

## ADOC, consapevolezza ed educazione dei consumatori

ADOC è l'Associazione per la Difesa e l'Orientamento dei Consumatori. Costituita nel 1988 da un gruppo di lavoratori e dirigenti della UIL, è presente capillarmente su tutto il territorio nazionale, con l'obiettivo di promuovere lo sviluppo e la diffusione della cultura del consumo responsabile.

### Contatti

Tel. 011 43 64 331  
WhatsApp 366 62 81 074

info@adocpiemonte.it

Via Parma, 10 - Torino

### Social



Adoc Piemonte



@adocpiemonte



@ADOCtorino



visita subito il nostro sito web  
**www.adocpiemonte.it**

# digitalmentis

**CYBERSECURITY**  
nell'era  
dell'**INTELLIGENZA**  
**ARTIFICIALE**



piemonte  
digitale 2030

REGIONE  
PIEMONTE

Più digitali. Più liberi. Più protetti.

**DIGITALMENTIS**  
Piemonte





Ministero delle Imprese  
e del Made in Italy

Iniziativa per le competenze digitali finanziata dal Fondo MIMIT per i consumatori - DM 31/07/2024; in Piemonte è realizzata in collaborazione con le Associazioni dei Consumatori presenti sul territorio riconosciute dalla Regione Piemonte, ed è correlata con la Misura 1.7.2 - "Rete di servizi di Facilitazione Digitale" del P.N.R.R."

## CYBERSECURITY

Ogni tipo di organizzazione è una potenziale vittima di cyber attacchi. Due metodi usati spesso dagli hacker per entrare nei sistemi aziendali o privati sono il social engineering e il phishing.

 Il **social engineering** consiste nel mettere l'utente in condizioni mentali tali da non capire il pericolo in cui mette il suo sistema.


 Il **phishing** invece consiste invece nel far credere che l'utente stia mettendo dati su un sistema sicuro quando in realtà si tratta di un clone.

La migliore protezione rimane sempre mantenere alta l'attenzione e **dubitare sempre dei link**, controllandoli prima di cliccarli. Neanche i cellulari sono immuni da tentativi di hacking.

Tre semplici precauzioni da prendere per usare il cellulare in sicurezza sono:

 **Evitare** di installare **app non dall'appstore**.


 **Non inoltrare i messaggi a catena** così da non dare accesso agli hacker ai nostri contatti.


 **Non scannerizzare QR di cui non conosciamo l'origine**. Bastano pochi accorgimenti da applicare sempre per non diventare vittime di un furto di dati.


## INTELLIGENZA ARTIFICIALE

Intelligenza Artificiale è un termine generico che raccoglie un'ampissima serie di **algoritmi**, i quali svolgono compiti estremamente diversi tra di loro.

Molti degli algoritmi che sono stati sviluppati di recente sono **chatbot**, ovvero programmi capaci di rispondere ai messaggi che ricevono in una maniera che simula benissimo come scriverebbe un umano. Questo può quindi essere usato dai malintenzionati per produrre contenuti ingannevoli. Per fortuna ci sono modi di **proteggersi**.

 **Dubitare** sempre **di chiamate o messaggi da sconosciuti** anche se imitano la voce di un conoscente. La soluzione è sorprendentemente semplice: telefonare al diretto interessato, così da confermare la veridicità di quanto sostiene lo sconosciuto che ti ha contattato.

 **Usare password lunghe e complesse** (minimo 15 caratteri, combinando lettere maiuscole, minuscole, numeri e caratteri speciali) e scriverle su di una agenda cartacea. L'alta complessità fa sì che i sistemi di sicurezza automatica possano bloccare i tentativi d'accesso prima che l'algoritmo IA trovi la password a forza bruta.

 **Usare l'autenticazione a due fattori**, così se il malintenzionato tenta un accesso a un tuo profilo è bloccato perché non ha accesso al tuo altro device di controllo.