DWPC Technology Newsletter

Technology news from David W. Potts Consulting, LLC

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

Volume 7 Number 2 March-April, 2018

Welcome to the thirty-sixth 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.

Dealing with the new distracted driving laws Many states are enacting laws against "distracted driving"—essentially prohibiting use of electronic devices while driving. There have been studies that show behaviors such as texting or making phone calls can cause similar issues as driving while under the influence of intoxicants. Oregon now has some of the most restrictive laws against distracted driving. Three distracted driving strikes in 10 years can result in jail time and a criminal record! Many of us need to do business while driving, but certainly want to comply with the laws. One option to comply with the new law is to use a "hands-free device". Most cellular phones support BlueTooth for hands-free communication. The lower-end BlueTooth headsets support the rudimentary functions, such as playing audio, answering calls and redialing the last number, but do not support "voice commands." Most smartphones should support "voice commands", which, in conjunction with a BlueTooth device that also supports "voice commands", can allow you to use your BlueTooth headset to perform functions such as calling a specific number or contact, verbally. Always make sure you know [and follow] your local regulations regarding use of electronic devices while driving. You can find the details about distracted driving in Oregon from the Oregon DOT Website, at http://www.oregon.gov/odot/safety/pages/distracted.aspx.

Help keep your [grand]kids safe with GizmoGadget! Although we, as adults, have things to worry about while using our technology, such as identity theft, our children also have online threats, which can lead to things such as abuse and human trafficking. Young children can often be targeted, through electronic devices. Enter the LG GizmoGadget smart watch for children. The GizmoGadget, a cellular device (only available on the Verizon Wireless network) that provides restricted voice and messaging access and allows parents to monitor the location of their children [while wearing the watch]. The GizmoHub smartphone app allows parents to monitor the location of the watch, as well as setting boundaries, and, when the watch is taken outside the boundary, the parent will be alerted. The watch can be configured to allow the child to take or make calls or texts with up to 10 predefined contacts (blocking other calls and texting). The watch also includes fitness tracking and a task apps. The MSRP of the GizmoGadget is $149.99 but requires the cellular service from Verizon Wireless, the price varying, depending on options (requiring a 2 year contract; with a $175 early termination fee, and a $40 activation fee). Verizon also offers a "protection and support plan" for $10/month. The device is water resistant (but the buttons cannot be operated when the device is wet). Further details about the GizmoGadget smart watch can be found at: http://www.lg.com/us/cell-phones/lg-VC200-Red-gizmo-gadget and https://www.verizonwireless.com/connected-devices/lg-gizmogadget.

Keep yourself safe . . . really! Although I have written multiple times about not calling phone numbers from pop-ups or allowing unknown callers access to computers, I have many clients who still succumb to these scams. Unfortunately, these scammers are getting more and more polished with their techniques. I cannot express strongly enough that, once you allow someone remote access to your computer, they [likely] have the same permissions on your computer as you. Many of these scammers will, after convincing you that you must allow them to access your computer to avoid a calamity, can take steps to "lobotomize" your computer and try to hold your computer hostage. NEVER allow someone you do not trust to access your computer. In many cases, we can help clients whose computers have been compromised by malicious remote access to recover, but there are some times where the malicious entity can do dastardly things in the bowels of Windows, making it nearly impossible to correct, without backing up the data, reimaging the computer, then loading back on the programs and data (unless you have a viable backup . . . another good reason for backing up your computer!). This is truly a time when an ounce of prevention can be worth pounds of cure.

What the loss of "Net neutrality" regulations can mean to you! The Internet is an invaluable resource . . . both for businesses and individuals. Net neutrality means that a provider cannot choose to block content or to restrict your speed for specific content (without further charges). Of course, if you pay for a 10Mbps connection, you will not get the same speed as your neighbor who pays for a 200Mbps connection. Now the current administration has removed the Net neutrality rules, we could be subjected to things such as an ISP that also provides a television service choosing to restrict the speed from streaming services or an ISP with specific political views could choose to block content from Websites that have content that differs from the views of the ISP. I doubt we will see radical changes, soon, or all at once. I expect we will see small changes, over time, making it less obvious that our freedoms are being further eroded. I urge you to contact your congresspersons, to express your disapproval of this deregulation and voicing support for its reversal.

Block ads while surfing the Internet! We have all experienced the plethora of advertisements targeted at us from Websites we visit. Many entities work with advertising vendors to generate revenue by posting these ads on their Websites. There are ad blockers that can be integrated into your Web browsers that can limit the advertisements that are displayed on your computer (or portable device), when browsing the Internet. Popular examples of ad blockers for Windows computers are AdBlock (free at www.getadblock.com, although donations are requested; for Google Chrome, Microsoft Edge Opera and Apple Safari); AdBlock Pro (no affiliation with AdBlock—for Chrome, Firefox and Opera Web browsers; add the extension or add-on through your Web browser) and AdBlocker Ultimate (for Chrome, Firefox, Opera and Safari; add the extension or add-on through your Web browser), the latter can also block malware and adware. There are multiple options for Android and iOS, as well. There are also other ad blockers and privacy extensions that can help protect you and limit ads, while surfing the Internet. Always research any software before installing it onto your computer!

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, 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 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. Either program can be uninstalled from the Winodws 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.