FRAUDULENT ONLINE TRADING PLATFORMS: THE FSMA UPDATES ITS LIST OF SUSPICIOUS SITES

WARNINGS

10/03/2021

During the last weeks, the FSMA continued to receive complaints from consumers concerning new fraudulent online trading platforms that are operating in the Belgian market.

These trading platforms try to arouse consumers' curiosity by placing **scam ads on social media**. In these fake ads, a well-known person often explains how to get rich quick. Trading platforms also **use mobile applications** to lure victims. These fake ads or mobile applications often form part of the offer of a virtual currency or training course. After clicking on the ad or downloading the mobile app and having given their contact details, the victims are usually swiftly called by fraudsters presenting a concrete investment proposal (in shares, alternative investment products, virtual currencies, etc.).

These platforms act very aggressively. Scammers even try to persuade the victims to allow them to take control of their computer remotely in order to make certain money transfers. The fraudsters also try to convince the victims to invest increasingly higher amounts of money.

Recently, these platforms have even hacked into user profiles on social media in order to further spread the aforementioned fake ads.

Victims who agree to do so complain in particular about:

- **finding themselves unable to recover their money**, or
- simply **not hearing any more from the platform** with which they have invested their money.

These are most likely cases of **investment fraud**.

***

The FSMA is aware of the following new fake-ads and websites that refer to subsequent projects and training courses:

- **Bitcoin Loophole** (www.bitcoin-loophole.io)
- **Idées Placement**
- **Yuan pay app (group)**

Moreover, various new trading platforms have appeared on the internet in recent weeks.

The FSMA therefore strongly advises against responding to any offers of financial services made by the following new trading platforms:

- **4TFX** (www.4tfx.io)
- **Binvesting** (www.binvesting.com)
- **BitStarMarkets** (www.bitstarmarkets.com)
- **BTC Brokerz** (www.btcbrokerz.com)
- **Capitalfx** (www.capitalfx.co)
- **Finexics** (www.finexics.com and www.finexics.io)
- **Global Alliance** (www.glballiance.com)
- **Mynetcoin** (www.mynetcoin.net)
- **Quantbitex** (www.quantbitex.com)
- **STR Capital** (www.str-capital.com)
- **Tradezmarket** (www.tradezmarket.com)
- **UnixBroker** (www.unixbroker.com)
- **XTRgate** (www.xtrgate.com)

***

In order to **avoid fraud**, the FSMA addresses the following **recommendations** to investors: **always check the identity** (company name, home country, registered office, etc.) **of the company**. If the company cannot be clearly identified, it should not be trusted.

Always verify if the company in question has the requisite authorization. To this end, an easy **search** on the financial supervisory authority's website will do. Important! Always beware of '**cloned firms'**: companies that pass themselves off as different, lawful companies even though they have no connection with them. A close look at the email addresses or contact details for the companies in question may prove useful in order to detect this type of fraud and prevent it.

More than ever, prudence is necessary. In case of any doubt, and before making any (more) payments, do not hesitate to contact the FSMA using the **consumer contact form**. As well, please feel free to notify it of any contact with a suspicious company that has not yet been the subject of a warning by the FSMA.

Should fraudsters moreover manage to take control of your computer, the FSMA recommends that you contact your bank and, if necessary, that you change your passwords.

***

For more recommendations aimed at avoiding investment fraud, the FSMA invites investors to consult the '**How to recognize and avoid fraud?**' page on its website.