IT Security - Protecting your Android device

This guide covers some of the basic steps you can take to begin to secure your personal Android device. It assumes you are running Android Marshmallow (v6).

Note: Not all features are available in earlier versions, and some menu options may differ slightly.

Tips

Update Android to the latest version

Google, and then your network, will release updates to Android to enable new features and address security issues. Try to install updates as soon as possible after release. You will be prompted when there is a new update but to manually check:

- Tap **Settings** > **About device** > **System Update**

Set a passcode

It's a good idea to set a password or PIN to unlock your device, to prevent others from using it.

- Tap **Settings** > **Security** > **Screenlock**

You can also set your device to auto lock after a short period of inactivity:

- Tap **Settings** > **Security** > **Automatically lock**

Turn on encryption

You can encrypt your device and protect your data, in case your device is lost or stolen. Android Marshmallow is encrypted by default.

- Tap **Settings** > **Security** > **Encryption** > **Encrypt device** > **Set a decryption password**

The encryption process will take some time to complete. You will need to supply the decryption password when you power on the device.

Backup data

You can set your device to backup data to your Google account. It will sync data in the background when the device is connected to a Wi-Fi network.

- Tap **Settings** > **Accounts** > **Google** > **Select your Google account** > **Select the data you want to sync**

When you have chosen the account you want to sync, you are ready to start backing up your data.

- Tap **Settings** > **Backup & reset** > **Switch on Back up my data**

Android Device Manager

If lost or stolen, you can use Android Device Manager to locate, phone, or lock your device.

- Tap **Settings** > **Security** > **Android Device Manager** > **Switch on Remotely locate this device** > **Switch on Allow remote lock and erase**

Location access must also be on.

- Tap **Settings** > **Location** > **Toggle on**

Apps

Installing

Only install apps from the **Google Play Store,** instead of 'sideloading' from unknown sources. This reduces the risk of installing a malicious app.

Updating

Keep apps up-to-date, to reduce the risk of security issues.

- **Enable Play Store** > **Menu** > **Settings** > **Auto update apps** > **Update over Wi-Fi**

Permissions

Check the permissions of an app before you install it, to make sure you are not sharing more data than you realise.

- For example, consider whether you wish to grant a torch app permissions to access your contacts, camera and microphone.

Change permissions

You can change the permissions that you have granted to installed apps.

- **Settings** > **Apps** > **Gear icon** > **App permissions** > **Select the permission type and review the apps listed > Switch off any apps that you do not want to use that permission type**

Selling your device

If you decide to sell your Android device, then you will need to remove links to any Google accounts that you have set up.

- Tap **Settings** > **Accounts** > **Google** > **Select your Google account** > **Tap menu (top right) then Remove account**
- Repeat for all Google accounts connected to your device

You should then erase and reset the device.

- Tap **Settings** > **Backup & reset** > **Factory data reset**.

Further information and help

The IT Service Desk are happy to help you connect your device to the University's wireless network. Sorry, but the Service Desk does not provide hardware support, including repairs of any kind.