TOPCARD

TopCard Service AG
Flughofstrasse 35
8152 Glattbrugg

www.topcard.ch

Phishing

Wie Sie betrügerische E-Mails, Textnachrichten und Anrufe erkennen – und richtig reagieren

Phishing ist der Versuch auf Ihre vertraulichen Informationen wie Kreditkartennummern, Passwörter und Kontoinformationen zuzugreifen. Vermeintlich seriöse Webseiten, E-Mails, Anrufe und Sofortnachrichten dienen als Mittel zum Zweck. Erfahren Sie, wie Sie solche Informationsdiebstahl- und Betrugsversuche erkennen und wie Sie reagieren sollten.

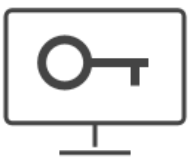
Vorsicht Phishing – so schützen Sie sich

Hinterfragen Sie jede unverlangte Kontaktaufnahme

Seien Sie auf der Hut vor unerwarteten E-Mails, Anrufen oder Faxmitteilungen. Besonders wenn Sie als Kontoinhaber einer Bank, eines Kreditkartenunternehmens oder eines Online-Anbieters kontaktiert werden. Sollte Ihnen der Absender, Anrufer oder Grund der Anfrage zweifelhaft erscheinen, geben Sie niemals vertrauliche Informationen preis. Wenn Sie im Namen von TopCard eine fragwürdige Mitteilung erhalten, teilen sie uns dies bitte mit.

Klicken Sie bei verdächtigen E-Mails nicht auf Links und öffnen Sie keine Anhänge

Es ist nicht immer einfach, eine seriöse E-Mail von einer Phishing-E-Mail zu unterscheiden. Achten Sie auf untypische Absenderadressen, Schreibfehler, Tonalität, Haftungsausschlüsse und Logos der E-Mail. Klicken Sie im Zweifelsfall nicht auf Links und öffnen Sie keine Anhänge.



Besuchen Sie nur vertrauenswürdige Webseiten

Steht https:// vor der Adresse, handelt es sich um eine sichere Webseite. Speichern Sie Webseiten, die Sie häufig besuchen, unter Ihren Favoriten. Füllen Sie niemals Webformulare mit vertraulichen Daten aus, wenn Sie Zweifel an der Vertrauenswürdigkeit der Webseite haben. Wichtig zu wissen: TopCard verschickt niemals E-Mails mit Links zu Login-Seiten wie etwa E-Banking – und wird Sie niemals nach Ihrer E-Banking-Vertragsnummer oder PINs fragen.

TOPCARD

TopCard Service AG
Flughofstrasse 35
8152 Glattbrugg

www.topcard.ch

Ignorieren Sie E-Mails über angeblich ungewöhnliche Kontobewegungen

Phishing-E-Mails wollen erreichen, dass Sie einen bestimmten Link anklicken oder Anhang öffnen. Dazu wird absichtlich Neugier, Angst oder Handlungsdruck provoziert. Vertrauenswürdige Organisationen informieren Sie hingegen kaum per E-Mail über ungewöhnliche Kontobewegungen. Löschen Sie verdächtige E-Mails und leeren Sie den Papierkorb des betreffenden Programms. Direkt abblocken können Sie E-Mails dieser Art auch mit einem Spamfilter.

Halten Sie Ihre Software auf dem neusten Stand

Aktualisieren Sie Ihr Antivirenprogramm regelmässig für noch besseren Schutz. Auch Spamfilter und sogar «Anti-Phishing»-Software helfen, Phishing Webseiten und E-Mails herauszufiltern.