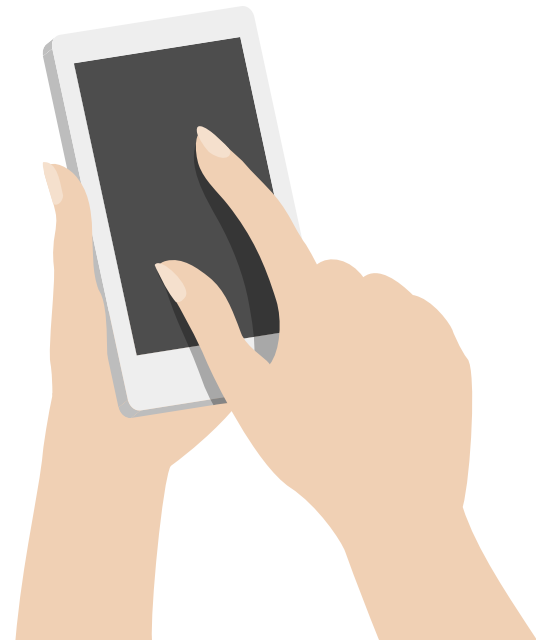
CYBER SECURITY TIPS #35

SIM SWAPPING: COS'È E COME DIFENDERTI.

LEGGI SUBITO LE NOSTRE TIPS!

1. COS'È IL SIM SWAPPING.

La truffa avviene con uno scambio di SIM. Il malintenzionato richiede una nuova SIM a TUO nome, facendovi associare il TUO numero di telefono. La tua SIM questo punto non funziona più.



LumIT
You Believe
We Create IT

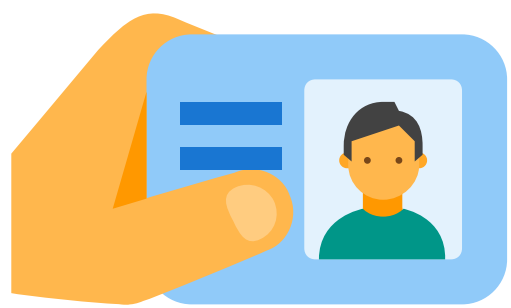
2. QUAL È IL RISCHIO.

Se per esempio usi l'autenticazione a due fattori per accedere al sito della banca, e uno di questi fattori è un SMS sul tuo cellulare, il criminale avrà accesso ai tuoi conti.

LumIT
You Believe
We Create IT

3. COME CI RIESCONO.

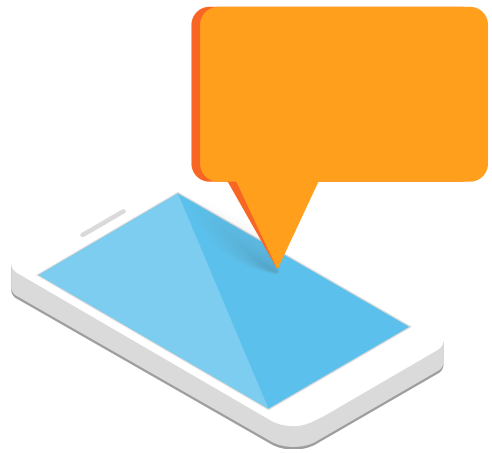
- Fingendosi te dopo aver rubato i tuoi dati su internet
- Inducendoti a farlo con l'inganno tramite tecniche di ingegeria sociale
- Corrompendo un operatore
- Con documenti di identità falsi.



LumIT
You Believe
We Create IT

4. COME DIFENDERTI.

Non usare l'SMS come strumento di autenticazione. Al suo posto puoi usare delle app come, per esempio, Google Authenticator.



LumIT
You Believe
We Create IT

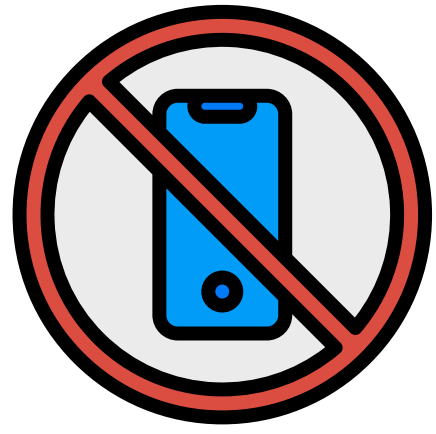
5. COME DIFENDERTI 2.

Se il provider di telefonia lo prevede, puoi impostare un PIN per accedere al tuo account. Senza di esso sarà impossibile effettuare modifiche, quali la sostituzione della SIM.

LumIT
You Believe
We Create IT

6. COME SAPERE SE SEI VITTIMA DI SIM SWAPPING.

Un sintomo di SIM swapping è la perdita del segnale. Se ti succede, spegni e riaccendi. Se il segnale NON torna, contatta il tuo gestore telefonico per una verifica.



LumIT
You Believe
We Create IT

TI È STATO UTILE QUESTO POST?

Faccelo sapere
con un like!

lumit.it