TOGGLE

THE MICROCOMPUTER TURN (ON)

MONTHLY NEWSLETTER FOR TACOMA-SEATTLE AREA MICROCOMPUTER USERS

Volume 33 Number 10 April 2013 Issue #359

IN THIS ISSUE

UPDATE

Communications

In *InfoAtoms Infection or Something I Didn't Ask For* Carl Tenning tells us about little advertising snippets that had crept into his presentation to last monthly meetings while he was accessing the Internet. Another memeber at the meeting was also online at the same site and did not have the same problem. Read all about it.

In *Spam Economics* the author tels us about ''CAPTCHA - a 'Completely Automated Public Turing test to tell Computers and Humans Apart.' CAPTCHAs are used to allow real people into certain areas of websites - comment sections on blogs, for example - and to keep automated services, like spammers, away.''

In *How to avoid the Google Redirect Virus* the author talks about avoidance of those sites where you are redirected to sites you don't want to go to.

In *Two-Factor Authentication: Stronger security* the author says:''Okay, I'll admit this sounds geeky, but it's important. Two-factor login security isn't all that complicated, and it can save your bacon from hackers and identity thieves. Read on to learn more about this relatively new security technique that I'm strongly recommending for PC, Mac and mobile users... ''

In *How to get good social network security* the author says: ''Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post. ''

In *Do Not Track Plus by Abine.com* the author notes that:''A new program offered free from Abine software allows you to block websites you visit from tracking where you browse.'' Worth a look.

In *Java: How to fix your biggest Internet security risk* the author discusses the inadequate steps Java author taken to protect Java users from viruses and such. Sugests that you stop using Java and steps tp take.

Operating System

In *Using the Command Prompt to Reveal Hidden Files* the author says:''When you view your desktop or click on your C: drive, it may appear that all of your files have been deleted, but they haven't. If this happens to you here is how to restore them.''

Software

In *Warning: Major License Change for Office 2013 May Cost You $$$$$* the author warns ''For retail customers, if you install Microsoft Office 2013 on your computer, and it fails or is lost or stolen, your Office 2013 license is no longer valid. That means you will have to buy another copy of Office 2013 when you replace that computer.''

In *If You Agree Check The Square Box* the author tells how he checked all the boxes ina software purchase thinking he was agreeing to ONE payment. He was not. Read about it.

Hardware

In *When troubleshooting, assume nothing is innocent* the author tells us about a troublesome BIOS battery.

General Interest

In *Myth-busting - Debunking Some ComputerMyths* This is an article that we ran before several years ago. It is an oldie but goodie so we're running it again.

COMMUNICATIONS NOTES & TIPS

InfoAtoms Infection or Something I Didn't Ask For

by Carl Tenning, Tacoma Open Group For Microcomputers

At the March 2013 meeting of the Tacoma Open Group For Microcomputers, I was demonstrating the TOGGLE website and discovered that certain links had been added to our web page, or at least to the browser display of the page. First, I checked the source code to see if the HTML file on the host had been hacked. The source can be viewed by right-clicking on a blank portion of the page and selecting ''Source'' from the popup. Doing this, we found that no link had been added to the source code. Another member at the meeting then also accessed the same web page, but did not get these links displayed in his browser. So now, we concluded that the links were only appearing on just my notebook. It was also noted that upon the first view of the web page, the links did not appear immediately, but after a second or two. With all the threats of viruses these days, we were savvy enough not to click on one of the links. But, hovering the mouse over the link brings up a popup that discloses the link. These were all ''InfoAtom'' links. So what gives?

A Google search for ''Infoatoms'' reveals that this is a virus. Infoatoms is a malicious plugin that displays unwanted ads and pop-ups on infected computers. This application loads itself as a browser extension and affects Firefox, Chrome and Internet Explorer. The recommended action is to use an uninstaller to remove the InfoAtoms application. I used Revo Uninstaller and it correctly identified and uninstalled the application. Following that, however, I did an antivirus scan with Symantec Endpoint Protection and found nothing. To be sure, I did another scan using Malwarebytes. There was nothing found by either scan.

Not every article discussing InfoAtoms identified it as malware. C/NET, for example, offers it as a legitimate download, stating that it provides a ''Search without leaving the page!'' Some users reported that they do not have permission to uninstall InfoAtoms, which resulted in the impossibility to conduct a complete removal from their machine. For this case, McAfee Secure offers a special removal tool: Download: Microsoft Windows InfoAtoms 1.0.10.0 Removal/Uninstall Tool

So, was this a virus or not? Because it uninstalled without difficulty it may have been a legitimate version of the application. But, as many entries found on the Google search indicate, it may be that there are malware versions as well. It may be that it got installed when I had to re-install Internet Explorer. I had recently tried to install Windows 8, but finally gave up and went back to Windows 7. In the process, Internet Explorer seemed to get buggy, so I did a re-install of Internet Explorer. Instead of going directly to the Microsoft site, however, I accidentally got it from Yahoo, which apparently did include some add-ons. Perhaps InfoAtoms was one of the add-ons.

Spam Economics

by Dan Lewis
As published in Now I Know*

Pictured above is something called a CAPTCHA - a ''Completely Automated Public Turing test to tell Computers and Humans Apart.'' CAPTCHAs are used to allow real people into certain areas of websites - comment sections on blogs, for example - and to keep automated services, like spammers, away. With probably millions of blogs, forums, etc. around the Web, the CAPTCHA is probably the best method we have at keeping feedback from being overwhelmed with links to sites which claim to cure baldness and other (typically more insidious) such things.

But of course, some of the spammers have found a way past the CAPTCHA. When computers can't get through, they turn to people.

The criteria for a CAPTCHA, per a team of U.C. San Diego researchers investigating how spammers weave their way though the gates (pdf here), is three-fold. First, the problem needs to be easily solved by people; after all, you want people to be able to leave their comments or thoughts. Second, the test has to be ''easily generated and evaluated,'' and practically speaking, by some sort of computer algorithm and database. This makes sense, as the number of, say, forum posts could easily overwhelm the forum owner if he or she had to create and/or evaluate each test by hand. Finally, the CAPTCHA cannot be easily solved by a computer, as the entire point is to weed out automated replies. (And the trick is not just to get readers to click. Because Googles search engine treats links to a page as a ''vote'' for that page's value, having a lot of links to your website may have a positive effect on your websites rank in the search results.)

The work-around, per the researchers, is something they call ''paid solving.'' They came across a blog post written in 2006 by an employee of computer security company Symantec, discussing an ad placed on a freelancer-finding job board. The advertiser was looking for someone to solve CAPTCHA's over a 50-hour workweek, and received 58 bids ranging between $30 and $1,000 within the first week. (The site canceled the advertisement thereafter.) The Symantec employee assumed that in 50 hours, someone could solve about 6,000 CAPTCHA's (at 30 seconds per puzzle), making the low-end bid come out to under two cents each.

Four years later, the New York Times delved deeper. A report from Mumbai, India noted that high-end spamming companies (yes, they exist) hired cheap laborers in India, Bangladesh, China, and in other developing nations where such labor is readily accessible. Those workers are asked to solve the cryptic-looking text, and, once through the door, sign up for accounts, post messages, or, as the Times so aptly phrases, ''carry out other mischief.'' For their trouble? Some students working on CAPTCHA-busting ''typically work two and a half to three hours a day from their homes and make at least $6 every 15 days,'' which sounds terrible, but isn't bad relative to other wages; the Times further notes that ''[u]nskilled male farm workers earn about $2 a day in many parts of India.''

While spammers may find these nickels and dimes well-spent on finding a solution, the advent of ''paid solving'' doesn't bother Google, which makes some of the leading anti-spam/CAPTCHA software. As one engineer told the Times, ''[o]ur goal is to make mass account creation less attractive to spammers, and the fact that spammers have to pay people to solve captchas proves that the tool is working.''.

Bonus fact: You may notice at the bottom right of the image above that the logo reads ''stop spam. read books.'' That particular anti-spam service, called reCAPTCHA (and now owned by Google), doesn't just keep the spammers away. One of the words shown is used for that purpose, but the other isn't. As reCAPTCHA explains, ''reCAPTCHA improves the process of digitizing books by sending words that cannot be read by computers to the Web in the form of CAPTCHA's for humans to decipher. More specifically, each word that cannot be read correctly by OCR [''Optical Character Recognition''] is placed on an image and used as a CAPTCHA.'' With literally millions of reCAPTCHA attempts happening each day, the service is helping digitized old texts. (And at $6 every 15 days, spammers are helping, too.)

From the Archives: From Sheep to Books: Why are books the size and shape they are?

Related: Spam.

Originally published February 4, 2013 NOW I KNOW is a free email newsletter of incredible things; you'll learn something new every day. Written and distributed by Dan Lewis. Now I Know is a participant in the Amazon Services LLC Associates Program, an affilaite advertising program designed to provide a means for site to earn advertising fees by advertising and linking to Amazon.com. Some images via Wikipedia, available for use here under a Creative Commons license, and copyright their respective owners.
Subscribe now! at ***nowIknow.com***

How to avoid the Google Redirect Virus

by Penny Cano, Cajun Clickers Computer Club,
www.clickers.org ccnewsletter (at) cox.net

You search Google for something that interests you and get a series of Google web pages with links to websites with pertinent information. But this time, no matter which link you click on, it takes you to a website selling something that has absolutely nothing to do with the topic of your search.

Suspecting something, you do a full scan with your virus program and don't find any infection. Then you may try some of the other malwareremoval programs like Malwarebytes, Spybot, or SuperAntiSpyware; they don't find anything either. But you know something is wrong. I ran into this when one of our club members became infected and came to me seeking help. Since most of us use Google search with some frequency, I thought it a good time to discuss how this Trojan and other similar Trojans work.

Incentive for infection

Some of the other names for this Trojan are Bac-door.Tidserv, Win32.TDSS, and Alureon. It's not new; it was first discovered in 2008 and additional variations have been created since then.

Its purpose is primarily profit-making. The person or enterprise that infects your computer actually gets paid for doing so. To go undetected, it hides itself using stealth techniques, including a rootkit.

Once it is on the computer, it installs itself where it cannot be detected, then deletes the original files to eliminate traces of itself. The payload then causes the user to be redirected to web sites associated with malicious schemes or ones that download and install software that is not needed or wanted. So the infector gets a kickback for each user who succumbs.

How you get infected

Social networking opens up a myriad of opportunities for these attackers. It can be spread by means of the KoobFace Trojan specific to FaceBook. Forums and Blogs are another source. A typical scenario involves some sensational topic with an associated link to what appears to be a video or pictures.

When the user clicks one of these links, the attacker has the opportunity to deliver the infection. The same attacker may place these links on many sites on the Web. Links in e-mail provide another opportunity.

When people see something they think is funny or interesting on the Internet, they feel compelled to forward the website or link to all their friends. This in turn gets forwarded and re-forwarded. You may not know the original sender or many of the other people it was sent to. (Of course you've never

received these - right?) And then there's spam with all sorts of links. If the link points to an infected site, the infection gets spread to anyone clicking on it.

Peer-to-Peer networking for the downloading of pirated software (music, movies, and programs) and shared files is another source of infection. The supplier of the illegal software (or files) is often anonymous. Who's to say the name of the malware file was not changed to that of a popular song, for example. When the pirated 'song' is downloaded the user is really downloading the Trojan. It is much safer to pay for legitimate content.

Hacked websites can actually be legitimate or well-known sites that have malicious software unknowingly installed on them. Web forms are particularly vulnerable if the system they are on is not properly secured. Those crazy looking letters that you are asked to type into the box below (don't you just hate them?) are a security measure to keep attackers from gaining access to the forms.

Avoiding infection

Be careful about clicking on links on Web sites and in e-mail. Sometimes, if you pause your cursor on a link, you can see where the link actually leads. Be cautious clicking on links in e-mail, particularly spam and those that have been forwarded multiple times to multiple people.

Some virus programs have link-checking as a built-in function and rate links on Web pages. This is particularly useful when following search engine results. If advertisements occur in pop-ups, do not click on them or follow the links they offer.

Buy your downloaded software from known sources. Pirated software is often booby-trapped with malware. Keep your Windows Operating System up-to-date. Windows Update provides patches that can lessen the risk of the system being compromised.

Removal

I found three removal tools online:

- Symantec: go to http://symantec.com/security_response and search the site for'Tidserv'
- Kaspersky provides TDSSKiller.exe http://bit.ly/h4FjC8
- McAfee offers Stinger.exe http://bit.ly/dJTzpJ

However, since this Trojan hides in areas outside the operating system and makes itself undetectable by normal means, I highly recommend that you take your computer to someone familiar with its removal if you experience these symptoms.

This article originally appeared in the July 2012 issue of the Cajun Clickers Computer News.

Two-Factor Authentication: Stronger security

from The Tip Corner by Bob Rankin, Ask Bob Rankin
www.askbobrankin.com

Okay, I'll admit this sounds geeky, but it's important. Two-factor login security isn't all that complicated, and it can save your bacon from hackers and identity thieves. Read on to learn more about this relatively new security technique that I'm strongly recommending for PC, Mac and mobile users...

What is Two-Factor Authentication?

In order to understand two-factor authentication (also called two-step verification) and how it can dramatically improve your online security, it's best to start with familiar examples of one-factor authentication and their vulnerabilities.

Authentication, in security speak, is the process of demonstrating that you have access privileges to some restricted environment. Each piece of proof that you can offer is called a factor. In a one-factor authentication system, only one piece of proof needs to be offered to gain access.

Take your car key: you need only that one authentication factor to open your car. The lock doesn't care who is holding the key. The key works even in the hand of a thief. The same is true of traditional website logins. A website doesn't care if the person who enters the password is who he or she claims to be. If a thief guesses or otherwise gets hold of your username and password, he can pretend to be you. That's relatively easy with keyloggers, phishing emails, and many other tricks.

Yes, a username and a password are two different things, but since the user names are public knowledge, they don't count as one of your authentication factors. They're also typically stored together and stolen together, so we need something in addition to the username/password as a second security factor.

Now, consider using an ATM. You have a PIN code, but that alone won't get you any cash. You also need the physical card with its magnetic strip. Someone who steals your card or PIN alone is out of luck. That is a simple example of two-factor authentication. Of course, if you keep your PIN written down on a scrap of paper in your wallet, next to your card, then you are a fool.

Two Out of Three Ain't Bad

Ever wonder if someone is looking over your shoulder while you log in to Facebook or Gmail at the coffee shop? It happens. But here's the really cool thing -- with two-factor authentication, it doesn't matter if someone guesses or steals your password. Let me explain further. Two-factor authentication systems require two out of three things to authenticate you:

- Something you know: a memorized PIN or password
- Something you have: an ATM card, smartphone or some other physical token
- Something you are: a biometric trait such as a fingerprint or retina pattern

Biometrics are used in some highly secured environments, and on some consumer laptops, but they have not caught on among the general public. Physical tokens such as cards or USB dongles are a bit more common. But in general, the public has been too lazy to employ twofactor authentication, even in the face of news stories about hackers gaining access to millions of passwords. However, some high-profile companies are offering simpler approaches that may change that.

What Services Offer 2-Step Verification?

Google offers two-step verification for Gmail and other Google services. If you activate this option for Gmail, you'll need to enter your username/password as usual. You'll then be prompted for an authentication code before the login can be completed. The code comes from Google Authenticator, an app for Android, iOS, and Blackberry devices. This time-sensitive code can be generated even if you're not online, and you can also print a list of codes for use when you don't have your phone handy. (https://support.google.com/accounts/bin/answer.py?hl=en&topic=1056283&answer=180744&rd=1)<http://bit.ly/xg1nKd>

Yes, it's a minor nuisance to enter the code. But you only have to do it once every 30 days, or if you're logging in from an unfamiliar device or location. Just remember the major benefit: even if someone obtains your password, they won't be able to log in to your account without that verification code. And in order to get the code, they'd also have to steal your mobile phone.

Yahoo offers their version, called second signin verification for Yahoo Mail users. (http://www.ymailblog.com/blog/2011/12/yahoo-introduces-stronger-user-authentication-%E2%80%93-second-sign-in-verif ication/)<http://bit.ly/tQRCHz>

Facebook recently introduced what it calls login approvals, a process that requires two independent factors to authenticate a user at login. When login approval is activated, you are first asked for your Facebook username and password as usual. Then, Facebook checks to see if you are attempting to log in from an IP address that you use regularly. If not, then Facebook sends a code to your registered mobile device in the form of an SMS message. You have to enter that code in order to log on from an unfamiliar IP address. (http://www.facebook.com/note.php?note_id=10150172618258920)<http://on.fb.me/lnfcpg>

SpiderOak.com, a cloud storage service like DropBox, offers phone-based two-factor authentication as an option.

Some banks, brokerage houses, and other financial institutions offer (and even require) twofactor authentication in different forms. Bank of America's SafePass is one example. If you want the extra security of two-factor authentication from a particular institution, call to see if it's available. (http://www.bankofamerica.com/privacy/index.cfm?template=learn_about_safepass) <http://bit.ly/Jep4>

In spite of the extra step required to login, I highly recommend that you turn on two-step verification, whenever it's offered. You'll be glad you did, every time a friend tells you their email or Facebook account was hacked. Two-factor authentication will probably become a required part of every online login process before long. You'll be doing yourself a favor by getting on board now.

From Rankin's August 15, 2012 newsletter, reprinted with permission.

How to get good social network security

from staysafeonline.com

Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post.

Have your family follow these tips to safely enjoy social networking:

- Privacy and security settings exist for a reason: Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.

- Once posted, always posted: Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research (http://www.microsoft.com/privacy/dpd/research.aspx) found that 70% of job recruiters rejected candidates based on information they found online.

- Your online reputation can be a good thing: Recent research (http://www.microsoft.com/privacy/dpd/research.aspx) also found that recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment.

- Keep personal info personal: Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker

or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.

- Know and manage your friends: Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a ''fan'' page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know and trust) more synced up with your daily life.

- Be honest if you're uncomfortable: If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them; respect those differences.

- Know what action to take: If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator. Protect Yourself with these Stop. Think. Connect. Tips:

- Keep a clean machine: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

- Own your online presence: When applicable, set the privacy and security settings on websites to your comfort level for information sharing. It's OK to limit how you share information.

- Make passwords long and strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.

- Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals.

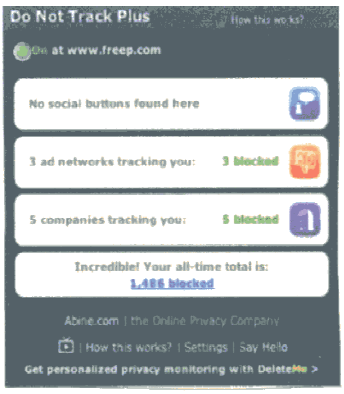
- When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

- Post only about others as you would have them post about you.

Do Not Track Plus by Abine.com

Reviewed by Larry Mobbs, President, Computer Operators of Marysville and Port Huron, MI March 2012 issue, COMP Communicator
www.bwcomp.org Lmobbs@comcast.net

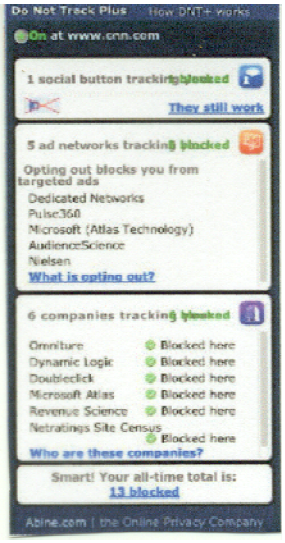
A new program offered free from Abine software allows you to block websites you visit from tracking where you browse. Many sites, and Facebook.com is one of the worst, want to track every site you visit so they can match-up your preferences to the items they want to display on your wall for advertisers.



In the software industry there is a movement to have the browsers include a plugin that prevents this action but as of yet it is not ordered and may never be. Browser publishers may take this on from their own volition but they will be pressured by advertisers not to.

One must remember that many sites depend on you or others visiting the links they place on their pages in order to pay for the website.

When you run Abine it puts a small icon in your browser and it displays a number with each site you visit, telling you how many attempts are made to track your visit and what type of tracking company is making the effort. They also keep a running grand total of how many blocks they have made. In the first few days of my use on one machine they blocked 1600 attempts.



Installation following the quick download is painless and there is virtually no setup. While writing this article I loaded Firefox, down loaded the software and ran it as a plugin.

This is required for each browser you use. After restarting Firefox I visited cnn.com and Donottrack Plus reported blocking 13 attempts to track my browsing on their site.

It looked like this (see right). The program came highly recommended by Cnet.com, which is where I read about it. It can be downloaded from Abiner.com.

Java: How to fix your biggest Internet security risk

Information found on Kim Komando's website:www.komando.com/columns/

The weekly - sometimes daily - security scares that occur with the Java programming language are starting to remind me of the old whack-a-mole arcade game.

Researchers or hackers discover a major flaw in Java. Java's developer, Oracle, whacks it with a patch. Another mole pops up. Oracle whacks it with a patch.

Many experts say Oracle is losing this game, or isn't trying very hard to win. And computer users are paying the price.

When a vulnerable version of Java is active in a Web browser, visiting a compromised website is all it takes for crooks to sneak malware on to your computer. In most cases, you won't even know the site is compromised until it's too late.

Here's how to stay safe: Stop using Java - or stay on top of the upgrades and use Java a lot more guardedly.

I'm going to help you do just that.

But first: What the heck is Java, and why is it capable of scalding your computer?

First developed back in 1995, Java became ubiquitous almost overnight because it allowed programmers to write one program and use it on Windows, Apple OS X and other operating systems.

Today, Internet browsers use Java for interactive Web content, such as popular online games. Computers use it to run useful programs such as the free Office alternative LibreOffice, and Adobe Creative Suite. And Java is pre-installed on most new systems. It's estimated that Java is running on 850 million computers around the world.

It's no wonder Java is a major target for hackers. It doesn't help that users frequently don't know it's installed and run outdated versions.

Java's security holes woke up Apple users last year when more than 600,000 Macs became infected with the Flashback malware that targeted Java.

Since then, moles have kept popping up through other holes. In response to the most recent exploit, the Department of Homeland Security a couple of weeks ago recommended that all Internet users disable Java in their browsers.

Apple and Mozilla have turned off Java plug-ins automatically in the latest editions of the browsers Safari and Firefox, respectively. But it doesn't hurt to double-check that Java is turned off.

Fortunately, the latest version of Java has a one-click button just for that purpose. That's handy because disabling it manually was a hassle, especially in Internet Explorer.

First, make sure you have the most recent version of Java from Oracle's site. The latest release as of this writing is Version 7 Update 11.

To bring up Java's new security settings, go to Start>>Computer and type ''Javacpl.exe'' in the search bar.

If it doesn't appear, you may have to find it manually. Go to Start>>Computer and open your Local Disk (C:). Go to Program Files (x86)>>Java>>jre7>>bin and scroll down until you see ''javacpl.exe''. On 32-bit computers, the file is in Program Files>>Java>jre7>>bin.

Run javacpl.exe to load Java's control panel and select the Security tab. Uncheck the box that says ''Enable Java content in the browser.'' Then restart any browsers you have running.

Mac users can find the setting by going to System Preferences and clicking on the Java icon - it looks like a steaming cup of coffee.

This will disable Java in your browser, but still let you use it for desktop programs.

Warning: If you do head into your browser settings to check that Java is disabled, you might see something called JavaScript. Don't disable JavaScript! It's a different animal and has no security issues.

Although it's safer to run Java for a desktop program, it's best to get it off your machine if you don't need it.

In Windows, go to Start>>Control Panel and click the Uninstall a program link. Find Java on the list of programs - you might see multiple installations of Java 6 and 7 - and uninstall any versions you see.

In OS X 10.7 and 10.8, go to Macintosh HD/Library/Java/JavaVirtualMachines/ and remove the 1.7.0.jdk file. Older versions of OS X might be running Java 6.

Even if you're keeping Java, you want to make sure you only have the latest version installed. Older versions leave your system vulnerable. Follow the steps above to remove the older versions.

If you need Java for a website or two that you know are absolutely trustworthy, you can enable Java briefly using the security control panel and then disable it again. Just make sure you stay on the trustworthy site while Java is enabled ?

OPERATING SYSTEM NOYES & TIPS

Using the Command Prompt to Reveal Hidden Files

excerpted from column by Bill Sheff nsheff@aol,com

Some viruses leave behind nasty side effects, even when your antivirus program has cleaned the actual virus from your computer. If your desktop icons are missing and your C: drive appears blank, don't panic, your files haven't gone permanently AWOL. Common viruses, such as the Windows 7 Recovery virus, will hide your files in an attempt to coerce you into paying for the virus's removal. When you view your desktop or click on your C: drive, it may appear that all of your files have been deleted, but they haven't. If this happens to you here is how to restore them. Click the Start button in the lower left corner of your task bar. Type cmd in the search box at the bottom of the menu and press Enter. If you're using Windows XP, click Run and type cmd into the Run box.

Type attrib -s -h -r c:/*.* /s /d and press Enter to execute the command.

Allow the command to finish executing (it may take a few minutes). When it's done, close the command prompt window and check your desktop - your files, hidden by the virus, have been restored. You can use the same trick to restore files the virus may have hidden on other drives, including removable storage such as flash drives and external hard drives; just change the drive letter (c:) in the command above to the drive letter of the storage device with the hidden files.

SOFTWARE NOTES & TIPS

Warning: Major License Change for Office 2013 May Cost You $$$$$

by Mike Morris, Front Range PCUG, http://www.frpcug.org

For retail customers, if you install Microsoft Office 2013 on your computer, and it fails or is lost or stolen, your Office 2013 license is no longer valid. That means you will have to buy another copy of Office 2013 when you replace that computer.

You will find a thourough discussion of this change at this Computerworld article (http://www.computerworld.com/s/article/9236818/Office_2013_retail_licensing_change_ties_suite_to_specific_PC_forever?taxonomyId=18&pageNumber=3. However, here are 3 quotes from that article to give you an appreciation of just how significant this change is:

- ''Microsoft yesterday confirmed that a retail copy of Office 2013 is permanently tied to the first PC on which it's installed, preventing customers from deleting the suite from one machine they own and installing it on another.''
- ''Prior to Office 2013, which debuted last month, Microsoft's EULA for retail copies of Office plainly stated that customers could reassign a license when, for example, they replaced an aged PC with a newer model or the original machine gave out.''
- ''...Microsoft confirmed that once a retail copy of Office 2013 is installed on a PC and activatedthe process of entering a 25-character ''key'' to prove the software was legitimately obtained - it cannot be uninstalled and then re-installed on another machine owned by the customer.''

So what can you do about this?

Here is what Microsoft wants you to do (quoted from the article):

- ''We've been very clear in all of our communications that customers seeking transferability should get Office 365 and that Office 2013 is licensed to one device,'' the Microsoft spokeswoman said in an email reply to questions.
- ''Very clear?'' Perhaps, but conveniently missing from that statement is the fact that Office 365 will cost you $100 each and every year you use it.

If you find that objectionable (and it will be interesting to see how many potential Office 2013 customers find it soif they know about it before they purchase the product), you have at least one other alternative.

That alternative is the open source (FREE) office suite Libre Office. You can download the latest version (v. 4.0) from http://www.libreoffice.org. This office suite includes these applications:

- word processor
- spreadsheet
- presentation
- database
- math
- drawing

In addition, if you have Microsoft Visio and Publisher documents, ''. . . (y)ou can retrieve and reuse your graphical content stored in these formats and edit it with LibreOffice's tools.''

There is much more. See http://www.libreoffice.org/home/Discover#/Discover%20it.

If you are concerned about compatibilty with Microsoft products, note that:

''Conversion with non-natives formats, like RTF or DOCX have significantly improved . . . .''

Although I have not extensively tested all of the Libre Office applications, my experience with the word processor leads me to conclude that there are only very minor issues, which are easily corrected.

It may be of interest that it is not easy to find the Office 2013 license (End User License Agreement, or EULA) on the Microsoft website. Eventually, I found this web page in a Google search and downloaded a pdf of the license, where it clearly states: ''You may not transfer the software to another computer or user.''

Save yourself some (perhaps a lot of) money and frustration. Download, install and use Libre Office in place of Microsoft Office 2013.

If You Agree Check The Square Box

by Ralph Smoyer, Lehigh Valley Computer Group (LVCG)
LVCG Journal, February 2013

If you agree to the following list of items please place a check mark in the small square box.

How often have you seen this line before? Well I have seen this line many, many times before, and I have also personally entered that check mark in that box at least one time too often.

You see I downloaded a MacAfee computer virus protection program via. the internet approx. three years ago and dutifully check marked the square box. I thought the MacAfee program worked quite well! How-ever. I belong to the Lehigh Valley Computer Group for many years as many of you do also, and I often use a lot of the knowledge that I get at our meetings. Well about three years ago one of our instructors mentioned that Microsoft offers a free virus protection plan, and I jumped on it (Wow, I could save $50.00 + bucks a year).

I chose to use my newly gained knowledge from the LVCG, and my present virus, malware and spyware protection is Microsoft Security Essentials (Free from Microsoft) and yes I did check mark the square box to have it actuated. It works great.

The bottom line of this article is that sometime in mid 2012 I checked my monthly credit card statement a little more thoroughly than usual, and I found that the $50.00 bucks that I thought I was saving a year was still being deducted from my credit card by MacAfee.

I then e-mailed, talked to them by phone, sent a letter, re-sent the letter via Certified mail! All to no avail.

My final realization was that I had to file a civil case with my local magistrate. I filed the paperwork, paid the court fees up front, and waited for my court date. On my court date the defendant, (MacAfee, headquartered in California) did not show. The judgment was in my favor and I received the McAfee 2012 credit card cost of $50.00 + bucks, and all of my court fees.

When talking by phone with a McAfee representative I mentioned that I didn't order their virus protection product this year and she replied, yes you did when you checked the square box. I then noted to her this could go on forever, and she agreed yes it could. I guess I now saved $50.00 bucks a year, and possibly forever, even for my heirs?

HARDWARE NOTES & TIPS

When troubleshooting, assume nothing is innocent

President's Message
By Sandy Rand n srand98[at]gmail.com
Brookdale Computer User Group, February 2013

One of my clients called me recently. Her Dell desktop computer wasn't working. As I started working on it I could see that it would start to boot, then 6 beeps, then nothing. Many times, it's the memory or a video problem. Not this time. I took out the 2 memory cards and reseated them. That didn't help. There were only 2 PCI cards, a modem and a wireless adapter. I took them out and reseated. Again, no help.

Next, I tried every combination with the memory cards, taking out one, then the other, swapping memory slots in case one of them was bad. I took out both memory cards and put in good ones that I had on hand. So far, nothing helped. I thought about the power supply. My power supply tester showed that it was good but still I swapped in a known good unit. Didn't help. Now what?

Going on the Internet, I looked up the beep codes for this PC. Some Dell computers have four troubleshooting lights on the case. This one does. The beep codes didn't help and the lights didn't either. Somehow in these codes, I got the idea that the boot process was doing some kind of a loop which needed to be ended. Hmm - .How about removing the battery on the motherboard?

It worked!!! I removed the battery and it started. There were error messages but no problem. Of course it had lost the date and time and a setting or two. Next, I shut it down and put the battery back in. Now booting up, I went into the BIOS setup screen and restored the date and time. Then, booting up, a message was telling me that it couldn't find the floppy drive. The computer doesn't have a floppy. I went back into the BIOS to disable the floppy. Now it booted with no errors.

The computer was running but way too slow. AVG antivirus didn't find anything but running MalwareBytes found 142 items to be removed including adware, spyware and 2 trojans. Finally, the computer was in good condition. Now I'm wondering how many computers I've thrown away over the years that might have been saved. The moral of the story is if nothing else works, try removing the BIOS battery.

GENERAL INTEREST

Myth-busting - Debunking Some Computer Myths

By Mindi McDowell, US Computer Emergency Readiness Team www.us-cert.gov

Here 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 http://www.us-cert.gov/cas/tips/ST04-005.html). However, none 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 http://www.us-cert.gov/cas/tips/ST04-006.html). 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 attackers 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 http://www.us-cert.gov/cas/tips/ST04-015.html and Understanding Hidden Threats: Rootkits and Botnets for more information http://www.us-cert.gov/cas/tips/ST06-001.html).

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 http://www.us-cert.gov/cas/tips/ST05-019.html .

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 http://www.us-cert.gov/cas/tips/ST04-016.html and Understanding Denial-of-Service Attacks for more information http://www.us-cert.gov/cas/tips/ST04-015.html).

Help Lines

HARDWARE HELP	Advisor No.
Reformat Hard Disk, FDISK	2, 4, 5
Install Hard Drive, CD-ROM/RW	2, 4, 5
Install Video Card	7
Partitioning Hard Drives	2
Internet/Intranet	6, 7
Audio Cards	4
MPs Files, WMA Files, WAV Files	3, 4
Burning CD's	3, 5
Homesite	7
Net Objects	7

SOFTWARE HELP	Advisor No.
Win 95/98/ME/2K/NT/XP	2, 3, 4, 7
Win 7	4, 7
Microsoft Word	2, 7
Microsoft Excel	4
Microsoft PowerPoint	4
WordPerfect	1, 7
Norton/Symantec AntiVirus	2, 3, 6, 7
Norton System Works	2, 7
CompuPic / CompuPic Pro	3, 7
Winzip, WinRAR	6
Ccleaner	3, 4
Outlook, Outlook Express	2
Internet Explorer	2, 7
RegSeeker	3, 5
Instant Messaging	2
Installing Software after Reformatting	5
Deleting Files; Wiping	6

ADVISORS

Name	Phone	Hours
[1] Fred Shelton	(253) 752-0120	Variable
[2] Bob Henkel	(253) 537-6732	8A-8P any day
[3] Tom Stepanek	(253) 922-7939	7-9P Mon-Fri
[4] Carl Tenning	(206) 824-3843	6-9P Mon-Fri
[5] Oclad Wesley	(253) 212-0352	6-9P
[6] Bob Thomson	(253) 752-5582	Variable
[7] Ray Mills	(360) 692-7568	6-9P Mon-Sat

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

Please print or type. Date:_____ Sponsored by:_____

Member's Name:_____

Address:_____

City:_____ State:_____ Zipcode:_____ Plus Four _____ Country:_____

Home Phone: (____) _____ Work phone: (____) _____ E-Mail Address _____

TACOMA MEETING

When: **Mon 9 Dec 2012 -7:00 PM**
Where: SE Tacoma Community Centre
1614 99th Street E.
Tacoma, Washington

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

Future Dates: 2nd Monday of Month

TOG BOARD MEMBERS

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

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 Ave 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 Portland off-ramp and turn north to 99th Street. Some folks in the middle of Tacoma may prefer to take Portland southbound to 99th. At 99th turn west over the tracks and there you are!

TOGGLE

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

Change Service Requested

PROGRAMS

This Month's Meeting

This will be a regular monthly meeting. 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 own experiences, problems and discoveries.

Program Presentation

No formal program has been announced at prees time.