Smishing, difendersi da SMS ed email sospette con i consigli di Poste Italiane

lunedì 28 ottobre 2019

Poste Italiane ha ricevuto numerose segnalazioni relative ad una delle truffe on-line più diffuse: lo Smishing. Che cos'è e come difendersi

In occasione delle nuove disposizioni introdotte dalla normativa PSD2 che – tra le altre novità – hanno eliminato il token per autorizzare le operazioni online, è opportuno richiamare l'attenzione dei consumatori su alcune basilari norme di sicurezza quando si effettuano operazioni online. Recentemente, Poste Italiane ha ricevuto numerose segnalazioni relative ad una delle truffe on-line più diffuse: lo Smishing. Cos'è lo smishing. Si tratta di un caso particolare di phishing. In questo caso, il link malevolo viene inviato attraverso messaggi SMS che sembrano provenire da mittenti ufficiali (come PosteInfo): nel testo del messaggio vengono chiesti dati riservati del cliente quali il nome utente, la password di accesso all'Internet Banking, gli estremi della carta o i codici OTP (One Time Password) ricevuti via SMS. Come proteggersi dalle truffe. È bene sottolineare invece che l'OTP è un codice che arriva tramite SMS solo ed esclusivamente nel caso in cui il cliente stia finalizzando un'operazione dispositiva sul proprio conto. Se il cliente non sta effettuando operazioni dispositive, l'SMS è sicuramente fraudolento. In caso di ricezione di email o SMS è bene tener presente queste semplici precauzioni: Non cliccare sui link contenuti nelle email, anche se apparentemente provenienti da indirizzi che potrebbero ricordare quello di Poste Italiane; se per errore dovesse accadere, NON autenticarsi su quest'ultimo, chiudere subito il web browser cestinando immediatamente l'email di phishing; Non seguire le richieste contenute in SMS che apparentemente provengono da PosteInfo che richiedano numero PAN o identificativo della carta, data di scadenza e CVV o codice di verifica carta o il codice dispositivo dell'Home-Banking generato dal Personal Card Reader (PCR); Non fornire a terzi alcuna credenziale e/o dati personali; Non dare per telefono alcuna informazione, quando non si può essere certi dell'identità dell'interlocutore: molti truffatori si fingono operatori di Poste Italiane. Fare attenzione al numero chiamante: potrebbe sembrare il vero numero di Poste Italiane. Spesso, infatti, i frodatori riescono a mascherarlo e a nascondere il proprio. Poste Italiane, infatti, non richiede mai ai clienti i dati riservati delle carte di pagamento e non manda e-mail /SMS con messaggi allarmanti su blocco di conti o carte, su pagamenti insoluti o su addebiti inaspettati.

Fonte: HelpConsumatori