



# GUIDA PRATICA

## Phishing: come riconoscerlo

Messaggi falsi, link sospetti e richieste urgenti: i segnali da controllare prima di cliccare.

### 1 Cos'è il phishing?

Il phishing è una tecnica di truffa che imita banche, corrieri, enti o servizi conosciuti per convincere la vittima a comunicare password, codici, dati della carta o altre informazioni personali.

### 2 Segnali tipici



#### Urgenza

Messaggi che chiedono di agire subito o minacciano blocchi.



#### Mittente strano

Indirizzo email o numero che non coincide con quello ufficiale.



#### Link sospetto

L'indirizzo del sito è insolito, abbreviato o scritto male.



#### Richiesta dati

Password, PIN, OTP o dati bancari vengono chiesti nel messaggio.



#### Allegato

File inatteso o formato insolito ricevuto senza motivo.



#### Premio o rimborso

Promesse troppo convenienti usate per spingere al clic.

### 3 Prima di cliccare

- 1 Controlla il mittente completo.
- 2 Passa sul link e verifica l'indirizzo.
- 3 Apri il sito digitando tu l'indirizzo ufficiale.
- 4 Non comunicare password, PIN o OTP.

### 4 Se hai già cliccato

- 1 Non inserire altri dati.
- 2 Cambia subito le password coinvolte.
- 3 Contatta la banca se hai dato dati di pagamento.
- 4 Esegui una scansione di sicurezza sul dispositivo.



#### REGOLA D'ORO

Se un messaggio ti mette fretta, fermati: verifica prima di agire.



# GUIDA PRATICA

## Phishing: cosa fare

Una procedura semplice per ridurre i danni e recuperare il controllo dei propri account.

### 1 Procedura in 5 passi

- 1 Chiudi la pagina o il messaggio sospetto.
- 2 Cambia le password da un dispositivo sicuro.
- 3 Revoca o controlla le sessioni attive degli account.
- 4 Contatta banca o servizio interessato se hai fornito dati.
- 5 Conserva screenshot e segnala la truffa se necessario.

### 2 Buone abitudini

- 1 Usa password diverse.
- 2 Attiva l'MFA.
- 3 Aggiorna browser e sistema.
- 4 Usa preferiti o app ufficiali per servizi importanti.

### 3 Da ricordare

- 1 Un logo non prova l'autenticità.
- 2 L'urgenza è una leva psicologica.
- 3 Un link può nascondere un dominio diverso.
- 4 Nessun OTP va comunicato a terzi.

### 4 Il controllo più importante

**La domanda da farsi è: mi aspettavo davvero questo messaggio? Se la risposta è no, verifica attraverso un canale ufficiale separato.**



### CONSIGLIO FINALE

**Meglio perdere un minuto per controllare che perdere un account o del denaro.**