The PULP

HUGE this month:

General Meeting: Oct. 15th

Computer Security Awareness

See you there!

New Location !!!!!

Knights of Columbus
2533 Main Street,
Glastonbury, CT

Q&A Session: 7:00PM–7:30PM
Meeting starts at: 7:30PM

Contents:

Member of Association of Personal Computer User Groups APCUG

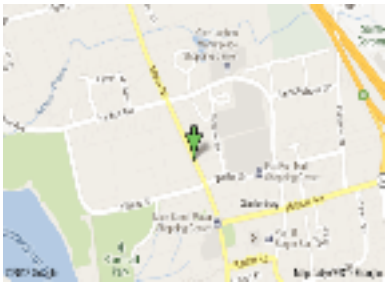
UGC

H.U.G.E.

Apple User Group

The **PULP** is published monthly by and for members of the Hartford User Group Exchange, Inc. (**HUGE**). **HUGE** is a nonprofit organization whose aim is to provide an exchange of information between users of personal computers. The **PULP** is not in any way affiliated with any computer manufacturer or software company. Original, uncopyrighted articles appearing in the **PULP** may be reproduced without prior permission by other nonprofit groups. Please give credit to the author and the **PULP**, and send a copy to **HUGE**. The opinions and views herein are those of the authors and not necessarily those of **HUGE**. Damages caused by use or abuse of information appearing in the **PULP** are the sole responsibility of the user of the information. We reserve the right to edit or reject any articles submitted for publication in the **PULP**. Trademarks used in this publication belong to the respective owners of those trademarks.

MEETING LOCATION
Knights of Columbus
2533 Main Street
Glastonbury, CT



Editor's Corner

October is Computer Security Awareness Month and that will be the theme for the meeting. I think it's also time to nominate new board members. So, if you have a few minutes a month to spare for HUGE, join the board.

In the news this past month, Hiroshi Yamauchi (was the head of Nintendo and father of console gaming) and Ray Dolby (noise reduction and surround sound,) passed away.

NASA reported that Curiosity found water molecules attached to grains of sand on the Martian surface.

Stanford University researchers announced they had built the first functioning computer that used only carbon nanotube transistors instead of silicon. This will allow computers to do more work with less heat/energy, but they are 5-10 years away.

Microsoft will pay at least $200 for used iPads that you can use to buy a Surface tablet. Of course, you can get more than that selling it on ebay or privately locally.

3D Systems, one of the largest consumer printer companies, has already been able to configure machines to create a variety of sugary goods, including cakes and candy. They're working toward chocolate (mine will be on order when they release).

Researchers at the Univ. of Illinois Urbana-Champaign have developed a cradle and app for the iPhone that uses the phone's built-in camera and processing power as a biosensor to detect toxins, proteins, bacteria, viruses and other molecules. I'll have the video for the meeting.

U.S. smartphone costs aren't highest in the world, they just feel that way. Australia is higher and the United Kingdom is less. The US is on par (within $20/ month) with Japan, Germany, & China. That includes the phone and monthly costs for 2 years.

A team at the University of Washington has managed to coax WiFi signals into recognizing basic gestures in order to control a computer or game console. The system doesn?t need any kind of camera, nor does it need users to wear any kind of sensor. All the system needs is a modified WiFi router, and a few wireless devices to bounce the signal around.
Dubbed WiSee,

Speaking of controlling a computer, ever thought about how to do that with Google glass? DoCoMo showed a prototype using any paper surface—a sheet

cont on pg. 9

Here is the appropriate copyright citation and a link to the full text. articles from "Tidbits"

http://creativecommons.org/licenses/by-nc-nd/3.0/

A Little Computer Quiz

by Stuart Rabinowitz

The trivia and minutiae of the computer related world. The answers will appear next month or you can submit an answer sheet at the General Meeting. Good Luck.

October is Computer Security Awareness Month, so in that vein is this month's quiz.

1 Computer viruses have been around a long time, any guesses as to when the first was released?

2 What was it called?

3 What did it do?

4 Once upon a time there was a virus called 'Elk Cloner'. When was it released and on what brand of machines?

5 What was the first documented internet worm and when was it released?

Answers to Sept.., 2013 Quiz

Wikipedia seems to have taken over the world of encyclopedic research. Have a question go to Wikipedia, But what about the conflict that seems to infest some of the articles (AKA -- edit wars)?

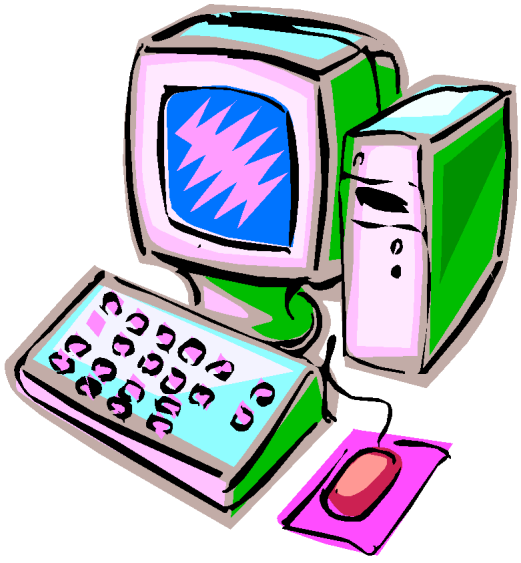
1 For 2012, what english entry generated the most re-edits?
A The article on George W. Bush

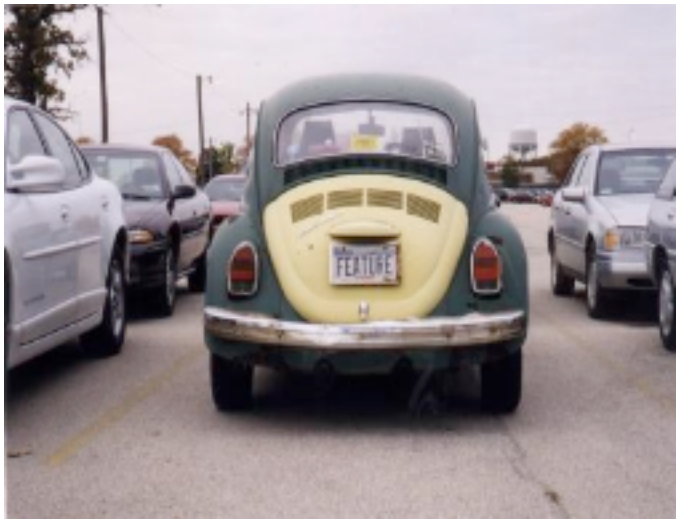
2 What was the most controversial set of topics world-wide?
A Politics & politicians

3 What percent of the total edits did those topics amount to?
A 25%

4 The top ten accounted for what percent of the total?
A 97%

5 We've all played computer games of various types; cards, shoot-m-up, strategy, etc, but what game do assembly language programmers play to test their coding skill?
A Code War, the object being to write assembly programs that try to destroy an opponents program in the memory of a simulated computer. You can read about it here: http://www.corewars.org/index.html





October is National Cyber Security Awareness Month
By Ira Wilsker
iwilsker (at) sbcglobal.com

WEBSITES:
http://staysafeonline.org/ncsam
https://isc.sans.edu/diary.html?storyid=11623&rss
http://news.yahoo.com/maryland-recognizes-national-cybersecurity-awareness-month-160244986.html
http://blogs.cisco.com/security/cisco-joins-the-national-cyber-security-awareness-month-party/
http://gta.georgia.gov/00/press/detail/0,2668,1070969_167558063_163659118,00.html
http://uit.tufts.edu/?pid=624
http://msisac.cisecurity.org
http://www.microsoft.com/security/resources/cybersecurity.aspx
http://staysafeonline.org/cybersecurity-awareness-month/2011-ncsam-champions
http://www.uscert.gov/reading_room/brochure_securityguidance.pdf
http://www.uscert.gov/reading_room/posters_all.pdf
https://www.sans.org/critical-security-controls
http://security.vpit.txstate.edu/training/csam_2011.html

PDF AND WORD FILES:
http://staysafeonline.org/cybersecurity-awareness-month/banners-and-more
(has links to PDF and Word files for child, parent, and student cyber safety)
http://staysafeonline.org/sites/default/files/resource_documents/Gaming%20Tips%20for%20Kids%20STC.pdf - Gaming Tips for Kids
http://staysafeonline.org/sites/default/files/resource_documents/College%20Students%20Internet%20Safety%20and%20Security.pdf - Internet Safety and Security for College Students
http://staysafeonline.org/sites/default/files/resource_documents/Parents%20Internet%20Safety%20and%20Security%20STC.pdf - Internet Safety and Security for Parents

It is that time of year again. In 2004, with the fear of cyber war increasing, and early indications of cyber-attacks already taking place against our critical infrastructure, private organizations, and government agencies, President Bush issued a proclamation declaring that October, 2004, would be "Nation Cyber Security Awareness Month" (NSCAM). Every October since, Presidents Bush and Obama have made similar declarations, acknowledging the degree of threats that we all face, in terms of cyber security. One consistent factor in the declarations and implementations of the program is that it is not just our public and private agencies that have been threatened, but our personal safety and security is at extreme threat as well. Our personal computers can be unknowingly hijacked by a foreign power or terrorist organization, and under remote command, be used to launch a potentially devastating cyber-attack against our government or infrastructure, simultaneously coming from millions of our personal computers!

Nation Cyber Security Awareness Month is a joint public - private partnership between the Department of Homeland Security (www.dhs.gov/files/programs/gc_1158611596104.shtm), the National Cyber Security Alliance (staysafeonline.org/ncsam), and the Multi-State Information Sharing and Analysis Center (msisac.cisecurity.org). Together, these three organizations have brought together government agencies (federal, state and local), educational institutions, corporations and community service entities to promote a coordinated national program designed to educate everyone on the risks endemic in the cyber world, and methods to harden our computers and other smart devices from cyber-attack.

Taking the lead is the National Cyber Security Alliance (NSCA), which is providing the primary coordination of activities, supplying free informational materials that anyone is free to copy and distribute (staysafeonline.org/cybersecurity-awareness-month/ncsam-tip-sheets). There is one common thread in all of these NCSA documents (staysafeonline.org/cybersecurity-awareness-month/about-ncsam-2011); "It starts with STOP. THINK. CONNECT., a simple action for all of us to employ to stay safer and more secure online. STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems. THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's. CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer. By incorporating Our Shared Responsibility and STOP. THINK. CONNECT. into your online routine, you will be doing your part in protecting yourself, your family, your community and your country."

To assist individuals and families in securing their computers, the NCSA has published a variety of "tip sheets" including Gaming Tips for Kids, Gaming Tips for Parents, Internet Safety and Security Tips for College Students, Internet Safety and Security Tips For Parents, Mobile Safety Tips, and Social Networking Tips. If individuals would follow and apply the tips presented in these documents, we and our families may become much safer and more secure while online. Support for these NSCA activities comes from several dozen private companies, non-profit organizations and government agencies (staysafeonline.org/cybersecurity-awareness-month/2011-ncsam-champions). The NCSA website also has age appropriate activities and learning materials for children that may be freely used by school teachers and parents.

The Department of Homeland Security (DHS) is most aware of the degree of danger that we are facing from cyber-attack on our computer and domestic infrastructure. DHS says, "The most serious economic and national security challenges we face are cyber threats. America's economic prosperity and competitiveness in the 21st Century depends on effective cyber security. Every Internet user has a role to play in securing cyberspace and ensuring the safety of themselves and their families online."

(http://www.dhs.gov/files/programs/gc_1158611596104.shtm)

While most of us are by now aware that we need to secure our personal computers, there is also an extreme need to secure our business, government and educational computers, as well as harden our infrastructure to cyber-attack. Several governmental and educational agencies have made free materials available to train employees, and increase awareness of the need for increased and improved cyber security. The United States Computer Emergency Readiness Team (US-CERT), a part of the Department of Homeland Security has released a two-page brochure "Protect Your Workplace, Guidance on Physical and Cyber Security and Reporting of Suspicious Behavior, Activity, and Cyber Incidents" www.uscert.gov/reading_room/brochure_securityguidance.pdf). While only two pages, this brochure contains pertinent information on Cyber Security Guidance, reporting Cyber Security Incidents, Physical Security Guidance, reporting Suspicious behavior and Activity, and a listing of the Joint Terrorism Task Force (JTTF) phone numbers. The information in this brochure is not just appropriate for government agencies, but is also relevant to any other business, college or other organization, as all of them may be vulnerable for a targeted cyber-attack. In order to help facilitate cyber security, US-CERT also has a series of free posters and other information available which can be printed and placed around the workplace (www.uscert.gov/reading_room/distributable.html).

State, cities, counties, and educational institutions are also active participants in the National Cyber Security Awareness Month activities. Several states, such as Georgia and Maryland, have issued statewide proclamations and implemented statewide activities to promote cyber security activities. Recently Maryland announced its "CyberMaryland, an aggressive business development and marketing initiative to strengthen Maryland's burgeoning cyber security industry and protect the nation's digital infrastructure." (source: news.yahoo.com/maryland-recognizes-national-cybersecurity-awareness-month-160244986.html). Maryland Governor O'Malley, in declaring the state's active participation in National Cyber Security Awareness Month said, "As a state and as a nation, we face unique security challenges. Maryland has a vital network of cyber security assets—from entrepreneurs who work to stop cyber-attacks by developing new and cutting edge technologies to educators who are training the next generation of cyber warriors. Together, working with our federal and local partners, we have an opportunity to create jobs and uphold our responsibility to protect and defend the nation's digital infrastructure."

In Georgia, "Governor Deal has proclaimed October as Cyber Security Awareness Month. It's part of a nationwide effort to share information about protecting business and personal data." Georgia has compiled and published a directory of computer security resources for home users and IT professionals which can be found online at gta.georgia.gov/00/press/detail/0,2668,1070969_167558063_163659118,00.html.

In Texas, several colleges and universities have announced programs and events to enhance cyber security awareness in recognition of National Cyber Security Awareness Month. One good example is Texas State University, in San Marcos, where it is sponsoring a series of informational events, culminating in a "Cyber Security Awareness Day 2011 (October 26th)". Texas State University explains the importance of National Cyber Security Awareness Month as, "Our shared responsibility means each of us must do our part—whether it's using stronger security practices in our day-to-day online activities or helping raise community awareness, we can all contribute towards this common goal" (security.vpit.txstate.edu/training/csam_2011.html).

While it is a great idea to set aside an entire month to promote awareness of the cyber security threats that we all face, and to widely distribute information on methods and technology to secure our computers, this is a practice that needs to be implemented and practiced 12 months a year, not just in October.

Malware, Viruses, Trojans Defined
By Ira Wilsker
iwilsker (at) sbcglobal.com

WEBSITES:
http://en.wikipedia.org/wiki/Malware
http://www.ilovefreesoftware.com/08/featured/definiton-of-various-security-related-terms.html
http://lifehacker.com/5560443/whats-the-difference-between-viruses-trojans-worms-and-other-malware
http://en.wikipedia.org/wiki/Computer_virus
http://en.wikipedia.org/wiki/Computer_worm
http://en.wikipedia.org/wiki/Trojan_horse_(computing)
http://en.wikipedia.org/wiki/Rootkit
http://en.wikipedia.org/wiki/Backdoor_(computing)
http://en.wikipedia.org/wiki/Rogue_antivirus
http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/12_december_2010_threat_roundup__010711_.pdf

In the past week, I was called upon four more times to clean malware off of infected computers. One user had a major name brand antivirus program installed, running, and updated and could not understand how the malware had penetrated his antivirus software and contaminated his computer. He had purchased the antivirus software last fall from a big box electronics store based on the recommendations of a salesperson. He had been told that this particular brand of security software was the best as it was their top seller, and that antivirus software was all that he really needed. Based on that recommendation he plopped his hard earned money on the counter, went home, installed it, updated it, and blissfully surfed the internet, opened email attachments, downloaded software and music, and had just a jolly good time online until his computer gradually slowed to a crawl, and friends informed him that they were receiving spam emails from him. This user was perplexed, as his antivirus software was running, and indicated that it was updating several times a day. He just could not understand how 90 different malware programs had infected his computer. His problem started when he purchased inadequate security software; while the product he bought was excellent at protecting his computer from viruses, and some Trojans and spyware, it did not offer the all-inclusive protection of the comprehensive security suite offered by that publisher (and others as well) that would have only cost him a few dollars more.

There is a common misconception in user circles that viruses are the primary computing threat, as users have had heard about viruses for several years. Today, viruses are present, but a relatively minor threat in terms of prevalence. I did a quick analysis of the most common new threats recently listed by TrendMicro, and found that viruses only made up 4% of the new significant threats to our computing security. On the other end of the spectrum, Trojans made up 42% of the commonly seen new threats, worms were at 14%, backdoors at 14%, web based threats were at 6%, java script malware was at 6%, 4% were hacking utilities, 2% adware, and about 8% other threats. It is obvious that protective software that protects the computer primarily from viruses is failing to protect the user from the majority of contemporary threats; it is precisely this fact that led to this user's infected computer, despite his premium quality antivirus software. A lot of users have a misconception about the common threats in circulation, believing that they are generically all viruses, but, as I saw in this case, this blissful ignorance may lead to a computing nightmare.

While not necessary to use a computer, it would likely be beneficial for computer users to be aware of the different threat groups that can impact our computing. According to Wikipedia, "A computer virus is a computer program that can copy itself and infect a computer." Many viruses attach themselves to legitimate programs or data files on the infected computer. The fact that a computer virus can copy itself to infect other computers is what makes it different from other types of malware, for which viruses are commonly confused. Viruses can be spread through digital media (USB drives, CD or DVD discs, and floppy discs) or through network connections that the virus can use to copy itself to other attached computers. Once a virus has infected a computer it may perform a variety of tasks as programmed by its author. Viruses may damage the data on a hard drive or degrade the performance of the computer. Some of the viruses are stealthy and their effect may not be noticeable by the user, as the viruses do their damage in the background. Some viruses are functionally benign, other than they reproduce themselves countless times on the infected hard drive, until they consume all of the free space on the hard drive.

Computer worms are a malicious computer program that wriggles through computer networks sending copies of itself to other computers attached to the network. Most worms are free standing programs, and are commonly programmed to spread themselves through the network without any action by the user. Most worms have an explicit nefarious function such as deleting files on the infected computer, or encrypting critical files, only releasing them after an extortion payment is made to the cybercriminal. Some worms open a backdoor into the computer that will enable the creator of the worm to take remote control of the computer, converting the computer into a "zombie" under his control, which can be used to generate revenue for the originator of the worm by sending spam mail from the infected computer, with the spam fees collected going to the author of the worm. Some worms are used to create a zombie network of computers, also called a "botnet", where the compromised computers can be used to launch directed cyber-attacks on other computers or networks, in an act of cyber terrorism.

For those who are aware of the epic "Helen of Troy" of Greek mythology, the term "Trojan

Debunking Some Common Myths
Author: Mindi McDowell
National Cyber Alert System
Cyber Security Tip ST06-002
February 2011

There are some common myths that may influence your online security practices. Knowing the truth will allow you to make better decisions about how to protect yourself.

How are these myths established?
There is no one cause for these myths. They may have been formed because of a lack of information, an assumption, knowledge of a specific case that was then generalized, or some other source. As with any myth, they are passed from one individual to another, usually because they seem legitimate enough to be true.

Why is it important to know the truth?
While believing these myths may not present a direct threat, they may cause you to be more lax about your security habits. If you are not diligent about protecting yourself, you may be more likely to become a victim of an attack.

What are some common myths, and what is the truth behind them?
Myth: Anti-virus software and firewalls are 100% effective.

Truth: Anti-virus software and firewalls are important elements to protecting your information (see Understanding Anti-Virus Software and Understanding Firewalls for more information). However, neither of these elements are guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.

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

Truth: Vendors may release updated versions of software to address problems or fix vulnerabilities (see Understanding Patches for more information). You should install the updates as soon as possible; some software even offers the option to obtain updates automatically. Making sure that you have the latest virus definitions for your anti-virus software is especially important.

Myth: There is nothing important on your machine, so you do not need to protect it.

Truth: Your opinion about what is important may differ from an attacker's opinion. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other people (see Understanding Denial-of-Service Attacks and Understanding Hidden Threats: Rootkits and Botnets for more information).
Myth: Attackers only target people with money.

Truth: Anyone can become a victim of identity theft. Attackers look for the biggest reward for the least amount of effort, so they typically target databases that store information about many people. If your information happens to be in the database, it could be collected and used for malicious purposes. It is important to pay attention to your credit information so that you can minimize any potential damage (see Preventing and Responding to Identity Theft for more information).

Myth: When computers slow down, it means that they are old and should be replaced.

Truth: It is possible that running newer or larger software programs on an older computer could lead to slow performance, but you may just need to replace or upgrade a particular component (memory, operating system, CD or DVD drive, etc.). Another possibility is that there are other processes or programs running in the background. If your computer has suddenly become slower, it may be compromised by malware or spyware, or you may be experiencing a denial-of-service attack (see Recognizing and Avoiding Spyware and Understanding Denial-of-Service Attacks for more information).

Internet -- Small Scams that Trick You
Written by Sandy Berger, Compu-KISS
www.compukiss.com
sandy (at) compukiss.com

I recently wrote about how companies who offer free software try to trick you into downloading extra programs. They do this during the download and/or installation process by having a pre-checked box indicating that the extra software will be included. Unless you uncheck the box, you get the extra programs along with the program that you requested. This is not illegal since you have, although often inadvertently, agreed to the download. It is not really a scam, but it is a form of trickery that is prevalent on the Web.

Free programs are notorious for this type of trickery as they try to offer something for free while still finding a way to make money. Another way they do this is by offering their free program, but encouraging you to purchase an upgraded version of that program instead of the free version. There is no problem with that. I have used several free programs and gone back to purchase the upgraded version to get more functionality or because I really like the free program. The problem comes when the company tries to trick you into purchasing the paid version.

Sometimes at websites like this, while there are numerous offers on every page for the paid version, the free program is very difficult to find. At other times you are given a list of features with columns comparing the paid version to the free version. Of course, the paid version has many more features and they almost always offer you a 30-day free trial, after which they will charge your credit card.

Again, there is nothing wrong with this, as long they make your choices clear. The problem arises when they try to trick you into downloading the paid version. Often, the download button for the paid version is very obvious while the download button for the free version is so small that it is almost non-existent. Even worse, is when the line is blurred between which download button is for which version. There may also be numerous pop-ups that lead you to the paid version.

These tactics, however, are a minor when compared to form of trickery that is really used to bamboozle you. One example of this is a pop up that appears on your computer informing you that your computer is infected with a virus and you need to click a button to get rid of the virus. In many cases, this is completely bogus. Your computer is not infected, but if you click on their button it will be. Then the pop ups will offer to get rid of the infection, if you pay a fee. Sometimes the pop ups look like they are from a legitimate antivirus company like Symantec or McAfee. They can be very realistic, so you have to be aware of which antivirus program you are currently using and what its real alerts look like. Once you have clicked on the button of the bogus antivirus promotion, it is usually too late to rethink what you are doing. So don't be trigger happy. If you think you are being approached with an antivirus scam, just close the window. If the window won't close, turn off the computer. Swindles like this are both illegal and upsetting for the computer user. On top of that, falling for a scam like this can cost lots of time and money.

There are many different cons of this type and there are several others that are equally disturbing. One is a company that tries to deceive you into moving your domain name registration to them. The one that I've seen over and over again is by a company called "Domain Registry of America." You don't have to worry about this if you don't have a website of your own, but if you do, you should be aware of the deceitful form of trickery that they are using. A domain name is the name of your website. For instance, my website is compukiss.com. The Pilot's website is thepilot.com. When you register a website, the name and address of the domain name holder and the date when it will expire become public record. The Domain Registry of America uses this information to send a "Domain Name Expiration Notice" to the registered user. They make it look like a bill and they indicate that if you do not pay the requested fee to them by as certain date your domain name will expire. Read the fine print and it says that "now is the time to transfer and renew your name from your current Registrar to the Domain Registry of America." So by filling out their form and sending them the requested amount, you are not simply renewing your domain name, you are also transferring it to them. Of course, their fee is higher than most and you will be paying them this fee for as long as you keep the domain name, unless you transfer it away from them. If you call the Domain Registry of America, you will find that they refer to the letter you received as an offer rather than a bill. They are right, but it is still extremely deceiving.

I guess there is no doubt that as long as humans are the flawed creatures that we, there will be trickery and deceit. More and more of it is found on the Internet and in Internet-related every day. So be careful out there!

---

from pg. 2

of writing paper or the page of a book—and with the tap of a finger turns it into a display suitable for taps and ...

On the paranoia front; Researchers showed a Black Hat audience how femotcell technology, used by phone companies to boost cell phone coverage, can be hacked to intercept cell phone calls, text messages and other data.

Other researchers have demoed the ability to install malicious software on a phone via a fake USB charger. Some user help is involved, in terms of not having a locked passcode.

Some retailers have partnered with technology companies to track the movement of shoppers by harvesting Wi-Fi signals within their stores. The stores include Nordstrom and Home Depot. At least one of the companies (Euclid) has promised to be a bit more transparent

Editor-in-Chief:
Stuart Rabinowitz

Protect Your Privacy with "Take Control of Your Online Privacy"

by Adam C. Engst: <ace@tidbits.com>, @adamengst
article link: <http://tidbits.com/e/14060>
2 comments

How concerned are you about your online privacy? Does it bother you when Amazon recommends products you might like, or you see Web ads related to sites you've just visited? Do you worry that your online communications could be used against you by an ex-spouse, employer, or insurance company? And while few of us have much to hide from government intelligence agencies, that doesn't mean we're all happy about the recent revelations about the NSA and its ilk. What should you do about all this? Besides watching Joe Kissell's extremely funny "None of Your Business" sketch video, that is?

<http://www.youtube.com/watch?v=5KxyF9S-1x0>

Concern about privacy is a spectrum, and we all hit it in different places. But it's a fact that your online activities are being tracked and analyzed. Some of that is good — if you're going to see ads, wouldn't you prefer they were for products that weren't offensive? — but what happens when that targeting results in you being charged higher prices or reveals an embarrassing medical condition to co-workers who see your computer screen? That's just the tip of the iceberg, but you can take steps to protect yourself from unwanted disclosures.

All this consternation is why Joe Kissell has penned what we believe is a truly essential book, "Take Control of Your Online Privacy."
Aided and edited by our old TidBITS friend Geoff Duncan, Joe has
done a fabulous job distilling all the questions we normal people
have about privacy — and what can be done about them! — into this
118-page ebook, available now for only $10.
<http://tid.bl.it/tco-online-privacy-tidbits>

The first step, for those who aren't already too concerned about privacy, is learning what you have to hide. Even if you consider your life an open book, that doesn't mean you'd be happy sharing financial details or travel plans with any random stranger. And it's not just strangers — Joe explains precisely who wants your private data and, equally important, why they want it and how disclosures can come back to haunt you.

His overall goal is to help you develop and maintain a privacy strategy, and, to aid in that effort, he explains how to lock down your Internet connection, how you can browse the Web privately, what you can do to improve email privacy, how to talk and chat privately, and the best ways to share confidential files. "Take Control of Your Online Privacy" even delves into how to keep your usage of Facebook, Twitter, and other social media sites sort of private — or at least ensure that your social media presence is unlikely to become a problem in the future.

At the end, Joe touches on how your privacy-related actions can affect your children, both now and far in the future when that picture that seemed so cute causes serious embarrassment at school. And once you've developed your online privacy strategy, you can use the one-page PDF handout and PDF-based slide deck linked in the "Teach This Book" chapter to help friends, colleagues, and family members understand online privacy issues as well. Please feel free to distribute the handout as widely as you like — it's a great summary of the main points in "Take Control of Your Online Privacy."

---
read/post comments:
<http://tidbits.com/e/14060#comments>
tweet this article: <http://tidbits.com/t/14060>

PULP Staff

Editor Stuart Rabinowitz
Distribution George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and include a one-year subscription to The Pulp as well as access to the HUGE Public Domain disk libraries. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

President:	George Carbonell	860.568–0492	george.carbonell@comcast.net
Vice President	Stuart Rabinowitz	860.633–9038	s.e.rabinowitz@att.net
Secretary:	Ted Bade	860.643–0430	tbade@cox.net
Treasurer:	Charles Gagliardi	860.233–6054	epencil@att.net
Director at Large:	Richard Sztaba		richer1@aol.com
Web Manager:	Bob Bonato		wmaster@huge.org
Membership:	Richard Sztaba		richer1@aol.com
Integrated SIG:	Stuart Rabinowitz	860.633–9038	s.e.rabinowitz@att.net

October 2013

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1 1982 Lotus 1-2-3 announced	2	3	4	5
6	7	8	9	10	11	12
13	14	15 *General Meeting 7 PM*	16 **Ada Lovelace Day**	17	18	19
20	21	22	23 **Mole Day**	24 2001 iPod announced	25	26
27	28	29 1951 IEEEE Computer Society founded	30	31		

from pg.6

Horse" means an object looks like it serves one purpose, but really has an unobvious, usually nefarious, purpose. Cisco, the networking company, describes a Trojan as, "It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems". In cyber speak, a Trojan Horse, typically shortened to the simple moniker "Trojan" is a program that appears to have a useful function, but after being installed by the user, the Trojan may be used to perform other undesirable functions. Some Trojans are money makers for their authors because they place paid (and usually unwanted) pop up advertisements (Adware) on the infected computer, redirect web searches, or shift online purchases to a seller not of the buyer's choice without his knowledge. Some Trojans are keyloggers, which are commonly used for identity theft, or to give unauthorized users access to a computer system. Trojans are often spread through intentionally downloaded software, surreptitiously bundled with another often legitimate program, from email attachments, and purloined websites with executable contact (ActiveX is sometimes used for this). Some Trojans can be installed on the target computer by way of code written in Java, or a Java script, that when executed, implants the harmful content on the victim computer.

One of the more recent and costly types of malware to attack our computers is generically referred to as "Rogue Antivirus Software", which is usually implanted on the victim's computer by a Trojan. There are thousands of these rogue programs in current circulation, infecting millions of computers at any given time. Rogue antivirus is sometimes installed by the user using "social engineering" tactics, which tricks the user into clicking on something that installs the rogue software. Some of the common lures to ensnare the user into loading rogue software on the computer are offers for free screen savers, toolbars, utilities to play specific video formats (often attached to an email), sham online security scanners, contaminated PDF files, insecure web browsers, and other vectors. The common thread of this rogue software is an authentic looking popup that informs the user that his computer is (falsely) infected with hundreds of viruses and Trojans, and for a fee it will clean the computer. These popups which will not permanently close will typically hijack the computer, destroy the installed legitimate security software, prevent access to online services that can kill it, prevent cleaning utilities from executing, and otherwise take control of the computer until the user pays a fee, typically $30 to $70. This fee is to be paid by credit card or other online payment service to a website that looks legitimate, but is really a complete scam. Not just will the rogue software not clean the computer of the pseudo infections after the fee is paid, but now a cybercriminal, often in Russia, has the user's credit card information. it is not uncommon for that same credit card information to promptly be sold on illicit websites, and to have substantial unauthorized charges appear on the compromised credit card account.

While there are many other cyber threats out there, those listed above are among the most commonly encountered by users. The traditional antivirus software will protect from some of the threats listed, but not all of them; this enhanced security capability is in the purview of the comprehensive security suite, or a combination of different types of individual security utilities, and not the free standing antivirus program. this is explicitly why I currently recommend a high quality integrated security suite, rather than an antivirus program. There are several good commercial security suites available, as well as a few free security suites. Just be aware that antivirus software by itself is inadequate to protect against today's contemporary cyber security threats.

Ira Wilsker is a member of the Golden Triangle PC Club as well as Director of the Management Development Program at Lamar Institute of Technology, in Beaumont, TX. He also hosts a weekly radio talk show on computer topics on KLVI News Talk AM560, and writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a police officer who specializes in cybercrime, and has lectured internationally in computer crime and security.