nLightened Thoughts

September 2013

William Blinn Communications
Worthington, Ohio 43085
www.n-lighten.us • 614/859.9359

Beware! There's Danger in Your Pocket.

Portable devices such as thumb drives, smart phones, and tablets are among the most powerful productivity tools available today, but they can also open gigantic security holes that can allow access to your company's proprietary data.

Security experts have long expressed concern about these and it doesn't matter what brand the device is or what type of device it is. Any electronic device that connects via Wi-Fi can be compromised, as can any device with enough memory to contain corporate files.

Everybody likes ease of use and convenience, but keeping proprietary data from falling into the hands of competitors is something that most people also want to do. These two interests compete because security usually means *harder to use* and convenience often means *reduced security*.

Research by Internet security specialist Webroot reveals some surprising and distressing figures, as the graphic above shows.

There's no one-size-fits-all solution because each situation is unique. The cost of security, both in terms of what you must pay for security software, hardware, and services and the cost that results from inconvenience, must be balanced against the potential cost of losing control of data.

Threats Abound

Mobile computing devices can store huge amounts of data and they're cheap.

Thumb drives that hold 64GB of data are readily available for $30 or less; tablets and phones may come with 32GB of storage and sometimes 64GB. A typewritten page contains approximately 2000 text characters, so a 64GB storage device would hold more than 33 million 500 thousand pages! Thumb drives and phones are so small that they fit easily even into a shirt pocket.

These portable devices are often unprotected and they can easily be lost or stolen.

Some people consider the greatest threat to be thumb drives, but these are old technology and a data thief must possess the device to use it. It's easier to just sit in a public location and grab data out of the air when unsuspecting business people connect to open Wi-Fi hotspots.

Once they've pulled user names and passwords out of the air, thieves can gain access to protected resources at their leisure.

Phones and tablets are a double threat because they usually come with large amounts of built-in memory and they can communicate wirelessly over non-secure networks. Thieves have two opportunities: They can steal the physical device or they can steal data as it's being transmitted to an open Wi-Fi hotspot.

nLightened Thoughts (ISSN 1543-1533) is for clients and friends of n-Lighten.us, 179 Caren Avenue, Worthington, Ohio 43085. Phone 614.859.9359. On the Web at www.n-Lighten.us.

Solutions Are Easy

For thumb drives and the memory in all portable devices, encryption is wise.

When devices are encrypted, the data contained on them is at least more difficult to extract. That's not to say *impossible* because someone with sufficient computing resources and a strong enough need to know what's on the device will probably be able to break the encryption. But it's enough to thwart run-of-the mill desperadoes.

As for eliminating the over-the-air threat, that's so easy that I'm always surprised when I learn that somebody isn't doing it.

Virtual private network (VPN) software can encrypt data when it's in the air, between your device and the open Wi-Fi hotspot.

Regardless of the type of portable device you use, you'll find variety of VPN products and services that are available. If you're protecting an Apple phone or tablet, you should obtain the app from the Apple Itunes Store. For Android devices, download the app from Google Play or the Amazon App Store. And for Windows tablets or phones, you'll want to visit the Windows Store.

Relying on official channels for apps won't guarantee that you'll never download malware, but it does provide some assurance that the app you've selected has been validated.

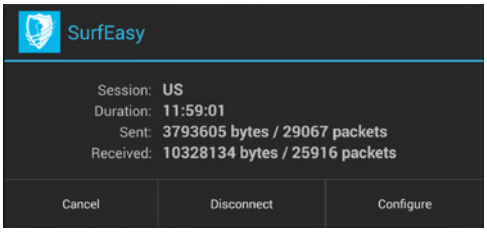
VPN applications require little or no technical knowledge to install and use. If you know how to download and install an app, which is essentially an automatic function on smart phones and tablets, and you can create an account using your e-mail address and a password, you already know how to set up most VPN apps. Many of the services provide the VPN without charge for limited use. If you spend a lot of time online via Wi-Fi, you will need to pay a few dollars per year for the service.

Given the amount of protection VPN provides, the small annual fee is well worth the cost.

A Recommended VPN Client

Most VPN clients are relatively easy to install and set up, and most offer adequate free bandwidth for the occasional user.

But if you need the services of a VPN on multiple devices and more than a few times per month, you'll need something that goes behond the basic free plan.



I recently found a service called SurfEasy that works with Windows computers, Apple computers, Apple phones and tablets, and Android phones and tablets. For just $4 per month, you can protect any combination of up to 5 devices. If you have just a single device that needs to be protected, you'll pay $3 per month.

In addition to encrypting the signal between your device and any Wi-Fi hotspot, SurfEasy also obfuscates your location. I'm less interested in pretending to be several hundred miles from my actual location than in simply encrypting information that I send over the Wi-Fi connection. Sending login IDs and passwords in the clear is never a good idea.

You can download the SurfEasy application (www.SurfEasy.com) and use the free service to see if you'll like it. Keep in mind that the free service does have bandwidth limitations. If you use it a lot, you'll soon run dry. In my case, it too just 2 days for me to decide that paying $48 per year would be a good deal to provide unlimited encrypted communications for 5 devices.

Because SurfEasy works for all types of computers and mobile devices, you can also sign up on the company's website and download versions for your Windows or Mac computer.

Other Good Ideas

Don't stop with just a VPN, though. There are many other relatively easy ways to protect the data on your portable computing devices.

- Label portable devices with your name and a phone number. You might be surprised how many people actually attempt to return things that they find, but they can't do that if there's no way to identify the owner. Many phones and tablets have a screen that can identify the owner, but if the device's battery is dead, it won't work. A label is a good idea.
- Password protect the device. That should be evident, but a surprising number of people carry around devices that aren't password protected and also aren't encrypted.
- Set timeout on the device so that it will automatically turn off and lock when it's not in use.
- Run updates frequently or allow the device to update the operating system and all apps automatically. Updates are sometimes designed to provide new features, but most updates address security flaws and you shouldn't skip them.
- Download apps only from official sources such as the Apple Itunes Store, Google Play, or the Amazon App Store. Malware can be distributed via these official channels, but the likelihood is reduced considerably because the store keepers vet apps before allowing them to appear. Apple's process is generally considered to be the strongest of the bunch.
- Services exist that will attempt to find your mobile device if it's lost or stolen. The service can report the device's approximate location and also might be able to engage the on-board camera to take pictures of the current user. Various services exist and some are specific to certain types of devices.
- Use hardware encryption if the device supports it. Sometimes encryption can be used in conjunction with device-finder software to delete data from a stolen device.
- Thumb drives, and any device that's used to store sensitive data, should be encrypted. Although software encryption such as TrueCrypt is free and easy to use, the easiest solution involves using flash drives that are self-encrypting. These are much more expensive than standard thumb drives ($125 for a 16GB drive) but devices such as the Apricorn Aegis Secure Key will automatically destroy all of its data if it determines that it's being attacked.

Being careful, using reasonable security practices, and adding applications that protect your privacy won't guarantee that you'll never be victimized by data poachers, but you'll make your data a much less attractive target. The harder you make a thief work, the more likely it is that the thief will forego your data and attack a softer target. Ω