The PULP

Newsletter of the Hartford User Group Exchange

http://www.huge.org Volume 34 Issue --11

November 17th General Meeting:

Pat with El Capitan

Knights of Columbus
2533 Main Street,
Glastonbury, CT

Q&A Session: 7 PM–7:15PM

Meeting starts at: 7:15PM

Member of apcug

An International Association of Technology & Computer User Groups

Contents	Page

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.

MEETING LOCATION

Knights of Columbus
2533 Main Street,
Glastonbury, CT

From The Editor

by Stuart Rabinowitz

This month's meeting is Pat doing a demo of El Capitan (OSX 10.11). I hope he points out the new features of "Disk Utility". Next month will be "Gifts for Geeks".

In the news: Microsoft seems to really want people to get Windows 10, so it plans to start automatically downloading it to users' computers next year.

If you are one of the CoinVault and Bitcryptor ransomware victims, you can now recover your files for free. The tool can be found at https://noransom.kaspersky.com.

Google plans to merge Chrome OS and Android.

There are some user reports of Surface Book and Surface Pro 4 problems, which is reportedly faster than a MacBook.

Windows-centric IBM has changed its tune on Mac deployments by planning to add 30,000 in 6 Months. It estimates a 40% support savings. Now

Researchers have demo'd how a tea kettle can kill your cloud. A report says headphones can be used to hack a smartphone, Researcher says Fitbit can be wirelessly hacked to infect PCs, Fitbit says not true.

Facebook has figured out why it's draining your iPhone battery, it calls home to see if there is anything new and plays a silent audio track.

Tech support scammers are starting to put Mac owners in crosshairs. Watch yourself.

Western Digital self-encrypting external hard disk drives have flaws that can expose data.

The original Sun Trust Bank severance deal requires IT workers to be on call for two years, They have since changed their mind.

It's official North America is out of new IPv4 addresses and the US rank drops to 55th in 4G LTE speeds.

Wikipedia blocks 381 user accounts for dishonest editing and Amazon is suing 1,000 fake(?) reviewers.

Until next month…Happy computing!!Send your comments to editor@huge.org

Stuart Rabinowitz, Editor

A Little Computer Quiz

1 This month marks the 34th anniversary of the founding of what nationally known computer user group?

2 Where was the first meeting held?

3 What were the original dues?

4 Who was the first President?

5 Who was the guest speaker at the tenth anniversary meeting?

October Quiz Answers

1 In 1973 MECC developed a business simulator educational game. What was it called?
A Lemonade Stand

2 Another early educational game had people shooting down UFOs while learning to type. What was it called?
A MasterType

3 Who developed it and on what computer platforms?
A Lightening Software for the Apple II, MS-DOS, & Commodore 64

4 In 1992 you could play Rube Goldberg and learn engineering and physics playing what game?
A The Incredible Machine which ran on MS-DOS & Mac.

5 Twitter began life in 2006 as an SMS-based blogging service, what was it called back then?
A "twttr" and the SMS explains the 140-character limit.

In 1991 the Ig Nobel Prize was initiated to recognize unusual scienitific research achievements. Ivette Bassa was recognized in 1992 for what achievement?
A She won for her role in the crowning achievement of 20th century chemistry, the synthesis of bright blue Jell-O.

Malvertising

By Dave Palmer, Member, Tampa PC Users Group, Florida
March 2015 issue, Bits of Blue
www.tpcug.org
dkp205 (at) hotmail.com

Just as 'malware' is short for malicious software, 'malvertising' is short for malicious advertising. Like many services on the Internet, online advertising has become highly automated. And like nearly everywhere else on the Internet, cyber criminals have found ways to corrupt that automation to turn a profit.

Have you noticed that after you do some online research for a specific purchase that you soon see online ads for similar products on different websites? That's a result of websites leaving 'cookies' on your computer. Cookies don't identify you personally but they can identify you as having an interest in a category of products. In addition, the IP address of your computer provides a general geographic location. When you visit other websites, they read your IP address and any cookies left recently. They also provide this information to an ad network which quickly adds interest-based or location-based ads to the websites you visit. Now advertisers and ad networks know your approximate location and the categories of products you're interested in.

How online advertising works

Ad networks consist of publishers, advertisers and the middlemen who connect the two. Publishers are the owners of the websites you visit. They sell advertising space on their websites. Then there's the advertiser, the individual or business that has a product or service they want to advertise. They buy advertising space on websites. The sites you visit usually do not play a direct role in choosing the ads you see. Instead, a middleman, a third-party advertising company, manages the ad selection and placement for both the publisher and advertiser. This makes the process more efficient for everyone. The process is highly automated – humans are only rarely involved – usually only at the beginning for initial approval.

This business model, advertising supported by ad networks, supports a large portion of the Internet, providing the 'free' information and web-sites we have come to rely on. Online advertising can come in many forms. Ads can be a single static image without animation, ads can be animated in one of several different ways, or ads can be video-based. There are popup ads, pop-under ads, banner ads and a dizzying array of shapes sizes, styles, formats and technologies involved.

As this advertising business model has developed, ad networks have spread across the Internet. Over time the sheer volume of ads has given rise to a massive and tangled conglomeration of ad networks, ad exchanges and other related businesses that buy, sell, trade and swap ads and ad space constantly as the tides of supply and demand shift constantly. Of course, opportunistic cyber criminals weren't far behind. They soon found many ways to abuse the system for profit.

Delivering the payload

Bad guys may scam the system by posing as legitimate advertisers. They may hack into legitimate but dormant accounts. Either way they gain access to the ad networks. They then create legitimate-looking ads to disguise malware to either deliver malware directly from booby-trapped ads, or to redirect viewers to a poisoned website that delivers the malware payload. In most cases neither the publisher (the website displaying the ad) nor the ad network providing the ad knows the ad is booby-trapped.

One major obstacle to detection of malicious ads is that they are not persistent. Once the user leaves a website or closes the browser, all traces of the ad disappear. In addition attackers take great pains to make their ads hard to detect. They may enable their malicious payloads only after their ads have been approved. They may set the malicious ads to only attack every 10th user. They may set up many different domains and redirect victims many times before the victims reach the poisoned website. These and other practices make detection quite difficult.

Once installed on the victim's computer, malware may look for login information for e-mail, social media, and bank accounts, as well as for identity information. In some cases the malware can lock the user's computer and demand a ransom.

Click fraud

Another way the bad guys' corrupt legitimate advertising is to commit 'click fraud.' Click fraud occurs in pay per click (PPC) online advertising when machines or programs imitate a legitimate user and click on an ad to generate a charge per click without having any interest in the ad itself.

Hackers may use the malware installed by ads to commandeer the victim's computer and add it to the hacker's botnet – a network of hijacked computers used for criminal activities. Botnets (bots) are often used for click fraud. Click fraud sometimes begins when unscrupulous publishers or ad networks hire hackers to boost their numbers or to generate income. Computers in the botnet are instructed to visit various websites and click on specific ads.

Here are a few eye-opening stats from an adweek.com article (http://goo.gl/9zrH7X). Up to 50% of publisher activity is from botnets - automated click fraud. Bots account for 11% of display ad views and 23% of video ads. Of the $43.8 billion in ad revenue, fraudulent activity accounts for $6.3 billion. More than half of traffic from 3rd parties claiming to lift publisher's traffic numbers comes from bots. Click fraud is a major problem in that it raises costs for legitimate publishers, advertisers and ad networks. Click fraud can also be used indirectly to attack legitimate competitors and force them to pay higher advertising costs.

What can be done?

Unfortunately there's little agreement on who is responsible for addressing these threats. Both publishers and advertisers need to take action to limit malvertising on their networks. In addition a number of companies now exist to validate that ads are being seen by humans. They include WhiteOps, ComScore, Integral Ad Science, The Media Trust and Double Verify, among others. But since consumers are under a serious and direct threat, we must do what we can to protect ourselves.

How to protect yourself

In some cases the bad guys are hoping they can redirect your browser from your intended website to a poisoned website so they can download malware into your computer. For that scenario to work your browser has to:

1) allow the redirect and
2) contain a vulnerability that allows malware to be installed and
3) operate in administrative mode to allow the installation.

I've included some instructions below on how to set up the Big 3 browsers to prevent redirects*. In case you still operate daily in administrative mode, Merle wrote an excellent explanation of how to create a standard user account in the October 2014 edition of the TPCUG newsletter.

In some cases the ad is booby-trapped with some executable script, often Flash, JavaS-

cript, etc. Your protection is to use script-blocking software - NoScript for Firefox and ScriptSafe or Script Blocker for Chrome. Things are a bit more complicated with Internet Explorer. Don't use Internet Explorer unless absolutely necessary. If you're an IE die-hard check out the instructions here: http://goo.gl/YTcQpK.

Although script blockers are not terribly convenient, removing malware is way beyond inconvenient. In the end, the threats from malvertising are really no different from other malware threats across the Internet. So the protection advice is no different either. To reduce the threat from vulnerabilities, first minimize your 'attack surface,' that is, remove programs you're not using. The next step towards minimizing your vulnerability is to keep everything updated – your operating system, browsers, programs, add-ons, plug-ins, etc. Backup your data and system regularly. Use a password manager and strong passwords.

Preventing redirects*
Chrome

To prevent Chrome from being redirected to another site without your knowledge, click the "Customize and Control Google Chrome" button. The button has three horizontal lines on it.

Click "Settings."
Click the "Show Advanced Settings" link to display more setting options.
In the Privacy section, click "Enable Phishing and Malware Protection."
Close the browser window.

Google now displays a warning if the browser is trying to redirect you.

Mozilla Firefox
In Firefox, click the "Open Menu" button, which has three horizontal lines.

Click the "Options" button in the panel that opens.
Click the "Advanced" button and then the "General" tab.
In the Accessibility section, check the "Warn Me When Websites Try to Redirect or Reload the Page" box. Click "OK."

Internet Explorer
Internet Explorer doesn't have a way to expressly stop redirects. Instead, you have to limit the whole Internet.

Click the "Tools" button, which looks like a gear
Click "Internet Options"
Click the "Security" tab.
In the Security Levels for This Zone pane, set the slider to "High." This prevents IE from running ActiveX controls, which is how many browser redirects are carried out. However, this might prevent some safe sites from loading correctly.
Click "OK."

These steps work for Google Chrome 40, Internet Explorer 11 and Mozilla Firefox 35. Other versions might use different steps.

*The above instructions were taken from: https://www.ehow.com/how_8744477_do-links-redirectingdifferent-sites.html

What are Websites Doing with Your Personal Information?

By Ira Wilsker, *Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper www.theexaminer.com; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.*

WEBSITES:
http://www.govtech.com/data/How-Do-Websites-Use-Your-Data.html
https://identity.utexas.edu/privacycheck-for-google-chrome
https://identity.utexas.edu/idwise
https://identity.utexas.edu/strategic-partners
https://chrome.google.com/webstore/detail/privacycheck/poobeppenopkcbjejfjenbiepifcbclg
https://www.ghostery.com

You have likely noticed that the banner ads and other forms of advertisements on many of the web pages visited appear to "coincidently" be for many of the same items that you have recently searched for online. You may even notice that many of these ads are also from many of the same online sellers whose web pages you have recently visited. In some cases, you may also see online ads for direct competitors of previously visited websites, offering many of the same or similar products that you have looked at on other websites. It should not be surprising that the owners of many websites, as well as many third party advertisers, use a variety of tracking technologies to gather information on you, as an individual, the types of websites that you visit, and the products and services viewed. While many users find this targeted advertising interesting and useful, and even possibly necessary in order to support "free" web sites and online services, many others consider the gathering of such personal information as a gross violation of personal privacy.

Some of the more common methods of compiling and distributing this personal information and shopping preferences are the placement of "tracking cookies" on the user's device; web bugs or web beacons (small graphic files which transmit information when opened, often 1 pixel in size); and the dissemination (sale) of personal information entered on a website. Cookies are small, alpha-numeric and text based pieces of data which are by default, placed on the hard drive or other storage of the device being used to view a website; while some types of cookies are benign and necessary to compile shopping carts, store passwords and other login information, and save other information that can speed the web process, some other types of cookies may not be so desirable.

The most common type of unwanted cookies is often known as "tracking cookies", which are typically placed on the hard drive or other storage medium, just as other cookies, but these cookies can also be read by other third parties as a method of gathering information about the user, mostly for targeted marketing purposes. There are many companies that have a lucrative and highly profitable business selling access to the tracking cookies which they have previously been placed in storage, most often by simply visiting a web page. Almost all browsers give the users the option to control which cookies can be saved and accessed, but the default is to accept all cookies. Tracking cookies that are currently saved in the device storage can often be easily and quickly removed by most of the reputable (and often free) security scanners, such as Malwarebytes (malwarebytes.org) and SuperAntiSpyware (superantispyware.com).

What many users might find shocking is that they unknowingly and explicitly allowed many of the websites that they visit to place tracking cookies and other marketing information on their computers and smart devices. When I

mention this to users at some of my security and privacy presentations, some of those present get very agitated, and vehemently deny that they ever gave permission for websites to place such information on their computers and other devices. My typical response is something to the effect of "Did you ever read the privacy statement on those websites when displayed, or simply click on the "I Agree" box when first visiting them?" Most of the honest, but still aggrieved users, acknowledge that they never fully read the privacy statements on the websites visited, with the typical response being that the privacy statement is too long to read, or it is written in "legalese" which they cannot readily understand, so they simply "agree" in order to get access to that particular website.

Complex privacy statements, often blindly agreed to, have been a popular tool to legitimize the placement of that website's or other third party commercial tracking information on your computer, smart phone, tablet, or other device. These tracking devices are often a significant source of revenue for the website owner, and are often utilized by some of the largest and most reputable online vendors. In a recent article by Omar L. Gallaga, of the Austin American-Statesman, dated May 11, 2015, and reprinted by "Government Technology", Gallaga wrote, "How Do Websites Use Your Data? A new tool in Google Chrome puts website privacy policy language in plain English, letting you easily know whether your email address is shared or the site has access to your Social Security number, and if it tracks your location."

This free new tool, currently only available for Google's Chrome browser, is "PrivacyCheck", a Chrome browser extension (plug-in) which was developed by the Center for Identity at the University of Texas - at Austin (identity.utexas.edu). According to the Center for Identity, "PrivacyCheck is a browser add-on intended to provide consumers an overview of the ways in which companies use their personal data in a graphical, 'at-a-glance' format. ... PrivacyCheck surpasses existing add-ons, apps, and certifications by using a Data Mining algorithm to access the text of any webpage. The user provides the URL for the company's privacy policy and PrivacyCheck searches the page, returning icons that indicate the level of risk for several types of PII (Personally Identifiable Information)". PrivacyCheck can be downloaded for Chrome from the Chrome web store at chrome.google.com/webstore, and entering "PrivacyCheck" in the search box. The latest version of PrivacyCheck, as I am typing this, is version 1.0.5, dated May 14. It is important to know that federal and state laws require businesses with a web presence to post their privacy policies, and there are often harsh penalties for violating those posted privacy policies.

To use PrivacyCheck to determine the degree of privacy risk on a particular web site, download and install PrivacyCheck from the Chrome web store (chrome.google.com/webstore). Once installed, open the selected website using the Chrome browser, and locate the privacy statement, often linked at the very bottom of the webpage; open the privacy statement page. On the top right of the Chrome address bar is a small icon which is light brown in color, and has what appears to be a lower case "i" within a brown circle; click on that icon. Once clicked, "Browse to a privacy policy and click Start". Within seconds a series of 10 larger icons will appear, with an easy to comprehend green, yellow, and red coloration, indicating the degree of privacy risks associated with that privacy policy and website.

Moving the cursor over each of the large icons will explain what it represents: the "envelope" icon represents what the website does with the user's email address, red indicating that

the website uses, sells and shares the email address to others; the second icon represents the magnetic stripe on a credit card, and indicates what the site does with credit card information; the three asterisks "***" represent what is done with the user's social security number, green indicating that it is not collected or otherwise used; the "megaphone" indicates the marketing use of your private information, red indicating that the website sells your information to others for marketing purposes; the "compass" icon indicates what the website does with detected location information, red indicating that the website sells the user's location information to third parties; the sixth icon, circular with two eyes, indicates the policy on information gathered from children; the "badge with star" icon indicates the distribution of information to law enforcement, red indicating that the site will provide information to law enforcement without a warrant or subpoena; the "open book" indicates the policy on posting privacy policy changes and giving the opportunity for users to opt-out; the "pie chart" icon indicates whether or not the user can modify his own information; the tenth icon, which looks like a cloud with directional arrows, indicates what the website does with aggregated information, yellow indicating that aggregated information is distributed, but personally identifiable information has been removed.

PrivacyCheck is an excellent method to determine what commercial websites are really doing with your personally identifiable information (PII), but its major weakness is that it (currently) only works with the Chrome web browser. Users of other browsers may find some privacy utilities that provide significant privacy protection while online.

On all of my PCs, as a browser add-on, I have been using a free, popular browser extension called "Ghostery" (www.ghostery.com), which will seamlessly run on computers using any of the major and popular browsers including Firefox, Chrome, Opera, Safari, and Internet Explorer, as well as on mobile devices running the Android and iOS operating systems. According to its website, Ghostery claims to have, "The largest tracker database on the internet, constantly growing; Ghostery has the largest tracker database available on the web. We meticulously select, profile and cull over 2,000 trackers and 2,300 tracking patterns." Ghostery displays the tracking information on almost every web page opened, and gives the user the ability to allow or block trackers as desired.

Our personal privacy should be taken very seriously. Once third parties have access to our personal information, it is virtually impossible to get it back. Most of the browsers offer an option or setting to control privacy, which may be called "Do Not Track", "Reject Third Party Cookies", or some similar name. By using PrivacyTracker, Ghostery, browser privacy settings, and other utilities, our individual privacy may be better protected.

PULP Staff

Editor Stuart Rabinowitz
Distribution George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and includes a one-year subscription to The Pulp. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

Leader:	George Carbonell	568–0492	george.carbonell@comcast.net
Secretary:	Stuart Rabinowitz		
Treasurer:	Charles Gagliardi	233–0370	epencil@aol.com
Director at Large:	Phil Manaker	659-4584	amanaker@earthlink.net
Director at Large:	Ted Bade	643-0430	tbade@cox.net
Director at Large:	Stuart Rabinowitz	633–9038	s.e.rabinowitz@att.net
Web Manager:	Bob Bonato		bob@bonatodesign.com
Membership:	Richard Sztaba		richer1@aol.com
Integrated SIG:	Stuart Rabinowitz		

November, 2015						
1	2 1920 KDKA broadcasts 1st radio program	3	4	5	6	7
8	9 1982 Compaq Computer announced	10	11	12	13	14
15	16	17 **General Meeting** **7 PM**	18	19 2004 *World of Warcraft* released	20	21
22	23	24	25	26 Thanksgiving	27	28
29 1972 Pong created	30					