

SIENA DIGITALE SICURA



Vademecum di Autodifesa Digitale

Una guida semplice.

Campagna di Prevenzione e Contrasto delle Truffe Digitali agli Anziani
2026 — III° Edizione

Iniziativa realizzata con il contributo del Ministero dell'Interno Prefettura di Siena



COMUNE
DI SIENA



Prefettura di Siena





Questo libretto è tuo

Le truffe capitano a tutti. Non solo a chi è ingenuo. Qui trovi, con parole semplici, come riconoscerle e cosa fare. Tienilo a portata di mano.

Nel dubbio, chiedi sempre a una persona di fiducia.

Chiedere non è debolezza: è la mossa più intelligente.



I truffatori non entrano nel tuo telefono.

Entrano nella tua testa.

Ti spaventano. Ti mettono fretta. Perché quando abbiamo paura smettiamo di ragionare.

Paura + urgenza = segnale di truffa



STOP

**Se un messaggio ti mette
fretta o paura:**

FERMATI.

Respira. Pensa. Poi decidi.

DA RICORDARE

Nessuna banca, ente pubblico o polizia ti chiederà mai di agire subito e in segreto. Se ti mettono fretta: è una truffa.

La calma è la tua difesa più forte.

Come riconosci un sito sicuro?

Ogni sito ha un indirizzo, come la targa su una porta.

Leggi l'indirizzo del sito **da destra** e guarda la parola subito prima del punto (.it, .com).



SICURO

www.poste.it/servizi

La parola prima del punto è "poste" → È davvero Poste Italiane



FALSO

www.poste.it.verifica.com

La parola prima del punto è "verifica" → **NON** è Poste Italiane!
È una truffa.

Attenzione: anche i siti falsi possono avere il lucchetto. Il lucchetto accanto all'indirizzo dice solo che la conversazione è privata, non chi c'è dall'altra parte. Il lucchetto non certifica l'identità del sito.

Hai cliccato per sbaglio?

Stai tranquillo. Cliccare apre solo una pagina: nessuno ti ruba niente finché non scrivi tu i tuoi dati.

Non scrivere nulla e **chiudi la pagina.**

Non condividere mai il codice **OTP**

SMS

Il tuo codice è:

5 8 3 2 1



**NON SI DICE
MAI**

È una password usa-e-getta che arriva via SMS per confermare un'operazione. Nessuna banca, nessun ente, nessun operatore ti chiederà mai di leggere il codice OTP al telefono.

Se qualcuno te lo chiede → è una truffa, riaggancia subito

Quando squilla il telefono, il nome che vedi sullo schermo può essere **falso**



Chiamata in arrivo

BANCA

02 1234567

Anche "Banca", "Polizia" o "Comune" possono essere nomi inventati. Quel nome **non è una prova** di chi sta chiamando.

Nel dubbio, riaggancia e richiama tu il numero che già conosci.

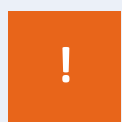
Quel numero è sul retro della carta o sul sito ufficiale.

Ricevere un'email non prova chi l'ha mandata: la casella è come la cassetta delle lettere, chiunque può imbucarci qualcosa.

Il nome è la **vetrina**; conta l'indirizzo vero. Toccando il nome del mittente lo vedi per intero.

Poste Italiane → servizio123@mail-strana.com **trappola!**

Come riconosci un'email sospetta?



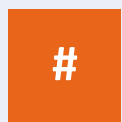
Ti mette fretta o paura

"Devi rispondere subito o perderai l'account"



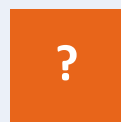
"Gentile cliente"

Non sa il tuo nome: è una mail inviata a migliaia di persone



Indirizzo o allegato sospetto

Non cliccare l'indirizzo e non aprire allegati non richiesti

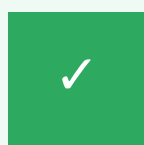


Errori o loghi sgranati

Le email vere delle banche sono scritte bene e con loghi nitidi

Nel dubbio: non rispondere, non cliccare, **chiedi aiuto.**

Comprare online: come pagare in sicurezza

**SÌ****Carta di credito****PayPal**

Se la merce non arriva puoi farti restituire i soldi.

**NO****Bonifico bancario****Ricarica PostePay****Buoni regalo**

Sono come contanti: spariscono

Se il prezzo è **troppo bello per essere vero**, di solito è un'esca.

La truffa del finto acquirente

Vendi qualcosa di usato e l'acquirente ti manda un indirizzo "per ricevere i soldi"?

ATTENZIONE

Per ricevere soldi non devi mai dare il numero della tua carta né nessun codice.

Se te li chiedono "per accreditare", è una **truffa**, stanno prelevando.

Non è colpa tua. Capita a tutti.

I primi 30 minuti sono **cruciali**

Agisci con calma ma senza aspettare:

1**Chiama subito la banca**

Blocca la carta o il conto corrente

2**Cambia le password**

Prima quella dell'email, poi le altre

3**Salva tutte le prove**

Messaggi, importi, date. Non cancellare niente

4**Fai la denuncia**

Carabinieri o Polizia Postale ([commissariatodips.it](https://www.commissariatodips.it))

5**Se hai fatto un bonifico**

Chiedi subito la revoca alla banca

ATTENZIONE ALLA SECONDA TRAPPOLA!

Dopo una truffa qualcuno potrebbe chiamarti dicendo: *"Recuperiamo noi i tuoi soldi"*. In realtà vuole altri tuoi soldi. → **Riaggancia.**

Nessuno recupera i tuoi soldi chiedendoti altri soldi.

Le 10 regole d'oro

- 1 Se ti mettono fretta o paura, fermati.
- 2 Leggi bene l'indirizzo internet partendo da destra: fai attenzione alle parole prima del punto (.it, .com)
- 3 Il nome sul telefono può essere falso.
- 4 Il codice OTP non si dice mai a nessuno.
- 5 SPID e Carta d'Identità valgono come la tua firma.
- 6 L'indirizzo email del mittente può essere falso.
- 7 Non aprire allegati che non aspettavi.
- 8 Paga con PayPal, mai bonifico a sconosciuti.
- 9 Per ricevere soldi non dare mai i dati della carta.
- 10 Truffato? Blocca subito, salva le prove, denuncia.

Nel dubbio, chiedi

Con queste regole sei più al sicuro della maggior parte delle persone. La **calma** e il **chiedere aiuto** sono le tue difese più forti. Se hai un dubbio su un messaggio o una telefonata, **fermati** e **chiedi** a una persona di fiducia.

Oppure chiama

112

Numero Unico di Emergenza

La tua banca	numero sul retro della carta
Numero Unico di Emergenza (NUE)	112
Il mio numero di fiducia	

Conserva questo libretto. Condividilo con un familiare o amico.