October 2011 Special Security Edition

October is National Cyber Security Awareness Month

By Ira Wilsker
iwilsker (at) sbcglobal.com

WEBSITES:

http://staysafeonline.org/ncsam
https://isc.sans.edu/diary.html?storyid=11623&rss
http://news.yahoo.com/maryland-recognizes-national-cybersecurity-awareness-month-160244986.html
http://blogs.cisco.com/security/cisco-joins-the-national-cyber-security-awareness-month-party/
http://gta.georgia.gov/00/press/detail/0,2668,1070969_167558063_163659118,00.html
http://uit.tufts.edu/?pid=624
http://msisac.cisecurity.org
http://www.microsoft.com/security/resources/cybersecurity.aspx
http://staysafeonline.org/cybersecurity-awareness-month/2011-ncsam-champions
http://www.uscert.gov/reading_room/brochure_securityguidance.pdf
http://www.uscert.gov/reading_room/posters_all.pdf
https://www.sans.org/critical-security-controls
http://security.vpit.txstate.edu/training/csam_2011.html

PDF AND WORD FILES:

http://staysafeonline.org/cybersecurity-awareness-month/banners-and-more
(has links to PDF and Word files for child, parent, and student cyber safety)
http://staysafeonline.org/sites/default/files/resource_documents/Gaming%20Tips%20for%20Kids%20STC.pdf - Gaming Tips for Kids
http://staysafeonline.org/sites/default/files/resource_documents/College%20Students%20Internet%20Safety%20and%20Security.pdf - Internet Safety and Security for College Students

http://staysafeonline.org/sites/default/files/resource_documents/Parents%20Internet%20Safety%20and%20Security%20STC.pdf - Internet Safety and Security for Parents

It is that time of year again. In 2004, with the fear of cyber war increasing, and early indications of cyber-attacks already taking place against our critical infrastructure, private organizations, and government agencies, President Bush issued a proclamation declaring that October, 2004, would be "Nation Cyber Security Awareness Month" (NSCAM). Every October since, Presidents Bush and Obama have made similar declarations, acknowledging the degree of threats that we all face, in terms of cyber security. One consistent factor in the declarations and implementations of the program is that it is not just our public and private agencies that have been threatened, but our personal safety and security is at extreme threat as well. Our personal computers can be unknowingly hijacked by a foreign power or terrorist organization, and under remote command, be used to launch a potentially devastating cyber-attack against our government or infrastructure, simultaneously coming from millions of our personal computers!

Nation Cyber Security Awareness Month is a joint public - private partnership between the Department of Homeland Security (www.dhs.gov/files/programs/gc_1158611596104.shtm), the National Cyber Security Alliance (staysafeonline.org/ncsam), and the Multi-State Information Sharing and Analysis Center (msisac.cisecurity.org). Together, these three organizations have brought together government agencies (federal, state and local), educational institutions, corporations and community service entities to promote a coordinated national program designed to educate everyone on the risks endemic in the cyber world, and methods to harden our computers and other smart devices from cyber-attack.

Taking the lead is the National Cyber Security Alliance (NSCA), which is providing the primary coordination of activities, supplying free informational materials that anyone is free to copy and distribute (staysafeonline.org/cybersecurity-awareness-month/ncsam-tip-sheets). There is one common thread in all of these NCSA documents (staysafeonline.org/cybersecurity-awareness-month/about-ncsam-2011); "It starts with STOP. THINK. CONNECT., a simple action for all of us to employ to stay safer and more secure online. STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems. THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's. CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer. By incorporating Our Shared Responsibility and STOP. THINK. CONNECT. into your online routine, you will be doing your part in protecting yourself, your family, your community and your country."

To assist individuals and families in securing their computers, the NCSA has published a variety of "tip sheets" including Gaming Tips for Kids, Gaming Tips for Parents, Internet Safety and Security Tips for College Students, Internet Safety and Security Tips For Parents, Mobile Safety Tips, and Social Networking Tips. If individuals would follow and apply the tips presented in these documents, we and our families may become much safer and more secure while online. Support for these NSCA activities comes from several dozen private companies, non-profit organizations

and government agencies (staysafeonline.org/cybersecurity-awareness-month/2011-ncsam-champions). The NCSA website also has age appropriate activities and learning materials for children that may be freely used by school teachers and parents.

The Department of Homeland Security (DHS) is most aware of the degree of danger that we are facing from cyber-attack on our computer and domestic infrastructure. DHS says, "The most serious economic and national security challenges we face are cyber threats. America's economic prosperity and competitiveness in the 21st Century depends on effective cyber security. Every Internet user has a role to play in securing cyberspace and ensuring the safety of themselves and their families online." (http://www.dhs.gov/files/programs/gc_1158611596104.shtm)

While most of us are by now aware that we need to secure our personal computers, there is also an extreme need to secure our business, government and educational computers, as well as harden our infrastructure to cyber-attack. Several governmental and educational agencies have made free materials available to train employees, and increase awareness of the need for increased and improved cyber security. The United States Computer Emergency Readiness Team (US-CERT), a part of the Department of Homeland Security has released a two-page brochure "Protect Your Workplace, Guidance on Physical and Cyber Security and Reporting of Suspicious Behavior, Activity, and Cyber Incidents" www.uscert.gov/reading_room/brochure_securityguidance.pdf). While only two pages, this brochure contains pertinent information on Cyber Security Guidance, reporting Cyber Security Incidents, Physical Security Guidance, reporting Suspicious behavior and Activity, and a listing of the Joint Terrorism Task Force (JTTF) phone numbers. The information in this brochure is not just appropriate for government agencies, but is also relevant to any other business, college or other organization, as all of them may be vulnerable for a targeted cyber-attack. In order to help facilitate cyber security, US-CERT also has a series of free posters and other information available which can be printed and placed around the workplace (www.uscert.gov/reading_room/distributable.html).

State, cities, counties, and educational institutions are also active participants in the National Cyber Security Awareness Month activities. Several states, such as Georgia and Maryland, have issued statewide proclamations and implemented statewide activities to promote cyber security activities. Recently Maryland announced its "CyberMaryland, an aggressive business development and marketing initiative to strengthen Maryland's burgeoning cyber security industry and protect the nation's digital infrastructure." (source: news.yahoo.com/maryland-recognizes-national-cybersecurity-awareness-month-160244986.html). Maryland Governor O'Malley, in declaring the state's active participation in National Cyber Security Awareness Month said, "As a state and as a nation, we face unique security challenges. Maryland has a vital network of cyber security assets—from entrepreneurs who work to stop cyber-attacks by developing new and cutting edge technologies to educators who are training the next generation of cyber warriors. Together, working with our federal and local partners, we have an opportunity to create jobs and uphold our responsibility to protect and defend the nation's digital infrastructure."

In Georgia, "Governor Deal has proclaimed October as Cyber Security Awareness Month. It's part of a nationwide effort to share information about protecting business and personal data." Georgia has compiled and published a directory of computer security resources for home users and IT

professionals which can be found online at gta.georgia.gov/00/press/detail/0,2668,1070969_167558063_163659118,00.html.

In Texas, several colleges and universities have announced programs and events to enhance cyber security awareness in recognition of National Cyber Security Awareness Month. One good example is Texas State University, in San Marcos, where it is sponsoring a series of informational events, culminating in a "Cyber Security Awareness Day 2011 (October 26th)". Texas State University explains the importance of National Cyber Security Awareness Month as, "Our shared responsibility means each of us must do our part—whether it's using stronger security practices in our day-to-day online activities or helping raise community awareness, we can all contribute towards this common goal" (security.vpit.txstate.edu/training/csam_2011.html).

While it is a great idea to set aside an entire month to promote awareness of the cyber security threats that we all face, and to widely distribute information on methods and technology to secure our computers, this is a practice that needs to be implemented and practiced 12 months a year, not just in October.

What is Cyber Crime?

By Gordon Giles, Committee Member, Perth PC Users Group, Australia
August 2011 issue, AXESS, Magazine of the Perth PCUG
www.perthpcug.org.au
gorgil51 (at) perthpcug.org.au

Well, it covers a wide range of law breakers. The card skimming you may have seen on the news, identity theft, internet hacking, pirating software, internet fraud, illegal transfer of money and hacking are the main problems we all face as computer users.

No matter how small or big you are, it's at your door step. About 10 years ago it was said if you have a home computer and never put it on line (connect it to the internet) then you are safe and nothing bad can happen. That's no longer true. If you just look at the computer without connecting to the internet, you probably swap files with others and they may be on line. Your grandson comes over and asks you to put this new game on your computer, and that program could have all sorts of problems that your computer protection may or may not find on installation.

The types of problems are Key Loggers, Viruses, Spyware, Data Loggers, bad cookies, Data miners, password collectors, and that's just the ones I can remember. As for viruses, they can attack your computer in so many ways from the simple advert that wants you to pay for a program to remove the advert that company has placed on your desktop to the virus that can damage hard drives and motherboards.

Then we look at what we do ourselves to make ourselves vulnerable.

You go to the shop and the sales person places your card in the reader. Well if possible you should never allow another person to handle your card as card skimmers are so small and inconspicuous.

Most of us are cautious about this fact, but when you are standing there with your card in hand someone with a camera has snapped your card and watched you enter the pin number. Cover your hand when entering your pin number; make a few false movements so the person watching has no idea what keys you actually pushed. Don't hold your card out in plain view but keep it covered and when using at a scanner make sure it looks ok and nothing has been added.

When on the computer set up something like Paypal or B-pay for paying bills or purchasing on line.

Absolutely no legitimate company will ever ask you for your passwords via email.

Scams are a dime a dozen so don't even answer them. Keep well away because if it sounds too good to be true then it is just that, a scam. Some will offer you millions of dollars and all they need is your bank account numbers. Why not ask for something simple like my first born.

So keep up the watch for possible problems, use and keep up to date a virus checker, Firewall, Spyware Blocker and some sort of program that can clean your registry of unused extensions and entries.

Don't keep passwords on your computer but make a file and keep them on a thumb drive if needed. Change them, and never use the same password, and make them with alphabet and numbers as this may protect you against wild card hackers.

I am sorry to say no matter what sort of protection you use we are all vulnerable. If they wish entry then they will get in. Locks and chains only keep out the honest few.

Downloading Deceptions

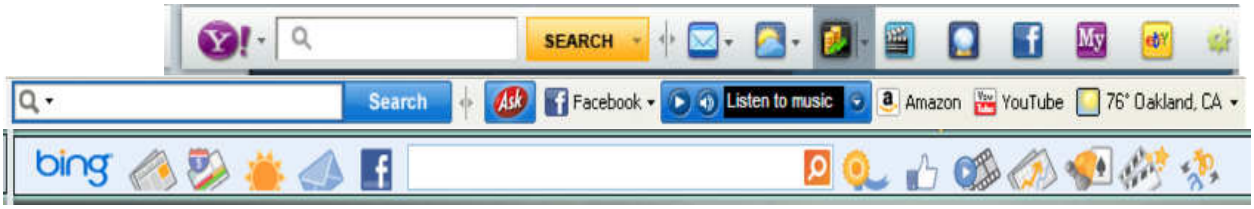
Written by Sandy Berger, Compu-KISS
www.compukiss.com
sandy (at) compukiss.com

Downloading programs from the Internet can be both fun and rewarding. There are, however, a few things that you have to be aware of when you grab any program from the Internet.

First, you should be sure that the program is from a reputable source. It may come from a recommendation from a friend, relative, or other trusted source. You may be following a recommendation from a columnist, like me, or a blogger who you know and trust. If you are at all unsure of the reliability of the program, you should research it thoroughly on the Internet before you download the program.

Once you have decided that the program you want is safe, there is one big "gotcha" that you should be aware of. Many programs that are themselves very safe and useful, make deals with other companies to promote their products in their download process. These offers are often integrated with the download so that unless you make changes during the download and install process, you will also get the add-on products, whether you want them or not.

These products are often toolbars like the Yahoo! Toolbar, the Ask Toolbar, and the Bing Toolbar. These are innocuous toolbars that allow you an easy way to use the Yahoo!, Ask, or Bing search engines from inside your browser. They can be useful or they can be aggravating, depending on your viewpoint.



If you have even looked up at the top of the screen while you browse the Web and wondered where all those new strips of icons came from, you have probably inadvertently downloaded them when you downloaded other programs.

Here's how it works. You download the new program. Then you install it. The installation consists of several screens. You press Next to get past each screen. At the end, you press Finish.

If you didn't read each screen, you may have just agreed to install these extra programs without even knowing it. In some cases, you have also agreed to let the program change your home screen (the one you see when you start your Web browser.)

Here's how it works. One of the installation screens will have one or more check boxes. Next to the checkboxes are the instructions. They read something like: "Install the Yahoo Toolbar" and/or "Make Yahoo my homepage". Here's the rub. The checkboxes are pre-filled with a checkmark indicating that you are choosing to let the program perform these tasks. If you don't want the program to install these extras, you have to click in each box to remove the checkmark and let the program know that you don't want to install these extra programs.

These little add-on programs often come along with free programs as the manufacturer is trying to get a little income from the piggy-back program's developer. Although not necessarily unethical, this is a bit of trickery on the part of the program developer. Yet everyone seems to be doing it, including well-known, reputable manufacturers. For instance Java, a program that you need to display Web pages properly is from a very stable company called Sun Microsystems. Yet when you download Java you will encounter pre-checked boxes to install the Yahoo! Toolbar.

Adobe, another reputable company, offers Adobe Reader, a program for displaying documents in the popular PDF format. They do something similar. When you go to their website to download the Adobe Reader program, there is a pre-checked box next to the download button that says, "Yes, install McAfee Security Scan Plus", a program that is supposed to make your computer more secure.

Although none of these programs contains a virus and none is particularly bad, the fact is that most of them start automatically when you start your computer or your Web browser. Feel free to let the programs install one or two if you would like to try them. Just remember that If you accumulate too many of them, they will slow down your computer and/or clutter your screen with unnecessary toolbars.

With that in mind, you should always read the download and installation pages when you install any program. Uncheck the boxes if you don't want to install the extra programs. In the words of the famous Sargent Esterhaus in Hill Street Blues, "Hey, let's be careful out there!"

Debunking Some Common Myths

Author: Mindi McDowell
National Cyber Alert System
Cyber Security Tip ST06-002
February 2011

There are some common myths that may influence your online security practices. Knowing the truth will allow you to make better decisions about how to protect yourself.

How are these myths established?
There is no one cause for these myths. They may have been formed because of a lack of information, an assumption, knowledge of a specific case that was then generalized, or some other source. As with any myth, they are passed from one individual to another, usually because they seem legitimate enough to be true.

Why is it important to know the truth?
While believing these myths may not present a direct threat, they may cause you to be more lax about your security habits. If you are not diligent about protecting yourself, you may be more likely to become a victim of an attack.

What are some common myths, and what is the truth behind them?
Myth: Anti-virus software and firewalls are 100% effective.

Truth: Anti-virus software and firewalls are important elements to protecting your information (see Understanding Anti-Virus Software and Understanding Firewalls for more information). However, neither of these elements are guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.

Myth: Once software is installed on your computer, you do not have to worry about it anymore.

Truth: Vendors may release updated versions of software to address problems or fix vulnerabilities (see Understanding Patches for more information). You should install the updates as soon as possible; some software even offers the option to obtain updates automatically. Making sure that you have the latest virus definitions for your anti-virus software is especially important.

Myth: There is nothing important on your machine, so you do not need to protect it.

Truth: Your opinion about what is important may differ from an attacker's opinion. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other people (see

Understanding Denial-of-Service Attacks and Understanding Hidden Threats: Rootkits and Botnets for more information).

Myth: Attackers only target people with money.

Truth: Anyone can become a victim of identity theft. Attackers look for the biggest reward for the least amount of effort, so they typically target databases that store information about many people. If your information happens to be in the database, it could be collected and used for malicious purposes. It is important to pay attention to your credit information so that you can minimize any potential damage (see Preventing and Responding to Identity Theft for more information).

Myth: When computers slow down, it means that they are old and should be replaced.

Truth: It is possible that running newer or larger software programs on an older computer could lead to slow performance, but you may just need to replace or upgrade a particular component (memory, operating system, CD or DVD drive, etc.). Another possibility is that there are other processes or programs running in the background. If your computer has suddenly become slower, it may be compromised by malware or spyware, or you may be experiencing a denial-of-service attack (see Recognizing and Avoiding Spyware and Understanding Denial-of-Service Attacks for more information).

Articles by Leo!

Articles you can re-use

Ask Leo! by Leo Notenboom

The Overlooked Risks of Staying Logged In

By Leo Notenboom on March 20, 2011
Article Source: http://articlesbyleo.com/

Have you ever checked your e-mail on a friend's computer, public computer, or even display model at the store, only to wonder later if that was a wise move? Is your information safe, or can someone use cookies to retrieve your log in information and access your account?

It depends on what webmail service you're using. But regardless, you may very well be at risk with any account that requires you to login.

There are three important questions that apply here:

- What does the website store in a cookie?
- How long does the website keep you logged in?
- Is the browser configured to remember passwords?

Each website determines what is and is not saved in cookies. It is possible for a site to use a cookie to save a password; however, this is poor security as anyone with access to the machine could access your account. Most commercial systems don't use this approach.

A password may be encrypted and only make sense to the service in question, but not decipherable to the user. Or, the cookie may use information to access the account that is not

related to your password, but related to data contained in the service's computer. Either way, it is unlikely a stranger can access your password through cookies saved on the computer.

The greater risk comes from the way most sites allow you to stay logged in for "a while" so that you don't have to re-enter your information each time you click through different pages on the site or temporarily browse to another site. Some servers, such as banks, keep that length of time short, others keep it fairly long. The result is the same – during that time anyone can walk up to the computer and access your account.

And the solution is very simple: always remember to sign out of your account so no one else can use it.

Finally, make sure you don't allow the browser to remember your password – typically an option you check when you sign in, or an optional feature of the browser or both. If you allow either, anyone with access to the machine can use a utility program to recover your password.

If you choose to log into your account on a public computer, or even that of a friend, understand you are taking a risk and extra caution is necessary. Make sure to log off completely when you are done, and never allow the browser to save your password.

Get more free tech help and advice from Leo Notenboom by visiting http://ask-leo.com With over 30 years of industry experience, including an 18 year career as a software engineer with Microsoft, Leo gives real answers to real questions from ordinary computer users at Ask Leo! Subscribe to Leo's newsletter at http://ask-leo.com/leos_answers_newsletter.html

TNO: Trust No One

By Mike Lyons, President, ORCOPUG (Orange County PC Users' Group), CA
www.orcopug.org
mike (at) orcopug.org

That's right. TNO means Trust No One. The stories abound: break-ins at Sony, Google, DOE Oakridge National Labs, etc. remind us that everyone can be vulnerable no matter how good you think your security is. Therefore, you need to protect yourself and realize that anything you put on the Internet is just one clever hack away from being available to others.

Take for example, Dropbox, a program we have demoed at one of our club meetings. It's a great program that lets you move data between devices using the cloud as a transfer medium and synching the files onto all of your devices (pcs, tablets, iPhones and smartphones, etc.) without having to be physically connected.

When you move data into your Dropbox directory, it gets encrypted before it is sent up to the cloud. Originally Dropbox said that they didn't have access to your data, but because they provide the encryption method, they have the keys and therefore can look at the data if they wanted to. In fact, they have stated they would turn over your data if subpoenaed—they would turn it over to authorities. Over time their terms of service has changed to reflect these changes.

Now most of us don't have anything to hide and think we don't need to encrypt our stuff. Encryption is only for the bad guys. But just imagine if someone could get hold of all your emails,

or all of your spreadsheets, etc. That's probably information that you probably don't want others to see. The only way you can truly be safe is to encrypt anything you send over or into the Internet. There are a variety of programs that will do this for you, for both email and data files being stored on the Internet.

The key is to control the whole process. You select the encryption tool and control the public and private keys. Two of the most popular encryption programs are True Crypt and PGP (Pretty Good Privacy). Now when you send your encrypted file to Dropbox, it will be double encrypted. And even if Dropbox removes their encryption, your data is still encrypted with your encryption, and is thus protected. TNO.

Secure Your Wireless Network - OR ELSE!

By Ira Wilsker
iwilsker (at) sbcglobal.com

WEBSITES:
http://news.yahoo.com/s/ap/20110424/ap_on_hi_te/us_wi_fi_warning
http://www.wi-fi.org/files/kc_25_Five Steps to Creating a Wireless Network.pdf
http://windowssecrets.com/comp/050526/#story1
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
http://news.cnet.com/8301-19518_3-20030160-238.html
http://www.wi-fi.org/knowledge_center/kc-fivestepsforcreatingwirelessnetwork

Many times in this column I have warned readers about the risks of having an unsecured wireless or "Wi-Fi" network. Similar warning have been written here about the risks of using Wi-Fi in hotels, airports, restaurants, and other quasi-public places where miscreants can intercept your wireless signal and gain access to what is on your computer. Some time ago I mentioned how a neighbor whose own broadband connection was out, surreptitiously used another neighbor's Wi-Fi without his consent or knowledge while waiting for repair.

The news media has been rife with stories about how bad guys and other crooks have broken into inadequately protected wireless networks and stolen information, committed identity theft, downloaded child pornography, planted malware and spyware on the computer, and committed other heinous acts, all made possible because the owner of the wireless network did not take proper precautions to harden his system from attack and intrusion. In a recent AP news story, "NY case underscores Wi-Fi privacy dangers" (April 24, 2011, by Carolyn Thompson), one Buffalo, NY resident learned the hard way. " Lying on his family room floor with assault weapons trained on him, shouts of "pedophile!" and "pornographer!" stinging like his fresh cuts and bruises, the Buffalo homeowner didn't need long to figure out the reason for the early morning wake-up call from a swarm of federal agents. That new wireless router. He'd gotten fed up trying to set a password. Someone must have used his Internet connection, he thought. "We know who you are! You downloaded thousands of images at 11:30 last night," the man's lawyer, Barry Covert, recounted the agents saying. They referred to a screen name, "Doldrum." ... Law enforcement officials say the case is a cautionary tale. Their advice: Password-protect your wireless router. ... Within three days, investigators determined the homeowner had been telling the truth: If someone was

downloading child pornography through his wireless signal, it wasn't him. About a week later, agents arrested a 25-year-old neighbor and charged him with distribution of child pornography."

The Buffalo case is far more common than people realize. In a recent Sarasota, FL, case, " (A Sarasota resident) ... got a similar visit from the FBI last year after someone on a boat docked in a marina outside his building used a potato chip can as an antenna to boost his wireless signal and download an astounding 10 million images of child porn."

These originally accused individuals might not have been guilty of a criminal act, but they were guilty of not properly securing their home wireless networks, thus unknowingly allowing others to use their broadband internet connections for illicit purposes. Virtually all wireless routers manufactured in the last several years have integral security features available, but many users do not implement these features because they feel that it is too complicated, or that the default settings are adequate. That type of blissful ignorance can lead to a lot of trouble, as reflected by the news story above. Older 802.11b wireless routers attempted to provide some security by implementing an encryption protocol called "WEP" (Wired Equivalent Privacy), which was promptly cracked, and readily available hacker utilities can breach WEP security keys in a matter of seconds, rendering the wireless network security null, and allowing unrestricted access to the home network. There was an interim upgraded protocol, Dynamic WEP, which changed the security key every few minutes, but the currently available hacker utilities can easily breach D-WEP in a matter of seconds. The introduction of the faster 802.11g, and the recent 802.11n standards provide much improved security. These newer standards incorporate a much improved Wi-Fi Protected Access 2 (WPA-2) encryption, which while not totally impervious to attack, does significantly harden a home wireless network, making unauthorized intrusion much more difficult. WPA-2 has been around since 2004, and became mandatory on all new standardized Wi-Fi routers in 2006. While WPA-2 encryption provides much improved security, the major flaw is that since it typically requires users to configure it, which many do not, many users leave the barn door open to attack.


Wi-Fi Alliance

Five Steps to Creating a Wireless Network

Can I set up a Wi-Fi network?
Setting up a wireless network is easier than you might think. Whether you are setting up a Wi-Fi network for your home, or for the office, you don't have to be a tech guru to handle the job. That is why the Wi-Fi Alliance has created this easy-to-follow, step-by-step plan to creating your own wireless network. Simply follow the five steps outlined below and you will be on your way to experiencing the freedom of Wi-Fi.

Five steps to setting up your Wi-Fi network:
- Step 1 — Planning
- Step 2 — Equipment Selection
- Step 3 — Set Up
- Step 4 — Adding Wi-Fi to Desktop Computers
- Step 5 — Security

The trade association representing the Wi-Fi manufacturers, the Wi-Fi Alliance, has published simple instruction on how to secure a wireless network at home or at work. These instructions are available online at www.wi-fi.org/knowledge_center/kc-fivestepsforcreatingwirelessnetwork, with a PDF file detailing the process available at www.wi-fi.org/files/kc_25_Five Steps to Creating a Wireless Network.pdf. The five steps listed by the Wi-Fi Alliance are: Planning, Equipment Selection, Set Up, Adding Wi-Fi to Desktop Computers, and Security. While an appropriate first step, many users do not really do any Wi-Fi planning, instead using the wireless router provided by their internet service provider, or purchased at a big-box store. Fortunately, most wireless routers available today, especially if they are Wi-Fi certified by the Wi-Fi Alliance, are capable of handling any reasonable networking needs; the "g" standard is adequate for normal household data needs, while the newer and faster "n" standard may be capable of the wireless distribution of TV grade video around the house. One common trap that many purchasers of wireless networks fall into, is that they over-buy, and purchase a Wi-Fi router that is much faster than anything that may be in their home in the foreseeable future; 802.11g has a theoretical maximum raw speed of 54 Mbit/s (really about 19 Mbit/s net throughput), and 802.11n

has a theoretical maximum raw speed of 600 Mbit/s (actual throughput is much lower). If used primarily to wirelessly link computers to the internet, the "weakest link in the chain" is often the internet connection itself, which is typically far below the speed capability of the Wi-Fi, thus wasting a lot of potential capacity. Now that video streaming from the likes of Netflix is becoming more common, and HD TV and DVDs can be wirelessly streamed around the house, the faster 802.11n may be appropriate.

It is imperative that whatever Wi-Fi equipment is provided or purchased, that the security features provided by the manufacturer are properly implemented. While each maker may have a different procedure to follow in setting up the security of its products, the basics are fairly similar. One of the most important features to implement is the data encryption, which will make your signal unintelligible by unauthorized users. The newer wireless routers offer WPA-2 encryption, which may require a "key" or phrase to decrypt; do not use anything simple like your name, address. or birth date, as they may be easily guessed by a hacker; instead use a random alpha-numeric key (random letters and numbers) to create a key that will be difficult for others to guess. Almost all wireless routers require a password for access, and by default incorporate a default password. Immediately, change your default password to something that others could not likely guess, such as another random alpha-numeric sequence. Users should be aware that if they do not change the default password to their wireless routers, they may be easy to crack, as many makers use the word "default" as the default password, and there are online directories of default passwords sorted by manufacturer. Since it is often easy to remotely determine the brand and model number of a wireless router, and many users never change the factory default, the network is prone to intrusion. With a complex password, unauthorized users will not likely be able to access or modify your settings.

Almost all wireless routers transmit a SSID, or Service Set Identifier, such that it is easy for other wireless devices to locate the network. According to the Wi-Fi Alliance, "All access points ship with a wireless beacon signal so that wireless PCs can more easily find them. In effect, the signal is shouting, I'm here! Log on!" By turning of the SSID, the network is effectively closed to outsiders, as it becomes somewhat invisible to them.

By default, most wireless routers or access points have a default network name, typically the manufacturer's name and model number, making the network vulnerable in several ways. If possible, change the network name to something that cannot be readily tracked back to you; do not use your name, street address, company name, or other personally identifiable name, but instead use a pseudonym or random alpha-numeric name.

The location of the wireless router in the home or business will have a significant effect on the ability of others on the outside to intercept your radio signal. If the wireless network is intended for use within the house, then locate the wireless router or access point away from windows and open doors; the more hard material between the router and the data thief, the less likely it is for him to intercept your signal.

Many better wireless routers and access points offer a "MAC (Medium Access Control) Control Table", where the unique MAC address of each authorized computer or device can be included in an Access Control List (ACL). By implementing this feature, only the devices with the listed MAC addresses can access your network, and unauthorized computers and devices not included in the ACL list will be blocked from access; this is an effective way of restricting unauthorized access to your network.

There may be some other security features offered by some manufacturers, but these are the most common, and often offer substantial compatibility among the different hardware types likely encountered. Implement as a rule that whatever security features are offered by your hardware that they should be fully implemented to the level of maximum protection. Failure to do so may result in unauthorized access to your network; and the FBI may be knocking on your door too.

Ira Wilsker is a member of the Golden Triangle PC Club as well as Director of the Management Development Program at Lamar Institute of Technology, in Beaumont, TX. He also hosts a weekly radio talk show on computer topics on KLVI News Talk AM560, and writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a police officer who specializes in cybercrime, and has lectured internationally in computer crime and security.

Is Identity Theft in Your Future?

By Barney Babin, a CCCC (Cajun Clickers Computer Club) member and instructor for XP, Vista & Win 7 Workshops
August 2011 issue, Cajun Clickers Computer News
www.clickers.org
ccnewsletter (at) cox.net

Now that hackers are running rampant not only attempting to access your computer, but your accounts via commercial entities, what is a person going to have to do the assure themselves that their credit is still in good standing?

First of all, what is identity theft? According the Federal Trade Commission (FTC), “Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.”

The FTC estimates that as many as 10 million Americans have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft.

The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector. If your credit card or Social Security card is stolen, simply asking the Social Security Administration or credit card companies to assign you new numbers will not solve your problem.

While on vacation in June, one of my online email accounts was hacked on a wired, not wireless, access point in my hotel room. I immediately performed some of the steps below and have had no repercussions. First, immediately change all passwords on compromised internet accounts, email accounts, etc. – and be sure that they are “strong” passwords, which can be verified at Microsoft, among others, at www.microsoft.com/security/pc-security/passwordchecker.aspx

Next, contact the fraud departments of each of the three major credit bureaus listed below and report your stolen identity. Ask that a "fraud alert" be placed on your file and that no new credit be granted without your approval.

Equifax
Report fraud: 1-800-525-6285
Order credit report: 1-800-685-1111
Website: www.equifax.com/

Experian
Report fraud: 1-888-397-3742
Order credit report: 1-888-397-3742
Website: www.experian.com/

TransUnion
Report fraud: 1-800-680-7289
Order credit report: 1-800-916-8800
Website: www.tuc.com/

Next, if any accounts have been fraudulently accessed or opened, contact the security departments of the appropriate creditors or financial institutions and close these accounts.

Finally, file a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank or the credit card company requires proof of the crime later on. Also contact the fraud hotlines of the Social Security Administration at 800-269-0271 or www.ssa.gov/oig/guidelin.htm and of the Federal Trade Commission at 877-382-4357 or www.ftc.gov/idtheft or which includes a video that includes a cornucopia of useful information: www.ftc.gov/bcp/edu/microsites/idtheft/video/avoididentity-theft-video.html

You should get a free annual credit check from the three bureaus above by logging onto the website www.AnnualCreditReport.com/, which requires your social security number. Do not get the report from all three at once, but stagger the three reports out over a one year interval as assurance that all is well throughout the year. This report will not have the credit score, but there is now a new website that will obtain this information for you free from Experian, www.quizzle.com/, -- and you do not have to give your social security number. You establish an account, give the information requested, answer some questions to verify information from Experian, and when you have answered the questions correctly, both the credit report and the credit score is given to you. Of course, they will try to sell you ways to increase your score, protect your identity, etc. but you are not obligated to do this.

We may not be able to stop all hacks, but, as you can see, there are ways to lessen the impact. The responsibility falls upon us to initiate these actions.

Internet -- Small Scams that Trick You

Written by Sandy Berger, Compu-KISS
www.compukiss.com
sandy (at) compukiss.com

I recently wrote about how companies who offer free software try to trick you into downloading extra programs. They do this during the download and/or installation process by having a pre-checked box indicating that the extra software will be included. Unless you uncheck the box, you get the extra programs along with the program that you requested. This is not illegal since you have, although often inadvertently, agreed to the download. It is not really a scam, but it is a form of trickery that is prevalent on the Web.

Free programs are notorious for this type of trickery as they try to offer something for free while still finding a way to make money. Another way they do this is by offering their free program, but encouraging you to purchase an upgraded version of that program instead of the free version. There is no problem with that. I have used several free programs and gone back to purchase the upgraded version to get more functionality or because I really like the free program. The problem comes when the company tries to trick you into purchasing the paid version.

Sometimes at websites like this, while there are numerous offers on every page for the paid version, the free program is very difficult to find. At other times you are given a list of features with columns comparing the paid version to the free version. Of course, the paid version has many more features and they almost always offer you a 30-day free trial, after which they will charge your credit card.

Again, there is nothing wrong with this, as long they make your choices clear. The problem arises when they try to trick you into downloading the paid version. Often, the download button for the paid version is very obvious while the download button for the free version is so small that it is almost non-existent. Even worse, is when the line is blurred between which download button is for which version. There may also be numerous pop-ups that lead you to the paid version.

These tactics, however, are a minor when compared to form of trickery that is really used to bamboozle you. One example of this is a pop up that appears on your computer informing you that your computer is infected with a virus and you need to click a button to get rid of the virus. In many cases, this is completely bogus. Your computer is not infected, but if you click on their button it will be. Then the pop ups will offer to get rid of the infection, if you pay a fee. Sometimes the pop ups look like they are from a legitimate antivirus company like Symantec or McAfee. They can be very realistic, so you have to be aware of which antivirus program you are currently using and what its real alerts look like. Once you have clicked on the button of the bogus antivirus promotion, it is usually too late to rethink what you are doing. So don't be trigger happy. If you think you are being approached with an antivirus scam, just close the window. If the window won't close, turn off the computer. Swindles like this are both illegal and upsetting for the computer user. On top of that, falling for a scam like this can cost lots of time and money.

There are many different cons of this type and there are several others that are equally disturbing. One is a company that tries to deceive you into moving your domain name registration to them.

The one that I've seen over and over again is by a company called "Domain Registry of America." You don't have to worry about this if you don't have a website of your own, but if you do, you should be aware of the deceitful form of trickery that they are using. A domain name is the name of your website. For instance, my website is compukiss.com. The Pilot's website is thepilot.com. When you register a website, the name and address of the domain name holder and the date when it will expire become public record. The Domain Registry of America uses this information to send a "Domain Name Expiration Notice" to the registered user. They make it look like a bill and they indicate that if you do not pay the requested fee to them by as certain date your domain name will expire. Read the fine print and it says that "now is the time to transfer and renew your name from your current Registrar to the Domain Registry of America." So by filling out their form and sending them the requested amount, you are not simply renewing your domain name, you are also transferring it to them. Of course, their fee is higher than most and you will be paying them this fee for as long as you keep the domain name, unless you transfer it away from them. If you call the Domain Registry of America, you will find that they refer to the letter you received as an offer rather than a bill. They are right, but it is still extremely deceiving.

I guess there is no doubt that as long as humans are the flawed creatures that we, there will be trickery and deceit. More and more of it is found on the Internet and in Internet-related every day. So be careful out there!

Articles by Leo!

Articles you can re-use

Ask Leo! by Leo Notenboom

How Do I Keep People From Finding Me on the Internet?

By Leo Notenboom on March 20, 2011
Article Source: http://articlesbyleo.com/

Do you wish you could erase yourself from the internet? In other words, do you want to stop your name and information from showing up when people Google or search for you on the internet? Sadly, you're not alone.

Not only is this disappointingly complex to do, ultimately… you can't.

What it boils down to is understanding how little control you have, what steps you can try, and how effective they may or may not be.

But first, you should know that prevention is the only real cure.

But even then it's not at all complete.

You need to assume that everything you place on the internet will remain there forever, and will be viewed in the worst light possible. To clarify, it may not be there forever, and may not be viewed in the worst light possible, but that's the safest way to look at how what you say, do and post in public might be used. You do have control over some of what goes up on the web before it goes up, so exercise caution.

Still feel like posting those party photos?

How about the example we hear about all the time: someone losing a job or job offer because they spoke their mind in a public post, posted unflattering photos of themselves, or otherwise made public information about themselves that they never should have. Information that their employer or potential employer eventually found.

It happens all the time.

It happens to those who have the freedom of speech mentality: “I should be able to post and say and do whatever I want.”

Absolutely. You should be able to. Go ahead. Post and say what you like. In most countries you have the right to say pretty much whatever you like. Just remember that freedom of speech does not mean freedom from consequences.

Because chances are you’re not going to get it removed from the internet once the day comes that you decide maybe it shouldn’t be there.

Even preventing what you do and post may not be enough. What about other sources of information that relate to you?

You cannot control what others say or post about you. (Within the legal limits of harassment, libel and slander, of course, and even then within the limits of your own legal or justice system and your resources.) Been mentioned in a newspaper? Listed in publicly records? Do you participate in discussion groups that are visible and/or archived publicly?

All of these are ways you can show up online. And there are plenty more.

And more than likely, all are places from which you probably can’t remove yourself.

Still want to try? Here’s what you can do:

Your first thought may be to try to get in touch with the search engine, but here’s the fundamental problem: the search engine has nothing to do with it. Even though people may use the search engine to find the information, that information is not in the search engine itself. It’s on one of the thousands of other sites on the internet, and the search engine is merely in charge of finding it. The only way to truly remove yourself is to find each of those sites and ask them to remove the information that pertains to you.

It’s common to want to have Google remove you from their index. There are two problems:

1. They won’t. Google is a search engine, and their “job” is to report what can be found on other sites on the internet. They’re simply showing you what’s out there, but what’s out there is not in their control.
2. Google is not the only game in town. Google is perhaps the most popular, but there are literally thousands of search engines on the internet. From Bing to Yahoo, to many medium and smaller niche search engines, there are more search engines than you could ever count. Even if you could get Google to remove you from their results, which you cannot, you’d still be faced with all those other search engines that might also be returning the same results that show your information on the internet.

Look out for a growing service area called “reputation management”. These services will promise to remove you from the search results. They can’t. If they tell you that they can, they’re wrong. The information cannot be removed. The best that they can hope to accomplish is to push whatever it is you want to hide further down the results list when people use common search terms for you. At best it’s simply somewhat harder to find… which may, or may not, be valuable to you.

It would be nice to think that you have control over the information that is placed on sites and services that you control on the web. But you don’t. This is another way that this issue gets so complicated.

You might think that if you wanted to remove something about yourself that’s been posted on your own website, all you need to do is exactly that – remove it. Problem solved.

Not so fast.

The “problem” is that there are other sites that take copies of the pages on your site and preserve them as a kind of historical record. Archive.org is a good example, but in fact there could once again be any number of sites archiving or duplicating information- and many of them are doing it illegally. You can certainly remove the information from your site, but you have no control over what these other sites do with the information that they’ve already captured and made publicly accessible.

So what can you do?

- Well, you can use the search engines yourself to see where all the information about you is, and then contact all of those sites (not the search engines) and ask them to remove it.
- You can use a reputation management service to try and “bury” your information, making it harder, but not impossible to find. If that’s enough for you.

And that’s about it. Once something is on the internet, you can pretty much plan on it being there for good.

In fact, it might be easier to change you: move, change your name, change all of your identifying information, and then make sure that as little of that new you as possible gets on the internet.

But even then, you’ll probably show up somewhere.

Get more free tech help and advice from Leo Notenboom by visiting http://ask-leo.com With over 30 years of industry experience, including an 18 year career as a software engineer with Microsoft, Leo gives real answers to real questions from ordinary computer users at Ask Leo! Subscribe to Leo’s newsletter at http://ask-leo.com/leos_answers_newsletter.html

Sauk Computer User Group

Using Task Manager to Get Out of Potential Harmful Situations

By Terry MacLennan, Member at Large, Sauk Computer Users Group, IL
October 2011 issue, The Computer Connection
www.saukcomputerusergroup.org
wcseniorcenter (at) gmail.com

There is an easy method of getting your computer out of two situations of potential harm. To do this, we will use the operating system's built-in program called the Task Manager.

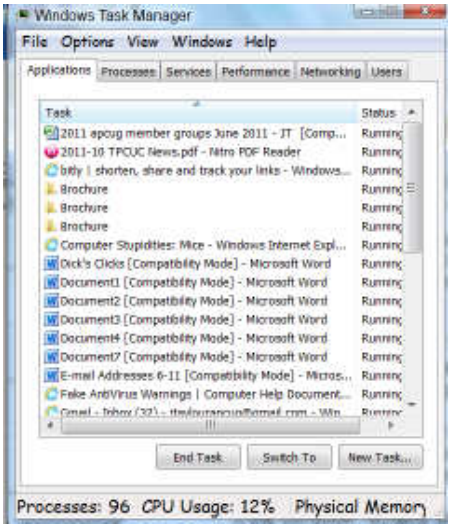
The first situation is when you have too many programs running at one time and the computer locks up. This lockup can also be caused by a single program that for one Reason or another, fails to run properly. Reaching over and hitting the power button may seem to be your only option but there is a much better choice.

The second situation occurs when you are on a webpage and one of those realistic looking but totally phony "security alerts" pops up on your monitor screen warning you of imminent danger of viruses and other malware that "it" has detected on your computer. These scare popups trick many naive people into clicking on them only to find out that now their computer truly is infected and control has been lost. You are totally helpless when you have clicked on one of these so-called "security" scam programs.

You absolutely must not click anywhere on these pop-ups including buttons that say something to the effect of "No Thanks," "Decline" or even "Continue Unprotected." But, instead of clicking one of those, you may decide, almost instinctively, to click the "X" in the corner of the pop-up box. Doing *any* of these actions is almost like turning your house alarm off, opening the door and saying "come on in" to the masked bandit standing outside. Paying the "bandits" for their "security program" which is holding your computer hostage is an extremely poor choice. Do you really want to pay the thieves with your credit card and its number?

But you are now stuck in a situation where you may try to click off the web page by clicking on its "X" in the upper right hand corner. But you soon find out that that won't work as you first need to close the window (the pop-up in this case) that is on top.

Hard shutting down the computer by using the power button may seem to be your only option but again there is a better alternative.



Your best friend in both situations is the Task Manager. To open this built-in program, press and hold the CTRL and ALT keys with your left hand, then tap the DEL key with your right hand.

In Win XP, this will automatically open the Task Manager while with Windows 7 it will take you to a page with a list of options. Click the bottom option and it will open the Task Manager which looks nearly identical to the XP one. From here, everything is the same for both systems.

Along the top edge of the Task Manager is a row of tabs. Click the *Applications* tab, if it doesn't happen to automatically be on that tab. When you have opened it up, you will see a listing of all the programs and web pages that are running.

If your computer is locked up, look for any programs that are "Not responding." Click the program one time to highlight it then click on End Task at the bottom. This should close the nonresponsive program and free your computer.

If the computer remains locked up, use the same method to close all of the remaining Programs that are running then shut down as you would normally. Everything should be back to normal when you reboot the computer.

A hard shutdown with the power button is absolutely the last resort as this could potentially damage files.

To close a web page with the dangerous fake security warning pop-ups, use the same method by highlighting the web page in the list then clicking End Task. This will safely shut down the web page with its pop-up without installing the malware "security program."

Malware, Viruses, Trojans Defined

By Ira Wilsker
iwilsker (at) sbcglobal.com

WEBSITES:
http://en.wikipedia.org/wiki/Malware
http://www.ilovefreesoftware.com/08/featured/definiton-of-various-security-related-terms.html
http://lifehacker.com/5560443/whats-the-difference-between-viruses-trojans-worms-and-other-malware
http://en.wikipedia.org/wiki/Computer_virus
http://en.wikipedia.org/wiki/Computer_worm
http://en.wikipedia.org/wiki/Trojan_horse_(computing)
http://en.wikipedia.org/wiki/Rootkit
http://en.wikipedia.org/wiki/Backdoor_(computing)
http://en.wikipedia.org/wiki/Rogue_antivirus
http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/12_december_2010_threat_roundup__010711_.pdf

In the past week, I was called upon four more times to clean malware off of infected computers. One user had a major name brand antivirus program installed, running, and updated and could not understand how the malware had penetrated his antivirus software and contaminated his computer. He had purchased the antivirus software last fall from a big box electronics store based on the recommendations of a salesperson. He had been told that this particular brand of security software was the best as it was their top seller, and that antivirus software was all that he really needed. Based on that recommendation he plopped his hard earned money on the counter, went home, installed it, updated it, and blissfully surfed the internet, opened email attachments, downloaded software and music, and had just a jolly good time online until his computer gradually slowed to a crawl, and friends informed him that they were receiving spam emails from him. This user was perplexed, as his antivirus software was running, and indicated that it was updating several times a day. He just could not understand how 90 different malware programs had infected his computer. His problem started when he purchased inadequate security software; while the product he bought was excellent at protecting his computer from viruses, and some Trojans and spyware, it did not offer the all-inclusive protection of the comprehensive security suite offered by that publisher (and others as well) that would have only cost him a few dollars more.

There is a common misconception in user circles that viruses are the primary computing threat, as users have had heard about viruses for several years. Today, viruses are present, but a relatively minor threat in terms of prevalence. I did a quick analysis of the most common new threats recently listed by TrendMicro, and found that viruses only made up 4% of the new significant threats to our computing security. On the other end of the spectrum, Trojans made up 42% of the commonly seen new threats, worms were at 14%, backdoors at 14%, web based threats were at 6%, java script malware was at 6%, 4% were hacking utilities, 2% adware, and about 8% other threats. It is obvious that protective software that protects the computer primarily from viruses is failing to protect the user from the majority of contemporary threats; it is precisely this fact that led to this user's infected computer, despite his premium quality antivirus software. A lot of users have a misconception about the common threats in circulation, believing that they are generically all viruses, but, as I saw in this case, this blissful ignorance may lead to a computing nightmare.

While not necessary to use a computer, it would likely be beneficial for computer users to be aware of the different threat groups that can impact our computing. According to Wikipedia, "A computer virus is a computer program that can copy itself and infect a computer." Many viruses attach themselves to legitimate programs or data files on the infected computer. The fact that a computer virus can copy itself to infect other computers is what makes it different from other types of malware, for which viruses are commonly confused. Viruses can be spread through digital media (USB drives, CD or DVD discs, and floppy discs) or through network connections that the virus can use to copy itself to other attached computers. Once a virus has infected a computer it may perform a variety of tasks as programmed by its author. Viruses may damage the data on a hard drive or degrade the performance of the computer. Some of the viruses are stealthy and their effect may not be noticeable by the user, as the viruses do their damage in the background. Some viruses are functionally benign, other than they reproduce themselves countless times on the infected hard drive, until they consume all of the free space on the hard drive.

Computer worms are a malicious computer program that wriggles through computer networks sending copies of itself to other computers attached to the network. Most worms are free standing programs, and are commonly programmed to spread themselves through the network without any action by the user. Most worms have an explicit nefarious function such as deleting files on the infected computer, or encrypting critical files, only releasing them after an extortion payment is made to the cybercriminal. Some worms open a backdoor into the computer that will enable the creator of the worm to take remote control of the computer, converting the computer into a "zombie" under his control, which can be used to generate revenue for the originator of the worm by sending spam mail from the infected computer, with the spam fees collected going to the author of the worm. Some worms are used to create a zombie network of computers, also called a "botnet", where the compromised computers can be used to launch directed cyber-attacks on other computers or networks, in an act of cyber terrorism.

For those who are aware of the epic "Helen of Troy" of Greek mythology, the term "Trojan Horse" means an object looks like it serves one purpose, but really has an unobvious, usually nefarious, purpose. Cisco, the networking company, describes a Trojan as, "It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems". In cyber speak, a Trojan Horse, typically shortened to the simple moniker "Trojan" is a program that appears to have a useful function, but after being installed by the user, the Trojan may be used to perform other undesirable functions. Some Trojans are money makers for their authors because they place paid (and usually unwanted) pop up advertisements (Adware) on the infected computer, redirect web searches, or shift online purchases to a seller not of the buyer's choice without his knowledge. Some Trojans are keyloggers, which are commonly used for identity theft, or to give

unauthorized users access to a computer system. Trojans are often spread through intentionally downloaded software, surreptitiously bundled with another often legitimate program, from email attachments, and purloined websites with executable contact (ActiveX is sometimes used for this). Some Trojans can be installed on the target computer by way of code written in Java, or a Java script, that when executed, implants the harmful content on the victim computer.

One of the more recent and costly types of malware to attack our computers is generically referred to as "Rogue Antivirus Software", which is usually implanted on the victim's computer by a Trojan. There are thousands of these rogue programs in current circulation, infecting millions of computers at any given time. Rogue antivirus is sometimes installed by the user using "social engineering" tactics, which tricks the user into clicking on something that installs the rogue software. Some of the common lures to ensnare the user into loading rogue software on the computer are offers for free screen savers, toolbars, utilities to play specific video formats (often attached to an email), sham online security scanners, contaminated PDF files, insecure web browsers, and other vectors. The common thread of this rogue software is an authentic looking popup that informs the user that his computer is (falsely) infected with hundreds of viruses and Trojans, and for a fee it will clean the computer. These popups which will not permanently close will typically hijack the computer, destroy the installed legitimate security software, prevent access to online services that can kill it, prevent cleaning utilities from executing, and otherwise take control of the computer until the user pays a fee, typically $30 to $70. This fee is to be paid by credit card or other online payment service to a website that looks legitimate, but is really a complete scam. Not just will the rogue software not clean the computer of the pseudo infections after the fee is paid, but now a cybercriminal, often in Russia, has the user's credit card information. it is not uncommon for that same credit card information to promptly be sold on illicit websites, and to have substantial unauthorized charges appear on the compromised credit card account.

While there are many other cyber threats out there, those listed above are among the most commonly encountered by users. The traditional antivirus software will protect from some of the threats listed, but not all of them; this enhanced security capability is in the purview of the comprehensive security suite, or a combination of different types of individual security utilities, and not the free standing antivirus program. this is explicitly why I currently recommend a high quality integrated security suite, rather than an antivirus program. There are several good commercial security suites available, as well as a few free security suites. Just be aware that antivirus software by itself is inadequate to protect against today's contemporary cyber security threats.

Ira Wilsker is a member of the Golden Triangle PC Club as well as Director of the Management Development Program at Lamar Institute of Technology, in Beaumont, TX. He also hosts a weekly radio talk show on computer topics on KLVI News Talk AM560, and writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a police officer who specializes in cybercrime, and has lectured internationally in computer crime and security.

Using Caution with USB Drives

Author: Mindi McDowell
National Cyber Alert System
Cyber Security Tip ST08-001
April 2011

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks.

What security risks are associated with USB drives?
Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

One option is for attackers to use your USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware, that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on their computers.

Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive. Victims may not even realize that their computers were attacked.

The most obvious security risk for USB drives, though, is that they are easily lost or stolen (see Protecting Portable Devices: Physical Security for more information). If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

How can you protect your data?
There are steps you can take to protect the data on your USB drive and on any computer that you might plug the drive into:

- Take advantage of security features - Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost (see Protecting Portable Devices: Data Security for more information).

- Keep personal and business USB drives separate - Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.

- Use and maintain security software, and keep all software up to date - Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions current (see Understanding Firewalls, Understanding Anti-Virus Software, and Recognizing and Avoiding Spyware for more information). Also, keep the software on your computer up to date by applying any necessary patches (see Understanding Patches for more information).

- Do not plug an unknown USB drive into your computer - If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into your computer to view the contents or to try to identify the owner.

- Disable Autorun - The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically. In How to disable the Autorun functionality in Windows, Microsoft has provided a wizard to disable Autorun. In the "More Information" section, look for the Microsoft® Fix it icon under the heading "How to disable or enable all Autorun features in Windows 7 and other operating systems."

Articles by Leo!
Articles you can re-use

What does “firewall” mean?
By Leo Notenboom, June 5, 2011
Article Source: http://articlesbyleo.com/

The bottom line is that a large class of viruses and other types of malware can be prevented simply by using a good firewall.

What’s a firewall? Well, in your car it’s the “wall” of metal behind the dashboard that sits between you and the engine. Its purpose is to prevent engine fires from roasting you and your passengers.

A firewall for your computer is much the same – its purpose is to keep you from getting burned.

A firewall is at its core very simple: it blocks or filters certain types of network traffic from reaching your computer.

What do I mean by “certain types”? There’s network traffic you do want to reach your computer: like the pages of web sites you visit or the software you might download. And then there’s other traffic you might not want like malicious people or computers trying to access your computer remotely or viruses and worms trying to infect your machine.

A firewall knows the difference. It lets the good stuff in and keeps the bad stuff out.

Firewalls can also usually be configured; they can allow you to say “this kind of connection from the outside is OK”. A good example is remote desktop. A firewall may by default block any attempt to connect via remote desktop. But you can also configure the firewall to allow that type of connection to come through. Doing so you would be able to access your computer from another computer, be it across the room or across the internet. But even though you’ve allowed one type of traffic – remote desktop – other types of traffic like certain types of viruses are still blocked.

Some firewalls will also monitor outgoing traffic for suspicious behavior.

One characteristic of many viruses is that once you're infected they attempt to establish connections to other computers in order to spread. Many software firewalls will detect and either warn you or simply prevent those attempts.

And that leads to a very important distinction. There are two types of firewalls: hardware and software.

- A hardware firewall is just that – a separate box that sits between you and the internet that performs the filtering function. Traffic that is filtered out never even reaches your computer. Even the least expensive broadband router can perform the function of a firewall quite nicely. The downside for a hardware device is that most will not filter outgoing traffic.

- A software firewall is a program that runs on your computer. It operates at the very lowest level, as close to the network interface as possible, and monitors all your network traffic. While all network traffic still reaches your machine, the firewall prevents malicious traffic from getting past it and on to the operating system. The firewall prevents your system from actually noticing or doing anything with malicious traffic.

The good news is that all versions of Windows after XP have a software firewall built in, and all versions after Windows XP SP2 have it turned on by default. In fact, the security center will take steps – perhaps even annoying you in the process – to ensure that the firewall is either turned on or that you're aware of the risks in not having it turned on.

The bad news is that a firewall can't protect you from everything. A firewall is focused on protecting you from threats that arrive via malicious connection attempts over the internet. A firewall will not protect you from things you invite onto your machine yourself such as email, attachments, software downloads and removable hard drives.

But even so, protecting from those network threats is important.

In general, I recommend a hardware firewall such as a broadband router and leaving the Windows firewall turned off. However, regardless of your approach, be it a router, be it the Windows firewall, or be it some other software or hardware solution, some kind of firewall is always a necessary part of keeping your computer safe when connected to the internet.

Get more free tech help and advice from Leo Notenboom by visiting http://ask-leo.com With over 30 years of industry experience, including an 18 year career as a software engineer with Microsoft, Leo gives real answers to real questions from ordinary computer users at Ask Leo! Subscribe to Leo's newsletter at http://ask-leo.com/leos_answers_newsletter.html

Social Networking Tips from avast!

1. Use strong passwords and use a unique password for each service. Strong passwords should include a mix of lower- and upper-case letters, numbers and symbols.

2. Keep your antivirus software up-to-date.

3. Install software updates in a timely manner, particularly updates that effect your web browsers or any software that regularly connects to the Internet.

4. Manage your privacy on each social network very carefully. Check the default privacy settings on Facebook, MySpace, and Google+ and set them to your comfort level. Only share what you are comfortable sharing.

5. Avoid suspicious third-party applications. Some third-party apps are trusted and secure, make sure you know which ones fall into that category.

Information is taken from a free seminar on “Protecting Yourself and Your Identity” by Bob Gostischa, avast! Contact Bob at bob3160@gmail.com to book the presentation for your UG.