FIDITALIA

SOCIETE GENERALE GROUP

RICONOSCERE LE FRODI ONLINE E COME DIFENDERSI.

17 gennaio 2025

Le truffe online sono sempre più sofisticate: conoscerle è importante per evitarle. Scopri alcuni consigli per mantenere alto il livello di sicurezza.

Riconoscere possibili attacchi finalizzati a carpire in modo illecito dati personali è ormai una necessità dato che sempre più spesso una scarsa conoscenza dei mezzi tecnologici, ma anche la distrazione o magari la tendenza a sottovalutare i rischi, possono rendere chiunque una possibile vittima di una truffa online.

Per garantire la massima sicurezza dei suoi Clienti, Fiditalia monitora costantemente e utilizza standard di sicurezza elevati in tutti i suoi processi ma è fondamentale che anche tu conosca quali sono le truffe online più diffuse per riconoscerle ed evitarne i rischi.

Ricorda che Fiditalia non richiederà mai via e-mail o SMS/Whatsapp i dati relativi a carte di pagamento, chiavi di accesso a MyFiditalia, l'area riservata dedicata ai clienti, o altre informazioni personali.

In caso di telefonata sospetta con richiesta urgente di comunicare o confermare i tuoi dati personali o dati di accesso Area Clienti, o altre istruzioni, non fare nulla di quanto viene richiesto e mettiti in contatto con Fiditalia.

Se non si è certi dell'identità di chi sta chiamando, si può contattare direttamente Fiditalia al numero unico 02.4301.8799 nei seguenti orari 9.30-13.30 14.30-18.00 (da lunedì a venerdì). Il numero di Fiditalia è abilitato solo alla ricezione di chiamate e non verrà mai utilizzato per effettuare chiamate in uscita.

FIDITALIA

SOCIETE GENERALE GROUP

Alcuni suggerimenti per "difendersi"

Tenersi informati sempre sulle principali frodi in modo da riconoscere le comunicazioni sospette e adottare una serie di precauzioni per proteggere i dati e il proprio computer o smartphone.

- **Non comunicare ad altre persone i Dati personali e codici di accesso (password, user-ID o codici):** sono strettamente privati e da conservare con estrema cura.

- **NON comunicare mai a sconosciuti, per telefono o per e-mail, dati personali, il numero della Carta, il codice PIN o altri dati collegabili a pratiche o conti** (es: codice IBAN o il codice fiscale).

- **Impara a riconoscere le comunicazioni fraudolente**: spesso non hanno nessun riferimento al tuo nome o cognome oppure contengono piccoli errori che ti consentono di capire la natura "malevola" della comunicazione.

- **Non rispondere a messaggi che sembrano non autentici, non cliccare sui link o scaricare allegati**;

- **Installa sul proprio computer solo software scaricati da fonti affidabili e fai costantemente l'aggiornamento dello smartphone**;

- **Usa un antivirus in grado di bloccare i siti di phishing**; si possono anche installare sul browser delle estensioni che segnalano possibili attacchi.

- **Accedi all'Area Clienti di Fiditalia solo da dispositivi fidati e protetti e da una connessione WiFi sicura.**

- Controlla che i siti dove vengono effettuati i pagamenti online adottino il **sistema di protezione antifrode 3D Secure** (*i siti che aderiscono presentano il logo Mastercard® Identity Check™ o Verified by Visa*).

FIDITALIA

SOCIETE GENERALE GROUP

Approfondimento: Cos'è il PHISHING?

Il **PHISHING** è l'attacco cyber più comune e più pericoloso.
È una modalità che gli hacker utilizzano fingendosi un ente affidabile in una comunicazione digitale per, indurti a fornire i dati sensibili (*come i dati personali, dati finanziari o codici di accesso*) oppure anche a scaricare un malware (*un software che crea danni al tuo computer e che può rubare i tuoi dati*) cliccando sul link presente nel messaggio che ti è stato inviato. **Si tratta di una truffa che consiste dunque nell'invio di E-MAIL, SMS o Messaggi whatsapp** o **chiamate telefoniche** che "sembrano" della tua banca o finanziaria e che richiedono di compiere un'azione immediata e magari con una certa urgenza e mirano principalmente a carpire dati riservati.

Sono 3 le tipologie di attacco Phishing:

- **Phishing - phishing via e-mail**
  richiesta di un'azione da compiere con urgenza, richiesta di informazioni sensibili, presenza di link o allegati da scaricare;

- **Smishing - phishing via SMS**
  offerta imperdibile o intervento di sblocco, urgenza per non perdere l'occasione o per intervenire; presenza di un link che indirizza a un sito malevolo;

- **Vishing - phishing via telefono**
  chiamata dalla banca o organizzazione conosciuta; senso di urgenza legato a un possibile rischio; richiesta di informazioni sensibili, pin, numeri carte.