

So schützen Sie Ihren Betrieb vor Betrug.

Betrug gegen Schweizer KMU folgt fast immer demselben Muster: Druck, eine Zahlung oder ein Code, und ein Absender, der echt aussieht. Wer kurz anhält und über die bekannte Nummer selbst zurückruft, stoppt die meisten Versuche.

Sieben Regeln

- **1. Nie Passwörter, Codes oder Kartendaten weitergeben**
Keine Bank, keine Behörde, keine Polizei und auch wir fragen Sie am Telefon, per SMS oder per E-Mail nach Passwort, Einmalcode oder Kartennummer. Wer danach fragt, ist ein Betrüger.
- **2. Bankverbindung nie wegen einer Nachricht ändern**
Schreibt ein Lieferant, sein Konto habe geändert, rufen Sie ihn über die Nummer an, die Sie schon kennen, nicht über die in der Nachricht. Erst dann zahlen Sie.
- **3. Dringend plus Zahlung heisst: anhalten**
«Sofort», «vertraulich», «ich bin gerade in einer Sitzung»: Druck ist das Werkzeug der Betrüger. Eine echte Zahlung hält zehn Minuten Rückfrage aus.
- **4. Selbst zurückrufen**
Legen Sie auf und rufen Sie die Firma über die offizielle Nummer an, die auf Ihrer Karte, Rechnung oder Website steht. Die angezeigte Nummer kann gefälscht sein.
- **5. Nicht klicken, selbst eintippen**
Links in SMS und E-Mails führen oft auf täuschend echte Login-Seiten. Tippen Sie die Adresse Ihrer Bank oder der Post selbst ein, oder nehmen Sie die App.
- **6. Niemandem Fernzugriff geben**
Programme wie AnyDesk oder TeamViewer installieren Sie nur für jemanden, den Sie selbst angerufen haben und kennen.
- **7. Vier Augen bei Geld**
Neue Empfänger und grössere Zahlungen gibt eine zweite Person frei. Reden Sie im Team über Betrug, besonders mit neuen Mitarbeitenden.

Fünf Maschen aus der Schweiz

- **Der falsche Bankanruf**
Eine «Sicherheitsabteilung» meldet verdächtige Zahlungen und will, dass Sie Geld abheben, Daten nennen oder eine Fernwartung installieren. Die Kantonspolizeien St. Gallen und Graubünden haben 2026 mehrfach davor gewarnt.
- **CEO-Betrug**
Eine E-Mail «vom Chef» verlangt eine dringende, vertrauliche Überweisung oder Geschenkkarten. Dem Bundesamt für Cybersicherheit BACS wurden 2025 971 Fälle gemeldet, nach 719 im Jahr davor. Inzwischen auch mit einer KI-Stimme am Telefon.
- **Die gefälschte Rechnung**
Eine echte Rechnung kommt nochmals, nur mit neuer IBAN und passendem QR-Code, oft aus dem gehackten Postfach eines Lieferanten.
- **Der falsche Paketbote**
Per SMS, E-Mail oder sogar als gelber Zettel im Briefkasten: Ein Paket warte auf eine kleine Gebühr. Wer zahlt, gibt seine Kartendaten preis; kurz darauf ruft oft eine falsche Bank an.
- **«Ihre Domain läuft ab»**
Eine «Registrierungsstelle» droht, Ihre Domain werde gelöscht oder jemand anderes registriere Ihren Namen, und verlangt eine Zahlung. Ihre Domain verlängern Sie nur bei Ihrem bekannten Anbieter.

Wenn es schon passiert ist

- **Sofort die Bank anrufen**
Über die offizielle Nummer. Eine Zahlung lässt sich manchmal noch stoppen. Sind Kartendaten weg, lassen Sie die Karte sperren.
- **Melden und anzeigen**
Melden Sie den Versuch beim Bundesamt für Cybersicherheit BACS. Bei einem Schaden erstatten Sie Anzeige bei der Polizei, im Notfall unter 117.
- **Passwörter ändern**
Haben Sie ein Passwort genannt oder eine Fernwartung installiert, ändern Sie Ihre Passwörter und lassen Sie das Gerät prüfen.