FINANCIAL SERVICES
AND MARKETS
AUTHORITY

COVID-19 : BEWARE OF FRAUDULENT INVESTMENT OFFERS AND SCAMS THAT ARE CIRCULATING ON SOCIAL MEDIA!

WARNINGS | 01/04/2020

Fraudsters are not hesitating to exploit the current COVID-19 situation. Beware, since the current climate is particularly propitious for these swindlers to create more victims. Most of the time, they contact their victims by using phishing techniques disseminated via different channels: email, social media or unsolicited phone calls.

The FSMA was informed that malicious persons were using these phishing methods to take advantage of the current COVID-19 situation. Fake messages are currently circulating on the internet and via text messages, containing, among other things:

- false offers of protective masks:
- fraudulent fundraising campaigns for victims of the virus;
- links to sites providing fake information;
- false offers of vaccines.

More than ever, prudence is necessary. Always think twice before clicking on a link, beware of any unsolicited message you receive and take into consideration the recommendations of the **Centre for Cybersecurity** (https://www.safeonweb.be/fr/actualite/coronavirus-protegez-vous-aussi-contre-le-phishing).

New communication channels enable 'fraudsters 2.0' to make even more victims. Social media such as Twitter, Facebook, Instagram or LinkedIn appear to be ideal channels for spreading false investment offers, for instance offers of **cryptocurrencies** (/en/warnings/cryptocurrency-trading-platforms-beware-fraud), **binary options and forex trading/CFDs** (/en/warnings/online-trading-platforms-are-making-new-victims-belgium-1), '**investment wines** (/en/warnings/offers-investment-wine-beware-fraud-fsma-renews-its-warning)', **offers of portfolio management agreements** (/en/warnings/offers-wealth-management-beware-fraud-fsma-renews-its-warning) and **credit offers** (/en/warnings/fraudulent-credit-offers-2).

In this regard, the FSMA has notably received, in recent weeks, numerous reports regarding:

- **Bitcoin-Evolution / Bitcoin-Revolution** (/en/warnings/bitcoin-evolutionbitcoin-revolution): this entity is not authorized to provide investment services in or from Belgium. In order to make contact with its victims, these entities are notably using fake press articles referring to public figures (see explanation below).

HOW DO FALSE INVESTMENT/CREDIT OFFERS CIRCULATE ON SOCIAL MEDIA?

The following techniques appear to be most popular among fraudsters when making fraudulent offers via social networks:

- **Sponsored links on Facebook and Instagram**

Investment fraud victims often report having been contacted by phone after having clicked on a sponsored link or post on Facebook or Instagram.

At present, it appears that fraudulent investment offers in cryptocurrencies, binary options and forex trade/CFDs, and 'investment wines', as well as fraudulent offers of portfolio management contracts in particular are being promoted via such links or posts (cf. the relevant **warnings** (/en/warnings) on the FSMA website).

Contrary to ordinary posts, which do not necessarily catch the eye in the newsfeed, sponsored posts pop up based on age, gender or areas of interest and depending on the pages consulted by the person concerned or the target audience.

Advertisements promoting 'very profitable' investments appear in the relevant advertising spaces or in the newsfeed of the user concerned. The user is often invited to provide his or her contact details so that he or she can be contacted again at a later stage.

Those advertisements are often illustrated with an image or video and accompanied by fake comments and automatically generated likes. The message disseminated looks intriguing but remains extremely vague.

The pages containing those sponsored advertisements seem to be specifically conceived for such advertising campaigns. They appear under a variety of names, referring to the financial world in one way or another. Nevertheless, they hardly ever mention a telephone number, website, address or company name.

- **Simple publications on Facebook**

Certain fraudulent offers, mostly of credit, are simply distributed by fraudsters through publications on Facebook groups specialized in, for example, buying and selling of real estate or second-hand goods. The swindlers choose groups with mostly Belgian consumers.

- **Fake press articles referring to public figures**

Fake press articles with alleged statements or interviews of public figures or celebrities praising financial investments, especially in cryptocurrencies, also circulate on the internet via fake news websites and via Facebook through sponsored advertisements.

The purpose of this practice is to gain your confidence by using images of well-known personalities in the media, sports or business world. These fraudsters try in this way get you to invest in their offers of investments that are too good to be true.

- **Fraudsters chat with their victims on social media**

Fraudsters 2.0 also use social media to contact their victims personally, either by sending them a friend request, or by chatting with them using the chat boxes of Facebook, Instagram and even LinkedIn.

When such unscrupulous operators initiate a conversation with a new victim, they will not try immediately to tempt the person to invest; quite the contrary. They first try to form a relationship of trust, as is the case with **friendship scams** (http://tropbeaupouretrevrai.be/fraude/les-fraudes-lamitie). Only after chatting for a few hours, weeks or even several months will the fraudsters casually let it slip that they have a golden investment tip.

Some swindlers also open fake accounts by using the identity and the picture of persons who are quite active on social media. To our knowledge, this practice is mostly observed on Instagram.

AVOID BEING A VICTIM OF INVESTMENT FRAUD ON SOCIAL MEDIA

- **Be wary of (promises of) disproportionate returns.** Where a return seems too good to be true, it usually is!
- **Do not accept uncritically the information provided by such companies**. It is not uncommon for a company to claim to be authorized to offer financial services although this is not the case. Be sure always to verify the information you are given (company identity, home country, etc.). If the company is located outside the European Union, you will also have to be aware of the difficulty of legal recourse in the event of a potential dispute.
- **Check whether the company holds an authorization** by searching the lists published on the FSMA website – **Check your provider** (/en). **Be wary as well of 'cloned firms'**: companies that pass themselves off as different, lawful companies even though they in fact have no connection with the latter. A close look at the email addresses or contact details for the companies in question may prove useful in order to detect potential fraud of this sort.
- **Consult the warnings** published on the FSMA website as well as on the website of foreign supervisory authorities and of **IOSCO** (https://www.iosco.org/investor_protection/?subsection=investor_alerts_portal). Check if the company offering you a financial service has been named in a warning. Search not only for the name of the company(ies) in question but also for the one(s) to which you are being asked to transfer money.
- On the FSMA website, this search can be conducted via the **search function** (/en) provided. In addition, all companies about which the FSMA has already published a warning are included on the '**List of companies operating unlawfully in Belgium** (https://www.fsma.be/en/warnings/companies-operating-unlawfully-in-belgium)' published on the FSMA website.
- **Please note**: the fact that the FSMA has not published a warning against a given company does not mean that that company is authorized to offer financial services. While the FSMA seeks to ensure that it publishes warnings in a timely manner, it is entirely possible that a company operating unlawfully on the Belgian market may not yet have come to its attention. Moreover, unauthorized companies regularly change their name.
- **Be wary of unsolicited phone calls/emails (cold calling)**, that is, where no prior request has been made by the investor. Such calls are often indications of an attempt at fraud.
- **Be wary of requests to transfer money to a country without any connection** to the company or to the State of which the investor is resident.
- **Never invest if you do not understand precisely what is being offered.**
- **Be all the more suspicious** if the payout of returns is conditional on an **additional payment** and/or the payment of a tax. These additional demands are often the signs of fraud.

If you have the least doubt about whether the financial services being offered to you are lawful, please don't hesitate to contact the FSMA directly using the **consumer contact form** (/en/consumer-contact-form). As well, feel free to notify it should you come across a suspicious company that has not yet been the subject of a warning by the FSMA.

WHAT TO DO IF YOU ARE A VICTIM OF FRAUD?

If you think you are the victim of fraud, make sure **you do not pay any additional sums** to your contact. Be especially wary if you are promised a refund in exchange for a final payment, as this is a technique frequently used by fraudsters in order to obtain additional funds.

Also, immediately **contact the local police** (http://www.police.be/en) to make a complaint and **alert the FSMA to the scam** via the **consumer contact form** (/en/consumer-contact-form).

The FSMA stresses the importance of filing a complaint **quickly** and with **ample documentation** (the company in question, bank accounts to which you transferred money, etc.).

Similarly, do not hesitate to alert the FSMA to any suspicious company that has not yet been the subject of a warning on its part.

- **Bitcoin-Evolution/Bitcoin-Revolution**