Newsletter of the Hartford User Group Exchange November, 2012

The PULP

HUGE this month:

General Meeting: Nov. 20th

PC (& Mac) Clinic -- Bring your problems (or questions) for some help

See you there!

East Hartford Public Library
Main St. & Central Ave., E. Hartford, CT.

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

H.U.G.E.

Contents:

Member of
Association of Personal Computer User Groups
APCUG

UGC

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 LOCATIONS
East Hartford Public
Library
Main & Central Avenue
in the Lion's Room
(downstairs)

Editor's Corner

Happy 31st Birthday HUGE! This month's meeting will be a PC (& Mac) clinic for your problems (or questions). December will be my gift suggestion night.

In the news: The (previously rumored) iPad mini will be on sale Nov. 2 starting at $329. Just in time for the holidays, there will be the new iMac, iPad,4 and a 13" MacBook Pro with a retina display.

Beginning some time around Oct. 21 Apple started scrubbing most Macs of older Java browser plug-ins (during the update process), a move that will force users to download the software from Oracle.

As part of a contest during the Hack In the Box Conference, Chrome was hacked. This earned the hacker $60,000.

In a copyright infringement takedown request to Google, Microsoft wrongly accused websites such as BBC, CNN, Huffington Post, Wikipedia and yes, even Microsoft, of linking to illegal content (i.e. copies of Win 8).

Major Internet Service Providers (AT&T, Comcast, Verizon and Time Warner Cable) have started a Copyright Alert System (CAS) which aims to warn Internet users who allegedly download (illegally) and share music, videos and other copyrighted content over peer-to-peer file sharing networks.

It's now official, it is illegal for employers and universities in California to request social media log-in information—that is, user names and passwords for Facebook, Twitter, or e-mail from employees and students.

Intel is working to develop tiny chips to run wearable computers. They are 'exploring' chips half the size of its Atom processor, which are currently used in many smartphones. Currently the Atom uses about 1 or 2 or 3 watts, the new chips would be in the milliwatt range.

Editor-in-Chief:
Stuart Rabinowitz

See some additional info on pg. 9 & 11

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.

Since HUGE will be celebrating its 31st anniversary in November, which probably puts it near the top in for oldest computer user groups, I thought this months quiz would be about other tech records.

1 Wendy Southgate holds a Google record, what is it?

2 Want to take a guess as to the record for the most people assembling the most computers at the same time?

3 Can you name the world's largest video arcade?

4 Can you name the largest (working) cell phone?

5 While not technically computer related, can you name the world's most expensive camera?

Answers to October, 2012 Quiz

This past June one of science fiction's greats passed away, so this month there is a theme to the quiz.

1 The butterfly effect describes how a small change at one place can result in large differences to a later state. The theoretical example is a hurricane's formation being contingent on whether or not a distant butterfly had flapped its wings several weeks before.. or a time traveller stepping on a butterfly in the past and changinging the future. Can you name the story and year it was published that first mentioned the concept?
A "A Sound of Thunder", a 1952 short story by Ray Bradbury

2 Google has a fleet of self-driving cars (300k miles & no accidents), but this author described an intelligent vehicle that can both drive itself and arrest people in 1951. What was the story?
A The Pedestrian

3 We all use Automated Teller Machines (ATMs) and the first appeared in Ohio in 1959. They were however described in a 1953 novel, what novel?
A Fahrenheit 451. To be fair an experimental ATM (for deposit only) was tried by City Bank of New York in 1939 but canceled after 6 months due to lack of use.

4 In what book did the author have characters walk around with “seashells” and “thimble radios” attached to their ears that were used to communicate with each other?
A Sounds like bluetooth cellphones, also from Fahrenheit 451

5 In 1953 TVs were a bit smaller and fatter then they are now, but again this same author wrote about interacting with “parlor walls”. Can you name the author?
A Ray Bradbury. The book was Fahrenheit 451 which also predicted the death of the printed word.

Secure Your Wireless (Wi-Fi) Connection

by Ira Wilsker
1Ira is a member of the Golden Triangle PC Club, an Assoc. Professor at Lamar Institute of Technology, and hosts a weekly radio talk show on computer topics on KLVI News Talk AM560. He also writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.

WEBSITES:
http://www.makeuseof.com/tag/7-important-features-wireless-router
http://compnetworking.about.com/od/wirelesssecurity/tp/Wi-Fisecurity.htm
http://wiki.answers.com/Q/How_do_I_change_my_wireless_network%27s_security_settings
http://en.wikipedia.org/wiki/Wi-Fi
http://www.wi-fi.org
http://en.wikipedia.org/wiki/War_chalking
http://www.blackbeltjones.com/warchalking/warchalkingo_9.pdf **(Pocket War Chalking Card)**
http://en.wikipedia.org/wiki/War_driving

Almost all newer laptop computers as well as tablets, smart phones, video game consoles, and home entertainment systems utilize Wi-Fi as a primary or secondary method of connecting to the internet or some other network. According to published reports from several sources, the majority of home internet users have some form of Wi-Fi in their homes, and Wi-Fi is very commonly used in business, commercial, and academic environments. While the basics of Wi-Fi security apply to almost all Wi-Fi networks, home users have become especially vulnerable because many have never implemented anything more than the minimum default security settings when installing and setting up the hardware.

The Wi-Fi Alliance (www.wi-fi.org) defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards." Wi-Fi is a fancy radio device that sends and receives streams of data through the air, just as any other 2-way radio device. As consumers, we often see the presence of Wi-Fi in terms of its standard designations, such as 802.11b, g, or n (as in 802.11n), each of these terms indicating the speed, bandwidth, and channels available under those industry standard protocols. While new speeds and protocols are always being developed and tested, the fastest and most powerful of the current widely available standards is 802.11n, which is capable of a theoretical speed of 540 Mbps. A portion of the standard provides for downward compatibility, meaning that devices made for one of the newer standards, such as the "n" standard, must also be capable of communicating with lesser devices, such as the "b" and "g" standard devices.

For home use, most of us have some form of Wi-Fi access point, typically either a free standing device directly connected to the internet, integrated with a wired (Ethernet) router, integrated with some form of modem (common with cable and DSL internet services), or as a combination unit of "all of the above." In my home I have a major name-brand integrated unit that combines a broadband modem, 4-port router (four Ethernet ports for Ethernet cable connected devices), a USB port to connect a printer or other USB devices to the network, and an 802.11n wireless Wi-Fi with MIMO (Multiple-Input-Multiple-Output technology) for improved performance. Purchased from one of the big box electronics stores for about $70, my multi-function device replaced the less-capable modem supplied by my internet service provider (ISP), and offers more features, speed, and security than the one provided by my ISP.

For me, enhanced security was one of the primary reasons for replacing the older technology modem provided to me from my ISP just a few years ago. This older broadband Wi-Fi modem from my ISP incorporated the mid-speed 802.11g wireless access point, with archaic security and encryption capabilities. Being fully cognizant that home (and business) Wi-Fi networks are common targets of hackers and crackers, I wanted to harden my system from attack, and the newer integrated Wi-Fi access point offered far superior protection than did my ISP provided unit.

One of the first requirements of a reasonably secure Wi-Fi network is to implement the best encryption available on that particular device, such that unauthorized individuals who pick up the Wi-Fi signal will only find random garbage, rather than a useful stream of data. Since only Wi-Fi devices with the proper encryption key can exchange readable data, enabling the best type of encryption compatible with both devices (access point and remote device) will help protect the personal Wi-Fi network from intrusion. Unencrypted Wi-Fi leaves the entire network open to attack which can be used to steal personal data, passwords, user names, credit card information, and other information that can be illicitly used for a variety of malevolent purposes, including identity theft. At a minimum, an unencrypted home Wi-Fi network works like a free open network at a coffee house, where anyone can "leach" (steal or otherwise use) your internet access, slowing your connection, as the crooks are using your bandwidth. This "leaching" or theft of internet service may lead to unintended consequences, as it is not unknown for illicit drug dealers, pedophiles and child pornographers to use an innocent persons unprotected Wi-Fi in order to conduct their evil enterprises; if law enforcement tracks the bad guys, it typically leads to the innocent Wi-Fi owner, rather than the miscreant who purloined the system.

A common game of hackers and crackers is "War Driving" (en.wikipedia.org/wiki/War_driving) where people with Wi-Fi computers and some readily available software drive around an area picking up and recording the locations of all detectable Wi-Fi networks, and posting the locations on a GPS coordinated electronic map. Even Google compiled a massive listing of Wi-Fi networks as its specialized vehicles travelled up and down virtually every street in the country for its Google Maps "Street View" service, creating a massive firestorm with privacy and security specialists. While Google has graciously removed public access to its "war driving" database, there are a myriad of websites that post the maps and data found by amateur War Drivers, such that anyone can easily locate and tap into an unencrypted Wi-Fi system. Parallel to war driving is war chalking, war walking, war jogging, and war bicycling, which is common in densely developed urban areas. The simplest iteration of these is to use chalk on the side of a building or sidewalk to show the presence of a vulnerable Wi-Fi system, telling anyone on the street about the unfettered broadband internet access, compliments of an often unwilling provider. There is actually a standardized list of chalk symbols indicating the type and availability of Wi-Fi signals, these symbols being available from en.wikipedia.org/wiki/War_chalking.

Virtually all Wi-Fi access points offer some form of encryption. During the initial setup of the Wi-Fi system, the user is often requested to select an encryption method, or else "no encryption" is often the default setting, making the network accessible to anyone within range. The most common forms of encryption for Wi-Fi access points are
WEP, WPA, and WPA-2. WEP (Wireless Encryption Protocol) is the oldest and least secure of the common encryption methods; while only having slight degradation in performance and speed, it is virtually useless against all except the least sophisticated hackers, with instructions on how to crack and defeat WEP being readily available on the internet. WPA (Wi-Fi Protected Access) is better than WEP in terms of security, but degrades performance a little more than WEP. On most contemporary home Wi-Fi access points, WPA-2 is the best of the commonly available encryption methods, but is slower and requires more computing resources then WPA; except for the most bandwidth intensive uses, the majority of users will not really notice the slightly slower performance of WPA-2.

Another security trick embodied in almost all Wi-Fi access points is the "Hide SSID" setting. SSID means "Service Set Identifier", also called "Network Name". At a minimum, the user should change the network name to some meaningless name that is not readily connected to the particular system. The reason for changing from the factory default name (often the name of the manufacturer, such as

cont. on pg. 8

Debunking Some Common Myths

Author: Mindi McDowell

Security Tip (ST06-002)
US-CERT
US Computer Emergency Readiness Team
www.us-cert.gov

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

How are these myths established?

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

Why is it important to know the truth?

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

What are some common myths, and what is the truth behind them?

? Myth: Anti-virus software and firewalls are 100% effective.
? Truth: Anti-virus software and firewalls are important elements to protecting your information (see Understanding Anti-Virus Software and Understanding Firewalls for more information http://www.us-cert.gov/cas/tips/ST04-005.html). However, neither of these elements are guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.

? Myth: Once software is installed on your computer, you do not have to worry about it anymore.
? Truth: Vendors may release updated versions of software to address problems or fix vulnerabilities (see Understanding Patches for more information http://www.us-cert.gov/cas/tips/ST04-006.html). You should install the updates as soon as possible; some software even offers the option to obtain updates automatically. Making sure that you have the latest virus definitions for your anti-virus software is especially important.

? Myth: There is nothing important on your machine, so you do not need to protect it.
? Truth: Your opinion about what is important may differ from an attacker's opinion. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other people (see Understanding Denial-of-Service Attacks http://www.us-cert.gov/cas/tips/ST04-015.html and Understanding Hidden Threats: Rootkits and Botnets for more information http://www.us-cert.gov/cas/tips/ST06-001.html).

? 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.

cont. on pg. 9

How to Keep Data on Your Laptop Secure

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

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

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

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

Instead, consider the free, open source program called TrueCrypt. This software provides industrial-strength encryption while being very easy to use.

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

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

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

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

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

While the encrypted drive is mounted, the contents can be accessed in their unencrypted form by any program you wish to use to access them.

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

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

TrueCrypt also supports a variety of high-powered encryption algorithms. TrueCrypt documentation is obviously targeting the overly paranoid, including directions on how to use "plausible deniability" if a thief ever

from pg. 5

"Linksys") to a non-descript name is that there are online directories with default encryption and password settings for unmodified Wi-Fi access points; hackers can easily break into networks that are only using the factory default settings. An even better trick, if available on the Wi-Fi access point, is to totally hide the SSID, meaning that the network name is not openly transmitted, and only those in range who know the network name can connect to it. While not foolproof or totally secure, hiding the SSID is a simple way to make it more difficult for hackers to find your network. If war driving through your neighborhood, hackers may likely miss networks with a hidden SSID, while picking up the other, possibly more vulnerable neighborhood networks.

Another feature that can be enabled to restrict unauthorized access to your home network is "MAC address filtering" (Media Access Control). Every device that can connect to the internet has a unique MAC address, usually a series of about six two-digit alphanumeric characters separated by periods. While MAC addresses can be counterfeited or spoofed, filtering only allows selected devices, as indicated by their individual MAC addresses, to access the network. By entering the authorized MAC addresses into the filter, and enabling the filter, only those approved devices can connect to the network. Likewise, the filter can prevent specific devices from accessing the network.

On my laptop computer and on my smart phone I can see several nearby homes that have Wi-Fi, some of which are not properly encrypted and accessible to anyone within range for any purpose, including illegal or other illicit activities. I cannot easily see networks with a hidden SSID. The unprotected household Wi-Fi networks are so vulnerable, when one neighbor had his home broadband connection out of service, and was waiting for the ISP to come and repair it, he illegitimately used another neighbor's Wi-Fi until his was repaired. Do you really want someone else using your network without your permission or knowledge? Secure your Wi-Fi, or face the possible consequences.

Can QR Codes Spread Computer Viruses?

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

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

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

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

Kasperky Labs has detected two samples of malware delivered via QR codes, both targeting Android phones. One of them sends SMS messages from the infected phone to a premium-priced number; each text message costs the victim six dollars! Other types of malware can scoop up your contacts list, send spam emails in your name, and wreak other sorts of mischief. (https://www.securelist.com/en/blog/208193145/Malicious_QR_Codes_Pushing_Android_Malware) <http://bit.ly/qGXZig>
http://bit.ly/qGXZig
Can a QR code itself contain malware? Theoretically, yes, but it wouldn't do much. A QR code can contain only a limited amount of data: 7089 numeric characters or 4296 alphanumeric characters. You can't write much of a program in that space. But a QR code can easily take you to a malicious site.

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

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

Cont. pg. 11

from pg. 6

If your information happens to be in the database, it could be collected and used for malicious purposes. It is important to pay attention to your credit information so that you can minimize any potential damage (see Preventing and Responding to Identity Theft for more information http://www.us-cert.gov/cas/tips/ST05-019.html .

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

? Truth: It is possible that running newer or larger software programs on an older computer could lead to slow performance, but you may just need to replace or upgrade a particular component (memory, operating system, CD or DVD drive, etc.). Another possibility is that there are other processes or programs running in the background. If your computer has suddenly become slower, it may be compromised by malware or spyware, or you may be experiencing a denial-of-service attack (see Recognizing and Avoiding Spyware http://www.us-cert.gov/cas/tips/ST04-016.html and Understanding Denial-of-Service Attacks for more information http://www.us-cert.gov/cas/tips/ST04-015.html).

Parallels--Critical and Urgent Windows 8 Service Advisory

Excited about Windows 8? So are we! Below is critically important information to help you successfully enjoy Windows 8 on your Mac. **Please read this entire notice, as it may affect your computer's performance.**

Upgrading from an existing Windows OS to Windows 8?

Upgrading from an existing Windows OS to Windows 8? We **strongly suggest** waiting until Parallels has finalized testing the upgrade process. **Upgrading now may damage your virtual machine, causing you to lose all your**

cont. on pg. 11

forced you to give them your password. Let’s all hope that’s just an extreme of little probability for most of us.

Here are a few warnings:

? The passphrase or word you use is going to be the weakest link. Encryption is still easily cracked if you use a bad password. If you choose a passphrase which is easy or obvious, then a dictionary attack can always be mounted on your machine to unlock the encrypted volume quickly.

? Having an encrypted volume is useless if your important files are also elsewhere in unencrypted form on your machine.

? Be sure to have secure backups which are updated regularly. It’s preferable to keep these unencrypted, but secure, just in case you lose the encrypted volume or happen to forget the password. Without your password, the data cannot be recovered.

? Understand that files are never 100% secure. All encryption can theoretically get hacked. The reason for encryption is to make the effort and cost of hacking the files so astronomical that it is simply impractical.

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

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

November 2012

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				1 1920 KDKA 1st radio program broadcast	2	3
4	5 **Back to the Future Day**	6	7	8 1984 Tandy 1000 introduced	9	10
11	12	13	14	15 1971 1st ad for Intel 4004	16	17
18	19	20 General Meeting 7 PM	21	22	23	24
25	26	27	28	29	30 **Computer Security Day**	

from pg. 8

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

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

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

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

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

from pg. 9

data, files and Windows applications. We're working hard on completing our testing of the Windows 8 upgrade, and **will inform you via in-product notification when you can successfully upgrade to Windows 8**. In the meantime, you can check here http://kb.parallels.com/en/114973 for status updates.

Are you planning on performing a full install of any of the Windows 8 versions into a new virtual machine?

This should work just fine. KB114973 has the steps to smoothly and effectively add Windows 8 to your Mac. **Be sure that you are using the very latest build of Parallels Desktop 8 to create this new virtual machine**. To be sure you are on the latest build, go to the Parallels Desktop menu and click Check for Updates.

Happy

Birthday

HUGE!!