Phishing and Fraud Awareness

Cybercriminals frequently attempt to take advantage of ThinkTank IFSC Pvt. Ltd.'s reputation to engage in fraudulent schemes, through which victims are tricked into thinking that they are dealing with trusted ThinkTank IFSC Pvt. Ltd. personnel, including through websites, texts, emails, mailings, telephone calls, social media, and other communication platforms. These fraudulent tactics are continuously evolving and usually involve using false pretenses to convince a victim to share personal information. Many of these attacks take the form of "phishing," a practice where a cybercriminal attempts to obtain your confidential personal information, such as your social security number, account/financial information, and usernames/passwords.

Below is general information on how to recognize and avoid common schemes.

Common Examples of Fraudulent Activities

Email or SMS (Text) Phishing: The most common form of phishing involves a cybercriminal sending an email or text message that looks like it comes from a legitimate source, asking you to click on a link, download an attachment, or provide personal information.

Vishing: Vishing, or telephone phishing, involves a cybercriminal calling you on the phone, pretending to be a company representative. The visher will say there is an urgent problem that will cause you financial harm, and their solution will involve you providing your personal information.

Job Offer/Social Media Scams: Scammers may pose as a company on a website or social media account, and may target job seekers through posts and paid advertisements. Imposters may also send fraudulent emails purporting to offer employment at ThinkTank IFSC Pvt. Ltd. and misusing the official ThinkTank IFSC Pvt. Ltd. logo. These emails do not originate from ThinkTank IFSC Pvt. Ltd. or any of our affiliates. The only social media accounts authorized by ThinkTank IFSC Pvt. Ltd. are: Twitter, Facebook, Instagram, LinkedIn, YouTube. The official ThinkTank IFSC Pvt. Ltd. podcast can be listened to on Apple, Spotify and SoundCloud.

Mobile Device App Scams: Scammers may steal personal information by creating mobile device apps which purport to be an official ThinkTank IFSC Pvt. Ltd. app, including a fraudulent mobile device app using a gold diamond logo. The scammers solicit investments into non-existent managed funds and are not in any way affiliated with ThinkTank IFSC Pvt. Ltd..

Bank Transfer Scams: Scammers may contact you, usually by phone but potentially by other means, presenting an urgent and false story that requires you to transfer money into or out of your bank account. Scammers purporting to be ThinkTank IFSC Pvt. Ltd. may also promise extraordinary returns on your investment at little to no risk.

Investment Scams: Scammers may contact you offering “high-yield” and similar investments through ThinkTank IFSC Pvt. Ltd.. These “high-yield investment programs” typically are frauds. For more information on high-yield investment programs and how to avoid them, visit the U.S. Securities and Exchange Commission webpage.

Best Practices

Confirm you are visiting a Best Practices

Confirm you are visiting a ThinkTank IFSC Pvt. Ltd. authorized site or communicating with an account authorized by ThinkTank IFSC Pvt. Ltd.

Read email carefully. Pay close attention to the details of your emails. Pay attention to things such as typos, unfamiliar links, attachments and any other awkward or urgent language. Do not click on any links in the email that appear suspicious or enter any of your bank [or personal] information.

Do not share password or login information. Certain ThinkTank IFSC Pvt. Ltd. web sites are private, available only to clients through secure log-in procedures. Apart from allowing you to use your password and log-in to enter an authorized website, ThinkTank IFSC Pvt. Ltd. will never ask you for your login information or password.

Avoid suspicious downloads. Be sure to double check the sources and validity of content and apps that you’re downloading while online and always avoid suspicious pop-up ads.

Be skeptical of unsolicited emails, text messages or phone calls. You should be suspicious of emails, texts or phone calls coming from unknown senders and unfamiliar organizations, especially if personal information is requested.

Be suspicious of phone calls asking for personal information. Often callers will impersonate your bank, a familiar company like ThinkTank IFSC Pvt. Ltd., or a government organization. Do not provide personal information, such as your bank information or credit card number, to these callers. If you think the call might be legitimate, hang up, separately look up the organization’s official contact information online and call them.

Be skeptical of changes to wire or payment instructions. If this happens, you should hang up, separately look up the official contact information of the organization requesting payment, and call them to verify. ThinkTank IFSC Pvt. Ltd. will never ask you to solicit payment of funds or wiring of funds over the phone, email, or text.

Be skeptical of job offers made through social media. ThinkTank IFSC Pvt. Ltd. does not hire from social media or conduct interviews via text or messaging services, nor will ThinkTank IFSC Pvt. request payment in connection with the hiring process. All openings at ThinkTank

IFSC Pvt. Ltd. can be found here. authorized site or communicating with an account authorized by ThinkTank IFSC Pvt. Ltd