COMUNE DI BRESCIA | Brescia, La Tua Città Europea.

Brescia Inclusione Digitale

GUIDA PRATICA CONTRO LE TRUFFE ONLINE

👀 Perché bisogna fare attenzione?

I truffatori approfittano spesso della scarsa dimestichezza con Internet e gli smartphone. Le truffe non colpiscono solo “chi è distratto”: basta un attimo di fiducia mal riposta per perdere soldi, dati o la propria serenità. Conoscere i raggiri più comuni e imparare semplici regole di sicurezza è il miglior modo per proteggersi.

⚠ Le truffe più frequenti

False email e siti ingannevoli *(phishing)* 

Ricevi email da finti enti pubblici (INPS, Agenzia delle Entrate, Poste). Ti chiedono di cliccare su un link per risolvere un “problema urgente”.

➡ **Non cliccare mai. Cancella l’email. Verifica se l’indirizzo del mittente è autentico: spesso contiene piccole differenze rispetto agli originali.**

SMS e messaggi truffa *(smishing)* 

Ricevi un SMS o WhatsApp che parla di pacchi in arrivo, premi da ritirare o conti bloccati.

➡ **Non rispondere, non aprire link. Cancella il messaggio.**

Chiamate da falsi operatori 

Telefonate da chi si finge impiegato INPS, comunale, bancario, tecnico o persino carabiniere. Ti chiedono dati, codici o soldi.

➡ **Riaggancia subito. Nessun ente serio chiede dati personali al telefono.**

Trucchi comuni dei truffatori

I truffatori utilizzano una serie di strategie:

- Ti spaventano (“il tuo conto è bloccato”)
- Ti promettono soldi o premi (“hai vinto un buono spesa”)
- Fingono di essere qualcuno che conosci (“sono il tuo nipote”)
- Usano loghi e linguaggio simili a quelli ufficiali

Non fidarti dell’apparenza: la prudenza è la tua migliore difesa!

10 Regole per difendersi

1. Non fornire mai dati personali, codici o PIN per telefono.
2. Controlla sempre l’indirizzo email o il numero da cui ricevi comunicazioni.
3. Non cliccare mai su link o allegati sospetti.
4. Diffida di chi ti mette fretta o crea paura.
5. Conserva con cura password e credenziali: non scriverle in giro.
6. Non usare reti Wi-Fi pubbliche per accedere a conti o dati sensibili.
7. Siti ufficiali iniziano con “https” e hanno un lucchetto vicino all’indirizzo.
8. In caso di dubbio, chiama direttamente l’ente usando il numero ufficiale.
9. Parla con familiari o amici prima di agire se qualcosa ti sembra sospetto.
10. Segnala subito truffe o tentativi sospetti alla Polizia Postale (www.commissariatodips.it).

Scannerizza il QR code per visualizzare il Vademecum ufficiale contro le truffe online