Formation Prevention

GUIDE TO GOOD SECURITY HABITS

Avoiding everyday traps

12 topics, the habits that protect your company. Keep it within reach.



formation-prevention.ch

BEFORE YOU START

Three habits that work everywhere

1

Pause

Urgency, fear or a reward that is too good to be true are the fraudsters' favourite levers. A pressing request is exactly the moment to slow down.

2

Check through another channel

Call the person or company back on the number you already know, never on the one given in the message.

3

Report it straight away

To the IT department or your manager, even if it is only a doubt, and even if you have already clicked.

This guide summarises the 12 Formation Prevention modules. It does not replace the modules: it reminds you of them, topic by topic.

TOPIC 01 / 12

Phishing

> A booby-trapped email, text message or QR code polishes everything you can see: the sender's name, the logo, the tone. What gives it away is hidden.

Look at the real address

The display name can be anything. Read the sender's full address, and hover over a link (long press on a phone) to see where it really leads.

Beware of urgency

Parcel on hold, account blocked, unpaid invoice: a very short deadline is a warning sign, not a reason to act fast.

Type the address yourself

To log in to your bank or a service, enter the address you know instead of following the link you received.

QR codes

Do not scan a QR code stuck on a parking meter or received by post without checking the address it opens.

REMEMBER

Suspicious message: do not click, do not reply, do not forward it to a colleague. Report it to the IT department or to reports@antiphishing.ch.

TOPIC 02 / 12

Identity fraud

> A fake director, supplier or fiduciary asks for an urgent, confidential transfer, or for a change of bank details.

- **Call back on a known number**

  Contact the person on a number you already had, never the one given in the message or the call.

- **Follow the procedure**

  An unusual payment goes through the planned double check, even if the "director" insists on secrecy.

- **Change of IBAN**

  Any request to change a supplier's bank details is checked by phone before it is recorded.

- **Read the domain**

  A single letter's difference in the sender's address is all the fraudster needs.

REMEMBER

Urgency, secrecy and payment together: stop and check. Nobody will blame you for checking.

TOPIC 03 / 12

Passwords

> A short or reused password falls quickly, and then opens every account that uses it.

- **Length first**

  At least 12 characters, ideally 16 or more. A phrase that is easy to remember beats a complicated word.

- **One password per account**

  If a website has its data stolen, your other accounts stay protected.

- **A password manager**

  It creates and remembers strong passwords for you: the one provided by your company, or for example Bitwarden or Proton Pass.

- **Nothing personal**

  No first name, date of birth, company name or year: these are a hacker's first guesses.

REMEMBER

Only one password to really remember: the one for the manager. Make it long and unique.

TOPIC 04 / 12

Two-factor authentication

> With a second factor, a stolen password is no longer enough to get into your account.

- **Turn it on everywhere**

  Email, password manager, work accounts: wherever it is offered.

- **Prefer an app**

  An authenticator app or a security key protects better than a code received by text message.

- **Never give a code away**

  Neither the IT department nor a bank will ask you for it, by phone or by message.

- **Refuse what you did not request**

  Repeated login requests mean someone has your password: refuse, change it and tell the IT department.

REMEMBER

Keep your recovery codes in your password manager, not in an email.

TOPIC 05 / 12

Web browsing

> A fake website can look exactly like the real one, padlock included.

The padlock is not enough

It encrypts the connection, it says nothing about the honesty of the site. Read the full address.

Watch out for ads

In search results, sponsored links can be paid for by fraudsters: type the official address instead.

Official downloads

Install a program only from its publisher's website, or ask the IT department.

Fake alerts

A virus alert with a countdown or a number to call is a trap: close the tab. A certificate warning is never to be ignored.

REMEMBER

If in doubt about a page, close it and go through the address you know.

TOPIC 06 / 12

Public Wi-Fi

> In a café, at the station or in a hotel, someone can pretend to be the official network and see what you send.

- **Your phone first**

  Your phone's hotspot is safer than an open network.

- **The company VPN**

  Turn it on before working on a network you do not control.

- **No sensitive operations**

  Avoid e-banking and confidential data on a public network.

- **Booby-trapped login pages**

  A page that asks for a bank card or for a program to be installed to access the Wi-Fi: refuse. Forget the network after use.

REMEMBER

A password displayed at the counter does not turn a shared network into a private one.

TOPIC 07 / 12

Ransomware

> Ransomware encrypts the company's files and demands a ransom. It often gets in through a booby-trapped attachment.

- **Do not enable the content**

  A document received by email that asks you to "enable content" to display is a warning sign.

- **Locked screen or renamed files**

  Cut the network connection at once (cable and Wi-Fi), then alert the IT department and your manager.

- **Do not pay**

  And do not contact the hackers: paying guarantees neither that the files come back nor that the data will not be published.

- **Do not plug in the backup**

  The backup drive would be encrypted in turn. Let the IT department decide what happens next.

REMEMBER

Cut the network, then raise the alarm: two actions, in that order.

TOPIC 08 / 12

USB drives and media

> A USB drive that is found or given away can contain malware, or even pretend to be a keyboard that types commands.

- **Never an unknown drive**

  A drive found, received by post or handed out at a trade fair is not plugged in: give it to the IT department.

- **Encrypted drives**

  For work data, use the encrypted media provided by the company, not a personal drive.

- **Deleting does not erase**

  Deleting files or a quick format does not really erase them: hand old media over to the IT department.

- **Lost media**

  A lost drive or disk with company data is reported immediately.

REMEMBER

You plugged in a suspicious device: unplug it, cut the network and raise the alarm.

TOPIC 09 / 12

Remote work

> At home, the internet router and the work computer are your first line of protection.

- **Set up your router**

  Change the default admin password, choose WPA3 (at least WPA2) and a Wi-Fi password of at least 16 characters, ideally 20.

- **A guest network**

  For visitors and connected devices, kept apart from your work computer.

- **A computer for work**

  Used only for work, kept up to date, and locked as soon as you get up. Data accessed through the company VPN.

- **Discretion**

  Confidential calls and screen out of sight, documents put away.

REMEMBER

Computer lost or stolen: tell the IT department immediately.

TOPIC 10 / 12

Deepfake and vishing

> A voice can be imitated from a few seconds of recording, a face in a video call too, and the number displayed can be faked.

- **Hang up and call back**

  On the number you know, even if the voice is your director's.

- **Never a code by phone**

  No password, no code received by text message, no PIN, whoever is calling.

- **No remote control**

  Refuse to install a program or to let a stranger (fake support, fake police) control your computer.

- **Behaviour counts more than appearance**

  Unusual request, pressure, secrecy: these are the signs to listen to.

REMEMBER

A doubt during a call: end the conversation. The real caller will understand.

TOPIC 11 / 12

Backups and sensitive files

> Breakdown, fire, ransomware: without an up-to-date backup kept safe, the work is lost.

- **The 3-2-1 rule**

  Three copies of the data, on two different media, one of them in another location (NCSC recommendation).

- **An offline copy**

  Unplug the drive after each backup, and regularly test the restore.

- **Share sparingly**

  A sensitive file is shared only with the people concerned, never through a link open to everyone.

- **Wrong recipient**

  A document sent to the wrong person is reported immediately: the company may have legal obligations.

REMEMBER

A backup that has never been restored is only a hope.

TOPIC 12 / 12

Incident reporting

> Every minute counts: the sooner the company knows, the sooner the attack is stopped.

- **Straight away**

  Report as soon as you have a doubt, even for a narrowly avoided incident.

- **By phone if possible**

  Your mailbox may already be in the wrong hands.

- **Say what matters**

  The time, what happened, the account or message concerned, and what you have already done.

- **Delete nothing**

  And do not play it down: these are valuable clues for the IT department.

REMEMBER

Reporting quickly is never a mistake.

IF AN INCIDENT HAPPENS

The five steps

1. **Stop**
   No more clicks. Files being encrypted: disconnect from the network.
2. **Warn right away, by phone**
   The IT department and your manager.
3. **Describe precisely**
   What, when, which account or message.
4. **Don't delete anything**
   Keep the evidence, don't contact the attackers.
5. **Follow the instructions**
   The IT department knows what to do.

YOUR CONTACTS

IT department _____

Manager _____

Emergency number _____

IN SWITZERLAND

Report phishing
reports@antiphishing.ch

Federal Office for Cyber Security (NCSC)
www.bacs.admin.ch

Financial loss
Your cantonal police

Formation Prevention

FORMATION PREVENTION

Learning by doing

Modules of about 10 minutes, realistic simulations and Swiss examples, so that good habits become second nature.

formation-prevention.ch

IMPRINT

Datalys
Grand Rue 8
1196 Gland
Switzerland

© 2026 Datalys