

Securing Laptops Seminar Notes***

Chris Papas CISSP

chris@netsecurity.pro

* 10,278 laptops are lost per week in US Airports. Most are left at TSA checkpoints and some are stolen by thieves targeting laptops. Sometimes the thieves target specific models of laptops and sometimes they target your laptop to get your data.

* 4,400 laptops are left in Chicago Taxis alone.

* Use Kensington type locks to secure laptops at home and at work. They attach to your laptop using a slot in the side of the case and have a cable that is attached to your desk or work area. The locks come in two models, key and combination lock. The locks can be defeated with enough force but Pawn shops won't take the laptops in if the case is broken at the attach point. The cable can also be cut but then again a pawn shop won't take a laptop with half a lock still attached. Also, thieves may leave the laptop alone if it takes too much time to break the lock since they want to be in and out as quick as possible.

* Use an unobtrusive laptop bag to carry your laptop. Identifying it as a Dell or Mac laptop will only let the thieves targeting a specific model know where to find one. *I got a generic laptop bag from Wall-Mart.*

* Don't leave a laptop in your car or rental car. They will break in the vehicle just for the laptop.

* If you see someone selling laptops with out the power adapters then the laptop is probably stolen. Thieves don't always take the time to get the power adapters when they take the laptop.

* Take precautions when using public transportation with your laptop; taxi, bus, train, etc. You may leave it behind or thieves working the crowd could steal the laptop and be gone in a minute. Pretty girls provide a great distraction to executives while the boyfriend is stealing your laptop. Keep the laptop in your lap and/or keep the strap for the bag around your arm or leg.

* Use a label service on your laptop like Inspice.com or Imhonest.com. If the laptop is "found" then it can be returned to you and Imhonest.com will even let someone take the laptop to a UPS or Fedex location and it will be returned to you at no charge to the person who found it. If someone goes to a Pawn Shop with a laptop that has one of these labels on it then the shop is going to call and find out if it is stolen before they do anything. With Pawn Shops typically paying \$400 for a laptop, they want to make sure that the police won't come and get it the next day and be out their \$400.

* Use a software tracking service on your laptop, ie Absolute.com The software phones home to the service on a regular basis. If you file a police report and notify the service that the laptop is stolen then the next time the laptop is fired up the service will track it .

They then help the police identify where it is and Absolute.com even helps the police fill out a search warrant. The software can also hide itself in the bios so if a new hard drive is installed in the laptop then it will reinstall itself on the hard drive and phone home again. If the laptop was stolen at work then prepare to get HR involved since it will usually be found with a soon to be former employee.

* Using a remote data delete software is not enough. Hard drives can be pulled from the laptop before it is turned on and your data can be copied off before any remote delete software can be triggered. If they are targeting your data then you lose.

* Get some insurance for your laptop. Safeware is the biggest company for this.

* People don't want to take the time to backup their systems but they sure want their data back after something happens. Backing up to a local USB drive is better than nothing but sometimes the laptop and the USB drive are stolen together. Francis Ford Coppola example.

The Oscar winning director suffered a break in at a studio in Argentina where he was working on a new film. The thieves stole computers, and crucially a back-up device that had been left on the premises.

"They stole our computers. They got all our data, many years of work," Coppola told the BBC.

* Use a Pirate backup system AARRGH

A – Automatic... It must be automatic or it won't get done.

A – Archive... Archiving you data means that you can get back if what you have is gone

R – Redundant... Have more than one backup of your data or at least in another location.

R – Restorable... Test it and make sure that the data can actually be restored.

G – Generations... Use different generations for data

H – Happiness... When the data can be restored they will be very happy.

“If you ain't got all these then you ain't got a backup”

* Backups come in three types

A. File based Backup – Continuous data protection & synchronized folders. Can be local or online. Services include: BelnSync and GoodSync.

B. Image backup – Takes a snapshot of every byte on the hard drive. This is the fastest way to get a system back up but doesn't include any data after the last image was taken of the system. Services include: Storage Protects, Acronis, True Imate

C. Online backup – Backs up specific files or whole drive. Services include: Mozy, Carbonite and many others. Mozy includes 2 GB free for home users.

* Use Pre-Boot Full Data Encryption (FDE) on your laptop hard drive. This software starts before the operating system starts and you have to enter in a password or the drive data will stay encrypted and not useable. Some new drives come with FDE installed. If someone takes out the hard drive and tries to copy data then they won't get anything useable. This also can be used on external drive such as USB drives and CD/DVDs. These sometimes cause performance issues depending on hardware. (your mileage may vary) Services include WinMagic.com (external disks), TrueCrypt.org (free), PGP.com.

* Defend against WiFi predators

- Turn off File Sharing
- Turn on Firewalls
- Disable Guest Account
- Use "Real" Passwords
- Make sure that you use strong encryption, no open systems, no WEP with weak passwords.
- Turn off/Disable WiFi altogether if you are not using

* Use VPN back to your network, especially from public places, ie Starbucks. This helps avoid the Man in the Middle attacks by using end to end encryption.

* Trade WiFi for Cellular Data Networks (CDN), you have to either add a plug-in (or USB) data card to access network. Some new laptops come CDN enabled.

* Performance Enhancements

- Remove old programs that you don't use
- Shut off resident programs from running esp when you are not using them, such as: Adobe, Desktop index, HP, Java, MS Office, Quicken.

* More Security

- Use personal Firewalls. Microsoft Firewall is not enough. Comodo and Zone Alarm are free and work much better.
- Use Anti-virus and Spyware protection. Microsoft Defender is not enough. *Both BitDefender and AVG have free versions that work very well although I recommend BitDefender as the better one for XP and older. Spybot anti-spyware is a must for any computer. Don't leave home without it.*
- There are now viruses out for Mac computers so they need virus protection also.
- Some companies disable all USB ports on laptops to prevent infections. Easy way to target companies or a specific computer is to provide an infected USB drive.
- Some companies use software like LanDesk or Cisco NAC to check computers for infections/compliance before they are plugged into the network.

* Preventive Maintenance

- Defrag Hard drives
- Keep airflow clear around laptop.
- Vacuum out dust
- Use a fan powered cooling pad. Heat buildup ruins laptops.

*** These notes were taken on 11/13/08 at the ITEC Atlanta 2008 Conference & Exhibition given by James Gaskin, Author and Columnist, Network World. I'm sending around so my Family and Friends can help keep their laptops safer in an unsafe world.