VOLUME 31, NUMBER 4

SEPTEMBER 2010,
ISSUE #328

TOGGLE

The Microcomputer Turn (On)

MONTHLY NEWSLETTER FOR TACOMA-SEATTLE AREA MICROCOMPUTER USERS

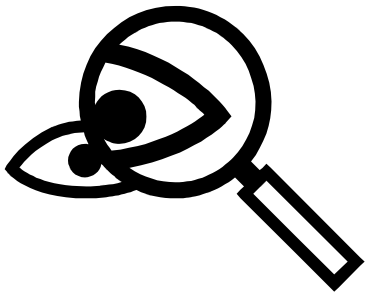
IN THIS ISSUE

Contents

Library News

- Librarian Tom Stepanek has released a new edition of his "Best of the Web". It is available at the club meeting for $2. Or, contact Tom and it can be mailed to you.
- More news ……... 12

UPDATE



Guest Editor and Security Issue

Spyware, Ransomware, Rogue Anti-Virus and Rogue Anti-Spyware

What Is the Malware World Coming To?

By Carl Tenning

Guest Editor

Imagine if the authors of such stuff put all that effort into making a better world of computing, how much we'd all benefit. Apparently, however, there's profit to be had in such stuff. So, we all have to protect ourselves. This issue, then, is devoted to what we need to do for our own protection. Here are some references on the subject giving lists of applications to avoid:

Rogue/Suspect Anti-Spyware Products & Web Sites
http://www.spywarewarrior.com/rogue_anti-spyware.htm

From Wikipedia, Rogue security software (a listing of rogues)
http://en.wikipedia.org/wiki/Rogue_security_software

ZD Net **Top 10 Rogue Anti-spyware**
http://www.zdnet.com/blog/spyware/top-10-rogue-anti-spyware/727

Guest Editor Issue

by Carl Tenning

TOG President, 2005-2010

One Problem of Exposing Malware

by Carl Tenning

Tacoma Open Group For Microcomputers

One problem in discussing or exposing malware is the threat of litigation. After I had purchased a supposed anti-spyware application, it looked like a scam to me. When I threatened to expose the ruse, I was threatened with a lawsuit. I had originally intended to publish it in TOGGLE, but withdrew it as a result of the threat of "being sued into the stone age". So, as a result of that unfortunate experience, I am keenly aware of any published reports on the subject. Suzi Turner reports on the subject on ZD Net and recommends to watch out for PestTrap. The top 10 rogue anti-spyware products and sites were published by ZD Net at: http://blogs.zdnet.com/Spyware/?p=727&tag=nl.e589

Now, fortunately, the Federal Trade Commission is taking action.

More suspected rogue spyware products are listed at : http://www.spywarewarrior.com/rogue_anti-spyware.htm

Notice: This newsletter is provided on behalf of subscribers and membership of Tacoma Open Group for Microcomputers who paid for this publication. If your label shows that it is a Complementary Copy, you are encouraged to join us in promoting computer use. See Application Form, page 11.

COMPUTER SECURITY

Stay Safe Online - 7 + 1

Steps to Internet Safety and Security For Your PC

By Leo Notenboom

Internet safety seems like an oxymoron these days with all the threats aimed at our computers. Staying safe online doesn't have to be difficult, and this article covers the basic steps that every computer user should take.

The phrase "Internet Safety" often seems like an oxymoron. Every day we hear of new threats aimed at our internet connected personal computers which seems to just make it that much harder to actually stay safe while connected online.

Knowing how to stay safe online has become a practical requirement these days for anyone using a computer connected to the 'net. Fortunately, a few relatively simply steps and a little education can go a long way to making sure that your internet experience is both safe and secure.

1. Use a Firewall - If you do nothing else, you must use a firewall. Firewalls act as a type of barrier between your computer and the internet, preventing remote computers from connecting to yours unless you explicitly allow it. A firewall can be a simple device such as a broadband router, it could be a feature of your operating system such as Window's own built-in firewall, or it can be a full featured software package that you purchase and install on each computer. Which one you choose is less important than making sure you have one and that it is enabled and deflecting threats.

2. Back Up - Failing to back up your computer, or at least your critical data, is perhaps the most common mistake I see being made today. And sadly it can also be the most costly regret you'll have when, not if, disaster strikes. If malware hits or hardware fails often your best if not your only resort will be to recover your system from its most recent backup. Don't have one? Then you might be severely out of luck. I regularly hear from people who've lost *all* of their data due to a malware infestation or a hardware failure. If nothing else, invest in a large external USB drive and a good backup utility and start backing up regularly right away.

3. Keep Critical Software Updated - Every day people experience problems that could have been completely avoided had they simply kept their operating system and other PC software up to date. Both Windows XP and Vista make staying up to date very easy with "Automatic Updates" and I definitely recommend that it be turned on. Similarly, most other software and applications will now also check for updates and notify you as new ones are available. Make sure your system and applications are checking for updates regularly and installing them as automatically as possible.

4. Educate Yourself - No matter what else you do, no matter what other protections you put in place, malware authors can bypass it all if they can fool you into doing something you shouldn't. The problem, of course, is that "what you shouldn't" isn't always immediately obvious. That's why it's so important to educate yourself on how to detect and avoid their attempts. In short: *be skeptical*. Don't open email attachments or instant messenger downloads unless you're positive they're safe. Don't click on links in email unless you're positive that they're taking you to where you expect them to. Don't download and install software without first checking it for malware. Don't ignore security warnings unless you're sure it's OK. Use strong passwords and never share them with anyone.

5. Scan for Viruses - Even with the best of intentions, viruses happen. Even with the firewall in place, the operating system up to date, and a healthy knowledge of what is and is not safe, sometimes something slips through. That's where you'll need a good anti-virus tool. There are many to choose from but the key factors boil down to this: select a reputable tool, enable its "real time" monitoring if you're at all uncertain of yourself or others using the computer, configure it to scan your hard disk completely once a day, and make absolutely certain that it's downloading the latest anti-virus information daily.

6. Protect Yourself from Spyware - Much like viruses, spyware can also occasionally make it through your defenses. Spyware is often relatively benign from a pure safety perspective - spyware doesn't often erase your hard drive or send spam, for example. However spyware does represent an intrusion, often presenting ads or modifying other programs in ways you didn't expect or ask for. And at its worst, spyware lives up to its name, spying on you and capturing potentially sensitive information. Anti-spyware utilities operate a little differently than anti-virus, so you'll want to make sure that you have a good spyware scanner in addition to your anti-virus tools. Like those tools, you'll want to make sure that it's downloading the latest spyware information daily as well.

7. Secure your WiFi - The default configuration of most WiFi equipment, and certainly the easiest configuration to set up, is completely unsecure. That means that anyone within range of your WiFi equipment can monitor what you're sending to and from the internet - including your account IDs and passwords. The same is true in most internet cafes and free WiFi hotspots. There are two steps you must take. First, at home, make sure you enable WPA security. This will require a password to connect to your wireless network, and will encrypt all the data so it cannot be monitored. (The older WEP security is no longer sufficient, as it is easily cracked.) Second, when you're using an open unsecure WiFi hotspot, take care to only access sensitive resources through encrypted connections. That means making sure that any web page you're visiting that requires personal information is connecting via an https connection. It also means that you shouldn't be downloading or sending email via your POP3 or SMTP based

email program unless you know those connections are configured to use encryption as well, since by default they do not.

Bonus Step: Understand Physical Security - An old saying that I've found myself repeating to people more and more in recent years is this: *"if it's not physically secure, it's not secure."* All of the preceding tips are for naught if someone else who doesn't understand these steps can use your computer and accidentally download malware. It's all for naught if someone with malicious intent can walk up to your computer, reboot it, install software or hardware and walk away without your noticing. It's all for naught if your computer can be stolen. Take care to understand just how physically at-risk you might be and take appropriate actions. Don't let others use your computer until you're comfortable with their understanding of the risks. Don't leave your computer unattended if you can't trust the people who might be able to touch it. Consider encrypting data on your laptop or other computer if it can be lost or stolen.

Everything I've outlined might at first seem overwhelming. The good news it that most of these steps are things you'll need to do only once, and then consider infrequently thereafter. And to put it perhaps into a little bigger perspective they're not nearly as overwhelming as the impact of an actual security problem if it happens to you. The practical reality of the situation is simply this: we as individual computer users need to take the responsibility of the steps required to Stay Safe Online.

More information about staying safe online, including specific recommendations for each of the aspects discussed above, can be found at the author's web site Ask Leo! There you'll also find hundreds of answers to every day technical and computer problems.

Three Quick Steps to Remove and Avoid Spyware

By Leo Notenboom

1. Install and Run an Anti-Spyware Program - The choices are endless, but popular anti-spyware tools which just happen to be free include Windows Defender, which may already be installed on your newer versions of Windows; Spybot Search and Destroy, which is a common and highly regarded recommendation, and Lavasoft's Adaware, which is free for personal home use. Download one of these programs and install it as soon as possible.

2. Update the Spyware Database - After downloading anti-spyware software, you should start by updating the database of spyware definitions that come with the installation. New spyware is created daily and your programs need to have the most current updates to remain effective. Most programs have update functions that will locate and install the latest databases automatically; make sure that this feature is enabled.

3. Run Regular Scans - Many anti-spyware programs will work automatically, which means once installed it goes to work checking your computer and will perform a complete scan daily. However, for those programs that don't have a regular scan as the default, you need to make sure to go in and set up a daily scan schedule so that the anti-spyware tool you've selected scans regularly.

Additional Notes

Many anti-spyware packages have advanced protection that can prevent spyware from installing. These programs may lock your browser home page so that you must approve any change, or simply not allow it to be changed. Some packages may also lock the "hosts" file - a common spyware target. These protections are valuable and should be turned on.

It's unfortunate, but there really is no single "best" anti-spyware program. Each operates differently and will catch some things others may miss. The best option is to select one to run as recommended, and perhaps have others "on call" for those times when spyware makes it past.

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 weekly newsletter now and receive a free ebook: "Internet Safety - Keeping Your Computer Safe on the Internet", a collection of steps, tools and concepts you need to know to keep your computer and your information safe.

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 weekly newsletter now and receive a free ebook: "Internet Safety - Keeping Your Computer Safe on the Internet", a collection of steps, tools and concepts you need to know to keep your computer and your information safe.

Fake Anti-Virus Software and Rogue Security Software

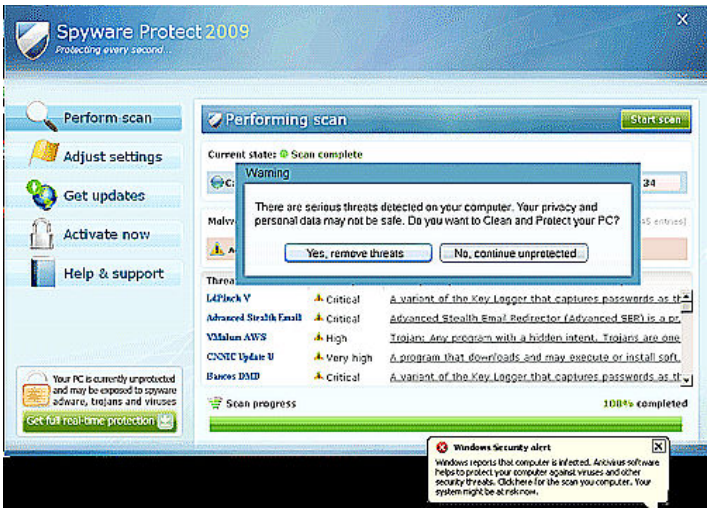
by Carl Tenning

Tacoma Open Group For Microcomputers

PC Pitstop has reported that fake antivirus software offerings are at epidemic proportions http://techtalk.pcpitstop.com/2009/08/02/fake-antivirus-at-epidemic-proportions/. Many of these fake applications appear as a pop-up, reporting that your computer is infected and to click on their scan to remove the infection. However, clicking anywhere on pop-ups such as these can install the malware, even if you think you are closing the pop-up window. PC Pitstop advises not to click anywhere on such pop-ups.

This particular one also installs a rootkit that blocks any valid anti-malware programs.

Here's another;

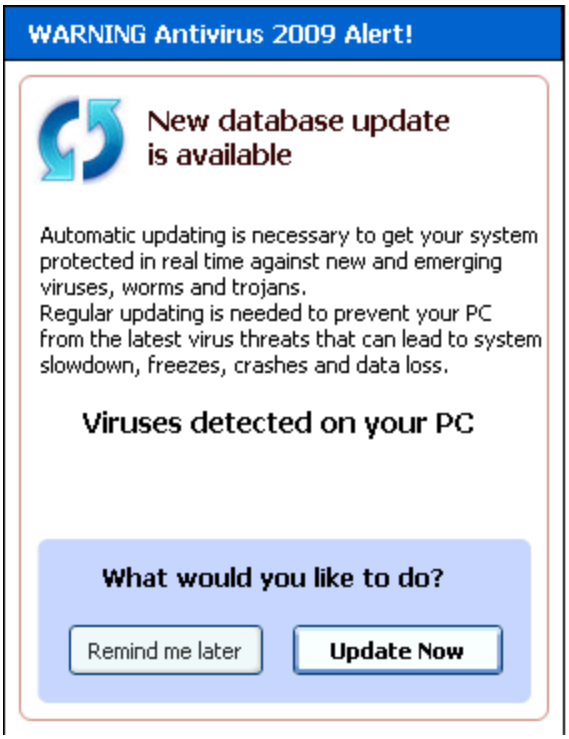


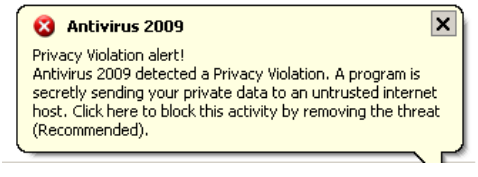
Trend Micro reports that if you see this pop-up, chances are that your computer is infected with the Conficker virus. You are warned not to click anywhere on a suspicious virus pop-up. Don't use your mouse to eliminate or scan for viruses nor use your mouse to close the window. Once you click on their link, you've been scammed. Instead, do a Ctrl+Alt+Delete to view a list of programs running and then shutdown the program from there.

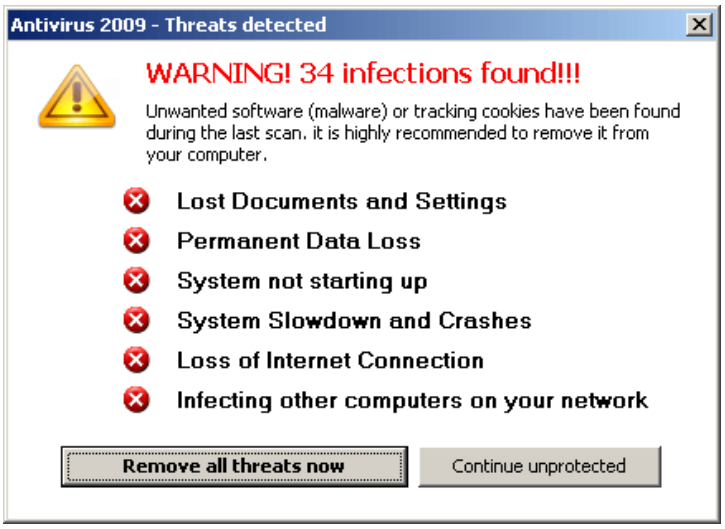
Here are some more examples:

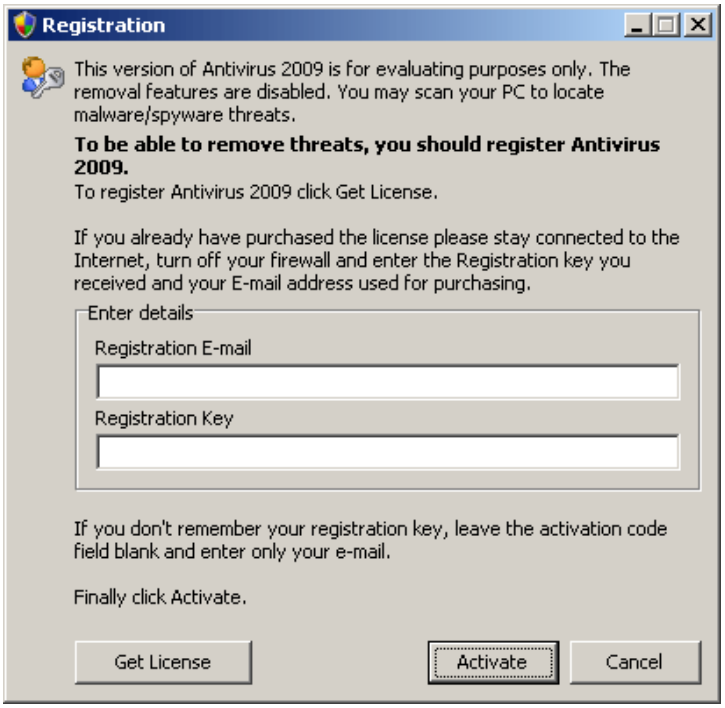
- Total Security 2009
- Windows System Suite
- Antivirus BEST
- System Security
- Personal Antivirus
- System Security 2009
- Malware Doctor
- Antivirus System Pro
- WinPC Defender
- Anti-Virus-1
- Spyware Guard 2008
- System Guard 2009
- Antivirus 2009
- Antivirus 2010
- Antivirus Pro 2009
- Antivirus 360
- MS Antispyware 2009

Some pop-ups to watch-out for:









Wikipedia had a list of over 100 rogue security software, with very convincing names: http://en.wikipedia.org/wiki/Rogue_security_software

In addition to just trying to scam you out of your money, this type of rogue security software also might not be able to be removed by the usual default Windows removal tool "Start > Control Panel > Add or Remove Programs." It will probably take special means of removal. There is a removal tool that covers the removal of 27 fake antivirus applications at:

http://freeofvirus.blogspot.com/2009/05/remove-fake-antivirus-10.html

Spyware Warrior is also a source of listings of Spyware Products & Web Sites: http://www.spywarewarrior.com/rogue_anti-spyware.htm

Bleeping Computer is another source for instructions for removing spyware and malware. Their Spyware And Malware Removal Guides Index, 2006-2008 is at:

http://www.bleepingcomputer.com/forums/topic171335.html

Legitimate online malware scanners (Reported safe by ZDNet) offered for free by their vendors include, but are not limited to:

- **Trend Micro's Housecall**
- **Kaspersky's Online Malware Scanner**
- **F-Secure's Online Malware Scanner**
- **ESET's Online Malware Scanner**
- **BitDefender's Online Malware Scanner**
- **PandaSecurity's Cloud Antivirus**
- **McAfee's Online Malware Scanner**
- **Rising's Online Malware Scanner**
- **Dr. Web's Online Malware Scanner**
- **Symantec's Online Malware Scanner**
- **CA's Online Malware Scanner**

What Is Ransomware?

by Carl Tenning

Tacoma Open Group For Microcomputers

Imagine having your computer infected with a malware that suddenly encrypted all of the files on your computer and demanded money to get the decryption key. This is the gist of "ransomware". Malware Armageddon maybe! It encrypts files on the victims computer and then demands paying a ransom for the encryption key. The ransom might be by calling a foreign phone number with exorbitant rates. Until now, cases of ransomware have been quite rare, but they are increasing at a very fast clip right now. A lot of ransomware is delivered via pop-ups. Use a pop-up blocker. And of course, be very careful about downloading software -- games, screensavers, etc. can include ransomware.

Most ransomware parasites are usually trojans and can be removed by antivirus products.

So keep your antivirus up to date.

It might also encrypt the entire computer, causing it to lock up the operating system. Although this tactic sounds self defeating, because once the computer is locked up there would seem to be no recovery short of paying the ransom for a boot disk to clear the lockup.

Recently, security experts have discovered a new ransomware variant in which the scammer demands that the victim purchase a specific amount of pharmaceutical drugs from a Russian online pharmacy to meet the ransom demand.

Ransomware programs also may try to embarrass victims to get them to comply quickly, using tactics like displaying adult images.

Ransomware is currently a PC (and not a Mac) problem.

Ransomware attacks can occur via email attachments or direct access to a computer network; however, most ransomware attacks are browser-based.

"Ransom.A" is one program that claims it will destroy one computer file every 30 minutes until the victim pays the ransom. In this case, however, Ransom.A doesn't actually delete or encrypt anything -- it's a hoax. Nonetheless, it's probably a very effective hoax.

Another ransomware program, Trojan.Archiveus, is a Trojan horse that password protects files and then asks the user to pay the ransom to get a password that unlocks the files. In this case, the virus writer made the critical error of placing the password in the code.

According to Symantec, the password is:
mf2lro8sw03ufvnsq034jfowr18f3cszc20vmw

Paying the Ransom?

What's to say that paying the ransom will actually work? It might work once, but then return again for more ransom. And some ransom threats are actually hoaxes!

Best solution:

Use firewalls, up-to-date anti-virus and anti-spyware software, and keeping your browser, system software and other software up-to-date with the latest patches.

Keep backups on external storage like USB hard drives.

Remote Access Support - Is it Worth the Risk?

By Leo Notenboom

Typically when you call a software company or computer manufacturer to fix a problem they rely on you to describe what is wrong and then work with you to troubleshoot the problem over the phone. This can often get quite confusing.

Frequently these days, and with your permission, many such support desks can use remote access technology to view and even use your computer as you watch to solve your problem directly. This is certainly very convenient, but is it safe?

Not necessarily.

The real question you must ask before allowing anyone remote access to your computer is simply this: how much do you trust them?

Depending on the technology being used, you're giving that remote technician access not only to the problem but the rest of your computer as well - all of it - often with full administrative access Some technologies allow you to watch what the technician does while he or she fixes the problem, which can be both helpful and informative. But beware; they may also be exploring elsewhere in ways that you cannot see.

That's why it's all about trust.

Even if you are working with a reputable firm that you trust not to have some malicious intent, how can you be certain the technician actually knows what he or she is doing?

Certainly most companies are very probably reputable, and most technicians are indeed trustworthy and competent. But regardless, unless you have some way to actually confirm that, remote access still feels like a huge risk that just might not be worth it.

The bottom line? If you choose to allow support via remote access, make sure you are with a company you trust, and that you've established a level of trust with the individual technician handling your case.

And above all, be sure to back up your entire machine first. That's the ultimate safety net in case of error.

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 weekly newsletter now and receive a free ebook: "Internet Safety - Keeping Your Computer Safe on the Internet", a collection of steps, tools and concepts you need to know to keep your computer and your information safe.

Article Source:

Viruses - How to Keep Yourself Safe

By Leo Notenboom

If you use a computer at all, chances are that at some point you've been effected by a virus. If you were lucky, the virus may have just been an annoying setback to your day, but if you weren't so lucky you may have lost all of your data... or your bank account information... or even your identity.

Computer viruses are a threat to everyone. So to lessen our risk of infection, we must not be complacent- we must take steps to make sure that our computers are safe.

Yet after all the news, the horror stories, and the warnings... after all this time...

Complacency is still a big problem.

There are four important steps you should take to ensure that your computer is safe:

1. Install and Run an Anti-Virus Program

There are many to choose from.

Malwarebytes AntiMalware got a good reputation quickly when it was among the first to be able to recognize and remove some particularly nasty viruses. Other popular anti-virus solutions with good reputations include the free versions of AVG, Avira and Avast.

Symantec maintains one of the best reference sites for security issues that are related to viruses, although their product offerings are often overly complex.

One thing to keep in mind is that not all virus scanners catch all viruses. For that reason, it's a good idea to have a variety of additional virus scanners to run as a "second tier". Many downloadable virus scanning solutions include free trial periods, which are great for one-time second-level scans.

The important thing is that you download and install your package of choice. Do it now. You don't want to forget.

2. Update the Anti-Virus Database

The next step after installing your anti-virus software is to update the virus signature database that came with it. The databases used by anti-virus programs are updated frequently, as new viruses are being created every day. For the best protection, you need to update to the latest database for your program right away.

In most of the programs there is a function that will locate, download and install the latest databases automatically and regularly. You just need to make sure that this is enabled.

3. Run Regular Scans

Most anti-virus programs work automatically. After installation, they will scan all incoming and outgoing files, and they will hook into your email to ensure that your received email is not infected.

Make sure that this "real time" scanning is enabled, unless you really know what you're doing. (However, if email scanning interferes with your email program, you can turn it off.)

It is also important that you periodically run scans of your hard disk(s). When you first install the software you should definitely run a full scan. From then on, depending on how much you use your machine, you should run a scan periodically.

With some programs you can schedule these scans to happen automatically. For example, if your computers stay on 24 hours per day, schedule the full virus scans to run at night while you're asleep.

4. Keep Windows Up-To-Date

Simply enable the automatic update feature in Windows, or make sure to visit Windows Update regularly.

Software has bugs- it's a fact of life. Unfortunately, virus writers are able to take advantage of some of those bugs to create the viruses that can infect your system. Microsoft fixes the affected components in the operating system as these bugs are found, and makes the fixes available for download and automatic installation via Windows Update.

However, virus writers know that not everyone stays up-to-date. So as soon as the bugs are discovered and publicized, and even when the fix is available, they are busy writing viruses that will still exploit them.

For example, many, many people continue to read a very popular Ask Leo! article on this subject because they are still being affected by a virus using an exploit that was patched years ago. Why? Because their systems are not up-to-date, and as a result they remain vulnerable to attack.

Keep Windows up-to-date. If you're not going to enable automatic update, then visit Windows Update weekly. Let other people have the pleasure of being affected with the latest viruses.

Some Additional Notes

You may be wondering why there are so many alternative anti-virus programs listed above. Well, the truth is there is no "best" anti-virus program, and even the ones that are better or worse than the others change over time. They each may catch something that the other misses, or vice versa. The best thing to do is to choose one as your primary, and keep the others "on call" in case something slips by the one you use regularly.

Make sure that if you do install more than one program, you do not enable the "real time" scanning for more than one at a time. Doing so will cause "unpredictable results", as they will conflict each other.

Article Source:
http://EzineArticles.com/?expert=Leo_Notenboom

Online Safety - Stay Safe While Enjoying the Ride

By Leo Notenboom

In an ideal world, you wouldn't have to worry about online safety. You wouldn't have to worry about others on the network trying to steal, harm, or infect your computers with malicious viruses or spyware. Unfortunately, this is not an ideal world. The days have passed where you can safely use the computer, browse the Internet and not be concerned about online security. And yet, if you're an average user you rarely think about security, if at all. If you ignore computer security, it is at your own risk, even the risk of your friends and family. What can you do to stay safe?

Granted, not using the computer will remove all risk. But, you

could also say that never being in a car removes the risk of getting in a traffic accident, or living in a cave reduces the risk of being hit by a meteor. Are giving up the risks worth giving up the rewards?

Driving is risky, but you still drive because the rewards are greater than the risks. However, do you drive recklessly, or do you take precautions to reduce the risk? Is the car in good shape? Do you have your license? Do you buckle up? Are the roads safe? Even with these precautions, someone could still drift over the center line and crash into you. To feel even safer, you become a defensive driver and learn how to keep an eye on "the other guy," just in case.

A computer crash is much less life threatening, but the rules of avoiding risk are very similar. Tech blogger Michael Horowitz has coined the term "Defensive Computing." As he notes "defensive computing, as I see it, is about taking steps when things are running well to avoid or minimize problems down the road. Rather than focusing solely on computer problems, it's about being smart and planning ahead to minimize problems and their impact."

Here are 6 important ways to practice defensive computing:

1. Don't open or click on SPAM.
2. Don't open attachments you aren't positive are safe.
3. Keep your system up to date.
4. Run anti-malware software and keep it up to date.
5. Use a firewall.
6. Back up regularly and often. A good back up can help you recover from almost anything.

It may seem overwhelming, but like driving a car, the rules and safety warnings will soon become second nature.

It is true, there are risks to using the Internet. There are risks to getting out of bed every day. However, computers and the Internet are valuable tools that open up a world of possibilities. Don't be frightened. Stay safe, follow the rules, be defensive and keep your equipment up to date. You too can enjoy the ride.

The Best Anti-Spyware and Anti-Virus Still Can't Protect You From Dancing Bunnies

By Leo Notenboom

You may wonder what anti-spyware program to use or which anti-virus program is the most effective.

There are many good anti-spyware and anti-virus tools out there but it's extremely important to remember that there is no perfect solution. All of these anti-malware programs will miss things that others may catch. The best approach is to choose one of the better ones - both an anti-spyware tool and an anti-virus tool - and then also keep a couple of others in reserve, just in case.

But whether it be for spyware or viruses, make sure you run something for both, and be sure to keep the databases for each as up-to-date as possible.

A post on Microsoft Software Engineer Larry Osterman's weblog is a good reminder of this. Larry is a long-time Microsoft developer that some time ago commented on a claim made by someone that a properly-designed operating system should not require any anti-virus or anti-spyware software at all. Larry pointed out the more practical reality of the situation in what he called the "dancing bunnies" problem.

The "dancing bunnies" problem is simply this: if you receive an email that says "click here to see dancing bunnies," then if you're like most users, you'll work around any protections your system may have in place because you want to see those dancing bunnies, and no one is going to stop you.

Also termed social engineering, the idea behind this approach is to promise you something that you'll react to, to get you to allow something else more sinister or malicious.

At that point, even an ideal operating system will make no difference. You'll need to have some kind of protection that makes sure that what you just clicked on, ran, or even installed, is safe. Today that means you need good anti-virus and anti-spyware tools installed on your system.

You might claim that education is the key - that by becoming more savvy about computer related issues and scams you can recognize and avoid situations like this. You wouldn't need any additional protection from yourself.

Theoretically you might be right - and certainly the education is a good thing.

But practically?

Sometimes those dancing bunnies can be pretty tempting..

Article Source:
http://EzineArticles.com/?expert=Leo_Notenboom

Important Information For All Users Of Malwarebytes Software

by Ron Hirsch - ronhirsch1439@comcast.net

Malwarebytes security software has been, and still is one of the best software programs available to help protect your system from the rash of malware and similar “bad stuff” out there in the computer underworld.

I have been using it in conjunction with Microsoft Security Essentials for quite a while now, starting with my older Windows XP Pro 32 bit system computer, and now with my new Windows 7 64 bit computer.

Malwarebytes comes in two versions, free and paid. The free version of Malwarebytes does not offer real time protection, but users can initiate a scan any time they want, to search for malware. The paid version is a lifetime license, with real time protection.

I recently learned that if you are using the paid version, and have set it for real time protection, there can be conflicts with your other security programs. But these conflicts can be stopped by listing the various Malwarebytes active files in the "exclusion" folder of your other antivirus/security software.

I discovered this by accident recently, when my copy of the paid Malwarebytes program notified me that a newer version had been downloaded. And, did I want to install it. Of course, I said OK, and that proceeded to close the program and then install the newer version. It then said I had to reboot, so I did.

After the machine had rebooted, everything was frozen solid, so I tried anther reboot, but that also locked everything up tight. It seemed pretty obvious that Malwarebytes was the cause here, but what was the cure? I booted up using SAFE mode, and it booted OK. While in SAFE mode, I decided to just uninstall Malwarebytes, until I could find out the proper solution.

The next normal boot had everything working fine, no lockups - all was normal, confirming that Malwarebytes was the cause. So I sent an email off to Malwarebytes . They got back to me very quickly, and gave me this link below to explain the problem and solution to the freezeups.

http://forums.malwarebytes.org/index.php?s=70b8be10374840dca65629a2162b6d60&showtopic=10138&st=0&p=167851&#entry167851

If you are not running the paid version, with real time protection, then this fix may well not be needed. But for those using real time protection, it is mandatory.

This is a thread on the Malwarebytes forum, and someone has clearly presented all the fixes to solve the problem, with a wide range of antivirus programs. The fixes are applicable to most versions of Windows, but I believe that the paths for the fixes here are primarily for Windows 32 bit systems. The information presented contains screen shots for those who have problems understanding the fixes.

If you have any trouble accessing this link, I have, as I noted below, created a PDF file of this complete presentation, and it is available on the BRCS site, along with the PDF versions of my articles. See later on, for the link.

The file locations for 64 bit Window's systems are different. Below are the respective locations for Windows 7 64 bit. I have no other 64 bit systems, but I would guess that Vista's locations are probably similar. Since most of you will still be using a 32 bit operating system, such as XP or Vista, you will probably find that the file locations will be as shown on the Internet page, and in the PDF file I've created from the site.

But, you must be familiar with copying files in Windows Explorer to a specified location, depending upon your software. If you cannot do this, get a friend to help you.

Once you have located the target area of your antivirus software, you must them copy the files specified in the online (or PDF copy) of the instructions.

And, remember for 64 bit Windows versions, such as Windows 7 64 bit, the location of the files to copy is different.

Where you see C:\Windows**System32**\drivers\

You should use C:\Windows**SysWoW64**\drivers\

Where you see C:**Program Files**

You should use C:**Program Files (x86)**

Once I added to the exclusion window for Microsoft Security Essentials, all my problems were resolved. There were no freezeups at bootup, and the freezeups of various programs during operation disappeared completely. So I have confirmed that the fix works just fine.

If you would like to download a copy to read, or save, of the info presented on the Malwarebytes site, please go to

http://brcs.org/hirsch.php ,

which is our society's home page, and look for the file named Malwarebytes Info. You can read it online, and/or save it, as desired. And you can also download a PDF of this article, which is named "Malwarebytes article", if you'd like a copy for your records.

REMEMBER - Malwarebytes remains as one of the best security programs out there. I recommend it to all users. And for the small price of $24.95 you will have lifetime free updates of the program and the malware database, and real time protection. If you will want to go with the free version, you will have free database update, and scans anytime you want.

Using this program, and Microsoft Security Essentials will afford you top notch protection.

VOLUME 30 TOGGLE INDEX

Beginners Notes & Tips

Communications Note & Tips

Feb-10	Local Shared Objects -- Flash Cookies
Mar-10	Netiquette Notes - Promote Respect
Mar-10	Editing Email Source Code
Mar-10	What Are RSS Feeds?
Mar-10	Panda Cloud Antivirus Released
Mar-10	Google Searches
Apr-10	Downloading and Converting YouTube Videos
Apr-10	A Static or Dynamic IP address?
May-10	Go Wireless Young Man
Jun-09	Dropbox
Jun-09	Alternative Internet Browsers - Maybe Better Than IE
Jun-09	Magic Jack- To Buy Or Not
Aug-09	Drive-by Infections
Aug-09	Performing Better Searches
Sep-09	How To Spot a Phishing Email
Nov-09	What If?
Nov-09	Online Storage
Dec-09	The web designers' guide to cloud hosting
Dec-09	Social Networking--What is it, really?

General Interest

Aug-09	How To Send An Email Message To Any Cell Phone
Oct-09	There Is More to Music than the iPod
Oct-09	Online Backup Services, There Are Pros & Cons But They Are Up & Coming
Dec-09	A "STRESS-FREE" PC
Dec-09	Broadsides
Feb-10	Is Free Software Really Free?
Feb-10	OPCUG Free Software Guide - Part II
Feb-10	Clean Up Your Computer Dust Bunnies
Mar-10	Microsoft Scanner & Camera Wizard
Apr-10	Review - Ai Squared's Zoom Text Express
Apr-10	Burning a DVD in Movie Maker
Apr-10	Cryptography - a big word that helps keep the internet secure
May-10	MotionDSP vReveal:
May-10	EaseUS Partition Master Home Edition
May-10	Lock Your PC With a USB Drive

General Interest Notes & Tips

Jun-09	File Managemnent - Part One
Jun-09	Things, Thinglets, And Thingassos
Jul-09	Backup -- The Ware Essential to Your Computer
Jul-09	Online Backup Services
Jul-09	The Kindle 2 May Make Newspapers Obsolete
Jul-09	OwnerIQ
Jul-09	ZONBU
Jul-09	Gog.is/ - simple URL slapper and forwarder
Jul-09	One Laptop per Child - update

Hardware Notes & Tips

Jun-09	10 Things You Should Look For in a Notebook
Jun-09	Setting Up A New Computer
Aug-09	Are You Considering A Netbook?
Aug-09	The Myth of Width: When wide screens don't work
Aug-09	The Disintegration of Service
Sep-09	CD-Rs Harder To Read Than Standard Discs
Oct-09	Third Generation USB
Oct-09	A Tale of Two Printers, a Scanner, and a CD Drive
Nov-09	USB vs Firewire Data Transfer
Nov-09	Computer Performance Considerations
Nov-09	Understanding Firewalls
Nov-09	Buying a TV-Tuner
Nov-09	GPS Accuracy Could Start Dropping in 2010
Nov-09	What Those Disk Drive and Thumb Drive Numbers Mean?
Jan-10	Digital Memory Cards
Mar-10	Remapping your keyboard
Mar-10	Power to the Pixels
Mar-10	8 Tips for the Beginning PC Builder
Apr-10	Lipo Batteries - Bursting With Energy Important Safety Information!!
Apr-10	Erasing Hard Drives

Operating System Notes & Tips

Jul-09	Driver Query Helps Resolve Driver Problems
Jul-09	Fun and Games with Ubuntu
Oct-09	A Slightly Different Kind Of Shortcut
Nov-09	Install Those Updates
Dec-09	Installing Windows 7 on a Vista Laptop
Dec-09	More on Installing Windows 7 Upgrade
Dec-09	Moving From XP to Windows 7
Dec-09	Ubuntu 64-bit Operating System
Jan-10	WUBI? What The Heck Is A WUBI?
Jan-10	Neat Things You Can do with a Flash Drive
Jan-10	Three reasons why Windows 7 isn't for everybody
Jan-10	How Windows 7 Will Finally Kill XP..
Jan-10	Ask DACS
Jan-10	Windows Experience Index
Jan-10	Controlling System Restore
Jan-10	Windows 7, 64 Bit
Jan-10	Password Protect Your Account
Feb-10	Make Windows Rediscover Your Monitor
Feb-10	2009 Come and Gone
Feb-10	Making Windows More Legible
Mar-10	Repairing file registry permissions may solve setup problems
Apr-10	Customizing The Mouse In Windows 7
Apr-10	Windows 7 Tech Tips
May-10	Eliminating Obsolete Windows Device Drivers
May-10	Best Windows Shortcuts
Sep-09	Is It Time to Switch to 64 Bit Windows?
Sep-09	Where Is That File?
Sep-09	Windows Task Scheduler
Sep-09	Speed Demons

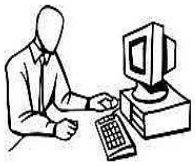
Spreadsheet Notes & Tips

May-10	Updating Values
May-10	Deleting a Hyperlink

Word Processing Notes & Tips

Mar-10	Using WORD 2007 or OFFICE 2007 Sometimes May Cause a Problem
May-10	Inserting the Total Number of Pages in Your Document
May-10	Mixing Column Formats On a Page
May-10	Convert a PDF File To a Text File
May-10	Understanding Digital Signatures

Help Lines

SOFTWARE HELP	Advisor No.	HARDWARE HELP	Advisor No.
Win 95/98/ME	2, 3, 4, 7	Reformat Hard Disk, FDISK	2, 4, 5
Win 2K/NT/XP	2, 3, 7	Install Hard Drive, CD-ROM/RW	2, 4, 5
MS Word	2, 7	Install Video Card	3
MS Excel	4	Deleting Files, Wiping	6
MS PowerPoint		Internet/Intranet	6, 7
WordPerfect	1, 7	Audio Cards	4
QuickBooks	8	MP3 Files, WMA Files, WAV Files	4
Norton/Symantec AntiVirus	2, 3, 6, 7	Burning CD's	3, 5
Norton System Works	2, 7	Partitioning Hard Drives	2
CompuPic/CompuPic Pro	3, 7	Net Objects	7
Winzip, WinRAR	6	Homesite	7
JV Registry Cleaner	3	MS Access	
Outlook, Outlook Express	2		
Internet Explorer	2, 7		
Netscape Navigator	7		
Instant Messaging	2		
Installing Software after Reformatting	5		
Ccleaner	3		
Easy CD DA Extractor	3		

ADVISORS	PHONE	HOURS
Fred Shelton [1]	(253) 752-0120	Variable
Bob Henkel [2]	(253) 537-6732	8A-8P anyday
Tom Stepanek [3]	(253) 922-7939	7-9P Mon-Fri
Carl Tenning [4]	(206) 824-3843	6-9P Mon-Fri
Oclad Wesley [5]	(253) 212-0352	6-9P
Bob Thomson [6]	(253) 752-5582	
Ray Mills [7]	(360) 692-7568	6-9P Mon-Sat
Sandee Gimblett [8]	(253) 952-3538	

Tacoma Open Group for Microcomputers (TOG)

New Member Application/Existing Member Change of Address Form

For Tacoma Open Group annual membership, send form (if needed) & $25 to Bob Henkel, 10613 25th Avenue E. Tacoma, WA 98445

Make checks payable to TOG

Member's Name:_____ Date:_____ Sponsored by:_____
Address:_____

City:_____ State:_____ Zip:_____ Plus Four:_____ Country:_____

Home Phone: (_____) -_____ Work Phone: (_____) -_____ E-mail Address:_____

TACOMA MEETING

When: Mon 13 Sep 2010—7:00 PM

Where:: SE Tacoma Community Center
1614 99th Street E.
Tacoma, WA 98445-3912

From I-5 take Exit 127 (Hwy 512) to Portland Ave.., north on Portland Ave. to 99th, left over tracks. Building is on south side.

Future Dates: 2nd Monday of Month

TOG BOARD MEMBERS

President: Carl Tenning (206) 824-3843

& S. King County Rep. c10ing@hotmail.com

Web page: http://carlten.tripod.com/

VP/Prog Chair Position vacant

Sec/Treas Bob Henkel
(253) 952-3538

Librarian:Tom Stepanek (253) 922-7939

Newsletter Editor: Bob Thomson (253) 752-5582

Kitsap County Rep Ray Mills (310) 692-7568 email: r.mills@rm-a.com

Web site: http://www.rm-a.com

TOG Web Site:

http://www.toggle.org

Deadline: 15th of this month to appear in next months issue, if room.

Corporate Sponsors:

Raymond Mills & Associates
www.rm-a.com

How To Get To The Meeting

For those readers still unfamiliar with how to find our meeting place, we have reproduced the map showing its relationship in Tacoma to Portland Avenue S. and the 512 Freeway. The 512 Freeway can be entered from I-5 in Tacoma on the west or from Hwy 167 in Puyallup on the east. Proceed to the Portland Ave. off-ramp and turn north to 99th Street. Some folks in the middle of Tacoma may prefer to take Portland Ave. southbound to 99th. At 99th, turn west over the tracks and you are there!

TOGGLE

Tacoma Open Group for Micros
1808 Lenore Drive
Tacoma, WA 98406-1920

Change Service Requested

Is your address correct?

ARE YOU MOVING?

SAVES THE COST OF FORWARDING

Please notify us of your new address by the 20th of the month BEFORE our next meeting.

PROGRAMS

This Month's Meeting

This will be a regular monthly meeting with discussions and a program. Meeting discussions are always interesting and the ever-popular Q & A (Question & Answer) period is sure to pique your interest, come up to your expectations, and tickle your fancy. Come and share your experiences, problems, and discoveries.

Library News

The following software titles are available from the Toggle librarian, Tom Stepanek:

WinUtilities 9.81; Advanced System Care 3, Best of the Web Jan-June2010A;

Best of the Web Year 2009 and Symantec AV 11.0 in 32 bit or 64 bit versions.

If you are interesting in receiving any of these CDs, give Tom a call or come

to the next meeting.