Frauds and Forgery through Mobile Devices

Mobile phones have led us humans to a very sorry state of affairs. Look around. Be it at the dinner table, a family function, a formal meeting or any social gathering. You can easily take stock of how a mobile phone has reared its ugly head! Do mobile phones really deserve so much attention and power to ruin our lives? Think about it.

People now find it difficult to stay without their mobile phones even for a split second. So much so that the addiction to mobile phones has led to a new form of a mental disorder called 'Nomophobia'- *the fear of being without a Mobile Phone* has now been gripping population of nations all across the globe. It is the result of the insidious addiction to mobile phones for various activities, often to avoid boredom and loneliness.

People suffering from nomophobia tend to experience stress, anxiety, depression, and loneliness when parted from their mobile devices.

Therefore, mobile phones have the potential of ruining your health as well as defrauding you through mobile phone frauds. Be wary of the common mobile phone frauds too!

Mobile phones have become the hot spot for hackers and fraudsters due to their widespread usage. This makes mobile users very susceptible to missed call frauds, mobile phone text frauds, and various other frauds. Through mobile phone frauds and forgery, we stand the chance of losing our respect, identity and/or money

Top Mobile Phone Frauds

Here are some of the top mobile phone frauds/frauds that users must be cautious of.

1. Mobile App-based Frauds

Google Play Store has more than 3.3 million apps at present. This is sure to spoil you for choice. While it may be fun and engaging to have multiple apps on your mobile phone for various activities, there may be malicious apps also in these offerings.

Make sure that you always demand the proper credentials of the caller including a return phone number. Abstain from disclosing any personal or financial information over the phone, especially when the call is not initiated by you.

5. Mobile Cloning

In case fraudsters gain access to your IMEI number, you stand the chances of being the victim of mobile phone frauds such as cloning.

The IMEI number is unique to a particular phone and can be used to program another mobile phone. This enables them to make you pay for the calls made or data used from the cloned phone!

It's shocking that more than 1,300 cases of mobile cloning were registered from 2009 to 2012 in India!

If you find yourself paying for mobile bills that you find suspicious, contact your network provider immediately. They may be able to assist you in tracking if the calls were made on your phone or a cloned phone? In fact, check with your mobile insurance provider about coverage of unauthorized calls.

6. Subscriber Fraud

Subscriber Frauds are also the top mobile phone frauds defrauding users by gaining access to their personal information. In such mobile phone frauds, a conman opens a mobile phone account using the victim's name. You may be paying ridiculously high bills even without realizing that you are a part of a mobile phone fraud. However, what you may not want to hear is that it's not an easy process to prove that you haven't opened the account yourself!

To avoid such mobile phone frauds, avoid sharing your identity or personal details with anyone. In case you feel you have been targeted for subscriber fraud, contact your mobile phone carrier immediately.

7. Ransomware Frauds

Yes, it is not just your computer but also your mobile phones that are prone to a ransomware attack! Mobile ransomware frauds are just like computer-based ransomware attacks. In this too, fraudsters hold the victim's phone ransom till a payment is received to free it.

Stay alert! In case your mobile's screen freezes suddenly while surfing the net, this is what is likely to happen next. You would then receive an official-looking message asking you to pay a fine for legal violations. It would ask you to deposit the penalty into a debit account in order to use your phone again.

This is a mobile ransomware fraud. Report such ransomware frauds immediately and NEVER make any payments for ransom.

8. Recorded Message Frauds

Recorded message frauds are similar to missed call frauds. However, in such cases, victims receive a voice message instead of a missed call.

Usually, an information about a prize prompts the user to call back for more information. When the victim calls back, he/she is charged a huge fee similar to the missed call frauds.

Please abstain from calling back if you ever receive such recorded messages on your phone

9.SIM Swap Fraud

The banks have built many security features around mobile numbers like transaction messages, One Time Passwords for financial transaction, Net Secure Code, etc. Such information's are very essential to defraud the customers. In SIM-Swap Frauds, the fraudsters try to get duplicate SIM card from telecom operators on the pretext of lost SIM or connivance with their representatives and then access such confidential information sent by the bank.

Fraudsters obtain your mobile no. and other bank account details from Phishing, Vishing or Trojan/Malware attack or social engineering. Then they ask the telecom service provider for replacement of SIM on some pretext like new handset to loss of SIM/handset.

Fraudsters may connive with representative of telecom operator or produce fake documents to get the duplicate SIM.

With the banking details stolen through Phishing or Trojan/Malware, fraudsters will access and operate your account and initiate financial transactions which you will not be aware of since SMS alerts, payment confirmations, etc. will go to the fraudster.

10.Smishing

Smishing, short for 'SMS phishing', uses text messages containing Malware or Virus which attempts to collect personal information of the user. This vulnerability is becoming increasingly popular among miscreants as many mobile phone users keep their personal data, like bank account information, card info, etc. stored on their smartphones.

Typically, the fraud is perpetuated by sending the user an SMS which asks him to download a legitimate-looking program which is actually a malicious software. Customers should be vigilant in using their mobile devices as a means to prevent this kind of attack.

Tips on How to Avoid Mobile Frauds

While it may not always be possible to avoid the ingeniously crafted mobile phone frauds, one can always exercise caution.

In fact, in case your phone is lost or stolen, you risk having your personal information out in the open! There isn't much you can do here other than NOT being careless about your phone.

Always ensure that you have strong passwords on your phone. We suggest you download a verified app that helps users track their mobile in case it is lost or stolen. These days' apps that enable a user to remotely wipe off data from their phone if it is online are also available.

Here are some more tips on how to avoid mobile frauds.

Avoiding Mobile Phone Text Frauds

- Be very careful of the text messages that you receive and respond to.
- In case you are suspicious of the sender, never call back on the numbers suggested or click on any link. Immediately call your network provider and keep them informed.

Avoiding Missed Call Frauds or One-Ring Frauds

- Never return a missed call from an unknown number, especially if it has an unfamiliar country code.
- If it's very critical to return the call, better use Google or Truecaller to check the authenticity of the number. Such numbers are often marked as 'spam'.

North East Small Finance Bank
Your Doorstep Banker

Avoiding Mobile Ransomware

- To avoid mobile ransomware, be very cautious of the apps that you download on your phone.
- Avoid downloading apps that evade the phone's genuine App Store.
- Avoid engaging in financial transactions or exchanging personal information when connected to a public Wi-Fi.
- Have an anti malware and privacy protection software installed on your mobile

Avoiding Mobile App-based Frauds

- Make sure that you always download apps from official mobile app stores.
- Review the permissions that the app seeks to access your personal files.
- Some malicious apps demand permission to access a long list of information on your device. This should ring the warning bells!

Avoiding SIM Swap

- Enquire with your mobile operator if you have no network connectivity and you are not receiving any calls or SMSes for unusually long periods.
- Do not neglect messages sent from your network provider that highlight a probable SIM-Swap. Remember to respond quickly to such messages.
- Never switch off your smartphone in the event of you receiving numerous unknown calls. It could be a ploy to get you to turn off your phone and prevent you from noticing a tampered network connection.
- Register for instant alerts (both SMS and Emails) that inform you of any activity in your bank account.
- Check your bank statements frequently to identify irregularities

Avoiding Smishing frauds

- Avoid clicking on links sent from unknown numbers or senders.
- Do not respond to messages asking for your personal information, even if the person claims that he/she is from Bank, any other bank or government office.
- Avoid downloading unauthorised applications on your mobile phone as it can leave your personal data exposed to threats.
- If a text message urges you to act or respond quickly, stop and think before you do anything.
- Never reply to a suspicious text message without verifying the source.

Jagrook Rahiye,Surakshit Rahiye !!!