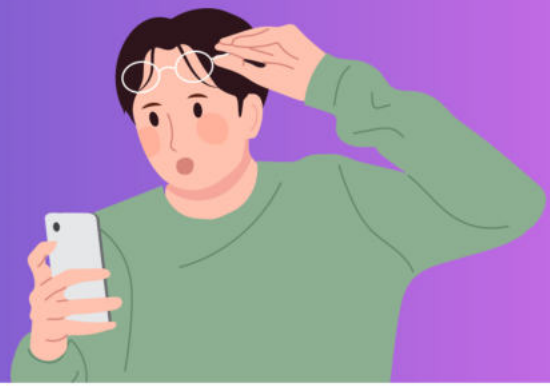
Truffe: occhio alle telefonate sospette!

Se ricevi una telefonata da una persona che si identifica come la tua banca o il tuo istituto di pagamento e ti chiede di effettuare operazioni: **non ti fidare.**
Ricorda che i truffatori possono falsificare un numero di telefono e **farlo sembrare quello autentico** della banca o dell'istituto di pagamento.

Raccomandazioni utili:

- Non fornire mai credenziali, dati sensibili o pin usa e getta
- Non dare seguito a richieste di conferma sul tuo smartphone
- Hai un dubbio? Chiudi la chiamata e contatta direttamente il Servizio Clienti della banca o dell'istituto di pagamento

Truffe: occhio agli SMS sospetti



Se ricevi un SMS da un numero di telefono che si identifica come il tuo istituto di pagamento e ti chiede di cliccare su un link non ti fidare e ignora il messaggio.
L'istituto di pagamento **non ti chiede mai di cliccare in link contenuti nei suoi SMS**.
Ricorda che i truffatori possono falsificare un numero di telefono e **farlo sembrare quello autentico** a quello dell'istituto di pagamento.

Cosa fare:

- NON cliccare su nessun link contenuto nell'SMS.
- NON fornire mai credenziali, dati sensibili o pin usa e getta
- NON dare seguito a richieste di conferma sul tuo smartphone

Hai un dubbio? Contatta il Servizio Clienti dell'istituto di pagamento

Attenzione alle truffe via SMS o via telefono

Se ricevi SMS o telefonate allarmanti che ti informano ad esempio del fatto che il conto o l'app sono associati a dispositivi sconosciuti o che chiedono conferma di eventuali transazioni, **non cliccare sul link e non seguire mai le indicazioni di sedicenti operatori degli istituti**.

Reperimento di informazioni su fonti pubbliche

L'accesso ad internet ci ha resi più connessi che mai, ma ci ha anche esposti a nuovi rischi.
Questo ha portato al proliferare di servizi che mettono a disposizione dei frodatori archivi anagrafici ai quali è possibile attingere.
I frodatori pertanto possono ottenere informazioni su di noi attraverso fonti pubbliche.
Quando ci iscriviamo a una newsletter o forniamo i nostri dati personali in generale, concedendo i consensi sulla privacy, **potremmo involontariamente alimentare tali archivi anagrafici a disposizione dei malintenzionati**.

Ricordiamoci: noi siamo i veri protagonisti della nostra esperienza.
Non permettiamo a nessuno di rubare il nostro potere digitale.
Scegliamo con cautela a chi affidiamo i nostri dati, leggendo attentamente le politiche sulla privacy.

Smishing (SMS phishing)

Lo smishing è una forma di attacco informatico che utilizza messaggi di testo (SMS) **per ingannare le persone e ottenere informazioni personali o finanziarie**. In genere, gli smishing vengono inviati come messaggi di testo che sembrano provenire da una fonte affidabile, come una banca o un'azienda di carte di credito. Il messaggio **può chiedere all'utente di fornire informazioni personali**, come il numero di conto bancario o il numero di sicurezza sociale, oppure **può includere un link che porta a un sito web fraudolento**. Tipicamente si tratta di un link che **apparentemente arriva da un mittente affidabile** e all'utente viene chiesto di rivelare informazioni riservate (ad esempio le proprie credenziali).

COSA FARE? Non cliccare sui link ricevuti e non fornire mai dati

GLOSSARIO

Vishing (Voice phising)

Il vishing è una forma di **attacco informatico che utilizza la voce**, invece della posta elettronica o dei messaggi di testo.

Il vishing può essere particolarmente pericoloso perché gli attaccanti possono utilizzare tecniche di "spoofing" **per falsificare il numero di telefono da cui proviene la chiamata**, facendo apparire che la chiamata provenga da una fonte affidabile.

COSA FARE? Non fornire mai credenziali, dati sensibili o PIN usa e getta e riagganciare

ATTENZIONE ALLE TRUFFE