Lo Smishing. Cos'è e come difendersi?

Lo **Smishing** è un nuovo tipo di truffa che si sta diffondendo molto in questo 2019. La parola "Smishing" sta per **SMS Phishing,** vale a dire un messaggio (SMS) con all'interno un tentativo di truffa. Con l'evolversi della tecnologia tantissimi utenti, ignari della trappola, possono al giorno d'oggi imbattersi in questa nuova frontiera delle truffe.

Attenzione allo Smishing

Ma come funziona questa nuova frontiera di truffe? Cosi come avviene per il **phishing**, **viene inviato un messaggio** con un tono "urgente" all'ignaro utente. All'interno di questo messaggio viene richiesto di fare una particolare azione. E quasi sempre quest'azione richiesta è quella di fare click verso un link esterno o di chiamare un numero di telefono. Viene chiesto all'utente di fornire informazioni private come le password o informazioni della carta di credito. Non cliccare sul link o chiamare il numero di telefono.

Differenza tra Phishing e Smishing

Quando i cybercriminali fanno **phishing**, inviano e-mail fraudolente che cercano di ingannare il destinatario inducendolo a far aprire un allegato pieno di malware o ad aprire un link dannoso. Lo steso avviene per lo **smishing**, che semplicemente usa gli SMS al posto delle e-mail. Per farla molto semplice e comprensibile a tutti.
Ed in genere il contenuto del messaggio, seppur in maniera ridotta rispetto alla mail, è sempre quello.

Come proteggersi dagli attacchi: i consigli dell'Associazione Noi Vittime Del Consumo

Ecco alcuni punti da tenere in considerazione prima di dar seguito al click o a qualsiasi altra azione.

- **Nessuna Banca invierà un SMS** in cui chiede di aggiornare le informazioni del conto o di confermare il codice del bancomat. Se avete qualche dubbio sempre meglio chiamare direttamente la propria banca che dar seguito all'SMS.
- Non bisogna mai cliccare un link o un numero di telefono presenti in un messaggio di cui non si è sicuri.
- Se un numero è "sospetto" non date seguito all'azione richiesta. Per numeri sospetti intendiamo, ad esempio, quelli tipo "5000". Come sostiene Network World, questi numeri sono collegati ai servizi che inviano SMS direttamente dalle caselle di e-mail, che spesso sono usati dai truffatori per evitare di fornire il loro reale numero di telefono.
- Evitare di abboccare all'esca: basta semplicemente non rispondere.

Redazione
(Settembre 2019)