IS2109 Information Systems Security-Practical 5
Mobile Security

1.

Firstly, when downloading a mobile app, we must check the permissions that the application is seeking. We must analyses whether those permissions and accesses are necessary for using that particular application. Some apps will request permission to see your location, information about the phone calls you make, or the ability to read and write to your SD card. So the responsibility is on us to check whether those permissions should be granted or not.

2.

- Must check whether it needs access to Storage where it can modify/delete USB storage contents.
- Some apps require device calls which read device state or identity to be able to pause when you get a phone call.
- Whether the full Internet access is necessary where the app needs to access the Internet to download the ads.
- Whether your location must be shared for the use of the app.
- Whether System tools are needed where it usually means that when you're using the app, it will keep your phone from going to sleep or in a power save mode.
- Whether it needs permission to access your personal information: read contact data, any social media or messaging app needs to access your contact information so you can use them with your friends.

3.

There are usually two ways to connect to the internet through your mobile phone

- cellular telephone service provider
- standard Wi-Fi

4.

When it comes to public Wi-Fi, there are more opportunities for attackers to exploit vulnerabilities via your connection over Wi-Fi than over 4G. Based on the security of these connections, the most to the least safe goes as follows,

1. Using a VPN over a cellular network or using a VPN over Wi-Fi
2. Cellular only
3. Wi-Fi only

So, really, the safest way to ensure your security while on the go is to use a multi-layered approach. The use of anti-malware protection, firewalls, VPNs, and online common sense are also vital.

5.

Lock your phone with a password or fingerprint detection.

- Encrypt your data.
- Set up remote wipe
- Backup phone data.
- Avoid third-party apps.
- Avoid jailbreaking your iPhone or rooting your Android.
- Update operating systems often
- Be wary of social engineering scams.
- Use public Wi-Fi carefully.
- Download anti-malware for your mobile device.

6.

Wipe, means to render all data on a hard drive unreadable. The term is often used in reference to making data stored on a computer, smartphone or tablet inaccessible before disposing of the device.

7.

Step 1:
First, turn off any screen locks.
Go to Settings > Security or Lock Screen Security > Screen Lock and change the type to None.

Step 2:
Remove the Google account from the device.
Go to Settings > Users and Accounts, tap your account and then remove.

Step 3:

If you have a Samsung device, remove your Samsung account from the phone or tablet as well.

Step 4:

Now you can wipe the device with a factory reset. However, this often only clears data at the application level, and other information such as SMS and chat messages can be restored with some standard data recovery tools.

8.

Lock your phone

Every major mobile operating system lets users secure their device with a password-protected lock screen. Many smartphone users set up lock screens to keep their personal data and messages safe from prying eyes, but it's an especially important tool if you use your phone for business.

Stick to approved apps

Google designed the Android operating system to be open and flexible. That means it's easy to install apps from sources other than Google's own app store. It is needed to be careful because unapproved apps can be a serious security threat, with the potential to unleash harmful malware onto your device.

Backup the data

Thieves and malicious software aren't the only threats to our data. Simply misplacing our smartphone can be disastrous if we haven't backed up the data stored on our phone. There are plenty of secure ways to keep our data backed up to the cloud.

Check the permissions

Before installing an Android app, it will ask us to first approve a long list of permissions. Instead of glossing over it in a rush to install the app, check the entire list for anything that looks suspicious.

Install an antivirus app

Malicious software can quickly cause sensitive data to become compromised or lost. If we use an Android smartphone to view, access or store private business data, make sure to install an appropriate app to protect our smartphone from malicious files.

9.

It is not necessary. Nobody will force us to set a password on our phone. However, if we are using the phone, without a password anybody could access all the files and accounts we have connected on our phone. For example, most mobile apps require account login when we first connect to these apps. And once connected, we will stay connected until you decide to log off.

If in the meantime, you lose your phone, anybody who finds your phone will have access to all the accounts connected on your phone.

10.

Early when the mobile banking apps were introduced, there was a risk of checking the bank balance because the security is very low. Even an outsider can get the password and log into the account and check the balance and do any transaction.
But with the time, Banks improved their systems to use One-time password (OTP) when doing the transaction instead of using the common password. And also BOC introduced an app only to check the balance and there is no need for any passwords for it. If they want, they can add a pin to that app to prevent viewing from others. Therefore, nowadays It is safer to access your bank account with the mobile phone.

11.

To use the mobile phone as a CCTV Camera we have an app named "Alfred". Alfred is one of the most popular security camera apps by a long shot, touting over 10 million downloads and a solid 4.7-star rating on the Google Play Store. After downloading this app to the mobile we can configure it to use as the main camera in the phone to be used as the CCTV camera. There you also should have another mobile phone which you currently use as the monitor/ controller.

Alfred app has some special features such as HD recording, Camera zoom, Record motion events up to 120 seconds, Motion detection schedule, Cloud storage for recorded events up to 30-days old. This is a very useful app for integrating CCTV for your home with small cost.

12.

Global Positioning System tracking is a method of working out exactly where something is. A GPS tracking system, for example, may be placed in a vehicle, on a cell phone, or on special GPS devices, which can either be a fixed or portable unit. PS works by providing information on the exact location. It can also track the movement of a vehicle or person.

A GPS tracking system uses the Global Navigation Satellite System (GNSS) network. This network incorporates a range of satellites that use microwave signals that are transmitted to GPS devices to give information on location, vehicle speed, time and direction. So, a GPS tracking system can potentially give both real-time and historic navigation data on any kind of journey.

GPS provides special satellite signals, which are processed by a receiver. These GPS receivers not only track the exact location but can also compute velocity and time. The positions can even be computed in three-dimensional views with the help of four GPS satellite signals. The Space Segment of the Global Positioning System consists of 27 Earth-orbiting GPS satellites. There are 24 operational and 3 extra (in case one fails) satellites that move around the Earth each 12 hours and send radio signals from space that are received by the GPS receiver.

The control of the Positioning System consists of different tracking stations that are located across the globe. These monitoring stations help in tracking signals from the GPS satellites that are continuously orbiting the earth. Space vehicles transmit microwave carrier signals. The users of Global Positioning Systems have GPS receivers that convert these satellite signals so that one can estimate the actual position, velocity and time.

13.

For Internet speed tracking, there are several mobile applications as well as web based applications. What these applications do is, they get connected to the device by internet connection and send some data to their server. When sending those data, the application will know the size and then by getting the time which takes these data to reach the server. Then with the simple calculation they will output the upload speed. Similarly, applications will download some data from the server and measure the time to reach the mobile. Then with the calculation application will output the download speed.

14.

Factory reset is a software restore of an electronic device to its original system state by erasing all of the information stored on the device. Doing so will effectively erase all of the data, settings, and applications that were previously on the device. This is often done to fix an issue with a device, but it could also be done to restore the device to its original settings.

15.

System itself includes its default settings and some apps which are needed for the functioning of the system. When Factory resetting, the device will erase all the data in the device including apps, files, contacts etc. and install the apps which are stored in the system as basic apps and include the default settings. This can make the device a fresh device just like brand new.

References

https://www.androidcentral.com/how-turn-old-android-phone-security-camera
https://boc.lk/index.php
https://www.quora.com/Is-it-really-necessary-to-put-a-password-on-your-phone
https://www.cnet.com/how-to/how-to-wipe-your-phone-or-tablet-before-selling/
https://www.businessnewsdaily.com/6015-protect-smartphone-data.html
https://www.valuepenguin.com/banking/is-it-safe-to-link-bank-account-online
https://www.eetimes.com/how-does-a-gps-tracking-system-work
https://computer.howstuffworks.com/know-if-app-safe.htm#:~:text=When%20you%20have%20chosen%20an,write%20to%20your%20SD%20card.
https://www.engineersgarage.com/how_to/how-internet-works-on-mobile-devices/#:~:text=There%20are%20usually%20two%20ways,connection%20isn't%20that%20strong.
https://us.norton.com/internetsecurity-wifi-how-safe-is-surfing-on-4g-vs-wi-fi.html
https://blog.malwarebytes.com/101/2016/09/top-10-ways-to-secure-your-mobile-phone/

Group 07

Name	Index Number
R.M.D.K.B. Rajakaruna	18020641
W.H.M. Gunathilaka	18020275
S. Maayura	18020461
T. Athavan	18020097
T. Thushanthan	18020844