Be Smart About Smartphone Safety

Smartphones are a fast-growing and undeniably popular technology but, aside from the fact that they are easily lost or stolen, there are a number of risks that go hand-in-hand with smartphones:

Spyware - Smartphone apps can be infected with spyware, just like your computer. Once spyware has been downloaded, criminals can hear your calls, see your text messages, emails and photos and track your location. They can take control of your phone and even make calls from it. Signs of spyware infection include:

- Outgoing texts to unknown numbers on your phone bill
- Warm battery even when phone is not in use or reduced battery life
- Flickering screen

Geotagging - Most smartphones encode a GPS stamp called a "geotag" onto digital photos, which can reveal the exact location a photo was taken. When shared on social websites, criminals can use this data to steal identities, stalk victims and scout locations.

Identity Theft - According to Javelin Strategy & Research's 2012 Identity Fraud Report, seven percent of smartphone users are victims of identity fraud. Sharing personal information publicly can help criminals authenticate your identity (e.g., if you share your pet's name on a public social media profile and then use it for passwords or security questions).

Protect Yourself

- Use a password to lock your phone.
- Install anti-virus, anti-malware and security software designed for smartphones and download updates.
- When installing apps, read the "fine print" to find out how your data is gathered and used.
- Don't open suspicious emails or click on suspicious links.
- Update your operating system regularly.
- Never store passwords on your phone.
- Enroll in a backup/wiping program through your smartphone's manufacturer or your wireless provider.
- Use your 3G or 4G instead of public Wi-Fi.
- If making a purchase using your smartphone, make sure the payment info starts with "https://"
- Disable geotagging.
- If your phone has data encryption features, use them.

If Your Smartphone is Lost or Stolen

- And you HAVE enrolled in a backup/wiping program, have the administrator "wipe" your phone and call your service provider to report your phone missing.
- And you HAVE NOT enrolled in a backup/wiping program, report the crime/loss to local law enforcement and sign up for fraud alerts through major credit reporting agencies.

When you're replacing your smartphone, wipe the memory from the phone and restore to factory settings. Destroy the SIM card unless it is being transferred to another device.

For more information, visit www.AUS.com/Tips