PROGETTO ANTIFRODE

ATTIVI DIGITALI

Per non cadere nella rete

PRONTUARIO DI PREVENZIONE DELLE TRUFFE

NON CI CASCO!

Piccoli accorgimenti per vivere sicuri, ogni giorno.

OBIETTIVI DEL PRONTUARIO

Questo prontuario è pensato per aiutarti a:

Riconoscere e prevenire i principali tentativi di truffe: telefoniche, online, porta a porta e bancarie

Individuare i segnali di allarme e i comportamenti da evitare

Sapere cosa fare e chi contattare in caso di sospetto

Essere informati è la miglior difesa!

RICORDA

Nessun ente pubblico, banca o azienda ti chiederà mai soldi, password o dati personali per telefono o via email.
Se succede, è una truffa!
Le vere emergenze non necessitano di un bonifico!
Ti sembra proprio lui, parla come lui, vedi foto o video credibili, potrebbe non essere vero. L'intelligenza artificiale può ingannare.
Riaggancia e chiama tu.

LE CINQUE REGOLE ANTI-TRUFFA

1	**IL DUBBIO È TUO AMICO** Se qualcosa non ti convince, ascolta il tuo istinto
2	**LA FRETTA È CATTIVA CONSIGLIERA** Prenditi sempre tempo per pensare e verificare
3	**MAI SOLI** Parla con qualcuno di fiducia prima di decidere
4	**NESSUNA VERGOGNA A CHIEDERE** Verifica e confronto sono segni di intelligenza e prudenza
5	**112** In caso di dubbio chiama sempre le Forze dell'Ordine

TRUFFE TELEFONICHE

“Pronto, sono tua nipote… ho bisogno di soldi subito”

“Sono il Maresciallo, suo nipote è nei guai”
“Mamma, sono io! Ho avuto un incidente…”
Voce alterata o persino clonata con l'intelligenza artificiale

Segnali di allarme

• Chiamate da numeri sconosciuti o privati
• Urgenze improvvise (“Ho avuto un incidente”, “Mi hanno arrestato”)
• Ti chiedono di non dire niente a nessuno
• Si spacciano per avvocati, carabinieri, impiegati di banca
• Richieste di denaro, codici bancari o dati personali

Comportamenti da evitare

• Non fornire mai password, dati personali o bancari al telefono
• Non fidarti di chi dice di essere un parente senza verifiche
• Non seguire istruzioni per bonifici o ricariche
• Non fornire codici che arrivano via SMS o WhatsApp o email

Cosa fare

• Riaggancia subito
• Richiama il parente vero o un familiare fidato al numero che conosci
• Prendi tempo: "Ne parlo prima con mio figlio/figlia" - “Mi scusi, verifico e richiamo io.”

Chi contattare

• Chiama il numero di emergenza 112
• Chiama un tuo familiare o una persona di fiducia
• Sportello anti-truffe del Comune o associazioni locali

TRUFFE ONLINE

“Hai vinto un premio! Clicca quì per ritirarlo.”

Profili falsi che dichiarano amore
Finto supporto tecnico
Vendite online di prodotti inesistenti
Email phishing, link malevoli e QR code

Segnali di allarme

- Email o messaggi con link sospetti
- Offerte troppo belle per essere vere
- Richieste di dati bancari o password

Comportamenti da evitare

- Non aprire email sospette
- Non cliccare su link sconosciuti
- Non scaricare allegati da mittenti non verificati
- Non condividere dati sensibili via email o social
- Diffida di email che creano un senso di urgenza e ti invitano a fornire dati
- Limita la confidenza su internet
- Non pubblicare troppo della tua vita privata

Cosa fare

- Usa antivirus aggiornati
- Controlla sempre che l'indirizzo email del mittente sia quello ufficiale
- Digita direttamente tu l'indirizzo del sito (banca, fornitore energia, gas…)
- Attiva l'autenticazione a due fattori
- Cancella subito l'email se riconosci la truffa

Chi contattare

- Chiama il numero di emergenza 112
- Chiama un tuo familiare o una persona di fiducia
- Chiama l'assistenza clienti del tuo gestore (banca, fornitore energia, gas…)
- Sportello anti-truffe del Comune o associazioni locali

TRUFFE PORTA A PORTA

“Siamo dell’Enel, dobbiamo controllare il contatore.”

Iniziano con un sms, email o telefonata che sembra provenire dalla banca ma non lo è
“Hai ricevuto un rimborso, clicca qui”
“Siamo del servizio antifrode, serve il tuo codice per sbloccare il conto”

Segnali di allarme

- Visite non annunciate da falsi tecnici o funzionari con divise che sembrano ufficiali
- Pressioni per entrare in casa
- Di solito sono in due: uno distrae e l'altro si aggira per casa
- Richiesta di visionare bollette o firmare documenti
- Richieste di pagamento immediato

Comportamenti da evitare

- Non aprire la porta a sconosciuti senza appuntamento
- Non farti mettere fretta o intimorire
- Non mostrare bollette o documenti personali e dove tieni soldi e gioielli
- Non firmare nulla

Cosa fare

- Guarda dallo spioncino o dalla finestra prima di aprire
- Chiedi sempre un tesserino identificativo
- Verifica con l'azienda chiamando il numero ufficiale e non quello fornito dal finto tecnico
- Se hai dubbi, non aprire e chiama aiuto

Chi contattare

- Chiama il numero di emergenza 112
- Chiama un tuo familiare o una persona di fiducia
- Sportello anti-truffe del Comune o associazioni locali

TRUFFE BANCARIE

“La sua carta è stata bloccata, serve confermare i dati”

Profili falsi che dichiarano amore
Finto supporto tecnico
Vendite online di prodotti inesistenti
Email phishing, link malevoli e QR code

Segnali di allarme

- SMS o email che chiedono di “verificare” il conto
- Chiamate da falsi operatori bancari che ti chiedono dati o di fare qualche operazione
- Movimenti sospetti sul conto

Comportamenti da evitare

- Non comunicare PIN, password o codici OTP
- Non accedere al conto da link ricevuti via SMS/email sospetti
- Non fidarti di chi ti chiede di “spostare” i soldi
- Non farti distrarre al bancomat

Cosa fare

- Contatta subito la tua banca usando il numero ufficiale
- Blocca la carta se sospetti un furto
- Verifica spesso i movimenti bancari

Chi contattare

- Chiama il numero di emergenza 112
- Chiama un tuo familiare o una persona di fiducia
- Sportello anti-truffe del Comune o associazioni locali

Progetto promosso da

FONDAZIONE LONGEVITAS ets

FONDAZIONE LOTTOMATICA

In collaborazione con

MINISTERO DELL'INTERNO

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO" 1928

anci