Windows

1. **Set a device password.** Turn the device passcode on and specify a lengthy combination of numbers to secure your device.
   
   **ACTION:** Settings > Lock screen. Toggle the slider and press Change Password.

2. **Set a low screen lock time.** This will help prevent others from using the phone immediately while unattended.
   
   **ACTION:** Settings > Lock screen > Require a password after. Select the length of time you want.

3. **Change Internet Explorer’s settings.** By default, Windows Phone queries Bing whenever you type an address, therefore collecting browsing history.
   
   **ACTION:** Settings > Slide to left for Applications Menu > Internet Explorer. Uncheck unwanted settings.

4. **Enable find my phone.** With this enabled, you can track down your device if it is ever lost. Note: You must also enable the phone’s location services for this to work.
   
   **ACTION:** Settings > Find My Phone.

5. **Turn off “Notify me when new networks are found”**.
   
   **ACTION:** Settings > Wi-Fi.

6. **Turn off unnecessary radios.**
   
   **ACTION:** Settings > Wi-Fi and Bluetooth.

7. **Limit background tasks.**
   
   **ACTION:** Settings > Slide to left for Applications Menu > Background Tasks. Tap a program to change its settings.

8. **Disable location information in photos.**
   
   **ACTION:** Settings > Slide to left for Applications Menu > Photos + Camera.

9. **Secure search functionality.**
   
   **ACTION:** Settings > Slide to left for Applications Menu > Search. Toggle slider to disable/enable location information and uncheck undesired features.

---

**mobile security**

Your security is in the palm of your hands

*Android, Blackberry, iOS, & Windows*

---

**Information Sciences and Technologies Department**

http://www.ist.rit.edu/

**Computing Security**

http://www.csec.rit.edu/

---

**get informed**

Visit the RIT Information Security website to view additional information on keeping devices safe.

**RIT INFORMATION SECURITY**

http://rit.edu/security

infosec@rit.edu

(S58) 475-4123

---

Revised 10/24/2013
1. **Set a device password, such as a password lock or a pattern lock.** This is the first line of defense against any unauthorized physical access.
   ACTION: Settings > Location & Security > Set up Screen Lock.

2. **Avoid downloading applications from third party websites** and un-check the ‘Unknown Sources’ options which enables these downloads.
   ACTION: Settings > Security > Unknown Sources.

3. **Use an anti-virus application based on the user ratings.** This would act as a defense against any malicious application gaining access to your device.

4. **Read carefully and understand the permissions being granted before installing any applications** from the Google Play Store to reduce the chance of installing harmful applications.

5. **Check frequently for firmware update**, as these updates might include programs to fix security issues present on the device.
   ACTION: Settings > About device > Software Updates > Updates or Check for system updates.

6. **Turn off wireless features**, such as GPS, Bluetooth, Wi-Fi and Portable Hotspot when not in use. An accidental connection to an unknown and unsecured network may lead to serious threats.
   ACTION: Settings > Wireless & Network.

7. **Do not ‘Root’ the device**, as it can leave the system open to vulnerabilities.

8. **Avoid highly sensitive transactions**, such as banking, on public Wi-Fi networks to reduce the chance of sensitive information being intercepted.

9. **Frequently back up data on the device** to prevent loss of information.
   ACTION: Settings > Privacy > Back Up My Data.

10. **Turn off Google’s location services**, which gives the user’s location information to the installed applications.

**Android**

1. **Maintain password protection.** Maintaining a device’s password greatly reduces risk of unauthorized physical access.

2. **Be aware of your phone’s location.** Most spyware requires physical access to the mobile device for installation.

3. **Enable firewall.** The firewall is not activated by default. It is an added layer of security for the BIS client once enabled.
   ACTION: Options > Security Options > Firewall.

4. **Be observant of what third party applications are given permission to install and run.** This mitigates many possibilities of man-in-the-middle attacks via several different applications (SMS, email, Bluetooth, etc).

5. **Minimize the amount of personal information that is entered into device.**

6. **Do not install unsigned applications.** Unsigned applications, while they have lower access than signed applications, are generally malware-susceptible applications.

7. **Exercise caution when connecting the device to a PC via USB.** Prevents the Blackberry from becoming a portable device storing malicious software, targeting either the PC or the mobile device.

8. **Set Bluetooth to deny.** Unless the Bluetooth capability is valuable to the user, it is best to disable it.
   ACTION: Options > Security Options > Application Permissions.

9. **Set theme data to deny.** Theme settings are popularly used as masquerade applications for malware.
   ACTION: Options > Security Options > Application Permissions.

10. **Avoiding email interception and worms.** As with computer worms, simply being aware of attachments opened or links followed mitigates risk.
   ACTION: User Data > Email. Set to Deny.

**BlackBerry**

1. **Set a complex device password.** Turn off simple passcodes and use a longer alpha-numeric password.
   ACTION: Settings > General > Passcode Lock.

2. **Use different passwords.** Don’t reuse your device lockscreen password for other applications.

3. **Enable “Find my iPhone/iPad/iPod.”** With this enabled, you can track, lock, and wipe your device if it is stolen or lost from www.icloud.com for free.
   ACTION: Settings > Privacy > Location Services > Find my [iDevice].

4. **Turn on data wipe.** After ten incorrect passcode guesses, the device will delete all content and settings.
   ACTION: Settings > General > Passcode Lock > Erase Data.

5. **Turn off ‘Ask to Join Networks.’** Only connect to trusted wireless networks and manually remove any public networks after use.
   ACTION: Settings > Wi-Fi > Ask to Join Networks.

6. **Set a low autolock time.** This can prevent others from accessing the device if it is left unlocked and unattended.
   ACTION: Settings > General > Auto-Lock.

7. **Periodically review location services.** Be aware of what applications have permission to share your location. If not essential to the application, disable location services.
   ACTION: Settings > Privacy > Location Services.

8. **Use iCloud, and other cloud services, sparingly.** Be aware of how companies use the information that you store with them and how they protect it. Keep alternate backups of data in another location.
   ACTION: Settings > iCloud.

9. **Turn off unnecessary radios.** Turn off Wi-Fi, Bluetooth, Personal Hotspot when not in use.
   ACTION: Settings > Wi-Fi AND Settings > Bluetooth AND Settings > Cellular > Set Up Personal Hotspot.

10. **Minimize amount of lock screen notifications.**
    ACTION: Settings > Notification Center.

**iOS**

1. **Set a complex device password.** Turn off simple passcodes and use a longer alpha-numeric password.
   ACTION: Settings > General > Passcode Lock.

2. **Use different passwords.** Don’t reuse your device lockscreen password for other applications.

3. **Enable “Find my iPhone/iPad/iPod.”** With this enabled, you can track, lock, and wipe your device if it is stolen or lost from www.icloud.com for free.
   ACTION: Settings > Privacy > Location Services > Find my [iDevice].

4. **Turn on data wipe.** After ten incorrect passcode guesses, the device will delete all content and settings.
   ACTION: Settings > General > Passcode Lock > Erase Data.

5. **Turn off ‘Ask to Join Networks.’** Only connect to trusted wireless networks and manually remove any public networks after use.
   ACTION: Settings > Wi-Fi > Ask to Join Networks.

6. **Set a low autolock time.** This can prevent others from accessing the device if it is left unlocked and unattended.
   ACTION: Settings > General > Auto-Lock.

7. **Periodically review location services.** Be aware of what applications have permission to share your location. If not essential to the application, disable location services.
   ACTION: Settings > Privacy > Location Services.

8. **Use iCloud, and other cloud services, sparingly.** Be aware of how companies use the information that you store with them and how they protect it. Keep alternate backups of data in another location.
   ACTION: Settings > iCloud.

9. **Turn off unnecessary radios.** Turn off Wi-Fi, Bluetooth, Personal Hotspot when not in use.
   ACTION: Settings > Wi-Fi AND Settings > Bluetooth AND Settings > Cellular > Set Up Personal Hotspot.

10. **Minimize amount of lock screen notifications.**
    ACTION: Settings > Notification Center.