Cybercrime und Betrug

Die Täter zielen auf den Menschen, nicht auf die Technik. Wer die Betrugsmaschen kennt, erkennt die Gefahr im entscheidenden Moment!

Fälschungen mit künstlicher Intelligenz: Stimmen, Gesichter und Texte wirken heute täuschend echt. Selbst Fachleute erkennen den Unterschied kaum noch.

1 Die häufigsten Betrugsmaschen

Phishing – die Betrugsmasche mit den vielen Formen

Phishing ist der Versuch, unter falscher, vertrauenswürdig wirkender Identität an fremde Zugangsdaten zu gelangen; also an Login, Passwort oder Bestätigungscode und damit an das E-Banking oder die Kreditkarte. Klassisch per E-Mail oder SMS mit Links auf gefälschte Bank- oder Paketdienstseiten. Verbreitet ist auch der Anruf eines falschen Bankmitarbeiters, der eine verdächtige Transaktion meldet und per Fernwartung «helfen» will; dabei erlangt er Zugriff auf Gerät und Login, oft mit gefälschter Rufnummer im Display (Call-ID-Spoofing). Die meisten Betrugsmaschen bauen auf diesem Abgreifen von Zugangsdaten auf.

Ausspähen & Kartendiebstahl

Ob am Automaten, an der Kasse oder im Gedränge: Die Täter spähen zuerst den PIN aus, entwenden dann die Karte und setzen sie rasch ein. Eng verwandt mit digitalem Phishing. Auch hier gilt: zuerst die Daten, dann der Zugriff.

Marktplatz- & Kaufbetrug

Ob gefälschter Bezahl- oder Lieferlink: Auf Kleinanzeigen wie Ricardo oder Tutti treten Betrüger oft als Käufer auf und leiten über einen Link oder einen QR-Code auf eine Phishingseite. Wer glaubt, die Zahlung zu empfangen, gibt in Wahrheit seine Zugangsdaten preis.

Anlagebetrug

Ob gefälschte Trading- oder Kryptoplattform: Kleine Scheingewinne wecken anfangs Vertrauen. Sobald man aber die Gewinne realisieren will, folgen Sperre und Gebührenforderungen, und das Geld ist weg.

Emotionale Manipulation

Ob vorgetäuschte Liebe beim Romance Scam oder der Schock- und Enkeltrickanruf mit einem angeblichen Notfall in der Familie: Die Täter erzeugen starke Gefühle und Zeitdruck, damit das Opfer unüberlegt zahlt.

Vorschuss- und Rückholbetrug (Recovery Scam)

Vor einer Auszahlung wird immer eine «Gebühr» fällig – und nach der Zahlung die nächste. Besonders perfid: Betrugsopfer werden erneut kontaktiert, angeblich um das Geld zurückzuholen, und verlieren so ein zweites Mal.

2 Woran man Betrug erkennt

- **Zeitdruck und künstliche Dringlichkeit:** Etwas müsse sofort bestätigt, gezahlt oder freigegeben werden, damit man nicht in Ruhe nachdenkt; seriöse Stellen lassen immer Zeit zum Prüfen.
- **Angebote, die zu gut sind, um wahr zu sein:** aussergewöhnlich hohe Gewinne, Rabatte oder Renditen ohne erkennbares Risiko.
- **Versprechen, online schnell und einfach Geld zu verdienen:** vermeintlich müheloser Nebenverdienst oder Jobangebote, bei denen man nur sein Konto oder etwas Zeit zur Verfügung stellen soll.
- **Aufforderung, Passwort oder Bestätigungscode herauszugeben:** eine Bank oder Behörde fragt nie danach, weder am Telefon noch per E-Mail oder SMS.
- **Unerwartete Links und QR-Codes:** eine nur beinahe stimmige Absender- oder Webadresse, Nachrichten zu einer angeblichen Sendung, Rechnung oder Kontosperre.
- **Aufforderung, das E-Banking über einen zugestellten Link oder QR-Code zu öffnen:** die Bank verlinkt den Login nie per E-Mail oder SMS; der Zugang erfolgt ausschliesslich über die selbst eingetippte Adresse, ein eigenes Lesezeichen oder die offizielle App.
- **Bitte, eine Software zu installieren:** angebliche Fernwartung oder eine App, mit der Fremde Zugriff auf Gerät oder E-Banking erhalten.

3 So schützt man sich

- **Zugangsdaten sauber verwalten:** für E-Banking und wichtige Konten je ein eigenes, starkes Passwort, am besten über einen Passwortmanager; Passwörter nie mehrfach verwenden oder offen notieren.
- **Zwei-Faktor-Authentisierung nutzen und jede Freigabe (auch neue Geräte) prüfen:** Zweck, Empfänger und Betrag bewusst lesen, bevor man bestätigt, denn ein Code gilt immer für genau eine bestimmte Transaktion.
- **Den Kontaktkanal selbst wählen:** Bei Anrufen, SMS oder E-Mails nicht auf mitgelieferte Kontaktangaben reagieren, sondern die Bank über die offizielle Nummer kontaktieren.
- **Geräte und Programme aktuell halten:** Betriebssystem, Browser und Banking-App regelmässig aktualisieren und Sicherheitsupdates nicht aufschieben.
- **Karte und PIN physisch schützen:** den PIN nie notieren oder weitergeben, bei der Eingabe die Tastatur mit der Hand abdecken und die Karte nie aus der Hand geben.
- **Beschränkungen, Limiten und Benachrichtigungen einrichten:** Zahlungs- und Bargeldlimiten massvoll halten und Transaktionen beschränken oder eine Push- oder SMS-Benachrichtigung aktivieren, damit Missbrauch auffällt.
- **Konto und Abrechnungen regelmässig kontrollieren:** Kontobewegungen und Kartenabrechnungen zeitnah durchsehen und Unstimmigkeiten umgehend der Bank melden.

4 Was tun im Schadenfall?

A

Sofort die Bank informieren und Zugang/Karte sperren. Alternativ: Passwort absichtlich dreimal falsch eingeben oder Karte in der App sperren.

B

Beweise sichern (Nachrichten, Screenshots, Zahlungsbelege) und **Anzeige bei der Polizei** oder Staatsanwaltschaft erstatten.

C

Vorfall melden dem Bundesamt für Cybersicherheit (BACS); verdächtige Seiten über antiphishing.ch.

5 Wer trägt den Schaden?

In der Schweiz beurteilt sich die Haftung für missbräuchliche Transaktionen nach der Risikosphärentheorie, konkretisiert in den Bank-AGB: Kunde und Bank tragen jeweils die Risiken, die sie selber kontrollieren können. Wurden Transaktionen mit korrekten Zugangsdaten durchgeführt, haftet in der Regel der Kunde, da die Legitimationsmittel aus seiner Sphäre zu den Betrügern gelangt sein müssen. Eine (anteilige) Bankhaftung bleibt die Ausnahme. **Prävention ist daher entscheidend.**