

Cos'è lo Spoofing?

La prevenzione di frodi e truffe è un impegno che Cherry Bank coltiva insieme ai propri clienti. **Una clientela informata è una clientela più sicura**: conoscere le principali minacce è il primo strumento di tutela a tua disposizione.

Tramite la tecnica dello **spoofing** i criminali falsificano il mittente di chiamate e messaggi: e-mail, SMS o numeri telefonici appaiono come se provenissero da Cherry Bank. Per questo motivo, non è sufficiente verificare il nome o il numero telefonico di chi ti sta contattando: è importante valutare cosa e come ti viene richiesto. Se nel messaggio o durante la telefonata ti vengono richieste le credenziali di accesso alla tua area riservata, i dati della tua carta di pagamento, o ti vengono segnalate operazioni di pagamento da bloccare con urgenza, diffida e non dar corso a queste richieste: è una truffa.

Esempio pratico:

Ricevi un SMS da Cherry Bank che ti invita ad “aggiornare i dati di sicurezza” cliccando su un link presente nel testo del SMS. Il messaggio presenta degli errori grammaticali e/o ortografici e compare all'interno della stessa chat dove nei giorni scorsi avevi già ricevuto altri SMS genuini da Cherry Bank. Se clicchi sul link, ti compare la schermata di accesso alla tua area riservata. Se inserisci le tue credenziali di accesso nel portale, consegnerai tali informazioni ai truffatori.

Come proteggerti:

- Non fornire mai dati o codici su richiesta via e-mail, SMS o al telefono;
- Accedi alla tua area riservata solo tramite i canali ufficiali di Cherry Bank (App e sito ufficiale).



Cos'è lo Spoofing?

Ricorda:

- Cherry Bank non ti contatta per chiederti codici personali, OTP o i dati di una carta di pagamento;
- Cherry Bank non invia e-mail, SMS o messaggi tramite altre App di messaggistica contenenti link diretti alla tua area riservata;
- Cherry Bank non ti chiede di installare software con il pretesto di darti assistenza da remoto.

Pensi che sia successo anche a te?

Non sentirti in imbarazzo, interrompi subito ogni contatto con il frodatore e segui questi consigli utili:

- Conserva una copia di tutte le chat e messaggi scambiati con il truffatore (se riesci, salva uno screenshot);
- Denuncia l'accaduto alle forze dell'ordine;
- Rivolgiti subito al tuo gestore o filiale Cherry Bank di riferimento.

