



Giovedì 24/03/2022

Attenzione alle truffe via e-mail

A cura di: AteneoWeb S.r.l.

Negli ultimi tempi stanno aumentando esponenzialmente episodi di cyber attacchi e/o truffe informatiche.

Lo scenario internazionale ha richiamato l'attenzione di molti al fenomeno dei cosiddetti hacker, ma molto più banalmente, i criminali informatici hanno spostato l'attenzione dalle infrastrutture alle persone, al punto che oltre il 99% dei cyber attacchi odierni si fondano sull'interazione umana.

Negli ultimi tempi infatti, anche sfruttando il massiccio impiego dello smart working, e il conseguente minore controllo esercitato dai sistemi di sicurezza attivati dalle aziende, sono aumentati gli attacchi indirizzati a utenti dei servizi di posta elettronica che spesso, invitati con l'inganno a cliccare su link dannosi o a inserire le loro credenziali, hanno inavvertitamente compromesso i propri dati (e quelli della loro azienda) a vantaggio dei cyber criminali.

È molto frequente, per esempio, l'utilizzo di esche email per attirare l'attenzione della potenziale vittima da truffare. Le email-esca vengono per lo più inviate da soggetti che si spacciano per un contatto fidato del destinatario, e sono di solito brevi e dirette: "Apri il file allegato", "Clicca su questo link".

Se il destinatario risponde assecondando la richiesta il danno è fatto!

È molto difficile, se non impossibile, azzerare il rischio di subire un attacco da parte hacker professionisti, ma è vero che nei casi più frequenti (ransomware o phishing) siano sufficienti anche semplici precauzioni personali per ridurre considerevolmente i pericoli:

- controllare sempre il mittente della mail; non solo il nome utente ma anche il dominio di posta elettronica;
- prima di cliccare su un qualunque link incorporato in una email, verificare che l'indirizzo mostrato sia davvero lo stesso indirizzo Internet al quale il link condurrà (per la verifica basta passare il mouse sopra il link stesso senza cliccare);
- usare solo connessioni sicure, in particolar modo quando si accede a siti sensibili. Come precauzione minima, si consiglia di non sfruttare connessioni sconosciute né tantomeno i wi-fi pubblici, senza una password di protezione;
- quando si accede a siti che contengono informazioni sensibili, come pagine per l'home banking, controllare che la connessione sia HTTPS e verificare il nome del dominio all'apertura di una pagina;
- non condividere mai i propri dati riservati con una terza parte.