Did you know there are steps you can take to secure your smartphone? If you have a Blackberry, iPhone or Windows Mobile device, instructions have been provided to increase the security of your smartphone. Please take a few moments and review these steps.

BlackBerry (System 4.5 and higher)
Go to Options, then Security Options, then:
1. Password-protect start-up. Under General Settings, set Password to Enabled. You may also want to change other settings here, such as the number of password attempts allowed before the device is locked, and whether the device should automatically lock on holstering. Commit your changes by pressing the Back button (the half-circle arrow) and enter your new password when prompted. Choose a password you'll remember and that will be quick and easy to type using the device's keypad. Confirm that password, then exit to the main menu.
2. Encrypt data. Scroll past General Settings to Content Protection, and enable it. Under Strength, you can select Strong (80 bits), Stronger (128 bits), or Strongest (256 bits). I recommend using Stronger for faster encryption/decryption or Strongest for the most security. Selecting Yes for Include Address Book will keep your contacts secure but also result in disabling caller ID when the phone is locked. Circle-arrow back out, then create an encryption key by randomly moving the trackball and typing characters. A good practice is to regenerate an encryption key every two to four weeks: Under Security Options | General Settings, click on any service, then click Regenerate encryption key.
3. Secure passwords. Please don't fall into the trap of saving usernames and passwords in your mobile device's browser. Anyone who finds your device and unlocks it then has access to all of your online accounts. Instead, use the Password Keeper utility to store and encrypt this info.
4. Lock down Bluetooth. By default, Bluetooth is on. In addition to wasting your battery, this leaves you open to Bluetooth-based attacks. From the Home screen, go to Set Up Bluetooth. When prompted to Add Device select Cancel. Press the Menu button, then select Options. Set Discoverable to No, so other devices can't find your BlackBerry, and set Security to High—or if the Bluetooth devices you use with your BlackBerry support it, set Security to High + Encryption to encrypt Bluetooth data transmissions. From the following checklist, enable only those services you think you are going to use with Bluetooth—most commonly headset and hands-free. Exit and save.
5. Clear memory. Also under Security Options, memory clearing can delete sensitive data, such as unencrypted e-mail messages and username, password, and other certificate-related info, from memory. You can set the BlackBerry to clear memory under certain circumstances—for example, when you holster your BlackBerry or lock it.

iPhone
Unfortunately, you won't find a list item called "Encrypt data" below. At this point, there doesn't seem to be any encryption available for iPhones.
1. Enable Passcode Lock and Auto-Lock. Click the main iPhone Settings icon, then click the General tab and select Auto-Lock. Select the time period you want (2 minutes is recommended), then exit out to the Home screen. Once Auto-Lock locks the phone, Passcode Lock will require a four-digit PIN to unlock it. Click the iPhone Settings icon, then General, then Passcode Lock. From there enable Turn Passcode On. Enter your passcode. Tap Require Passcode and then choose "immediately."

2. Erase Data. Back on the Passcode Lock screen, you can turn on the Erase Data function. This will wipe the iPhone clean after ten failed passcode attempts.
3. Wi-Fi Security. WiFi should be turned off when it is not being used to reduce the risk of a remote attack. You should also turn off 'Ask to Join Networks'. To do this, click on the main iPhone Settings icon, then click Wi-Fi.
4. Lock down Bluetooth. It's great that Bluetooth is off by default on iPhones, but you should also set yours to require an eight-character PIN for connections. Turn on Bluetooth only when you need it.
5. Lock down Safari. JavaScript and Plug-Ins should only be enabled before browsing trusted sites. Click on the main iPhone Settings icon, then click Safari. Turn off JavaScript and Plug-Ins. Ensure Fraud Warning and Block Pop-ups are turned on. You can clear cookies, browser cache, and history from here too.

Smartphone (Windows Mobile 6.1)
1. Password protect start-up. Go to Start | Settings | Lock and configure a password. Check the box next to Prompt if the device is unused for and then select a time period from the drop-down box, something in the 5-to-30-minute range. You can set your password to be a simple four-digit PIN or a strong alphanumeric string and then enter your password in the boxes below. You can also set a hint, but remember that this can be read by anyone with physical access to your phone. At this point, it would help to go to Settings | Today, click the Items tab and check the box next to Device Lock to provide a quick locking option on your Home screen.
2. Encrypt data. Under Settings | System | Encryption, check the box that says Encrypt files placed on the storage card, then click OK. A storage card can actually contain both encrypted and nonencrypted data, but encrypted data can be read only from the device in which it was encrypted and written, or from a Windows PC using ActiveSync and Windows Mobile Device Center. There's also a big gotcha lurking: If you have to perform a hard reset of your device or update the ROM, you will lose the encryption key stored on the device, and with it, access to your data. Companies can push encryption policies to Windows Mobile devices using Exchange Server 2007.
3. Secure passwords. This requires a third-party solution, such as KeePass or some other eWallet type of encrypted password manager.
4. Lock down Bluetooth. Go to Start | Settings, then the Connections tab, then Bluetooth. On the Mode tab you can enable or disable Bluetooth and make your device visible; Off and Not visible are the more secure settings. Scroll all the way right to the Security tab and check the box to require authentication for data beaming.
5. Clear the memory and cache. In Internet Explorer, go to Menu | Tools | Options; in the Memory tab you can set a history retention time in days or clear the history manually. Click the Delete Files button to clear the Web cache. Navigate to the Security tab and click the Clear Cookies button.