Factsheet Fraud und Phishing

Erfahren Sie mehr über die perfiden und raffinierten Tricks der Online- und Telefonbetrüger.

«Social Engineering» – dieser Begriff rückt im Zusammenhang mit betrügerischer Abzocke neben dem klassischen «Phishing» immer stärker in den Fokus. Und das in ständig neuen Varianten. Was steckt dahinter? Und wie kann man sich schützen?

Die Betrüger versuchen es im wahrsten Sinne des Wortes mit allen Tricks. Da die technischen Sicherheitssysteme der Banken zuverlässig funktionieren, werden Social-Engineering-Angriffe [1]der Kriminellen immer ausgefeilter. Im Zentrum stehen Angst, Zeitdruck, Neugier oder Respekt. Die Betrüger versuchen, ihre potenziellen Opfer zu manipulieren und dazu zu bringen, Geld zu senden oder sensible Daten wie PIN, Passwörter und Konto- sowie Kartennummern preiszugeben. Mit den ergaunerten Daten lassen sich dann die Sicherheitssysteme umgehen – Stichwort «Identitätsdiebstahl» und «Account-Takeover»

Phishing

Beim Phishing wird mit gefälschten E-Mail- Nachrichten versucht, persönliche Zugangsdaten zu Konten, Kennwörtern sowie Kredit- oder Debitkartendaten «abzufischen». Phisher schicken E-Mails an viele Adressen und geben sich als vertrauenswürdige Quelle aus.

Beispiele:

- *«Ihr Konto wurde vorübergehend gesperrt», «Sie müssen Ihre Zugangsdaten aktualisieren»*
- *«Ihr Paket trifft bald ein. Zahlen Sie die Zollgebühren für die Paketzustellung.»*

Die Opfer werden aufgefordert, auf einen Link zu klicken und dort die entsprechenden Zugangsdaten einzugeben. Auf den gefälschten, aber täuschend echt aussehenden Webseiten werden diese Daten von Kriminellen abgegriffen, um diese danach betrügerisch einzusetzen. Oftmals beinhalten die «Phishing-E-Mails» auch schädliche Anhänge, die den Betrügern beim Öffnen der Anhänge weiteren Zugang zu wertvollen Daten liefern.

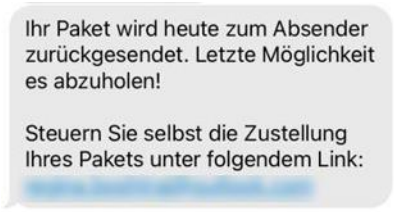
[1] Bei Social-Engineering-Angriffen werden Mitarbeiter manipuliert, damit sie den Wünschen der Betrüger nachkommen, indem sie sich oft als Chef, Lieferant oder Partner ausgeben.

Factsheet Fraud und Phishing

Mai 2023

Smishing und Vishing

Nicht alle Angriffe werden über E-Mail-Nachrichten abgewickelt. Beim **Smishing** erfolgt die Kontaktaufnahme über SMS mit der Aufforderung, einem Link zu folgen oder eine Telefonnummer anzurufen. Dabei soll beispielsweise das Konto «geprüft» werden. Der Link führt zu einer gefälschten Webseite oder zu einem Anruf bei einer Person, die sich als vermeintliches Teammitglied eines tatsächlich existierenden Unternehmens ausgibt.



Beim **Vishing** erfolgt der Kontakt über einen Telefonanruf. Die Anrufer/innen wirken sehr vertrauenswürdig und geben vor, vermeintliche (Sicherheits-) Probleme lösen zu müssen, wofür die Daten der Kunden gebraucht werden. Sie geben sich dabei als Mitarbeiter/innen eines existierenden Unternehmens aus. Auf mögliche Einwände und Zweifel reagieren sie glaubwürdig und mit verständlichen Argumenten.

Mit wenigen Regeln geschützt vor Cyberkriminellen

Die Grundregel für Ihre Kundschaft lautet: Banken, Behörden oder seriöse Firmen werden niemals darum bitten, vertrauliche Informationen weiterzugeben - weder telefonisch noch digital! Ausnahme bildet die Registration im E-Banking und der debiX+ App.

Der beste Schutz: Ruhe und Skepsis

Druck bringt in diesen Situationen nichts - daher ruhig bleiben! Bewahren Sie sich eine gesunde Skepsis, auf allen Kommunikationskanälen, vor allem bei Nachrichten oder Anrufen von Unbekannten. Vergewissern Sie sich im Zweifel bei der genannten Firma. Rufen Sie zurück. Nutzen Sie dazu die offizielle oder Ihnen bereits bekannte Telefonnummer (z.B. die 24/7 Debit Helpline auf der Rückseite der Debit Mastercard).

Den Überblick behalten und notfalls schnell reagieren

Kontrollieren Sie regelmässig die Abbuchungen auf Ihrem Bank- und Kreditkartenkonto. Sollten Sie persönliche Daten weitergegeben haben, sperren Sie umgehend den E-Banking-Zugang und die Karten bei Ihrer Bank. Neue Warnmeldungen werden regelmässig auf der Website von card-security.ch veröffentlicht – schauen Sie vorbei.

Factsheet Fraud und Phishing

Mai 2023

So schützen wir uns vor Cyberkriminalität:

Debit Mastercard / PIN-Code

- ✓ Kartendaten keiner Drittperson weitergeben
- ✓ Offensichtliche Zahlenkombinationen als PIN vermeiden
- ✓ Karteninformationen auf Webseiten nicht abspeichern
- ✓ PIN immer verdeckt eingeben
- ✓ PIN nirgends notieren
- ✓ Banken erfragen nie die PIN der Karte
- ✓ Banken erfragen nie Kartendaten per E-Mail oder SMS
- ✓ Zahlungen mittels 3D-Secure (debiX+ App) nur freigeben, wenn die Zahlung selbst getätigt wurde

E-Banking / Mobilebanking

- ✓ Vertrags-/Zugangsdaten keiner Drittperson weitergeben
- ✓ Schwierige Passwörter nutzen (Beispiel unsicheres Passwort: Regina2001. (Vorname und Geburtsjahr)

Betrugsmaschen erkennen

- ✓ Keine Links oder Anhänge von unbekannten Mailadressen öffnen (gilt auch bei SMS oder WhatsApp)
- ✓ Mailadresse des Absenders überprüfen
- ✓ Nur vertrauenswürdige Webseiten nutzen

Verdacht auf Missbrauch, Verlust oder Diebstahl

Schöpfen Sie einen Verdacht auf Missbrauch, Verlust oder Diebstahl, so muss sofort gehandelt werden:

Debit Mastercard

- ✓ Karte im E-Banking / Mobile Banking / debiX+ App sperren
- ✓ Karte bei Bank sperren lassen
- ✓ Bank kontaktieren - Bank bestellt komplett neue Karte (neue Karten-Nummer)
- ✓ Anzeige bei der Polizei erstatten

E-Banking

- ✓ Helpline kontaktieren und sperren lassen
- ✓ Bank kontaktieren - Bank erstellt neuen E-Banking Vertrag

Nützliche Links / Kontakte

Card-security.ch: Sicher mit der Karte bezahlen.

«eBanking – aber sicher!» (ebas.ch)

0800 850 019 (Helpline E-Banking)

+41 55 645 35 59 (Helpline DMC)