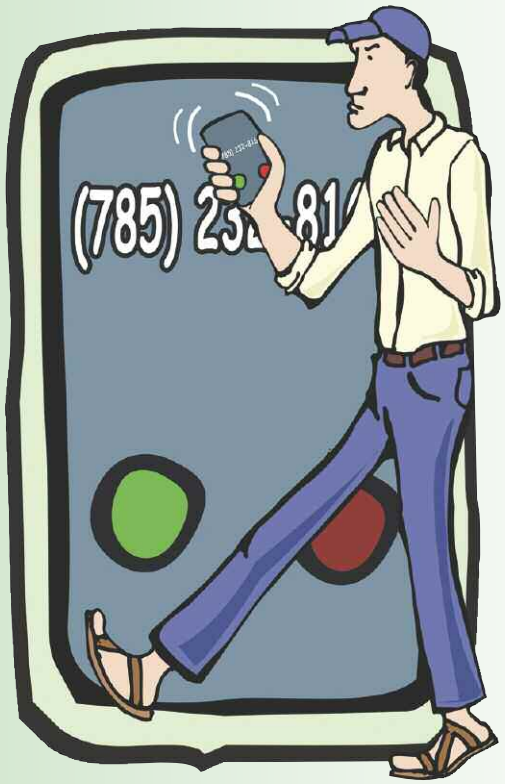
By Merle Windler, Thoroughbred Systems, Inc.

Computer Corner

Keeping Abreast of New Technologies

Phrases and Terms You Should Know About – and Why



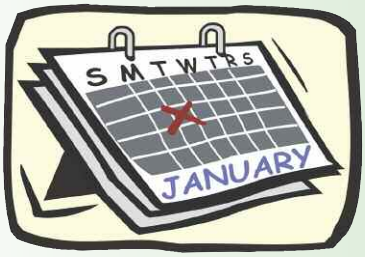
I want to take this opportunity in this issue to write about some phrases and terms and new technologies that would be good to be aware of. There are many.

"NEIGHBOR SPOOFING" – No, We Are Not Talking About A Bag Of Flaming Poo On The Doorstep!

Ever had somebody call you and ask who you are and why you called them today? You answer that "I didn't call anyone" and they, assuming you are a wiseguy and start chewing you out? Well, next time it happens suggest they Google "Neighbor Spoofing". Yes, yet another word to add to our techno-vocabulary. Telemarketers know that a person living in Kansas may well ignore a New Jersey call, so, now they use technology to lie to the Caller ID display on our phones. They pick another Kansas phone number at random (sometimes mine; I've had this happen twice in the last two days) and when the telemarketer calls some other unsuspecting victim, they cause the caller ID to display a "neighbor number", i.e., a Kansas number and, assuming that a call from someone else in Kansas is likely to be legitimate, the duped person answers the phone. Usually it's another one of those annoying robocalls. Cute, huh? If the misled person returns a missed call, they may find a confused person on the other end saying, "I didn't call you; I don't know what you're talking about." The problem is increasingly more common and the FCC is making efforts to control it. The good news is that the scammers usually only use the same "spoofed" number for a few hours or days, so at least it is not likely to be a constant and ongoing annoyance.

Microsoft will stop releasing updates and patches for the Windows 7 operating system when it reaches its End of Life phase on January 14, 2020.

"WINDOWS 7 END OF EXTENDED SUPPORT COUNTDOWN" – Abandonment Issues?



No, we're not talking about a spouse stepping out or a friend leaving one high and dry. This discussion is about the upcoming need to upgrade – specifically, upgrading to Windows 10. Anyone running Windows 7 should buy a new Windows 10 computer BEFORE January 14, 2020. Microsoft will stop releasing updates and patches for the Windows 7 operating system when it reaches its End of Life phase on January 14, 2020. By the time most people read this article, there will be less than 200 days remaining to get this accomplished. To go on using an operating system that has been abandoned by the almighty Microsoft will leave one's computer shaking in its boots and a sitting duck target for bad things to happen when out on the World-Wide-Web.

One may ask, "Can't I keep my old computer and just get a Windows 10 upgrade by then? Maybe, but that is probably not the most satisfactory idea as any Windows 7 computer would, by now be, as the saying goes, pretty long in the tooth. Putting off a complete upgrade may only leave other problems to be faced. This would also be a good time to review the upgrade status of other software. Intuit, for example, does NOT support any versions of QuickBooks more than three years old.

Intuit, for example, does NOT support any versions of QuickBooks more than three years old.

No, A "LOCKED DOWN" Computer Does Not Mean It Comes With A Padlock.

Thinking of buying a new laptop? There have been two primary computer platforms dominating the personal computer market for decades; they are Apple or Microsoft. Most people who have been using computers in the business world for a number of years have been primarily exposed to advancing versions of Microsoft Windows. They may have started on Windows XP, then moved to Windows 7 and now use Windows 10, or had experience with an even longer list of Windows operating system versions.

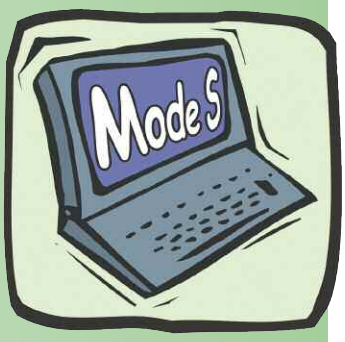
Now, to confuse the issue, a new generation of devices like laptops, notebooks, tablets, 2N1s, etc., have emerged that do not use an Apple Operating System (OS) or Windows, but, instead use a more limiting OS aimed primarily for use on the Internet. Often these devices are less expensive than their Microsoft Windows counterparts. That's good news, right? Well, it is only if the user's reason for purchasing the device is limited to certain Internet activities. This generation of little computers are "locked down" meaning that one cannot expect them to have the versatility of a Windows computer.

Google's Chrome Operating System (OS) is a simple, locked down, i.e., limited PC, optimized to function primarily as little more than a Chrome browser. In other words, one buys these devices primarily for "surfing the Net", sending emails, checking Facebook, etc. There are only VERY limited choices concerning software.

New Android-based tablets and laptops have appeared, as well. In both cases, they can cost hundreds of dollars less than a comparable Windows PC but they have a very limited pool of software to choose from compared to the Windows world. Most software programs do not have Chrome or Android versions.

Are You In The Mood For Mode – "MODE S", That Is?

Microsoft's entry to compete with these new 'Internet Browser' laptops and tablets is a new flavor of Windows 10 called "Mode S". Microsoft sales literature says Mode S will increase security and performance, as Windows 10 in S mode runs only the Microsoft Web Browser and security software and will only run software apps from the Microsoft Store (Internet/Virtual Store). Anyone wanting to install an app that isn't available in the Microsoft Store would need to permanently switch out of S mode. There's no charge to



switch out of S mode, but once it is done it cannot be turned back on. For anyone who has purchased one of these "Mode S" computers and now find themselves needing more, i.e., needing to return to regular Microsoft Windows 10, follow these instructions...

Open Settings > Update & Security > Activation. Find the Switch to Windows 10 Home or Switch to Windows 10 Pro section, then select the Go to the Store link.

The Term "CYBERSECURITY" – Becoming Less Of A Misnomer?

Whenever I hear someone touting something on the Internet as being "Completely Secure" I feel like I am back in the year 1912 listening to representatives of the White Star Lines explaining to the population how the ship the RMS Titanic is unsinkable! However, there is good news that will help those of us who wish to stay clear of icebergs hiding in the depths of the Internet. There is new technology that addresses Internet security exposure issues that have existed for decades. I refer to the latest improvements in WIFI devices. If you find yourself shopping for a new router anytime soon, don't be tricked by the unbelievable prices on the clearance shelf. That may be the management trying to unload yesterday's technology on an, as yet, uninformed public. Instead, be sure to look for the WIFI 6 compatible label on any WIFI devices before purchase.

In previous articles, we reviewed the upcoming newest, fastest version of WIFI. It is now readily available on the market. New routers and even mobile phones and other devices are now available with more hitting the market every day that support the new 802.11ax standard. Because it is the sixth generation of the wireless networking standard, you will see all these new devices supporting the new 802.11ax standard labeled as WIFI 6 compatible. The new generation of WIFI 6 devices, capable of a maximum speed of 9.6 Gbps, is expected to perform at speeds more than 30 to 250 percent faster than previous WIFI devices. Even with the faster individual device performance, WIFI 6 is more about improving the network performance when a bunch of devices are connected. A single WIFI 6 laptop connected to a WIFI 6 router may only be slightly faster than a single WIFI 5 laptop connected to a WIFI 5 router. However, as more devices are in use on the network, the performance of all the devices will be noticeably better with WIFI 6.

WIFI 6 will increase speeds, improve coverage area, expand the number of devices that can run simultaneously, boost video streaming capabilities, and provide better battery life. WIFI 6 is an upgrade for routers and WIFI devices; it is not an upgrade to your WIFI service. So, If you have a slow connection from your service provider, a WIFI 6 router won't fix that.

Asus, Broadcom, Dell, Hewlett Packard, Netgear, Qualcomm, Synology, TP-Link and many others now have new routers that support both the new WIFI 6 and WPA3 encryption standard we reviewed in the March 2019 KRWA magazine. A constant stream of new routers and devices of all types is becoming available that support the new WIFI 6 (802.11 ax) and WPA3 encryption standards. If you are looking for a new device for your city, water district or personally, make sure to look for devices that comply with the new WIFI 6 and WPA3 standards. (Don't purchase a new device using what is already considered the obsolete technology.) But, before investing in these new modern devices, make sure to check for any compatibility issues with local WIFI ISP providers or vendors of systems you need to interface with that may NOT YET be compatible with the new standards.

LG and Samsung are the first to bring to market mobile phones that are compliant with the new WIFI 6 and WPA3 security encryption standards. The Samsung Galaxy S10 became the world's first WIFI 6 smart phone several months ago.

Intel and several other companies now have new WIFI 6, WPA3 Wireless Adapters for Laptops, so we should start seeing the new model laptops come with this as a standard feature.

Before you buy, look for the WIFI certified logo on products and Search the WIFI Alliance website to look for approved, certified products that comply with the new

WIFI 6 and WPA3 standards: https://www.WIFI.org/product-finder

Note, some current devices and routers can support WPA3, but it's optional. For a WIFI 6 device to receive certification from the WIFI Alliance, WPA3 is required, so most new WIFI 6 devices are likely to include the stronger security.

The Most Important Security Term Of All – "CEREBRUM" – That's What Occupies The Space Between Your Ears!

In case you missed my session on Tech Security for Water Systems at the March 2019 KRWA Conference, one of the subjects covered was specifically aimed at utility operators and maintenance staff. The focus of the session was to acknowledge that while there is no such thing as complete security on the Internet, there are steps that can minimize risk.

There are many utilities implementing technologies like Industrial Control Systems (ICS) and Supervisory Control And Data Acquisition (SCADA) Systems remotely controllable over the Internet. The problem is that the bad guys out there on the Internet also use that technology.

Positive Technologies Company is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. In May 2018 they reported "America's Water and Power Plants are 'Shockingly' Vulnerable to Hacking Attacks". Their researchers were able to penetrate 73 percent of those entities tested.

The FBI confirmed the report's findings that foreign government-sponsored hackers were targeting Industrial Control Systems (ICS) and SCADA Systems. One of the primary factors allowing water systems to be compromised was entities failure to "keep up" with the latest updates and patches that included fixes to security weaknesses. Operators not wanting the "down time" required to install updates knowingly allowed their systems to be vulnerable, believing they were unlikely to be targeted.

Just before the March 2019 KRWA Conference, the well-respected CNet tech magazine had security experts attempt infiltration of their computer network. They were shocked at how easily experts tricked them into unknowingly allowing access and control of their network system by using info from staff members' own posts on social media, web sites and email.

How many readers (you) post photos and info on Facebook about your children, pets, your favorite car, etc., and then use a variation of the name as a password to your work computer system, ICS or SCADA?

The Internet is a big world with a lot of "bad players". It's up to YOU to act responsibly.

Merle Windler and his wife Linda are owners of Thoroughbred Systems, Topeka. The company specializes in software solutions for utilities and municipalities, computer networking and associated training. Contact: merlewindler@yahoo.com