Le nuove truffe sui supermercati: come difendersi

22 Marzo 2021

A tutto smishing: sempre di più, gli hacker colpiscono tramite WhatsApp.

La messaggistica istantanea sta diventando lo strumento preferito dei criminali informatici per adescare ignari utenti e, purtroppo, spesso il tranello riesce.

Nell'ultimo periodo, le truffe telefoniche e informatiche si sono moltiplicate. Ma se, fino a non molto tempo fa, strumento privilegiato del *phishing* era l'email con un link malevolo, ora gli hacker prediligono WhatsApp.

Il fenomeno ha ultimamente preso il nome di *smishing*, ma il meccanismo è esattamente quello del *phishing*: l'invio di un messaggio per far cliccare su un link il destinatario, allo scopo di sottrargli dati preziosi, come password e credenziali di accesso al suo conto corrente.

Indice

Le ultime due truffe

Spesso, *phishing* e *smishing* riescono grazie al fatto di «vestire» le comunicazioni di una patina di ufficialità. Si fa credere che la mail o il messaggio provengano, ad esempio, da un istituto di credito, da un ente, da una società molto conosciuta.

Ma questi soggetti vengono sfruttati dai criminali informatici, a loro insaputa e loro malgrado, come «cavalli di Troia»: gli hacker se ne servono, fingendo che siano loro i mittenti, quando invece non sono coinvolti in alcun modo.

Le ultime due truffe di questo tipo hanno interessato Coop ed Esselunga, nel senso appena descritto: i malintenzionati si sono spacciati per i due supermercati in modo da far pensare all'utente che la comunicazione venisse da loro, o comunque riguardasse iniziative di queste due catene di negozi.

Ovviamente, non era così: Coop ed Esselunga erano all'oscuro di tutto e hanno subìto il raggiro in qualità di vittime, allo stesso modo di chi ci è caduto.

Il raggiro a danno di Coop e degli utenti

Nel caso del Coop, gli hacker hanno inviato messaggi in cui comunicavano agli utenti che l'azienda compiva sessant'anni il 22 marzo 2021 (in realtà, ne ha appena compiuti 54). In occasione di questa – finta – ricorrenza venivano messi in palio dei regali, sotto forma di buoni da spendere al supermercato. Per partecipare, però, bisogna rispondere alle domande di un questionario, cui accedere attraverso un link inviato via WhatsApp.

Vengono chiesti anche dati riguardanti la propria carta di credito, perché la reale intenzione dei criminali informatici è quella di accedere al conto dell'utente.

Il raggiro a danno di Esselunga e degli utenti

Anche nel caso dell'altra truffa è stato usato un anniversario come pretesto: il 70esimo dalla nascita di Esselunga (che invece ha 64 anni).

Il messaggio sembra arrivare da un amico o da un parente, comunque da un contatto sulla rubrica del proprio cellulare; informa di una specie di lotteria organizzata dalla catena di supermercati, o almeno così sostiene il messaggio.

L'immancabile link per partecipare non rinvia al sito ufficiale di Esselunga, ma a un'altra pagina e sull'url, ossia sull'indirizzo identificativo del sito compaiono stringhe anomale come le seguenti: «447814.yz», «icpkwey.asia», «c12081.top» e simili.

Il sito dice che ci sono settemila regali in palio, ma si può partecipare solo se si invia lo stesso messaggio ai propri amici e se si compila un'altra specie di questionario. Sempre allo scopo di rubare dati.

Come proteggersi

Mai cliccare su questo tipo di link. Quando si ricevono messaggi come questi ci si può facilmente accertare della veridicità dei contenuti. In tal caso, basta controllare le

date di nascita di Esselunga e Coop che, infatti, non corrispondono a quelle degli anniversari citati, come accaduto in passato, quando i truffatori hanno tirato in ballo Amazon per ordire il loro ennesimo raggiro (per approfondire leggi qui: Finti buoni e regali Amazon: nuova truffa su WhatsApp).

È sempre sconsigliabile inserire dati anagrafici e numeri di carte di credito online, a meno che non ci si trovi su piattaforme ufficiali di e-commerce o sul portale della propria banca, siti rodati e consultati abitualmente. Ma bisogna essere certi di trovarsi sul portale giusto e non su una sua copia fake, creata ad arte per sottrarre password o altri dati.

Per accertarsi di questo, viene in aiuto l'url del sito, cioè a come è fatto l'indirizzo: stringhe anomale, composte da sequenze casuali di lettere e numeri, come quelle citate poco fa, sono la spia di una piattaforma non affidabile. Dunque, è bene non rispondere ad alcuna richiesta di informazioni perché è quasi certo che si tratti di una truffa.

Se invece si è già cliccato sul link e le informazioni richieste, ormai, sono state fornite è bene bloccare la propria carta e sporgere denuncia alle forze dell'ordine.

(da www.laleggepertutti.it)