UNIVERSITY OF TORONTO

Securing Smartphones and Tablet Devices

Smartphones and tablet devices are storing more and more information with each new model. It is important to ensure that you are protecting what is possibly sensitive personal information stored on your phone. The steps you follow to secure your smartphone or tablet device will differ depending on which device you have, but there are some general principles that should be followed.

1. **Encryption** - You should enable encryption on your device if possible. If your device does not support encryption, it should not be used for email / confidential information.
2. **PIN / Passcode** - Locking your device with a PIN or passcode is essential to protecting information should it go missing or be stolen.
3. **Updates** - Make sure that you have the latest software updates installed on your device.
4. **Services** - There are a number of services running on your phone that could possibly be exploited, giving access to confidential information. It is recommended that any non-essential services (such as Bluetooth and Wifi) be turned off. Only follow the instructions in this section if you are not using these services.
5. **Backups** - Make sure that you are regularly backing up your device.
6. **Recovery** - Some manufacturers have tools available to their users that can help in the event that their phone is lost or stolen. These tools include being able to locate your phone and/or remotely wipe the content on the phone.

In addition to these six basic principles, "jailbreaking" (the process of circumventing a device's operating system to gain full access to the device) it is highly discouraged. Jailbreaking your device can open your phone or tablet up to software that has not been properly checked for bad code.

This document will cover these basic steps for each of the 4 main operating platforms available: iOS (including iPhones and iPads), BlackBerry OS (including BlackBerry phones and the Playbook tablet), Android OS (including both phones and tablet devices) and Windows 7 Phones.

UNIVERSITY OF TORONTO

iOS (iPhone, iPad)

These instructions relate to devices running iOS 5 and later.

Encryption

Full-device encryption is automatically enabled when a passcode is established for your device. You can ensure that your device has encryption turned on by navigating to *Settings* ➜ *General* ➜ *Passcode* and verifying that "Data protection is enabled" is visible.

PIN / Passcode

1. Go into the *Settings* ➜ *General* ➜ *Passcode* screen.
2. Click on "Simple Passcode" to turn OFF the simple 4 digit passcode.
3. Click "Turn Passcode On", and enter your passcode when prompted.

To ensure the maximum security of the device, set "Require Passcode" to "Immediately", and enable "Erase Data" to automatically erase your device after ten failed passcode attempts.

Updates

1. Make sure you have the latest version of iTunes installed on your computer.
2. Connect your iPhone to your computer, and select it under the Devices section on the left hand side.
3. Click "Check for Update" on the Summary tab.

Services

If you are not using Bluetooth to connect a headset to your device, it is recommended that you turn it off. Navigate to Settings ➜ General ➜ Bluetooth. If it is currently turned on, click the toggle button to turn it off.

Many people use Wifi to connect their device to a wireless network. At the very least you should ensure that your device does not automatically join wireless networks. Navigate to Settings ➜ Wifi and make sure that Ask to Join Networks is ON.

In the Mail app settings, you should disable loading of remote images. This can be done by navigating to Settings ➜ Mail, Contacts, Calendar and moving the Load Remote Images slider to OFF.

UNIVERSITY OF TORONTO

Backups

The iPhone is backed up by iTunes each time the device is synced, updated or restored. The content on your device such as downloaded applications, audio, video and photos are not included in the backups because they are automatically synced if you have the "Sync" option checked in their respective tabs. When your device is plugged into iTunes, ensure that the "Encrypt Backups" option is selected on the "Summary" screen in iTunes. If your device is storing confidential information, you should turn off iCloud backups. Navigate to Settings ➜ iCloud ➜ Storage and Backup and make sure that the "iCloud Backup" slider is set to OFF.

Recovery

iOS devices come with a "Find My iPhone" app that allows you to locate your phone if it goes missing. Details about how to use this app to find your lost phone or remotely wipe it if it has been stolen are available on Apple's website: http://www.apple.com/iphone/built-in-apps/find-my-iphone.html

iCloud

If you have an iCloud account registered on your device you should be careful that confidential information is not being stored on Apple's servers. Under Settings ➜ iCloud, turn off at least "Documents and Data" and "Notes", as well as any other services that you do not explicitly need. If you do not need the iCloud service, it is recommended that you turn it off entirely.

UNIVERSITY OF TORONTO

BlackberryOS (Blackberry Phones)

Encryption

To enable content protection, go to Options ➜ Security and set Content Protection to enabled. You will be required to enter a password to encrypt your data. Once you have entered this your Blackberry will begin to encrypt your data; this may take some time, and an Open Pad Lock icon will be displayed during the operation. Doing this will protect information that your Blackberry considers sensitive, for example your emails, browser cache and address book.

You should also encrypt any data stored on a media card, if your device has one. To do this:

1. Navigate to the device options and click on "Media Card".
2. Change the "Encryption Mode" to "Security Password & Device".
3. Change the "Encrypt Media Files" to "Yes".
4. Press the Menu key and click "Save".

If your email account uses a BlackBerry® Enterprise Server that supports this feature, you can digitally sign or encrypt messages to add another level of security to email messages and PIN messages that you send from your BlackBerry device. Digital signatures are designed to help recipients verify the authenticity and integrity of messages that you send. When you digitally sign a message using your private key, recipients use your public key to verify that the message is from you and that the message has not been changed. To sign or encrypt an email message or PIN message:

1. When composing a message, change the Encoding field to Encrypt or Sign and Encrypt.
2. Press the Menu key.
3. Click Options.
4. Set the Use Password-Based Encryption field to Yes.
5. In the Allowed Content Ciphers section, select the check box beside one or more allowed content ciphers.
6. If you are signing the message, in the Signing Options section, select a certificate.
7. Press the Menu key.
8. Click Save.
9. Type your message.
10. Press the Menu key.
11. Click Send.
12. Type a pass phrase to encrypt the message.
13. Confirm the pass phrase.
14. Click OK.

You must then use a secure method to let the recipient know what the pass phrase is.

UNIVERSITY OF TORONTO

PIN / Passcode

1. Select the Options ➜ Security screen.
2. Change the "Password" option to "Enable".
3. Enter your password twice to verify it.
4. Select a reasonable "Security Timeout"; maximum security would be to set this to immediately.
5. Save the changes and exit.

When using your Blackberry ® be sure to lock it by selecting "Lock" from the main menu before putting it down.

Updates

1. Connect your device to your computer with a USB cable and enter your PIN.
2. If a software update is available you be automatically prompted to update.

Services

Click on the Menu button and then go into the "Manage Connections" application and you will see three options (Mobile Network, Wi-Fi and Bluetooth). Remove the checkmark next to Bluetooth.

Backups

1. Connect your device to your computer and open up the Blackberry ® Desktop Manager.
2. Double-click Backup and Restore
3. Select Backup to perform a full backup.
4. Choose a location to save the backup file, and then click save.

Recovery

Without a BES (Blackberry Enterprise Server), a third party application must be installed to remote wipe your Blackberry ®. One such application is offered by Roblock: http://www.xroblock.com/

UNIVERSITY OF TORONTO

Android (Phones and Tablets)

Encryption

Starting with Android 4.0 Ice Cream Sandwich, Android Phones support on-device encryption. To enable this go to Settings ➜ Security and enable encryption. You will be asked to set a password at which point the device will reboot and the encryption process will begin.

For those with Android Phones running a version of the OS before version 4.0, there are a few third-party applications that can provide this functionality for specific parts of the operating system. The following page highlights a some of the best:
http://www.brighthub.com/mobile/google-android/articles/106101.aspx

PIN / Passcode

1. Go to Android Settings ➜ Security ➜ Change Unlock Pattern.
2. Check "Require Pattern" and you will be able to enter a swipe pattern.
3. Choose a pattern by running your finger over the dots; don't choose anything overly simple.

Those running a version of Android OS later than 2.2, there is also the option to set a PIN or password.

Updates

Android phones automatically update themselves "over-the-air". It varies from carrier to carrier how quickly these updates are pushed out to phones. When a system update becomes available the carrier will push a notification out to your home screen giving you the option to update your phone. Be sure that your phone is either plugged in or fully charged before choosing to update to avoid it running out of battery half way through the update process. Be patient!

Services

Click on Settings ➜ Wireless Connections. From this screen you can turn off both Bluetooth and Wifi if you are not using them.

Backups

Backing up an Android phone is not as simple as the BlackBerry or iPhone. Your email, contacts or events are automatically backed up the GMail account you configured the phone with. Other third party applications are available to back up other parts of the phone. The following web page details some of the options available to the Android Phone user:
http://www.tested.com/news/feature/2468-the-new-complete-guide-to-backing-up-your-android-phone/

Recovery

There is a free third-party application called "Mobile Defense" that allows you to track your Android phone using its GPS. This application is available from their website at
https://www.mobiledefense.com/

UNIVERSITY OF TORONTO

Windows 7 Phones

Encryption

Windows 7 Phones do not support on-device encryption although support has been promised in the future.

PIN / Passcode

1. On "Start", flick left to the App list and then tap "Settings".
2. In Settings, tap "Lock & wallpaper".
3. Tap turn on Password and enter your new password twice to verify.
4. Optionally you can tap "Screen time-out" to set how long the phone will wait before locking the screen. 15 minutes or less is a reasonable amount of time for this option.
5. Tap "Done" to save your changes.

Updates

Connect your device to your computer and start up the Zune software. When there is a new update available, you will be notified. If the Zune software does not start the update automatically, you can begin the process by selecting *Settings* ➜ *Phone* ➜ *Update* from the menu.

Services

Bluetooth: Go to the application list and tap Settings ➜ Bluetooth. Turn the status to off with the scroll bar. *Wifi*: Go to the application list and tap Settings ➜ WiFi. Pull the scroll bar to the left to turn off WiFi.

Backups

Anything that is synced via your Windows Live account will automatically be backed up. Zune content such as applications are backed up when a sync is performed within Zune. It should be noted that individual application settings and content are not backed up, only the applications themselves.

Recovery

It appears that Microsoft is committed to supporting this feature in the future, but it is currently supported only in an Exchange environment.

UNIVERSITY OF TORONTO

Some Terms to Know

Locking
Most smart phones come with the ability to set up a password or PIN. The user is then required to type in this password before being able to access the phone.

Encryption
Encryption is the process of rendering data stored on a smart phone unreadable without access to a private key. This is different than "locking" your phone because it actually protects your data "at rest". Meaning, even if a person was able to download all the data off the phone, it would only appear as meaningless gibberish.

Bluetooth
Bluetooth is a protocol that all smart phones support that allows them to connected to other bluetooth enabled devices. A common example would be a hands free headset.

WiFi
WiFi is a wireless networking protocol that is common in both smart phones and home networks. It is a very handy feature in a smart phone since it allows the user to avoid using their generally more expensive data plans when they have access to an internet connection available over WiFi.