ASANSOL ENGINEERING COLLEGE

SUBJECT-

CYBER LAWS AND ETHICS

SUB CODE- OEC-IT801B

TOPIC :- WRITE A REPORT ON CYBERCRIME MOBILE AND WIRELESS DEVICES

NAME – AISHWARYA GHOSH
ROLL NO. – 10800219074
REG NO. - 036064 OF 2019-20
DEPT – INFORMATION TECHNOLOGY
YEAR – 4TH YEAR (8TH SEM)

INTRODUCTION

Mobile devices are now an essential need for every person for day-to-day tasks. As a result, the number of mobile users is rising exponentially. This gives us the direction to think about the data they process and what security mechanisms are being taken by mobile application developers to keep the user's data secure. There was a time when the biggest threat to the data was due to spyware which runs silently on the computer background and steals user data. Now even mobile devices are a fruit target for cyber-criminals to steal your data without even getting noticed. When it comes to securing mobile data, use an antivirus application that tends to protect your data from getting breached.

BODY OF THE REPORT

There was a time when the biggest threat to the data was due to spyware which runs silently on the computer background and steals user data. Now even mobile devices are a fruit target for cyber-criminals to steal your data without even getting noticed. When it comes to securing mobile data, use an antivirus application that tends to protect your data from getting breached.

4 Different Types of Mobile Security Threats–

1) Mobile Application Security Threats:- Websites available for software downloads are home to these threats. They tend to be genuine software but in fact are specially designed to carry malicious activities.

For example:-

Malware : Malware is designed to send unwanted messages to recipients and further use your personal and business information by hacking your devices.

Spyware : They are the software that are used to collect specific information about an organization or person which later can be used for fraud and identity threats.

2) Web-Based Threats :- These types of threats happen when people visit sites that appear to be fine on the front-end but in reality, automatically download malicious content onto the mobile devices. Also, many mobile applications continue to sync their data in the background which poses a threat. These threats usually go unnoticed by the users.

For example:-

Phishing Through Links : Some legitimate-looking links are sent through messages, emails, or social media platforms. They extract personal information by tricking with several schemes. It is not possible to categorize them as real or fake as they copy the original website.

Forced Downloads : When you visit a page through anonymous links, it automatically directs you to the download page. This method is called drive-by downloads.

3) Physical Threats :-These threats happen when someone physically tries to access your device. When you lose your mobile, or it is stolen there is a possibility for physical threats. Mobile devices carry your transactional data as well as has connected applications to your bank accounts, which is a threat to your privacy breach.

For example:-

No Password Protection : With keeping all measures to secure your data, it is surprising to know that some people find it difficult to use a password on their devices, or they rather use a password that is easy to crack by hackers. This leads to physical threats.

Encryption : While using carrier networks they generally provide good encryption while accessing servers. But while accessing some client and enterprise servers they are explicitly managed. They are not end-to-end encrypted which can lead to physical threats.

4) Network-Based Threats :- Mobile network includes both Cellular and Local network support such as Bluetooth and Wi-Fi. These are used to host network threats. These threats are especially dangerous as the cyber-criminals can steal unencrypted data while people use public WiFi networks.

For example:-

Public WiFi : While we are using our devices for every task, at public places we are provided with public open WiFi which tends to be legitimate while they are controlled by hackers which results in data leakage.

Network Exploits : Network exploits are due to the vulnerabilities in the operating system in your mobile devices. Once this software is connected to the network they are capable of installing malware onto the device without being known.

Steps to prevent from Mobile Security Threats :-

- Prefer using communication apps that encrypt data transfers.
- Update your device software regularly to ensure protection against spyware threats.
- Create unique passwords for different accounts created while using mobile devices.
- Delete the non-active apps to limit the threat to data access and privacy.
- Categories your applications under Blacklist and Whitelist.
- Check for apps accessing location and storage.
- Do not allow forced downloads from browser.
- Check on security that stops sharing of network unnecessary.
- Do not add your data to public servers.

CONCLUSION

Computing Technologies are the technologies that are used to manage, process, and communicate the data. Wireless simply means without any wire i.e. connecting with other devices without any physical connection. Wireless computing is transferring the data or information between computers or devices that are not physically connected to each other and having a “wireless network connection”. For example, mobile devices, Wi-Fi, wireless printers and scanners, etc. Mobiles are not physically connected but then too we can transfer data.

For example laptops, tablets, smartphones, etc. Mobile computing allows transferring of the data/information, audio, video, or any other document without any connection to the base or central network. These computing devices are the most widely used technologies nowadays.