DWPC Technology Newsletter

Technology news from David W. Potts Consulting

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

Volume 3 Number 4 July-August, 2014

Welcome to the fourteenth edition of the David W. Potts Consulting ***DWPC Technology Newsletter***. I hope you find this information helpful. If you no longer wish to receive this newsletter, please send me an email, indicating such. If you received this newsletter from a friend and wish to be added to the mailing list, please email me at the address above and indicate your desire to receive the newsletter.

What do you mean by "Safe Computing"? I often mention that you can keep your computer safer by practicing "Safe Computing". What do I mean by that? First, to keep your computer safe, it is necessary to keep your software updated (e.g. Microsoft Windows, Microsoft Office, Mozilla Firefox, Adobe Flash Player, Adobe Reader, Java, etc.). You must also keep your antivirus software current and update and run your antivirus and anti-malware software scans on a regular basis. When updating software, it is important to read the notices, as many updates (e.g. Java, Adobe, etc.) attempt to also install ancillary software that is not needed (and, likely, not desired). Generally, these update utilities automatically select to download and install these ancillary components, unless you select to not include them with your update. According to Microsoft, the "User Account Control" feature in Microsoft Windows Vista, Microsoft Windows 7 and Microsoft Windows 8[.1] allows these operating systems to be 30% less likely to be infected by viruses and malware than earlier versions of Microsoft Windows (including Microsoft Windows XP), **but only if you pay attention to messages displayed by User Account Control and don't simply allow processes to run**. It is important to read notices during installation to help ensure your safety. In addition to keeping your computer updated, you should not open attachments in unsolicited or unexpected email. You should also avoid visiting questionable Web sites. Before clicking on links, view their properties, to help ensure you aren't spoofed into visiting a malicious site (if you are being alerted a new version of Adobe Reader is available, ensure it is being downloaded from adobe.com, not some spoofing site, such as www.adware.com/adobereader. When searching for software, ensure you research the software and that you are downloading from a safe Web site, before downloading and installing software. For those who prefer not updating their computers themselves, David W. Potts Consulting offers remote and onsite preventative maintenance for computers running Microsoft Windows and can help you with installation decisions. Please contact us for details.

Phishing . . . not just for computers, anymore. Phishing is a method identity thieves use to obtain information that can be used for stealing identities. Phishing began with emails from thieves who impersonated financial institutions, trying to trick people into logging into their site, to provide them with the a user ID and password, to drain your account. Phishing has become even more elaborate. They can redirect you to Web sites that look nearly identical to those from your financial institution. Over the last 3 months, I have received two calls to my cell phone--"robocalls", indicating my Wells Fargo credit card had been placed on hold, and that I needed to speak with their representative to correct the issue. I don't have a Wells Fargo credit card! Your financial institution should never ask you for your personal information. If you ever question a call or email, contact your financial institution to ensure the inquiry is legitimate, and don't use links or contact information from the call or email.

"Microsoft Support" phone scam, revisited. Since originally warning of the telephone scams where, in my experience, an apparent Indian (not Native American) informs me that he is from "Microsoft Support" and, unless I let him connect to my computer to correct issues, my computer will have a catastrophic failure. Of course, this is a problem that he must fix, immediately. Since my first article about these scams, I have received at least two more of these phone calls. I have never heard of a legitimate Microsoft entity that contacts an individual to warn them about an infection. When I receive these calls, once the "technician" introduces himself as a Microsoft representative, before he states he has detected "problems with my computer", I break in and tell him that my computer has issues and he must immediately connect to fix them, to avoid serious problems. They tell me that I am correct! I then inform them I am an IT consultant and I know they are a scam . . . and they, immediately, hang up.

Revamped Preventative Maintenance Program! I have recently updated my preventative maintenance procedure to include some items to help clean up common issues I have recently seen that can adversely affect computers. As long as you practice "safe computing" (please see my "What do you mean by Safe Computing" article, above), all currently-support versions of Windows (Windows Vista and above) can generally benefit from preventative maintenance every 6 months. If you would like to have us provide you with preventative maintenance services, or have questions about it, please contact David W. Potts Consulting and we will be happy to help you!

Wireless Virus Created! A new virus, named Chameleon, has been created by researchers at the University of Liverpool. As routers do not have integrated antivirus software, conventional antivirus techniques will not detect this type of infection. This "proof-of-concept" virus will replace code in the infected wireless router, then will attempt to infect nearby wireless routers or access points. Viruses like Chameleon could be able to harvest data from the host network. This new virus does not need to have physical access to your wireless router. To help protect your wireless network, use "strong" passwords (upper and lower case characters, as well as at least one number or special character, at least 8 characters long, and do not use common words or patterns (e.g. Abc12345)) both for your router administration password and for your wireless key (password). Until Chameleon, wireless routers were generally safe with the default administration password. As such, unless I have had a reason to secure the router, I have generally left them with their default administration password. David W. Potts Consulting will be happy to help you [further] secure your wireless network.

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 visit their 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 Security Alert! As Oracle's Java continues to be a security risk, I am continuing to include warnings in my newsletters. Oracle has published a Web page that details how to disable the Java program. Please visit the page at: http://www.java.com/en/download/help/disable_browser.xml. 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 us and we will be happy to help you.

Windows XP End-of-Life IS PAST If you are still using a computer that is running Microsoft Windows XP, that computer IS NOW more vulnerable. **There are many who believe future updates to [supported versions of] Windows will be reverse engineered by malware authors, who may test Windows XP for the same vulnerabilities, allowing the malware authors to exploit vulnerabilities in Windows XP that will *never* be patched! This means that Windows XP is vulnerable to what IT calls "zero day exploits", forever forward!** If you are still a computer running Microsoft Windows XP and would like assistance migrating to Microsoft Windows 7 or Microsoft Windows 8, or a new computer, please allow David W. Potts Consulting to assist you.

How do I . . . Please submit questions to me via email to the 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.