Bal Bharati PUBLIC SCHOOL
Sector -21, Noida

Circular No.19/2021-22 Date : 02 Aug, 2021

# MODUS OPERANDI OF FINANCIAL FRAUDSTERS

Dear All,

It is my bounden responsibility as a school educator to spread awareness about financial fraudsters. They have been using innovative methods to defraud the hard-earned money of common gullible people, especially new entrants and senior citizens who are not entirely familiar with techno-financial eco-system. In this regard a paper on modus operandi of financial fraudsters is being forwarded by the Financial Management Wing of the School.

Hope this helps you to an extent to cope up with fraudsters in near future.

1. **Phishing Links**

Modus Operandi

- Fraudsters create a third-party website which looks like existing genuine website, such as bank's website or e-commerce website or search engine, etc.
- These links are generally circulated by fraudsters through SMS/ social media / email / Instant Messenger etc.
- Most of the time, customers enter secure credentials by just having a glance and clicking at the link but not checking the detailed URL.
- The links are masked through authentic looking names of websites, but in reality, the customer gets redirected to phishing website.
- When customers enter secure credentials on these websites, the same is captured and used by the fraudsters.

Precaution

One should not click unknown links and should delete the SMS/email immediately to avoid accessing them in future. Care should be taken to verify the website details especially where it requires entering financial credentials.

2. **Vishing Calls**

Modus Operandi

- Imposters call or approach the customers through telephone call / social media as bankers / company executives / insurance agents / government officials, etc., and seek confirmation of the secure credentials by sharing few details such as name or date of birth to gain confidence.
- In some cases, the imposters pressurize / trick customers into urgently / immediately sharing confidential details citing emergency, details required to block transaction, payment required to stop penalty, get attractive discount, etc. These credentials are then used to defraud the customers.

Precaution

Banks officials / financial institutions / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP.

3. **Frauds using online selling platforms**

Modus Operandi

- Fraudsters pretend to be buyers on online selling platform & show interest in your product.
- Instead of paying money to you, they use "request money" option through UPI app and insist to approve the request to pull money from your bank account.

Precaution

- One should be careful while making financial transactions for online products.
- Always remember, to receive money there is no need to enter your PIN /password anywhere.
- If UPI or any other app asks you to enter your PIN to complete transaction, it means you will end up sending money instead of receiving it.

4. **Frauds due to use of Unknown / Unverified Mobile Apps**

Modus Operandi

- Fraudsters gain access to your mobile device /laptop /desktop once you download unknown / unverified mobile apps.
- These application links are generally shared through SMS / social media / Instant Messenger, etc. The links are masked through authentic looking names but in reality customer is redirected to download unknown application.
- Once the malicious application is downloaded, the fraudster can gain complete access to the device.

Precaution

Never download application from unverified / unknown sources.

5. **Frauds using Screen Sharing App / Remote Access**

Modus Operandi

- Fraudsters trick you to download screen sharing apps through which they can watch / control your mobile / laptop to gain access to your financial credentials.
- Later they make payments using your Internet banking / payment apps.

Precaution

Do not download or activate share screen share feature with unknown people.

6. **Frauds by compromising credentials on results through Search Engines**

Modus Operandi

- It has been observed that customers use search engines for obtaining contact details of their bank, insurance company, Aadhar updating centres, etc., and may end up contacting unknown / unverified contact numbers displayed on search engine.
- These contact details on search engine are often camouflaged by fraudsters to attract their victims towards them.
- Once the customers call them, the imposters ask the customers to give their card credentials / details for verification.
- Assuming this contact to be genuine, people compromise all their secure details & thus fall prey to frauds.

Precaution

Avoid searching for customer care contact details on search engine. These are often camouflaged by fraudsters. One should always look for official websites of Banks / companies to get contact details.

7. **Impersonating through Social Media**

Modus Operandi

- Fraudsters create fake account on popular social media platforms like Facebook and Instagram. They send a request to your friends asking for money for urgent medical purposes, payments, etc.

- Fraudsters also gain trust over a period of time and use the private information for extortion or blackmail later.

Precaution

- Do not make payments to unknown persons online.
- Do not share personal and confidential information on social media platforms.
- Always verify genuineness of fund request with the friend / relative or confirm by a phone call / physical meeting to be sure that the profile is not impersonated.

8. **Juice Jacking**

Modus Operandi

- The charging port of a mobile, can also be used for transfer of files / data.
- Juice jacking is a type of cyber stealing, where, once your mobile is connected to unknown / unverified charging ports, unknown apps / malware are installed with which, the fraudsters can control / access / steal sensitive data, email, SMS, saved passwords.

Precaution

Always avoid using public / unknown charging ports / cables.

**(RELEASED TO SPREAD AWARENESS BY THE FINANCIAL MARKETING AND MANAGEMENT CELL OF THE SCHOOL)**

**Asha Prabhakar**
(Principal)
स्वच्छ भारत
एक कदम स्वच्छता की ओर