Suggerimenti Vincenti per la Tua Sicurezza

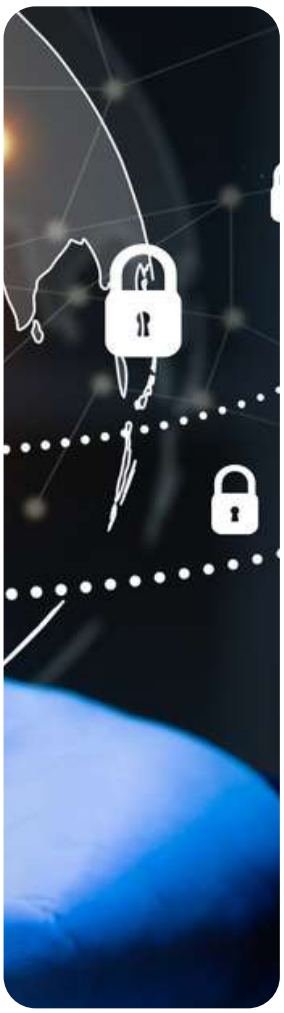
Un vademecum per salvaguardare
i tuoi dati e proteggere le tue operazioni

mediolanum





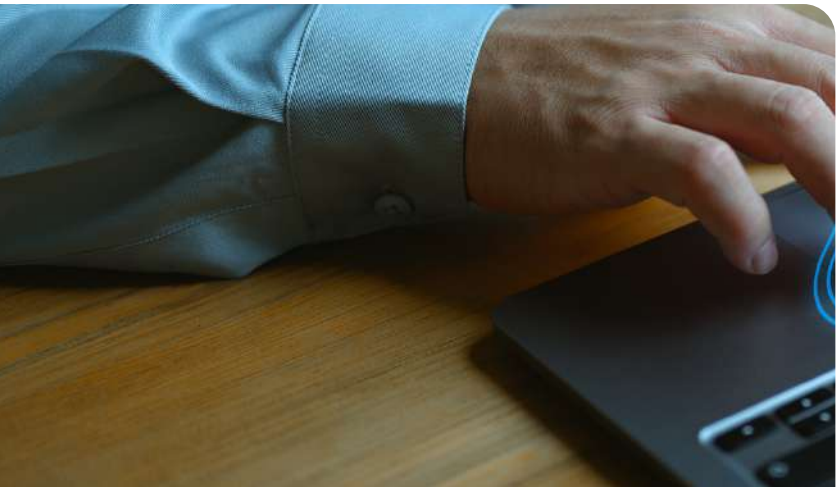





SOMMARIO

Banca Mediolanum

è la tua ALLEATA.



LE STRATEGIE DEGLI AVVERSARI

Esistono diverse tipologie di frodi che hanno l'obiettivo di entrare in possesso di dati personali, sfruttando l'emotività e la sensibilità degli utenti.

Per non farsi cogliere impreparati bisogna conoscere e anticipare i propri avversari!

Cos'è lo SMISHING?

È una frode che consiste nel tentativo di carpire informazioni personali degli utenti (es. codici segreti, dati anagrafici o numeri delle carte di pagamento), **tramite l'invio di messaggi SMS contraffatti**, apparentemente provenienti da soggetti affidabili (es. la banca).

Questi messaggi **invitano a contattare un numero di telefono diverso dai numeri ufficiali della Banca oppure a collegarsi al sito tramite un link**, contenuto nel testo, per confermare o comunicare dati riservati. **In realtà il sito in cui si atterra è un sito pirata**, simile a quello ufficiale.

Talvolta, a queste comunicazioni fraudolente, **può seguire una telefonata** durante la quale i malfattori si identificano come operatori della Banca **(Vishing)** al fine di **ottenere ulteriori dati personali e/o codici segreti, camuffando il numero chiamante con la tecnica dello Spoofing.**

Cos'è il VISHING?

È una frode che **usa le chiamate telefoniche per ingannarti.** Il frodatore **finge di essere la Banca** e con senso di **urgenza e pressione** cerca di convincerti a **fornire dati personali, delle carte di pagamento e/o i codici segreti o ad effettuare un pagamento** (Push Payment fraud). Avviene spesso a seguito dello smishing!

Cos'è lo SPOOFING?

È una tecnica che consente al frodatore di **nascondere la propria identità** al fine di risultare "affidabile" agli occhi della vittima, **facendo apparire le comunicazioni fraudolente tra quelle realmente inviate dalla Banca o da un numero di telefono riconducibile alla Banca o un Family Banker Office.**

Spinta al PAGAMENTO FRAUDOLENTO:

Durante una "**Authorised push payment fraud**" i frodatori potrebbero **contattarti fingendo di essere la banca** o un'altra organizzazione fidata, affermando che sei stato vittima di una frode e che **devi trasferire i tuoi soldi su un conto bancario (IBAN) o su una carta a te sconosciuti, facendoti effettuare il pagamento o facendoti confermare l'operazione.**

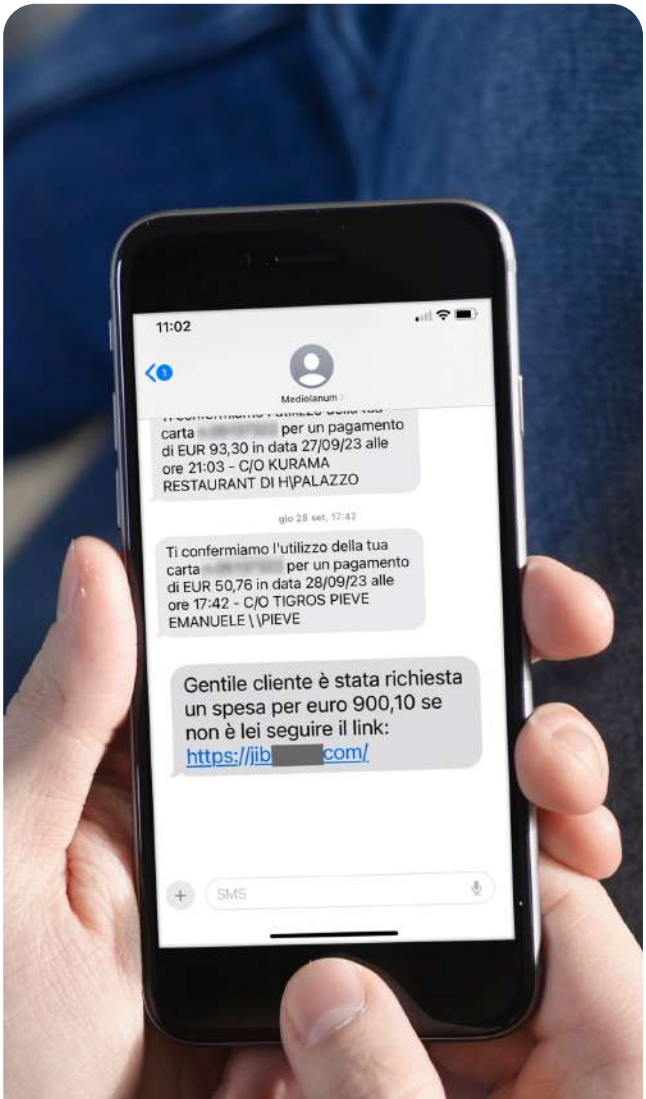
Truffa dell'EMERGENZA FAMILIARE:

Il truffatore che attua una "**Family emergency scam**", **si finge un membro della tua famiglia o un tuo amico** e potrebbe contattarti per telefono, SMS, email o social media, simulando di avere qualche tipo di problema e di **aver bisogno di soldi immediatamente, fornendo un IBAN a cui bonificare una somma.**


ORA È IL TUO TURNO,
FAI LE TUE MOSSE!

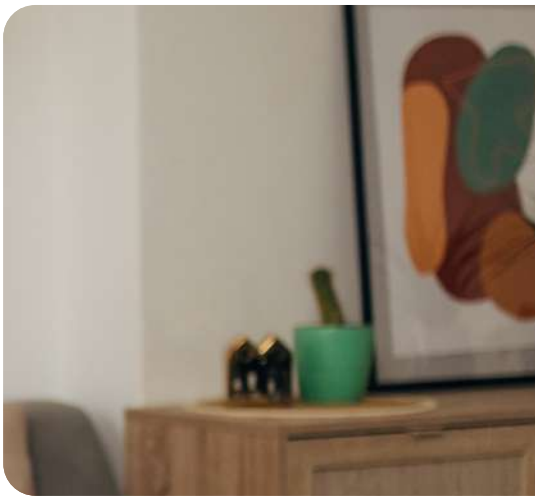
DIFENDITI DALLO SMISHING:

- I frodatori utilizzano la **scusa di un blocco sul conto, sulla carta o di un pagamento sospetto,** con il pretesto di dover effettuare una verifica di sicurezza, **invitano il cliente ad aprire con urgenza un link o a contattare un numero di telefono** non ufficiale della banca.
- **Non essere frettolosi** quando si leggono i messaggi che arrivano, prestare sempre attenzione al reale mittente e al contenuto.



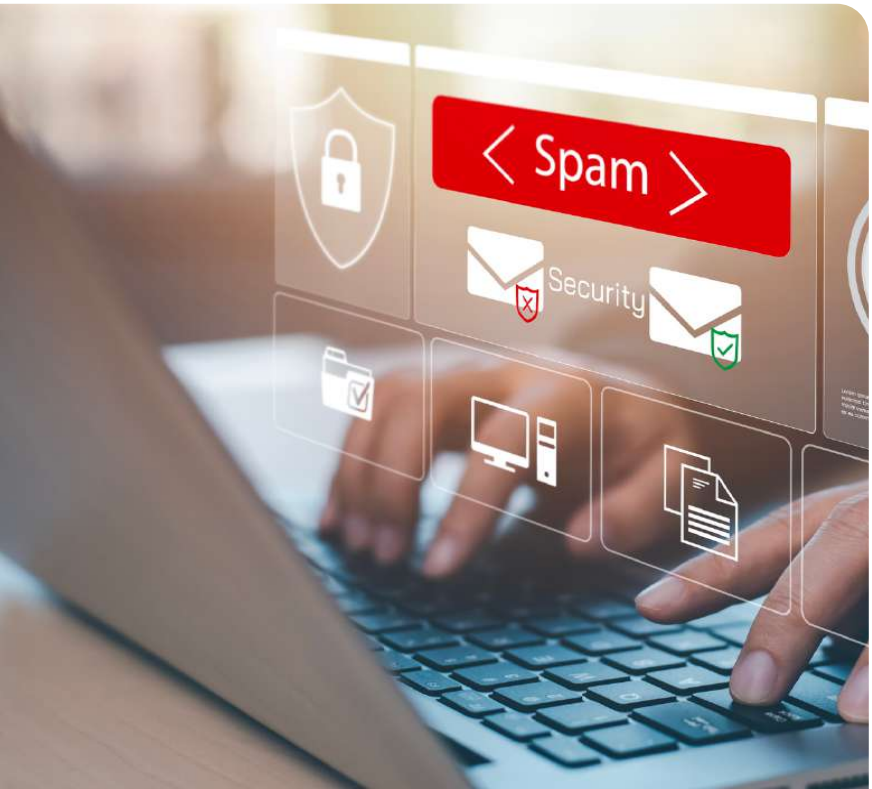
Identifica il VISHING e lo SPOOFING:

- In caso di richieste insolite, **comunicare alla persona che vi sta contattando telefonicamente che sarete voi a richiamarlo al numero verde della Banca, senza fornire alcun tipo di dato.** Una volta chiusa la telefonata, chiamare la Banca **al numero verde,** per accertare quanto accaduto.
- **Contattaci sempre e solo al numero 800.107.107.** Banca Mediolanum non ti contatterà mai dal numero 800.107.107, potrai contattarci solo tu a questo numero.
- Dal momento che molte informazioni personali possono essere reperite online (per esempio sui social network), si consiglia di **non dare credito a chi chiama soltanto perché possiede questi dati.**



Riconosci la SPINTA AL PAGAMENTO FRAUDOLENTO e la TRUFFA DELL'EMERGENZA FAMILIARE

- **Non ti chiederemo mai di effettuare un trasferimento di denaro dal tuo conto corrente e dalle tue carte o di autorizzare una notifica push relativa ad una operazione da te non richiesta**, con la scusa di bloccare un pagamento sospetto o per verifiche di sicurezza.
- Se un tuo **familiare o un conoscente** ti scrive sostenendo di avere un urgenza economica, prima di concedere il sostegno economico richiesto, **accertati che il richiedente sia reale, contattandolo e riconoscendolo tu stesso.**



TUTELA I TUOI STRUMENTI DI PAGAMENTO:

- **La carta** è personale e deve essere **custodita** con premura, **separata dal pin.**
- **Le informazioni della carta sono private, non fornire i codici delle tue carte di pagamento o i codici OTP** che la Banca ti invia per confermare le operazioni.
- **In caso di uso improprio o smarrimento procedi subito al blocco**, per tale motivo tieni sempre a portata di mano i riferimenti telefonici utili.
- **Attiva i servizi informativi SMS** per ricevere informazioni su pagamenti e prelievi effettuati con la tua carta.

NUMERI UTILI

BLOCCO CARTA DI DEBITO - circuiti BANCOMAT®/ PagoBANCOMAT®-Cirrus®/Maestro® e Fastpay - Centrale di allarme S.I.A.
dall'Italia 800.822.056
e **dall'estero 0039.02.60843768**

BLOCCO CARTE DI CREDITO e Nuova Mediolanum Debit Card- Servizio blocco carte
dall'Italia 800.15.16.16
dall'estero +39.023498.0020
e dagli Stati Uniti 1.800.4736.896

ACQUISTA ONLINE IN SICUREZZA:

- Fai attenzione a **non fare acquisti online utilizzando computer condivisi** con altre persone.
- **Utilizza credenziali diverse** per autenticarti su siti e servizi differenti.
- Ricorda di **non effettuare il salvataggio automatico delle password** sul browser.
- **Effettua sempre il logout** in uscita dal sito in cui hai avuto accesso tramite le tue credenziali.
- Quando concludi un acquisto, inserendo i dati, **assicurati di non essere osservato.**
- **Verifica sempre l'affidabilità dei venditori** a cui ti rivolgi.

Banca Mediolanum è la tua alleata.

In Banca Mediolanum puoi operare in completa **sicurezza e riservatezza** grazie all'utilizzo di un codice cliente e **3 codici segreti.**

- **Banca Mediolanum non ti contatterà mai dal numero 800.107.107**, potrai contattarci solo tu a questo numero.

- Non comunicare a nessuno **i tuoi codici segreti per intero e il codice B.med** oppure **i dati della carta di pagamento, il codice OTP di conferma operazione ed il MasterCard® Identity Check™.**

- **Contattaci sempre e solo al numero 800.107.107.** Verifica sempre la legittimità della richiesta componendo tu stesso il numero.

- **Non ti chiederemo mai di effettuare un trasferimento di denaro dal tuo conto corrente o dalle tue carte** per bloccare un pagamento sospetto o per verifiche di sicurezza.

SEMPRE AL TUO FIANCO.

Banca Mediolanum S.p.A. - Sede Legale e Direzione Palazzo Meucci,
via Ennio Doris, Milano 3 - 20079, Basiglio (MI) – T: +39 02 9049.1 -
bancamediolanum.it