

27.10.2022

# Smishing: nel mirino anche i clienti delle banche svizzere

**Fate sempre attenzione – anche con i messaggi brevi! I truffatori, infatti, sfruttano spesso anche i nomi di imprese svizzere.**

Siate scettici quando ricevete SMS, MMS, messaggi di WhatsApp o di altri sistemi di messaggistica che vi invitano ad aprire un link. Soprattutto se sembrano provenire da un noto fornitore di servizi finanziari o di spedizione.

Come dimostra l'avviso pubblicato questa settimana dalla [polizia cantonale zurigese \(https://www.cybercrimepolice.ch/de/fall/sms-zkb-access-app-voruebergehend-ingeschraenkt-ist-ein-perfider-phishingversuch/\)](https://www.cybercrimepolice.ch/de/fall/sms-zkb-access-app-voruebergehend-ingeschraenkt-ist-ein-perfider-phishingversuch/), lo smishing è tuttora un mezzo usato di frequente dai criminali per sottrarre denaro alle vittime, anche in Svizzera.

Non fate clic sui link contenuti nei messaggi brevi, ma digitate manualmente nel browser l'indirizzo noto del sito Internet dell'istituto finanziario controllando che la connessione sia sicura (https://, icona a forma di lucchetto, indirizzo di destinazione). In caso di incertezze o dubbi contattate il vostro istituto finanziario e chiedete conferma dell'invio del messaggio breve.

Ulteriori informazioni sono disponibili nel nostro articolo «[Phishing \(https://www.ebas.ch/it/phishing/\)](https://www.ebas.ch/it/phishing/)».