COME PROTEGGERSI DAL PHISHING?

Il phishing è una tecnica di frode che si avvale di contatti telefonici o comunicazioni ingannevoli per **sottrarre dati personali particolarmente sensibili**, come credenziali di accesso ai servizi di homebanking, codici dispositivi o dati delle carte di pagamento.

Con questo obiettivo, vengono utilizzati SMS, email, messaggi WhatsApp, numeri di telefono o siti internet che simulano – per grafica e contenuto – **le comunicazioni e i canali ufficiali della banca.**

Questi tentativi di frode spesso si appellano a **situazioni di urgenza** per indurre l'utente a rilasciare velocemente le proprie informazioni personali, che vengono poi utilizzate in modo illecito.

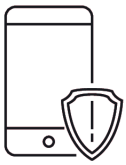
I NOSTRI CONSIGLI

Per tutelare al meglio la tua sicurezza, è essenziale essere cauti: il primo suggerimento è di **contattarci attraverso i canali ufficiali** che trovi **pubblicati su chebanca.it**, sezione Contatti, se ricevi una **richiesta** che ti sembra **anomala**.

Ricorda inoltre che:

Nessun operatore CheBanca! **ti chiamerà** mai per chiederti un'**OTP** o un **codice ricevuto via SMS**. Inoltre, non ti chiederemo mai di comunicarci, a voce o in forma scritta, Codice cliente, Codice di accesso o il PAN completo di una carta.

Quando accedi alla tua **Area Clienti**, prima di inserire i tuoi codici, è opportuno controllare l'autenticità della pagina web a cui sei collegato: l'indirizzo corretto è **clienti.chebanca.it**. Non ti invieremo mai, per SMS o email, il **link diretto** all'Area Clienti: ti consigliamo di accedervi passando sempre da chebanca.it.



Se ricevi una **notifica** che ti avvisa di una modifica al tuo profilo in CheBanca! che non hai effettuato tu (ad esempio riguardo il tuo numero di cellulare), puoi **bloccare la Strong Authentication** per impedire accessi non autorizzati alla tua posizione.
Per farlo, collegati a clienti.chebanca.it, inserisci Codice cliente e Codice di accesso e seleziona "Devi bloccare la Strong Authentication?".

Nella pagina seguente, trovi alcuni elementi a cui prestare attenzione per **riconoscere SMS fraudolenti e siti contraffatti.**

1. Il **mittente** di un SMS di phishing può apparire con il nome corretto, per mimetizzarsi tra i messaggi ufficiali della banca.
Ricorda quindi di non limitarti a questa verifica.

2. Spesso questi messaggi si appellano a presunti **problemi di accesso** al conto online, necessità di verificare la propria identità o aggiornare **credenziali in scadenza** e invitano l'utente ad agire con urgenza.

3. Solitamente viene incluso un **link diretto all'accesso online** a cui collegarsi per sbloccare o regolarizzare la propria posizione bancaria.

4. Potresti inoltre notare errori ortografici, imprecisioni o punteggiatura non corretta.

1. Se sei collegato a un sito web contraffatto, 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, ossia l'indirizzo web della pagina, potrebbe contenere il nome della banca, ma non corrisponde esattamente all'indirizzo ufficiale: **https://clienti.chebanca.it**.
La dicitura "https" è importante, perché indica che il **protocollo di sicurezza** del sito è **aggiornato**.

3. I siti web contraffatti possono essere **graficamente simil**i alla pagina di accesso online alla tua banca, ma chiederti **informazioni personali diverse dal solito**.

Per accedere alla tua **Area Clienti** CheBanca!, ti vengono richiesti **– in due passaggi diversi –** questi dati:

- Codice cliente e Codice di accesso
- Strong Authentication.