La Polizia postale informa: attenzione alle truffe tramite spoofing

La Polizia postale ha diramato un avviso a seguito di molte segnalazioni ricevute riguardanti dei tentativi di truffa attraverso la tecnica dello “Spoofing telefonico”.

I truffatori, utilizzando la tecnologia Voip (Voice over internet protocol) o un telefono Ip con Voip, che trasmette le chiamate sulla rete internet, telefonano nascondendosi dietro a dei reali numeri di telefono. Chi riceve la telefonata vede un numero o un nome sul display, che a volte è appartenente ad un reale contatto della rubrica o che è conosciuto perché magari è un numero usato dalla Banca o da Poste per comunicazioni di servizio.

Di recente sta capitando che ad essere replicati siano i numeri telefonici degli uffici della Polizia postale. L’utente viene in questo modo contattato da un falso operatore della Polizia, che riferisce di aver riscontrato un non meglio precisato “attacco informatico” ai danni del conto corrente del malcapitato e preannuncia l’invio di un Sms, al cui interno è presente un link, sul quale cliccare per ricevere le istruzioni necessarie a mettere in sicurezza i propri risparmi.

Per guadagnare ancor più la fiducia del malcapitato, il truffatore lo invita a verificare su Internet la corrispondenza del numero chiamante con quello dell’ufficio della Polizia postale presente in Rete. La vittima, verificata la corrispondenza del numero e confidando nella veridicità della chiamata, esegue le movimentazioni di denaro, perdendone la disponibilità, ignara di essere caduta in una truffa.

In altri casi la vittima viene prima contattata tramite un messaggio Sms, apparentemente proveniente dal numero dell’istituto di credito presso cui ha il proprio conto, e che proprio per questo si accoda alle notifiche già effettivamente ricevute dalla banca, rendendo la comunicazione credibile. Questo messaggio avvisa l’utente di un probabile accesso abusivo al conto, da cui sarebbero in corso dei prelievi non autorizzati.

Sono giunte segnalazioni anche di sms inviati da un falso numero, solo in apparenza riconducibile a Poste Italiane, ad esempio con mittente “PosteInfo”, con cui l’utente viene informato di connessioni anomale al proprio conto e viene invitato a cliccare su un link. Il link apre, in genere, “pagine clone” di Poste Italiane o del proprio istituto di credito, inducendo in errore la vittima, che spesso fornisce le proprie credenziali.

Successivamente, giungono anche delle chiamate, sempre attraverso numeri oggetto di spoofing, da parte di ipotetici “operatori antifrode”, per convincere l’utente ad eseguire le operazioni dispositive dal proprio conto, come effettuare direttamente un bonifico su un conto diverso, in modo da “mettere al sicuro i propri risparmi”. Succede persino che, se l’utente non si lascia facilmente convincere, il truffatore prospetti una successiva chiamata da parte della Polizia postale, che confermerà l’attacco al proprio conto e suggerirà di effettuare le operazioni di trasferimento del denaro su un conto “sicuro”, diverso da quello della vittima, la quale, presa dal panico, finisce per cadere nel tranello e segue le indicazioni fornite dal truffatore.

Fate attenzione e in caso di dubbio contattate la vostra banca, la filiale di Poste dove avete il conto o direttamente la Polizia di Stato al numero di emergenza 113 o NUE 1-1-2. Se vi rendete conto che è in atto un tentativo di truffa potete segnalarlo sul sito www.commissariatodips.it.

Sergio Foffo

09/11/2023