Securing Your Smartphone
Android and iOS

Smartphones are a crucial part of our lives today, and they can be a great tool to have at your disposal. However, because we use our phones for so much, odds are, you have sensitive information stored on them, be it pictures, emails or other documents. This guide will aim to help you secure your smartphone, and the information stored on it.

Android (4.4 or later)

To secure your smartphone running Android 4.4 or later, you will first need to open up the Settings menu.
Once in the settings menu, click on the “Security” tab.

In the security tab, first uncheck the box that says “Unknown sources”.
After unchecking the box, click on the Screen Lock tab.

In the Screen Lock tab, create a PIN or Password to secure your device with. (Note: If you have a newer device, you may also see a fingerprint option here, which is also acceptable.)
After creating the PIN or Password, press the back button at the bottom of your screen to return to the **Security** tab. Here you will select the **Encrypt phone** option. (Note: “phone” will be replaced with “tablet” depending on your device)

![Security screen](image)

Ensure your device is fully charged and plugged in, and that you will not need it for an hour or more, and click **Encrypt phone** (or tablet).

![Encrypt tablet](image)
iOS 8.0 or later

To begin, start on the home screen of your device, and select the Settings icon.

In the settings menu, scroll down and select Touch ID and Passcode.
If you already have a finger print or passcode set up, you will have to enter your PIN here to access these settings.

After entering your PIN, you will see this screen.
Select the **Add Fingerprint** option if your phone has a fingerprint reader and you would like to utilize it. If not, select **Turn Passcode On**.

You will be prompted to scan your desired finger if you opted to use a fingerprint, and then you will need to create a backup PIN to lock your device.

Once you have added a Fingerprint or Passcode, scroll to the bottom of the **TouchID and Passcode** page. Set **Require Passcode** to **Immediately** and slide **Erase Data** to the **On** position. Note: This will completely erase your device after 10 failed login attempts.