Type of Threat/Fraud	Details	Impact of fraud	Preventive measures
Smishing in Smartphone	It occurs when cell phone user is the recipient of a SMS with a link directed to phishing websites, allowing hackers to access your device	•Financial loss i.e., Illegal withdrawal of money from bank account	1.Never enter details into a website you've accessed via a link as it can be fake.
Wi-Fi Fraud	Fraudsters will often set up a Wi-Fi hotspot of their own and disguise it as genuine public Wi-Fi. The “spoofed” connection will have a name similar to the outlet in question, e.g. a coffee shop	•"Man in the middle" attack, in which a hacker is able to steal the information you send over the Internet	1.Never auto-connect to open Free and fake Wi-Fi networks in public places, set your device settings accordingly 2.Do ask the staff at an establishment that offers free Wi-Fi for the exact name of its network 3.Do not make financial transactions using public Wi-Fi networks
Bluesnarfing	It involves the theft of data from a wireless device having a Bluetooth connection – which could include information from contact lists, emails, or text messages without the user’s knowledge, and so may go on indefinitely unless discovered.	•Theft/illegal access to personal information/ data	Do not turn on Bluetooth and make it visible unless required

Note: The frauds possible in feature phone are also possible in smart phone as well.

FEATURE PHONE:

Dos

- Use phone lock feature compulsorily
- Use SIM card lock feature. You can ask customer care for default PIN (Personal Identification Number).SIM will be locked after 3 successive failure attempts
- Note the IMEI code and keep invoice safe. It can help in filing police complaint and prevent misuse for illegal activities since operator can block the device
- Make sure to reset to factory settings when a phone is permanently given to another user to ensure that personal data in the phone is wiped out

Don’ts

- Never store important and sensitive information on mobile. The not so sensitive information that is stored need to be secured using password
- Do not keep passwords saved in mobile phone. If necessary at least use some form of encryption (i.e. letter scrambling) rather than saving it on plain
- Do not keep personal information like mobile number, date of birth etc in social media profiles enabling fraudsters to answer basic security questions that your TSP might ask for authentication
- Do not handover SIM/mobile phone to anybody to avoid any illegal activity
- Do not provide SIM card along with mobile phone to mobile repair shop to prevent possibility of SIM swapping or SIM cloning
- Do not avoid service emails and SMSs from the TSPs

SMART PHONE:

Dos:

- Install antivirus software and also use it regularly
- Uninstall unused and idle apps on regular basis. It not only free up memory of the device but also improve security of the device
- Be careful while installing e-wallet since there are many fake e-wallet apps
- Update the operating system on regular basis to enhance security of your device
- Apply principle of proportionality i.e., the permissions to collect data should be proportional to the service provided by the app
- Do Keep a back up of phone’s data on regular basis to avoid loss of information if phone was lost

Don’ts:

- Never lend your phone to unknown person. Because a single minute is needed for someone to install malicious software in the phone
- Do not switch on Bluetooth, leaving the phone vulnerable. Use Bluetooth only when required
- Never connect to unknown Wi-Fi networks. If connected do not make financial transactions using such networks

Disclaimer: The information provided is solely for awareness purposes

सत्यमेव जयते

MOBILE SECURITY AWARENESS

THREATS AND PRECAUTIONS

The financial frauds involving Mobile/SIMs are on rise in the recent times. To bring awareness among public, some of the frauds are listed. Public are requested to spread the awareness among near and dear and known people.

FEATURE PHONE:

Type of Threat/Fraud	Details	Impact of fraud	Preventive measures
Theft	Loss of mobile phone	• Exposure or Loss of user's personal Information/Data • Monetary loss • Misuse for anti-national activities	1.Never store important and sensitive information on mobile 2.Use SIM card lock and phone lock feature 3.Note the IMEI code and keep the invoice safe. It can help in filing police complaint and blocking the device to prevent misuse for illegal activities
SIM Swapping	Your SIM card can be blocked and exchanged with a fake one through your operator	• Loss of identity • Misused for OTP and UPI frauds leading to withdrawal of money from bank account	1.Update alternate contact number & email id with TSP so that customer will be alerted via SMS & email whenever someone attempts SIM swap. He can respond to the alerts & stop the process 2.Do not share KYC details with anyone 3.If copy of KYC document is required to be submitted, then always write the purpose of submission along with date on the copy of the document
SIM Cloning	It is the process of cloning a original SIM card to create another duplicate SIM card without the knowledge of an individual mobile subscriber		
Vishing (Voice phishing)	It occurs when a cell phone receives a call from a fake person or entity to acquire personal and financial information	•Financial loss i.e., Illegal withdrawal of money from bank account	1.Do not share bank details to the calling party offering benefits or threatening service disconnection 2.Call 1909 to activate Do Not Disturb(DND)
Smishing (SMS phishing)	It occurs when a cell phone receives a SMS from a fake person or entity to acquire personal information such as passwords	•Financial loss i.e., Illegal withdrawal of money from bank account	1.Do not reply to unknown SMSs 2.Call 1909 to activate Do Not Disturb(DND)
OTP frauds	Fraudsters will get OTP by vishing or SIM swapping or SIM cloning or changing the mobile number linked to bank account or Bypassing the OTP process since 3D international gateways don't ask for OTP	•Financial loss i.e., Illegal withdrawal of money from bank account	1.Never share any OTP with others 2.Be judicious about sharing your phone number with unknown persons 3.Do not share card number and CVV on debit/credit card or other bank details
Wangari scam-'One ring and cut' scam	It is a missed call scam where premium rates are charged when customer calls back the unknown ISD number	•Loss of money from the mobile account balance	1.Never call back an unknown ISD number
Biometric Fraud	It occurs when salesman of SIM cards ask to give biometrics by saying initial one could not capture properly	•Identity theft •Can be used for illegal / anti-national activities like spying	1.Give biometrics second time only after ensuring that salesman is true
Preactivated SIM fraud	It happens when customer buys SIM card which is already activated on somebody else name	•Identity theft •Can be used for illegal / anti-national activities like spying	1.Do not buy and use SIM card if it is active without any verification from the Telecom service provider

सत्यमेव जयते

Department Of Telecommunications
Ministry Of Communications
Government of India

BSNL Connecting India · airtel · vodafone · Idea · Jio

SMART PHONE:

Type of Threat/Fraud	Details	Impact of fraud	Preventive measures
UPI frauds	Hackers can get a duplicate SIM card by SIM swapping or SIM cloning. They can download the UPI app on a cell phone and then register the bank account details with it to illegally transfer money	•Financial loss i.e., Illegal withdrawal of money from bank account	1.Be judicious about sharing your number with unknown persons 2.Do not share bank account details with anyone since UPI frauds require only bank account details and not credit/debit card details
Fake e-wallet Apps	Fake apps of a bank or e- wallet company which have been used to collect sensitive personal data from users that include credit card numbers, CVV, the expiry date of the card as well as login credentials.	•Financial loss i.e., Illegal withdrawal of money from e-wallet or bank account	1.Note the number of downloads, in case you observe a few downloads, there are chances that the app could be fake.
'AnyDesk' app fraud	Scammers ask to download Anydesk app to bank customers to get remote access to your device	•Financial loss i.e., Illegal withdrawal of money from bank account	1.Do not share passcode generated after download to anyone over the phone.
Mobile ransomware	A form of malware that can lock a victim's phone by changing the device's PIN and encrypts all the data stored. In other words, it kidnaps your data or device.	•Unable to use the device or data	1.Install antivirus software and also use it regularly 2.Update the operating system on regular basis to enhance security of your device