



FINANCIAL SCAMS AND HOW TO AVOID THEM

The MFSA has seen an increase in financial scams reported. This publication is intended to give a snapshot of the most popular scams, tips on how to detect red flags and avoid getting scammed.

FOREX SCAMS

DEFINITIONS • WARNING SIGNS



What is Forex Trading?

Foreign Exchange (FX or forex) Trading is when you attempt to generate a profit by speculating on the value of one currency when compared to another. Foreign currencies can be traded because the value of a currency will fluctuate, or its exchange rate value will change, when compared to other currencies.

Forex trading is considered to be complex and risky, therefore scammers may attract clients by promising to “double” their investment and provide fast, easy, secure, and guaranteed gains. This cannot be guaranteed.

Scammers may request higher deposits and after receiving funds from the consumer, all contact with the consumer might stop.

Consumers should be aware that scammers may make unauthorised use of the details of MFSA licensed entities, in order to mislead the public.

Asking for additional fees or charges in order to withdraw profits, may be a red flag as this tactic is used by the scammer in an attempt to gain more funds from the scammed client.

The MFSA advises consumers to conduct services with licensed and regulated providers. Consumers may check the MFSA [Financial Services Register](#) when in doubt regarding the status of an entity.

CRYPTOCURRENCY SCAMS

DEFINITIONS

• WARNING SIGNS



What are cryptocurrencies?

Cryptocurrencies are virtual currencies which use encryption to ensure the security of transactions and are not centralised or regulated by a financial authority, unlike FIAT currencies (e.g., euros, dollars, pounds, etc.). Cryptocurrencies do not have a physical counterpart and only exist in digital form.

The most common scams are unregulated/fake crypto exchange platforms and fraudulent Initial Coin Offerings (“ICO”). Fake ICOs involve the issuing and selling of a fake coin or token or crowdfunding for the issuing of such coin, which has no underlying value. Consumers are advised to research such investments and refrain from products which they do not understand or cannot guarantee its legitimacy.

Fake cryptocurrency exchanges may attract consumers with their advertised high rates of return or guaranteed gains. However, such exchanges may entice and pressure consumers to invest large sums of money or have hidden fees.

Additionally, scammers may mislead consumers with what appear to be profits made from their investment in order to pressure the consumer to pay withdrawal fees, which consumers may be fooled into paying, especially after investing a large sum of money.

More information on how to detect cryptocurrency scams can be found in the [MFSA guidance note](#).

CLONES

DEFINITIONS

• WARNING SIGNS



What are Clones?

Clones are entities making unauthorised use of the details of a genuine entity, such as company number, license number, company name, registered address, website interface, as well as impersonate officials of the genuine company in an effort to deceive consumers into thinking that they are dealing with a licensed and regulated entity.

Clone entities can come in many forms, the most common being clone websites. Such websites may clone the full content of the legitimate entity's website or may only make use of information which may provide consumers with the illusion that they are licensed and regulated.

Consumers are advised to proceed with caution, remain alert and ask questions about the identity of the entity to ensure the safety of their funds.

Prior to investing, consult the MFSA [Financial Services Register](#) and conduct some internet searches for further information on the entity in question. By searching the name of the company followed by the word "scam" or "fake" may result in reviews or alerts regarding such entity.

More information on how to detect clone entities can be found in the MFSA [guidance note](#).

BANKING SCAMS

DEFINITIONS

- WARNING SIGNS



What are Banking Scams?

Banking scams are unlicensed entities or individuals illegally providing services associated with banking institution, such as loans, payment transfers, credit, and debit card services.

Consumers may be contacted by individuals or entities *via* social media, email, telephone, mail, text messages or messaging apps such as WhatsApp or Telegram (which allow messages to disappear). Scammers may threaten that your bank account is in danger unless you take immediate action (example: urging consumers to click links sent *via* text).

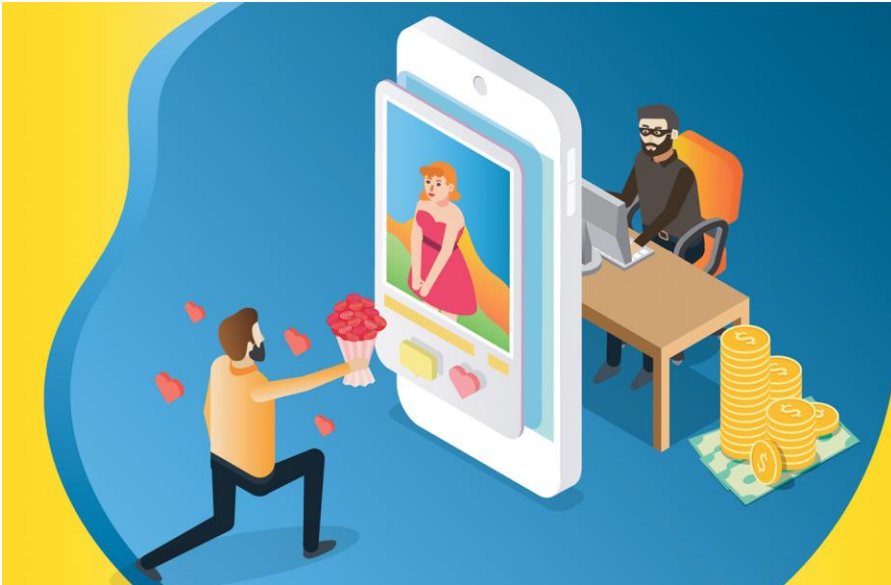
One should be aware of *spoofing* attempts; this is when scammers use technology to disguise the real number and make it appear to be from someone you know or a company you trust (such as your bank) in an attempt to trick you into clicking links and providing personal information. The MFSA advises consumers to proceed with caution and inspect all text messages and calls received.

Scammers may promise fast and easy loans (“**instant approval**”, “**no initial deposit**”, and “**cheap loans**”) however they will have hidden high interest rates and fees. They may also ask for personal bank details in order to make the “deposit”, however providing your personal information to such individuals may lead to possible loss of funds and/or identity theft.

The MFSA advises consumers to conduct services with licensed and regulated providers. Consumers may check the MFSA [Financial Services Register](#) when in doubt regarding the status of an entity.

GENERIC SCAMS

DEFINITIONS • WARNING SIGNS



General Scams?

The general public should be aware that scams appear to have increased in different areas, not only financial services. Scammers may target those emotionally and financially vulnerable.

Romance scams – Involve building a personal relationship with the victim, be it romantic or otherwise in order to request money from such person, common scenarios include medical bills, plane tickets, debt, and other urgent situations. Scammers may invest considerable amount of time into such schemes.

Money recovery scams – Situations in which scammers may take advantage of a recent scam victim and promise to recover their losses but these may in fact be the same individuals which scammed the consumer to begin with.

Phishing email scams – Be aware of emails received from what appears to be a service provider you utilise, such as your bank or insurance provider. These may request you to take some sort of quick action, click a link, change your password or provide any personal information. Banks have secure methods where they communicate with consumers, always double check!

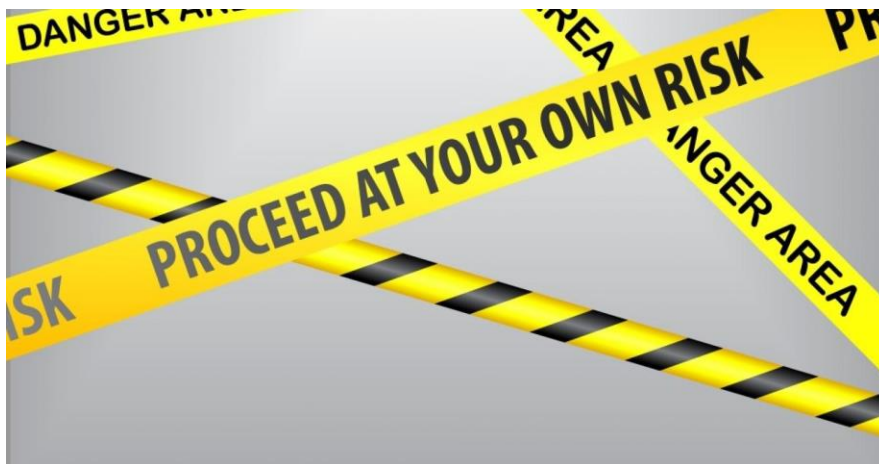


WHAT TO CONSIDER BEFORE INVESTING



Proceed with caution!

The MFSA advises consumers to proceed with caution when considering new investment avenues and take into consideration a number of risk factors.



- ✓ Take your time to research the entity or individual, a legitimate entity will not pressure you to invest.
- ✓ Carefully read any documentation, contracts or terms and conditions for potential red flags (spelling mistakes, inconsistencies, signs of tampering).
- ✓ **Do not share personal details such as ID card number, address, bank or card details, passwords to personal accounts and other identifiable information.**
- ✓ Do not invest in products you do not understand.
- ✓ Be aware of suspicious emails from service providers which include links or requests for personal information.
- ✓ Do not respond to financial offers made over telephone, social media, or mail.
- ✓ Do not invest unless you have identified the company or individual with whom you are undertaking a business transaction.

The MFSA advises consumers to conduct services with licensed and regulated providers. Consumers may consult the MFSA [Financial Services Register](#) when in doubt regarding the status of an entity.

RED FLAGS



- Use of aggressive selling techniques (promises of extra earnings, special benefits and “not to be missed” discounts).
- Entity or individual does not hold financial services license and is not a registered company.
- Promising unrealistic returns, quick riches, risk free and guaranteed gains.


Join Us and Start Getting Rich

- Does not provide reliable documentation, client contracts or provides fake documents.
- Modern advance fee scam, requesting a fee as seen below, (holding your “earnings” behind a fee).



- Limited offers or timers as seen below, pressuring consumers to invest as soon as possible.

WARNING: Due to extremely high media demand, we will close registration as of 28/08/2019 - HURRY! 03:30.2

- Requesting personal details without providing proof of their own identity.  <https://>
- Lack of secure networks and websites (no padlock near the URL of the website)
- If it sounds too good to be true, it probably is!**

I think I have been scammed, now what?

If you are a victim of a scam or think you might be dealing with a scam you should immediately cease to conduct any transaction with the company or entity and contact the MFSA at <https://www.mfsa.mt/about-us/contact/> as soon as suspicion arises.

Gather as much information as possible which may assist the MFSA to identify the individual behind the scam.

It should be noted that scams may be considered fraudulent in nature which constitutes a criminal offence, therefore you may consider contacting the appropriate law enforcement agencies.