

EMAIL DI PHISHING BANCARIO

Il phishing si riferisce a email fraudolente che ingannano i destinatari nella condivisione delle proprie informazioni personali, finanziarie o di sicurezza.



COME FUNZIONA?

Queste email:

possono **sembrare** identiche ai tipi di corrispondenza che le vere banche inviano.

replicano i loghi, il layout e il tono delle vere email.



chiedono di scaricare un documento in allegato o fare clic su un link.

usano un linguaggio che trasmette senso di urgenza.

COSA PUOI FARE?

- **Tieni il tuo software aggiornato**, inclusi browser, antivirus e sistema operativo.
- Presta particolare **attenzione** se un'email 'bancaria' ti richiede informazioni sensibili (ad esempio, la password del tuo conto bancario online).
- **Studia l'email**: confronta l'indirizzo del mittente con le altre email ricevute dalla tua banca. Controlla grammatica e ortografia.
- **Non rispondere ad un'email sospetta**, ma inoltrala alla tua banca digitando tu stesso l'indirizzo.
- **Non cliccare sul link o non scaricare l'allegato**, ma digita l'indirizzo nel tuo browser.
- In caso di dubbio, **ricontrolla** il sito web della tua banca o telefona alla banca.



I criminali informatici fanno affidamento sul fatto che le persone sono indaffarate; a colpo d'occhio, queste email contraffatte sembrano autentiche.



Fai attenzione quando usi un dispositivo mobile. Potrebbe essere più difficile individuare un tentativo di phishing dal tuo telefono o tablet.

#CyberScams

