WELCOME

To The Net

Ovvero
sopravvivere alla rete
ed altre storie incredibili

Truffe via SMS

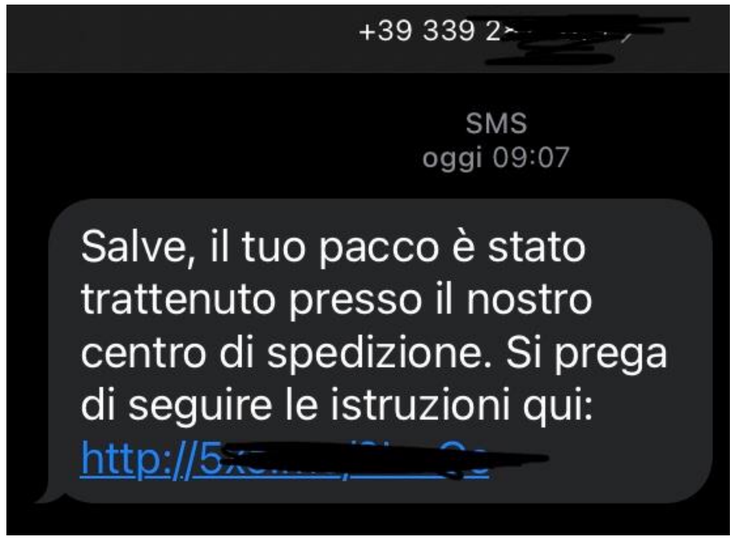
Le truffe informatiche potrebbero non arrivare solamente tramite browser o posta elettronica:
sta tornando infatti “di moda” lo **SMISHING**, ovvero i messaggi di phishing tramite SMS

SMS + **phishing** = **SMISHING**

Solitamente il mittente di smishing si finge un corriere, una banca, le poste o aziende di e-commerce, come Amazon.

Truffe via SMS

Gli SMS spesso sono legati a **comunicazioni di servizio**, pertanto la ricezione di un messaggio da parte di poste, istituti bancari o corrieri, assume automaticamente una certa autorevolezza e tendiamo a dare credito a quello che c'è scritto.



Truffe via SMS

Lo smishing ha come obiettivo **l'acquisizione dei dati personali** come password, numeri di carte di credito o password degli account e questi furti possono avvenire in due modi:

Facendo **scaricare app** che promettono determinate funzioni, mentre invece collezionano i dati dei clienti e li inviano a chi ha programmato la app (keylogger).

Facendo **visitare falsi siti web** che richiedono l'inserimento di dati personali, credenziali o numeri di carte di credito.

Truffe via SMS

Una volta acquisiti i nostri dati, le possibilità sono moltissime: **sottrazione degli account**, uso delle nostra **carta di credito**, furto di **identità**, uso della nostra mail per **phishing o truffe** e molto altro.

Spesso il problema non sta nel messaggio in se,
perché con dei semplici accorgimenti possiamo evitare facilmente queste situazioni; spesso veniamo fregati dalla **poca attenzione**, dalla **fretta** o dal fatto che spesso **sottovalutiamo i rischi** ed affrontando la situazione in maniera superficiale, finendo per assecondare chi ha organizzato la truffa.

Truffe via SMS

Come facciamo quindi a **riconoscere** ed a **proteggerci** da questi messaggi?

Smishing e phishing sono fenomeni molto meno pericolosi,
se siamo informati e se **non sottovalutiamo** il problema.

Per proteggersi dallo smishing infatti bastano una manciata
di norme da tenere bene in mente.

Truffe via SMS

A - Istituti bancari, Poste Italiane ed altri istituti di credito **non richiedono mai** le nostre informazioni personali attraverso SMS o mail.

B - Nel caso ricevessimo un SMS dalla banca, volendo controllare la situazione, **non seguiamo i link ma apriamo il browser** ed accediamo al sito web digitando l'indirizzo.

C - Avvisi urgenti di istituti bancari, poste o altre aziende che minacciano **blocchi del conto** o **vincite inaspettate**, devono costituire un campanello d'allarme.

Truffe via SMS

D - Se abbiamo dubbi sul messaggio, **contattiamo direttamente il mittente** con una telefonata o tramite il sito ufficiale.

E - Ricevuto un SMS importante, prendiamo **il tempo necessario** per leggerlo bene e **controllare con attenzione** il nome del mittente, riferimenti, firme ecc.

F - Controllare la **grammatica del messaggio**: spesso vengono tradotti automaticamente da software, pertanto non sarà difficile trovare errori ortografici o frasi sconnesse.

Truffe via SMS

Ed infine, ecco cosa NON fare se riceviamo una SMS sospetto da un istituto bancario o simili

- NON farsi prendere dal panico ma **ragionare** su quello che stiamo leggendo
- NON cliccare sui link presenti nelle mail ma **accedere manualmente** dal browser
- NON **inoltrare SMS** sospetti ai nostri contatti (catene di S.Antonio) per non trasmettere una potenziale minaccia
- NON **inserire dati personali** su siti che non conosciamo ne inviarli come risposta agli SMS
- NON **rispondere agli SMS** per evitare di dare conferma che il nostro numero è attivo