Le truffe tramite phishing e smishing: due esche pericolose

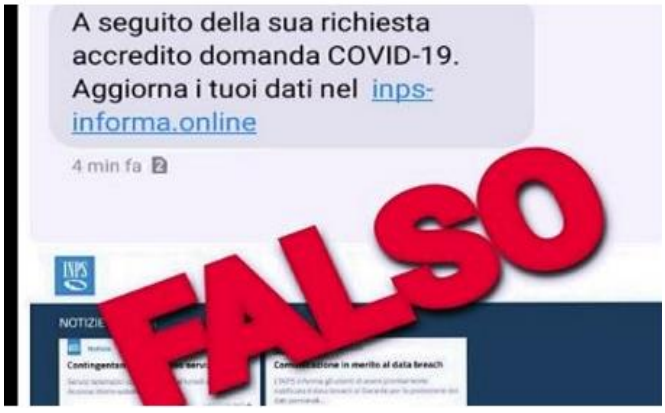
Il Coronavirus rende fragili e preoccupati ed è l'argomento più ricercato e letto di questo periodo. Questo alimenta il numero di truffatori che approfittano della nostra vulnerabilità per lanciare campagne di ***phishing e di smishing.***

Di cosa si tratta: le prime prevedono l'invio massiccio di e-mail esca, mentre con lo smishing (acronimo di SMS phishing) vengono inviati messaggi di testo con un tono urgente per richiedere informazioni riservate all'utente.

Rispetto agli spam che spesso riceviamo nelle e-mail, lo smishing usa i messaggi di testo sui telefonini per attirare le vittime nella trappola ed estorcere dati personali, numeri di carte di credito e altri dati riservati.

Spiega la Polizia Postale che nelle ultime varianti di smishing, inoltre, i criminali hacker hanno scoperto il modo di usare versioni modificate di normali applicazioni scaricabili dai vari app store per installare sullo smartphone della vittima un software malevolo in grado di simulare la ricezione di un messaggio SMS. In particolare, su Android viene sfruttata una vulnerabilità conosciuta con il nome di "write-sms" che comunque è stata corretta con gli ultimi rilasci del sistema operativo mobile di Google.

Caso del falso messaggio INPS



La Polizia Postale avverte che "...in questi giorni dei cybertruffatori stanno facendo un massiccio invio di sms che contengono un falso messaggio dell'Inps simile al seguente: "***A seguito della sua richiesta accredito domanda COVID-19. Aggiorna i tuoi dati nel inps-ixxxxx.online***".

Cliccando sul link contenuto nel messaggio viene scaricato un file Apk (Application package) all'interno del quale si nasconde un malware che, installato sul cellulare, permette ai criminali di accedere al dispositivo ottenendone il controllo e di impossessarsi dei dati sensibili.

Ed ecco che password, dati delle carte, codici Otp, Pin, credenziali, chiavi di accesso all'home banking o altri codici personali entrano a far parte della banca dati dei truffatori del web. E' questo il fenomeno dello smishing.

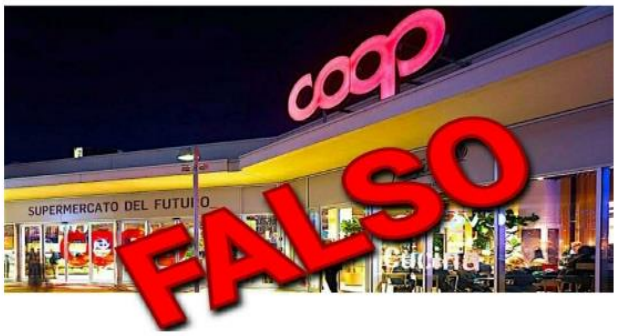
Ricorda quindi la Polizia di Stato di fare sempre molta attenzione. Verificate le informazioni sul sito ufficiale dell'ente che invia il messaggio, evitando di utilizzare il link contenuto ma digitandone il nome direttamente sulla barra degli indirizzi (Url).

Loredana Masseria per *Fake news e Coronavirus*
Loredana.masseria@aslcittaditorino.it

L'invito è di segnalare i casi sospetti tramite sito della Polizia postale.

I casi Coop, Nike e Adidas

La Polizia Postale ha individuato nuove truffe. Si tratta di una serie di messaggi pubblicitari truffaldini che riguardano:



La Coop. Attenzione a messaggi di questo genere: *"Coop sta distribuendo generi alimentari gratuiti del valore di 250 euro per sostenere la nazione durante la pandemia di Corona. Sbrigati! Raccogli il tuo voucher GRATUITO qui: http://xxxxxxxxxxxxxx".*

E' una truffa: si invitano i cittadini a cliccare su un falso sito internet della società Coop e ad inserire i propri dati anagrafici per garantirsi un voucher gratuito.

La società Coop, che ha presentato denuncia alla Polizia postale di Bologna, ha disconosciuto tale attività truffaldina e raccomanda a tutti i consumatori di consultare esclusivamente il proprio sito www.e-coop.it.

La stesso tipo di truffa ha riguardato Adidas che in messaggio avrebbe promesso 5000 paia di scarpe in regalo cliccando un link in occasione di un falso 80° compleanno della società dell'abbigliamento sportivo.

E anche attraverso il nome della Nike è stata commessa la stessa truffa.

L'invito della Polizia Postale è di diffidare da questi e da simili messaggi, evitando accuratamente di aprire gli allegati che essi contengono.
Per richiedere ulteriori informazioni, potrete utilizzare il servizio che la Polizia di Stato mette a disposizione, raggiungibile all'indirizzo www.commissariatodips.it .

Loredana Masseria per *Fake news e Coronavirus*
Loredana.masseria@aslcittaditorino.it