Fox Bytes

Newsletter of the Foxwood Springs Computer Club

February 3, 2018 Foxwood Springs Raymore, MO 64083

Visit www.foxwoodsprings.org for more information about our excellent retirement center.

COMPUTER CHAT

Holiday activities and the weather have reduced our Computer Chat participation, but we have had both old problems and new programs to discuss. Roger Hunt visited us last Monday, and it is always beneficial for our participants to have a qualified technician to answer some of our questions. Roger helped us demonstrate some answers to questions using our computer and large screen. We really appreciate being able to illustrate on the large monitor the topics we discuss and possible solutions.

Byron Gilbreath asked about finding files. He said he sometimes saves files in a folder and has difficulty finding them when he wants to edit them later. Roger showed him how he can find the search blank, write in Name: and either the title or some words that would be in the file. He can search in Documents for his files or search for pictures or videos from those folders. One can bring up File Explorer or This Computer to find the Documents, Pictures, or Videos folders in which the search is made.

Marjorie Slavens said she searches in either Windows 7 or Windows 10 by pressing the Windows key to bring up a blank to use for a search. In Windows 7, documents are searched. In windows 10, however, Internet searches, which she probably does not want, as well as document searches are included in the results of the search. One needs to select the search categories on the computer to limit the scope of the search.

Roger also helped us look at the Seeing A I program that Microsoft has developed to provide assistance for people who have visual limitations. We watched the instructional video on Youtube. The various parts of this program are called "Channels". We watched the channel for short text, such as reading an envelope, a restaurant bill, etc. The program reads the text aloud. There is also a "Documents" channel for reading longer text. This program also has a beta version that proposes to read handwriting, a real challenge. Seeing A I is a free download on the iPhone.

Roger has left some of his brochures on the bulletin board in the Computer Lab. Several of our participants thought they might be able to use some additional professional help.

Art Tees was not able to write his usual "The 10 Spot" article this month because, in spite of having had the flu shot, he now has the flu. He and Lee Hankins have worked very hard to get our FSTV back on the air, and both of them have been flu victims recently. Lee is some better now, and we all hope Art will soon conquer this challenge as he has so many others in the past. We also hope Comcast will work out their problems and get FSTV back on the air.

COMPUTER CHALLENGES

Recently, our Webmaster, Del Sherwood, told us that our website, www.foxwoodsprings.org, needed to be upgraded to protect its security. Fortunately, Go Daddy, our web host, had a program at a very reasonable price to provide some additional protection for our viewers. Our Address is https://www.foxwoodsprings.org. Our protection plan will cover the next three years, and we and Brookdale believe this protection is extremely important. Financial institutions use this type of security for their sites. It would seem that all of us need to increase our awareness of the possible challenges and available protection online.

In their January newsletter, Malwarebytes describes some of the threats and actions they are taking to protect their viewers.

"Ransomware grabbed headlines in 2017, with massive outbreaks affecting people and businesses worldwide. Led by WannaCry, NotPetya, and BadRabbit (names from a failed James Bond script?), ransomware resulted in millions of dollars paid in ransom, locked files, and late nights for anyone concerned about cybersecurity. And that, my friend, may have been you. So we're here to help. We gathered everything you need to know about ransomware in one reference page. Its history, how to protect against it, what to do if you're infected-it's all there. We'll keep the page updated with the latest on major ransomware outbreaks (so you might want to bookmark it or add it to your RSS feed)".
(www.malwarebytes.com)

These are some of the categories now listed on their page that will be updated regularly.
a. Latest ransomware attacks.
b. What is ransomware?
c. How do you get ransomware?
d. Types of ransomware.
e. History of ransomware
f. Mac ransomware
g. Mobile ransomware
h. Who do ransomware authors target?
i. What to do if you're infected.

These are links on the Ransomware page, and we can check that page for new developments in the struggle to eliminate ransomware. Generally, this affects business more than private users, but some of our residents have had such contacts, and we all want to be protected.

HISTORY OF RANSOMWARE

(This is an example of the material about Ransomware on the Malwarebytes site.)

The first ransomware, known as PC Cyborg or AIDS, was created in the late 1980s. PC Cyborg would encrypt all files in the C: directory after 90 reboots, and then demand the user renew their license by sending $189 by mail to PC Cyborg Corp. The encryption used was simple enough to reverse, so it posed little threat to those who were computer savvy.

With few variants popping up over the next 10 years, a true ransomware threat would not arrive on the scene until 2004, when GpCode used weak RSA encryption to hold personal files for ransom.

In 2007, WinLock heralded the rise of a new type of ransomware that, instead of encrypting files, locked people out of their desktops. WinLock took over the victim screen and displayed pornographic images. Then, it demanded payment via a paid SMS to remove them.

With the development of the ransom family Reveton in 2012 came a new form of ransomware: law enforcement ransomware. Victims would be locked out of their desktop and shown an official-looking page that included credentials for law enforcement agencies such as the FBI and Interpol. The ransomware would claim that the user had committed a crime, such as computer hacking, downloading illegal files, or even being

involved with child pornography. Most of the law enforcement ransomware families required a fine be paid ranging from $100 to $3,000 with a pre-paid card such as UKash or PaySafeCard.

Average users did not know what to make of this and believed they were truly under investigation from law enforcement. This social engineering tactic, now referred to as implied guilt, makes the user question their own innocence and, rather than being called out on an activity they aren't proud of, pay the ransom to make it all go away.

Finally, in 2013, CryptoLocker re-introduced the world to encrypting ransomware—only this time, it was far more dangerous. CryptoLocker used military grade encryption and stored the key required to unlock files on a remote server. This meant that it was virtually impossible for users to get their data back without paying the ransom. This type of encrypting ransomware is still in use today, as it's proven to be an incredibly effective tool for cybercriminals to make money. Large scale outbreaks of ransomware, such as WannaCry in May 2017 and Petya in June 2017, used encrypting ransomware to ensnare users and businesses across the globe.

Mac ransomware

Not ones to be left out of the ransomware game, Mac malware authors dropped the first ransomware for Mac OSes in 2016. Called KeRanger, the ransomware infected an app called Transmission that, when launched, copied malicious files that remained running quietly in the background for three days until they detonated and encrypted files. Thankfully, Apple's built-in anti-malware program XProtect released an update soon after the ransomware was discovered that would block it from infecting user systems. Nevertheless, Mac ransomware is no longer theoretical.

Mobile ransomware

It wasn't until the height of the infamous CryptoLocker and other similar families in 2014 that ransomware was seen on a large scale on mobile devices. Mobile ransomware typically displays a message that the device has been locked due to some type of illegal activity. The message states that the phone will be unlocked after a fee is paid. Mobile ransomware is often delivered via malicious apps, and requires that you boot the phone up in safe mode and delete the infected app in order to retrieve access to your mobile device.

Who do ransomware authors target?

When ransomware was introduced (and then re-introduced), its initial victims were individual systems (aka regular people). However, cybercriminals began to realize its full potential when they rolled out ransomware to businesses. Ransomware was so successful against businesses, halting productivity and resulting in lost data and revenue, that its authors turned most of their attacks toward them. By the end of 2016, 12.3 percent of global enterprise detections were ransomware, while only 1.8 percent of consumer detections were ransomware worldwide. And by 2017, 35 percent of small and medium-sized businesses had experienced a ransomware attack.

Ransomware report on small- and medium-sized businesses.

Geographically, ransomware attacks are still focused on western markets, with the UK, US, and Canada ranking as the top three countries targeted, respectively. As with other threat actors, ransomware authors will follow the money, so they look for areas that have both wide PC adoption and relative wealth. As emerging markets in Asia and South America ramp up on economic growth, expect to see an increase in ransomware (and other forms of malware) there as well.

What to do if you're infected

The number one rule if you find yourself infected with ransomware is to never pay the ransom. (This is now advice endorsed by the FBI.) All that does is encourage cybercriminals to launch additional attacks against either you or someone else.

However, you may be able to retrieve some encrypted files by using free decryptors.

To be clear: Not all ransomware families have had decryptors created for them, in many cases because the ransomware is utilizing advanced and sophisticated encryption algorithms. And even if there is a decryptor, it's not always clear if it's for the right version of the malware. You don't want to further encrypt your files by using the wrong decryption script. Therefore, you'll need to pay close attention to the ransom message itself, or perhaps ask the advice of a security/IT specialist before trying anything.

Other ways to deal with a ransomware infection include downloading a security product known for remediation and running a scan to remove the threat. You may not get your files back, but you can rest assured the infection will be cleaned up. For screenlocking ransomware, a full system restore might be in order. If that doesn't work, you can try running a scan from a bootable CD or USB drive.

If you want to try and thwart an encrypting ransomware infection in action, you'll need to stay particularly vigilant. If you notice your system slowing down for seemingly no reason, shut it down and disconnect it from the Internet. If, once you boot up again the malware is still active, it will not be able to send or receive instructions from the command and control server. That means without a key or way to extract payment, the malware may stay idle. At that point, download and install a security product and run a full scan.

How to protect yourself from ransomware
Security experts agree that the best way to protect from ransomware is to prevent it from happening in the first place.

Read about the best ways to prevent a ransomware infection.
While there are methods to deal with a ransomware infection, they are imperfect solutions at best, and often require much more technical skill than the average computer user. So here's what we recommend people do in order to avoid fallout from ransomware attacks.
The first step in ransomware prevention is to invest in awesome cybersecurity—a program with real-time protection that's designed to thwart advanced malware attacks such as ransomware. You should also look out for features that will both shield vulnerable programs from threats (an anti-exploit technology) as well as block ransomware from holding files hostage (an anti-ransomware component). Customers who were using the premium version of Malwarebytes for Windows, for example, were protected from all of the major ransomware attacks of 2017.

Next, as much as it may pain you, you need to create secure backups of your data on a regular basis. Our recommendation is to use cloud storage that includes high-level encryption and multiple-factor authentication. However, you can purchase USBs or an external hard drive where you can save new or updated files—just be sure to physically disconnect the devices from your computer after backing up, otherwise they can become infected with ransomware, too.

Then, be sure your systems and software are updated. The WannaCry ransomware outbreak took advantage of a vulnerability in Microsoft software. While the company had released a patch for the security loophole back in March 2017, many folks didn't install the update—which left them open to attack. We get that it's hard to stay on top of an ever-growing list of updates from an ever-growing list of software and applications used in your daily life. That's why we recommend changing your settings to enable automatic updating.

Finally, stay informed. One of the most common ways that computers are infected with ransomware is through social engineering. Educate yourself (and your employees if you're a business owner) on how to detect malspam, suspicious websites,

and other scams. And above all else, exercise common sense. If it seems suspect, it probably is. (Malwarebytes Labs, www.malwarebytes.org)

GENEALOGY NEWS

Marjorie Slavens

Midwest Computer Genealogists is a regional genealogical organization which has been meeting at Foxwood Springs for about 15 years. We previously met at Bannister Mall until shortly before it closed. Although our participation is not as large as when we met at Bannister with about 100 members, we have had excellent speakers here and some good volunteers who have worked to continue this organization. Since we have met at Foxwood, Jim Stout and Don Bjuland of Independence have served as President. Rowena Schaffer and Roger Rhoades of Johnson County have served as Program Chairs.

Al Morse, who came with his wife, Dorothy, to Foxwood Springs in 2008, has been MCG President since 2011. He is Furniture Garages Manager for the Fellowship of John fund-raising program. He writes a column, "The President's Corner", each month and has provided many stories about their family history, which he has compiled and given to his brother and their two sons, preserving the family research for future generations. His cousin, Laura Frances (Seals) Scott, was the family historian for the family lines of their mothers, Amy (Janssens) Seals and Mildred (Janssens) Morse. Al has continued this research but has added his father's family and the family lines of both of Dorothy's parents to his research.

Ivan Waite was our Secretary for many years. He also wrote several articles for our newsletter and made several presentations about his family lines. He has been an MCG member for more years than the rest of us.

Byron Gilbreath has succeeded Ivan as our Treasurer. He is currently serving as Parish Council Chair and as Treasurer of the Foxwood Springs Residents' Council, which administers our Fellowship of John program. He previously served on the MCG Programs Committee and was also responsible for our publicity. He moved to Foxwood Springs in 2003 with his wife, Joyce. Joyce was their family historian for many years. Byron has researched his Gilbreath line, and they have also made many research trips in the past. His most recent trip was to Scotland with his daughter, Carol.

I moved to Foxwood Springs with my mother, Mildred Welty Slavens, our family historian, in 1998. I have been Newsletter Editor since 2006, Program Chair for the past few years, and assumed the role of Secretary last year.

This year, we will have an excellent series of programs. At our January meeting, we shared our family research and met some new members. One of our new members, Donald Knight, will be our speaker on February 17. He has researched his line and has previously done a newsletter for his family.

On March 17, Jim Beckner will speak on "Whistler's Mother and the American Civil War". Our April program has not yet been finalized, but we will soon have that program scheduled.

Peggy Buhr, Director of the Bates County Museum in Butler, will return in May. She has not yet finalized her program but has several topics in mind. Julia Morse from Manhatten, Kansas, Al's cousin, will be our speaker in June. She previously gave a presentation about the Morse family. In June, she will discuss genealogical research through newspapers.

In July, Chelsea Clarke, Manager of the Genealogical Branch of the Cass County Library in Harrisonville, will be our speaker. She has previously made presentations on Native Americans and Irish family research. She has

suggested three very good topics, and we will need to choose one. Debora Downard from Belton will be our speaker in August. She has done research for her own family and also works with the research for other families . Her topic will be "Jacob's Diary".

Tom Rafiner will be here in October, and we are all looking forward to his excellent presentation. He is the author of *Caught Between 3 Fires* and *Cinders and Silence,* both of which present the history of this area before, during, and following the Civil War. In November, Beth Foulk will return Her topic will be "In Search of My Brother's Mother...a personal adoption story".

We invite new residents who are interested in genealogy to join us at our meetings. Everyone is welcome to attend.

COMPUTER DEFINITIONS AND TIPS

Clipboard (Updated: 10/04/2017 by Computer Hope)
The clipboard is a special location in your computer's memory that temporarily stores data that has been cut or copied from a document. This data can then be pasted to a new location. The clipboard will typically hold its information until you cut or copy something else, or log out of the computer. For example, a user may copy information from a word processor and paste that information into an e-mail message.

Cut–-Ctrl/X: Move from one place to another using the Clipboard
Copy–-Ctrl/C: Copy text from one place to another using the Clipboard, leaving the original in place.
Paste–-Ctrl/V: Place the text from the clipboard to its new location

Disk Cleanup
Use Disk Cleanup to remove unnecessary files from the computer, providing more space. Go to Disk Cleanup under Accessories or go to Computer, highlight the C Drive, right click and select Properties and Disk Cleanup. You may search in Windows 10 for "Disk Cleanup". . Run Disk Cleanup. You can decide which of the options you want to eliminate by checking the appropriate box. (I remove all options in the list provided except for the Recycle Bin, where I would prefer to look at each file to see if it really should be deleted. M. S.) Some of the options to delete include Temporary Files, some files not needed after a Windows update. It is recommended that you not compress your drive, but Disk Cleanup will provide more space when you complete the process.

Word Processor
Features of a word processor
Microsoft Word
Overview of Word
In a word processor, you are presented with a blank white sheet. The text is added to the document area and after it has been inserted, formatted or adjusted to your preference.

Features of a word processor
Unlike a basic plaintext editor a word processor offers dozens of additional features that can give your document or other text a more professional appearance. Some of the most popular features of a word processor are: Changing the font, font size, font color, bold, italicizing, etc; insert clip art, charts, images, pictures, and video into a document; check spelling and grammar; modifying the margins and layout of a document; set and format tabs, bullet lists, and number lists. You can add tables to a document. You can automatically correct common errors.

Other Word processors
Abiword
Apple--Pages
Corel--WordPerfect
Google Docs--(Online and Free)
LibreOffice Writer--Free
Microsoft Office–Microsoft Word
OpenOffice Writer--Free