

Cos'è lo Smishing?

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.

Ti è mai capitato di ricevere un SMS o un messaggio WhatsApp/messaggistica istantanea simile a questo?

“Cherry Bank: rilevato pagamento anomalo sul tuo conto corrente. Se non sei stato tu a disporlo, bloccalo subito: <https://sicurezza-cherry.it>”

Se hai ricevuto un messaggio come questo, sei stato vittima di un tentativo di **smishing**.

Il messaggio può apparire nel thread ufficiale di comunicazioni precedenti inviate da Cherry Bank. Spesso vengono utilizzati toni decisi e volti a suscitare ansia: “Pagamento sospetto”, “Conto bloccato”, “Aggiorna i dati”. Certe volte questi SMS segnalano un addebito avvenuto sul conto corrente e invitano a cliccare su link sospetti per disconoscere tali operazioni. Il link, se cliccato, conduce a una copia del sito di Cherry Bank creata appositamente per sottrarre le credenziali di accesso all'area riservata o dati della carta di debito/credito.

Come proteggerti:

- Non cliccare su link ricevuti via SMS/WhatsApp o altre App di messaggistica;
- Diffida dai messaggi che presentano errori ortografici e grammaticali;
- Non fornire mai dati personali o codici di accesso via messaggio;
- In caso di dubbio, cancella il messaggio e contatta Cherry Bank ai recapiti ufficiali che trovi su www.cherrybank.it.