IN THIS ISSUE:
~ Security

COMING NEXT MONTH:
~ All About PDFs

READY NET GO … NEWS

November 2005 **http://www.readynetgo.net** **610-856-0990**

Tip of the Month

Free Credit Reports

Last year, the federal government signed into law an amendment that will allow all Americans to obtain a free copy of their credit report from the three credit reporting agencies: **Equifax**, **TransUnion** and **Experian**.

Those living on the East Coast can now call or go online and request a free credit report from each of these agencies each calendar year.

The central website to obtain your credit report is:

http://www.annualcreditreport.com

OR you can call **1-877-322-8228** or visit the website for the address to send your request by mail.

Tip 1: The website www.freecreditreport.com is not affiliated with this federal site – there is a charge to obtain your credit report from this company.

Tip 2: Although each of the agencies will have different information on your credit history, you don't need to get all three credit reports at the same time. Since you are allowed one free credit report from each of the three agencies, you can request one report from one agency in December, another report from another agency in March and the third report from the last agency in August. This way you'll be able to monitor your credit throughout the entire year.

Tip 3: Your credit score is different from your credit report. You'll have to purchase this report separately.

Security … Are You Concerned?

I recently overheard a conversation. It went like this:

Paul: Mary, you're not going to believe what happened to me yesterday. I was surfing the web when all of a sudden my screen went black. I tried to restart my computer but it just kept going into an endless loop.

Mary: Wow – what did you do?

Paul: I had to call the tech department to fix it. They said I had loads of spyware on my computer including keyloggers and even a Trojan horse (whatever that is)

Mary: That doesn't sound good. Did you lose any data?

Paul: Oh yeah, I was working on a presentation at the time. I was surfing the web and looking for some specialty fonts and all of a sudden all of these pop-up boxes came out of nowhere. When they got my computer working again – after 5 hours!! – my whole presentation was gone. I had start all over again …

Mary: Did they offer any suggestions for preventing that from happening again?

Paul: Yeah, they were pretty cool about it. They said that they can only go so far in protecting people's computers like setting the computer to update the OS and anti-virus software automatically but that each user needs to play a part. One of the guys suggested to run anti-spyware software regularly, don't click on banner ads on webpages, don't click on advertising links in emails, don't use Instant Messaging programs, and be extremely careful about what software I download over the Internet especially file sharing apps, specialty fonts, browser toolbar add-ons, and screen savers.

Mary: Well, I can do all of those things especially if it will keep my computer running smoothly. Thanks for the tips!

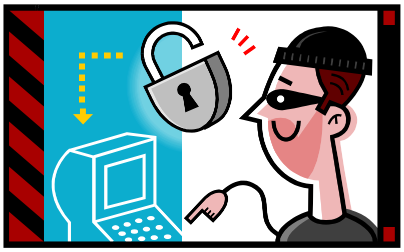
WWW (Websites Worth Watching)

1. www.wunderground.com – if you're into weather, check out this site (just disregard the ads). There's a lot of information including lunar cycles, storm watches, aviation reports, historical data and a lot more.
2. www.ftc.gov/credit - Federal Trade Commission site provides information to consumers on how to protect your finances during transactions.

When it comes to computers, security is everyone's concern; we must all take an active role. Not only is there an increased risk from viruses or spyware but the likelihood of someone tracking your personal data is increasing. How personal data is stored and transmitted is very concerning to a lot of folks. Groups like the **Center for Democracy and Technology** and **Privacy Rights Clearinghouse** are working to ensure that people's privacy rights are not violated while they are online. The issue goes far beyond having a ton of advertising emails (SPAM) in your Inbox. The issue involves the transmission of your personal contact information like name, address, age, credit card numbers, financial data, credit history, and even products you've bought, to people who will use this information to their advantage not yours.

Who are these hackers and why are they trying to disrupt our lives?

The majority of people in the world are good-natured, loving souls who just want to carve out a little niche in the world and have a few laughs along the way. Hackers are a different breed…



The term hacker can mean different things to different people. For the sake of this newsletter, we consider hackers to be individuals who exploit a system or gain unauthorized access to a computer or network. Some examples of hackers would include an adolescent who enjoys computers and wants to push the limits, a disgruntled employee of a major corporation or university, an individual who wants to make a political statement by denying access or someone who seeks economic gain in disrupting networks.

Hackers, therefore, create malicious programs for intellectual curiosity, economic gain, political opposition, entertainment, and revenge. Basically, as long as we have computers and the world is connected via the Internet, security is, and will continue to be, a major concern that is forever evolving.

What makes matters worse is that many networks are unprotected and are relatively easy to break into. If a network is compromised it's very difficult to trace who the intruder is or where the intrusion originates which increases the appeal. In effect, a hacker is like a well skilled burglar who wears gloves, has night vision goggles, and has already obtained a detailed map of your house…as soon as he/she finds the key hidden under the rock, its smooth sailing…

How can hackers get into my computer?

There are many **ports** on your computer that **act like doors** in a house. Each port is used for a specific type of communication just like each door enables you to enter a different room in your house. Some examples: the parallel printer port is used for attaching a printer; the USB port is used for attaching printers, digital cameras, flash drives, etc; email communication is transmitted through its own SMTP port; and connecting to the Internet has various ports of entry/exit. With this many ways into your computer, you need to make sure that these ports are not wide open for anyone to enter at anytime.

An Example:

If your computer is connected to the Internet, it's set up for **two-way communication** which means you can ask for information and you can receive information. When you open a browser and surf the web this is what is happening. You click a link, the server receives your request, and sends the website to your computer so you can look at the information. If it's a reputable site, you probably won't experience any problems but if the site has special code installed to download programs to your computer or the site has been hijacked by a less reputable company, then problems will arise and you won't even be aware of it until the damage is done (since most viruses and Trojan Horses run behind the scenes altering the underlying code on your computer).

How do I prevent hackers from getting into my computer?

Well, you can go to the extreme and pull the plug but that's impractical. So we've created a list of security measures everyone should implement:

1) Learn about security – don't push it away thinking it isn't going to happen to you. As marketers increase their advertising and unscrupulous people continue to make money, the chance of your data getting into the wrong hands will increase. Start now and you may avoid a major hassle in the future.

2) Heed the warnings – if you hear on the nightly news that there is a new virus going around, the first thing you should do is make sure your computer has the latest security patch from **Windows Update** installed and install the latest virus definitions from your anti-virus software. Windows 2000 and XP and most anti-virus software have a scheduled update feature so you don't even have to remember to update your computer. Just make sure the feature is turned on if you know you won't remember to do it manually. In Windows XP and 2000, click Start, Settings, Control Panel, Automatic Updates – click the button for Automatic.

3) Use firewalls – software and hardware firewalls block certain types of data. A firewall is like a big, steel door. If you have the right key, it opens easily. If you don't have the right key, you're going to have a hard time breaking in. **Hackers prefer the easy jobs** – don't give them an easy way into your computer.

Note: Verizon is offering special pricing on DSL service right now. With all broadband connections, security is a concern so you'll also need a **router** (cost ~ $50) in addition to the modem they provide. Keep in mind that you don't need to use Verizon's products, especially if they offer to rent you equipment. Some modems you can purchase have an integrated router/firewall which will help to keep your peripherals under control. And if you decide to add computers to your network, you'll be able to share the broadband connection via the router.

4) Malware – Viruses, worms and Trojan horses aren't the only ways to ruin your day. Spyware and Adware can do equal amounts of damage causing your data to be inaccessible, your personal information being sold for big profits, and even for your computer to be so overloaded you have to reinstall the Operating System (effectively losing all your data unless you recently backed up your computer). This could happen to anyone who accesses the Internet despite their good-natured intentions. Protect your computer and your personal information by using anti-spyware applications like Lavasoft's **Ad-Aware** (http://www.lavasoftusa.com – it's free for personal use and it works).

5) Password protection – make it hard to crack – use upper and lower case letters, special characters and numbers. If it's in a dictionary, your password will be figured out.

6) File Extensions – one of the ways that Malware can get on your computer is if a user clicks on an attachment in an email. To prevent this, make sure that all file extensions are visible so you'll be able to detect if that photo you got from Aunt Mary is really "cat.jpg" and not "cat.jpg.exe". To do this: open **Windows Explorer**, click **Tools** on the main menu, scroll down to **Folder Options** and click the **View** tab. Scroll down the list and **UNCHECK the box** next to: Hide extensions for known file types. While you're there, click the radio button for Show hidden files and folders.

Email tips

1) As tempting as it may seem, don't open email attachments that you haven't specifically requested. A common email is one with an individuals name in the sender field and in the subject field, it states: **Your order has been refunded** or **Here is the information you requested**. Before you open or view these messages, think about what's happened in your life recently. Have you placed an order and asked for a refund? Have you specifically requested information from an organization or individual – and if so, does the name look familiar? If you haven't, delete these messages without opening them. At the least, these messages are SPAM and at the worst, they could contain a virus or Trojan Horse ready to disrupt your computer.

2) If you use MS Outlook as your email client, **turn off the preview pane** so that when you open your Inbox, all you see are the initial headers (Sender, Subject and Date). You can delete the messages that are suspect and open the ones you want to read without worry that you may inadvertently start a process that you can't stop.

3) If you're not sure if an email message is harmful, in Outlook 2003, right click the message and scroll down to **Options …** In the box, **Internet Headers**, look for the sender's email address. If it looks suspect, delete it!

4) Spammers love it when people click on their emails because it indicates you're a real person and your email address is "live". Spammers regularly sell their "live" lists for big money. If you don't click on an advertising email, the spammer is left guessing and has no proof your address isn't "dead". Images in emails can be spoofed as well – which means the images can actually be fabricated and have damaging code hidden so that when you click on an image to open a website, the code is installed on your computer. Steer clear of images in emails to avoid spoofed websites!

5) Setting your email client to view emails in HTML may look better but it isn't safe. Set your client to **view emails in plain text** and you'll avoid the cleverly disguised HTML code (described above) that will wreak havoc on your computer.

Check out these various sites on Internet Security:

1) www.idtheftcenter.org – Non-profit organization that dispenses ID theft information. Check out the Scams and Consumer Alert section.

2) www.privacyrights.org – Non-profit Consumer Information and Advocacy Organization. Click on **Identity Theft** on the left side navigation bar and take the **Identity Theft IQ Test**.

3) www.cdt.org – **Center for Democracy and Technology** - seeks practical solutions to enhance free expression and privacy in global communications technologies.

4) www.cert.org – **Computer Emergency Readiness** (or Response) **Team** – Research facility based out of Carnegie Mellon University in PA seeks to analyze and respond to threats to networks and technology. Also see www.us-cert.gov

5) www.ftc.gov/infosecurity/ - **Federal Trade Commission** – Meet Dewie the e-turtle, get information on computer security for both adults and children, and learn how to safeguard your personal information.

Have you backed up your data recently??