Dalla cybersecurity al phishing: l'era digitale porta con sé tanti vantaggi ma anche nuovi pericoli

23 Gennaio 2017

Il fenomeno degli hacker riguarda scenari di politica internazionale e lo spionaggio industriale, ma sappiamo bene che c'è un **rischio sicurezza anche per i device** (telefoni, tablet e computer) che usiamo **tutti i giorni come semplici utenti di beni e servizi**.

I rischi che corriamo non sono da poco, considerando che l'accesso da parte di malintenzionati ai nostri dati personali può portare alla **violazione della nostra privacy o a rischi concreti per il nostro patrimonio**.

Del resto, ognuno di noi accede quotidianamente a nuovi servizi (pensiamo a quante App scarichiamo ogni mese), mentre **tra i primi consigli di autodifesa ci sarebbe proprio quello di "ridurre la propria superficie di attacco"**, riducendo la nostra **presenza su tutte quelle piattaforme che non ci servono davvero** o che non usiamo da tempo, utilizzando **credenziali di accesso differenti per ciascun account**, cambiandole con una certa frequenza.

Inoltre, a rigore, dovremmo essere capaci di tenere separati i diversi ambienti digitali in base al loro "livello di rischio", **evitando quindi utilizzare lo stesso dispositivo sia per attività che comportino il trattamento di informazioni riservate, come home-banking, sia per scaricare film o musica.**

Ma a parte virus e malware c'è la possibilità di essere noi stessi a svelare password e credenziali, magari abboccando ai **tranelli del phishing**.

Ecco allora qualche consiglio:

- **Diffidate di qualunque e-mail che vi richieda l'inserimento di dati riservati** riguardanti codici di carte di pagamento, chiavi di accesso al servizio home banking o altre informazioni personali. La vostra banca non richiederà tali informazioni via e-mail.
- **E' possibile riconoscere le truffe via e-mail con qualche piccola attenzione**, generalmente queste e-mail non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici); fanno uso di toni intimidatori, ad esempio minacciano la sospensione dell'account in caso di mancata risposta da parte

dell’utente; non riportano una data di scadenza per l’invio delle informazioni.

- **Non cliccate sui link presenti in e-mail sospette**, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall’originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l’indirizzo corretto, non vi fidate: è possibile infatti per un hacker visualizzare nella barra degli indirizzi del vostro browser un indirizzo diverso da quello nel quale realmente vi trovate.
- **Diffidate inoltre di e-mail con indirizzi web molto lunghi**, contenenti caratteri inusuali. Quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l’indirizzo che compare nella barra degli indirizzi del browser comincia con ‘‘https://’’ e non con ‘‘http://’’ e nella parte in basso a destra della pagina è presente un lucchetto.

Per informazioni e assistenza vai sul nostro **sportello E-Commerce**

Autore: Massimiliano Dona
Data: 23 gennaio 2017