27.10.2022

Smishing : les clients des banques suisses sont également dans le collimateur

Restez vigilant, notamment avec les messages courts ! Des escrocs détournent en effet parfois les noms d'entreprises suisses.

Soyez méfiants lorsque vous recevez des SMS, MMS, messages WhatsApp ou Messenger vous invitant à ouvrir des liens. Surtout si ces messages semblent provenir d'un service de transport de colis ou d'un prestataire de services financiers.

Comme le montre le communiqué de la police cantonale zurichoise (https://www.cybercrimepolice.ch/de/fall/sms-zkb-access-app-voruebergehend-eingeschraenkt-ist-ein-perfider-phishingversuch/) de cette semaine, le smishing reste très en vogue parmi les hackeurs-braqueurs qui s'intéressent à l'argent des Suisses.

Ne cliquez pas sur les liens contenus dans les SMS. Au contraire, tapez vous-même l'adresse de votre institut bancaire dans la barre d'adresse et assurez-vous qu'il s'agit d'une connexion sécurisée (https://, symbole du cadenas, adresse cible). En cas de doute ou d'incertitude, n'hésitez pas à contacter votre institut financier pour confirmer qu'il est bien à l'origine du message.

Vous trouverez d'autres informations sur le sujet dans notre article consacré au Phishing (https://www.ebas.ch/fr/le-phishing/) .