Spear phishing: truffa, non un passatempo

June 08, 2011

Introduzione

La svolta più recente nel phishing è lo spear phishing. Non si tratta di un passatempo o di uno scherzo, ma di una truffa vera e propria nella quale tu sei il bersaglio. Lo spear phishing è un'e-mail che sembra provenire da una persona o un'azienda che conosci. In realtà proviene dagli stessi hacker criminali che vogliono i dati della tua carta di credito e del tuo conto corrente bancario, le password e le informazioni finanziarie presenti sul tuo PC. In questo articolo viene spiegato come proteggersi da questi pericoli.

E-mail da un "amico"

Lo spear phisher basa le sue azioni sulla familiarità delle persone con molti aspetti della vita quotidiana. Egli conosce il tuo nome, l'indirizzo di e-mail e certamente qualche altra informazione. È probabile che i saluti nel messaggio che ti invia siano personalizzati: "Ciao Mario" invece di "Gentile Sig.". L'e-mail può fare riferimento a un "comune amico". Oppure a un recente acquisto online che hai fatto. Poiché le e-mail sembrano provenire da qualcuno che conosci, è plausibile che tu sia meno sospettoso e fornisca le informazioni che ti vengono chieste. Se poi è un'azienda che conosci che ti chiede di agire con urgenza, potresti essere tentato di obbedire senza riflettere.

Uso della tua presenza Web contro te stesso

Come si diventa il bersaglio di un spear phisher? Dalle informazioni che inserisci in Internet dal tuo PC o dal tuo smartphone. Ad esempio, costoro possono passare in rassegna i siti di social network, trovare la tua pagina, il tuo indirizzo di e-mail, l'elenco degli amici e un post recente in cui parli della tua nuova fotocamera che hai acquistato su un sito online. Utilizzando queste informazioni, uno spear phisher potrebbe spacciarsi per un amico, inviarti un'e-mail e chiederti la password per accedere alla pagina delle tue foto. Se rispondi con la password, il malintenzionato la proverà con tutte le variazioni possibili per cercare di accedere al tuo account sul sito di acquisti online che hai citato. Se riesce a scoprirla, la utilizzerà per addebitarti qualche acquisto poco simpatico. In alternativa, lo spear phisher può utilizzare le stesse informazioni per impersonare un addetto del rivenditore online e chiederti di reimpostare la password o di verificare il numero della tua carta di credito. Se rispondi alle sue richieste, il danno finanziario è fatto.

Tieni segrete le tue informazioni segrete

La sicurezza delle informazioni personali dipende in parte dalla tua capacità di essere prudente. Presta attenzione al tuo profilo online. Quante informazioni esistono su di te in circolazione che potrebbero essere sfruttate per indurti in inganno? Il tuo nome? L'indirizzo e-mail? Nomi degli amici? I loro indirizzi di e-mail? Sei presente, ad esempio, su quale popolare sito di social network? Dai un'occhiata ai tuoi post. C'è qualcosa che sarebbe meglio non venisse a conoscenza di un truffatore? Oppure, hai pubblicato qualcosa sulla pagina di un amico che potrebbe rivelare troppe informazioni?

Password efficaci

Pensa alle tue password. Ne utilizzi solo una o più variazioni della stessa facili da indovinare? Entrambi i casi non vanno bene perché rischi di rendere più facile a un truffatore l'accesso alle tue informazioni finanziarie. Ogni password per ogni sito che visiti deve essere diversa, molto diversa. La soluzione migliore è una combinazione casuale di lettere e numeri. Cambiale spesso. Il tuo software per la protezione in Internet e il sistema operativo possono aiutarti a tenere traccia delle tue password.

Patch, aggiornamenti e software per la sicurezza

Quando i produttori di software ti avvisano di aggiornare il tuo prodotto, fallo. La maggior parte degli aggiornamenti del sistema operativo e del browser comprendono patch della sicurezza. Il tuo nome e l'indirizzo di e-mail possono essere sufficienti per consentire a un hacker di introdursi attraverso un punto debole della sicurezza presente nel tuo sistema. Quasi superfluo aggiungere che devi essere protetto da software per la sicurezza in Internet e che questo deve essere sempre aggiornato.

Sii prudente

Se un "amico" ti invia e-mail e chiede una password o altre informazioni, telefonagli o rispondigli con un'e-mail separata per verificare che sia effettivamente lui che ti ha contattato. Lo stesso vale per banche e aziende. Prima di tutto, le aziende legittime non invieranno e-mail per chiedere password o numeri di conto. Se ritieni che l'e-mail possa essere autentica, contatta la banca o l'azienda e chiedi chiarimenti. Oppure visita il sito Web ufficiale. La maggior parte delle banche prevede un indirizzo di e-mail al quale puoi inoltrare e-mail sospette da verificare.

E ricorda sempre: non rivelare troppe informazioni personali online perché non puoi mai sapere chi potrebbe usarle contro di te. O come.

Articoli correlati

Regole da rispettare per le password
Marian Merritt offre 12 suggerimenti per creare delle password sicure.
Ulteriori informazioni

La sicurezza del tuo dispositivo mobile è una priorità
I dispositivi mobili sono strumenti fondamentali nel nostro stile di vita moderno, e lo stesso vale per la loro protezione.
Ulteriori informazioni

Visualizza tutti gli articoli

Risorse Norton

Aggiorna il tuo prodotto

Rinnovare il prodotto

Prodotti Norton

Ulteriori informazioni

Norton™ Internet Security2012

Norton™ Internet Security offre protezione avanzata per navigare, eseguire operazioni bancarie e acquisti online senza interruzioni.

Ulteriori informazioni