Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

ARPAC CAMPANIA

Cybersecurity & Data Protection

Newsletter mensile: Ottobre 2025

Questo mese parliamo di...

SOCIAL ENGINEERING: RICONOSCERLO E DIFENDERSI

Il Social Engineering è una minaccia informatica che mira a ingannare gli utenti per rubare informazioni sensibili. È essenziale che tutti i membri dell'organizzazione siano in grado di riconoscere i segnali di allerta e le tecniche utilizzate dai truffatori, contribuendo così a proteggere le informazioni personali e aziendali.

LE PRINCIPALI TECNICHE

STRATEGIE DI DIFESA

Phishing

Truffa tramite email

Si verifica attraverso **email ingannevoli** che appaiono originate da fonti attendibili, con l'obiettivo di **raccogliere informazioni riservate**, inducendo l'utente a fare **click su link o allegati pericolosi.**

- Verificare **l'autenticità del mittente**, controllando non solo il nome ma anche l'indirizzo email.
- Verificare che i **link** siano **affidabili** prima di aprirli.
- **Non aprire allegati di dubbia provenienza.**

Smishing

Truffa tramite SMS

Avviene tramite **sms fraudolenti** che appaiono originati da fonti attendibili, con l'obiettivo di indurre le vittime a **fornire informazioni personali** o a **cliccare su link dannosi.**

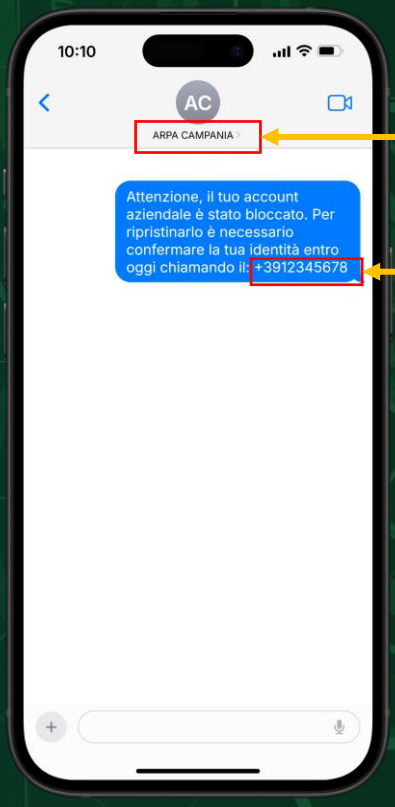
- I **Cyber Criminali** possono utilizzare software per **camuffare il mittente** degli SMS. Quindi, anche se il mittente sembra autentico, potrebbe trattarsi di una **truffa**, specialmente se viene richiesto di **richiamare su un altro numero** o aprire link.
- **Evitare di aprire link e allegati**, se non si è certi della provenienza.

Vishing

Truffa tramite telefonate

Si realizza attraverso **telefonate ingannevoli** per **truffare le vittime** e **raccogliere dati riservati**, spesso **spacciandosi per rappresentanti di enti fidati.**

- I **Cyber Criminali** possono utilizzare software in grado di **camuffare il numero del chiamante**. Se si hanno **dubbi** sull'identità dell'**interlocutore**, conviene **riagganciare** e **richiamare**.
- **Evitare di fornire informazioni sensibili**, se non si è certi dell'identità dell'interlocutore.



ATTENZIONE AL MITTENTE

Il **mittente potrebbe apparire autentico** ma in questo caso **non lo è**.

ATTENZIONE AL CONTENUTO DEL MESSAGGIO

Viene chiesto di confermare con **urgenza** la propria identità chiamando un **numero** che **non appartiene** al perimetro di **ARPAC**.

Esempio di Smishing

ATTENZIONE AL NUMERO

La chiamata **potrebbe sembrare** provenire da un **numero autentico**. Nel caso in cui quel **numero sia salvato in rubrica, comparirà il nome di quel contatto**.

ATTENZIONE ALLE INFORMAZIONI PERSONALI

Non fornire mai **informazioni personali** come credenziali, codici d'accesso e altri dati sensibili.

Esempio di Vishing

Non perderti la prossima newsletter mensile in cui verrà approfondito, anche con esempi pratici, come riconoscere e difendersi dal Phishing!