RICONOSCERE LE FRODI ONLINE E COME DIFENDERSI

21 gennaio 2026

Diffida sempre da richieste di dati riservati, come ad esempio le credenziali di accesso allo SPID: segnale inequivocabile di tentativo di frode.
Fiditalia non chiederà mai credenziali SPID, PIN o password via e-mail, SMS o telefono.

Riconoscere possibili attacchi finalizzati a carpire in modo illecito dati personali è ormai una necessità, considerato che la crescente complessità degli strumenti tecnologici ma anche la distrazione o la tendenza a sottovalutare i rischi, possono rendere chiunque una possibile vittima di una truffa. Fiditalia adotta i più elevati standard di sicurezza a tutela dei propri Clienti, ma è fondamentale che anche tu conosca quali sono le truffe online più diffuse per riconoscerle ed evitarne i rischi.

Scopri alcuni consigli per mantenere alto il livello di sicurezza.

Le truffe online vengono messe in atto anche tramite i socialnetworks (Instagram, Facebook, ecc.) e i canali di messaggistica istantanea come Telegram: conoscerle è importante per evitarle.

Ricorda che Fiditalia e gli Agenti della propria rete commerciale non dispongono di un canale ufficiale Telegram e non usano tale strumento per pubblicizzare i propri prodotti e/o servizi né tantomeno per richiedere pagamenti a proprio favore.

Tieni a mente che Fiditalia non chiede mai tramite Telegram (né altri canali di messaggistica istantanea SMS/Whatsapp o socialnetworks) copia di documenti di identità, dati relativi a carte di pagamento, chiavi di accesso a MyFiditalia (l'area riservata dedicata ai clienti) o altre informazioni personali.

In caso di invito a partecipare a canali Telegram apparentemente riferibili a Fiditalia o ad una Agenzia di Fiditalia, stai in guardia!

Diffida dalle richieste di pagamento anticipato di commissioni, spese o acconti come condizioni per ottenere un finanziamento. Si tratta di un tentativo di truffa!

Ricorda che nessun intermediario o operatore autorizzato può pretendere il pagamento di somme di denaro prima dell'effettiva erogazione del finanziamento.

In caso di richieste sospette, non fare nulla di quanto viene richiesto e mettiti in contatto con Fiditalia:
- chiamaci al numero unico 02.4301.8799
  nei seguenti orari 9.00-13.00 14.00-17.00 (da lunedì a venerdì);
- usa i nostri canali social ufficiali Facebook, Linkedin e X;
- collegati all'Area Clienti di Fiditalia.

Fiditalia S.p.A.

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, altri dati collegabili a pratiche o conti (es: codice IBAN o il codice fiscale).
- Non comunicare mai le credenziali di accesso allo SPID.
- 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).
- Non trasmettere ad altre persone copia dei tuoi documenti di identità tramite e-mail e/o tramite strumenti di messaggistica istantanea e/o socialnetworks.

FIDITALIA

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.