Ten Steps to Smartphone Security (Windows Phone)

Smartphones continue to grow in popularity and are now as powerful and functional as many computers. It is important to protect your smartphone just like you protect your computer to avoid growing mobile cyber threats. Mobile security tips can help you reduce the risk of exposure to mobile security threats. Please note that these security tips reflect Windows Phone 8 and may not be accurate for previous versions:

1. **Set passwords.** To prevent unauthorized access to your phone, set a password on your phone's screen as a first line of defense in case your phone is lost or stolen.

    - Windows Phone (Lock screen FAQ)

2. **Do not modify your smartphone's security settings.** Other than setting a password, do not alter security settings for convenience. Tampering with your phone's factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, while making it more susceptible to an attack.

3. **Backup your data.** You should backup all of the data stored on your phone – such as your contacts, documents, and photos. Windows Phone 8 provides a service for copying certain types of content using a cloud service. Microsoft enables users to save text messages, call history, Internet Explorer favorites, theme color, and certain phone settings to the cloud. This will allow you to conveniently restore the information to your phone should it be lost, stolen, or otherwise erased.

    - Windows Phone (Back up my stuff)

4. **Only install apps from trusted sources.** Before downloading an app, conduct research to ensure the app is legitimate. Checking the legitimacy of an app may include such thing as: checking reviews and comparing the app sponsor's official website with the app store link to confirm consistency. Many apps from untrusted sources contain malware that once installed can steal information and cause harm to your phone's contents.

5. **Understand app permissions before accepting them.** You should be cautious about granting applications access to personal information on your phone or otherwise letting the application have access to perform functions on your phone. Make sure to also check the privacy settings for each app before installing.

6. **Set up "Find My Phone."** Find My Phone is a free service that can help you locate your phone if it is lost.

    - Windows Phone (Find a lost phone)

7. **Keep your smartphone's software current.** You should keep your phone's operating system and other software up-to-date by enabling automatic updates or accepting updates when prompted from your service provider, operating system provider, device manufacturer, or application provider. By keeping software current, you reduce the risk of exposure to cyber threats.

    - Windows Phone (How do I enable automatic updates?)
    - Windows Phone (How do I update my phone software?)

8. **Be smart on open Wi-Fi networks.** When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals. You should limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless connection to reduce your risk of exposure, especially when accessing personal or sensitive information. Always be aware when clicking web links and be particularly cautious if you are asked to enter account or log-in information.

9. **Wipe data on your old phone before you donate, resell, or recycle it.** Your smartphone contains personal data you want to keep private when you dispose your old phone. To protect your privacy, completely erase data off of your phone and reset the phone to its initial factory settings. Note, however, that resetting your phone will erase all content stored on your phone, including apps, text messages, call history, music, photos, and more. Even if you've already donated or sold your phone, you can erase it remotely by using "Find My Phone," see Tip #6 above.

   - ➢ Windows Phone (Reset my phone)

   Now having wiped your old device, you are free to donate, resell, recycle, or otherwise properly dispose of your phone.

10. **Report a stolen smartphone.** The major wireless service providers, in coordination with the FCC, have established a stolen phone database. If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider. This will provide notice to all the major wireless service providers that the phone has been stolen.

For more information and resources on mobile and cybersecurity, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign at www.dhs.gov/stopthinkconnect.