Auflegen. Nicht klicken. Nachfragen.

Ihr Merkblatt gegen Telefonbetrug, Phishing und falsche Nachrichten

Die fünf wichtigsten Schutzregeln

1 AUFLEGEN
Jemand fordert am Telefon Geld, Schmuck oder eine sofortige Zahlung? Gespräch beenden.

2 NIE WEITERGEBEN
PIN, Passwörter und SMS- oder Sicherheitscodes bleiben geheim.

3 NICHT KLICKEN
Keine unerwarteten Links in E-Mails, SMS oder Chats öffnen.

4 SELBST PRÜFEN
Banking-App, Kundenkonto oder offizielle Website selbst öffnen. Bekannte Nummer selbst wählen.

5 FRAGEN STATT HANDELN
Bei Unsicherheit eine vertraute Person einbeziehen. Lassen Sie sich nicht drängen.

So erkennen Sie das Muster

Unerwarteter Kontakt → starke Gefühle → Zeitdruck → Forderung.

Betrüger machen Angst, wecken Sorge oder locken mit einer Belohnung. Am Ende wollen sie Geld, Daten, einen Sicherheitscode oder einen Klick.

Besonders wichtig am Telefon

Die echte Polizei holt niemals Geld oder Schmuck bei Ihnen ab. Auch die angezeigte Telefonnummer kann gefälscht sein. Legen Sie auf und wählen Sie selbst eine bekannte Nummer.

Im Zweifel: stoppen und selbst prüfen.

Sie müssen nicht jede Betrugsmasche erkennen. Entscheidend ist, wie Sie reagieren.

Typische Situationen – der sichere Weg

«Ihr Kind hatte einen Unfall. Zahlen Sie sofort!»
Auflegen. Angehörige über eine bekannte Nummer selbst kontaktieren.

«Hallo Mama, neue Nummer. Bitte Rechnung bezahlen.»
Nicht über die neue Chatnummer prüfen. Angehörige selbst oder über weitere Familienmitglieder erreichen.

«Ihr Bankkonto wird gesperrt.»
Nicht auf den Link klicken und keine Codes nennen. Banking-App selbst öffnen oder Bank über bekannte Nummer kontaktieren.

«Ihr Paket konnte nicht zugestellt werden.»
Nicht den SMS-Link verwenden. Paketdienst-App oder offizielle Website selbst öffnen.

«Ihr Computer ist gefährdet. Wir helfen Ihnen.»
Unerwarteten Anrufern keinen Fernzugriff auf Computer oder Handy erlauben.

Wenn bereits etwas passiert ist

1. Sofort stoppen: Keine weiteren Zahlungen, Angaben oder Klicks.

2. Bank kontaktieren: Bei Überweisungen oder preisgegebenen Kartendaten sofort die Bank informieren und notwendige Sperren veranlassen.

3. Zugang sichern: Weitergegebene Passwörter umgehend über einen vertrauenswürdigen Weg ändern. Bei gewährtem Fernzugriff die Verbindung beenden und fachliche Hilfe holen.

4. Beweise sichern: Nachrichten, Telefonnummern, Screenshots und Zahlungsbelege aufbewahren.

5. Polizei kontaktieren: Betrugsfall melden. Bei einer akuten Gefahr oder bevorstehenden Geldübergabe 117 wählen.

Auch Angehörige und Freunde können helfen

Nehmen Sie Sorgen ernst, prüfen Sie gemeinsam und machen Sie keine Vorwürfe. Ein guter Satz ist: «Gut, dass du es mir zeigst. Wir schauen das gemeinsam an.»

Merksatz: Je grösser der Druck, desto wichtiger die Pause.

Präventionsreferat · Telefonbetrug und Phishing · Kantonspolizei Zürich – Prävention