



# Fox Bytes

Newsletter of the Foxwood Springs Computer Club

January 3, 2019

Foxwood Springs

Raymore, MO 64083

Visit [www.foxwoodsprings.org](http://www.foxwoodsprings.org) for more information about our excellent retirement center.

## HAPPY NEW YEAR!

In recent years, the first article in this newsletter has been "Computer Chat". However, this month is a little different. Because Christmas Eve and New Year's Eve were on Monday, and Chat meets at 1:00 on Monday afternoons, we cancelled this activity so our participants could celebrate the season with their families and friends. We will be back in the Computer Lab for Chat next Monday, January 7, 2019, and we look forward to seeing our old friends and to welcoming new friends who want to share their computer questions and successes with us. If you received a new computer, cell phone, or other similar electronic device, come and share your new acquisitions or new programs and computer experiences with us.

"Fox Bytes" is beginning its 20<sup>th</sup> year this month, although it has not always had this name. Former resident Rita Kirby created our monthly newsletter, and it did not have a special name,; it was "Computer Club Newsletter". That publication was about twice the size of the present publication. Rita had a larger staff of contributors; now, there are only two of us. Some of us interviewed other residents about their lives before they came to Foxwood and also about their computer use. The newsletter was printed, assembled by volunteers on Thursdays, and distributed in the Friday mail, not by E-mail. The publication became "Fox Bytes" when Cloyce and Orinne Wiley moved here around 2004 and became its publishers.

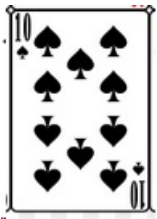
We had many more regular activities in 1999, including weekly Imaging, Windows, and Genealogy SIGS (Special Interest Groups).. Yes, Computer Chat was at 1:00 on Mondays then. Doris Kohl was President of the Computer Club and was the Chat Leader. Our lab was where the Foxwood Room is now, but it was smaller than that room is currently. We had old computers that were donated by residents or friends. We did not have a large TV or a projector then; any demonstrations were done on a single computer, and people had to look at a very small monitor operated by the presenter. George Wiszneuckas and Lee Keith repaired our computers, and they required a lot of repair. They were not networked and the computers were not all connected to a printer.

We had several different activities then in addition to Chat. There was a monthly evening program with speakers who came from outside the community, including from the city of Raymore, the schools, the "Kansas City Star", the FBI, etc. Times have really changed!



Church Camp Hymn Parody:

*The organ peeled potatoes;  
Lard was rendered by the choir.  
And while the Sexton rang the dishrag,  
Someone set the church on fire.  
"Holy Smoke!" the parson shouted  
As in the blaze he lost his hair.  
Now his head resembles heaven  
For there is no parting there!*



## The Windows 10 Spot

Arthur Tees

### New Year's Resolutions

January takes its name from the Roman god Janus, who supposedly had two faces—one looked back at the year past, and one stared forward at the year ahead. So might we look back at 2018 and see what we should do differently in 2019—a resolution for computer users.



Janus

Did we forget to back up regularly? A monthly backup is a small chore, but it will save grief in the new year should something happen to your machine. It makes an excellent New Year's Resolution.

If you didn't start that OneNote Notebook section listing what your next of kin should know about your home or apartment that is not in your will, that is another good New Year's Resolution to start. For more information on this, see last month's 10 Spot column.

### Home Inventory

One January chore for many merchants is taking inventory of the merchandise on hand after the busy Christmas season. This is a good time for homeowners and apartment dwellers to do the same, especially if Santa has been good to you. Did you get a new computer for Christmas, a new TV perhaps, or other smaller but valuable present? While theft is not a problem at Foxwood and fires are extremely rare, homeowners are expected to carry insurance against just such an eventuality. But if a loss should occur, how would you be able to file a claim if you did not have some way of showing what was lost?



One easy home inventory solution is to grab your digital camera and

photograph your possessions. Store the resulting files off site, either in you safety deposit box or in the cloud.

Photos are nice, but a welcome addition would be a list, literally a table with columns for Description, Purchase Date, Cost, and, when appropriate, Serial #.

| Description | Purchased | Cost | Serial # |
|-------------|-----------|------|----------|
|-------------|-----------|------|----------|

### Not A Perfect 10

Microsoft believes it has finally solved all the problems associated with its planned October Windows 10 semi-annual update. The update had been delayed for two months by a series of problems, including most recently one that would freeze its new expensive Surface tablet. Known as Windows 10 KB4023057, the update has probably already been installed on reader's machines. Microsoft promises to do better and indeed is faced with a herculean task of providing error-free code across thousands of different configurations of personal computers.



### Sharpening the Edge



Microsoft's Edge browser trails most other Internet browsers in use. Its August 2018 share was about 4%, well below venerable Internet Explorer's 7%.. Google's Chrome, which has 67%, is the most popular browser, with Firefox second at 11%. Apple's Safari has a 5% share.

It's not surprising, then, that Microsoft will, in the next year, revamp Edge by incorporating large amounts of Google's open source Chrome in its rendering engine—the part of the browser that displays the search results. The replacement of its own Edge HTML with Chrome will make it easier for developers to write extensions that will work across both Chrome and Edge. The result will hopefully increase the market share claimed by the Microsoft product.

Bill Gates, Microsoft's founder, dismissed the need for a browser when the Internet was in its infancy, ceding that market to the upstart Netscape Navigator. Google joined the fray later and soon dominated market. Microsoft has been playing catch up ever since; the new approach is not likely to make Edge a winner.

### “Reach Out and Touch Someone”



That old long-distance phone advertising line got a new twist this holiday season. With low calling rates, scammers are hard at work bringing calls from supposed relatives.

Three grandsons have each called one resident recently, overlooking the fact that he had no children. It’s a modern miracle!

Another call announced a \$299 payment was due for computer protection; the phone was put back on the hook before the details of the offer could be described. A third caller with a sub-continent Indian accent did not get a chance to explain his pitch. No-call lists, both state and federal, are no protection now, but the scammers do provide a diversion. Always remember, however, that Microsoft *never* calls you to help with a computer problem.

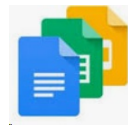
### Choosing an Office Suite

Most of us have grown accustomed to whatever software we use to create documents, spreadsheets, and slide presentations, but it behooves us periodically to review the ever-changing offerings of the office application market. If Santa brought us a new computer this season but neglected to include software, and we have lost the installation CDs for our old familiar apps, this is time to look over the field. We can also keep in mind that with today’s 1 to 2 TB hard drives found on many a desktop unit, we have ample room for more than one weapon in our software arsenal. Each of these offer specific advantages, depending on our needs, and each has the basic three apps—word processing, spreadsheet, and presentation (PowerPoint-like) with others as noted.

**Free**—Libre Office, Google Docs, and Office on-line. Most people would find that either of these first two would meet their basic needs in all three applications. Libre Office should be on our hard drives because of its ability to open



almost any word processing file format since WordStar. An installed program, it can be used offline, as can Google Docs with a supplemental free app installation. If cooperation with other workers or the ability to move from a desktop to a laptop and work on the same file is important, Google and, to some extent, the on-line Office apps are superior, running in a browser and accessing cloud-based data files. Libre Office can be so used if the data is stored in Google Drive or One Drive locations.



Google Docs

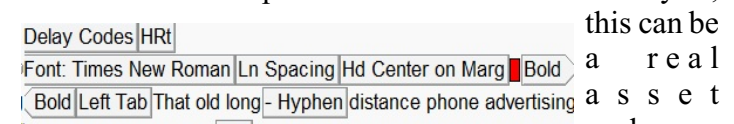
**Rented**—We don’t think of renting software, but Microsoft’s Office 365 has changed that. As its name implies, the user pays an annual fee in return for always having the latest update. At \$69.95 for one installation or \$99.95 for up to six friends/relatives on a single license (each of whom can install it on 5 devices and each having 5 GB of One-Drive storage), the cost is not excessive. For those not desiring to rent, the 2016 purchased version is advertised on the web for \$59.95, the 2019 Pro Plus version at \$89.95. Note that additional apps such as Publisher, Access, and OneNote may be included in these offerings.



**Purchased**—WordPerfect Office requires a purchase and does not run in a browser. The current version costs from \$135-\$200, the latter price including the database program, Paradox and its ObjectPal programming language. Most potential users will opt for the lower-priced version, though it should be noted that programs written in ObjectPal and accessing Paradox can be distributed in a run-time version free of charge.



WordPerfect has features not found in other word processors. Among these is the Reveal Codes command. This opens a small window just below the main one, showing the various formatting codes in their place in the text. For more complex documents such as Fox Bytes,



formatting problems occur. Additionally, few other word processors allow vertical line spacing increments of .01".



*Pity the indifferent owl:  
He didn't give a hoot!*

## **FSTV is Back—And We're Glad!**

Foxwood's closed-circuit TV station, FSTV, is once again broadcasting after a technical problem kept it dark for some time. It appears that a vital group of settings



### **Radiant Encoder**

in the encoder, the device that translates computer-based sound and pictures into TV language, were changed to the point that our programming signal was interfering with other channels, even outside of Foxwood. How those changes came to be made is a mystery, but the result was that Comcast simply cut the cable that runs outside the studio to the rest of the world.

The question is, who changed the encoder settings? The control room is locked except when FSTV staff are in there, and they would hardly adjust the encoder. Changing the settings is not a simple task, best accomplished by someone acquainted with the unit and with a laptop computer.

The unit has been restored to its original settings and a passcode installed to prevent future tampering. A technician from AVI in North Kansas City has verified the installation's settings, increased the signal's power, and persuaded Comcast to restore the connection.

Our CEO, Brian Petersen, has been most helpful in supporting financially Lee Hankin's efforts to get FSTV back. AVI's technicians don't make free house calls.

## **PROTECTING OURSELVES**

Marjorie Slavens

Our phones and computers are still vulnerable, and we need to be on guard constantly to avoid responding to inappropriate, or, perhaps illegal, contacts.

Our cell phones used to offer some protection that land lines did not, but that

protection seems to be gone too. Apparently, the communications companies are all selling our cell phone numbers as well as the others.

In the past few weeks, my inappropriate phone calls have increased. I deleted a long list of calls from my answering machine and saw some numbers that are frequently repeated. One was a 660 area code that kept calling me every day. A couple of others have the same first three numbers like those on my iPhone. I have heard from other people that they are experiencing the same thing. Sometimes I get three or four phone calls from numbers with different area codes that are repeated day after day.

I do not answer any phone call if I do not recognize the number. I may be missing some calls from people whom I know but do not recognize their phone numbers. Because this is such a frequent occurrence, I do not answer. If the callers are people I should know, they can leave a message on my answering machine, and I will return the calls. My phone rings 6 times before the answering machine offers to take a message.

At the last Parish Council meeting, Dorothy Eubank said she had contacted the Attorney General's Office to report such calls. They told her she should never respond in any way, including when they say you will be taken off their list if you press 9. This simply confirms that you exist, and the AG's staff says you should not press 9; they will simply invent another number and call you again!

It is helpful to contact the Attorney General's Office if you get calls that are not appropriate and you are on the "No Call" list. They say the fines they receive from violators are very beneficial.

Remember, **the FBI, Microsoft, Social Security, Medicare, the IRS, etc. will not call you.** If you want to talk to these agencies, you must initiate the phone call. Never give your personal information to people who call you and request such information.

## **GENEALOGY NEWS**

The January meeting of Midwest Computer Genealogists will be on Saturday, January 19 at 9:30 a.m. in Bromwell Lounge. We do not meet in December because all of our schedules are full of holiday activities.

Each year in January, we ask our members and friends to discuss their research in 2018. We have had excellent speakers in the past year, and it is helpful for us



to share our progress in our own research with others. It is a good opportunity for us to learn from each other.

We welcome articles for our newsletter about genealogical research, and your recommendations of speakers for this year are also very welcome. We hope to have our 2019 schedule finalized soon.

## MALWARE AND VIRUSES

Marjorie Slavens

We have used anti-virus programs for many years, and we all either have our favorites or we just continue to use familiar programs without determining if they are still providing adequate protection for our computers and mobile devices. This month, Malwarebytes has provided a good analysis of this problem and some answers to the questions we are frequently asked about whether our anti-virus programs are still adequate for this protection.



Malwarebytes is a highly-rated program because of the protection it is providing to individual users and to businesses, and it is a program which is being updated constantly. The premium version of this program prevents potential threats from accessing our computers. The free version will remove some of these threats, but we must update it and remember to frequently run the program manually in order for it to protect us.

Malwarebytes says, "For the most part, "anti-virus" and "anti-malware" mean the same thing. They both refer to software designed to detect, protect against, and remove malicious software. Contrary to what the name might suggest, antivirus software protects against more than viruses—it just uses a slightly antiquated name to describe what it does. Anti-malware software is designed to protect against viruses too. Anti-malware just uses a more modern name that encompasses all kinds of malicious software, including viruses. That

being said, anti-malware can stop a viral infection from happening and remove infected files. However, anti-malware isn't necessarily equipped to restore files that have been changed or replaced by a virus.

Both anti-virus and anti-malware fall under the broader term "cybersecurity". Cybersecurity, or computer security, is a catchall term for any strategy for protecting one's system from malicious attacks aimed at stealing money, personal information, system resources (cryptojacking, botnets), and a whole host of other bad things. The attack might occur on your hardware or software, or through social engineering.

Cybersecurity threats and their countermeasures are varied and nuanced nowadays, but the marketplace naturally strives for simplicity when communicating to consumers. This is why many people still see "viruses" as the biggest threat to their computer. In reality, viruses are just one type of cyberthreat that happened to be popular when computers were in their infancy. They're far from the most common threat today, but the name stuck. It's a bit like calling every disease a cold."

Malwarebytes says "viruses" date from the 1940s. Companies which continue to advertise "anti-virus" protection are using an old term; these programs do more than protect us against viruses. The term is used because it is a familiar term. According to Malwarebytes, "In fact, the last truly "new" virus that replicated itself through user interaction occurred in 2011 or 2012."

The following terms are included in today's understanding of "malware. Malwarebytes protects us against these threats. "If viruses aren't as big of a threat anymore, why do I need cybersecurity?

Viruses are just one kind of malware. Though viruses still exist, there are other forms of malware that are more common these days. For example, here are several common threats that Malwarebytes can stop:

1. **Adware** is unwanted software designed to throw advertisements up on your screen, most often within a web browser, but sometimes within mobile apps as well. Typically, it either disguises itself as legitimate, or piggybacks on another program to trick you into installing it on your PC, tablet, or mobile device.
2. **Spyware** is malware that secretly observes the computer user's activities without permission, then reports it to the software's author.
3. A **virus** is malware that attaches to another program and, when triggered, replicates itself by modifying other computer programs and infecting them with its own bits of code.

4. **Worms** are a type of malware similar to viruses in that they spread, but they don't require user interaction in order to trigger.

5. A **Trojan**, or Trojan horse, is more of a delivery method for infections rather than an infection itself. The Trojan represents itself as something useful in order to trick users into opening it. Trojan attacks can carry just about any form of malware, including viruses, spyware, and ransomware.

6. **Ransomware** is a form of malware that locks you out of your device and/or encrypts your files, then forces you to pay a ransom to get them back. Ransomware has been called the cybercriminal's weapon of choice, because it demands a profitable quick payment in hard-to-trace cryptocurrency. The code for a ransomware attack is easy to obtain through online criminal marketplaces, and defending against it is difficult.

7. A **rootkit** is malware that provides the attacker with administrator privileges on the infected system and actively hides from the normal computer user. Rootkits also hide from other software on the system—even from the operating system itself.

8. A **keylogger** is malware that records all the user's keystrokes on the keyboard, typically storing the gathered information, and sending it to the attacker, who is seeking sensitive information like usernames and passwords, or credit card details.

9. **Malicious cryptomining**, also sometimes called drive-by mining or cryptojacking, is an increasingly prevalent form of malware or browser-based attack that is delivered through multiple attack methods, including malspam, drive-by downloads, and rogue apps and extensions. It allows someone else to use your computer's CPU or GPU to mine cryptocurrency like Bitcoin or Monero. So instead of letting you cash in on your computer's horsepower, the cryptominers send the collected coins into their own account—not yours. So, essentially, a malicious cryptominer is stealing your device's resources to make money.

10. **Exploits** are a type of threat that takes advantage of bugs and vulnerabilities in a system in order to allow the exploit's creator to deliver malware. Among other threats, exploits are linked to malvertising, an attack that uses malicious ads on mostly legitimate websites to deliver exploits. You needn't even click on the ad to be affected—exploits and their accompanying malware can install themselves on your computer in a drive-by download. All you have to do is visit a good site on the wrong day.”

The information below is a little more technical, but some of our reader are more advanced and may appreciate reading the following.

#### **“How does antimalware work?”**

The old school method of signature-based threat detection is effective to a degree, but modern anti-malware also detects threats using newer methods that look for malicious behavior. To put it another way, signature-based detection is a bit like looking for a criminal's fingerprints. It's a great way to identify a threat, but only if you know what their fingerprints look like. Modern anti-malware takes detection a step further so it can identify threats it has never seen before. By analyzing a program's structure and behavior, it can detect suspicious activity. Keeping with the analogy, it's a bit like noticing that one person always hangs out in the same places as known criminals, and has a lock pick in his pocket. This newer, more effective cybersecurity technology is called heuristic analysis. **“Heuristics”** is a term researchers coined for a strategy that detects threats by analyzing the program's structure, its behavior, and other attributes. Each time a heuristic anti-malware program scans an executable file, it scrutinizes the program's overall structure, programming logic, and data. All the while, it looks for things like unusual instructions or junk code. In this way, it assesses the likelihood that the program contains malware.

What's more, a big plus for heuristics is its ability to detect malware in files and boot records before the malware has a chance to run and infect your computer. In other words, heuristics-enabled anti-malware is proactive, not reactive.” (www.malwarebytes.com) If you are not currently running the Premium version of Malwarebytes, you might want to consider doing so. It is a relatively inexpensive program for the good protection it provides.

*(Note: Join us for Computer Chat on Mondays at 1:00. Ipad users: Join Nancy Lincoln Mondays at 3:30.)*