

Cosa fare se pensi di aver subito una truffa con l'AI

1. Blocca tutto subito

Interrompi la comunicazione e non fornire altri dati.

2. Conserva le prove

Non cancellare messaggi, email o screenshot.

3. Avvisa la tua banca

Se hai dato dati o codici, blocca subito carte e accessi.

4. Fai una denuncia

Contatta la Polizia Postale o segnala su:

www.commissariatodips.it

5. Chiedi aiuto

Parlane con familiari o rivolgiti a un **Punto Digitale Facile**.

L'Intelligenza Artificiale può creare illusioni perfette. La tua sicurezza nasce dalla consapevolezza.

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



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



I rischi della Intelligenza Artificiale

Impara a riconoscerla e a difenderti dalle truffe



Più digitali. Più liberi. Più protetti.

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

L'intelligenza Artificiale

L'**Intelligenza Artificiale (AI)** è una grande opportunità...ma, come ogni tecnologia, può essere usata anche per ingannare.

Oggi truffatori e hacker sfruttano strumenti di IA per rendere le loro truffe più realistiche e difficili da riconoscere.

Con pochi clic è ormai possibile clonare una voce, ricreare un volto umano, imitare una scrittura o persino generare intere conversazioni. Queste tecniche, un tempo complesse e riservate agli esperti, sono oggi alla portata di chiunque e vengono impiegate per costruire truffe sempre più convincenti.

Ecco perché serve consapevolezza: riconoscere le nuove forme di manipolazione digitale è il primo passo per difendersi.



Le nuove forme di truffa

1. Deepfake (video o audio falsi)

Possono imitare la voce o il volto di una persona cara o di un funzionario. Se ricevi una videochiamata o un messaggio vocale che ti chiede denaro o codici, verifica sempre da un'altra fonte.

2. Clonazione di personaggi famosi

Alcune truffe usano video o spot con volti di celebrità, politici o imprenditori "ricreati" dall'IA per promuovere investimenti falsi o prodotti inesistenti. Anche se il volto è noto e il messaggio sembra autentico, non fidarti: nessun personaggio pubblico chiede denaro o dati personali online.

3. Chatbot truffaldini

Sembrano assistenti veri, ma servono a rubare dati o convincerti a cliccare su link pericolosi. Diffida da chi ti chiede password o codici via chat.

4. Email e messaggi "perfetti"

Grazie all'IA, i testi sono scritti senza errori e con toni credibili anche se la truffa parte dall'estero. Controlla sempre il mittente e non aprire allegati sospetti.



Come difendersi

1. Verifica sempre chi ti scrive o ti chiama.
2. Non fidarti di voci, video o foto "troppo perfette".
3. Controlla i link prima di cliccare.
4. Non fidarti dei "volti noti" online.
5. Non fornire mai dati personali o codici di sicurezza.

In caso di dubbio, chiedi aiuto a familiari o recati in un Punto Digitale Facile: insieme si impara a riconoscere anche le truffe più "intelligenti".

