Best practices for mobile device encryption and security

Introduction

College sensitive information stored on a mobile computing device is at risk for unauthorized access and disclosure if appropriate security measures are not implemented to protect the device against loss or theft of information. Often disclosure can occur by simply misplacing a device and having it found by someone else.

This article provides recommendations for protecting College data that may be stored on your personally-owned mobile device.

Applicability

This article is for anyone at Lethbridge College who uses a personally-owned mobile for College work purposes.

This will provide information on how to secure/encrypt an iOS device (iPhone or iPad) or Android device (Ice Cream Sandwich, Jelly Bean, KitKat, Lollipop, or Marshmallow) to comply with the Information Technology Services standard for Mobile Computing Security.

Procedure

Personally-owned devices, used for College purposes, should be secured with the following measures:

- **Use a device password/passcode to secure your device**. For optimum security, set your password using the password policy outlined in the Acceptable . At minimum, a six-digit passcode is required.
  Apple iOS Touch ID is acceptable.
- **Set your device so that it auto-locks** after no more than fifteen (15) minutes of inactivity.
- **Turn the "Erase Data" feature on**, so that ten (10) failed attempts at guessing your password will cause the device to be wiped.
- **Accessing your college email via Office 365 allows the College to remotely administrate your device. (This is enabled when you accept the conditions of use upon installation of the mobile client)** This will allow information technology services administrators to trigger a remote wipe of your device, at your request, in the event that it is stolen.
- **Ensure backups are kept securely.** Make sure that backups of the information contained on your device are securely managed. At the time this article was written, it is advised that data should not be stored in iCloud or any other cloud-based storage system.

Instructions and further information on how to configure these settings can be found below.

Contents

iOS 9 and 10 (iPad/iPhone)

Passcode Lock Settings

Refer to Apple's information on how to use a passcode with your iPhone, iPad, or iPod touch to set or change a device passcode.

Notes:

- By default, iOS will suggest a six-digit passcode. The College recommends using an complex alphanumeric code, similar to the style of password you use for your college account.
- One option on the "Touch ID & Passcode", called Require Passcode, determines how long your device will wait before requiring a passcode to be entered. The College recommends this be set to **Require Immediately**, if possible. Do not set it for anything longer than 15 minutes.

Set Your Device to Erase after 10 Failed Password Attempts

1. Tap **Settings**.
2. Scroll down and select **Touch ID & Passcode**. (Note: If you already have a passcode set on your device, you will be prompted to enter it here.)
3. Scroll down to the bottom and set the "Erase Data" toggle to **On**. A confirmation screen will appear stating: "All data on this iPhone will be erased after 10 failed passcode attempts".
4. A slider will appear stating "All data on this iPhone/iPad will be erased after 10 failed passcode attempts." Tap **Enable**.
5. Tap the **Settings** button in the upper left-hand corner.
6. Click the Home button to return to your device's main screen.

Touch ID

Refer to the Apple article on how to Use Touch ID on iPhone and iPad.

Notes:

Every fingerprint is unique, so it’s rare that even a small section of two separate fingerprints are alike enough to register as a match for Touch ID. The probability of this happening is 1 in 50,000 with a single, enrolled finger. And Touch ID allows only five unsuccessful fingerprint match attempts before you must enter your password. By comparison, the odds of guessing a typical 4-digit passcode are 1 in 10,000. Although some codes, like “1234,” might be more easily guessed, there is no such thing as an easily guessable fingerprint pattern.
To start using Touch ID, you must first set up a six-digit passcode on your iPhone or iPad (or a password on your Mac).
You must enter your passcode or password for additional security validation:

- after you restart your iPhone, iPad, or Mac;
- when more than 48 hours have passed from the last time you unlocked your device;
- to add or delete a fingerprint to use with Touch ID;

- to change the iPhone or iPad passcode or Mac system password, and for other security settings like FileVault on your Mac;
- when there have been more than five unrecognized Touch ID authorization attempts in a row; and
- after you log out of your Mac.

iOS 7 and 8 (iPad/iPhone)

Passcode Lock Settings

1. Tap **Settings**.

2. Tap **General**.

3. Scroll down and tap on **Auto-lock**.

4. Set this to anything other than "Never".

5. Tap the "back" button (labeled "General") in the upper right-hand corner.

6. Tap **Passcode Lock.**

7. If you already have a passcode set on your device, you will be prompted to enter it.

8. On the next screen, set Simple Passcode to **OFF**. If you already have a passcode set, you will be prompted to enter it, and then tap **Next**

9. Enter a new passcode. If possible, when setting this passcode, follow college password rules (at least 8 characters long, containing upper- and lower-case letters, at least one number, and at least one non-alphabetic character).

10. Tap **Next**.

11. Re-enter your new passcode, to confirm it.

12. Tap **Done**.

13. Tap **Require Passcode**.

14. Set this value to **15 minutes**, or any setting less than 15 minutes.

15. Tap the Back button (labeled **Passcode Lock**) in the upper left-hand corner.

16. Tap the Back button (labeled **Settings**) in the upper left-hand corner.

17. Click the Home button to return to your device's main screen.

Set Your Device to Erase after 10 Failed Password Attempts

1. Tap the **Settings** app icon.

2. Tap **General.**

3. Scroll down and tap **Passcode Lock**. Enter your current passcode when prompted.

4. Set "Erase Data" to **ON.** A confirmation screen will appear: "All data on this iPhone will be erased after 10 failed passcode attempts".

5. Tap **Enable.**

6. Tap the Back button (labeled **General**) in the upper left-hand corner.

7. Tap the Back button (labeled **Settings**) in the upper left-hand corner.

8. Click the Home button to return to your device's main screen.

Android 6 (Marshmallow) and 7 (Nougat)

Note: Due to the wide range of Android devices and interfaces, the information here may not apply to your specific model. For example, some older hardware may support Android 6, but not its "default encryption" feature. If the information here does not assist with encrypting or setting a passcode on your device, consult your phone manufacturer's website for assistance.

By default, devices running the latest version of Android OS (6.0 or higher) will have full-disk encryption and passcodes enabled by default. If you own one of these devices, these features will be enabled as part of the setup process.

Android fingerprint ID is an acceptable method of locking and unlocking your device.

Android 3, 4 and 5 (Honeycomb, Ice Cream Sandwich, Jelly Bean, and Lollipop)

Note: The information here applies to "stock" Android OS devices. Many phone manufacturers have built custom interfaces for their devices that will not match the steps that you see here. If the information here is not sufficient to help you encrypt or set a passcode on your device, consult your device manufacturer's website for specific instructions and support.

Note: You cannot reverse Android device encryption once it is enabled. If you decide to decrypt your device later, you will need to perform a factory reset, which will wipe all data.

1. Plug in your device’s power cable and allow the battery to charge. Keep the power cable connected throughout this process. The device encryption process can take thirty (30) minutes or more. If your battery dies and the phone shuts off in the middle of the process, the process will fail, and you will lose data.

2. Open the device’s **Settings** and look for the **Security** menu item.

3. Select the **Screen Lock** menu item.

4. Choose a PIN or Password and follow the prompts to confirm it. If possible, when setting this passcode, follow college password rules (at least 8 characters long, containing upper- and lower-case letters, at least one number, and at least one non-alphabetic character).

5. Scroll to the **Encrypt phone** or **Encrypt tablet** option within the Security settings, and choose the **Encrypt SD card** option by checking the checkbox.

6. Select **Next**.

7. Confirm your PIN at the prompts.

8. Press the **Encrypt phone** or **Encrypt tablet** button.

The device will reboot several times during the encryption process, which can take thirty (30) minutes or more. On completion, you'll be prompted to enter your passcode/PIN.

Blackberry Devices

Blackberry smart phones have built-in encryption that is automatically enabled. To secure a Blackberry device, you only need to set up a device passcode, using the following steps:

1. Tap the **Settings** icon on your home screen.
2. Tap **Security and Privacy**.
3. Tap **Device Password**.
4. Set "Simple Password" to **Off**, and then set "Device Password" to **On.**
5. Enter and confirm your new device password, then tap **OK**.
6. Your password is now set.

Additional Recommendations for personally-owned mobile devices

Set Up Remote Wipe

Remote wipe of your device will be possible if you have configured your device to access Lethbridge College Office 365 Mail as an Exchange service.

If your device is stolen and you would like to request that the data be wiped, please contact the HelpDesk.

Secure Device Backups in iTunes (for iOS devices)

Apple has published this article to describe how to configure iTunes to make secure device backups.