Blocco del conto causa Covid-19, attenzione allo smishing che ruba i vostri dati

Arriva un sms nel quale il servizio clienti di un presunto istituto bancario ci chiede di cambiare le nostre credenziali di accesso tramite un link ad una pagina web di login, identica a quella della banca, attraverso una connessione criptata, che quindi sembra sicura.

Il messaggio, apparentemente inviato dalla banca, è simile al seguente: ”a causa del virus COVID 19 nuove restrizioni determinano il blocco del conto si prega di sbloccarlo tramite link https://securexxxxx.com con l’inserimento dell’acronimo dell’istituto bancario”.

Attenzione, è altamente probabile che si tratti di smishing, sistema usato dai cybercriminali per carpire dati sensibili relativi all’accesso da remoto ai conti correnti bancari. Il termine deriva dall'unione delle parole sms e phishing, dove l'ultimo termine indica la "pesca" dei dati.

La trappola scatta quando gli utenti, dopo aver cliccato sui link, approdano su siti web accuratamente artefatti che chiedono l'inserimento di dati personali.

La truffa in questo momento sta sfruttando l’emergenza Coronavirus per indurre le persone a cadere nel raggiro. Ma un cittadino che aveva ricevuto il messaggio si è insospettito per la richiesta anomala e ha avvisato la Polizia postale e delle comunicazioni.

Gli investigatori della Postale hanno immediatamente attivato le verifiche del caso, accertando che si trattava di un sito fake.

Vi ricordiamo che nessun istituto bancario invita i propri clienti attraverso mail, Sms, telefono o messaggi sui Social, a fornire password, dati delle carte, codici Otp, Pin, credenziali, chiavi di accesso all'home banking o altri codici personali.

Vi raccomandiamo quindi di verificare sempre eventuali messaggi di questo genere con le vostre banche prima di inviare i dati di accesso, e, in caso di sospetti, di fare una segnalazione alla Polizia postale.

Sergio Foffo

27/03/2020