TOGGLE

THE MICROCOMPUTER TURN (ON)

MONTHLY NEWSLETTER FOR TACOMA-SEATTLE AREA MICROCOMPUTER USERS

Volume 31 Number 9 February 2011 Issue #333

IN THIS ISSUE

New Malware

A new kind of malware emerging in October 2010 is disguising itself as disk utilities. VIPRE, a valid malware detector has detected the following rogue disk utilities:

HDDDiagnostic, HDDRepair, HDDRescue and HDDPlus
FastDisk
GoodMemory
WindowsSystemOptimizator
DiskOK
Palladium
MemoryFixer
HDDFix

Samples of what to watch out for will be demonstrated at the February meeting.

UPDATE

Communications

In *Remove Malware From Your Computer or Face the Dire Consequences* the author discusses the threat of current malware programs and suggests what you can do about that threat.

In *Analyzing My Web Page Visitors* Carl Tenning discusses in detail some of the reports he recieves as a web site operator and how he manipulates the information to make it useful to him.

In *Make Yourself Invisible to Wi-Fi Hackers* Steve Bass discusses a couple of new programs that seem to provide protection to you while you surf the net at a price. Take a look.

In *Search Engine Optimization or SEO* the author discusses how search engines analyze information on the net and finds what you are looking for.

In *Do You Know the Difference Between http and https?* the author starts out be saying:"The main difference between http:// and https:// is: It's all about keeping you secure." I The main difference between http:// and https:// is: It's all about keeping you secure. If a site is not secure it is possible for someone to eavesdrop on your visit to the site. If you are going to enter confidential information to a site check to see if it is secure or not.

In *Along Memory Lane Via You Tube - Part One* the author discusses using various software choices to download movie and music files from the Internet.

In *Along Memory Lane Via YouTube - Part Two* the author goes on to discuss how to improve the quality of the files that you have downloaded in Part One.

In *6 Simple Rules to Fight Phishing* the easy steps to take are listed. There is even a ''Fight Phishing'' test offered.

Operating System

In *The Extremely Useful Control Panel* author Sandy Berger says you can ''...use a computer without changing any settings. However, at a certain point you will want to correct a setting, uninstall a program, change the way your mouse works, or add another user. All of these functions and many more are found in the Windows Control Panel.'' Read the article and find out more.

Hardware

In *Variations On a Theme of Flash Drives.* the author discusses the most recent products of this type and their usefulness enhanced by their sturdiness and portability. Worth a look.

In *Bigger capacity Computer Hard Drives are here* the author says: ''Hitachi just announced the Deskstar internal hard drive kit which hits the 3TB mark easily and somehow skirts the 2.2TB limit placed on its predecessors by Windows XP 32-bit systems.'' If you are in the market for such a drive you may be in for some ''sticker shock.''

COMMUNICATIONS NOTES & TIPS

Remove Malware From Your Computer or Face the Dire Consequences

by Ira Wilsker

For the past few weeks I have been inundated with calls, emails, and personal visits from frustrated people who have computers badly infected with malware. All of them had popular brands of free or commercial antivirus software installed which, not surprisingly, was penetrated by the vector carrying the malware. The two most common sources of the difficult to cure infections are purloined websites and contaminated email messages. To a lesser, but not unusual extent, some of the computers I cleaned were contaminated by instant messages, posts on social networking sites, and some were carried on contaminated USB flash drives.

In earlier columns, I explained that much of the new crop of malware circulating rapidly around the internet, by some accounts as many as 50,000 new threats a day, are explicitly written to penetrate contemporary antivirus software. Some recent studies showed that only about 45% of the newly released malware is even detected by the major antivirus products, allowing as much as 55% of the new malware to penetrate its defenses. I also write columns about how to protect a computer from dangerous websites using any of the several link scanner utilities (mostly free) from several security companies including AVG, Threatfire, Trend Micro, and McAfee. If any one of these utilities had been used prior to the malware infection, the user would not likely have been infected. Some of the new versions of the comprehensive internet security suites provide some protection against infestation from contaminated social network sites and USB flash drives; most of the security suites provide some protection from email borne malware, but protection from the very newest threats is often beyond the capability of many products for a period ranging from just a few hours to several days, depending on how fast the security company can detect, identify, dissect, and come up with a cure. It is then up to the user to be sure to download and install the updated signature files for his security software, unless he is using one of the few ''cloud based'' security products that do not require frequent updating (such as Immunet and Panda's CloudAntivirus).

If your security software provides for automated updates, set it to update as frequently as possible; if it requires manual updates (as do several of the free security utilities), run the update feature every hour or two. One user whose computer I recently cleaned could not understand how his computer became infected because he had one of the best free antivirus utilities installed and he updates it every week or two, whenever he thinks of it. In reality, he had no protection from the hundreds of thousands of new threats that were circulating since his last infrequent update, and it was several of these new threats that nailed his inadequately updated computer.

Just remember that antivirus and other antimalware software is like a newspaper; the newspaper in the driveway this morning is really yesterday's news; the antivirus update that you ran this morning is yesterday's malware signatures, and be totally cognizant that you may have little or no protection from the thousands of new threats that evolved or were otherwise created and released since your security software was updated.

Much of the new crop of malware does not just penetrate malware defenses provided by security software, but it also invisibly kills or otherwise neutralizes the security software, usually leaving the icon running in the system tray, even appearing to update regularly. Since the user sees the icon in place, and sees the update notices, he blissfully believes that he is protected from malware, but not just is he no longer protected, but some of the malware ''phones home'' and tells other miscreants that this computer is available and vulnerable; that is expressly why it is usually necessary to totally reinstall the security software on the computer after malware is annihilated. This now unprotected computer may then be hijacked as a ''zombie'' to send spam email, or launch cyber attacks against other computers. Keyloggers may be installed to steal usernames and passwords, as well as credit and banking information, and sold to identity thieves. Personal information, address books, spreadsheets, tax information, and personal documents may be read and distributed by cyber crooks for their own nefarious purposes.

Businesses may find bank accounts drained, merchandise shipped to phantom recipients, trade and client secrets stolen, and become the victim of industrial espionage; all because they did not adequately protect themselves from malware attack.

If the user with the contaminated computer can get online, it is often easy to kill the malware, unless the malware protects itself by restricting access to malware removal tools and websites. Popular malware detection and removal tools are the free versions of Malwarebytes (***malwarebytes.org***), a-squared Free (***emsisoft.com/free***), and SUPERAntispyware (superantispyware.com). If any of these can be downloaded, updated, and run, they will likely detect and remove the malware. A common problem is that malware prevents access to these websites, as well as free online scanners such as TrendMicro's Housecall (***housecall.antivirus.com***). Many malware products insert items in the computer's registry that prevents the installed antimalware software from running. One common example is the excellent Malwarebytes, which has an executable filename of ***mbam.exe;*** some of the malware does not let mbam.exe load and run. In one case, where Malwarebytes had already been installed on the computer, I simply renamed mbam.exe to another name (***killmalware79.exe***), and it ran and killed the malware that was controlling the computer.

All too often, since the computer has been totally hijacked and placed under the complete control of the malware that is infecting it, it is nearly impossible to download any antimalware

software or to access the online antimalware scanners, as well as even run the software that is already on the computer. In these difficult cases it is necessary to go to ''plan B'' to clean the computer.

I carry a USB flash drive attached to my car keychain. On it I carry the portable versions of the three antimalware utilities discussed above.

a-squared Free has a version available for free download that is kept updated, and intended to be installed to a USB flash drive, and run from the USB drive without the need to install it on the computer. This program is called ***a-squared Emergency USB Files***, and can be downloaded from ***download1.emsisoft.com/a2usb.zip***. This file can be uncompressed and extracted to the flash drive, and run directly from it by clicking on the executable file ***a2free.exe***. When downloaded, the signature files are fairly up to date, but as a matter of practice I manually update it from my computer regularly, such that the files on my flash drive are reasonably current. When run from the USB drive, the program is as complete as one installed on the hard drive, and has all of the same capabilities of detecting and killing malware.

I carry a second program on my USB flash drive, the free portable version of SUPERAntispyware, available for download from ***portablescanner.html***. This scanner can be installed on a flash drive or CD by following the instructions on the website. In order to prevent the program from being blocked from running by the malware that is on the infected computer, a program name will be randomly generated. This program is excellent at detecting / removing malware.

The third program I carry on my flash drive is not currently available as a portable version. It is the very popular Malwarebytes Free version, available from Malwarebytes.org. I downloaded the file to my flash drive so I can install it on the infected computer to be cleaned, if the malware will allow it. Just to be safe, as the malware will often block the update process as well, I also frequently download the manual update files to my flash drive from ***http://www.mbam.com/***. If I can install the program on the infected computer, I then run the recently downloaded ***mbam-rules.exe*** to update the program. As a matter of practice, I rename the mbam.exe to another name so the malware will not block it, and then run it to kill the malware. (See ***killmalware79.exe*** on previouys page - Ed)

I believe in redundancy, well aware that no utility is always 100% capable of detecting and removing malware, so I selectively run one of the antimalware utilities from the flash drive (usually a-squared), then another (usually SUPERAntimalware). I typically select the quick scan first to provide fast cleaning of the computer's most common places of infection, then do a deep scan, which may take a much longer time to run. If the computer appears to be cleaned, I then install and run the Malwarebytes on the target computer, leaving the Malwarebytes installed so the user can update it and rerun it as needed. After removing the malware, it is often necessary to reinstall any security software that had been present, as well as change all of the user's passwords. I also advise the user to carefully and frequently check his bank accounts and credit card websites to check for unauthorized activity.

Sometimes a computer is so badly infected that it will not run the antimalware software from the USB drive, or may not boot at all into Windows. Fortunately, there is a solution. In addition to carrying my flash drive with the antimalware software, I also carry a bootable CD with an antimalware program, as well as several other utilities. I like the free AVG Rescue CD, available for download from ***avg.com/us-en/avg-rescue-cd***. A file is also available to create a bootable USB flash drive, although many computers will not easily boot from of a flash drive, almost every computer will boot from a CD. The downloaded file is in ISO format, which must be burned to the CD by an ISO burning utility, included in most burning suites; it cannot be simply copied to the CD. If an ISO burning utility is needed, there are several good free ones that can be downloaded. Once properly burned to the CD, the CD is bootable, but into an operating system called Linux, not Windows. Simply boot the computer with the AVG Rescue CD, and run the Linux versions of AVG's very popular antivirus and antispyware against the hard drive on the Windows computer. The CD includes several other utilities including a file manager, registry editor, and recovery tool. Once the AVG antivirus and antispyware has been run from the bootable CD, and the infected computer cleaned, the CD can be removed from the drive, and the computer rebooted into Windows. If Windows runs properly, I rescan it with the utilities on my flash drive, and instruct the user to reinstall his security software.

This sounds like a lot of trouble cleaning malware off of your computer, but the risks of failing to do so may lead to a lot more trouble. The local computer stores can perform much the same tasks, but typically charge $50 to over $100 for the service. Local computer clubs often have volunteers who will perform the service for free or nominal donations on a time available basis. Be suspicious of the neighborhood self-proclaimed geek who wants to reformat your hard drive and reinstall your operating system, as you will likely lose your programs and data files, unless you have a good backup. It is rarely necessary to reformat your hard drive and reinstall your operating system to remove malware, so do not even consider doing that unless the methods above totally fail, which while possible, is unlikely.

If the user has adequate multi-level security protection in place, and practices safe computing practices, the probability of becoming a victim is small, yet since most users do not have such protections and practices in place, it is only a question of when the user will be victimized, probably sooner rather than later. It would be a good practice to download and do a frequent scan with any of the utilities mentioned above, being sure to update them before any scan. If something happens to penetrate your security, these utilities will likely detect and remove them. To quote the grizzled desk sergeant from the old TV show ''Hill Street Blues'', ''Be careful out there!''

Analyzing My Web Page Visitors

By Carl Tenning,
Tacoma Open Group For Microcomputers

Most web host providers furnish the site owner with a monthly report on visitor statistics. I have two personal web sites that I access the visitor data to (1) find out if anyone really looks at my web site, (2) what they are viewing, and (3) how they are finding the site. Here is a typical line of a daily report:

/173.164.173.236[19/Dec/2010:15:40:09 -0600]''GET /Page-5/Page-5.html HTTP/1.1" 200 3898
''http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBMQFjAA&url=http%3A%2F%2Fcruiseahome.com%2FPage-5%2FPage-5.html&rct=j&q=31%20cruiseahome%20&ei=msOTfrTLNWinQemtZz1DQ&usg=AFQjCNHK3vFj8R7eHb0pS7kD12Q2pVdtQw''
''Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10
(KHTML, like Gecko) Chrome/8.0.552.224 Safari/534.10"/

The first thing it shows is the IP address of the requesting viewer, ''173.164.173.236'' in the above example followed by the date and time. Next it shows the page or object requested by the visitor's browser, ''//Page-5/Page-5.html'' /in the above example.Embedded in the rest of the data, may be a link to the source of the request, in this case a Google inquiry, and lastly information concerning the requestor's browser.

Unfortunately, the raw data report includes every request for images, JPG and GIF, as well as favorite icon objects, (GET /favicon.ico). Since all that I am interested in is the individual page views, not every object on every page, I want to parse out of the report all requests for anything other than an HTML page. So I have written a Borland Turbo Basic program to do that:

```
REM Remove other than HTML or HTM queries
PRINT ''Analyze TRIPOD Traffic Report''
OPEN ''SEARCH.TXT''FOR INPUT AS #1 LEN=1024
OPEN ''REPORT.TXT''FOR OUTPUT AS #2
PRINT ''Removing JPG and GIF pages''
WHILE NOT EOF(1)
  LINE INPUT #1, L$
  Q=LEN(L$)
  FOR N=1 TO Q
    Q$=MID$(L$,N,1)
    IF Q$=''[`` THEN proceed
  NEXT N
GOTO getnextline
proceed:
  FOR N=1 TO Q-4
    IF MID$(L$,N,4)=''.jpg'' THEN getnextline
  NEXT N
  FOR N=1 TO Q-4
    IF MID$(L$,N,4)=''.JPG'' THEN getnextline
  NEXT N
  FOR N=1 TO Q-4
    IF MID$(L$,N,4)=''.gif'' THEN getnextline
  NEXT N
  FOR N=1 TO Q-4
    IF MID$(L$,N,4)=''.GIF'' THEN getnextline
  NEXT N
  FOR N=1 TO Q-4
    IF MID$(L$,N,4)=''.ico'' THEN getnextline
  NEXT N
  FOR N=1 TO Q-4
    IF MID$(L$,N,4)=''.ICO'' THEN getnextline
  NEXT N
  FOR N=1 TO Q-11
    IF MID$(L$,N,12)=''GET /favicon'' THEN getnextline
  NEXT N
  IF Q<256 THEN
    PRINT #2, L$
  ELSE
    PRINT #2, LEFT$(L$, 255);
    PRINT #2, RIGHT$(L$,Q-255)
  END IF
getnextline:
WEND
9000 REM Finish
9001 CLOSE #1
9002 CLOSE #2
9004 OPEN ''I'',#2,''REPORT.TXT''
blankline:
WHILE NOT EOF(2)
  LINE INPUT #2, dummy$
IF LEN(dummy$)=0 THEN blankline
INCR C
WEND
CLOSE #1
PRINT C; ''records (lines) in file REPORT.TXT''
9005 END
```

Running this program on the file shortens the report considerably.

Next, I find that 60% to 75% of the page hits come from search engines and robots instead of actual human viewers. Since I am only interested in human viewers, I want to strip out the search crawlers and robots as well. Here is a Borland Turbo Basic application I wrote for that purpose:

```
REM Search for robots
PRINT ''Analyze Traffic Report''
OPEN ''SEARCH.TXT''FOR INPUT AS #1 LEN=512
OPEN ''REPORT.TXT''FOR OUTPUT AS #2
WHILE NOT EOF(1)
    LINE INPUT #1, L$
    Q=LEN(L$)
    FOR N=1 TO Q
        Q$=MID$(L$,N,1)
        IF Q$=''[`` THEN proceed
    NEXT N
        GOTO getnextline
proceed:
   IF LEFT$(L$,LEN(K$))=K$ THEN getnextline 'sel
  IF LEFT$(L$,13)=''91.205.124.15" THEN getnextline 'Russian
      search engine
  IF LEFT$(L$,13)=''38.113.234.18" THEN getnextline 'Whois
      search engine
  IF LEFT$(L$,15)=''208.115.111.250" THEN getnextline 'Dotnet
      crawler
  IF LEFT$(L$,14)=''206.193.198.34" THEN getnextline
      'HyperEstraier
  IF LEFT$(L$,14)=''66.235.124.132" THEN getnextline 'Ask
      Crawler
  IF LEFT$(L$,12)=''65.36.241.81" THEN getnextline
      'InternetSeer.com
  IF LEFT$(L$,14)=''208.111.154.15" THEN getnextline
```

```
   ‘searchme.com
IF LEFT$(L$,14)=’’208.111.154.16" THEN getnextline
   ‘searchme.com
IF LEFT$(L$,13)=’’91.205.125.15" THEN getnextline ‘Yanga
      Bot
IF LEFT$(L$,13)=’’99.157.98.160" THEN getnextline ‘favicon
   crawler
IF LEFT$(L$,15)=’’202.171.136.146" THEN getnextline
   ‘dewdropip                              crawler
FOR N=1 TO Q-6
   IF MID$(L$,N,5)=’’slurp’’ THEN getnextline
NEXT N
FOR N=1 TO Q-4
   IF MID$(L$,N,3)=’’bot’’ THEN getnextline
NEXT N
FOR N=1 TO Q-8
   IF MID$(L$,N,7)=’’crawler’’ THEN getnextline
NEXT N
FOR N=1 TO Q-7
   IF MID$(L$,N,6)=’’Yandex’’ THEN getnextline
NEXT N
FOR N=1 TO Q-9
   IF MID$(L$,N,8)=’’GET /lib’’ THEN getnextline
NEXT N
FOR N=1 TO Q-7
   IF MID$(L$,N,6)=’’adodb_’’ THEN getnextline
NEXT N
FOR N=1 TO Q-10
   IF MID$(L$,N,9)=’’index.php’’ THEN getnextline
NEXT N
FOR N=1 TO Q-8
   IF MID$(L$,N,7)=’’phpwcms’’ THEN getnextline
NEXT N
FOR N=1 TO Q-10
   IF MID$(L$,N,9)=’’write.php’’ THEN getnextline
NEXT N
FOR N=1 TO Q-13
   IF MID$(L$,N,12)=’’//components’’ THEN getnextline
NEXT N
FOR N=1 TO Q-14
   IF MID$(L$,N,13)=’’speedy_spider’’ THEN getnextline
NEXT N
FOR N=1 TO Q-10
   IF MID$(L$,N,11)=’’Baiduspider’’ THEN getnextline
NEXT N
FOR N=1 TO Q-8
   IFMID$(L$,N,9)=’’GET /temp’’ THEN getnextline
NEXT N
FOR N=1 TO Q-7
   IFMID$(L$,N,8)=’’//assets’’ THEN getnextline
NEXT N
FOR N=1 TO Q-7
   IFMID$(L$,N,8)=’’/appserv’’ THEN getnextline
NEXT N
FOR N=1 TO Q-13
   IFMID$(L$,N,14)=’’/administrator’’ THEN getnextline
NEXT N
FOR N=1 TO Q-8
   IFMID$(L$,N,6)=’’//skin’’ THEN getnextline
NEXT N
FOR N=1 TO Q-11
   IFMID$(L$,N,12)=’’GET /include’’ THEN getnextline
NEXT N
FOR N=1 TO Q-9
   IFMID$(L$,N,10)=’’/snippets/’’ THEN getnextline
NEXT N
FOR N=1 TO Q-7
   IFMID$(L$,N,8)=’’/include’’ THEN getnextline
NEXT N
FOR N=1 TO Q-6
   IFMID$(L$,N,7)=’’start//’’ THEN getnextline
NEXT N
IF Q<256 THEN
   PRINT #2, L$
ELSE
   PRINT #2, LEFT$(L$, 255);
   PRINT #2, RIGHT$(L$,Q-255)
END IF
getnextline:
WEND
9000 REM Finish
9001 CLOSE #1
9002 CLOSE #2
9004 OPEN ‘‘I’’,#2,’’REPORT.TXT’’
blankline:
WHILE NOT EOF(2)
   LINE INPUT #2, dummy$
   IF LEN(dummy$)=0 THEN blankline
   INCR C
WEND
CLOSE #1
PRINT C; ‘‘records (lines) in file REPORT.TXT’’
9005 END
```

Running this application produces the final report I use to analyze the visitors. From this report, I first take the IP address and enter it into a web application that gives me the geographiclocation on the viewer. There are several web sites that will do this, some for free and others for a fee. The one I typically use is:

http://whatismyipaddress.com/ip-lookup

It reports your own IP address as well as any that you input.

Next, I enter this data and the other data in the daily report into a spreadsheet with column headings:

DATE, HITS, IP ADDRESS, FROM LOCATION, GET, LINK FROM

I find that many of the visitors view only one or two pages, and then disappear. Thus, to simplify the report, I only tabulate visitors that access three or more pages.

I then convert the data from the spreadsheet into an HTML file for posting on the web site. For one of my web sites this report can be viewed at:

http://cruiseahome.com/cah_viewers.html

While the whole of the above process might seen rather tedious, it becomes rather straightforward and quick after practice.

Make Yourself Invisible to Wi-Fi Hackers

by Steve Bass, as seen in The Rochester Computer Society, Monitor / November 2010

You're at Starbucks, busy working on your Facebook page. Bad news: The guy at the next table is a hacker, and he's also working on your Facebook page. Sit tight, I have a few ways for you to make yourself invisible to hackers.

One Very Serious Threat

There's a pervasive, serious Facebook and Twitter exploit that leaves you wide open to any and every hacker who can download a simple-to-use, free tool called Firesheep. It's a threat if you're using an unsecured, public Wi-Fi network, typically available at an Internet cafe, airport, hotel, or RV campground.

Last week TechBite paid subscribers got the first dispatch about this in the Extra newsletter; here's a more detailed version.

The Hacking Tool

Firesheep is an HTTP session hijacker that runs as a Firefox extension and sniffs around for cookies on any unsecured Wi-Fi connection. When you log onto Facebook, Twitter, or any of over 26 other social networking sites, your computer sets a session cookie. A person running Firesheep can read the cookie and log onto your Facebook page. Then he (okay, or she) can do anything from your Facebook account, such as send e-mail or write on a wall. Every browser is vulnerable to the exploit.

The one saving grace is that Firesheep doesn't have access to your password - that's encrypted and safe. If the hacker tries to change it from within Facebook, you'll get an e-mailed alert. But everything else on Facebook is fair game.

Download and try Firesheep if you don't believe me. There's nothing as shocking as reading a stranger's Facebook or Twitter account without their knowledge or consent. It might actually motivate you to do something to protect yourself.

Who's Behind Firesheep?

Firesheep's author has an open agenda: to force social networking sites to make the entire online session secure, just as the online banking sites do. (When you're on PayPal or your bank's site, you'll see an icon of a lock somewhere on your browser, and the link will start with ''https'' rather than just ''http.'') I think it's a dang stupid way of getting people to see the problem, but what do I know?

Are You at Risk?

Sure, but you always were: HTTP and packet sniffers are nothing new. The first one I tried was in 1999. The problem now is that any knucklehead with a modicum of computing skills can sit at Starbucks, latte in hand, and poke around your Facebook account. (I know how boring your page is, and stay away from it, but hackers aren't always so bright.)

Is it wiretapping? Kinda. Illegal? Yep. Has that stopped anyone from using Firesheep? Probably not.

Three Sure-Fire Solutions

It was difficult to find a product to defeat Firesheep that I liked and trusted. Most of the tools I tried - VPNs with proxy features - were either difficult to use or half-baked. I'll get to those in a minute. But first, three recommendations for safer Wi-Fi journeys:

Hide My Ass! Pro VPN (known in polite circles as HMA) creates an encrypted Internet connection, so Web browsing, using Skype, sending e-mail, chatting - whatever - is protected. HMA can change your IP address so you can browse anonymously (test it with WhatsMyIP Adress). The site has freebies, too a file upload hosting service, Web proxies, anonymous e-mail, and search and link anonymizers.

Hide My Ass VPN Pro Protecting me.

Tech Note: There's no bandwidth limitation; connection slowdown is minimal; and HMA's servers are mostly in the U.S., with some in Europe, Canada, and elsewhere. It met my criterion: It's easy to use. After you download and install it, one click is all you need to start it cooking. And it provides all-inclusive, non-intrusive online protection.

Of course, it's not free - but I think it's a reasonable pay-as-you-go deal at $11.50 a month. If you don't travel much, the month-to-month is appealing. If you're out and about often, it makes sense to pop for the yearly payment of $79, just a little over $6 per month.

If you have a PC at home and are on the road with your notebook, use LogMeIn Free. It's a VPN, a program that lets you securely connect to your home computer. Once you log in, you're using your home PC. Every application including the browser - is on an encrypted connection. And with a fast connection at both ends, there's minimal slowdown.

Most important, if you travel often, don't use public Wi-Fi. Bite the bullet and invest in a portable B and secure B Sprint or Verizon hotspot card. To date, there are a gazillion plans and providers, but they generally run about $40 to $60 per month with a set amount of bandwidth use. An neat alternative is Boingo, with 125,000 hotspots around the world, for about $10 per month.

Protection That Won't Cost a Dime

I tried dozens of free tools, but rejected them because they were difficult to use or didn't offer enough protection. (Well, except for LogMeIn Free.) The apps below two are Firefox add-ons - offer protection, but have limitations.

s *ForceTLS*, a Firefox add-on, changes regular links to secure links (including Firefox and Twitter). The problem is convenience: You have to add each link you want changed to its database. It's hit or miss because not all links can be made secure.

s *HTTPS Everywhere* forces about 30 sites into a secure https condition. For me, that's half-baked, because to add a site you need to learn Bulgarian (well, okay, Rulesets).

s *Hotspot Shield* (an ad-supported freebie) failed the Bass International Sniff Test. It protected me, sure, but the intrusive toolbar was littered with ads. Even if I didn't use the toolbar, the product tried to change my home page and attempted to switch my search engine. And I wasn't keen on the product's cozy relationship with advertisers. (Privacy Notice: ''third-

party ad servers or ad networks use technology to send, directly to your browser, the advertisements and links that appear on the Hotspot Shield ... [including the use of] cookies, JavaScript, or web beacons.'') No thanks.

Steve Bass is the publisher and self-appointed Chief Content Officer at TechBite; he continues to experience the cool feeling of having his own newsletter. Send him your feedback at TechBite. To sign up for TechBite's free Steve Bass Technology newsletter, head for our signup page. http://www.techbite.com/

Search Engine Optimization or SEO

by Jason Mills, Durham PC User's Club
Oshawa, Ontario

Have you ever wondered how an Internet search engine finds web pages when you do a search? After all, there are over 110 million websites on the Internet and over 25 billion web pages. So how exactly does Google find pages that match my search for ''alligator shoes''? Web pages are indexed by search engines using a few basic methods. They look at Key Words, Page Optimization, and Link Analyzing.

Spiders, or Web-Crawlers, are small applications that search engines use to examine a website. They look for keywords in the document or page that match your search. The more links you have, the more chances for these spiders to have a chance to crawl over your site, which results in a better ranking.

Ranking is the position that the web page shows up on the result page. Most people do not look past three pages to find something of interest so it's very important to get the best ranking you can. No one wants to spend his or her time looking for information. Let's put it this way, if I were selling Alligator Shoes I would want to be listed right at the top of the search engine's result page as more people are more likely to visit my website. The higher the ranking the better, as this is like free advertising for me.

Google is a bit different. Their search engine relies on relevancy. Rather than looking at just out going links to other websites, their spiders will look for incoming links as well. Remember, the more spiders that crawl over the website means better indexing. Google explains the ranking algorithm on their website:

''Traditional search engines rely heavily on how often a word appears on a web page. Google uses PageRank to examine the entire link structure of the web and determines which pages are most important. It then conducts hypertext-matching analysis to determine which pages are relevant to the specific search being conducted. By combining overall importance and query-specific relevance, Google is able to put the most relevant and reliable results first.''

Google uses PageRank (which is a mathematical formula) and hypertext-matching analysis to rank the web pages. To get good results for the PageRank factor, you need good links from related pages that point to your site. It's a simple principle: if page ''a'' links to page ''b'' then it is a recommendation from page ''a'' to page ''b''. The more links pointing to your website, the better your rankings.

The quality of the links is also important. A link that contains the keyword for which you want to have high rankings in the link text is better than five links with the text Click here. A link from a web site that has a related topic is much better than links from unrelated sites or link lists.

While the linking concept is easy to understand, the hypertext-matching analysis factor is a bit more complicated. Google explains hypertext-matching analysis as follows:

''Hypertext-Matching Analysis: Google's search engine also analyzes page content. However, instead of simply scanning for page-based text (which can be manipulated by site publishers through meta-tags), Google's technology analyzes the full content of a page and factors in fonts, subdivisions and the precise location of each word.

Google also analyzes the content of neighbouring web pages to ensure the results returned are the most relevant to a user's query.'' So basically, if my website has key words and a description for Alligator Shoes plus other pages that either relate to Shoes and/or Alligators, and other people are linking to my website, most likely I will get good ranking with Google.

For more information on how Google works: http://www.google.com/intl/en/corporate/

Do You Know the Difference Between http and https?

The main difference between http:// and https:// is: It's all about keeping you secure.

HTTP stands for Hyper Text Transfer Protocol

The S (big surprise) stands for ''Secure.'' If you visit a website or web page, and look at the address in the web browser, it will likely begin with the following: http:///.%C2%AO;; This means that the website is talking to your browser using the regular ''unsecured'' language. In other words, it is possible for someone to ''eavesdrop'' on your computer's conversation with the website. If you fill out a form on the website, someone might see the information you send to that site.

This is why you never ever enter your credit card number in an http website! But if the web address begins with https:// that basically means your computer is talking to the website in a secure code that no one can eavesdrop on.

You understand why this is so important, right?

If a website ever asks you to enter your credit card information, you should automatically look to see if the web address begins with https://. If it doesn't, you should NEVER enter sensitive information - such as a credit card number.

Source: Pete Everett, HHICC, SC

Along Memory Lane Via YouTube - Part One

By Marian Smith, a member of the Perth PCUG, Australia
Axess, Magazine of the Perth PC Users Group,
Australia, May 2010 Issue
www.perthpcug.org.au / editor (at) perthpcug.org.au

A few months ago the unthinkable happened for those of us who enjoy downloading old music, old movies and other reminders of an almost forgotten era, and then there are some modern-day enjoyments such as some TV documentaries, if they are available from YouTube, that is. Both the previous version of YouTube Downloader and RealPlayer Download stopped working simultaneously. I'm still not aware of the details, but at least the new version of 'YouTube Downloader' (which was version 2.5.3 when this catastrophe occurred) has recently been updated to version 2.5.4, which works and, just a short time ago, I found an update for RealPlayer.

You will find the updated version of YouTube Downloader available from ***http://www.youtubedownload.altervista.org*** and the you-beaut point is that is it free. If you bought 'RealPlayer', you can also update it 'free'. RealPlayer Downloader is so simple to use. When you start to play the video-clip you are after, simply move the mousepointer tab to near the top of the main ''video'' display and a (menu?) will appear, inviting you to 'Download with RealPlayer'. Just click it, and the download will happen automatically. It will be downloaded to a 'RealPlayer' folder created within your 'Videos' folder during RealPlayer's installation. When the download is finished, you can convert the file if you wish, using the included ''Convert'' function.

If you've been using the YouTube Downloader program through a few of its previous updates, you'll find this version somewhat different in a few aspects. When you find an item you want to download from YouTube, so that you can enjoy watching or listening to it at your leisure, be aware that, now, there is no URL conveniently displayed to the right of the main display. Instead, you get to it by right-clicking on the title displayed above the main part of the screen. A drop-down menu will appear which includes the word 'Properties' well down the list. Click on it and a panel will appear with the URL displayed in it. Select this URL by dragging your mouse-pointer along it. Then right-click on it and another list will appear with the word 'Copy' included in it. Click on that word, then:-

If you have YouTube Downloader pinned to your 'Start' menu, open it. One button displayed there will be labelled as ''Download options. Here is where you can set the program to simply give you the 'best available' sound and picture-quality. Now you just point to the blank 'Download' panel and the URL will be automatically 'pasted' there. That's easy to do, isn't it?

Next, click the OK button and you will see two more messages appear - one asking you if you want to show the file's URL - click OK. The next will simply indicate where the file will be saved - very useful information when you want to find it later. Click 'Save' for that option and the download will begin. You may find that the file-icon with the familiar small picture representing what you downloaded has the RealPlayer logo in one corner. If you have RealPlayer installed, you can play such files with no further attention needed.

Along Memory Lane Via YouTube - Part Two

By Marian Smith, a member of the Perth PCUG, Australia
Axess, Magazine of the Perth PC Users Group,
Australia, May 2010 Issue
www.perthpcug.org.au / editor (at) perthpcug.org.au

If you want to use Windows Media Player to look at or listen-to whatever it is you just downloaded, your file needs to be 'converted' to a different type. Here is what you do.

When your download has completed, close all windows except the main window for YouTube Downloader. Click the 'button' next to the word 'Convert,' and a drop-down list of file-types will appear. Choose the file-type you wish to convert to (for Windows Media Player it is WMV7 if it is a video-file you have just downloaded). Then go to where your original file was saved, so that you can drag its icon across to the ''Convert'' option in YouTube Downloader, and its name will appear there automatically. Click OK. A smaller panel will appear, inviting you to adjust picture quality and audio-volume. If the volume is loud and distorted, you can repeat this step over and over - moving the ''volume' slider down more. Each time you save a ''change' you will be asked if you want to replace the file. Click ''Yes'. Don't delete the original ''YouTube'' video-file until you are satisfied with the result of the latest change you have made.

When you are finished using YouTube Downloader, remember to close the program by clicking on the ''Close' icon in the top-right corner of its panel, not the OK button. If you click on the OK button, the program will attempt to repeat what it just did. Finally, it is an unfortunate reality that the new version of YouTube Downloader doesn't convert to .wav format although, strangely, it will convert from the .wav file-format. There is an alternative program available (ConvertHQ), which can handle quite a number of input file-formats including extracting audio information from a video file, but even it doesn't write a .wav file. It writes mp3 files. This program is not free, but it's worth having despite this little inconvenience.

For those of you who know something of 'audioediting,' if you have Adobe Audition 1.5, which is a virtual 'clone' of Syntrillium's ''Cool Edit Pro v2,' and can still be bought from a few online stores; you can use this program's ''Open audio from video' function to ''rip'' the audio information from the file and save it as a .wav file. I hope this information helps you to download favourite music and videos from YouTube and enjoy watching and listening to those oldies-but-goodies yet again.

6 Simple Rules Fight Phishing

As seen in ACGNJ, New Jersey Newsletter, January 2011

- Be skeptical
- Always look at link URL before clicking
- Check email headers for actual sender
- Use Google toolbar or any other anti-phishing technique/ filter
- Use a secure browser (to verify URLs)
- Report phishing

Read details of rules at ***http://bit.ly/c3XBog***

Test how safe you are from a phishing attack...

Take a ''fight phishing'' test offered by Paypal at ***https://www.paypal.com/fightphishing***. It's free and you don't need a Paypal account to take the test.

You'll be asked five simple questions, and if you can answer all of them you won't need to learn more about phishing at ***http://bit.ly/bB1llL***.

OPERATING SYSTEM NOTES & TIPS

The Extremely Useful Control Panel

by Sandy Berger, www.compukiss.com

Just as you can use a car without manipulating anything under the hood, you can also use a computer without changing any settings. However, at a certain point you will want to correct a setting, uninstall a program, change the way your mouse works, or add another user. All of these functions and many more are found in the Windows Control Panel. Don't worry; the Control Panel is much easier to navigate than the cables, wires, and mechanisms that you find under the hood of a car....and you can use the tools in the Control Panel without getting your hands dirty.

9 In geek-speak, the Control Panel is the central location for all of the Windows operating system configuration needs. In everyday terms, it the place where you can work with the many tools that Windows offers to change and customize all of the settings. The Control Panel is part of the Window's operating system's graphical interface. As such, you will find that it consists of easy-to-understand icons that are each labeled as to their function.

The Control Panel has been around since the first version of Windows. Over the years, it has morphed into a very useful set of management tools for your computer. In a car you need to know where the hood release lever is, in Windows, you need to know how to access the Control Panel. In Windows Vista and Windows 7, you can access the Control Panel by clicking on the Start button and choosing Control Panel from the right column of choices. In Windows XP, you will click Start, then choose Control Panel from the left column. If you don't see the Control Panel listed, click on Settings from the left column and then click on Control Panel.

The Control Panel is a little different in XP than it is in Vista and Windows 7. So let's talk about XP first. By default, the Windows XP Control Panel appears in what is called ''Category View''. This means that various functions have been put into Categories. Previous versions of Windows showed a list of icons, one for each function, in Windows XP, this is called the ''Classic View''. When you open the Control Panel in Windows XP if you see several categories listed you are in ''Category View''. If you see a window full of individual icons, you are in ''Classic View''. You can change the view by clicking on the words ''Switch to Classic View'' or ''Switch to Category View'' which is on the left side of the screen. Check out these two options and see which one you like. You can switch between them quite easily at any time.In Windows Vista, you have the same choices, but you may have to click on ''Control Panel Home'' on the left side of the screen before you can click on ''Classic View'' or ''Category View''.

Microsoft made some changes in the Control Panel in Windows 7. They have eliminated the name Classic View. In Windows 7 you will see the words ''View by'' on the upper right side of the screen. Click on the down arrow next to those words and you will have three views to choose from: Category, Large Icons, or Small Icons. This Icon view is really the same as the Classic View. I prefer to use the Classic or Icon view, but again, you can check out all the views and see which one you like best.

There are 45 icons in the icon view in Windows 7 and about the same number in previous versions. If you look at the Classic or Icon view, you will see that the icons have labels, like Display, Sound, Power Options, Mouse, Keyboard, User Accounts, Folder Options, and Devices and Printers. You can click on any of these icons to open a window that will allow you to adjust, correct, and/or customize the settings of these areas. Take a look around. Check out Mouse area first. When you click on the mouse icon a windows with options will appear. It will have tabs at the top. You can click on each tab to see even more options. If you have never looked at these before you will be amazed at the number of things that you can do to customize your mouse. You can switch the buttons if you are left-handed. You can speed up or slow down the double-click speed. You can change the looks of the pointer. If you are using a mouse with a scroll wheel, you can even change how the wheel behaves.

Try a few things. The only caveat here is to document the changes that you are making so you can change them back if you want to.

Each of the items in the Control Panel allows you to change the settings in your computer. Look through and open up a few of them. There are hundreds of things that you can change and/or customize in the Windows operating system. Some of the Control Panel items are very useful for everyday tasks in Windows. Be sure to take a look.

HARDWARE NOTES & TIPS

Variations On a Theme of Flash Drives

Reviewed by Fred Wasserman, Vice President, Programs
Seniors Computer Group, California
December 2009 issue, Bits and Bytes
www.scgsd.org / scgsd (at) cox.net

Flash drives have become not just interesting little toys but essential storage and data transfer tools. How many of us still use floppy disks to pass data along from one computer to another? They fit in a shirt pocket. For bigger stacks of data, a CD or DVD was necessary, but didn't fit in that shirt pocket. When flash drives came along disk media were relegated to just long-term storage or for sending data by mail. Flash drives in use is doubling every year. That means there is a real opening for manufacturers to come up with newer and better versions of the product.

I came into possession of some really interesting and useful variations on the flash drive, or thumb drive, as it is sometimes called. They both held my interest as very useful devices. One is so small and flat that it can easily be put in your wallet where it would probably make less of a bulge than a folded dollar bill. Great idea. They both come equipped to clip on to your key chain. The larger one, called ''TUFF-CLIP'' has a retractable protector on the connector end and a spring latch to connect to anything like a key ring. The little one, called ''TUFF-NTINY'' can also be attached to a key chain with the supplied lanyard. A consideration with that USB Drive is you must remember to keep the contacts facing up when connecting it to the USB port, though it won't suffer damage if you don't.

It doesn't just stop there. The TUFF-N-TINY is completely sealed, water and dust resistant, measures just 1 by = inch and is no thicker than a penny and offers 2, 4 or 8 Gb of storage for $12 to $27. Until now, the one flash drive weakness was their fragility. These are complex little devices with their delicate circuit board components within some kind of brittle plastic casing soldered to the external connector. But this Verbatim product addresses the fragility problem by design and elimination of the weakest point, the connector-to-body attachment. The connector, electronics and housing are just a single strong plastic potted circuit board.

TUFF-CLIP, the other innovative USB drive, is an extremely tough unit that is designed for extreme environments and can be clipped to backpacks, belt loops key chains or what have you.

As an added convenience, both come with the application built in to encrypt the data contents in any Windows environment. If lost or stolen, your data is safe but only if you use that capability.

Last, but in no way least, is that these USB drives are enhanced for users of the newer versions of Windows. They are Readyboost capable. You will ask, what is Readyboost? With Windows Readyboost which is available with Windows Vista and Windows 7, you can use appropriately designed USB flash memory to improve performance without having to add additional memory to the computer internals. The flash drive acts as the additional memory cache that, like your installed RAM, can be accessed faster than hard drive storage. Visualize 4- or 8-Gigabytes of additional memory to speed up your large file-intensive programs such as working on a large Photoshop image.

Verbatim, producer of the old 3 1/2 inch floppy that my first computer ran from has added these new products to its expanding line of useful media and is still making the good stuff.

Bigger capacity computer hard drives are here

By Larry Mitchum, Central Kentucky Computer Society,
CKCS Board member

It appears that the ceiling for digital hard drives has been raised yet again. Hitachi just announced the Deskstar internal hard drive kit which hits the 3TB mark easily and somehow skirts the 2.2TB limit placed on its predecessors by Windows XP 32-bit systems. This gives you massive amounts storage with the convenience of having it inside your PC instead of out on your desk where flying monkeys or ?accidentally? spilled cups of coffee can wreak havoc.

You might be wondering what a Terabyte TB is. Well 1TB= One Trillion Bytes or if the term Trillion also seems to be a foreign term, you can say that 1TB is equal to 1000 Gigabytes. This means you might be able to store your family home movies, photos, and music collection all on one hard drive.

This might be just what you needed, but please remember that you still should back up all your digital files.

The 3TB drive is available as an internal hard drive or as a desktop drive that connects via a USB 2.0 cable. These drives are not cheap. They will perform a wallet-ectomy for the better part of $250 US dollars, but that is about right when you consider that the 1TB drive costs about $50-85.

Hit up Hitachi Global Storage Technologies for more info, full specs, and a handful of photos.

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 14 Feb 2011 -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

Corporate Sponsors:

Raymond Mills & Associates
www.rm-a.com

How To get To The Meeting

For those readers still unfamiliar with how to find our meeting place we have reproduced the map showing its relationship in Tacoma to Portland 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.

New Malware

A new kind of malware emerging in October 2010 is disguising itself as disk utilities. VIPRE, a valid malware detector has detected the following rogue disk utilities:

HDDDiagnostic, HDDRepair,
HDDRescue and HDDPlus
FastDisk
GoodMemory
WindowsSystemOptimizator
DiskOK
Palladium
MemoryFixer
HDDFix

Samples of what to watch out for will be demonstrated at the February meeting.