Smartphone Security

In this edition of Beyond the Firewall we will discuss Smartphone Security. Once upon a time, a phone was just a phone. It simply made and received calls. The only security you worried about was if someone had picked up in the other room to listen in. In this day and age the line between phones and computers has all but vanished. Your smartphone is likely more powerful and feature-rich than your desktop computer was not too many years ago. With that increased utility comes more vulnerability. Having a wealth of information stored on your device makes your phone a target and proper security measures should be taken.

Does Smartphone Security Really Matter?

Yes, Smartphone Security is important. The degree of importance depends on the individual user, or the individual company. Threats to your mobile security are not always easy to see. They can range from the simple such as when someone finds your phone and reads through your personal emails, to the not so simple such as malware or third-party apps that share your personal information. Here are some Smartphone Security tips for you to think about.

1. **Have a PIN number or password**

A PIN number or password is the simplest way to stop the average thief from looking through a smartphone. Otherwise, if the phone gets into the wrong hands, it's easy to get access to all of your personal information as well as make phone calls.

2. **Run the latest operating system and download every OS update**

Updates often contain changes that will make a smartphone more secure. For example, Apple's iOS 7 has a feature called Activation Lock. When the Find My iPhone app is enabled, Activation Lock kicks in and a thief must know the Apple ID and password to erase and reactivate the device.

3. **Have a security product on board**

It's not something many smartphone users think about, but those devices can get viruses too. Installing anti-virus and encryption software specifically for smartphones can help combat this.

4. **Download apps from a trusted source**

According to a report by Appthority, a mobile app security firm, 83 per cent of the most popular apps are associated with security risks and privacy issues. Only four to five per cent of apps are developed by trusted sources, such as Apple or Google. The rest can be developed by just about anyone, including cybercriminals.

5. **Don’t let websites cache a smartphone login**

Letting websites and apps store passwords allows thieves to gain access to accounts with sensitive information. Although it’s incredibly convenient to check emails with a single tap, it’s far safer not to have passwords saved on a phone.

6. **Register a phone for a Lock Locate Wipe program**

With these programs, a smartphone user can lock a phone remotely, use GPS signals to help locate it and then wipe the phone of its data.

7. **Make sure WiFi networks are secure**

Not all WiFi links are legitimate. Some could be set up by people looking to steal personal information. When using public WiFi, don’t go on sites that contain private or financial data.

8. **Buy your own VPN (virtual private network)**

Obtaining a VPN adds an extra layer of protection. It secures a wireless internet connection by encrypting the data that passes through the network to keep data safe.

9. **Don’t leave your smartphone lying around**

Keeping the phone out of sight is one of the most obvious and easiest ways to protect it.

10. **Be aware of the risks with e-banking on a smartphone**

Banking on a smartphone can put your money and identity at risk. Phones that allow multiple apps to run at the same time pose the biggest threat when banking on a phone. These apps could contain malware that monitor your activities.