QBITS

Quad-Cities Computer Society
Newsletter for June 2012
Volume 30, number 5
563-265-1728
www.qcs.org

QCS Notice!
All Dues Due

Membership Corner
The Dues are
NO More ***prorated***

Any New Members joining and Members renewing in the month of July **2012**, your dues are
Individual : $ 30.00
Family: $ 40.00

The QCS board has changed dues payments :
Dues are annual and due on July 1st.

On July 1, 2012

QCS Review: AVAST anti-virus software
presented by Bob Gostischa

About the presenter:
Norbert “Bob” Gostischa, after a successful career in banking, enjoys his retirement as an enthusiast IT security expert, most notably for Avast Software**.** Avast is the creator of avast! antivirus software. The avast! website has a discussion and help forum, where Bob has been helping with security-related issues since 2004, having contributed over 17,000 forum interactions. Avast! is one of the most popular antivirus softwares in the world. Avast has been making security software for over 20 years and has more than 160 million users worldwide.

by Joe Durham

AVAST! Download page
goo.gl/DKqF

Views and opinions expressed by presenters do not necessarily reflect those of the Quad-Cities Computer Society. Monthly meetings are open to the general public.

We thank NBS, the host of the QCS.org site!
ENGAGE Network Business Systems Inc. NBS

Bob, visited our club to share with us his insights about the virus maladies we encounter in everyday computing and why Avast! is the correct software solution to manage these problems and keep them at bay.

He prefaced his remarks by running a short video course of computer history, the rise of virus infections and the potential for mayhem on our computers and even the country's infrastructure in the years ahead by these software shenanigans.

The first virus was written in 1971. The first Trojan in 1986. In the year 2000 was the one of the “I Love You” virus which infected 50 million computers. He noted that originally virus creation was a prank. Now the authors are just out to get your money. Because there are so many virus types out there, the chances of catching the authors is slim. When they are apprehended, they serve their time and are at it again or in some cases hire themselves out to companies because they know how these things are made.

In 2003 Bob was looking for a replacement for Norton Antivirus because it was using too much of his system's resources. He looked around the Internet and found Avast! and has been using Avast! since then. It uses few system resources, less than 1.1%.

Bob astutely stated that there is a way to protect yourself from com-

Would You Like to receive
your *QBITS* via email?
The *QBITS* can now be produced
in Acrobat PDF format and sent to
your email box. If you desire to
have the newsletter sent to you
electronically instead of by US
Mail, notify:
Patty Lowry,
QBITS co-editor
(563) 332-8679
pattylowry@rocketmail.com

QBITS
Published monthly by the
Quad Cities Computer Society
c/o Dave Tanner
3449 - 52nd St
Moline, IL 61265
webpage: www.qcs.org
Co-editors
Joe Durham
joseph85_us@yahoo.com
Patty Lowry
pattylowry@rocketmail.com

puter virus infections: don't use the Internet or USB thumb drives. This would protect you 100 %, but then again he wondered why you would have a computer:) In the real world we must use the Internet and all that it implies.

When protecting yourself on the Internet there a several things of which all should be aware. You can have a router, this hardware protects very well from incoming Internet attacks, but it does not protect your outgoing Internet transmissions. A software firewall is needed to protect those outgoing issues.

Creating a secure password is essential. Don't use your user Id, or the name “password”, or dictionary words. Hackers can easily crack and defeat these password choices. Bob recommends a password 6 to 10 characters in length that uses Capitals, lower case characters, numbers and symbols. When you create it, write it down on a sticky note and put it on your refrigerator. If you forget it you will have to create a new one.

When using email do not forward interesting emails with the Forward button. If the content is worth the effort, copy the paragraph to the clipboard. Create a new email addressed to yourself, and then use BCC (blind carbon copy) to insert all of your friends and relatives email addresses. Then paste the content into this new email and send it on its way.

Bob noted that if we all took care in doing so, we would be able to eliminate much of the spam in our email inbox each day. Hackers and Spammers snag your other friends emails that are blithely shown on Forwarded emails. These precautions protect from 15% of Virus attacks. However 85% percent of the virus attacks reach us by browsing the Internet.

Six out of ten infections originate from “legitimate” web sites, only 1% from porn sites. On these sites the infiltration occurs via scripts, and any user interaction with the web site that we invoke.

Bob displayed a phishing attack with a Comcast company Internet example. This email looks legitimate but there were several tell tale signs that all was not correct. Below the office Comcast logo was a personal email address. The action email address was fraudulent also. By hovering your mouse over the link you could see where it was headed. The link was a Google shortcut not to an official Comcast address.

Another cautionary tale was described by Bob in those pop ups on the net which claim that your computer has been infected in its scan, and to click here to download a program to “clean” up your system. These programs are “Scareware”. In this case he stated that a scan of your system by any reputable anti-virus program would take a long time, not seconds. So he advised not to do anything when these things appear on your screen. He displayed another scenario where a “blank” screen appeared when you took action on an Internet site. It was not harmless, as there lurked within it code to send a rootkit to your computer. Also do not assume that Kid's sites are safe. In many cases these have hacker code inserted. It waits for people to activate it, unknowingly.

On Facebook, open up the privacy settings and insure that the ones active are your choice. Also think twice before posting comments, photos or videos on Facebook. Is it something you wish the world to know about you? Once things are on the Internet they are there almost forever. For his own Facebook use, Bob said he does not uses any third party applications or games. These options create too great a chance for misuse of the information they gather.

There are a few more things that you do can to protect yourself in addition to anti-virus software installation. Make an image backup of your system. Before you install new software create a restore point so that you can return to the same position if sometime goes wrong or you don't like the software. Also when you install software never accept the default installation, select the custom or advanced mode. These actions gives you more control over what the program will place on your machine. And when it has completed its installation do not select reboot now, but select reboot later. In reboot now selections the program often hides program screens that install other program portions that you didn't want or third party software that you don't need.

Another useful method is to not visit the Warez download type sites where they offer to download programs for free. These sites inherently have virus code inside. By avoiding them you avoid the infection.

All these issues that Bob described. the Avast!Free version 7 handles well. By using is real time updated Virus signature database it can help you keep ahead of the hackers. And for a virus that hasn't been identified it has a Heuristic program that analyses programs to see if it has virus code within it.

Avast! also use a Behaviour analysis to see if the computer and registry changes in your system are virus like.

Avast! 7 offers streaming real-time virus database updates. Other anti-virus companies offer daily updates, Avast! offers them in real-time. Bob offered several examples of virus attack that were caught in realtime by Avast! a day before their anti-virus competitors.

When you download the Free Avast! version 7, it will ask if you wish to be a part of the Avast! CommunityIQ. By doing so you will be sending virus feedback to their virus labs that can go out to protect the community of other Avast! users of which there are over 160 million and growing. Bob noted that Avast! checks you system on boot up before it scans your hard drive files, and this helps to catch virus and rootkits that hide in boot-up modes.

Avast! is available for PC, Mac, Linux, Android, and soon Windows 8. The Android Mobile version offers a Anti-Theft feature. You create a user only word. If you phone is stolen, it has the capacity to protect you private data by erasing every thing from the device automatically and render it a doorstop to the thief. A nice option.

Bob offered a brief review of three other free software programs that he has found useful in computing: Malware Bytes, CCleaner, and WinPratrol.

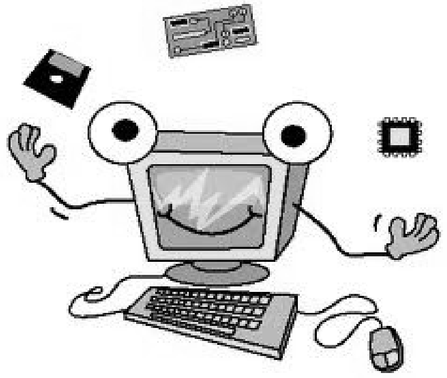
Malware Bytes helps to capture malware. Do a full scan and then quick scans there after.
www.malwarebytes.org/

Ccleaner helps manages your program removal and registry maintenance.
www.piriform.com/ccleaner/download

WinPratrol monitors changes in your system and notifies you of them.
www.winpatrol.com/

The QCS wishes to thank Bob for his fine presentation of Avast! and for raising the curtain on Internet security and Avast!'s role in helping to slay the virus dragons out here.

Beginner Bytes!



With Ted Huberts
Internet SIG Leader
s1owhand54@sbcglobal.net

by Joe Durham

The QCS inaugurates a new program feature each month at our main meeting before the presenter speaks. Each month a member of our group will discuss Beginner tips for computer and take questions about them. Ted Huberts spoke about his tip.

PASSWORD SAFETY

He asked the audience if anyone use the password, PASSWORD. Seven people in the audience raised their hands. Ted mentioned that this password name is easy to hack and dangerous to the user. He reminded us to not use dictionary words as these are easily dsicovered and missued. By using passwords of 6 characters or greater you will make them more difficult to be comprom-

--continued on next page--

ised and make it easier for you to protect your vital information on the Internet. Example: pick out the name, model of an old car and they year you owned it.

QCS User Group Benefits:

by Joe Durham

Focal Press User Groups
learn · master · create www.focalpress.com

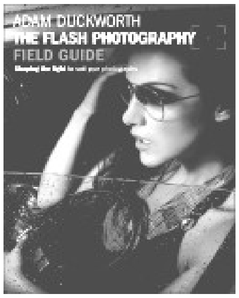
focalpress.com

Recently our group has joined several organizations that offer User Group Support and discounts. Focal Press is one of these organizations that have approved our application. Each month they offer a selections of book for our members to read for free. We can select two books each month. All they ask in return is that you submit your impressions of the book after you have read it. It will be printed in the *QBITS*, and our website and forwarded to Focal Groups.

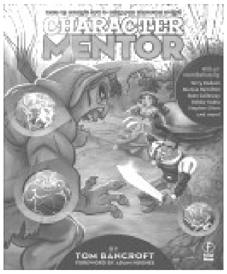
Contact me with your selection and I will get it to you, it is yours free to keep:

joseph85_us@yahoo.com
309-764-5570

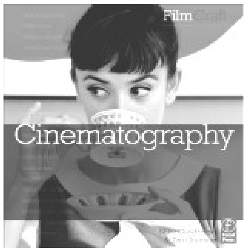
The Flash Photography Field Guide
goo.gl/Mq7MW
by Adam Duckworth



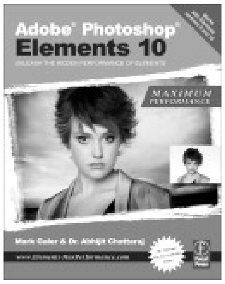
Character Mentor
goo.gl/rgxWX
by Tom Bancroft



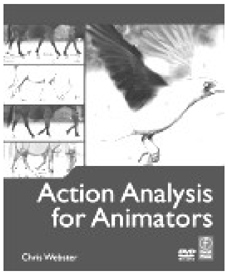
Cinematography
goo.gl/1X3L7
by Tim Grierson and
Mike Goodridge



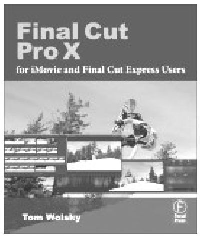
Adobe Photoshop Elements 10
goo.gl/wBfFi
by Mark Galer and
Abhijit Chattaraj



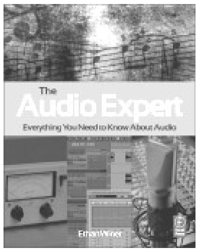
Action Analysis for Animators
goo.gl/laEAw
by Chris Webster



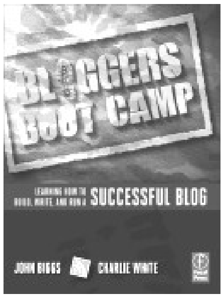
Fine Cut Pro X
goo.gl/agXRg
by Tom Wolsky



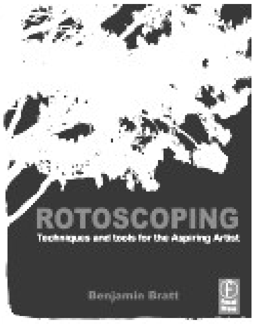
The Audio Expert
goo.gl/MeZmw
by Ethan Winer



Bloggers Boot Camp
goo.gl/Cck2U
by Charles White and John Biggs



Rotoscoping
goo.gl/0UTDE
by Benjamin Bratt



FBI: Hundreds of Thousands of Computers May Lose Internet on July 9

By Ira Wilsker

WEBSITES:
FBI
goo.gl/1P2rL
goo.gl/fl6Mw
www.dcwg.org
DETECT IF COMPUTER IS AT RISK
www.dcwg.org/detect
Yahoo
goo.gl/dkU2y
Gizmo
goo.gl/8P47n
FBI
goo.gl/2rMIF
https://en.wikipedia.org/wiki/Domain_Name_System
FIND FASTEST FREE DNS
https://code.google.com/p/namebench
HOW TO RESET DNS ON ANY OPERATING SYSTEM
https://use.opendns.com
HOW TO RESET DNS ON ANY OPERATING SYSTEM
https://developers.google.com/speed/public-dns/docs/using

In case you have not heard the news, on July 9, 2012, hundreds of thousands of computers will lose access to the Internet. This is not some hoax or urban legend, but a fact announced by the FBI. Following the arrest of an Estonian hacker group which had made millions of dollars from a fraud scheme that infected millions of computers worldwide with a "DNS Changer" malware that redirected legitimate commercial transactions to a series of scam websites. These cyber crooks created a sham company called "Rove Digital" to receive the revenues of the scam. DNS is an acronym for a Domain Name Server, which serves somewhat like an Internet phone book, which converts web addresses, also known as domain names (ie. www.theexaminer.com), into an IP (Internet Protocol) address (theexaminer.com is really 50.116.108.205). By changing the Domain Name Server accessed by an infected computer, it is like replacing an authentic phonebook with a purloined one that has the correct names, but intentionally different phone numbers. Dialing a correct phone number will intentionally connect you to someone who pretends to be the person whom you called, and that person is a crook; this is what the DNS Changer malware does to an infected computer. As many as 500,000 American computers may have been infected by this DNS Changer malware, as were an estimated 4 million other computers around the world. In addition to modifying the computer's DNS, the malware also made the infected computers vulnerable to a variety of other malware. The rogue servers were hosted in Estonia, New York, and Chicago.

This scam was very lucrative to the Estonian hackers who made an estimated $14 million in illicit fees. According to the FBI, this cyber-gang started infecting computers with the DNS Changer malware in 2007, successfully infiltrating millions of computers owned by individuals, businesses, schools and colleges, and government agencies, including NASA. The malware was able to penetrate many of the anti-virus products in use, and prevented the installed antivirus and operating system software from updating, which would have likely enabled the antivirus software to detect and kill the DNS Changer. Since the security software would not be updated, there would be no protection from the thousands of new viruses, worms, and Trojans that appear every day, which allowed those computers to become infected with countless additional malware programs and other threats. According to the FBI, “They were organized and operating as a traditional business but profiting illegally as the result of the malware. There was a level of complexity here that we haven’t seen before.” Since DNS Changer redirected the unsuspecting victims to rogue Internet servers, the crooks were able to manipulate the destination of the web connections. In one example of how this scam worked, the FBI said, "When users of infected computers clicked on the link for the official website of iTunes, for example, they were instead taken to a website for a business unaffiliated with Apple Inc. that purported to sell Apple software. Not only did the cyber thieves make money from these schemes, they deprived legitimate website operators and advertisers of substantial revenue." The FBI announced the arrest of the "Rove Digital" Estonian hackers on November 9, 2011.

Since there are likely millions of computers still infected with the DNS Changer malware, the sudden shutdown of those rogue servers would have prevented the victims from accessing many of their favorite websites. In order to allow the infected computers to continue

--continued on next page--

to access the Internet, but actually reach their intended websites. the FBI arranged for the rogue servers to be temporarily replaced with legitimate servers, such that the victims' Internet access is not disrupted. It is these temporary replacement Internet servers that will be shut down on July 9, meaning that anyone who still has a computer infected with DNS Changer as of that date may lose Internet access.

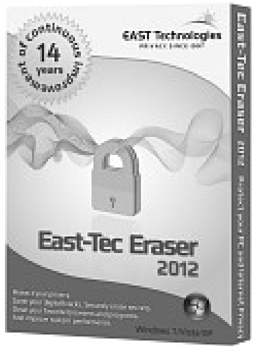
In order for users around the world to determine if their computers are infected with the DNS Changer malware, a consortium of academic, governmental, and private organizations created the DNS Changer Working Group (DCWG), which initially administered the servers that replaced the illicit Rove Digital servers. The DCWG consists of representatives from Georgia Tech, Internet Systems Consortium, Mandiant, National Cyber-Forensics and Training Alliance, Neustar, Spamhaus, Team Cymru, Trend Micro, and the University of Alabama at Birmingham. The website for the DCWG, **www.dcwg.org**, is hosted at the Georgia Institute of Technology, under a research grant provided by the Office of Naval Research. The DCWG provides a quick method for users to determine whether or not their computers are infected with the DNS Changer malware. According to the DCWG, there are still 350,000 computers infected by the DNS Changer malware that are using the clean servers maintained by the DCWG which replaced the Rove Digital servers.

In order to quickly and safely test if a computer has been hijacked by the DNS Changer malware, the DCWG has created 11 international servers which will report back to the user if his computer is indeed hijacked by DNS Changer; in the U.S. the link for this test is **www.dns-ok.us**. The test can be run from any browser, and nothing is downloaded or installed on the computer during the test; it is simply a test to see if the computer is connecting to a correct IP address. The results are almost instantaneous, with a "DNS Changer Check Up" result displayed in an IP graphic; if it is green, the user is possibly free of the DNS Changer malware, but the green graphic does not certainly prove that the computer is clean. When the green display appears, it also says, "Your computer appears to be looking up IP addresses correctly! Had your computer been infected with DNS changer malware you would have seen a red background. Please note, however, that if your ISP is redirecting DNS traffic for its customers you would have reached this site even though you are infected." If the display is red, then it is likely that the computer is one of the many that have been compromised by DNS Changer.

For the computer that is "red", it will be necessary to clean the DNS Changer malware and then reset your DNS. Most of the current anti-spyware products such as the free versions of SuperAntiSpyware (**www.superantispyware.com**) and the free version of MalwareBytes (**malwarebytes.org/products/ malwarebytes_free**) can detect and remove the DNS Changer malware, but it will still be necessary to reset your DNS in order for the Internet to properly function on your computer. Almost all ISP's (Internet Service Providers) offer telephone support that will help the user reset the DNS to the ISP's preferred DNS server. Gizmo's TechSupportAlert has instructions and links on how to find the best DNS server for you (**techsupportalert.com/content/ how-find-best-dns-server.htm**), as well as detailed instructions on how to change or reset the DNS settings on your computer (**techsupportalert.com/content/ how-change-dns-server.htm**).

Google has a free DNS utility "Namebench" at **code.google.com/p/namebench** that can help the user find the fastest free DNS, with instructions on how to change your DNS at **developers.google.com/speed/public-dns/docs/using**. Another excellent DNS service, OpenDNS, has simple but detailed instructions on how to change your DNS at **use.opendns.com.** If you use Google's Namebench to find the best combination of DNS for your computer and connection, you can use those DNS on your computer by following the instructions given on Google or OpenDNS on how to change your DNS settings; while the default DNS listed on the Google and OpenDNS instructions are excellent and totally adequate, there may be some performance improvement by using the DNS recommended by Namebench. You can always change them again later.

If you enjoy or depend on the Internet, it is imperative that you go to **www.dcwg.org/detect** and see if your browser is connecting to a legitimate DNS. If the results are "green" you are likely (but not certainly) safe from the DNS Changer Trojan, and can probably continue to use the Internet after July 9. If you are "red" you must clean your computer of the DNS Changer malware and reset your DNS as instructed above. Regardless of "green" or "red" results, it is always a good practice to periodically scan your computer with a good third-party utility such as SuperAntiSpyware or MalwareBytes to verify that nothing slipped by your security software. Failure to check your computer prior to July 9 may mean no Internet for you on July 10.



East-Tec Eraser

take out the garbage permanently and forever

A Software Review

by Herb Goldstein, Editor,
Sarasota PCUG, Florida
January 2012 issue, *Sarasota PC Monitor*
www.spcug.org
pcugedit@Verizon.net

There's no shortage of software that will permanently erase files, but if you simply want the very best there is one that spares none of the bells and whistles, East-Tec Eraser leads the pack. It's for people that demand that their erasures, albeit a single file or an entire disk is erased in such a way as to be totally, completely, and unequivocally gone and unrecoverable by any means or entity known to man. In fact, it surpasses even top-secret military requirements.

East-Tec erasure is not only a leading permanent deleting utility, it offers an extremely useful associated bag of tricks you can employ at your choosing:

1. It will search any of your drives or partitions for remnants of previously deleted files and remove any trace.
2. It will wipe any remnants that exist in the free space of your drives and in your swap files.
3. East-Tec's Privacy Guard will wipe web pages, pictures, temp files, history, recent docs and all other tracks you usually accumulate in your Internet wanderings, newsreaders and web browser.
4. It will permanently erase the contents of your recycle bin.
5. It will permanently erase the contents of your "deleted items" folder in Outlook Express and compact the information in your other folders.
6. It will permit you to schedule regular erasure tasks of your time and choosing.
7. In Windows XP and in 32-bit versions of Windows 7, Eraser installs in your context (right-click) menu in Windows Explorer or your alternative file manager. If you right-click on any files or folders you have selected, eraser will promptly dispatch them beyond recovery. While Eraser is not available in the *context menu* of 64-bit Windows 7, it is fully functional everywhere else in Windows 7.
8. Eraser can completely wipe an entire hard drive, CD or other media, making it safe for disposal.
9. You can password protect the use of Eraser.
10. You are provided a choice among several permanent and secure erasure methods which are fully explained.
11. Eraser will conveniently destroy the accumulation of an Internet session with a single click.

The program is easy to install and use. A total novice will have no problem employing any or all of its wizard-driven features. It has received top awards in such computer publications as PC World. East-Tec Eraser provides the most advanced, thorough and effective erasure utility of its kind, to safeguard and protect your privacy. It is well worth its cost of $39.95. You can try it for free or purchase it a **www.east-tec.com.**

Do Not Track Plus

BY ABINE.COM

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

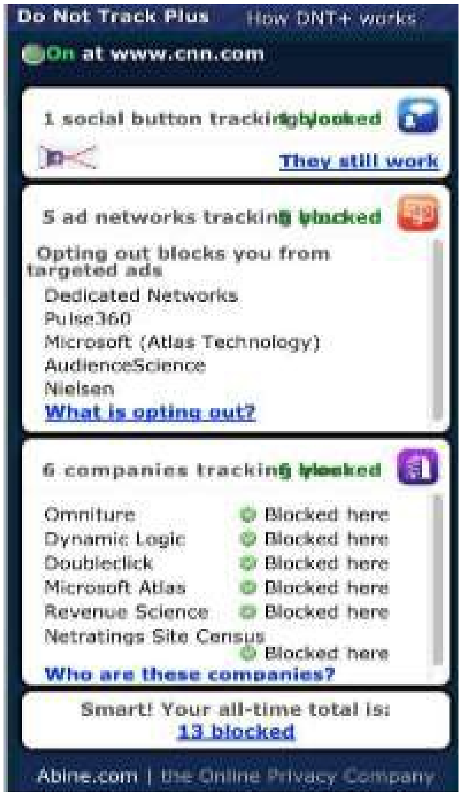
In the software industry there is a movement to have the browsers include a pllug-in that prevents this action but as of yet it is not ordered and may never by. Browser

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

When you run Abine it puts a small icon in your browser and it displays a number with each site you visit, telling you how many attempts are made to track your

-continued on next page-

visit and what type of tracking company is making the effort. They also keep a running grand total of how many blocks they have made. In the first few days of my use on one machine they blocked 1600 attempts.



Do Not Track Plus How DNT+ works

On at www.cnn.com

1 social button tracking 1 blocked
They still work

5 ad networks tracking 5 blocked
Opting out blocks you from targeted ads
Dedicated Networks
Pulse360
Microsoft (Atlas Technology)
AudienceScience
Nielsen
What is opting out?

6 companies tracking 6 blocked

Omniture	Blocked here
Dynamic Logic	Blocked here
Doubleclick	Blocked here
Microsoft Atlas	Blocked here
Revenue Science	Blocked here
Netratings Site Census	Blocked here

Who are these companies?

Smart! Your all-time total is: 13 blocked

Abine.com | the Online Privacy Company

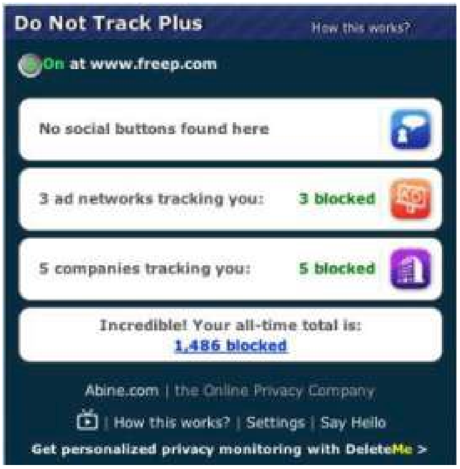
Installation following the quick download is painless and there is virtually no setup. While writing this article I loaded Firefox, downloaded the software and ran it as a plugin.

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

It looked like this (see end of article).

The program came highly recommended by **Cnet.com,** which is where I read about it. It can be downloaded from **Abine.com.**

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



Do Not Track Plus How this works?

On at www.freep.com

No social buttons found here

3 ad networks tracking you: 3 blocked

5 companies tracking you: 5 blocked

Incredible! Your all-time total is: 1,486 blocked

Abine.com | the Online Privacy Company

| How this works? | Settings | Say Hello

Get personalized privacy monitoring with DeleteMe >

ON FACEBOOK, THINK BEFORE YOU "LIKE"

By Anne Kandra, PCWorld, May 2012

Anyone who has survived middle school knows that publicly admitting you "Like" someone can have serious repercussions. On Facebook, you might want to consult your inner "tween" before clicking a "Like" button. That's because Facebook, not unlike that nosy girl in 7th grade, wants to tell everyone about your objects of affection, via ads that make you an unwilling and unpaid endorser.

These ads, called Sponsored Stories, repurpose users' updates and activities to hawk an advertiser's products or services. Once you "Like" a company page, check in at a merchant location, post an update mentioning a product, service, or company, or otherwise interact with a Facebook advertiser, your activity becomes potential ad fodder. Your friends could then receive an update about it - whether you want Facebook to share it or not.

In a video on a Facebook site, a product manager notes that the Stories go only to your friends, and they aren't getting anything you aven't already sent them. True, but isn't there a difference between your recommending a movie to your friends, and Facebook taking it upon itself to do so? Plus, the Stories don't always take context into account. Consider the case of blogger Nick Bergus, who made a funny post about an Amazon ad for a 55-gallon drum of "personal lubricant." Next thing he knew, he was in ads hawking the tube to his friends. One pal told Bergus he saw the ad every time he logged into Facebook. (You can read Bergus's full story at **find.pcworld.com/72733**.)

If Sponsored Stories were to stay in the ticker feed, where they are relatively easy to ignore or hide, they might not be such a big deal. Unfortunately, as of this writing, Facebook has started releasing them into users' news feeds.

You can't stop Facebook from using you as an unpaid endorser or tainting your news feed with ad pitches, but you can minimize the noise by being judicious about your activities. Before you click a "Like" button, check in at a shop or restaurant, post an update about a product or service, or install an app that tracks or shares your actions, ask yourself if you feel strongly enough about the product or service to endorse it to your friends. You might still end up being an involuntary shill, but at least you can be selective about it. After all, a little "Like" can go a long way.

Gary Stanley's Cyber News

gary.stanley.net/cyber_news.htm

Futuristic technology is what we thought about and invented yesterday. Futuristic technology is also what scientists are thinking about and experimenting with today. How about a sexy looking pair of glasses that will take the place of your smart phone! Project Glass, as Google calls it, is the company's prototype of a hands-free system that can pull up maps, directions, events notifications, and the locations of nearby friends right in a wearer's line of sight. Here's the scoop and a video from CNET **goo.gl/Ta7tM**.

Have I told you how much I love my new ilPad? Every time I pick it up, it truly amazes me and everyday you see these devices being used in new and different ways.12 million were sold the first quarter of this year! I doubly enjoyed the Masters tournament because of the awesome Master's app on the iPad.I love being able to edit and show photos, that I just took with my Nikon camera, on the iPad as this is much more advantageous than viewing them on the small camera LCD. Whether you own one or not, you'll enjoy this presentation by two magicians using 7 iPads! **goo.gl/loZnH**

If you're one of the newcomers to the Apple iPad, I strongly recommend that you download "Flipboard." It's a free app where I spend most of my time on the iPad. It will allow you to choose hundreds of magazines and news sources to customize as per your tastes. Now just sit back and be entertained and educated!

Las Vegas is known for its fabulous shows and this one is no exception! Every magician likes to involve a pretty girl in his magic tricks but it's not often that the pretty girl is also a magician herself. **goo.gl/mTWBb**

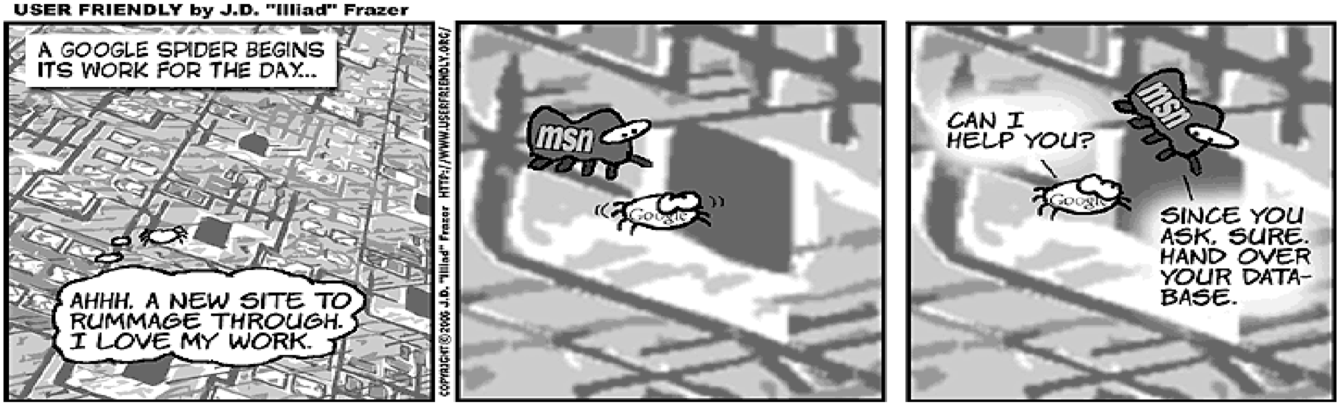
Computer technology has birthed "Augmented Reality." Augmented reality is what I call pure magic. An example of this would be to experience the ultimate vacation without ever leaving your easy chair. Oh if we could just look into the future. But today is the tomorrow that we dreamt about yesterday. The future is here and now! Watch this incredible demonstration of computer generated magic. **goo.gl/dZSv7**

The summer heat is here as Phoenix has already experienced temperatures over 100 degrees. Consequently we must remind you that direct sunlight on your iPhone, iPad, iPod, MP3 player, laptop, or any other electronic device, is dangerous and can cause serious problems.If you have your computer tower stored inside of a desk be sure to leave the door open when using it for better air circulation.

I get asked in every computer seminar; "What do I think of Cloud Storage." My answer has always been, and still is, that I don't trust it. Cloud storage is when you send your personal data files, music files, photos, to some company's servers. There are many companies who offer this service. The big advantage is that you can access your files from any computer you may be using, whether at home or anywhere else. The disadvantage is you don't know where your files are located, what type of encryption they are using, how safe they are, and the stability and trustworthiness of the company. I might not mind "clouding" my photos, or music, but never my personal data. In my opinion the only safe and secure way to store your files is on your own external hard drive. That way you are in full control of the safety of "your stuff." When I go out of town, my external hard drive goes with me incase of fire or other unforeseen circumstances. More on this subject from PC World. **goo.gl/zYdhq**

There is so much to understand about using a computer. Over the years computer's have increasingly become more user friendly and the operating systems more stable and

USER FRIENDLY by J.D. "Illiad" Frazer


A GOOGLE SPIDER BEGINS ITS WORK FOR THE DAY...
AHHH. A NEW SITE TO RUMMAGE THROUGH. I LOVE MY WORK.
COPYRIGHT © 2006 J.D. "Illiad" Frazer HTTP://WWW.USERFRIENDLY.ORG/
msn
Google
CAN I HELP YOU?
SINCE YOU ASK, SURE. HAND OVER YOUR DATABASE.

--continued on next page--

reliable. But, they still develop problems and there is so much we still don't understand. There are mysteries and I've found an article to explain a lot of these mysteries. Read this over **goo.gl/va0Gr** and take away what you can to more fully understand your computer.

Have you heard of HULU? HULU is a great place to hang out and watch TV shows, and movies. You'll experience great quality and you can watch everything in full screen. I clicked on one because it was about Facebook, and got a good laugh! Give it a try. **goo.gl/4X9kR** Hold on...here's another one about text messaging that maybe even funnier! **goo.gl/y6uoA**

Photo Tip of the Month:This month's tip is pure and simple; learn your camera. None of us like to read manuals, but every time I open mine I learn something new. Knowing your camera will allow you to take better pictures, and taking better pictures is the name of the game! There are actually two equations to taking better photos and that is being familiar with your camera and being familiar with a software editing program. When both of these become second nature that's when the real fun begins!

Secrets to Safe Computing : Read each point below and follow the advice as outlined. Just a few minutes of work each month will go a long way in keeping your computer running smoothly!

- Make sure System Restore and Firewall are active.
- Follow guidelines in "Secrets to Safe Computing." **goo.gl/R00Yq**
- Keep your Operating System Updated. **goo.gl/AAVzU**
- Don't open Email from strangers.

Officers 2011-2012

Elected Officers

President	Judi McDowell	(309) 314-1780	julee89@gmail.com
Vice President	Nancy Polios	(309) 755-4926	npolios@gmail.com
Secretary	Diana Wolf	(309) 797-5413	theqcs.sec@mchsi.com
Treasurer	Dave Tanner	(309) 764-6455	dl.tanner@mcshi.com
Directors at Large	Jim Buche	(309) 755-4893	jhbuche@mchsi.com
	Marie Drexler	(309) 755-8138	drexlerm@mchsi.com
	Ralph Drexler	(309) 755-8138	drexlerm@mchsi.com
	Tina Gean		tina2121@yahoo.com
	Melinda Missman	(309) 235-7579	mamissman@msn.com
	Shari Peterson	(563) 468-1958	skp4joy@q.com
	Susan Peterson	(309) 721-7048	felspaw@@gmail.com
	Karen Reynolds	(309) 797-6572	kajor31539@gmail.com
	Emily Smith	(309) 794-9320	ginghis18@mchsi.com
Director Past President	Patty Lowry	(563) 332-8679	pattylowry@rocketmail.com

Director/SIG Leader

Beginners	Jim Kristan	(309) 755-8277	jmkris@gmail.com
Genealogy	Len Stevens	(563) 359-9672	judylenstevens@msn.com
Digital (coordinator)	Vicki Wassenhove	(309) 787-2239	wazz123@gmail.com
Internet	Ted Huberts	(309) 792-9470	s1owhand54@sbcglobal.net
Office	Judi McDowell	(309) 314-1780	julee89@gmail.com
QBits	Joe Durham	(309) 764-5570	joseph85_us@yahoo.com
Windows	Larry Stone	(309) 787-5574	lstone521@mchsi.com

Appointed Officers

Membership Director	Susan Peterson	(309) 721-7048	felspaw@sbcglobal.net
Program Director	Nancy Polios	(309) 755-4926	npolios@gmail.com
Public Relations Dir.	Melinda Missman	(309) 235-7579	mamissman@msn.com
Publicity	Joe Durham	(309) 764-5570	joseph85_us@yahoo.com
Financial Committee	Mel VanderHoek	(563) 355-5085	vanderhoek@netexpress.net
APCUG Representative	Patty Lowry	(563) 332-8679	plowryapcug@gmail.com
Membership Records	Susan Peterson	(309) 721-7048	felspaw@sbcglobal.net
Web Master	Vicki Wassenhove	(309) 787-2239	wazz123@gmail.com
QBITS Newsletter	Joe Durham	(309) 764-5570	joseph85_us@yahoo.com
	Patty Lowry	(563) 332-8679	pattylowry@rocketmail.com
Mailing	Patty Lowry	(563) 332-8679	pattylowry@rocketmail.com
Resource Manager	Judi McDowell	(309) 314-1780	julee89@gmail.com

Name ________________________________

Company ______________________________

Address ______________________________

City _________________________________

State, Zip +4 __________________________

Home Phone ___________________________

Cell Phone ____________________________

Email ________________________________

Referred by ___________________________

QCS Meeting Dates – JUNE 2012

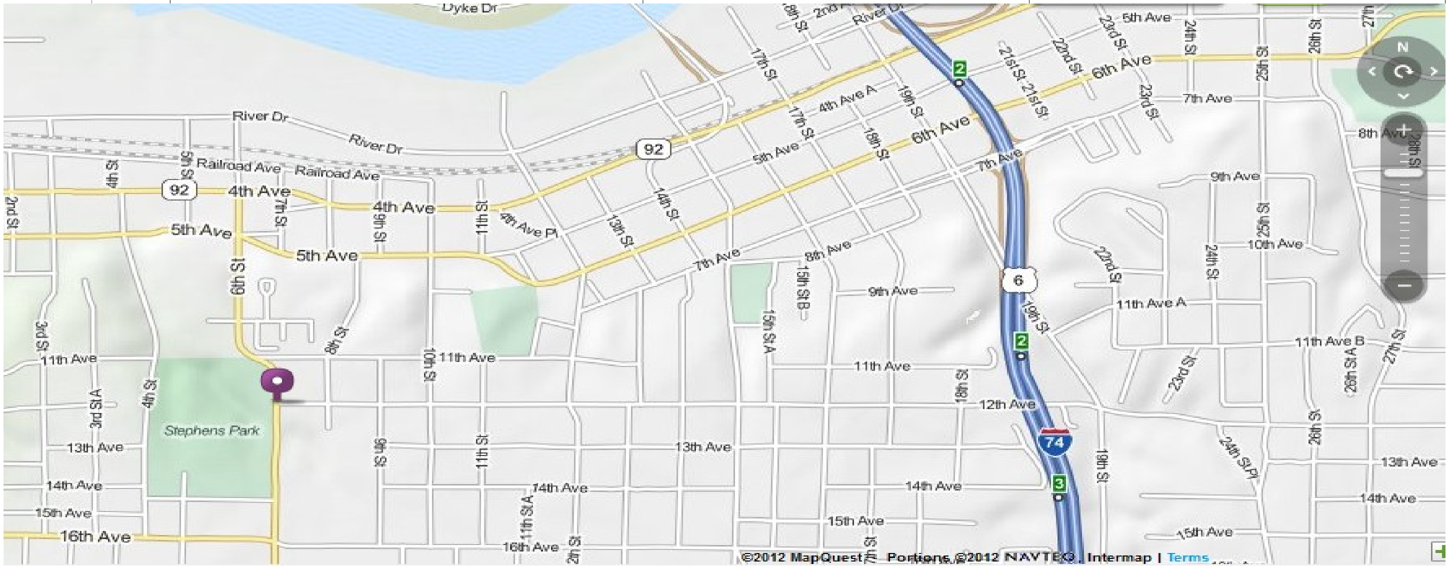
S	Mon	Tue	Wed	Thu	F
					1
3	4	5	6	7	8
	5:30 PM **Beginners SIG** **Jim Kristan** **309-755-8277** jmkris@gmail.com **7:00 PM** **Ted Huberts** **VACATION PLANNING ONLINE**	**QCS Officers** President Judi McDowell **julee89@gmail.com** Secretary Diana Wolf **theqcs.sec@mchsi.com**			
10	11	12	13	14	15
17	18	19	20	21	22
	5:30 PM **Genealogy SIG** **Len Stevens** **563-359-9672** judylenstevens@msn.com **7:00 PM** Internet SIG **Ted Huberts** **309-792-9470** slowhand54@sbcglobal.net	Vice-President Nancy Polios **npolios@gmail.com** Treasurer Dave Tanner **dl.tanner@mcshi.com**			
24	25	26			
	5:30 PM **Digital SIG** **To be announed** **7:00 PM** **Windows SIG** **Larry Stone** **309-787-5574** lstone512@mchsi.com	**6:00 PM** **QCS Board Meeting** **2nd Floor** **Orchid Room** **Butterworth Home**			

Location: Butterworth Education Center

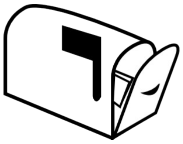
7th ST and 12th Avenue

Moline, IL 61265

During the Summer months we are required to relocate at other Butterworth Locatoins, please consults our web site **qcs.org** frequently for directions.



Quad Cities Computer Society
c/o Dave Tanner
3449 - 52nd St
Moline IL 61265



Moving? Send an address change to:
felspaw@sbcglobal.net

This Month in *QBITS* ....

Tuesday
June 4, 2012
7:00 PM
Ted Huberts
Vacation Planning Online