TOPCARD

TopCard Service AG
Flughofstrasse 35
8152 Glattbrugg

www.topcard.ch

Phishing

Comment détecter des e-mails, textes et appels suspects? Quelle est la meilleure façon de les contrer?

Le «phishing» est un procédé frauduleux dont le but est d'accéder à des données sensibles telles que vos numéros de cartes de crédit, vos mots de passe et les informations sur vos comptes par le biais de sites web qui, en apparence, semblent légitimes, d'e-mails, d'appels téléphoniques et de messages instantanés. Découvrez comment repérer les tentatives de vol d'informations et de fraude et la meilleure façon de les contrer.

Alerte au «phishing»: comment vous protéger

Posez-vous toujours des questions sur les contacts non sollicités

Soyez vigilant face aux e-mails, appels téléphoniques et fax non sollicités, censés provenir d'une banque, d'une société émettrice de cartes de crédit ou d'une entreprise en ligne auprès de laquelle vous êtes titulaire d'un compte. Ne divulguez jamais d'informations confidentielles si vous avez des doutes sur l'expéditeur, la personne qui appelle ou le motif de la requête. En cas de doute concernant une communication envoyée au nom de TopCard, nous vous prions de nous informer.

Face à un e-mail suspect, ne cliquez pas sur les liens et ne téléchargez pas les pièces jointes

Il est parfois difficile de distinguer un e-mail sérieux d'un e-mail de «phishing». Vérifiez si les adresses des expéditeurs ne paraissent pas suspectes, dépistez les fautes d'orthographe ou autres éléments étranges tels que la formulation des e-mails, les «disclaimers» (déni de responsabilité) et les logos. Ne cliquez pas sur les liens ou les pièces jointes si vous avez des doutes quant à l'authenticité de l'e-mail.

Ne naviguez que sur les sites web dignes de confiance

L'adresse d'un site web sécurisé commence par https://. Enregistrez dans vos favoris les adresses des sites web que vous consultez régulièrement. Ne saisissez jamais de données confidentielles dans un formulaire web si vous avez des doutes concernant la légitimité du site. Informations importantes: TopCard n'envoie jamais d'e-mails contenant des liens vers des pages de login comme celles d'E-Banking et ne demande jamais de numéro de contrat E-Banking ni de NIP.

TOPCARD

TopCard Service AG
Flughofstrasse 35
8152 Glattbrugg

www.topcard.ch

Ignorez les e-mails mentionnant une soi-disant activité inhabituelle du compte

Les e-mails de «phishing» ont souvent pour but de susciter la curiosité, la panique et d'alerter sur le caractère urgent du contenu afin de vous amener à cliquer sur un lien ou à ouvrir une pièce jointe. Il est très peu probable que des organisations dignes de confiance vous contactent par e-mail pour vous informer de paiements ou de transferts d'argent suspects effectués depuis votre compte. Supprimez ce genre d'e-mails et videz la corbeille du programme. Pensez à utiliser les filtres antispam pour bloquer ce type d'e-mails.

Mettez votre logiciel à jour

Pour bénéficier d'une protection encore plus efficace, vérifiez que votre logiciel antivirus est régulièrement mis à jour. Pensez à utiliser des filtres antispam et même un logiciel anti-«phishing» pour tenter de dépister les escrocs sur les sites web et les e-mails.