Warning on Frauds and Scams

Protect Yourself – Be Scam Aware

REMEMBER: If it is too good to be true, it probably is! When in doubt, apply the scam test:

S – seems too good to be true

C – contacted out of the blue

A – asked for personal details

M – money is requested

Anyone can be the target of financial fraud and scams. Your best defence is to stay informed, alert and secure. Below you will find information on the most common financial services scams, as well as key advice and tips to help you avoid becoming the next victim!

Examples of Common Scams

The following are just some examples of common financial frauds. However, it is important to remember that perpetrators of fraud are constantly designing new ways to target their next victims. For this reason, you should remain vigilant and consider the possibility of fraud, even if the circumstances do not exactly fit one of the below examples. You should also keep an eye out for notices or warnings issued by your local regulator, exchanges or other market participants regarding patterns of fraudulent activity.

Clone Firm Scams:
Scammers may pretend to be from a legitimate firm to get you to transfer money to their account. In some cases, scammers may pretend to represent or be part of a reputable financial services company, including XTB. The purpose of a Clone Firm Scam is to get you to transfer your money to an account that appears legitimate but which in fact belongs to the fraudsters.

These scams often involve the fraudster using a reputable firm's logo or letterhead, adopting names that resemble those of the reputable firm, or even using names and addresses of persons who are associated with the real firm.

Be wary of cold calls or emails you receive requesting money from you. Check to make sure all emails use the firm's real domain name (for XTB, xtb.com or xtb.co.uk). Be especially careful of any unprompted interactions through social media platforms – XTB may promote its general products and services on social media but it will never interact with you through these channels in relation to your account nor prospective account. If you are unsure whether a communication is legitimate, please contact XTB Client Services.

Remember, if you invest your money with an unregulated firm you will not be entitled to compensation schemes, such as the Investor Compensation Scheme, Financial Services Compensation Scheme, or recourse to the relevant financial ombudsman for dispute resolution.

Identified XTB Clones

Here are individuals operating as Clone Firms of XTB the FCA has identified:

https://www.fca.org.uk/news/warnings/xtb-limited-clone-fca-authorised-firm

https://www.fca.org.uk/news/warnings/xtb-trading-world-clone-fca-authorised-firm

https://www.fca.org.uk/news/warnings/xtb-group-clone-fca-authorised-firm

https://www.fca.org.uk/news/warnings/xtb-global-clone-fca-authorised-firm

Watch out for Red Flags!

Here are some red flags you should watch out for, if contacted by someone claiming to work for XTB or otherwise be affiliated with XTB:

- XTB does not cold call consumers to offer services or products nor does it make investment recommendations.
- XTB does not directly interact with customers through social media channels.
- XTB does not charge you for assistance or guidance in completing an account application.
- XTB does not charge you a fee to withdraw your funds.
- XTB does not ask for remote access to your computer or mobile device.
- XTB does not ask you to action an internal or external transfer of stock or money over the phone.
- XTB does not ask you to share login details, particularly when this is done by creating a sense of urgency (e.g. “we have detected a fraud/theft attempt on your account and need your log in details to stop/deflect it” or “we have been made aware of a crash in one of the products you currently hold and will help you sell it now before it loses X% of its value”).

Check and Double Check!

If you are contacted by someone claiming to work for a regulated firm, remember:

- Verify the details of the firm on its local regulator’s website. For XTB UK check:
    - Financial Conduct Authority, in the United Kingdom: https://www.fca.org.uk
- Beware that scammers may point you to the real firm’s genuine website but use different details for their communications with you. You should use the information you found on the local regulator websites to contact the firm.
- You can contact XTB to verify the information or to report your concerns from this page: uksales@xtb.com
- You can check what products and services we offer: https://www.xtb.com/en

- If you do not hold an account with XTB please report any concerns of fraud to the police in your home jurisdiction. In the UK, you can make a report directly to;
    - https://www.fca.org.uk/consumers/report-scam
    - https://www.fca.org.uk/contact
    - https://www.reportfraud.police.uk

- The FCA also has a Firm checker to check if a Firm is authorised by them and has their permission to provide the services you want;
    - https://www.fca.org.uk/consumers/fca-firm-checker

Pump-and-Dump or Ramp-and-Dump Schemes: In these schemes, scammers invest in a stock and then spread false or misleading information to create a buying frenzy that will artificially "pump" up the price of a stock. They then "dump" their own shares at the inflated price and stop hyping the stock, leading other investors to lose money as the stock price fails. Those recommendations may be presented as 'hot' information, from people in 'the know' and made available to you due to some privileged or special status.

Scammers often take full advantage of new technologies to spread false or misleading information about a company's stock price. For example, trading "recommendations" are frequently spread through messaging apps, social media platforms and/or web blogs.

Please also remember that XTB does not provide investment advice. Be wary of anyone stating otherwise.

Trash-and-Cash Schemes: These are the opposite of pump and dump schemes. In Trash-and-Cash schemes, scammers circulate false information to encourage people to believe that a relatively illiquid security is likely to plunge in value and should be sold. When those who see this information sell the security, the price plummets and the scammers then swoop in to buy it up at a low price.

Pension Liberation Scam: Pension benefits are, in most jurisdictions, only accessible once a minimum pension age has been reached. Early access is normally possible but often leads to "early withdrawal penalties". With this scam, fraudsters promise "penalty free" early access to pension benefits through alleged tax loopholes and use complex schemes to erode pension accounts through commissions, investments, etc.

Affinity Fraud: Scammers who carry out affinity scams frequently are (or pretend to be) members of the group they are trying to defraud. Scammers exploit their victim's age, religious, ethnic, sexual, or professional identity to gain their confidence knowing that it's human nature to trust people who are like you. Affinity fraud almost always involves either a fake investment or an investment where the fraudster lies about important details (such as the risk of loss, the investment's track record, or the scheme promoter's background).

Many affinity frauds are Ponzi or pyramid schemes, in which money given to the promoter by new investors is paid to earlier investors to create the illusion that the so-called investment is successful. Eventually, when the supply of investor money dries up and current investors demand to be paid, the scheme collapses and investors discover that most or all of their money is gone.

To protect yourself against affinity fraud, always carry out your own research and due diligence before entering into arrangements to accept investment advice or services. In particular, you should always verify the credentials of the person or company offering the service and confirm whether they are regulated to carry out that activity by checking the register of your local regulator.

Holy Grail Scams: Scammers are well aware of the attraction of a 'holy grail' trading system that will generate profits 24/7/365 with no risk or losses. One common tactic is to market a secret formula or strategy that promises extraordinary returns. Be aware of extravagant claims and testimonials that seem too good to be true. They usually are!

Romance / "Pig-Butchering" Investment Scams: Scammers build a personal or romantic relationship (often via dating apps, WhatsApp, Telegram, or social media) and gradually introduce "investment opportunities" (often crypto, FX, or commodities). Key features include; long grooming phase to build trust, fake trading platforms showing "profits", pressure to reinvest and add more funds, withdrawal blocked unless additional "fees" are paid.

Crypto-Specific Scams: Examples include; fake crypto exchanges or wallets, "Airdrop" scams asking for wallet credentials, rug pulls (developers abandon a project after funds are raised), impersonation of crypto support teams.

Recovery Room / Fund Recovery Scams: Victims of previous scams are contacted by someone claiming they can **recover lost funds** — often pretending to be: regulators, law firms, blockchain investigators, asset recovery specialists. These may be **scams**, and victims are targeted *because* they were previously scammed.

Impersonation of Regulators or Law Enforcement: Fraudsters can pretend to be from; financial regulators, police, tax authorities, courts. They can claim; your account is under investigation, funds must be "secured" or transferred, immediate action is required to avoid arrest or penalties.