I NOSTRI CONSIGLI, LA TUA ATTENZIONE. UN VERO SCUDO CONTRO LE TRUFFE.

Vademecum Antifrode
per i Clienti Poste Italiane e PostePay.

Posteitaliane

Postepay

OPERIAMO IN SICUREZZA

Poste Italiane S.p.A. e PostePay S.p.A. hanno a cuore la tua sicurezza. Per questo, insieme alla nostra esperienza, ti offriamo queste poche e semplici regole raccolte nel Vademecum Antifrode dedicato a te che ogni giorno utilizzi i nostri prodotti e servizi. Con la tua collaborazione sarà più facile operare in sicurezza.

OPERAZIONI FINANZIARIE

Anche le tradizionali operazioni finanziarie presentano alcuni rischi che, se conosciuti, impediscono ai frodatori di ingannarci.

VERIFICA SOLDI IN CONTANTI

A volte accade che il Cliente che ha appena ritirato del denaro contante presso lo sportello dell'Ufficio Postale, venga seguito da qualcuno che **si presenta come un operatore dell'Ufficio Postale**.

Come funziona

In genere, il finto direttore o operatore dell'Ufficio Postale si avvicina alla vittima dicendole che potrebbe esserci stato un errore ed è necessario verificare il numero di serie delle banconote appena ritirate. La vittima consegna i soldi e il truffatore, fingendo di contarli o controllarli, **li sostituisce con banconote false**.

Cosa puoi fare tu:

- durante il percorso di andata o ritorno dall'Ufficio Postale, non farti avvicinare da sconosciuti, anche se dall'aspetto distinto e cordiale. Se ti chiedono di mostrare soldi o documenti relativi all'operazione svolta nell'Ufficio Postale, o se ti propongono investimenti finanziari, ignora tali richieste;
- ricorda che **Poste Italiane non manda mai i propri dipendenti in strada** a controllare la validità delle banconote, a sostituire quelle false, o a proporre investimenti finanziari. Se qualcuno si avvicina chiedendoti di controllare le banconote appena prelevate, stai attento: **potrebbe essere una truffa!**

FALSI PROMOTORI FINANZIARI

L'offerta di prodotti finanziari (azioni, obbligazioni, quote di fondi, ecc.) **dev'essere proposta esclusivamente da operatori autorizzati e iscritti in appositi albi pubblici**, previa verifica dei necessari requisiti. Gli operatori abusivi sono tuttavia molto abili e convincenti nel procacciare la clientela. Affidare alle persone sbagliate i propri risparmi **può causare la perdita di tutto o gran parte del patrimonio investito**.

Cosa puoi fare tu:

- verifica sempre che il tuo interlocutore sia un soggetto abilitato a svolgere l'attività. Non consegnare mai contanti alla persona che propone l'investimento. Non anticipare mai denaro - neppure tramite l'esecuzione di una ricarica, bonifico o postagiro in favore di un terzo - per poter acquistare dei prodotti di investimento;
- per investire i tuoi risparmi, rivolgiti a soggetti che possiedono una specifica autorizzazione. Controlla l'elenco sul sito della Banca d'Italia (www.bancaditalia.it);
- l'attività di offerta dei prodotti finanziari presso il domicilio del Cliente può essere effettuata solo da **consulenti abilitati all'offerta fuori sede** iscritti in appositi albi;
- **non consegnare il denaro e/o la carta a persone che non siano autorizzate** e non comunicare loro **il PIN** per eseguire il prelievo;
- **non lasciare mai incustoditi in Ufficio Postale i tuoi titoli** (Libretti di Risparmio, Buoni Postali, carte).

Ricorda

- Poste Italiane S.p.A. non ferma **MAI** i Clienti per strada per proporre investimenti.
- L'Ufficio Postale autorizza **solo il proprio personale** a effettuare le operazioni di sportello e di investimento finanziario e non custodisce i titoli dei Clienti.

RISCOSSIONE VAGLIA

Può succedere che navigando in rete, alla ricerca di un qualsiasi prodotto o servizio da acquistare, ci si imbatta in un truffatore.

Come funziona

Il truffatore **si presenta come il venditore di un prodotto o servizio**.
Una volta accordatosi con la vittima acquirente, le chiede di compiere due azioni:

A. **emettere un vaglia** dell'importo pari al valore del prodotto o servizio - come garanzia della disponibilità economica - per concludere l'acquisto;

B. **inviare** un'immagine del Titolo, come prova dell'avvenuta emissione.

In questo modo il truffatore è in possesso di tutti gli estremi per replicare il Titolo e richiederne il pagamento presso un Ufficio Postale, o per versarlo presso un Istituto di credito. A somma incassata, il truffatore fa perdere le proprie tracce mentre nessun bene o prodotto viene corrisposto alla vittima acquirente.

Cosa puoi fare tu:

- quando navighi in rete e vuoi acquistare un prodotto o un servizio, **scegli sempre siti ufficiali**, **conosciuti** e seleziona con cura il potenziale venditore;
- **non comunicare MAI gli estremi del vaglia e la password** valida per la riscossione, finché non ti è stato recapitato l'oggetto che hai deciso di acquistare;
- **non inviare MAI fotocopie e/o foto del Titolo** (vaglia, assegno, etc) tramite WhatsApp, Facebook o e-mail, finché non sei in possesso del prodotto o servizio.

ASSEGNI E MOVIMENTI DI C/C

Anche l'accettazione degli assegni può essere un'operazione rischiosa.

Cosa puoi fare tu:

- **non accettare mai assegni da sconosciuti o persone non fidate**, né quelli privi di alcune informazioni; l'Ufficio Postale potrebbe rifiutarne il pagamento;
- **non affidare mai in custodia ad altri il tuo libretto** degli assegni;
- **evita di spedire assegni e vaglia circolari**, non trasmettere mai fotocopie e/o foto di questi Titoli e non consentire che altri, se non legittimati, ne possano fare una copia;
- **controlla sempre con attenzione l'estratto conto** che riepiloga le entrate e le uscite del Conto Corrente e segnala ogni presunto errore;
- quando compili un assegno postale, **accertati che sul tuo conto ci sia il denaro necessario per pagarlo**;
- prima di firmare, **controlla che tutte le parti "bianche" siano compilate**: non lasciare scoperti i campi come luogo, data, beneficiario, importo (sia in lettere, sia in numeri).

OPERAZIONI POSTAMAT (ATM)

Prelevare denaro contante tramite lo sportello automatico ATM è un'operazione che può comportare dei rischi collegati alla possibilità di clonazione della carta, alla mancata erogazione delle banconote, al furto dei contanti e/o della carta e del PIN o al raggiro con l'intento di indurti a compiere una operazione di trasferimento fondi.

Cosa puoi fare tu:

- **custodisci con cura il codice PIN** della tua carta tenendolo sempre separato dalla carta. Se possibile, impara il PIN a memoria ed in ogni caso **non comunicarlo mai a terzi**;
- **verifica sempre che l'ATM non presenti alcuna anomalia** e che la tastiera non presenti **irregolarità**;
- se sospetti che lo sportello ATM sia stato manomesso, **non utilizzarlo**;
- **controlla di non avere nessuno alle spalle** prima di effettuare una qualsiasi operazione presso l'ATM;
- quando digiti il PIN, **fai attenzione a non essere osservato** né a farti distrarre;
- **rifiuta** sempre l'aiuto di terzi;
- ricorda che **nessun codice deve essere inserito per aprire la porta di accesso ai locali** dove si trovano gli sportelli automatici in cui fare prelievi o versamenti;
- se terminata l'operazione, l'**ATM non restituisce la carta di pagamento**, rivolgiti immediatamente all'Ufficio Postale per segnalare l'evento;
- **se il denaro non viene erogato**, chiedi una verifica all'Ufficio Postale o chiama il Servizio Clienti al numero riportato sul retro della carta.

Come proteggersi dalle truffe nelle proposte di acquisto per prodotti messi in vendita on line

Se metti in vendita un prodotto su un sito internet e vieni contattato da un presunto acquirente che si dichiara interessato all'acquisto, proponendoti di pagare subito ed invitandoti ad andare all' ATM per ritirare i soldi o per ricevere l'accredito del prodotto venduto, presta attenzione: **è una truffa.**

Come funziona

Il truffatore, fingendosi interessato ad acquistare il bene che stai vendendo, ti chiede di inserire la carta nell'ATM e ti guida telefonicamente nel fare un'operazione di ricarica di una carta prepagata (quella del truffatore!), spesso facendoti anche ripetere l'operazione più volte finché il plafond della tua carta non è terminato.

Ricorda

Diffida da chi ti invita ad andare presso un ATM per fare operazioni di ricarica o ricevere presunti accrediti.

SMS PERICOLOSI

Come riconoscere se un SMS è truffaldino e non proviene dal canale istituzionale di Poste Italiane:

- il testo del messaggio presenta **errori grammaticali e/o di sintassi**;
- il **link** contenuto nel messaggio **non è riferibile in alcun modo a Poste italiane** benché sembrerebbe rimandare ad una pagina simile a quella ufficiale dell'intermediario;
- **vengono utilizzati toni allarmanti** (ad es. per evitare un presunto blocco del conto e/o della carta, per stornare un'operazione da te non autorizzata etc) con il solo scopo di indurti ad effettuare alcune operazioni di pagamento nel più breve lasso di tempo.

Come difendersi dal furto del codice PIN della tua carta sottratto nell'ambito di un presunto processo di spedizione della carta di pagamento in scadenza

Se ricevi un sms e/o una telefonata, anche apparentemente proveniente dal canale istituzionale di Poste Italiane, in cui vieni informato che **la tua carta è in scadenza e che devi dare alcune informazioni affinché ti venga consegnata la nuova**, presta la massima attenzione!

Poste Italiane S.p.A. e PostePay S.p.A. non ti chiederanno MAI di condividere il tuo codice personale PIN

Ricorda, infine, che il codice PIN, nell'ambito del processo di rinnovo a scadenza della tua carta di pagamento, **resta lo stesso della carta scaduta** e che potrai in qualunque momento modificarlo con l'utilizzo delle credenziali personali in tuo possesso presso un ATM oppure nella tua area personale Home Banking.

Come difendersi dai principali raggiri volti a sottrarre la tua carta di pagamento (furto)

Se ti trovi in uno spazio pubblico, come ad esempio un parcheggio all'aperto di un supermercato e, nell'intento di caricare la spesa nella tua autovettura, vieni avvicinato da sconosciuti che ti chiedono informazioni o ti distraggono con artifici o raggiri, stai attento: **potrebbero sottrarti** la borsa, lo smartphone, il portafogli contenente **le tue carte di pagamento.**

Ricorda

- **non custodire MAI il tuo PIN insieme alla tua carta di pagamento**;
- abbi l'accortezza di **non lasciare incustoditi e visibili dall'esterno i tuoi oggetti personali (borsa, portafogli) all'interno della tua autovettura** anche se chiusa a chiave;
- appena ti accorgi che ti è stata sottratta la carta di pagamento, **contatta immediatamente il Servizio Clienti** di Poste Italiane per **bloccare la carta**.

OPERAZIONI IN UFFICIO POSTALE

Come proteggersi dagli inviti presso uno sportello di un Ufficio Postale ad effettuare operazioni di bonifico o postagiro con il presunto scopo di tutelare i propri risparmi

Come funziona

Ricevi un sms inaspettato ed apparentemente proveniente dal canale istituzionale di Poste Italiane (es. PosteInfo) contenente un invito a selezionare un link e, a seguito del sms, ricevi anche una chiamata da un presunto operatore Antifrode di Poste Italiane o da un ufficiale delle Forze dell'Ordine che ti invita a mettere in sicurezza i tuoi risparmi o il saldo del tuo conto e/o carta poichè è in corso una presunta indagine antifrode sugli operatori dell'Ufficio Postale in cui hai aperto il tuo rapporto. Nel corso della telefonata, vieni invitato a non rivelare all'operatore di sportello le vere motivazioni delle operazioni che stai effettuando, vieni sollecitato, spesso con toni allarmanti a recarti presso il più vicino Ufficio Postale o ATM ad effettuare una ricarica, un bonifico o un postagiro in favore di un terzo che non conosci al solo scopo di mettere in sicurezza il saldo del tuo conto o carta, importo che poi ti viene promesso ti verrà restituito su un conto o carta "più sicuri" una volta che l'indagine si sarà conclusa.

Ricorda

Poste italiane S.p.A. e PostePay S.p.A. non ti chiederanno mai dati personali, password di accesso alla tua area personale Home Banking, PIN, numeri delle tue carte o dei tuoi conti correnti nè di eseguire operazioni di trasferimento fondi verso terzi da te non conosciuti per presunti motivi di sicurezza. **Diffida da qualsiasi SMS e/o e-mail che non sia in linea con queste caratteristiche.**

Attento anche alle chiamate: il Numero Verde di Poste Italiane dedicato all'Assistenza Clienti è abilitato esclusivamente a ricevere le chiamate.
Se arriva una chiamata apparentemente proveniente dal numero verde di Poste Italiane, o da un Ufficio Postale o da una filiale, presta attenzione: **potrebbe essere un tentativo di truffa.**

OPERAZIONI INTERNET

Se utilizzi i servizi a disposizione sui canali Internet e sulle APP di Poste Italiane è necessario che tu faccia attenzione ai rischi. Impara a riconoscerli e a proteggerti rispettando alcune regole di base.
Se ricevi un SMS inaspettato ed apparentemente proveniente dal canale istituzionale di Poste Italiane (es. PosteInfo) con l'invito a selezionare un link o a chiamare un presunto numero verde per evitare un blocco carta o per mettere in sicurezza i tuoi risparmi, diffida: **potrebbe essere una truffa.**

COS'È IL PHISHING?

È una frode che si realizza con l'invio di e-mail o sms dal contenuto ingannevole, con lo scopo di carpire i codici di sicurezza personali del cliente vittima inconsapevole della frode stessa.

Come funziona

Il frodatore invia una e-mail o un sms (il cui mittente sembra essere Poste Italiane o PostePay) dal contenuto accattivante o perentorio, che induce il cliente a cliccare sul link presente nel testo e a connettersi a un sito apparentemente identico al sito web di Poste Italiane. Qui vengono richieste informazioni riservate e personali: nome utente, password di accesso all'Internet Banking, numero del cellulare, estremi della carta e, in alcuni casi, persino codici dispositivi finanziari ricevuti per sms.

Cosa puoi fare tu:

- **evita di aprire e-mail o sms di questo tipo o di scaricarne gli allegati e soprattutto non inserire UserId, password, pin, informazioni personali e codici conto** nei form dei siti Internet raggiunti tramite i link presenti all'interno di queste mail o sms. Nascondono un tentativo di frode, soprattutto quando richiedono codici personali.

Ricorda

Ricorda che Poste Italiane S.p.A. e PostePay S.p.A. **non chiedono mai in nessuna modalità** (e-mail, sms, chat di social network, operatori di call center, Ufficio Postale e prevenzione frodi) e per nessuna finalità:

- le tue credenziali di accesso al sito www.poste.it e alle App di Poste Italiane (il nome utente e la password);
- i dati delle tue carte (il PIN, il numero della carta con la data di scadenza e il CVV);
- i codici di sicurezza personali per autorizzare le operazioni (codice PosteID, il codice conto, le OTP- One Time Password ricevute per sms);

Conserva con la massima cura il nome utente, la password, il pin, il codice dispositivo conto, il codice Poste ID e ogni codice di sicurezza collegato ai tuoi strumenti di pagamento. **Non renderli noti a nessuno**;

Se qualcuno, spacciandosi per un operatore di Poste Italiane S.p.A. o PostePay S.p.A., dovesse chiederti quanto sopra riportato, puoi essere sicuro che si tratta di un tentativo di frode, quindi non fornire dati di alcun tipo e non ti fidare.

COSA SONO SMISHING, VISHING E SPOOFING?

Il phishing può essere effettuato anche via sms (**Smishing**) oppure attraverso una chiamata telefonica in cui il frodatore dichiara di essere un operatore di call center (**Vishing**).
Lo **spoofing** è una tipologia di truffa ormai nota e molto diffusa attraverso cui i malviventi riescono a camuffare il vero mittente, mascherandolo con una numerazione o un nominativo apparentemente riconducibile a Poste Italiane o a PostePay.

Cosa puoi fare tu:

- **non rispondere MAI a sms e/ o e-mail e non comunicare MAI telefonicamente gli estremi della tua carta** (numero PIN o identificativo della carta, data di scadenza e cvv o codice di verifica carta);
- nel caso avessi associato il tuo conto o la tua Carta Postepay al tuo smartphone, **NON comunicare codici personali o temporanei** e valuta sempre con attenzione le notifiche che il tuo dispositivo ti propone.

COS'È IL MALWARE?

Tra le tecniche di raggiro più insidiose c'è il malware, ovvero un **software malevolo, installato anche in maniera inconsapevole nel device** (smartphone, tablet, pc) della vittima, **con lo scopo di rubare dati e codici di sicurezza personali** ed eseguire operazioni di trasferimento fondi a discapito delle vittime.
Presta attenzione:

- ti suggeriamo di tenere sempre aggiornati il sistema operativo, i programmi antivirus e altri software o app presenti sui tuoi dispositivi;
- non cliccare sui link contenuti in email o sms sospetti e non installare, convinto magari da presunti operatori postali che ti hanno contattato telefonicamente, APP di dubbia provenienza specie se non scaricate dagli store ufficiali.

RESTA AGGIORNATO SU COME DIFENDERTI DALLE TRUFFE, VISITA LA PAGINA
https://www.poste.it/come-difendersi-dalle-truffe.html

Come possiamo aiutarti?

Chiamaci
Assistenza su tutti i servizi finanziari, sull'Internet Banking e sulle App BancoPosta e Postepay: **06.4526.3322** (dall'Italia e dall'estero)

- Il costo della chiamata da cellulare o da linea fissa dipende dall'operatore telefonico dal quale si effettua la chiamata.
- Attivo dal lunedì al sabato esclusi festivi, dalle ore 8.00 alle ore 20.00.

Scrivici
Vai su **poste.it** nella sezione Assistenza e invia la tua richiesta on line.

Puoi bloccare la carta:
Assistenza su tutti i servizi finanziari, sull'Internet Banking e sulle App BancoPosta e Postepay: **06.4526.3322** (dall'Italia e dall'estero)

- da **App Poste Italiane, App Postepay**, App BancoPosta o dai siti postepay.it o poste.it
- chiamando il numero 800.003.322 (dall'Italia) o il numero +39.06.4526.3322 (dall'Italia e dall'estero, il costo della chiamata da cellulare o da linea fissa dipende dall'operatore telefonico dal quale si effettua la chiamata)

Puoi anche bloccare temporaneamente la tua carta ai pagamenti, ai prelievi e agli acquisti online accedendo alla sezione "Impostazioni carta" direttamente da App Poste Italiane, App Postepay e App BancoPosta.

I.P. 10/24 Ed. Ottobre 2024 MP1024VA

poste.it

Posteitaliane