

# BANK PHISHING E-MAILS

Phishing bezeichnet betrügerische E-Mails, die die Empfänger dazu verleiten, persönliche, finanzielle oder sicherheitsrelevante Informationen preiszugeben.

## WIE FUNKTIONIERT ES?

Diese E-Mails:

können identisch **aussehen** wie die Korrespondenz Ihrer aktuellen Bank.

**kopieren** Logos, Layout und Tonfall echter E-Mails.



**verlangen** das Öffnen eines Anhangs oder das Klicken auf einen Link.



**vermitteln** das Gefühl von Dringlichkeit.

## WAS KÖNNEN SIE TUN?

- **Halten Sie Ihre Software auf dem neusten Stand**, inklusive Browser, Antivirusprogramm und Betriebssystem.
- Seien Sie speziell **wachsam**, wenn eine 'Bank' sensitive Informationen von Ihnen verlangt (z.B. Ihr E-Banking Passwort).
- **Schauen Sie die E-Mail genau an**: Vergleichen Sie die Adresse mit früheren echten Nachrichten Ihrer Bank. Achten Sie auf Schreibfehler und Grammatik.
- **Beantworten Sie verdächtige E-Mails nicht**, leiten Sie diese vielmehr unter manueller Eingabe der Adresse an die Bank weiter.
- **Klicken Sie nicht auf den Link oder öffnen Sie den Anhang nicht**, geben Sie die Adresse manuell im Browser ein.
- Im Zweifelsfall **schauen** Sie auf der Webseite Ihrer Bank nach oder rufen Sie Ihre Bank an.



Cyberkriminelle bauen darauf, dass die Menschen vielbeschäftigt sind; oberflächlich sehen diese gefälschten E-Mails echt aus.



Aufgepasst bei mobilen Geräten! Es kann schwieriger sein, einen Phishing-Versuch auf Ihrem Mobiltelefon oder Tablet zu erkennen.

#CyberScams

