InfoSec *for* WOMEN

NATIONAL CYBER SECURITY AWARENESS MONTH

October, 2020

SMART PHONE SECURITY

Cybercrime is on the rising at an alarming rate, and women are its biggest targets. Smart phone and Internet allow predators to exploit women and girls anonymously and easily.A study claims that women use smart phones for more than four hours a day and are likelier to get addicted to them than men. [1] Women use smart phones mainly for social networking website and online shopping, than just making calls, games and searches combined. These devices have their own characteristics but also with security concerns such as sensitive information access. There are various threats, which can affect the smart phone users in several ways. In current scenario it is vital for women to be aware of cyber threats through smart phone and the various dangers that come with it.

Mobile Phone Security Threats Categories:

Mobile Device and Data Security Threats

Threats related to unauthorised or intentional physical access to mobile phone and Lost or Stolen mobile phones.

Lost or Stolen devices

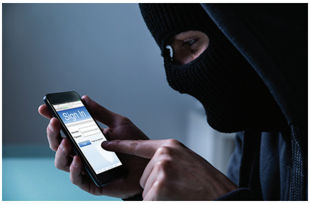
Nowadays smart phones have become the inevitable part of an individual's life. By any chance we lost/misplaced our phone; it causes a serious threat to the sensitive data that can reach a cyber criminal. Just by looking at apps that are installed on the phone, anyone can have an idea about the user's age, gender, location, interest in workout activities, possible medical conditions the user is suffering from, even whether the smart phone user is expecting a baby.

Always use a password or biometric authentication for unlocking your phone.

Activate SIM lock for your SIM card, because even if you lock your phone anyone will easily have a physical access to your SIM card once you lose your phone.

It is advisable not to store important information like credit card and bank cards passwords, etc in a mobile phone.

Make sure you log out of the Apps after using it

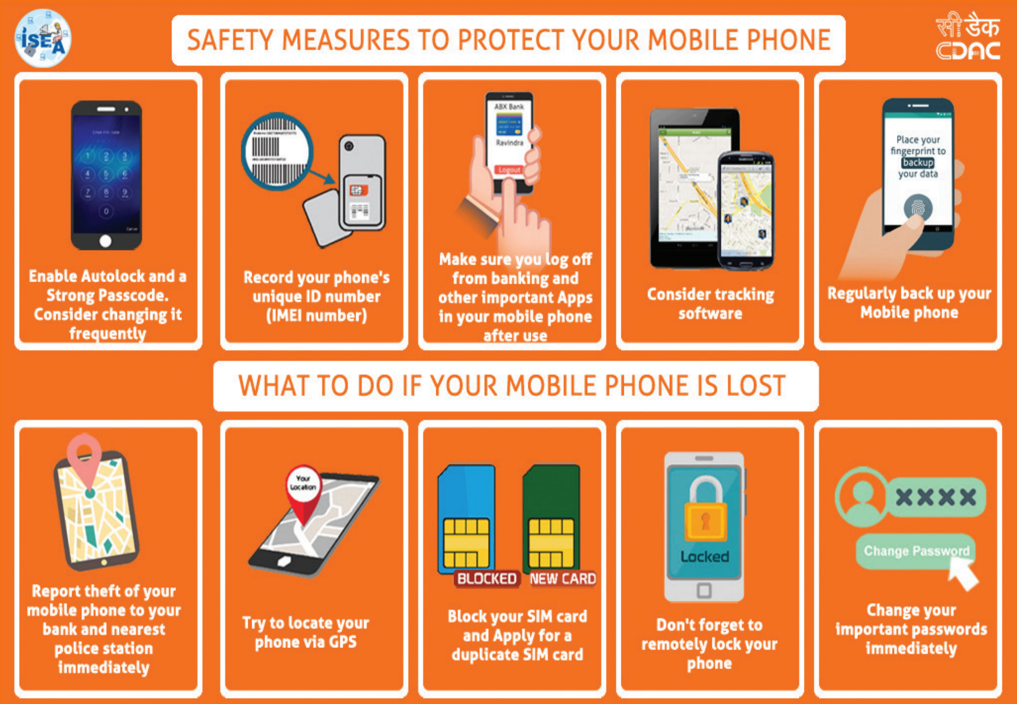


Exposure of critical information

Lack of data protection or data leak prevention capabilities on mobile devices. This can lead to serious threat to identity of any individual. Your personal banking information can also be at risk.

Typical impact of attacks against Mobile Phones :

- Exposure or Loss of user's personal Information/Data, stored/transmitted through mobile phone.
- Monetary Loss due to malicious software unknowingly utilizing premium and highly priced SMS and Call Services.
- Privacy attacks which includes the tracing of mobile phone location along with private SMSs and calls without user's knowledge.
- Loosing control over mobile phone and unknowingly becoming zombie for targeted attacks.



SAFETY MEASURES TO PROTECT YOUR MOBILE PHONE

Enable Autolock and a Strong Passcode. Consider changing it frequently

Record your phone's unique ID number (IMEI number)

Make sure you log off from banking and other important Apps in your mobile phone after use

Consider tracking software

Regularly back up your Mobile phone

WHAT TO DO IF YOUR MOBILE PHONE IS LOST

Report theft of your mobile phone to your bank and nearest police station immediately

Try to locate your phone via GPS

Block your SIM card and Apply for a duplicate SIM card

Don't forget to remotely lock your phone

Change your important passwords immediately

Mobile Connectivity Security Threats

Threats related to mobile phone connectivity to unknown systems, phones and networks using technologies like Bluetooth, WI-Fi, USB etc.

Open Wi-Fi.

Most often open Wi-Fi networks cause lot of threats to our mobile phones if connected in these networks. It is often advisable not to make any bank transactions and not to use any sensitive data using open Wi-Fi networks.

Keep the Bluetooth connection in an invisible mode, unless you need some user to access your mobile phone or laptops. If an unknown user tries to access the mobile phone or laptop through blue tooth, move away from the coverage area of blue tooth so that it automatically gets disconnected.

Don't perform financial, medical or business tasks while logged in to open Wi-Fi If you have to, then get a VPN or use a secured network.

Don't use any passwords and sensitive data while logged in to open Wi-Fi

Phishing emails

Email users continue to fall prey to emails that appear to come from trusted senders like banks and retailers. Manipulative language creates a sense of urgency that prompts recipients to make an impulsive decision. They click embedded links and share data on non-trusted sites, download attachments that contain hidden data-mining malware or share infected emails with contacts.

Check that email addresses always match sender names, visit sender websites via bookmarks or typed URL address bar submissions and scan all downloads with a trusted anti-virus program.

SMiShing Messages

The same phishing rules above apply to text messages. If you still doubt the origin of a message or a sender's intentions, contact the assumed sender via a phone call to confirm that they sent you the message. Consider reaching out to your bank – but contact them via the usual channels, do not click any URLs sent via text.

Weak Authentication

Criminals love mobile payment systems that have weak authentication tools. Any payment systems that you use, including e-commerce browser apps and virtual wallets, should have multi-factor authentication and multi-level data encryption. For example, a secure system might require a user ID, password and security image confirmation or message you a one-time-use PIN. The best payment systems turn your credit card data into a token so that it cannot be read anywhere else.

Mobile Application and Operating System Security Threats

Threats arising from vulnerabilities in Mobile Applications and Operating Systems.

When we unknowingly download Applications which are free, we never check on what are the privacy settings we are compromising by downloading those Apps. There are many Applications which steal your data after you download the Application on your mobile known as malware applications.

Avoid downloading the content into mobile phone or laptop from an unauthorised source.

Think before grantingapp permissions. Does a flashlight really need to know your device's location?

Consider revoking critical permissions when apps are not using them.