

Cos'è il Vishing?

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.

Nelle frodi con tecnica di **vishing** (voice phishing) i truffatori contattano telefonicamente la vittima fingendosi operatori antifrode, addetti alla sicurezza o personale di Cherry Bank. Possono far apparire sul display del tuo cellulare lo stesso numero del centralino di Cherry Bank o della filiale (utilizzando la tecnica di spoofing) e durante la telefonata creano un senso di urgenza per indurti a rivelare codici o autorizzare operazioni di pagamento. Tuttavia, ricorda che Cherry Bank non chiederà mai password o OTP al telefono, né ti inviterà a fare bonifici per mettere in sicurezza il tuo conto corrente.

Esempio pratico:

“Buongiorno, abbiamo rilevato accessi sospetti al suo canale internet banking. Mi fornisca le sue credenziali di accesso all'internet banking e il codice OTP appena lo riceve così da consentirmi di bloccare l'operazione”.

Se asseconi queste richieste, autorizzi inconsapevolmente una transazione che il truffatore ha già predisposto.

Come proteggerti:

- Riaggancia e contatta il numero telefonico ufficiale di Cherry Bank, indicato sul sito www.cherrybank.it nella sezione “Contatti”;
- Non comunicare mai a terzi credenziali di accesso alla tua area riservata, codici OTP, password o i dati della tua carta di pagamento.



Cos'è il Vishing?

Pensi che sia successo anche a te?

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

- Conserva uno screenshot con il dettaglio della telefonata con il truffatore (es. numero telefonico, durata della telefonata, ecc.);
- Denuncia l'accaduto alle forze dell'ordine;
- Rivolgiti subito al tuo gestore o filiale Cherry Bank di riferimento.

