بيت الاستثمار
Investment House

FRAUD AND CYBER ATTACK AWARENESS

Fraud and Cyber Attack Awareness:

Investment House is a leading company in alternative investment management, encompassing various business sectors. Criminals, including cyber attackers, may attempt to exploit the name of Investment House to engage in fraudulent activities or other criminal acts. Victims are deceived through the impersonation of the company's name, reputation, or employees. Through this impersonation, victims are misled into believing they are interacting with Investment House or its employees, resulting in the disclosure of sensitive personal information or even the transfer of funds under the false impression that these funds are being sent to Investment House.

Recently, we have found that fraudulent entities are carrying out actual scams via email and websites. These platforms target members of the public and potential investors (victims) by unlawfully using the identities of the executive team or board members of the Investment House. Their objective is to solicit investments, present fake job offers or engage in other transactions without authorization and for malicious purposes.

The CEO of Investment House and any member of its Board of Directors or the Executive Team, has not made any offers for investment partnerships, job opportunities, or any transactions through these channels. The names and identities of these individuals are being used illegally and without their consent.

These fraudulent activities are carried out through various means, including websites, mobile applications, text messages, emails, postal mail, phone calls, social media platforms (including videos uploaded to social media), and other communication platforms such as WhatsApp, Telegram, and others. Although the tactics of these criminals are constantly evolving, many of these scams rely on a method known as "phishing." In phishing, cybercriminals attempt to obtain your confidential personal information (such as your name, date

of birth, address, social security number or other official documents, account/financial details, usernames, and passwords) to use them for unauthorized and illegal purposes.

Investment House is committed to upholding the highest standards of security and integrity, ensuring the protection of personal data in compliance with Law No. 13 of 2016 on the Protection of Personal Data. Our policies and procedures are designed to prevent unauthorized access, data breaches, and fraudulent activities. We strictly ensure that personal data is not collected, stored, or processed without a clear legal basis or the individual's explicit consent. In the event of a data breach or unauthorized access to personal information, affected individuals and relevant authorities will be promptly notified.

Fraud reports are handled with strict confidentiality and retained solely for investigative purposes. Additionally, Investment House ensures that personal data is not shared or transferred outside Qatar unless required by law and done in compliance with applicable regulations.

Examples of common scams:

1. Phishing/Vishing Fraud: This involves a criminal sending an email, text message, or any other type of electronic communication (such as through mobile apps, social media platforms, or other messaging tools like WhatsApp or Telegram etc.) that appears to come from a trusted source. These messages typically ask you to click on a link, download an attachment, or provide personal information. A similar tactic, called "vishing" (voice phishing), involves a criminal calling you and pretending to represent a company (for example, Investment House), warning of a potential issue with your information that could lead to financial loss or harm. They claim they can resolve the issue if you provide your personal information.

2. Recruitment Scams: Criminals may target job seekers by impersonating an organization and offering job opportunities through unauthorized websites, social media accounts, or untrustworthy emails. Please note that all legitimate job openings at Investment House can be found here.

3. Mobile App Scams: Criminals may attempt to steal personal information by creating mobile apps that claim to be the official application of the company. Please be advised that Investment House currently does not offer a mobile application.

4. Bank Transfer Scams: Criminals may contact you via phone, email, or other means, presenting an urgent and fabricated story. They may request you to transfer funds to or from your bank account or another party's account.

5. Investment Scams: Criminals may approach you with fake or non-existent investment opportunities, claiming exceptional returns on products allegedly managed by Investment House. They may promote these investments via websites, mobile apps, or social media channels, aiming to unlawfully persuade you to transfer funds to them.

How to Report Fraud:

We encourage you to contact us immediately at "fraud-detection@inveshouse.com" if any of the following occur:

1. If you have received any untrusted communications, investment advice, or been contacted regarding a fraudulent activity (whether via phone, email, or postal mail) from sources impersonating members of the Board of Directors or any member of the executive team of Investment House.

2. If you have been notified by someone outside Investment House that they have been contacted by sources impersonating members of the Board of Directors, executive team, or employees of Investment House.

3. If you receive any communication referencing the names of Investment House Board Members and feel that these messages are suspicious or are unsure how to respond to them.

4. If you have any doubts about the credibility of a website claiming to be affiliated with Investment House or referencing the names and identities of the Board Members or any executive team members without permission.

5. If you have any questions about the above or suspect that a website, mobile application, email, or any other communication (including on social media) claiming to be from or associated with Investment House may be fraudulent, please contact us at " fraud-detection@inveshouse.com"

Protect Yourself:

We strongly recommend that you do not engage in conversations with fraudsters or disclose any personal or identifiable information. Instead, try to record the alleged name of the individual, the organization, and any other information they provide (such as a phone number or address). Send all this information to "fraud-detection@inveshouse.com".

To invest in portfolios and funds managed by the company or represented by the company as an agent, you must do the following:

- Meet directly with the company's representatives or customer service team at the company's premises, as the company does not offer its products or investment services online or remotely.

- Seek independent legal, financial, and advisory consultation before handing over any funds or entering into any agreements related to such solicitations.

-We also recommend that you avoid responding to, opening attachments from, or clicking on links in suspicious emails.