

National Cyber Security Awareness Month: "Be Smart with Mobile Devices"  
By Sue Rivera

As the holiday season approaches and retailers get ready for the latest technology to be sold, so can you be prepared by safeguarding your mobile devices. "A survey of 1,008 consumers in the U.K. found that 36% had lost an electronic device in public. Among the devices lost or left in an unsecure place, 42% had no active security measures", according to Sophos. In this last article for National Cyber Security Awareness Month, we discuss various options to help keep your mobile device from getting into the hands of others and how to minimize the possibilities of others getting access to the information on your device if it's lost.

Mobile devices are just as powerful and vulnerable as any computer or laptop. A huge difference is that you are now carrying information about your life around with you, wherever you go. Mobile devices are appearing in more people's pockets, purses, and briefcases. According to Homeland Security, the popularity and relatively lax security have made them attractive targets.

To help prevent your device from being stolen:

- Be aware of your surroundings at all times.
- Don't allow strangers to borrow your device. Offer to call for them.
- Keep your purse closed and out of the reach of thieves.
- While in shopping malls, bus or train stations as well as airports, minimize the use of your device where quick hands can snatch and run.

For safe-keeping the information on your device, it can't be stressed enough to use a strong password (passcode). Did I mention strong? There are several other tips that are just as important.

- Use at least 8 characters and mix them with lowercase, uppercase, numbers and symbols.
- Do NOT use words found in a dictionary.
- Lock your device.
- Get used to entering a password into your device regularly. Your device should go into a black screen after a minimum of 30 seconds, less if possible. If your device was ever lost or stolen, this will make it more difficult for someone to access your information.
- Use your wireless company's recommendation for backing up and managing your device. Backup to iCloud or iTunes. SpiderOak and iDrive are also available.
- The software should be kept up-to-date, use anti-virus software, and use encryption.
- Carefully consider what information you store on your device: account and password information, banking and credit card information should never be stored.
- Do you ever answer those security questions when you open an account? Don't post the answers on social networking sites.
- If your device is stolen or lost, it's important to deactivate and wipe your device.

Have a safe and secure holiday season. Take time to familiarize yourself with your device and protect what is yours. Secure your device now. Stay in control of your device and choose what is best for you. Thank you for reading these articles and supporting National Cyber Security Awareness Month. Remember: Stop. Think. Connect.