## Threats and Precautions

### Mobile Security Awareness

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.

<table>
<thead>
<tr>
<th>Type of Threat/Fraud</th>
<th>Details</th>
<th>Impact of fraud</th>
<th>Preventive measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smishing in Smartphone</td>
<td>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</td>
<td>• Financial loss i.e., illegal withdrawal of money from bank account</td>
<td>1. Never enter details into a website you’ve accessed via a link as it can be fake.</td>
</tr>
<tr>
<td>Wi-Fi Fraud</td>
<td>Fraudsters will often set up a Wi-Fi hotspot of their own and disguise it as genuine public Wi-Fi. The &quot;spoofed&quot; connection will have a name similar to the outlet in question, e.g. a coffee shop</td>
<td>• &quot;Man in the middle&quot; attack, in which a hacker is able to steal the information you send over the Internet</td>
<td>1. Never auto-connect to open 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</td>
</tr>
<tr>
<td>Bluesnarfing</td>
<td>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.</td>
<td>• Theft/illegal access to personal information/data</td>
<td>Do not turn on Bluetooth and make it visible unless required</td>
</tr>
</tbody>
</table>

###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

### FEATURE PHONE:

**Dos:**

- Use 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 backup of your 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

### 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 backup of your 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

---

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

Disclaimer: The information provided is solely for awareness purposes.
<table>
<thead>
<tr>
<th>Type of Threat/Fraud</th>
<th>Details</th>
<th>Impact of fraud</th>
<th>Preventive measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>Loss of mobile phone</td>
<td>• Exposure or Loss of user’s personal information/Data</td>
<td>1. Never store important and sensitive information on mobile phone. 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.</td>
</tr>
<tr>
<td>SIM Swapping</td>
<td>Your SIM card can be blocked and exchanged with a fake one through your operator</td>
<td>• Loss of identity</td>
<td>1. Update alternate contact number &amp; email id with TSP so that customer will be alerted via SMS &amp; email whenever someone attempts SIM swap. He can respond to the alerts &amp; 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.</td>
</tr>
<tr>
<td>SIM Cloning</td>
<td>It is the process of cloning a genuine SIM card to create another duplicate SIM card without the knowledge of an individual mobile subscriber</td>
<td>• Financial loss i.e., illegal withdrawal of money from bank account</td>
<td>1. Do not share bank details to anyone over the phone. 2. Do not share bank account details with anyone since UPI frauds require only bank account details and not credit/debit card details.</td>
</tr>
<tr>
<td>Vishing (Voice phishing)</td>
<td>It occurs when a call is received from a fake person or entity to acquire personal and financial information</td>
<td>• Financial loss i.e., illegal withdrawal of money from bank account</td>
<td>1. Install antivirus software and also use it regularly. 2. Update the operating system on regular basis to enhance security of your device.</td>
</tr>
<tr>
<td>Smishing (SMS phishing)</td>
<td>It occurs when a call or SMS is received from a fake person or entity to acquire personal information such as passwords</td>
<td>• Financial loss i.e., illegal withdrawal of money from bank account</td>
<td>1. Never buy SIM card if it is active without any verification from the Telecom service provider.</td>
</tr>
</tbody>
</table>

**Preventive measures for SIM frauds:**
- 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.

**Preventive measures for Wangari scam ‘One ring and cut’ scam:**
- 1. Never call bank an unknown SD number.
- 2. Give biometrics second time only after ensuring that salesman is true.

**Preventive measures for Biometric Fraud:**
- 1. Identity theft
- 2. Can be used for illegal/anti-national activities like spying
- 3. Financial loss i.e., illegal withdrawal of money from bank account

**Preventive measures for Preactivated SIM fraud:**
- 1. Identity theft
- 2. Can be used for illegal/anti-national activities like spying
- 3. Financial loss i.e., illegal withdrawal of money from bank account

**Preventive measures for OTP frauds:**
- 1. Never store important and sensitive information on mobile phone.
- 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.

**Preventive measures for UPI frauds:**
- 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.

**Preventive measures for Fake e-wallet Apps:**
- 1. Note the number of downloads, in case you observe a few downloads, there are chances that the app could be fake.

**Preventive measures for 'AnyDesk' app fraud:**
- 1. Do not share passcode generated after download to anyone over the phone.

**Preventive measures for Mobile ransomware:**
- 1. Unable to use the device or data.

Department of Telecommunications
Ministry of Communications
Government of India

[Image of a phone with text: "FEATURE PHONE"]

[Image of a phone with text: "SMART PHONE"]