AbruzzoWeb
Tutte le notizie d'Abruzzo a portata di click

TRUFFE INFORMATICHE: 8MILA EURO SOTTRATTI DA CONTO DONNA PESCARESE, INDAGINI SU PREGIUDICATO 50ENNE

23 Maggio 2022



PESCARA – La Polizia di Stato ha sventato una frode informatica recuperando ben 8.000 euro sottratti dal conto corrente di una donna. Le indagini, coordinate dalla Procura de L'Aquila, si stanno concentrando nei confronti di un uomo del napoletano, un cinquantenne con precedenti specifici.

La vittima, una cittadina pescarese, dopo aver ricevuto un messaggio SMS apparentemente proveniente da un noto Istituto di credito con cui venivano riferite anomalie al proprio conto corrente, veniva tratta in inganno e indotta ad aderire alle indicazioni contenute nel messaggio: cliccare su un link che riconduceva ad una pagina web del tutto simile a quella del proprio istituto di credito. A quel punto veniva invitata a digitare i dati del proprio conto/carta.

Subito dopo, veniva anche contattata telefonicamente da una persona che, presentandosi come un operatore dell'Istituto di Credito, la induceva a comunicare un codice che nel frattempo era pervenuto sul proprio cellulare.

Solo dopo qualche minuto, nell'accedere – online – al proprio conto, l'utente si avvedeva che era stata appena effettuata a sua insaputa un'operazione di bonifico online dell'importo di € 8.000,00.

Non riuscendo in alcun modo ad annullare l'operazione, la titolare del conto si rivolgeva alla Polizia Postale di Pescara, ove gli operatori della Sezione Financial Cybercrime riuscivano a far bloccare immediatamente il conto beneficiario del bonifico per poter poi restituire la somma alla malcapitata.

La Polizia Postale e delle Comunicazioni informa che sono in continuo aumento questo tipo di raggiri, comunemente noti con noti con il termine di "Vishing" (dall'inglese voice-phishing o phishing vocale).

La vittima di tali frodi viene contattata telefonicamente da finti operatori bancari o di società emittenti carte di credito, i quali riferendo di presunte "anomalie" nella gestione della carta di credito o del conto corrente, avvisano la persona che, nel suo stesso interesse, è necessario attivare fantomatiche "procedure di sicurezza".

I truffatori richiedono quindi alla vittima di leggere a voce alta il "codice di conferma" che, proprio in quel momento, appare via messaggio sul display del telefono.

Tale codice, tuttavia, altro non è che il codice autorizzativo di una transazione che in quel momento i truffatori stanno tentando di effettuare via web ai danni dell'ignara vittima.
I cyber-criminali infatti, entrati precedentemente in possesso dei dati della carta di credito (numero di carta, data di scadenza e CVV), necessitano di conoscere tale codice di sicurezza per completare una transazione in corso, e sottrarre così il denaro della vittima.

Questa, credendo in buona fede di aver agito correttamente per mettere in sicurezza il proprio conto o la propria carta di pagamento, si accorge solo successivamente (spesso, al momento della ricezione dell'estratto-conto) che vi sono in realtà movimentazioni in uscita non autorizzate, pari anche a diverse migliaia di euro, per l'acquisto di beni e servizi mai richiesti su piattaforme online.
Si sottolinea ancora una volta l'importanza di non rivelare mai a nessuno, via telefono come via social o via email, i nostri dati più sensibili, le nostre password dispositive, i PIN o i nostri codici di accesso comunque denominati.

È opportuno diffidare sempre di fronte a soggetti che richiedono tali dati, presentandosi come operatori di istituzioni pubbliche, importanti aziende o istituti bancari. Utile invece procedere a semplici ed attente verifiche, contattando direttamente l'ente coinvolto che potrà confermare i nostri sospetti.

© 2026 Abruzzo Web Enfasi srl - Quotidiano digitale registrato presso il Tribunale dell'Aquila con decreto n°501 del 2 settembre 2003
Iscrizione al ROC n. 26362 - P.IVA 01812420667
Direttore responsabile Berardo Santilli