Dalla cybersecurity al phishing: come difenderci

16 Maggio 2022

Cybersecurity e phishing sono due termini che ormai tutti dobbiamo imparare a conoscere: se l'era digitale ha portato con sé tanti vantaggi, esistono infatti anche nuovi **pericoli** dai quali dobbiamo saperci difendere. Vediamo di cosa si tratta e come possiamo **evitare di cadere nella trappola.**

Focus sulla cybersecurity

ll fenomeno della **cybersecurity** e 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: occhio a privacy e patrimonio

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.**

I nostri consigli per difenderci

Ecco i nostri consigli per difenderci e proteggere i nostri dati e i nostri soldi:

- genera sempre **password diverse e complesse.**
- Evita qualsiasi **accesso a Wi-Fi pubbliche e connessioni gratuite.**
- **Aggiorna** regolarmente **software e sistemi operativi.**
- Attiva almeno sugli account dove sono salvati i dati più importanti l'**autenticazione a due fattori** (per es. richiesta della **password** e la richiesta di un **codice generato dal cellulare** dell'utente).
- **Diffida di qualunque e-mail che ti richieda l'inserimento di dati riservati** riguardanti codici di carte di pagamento, chiavi di accesso al servizio home banking o altre informazioni personali. La tua 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 cliccare 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 ti fidare: è possibile infatti per un hacker visualizzare nella barra degli indirizzi del tuo browser un indirizzo diverso da quello nel quale realmente ti trovi.
- Quando inserisci **dati riservati in una pagina web**, assicurati 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**.

HAI BISOGNO DEL NOSTRO AIUTO? CONTATTA I NOSTRI ESPERTI!

Autore: Sonia Galardo
Data: 15 maggio 2022