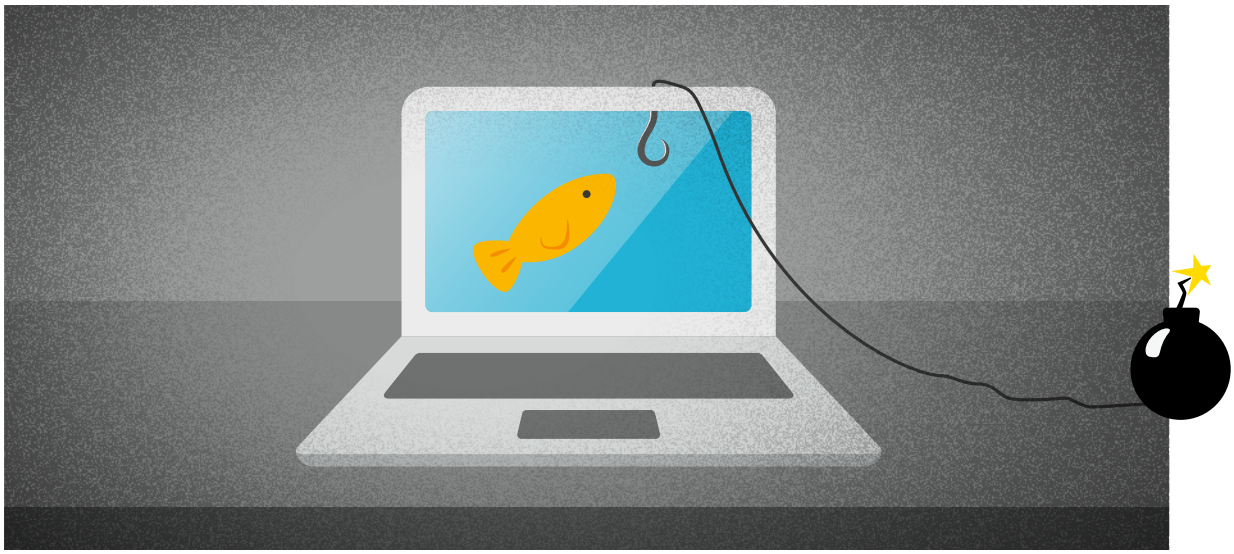
Reden wir über Geld

ÜBER GELD SPRICHT MAN NICHT? ... SOLLTEN WIR ABER!

Phishing

Banken versenden keine Links zu Webseiten, auf denen Sie Ihre persönlichen Kontodaten und Passwörter eingeben sollen!



Was ist Phishing?

»Phishing« setzt sich aus den Wörtern »Passwort« und »fishing« (Fischerei) zusammen. Es wird nach Passwörtern und persönlichen Informationen gefischt, indem Kriminelle Ihnen per E-Mail einen Link senden, den Sie öffnen und wo Sie Ihre Bank- oder Kreditkartendaten eingeben sollen. Layout und Design sehen dem Ihrer Bank zum Verwechseln ähnlich. Wenn Sie Ihre Daten eingeben, geben Sie den Zugriff auf Ihr Konto und damit auf Ihr Geld frei. Auch per SMS (Smishing) und Telefonanruf (Vishing) wird nach Ihren Daten gefischt.

Wie erkennen Sie Phishing-Nachrichten?

Phishing Mails gaukeln vor, von Ihrer Bank zu stammen, und enthalten eine überzeugende Begründung, warum Sie Ihre Zugangsdaten eingeben sollen.

- Die Anrede ist unpersönlich, da die Nachrichten an eine große Zahl von Menschen versendet werden. Ihre Bank spricht Sie mit Ihrem Namen an.
- Fehlerhafte Rechtschreibung und Grammatik können ein starkes Indiz sein.
- Unter Androhung von Konsequenzen wie Gebühren und Sperren werden Sie dringend aufgefordert, persönliche Daten preiszugeben.

Wie können Sie sich schützen?

- Seien Sie vorsichtig bei E-Mails und SMS-Nachrichten! Klicken Sie niemals auf Links in einer verdächtigen Nachricht, und laden Sie keine Anhänge herunter.
- Vergleichen Sie die E-Mail-Adresse des Absenders und die Website-URL genau mit jenen Ihrer Bank!
  Oft ändern Betrüger nur ein Zeichen oder fügen ein Präfix wie »Info-« hinzu.
- Versenden Sie niemals Ihre Kontodaten und Passwörter per E-Mail, und geben Sie diese auch nicht auf verdächtigen Websites ein.
- Kontrollieren Sie regelmäßig Ihren Kontostand sowie Ihre Umsätze. So können Sie bei missbräuchlichen Abbuchungen schneller reagieren.
- Schauen Sie auf die Webseite Ihrer Bank, ob bereits Warnungen veröffentlicht wurden.
- Im Zweifel fragen Sie am besten immer telefonisch bei Ihrem Finanzdienstleister nach.

Was tun, wenn Sie Opfer geworden sind?

- Kontaktieren und informieren Sie sofort Ihre Bank bzw. Ihr Kreditkarteninstitut.
- Möglicherweise müssen Sie Konto und Karte sperren lassen.
- Ändern Sie Ihre Passwörter und verwenden Sie einen Passwort-Manager, um sichere Passwörter zu generieren und zu verwalten.
- Achtung vor »Nachschussbetrug«!
  Oft kontaktieren die Kriminellen Sie ein weiteres Mal und fordern weitere Zahlungen.

Watchlist Internet
Sie können Phishing-Nachrichten an die Watchlist Internet melden. Auf der Webseite www.watchlist-internet.at wird unter »Unseriöse Webseiten« eine Liste von Phishing-Warnungen veröffentlicht und laufend ergänzt.

Neben dem Finanzdienstleistungsbereich sind folgende Branchen häufig betroffen:

- Onlineshops
- Soziale Medien
- IT-Firmen
- Telekommunikationsunternehmen
- Lieferfirmen

⟶ weitere Ausgaben

→ 14 Authority Scam
→ 13 Sicher online zahlen
→ 19 Strukturvertrieb
redenwiruebergeld.fma.gv.at

⟶ Finanz ABC

Auf unserer Website finden Sie wichtige Basisinformationen:
www.fma.gv.at ▸ Finanz ABC ▸ Finanzbetrüger erkennen

IMPRESSUM:
Finanzmarktaufsichtsbehörde (FMA)
Otto-Wagner-Platz 5
1090 Wien
Tel.: +43 1 249 59 0
Fax: +43 1 249 59 5499
E-Mail: fma@fma.gv.at