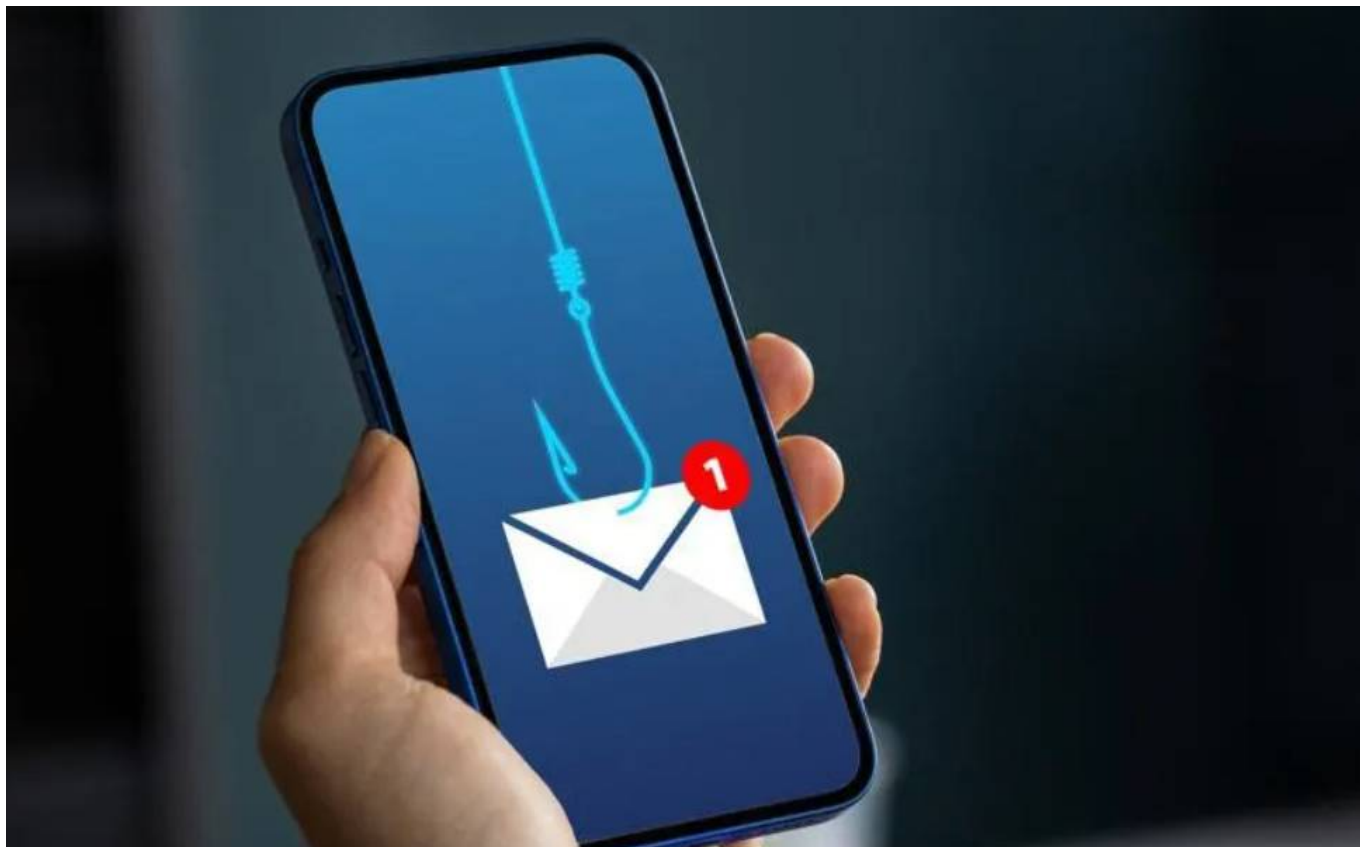


TRUFFE ON LINE: POLIZIA POSTALE L'AQUILA SVENTA TENTATIVI DI SMISHING E VISHING

28 Marzo 2024



L'AQUILA – Nelle ultime settimane, in Abruzzo, gli investigatori della Polizia di Stato, appartenenti alla Sezione operativa della sicurezza cibernetica della Polizia postale dell'Aquila hanno sventato due tentativi di truffa online, consentendo di evitare la perdita di considerevoli importi.

I truffatori hanno utilizzato le tecniche dello smishing e del vishing, rispettivamente volte a carpire illegalmente dati finanziari e sensibili delle vittime inducendole a cliccare su un link allegato ad un messaggio e attraverso una telefonata.

LA NOTA

Più in particolare, nello smishing, i messaggi sms – che avvisano di presunti accessi non autorizzati o movimenti sospetti sul conto – sono provenienti da mittenti apparentemente attendibili (banca, poste o istituto di credito delle possibili vittime), spesso con allegato un link che reindirizza ad un sito “clone”, del tutto simile a quell' ufficiale, dove però i dati inseriti vengono carpiri illegalmente dai malfattori.

Nel vishing (che può anche essere abbinato allo smishing) invece, i truffatori – che si presentano come dipendenti dell'istituto di credito o appartenenti alla Polizia Postale o ad altre forze dell'ordine – contattano le vittime per avvisarle di movimenti sospetti o accessi abusivi al conto corrente ed esortarle a spostare velocemente quanto depositato su un conto definito “sicuro” con la promessa che successivamente il denaro gli verrà restituito mediante bonifico.

In tutti questi casi, l'utente è spesso tratto in inganno dal fatto che il numero di telefono da cui proviene la chiamata o il messaggio è effettivamente corrispondente a quello della banca o dell'ufficio di Polizia presente sul territorio. Ciò avviene attraverso il cd. “Spoofing”: una tecnica che consente di inviare SMS ed effettuare telefonate di tipo VoIP (Voice over Internet Protocol), mediante personal computer e altri dispositivi informatici, potendo scegliere liberamente il numero di

telefono che apparirà sul display del dispositivo ricevente.

In uno dei casi segnalati, alla vittima è giunta la telefonata di un presunto operatore della Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale aquilana, qualificatosi come “Commissario Rizzo”. Solo l’interruzione improvvisa della telefonata faceva sì che l’utente contattasse direttamente la Polizia Postale per poter riprendere interlocazione con il presunto ufficiale e scoprisse l’inganno, sporgendo immediatamente denuncia e consentendo il tempestivo intervento degli operatori.

La Polizia di Stato ricorda che banche, poste o istituti di credito non utilizzano mai SMS, mail o telefonate per richiedere ai clienti dati personali, credenziali di accesso o informazioni urgenti. In caso di dubbi su presunti movimenti sul proprio conto, contattare direttamente l’istituto di credito.

Allo stesso modo, in nessun caso bisogna cliccare su link allegati a messaggi o e-mail, anche se apparentemente provenienti da mittenti attendibili, ma in caso accedere ai servizi attraverso app scaricate dalle piattaforme ufficiali o siti Internet raggiunti digitando le url direttamente sulle barre di indirizzo del proprio browser.