Security Newsletter No. 6

July 2006

SECURITY NEWSLETTER

Our last newsletter covered VOIP, Skype, Norton Internet Security, and Flash Drives. In this issue, I'd like to cover Laptop Security and Credit Card Fraud.

Laptop Security

More and more users have a laptop, travel with a laptop, and fall victim to laptop theft! They can be a great convenience, but also a great security risk – we've all heard the stories of company laptops that are stolen with private data on them. This is not only a major inconvenience for the business, but a breach of privacy. Yet theft and data loss are very preventable. Here are some things that you need to be doing to secure your laptops and the data contained within them.

My 7 Step Plan

7. When traveling, always carry your laptop with you rather than checking it with your luggage.
6. Pack your laptop bag inside of a standard small suitcase to disguise it, laptop bags can be a standout for a thief just waiting for a momentary lapse on your part when you set your bag down.
5. Never leave passwords or access numbers on notes in your laptop bag. By separating passwords from your laptop you'll make it impossible for a thief to gain access to bank accounts or password protected files by using internet shortcuts, etc. It is ALWAYS advisable to **never** let your internet browser "remember" passwords when prompted to do this.
4. Use laptop security devices when working out at an unfamiliar office. Most have a security slot for such devices like a Kensington lock to be attached and connected to a desk or table leg. The harder you make it, the less likely a thief will try to steal YOUR laptop.
3. Consider special security software that allows physical tracking of your laptop such as Computrace and others. These services require annual fees (small) but will report the location of your laptop when it is connected to the internet and used by a thief.
2. Secure VPN clients by requiring passwords to login to your network. Many laptops have VPN software installed to communicate with your office – most can be configured to require a password in addition to a simple shortcut, make sure you do this!
1. NUMBER ONE – Encrypt important and private data on your hard drive. If your laptop is stolen after taking all of the above precautions, at least your private data won't be compromised.

Encryption Options Examined

Although all of the above steps are important, we'll examine my number one consideration in detail because it is often the one most overlooked.

If you are using Windows XP Professional, you already have a method to encrypt data built into the operating system. Simply locate a folder or file, right-click, select Properties, Advanced Attributes, and then check the "Encrypt contents to secure data" box. This ONLY works if your computer is password protected and not set to login automatically. This feature will prevent someone from logging in as another user or pulling the hard drive and copying off the encrypted data.

Please note that by using this feature, however, you can prevent yourself from recovering your own data if you forget your password or your user profile gets corrupted. Therefore, my recommendation is to use this feature only for selected files or folders. It is often better to look at options not linked to your Windows password, or be sure to use good passwords – length is the most important password attribute.

A second choice is a very inexpensive product by Stompsoft called Digital Vault for about $29 that can encrypt files. This is a simple-to-use encryption utility that installs a hidden file on your hard drive where files are stored encrypted when you add files to the vault.

A third choice is PGP Desktop Home 9.0 or Professional 9.0. This more full-featured product and is from a company that has been around many years doing file encryption. Starting at $99, these products can encrypt a virtual disk, create self-decrypting archives, plus offer file shredding capability. The Pro version adds whole disk encryption and integrates with their enterprise products.

There are many other products out there, often they may be overkill for small business, but the important thing to take away is that additional security on a laptop is very important. Even if this simply means password-protecting files like Excel or Word documents – this is better than nothing, but full encryption software is the best way to go.

Credit Card Fraud and Identity Theft

Most of us make internet purchases and credit card usage is frequent not only on the internet but in everyday purchasing. Here are some tips to help avoid credit card fraud and identify theft.

Ways to reduce risk

1. Use the internet and be pro-active by checking your account statement online frequently. Unrecognized charges may go undetected by your

credit card company but you may notice them sooner. Why wait for your paper statement to arrive!
2. Sign up for e-mail alerts if your credit card company offers that. Anytime account activity takes place you will be alerted.
3. Make sure your credit card companies' email address is in your email software "whitelist" or not blocked as spam.

Stay informed about identify theft

1. Check with your credit card company, they usually have identity theft "kits" on their website, forms to use to fraudulent activity and the like.
2. Keep on top of your credit reports by using the credit bureaus – www.equifax, www.experian.com, and www.transunion.com.

Avoid social engineering scams

1. I've highlighted this several times before, but NEVER respond to emails asking to update your account (credit card or any other) where you click on a link and go to a website.
2. When in doubt, pick the phone and speak to your credit card company.

That's it for this issue – my next issue should be out in September. Till then, stay secure and encrypt those important laptop files…