

Truffe online: come difendersi

Progetto Digitalmentis regione Piemonte
Guida pratica n.1

Navigare, comunicare e fare acquisti online sono attività che ormai fanno parte della vita quotidiana di ognuno di noi. Tuttavia, con la crescente digitalizzazione si sono aperte nuove strade anche per truffatori e criminali informatici, pronti ad usare tecniche sempre più sofisticate per ingannare cittadini e imprese.

Oggi è la conoscenza la prima forma di prevenzione: capire come agiscono i truffatori, e sapere quali sono i segnali a cui prestare attenzione, significa evitare errori che possono costare molto cari.

Truffa o frode: due reati diversi

Il Codice Penale distingue due fattispecie di reato:

Truffa (art. 640 c.p.): si realizza quando si inganna una persona inducendola in errore, con artifici o raggiri, allo scopo di ottenere un profitto ingiusto.

Frode: il legislatore ne individua diverse tipologie e tra queste esiste, appunto, la frode informatica (art.640-ter c.p.), che si realizza alterando il funzionamento di un sistema informatico o telematico senza che la vittima se ne accorga, intervenendo illecitamente su dati e programmi per ricavarne un profitto illecito.

A differenza della truffa, che vede la vittima raggirata direttamente, nella frode non si configura l'induzione in errore di una persona perché il reato avviene "dietro le quinte", agendo sui sistemi tecnologici.

Spoofing, phishing, malware: i volti della truffa digitale

Una delle tecniche più comuni di attacco informatico è quella definita 'Sms-Spoofing', con cui i truffatori modificano l'identificativo del mittente di un messaggio in modo che sembri provenire dalla propria banca o da un ente pubblico.

Come si configura?

- Il testo generalmente invita a cliccare un link o a contattare un numero telefonico.
- Dietro il link c'è un sito fasullo, identico a quello reale, oppure un finto operatore che convince la vittima a comunicare codici di accesso o credenziali bancarie.
- Obiettivo: bastano pochi secondi e il conto viene svuotato.

Accanto allo 'Spoofing', si diffondono sempre di più altre forme di attacco informatico:

- Phishing: e-mail o messaggi che imitano comunicazioni ufficiali;
- Malware: software che rubano dati o bloccano i dispositivi;
- Ransomware: virus che chiedono un riscatto per sbloccare file o sistemi;
- Furti d'identità digitale con uso fraudolento di documenti o dati personali.

Cyber-security e prevenzione

Secondo una recente indagine oltre quattro italiani su dieci si sentono esposti a rischi legati alla cybersicurezza. Ma di certo la tecnologia da sola non basta a proteggersi: servono consapevolezza e buone abitudini.

Ecco le principali:

- ✓ usa password lunghe, uniche e complesse, con lettere maiuscole, numeri e simboli;
- ✓ attiva sempre l'autenticazione a due fattori;
- ✓ non condividere mai password o codici con nessuno;
- ✓ aggiorna regolarmente sistema operativo e antivirus;
- ✓ verifica l'indirizzo dei siti e diffida dei link inviati via sms o e-mail;
- ✓ evita di collegarti a reti Wi-Fi pubbliche per operazioni sensibili;
- ✓ in caso di dubbi, chiama i numeri ufficiali della banca o dell'ente.

Se la truffa o una frode informatica sono già avvenute, cosa fare?

Chi sospetta di aver subito una frode o una truffa deve agire subito per:

- ✓ Bloccare l'accesso ai propri conti o account digitali.
- ✓ Cambiare le password di tutti i servizi collegati.
- ✓ Conservare e-mail, sms o numeri sospetti come prova.
- ✓ Presentare denuncia alla Polizia Postale o ai Carabinieri.
- ✓ Avisare la banca o l'azienda coinvolta.

La segnalazione tempestiva aiuta a limitare i danni e ad evitare che altre persone cadano nella stessa trappola.

C'è da dire che le truffe informatiche non colpiscono solo i cittadini: gli attacchi cibernetici sono oggi usati anche per indebolire infrastrutture critiche, reti energetiche e sistemi pubblici.

La cosiddetta guerra cibernetica è purtroppo una realtà che rende ancora più importante la cultura della sicurezza digitale a tutti i livelli.

In sintesi

La prudenza è la miglior difesa e non è mai troppa!

Diffidare sempre delle richieste urgenti o non verificate, aggiornare costantemente i propri dispositivi e segnalare i tentativi di frode, sono azioni semplici ma decisive per tutelare se stessi e gli altri.

Sportello del Consumatore Torino

Via San Francesco d'Assisi 17 - 10122 Torino

Telefono: 011/436.65.66 – 011/436.74.13

sportello@consumatoripiemonte.it

Sportello del Consumatore Alessandria

Via dei Guasco 97 - 15121 Alessandria

Telefono: 0131/341.120

al@consumatoripiemonte.it

Sportello del Consumatore Biella

Corso Risorgimento 15 - 13900 Biella

Telefono: 015/84.61.457

info@consumatoribiella.it

Sportello del Consumatore Vercelli

Via Mameli 19 - 13100 Vercelli

Telefono: 0161/211.943

vc@consumatoripiemonte.it

www.consumatoripiemonte.it

Guida realizzata nell'ambito del progetto DIGITALMENTIS 2025, finanziato dal programma della Regione Piemonte con fondi MIMIT (DM 31/07/2024 e D.D. 14/02/2025)