Online-Sicherheit

Betrüger setzen zunehmend raffinierte Techniken ein, um über das Internet, Telefonanrufe und modernste Technologien an Ihr Geld zu gelangen. Wir informieren Sie über die diversen Betrugsmaschen, damit Sie sich bestmöglich selber schützen können. Bleiben Sie aufmerksam und wachsam.

Betrügerische E-Mail und SMS

Betrügerische Mail und SMS-Nachricht, in welcher die Kunden aufgefordert werden, ihre persönlichen Daten per Link zu bestätigen.

Wie erkenne ich eine betrügerische Mail oder betrügerische SMS?
// Es fehlt meistens die persönliche Anrede.
// Die E-Mail enthält Rechtschreibfehler, seltsamer Satzbau, und einen schlechten Schreibstil.
// Drohungen und gesetzte Fristen suggerieren bei den Kunden einem dringenden Handlungsbedarf.
// Aufforderung persönliche Daten einzugeben.
// Direkte Aufforderung das Anhänge oder Links angeklickt werden sollen.

Wie gehe ich damit um?

// Löschen Sie die Mail oder SMS sofort.
// Klicken Sie keine Links an und öffnen Sie auch nicht die Anhänge!
// Füllen Sie die enthaltenden Formularfelder nicht aus.

WhatsApp Betrug „Hallo Mama, hallo Papa ...“

Die betrügerischen Absender geben sich dabei als Kind der jeweiligen WhatsApp-Empfänger aus und versuchen diese zu Zahlungen zu animieren.

Wie erkenne ich einen WhatsApp-Betrug?
// Die Nachricht ist unaufgefordert und stammt von einer unbekannten Nummer.
// Es wird ein Gefühl der Dringlichkeit vermittelt.
// Es wird um Geld oder persönliche Daten gebeten.
// Die Nachricht enthält verdächtige Links oder Anhänge.

Wie gehe ich damit um?

// Rufen Sie Ihre Tochter oder Sohn unter der gewöhnlichen Telefonnummer an, um die Behauptung zu überprüfen.
// Seien Sie misstrauisch, wenn Sie per WhatsApp zu Geldzahlungen gedrängt werden.

Telefonbetrug

Betrüger rufen mit der angeblichen Nummer der Bank oder der Verbundpartner an und geben sich als Mitarbeiter aus.

Wie erkenne ich einen Telefonbetrug?
// Anrufer gibt sich oft als Sicherheitsbeauftragter der Bank aus und will persönliche Daten abfragen (TAN-Nummern, Passwörter, etc.).
// Vermeintlicher Bankmitarbeiter teilt dem Kunden mit, dass er sich aus verschiedensten Gründen authentifizieren soll.
// Häufig wird auf den Kunden Druck ausgeübt.

Wie gehe ich damit um?

// Bestätigen Sie keine Aufträge, welche Sie im Online Banking nicht selbst in Auftrag gegeben haben.
// Geben Sie keine Kreditkartendaten, Debitkartennummer, TAN-Nummern oder Passwörter am Telefon preis – auch nicht gegenüber den bekannten Bankberater. Banken fragen niemals nach diesen vertraulichen Informationen.
// Rufen Sie die eigene Hausbank unter einer zentralen Rufnummer zurück.
// Lassen Sie sich nicht unter Druck setzen. Beenden Sie das Gespräch direkt.

Microsoft-Betrug

„Darf ich mich kurz aufschalten?“
Kunden werden dazu gebracht ein Programm (z.B. Team Viewer, Chrome Remote Desktop) zu installieren, mit dem die Betrüger auf den Computer zugreifen und diesen komplett steuern können.

Wie erkenne ich einen Microsoft-Betrug?
// Der PC-Nutzer erhält zunächst eine Viruswarnung, die dazu auffordert, eine gefälschte Kundendienstnummer des Windows-Herstellers anzurufen.

Wie gehe ich damit um?

// Beenden Sie die Gespräche sofort.
// Lassen Sie Keine Fernwartungssoftware installieren.
// Sollte ein Zugriff erfolgt sein, trennen Sie sofort das Endgerät vom Internet.

FakeShop

Fakeshops bieten teure Ware für sehr günstige Preise an. Die Bezahlart ist stark eingeschränkt, meist nur gegen Vorkasse möglich.

Wie erkenne ich einen Fake-Shop?
// Unvollständiges oder fehlerhaftes Impressum.
// Vermehrte Rechtschreibfehler oder die Texte sind in einem schlechten Deutsch verfasst.
// Eine fehlende Hotline oder keinerlei Kontaktmöglichkeiten sind über die Shop-Seite aufzufinden.
// Werden nur Bezahlmöglichkeiten wie PayPal/Klarna etc. angeboten, bitte sehr genau hinschauen und überprüfen.
// Sehr günstige Angebote im Vergleich zu anderen Anbietern.

Wie gehe ich damit um?

// Informieren Sie sich vorher im Netz immer über den betreffenden Shop.
// Nutzen Sie zur Überprüfung der Shopseite Kundenbewertungen außerhalb der Shopseite, etwa Google Rezensionen etc.
// Bei Online-Einkäufen sollten nur die bekannten Bezahldienste oder der Kauf auf Rechnung genutzt werden.

Ebay-Betrug

Der Kunde bietet etwas über Kleinanzeigen oder einen Second-Hand-Shop zum Verkauf an und dann werden Daten abgegriffen.

Wie erkenne ich einen Ebay-Betrug?
// Kriminelle melden sich beim Anbieter und geben an, diesen Artikel kaufen zu wollen.
// Geht es ums Bezahlen, schlagen die Käufer die Möglichkeit „sicher Bezahlen“ von eBay Kleinanzeigen vor. Alle anderen Bezahlmethoden werden mit plausiblen Gründen ausgeschlagen.
// Im Betrugsfall erhält der Kunde jedoch für den Abruf des Kaufpreises einen Link. Auf diesen Link sollen lediglich seine Zugangs- oder Kreditkartendaten angeben werden.
// Nach der anschließenden Freigabe mit der Banking App oder eine TAN wird dem Kunden die Gutschrift versprochen.

Wie gehe ich damit um?

// Starten Sie niemals die Zahlung oder das Banking aus einem Link heraus – egal ob dieser per Mail, App oder einen anderen Kanal heraus gesendet wurde.
// Nutzen Sie immer die offizielle App oder starten Sie die Zahlung direkt auf der Website des Zahlungsanbieters.

Erste Hilfe-Checkliste (Checkliste auf unserer Homepage)

1. Online-Banking sperren – Sperr-Nummer +49 116 116
2. Volksbank im Münsterland eG über das Kontaktformular oder telefonisch kontaktieren
3. ggf. Anmeldenamen und Passwörter von weiteren Accounts ändern
4. Den PC (System) auf Schadsoftware untersuchen
5. Anzeige bei der Polizei erstatten