# BITS AND BYTES

**October 2012**

Newsletter of the Midland Computer Club

http://mcc.apcug.org/

**GENERAL CLUB MEETING**
**7:00 P.M.**
4th Wednesday of the month at the
Midland Community Center
2001 George St., Midland, MI

**This month's date: October 24, 2012**

**This month's topic:** Greg West, APCUG Advisor, will talk about what APCUG is and does for user groups.

**What you missed!**
At the September meeting several Board members shared some of their favorite programs.

**Upcoming Activities:** November meeting - Joe Lykowski will discuss new technology items, aka holiday gift ideas.

**Program Coordinators**

| | |
|---|---|
| Howard Lewis | lewis3ha@chartermi.net |
| Bill Tower | stressed@tir.com |

Please let Howard or Bill know of topics you would like covered at future meetings.

## President Piper's Ponderings

I formulated my thoughts for this article while in a dentist chair, having a root canal. To put the pain out of my mind, I am thinking about how nice a new computer I could buy for the same cost. Then I discover a new cap will have to be installed--there is a second, new computer down the drain. I also compare how far the technology of the dentist and medicine in general has progressed; again, like the computer industry has progressed (but at a much lower cost escalation).

Yesterday I learned some details on the recent closing of WebShots website. It was an original, free image storage site from 6-10 years ago. Then it started charging and I got away from them. I do know they were heavily used by "professional" sites, with massive amounts of picture storage. Now that they have closed, it seems that, while you can get your pictures back, all the organization (folders) are gone. If you had 100 pictures in each of 100 folders, what you got back was 10,000 pictures in random order. This goes on the heels of Kodak's closing earlier this year. So the message again is: Be wary of off-line storage, and have a backup plan for your backup. This flies in the face of all our recent Cloud storage discussions. It is sort of like our grandparents being wary of keeping money in banks.

Then today I read and heard an update about the current college student debt loans combined with the inability to find jobs for new graduates. We also see something like 46% of current grads working at jobs that don't require a college degree. Then the figure is thrown out that 40% of young people aren't even graduating from high school. What a mess in our educational system.

(continued on Page 3)

## 2012 MCC OFFICERS

| | | |
|---|---|---|
| President | Larry Piper | larryp56@chartermi.net |
| Vice Pres. | Joe Lykowski | joseph@lykowski.com |
| Treasurer | Laura Hammel | Lhammel@gmail.com |
| Membership | Gary Ensing | btiger6@gmail.com |
| Editor<br>Webmaster | Carol Picard | webbyte@yahoo.com |

### Special Interest Groups:

**PROGRAM COORDINATORS**

| | |
|---|---|
| Howard Lewis | lewis3ha@chartermi.net |
| Bill Tower | stressed@tir.com |

**BOARD MEMBER**

Shirley Salas

**PUBLICITY**

| | |
|---|---|
| Al Adams | aladams12@yahoo.com |

## Board Meeting

Thursday, November 1, 2012
7:00 PM
Chapel Lane Presbyterian Church,
5501 Jefferson Ave., Midland MI

**Useful, useless and strange (in no particular order) Web Sites** (submitted by Howard Lewis)**:**

Since this is an election year, here are some websites to help you make up your mind (if you haven't already).

http://www.democrats.org/ Democratic Party
http://www.gop.com/ Republican Party
http://www.gp.org/index.php Green Party
http://www.lp.org/ Libertarian Party
http://www.constitution-party.net/ Constitution Party
http://tinyurl.com/8m38kx8 People on the ballots
http://www.politicalresources.net/usa1.htm Political resources on the net
http://www.politics1.com/parties.htm A guide to the political parties
http://www.followthemoney.org/ Find out who is donating money
http://www.factcheck.org/ Verify if what the candidates say is true
http://www.politifact.com/ Another site for checking candidates claims
http://www.lwvmi.org/ Michigan League of Women Voters
http://www.vote411.org/ Non-partisan information on the election and it's candidates
http://votesmart.org/ Bills itself as the voters self-defense system
http://taxfoundation.org/ Tax information
http://www.taxpayer.net/ Obtain more transparency from the government
http://www.stateintegrity.org/ How transparent is your state government?

## *Membership Enrollment Form*

*NAME* ______________________________ *PHONE* ______________

*ADDRESS* ________________________________________

*CITY* ______________ *ZIP* ____________

*EMAIL ADDRESS* ________________________________

*Membership dues FAMILY ($20) STUDENT ($15) New Member ____ Renewal ____*

*Please fill out the above form and mail it along with payment of check or money order to :*

**MIDLAND COMPUTER CLUB Attn: Membership Chairman**
**1816 Bauss Ct**
**Midland, MI 48642-4023**

You may also pay for membership at a regular club meeting

***President Piper's Ponderings*** *(continued from Page 1)*

And then on Squawk Box the resident financial advisor starts throwing out comments on recent cyber attacks on the American banking system. A sequential series of attacks coming from various geographical locations -- supposedly orchestrated from a central location like Iran--has flooded every web portal at the rate of 58 Gbits/sec for 38 straight hours, probing for weaknesses. Each of us should go back and review Laura Hammel's presentation last April on disaster planning in the digital age.

Sorry for the soapbox comments, but it seems like our country needs more technology minds to help with our problems, but we are graduating and employing fewer and fewer.

*(The above comments are the opinion of the author and do not necessarily reflect the views of the Midland Computer Club.)*

## Tips, Tricks & Techniques (submitted by Howard Lewis)

### Getting Useful Information Quicker Using Google Search

Google has several ways to find certain information quickly. For example:

**To find flight information** — enter the name of the airline with the flight number (e.g., *Delta 507*)

**To check your weather** — type in **weather** followed by the zipcode or city (e.g., *weather 48640*)

**To check local movie times** — type in **movies** followed by the zipcode or city (e.g., *movies midland, mi*)

All three searches will return a search results page with information specific for the location specified. Other keywords are also useful to make your searching quicker.

### Use the Keyboard to Resize a Window

If you prefer to do things with the keyboard rather than the mouse, it is possible to resize an open window without using the mouse. To accomplish this:

> Enter the keyboard combination *Alt+Space-Bar* to open the **System Menu**
> Type the letter *m* and a double-headed pointer will appear.
> Press the appropriate arrow key of the side you wish to change and the cursor will move to that edge.
> Then repeatedly press that arrow key to increase or decrease the size of that edge.
> Press *Enter* when you are done.

For example, to make the window wider, you would use the right arrow key (or left arrow key depending on which side of the screen you have more room).

### Quickly Delete Text in Word

To delete text, many users either highlight the text with their mouse and hit **Delete** or place the cursor at the deletion point and repeatedly press **Delete** (to delete to the right of the cursor) or **Backspace** (to delete to the left of the cursor). But there are faster ways to delete text.

You can delete a whole or partial word to the left of the cursor by pressing *Ctrl+Backspace*.

To delete a whole or partial word to the right of the cursor, press *Ctrl+Delete*.

By repeatedly hitting these key combinations, you can quickly delete a group of words without your hands leaving the keyboard.

## *ARTICLE INDEX*

*Articles in this Newsletter have been obtained from APCUG with the authors' permission for publication by APCUG member groups. The Midland Computer Club has not verified the information contained in the articles nor tested procedures or hardware/software. Articles do not necessarily reflect the views of the Midland Computer Club.*

## October is National Cyber Security Awareness Month

by Ira Wilsker

Ira is a member of the Golden Triangle PC Club, an Assoc. Professor at Lamar Institute of Technology, and hosts a weekly radio talk show on computer topics on KLVI News Talk AM560. He also writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.

WEBSITES:
http://www.dhs.gov/national-cyber-security-awareness-month
http://staysafeonline.org/ncsam
http://staysafeonline.org/ncec/ (Educational information K-12 and College)
http://msisac.cisecurity.org
http://www.stopthinkconnect.org
http://www.prnewswire.com/news-releases/new-national-cyber-security-awareness-month-web-portal-offers-wealth-of-resources-to-stay-safe-online-169306026.html
http://staysafeonline.org/ncsam/events
https://www.facebook.com/staysafeonline
http://www.prweb.com/releases/cybersecuritytraining/cybersecurityconference/prweb9920629.htm
http://www.microsoft.com/security/resources/cybersecurity.aspx

*(Continued on page 5)*

*(Continued from page 4)*

Regular readers of this column are well aware that one of the most frequent topics covered is cyber security. Most computer users are blissfully unaware of the degree of cyber crime that is currently taking place, and the current threats to our computing safety. Virtually all computing devices are at substantial risk, regardless of operating system; Mac computers have recently become the targets of a large number of types of malware; Android devices, smart phones and tablets, are now being attacked at alarming rates; iOS devices (iPhones and Apple tablets) are likewise falling prey to malware attacks; Windows powered devices continue to be widely targeted due to the prominence of Microsoft operating systems (XP, Vista, Windows 7, and now Windows 8). According to Troels Oerting, the new chief of the European Union's (EU) European Cybercrime Centre (as quoted on EUobserver.com, September 17, 2012), " There is no absolute security, it is a myth." Oerting went on to describe, " ... that more than 200 billion spam emails are being sent every day and that 46 new malicious codes aimed to steal online data are being created every second. Foreign intelligence services are among the long list of culprits who increasingly use the Internet to steal data to gain inside advantages on trade. Activists, hackers and organised crime are also becoming more active."

Cyber security is a concern and a necessity at all levels. While computers and networks operated by governments, businesses, academia, and other associations and agencies have been prime targets of cyber attack, the number and rate of attacks on privately owned personal computers and smart devices has become explosively endemic. While cyber security and safety is a responsibility of all computer and smart device users, the federal government along with a variety of private and public partners has promoted "National Cyber Security Awareness Month" (NCSAM) for many years. Traditionally, the President of the United States had inaugurated NCSAM with a presidential declaration calling on everyone to be aware of cyber security, and to take all appropriate precautions to secure their digital devices from attack. During October, 2012, there will again be a national effort to encourage and promote cyber security.

This year, the lead federal agency promoting Cyber Security Awareness Month will be the Department of Homeland Security (DHS), which will be coordinating events and activities with the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). According to the DHS, this joint operation, " ... encourages Americans to ACT – Achieve Cybersecurity Together – reflecting the interconnectedness of the modern world and the responsibility each of us in securing cyberspace."

One may ask himself, "So what can I really do to help the cyber security effort?" The various agencies working together have come up with a list of actions and activities all computer and smart device users should implement. One of several behaviors encouraged by the alliance is to "STOP, THINK, CONNECT" (stopthinkconnect.org). According to the alliance, all users should: "STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems. THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's. CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer. Protect yourself and help keep the web a safer place for everyone."

There are several definitive steps that users can take to implement and improve the security of their digital devices. According to a Microsoft webpage devoted to the National Cyber Security Awareness Month (www.microsoft.com/security/resources/cybersecurity.aspx), there are six major practices that we should all accomplish in order to improve our cyber safety and security. Microsoft's first recommendation is to defend your computer by strengthening your computer's defenses, and not to be tricked into downloading malicious software. While these first recommendations may seem to be common sense for most computer users, these recommendations are also some of the least implemented. In order to defend our computers and other devices from attack, we need to keep all software (especially web browsers) up to date; install legitimate and comprehensive security software and keep it current with the latest updates

*(Continued on page 6)*

*(Continued from page 5)*

(most security publishers now push hourly or continuous updates); use and never turn off the firewall; be sure to have a hard to guess password on your router (and my urging to implement the highest level of encryption available on your wireless access point or device); and to use USB and other flash memory devices cautiously, as they have become a major vector for passing malware between computers and other devices. Microsoft also warns, "Think before you open attachments or click links in an email message, an instant message (IM), or on a social network, even if you know the sender." Much of the spam and malware being disseminated appears to come from someone we know, as their computers, instant messaging account, address books, or email accounts have been hijacked, and used to spread malware and spam to others, under the guise that it is OK because it is from someone you know. Another component of this second recommendation is to never click on links or buttons that appear in pop-up windows.

Identity theft and related financial crimes has become a huge source of revenue for cyber crooks the world over, and Microsoft covers this in its second recommendation, "Protect Sensitive Information." Microsoft warns users that before they enter any sensitive data on a website or online form, look for indications that the webpage is secure, such as the web address beginning with "https" rather than "http", and some indication from the browser that the connection is secure. Most browsers use a padlock (clearly open or closed) or some similar indication of a secure connection. Another common trick to steal personal information, such as usernames, passwords, banking and credit card information, and other personal information is commonly referred to as "Phishing", where identity thieves attempt to trick the user into disclosing personal information. Much of this phishing is by way of emails informing the user that their email account will be locked unless they respond with their username and password; apparently legimate (but false) contacts from retailers, credit card companies, banks and other institutions asking for personal credit card or bank account information; offers of riches in exchange for helping some foreign official or widow to place investments in this country; foreign lottery winnings; and a variety of other scams. One of the latest common scams is known as "ransomware", where the user's computer is locked, and a warning from the FBI or other law enforcement agency appears on the screen informing the user that unless he pays a "fine", typically $200, his computer will remain locked, and he will be prosecuted for several felonies, including possessing child pornography.

Similar requests for personal information that can be abused often arrives in instant messages or social networking postings. Another common email scam is a post apparently from a friend or relative that claims they lost their wallet, checkbook, passport, return airline tickets, and credit cards while visiting a foreign country, and are stranded unable to return home. This recognizable friend or relative then asks you to make him a loan and wire a large sum of money to him such that he can get home; of course, "I will pay you back as soon as I get home." The problem is that this is a complete fraud, and that friend or relative overseas is a name stolen from a hijacked email account or address book! Also be aware of phone calls claiming to be from Microsoft (or a recognizable computer security company) telling you that your computer is infected with a virus, and that either for free or for a fee charged to your credit card, they will remotely access your computer and clean it for you, "so please give us remote access to your computer". Not just will they not clean your computer of malware, but they will likely plant malware on your computer as well as access and steal all of your personal data and information on your machine.

Third on Microsoft's list of recommendations is to create strong passwords, and keep them secret. Passwords should be complex long phrases, consisting of upper case (capital) and lower case letters, along with numbers and symbols. These passwords should not be easy for other to guess like permutations of your name, address, phone number, kids names and birthdays; pets' names; and other information that can be easily obtained through public or online resources. It is also necessary to utilize different passwords on different websites, such that if one website is compromised, it will not adversely impact your passwords and accounts on other websites. Microsoft emphasizes that it is especially important to use different complex passwords on websites that contain your financial information, such as banking, credit card, and shopping websites.

*(Continued on page 7)*

*(Continued from page 6)*

Number four from Microsoft is "Take charge of your online safety and reputation. Discover what is on the Internet about you and periodically evaluate what you find." What others say about you online in social networking services, blogs, and even eBay user ratings can adversely impact your online reputation. It is important to both maintain a positive online reputation, and correct erroneous postings about you, but be careful not to fall into someone's trap and disclose too much personal information.

In its fifth security recommendation, Microsoft urges that users exercise care when using social networks, such as Facebook and Twitter. All of the legitimate social networking services offer "settings" or "options" where users can set and manage their privacy and security settings. Users should control who can access their private information, what private information is available, and how others can search for your information. It may often be very appropriate to block other people from viewing your information. In addition to Microsoft's suggestions, I would also add do not post information that you are out of town, on vacation, or even at a movie or at dinner, as burglars and other literal crooks read Facebook and Twitter looking for empty homes to burglarize. Turn off the GPS in your digital camera or Smartphone before taking pictures that you want to post on a social networking site, such as Facebook, or otherwise strip off the GPS information, as crooks and pedophiles have been well known to use the GPS information encoded in digital photographs posted online to locate homes, cars, valuables, and children for the purposes of victimization. An old cliché' says "Don't do anything that you would not want your grandmother to read in the newspaper," and that applies to social media postings as well.

Number six from Microsoft says, "Take extra steps to help keep kids safer online." Online safety and security must be a family effort, and incorporate some mix of guidance and monitoring. Microsoft suggests that, " (Parents) negotiate clear guidelines for web and online game use that fit your kids' maturity and your family's values. Pay attention to what kids do and who they meet online." Pedophiles and identity thieves troll chat rooms, social networking websites, blogs, and other online resources looking for potential victims. Parents and children need to be cognizant of the risks and educated in what to watch for that may indicate potential risks to children. Children must never disclose personal information to anyone, especially others who claim to be the same age and gender as the child (pedophiles often pretend to be a child in order to gain the confidence of the potential victim). Identity thieves try to gain the trust of children and trick them into disclosing private family information; residential burglars will do the same, asking the child about vacation or dinner plans; "We are going out for pizza and then a movie" tells the burglar that the house may be a good target. Children should never go to meet someone face to face that they met online, unless under the direct supervision and participation of a parent.

There are a number of National Cyber Security Awareness Month events posted online (staysafeonline.org/ncsam/events), several of which will be streamed free over the internet. There are also free materials available for parents, teachers, children, and businesses that can be used in a variety of environments for educating others (staysafeonline.org/ncsam). While October is officially National Cyber Security Awareness Month, every month should be a NCSAM. Stop, think, and connect properly, and stay safe online.

## Can QR Codes Spread Computer Viruses?

**by Bob Rankin, Ask Bob Rankin,** www.askbobrankin.com

From Rankin's June 4, 2012 newsletter, reprinted with permission

Any doubts I may have had about the viability of QR codes have evaporated. You know a new technology is catching on when malware authors start using it to snare unwary users. Read on to learn how those funny black squares can carry a nasty (and expensive) payload...

*(Continued on page 8)*

*(Continued from page 7)*

QR codes are squares of black and white patterns that encode the URLs of Web sites in a format that can be scanned and deciphered by smartphones equipped with the right apps. Instead of typing a URL into your phone's browser, you can just snap a picture of a QR code and be whisked to an ad, an informative Web page... or a malicious site that silently downloads a virus, rootkit, or trojan to your phone.

Kasperky Labs has detected two samples of malware delivered via QR codes, both targeting Android phones. One of them sends SMS messages from the infected phone to a premium-priced number; each text message costs the victim six dollars! Other types of malware can scoop up your contacts list, send spam emails in your name, and wreak other sorts of mischief. (https://www.securelist.com/en/blog/208193145/Malicious_QR_Codes_Pushing_Android_Malware) <http://bit.ly/qGXZig>

Can a QR code itself contain malware? Theoretically, yes, but it wouldn't do much. A QR code can contain only a limited amount of data: 7089 numeric characters or 4296 alphanumeric characters. You can't write much of a program in that space. But a QR code can easily take you to a malicious site.

Humans cannot tell one QR code from another, generally speaking. You have no idea where a QR code is going to take you until you scan it, and then it's too late. So it pays to be skeptical of all QR codes, while exercising some common sense.

QR codes printed in paper publications, on in-store posters, on coupons from well-known retailers, and similar places are unlikely to be malicious. But never forget the days when shrink-wrapped software packages were infected with malware at the factory by disgruntled workers.

A QR code on a Web page is more easily compromised. If a hacker can crack the site's security, he can replace a legitimate QR code with a malicious one of his own. There have already been reports of malicious QR codes showing up in spam emails. Be a bit more cautious before scanning online QR codes, and especially if they arrive in unsolicited emails.

If you notice a sticker bearing a QR code just randomly slapped up on a wall or a sign post, think twice before scanning it. On the other hand, this method of distributing malicious QR codes is so inefficient that it probably isn't used much.

Malicious QR codes can be countered by anti-malware apps that translate a QR code into a URL and allow a user to review it in plain text before deciding whether to let the Web page be fetched. Better still, look for an app that prescreens all URLs against a blacklist of known attack sites. Norton Snap is one such app that works on both Android and iOS devices. In addition, Lookout Mobile Security and the McAfee Antivirus & Security app (both for Android) claim to protect you from malicious URLs in QR codes.

On a semi-related note, I should mention that Microsoft has invented its own version of QR codes, presumably to inject a little more confusion into the world of computing. Microsoft Tag barcodes are similar to QR codes, but different. Some QR code readers can understand Tags, and some Tag readers can understand QR codes. But not all of the code reader apps do both. Hopefully, a unified qr/barcode/tag standard will evolve in our lifetime, and malware authors won't have to work so hard to scam smartphone users who scan random codes.

Malicious QR codes are still rare, but if they work you can be sure that many more will appear quite rapidly. It's better to be on your guard now than after you scan the wrong QR Code.

## Create Safe Passwords

By Sandy Berger, CompuKISS, www.compukiss.com, sandy (at) compukiss.com

Using passwords correctly is one of the best ways to protect yourself and your computer. If you use the same password for everything, read this article and make some changes as soon as possible.

Just about everyone can relate to the frustration of trying to make an online purchase or to access information at a website and not being able to remember your user name and password. If you are over 50 and have that problem, you may attribute it to senior memory loss. That, however, is not really the problem. Even younger folks forget passwords.  It is because so many websites and web services require passwords. When written down, my list of passwords spans 12 sheets of double-column letter-sized paper.

Obviously if you use a different password for each website, you will have pages of passwords, as well. Yet, if you're like many others, you may use the same password for all of your websites A recent Washington Post survey show that 30% of respondents said they use the same password for different websites including banking, social networking and shopping sites. This is a very risky practice.
We are constantly bombarded with news about stolen passwords. Recently 6 million passwords were stolen from LinkedIn. Recently more than 400,000 email addresses and passwords were stolen from Yahoo and posted online. It is obvious that if people use the same password at numerous websites, it was only time before hackers would use those passwords to try to access different websites.
BestBuy recently confirmed that hackers are using credentials stolen from other sites to make purchases at their online retail site. The same thing is happening at other retail and banking sites.

So the first rule of thumb is to use unique passwords for any e-commerce or banking websites. The second rule is to never use commonly used passwords. What are the most common? Although different research on this produces different results, several passwords are always in the top 25 most common. If you think you are being unique by choosing the word "password", you are wrong. It is usually the most commonly used password choice. This is often followed by 1234, 12345, 123456, 1234567, 111111, 123abc, and querty. Anyone who uses "letmein" as a password has many like-minded friends. It is usually on the top password lists along with other simple words like baseball, football, michael, jennifer, and monkey. Seems like everyone is a dreamer as indicated by other popular passwords like harley, mustang, master, and superman.

It is also a known fact that hackers can use words from a dictionary to perform an automated attack to "guess" your password. So you don't want to use plain words, even in combination. Hackers now also use rainbow tables which are alphanumeric combinations of words and numbers. They also have common substitutions included. So using a zero instead of the letter "o" or an eight instead of the letter "B" is not always enough to keep your passwords safe. Some of these tables also have symbols, but using a password with one or more symbols is still much safer than one without any symbols.

A really safe password will use a combination of uppercase and lowercase letters, numbers, and symbols that do not spell out any words. The length of the password is also very important. To give you an example of that, let's consider a password that includes letters and numbers, but no upper and lower case combinations and no symbols. If the password has six characters there are 2.25 billion possible combinations. A ten character password will have 3.76 quadrillion possible combinations. Every time you add a character, you make the password exponentially more difficult to break.

*(Continued on page 10)*

*(Continued from page 9)*

If all this makes your head spin, remember that you can use simple passwords at websites that require passwords, but have none of your personal information. These sites usually also require an email address. So if you open a Gmail or other email account and use that specific email address only for this type of website, you don't have to worry about compromising your security.

You should, however, be very careful with passwords for banking and e-commerce websites where your personal information and/or credit card numbers are stored. Use strong passwords for these sites and have a different password for each site.

## Debunking Some Common Myths

Author: Mindi McDowell
Security Tip (ST06-002), US-CERT, 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, neither of these elements are guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.

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

Truth: Vendors may release updated versions of software to address problems or fix vulnerabilities (see Understanding Patches for more information 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 attacker's opinion. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other people (see Understanding Denial-of-Service Attacks 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).

*(Continued on page 11)*

*(Continued from page 10)*

- 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).

## The Google Redirect Virus

By Penny Cano, member and instructor for the Dumb & Dumber Workshops, Cajun Clickers Computer Club, LA, July 2012 issue, Cajun Clickers Computer News
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 malware-removal 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 that 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

*(Continued on page 12)*

*(Continued from page 11)*

forward the website or link to all their friends. This in turn gets forwarded and re-search 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.

## Hotel Wi-Fi Networks Installing Malware

By Sandy Berger, CompuKISS, www.compukiss.com, sandy (at) compukiss.com

If you are traveling this year, there is a new hacking scheme that you should be aware of. The Federal Bureau of Investigation is warning travelers to watch out for malware that comes through hotel Internet connections.

Here’s how it works. When you get to the hotel and connect to the Internet through their wireless or wired Internet connection, you get a pop-up notifying you that you must update your Java in order to have the connection work. When you give your approval, malware is installed on your computer giving the hackers access to your personal information. The malware also serves third-party advertisements to infected computers.

*(Continued on page 13)*

*(Continued from page 12)*

Bloomberg has recently reported that Chinese hackers have stolen private data from as many as 760 firms by hacking into the iBahn, a broadband and entertainment service that offered to guests of hotel chains such as Marriott International Inc.

The advice offered by the FBI's Internet Crime Complaint Center (ISC3) includes:

- Carry out all software updates before traveling.
- Checking the author or digital certificate of any prompted update to see if it corresponds to the software vendor.
- Download software updates direct from the vendor's website.

I recommend skipping any software updates that you are offered when traveling and using an encrypted connection for handling email when you are on the road. The way to do this depends on how you access your email when you travel.

Gmail is secure since it is encrypted. Other email, however, may not be encrypted. For instance, Time Warner's Road Runner Web Mail that you can use when you travel encrypts your user name and password, but not your email itself. Other services may be different. You will want to investigate the service you are using. If you are not sure if your email is encrypted, you can use a free service called Mail2Web at www.mail2web.com. To use it you simply click on "Secure Login" then put in your email address and password. (Make sure you don't just click "Check Mail" which gives you an unencrypted connection.)

If you are not traveling, you still need to keep your guard up. I recently received a very real-looking email that was supposed to be from Order-update@amazon.com. Since I often make purchases at Amazon, this piqued my interest. The email said that my Amazon order had been successfully canceled and gave a link to the order in question as well as to Amazon's website. I didn't want any orders cancelled, so I read the entire email. Then I hovered my mouse over the two links that supposedly went to Amazon and found that they went to some other website. (This is a great way to check the links in an email. Just remember that you only put your mouse over the link rather than actually clicking on it).

Remember that if you come across these or any other suspected hacking or phishing schemes, you can report them to the FBI's Internet Crime Complaint Center (ISC3) at www.ic3.gov. This website also has great information and alerts for the latest scams.

You will be amazed by the sheer number of crime schemes that are floating around the Internet. There is everything from Ponzi and Pyramid schemes to Internet Extortion. So check out this website. Just as in real life, you have to be aware of the pitfalls to keep yourself safe. It's always good to follow the advice given by Sergeant Phil Esterhaus in Hill Street Blues. "Let's be careful out there."

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

by Leo Notenboom, http://articlesbyleo.com/, www.ask-leo.com

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

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

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

*(Continued on page 14)*

*(Continued from page 13)*

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

But even then it’s not at all complete.

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

Still feel like posting those party photos?

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

It happens all the time.

It happens to those who have the freedom of speech mentality: “I should be able to post and say and do whatever I want.”
Absolutely. You should be able to. Go ahead. Post and say what you like. In most countries you have the right to say pretty much whatever you like. Just remember that freedom of speech does not mean freedom from consequences.

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

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

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

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

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

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

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

It’s common to want to have Google remove you from their index. There are two problems: 1. They won’t. Google is a search engine, and their “job” is to report what can be found on other sites on the internet. They’re simply showing you what’s out there, but what’s out there is not in their control. 2. Google is not the only game in town. Google is perhaps the most popular, but there are literally thousands of search

*(Continued on page 15)*

*(Continued from page 14)*

engines on the internet. From Bing to Yahoo, to many medium and smaller niche search engines, there are more search engines than you could ever count. Even if you could get Google to remove you from their results, which you cannot, you'd still be faced with all those other search engines that might also be returning the same results that show your information on the internet.

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

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

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

Not so fast.

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

So what can you do?

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

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

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

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

## How to Keep Data on Your Laptop Secure

by Leo Notenboom, http://articlesbyleo.com/, www.ask-leo.com

Understandably, the biggest fear most people have about losing their laptops, is not actually centered on the laptop itself. The biggest fear is having sensitive information end up in the wrong hands. Most can handle the material loss, but all that data in the hands of malicious individuals is scary!

There is a solution which is secure, fairly easy, and best of all, free.

Of course, you can just encrypt all of your data with different archiving tools which allow you to assign each file a password. The problem associated with this method is that these passwords are often easy to

*(Continued on page 16)*

*(Continued from page 15)*

crack and this process is a pretty big hassle. Instead, consider the free, open source program called TrueCrypt. This software provides industrial-strength encryption while being very easy to use.

TrueCrypt can be used many ways, but the two most common are:

- Encrypting an entire disk such as a floppy disc, USB thumb drive, or entire hard disk.
- Creating an encrypted virtual disk container or “volume”.

The latter approach is the easiest for copying entire containers from machine to machine.

Truecrypt simply mounts the encrypted virtual disk so that it appears as an additional drive on your laptop. You enter the pass phrase once when you mount the virtual drive and from then on everything read from there is decrypted and everything written there is encrypted automatically.

For example, you can have Truecrypt generate a drive called C:/windows/secritstuff. Then, if someone were to look at that file directly, they’d see nothing but random gibberish as a result of the encryption. When you use TrueCrypt to mount the virtual drive (such as selecting the drive letter “P”) then that drive – P: – would look just like any other disk on the machine. Every file placed in the drive is encrypted, so encryption becomes as easy as simply moving your sensitive files into that drive. While the encrypted drive is mounted, the contents can be accessed in their unencrypted form by any program you wish to use to access them.

The trick is to set the drive so that it never mounts automatically. As your machine boots up the virtual drive would be nowhere to be found. The corresponding file c:/windows/secritstuff would be visible only as encrypted gibberish. Someone trying to access your files would only find that.

The data is not accessible until you use the TrueCrypt software to select the file at c:/windows/secritstuff, choose the drive to mount it as P: and type the correct pass phrase.

TrueCrypt also supports a variety of high-powered encryption algorithms. TrueCrypt documentation is obviously targeting the overly paranoid, including directions on how to use “plausible deniability” if a thief ever forced you to give them your password. Let’s all hope that’s just an extreme of little probability for most of us.

Here are a few warnings:

- The passphrase or word you use is going to be the weakest link. Encryption is still easily cracked if you use a bad password. If you choose a passphrase which is easy or obvious, then a dictionary attack can always be mounted on your machine to unlock the encrypted volume quickly.
- Having an encrypted volume is useless if your important files are also elsewhere in unencrypted form on your machine.
- Be sure to have secure backups which are updated regularly. It’s preferable to keep these unencrypted, but secure, just in case you lose the encrypted volume or happen to forget the password. Without your password, the data cannot be recovered.
- Understand that files are never 100% secure. All encryption can theoretically get hacked. The reason for encryption is to make the effort and cost of hacking the files so astronomical that it is simply impractical.

Data encryption is a very important aspect of an overall security strategy. Keeping your important files secure doesn’t require much more than forethought and planning. With spyware and viruses running rampant, not to mention possible theft, there is really no excuse not to take the little bit of time and save yourself a lot of grief should the unthinkable happen.

## Why You Might be Sending Spam

by Leo Notenboom, http://articlesbyleo.com/, www.ask-leo.com

As you probably already know there's a lot of spam – unsolicited and unwanted email – flying around on the internet these days. Some estimates say that well over 80 to 90 percent of all email is, in fact, spam.

That's bad enough, but when someone tells you that it looks like spam is being sent from your email address … well, then it gets personal.

The most common causes of spam being sent from your email address have nothing at all do with your computer.

In other words, while it's possible, it's not necessarily because your computer has a virus.

Your email account may have been hacked.

Actual account theft and hacking has risen dramatically in recent months.

The scenario is very simple: a hacker learns your password and logs in to your email account. Once in he starts using it to send spam. The hacker never even has to come close to your computer, and in fact often performs his activities from overseas.

The question, of course, is how did he learn your password?
Unfortunately there are many ways: perhaps your password is easy to guess, perhaps your so-called "secret questions" are easy to guess, perhaps you logged in to a public computer in a library or other public location that itself was compromised with malware or a keyloggers.

Perhaps you used your computer in an open Wifi hotspot, and the connection to your mail service was not encrypted and a nearby hacker was monitoring and saw your login information.

Perhaps you responded to a phishing attempt – an attempt to fool you into providing the hacker with your email login information including your password.

Perhaps you told a friend or family member who wasn't quite as careful about keeping it private as you are.

And, of course, there could indeed be malware on your machine. In my experience that's significantly less likely in this case than most of the possibilities above.

There could be absolutely nothing wrong.
One of the most frustrating aspects of this scenario is that it's very possible that there's nothing wrong at all.

The issue is simply this: it's trivially easy to make email look like it's from someone that it is not. So called "From spoofing" is used by spammers to hide their own identity. They pick email addresses at random – often email addresses to who they are also sending spam – and use those as the fake sender of the email.

In other words you may have had absolutely nothing do to with email that lists you as the sender.

And there's nothing you can do about it.

*(Continued on page 18)*

*(Continued from page 17)*

Before you assume this is the case, though, look at who's getting spam email "from" you.
If they are mostly people you know, then it's very likely that your email account has been hacked and your address book or contact list is being spammed. You need to take action right away by changing your email password.

In fact, you need to more than just change the password – you need to change or verify all the information in your account that could be used to recover your password. While the hacker had access to your account he had access to that too, and could have changed it or written it down so that he can easily come back and hack your account again.

You can certainly run up-to-date anti-malware tools on your computer if you like – you should be running those regularly anyway – but as we've seen, in all probability your computer wasn't involved.

## VIPRE

Presented at the Southwest Technology & Computer Conference, San Diego, by Dodi Glenn (with Kathy Wattman, Vipre Product Manager)
By Susan Kennedy, Member, TUGNET, California, www.tugnet.org /newsletter (at) tugnet.org

Dodi Glenn, Product Manager for GFI, started by asking us "What is malware? What dangers are out there?"  Malware includes adware, bots, dialer programs, keyloggers, rogue anti-virus programs, rootkits, and spyware along with the usual viruses, worms and Trojans. He described malware as having "gone wild" with a huge increase in recent years. The purpose is no longer to damage people's computers; the motive today is almost 100% financial. Cyber criminals want access to your computer, your passwords and account information, and thus to your money! Besides stealing from your accounts directly, crooks make fortunes in selling credit card information. Much of this criminal activity originates in Russia and China.

Top threats include various forms of Java script. Some of the threats he named are the System Restore Rogue and S.M.A.R.T. Repair that may harm your hard disk drive.

A few threats created by governments have escaped into the world at large. We probably all know of the Stuxnet virus, believed to have been created to wreak havoc with Iran's nuclear program, but coming along today is Duqu, first spotted in September 2011.  Another is Flame, a program developed by the CIA, NSA and Israeli military, to attack nukes in the Middle East. For those of you who are fluent in high-level "geek-speak," GFI produced a video (33 minutes) on their analysis of Flame at http://vimeo.com/44382073; it's pretty heavy on the technical stuff.

Another type of threat involves social engineering, and many of these come out of India. One example spoofs Microsoft's tech support center, where a person calls on the telephone to tell you of a problem with your computer that he can fix if you just allow him remote access.  The Better Business Bureau published an article you can read at http://tinyurl.com/7noulky. You can also see videos on this threat on YouTube by searching for Microsoft Service Support Center.

Where does this malware come from? Today it's mostly social networking (e.g., Facebook), online games, and email or through "portals" you access either for games or chatting in forums. Malware (including spam) gets into your email through hacked web sites you visit, instant messages (such as posting on Facebook), and what are known as "exploits" in valid programs such as PDF, Java script, and Flash Player.

*(Continued on page 19)*

*(Continued from page 18)*

One threat few recognize is the "lost" flash drive. If you find a flash drive dropped in a parking lot or lying on a library table, for example, the natural instinct is to plug it in to a) see if the owner's name is available or b) just to see what might be on it. Don't do it! That drive may have been left intentionally because it was deliberately infected with malware (such as a keylogger or remote dialer) that will infect your computer when you try to access the info.

Dodi then described the steps one should take if your computer becomes infected or you suspect it may be.

- Be sure you have a good up-to-date antivirus program on all machines before you access the internet.
- Scan all your machines if you are on a network.
- If you discover a worm or virus on one machine, unplug it from your network.
- Get VIPRE Rescue from http://live.sunbeltsoftware.com or http://live.vipreantivirus.com; then restart your machine in Safe Mode and run the Rescue program. When the report displays, any entries in red are serious threats that must be removed.

Some other good anti-malware programs that Dodi recommends (many free) are

- Malware Bytes (www.malwarebytes.org)
- Super Anti-Spyware (www.superantispyware.com)
- TDSS Killer (www.super.kaspersky.com/)
- ComboFix (www.bleepingcomputer.com/download/anti-virus/combofix) and
- HijackThis (from any of several sites such as www.majorgeeks.com or www.filehippo.com.)

How can you prevent these threats from getting to your computer?

- Keep Adobe Flash Player and Java updated.
- Disable Java scripts from running in Adobe.
- Disable the function that lets your browser open PDF files automatically.
- Keep your operating system patched and updated.
- Use a reliable anti-virus program or internet security suite.

Some other tips Dodi offered include:

- Don't click links that you find in emails or on web sites; or at least do so with great caution.
- Be very wary of attachments to emails, even from people you know. The bad guys may have "spoofed" your friend's email address and sent you malware.
- Use a "site advisor" such as Web of Trust or MacAfee's Site Advisor. These program add-ons check web sites to see if they are safe and secure for you to visit. Web of Trust (WOT) (www.mywot.com) is one that works in all browsers. It is community driven; that is, it is run by its users. When you are checking a web site, a red circle means the web site is infected.
- Watch your mobile devices (tablets, smart phones, ebook readers) as carefully as your main computer. "Lookout" and VIPRE Mobile for Android are free programs for this. VIPRE Android also backs up your contacts and has a locator should you misplace your phone. (Kindle readers run on Android, but VIPRE Mobile is currently restricted by Amazon.)

A new threat is those ubiquitous QR codes that are popping up everywhere. The Norton security program warns of bad QR codes.

Following these tips will not protect you 100%-nothing can, but they will go a long way to keep your internet experience safe.