

How to protect your business from fraud.

Fraud against Swiss small businesses almost always follows the same pattern: pressure, a payment or a code, and a sender who looks genuine. Pausing for a moment and calling back on the known number stops most attempts.

Seven rules

- **1. Never give out passwords, codes or card details**
No bank, no authority, no police and not us either will ask you for a password, one-time code or card number by phone, text or e-mail. Whoever asks is a scammer.
- **2. Never change bank details because of a message**
If a supplier writes that their account has changed, call them on the number you already know, not the one in the message. Only then pay.
- **3. Urgent plus payment means: stop**
«Right away», «confidential», «I'm in a meeting»: pressure is the scammer's tool. A genuine payment can wait ten minutes for a call back.
- **4. Call back yourself**
Hang up and call the company on the official number on your card, invoice or website. The number shown on your phone can be faked.
- **5. Don't click, type it yourself**
Links in texts and e-mails often lead to convincing fake login pages. Type the address of your bank or Swiss Post yourself, or use the app.
- **6. Never give anyone remote access**
Install programs such as AnyDesk or TeamViewer only for someone you called yourself and know.
- **7. Four eyes on money**
New payees and larger payments are approved by a second person. Talk about fraud in your team, especially with new staff.

Five scams from Switzerland

- **The fake bank call**
A «security department» reports suspicious payments and wants you to withdraw cash, give details or install remote support. The cantonal police of St. Gallen and Graubünden warned about it several times in 2026.
- **CEO fraud**
An e-mail «from the boss» asks for an urgent, confidential transfer or gift cards. The Federal Office for Cyber Security (BACS) received 971 reports in 2025, after 719 the year before. Now also with an AI-cloned voice on the phone.
- **The fake invoice**
A real invoice arrives again, only with a new IBAN and a matching QR code, often from a supplier's hacked mailbox.
- **The fake parcel notice**
By text, e-mail or even a yellow slip in the letterbox: a parcel is waiting for a small fee. Whoever pays gives away their card details; soon after, a fake bank often calls.
- **«Your domain expires»**
A «registration office» threatens that your domain will be deleted or that someone else is registering your name, and asks for payment. Renew your domain only with the provider you know.

If it has already happened

- **Call your bank at once**
On the official number. A payment can sometimes still be stopped. If card details are gone, have the card blocked.
- **Report it**
Report the attempt to the Federal Office for Cyber Security (BACS). If you lost money, file a report with the police, in an emergency on 117.
- **Change passwords**
If you gave a password or installed remote support, change your passwords and have the device checked.