By Merle Windler, Thoroughbred Systems, Inc.

Computer Corner

Guarding Against The Monsters of the Dark Web... and Other Cyber Dangers

In the March issue of *The Kansas Lifeline*, the article "What Monsters Are Lurking On the Dark Web?" reviewed some of the more notable incidents of data theft and hacker attacks during 2017. There were dramatic demonstrations of just how dangerous and vulnerable any and all data placed on the Internet has become.

This article presents some simple safety tips that can be employed by the average user to minimize risks in today's Cyber World.

1. Never open email with suspicious Subject lines or email attachments. And, never open an email without absolute certainty that it is from a verified address of a known and trusted sender. Request that email contacts always include a subject line that makes it clear the email is legitimate. Many people have been inconvenienced when they open an email from a trusted friend at a familiar address with the subject matter reading a friendly sounding "Hi!" only to find themselves victims of a phishing attack, malicious email that forwards to everyone on their contacts list and steals all contact information.

2. Don't use office computers to go places on the internet that are not work related. The boss is not likely to be pleased when an employee shopping for shoes or a jet ski turns into a major headache and large bill from a computer IT company!

3. Never download apps, updates, upgrades or software from pop-up advertisements or sites that pop up messages. There might be a message something like.... "The required update to Java (or whatever) is necessary to play the video attached to this article.... click here to install the update. DON'T DO IT... NEVER click on the Update option on such pop ups. Instead, go directly to the real website for the software in question. Java.com of the Oracle Corporation or Microsoft.com of Microsoft, for example, and load any updates direct from that verified source. These update needed ruses have tricked tens of thousands of people into installing malicious software on computers thinking they were installing legitimate updates or upgrades.

4. Don't be naively trusting and don't panic when an ominous recorded voice of doom suddenly announces out of nowhere that security has been breached or that

DON'T DO IT... NEVER click on the Update option on such pop ups.

private information has been compromised or that viruses have been detected. These scam artists are experts at creating panic and fear and suckering the unsuspecting user into clicking a button or calling some phone number that appears to offer redemption. These criminal enterprises are out to convince the user that they are legitimate technical support personnel from Microsoft or some other company that has miraculously detected this tragedy and are available to come to the rescue.

NEVER Accept. NEVER click OK. NEVER call the phone number displayed, etc... in fact don't choose ANYTHING offered on such a screen, not even what may appear as an Exit or Close Button as a way out. Instead... use the Windows Task Manager to Close the entire Browser (Internet Explorer, Chrome, Firefox, etc...) by pressing CTRL, SHFT, ESC all at once... or CTRL ALT DEL... and choose Task Manager. When Task Manager opens.... highlight the name of the Internet Browser program.... Chrome, Internet Explorer, etc... and Choose END TASK. If neither works, just turn off the power button or unplug the computer, but DO NOT click on any of the options the 'bad guys' are hoping will be picked allowing them to install their malicious software. When the computer comes back up, immediately RUN valid Internet safety cleanup tools. Here are three trusted cleanup tools:

Glary Utilities – A system optimizing tool

CCleaner – An anti-malware program protecting privacy and clearing away unwanted/malicious programs

Avast – An antivirus program (never have more than one antivirus program loaded onto a computer)

After running these, restart the computer.

There are other good choices including MalwareBytes, an anti-malware tool and AVG, another antivirus. Some tools are available at no charge depending on the application, while others come at a cost.

5. Never use Passwords of common things that could, with a little cunning and research, be guessed. NEVER use children or grandchildren's names, pet names, Social Security numbers, birthdates, street addresses, maiden names or other items that can be discovered with a bit of effort on Google or Facebook. Never use a Social Security Number or birthday as personal identification, unless absolutely necessary. And, avoid old fashioned crimes like burglary; don't post on Facebook how exciting the thought of next week's trip to Jamaica is!

And, avoid old fashioned crimes like burglary; don't post on Facebook how exciting the thought of next week's trip to Jamaica is!

6. As of July 2018, a Google Chrome warning may show up on any website not using Hyper Text Transport Protocol Secure (HTTPS) as part of the new PCI Data Security Standard (PCI DSS) for safeguarding payment data. Non-HTTPS websites may remain perfectly safe to use for looking up information, but Do NOT

A DSL/Cable Modem and Router are a gateway to the Internet. Network performance and Internet Safety start with them. Following are steps one can take to not only reduce risk but possibly improve performance:

1. Update router firmware.

Everyone should immediately check the website of their router's manufacturer or check with Internet hardware support to see if there are firmware updates that can be downloaded and installed to block the WPA2 encryption exploit 'KRACK '. Most newer model routers have an easy to use option to update them with software improvements and security fixes with downloaded firmware upgrades. Some may even have upgrades to the new WPA3 Encryption security system later this year. On our business router, installing the new security and software firmware update simply took opening an Internet browser, logging into the router, selecting the option to download available firmware updates and waiting several minutes while it installed the update and restarted itself.

In reference to recent hacking and malware attacks, "The FBI has several recommendations for any owner of a small office or home office router. The simplest thing to do is reboot the device, which will temporarily disrupt the malware if it is present. Users are also advised to upgrade the device's firmware and to select a new secure password. If any remote-management settings are in place, the FBI suggests disabling them. Here are suggestions:

a. Restart DSL/Cable modem, once a month or more often. This often solves many Internet connection and performance problems, such as; intermittent loss of signal, difficulties when connecting, slow connection, speed fluctuations, and browsing problems. Unplug the Modem for a minute. Don't just turn if off or reset it, unplug it from power. It may be necessary to wait a minute for the Internet Service Provider (ISP) equipment to autodetect that it's off and reset the connection. Many ISPs schedule regular reboot of modems during off-peak use times. If in doubt, do it yourself.
b. Unplug the Router as well. The router is basically a tiny computer dedicated to communications. Restarting it 'fresh' is not only a good idea for security, but a good practice for better performance. How often is a computer tech heard to say? "Have you tried turning it off and back on?" The reason one needs to wait a minute is to allow all the stored electricity to fully dissipate that is stored in electronic parts called capacitors.
c. Change the name of the WIFI Router network SSID (Service Set Identifier) to something that would not help anyone in recognizing who this is.
d. Change the default manufacturer router login and passwords and network administrator password and make sure to set a strong, unique password to secure the wireless network.
e. Turn off the wireless network when not at home or in the office to minimize the time available as a target for hackers and lower the risk of power surge damage during thunderstorms or electric power fluctuations.
f. Turn Off the Router Remote Access feature to prevent others from gaining access to the router's privacy settings from a device not connected to the wireless network.
g. Place the wireless router as close as possible to the middle of the office or home to provide the best signal to all the rooms. This will also reduce the distance the wireless signal range reaches beyond the building where it could be easily intercepted by malicious persons.

2. Tighten down security with the help of a technical advisor:

a. Change the default IP address on the wireless router to a less common one to make it more difficult for hackers.
b. Turn off Dynamic Host Configuration Protocol (DHCP) server so each device must be manually assigned a static IP address to connect to the network instead of automatically being assigned a connection.
c. Secure the Wi-fi network by setting up a hardware firewall. Many new routers have this feature built in. If a router doesn't have a built-in firewall, one can install a firewall device in addition to the router in order to protect the system from malicious hacking attempts against the network. These electronic firewall devices add one extra layer of security that should protect the network from most potential cyber attacks.

Enter Passwords, Credit Card numbers, Payment Information or personal information on any websites not displaying HTTPS. The key here is the S on the end, as it signifies that this is the secure version of the protocol which sends data between browsers and websites. HTTPS encrypts all the information that is sent and means that even if a hacker had access, the information would be illegible and unusable to them. This is the type of security that is used by most financial and ecommerce websites. Before sharing any sensitive information, check for the little lock icon on a browser screen and the HTTPS: on the URL line (usually found at the top left of the screen).

7. Use a VPN (virtual private network) to make even compromised intercepted data useless to any third party. A VPN is a heavily encrypted connection between the user and the VPN Service Server that can even make activities on a public WIFI network safe while we all wait for the release of the new WPA3 security encryption. Many of the AntiVirus companies, as well as others, offer VPN services for a small monthly or annual fee.

One of the really scary things discussed in the prior article was the WPA2 WIFI security weakness to a hacking attack called the Key Reinstallation Attack or KRACK. This allowed attackers to track traffic between devices and a router or access point. The KRACK attack exposed nearly 'All' WIFI devices and network data to possible interception. In just the last four months, a whole new generation of WIFI Routers have been announced and will 'hit the market' in the next few months that address the security problem by introducing the new improved WIFI Alliance approved WPA3 encryption system.

WPA3 has 192-bit security and new encryption features that will improve the privacy of users in open networks by creating individualized encrypted VPN data connections. For the first time ever, WPA3 will vastly reduce exposure risk when using open networks used in public places like hotels, restaurants, and airports with individual encrypted data on an open network. This is a HUGE improvement in Security.

8. Keep all routers, computers, mobile phones, tablets or other devices that connect to wifi updated. Make sure all WIFI devices have the latest updates that include a fix for the WPA2 WIFI 'Krack' exploit.

9. Increase WIFI security by activating the new Improved WPA3 (Wi-Fi Protected Access) network encryption as soon as it becomes available or purchase one of the soon to be available new Routers with WPA3.

10. Keep Microsoft Windows and AntiVirus programs up-to-date. Make sure to allow updates. In Windows, click the search bar on the bottom left > type "Update" > click "Check for Updates > click "Check for updates" again in the Windows Update menu. Also, Keep anti-virus programs, Anti Malware tools and other protection software up-to-date.

11. If using any of the new Voice Activated Assistant devices like Alexa, Echo, or Google Home, turn them off when not is use or away. Security experts at Symantec advise voice command users against control of security functions like door locks or security systems. Turn Off permissions to make Voice Activated purchases and the DropIn feature that allows like devices to auto connect to the virtual assistant when within signal range. If these voice activated devices are used carelessly, the user might find themselves victimized by an associate or a stranger that manages to get some voice samples recorded in a public place or over the phone that could later be employed to provide Alexa or similar assistants with instructions to benefit the thief.

Of course, one could also follow the Internet Security Safety rules of the Wolf Creek Nuclear Power facility by not allowing access to the Internet of critical office computer systems and devices. It's not a very acceptable solution in today's hyper-connected world for most of us, but, nonetheless, that's a security solution that works.

Of course, one could also follow the Internet Security Safety rules of the Wolf Creek Nuclear Power facility by not allowing access to the Internet of critical office computer systems and devices. It's not a very acceptable solution in today's hyper-connected world for most of us, but, nonetheless, that's a security solution that works.

Merle Windler and his wife Linda are owners of Thoroughbred Systems, Inc., Topeka. The company specializes in utility billing for cities and rural districts, computer networking and associated training.
Contact: merlewindler@yahoo.com