EXTRABANCA
we bridge your dreams

Il Smishing

Lo **Smishing** è una forma di frode informatica che utilizza gli SMS per ingannare le vittime e indurle a fornire informazioni personali, dati bancari o credenziali di accesso.

Come avviene la frode

I messaggi di smishing si presentano spesso come comunicazioni urgenti o ufficiali provenienti da enti affidabili, come banche, corrieri o istituzioni pubbliche. L'obiettivo è spingere il destinatario a cliccare su un link malevolo o a rispondere con dati sensibili. L'SMS di solito si riferisce a:

- blocco del conto o della carta;
- attività sospette;
- richieste di aggiornamento dati;
- bonus o rimborsi da riscattare.

Il messaggio include un link che rimanda a un sito contraffatto, visivamente simile a quello ufficiale della banca. Una volta inseriti i propri dati sul sito fraudolento, questi vengono immediatamente raccolti dai truffatori, che possono utilizzarli per accedere al conto corrente, effettuare bonifici o acquisti non autorizzati.

Come difendersi dallo Smishing

Per tutelare la propria sicurezza, è fondamentale conoscere i comportamenti corretti da adottare:

❌ **Cosa NON fare:**

- Non fornire mai credenziali bancarie, PIN, codici OTP o password via SMS.
- Non cliccare sui link sospetti ricevuti tramite SMS.
- Non fidarti del numero del mittente o del nome visualizzato sul display: anche se sembra quello della banca, può essere contraffatto.

✅ **Cosa fare:**

- Segnala immediatamente se hai ricevuto un SMS fraudolento o hai inserito dati su un sito sospetto alla tua Filiale Extrabanca di riferimento o il numero 02 27727610.
- Evita di accedere a siti bancari attraverso link ricevuti via SMS. Digita sempre manualmente l'indirizzo del sito ufficiale della banca nel browser.
- Se hai cliccato su un link, verifica attentamente l'indirizzo (URL) del sito: errori ortografici, domini insoliti o assenza di protocollo "https" sono chiari segnali di truffa.

Ricorda:

Extrabanca non ti chiederà **mai**:

- Codici di sicurezza temporanei (OTP);
- Password di accesso all'online banking;
- Dati completi della tua carta di pagamento.

La sicurezza dei tuoi dati è una priorità. Mantieni sempre alta l'attenzione e, in caso di dubbio, chiedi supporto direttamente alla tua Filiale di riferimento o contattaci allo 0227727610.