Phishing, Social Engineering & Co

Ihr Geld ist in Gefahr

Phishing: E-Mails sind Spam und Betrug

Haben Sie auch eine dubiose E-Mail im Namen Ihrer Bank bekommen und wundern sich über den Inhalt? Dann haben Sie sicher eine der vielen Phishing-Nachrichten erhalten, welche derzeit im Namen der Volksbanken Raiffeisenbanken unterwegs sind. Deswegen möchten wir Sie an dieser Stelle warnen: Klicken Sie keine Links in unaufgefordert zugesendeten E-Mails an und geben Sie keine vertraulichen Daten am Telefon preis.

Phishing kann per E-Mail, SMS, Telefon sowie gefälschter Internetseiten oder sozialer Netzwerke erfolgen. Dabei versuchen Betrüger, Sie unter einem Vorwand beispielsweise dazu zu verleiten, eine Überweisung durchzuführen, Ihre girocard freizuschalten, Ihre Zugangsdaten für das Online-Banking anzugeben, Ihr TAN-Verfahren zu wechseln oder Ihre Kreditkartendaten preiszugeben. Es gibt viele Varianten – eines haben sie aber alle gemeinsam: Sie nutzen Vorwände, gefälschte Absenderadressen, Webseiten und Eingabemasken, die zum Beispiel einer Banking-Anwendung täuschend ähnlich sehen. Außerdem können Ihr PC oder das Smartphone geschädigt werden, wenn Sie sich mit diesen E-Mails Viren und Trojaner einfangen. Aufgrund der hohen Anzahl an falschen E-Mails und SMS ist es wichtig, dass Sie wachsam sind und die eingehenden Nachrichten kritisch hinterfragen, um echte Nachrichten von Spam-Mails und Fake-SMS zu unterscheiden.

Betrugsmasche: angebliche Microsoft-Mitarbeiter fordern zu Überweisungen auf

Wir warnen vor einer weiteren Betrugsmasche, bei der die Betrüger ihre Opfer unter dem Vorwand eines Schadcodebefalls oder einer abgelaufenen Lizenz anrufen und sich als Microsoft-Mitarbeiter ausgeben. Geht der Angerufene in die Falle, schalten sich die Betrüger über eine Fernwartungs-Software wie beispielsweise Teamviewer auf den Rechner des Betroffenen auf. Im Anschluss fordern sie ihr Opfer zu einer Online-Überweisung für die erbrachten Leistungen auf.

Beim Anklicken des Login-Buttons im Online-Banking wird augenscheinlich eine Bildschirmsperre am Rechner aktiv. Es erscheint der Hinweis auf eine Support-Telefonnummer. Ruft man diese an, scheint die übliche Phishing-Masche abzulaufen. Der betroffene Rechner wird ggf. gesperrt oder die Bildschirmsperre wird beispielsweise via eines sogenannten Webinjects vorgetäuscht.

Empfänger solcher Telefonanrufe sollten nicht auf die Forderungen eingehen und keinesfalls Daten oder andere Informationen weitergeben oder in dieser Kombination das Online-Banking aufrufen. Sollten Sie auf eine solche Forderung eingegangen sein, lassen Sie Ihre Karte und Ihr Online-Banking unverzüglich sperren. Bitte nehmen Sie außerdem Kontakt mit Ihrer Bank auf. Sollten Sie auf einen Link geklickt haben oder unsicher sein, ob sich bereits ein Trojaner auf Ihrem Computer befindet, lassen Sie sich bitte von einem IT-Spezialisten beraten. Der Rechner sollte genau untersucht und bis zur endgültigen Klärung beziehungsweise Beseitigung der Schadsoftware auf keinen Fall mehr für das Online-Banking genutzt werden.

Bitte seien Sie vorsichtig und fallen Sie nicht auf Betrugsmaschen herein!

Stand: Juli 2021

VR Bank
Oberfranken Mitte eG

vr-ofrm.de

Phishing, Social Engineering & Co

So handeln Sie richtig

Phishing persönlicher Daten: Betrüger versuchen, mit sogenannten Social-Engineering-Methoden an Ihre Daten zu kommen

Anstatt aufwändig Internetseiten zu bauen, die denjenigen einer Bank möglichst stark ähneln, versuchen Betrüger auf viel einfachere Art und Weise an persönliche Daten zu gelangen. Sie schicken Phishing-Mails oder starten Telefonanrufe, in denen sie die unterschiedlichsten Vorwände angeben, damit die Empfänger persönliche Daten preisgeben. Die Vorwände sind so gewählt, dass sie die Empfänger auf zwischenmenschlicher, persönlicher Ebene ansprechen. So versuchen die Betrüger, das Vertrauen der Empfänger zu gewinnen und sie zu beeinflussen. Diese Methode nennt sich Social Engineering.

Beispiele für Vorwände, mit denen Betrüger versuchen, das Vertrauen der Empfänger zu gewinnen:

- Absender gibt sich als Dienstleister aus,
- Absender gibt sich als Mitarbeiter einer Meldebehörde aus,
- Absender gibt sich als Mitarbeiter der Bundesregierung aus,
- Absender gibt sich als Bankmitarbeiter aus (Zum Beispiel sieht ein Betrugsszenario vor, dass Kunden von einem vermeintlichen Bankmitarbeiter kontaktiert und zur Initiierung mehrerer Zahlungen aufgefordert werden. Hierbei wird der Vorwand verwendet, dass man eine verdächtige Überweisung verhindert hätte und bittet nun den Bankkunden um Mithilfe. Auch das Thema Corona könnte in diesem Zusammenhang durch die Anrufer vorgeschoben werden. Schließlich verfolgen die Betrüger in allen Fällen das Ziel, den Bankkunden zur Freigabe von Aufträgen mittels TAN zu verführen.)

Empfänger von Mails oder Telefonanrufen sollten keinesfalls persönliche Daten preisgeben oder ihre Identität auf irgendeine Weise bestätigen.

So handeln Sie bei Betrugsverdacht: Karte und Online-Banking sperren, Bank kontaktieren, Anzeige bei der Polizei erstatten

Wenn Sie vermuten, dass Sie einem Betrüger zum Opfer gefallen sind, sollten Sie schnell handeln:

- **Sperren Sie Ihre Karte und/oder das Online-Banking - Sperrhotline: 0049 116 116**
- **Nehmen Sie umgehend Kontakt mit Ihrer Bank auf.**
- **Unter der folgenden kostenfreien Telefonnummer können Sie sich melden, wenn Sie einen Betrugsverdacht – zum Beispiel einen Fall von Phishing – vermuten. Ihr Anruf wird täglich in der Zeit von 8 bis 24 Uhr entgegengenommen: 0800 5053 111.**
- **Erstatten Sie bei der nächsten Polizeidienststelle eine Anzeige. In vielen Bundesländern ist dies auch online möglich.**
- **Sichern Sie Beweise: Bewahren Sie alle Dokumente wie die Phishing-Mail oder die Phishing-SMS auf.**

Bitte seien Sie vorsichtig und fallen Sie nicht auf Betrugsmaschen herein!

Stand: Juli 2021

VR Bank Oberfranken Mitte eG