finirete con l'avere un prodotto reale, lecito e senza problemi per la vostra carta di credito.

Proteggiti acquistando online solo da siti di fiducia e con una reputazione consolidata.

Il computer e i dispositivi mobili

Oltre ad acquistare su siti web legittimi, dovete anche assicurarvi che il computer, il tablet e lo smartphone siano sicuri. I criminali informatici cercano di infettare i vostri dispositivi in modo da riuscire a raccogliere i dati del vostro conto in banca, della vostra carta di credito e le vostre password. Seguite i seguenti consigli per mantenere al sicuro il vostro dispositivo.

- Se avete bambini, usate un dispositivo dedicato a loro, diverso dal vostro. I bambini sono curiosi e molto interattivi con la tecnologia e, come conseguenza di questo, è più probabile che il loro dispositivo venga infettato. Utilizzando un computer o un tablet separato per le vostre operazioni di e-banking o di shopping online, ridurrete la probabilità di infezione. Se non è possibile adottare dispositivi diversi, usate account separati sullo stesso computer, assicurandovi che l'account dei vostri figli non abbia i privilegi di amministratore.
- Collegatevi solo a reti wireless che gestite personalmente, come la vostra rete di casa, o reti di cui avete fiducia quando dovete svolgere operazioni finanziarie. Utilizzare una delle wi-fi pubbliche sempre più diffuse è l'ideale per leggere le notizie, ma non per accedere al vostro conto corrente.
- Installate sempre gli ultimi aggiornamenti e verificate che anche il vostro anti-virus sia aggiornato, in modo da rendere più difficoltosa l'infezione del vostro dispositivo.

Le carte di credito

Esaminate sempre il rendiconto della carta di credito per individuare transazioni sospette: dovreste farlo regolarmente,

Acquisti online in sicurezza

almeno una volta al mese. Alcuni emettitori di carte offrono l'opzione di notificare via mail o SMS ogni transazione effettuata sul vostro conto o quando il vostro plafond mensile viene superato. Un'altra possibilità consiste nell'avere una carta di credito dedicata esclusivamente agli acquisi online, così che, nel caso venisse compromessa, potrete facilmente bloccarla o sostituirla senza aver conseguenze sulla vostra carta di credito principale. Se credete di essere stati oggetto di una frode, chiamate il gestore della vostra carta e spiegategli la situazione.

Esistono, infine, nuove tecnologie che permettono di effettuare un pagamento senza esporre i numeri di carta di credito, come ad esempio le carte di credito che generano un numero di carta unico per ogni acquisto online, oppure i servizi di pagamento online come PayPal, che non richiedono che comunichiate il vostro numero di carta al venditore.

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

Sicurezza in cinque punti:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201410_it.pdf
La sicurezza della rete di casa:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201401_it.pdf
Rendere sicuro il tablet:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_it.pdf

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