

Sms truffa ai clienti Unicredit: i consigli della banca per evitare di farsi svuotare il conto

di **Redazione**

06 Luglio 2021 - 8:05



Genova. In questi ultimi giorni sono tantissime le persone che sono state raggiunte da un **sms truffaldino** che, annunciando il blocco del **conto bancario**, chiede dati personali per risolvere la situazione, ma di fatto ruba gli accessi per accedere al denaro. Dopo l'allarme lanciato nelle scorse ore, **Unicredit**, l'istituto di credito i cui clienti sono stati messi nel mirino, risponde con nuovi consigli e procedure di sicurezza. Ecco il dettaglio

Primo passo: riconoscere se un SMS è inviato da UniCredit

Può capitare di ricevere SMS ben congegnati ed ingannevoli attraverso i quali malintenzionati del web potrebbero indurti a condividere dati personali, credenziali e informazioni sensibili. In questo caso si parla di "smishing". Riconoscere le comunicazioni di UniCredit può salvarti da questo tipo di frodi.

Negli SMS contenenti un link:

non è previsto MAI il collegamento alla pagina di accesso alla Banca Multicanale;
è presente sempre il tuo nome nell'intestazione;
è indicata la tua Filiale di riferimento con le specifiche della città e dell'indirizzo;
il link sarà così composto: <https://unicred.it/nomeprodotto> e ti consentirà di conoscere i nostri prodotti/servizi.

Negli SMS senza link:

se è presente un numero telefonico da contattare per informazioni, ricorda che non ti verranno mai richiesti dall'operatore password dispositivi (generata da Mobile Token, Unicredit Pass o inviata tramite sms) e/o di accesso al servizio di Banca Multicanale, il PIN della carta e/o il codice di sicurezza di tre cifre riportato sul retro della carta (cvc2/cvv2). Ricorda: non ti verranno mai richiesti da UniCredit dati personali, password di accesso alla tua Banca Via Internet, numeri delle tue carte o dei tuoi conti correnti. Diffida da qualsiasi SMS che non sia in linea con queste caratteristiche.

Com riconoscere un contatto telefonico truffaldino

Una truffa che avviene tramite telefono è detta “vishing” e ha lo scopo di carpire informazioni personali e riservate come dati di accesso al servizio di Banca Multicanale, la password dispositiva, numeri di carte di credito/di debito/prepagate o il PIN ad esse collegato per poi effettuare delle operazioni fraudolente (ad esempio ricariche, bonifici, acquisti internet).

Alcuni comportamenti messi in atto dal truffatore:

contatta telefonicamente la vittima, fingendo di essere del Servizio Clienti della Banca, della Filiale o dell'ufficio Antifrode; prova a stabilire un rapporto di fiducia dimostrando di essere a conoscenza di alcuni dati bancari, al fine di indurre il malcapitato a credere che la chiamata provenga dalla propria Banca; fa riferimento a movimenti sospetti relativi al conto o alla carta, problemi di accesso al servizio di Banca Multicanale o tentativi di accesso da parte di terzi; chiede i dati di accesso al servizio di Banca Multicanale, la password dispositiva (generata da Mobile Token, Unicredit Pass o inviata tramite sms), numeri di carte di credito/di debito/prepagate o il PIN ad esse collegato.

Ricorda: UniCredit non ti contatterà mai per chiederti password dispositive e/o di accesso al servizio di Banca Multicanale, il PIN della carta e/o il codice di sicurezza di tre cifre riportato sul retro della carta. Tutela la riservatezza dei dati bancari e personali e diffida da qualsiasi contatto telefonico che abbia queste caratteristiche.

Ricevere le notifiche Sms per una maggiore sicurezza

Puoi ricevere gratuitamente SMS contenenti informazioni e comunicazioni della tua Banca relative a disposizioni eseguite su Banca Multicanale o attraverso l'utilizzo di carta di debito e carta di credito meritevoli di attenzione per importanza, caratteristiche o atipicità, da parte dei nostri sistemi di monitoraggio delle transazioni per permetterti la verifica della correttezza dei dati del pagamento inserito. **Ricorda: mantieni aggiornati i tuoi dati personali per essere sempre in contatto con la tua Banca.**

SEGNALAZIONI DI SICUREZZA

Per segnalare eventuali situazioni dubbie o sospette eventualmente legate a fenomeni fraudolenti e per qualsiasi domanda, reclamo, richiesta, supporto e comunicazione di anomalie e incidenti riguardanti i pagamenti via internet e relativi servizi sono a tua disposizione i contatti, o il Numero Verde gratuito 800.57.57.57, dal lunedì al venerdì dalle 8.00 alle 22.00 e il sabato dalle 8.00 alle 14.00.

PER ULTERIORI APPROFONDIMENTI

Nell'ambiente di Banca via Internet al percorso Impostazioni > Sicurezza > Sicurezza Online.

Chiamando il Servizio Clienti al Numero Verde gratuito 800.57.57.57, dal lunedì al venerdì dalle 8.00 alle 22.00 e il sabato dalle 9.00 alle 14.00.