

Modulo 5: Sicurezza Digitale e Prevenzione Truffe

Guida pratica per difendersi da phishing, smishing, vishing e furti d'identità

1. L'IMPORTANZA DELLA SICUREZZA DIGITALE

Con l'aumento dell'operatività online, la protezione dei propri dati personali, finanziari e dei propri dispositivi è diventata una priorità assoluta. La prevenzione e la consapevolezza rappresentano la prima linea di difesa contro cyberattacchi e truffe informatiche.

2. LE PRINCIPALI MINACCE ONLINE E COME RICONOSCKERLE

Tipologia Truffa	Canale e Modalità d'Attacco	Segnali d'Allarme da Rilevare
Phishing	Email ingannevoli inviate a nome di banche, INPS o Poste Italiane.	Link sospetti, grammatica scorretta, urgenza di cliccare.
Smishing	SMS che segnalano finti blocchi di conto o pacchi in giacenza.	Richiesta di inserire dati di carta di credito o PIN.
Vishing	Chiamate telefoniche da finti operatori di banca o forze dell'ordine.	Richiesta di dettare codici OTP o effettuare bonifici.
E-commerce Falso	Siti web trappola con sconti irrealistici su beni di consumo.	Mancanza di P.IVA, pagamenti solo con ricarica carte.

3. STRUMENTI FONDAMENTALI DI PROTEZIONE

- **Passphrase Sicure:** Utilizza frasi lunghe (almeno 12-15 caratteri) composte da parole casuali, numeri e simboli speciali. Evita date di nascita o nomi propri.
- **Autenticazione a Due Fattori (2FA):** Abilita sempre la verifica in due passaggi su tutti i tuoi account (email, social network, servizi bancari).
- **Aggiornamenti Software:** Mantieni aggiornato il sistema operativo dello smartphone e le singole app per correggere le vulnerabilità di sicurezza.

PROTOCOLLO DI EMERGENZA IN CASO DI TRUFFA:

1. Chiama subito la banca per bloccare carte e conto corrente.
2. Modifica immediatamente le password degli account compromessi.
3. Sporgi denuncia presso la Polizia Postale o i Carabinieri.
4. Contatta lo Sportello Codacons Lazio per avviare la procedura di reclamo e rimborso.

4. VADEMECUM DI AUTODIFESA DIGITALE

- ✓ Non cliccare mai su link ricevuti via SMS o email non richieste.
- ✓ Verifica la presenza del lucchetto **https://** e della P.IVA sui siti di acquisto.
- ✓ Nessun ente istituzionale ti chiederà mai password o PIN via telefono.
- ✓ In caso di dubbio, interrompi la comunicazione e contatta lo sportello di tutela.