DWPC Technology Newsletter

Technology news from David W. Potts Consulting, LLC

david.w.potts@att.net www.oregoncomputer.com 503.659.5588

Volume 6 Number 2 March-April, 2017

Welcome to the thirtieth edition of the ***DWPC Technology Newsletter***. We hope you find this information helpful. If you no longer wish to receive this newsletter, please send us an email, indicating such. If you received this newsletter from a friend and wish to be added to the mailing list, please send an email to the address above and indicate your desire to receive the newsletter. Please feel free to share this newsletter with your friends.

Do you still have tech from Christmas in its box? Many people receive (or give themselves) a cool high-tech gadget for Christmas, but postpone using it, because they don't have time to deal with the learning curve. Technology is our forte. Please let us teach you to use your new equipment, so you don't need to spend the time (or experience the frustration), reading the manual.

Web browser-based malware scams: I have been recently receiving an increasing number of reports of malware scams hijacking Web browsers. These scams often cause persistent pop-ups, informing the user they have been infected with malware and need to call the provided telephone number to have the issue resolved. These Web pages often misrepresent themselves as being warnings from Microsoft or of the phone number being a Microsoft "partner". These scams can easily change the settings in your Web browser after simply visiting an infected Website. Often, resetting the settings of your Web browser(s) can correct the issues, although they can make it difficult to navigate to where you can change the settings or cause other issues. Practicing "safe computing", by only browsing the Web to mainstream Websites, not clicking on unfamiliar links (from Web pages, email, etc.), ensuring email attachments are legitimate (by calling the source of the message to ensure they sent the attachment to you) and reading pop-ups before accepting them, can help keep you safer. Truly, an ounce of prevention can be worth pounds of cure. If you have Malware on your computer, please let us help you clean your computer.

Careful where you click! There are lots of Internet entities that want to have you visit their Website so they can make money from you or your identity. Simply visiting a Website can cause things such as browser-based malware scams, ***or worse!*** Nefarious Internet entities use social networking techniques to entice people to visit their Website (***don't*** click on the link to find why "we will never see Sylvester Stallone, again"). Search providers are paid to "sell" keywords, which can guarantee their Website is returned, before the legitimate Website, when doing a search of the Web. How can you help protect yourself? Look at the URL (the Universal Resource Locator, or "Website name"), before clicking on it. If you question the validity of a link, most Web browsers will, by default, display the destination URL in the lower-left corner, when hovering over a link. If you were planning to update your animation player, but the URL points to http://www.malwareinfections.ru, you shouldn't be selecting that link. Update utilities from the utility manufacturer's Website. Another way to help protect your computer is to read the installation or Windows User Account Control dialogs or pop-ups, before simply selecting "yes". According to Microsoft, using the Windows User Account Control at its default level can help prevent the installation of malicious software on your computer by 30%. We have become complacent—tired of all these dialog boxes—but, in these days of identity theft and malware, we, the end users, must be the first line of defense to help ensure our safety. We must read these dialogs, and reply, properly, to help prevent malicious software from infiltrating our systems.

Protect yourself with "strong" passwords Unfortunately, we live in a time of identity theft and fraud. One of the easiest ways to help protect your identity is by using "strong" passwords. A "strong" password is one that is at least 8 characters in length, contains both upper- and lower-case characters and at least one number or special character. The longer and more complex the password, the better (but don't choose something TOO cumbersome). **Use a unique [strong] password for every financial institution** (bank, retirement account, brokerage account, etc.). Make sure to record your passwords and keep them in a safe and secure location (keeping a Post-it-Note with passwords, under your keyboard, is not safe). There are ways to use pneumonic references and two-step authentication to help secure your passwords. Please let us help you with your online security.

Ransomware Update I recently read an article, indicating about 40% of spam email sent in 2016 contained ransomware. Ransomware can encrypt files on your computer, making them unusable, without paying a "ransom" for a decryption key. Practice safe computing and don't click on links or open attachments in unsolicited, questionable or unexpected email (check with the sender, when receiving unexpected email, to ensure they really sent it). To recover from encrypting ransomware, a recent backup (containing the unencrypted files) is required to access your files again, without paying the ransom. Please let us help you create a backup strategy.

Microsoft Windows "license expired" SCAM I have recently had a number of clients inform me they had received telephone calls (I received an automated one, in February), informing them their Microsoft Windows license had expired and they needed to call back to have it reactivated—otherwise Windows services will be shut down, or other terrible things would happen. THIS IS A SCAM! Your Microsoft Windows license is perpetual. Currently-supported versions of Microsoft Windows *do* require activation, which may need to be performed, manually, but, after Microsoft Windows has been activated, it is a perpetual license. To verify your copy of Microsoft Windows is activated, open the Windows [File] Explorer, RIGHT-click on your computer ("Computer", "This PC", etc.) in the left sidebar, select "Properties" then, near the bottom of the Windows System Properties window, you should find a section labeled "Windows activation", which should indicate "Windows is activated".

Is it time to consider a 4K UHD TV or monitor? 4K, also known as ultra-high definition (UHD) television, is 4x the resolution of 1080p (or 1080i) "full HD" (twice the vertical and twice the horizontal resolution—3840 x 2160). These sets look almost like you are looking through a window . . . even up close! Until recently, the content has been lacking and there had not been a standard for 4K optical media (like Blu-Ray). There has been more content created for 4K and there are now 4K UHD Blu-Ray players. The 4K televisions and monitors have come down in price, significantly, and the UHD Blu-Ray players are now affordable. Although I don't suggest replacing your existing [working] HDTVs, if you are in the market for a new TV or monitor, it's time to consider 4K. If you are considering a curved TV or monitor, please check out my article, "What's this about curved TVs?" available from the following link: http://www.oregoncomputer.com/site/Technology_Newsletter_V4_%234.pdf.

Windows Vista sunsets, April 11, 2017! If you are still using a computer running Windows Vista, I strongly suggest replacing it, before April 11, 2017, when its support from Microsoft ends. We can help you!

Java and QuickTime security alerts! As Oracle's Java and Apple's QuickTime continue to be security risks, I am continuing to include warnings in my newsletters. You can view the alert from Homeland Security about QuickTime, here: https://www.us-cert.gov/ncas/alerts/TA16-105A. Oracle has published a Web page that details how to disable the Java program, at: http://www.java.com/en/download/help/disable_browser.xml. Either program can be uninstalled from the Programs and Features Control Panel. If you do need to run Java, ensure you are using the latest release and remove any old versions. If you have any questions about this or other security issues (or any other computer questions), please feel free to contact David W. Potts Consulting and we will be happy to help you.

How do I . . . Please submit questions to me via email to the email address at the top of page 1. Questions may be answered in future issues of this newsletter, or may be addressed individually. I often have clients who exclaim, after my correcting their issue, how they have been frustrated by working on an issue for weeks before calling me. Often the problem takes less than an hour to correct. Many mention how, next time, they will call me first to avoid the frustration! I have helped people do things from selecting and programming a high-tech remote control to setting up a company's network infrastructure.

David W. Potts Consulting will be happy to assist you with your hardware, software and network selection, purchase, integration, troubleshooting and training. We specialize in Microsoft Windows computers and networking and can also assist you with home theatre and other electronics and technology consulting.