

Sicurezza digitale.

Diamo valore alla cultura della sicurezza  
informatica e promuoviamo l'uso consapevole  
degli strumenti digitali.



MEDIOBANCA  
PREMIER

# Indice

---

|                                |    |
|--------------------------------|----|
| Sicurezza: una nostra priorità | 3  |
| Frodi: un mondo in evoluzione  | 4  |
| Phishing                       | 4  |
| Smishing                       | 6  |
| Vishing                        | 7  |
| Altre tipologie                | 8  |
| I nostri consigli              | 10 |

---

# Sicurezza: una nostra priorità

In Mediobanca Premier investiamo con impegno costante in innovazione al fine di **rendere protetta** l'operatività bancaria quotidiana e **tutelare** dati e informazioni dei nostri clienti.

**Diffondiamo** inoltre **cultura** nell'ambito della sicurezza informatica così da **condividere consigli** per navigare sul web in modo sicuro, per utilizzare consapevolmente gli strumenti digitali e per contrastare eventuali tentativi di frodi bancarie.

**Essere informati è infatti il primo passo per proteggersi.**

Per questa ragione, siamo sempre al tuo fianco per sensibilizzarti ed aggiornarti sull'evoluzione delle minacce informatiche, così da consentirti di **identificarle tempestivamente**.



# Frodi: un mondo in evoluzione

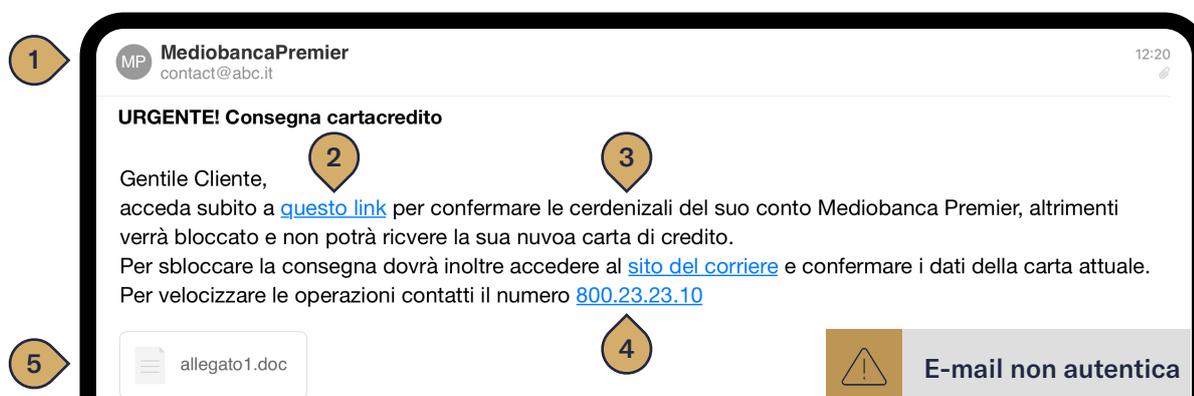
Le **frodi informatiche** hanno l'obiettivo di indurre a comunicare **informazioni personali, dati degli strumenti di pagamento** o **codici identificativi** per operare attraverso i Canali Digitali messi a disposizione dalla banca.

Sono sempre più **sofisticate** e si differenziano a seconda del **canale di contatto** attraverso il quale vengono attuate: e-mail, SMS, messaggi WhatsApp e chiamate.

Questa Guida ha lo scopo di aggiornarti sulle **principali tecniche** utilizzate dai truffatori e aiutarti a difenderti dai rischi più comuni fornendo **efficaci consigli** per contrastarli.

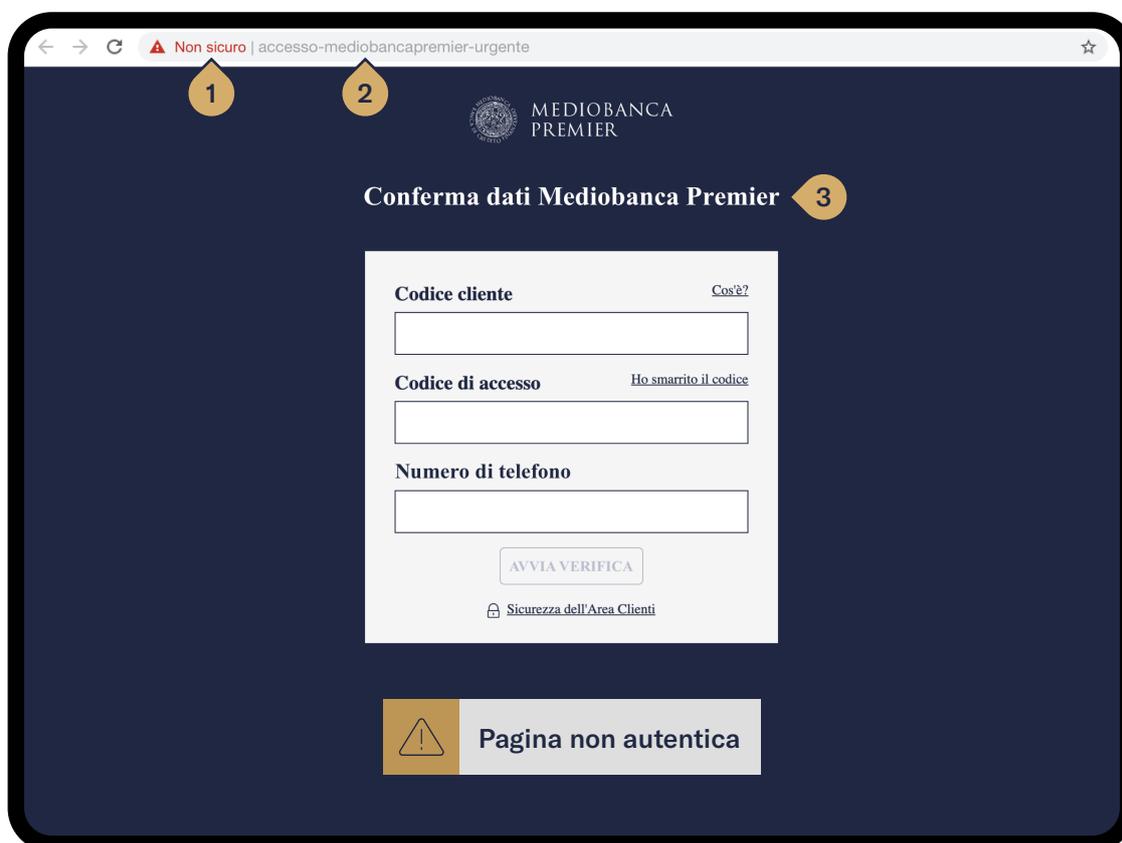
## Phishing

Avviene principalmente attraverso un'**e-mail** che imita una comunicazione ufficiale della banca. Nel messaggio sono però presenti **elementi anomali** che possono insospettire e quindi aiutare a valutarne l'attendibilità.



- 1** **Nome del mittente** simile o identico a quello della banca, ma indirizzo e-mail non corrispondente a quello ufficiale.
- 2** **Link** a siti o pagine web che invitano a fornire tempestivamente informazioni sensibili, dati della Carta o codici identificativi.
- 3** **Errori grammaticali** e/o **toni intimidatori**.
- 4** **Numeri di telefono** diversi da quelli del Servizio Clienti della banca, da contattare con **urgenza** per verificare operazioni bancarie o accessi all'Area Clienti.
- 5** **File allegati** che, se aperti o scaricati, potrebbero contenere un virus e/o consentire ai truffatori di navigare nel tuo PC ed entrare in possesso di informazioni e documenti personali.

I link contenuti nelle e-mail di phishing possono anche rimandare ad una pagina che **imita** la schermata di accesso all'**Area Clienti** della banca. L'obiettivo in questo caso è quello di invitare l'utente ad inserire i propri codici identificativi, così da intercettarli e poter operare sui suoi conti.



**1** Il browser potrebbe informarti che la tua **connessione non è sicura**, attraverso un'icona e/o un'etichetta poste prima dell'indirizzo web.

**2** La URL potrebbe contenere il nome della banca, ma non corrispondere all'indirizzo ufficiale: **<https://clienti.mediobancapremier.com>**. La dicitura "https" è importante, perché indica che il **protocollo di sicurezza del sito è aggiornato**.

**3** La **grafica** potrebbe essere **simile** a quella della pagina di accesso all'Area Clienti della banca, ma chiedere **informazioni** aggiuntive o **differenti**.

Per accedere all'**Area Clienti Mediobanca Premier** vengono richiesti:

- ❖ Codice cliente e Codice di accesso
- ❖ Strong Authentication.

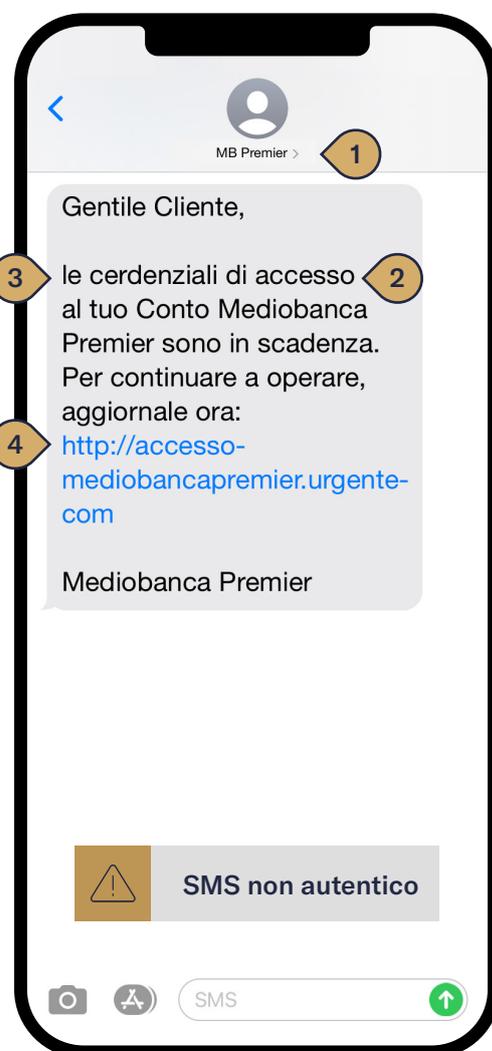
# Smishing

È l'equivalente via **SMS/WhatsApp** delle e-mail di phishing dove si invita, ad esempio, a **clickare su un link** per connettersi all'Area Clienti e verificare transazioni sospette. Può inoltre essere presente un **numero telefonico** da contattare per comunicare informazioni personali o disconoscere un recente addebito.

Anche in questo caso il link porta ad un **sito fraudolento**, mentre il numero di telefono rimanda ad un **truffatore**: il male intenzionato potrebbe dire di essere un operatore della banca e, fingendo di conoscere i tuoi dati e l'operatività dei tuoi conti, avrà invece lo scopo di entrare in possesso dei codici di accesso per operare in Area Clienti e App.

Alcuni **elementi** a cui prestare attenzione.

- 1 **Mittente** che può apparire con il nome corretto, per mimetizzarsi tra i messaggi ufficiali della banca. Ricorda di non limitarti a questa verifica in quanto i truffatori, utilizzando la tecnica dello spoofing, possono effettuare chiamate o inviare SMS da un mittente che a tutti gli effetti sembra quello autentico.
- 2 Rimandi a presunti **problemi di accesso** alla tua Area Clienti, alla necessità di **verificare** la tua identità o di **aggiornare** credenziali in scadenza. Si invita l'utente ad agire con **urgenza**.
- 3 **Errori** ortografici, imprecisioni o punteggiatura non corretta.
- 4 **Link** a siti o pagine web contraffatte.



# Vishing

Avviene attraverso una **telefonata**: i truffatori inducono a comunicare codici personali o informazioni sensibili per riuscire a disporre operazioni dal tuo conto.

La telefonata potrebbe provenire da un **numero che appare quello del Servizio Clienti** della banca. Viene resa ancora più credibile perché **seguita o anticipata da un'e-mail o un SMS**, il cui mittente potrebbe essere sempre la banca.

Chi ti contatta può:

- ❖ fare riferimento a **movimenti sospetti** relativi al tuo conto, alla tua carta o segnalarti tentativi di accesso all'Area Clienti da parte di terzi;
- ❖ chiedere di disinstallare e **scaricare nuovamente l'App** Mediobanca Premier adducendo pretesti diversi dalla veritiera operatività quotidiana;
- ❖ invitare a **clickare su un link** per fornirti supporto;
- ❖ cercare di instaurare un **rapporto di fiducia**, dimostrando di conoscere già alcuni tuoi dati e convincendoti così a fornire informazioni riservate;
- ❖ sollecitare una risposta o un'azione immediata, con il pretesto che si tratta di una **richiesta urgente**.



Mediobanca Premier non utilizza **mai l'800.10.10.30 o lo 02.3200.4141 per effettuare chiamate in uscita**: questi sono i numeri che puoi utilizzare tu per contattare il nostro Servizio Clienti.

# Altre tipologie

## Frode all'ATM

Anche gli **ATM** possono essere canali utilizzati per mettere in atto delle frodi volte, ad esempio, a intercettare e leggere i dati della tua carta per poi clonarla e sottrarti denaro.



### Come tutelarti

- ❖ prediligi uno sportello **ben illuminato** o all'interno di un istituto finanziario;
- ❖ prima di utilizzare l'ATM verificane la **stabilità**, assicurati che la tastiera aderisca bene alla superficie e che il lettore delle carte non sia mobile;
- ❖ per una maggiore sicurezza, **copri la tastiera** con la mano quando digiti il PIN;
- ❖ assicurati che **nessuno ti osservi** e allontana eventuali sconosciuti che dovessero avvicinarsi. Se qualcosa o qualcuno dovesse insospettirti termina subito l'operazione, ritira la carta e allontanati.

## QRishing

È una tecnica che ha l'obiettivo di sottrarre credenziali, informazioni o dati sensibili attraverso i **"QR-Code"**. Questi ultimi possono infatti essere contraffatti dai frodatori e reindirizzare così a link malevoli.

### Come tutelarti

- ❖ **scansiona** solo **codici** generati da **applicazioni sicure** e che non portano a siti dove vengono richiesti dati personali;
- ❖ **presta attenzione** al **contenuto** della pagina a cui rimanda il QR-Code;
- ❖ **installa applicazioni di sicurezza** anche sui dispositivi mobili.



## Money Muling

È una truffa volta al **trasferimento** o al **riciclaggio di denaro**. I frodatori attraverso **annunci online**, **offerte di lavoro**, **social media** o **contatti diretti** reclutano i cosiddetti **“money mules”**, ovvero persone inconsapevoli che possono diventare complici di un reato finanziario.

Questi ultimi, in **cambio di un compenso**, **offrono infatti la propria identità** per la sottoscrizione di conti correnti, carte di credito e altri strumenti di pagamento sui quali transitano poi somme di denaro provenienti da attività illecite.



### Come tutelarti

- ❖ affidati solo a **siti accreditati** per cercare lavoro e controlla sempre la veridicità delle informazioni fornite da chi ti offre un'offerta lavorativa particolarmente vantaggiosa;
- ❖ non aprire mai un **conto corrente** su richiesta di qualcuno che hai appena conosciuto;
- ❖ **non** permettere che il tuo **conto** venga **utilizzato da altri**;
- ❖ diffida di **contatti non richiesti** provenienti dai social media che promettono **facili guadagni**;
- ❖ non rivelare mai ad altri le tue **credenziali di accesso** ai servizi di online banking, né i dettagli delle tue carte di pagamento.

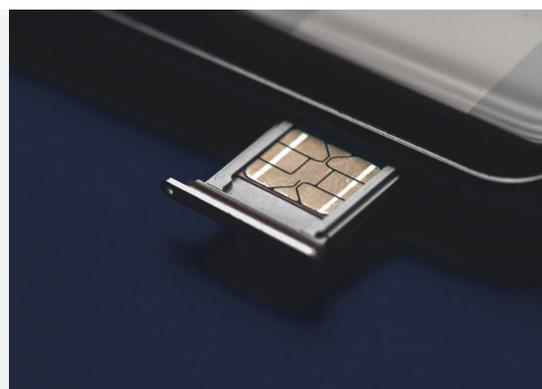
## SIM swapping

È una tipologia di frode attraverso la quale un male intenzionato convince l'operatore telefonico a **spostare un numero su una nuova SIM**, fingendo di esserne il legittimo intestatario.

Il frodatore riesce così ad intercettare le **password inviate via SMS** utilizzandole per accedere agli account online o per operare sui conti della vittima.

### Come tutelarti

- ❖ se il tuo **telefono perde inaspettatamente il segnale** rivolgiti al gestore telefonico per verificarne il motivo;
- ❖ **prediligi** la generazione di password temporanee attraverso **app di autenticazione**, piuttosto che tramite SMS.



# I nostri consigli

---

## Applicazioni

---



Scarica le applicazioni, come l'App Mediobanca Premier, solo dagli **store ufficiali** e tienile sempre **aggiornate**. Non lasciarti indurre nell'**installare software** sui tuoi dispositivi per condividere lo schermo o per controllarli da remoto, con il pretesto di effettuare **interventi tecnici** o darti **assistenza**.

## Connessioni

---



Prediligi l'utilizzo di **dispositivi personali** quando accedi ad ambienti in cui sono presenti dati bancari. Se possibile, evita di collegarti da **reti pubbliche** che potrebbero non essere sicure.

## Notifiche e Alert

---



Attiva le notifiche e gli alert, in modo da **avere sotto controllo le operazioni** da te eseguite e individuare tempestivamente movimenti sospetti e non autorizzati.

## Password

---



Scegli **password robuste**, ovvero formate da lettere, numeri e caratteri speciali; **cambiale frequentemente** e **disabilitane il salvataggio automatico**. Individua poi **password differenti** per gestire diversi account.

## Richieste sospette

---



In caso di richieste che sembrano provenire da Mediobanca Premier ma che ti appaiono sospette, prima di rispondere o compiere azioni **verificane l'autenticità** rivolgendoti ai nostri **canali ufficiali**, consultabili su **mediobancapremier.com**, nella sezione *Contatti*.



# MEDIOBANCA PREMIER