Fortune Integrated Assets Finance Limited

THE INVESTMENT TRUST OF INDIA
ASSET FINANCE

May 23, 2020

Dear Customer,

Sub: Alert about cyber attack on financial institutions and awareness to follow secure practices as advised by Reserve Bank of India (RBI) in its Alert 5/2020 dated May 21, 2020 issued by Cyber Security & IT Risk (CSITE) Group of RBI.

Among numerous precautionary measures, the COVID-19 outbreak is also encouraging the use of digital payments. Even the RBI has urged customers to use digital banking facilities, ensuring contactless transactions with secure practices to be followed as mentioned below.

1. **Search the Internet carefully**

When you are looking for any product reviews or price comparisons on a search engine on mobile or PC, you run the risk of unintentionally clicking on a 'poisoned' search result that can lead you to malware instead of your intended destination. Poisoned search results are created by Hackers who use search engine optimization tricks

2. **Avoid public Wi-Fi/computers**

Never do financial transactions on a public Wi-Fi. Hackers can intrude easily into a public Wi-Fi network and steal your login details. If you need to make a financial transaction when you are out, use your own mobile phone network. Avoid using unsecured, unknown Wi-Fi networks. Hackers are having access points at public places used for distributing malicious applications.

3. **Keep your data to yourself**

Don't save your bank and personal details in a browser or a payment site. Type the information whenever you make a transaction. Don't forget to log out every time you log in.

4. **Avoid apps that you can't trust**

Often, smartphone apps carry malware. If you are not sure of an app, don't download it instantly. Spend a little time reading about it, going through its terms and conditions and knowing what current users say about it. Only download apps from the official app store. Not to download and install applications from untrusted sources. Verify app permissions and grant only those permissions which have relevant context for the app's purpose. In settings, do not enable installation of apps from "untrusted sources"

5. Check for latest updates of your Smartphone's operating system

Smartphone users should make sure their operating system is updated with the latest security patches and updates. You should also not remove the security controls from the phone often called 'jail breaking' or 'rooting'. You should always look to restrict access that apps ask for when being installed to only what the app really needs.

6. Change your password regularly and ensure it's a strong one

It is important to keep your account safe and helps you maintain confidentiality. And needless to say, don't share your details with anyone. Your bank will never ask for your confidential information via phone or email. If you have written your banking passwords in a notepad or a dairy, make sure it remains confidential.

Further, be sure to choose strong and long passwords. For additional security to financial transactions through Internet Banking, create and maintain different passwords for log-in and for transactions.

7. Avoid signing-in to your net-banking account via mailers

It is always safer to type the bank URL yourself than getting redirected to it via a promotional mail or any other third party website. As mentioned earlier a bank will never ask you to for the login credentials to your account. So if there's a fraudulent email which offers to redirect you to your bank's website and you enter your personal details on landing page after clicking it, there's a huge risk of your login credentials being stolen. Hence, if you receive an email from a bank asking for login details, treat it with suspicion.

8. No Phishing Allowed

Beware of phishing emails. These emails are designed to prompt you to click links provided within the email to verify or change your account in some way. Often, the links included in the email are ways for fraudsters to install malicious software (also called Malware) onto the computer or device you use to access your email. This Malware can be used to obtain personal information. Refer to security best practices for mobile phone users: https://www.cyberswachhtakendra.gov.in/documents/Mobile_phone_Security.pdf

9. Use a dedicated computer

You can keep a computer solely for financial transactions. Install Google Chrome with HTTPS enforcement and also a trusted anti-virus program. Keep the dedicated computer clean: don't use it for casual surfing or social networking.

10. Be a Selective Sharer

These days, there are a lot of opportunities to share our personal information online. Just be cautious about what you share, particularly when it comes to your identity information. This can potentially be used to impersonate you, or guess your passwords and logins.

Thanking you

Chintan Valia
Managing Director