FRAUD WARNING

Protecting Yourself from Cryptocurrency Scams: A Guide for Our Clients

At GXO, we prioritize your security and want to ensure that you are well-informed about the risks associated with cryptocurrency. Cryptocurrency transactions are irreversible, which makes security awareness essential. While we strive to offer a secure environment for your crypto-related activities, it is crucial to stay alert to potential scams, which are becoming increasingly sophisticated.

Below is an overview of common cryptocurrency scam tactics and ways to avoid them.

Common Cryptocurrency Scam Types and Warning Signs

1. Phishing Scams

• Description: Scammers often impersonate companies or trusted entities through emails, fake websites, or social media, prompting users to provide sensitive information or log in to a fake account.

• Signs to Watch For: Be cautious of unexpected messages, especially those urging you to click on links or log in. Look for slight misspellings in URLs or suspicious email addresses that do not align with official company contact information.

2. Investment Scams

• Description: Scammers promise high returns on "guaranteed" cryptocurrency investments, often through social media or websites that appear legitimate. They may impersonate famous personalities or crypto influencers to gain trust.

• Signs to Watch For: Be wary of any investment that seems too good to be true, or if you are pressured to "act now" to avoid missing out. Legitimate investments never come with guaranteed returns or urgent demands.

3. Fake Customer Support or Tech Support Scams

• Description: Scammers pose as customer service representatives for crypto exchanges, wallets, or service providers, often contacting victims via email or social media, claiming that there is an issue with their account.

• Signs to Watch For: Legitimate customer support will never ask for sensitive information like passwords or private keys. Always verify support contacts by checking the official website.

4. Ponzi and Pyramid Schemes

• Description: Ponzi schemes promise consistent returns by paying earlier investors with funds from new investors, rather than legitimate profits. These scams collapse once new investments can't cover the payouts to previous investors.

• Signs to Watch For: Be cautious of any program that promises high returns with little or no risk, or requires you to bring in new members to earn commissions.

5. Romance Scams

• Description: Scammers build personal relationships with victims online, often on social media or dating platforms, and then persuade them to invest in fake cryptocurrency opportunities or send cryptocurrency directly.

• Signs to Watch For: If someone you have never met in person begins asking for money or encourages you to invest in a specific cryptocurrency, this is a major red flag.

6. Impersonation Scams

• Description: Scammers pose as GXO employees or other legitimate organizations, requesting funds or sensitive information.

• Signs to Watch For: GXO will never contact you to ask for sensitive information such as passwords, private keys, or to send funds. Always contact us directly atfraud@gxo.limited to verify any communication.

7. Fake Initial Coin Offerings (ICOs) and New Cryptocurrencies

• Description: Fraudsters launch fake ICOs or new coins, promising they will be the next big investment. They create convincing websites and whitepapers to appear legitimate.

• Signs to Watch For: Research thoroughly before investing in new ICOs or cryptocurrencies. Verify the credibility of the development team, check for reviews from reliable sources, and avoid "exclusive" investment deals.

8. Malware Scams

• Description: Malware (malicious software) can compromise your computer or smartphone, giving scammers access to your private data and funds. This malware can be hidden in fake wallet apps, malicious ads, or phishing links.

• Signs to Watch For: Only download apps and software from trusted sources. Avoid clicking on unfamiliar links, especially those in emails or messages from unknown senders.

How to Protect Yourself from Scams

1. Secure Your Private Keys

Never share your private keys, passwords, or account details with anyone. Your private key is the most sensitive information in your crypto wallet and must be kept secure.

2. Verify All Communications

Any legitimate communication from GXO will come through official channels. If in doubt, contact

us directly atfraud@gxo.limited.

3. Stay Informed and Vigilant

Cryptocurrency scams evolve quickly. Stay up to date on the latest security threats and regularly review this page for updates.

4. Double-Check Links and URLs

Only visit our official website: www.GXOcapital.io and trusted cryptocurrency exchanges. Bookmark these pages for safety and never click on links sent via email or social media unless you are sure they are legitimate.

Important Notice: Our Responsibility

GXO is committed to providing a safe environment for transactions and follows strict security protocols. However, we do not assume responsibility for any losses due to scams or fraudulent activities.

Since cryptocurrencies are decentralized and transactions irreversible, the responsibility to secure your funds and avoid scams ultimately lies with you, the account holder.

Stay Safe, Stay Informed

Cryptocurrency offers new opportunities and risks. By understanding and recognizing these scams, you can protect your assets and have a safer experience in the digital currency world.

If you have any concerns or questions about secure transactions, please contact us at:fraud@gxo.limited