Come possiamo aiutarti?

Contattaci
Vai su **poste.it** nella sezione Assistenza
e compila il modulo

Chiamaci
803.160 attivo dal lunedì al sabato
dalle 8.00 alle 20.00
(chiamata gratuita per chi chiama da rete fissa)

199.100.160 per chi chiama da rete mobile (il costo della chiamata è legato all'operatore utilizzato ed è pari al massimo a euro 0,60 al minuto più euro 0,15 alla risposta)

Scrivici
Casella Postale 160 – 00144 Roma
Invia una mail a
servizio.clienti@posteitaliane.it

poste.it

Posteitaliane

I.P. 07/18 Ed. luglio 2018 MPD/18VA

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 che possono esserci.
Impara a riconoscerli e a proteggerti rispettando alcune regole di base.

COS'È IL PHISHING?

È una frode che si realizza con l'invio di false e-mail allo scopo di carpire i dati personali della vittima.

Funziona così.

Il frodatore invia una e-mail (il cui mittente sembra essere Poste Italiane) di contenuto accattivante o perentorio, che spinge il Cliente a cliccare sul link presente nel testo e a connettersi a un sito fittizio identico al sito web di Poste Italiane. Qui vengono richieste informazioni riservate: 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.

Accorgimenti

- **Evita di aprire e-mail di questo tipo o di scaricarne gli allegati e soprattutto non inserire UserId, password, informazioni personali e codici conto** dispositivi su siti Internet raggiunti cliccando sul link presente in una e-mail. Nascondono un tentativo di frode, soprattutto se chiedono codici personali.

Ricorda

- Poste Italiane non richiede MAI i dati riservati delle carte di pagamento.
- Poste Italiane non manda MAI e-mail con messaggi allarmanti su un blocco del conto, su pagamenti insoluti o su addebiti inaspettati.
- Per visitare il sito di Poste Italiane **digita direttamente l'indirizzo Internet** nella barra degli indirizzi.
- **Conserva con la massima cura** il nome utente, la password e il codice dispositivo e non renderli noti a terzi.
- **NON collegarti al sito indicato nella e-mail**; se per errore dovesse accadere, **NON autenticarti** sul sito falso e chiudi subito il web browser cestinando immediatamente l'e-mail di phishing.
- **NON fornire a terzi alcuna credenziale** e/o dato personale.
- Puoi **segnalare a Poste Italiane l'e-mail di phishing** prima di cestinarla, inoltrandola all'indirizzo antiphishing@posteitaliane.it

COSA SONO SMISHING & VISHING?

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"**).

Accorgimenti

- **Non rispondere a sms e non comunicare MAI telefonicamente gli estremi della tua carta** (numero PAN o identificativo della carta, data di scadenza e cvv o codice di verifica carta) o il codice dispositivo dell'Home-Banking generato dal Personal Card Reader (PCR).
- Nel caso avessi associato il tuo conto o la Carta Postepay al tuo smartphone, **NON comunicare codici personali o temporanei** e valuta sempre con attenzione le notifiche che il tuo dispositivo ti propone.
- **Fai attenzione al numero chiamante**: potrebbe sembrare il vero numero di Poste. Spesso, infatti, i frodatori riescono a mascherarlo e a nascondere il proprio.

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

vademecum**antitruffe**

Segui queste semplici regole per tutelare
la tua sicurezza ovunque, in strada come sul web.

Posteitaliane

ANDIAMO SUL SICURO

La tua sicurezza ci è sempre stata a cuore. Per questo, insieme alla nostra esperienza, ti offriamo queste poche e semplici regole, facili da ricordare e da seguire.
Ma soprattutto capaci di tutelare le tue operazioni: quelle tradizionali, come quelle digitali. Leggi e conserva queste pagine: l'accortezza non è mai troppa.

TRADIZIONALI 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**.

Funziona così

In genere, il finto direttore o operatore dell'Ufficio si avvicina alla vittima dicendo 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**.

Accorgimenti

- 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.

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**.

Accorgimenti

- 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 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 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.

Funziona così

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.

Accorgimenti

- 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 immagini/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

Infine, quando si parla di Conto Corrente e assegni ricorda:

Accorgimenti

- **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/immagini 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 o al furto dei contanti e/o della carta e del PIN.

Accorgimenti

- **Custodisci con cura il codice PIN** della carta, tenendolo sempre separato dalla carta. Se possibile, impara il PIN a memoria e non comunicarlo ad altri.
- Quando digiti il PIN, **fai attenzione a non essere osservato** e a non farti distrarre. Ricorda che con la nuova Carta BancoPosta **puoi modificare il PIN quando vuoi**.
- **Verifica che l'ATM non presenti anomalie** e che la tastiera non presenti irregolarità.
- Se sospetti che lo sportello ATM sia stato manomesso, **non utilizzarlo**.
- Ricorda che **nessun codice dev'essere inserito** per aprire la porta di accesso ai locali dove si trovano gli sportelli automatici dove fare prelievi o versamenti.