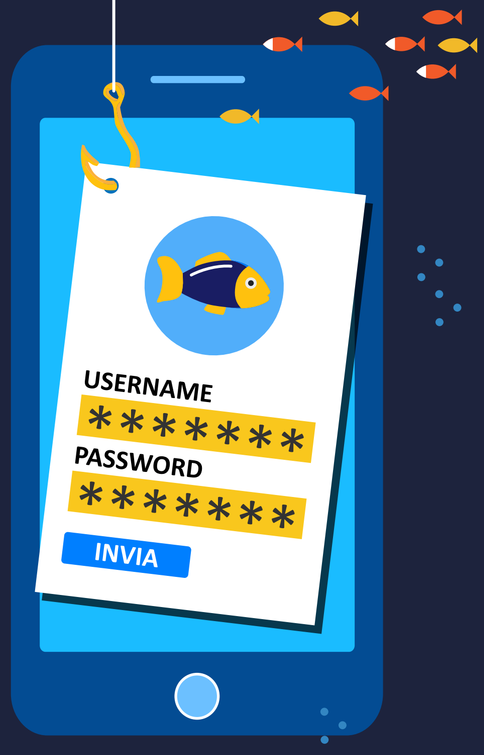
MINACCE VIA INTERNET

VALUTATE BENE PRIMA DI FARE CLIC

Se il vostro dispositivo smette di funzionare, potreste perdere il vostro denaro e i vostri dati personali oltre ai dati memorizzati. Non fatevi raggirare!



COME PUÒ SUCCEDERE?

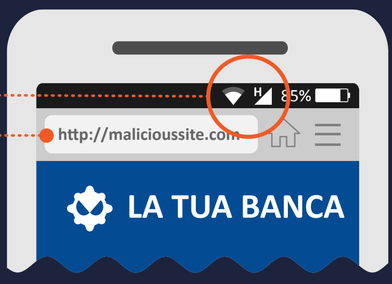
ATTACCHI DI PHISHING: gli utenti vengono ingannati e convinti a fornire i propri dati presentandosi come un'entità affidabile. Si diffondono tramite e-mail, messaggi di testo o piattaforme di social network.

ESPLORAZIONE DI SITI: il vostro dispositivo mobile potrebbe infettarsi semplicemente visitando un sito non sicuro.

DOWNLOAD DI FILE: un'e-mail può contenere link e allegati dannosi.

PERCHÉ È EFFICACE?

I dispositivi mobili sono COSTANTEMENTE CONNESSI a Internet.



Le DIMENSIONI RIDOTTE DELLO SCHERMO DI UN DISPOSITIVO MOBILE rappresentano un limite generale. I browser dei dispositivi mobili visualizzano gli URL su uno schermo dallo spazio limitato, pertanto è difficile vedere se un determinato dominio è autentico.

L'UTENTE NUTRE UNA FIDUCIA IMPLICITA nella natura personale di un dispositivo mobile.

COSA POTETE FARE PER PROTEGGERVI?

Siate sospettosi se ricevete un SMS o una telefonata da un'azienda che vi chiede di fornire i vostri dati personali. Potete verificare l'autenticità della chiamata o del messaggio ricevuto richiamando direttamente l'azienda al loro numero.

Quando navigate su Internet con il vostro dispositivo mobile, assicuratevi che la connessione sia protetta tramite HTTPS. Potete sempre controllare la parte iniziale dell'URL.

Non fate mai clic su un link o un allegato contenuto in un'e-mail o un SMS indesiderato. Eliminatelo immediatamente.

Diffidate dei siti dalla grammatica povera, con errori ortografici o a bassa risoluzione.

Se possibile, installate un'app di mobile security in grado di segnalare eventuali attività sospette.

EUROPOL EC3 European Cybercrime Centre

Polizia di Stato

#MobileMalware