U.Di.Con.
UNIONE per la DIFESA dei CONSUMATORI
REGIONALE SICILIA

Scopri cos’è il phishing, come riconoscere email e SMS falsi e come proteggerti dalle truffe online. Guida completa con esempi pratici, consigli e supporto.

---

# Cos’è il phishing e perché è pericoloso

Il **phishing** è una delle truffe informatiche più diffuse al mondo. Consiste nell’invio di email, SMS o messaggi WhatsApp falsi che imitano comunicazioni ufficiali di banche, poste o enti pubblici.
L’obiettivo dei criminali è quello di ingannare le persone e ottenere **dati personali, credenziali di accesso, password o informazioni bancarie**.

Questa tecnica è estremamente pericolosa perché:

- sfrutta la fiducia dell’utente,
- utilizza loghi e grafiche simili a quelle ufficiali,
- porta le vittime su **siti clonati** difficili da distinguere da quelli reali.

---

# Esempi di phishing più comuni

Riconoscere il phishing non è sempre semplice, ma alcuni segnali possono aiutarti. Ecco i casi più diffusi:

- **Email false da banche o Poste Italiane** che invitano ad aggiornare i dati o a “sbloccare” il conto.
- **SMS con link sospetti** che rimandano a siti non ufficiali.
- **Messaggi WhatsApp** che spingono a scaricare file o applicazioni dannose.
- **Avvisi di pagamento urgente** o di pacchi in giacenza, che giocano sulla fretta dell’utente.

---

# Come riconoscere un tentativo di phishing

Per difenderti, è importante imparare a riconoscere i dettagli che rivelano la truffa:

### 1. Controlla il mittente

Gli indirizzi email o i numeri di telefono sono spesso strani o leggermente diversi da quelli ufficiali.

### 2. Analizza il link

Diffida dei link abbreviati, con errori ortografici o che non corrispondono al dominio dell'ente.

### 3. Attenzione al linguaggio

Molti messaggi di phishing contengono errori di grammatica o traduzioni malfatte.

### 4. Non fidarti di richieste urgenti

Il phishing sfrutta la fretta: "il tuo conto sarà bloccato", "devi aggiornare subito i dati", "clicca qui entro 24 ore".

---

## Come difendersi dal phishing

Ecco alcune **regole di sicurezza online** che possono proteggerti:

- Non inserire mai password, PIN o dati bancari tramite email o SMS.
- Usa un **antivirus aggiornato** e attiva i filtri antispam.
- Digita sempre manualmente l'indirizzo del sito ufficiale nel browser.
- Attiva l'**autenticazione a due fattori** sui servizi più importanti.
- Se hai dubbi, chiama direttamente l'ente o la banca.

---

## Cosa fare se hai cliccato su un link sospetto

Se pensi di essere caduto in una trappola di phishing:

1. Cambia subito le password dei tuoi account.

2. Contatta la tua banca per bloccare eventuali operazioni non autorizzate.
3. Fai una scansione del tuo dispositivo con un antivirus aggiornato.
4. Segnala l’episodio alla Polizia Postale.

---

## La prudenza è la tua prima difesa

Il **phishing** è una minaccia concreta, ma con le giuste precauzioni puoi evitarlo. Ricorda sempre: banche, poste ed enti ufficiali non ti chiederanno mai credenziali o PIN tramite email o SMS.

Proteggiti e aiuta anche i tuoi familiari a non cadere nelle trappole online: **condividi queste informazioni**.

---

## Hai bisogno di supporto?

Se hai ricevuto un’email sospetta o vuoi saperne di più sulla sicurezza informatica, puoi rivolgerti ai nostri sportelli:

- **SIRACUSA** – Via Brenta 43
- 0931 091860 – 351 6310935
- siracusa@udicon.org
- Lunedì, Mercoledì e Venerdì: 9:30 – 12:30 | 15:00 – 18:00

Facile, veloce, sicuro.

seguici su Facebook https://www.facebook.com/udiconsicilia/

**Finanziato nell’ambito del programma della Regione Siciliana con fondi MIMIT D.M. 31/07/2024,**
**Avviso del 29/11/2024 ,D.D.14/02/2025, D.S.G N° 39 6/03/2025 della Regione Siciliana**