

POSTE ITALIANE LANCIA ALLARME: NUOVA TRUFFA VIA SMS, ECCO COME DIFENDERSI

1 Ottobre 2019



L'AQUILA - Nuova truffa ai danni dei clienti di Poste Italiane.

Un sms chiede di cambiare per sicurezza ("Gentile Cliente, ci sono problemi sul tuo conto...") le credenziali del conto e di cliccare su un link, contenuto nello stesso sms, per farlo. Al link c'è una pagina web che finge di essere quella di Poste. Se l'utente fa login con i propri dati di accesso (nome utente, password, otp) ne subisce il furto.

I truffatori possono usare i dati per sottrarre denaro dal conto.

Poste Italiane sta diffondendo alcune raccomandazioni di difesa, alcune delle quali valgono contro ogni tipo di phishing bancario. Ecco cosa si può fare.

In generale, non rispondere ai messaggi di testo di persone che non si conoscono, né cliccare sui link;

Entrare nel sito di Poste digitandone direttamente l'indirizzo sul browser (è vero, i truffatori possono avere installato un malware che dirotta la nostra navigazione sul sito-truffa, ma non è così frequente e comunque non è il caso dell'ultimo attacco smishing);

Non divulgare il proprio numero di telefono sui social o altri canali, per ridurre il rischio che sia usato per mandare questi sms truffa; (i truffatori potrebbero anche riuscire a clonarlo, per intercettare l'sms otp di accesso al conto; la nuova Psd2 bandisce gli sms otp ma non tutte le banche si sono ancora adeguate);

Ricordarsi in generale che Poste, come le altre banche, non chiedono mai i dati di accesso; ne contattano il cliente via mail o sms per chiedergli di compiere azioni online di questo tipo (al solito si limitano a dare informazioni su cambi di contratto o sulla presenza di nuovi documenti online).

Nemmeno i corrieri o i negozi online possono mandare sms con link per scrivere le proprie credenziali (altro tipo di truffa in voga); mandano solo sms con il tracking del pacco;

Non installare mai app dai messaggi di testo (sms). Tutte le app installate sul dispositivo devono provenire direttamente dall'app store ufficiale. Questi programmi hanno procedure di test vigorose da eseguire prima di essere autorizzati sul mercato;

Assicurarsi che il sistema operativo del tuo telefono sia aggiornato. Android e iOS vengono costantemente aggiornati con funzionalità di sicurezza avanzate. Sui modelli Android e iPhone, la pagina delle impostazioni del telefono dovrebbe indicare quale sistema stai utilizzando e se è disponibile un aggiornamento.