



Detecting fraud

The most common scams explained



Zürcher
Kantonalbank

Contents

4	Investment scam
6	Refund scam
8	Romance scam
10	WhatsApp scam
12	Phone scam I
14	Phone scam II
16	Support scam
18	Phishing
20	Malware
22	Shopping scam
24	Advance payment scam
26	CEO scam
28	Grandchild scam
30	Inheritance scam

Detecting fraud

A critical eye on scam tactics

In an increasingly networked world, acts of fraud are a serious and daily challenge. These include both sophisticated online scams and traditional methods that are professionalised with modern technologies. It is therefore crucial to recognise and understand the different types of fraud – because it can affect us all, regardless of age, gender or location. From online scams and telephone fraud to credit card fraud and identity theft, the general structure is always the same:

- 1) The irresistible offer
- 2) The absolutely necessary investment or payment
- 3) The disappointment

This brochure highlights various aspects of the most common scams and gives you valuable tips on how you can protect yourself. The following scenarios show how a scam may play out.



Easy money

Investment scam

Fraudsters advertise seemingly lucrative investment opportunities online that quickly generate huge profits. These ads often feature famous personalities who are said to have made a fortune with them.

Request for ID documents

Once you respond to the ad, the fraudsters quickly get in contact and offer their support, including in opening an account. They then ask for the relevant documents (e.g. passport or ID). You are also urged to make an initial payment.

Lure of fake profits

The fraudsters direct you to fake dashboards during their regular calls to show alleged profits. This encourages you to invest more money.



Demand for more and more money

The fraudsters persistently talk you into investing more and more money. They may even pay you small amounts to gain your trust. As soon as they can no longer extract money from you, the fraudsters break off all contact. The money has long since been transferred to other accounts and you lose the entire investment.

- Do not engage in online advertising that promises easy money.
- Never send your personal documents (or copies of them) to unknown third parties.
- Do not invest money in companies or people unknown to you.

The empty money-back promise

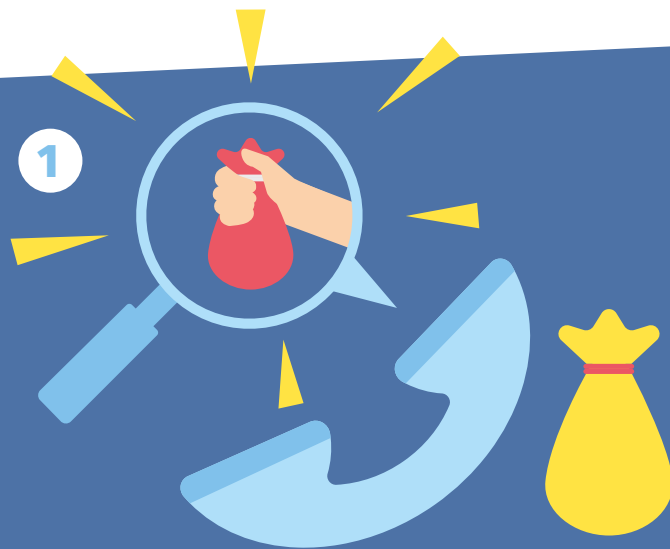
Refund scam

Fraudsters contact you by phone claiming to have found the money you lost on a previous investment and want to repay it. You are asked to pay fees.

Exerting pressure for payment of fees

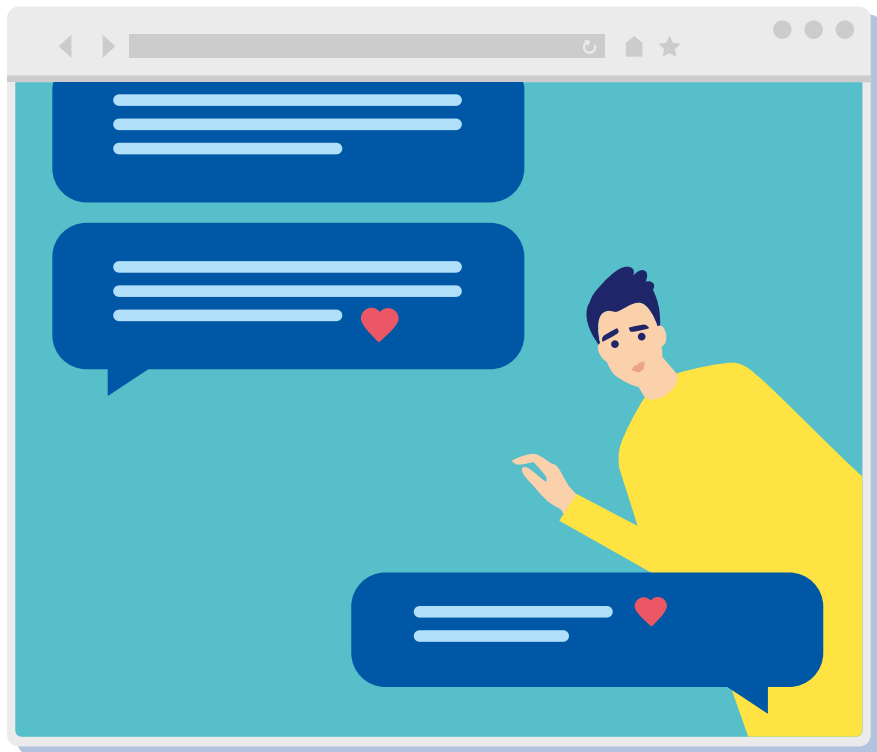
You are often put under time pressure. If you hesitate to accept the offer, they threaten to report you for money laundering or invoke consequences from the police. However, as long as you pay the fees, the fraudsters always come up with new fees or taxes. Once you are no longer willing to pay, they break off all contact.

- Do not transfer money to callers who promise to give you money back.
- Beware if you are put under time pressure on the phone and hang up the call.



"We have secured your money.
You will have to pay a small
processing fee for its release."





The unknown lover

Romance scam

Fraudsters contact you on social media platforms such as Facebook, WhatsApp or Instagram. They hide behind a particularly attractive profile or pretend to be working for a humanitarian company or as a soldier, for example.

- Be sceptical when strangers contact you online or via smartphone.

"I love you and want to be with you!"

Building trust with stories

The fraudsters develop a relationship with you over a prolonged period of time. They overwhelm you with compliments, make contact every day and feign interest in a future together with you.

Requesting money for personal emergencies

Once a personal relationship is sufficiently established, the fraudsters invent personal emergencies and ask for money. They maintain the relationship for a long time and constantly invent new emergencies to encourage you to transfer money.



- Be alert if someone wants money from you for personal emergencies.
- Do not transfer money to people you have never met in real life.

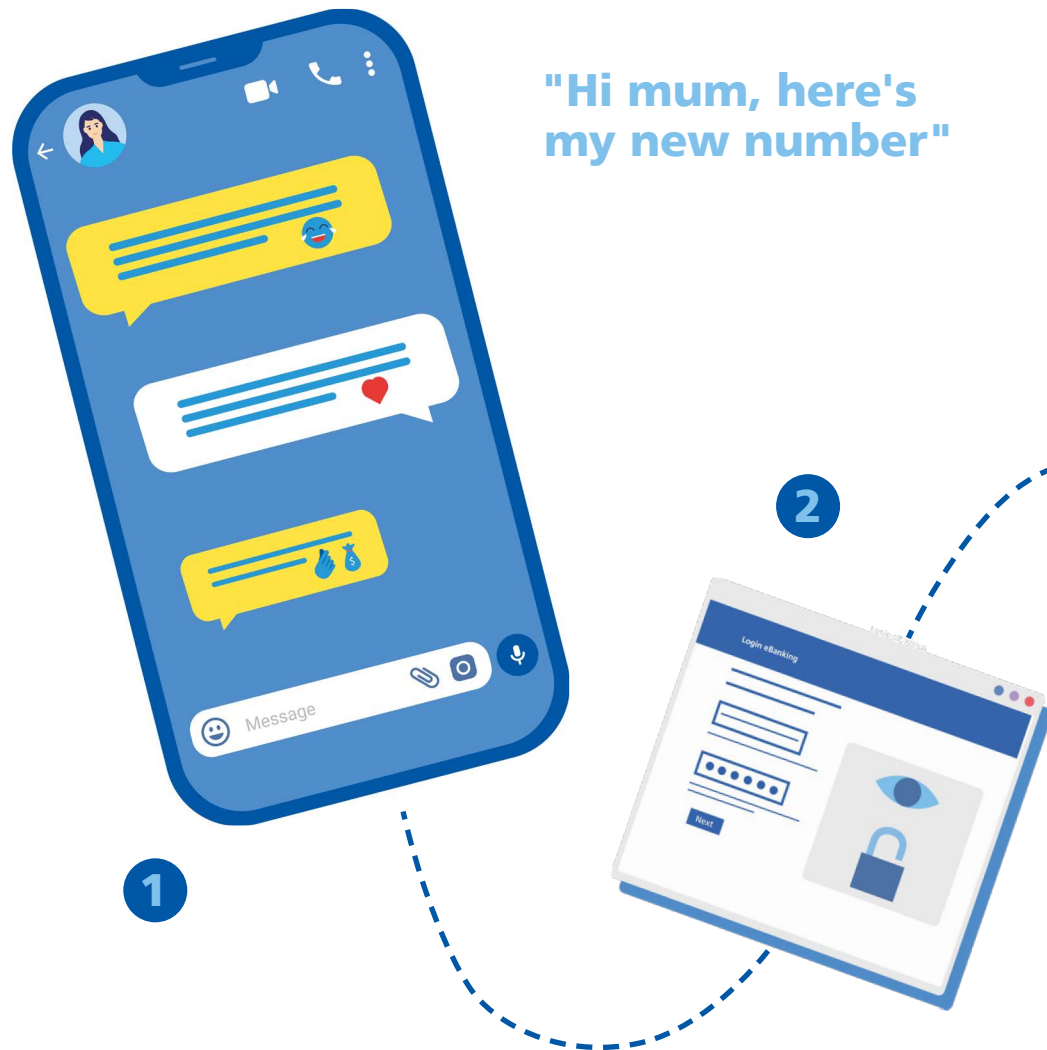


Fake family members

WhatsApp scam

You receive a WhatsApp message or SMS from an unknown number. The sender pretends to be your son or daughter, who has lost or broken their mobile phone.

"Hi mum, here's my new number"



Messages requesting financial help

After some trivial messages, the conversation soon turns to an urgent need for money. The alleged relative may claim that a bill needs to be paid by the end of the month or there are other legitimate reasons why the money is urgently needed. Since the old phone is broken, they claim they have no access to eBanking.

Bank details under time pressure

You are asked to provide your eBanking login details for an urgent payment. As soon as the fraudster has this information, they will try to register their own device for authentication in order to gain access to your eBanking.



3

- Do not be deceived by the sense of urgency. Contact your children using the numbers you already know.
- Do not give anyone else access to your bank account.
- If you have already transferred money, inform your bank immediately.

The shock call

Phone scam I

You receive a call and are told that a serious accident has just happened, for example. The police or someone claiming to be close to you who was seriously injured in the accident is on the phone. They ask you to urgently pay for hospital care or emergency surgery.

Inducing shock with an emergency situation

The fraudsters impersonate the police or the injured person. Technical voice distortion may also be used. You are urged to take immediate action, because the situation is a matter of life and death. The fraudsters convey a terrible scenario and want to take advantage of your state of shock.



No time for reflection

The money must be handed over as quickly as possible. For this purpose, they will arrange for you to be either picked up by a taxi or they will send a third party to collect the money from you. After handover, the money is gone and you find out that the loved one is doing well and has not been involved in an accident.

- Do not be tricked by the sense of urgency. Contact the allegedly injured person.
- Prepayment is never necessary for treating an accident victim. Hang up the phone.



The fake police officer

Phone scam II

You are called by the police because your help is important in a case. A person is suspected of committing a crime near your address. You are asked to help put an end to the person's criminal activities. It is also important that your valuables are put somewhere safe, because the criminals have also set their sights on you.

Cooperation with the police

The fraudsters try to gain your trust by accusing other people of fraud and pretending that there has been an incident in the nearby area. In most cases, bank

employees are also involved, which is why you are not allowed to contact the bank under any circumstances.

Your friend and helper

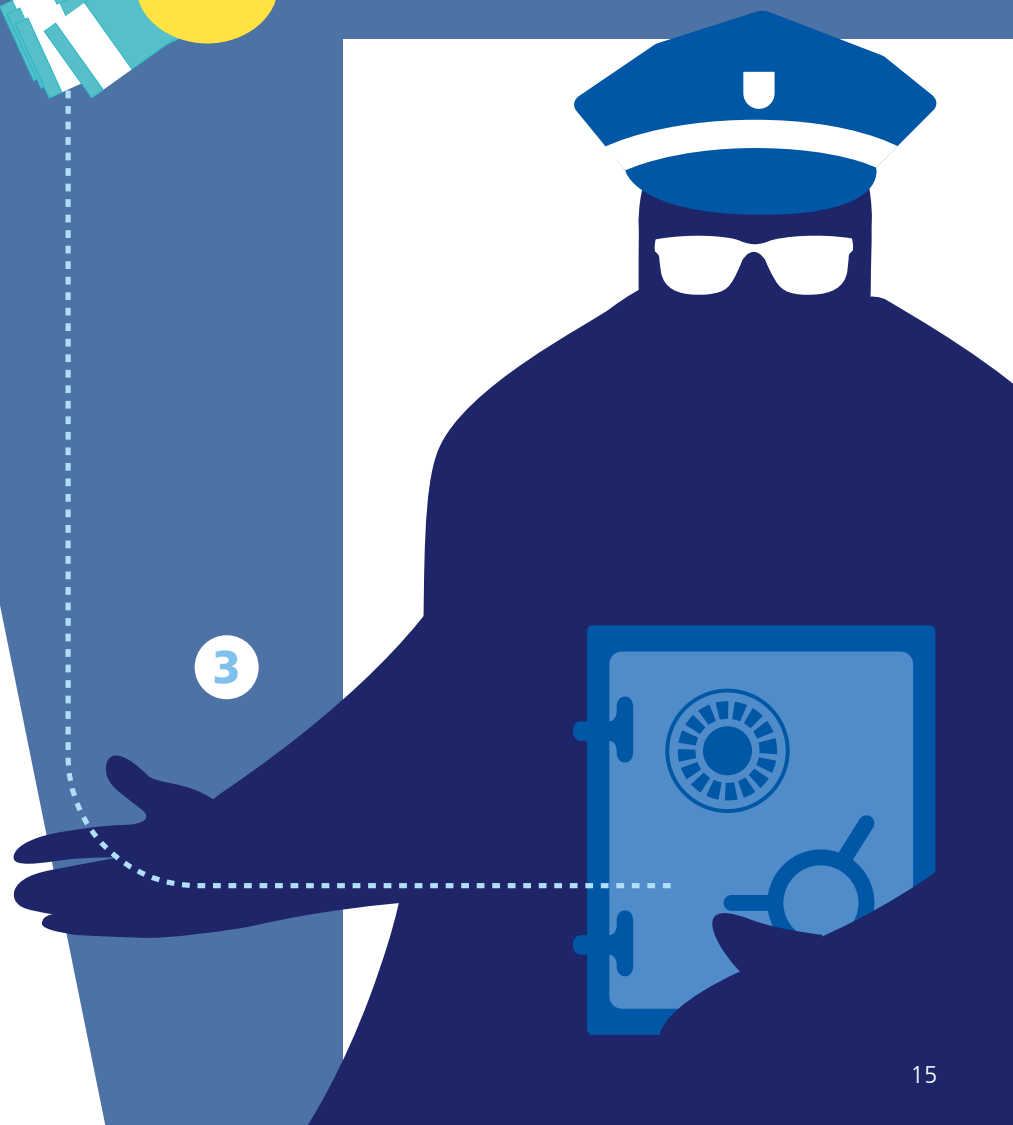
The alleged police officer wants to help you keep your valuables safe. A third party, an alleged police officer or a police officer in civilian clothing collects the valuables and cash from you. If you do not have anything at home, they ask you to go to the bank. You also receive instructions on how to deal with the bank's employees.

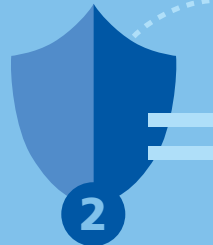
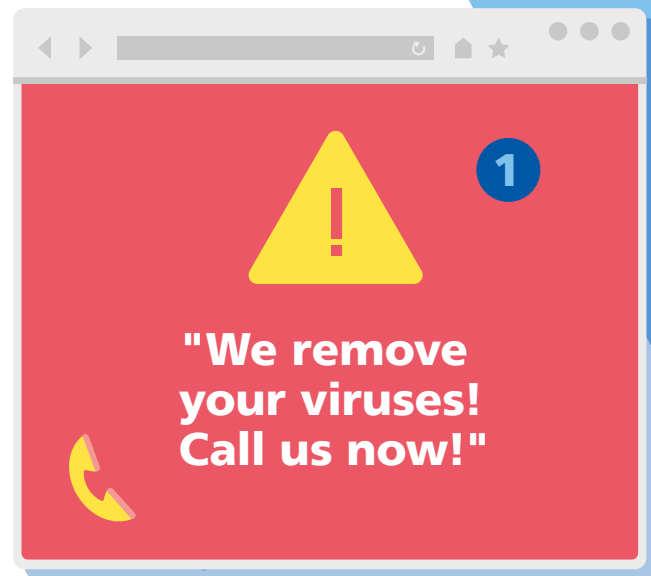
2



- Never hand over valuables or cash to the police or anyone else.
- Be alert if you are not supposed to tell others about a phone call.

3





Selling software for long-term support

The fraudsters claim they want to sell you a security program, such as an antivirus program. The term is usually several years or even for life.



Trojan help

Support scam

A message appears on your computer screen stating that a technical error has occurred or that hackers have gained access to your computer. You are prompted to immediately call a displayed number to resolve the problem.

Installing software for support

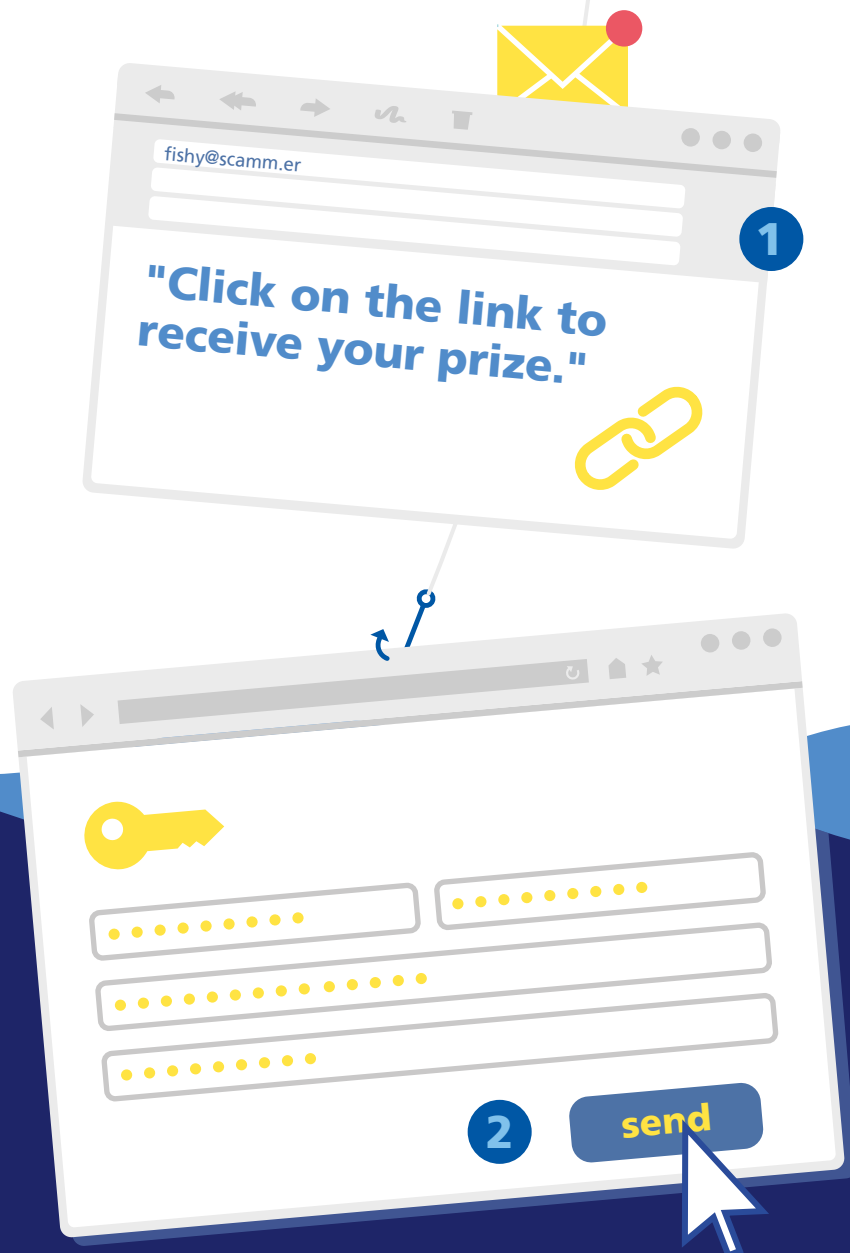
The fraudsters pretend to be support staff from a well-known technology

company, such as Microsoft or Amazon. Over the phone, they ask you to install software. Using this software, the fraudsters gain unrestricted access to your computer with the possibility to steal personal data. They often say that eBanking is affected and that you must log in there, too. With the option to "turn off" your screen, they can then make fraudulent payments.

- Obtain trustworthy advice before downloading third-party software.
- Be vigilant whenever you are being sold something.

Fraudulent e-mail

Phishing



You receive an e-mail inviting you to click on a link or download a document. At first glance, the e-mail seems to come from a known sender, for example your employer.

Gaining access to data and systems

The link often leads to a form in which you have to enter personal data, for example an input field for your user name and password. The documents in the e-mail attachment contain malicious programs that collect data or damage computer systems.

Selling personal data or demanding a ransom

The fraudsters want to use the links and the malicious software to collect and sell your personal data or damage your computer system in such a way that a ransom can be demanded for release.

3

- Do not open unexpected e-mail attachments.
- To log in to your eBanking, always type in your bank's website address and do not click on ads.
- If you need to enter personal information, first check the sender's address and the link in the e-mail.
- If you are unsure, contact the alleged sender by other means (e.g. by phone).



"Please find attached your telephone bill. Thank you for your timely payment."



The hijacked computer

Malware

Fraudsters want to install software on your computer to access it and cause damage. Malicious software (called malware) usually ends up on your computer via e-mail attachments that are downloaded. Other methods are USB sticks or downloads that start unnoticed in the background.

The software causes unnoticed damage

Once installed, it can pursue different goals:

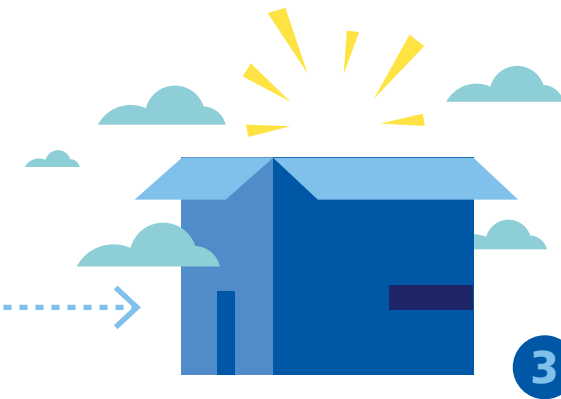
- Encrypt data to demand a ransom
- Spy on data
- Record keystrokes
- Redirect data streams etc.

Fake eBanking link that appears deceptively real

In the case of banking Trojans, you are sent an e-mail containing a fake link. If you click on it, changes will be made to your computer. The next time you open your bank account, you will be redirected to a fake website. The page looks like your bank's real website and your eBanking login seems to work as usual. This is how you reveal your login information and fraudsters gain access to your eBanking.

- Do not open unexpected e-mail attachments.
- If you are unsure, contact the alleged sender by other means (e.g. by phone).
- Check each link in your e-mails before clicking on them.
- Be careful when you log in to your eBanking.
- Check the URL of the website.

"Buy this special offer!
Only 2 products left in stock."



The fake online purchase

Shopping scam

You see a desired product online at an attractive price. The pictures and ads present a good offer, so you can get in touch via e-mail or chat.

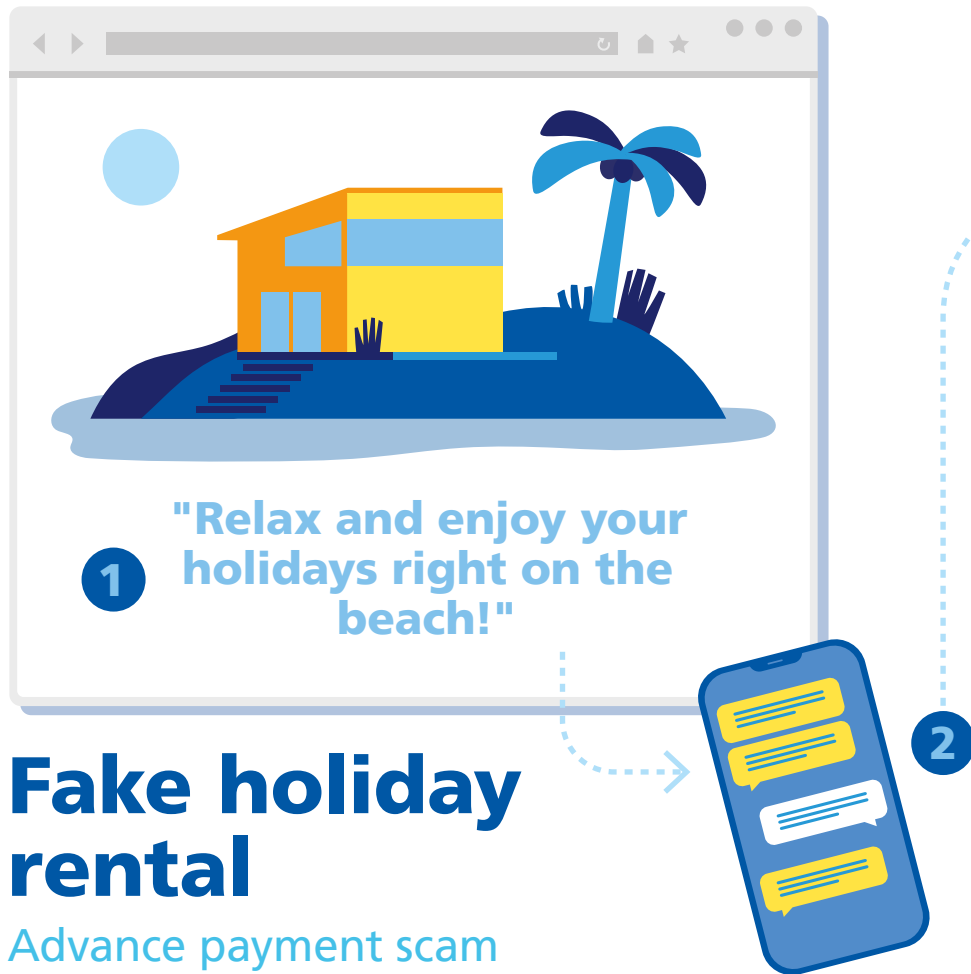
Fast payment for exceptional value for money

The fraudsters insist on a quick transaction. Payment is usually not made via the platform, but via another payment processor. You may be very pleased with the deal offered and therefore make the payment, albeit against your gut feeling.

Ordered product does not exist

After the payment, the fraudsters stop contacting you. The ordered product never arrives and your money is gone.

- Be sceptical about good offers that are only available for a limited time.
- Listen to your gut feeling, even if (or especially if) the offer is tempting.



You discover an offer for a holiday rental at an attractive price on a reputable on-line platform. The pictures and ads present a good offer and you get in touch.

Switch to another communication channel

Fraudsters often quickly switch to an alternative communication method such as e-mail or WhatsApp. Payment information is exchanged on these new

channels. Once you have paid, all contact is cut off.

Holiday rental is nowhere to be found

When you finally arrive at your holiday destination, the holiday rental is not accessible or does not exist at all. Refunds for the money paid are almost never possible because you left the official communication channel of the platform.

The fake payment

CEO scam

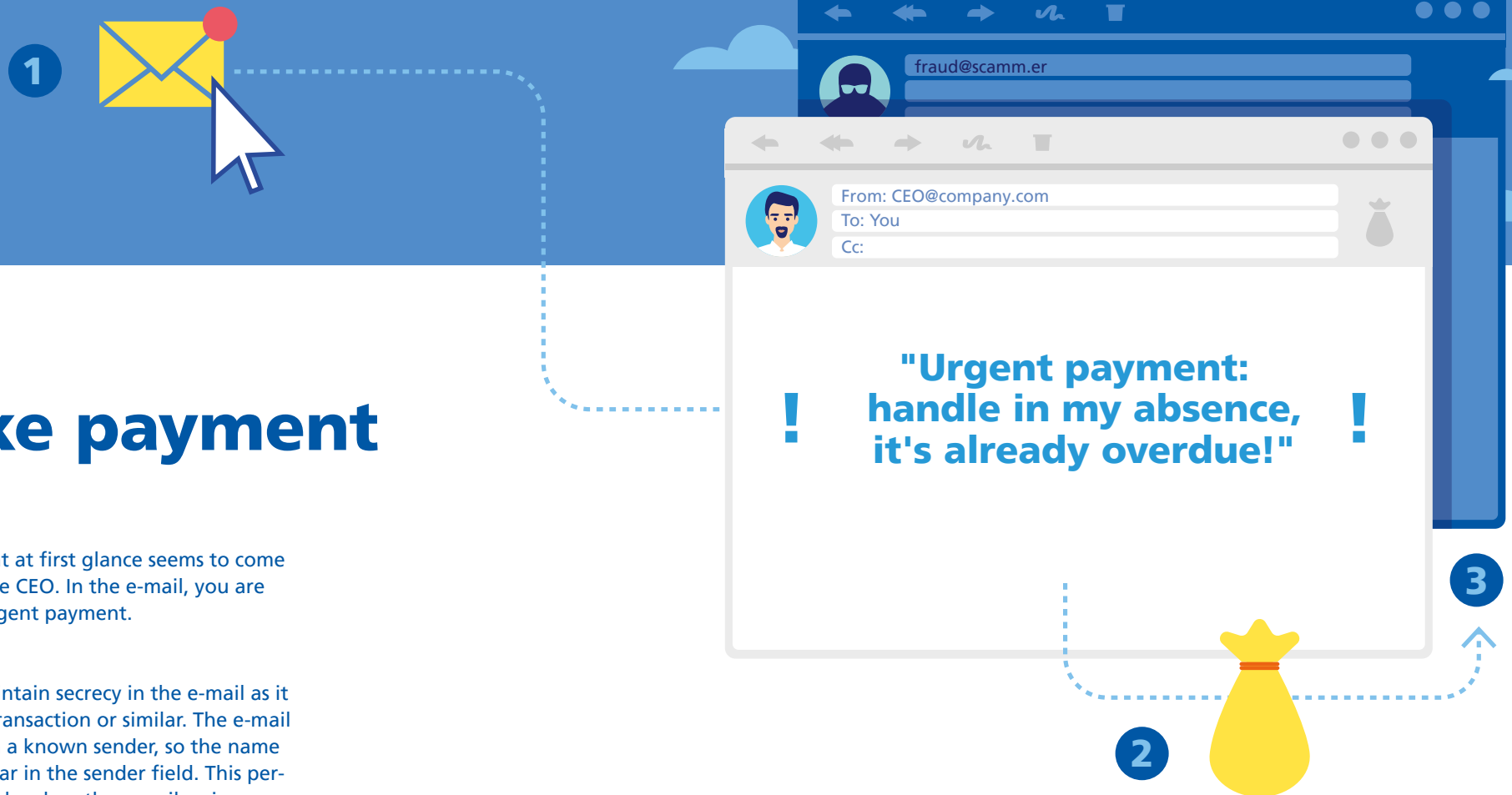
You receive an e-mail that at first glance seems to come from your manager or the CEO. In the e-mail, you are prompted to make an urgent payment.

Quick, secret payment

You are requested to maintain secrecy in the e-mail as it concerns a confidential transaction or similar. The e-mail often appears to be from a known sender, so the name of a supervisor may appear in the sender field. This person is usually not reachable when the e-mail arrives, so it is difficult to check with them.

An inconspicuous payment that raises no suspicion

To avoid further investigation, the payment is inconspicuous in terms of the amount, currency and destination country. The requirement for official approval in companies, combined with an often urgent or confidential payment, may result in control mechanisms being bypassed, facilitating fraud.



- Be alert when put under time pressure: check the sender carefully. Enquire with supervisors you can reach.
- Always have a payment double-checked.

The fake grandchild

Grandparent scam

You receive a call from an unknown person. The caller drops the name of one of your relatives during the call, for example the name of a grandchild. The fraudster pretends to be this relative on the phone.



"Do you recognise me? It's me, your grandson."

Fraudster:
"Albert, don't you recognise me?
That makes me feel quite sad..."

You:
"Is that you, Thomas?"

Fraudster:
"Of course, it's me – Thomas."

Request for financial help over the phone

The fraudster on the phone speaks to you in a very personal way. After a nice conversation, the caller tells you that they urgently need help. Often an investment or a business is at risk or other good reasons are given why the relative needs money quickly.

Time pressure and instructions for coming up with the money

The fraudster urges you to withdraw

money the same day. Often, you are told exactly how to withdraw the money and answer questions from bank employees.

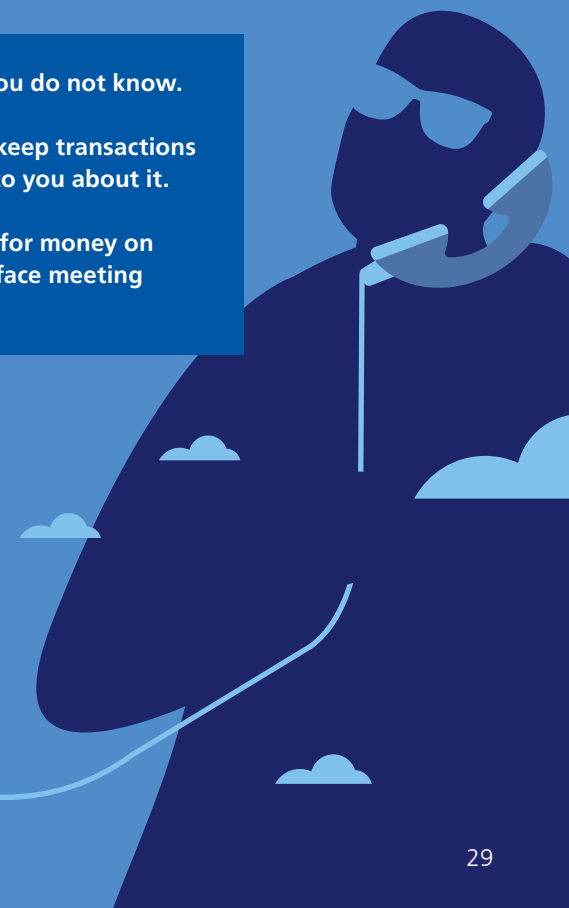
Handing over money to a "friend"

The fraudster claims not to be able to collect the money personally. You are told that a trusted person will collect the money on their behalf. You are asked not to tell anyone about the transaction. Once the money is given to this unknown person, it is lost.

- Never give money to people you do not know.
- Be alert when you are told to keep transactions secret. Talk to someone close to you about it.
- If a relative or friend asks you for money on the phone, insist on a face-to-face meeting at a cafe or restaurant.



3



The fictitious inheritance

Inheritance scam

You are contacted over the phone by an unknown person who claims to be a notary, heir, executor or similar. The fraudsters mislead you into believing...


- that a distant relative has died and left you with a considerable sum;
- that an unknown person died and randomly left you a lot of money;
- that you are due to receive a large inheritance, but your support is needed in settling the claims to pay out the inheritance.

Money for lawyers, fees or taxes

You are asked to pay money in order to receive the inheritance. This money, you are told, is necessary to pay a fee, the costs of a lawyer or a tax bill. You are deceived into believing that you will receive the inheritance as soon as the stated amount has been transferred. However, the alleged inheritance is never paid out. Your money is gone.

Combination with the romance scam

The inheritance scam is also used in combination with the romance scam. The fraudsters first deceive you into a romantic relationship and then ask you for help to be able to pay a fee for an inheritance settlement. However, neither the fee nor the inheritance (or the romantic relationship) exist.



"You are entitled to an inheritance and can expect a decent sum of money."

- Be sceptical when strangers contact you promising money from an inheritance.
- Do not transfer money to people you have never met in real life or whose identity you cannot verify.

What can you do?

Equipped with the knowledge of different types of scams and with a little caution, together we can help detect fraud and create a safer environment for everyone. Be alert, ask questions and verify the information before making any decisions or disclosing any personal information.

Find information and support here:



eChannel Security

Phone: 044 292 90 30

E-mail: fachstelle_ecs@zkb.ch

Service hours:

Monday to Friday: 8 a.m. to 4.30 p.m.



eBanking Support

Contact support directly in your eBanking or
by phone: 0844 840 140

International number: +41 44 293 95 95

Service hours:

Monday to Friday: 8 a.m. to 10 p.m.

Saturday/Sunday: 9 a.m. to 6 p.m.



Police

In emergencies, contact the police directly.

Phone: 117



Internet research

Find out more from specialist agencies.

Swiss Financial Market Supervisory Authority:

www.finma.ch/en/finma-public/warnungen/

Zurich cantonal police:

www.cybercrimepolice.ch, www.telefonbetrug.ch

National Cyber Security Centre:

www.ncsc.admin.ch

University of Lucerne "eBanking – but secure!":

www.ebas.ch/en/



Enquire within the company

Discuss suspected scams in a professional context with
your colleagues and supervisors.



PC Support

If you suspect that your computer is infected with a virus
or malware, contact professional PC support.



Friends and acquaintances

Confide in someone you trust and seek advice in your
personal environment.

Notes

Find updated information about different scam tactics online:

Our website

zkb.ch/betrug



Legal Information

This document is for information purposes only. The types of fraud covered in this brochure are a selection. This brochure does not replace the individual product contracts and specifications. For you as a client, the risk information given and the safety precautions and due diligence obligations regulated therein have priority.

