Setup your lock screen and passcode

Mobile devices store a lot of personal information about yourself. This information can range from text messages and photos to email and banking apps.

It is important to setup a password/PIN on your mobile device to prevent unauthorized access to your device in the event of it being lost or stolen.

In addition to setting up your passcode, it’s important to setup a lock screen time-out. This means that after a period of inactivity, your mobile device will automatically lock itself.

SWIPE TO UNLOCK

Keep your device updated

Mobile devices are little computers that can fit into your pocket. They’re just as vulnerable to cyber threats as your desktop. For this reason, it’s important to keep your device’s operating system and installed apps updated. This ensures that the system is patched from known bugs and security threats and ensures your system runs at its best.

University of Hawai‘i InfoSec

www.hawaii.edu/infosec

infosec@hawaii.edu

www.facebook.com/UHInfoSec

www.twitter.com/ITSecurityUH

Learn more about Mobile Device Security @

www.hawaii.edu/infosec/mobiledevices

Need Help?

ITS Help Desk
Website: www.hawaii.edu/its
Email: help@hawaii.edu
Oahu: (808) 956-8883
Neighbor Islands: (800) 558-2669

For your Mobile Device
Dangers of FREE WiFi

Be aware that when on public WiFi it is possible for malicious users to snoop on the traffic going through the network potentially picking what you are searching for and logging into.

Avoid banking and shopping while on public WiFi as it is possible for an attacker to intercept the information and steal your credit card or other sensitive information.

Location Services

Beware of what apps are using your location! Your camera application could be attaching location data to your pictures which could allow malicious users to find out where you live or frequent. Check your camera apps to see if that feature is enabled.

Scrubitize and scan apps before installation!
Check the apps permissions before installation. Ensure that you are downloading from the official app store.

Monitor your device with a mobile security app!
Use a device finder and enable the remote wipe feature. Disable the auto login and password autofill features.

Avoid banking and shopping when using public WiFi!
Don’t join suspicious or unfamiliar WiFi hotspots. Disable wireless connectivity when you’re not using it (e.g. Bluetooth, NFC, WiFi).

Review all requests for your password and personal data!
Inspect URLs before visiting by tapping and holding down on links. Limit the amount of personal data you store on your device.

Turn on screen lock with a short timeout!
Turn on device encryption and use a strong password. Disable lock screen features and unnecessary notifications.

Secure your device by applying security updates!
Keep your system and all apps up-to-date. Don’t root/jailbreak your device as it could create new security holes that hackers could use to steal your information.