BPER: | BANCA PRIVATE CESARE PONTI

# Naviga in sicurezza.

## Conosci i principali rischi online e impara a proteggerti.

# Come mantenere al sicuro il proprio conto

Le principali pratiche illegali per sottrarre denaro o informazioni sensibili sono messe in atto da malintenzionati che fingono di essere la tua Banca attraverso email, sms, chat e telefono.
Per un utilizzo responsabile del tuo conto online e per aumentare la tua consapevolezza rispetto alle frodi bancarie, trovi qui un elenco di suggerimenti da mettere subito in pratica.

**DIFFIDA DA CHI TI CHIEDE CREDENZIALI O PIN**

Le informazioni e gli strumenti con cui accedi ai servizi della tua Banca (password, codici, carte, ecc...) sono strettamente personali e vanno custoditi con cura. La Banca può contattarti telefonicamente o via email, ma non ti chiederà mai di fornire credenziali, dati sensibili o codici usa e getta (OTP).

**CONSERVA LE TUE CREDENZIALI IN SICUREZZA**

Modifica periodicamente i codici di accesso alla tua area riservata e conservali/memorizzali in maniera sicura (non nel portafoglio!).

**NON AUTORIZZARE OPERAZIONI SCONOSCIUTE**

Controlla regolarmente la movimentazione del conto per assicurarti che non vi siano operazioni sconosciute. Ricorda che la tua Banca invia una notifica di approvazione ed una notifica successiva per conferma in tempo reale quando effettui operazioni dal tuo conto.

**NON ACCEDERE ALL'INTERNET BANKING CLICCANDO LINK ALL'INTERNO DI EMAIL O SMS**

Le informazioni e gli strumenti con cui accedi ai servizi della tua Banca (password, codici, carte, ecc...) sono strettamente personali e vanno custoditi con cura. La Banca può contattarti telefonicamente o via email, ma non ti chiederà mai di effettuare bonifici o ricariche dal tuo conto.

**MANTIENI SEMPRE AGGIORNATA LA TUA APP**

Accedi al tuo Internet Banking solo attraverso l'App ufficiale che trovi su App Store o Play Store oppure digitando l'indirizzo ufficiale nella barra di navigazione.

**EVITA DI CONSERVARE IL PIN NEL PORTAFOGLIO INSIEME ALLA CARTA DI PAGAMENTO**

In caso di furto o smarrimento, chiunque potrebbe usarli per prelevare denaro. È più sicuro tenere il PIN in un luogo diverso dalla carta.

**NON USARE LA STESSA PASSWORD PER PIÙ SERVIZI ONLINE**

Se un sito venisse compromesso, tutti i tuoi account potrebbero essere a rischio. Crea password diverse per ogni account per aumentare la sicurezza.

**IL KEY6 È FONDAMENTALE PER LA SICUREZZA DELLE TUE CARTE DI PAGAMENTO**

Aggiunge un ulteriore livello di protezione attraverso la verifica del codice a 6 cifre durante i pagamenti online. Questo significa che, anche se qualcuno rubasse i tuoi dati della carta, non potrebbe utilizzarli senza la verifica aggiuntiva, mantenendo i tuoi fondi al sicuro

# Fai attenzione al phishing via sms

Lo smishing (o phishing tramite sms) è una forma di truffa che utilizza messaggi di testo e sistemi di messaggistica (compresi quelli delle piattaforme social media) per appropriarsi di dati personali a fini illeciti.

## COME FUNZIONA LO SMISHING?

I malintenzionati fanno leva sul timore legato ad un rischio incombente per convincerti ad abbassare il livello di prudenza e a reagire d'impulso. I messaggi di smishing invitano a compiere azioni (cliccare link, effettuare ricariche o bonifici) o fornire informazioni con urgenza, per non rischiare danni (es: blocco del conto o blocco della carta di credito) o sottrazioni di denaro. Di solito, inviano messaggi per chiedere alle vittime di:

- **Cliccare un link** che conduce ad un finto sito web in cui inserire dati personali, dati bancari e/o di carte di pagamento.

- **Scaricare un allegato** che può contenere programmi malevoli capaci di prendere il controllo dello smartphone o accedere ai dati in esso contenuti.

- **Rispondere ai messaggi ricevuti**, inviando dati personali (il codice fiscale, il PIN del Bancomat o quello utilizzato per l'Internet banking, il numero della carta, il codice di sicurezza della carta, il codice usa e getta (OTP) da utilizzare per eseguire operazioni sul conto bancario e sulla carta di credito.

- **Chiamare un numero di telefono**, dove poi un finto operatore o un sistema automatizzato chiede di fornire informazioni di vario tipo, compresi dati bancari e/o di carte di pagamento.

## ESEMPIO DI TENTATIVO DI FRODE

**ATTENZIONE!**
**Il mittente dell'SMS sembra corretto ma può essere facilmente falsificabile**

**Il contenuto del testo serve a trasmettere la sensazione di urgenza**

**Il link contenuto nel messaggio NON È DELLA BANCA!**

**Non inserire mai credenziali dopo aver aperto un link presente in una comunicazione**

**Il numero non è quello ufficiale del Servizio Clienti**

## COME DIFENDERSI?

Per aiutarti a comprendere al meglio come riconoscere le situazioni di frode, abbiamo stilato una lista di regole che è bene tenere a mente.

- La Banca **non invia sms con link che rimandano alla pagina di accesso**, quindi se ricevi un sms con un link, evita di inserire le tue credenziali.

- La Banca **non chiama mai** per chiedere PIN, PASSWORD, CODICI USA E GETTA (OTP) o dati delle CARTE DI PAGAMENTO.

- La Banca **non chiama mai** per chiedere di effettuare operazioni di pagamento o per effettuare ricariche sulla carta. Indipendentemente che si tratti di pagamenti online o da ATM.

- Il nome mittente presente nelle comunicazioni (sms o email) ed il numero chiamante, **sono falsificabili**. Ti ricordiamo che se un sms si accoda a messaggi autentici della Banca non ne garantisce la veridicità; gli smartphone organizzano infatti le comunicazioni in base al mittente, senza valutarne l'affidabilità.

- **Digita tu stesso** l'indirizzo web relativo al sito della tua Banca nella barra di navigazione e controlla che il **nome del sito sia scritto correttamente**.

- Utilizza solo la nostra **App ufficiale** per monitorare i pagamenti e per bloccare le tue carte in caso di necessità.

- Non chiamare numeri differenti da quelli ufficiali, soprattutto se ricevuti via sms.

# Riconosci un tentativo di vishing

Il termine "vishing" deriva dall'unione di due parole: "voice" e "phishing". Si tratta di una truffa telefonica usata per ingannare le persone ed ottenere informazioni sensibili, come dati riservati, finanziari o credenziali d'accesso.

## COME FUNZIONA IL VISHING?

Il truffatore sfrutta tecniche di manipolazione emotiva (social engineering) e trucchi psicologici per convincerti a rivelare informazioni personali. Solitamente fa leva sull'urgenza della situazione, ad esempio un problema da risolvere, come un pagamento non riconosciuto, per sollecitare risposte rapide e immediate.

## COME RICONOSCERLO?

- Il **numero di telefono è sconosciuto** oppure sembra un numero autentico (questo è possibile tramite il fenomeno dello spoofing), non ti fidare quindi se vedi il numero della tua banca, i truffatori riescono a contraffarlo.

- Chi chiama dice di appartenere ad un call center di un istituto di credito, di una società di software o di telecomunicazioni.

- Ti **chiedono di trasferire denaro** su un altro account a richiesta. La tua banca non ti chiederà mai di farlo.

- L'interlocutore che ti ha telefonato **ti chiede di fornire pin o codici di carte di pagamento, di effettuare operazioni bancarie** per mettere al sicuro il tuo conto corrente oppure **di scaricare un'app** sul telefono per controllare da remoto il dispositivo.

- I **truffatori possono trovare le tue informazioni di base online** (ad es. attraverso i social media). Non presumere che chi chiama sia autentico solo perché possiede questi dati.

## COME EVITARLO?

- **Fai attenzione** alle chiamate telefoniche indesiderate.

- **Segnati il numero** del chiamante e avvisalo che lo richiamerai.

- Per verificare l'identità, **contatta direttamente la banca o l'organizzazione**.

- Ricorda quali **informazioni personali non dovrai mai fornire** e fidati solo delle tue chiamate in uscita.

- Se hai dubbi, **interrompi la conversazione e contatta direttamente il servizio clienti** dell'azienda per assicurarti che si tratti di una procedura regolare.

## COME RICONOSCO UN CONTATTO AUTENTICO DA PARTE DELLA MIA BANCA?

La banca ti può chiedere solo informazioni inerenti alle transazioni appena effettuate e dati per identificarti.
Non ti verranno mai chiesti dati sensibili come pin e password o di fare operazioni per mettere al sicuro il tuo conto.
Inoltre, non ti verrà mai comunicato di verificare un movimento tramite un link inserito in un SMS.

# Difendersi dai malware

I malware sono software sviluppati per compromettere la sicurezza dei tuoi dati. Alcune tipologie di malware possono infettare il tuo dispositivo (PC/ Tablet/Smartphone) attraverso azioni che puoi compiere inconsapevolmente come aprire il file di un'email sospetta o installare un programma scaricato da fonti non sicure.

**PER TUTELARE LA SICUREZZA DEI TUOI DISPOSITIVI, TI CONSIGLIAMO DI:**

Scaricare sul tuo smartphone solo **App da fonti sicure** come Play Store o Apple Store.

Proteggere i tuoi dispositivi con un **buon antivirus e mantenerlo sempre aggiornato.**

**Evitare di salvare le password** sui tuoi dispositivi.

**Non aprire mai allegati e non cliccare su link provenienti da indirizzi sospetti** o da persone che non conosci.

**Verificare accuratamente le email contenenti un allegato** anche se provenienti da una persona che conosci. Talvolta i computer infettati dei tuoi conoscenti possono inviare email contenenti virus a loro insaputa.

**Prestare attenzione ai siti web a cui accedi**:
un vettore di infezione dei malware è l'accesso a siti "strani", legati ad esempio a pubblicità online dove viene avviato un download automatico o sfruttata una vulnerabilità per infettare il device.

## PROTEGGI I TUOI DISPOSITIVI

Installa adeguati software di protezione antivirus sui tuoi devices (pc, tablet, smartphone) e aggiornali sempre.

## COLLEGATI DA RETI WI-FI SICURE

Accedi al tuo conto online soltanto dai tuoi dispositivi e da reti wifi personali. Le reti wifi pubbliche di hotel, bar, ristoranti o aeroporti sono assolutamente da evitare.

## PRESTA ATTENZIONE AI TUOI PAGAMENTI

Se ti accorgi di un uso improprio della tua carta oppure in caso di furto o smarrimento, contattaci subito. Ricorda che puoi utilizzare la nostra App anche per mettere in sicurezza le tue carte.

# Indirizzi e contatti ufficiali

Se hai qualche dubbio o ricevi comunicazioni sospette, contatta il nostro Servizio Clienti attraverso l'App oppure scegli il canale che preferisci dalla nostra pagina "Parla con noi" su bper.it.

Se rilevi **pagamenti non autorizzati** oppure ritieni di essere stato vittima di una frode contatta immediatamente la tua filiale o il Servizio Clienti del Gruppo BPER chiamando il numero **059 42 42**.

Per approfondire puoi leggere le informazioni riportate sul nostro sito www.bper.it nella sezione dedicata alla **Sicurezza Online**.

Questi sono i canali da cui ti contattiamo, **ricorda che non ti chiederemo mai di comunicare le tue credenziali.**

**TI CONTATTIAMO DAI CANALI UFFICIALI ELENCATI QUI SOTTO E SOLO PER DARTI INFORMAZIONI, PER RISPONDERE AD UNA TUA RICHIESTA O PER FISSARE APPUNTAMENTI IN FILIALE.**

**Email**
info@gruppobper.com
info@bperbanca.it

**Whatsapp**
+39 3351707442 - unico numero ufficiale verificato, controlla la doppia spunta.

**Servizio Clienti**
Il nostro Servizio Clienti ti contatta dal numero 059 4242, ma non ti chiederemo mai password o numeri delle tue carte di pagamento.

**Visita la pagina "Parla con noi" su bper.it e verifica i nostri canali ufficiali di contatto.**

## LA BANCA È SEMPRE AL TUO FIANCO

Svolgiamo costantemente un servizio di monitoraggio e prevenzione delle frodi sugli strumenti di pagamento. In caso di operazioni sospette, la banca contatta l'utente e, se il sospetto è confermato, blocca lo strumento di pagamento. In caso di notifiche massive, come attacchi phishing via SMS, avvisiamo i clienti tramite il nostro sito bper.it e con comunicazioni via app. **Ricorda che durante l'identificazione per il controllo dell'operazione non ti chiediamo mai credenziali bancarie, pin o di effettuare operazioni sul tuo conto, tantomeno ti manderemo link via SMS che ne richiedono l'inserimento**.
Ti chiamiamo solo per verificare una transazione effettuata sul tuo conto corrente per capire se qualcuno sta agendo al tuo posto.

**FIDATI SOLO DELLE NOSTRE COMUNICAZIONI UFFICIALI.**