SANS SECURITY AWARENESS
ITALTEL
OUCH! | Novembre 2017
La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per tutti

OUCH!

IN QUESTO NUMERO...

Acquistare Online in sicurezza

Introduzione

Il periodo delle vacanze si sta avvicinando per molti di noi e presto milioni di persone in tutto il mondo si dedicheranno all'acquisto dei regali perfetti. Molti sceglieranno di acquistare online, alla ricerca di grandi occasioni, evitando lunghe code e folle impazienti. Sfortunatamente, questo è anche il periodo dell'anno nel quale molti cyber criminali creano negozi online fasulli per truffare e derubare. Qui sotto spieghiamo i rischi dello shopping online e come fare affari fantastici, in sicurezza.

L'autore di questo numero

Lenny Zeltser sviluppa prodotti di sicurezza al Minerva Labs ed insegna tecniche per contrastare i malware presso il SANS Institute. Lenny è attivo su Twitter come **@lennyzeltser** e gestisce un security blog su **zeltser.com**.

Negozi Online fasulli

Sebbene la maggior parte dei negozi online siano legittimi, esistono alcuni siti web fasulli creati dai criminali informatici. I criminali creano questi siti fasulli replicando l'aspetto dei siti reali o utilizzando i nomi di negozi o marchi famosi.
Questi criminali informatici utilizzano quindi siti web fraudolenti per derubare le persone che cercano le migliori condizioni d'acquisto sul web. Quando si cercano on-line i prezzi più bassi in assoluto, si possono trovare alcuni di questi siti fasulli.

Quando si visita un sito web, per fare un acquisto, bisogna diffidare di quelli che propongono prezzi decisamente inferiori rispetto agli altri siti online oppure di quei siti web che offrono prodotti che vengono venduti fuori dalla nazione. Il motivo per cui i loro prodotti sono così a buon mercato o disponibili è perchè quello che riceverete non è legittimo, i prodotti potrebbero essere contraffatti o rubati, inoltre in alcuni casi potrebbero non essere perfino consegnati. Per proteggersi bisogna seguire queste regole e consigli:

- Quando è possibile, acquistate da siti web che già conoscete, di vostra fiducia, con i quali avete già fatto acquisti in precedenza.
- Verificate che il sito abbia un indirizzo di posta elettronica legittimo ed un numero di telefono per le vendite o informazioni relative al supporto. Se il sito sembra sospetto, dovete chiamare e parlare con un interlocutore umano. Se non è possibile parlare con qualcuno, questo è il vostro primo segnale significativo che si tratta di un sito web falso.
- Cercate segnali di pericolo evidenti come offerte che sono, ovviamente, troppo belle per essere vere oppure con una scarsa grammatica e ortografia del testo.
- Siate molto sospettosi se un sito web sembra essere una replica esatta di un sito noto che avete già utilizzato

Acquistare Online in sicurezza

in passato, dove però il nome di dominio del sito web o il nome del negozio è un pò diverso. Ad esempio, se avete acquistato online da Amazon, il cui sito è https://www.amazon.com. dovete essere molto sospettosi se vi trovate in siti web simili, che fingono di essere Amazon con il sito web chiamato http://store-amazoncom.com.

- Scrivete il nome dello Store o digitate l'URL in un motore di ricerca e verificate quello che altre persone hanno detto in merito in passato. Se volete, potete inserire termini come "frode", "truffa", "mai più" o "falso". Una mancanza di recensioni può anche essere un segno che il sito è nuovo e potrebbe non essere affidabile.
- Prima di acquistare tutti i prodotti, assicuratevi che il collegamento al sito web sia crittografato. La maggior parte dei browser mostrano una connessione crittografata con un lucchetto e/o le lettere HTTPS verde alla sinistra prima del nome del sito.

Proteggiti acquistando solo su siti affidabili con una reputazione consolidata.

Ricordate, solo perché il sito sembra professionale non significa che sia anche legittimo. Se non si ha familiarità con un sito web, evitatene l'uso. Trovate invece un sito web noto di cui vi fidate o che avete usato in passato in sicurezza. Forse non farete affari incredibili, ma eviterete di trovare un prodotto probabilmente non legittimo e di essere derubati dei vostri dati personali e finanziari.

Computer e Dispositivi Mobili

Oltre a fare acquisti su siti web legittimi è necessario verificare che il vostro computer o dispositivo mobile siano sicuri. I criminali informatici cercheranno infatti di infettare i dispositivi in modo che possano raccogliere i vostri conti bancari, informazioni sulle carte di credito e le vostre password. Seguite i seguenti consigli per mantenere al sicuro i vostri dispositivi:

- Se avete dei bambini in casa, prendete in considerazione di avere due dispositivi: uno per i vostri bambini ed uno per gli adulti. I bambini sono curiosi e interagiscono con la tecnologia, di conseguenza è più probabile che possano infettare il proprio dispositivo. L'uso di un computer o un tablet dedicato solo per le transazioni online, come l'online banking e lo shopping, riduce la possibilità di essere "infettati".
- Installate sempre gli ultimi aggiornamenti ed eseguite l'upgrade del software antivirus. Questo accorgimento rende molto più complicato, per un criminale informatico, l'attacco volto ad infettare il vostro dispositivo.

Carte di Credito

Controllate con regolarità l'estratto conto, identificando addebiti sospetti, in particolare dopo aver utilizzato la carta di credito

Acquistare Online in sicurezza

per fare molti acquisti online o aver utilizzato un nuovo sito. Alcune carte di credito consentono la notifica via email o sms ogni qualvolta viene effettuato un addebito o quando quest'ultimo supera un certo importo. Un'alternativa è riservare una carta di credito solo per gli acquisti online, nel caso in cui venisse compromessa, puoi cambiarla facilmente senza impattare altre attività di pagamento. Se pensate di essere stati frodati, chiamate subito l'emittente della vostra carta di credito.
Di seguito è riportato un altro motivo per utilizzare le carte di credito per tutti gli acquisti online, evitando di utilizzare, quando possibile, le carte di debito. Le carte di debito infatti prelevano il denaro direttamente dal tuo conto corrente; se sei stato oggetto di una frode, può essere molto più difficile ottenere la restituzione del maltolto. Infine, è possibile utilizzare carte di credito che generano un nuovo numero di carta per ogni acquisto online, oppure le carte regalo o i noti servizi di pagamento online come Paypal, che non richiedono di rendere disponibile il numero della tua carta di credito al venditore.

PER SAPERNE DI PIU'

Iscriviti ad OUCH!, la newsletter mensile di sensibilizzazione alla sicurezza informatica, consulta gli archivi di OUCH! e approfondisci le soluzioni SANS per la sensibilizzazione alla sicurezza visitando il sito securingthehuman.sans.org/ouch/archives.

Versione Italiana

Italtel è una società multinazionale che progetta e realizza soluzioni e servizi di Information & Communication Technology basati su prodotti propri e di partner. Offre un ricco catalogo di servizi professionali di ingegneria, di servizi gestiti e soluzioni di Cybersecurity, collaboration, IoT, digitalizzazione delle reti e servizi di comunicazione.
Per maggiori informazioni www.italtel.com e seguici su Twitter (@Italtel)

Risorse

Ingegneria Sociale:	https://securingthehuman.sans.org/ouch/2017#january2017
Sicurezza in quattro punti:	https://securingthehuman.sans.org/ouch/2016#october2016
Proteggere la rete di casa:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS Security Consiglio del giorno:	https://www.sans.org/tip_of_the_day.php

Direzione Editoriale: Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley
Tradotto da: Italtel Solutions Business Unit - Cyber Security

