



# DWPC Technology Newsletter

Technology news from David W. Potts Consulting, LLC

[david.w.potts@att.net](mailto:david.w.potts@att.net) [www.oregoncomputer.com](http://www.oregoncomputer.com) 503.659.5588

Volume 7 Number 4 July-August, 2018



**Welcome to the thirty-eighth 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.

**‘NET NEUTRALITY GONE??** The US Senate voted on May 16, 2018 to narrowly overturn the FCC ruling to restore ‘Net neutrality. The bill to overturn the FCC ruling now goes to the House of Representatives, for their vote, then on to the President. The President has already indicated he does not favor ‘Net neutrality, so the President’s likely veto would then need to be overturned, to restore ‘Net neutrality. I would like to say “good work” to everyone who petitioned their Senators to overturn the ruling that allows ISPs to throttle back speed to or block access to specific Web content, and remind you that the fight isn’t over, yet. Please petition your Senators and Representatives to restore ‘Net neutrality, by supporting the Congressional Review Act (CRA).

**“Brain Food” phishing attack!** A new phishing attack, dubbed “Brain Food” has been circulating around the Internet. The attack begins by a user opening an email message, and selecting links to Websites that supposedly offer pills to promote brain health or weight loss. When the user selects one of the links, they are directed to a bogus Website, where, if the user selects to purchase a product, allows their personal information to be collected which could then be used, maliciously. This new phishing attack differs from most phishing attacks, in that it uses “polymorphic code” to change, every time it is released, making it very difficult to detect and stop. “Phishing” uses techniques to coerce a user into providing their personal information for what appears to be a legitimate purpose (e.g. issues with your bank account, credit card, etc.), that is then used, maliciously. With the amount of attacks around, the end user must be the first line of defense with their cybersecurity. Do not open links or attachments in unsolicited email, allow an unsolicited party access to your computer and always ensure you are at a legitimate Website, before providing any personal information.

**CERT warns about malware using router vulnerabilities** The US Department of Homeland Security’s Computer Emergency Readiness Team (US-CERT) is warning that “foreign actors” have compromised hundreds of thousands of SOHO (small office/home office; including non-business home users’) routers with malware that can do things such as gathering information from your network and “exploiting LAN devices.” US-CERT suggests ensuring you have the latest version of firmware in your router(s) and that you restart your router(s) to “disrupt non-persistent portions of the malware.” They further suggest running full scans with antivirus and antimalware software. You can see the entire article, here: <https://www.us-cert.gov/ncas/alerts/TA18-145A>. If you would like assistance with your computer or network security, please let us help you.

**Are you *really* backing up your computer?** As I have discussed in earlier newsletters, all currently-supported versions of Microsoft Windows (Windows 7, Windows 8.1 and Windows 10) support methods of backing up your data. Windows 7 and Windows 10 both easily allow users to schedule backups, using multiple options . . . including a System Image, that should allow rebuilding a new hard disk drive to be bootable and look like the old hard disk drive . . . including Windows, programs, settings and personal data. Unfortunately, unless you occasionally check the backup status, there are multiple things that could cause Windows to stop its scheduled backups. Other backup utilities may also not alert you if they fail to complete, successfully. As such, it is important to occasionally open your backup program and ensure it is backing up your data as expected. Any data you would prefer to not lose should be saved in at least two locations. There are many backup options, and associated costs, depending on the level of protection you deem appropriate. Please let us help you with your backup strategy and solution.

## **You may still be able to upgrade your Windows 7 and Windows 8.1 to Windows 10, free!**

Although the “free upgrade” to Windows 10 expired in July of 2016, your computer may have “registered” for the free upgrade, even if you chose to not upgrade your computer to Windows 10 (yet). If your computer had registered for the free upgrade to Windows 10, you should be able to download the Windows 10 installation media creation tool and upgrade your computer to Microsoft Windows 10 . . . simply using the reservation that you had not yet used. Although Windows 10 has the same basic requirements as Windows 7 or Windows 8[.1], Windows computers generally last about 5-6 years, then, unless the computer was fairly high end, the user will greatly benefit from the newer technologies in a new machine. If you find your [Windows 7 or Windows 8.1] computer seems to keep up with all you do, you may want to consider trying the Windows 10 upgrade, as support for Windows 7 ends in January of 2020 (support for Windows 8.1 continues). Please keep in mind that some of the older hardware in earlier Windows 7 computers may not be supported in Windows 10. If you do plan to perform the Windows 10 upgrade, I strongly suggest that you perform a Windows Image Backup to a USB hard disk drive, so you should be able to revert back to the working Windows 7, if you experience issues with the Windows 10 upgrade. Please let us help you with your Windows 10 upgrade, or selecting and transitioning you to a new computer, before Windows 7 reaches its end-of-life.

**FTC Promoted Privacy Week, May 14-18, 2018.** Details, along with links to materials to help consumers protect their privacy can be found, here: <https://www.us-cert.gov/ncas/current-activity/2018/05/14/FTC-Promotes-Privacy-Awareness-Week>. In these days of identity theft, we must be aware of what we can do to help safeguard our identities, as each of us must be our first line of defense.

**What is the “Dark Web?”** The “Dark Web” is a “hidden” area of the Internet, used by criminals to trade or sell information, such as Social Security Numbers, or collaborate with other criminals on things such as malware. Security companies “find” some of these sites, and can search them for personal information, to help avoid ID theft.

**Scam and Fraud Resources** are available through the office of the Oregon Attorney General. As scammers are quickly creating elaborate ways to separate you from your money, I strongly suggest you use complex passwords, that you change often, and visit the Oregon Attorney General's Web site at [www.oregonconsumer.gov](http://www.oregonconsumer.gov), to keep abreast of newer scams and help learn ways to keep you and your family safer. You can also contact Ellen Klem of the Oregon Attorney General's office at [ellen.klem@state.or.us](mailto:ellen.klem@state.or.us) or 503.507.1061.

**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 the US Computer Emergency Readiness Team about QuickTime, at <https://www.us-cert.gov/ncas/alerts/TA16-105A>. Oracle has a Web page that details how to disable Java, at: [http://www.java.com/en/download/help/disable\\_browser.xml](http://www.java.com/en/download/help/disable_browser.xml). Either program can be uninstalled from the Windows 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.

The information contained in this newsletter is provided at no cost. David W. Potts Consulting, LLC provides no warranty, express or implied, for this information and the user assumes all liability for any issues arising out of the use of the information contained herein. The information contained herein is the intellectual property of David W. Potts Consulting, LLC. This information may be freely distributed, as long as it is distributed in its entirety and David W. Potts Consulting, LLC is acknowledged as the source of its content. Happy computing!