



DIFENDITI ONLINE

Guida pratica per conoscere ed evitare le truffe

Alia
PLURES

I truffatori sfruttano sempre più spesso la fiducia che i cittadini ripongono nelle comunicazioni di aziende, gestori di servizi pubblici ed enti. Per aiutarti a riconoscere i tentativi di frode più comuni, **Polizia di Stato** e **Plures** hanno realizzato questa guida pratica con esempi concreti e consigli utili per difenderti.

1



Falso SMS sulla Tari

"La sua posizione Tari risulta irregolare. È richiesto un tempestivo contatto al numero... per evitare aggravamenti"

Potresti ricevere un SMS che sembra inviato da Plures e che segnala presunte irregolarità nella tua posizione Tari, invitandoti a richiamare un numero, cliccare su un link o fornire dati personali.



ATTENZIONE SE IL MESSAGGIO:

- Ti invita a richiamare numeri sconosciuti o a pagamento
- Chiede dati personali o bancari
- Contiene link di cui non puoi verificare l'autenticità.

Prima di agire verifica sempre la tua posizione attraverso i canali ufficiali di Plures

2



Numero di telefono contraffatto

"Sul display compare il numero di un'azienda o di un ente pubblico. Sembra una chiamata autentica"

I truffatori possono alterare il numero visualizzato sul telefono per far credere che la chiamata provenga da un'azienda, da una banca o da un ente pubblico.



DIFFIDA SE CHI TI CHIAMA:

- Ti chiede **password, PIN, codici OTP** o **dati bancari**
- Ti invita a effettuare un pagamento urgente
- Ti mette fretta o ti scoraggia dal verificare la sua identità

Se hai dubbi interrompi la chiamata e richiama tu l'ente o l'azienda utilizzando i recapiti ufficiali

3



Promessa di rimborso

"Le spetta un rimborso. Per riceverlo ci comunichi i dati della sua carta di pagamento."

I truffatori possono promettere un rimborso inesistente per convincerti a fornire dati bancari, codici di sicurezza o a cliccare su un link.



ATTENZIONE SE IL MESSAGGIO:

- Chiede i dati completi della carta di pagamento
- Chiede PIN, password o codici OTP
- Invita a cliccare su un link

Non fornire dati bancari o codici e verifica la comunicazione attraverso i canali ufficiali dell'azienda

4



Richiesta di PIN e password

"Per completare la verifica mi serve il codice che ha appena ricevuto sul cellulare."

I truffatori possono chiederti codici OTP, PIN o password sostenendo che servono per una verifica, un rimborso o la risoluzione di un problema.



ATTENZIONE SE VENGONO RICHIESTI:

- Codici OTP ricevuti via SMS
- Password di accesso
- PIN, codici di sicurezza della carta di pagamento

Ricorda che questi codici autorizzano operazioni e non devono essere condivisi con nessuno

5



Richiesta di pagamento

"Hai una comunicazione urgente. Consulta l'avviso ed effettua il pagamento entro oggi."

I truffatori possono inviare messaggi che sembrano provenire da un ente pubblico, da PagoPA o da un'azienda di servizi per indurti ad aprire un link, scansionare un QR code o inserire dati personali



ATTENZIONE SE IL MESSAGGIO:

- Crea urgenza o minaccia sanzioni e maggiorazioni
- Ti chiede dati bancari, credenziali o codici di sicurezza
- Rimanda a un sito diverso da quello ufficiale

Accedi direttamente al sito o all'App ufficiale dell'ente o dell'azienda

6



Tecnico a domicilio

"Buongiorno, siamo incaricati di effettuare un controllo presso la sua abitazione..."

I truffatori possono presentarsi come tecnici o incaricati di un'azienda di servizi per entrare in casa o ottenere denaro, documenti o informazioni personali.



ATTENZIONE SE LA PERSONA:

- Chiede di entrare senza che tu possa verificarne l'identità
- Richiede denaro, dati bancari o documenti
- Prospetta un'urgenza per convincerti ad aprire la porta

Verifica sempre l'identità dell'incaricato attraverso i canali ufficiali dell'azienda

ATTENZIONE: NON SEMPRE È COME SEMBRA



Sei convinzioni che possono metterti a rischio



"Se compare il numero della banca, della Polizia o di un'azienda, posso fidarmi."



Non è sempre così. I truffatori possono alterare il numero visualizzato sul telefono per far apparire la chiamata autentica.



"Mi chiede un codice solo per verificare la mia identità."



No. I codici OTP, i PIN e le password servono ad autorizzare operazioni e non devono essere comunicati



"Conosce il mio nome e il mio indirizzo: allora è davvero chi dice di essere."



Non è una garanzia. Alcuni dati personali possono essere reperiti o sottratti e utilizzati per rendere la truffa più credibile.



"Se mi mettono fretta, vuol dire che è davvero urgente."



Diffida dell'urgenza. La pressione psicologica è una delle tecniche più utilizzate dai truffatori.



"Il sito ha il logo ufficiale, quindi è sicuro."



Attenzione. Anche siti e pagine web possono essere copiati e sembrare identici agli originali.



"Ormai ho risposto, tanto vale continuare."



Puoi ancora fermarti. Interrompi la conversazione, non effettuare pagamenti e verifica sempre attraverso i canali ufficiali.



HAI UN DUBBIO?

Prima di rispondere, pagare o comunicare dati personali, verifica sempre attraverso i canali ufficiali

Polizia di Stato



112 (emergenze)



www.commissariatodips.it

Alia Plures



AliaEstra App



Call center

800 888 333 (rete fissa)

199 105 105 (rete mobile)

0571 1969333 (rete fissa e mobile)



Area clienti:

www.aliaestra.it

CONSULTA LA GUIDA ONLINE

Scansiona il QR code e scopri come riconoscere e prevenire le truffe

