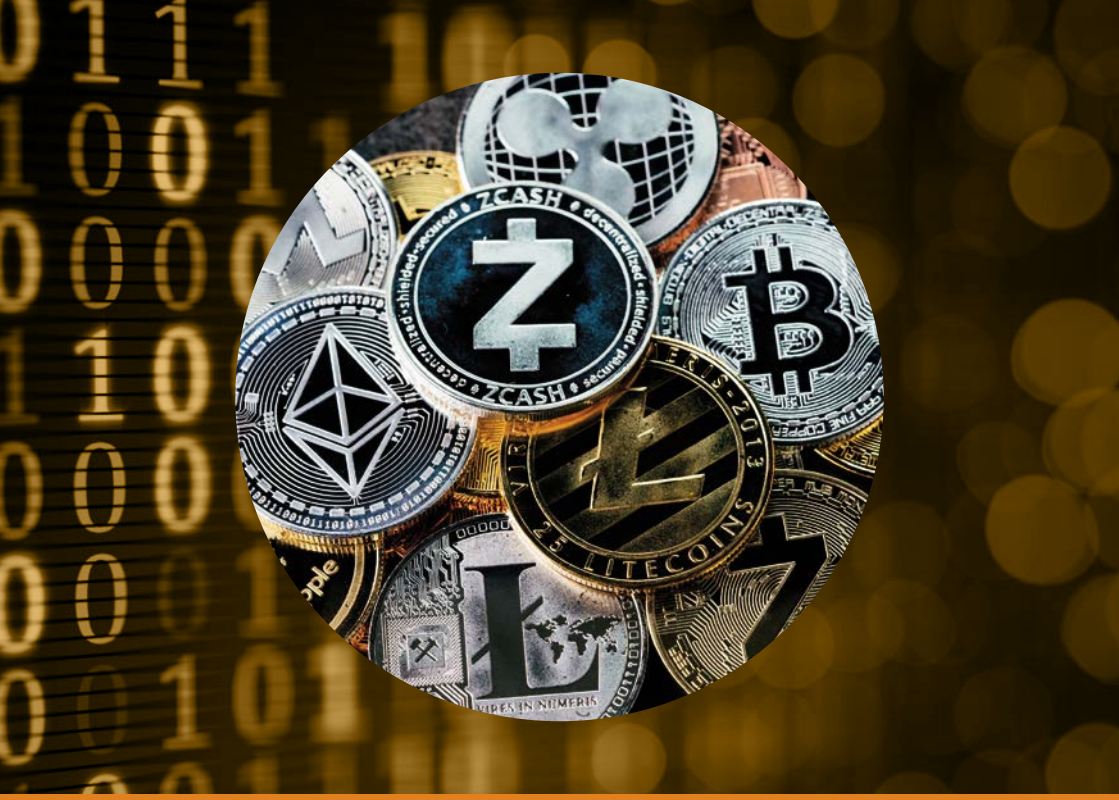

Fantastic returns are pure fantasy

What you should know about online investment fraud

Police and Swiss Crime Prevention –
an office supported by the cantonal
ministries of justice and police.

Use your head when investing your money

With bank accounts earning zero interest and a generally more uncertain economic and market climate, it has become difficult to maintain – let alone grow – the value of your carefully accumulated nest egg. As a result, many investors are seeking out the stability of asset classes such as gold or real estate. Alternatively, they may look to **new forms of investment** that promise high returns even in times of crisis. **Cryptocurrencies** are one example. Scammers love this kind of situation. They can present themselves as progressive financial services providers, enticing unsettled small investors into putting their money into schemes in which they have nothing to gain, but everything to lose. It's known as **online investment fraud,** and this leaflet describes a typical case.

Phase 1: Bait

The fraud attempt usually starts with a broad online **advertising campaign,** in the form of popups, banners, spam mails, etc., as well as via online news portals. It may also involve cold calling, and attempts to add you as a contact on social media or an online dating platform.

Initially, the scammers only want to get you **interested** in their new investment vehicle, and to trick you into giving your **contact details.** To achieve this, you are guided to websites that look legitimate (and are more than likely search-engine-optimised), but are nothing of the sort. It might even happen if you've been googling investment options yourself. Once on the website, you're conned into believing convincing arguments, which sometimes offer **testimonials** from celebrities who have apparently made lots of money with the investment on offer.

Phase 2: First contact

When you've registered on a website like the one described, a short time later you'll get a **call from someone pretending to be an investment advisor.** You're probably still a little sceptical at this stage, so this person won't try to talk you into making a major commitment just yet. Instead, you'll be invited to make only a small of investment of, say, CHF 250 to CHF 500, just to "give it a try". They want you to feel that it's all your decision. Afterwards, you'll be given access to your "account" on the website, so that you can track the supposed performance of your investment. In all probability, you'll see that you're making money every time you log in. **It's intended to convince you to invest more – and it will.**

Phase 3: Building trust

Your investment is performing well, so you're no longer so sceptical. You might look forward to the next call from your "advisor". That's exactly what the fraudsters want. You should feel increasingly confident that you're getting a very **personal service** as you continue to invest. Fraudsters are masters of social engineering. In other words, they know what interpersonal skills and techniques to use to manipulate their victims. They probably **won't put any direct pressure on you** at first. Instead, the pressure will be indirect, telling you that offers are subject to **limited availability,** or **only open for a short time.** What's more, they'll use this new trust to drive a wedge between you and the financial partners you've relied on for years, such as your main bank. The fraudsters will then open an account (wallet) in your name, using your ID, with genuine cryptocurrency traders. The additional catch is that your access rights – if you have any at all – will be shared with the fraudsters. They may even gain backdoor access to your computer using remote maintenance software, and then use e-banking to make transfers in your name.

Phase 4: Additional payments

You've been watching your profits grow for a while now, and for whatever reason want to take some of your money out of the scheme – only to find that you can't. Your advisor might tell you, for example, that there's been a **sudden crash,** or that you'll have to pay **high taxes** in advance. They'll now attempt to convince you of the special nature of your investment, and of the need to put even more money in to secure your gains. This may be when they'll lay on the direct pressure, or even threats. Sooner or later, someone purporting to be their line manager, or even the **big boss,** will be brought in. Their role is to use their supposed authority to reassure you, and offer up the prospect of continued financial gain if you only stay the course. If you still want to get out, you may be offered **loss insurance,** which they'll tell you should have been taken out right from the start. As a gesture of goodwill, in your case they are prepared to backdate it. None of this is true. It begins to dawn on you that you may have fallen victim to fraud but, irrationally, you cling all the more to what your "trusted" advisor tells you. In the end, they claim that they may be able to find a way to get your money out, but they will need **bank, legal or notary fees paid in advance...**

Phase 5: Realisation

Whatever you've tried, **you're not getting any money back,** except perhaps in the initial phase, and then only in small amounts to give you a sense of security, and to draw you further in. Now you know for certain that you've been had.

General rules:

- There is no such thing as fast, easy, risk-free money.
- Nobody reveals their investment "secrets" on the internet – anyone who has to advertise doesn't have any to offer.
- Nobody shares promising investment strategies with total strangers without being asked. Why should this "expert"?
- Investment tips advertised by celebrities are generally fake, and used only as bait. The celebrities themselves are normally completely unaware that they are being used in this way.

What to do before investing in new instruments:

- Exercise caution, especially if you're being promised high returns, and in complex areas such as cryptocurrencies, forex trading and trading in binary options (or so they say). Take your time and gather information from as many different sources as possible. Never allow yourself to be put under pressure, whether it's from "advisors" or "limited" offers.
- Don't be dazzled by unrealistic promises. No reputable financial services provider will offer you substantial returns, fast.
- Check whether the provider is authorised by FINMA (www.finma.ch → FINMA Public → Authorised institutions, individuals and products), or features on FINMA's warning list (www.finma.ch → FINMA Public → Warnings). If you come across anything that looks dubious, let FINMA know using the report form (www.finma.ch → FINMA Public → Reporting information). Tip-offs like these enable FINMA to identify unauthorised providers and take them out of circulation.
- Check the commercial register extracts of Swiss providers at www.zefix.ch.
- If the provider operates abroad, go online and do your research. Even if there are only a few isolated warnings of fraud, stay away.
- Talk to your client advisor at your main bank, and to experts you trust, for their professional opinion.

- Never trust anyone you only know virtually with your money.
- Never give anyone you only know virtually remote access to your computer (with remote access software such as TeamViewer, Anydesk, Supremo, etc.).
- Don't throw good money after bad! You can't get back what you've already invested by putting more and more into the same scheme.

What to do if you've been a victim of online investment fraud:

- Report it immediately to your local or cantonal police, and make a formal complaint.
- Immediately let your bank know that the transfers in question were the result of fraud. You may be able to stop money that is still on its way to the fraudsters.
- If someone saying they're a private investigator, lawyer or public prosecutor contacts you by phone or mail at a later date, it is highly likely that they're part of the same gang of scammers. Do not give them any money, either.

Further information: **www.ebas.ch/investmentfraud**

March 2021

SKPPSC

Swiss Crime Prevention (SCP)
Haus der Kantone
Speichergasse 6
CH-3001 Bern

www.skppsc.ch

This leaflet was created in co-operation with the **University of Lucerne** and **"eBanking – but secure!"**

www.ebas.ch | www.ebankingbutsecure.ch

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

eBanking but secure!