VOLUME 17 | ISSUE 2

PARTNERS IN CRIME PREVENTION

MARCH/APRIL 2013

INSIDE THIS ISSUE

MOBILE SECURITY PROTECTING YOUR INFORMATION ON THE GO 1

MOBILE SECURITY PROTECTING YOUR LAPTOP FROM THEFT 2

MOBILE SECURITY PROTECTING YOUR TABLET 2

MOBILE SECURITY PROTECTING YOUR SMARTPHONE 3

MOBILE SECURITY MORE TIPS 3

MOBILE SECURITY WHAT IS THE THREAT? 4

John Lovick, Sheriff
Snohomish County Sheriff's Office

3000 Rockefeller
M/S 606
Everett, WA 98201
425-388-3393
http://sheriff. snoco.org

MOBILE SECURITY—PROTECTING YOUR INFORMATION ON THE GO

With the proliferation of mobile computing that includes laptops, notebooks, tablets, ipads and now smartphones, criminals have more opportunity to steal not only your equipment, but also your vital information. And we use our mobile devices in more public areas than just our office or home. Coffee shops, the library, on a plane, where we have lunch, in a park are just a few places where people will work or relax with their equipment.

According to the Kensington SafeZone blog (http://blog.kensington.com/security/2012/01/10/the-cost-of-stolen-laptops-tablets-and-smartphones/) nationally:

- A laptop is stolen every 53 seconds. 52% are stolen from office or work, 24% from conferences, 13% from meeting rooms and 6% from cars. One out of ten laptops are stolen or lost over the lifetime of the device.
- 70 million smartphones are lost each year with only 7% recovered. 4.3% of smartphones that were issued to employees are lost or stolen every year.
- 50% of all mobile device users keep passwords, personal information and credit card information on their device.
- 60% of lost or stolen smartphones contains sensitive data such as:
  - Contact list- 62%
  - Emails- 58%
  - Internet credentials- 52%
  - Security codes and Settings- 35%
  - Business apps- 34%
  - Mobile payments- 30%
- The monetary cost of a laptop loss is over $49,000, including downtime, support and management time. And the average cost of recovering from a single corporate data breach is growing:
  - 2005- $3.3 million
  - 2006- $4.6 million
  - 2007- $6.3 million
  - 2008- $6.7 million
  - 2009- $6.8 million
  - 2010- $7.2 million

So, with all of the information that we now take with us and the risk of losing laptops, cell phones and tablets, it pays to be security conscious. Following are some suggestions that you can use to protect your equipment and your personal information.

MOBILE SECURITY- PROTECTING YOUR TABLET

Protecting your tablet computer from physical theft and theft of sensitive information is very much like for a smartphone. Here are 5 tips you can use:

1. ***Keep track of your tablet.*** *Don't leave it unattended. Install a location app.*
2. ***Set a strong password.*** *That way if it is stolen, the thief won't be able to get to your information.*
3. ***Look out for malicious apps.*** *Use "official" app stores from the operating system of your tablet.*
4. ***Use secure Wi-Fi.*** *Don't do financial transactions over unsecured networks. Look for "https" in shopping and financial web sites.*
5. ***Install a wipe app.*** *This way you can remotely erase your information if your tablet is stolen and you can't recover it.*

MOBILE SECURITY– PROTECTING YOUR LAPTOP FROM THEFT

While you are using your laptop around town or traveling, use the following tips to keep it in your possession:

- **Avoid using computer bags.** Computer bags have become an easy signal to thieves that you have something valuable to steal. Try using a more common case such as a padded briefcase, backpack, or luggage.
- **Use strong passwords and do not keep them in your laptop's bag.** Strong passwords keep unauthorized eyes from seeing sensitive files or personal information on your laptop. Security experts recommend that to make your passwords strong that you:
  - Make your passwords eight or more characters long.
  - Make your passwords complex by including letters, punctuation, symbols and numbers.
  - Change your passwords often.
  - Don't use the same password for everything.
- **Encrypt your data.**
- **Use a screen guard.** A screen guard can prevent preying eyes from seeing sensitive information when you are using your laptop in a public place.
- **Carry your laptop with you.** At the airport or train station, take your laptop with you in the plane or train, do not place in the checked luggage. When traveling by car, place it out of sight in your trunk when you have parked your car and you are not using it.
- **Keep an eye on your laptop.** When going through security at the airport hold on to your laptop until the person ahead of you has gone through screening.
- **Avoid setting your laptop on the floor.** If you do need to set it down, place it between your legs so that you won't forget it.
- **Use a security device or program.** Use a security cable to attach your laptop to a heavy chair, table or desk. Install a program that can report your laptop's location.
- **When traveling, try not to leave your laptop in your hotel room.** If you must leave your laptop in your room, place the "Do not disturb" sign outside of the door to keep the hotel staff out.
- **Affix your name and your personal code to your laptop.**

MOBILE SECURITY– PROTECTING YOUR SMARTPHONE

Another amazing tool that has become prominent in usage is the smartphone. These are basically computers with a capability well beyond the computers that we used 10 or 15 years ago. Not only are smartphones susceptible to theft they are also susceptible to being hacked so that someone else can gather the private information that they contain.

Some things to consider to protect your smartphone include:

- Use a password or PIN number to protect your information should you lose your phone or it is stolen.
- Be sure that your phone has a capability that helps you find it should it be stolen or you lose it. This can be an app that you add to your phone or it can already be included in your phone or as part of your cell phone carrier's system.
- Look for features that allow you to lock your phone remotely and to wipe the information in your phone should you not be able to retrieve it. If a locking wipe feature is not included, find an app that can lock and wipe.
- Be careful of the source of the apps that you install. Use the official online stores for the operating system of your phone such as from Apple or Microsoft.
- When considering apps to download, take time to look at the terms of service, the permissions the app will ask for and make sure you understand what the app is going to do. For Android users, consider installing a malware scanner app to protect your phone from malware apps.
- Like you should with your PC or laptop, be sure to install the latest updates for your operating system and your apps. This way you can be sure that you have the latest security features as well as the latest feature enhancements for your phone.
- When you are surfing the web try to use secure Wi-Fi networks. This way you can ensure that the data you are transmitting is encrypted and more difficult to intercept by a stranger. If you are planning to do sensitive tasks such as online banking use your carrier's 3G or 4G network. Definitely do not do sensitive tasks over an unsecured Wi-Fi network. Some security analysts recommend turning off connectivity capabilities such as Bluetooth, Wi-Fi, and near-frequency communications (NFC) unless you are actively using them.
- Go to the Federal Communications Commission's "Smartphone Security Checker"- (http://www.fcc.gov/smartphone-security) for more specific information on the steps to take to secure your phone.

MOBILE SECURITY– MORE TIPS

- ***Do not modify your smartphone's security settings.*** *This can make you more susceptible to attack.*
- ***Backup and secure your data.*** *Regularly backup your data, contacts, documents, photos, to your PC at home, a removable storage card or the cloud.*
- ***Wipe your old phone before you donate, sell or recycle it.*** *Completely erase the data from your phone and then reset it to initial factory settings.*
- ***If your smartphone is stolen, report it.*** *Report the theft of your phone to your local law enforcement and to your wireless provider.*

MOBILE SECURITY– WHAT IS THE THREAT

So what is the threat to my mobile device? Why should I be worried?

According to Wikipedia (http://en.wikipedia.org/wiki/Mobile_security) there are three major threats to your mobile device from four major actors.

Mobile device targets:

1. **Data.** Your mobile device potentially holds lots of private information that a thief can use such as your credit card numbers, authentication information, private information such as your medications, your address book, etc. Thieves might even be interested in your activity logs such as your calendar and call logs.
2. **Identity.** Your smartphone holds information that is specific to you. A hacker could gather the account information for your cell phone plan to use in another crime.
3. **Availability.** A hacker might want to deny you access to your phone service.

People who want your personal information:

1. **Professionals.** These can be from commercial or military organizations who steal from the general public to gain access to sensitive personal, business or military data. They may also conduct industrial espionage.
2. **Thieves.** ID thieves want to collect your identity information to gain income or buy products or services with your money.
3. **Black hat hackers.** Black hat hackers have a goal of developing viruses that can damage your device or steal data.
4. **Grey hat hackers.** Grey hat hackers try to expose vulnerabilities in your device or the cell phone system. Generally, they do not intend to damage your device or steal your data.

CRIME PREVENTION COORDINATORS

ANN GIFFORD, OFFICE OF COMMUNITY PARTNERSHIPS
neighborhoodwatch@snoco.org

425-388-7375

SHERIFF'S OFFICE CRIME PREVENTION WEB PAGE:

http://sheriff.snoco.org/Sheriff_Services/Crime_Prevention.htm

NEWSLETTER INFO

EDITOR
Steve Moller

If you have questions regarding this newsletter or any articles that appear in it, please contact the editor at neighborhoodwatch@snoco.org

TIP LINES

Snohomish County Sheriff's Office: 425-388-3845

http://www.snoco.org/app/ssh/anonymoustips/

Crime Stoppers of Puget Sound: 1-800-222-8477