

Connessi e consapevoli

Navigare in sicurezza non significa solo evitare truffe o siti falsi, ma anche proteggere i propri dispositivi e i propri dati da virus, programmi malevoli e intrusioni.

Prima di cliccare, chiediti sempre:

"So davvero chi c'è dietro questo sito o questa app?"

"Mi stanno chiedendo troppe informazioni personali?"

Se qualcosa ti sembra strano, fermati e rifletti. Un minuto di attenzione può evitare un grande problema.

Con pochi gesti e un po' di attenzione puoi navigare libero, sicuro e protetto.



La prudenza è la migliore connessione. Aggiornare, verificare e chiedere aiuto quando serve è il modo più semplice per restare al sicuro, ogni giorno..



Imparare a difendersi è facile se sai come fare...

Più digitali. Più liberi. Più protetti.



Per qualsiasi dubbio, non esitare...

... vieni in un **Punto Digitale Facile** o contatta una delle **Associazioni dei Consumatori**



Il progetto Digitalmentis è un'iniziativa per le competenze digitali finanziata dal Fondo MIMIT per i consumatori - DM 31/07/2024. In Piemonte è realizzato in collaborazione con le Associazioni dei Consumatori presenti sul territorio riconosciute dalla Regione Piemonte*, ed è correlato con la Misura 1.7.2 - "Rete di servizi di Facilitazione Digitale" del P.N.R.R.:

 www.regione.piemonte.it/web/comunicazione/digitalmentis-piemonte

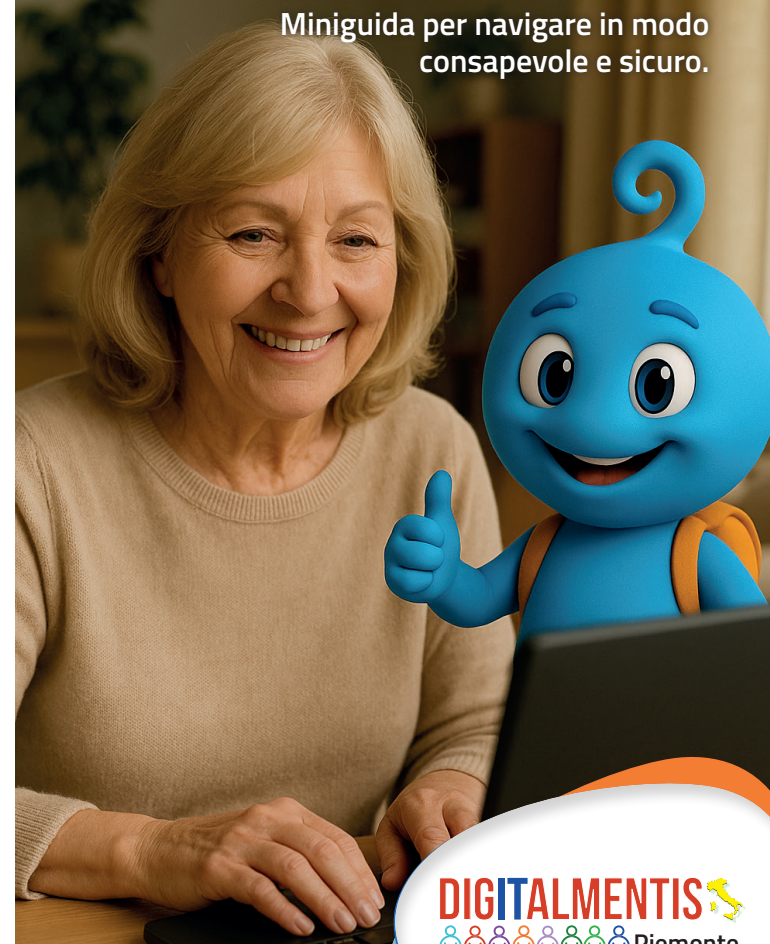


*Inquadra il QR code e scopri le associazioni dei consumatori che collaborano al progetto



Come riconoscere App e siti sicuri

Miniguida per navigare in modo consapevole e sicuro.



Più digitali. Più liberi. Più protetti.

www.regione.piemonte.it/web/comunicazione/digitalmentis-piemonte

Attenzione alle App sospette

Non tutte le app sono sicure, anche se sembrano ufficiali.

Prima di scaricare, verifica sempre:

- Chi è lo sviluppatore – è una società conosciuta o un nome sconosciuto?
- Le recensioni e il numero di download – poche valutazioni o voti tutti uguali possono essere un segnale di allarme.
- Le autorizzazioni richieste – se un'app ti chiede accesso a rubrica e microfono... qualcosa non va!
- L'origine del download – usa solo **App Store**, **Google Play** o **siti ufficiali**.

Se hai dubbi, non scaricare. Meglio un click in meno che un problema in più!



Installa sempre un antivirus affidabile e mantienilo aggiornato: gli antivirus moderni riconoscono siti pericolosi, app infette e link fraudolenti, bloccandoli prima che possano danneggiare il tuo computer o il tuo smartphone.

- Navigando online, fai attenzione a questi dettagli:
1. Controlla l'indirizzo: deve iniziare con **https://** (la "s" significa "sicuro").
 2. **Verifica il dominio:** diffida di siti con nomi strani o con lettere invertite (es. amazOn, gooogole...).
 3. **Cerca i contatti reali:** un sito affidabile mostra sempre indirizzo, telefono e partita IVA.
 4. Leggi le **condizioni e la privacy policy:** devono essere chiare e facilmente visibili.
 5. **Evita link ricevuti via SMS o e-mail:** potrebbero portarti a siti falsi.

Come riconoscere un sito sicuro

- Navigando online, fai attenzione a questi dettagli:
1. Controlla l'indirizzo: deve iniziare con **https://** (la "s" significa "sicuro").
 2. **Verifica il dominio:** diffida di siti con nomi strani o con lettere invertite (es. amazOn, gooogole...).
 3. **Cerca i contatti reali:** un sito affidabile mostra sempre indirizzo, telefono e partita IVA.
 4. Leggi le **condizioni e la privacy policy:** devono essere chiare e facilmente visibili.
 5. **Evita link ricevuti via SMS o e-mail:** potrebbero portarti a siti falsi.

Come riconoscere un sito sicuro

- Navigando online, fai attenzione a questi dettagli:
1. Controlla l'indirizzo: deve iniziare con **https://** (la "s" significa "sicuro").
 2. **Verifica il dominio:** diffida di siti con nomi strani o con lettere invertite (es. amazOn, gooogole...).
 3. **Cerca i contatti reali:** un sito affidabile mostra sempre indirizzo, telefono e partita IVA.
 4. Leggi le **condizioni e la privacy policy:** devono essere chiare e facilmente visibili.
 5. **Evita link ricevuti via SMS o e-mail:** potrebbero portarti a siti falsi.

Segnali di truffa digitale

Se noti uno o più di questi segnali, potrebbe trattarsi di un sito o app fraudolenti:

- Ti chiedono subito codici personali o password
- Promettono guadagni facili o premi immediati
- Ti mettono fretta o paura ("Ultima occasione!", "Il tuo conto verrà bloccato!")
- Hanno errori di ortografia o loghi poco chiari
- Non trovi informazioni chiare su chi gestisce il sito

Se hai dubbi, non inserire dati e chiedi consiglio al Punto Digitale Facile più vicino o a una persona di fiducia.

