Phishing: come difendersi

25 Novembre 2020

Con l'avvicinarsi del **Black Friday** sono purtroppo in aumento i casi di *phishing*. Di che si tratta e come difendersi?

Innanzitutto è bene sapere che il phishing è una **truffa**, una **frode informatica** ideata allo scopo di rubare i **dati personali**, come il numero di **carta di credito** o le chiavi di accesso al servizio di home banking. Il **phishing** viene attuato da truffatori che inviano **false e-mail apparentemente provenienti da una banca o da una società emittente di carte di credito.** Le e-mail utilizzano il **logo**, il nome e il layout tipico dell'azienda imitata, invitando il destinatario a collegarsi tramite un link ad un sito Internet del tutto simile a quello della banca e ad inserirvi, generalmente attraverso una finestra **pop-up** che si apre dallo stesso link, le informazioni riservate. Grazie ai dati ottenuti con l'inganno, il truffatore può effettuare transazioni bancarie a nome della vittima o sfruttare la sua carta di credito.

Ecco un esempio di email di **phishing:**
"Gentile utente, durante i regolari controlli sugli account non siamo stati in grado di verificare le Sue informazioni. In accordo con le regole di ... abbiamo bisogno di

*confermare le Sue reali informazioni. E' sufficiente che Lei completi il modulo che Le forniremo. Se ciò non dovesse avvenire saremo costretti a sospendere il suo accou*nt".

Cosa fare per proteggersi dal **phishing**?
• 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 minacciando 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.

Ricordiamo che per avere assistenza è possibile contattare i nostri consulenti attraverso lo **sportello Generico** sul nostro sito

Autore: Giuseppe Mermati
Data: 26 febbraio 2019
Aggiornamento: 25 novembre 2020