27.10.2022

Smishing: Auch Schweizer Bankkunden im Visier

Bleiben Sie wachsam, auch bei Textnachrichten. Denn die Namen von Schweizer Unternehmen werden gerne von Betrügern missbraucht.

Bleiben Sie skeptisch beim Erhalt von SMS oder Messenger-Nachrichten, welche Sie auffordern einen Link zu öffnen. Insbesondere wenn diese angeblich von einem bekannten Paketboten oder Finanzdienstleister stammt.

Wie die dieswöchige Meldung der Zürcher Kantonspolizei (https://www.cybercrimepolice.ch/de/fall/sms-zkb-access-app-voruebergehend-eingeschraenkt-ist-ein-perfider-phishingversuch/) zeigt, ist Smishing weiterhin ein Beliebtes Mittel von Betrügern um auch Schweizerinnen und Schweizer um ihr Geld zu bringen.

Klicken Sie also niemals auf Links in SMS-Nachrichten, sondern geben Sie die Ihnen bekannte Adresse der Website des Finanzinstituts von Hand im Browser ein und überprüfen Sie die sichere Verbindung (Schlosssymbol, Zieladresse). Kontaktieren Sie bei unerwarteten SMS-Nachrichten die Bank über die Ihnen bekannten Kontaktinformationen (z.B. offizielle Telefonnummer), und lassen Sie sich den Versand der SMS-Nachricht bestätigen.

Weitere Informationen finden Sie in unserem Artikel zu Phishing (https://www.ebas.ch/phishing/) .