CYBER SECURITY TIPS #51

COS'È LO SPOOFING E COME DIFENDERSI.

LEGGI SUBITO LE NOSTRE TIPS!

1. DEFINIZIONE DI SPOOFING.

Lo Spoofing avviene quando
un criminale si finge una fonte
affidabile* per conseguire i propri fini
personali (e malvagi!).

Lo Spoofing assume diverse forme,
vediamo quali sono le più comuni
e come puoi tutelarti.

*Esattamente come quando
il lupo si traveste da nonna
nella fiaba di Cappuccetto Rosso!

LumIT
You Believe
We Create IT

2. EMAIL SPOOFING.

Si tratta delle email contraffatte:
ad esempio un hacker che si finge
la tua banca per estorcerti
le credenziali di accesso. La tecnica
dello Spoofing, in questo esempio,
viene usata per compiere un attacco
di Phishing. Un'email contraffatta
potrebbe, però, anche
veicolare del Malware.

LumIT
You Believe
We Create IT

3. COME DIFENDERTI?

Non cliccare, non rispondere
ed elimina il messaggio se:

- Ti vengono richiesti dati privati;
- Ti viene richiesto di scaricare un file .exe;
- L'indirizzo email è leggermente diverso da quello con cui ti interfacci di solito;
- Nel corpo dell'email ci sono errori di grammatica o refusi;
- Il messaggio ti mette fretta, ansia o pone promesse troppo allettanti per essere vere.

LumIT
You Believe
We Create IT

4. WEBSITE SPOOFING.

Ovvero quando un hacker crea un sito fasullo per rubarti informazioni o farti scaricare Malware.
Per reindirizzare le vittime su questi "siti civetta" spesso viene usata la tecnica del **DNS Spoofing** che dirotta il traffico dal sito legittimo a quello malevolo.

LumIT
You Believe
We Create IT

5. COME DIFENDERTI?

Quando ti colleghi a un sito web per effettuare pagamenti o quando devi accedere a dati sensibili, abituati a:

- Usare connessioni protette
  e MAI reti pubbliche;
- Verificare che l'URL sia corretta,
  normalmente i siti fasulli differiscono
  per la parte del dominio
  (esempio: .com invece che .it);
- Usare browser aggiornati
  per navigare in sicurezza.

LumIT
You Believe
We Create IT

6. SPOOFING TELEFONICO.

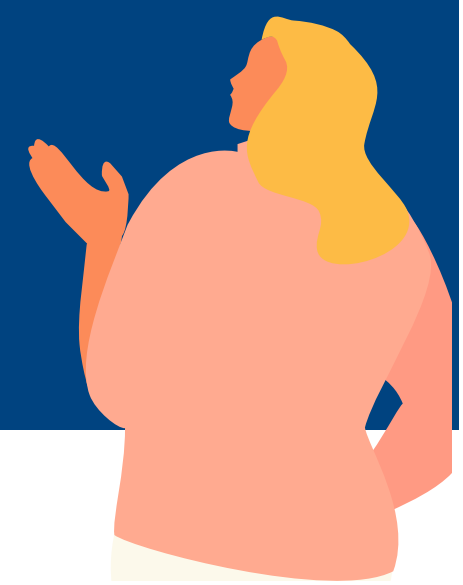
In questo caso potresti ricevere delle **chiamate** da un numero telefonico che conosci, per esempio quello della tua banca, e sentirti richiedere di condividere dati personali o di effettuare transazioni. In realtà, si tratta di un hacker, che ha alterato l'ID chiamante che visualizzi sul tuo dispositivo.
Lo stesso può avvenire tramite **SMS**.

LumIT
You Believe
We Create IT

7. COME DIFENDERTI?

Per tutelarti dallo Spoofing telefonico:

- Non condividere mai
  i tuoi dati personali con nessuno;
- Non cliccare su link arrivati via SMS,
  nel dubbio verifica che siano legittimi
  usando un canale diverso e sicuro;
- Installa un app specifica
  per filtrare il traffico voce
  e SMS e bloccare
  i numeri sospetti.



LumIT
You Believe
We Create IT

TI È STATO UTILE QUESTO POST?

Faccelo sapere
con un like!

lumit.it