TOPCARD

TopCard Service AG
Flughofstrasse 35
8152 Glattbrugg

www.topcard.ch

Phishing

How to spot suspicious emails, text messages and calls – and the best way to deal with them

Phishing is an attempt to access your sensitive information such as credit card numbers, passwords and account information through seemingly legitimate websites, emails, telephone calls and instant messages. Find out how to spot attempted theft of information and fraud, and how to deal with it.

Beware of phishing – how to protect yourself

Always question unsolicited contact

Be alert to any unexpected email, phone call or fax that claims to be from a bank, credit card or online company with whom you have an account. Never divulge confidential information to anyone if you are unsure of the sender/caller, or the reason for the request. If you are in any doubt about a communication sent in the name of TopCard then please notify us.

If an email is suspicious, don't click on the links or download any attachments

Sometimes it can be difficult to spot a genuine email from a phishing email. Look out for an unusual sender address, spelling mistakes and strange elements such as the tone of the email, disclaimers and logos. Don't click on any links or attachments if you have any doubt about the authenticity of the email.

Only visit trustworthy websites

A secure website will start with https:// in front of the address. Bookmark any websites you frequently use to your favourites. Never input any confidential data into webforms if you are uncertain about the legitimacy of the site. Important information: TopCard never sends out emails with links to login pages such as e-banking and will never ask you for your e-banking contract number or PIN.

TopCard Service AG
Flughofstrasse 35
8152 Glattbrugg

www.topcard.ch

Ignore emails about allegedly unusual account activity

Phishing emails are often designed to incite curiosity, fear or a sense of urgency in order to get you to click a link or open an attachment. Genuine organizations are highly unlikely to contact you by email in order to tell you about suspicious payments or transfers from your account. Delete any such email and also empty the program's bin. Consider the use of spam filters to block out such emails in the future.

Keep your software up to date

To be even better protected, make sure your antivirus software is regularly updated. Consider the use of spam filters and even "antiphishing" software to help screen out potential phishers on websites and emails.