Il Phishing

Attenzione ai «pescatori» di dati personali

COS'É IL PHISHING

Il phishing è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

COME AVVIENE

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, assicurazione, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc.

COME SI RICONOSCE

In genere, i messaggi di phishing fanno leva su un'urgenza, sfruttando il pressing per indurre il ricevente a compiere un'azione immediata, come fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un form da compilare.
I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

Fonte: Garante per la protezione dei dati personali

ALCUNI CONSIGLI PRATICI

Dati, codici di accesso e password personali non dovrebbero mai essere comunicati a sconosciuti.
È bene ricordare che, in generale, banche, assicurazioni, enti pubblici, aziende e grandi catene di vendita non richiedono informazioni personali attraverso e-mail, sms, social media o chat.

1. Messaggio sospetto? Non cliccare

È buona regola non cliccare sui link contenuti in messaggi sospetti e non aprire eventuali allegati, che potrebbero contenere virus o programmi trojan horse capaci di prendere il controllo di pc e smartphone. Una piccola accortezza consigliata è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.

2. Occhio agli indizi

I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, assicurazioni, aziende ed enti.
Tuttavia, capita spesso che contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue. È utile anche prestare attenzione al mittente (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali).

3. Perché tutta questa urgenza?

Diffida dei messaggi intimidatori, che contengono minacce di chiusura di conti o contratti o addirittura di sanzioni, e di quelli che puntano a ricreare un contesto di emergenza, paura e urgenza (come "blocco pagamento").

4. Nessuna protezione? Il rischio aumenta

È utile installare e tenere aggiornato sul pc o sullo smartphone un programma antivirus che protegga anche dal phishing. Programmi e gestori di posta elettronica hanno spesso sistemi di protezione che indirizzano automaticamente nello spam la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni. Meglio non memorizzare dati personali e codici di accesso nei browser utilizzati per navigare online.
In ogni caso, è buona prassi impostare password alfanumeriche complesse, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato: banca online, e-mail, social network, ecc., a meno di disporre di sistemi di autenticazione forte (strong authentication).