Fox Bytes

Newsletter of the Foxwood Springs Computer Club

September 3, 2020 Foxwood Springs Raymore, MO 64083

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

PROTECTING YOURSELF AND YOUR COMPUTER

For the past six months, computers have played a major part in all of our lives, whether we have previously been generally computer users. Many people are not able to go to work each day, and they have, if they are fortunate enough to do so, been able to work from home. We do not know how long the Corona virus will continue to control our lives, but some of these workers may discover that they like working from home if they can do their work easily and efficiently; they might want to continue after the virus is controlled. Some companies may discover that they would benefit from having their staff working from home. It might be more beneficial for them if they could reduce their overhead and require less space to accommodate their staff in one location.

We all know it would be more beneficial for elementary schools, high schools, and colleges to have their teachers and students working together rather than online. However, we know so little so far about Covid-19 and its transmission from person to person and have no vaccine at present, so it is still dangerous for teaching and learning to take place in person. Many must teach and learn online in order to protect themselves from the virus.

In order for all of us to communicate with each other, work from home, attend classes, etc, we may have to continue to use our computers to search online, no matter which activity we are performing. It is very important for us to protect our computers so these resources are readily available to us at this time when they have become more important in our daily lives.

"JUST TELL ME HOW TO FIX MY COMPUTER": MALWARE DETECTION

Philip Christian

Malware. You've heard the term before, and you know it's bad for your computer—like a computer virus. Which begs the question: Do the terms "malware" and "computer virus" mean the same thing? How do you know if your computer is infected with malware? Is "malware detection" just a fancy phrase for antivirus? For that matter, are anti-malware and antivirus programs the same? And let's not forget about Apple and Android users, who are probably wondering if they need cybersecurity software at all.

This is the point where your head explodes. All you want to do is get your work done, Zoom your friends/family, Instacart a bottle of wine, and stream a movie till you go to bed. But it's during these everyday tasks that we let our guard down and are most susceptible to malware, which includes such cyberthreats as ransomware, Trojans, spyware, stalkerware, and, yes, viruses.

To add insult to injury, cybercriminals deliver malware using sneaky social engineering tricks, such as fooling people into opening email attachments that infect their computers or asking them to update their personal ~~~information on malicious websites, pretending to be legitimate. Sounds awful, right? It sure is!

The good news is that staying safe online is actually fairly easy. All it takes is a little common sense, a basic understanding of how threats work, and a security program that can detect and protect against malware. Think of it like street smarts but for the Internet. With these three elements, you can safely avoid the majority of the dangers online today.

So, for the Luddites and the technologically challenged among our readership, this is your crash course on malware detection. In this article, we'll answer all the questions you wish you didn't have to ask like: What is malware? How can I detect malware? Is Windows Defender good enough? Do Mac and mobile devices need anti-malware? How do you remove malware? How do you prevent malware infections?

What is malware?

Malware, or "malicious software," is a catchall term that refers to any malicious program that is harmful to your devices. Targets for malware can include your laptop, tablet, mobile phone, and WiFi router. Even household items like smart TVs, smart fridges, and newer cars with lots of onboard technology can be vulnerable. Put it this way: If it connects to the Internet, there's a chance it could be infected with malware. There are many types of malware, but here's a gloss on the more infamous and/or popular examples in rotation today.

Adware

Adware, or advertising-supported software, is software that displays unwanted advertising on your computer or mobile device. As stated in the Malwarebytes Labs 2020 State of Malware Report, adware is the most common threat to Windows, Mac, and Android devices today. While it may not be considered as dangerous as some other forms of malware, such as ransomware, adware has become increasingly aggressive and malicious over the last couple years, redirecting users from their online searches to advertising-supported results, adding unnecessary toolbars to browsers, peppering screens with hard-to-close pop-up ads, and making it difficult for users to uninstall.

Computer virus

A computer virus is a form of malware that attaches to another program (such as a document), which can then replicate and spread on its own after an initial execution on a system involving human interaction. But computer viruses aren't as prevalent as they once were. Cybercriminals today tend to focus their efforts on more lucrative threats like ransomware.

Trojan

A Trojan is a program that hides its true intentions, often appearing legitimate but actually conducting malicious business. There are many families of malware that can be considered Trojans, from information-stealers to banking Trojans that siphon off account credentials and money. Once active on a system, a Trojan can quietly steal your personal info, spam other potential victims from your account, or even load other forms of malware. One of the more effective Trojans on the market today is called Emotet, which has evolved from a basic info-stealer to a tool for spreading other forms of malware to other systems—especially within business networks.

Ransomware

Ransomware is a type 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. Many high-profile attacks against businesses, schools, and local government agencies over the last four years have included ransomware of some kind. Some of the more notorious recent strains of ransomware include Ryuk, Sodinokibi, and WastedLocker.

How can I detect malware?
There are a few ways to spot malware on your device. It may be running slower than usual. You may have loads of ads bombarding your screen. Your files may be frozen or your battery life may drain faster than usual. Or there may be no sign of infection at all.

That's why good malware detection starts with a good anti-malware program. For our purposes, "good" anti-malware is going to be a program that can detect and protect against any of the threats we've covered above and then some, including what's known as zero-day or zero-hour exploits. These are new threats developed by cybercriminals to exploit vulnerabilities, or weaknesses in code, that have not yet been detected or fixed by the company that created them. (That's why when companies do fix these vulnerabilities, they issue patches, or updates, and notify users immediately.)

Antivirus and other legacy cybersecurity software rely on something called signature-based detection in order to stop threats. Signature-based detection works by comparing every file on your computer against a list of known malware. Each threat carries a signature that functions much like a set of fingerprints. If your security program finds code on your computer that matches the signature of a known threat, it'll isolate and remove the malicious program.

While signature-based detection can be effective for protecting against known threats, it is time-consuming and resource-intensive for your computer. To continue our fingerprint analogy, signature-based detection can only spot threats with an established rap sheet. Brand-new malware, zero-day, and zero-hour exploits are free to spread and cause damage until security researchers identify the threat and reverse-engineer it, adding its signature to an increasingly bloated database.

This is where heuristic analysis comes in. Heuristic analysis relies on investigating a program's behavior to determine whether a bit of computer code is malicious or not. In other words, if a program is acting like malware, it probably is malware. After demonstrating suspicious behavior, files are quarantined and can be manually or automatically removed—without having to add signatures to the database.

The best anti-malware programs, then, can protect against new and emerging zero-day/zero-hour threats using heuristic analysis, as well as threats we already know about using traditional signature-based detection. If your antivirus or anti-malware relies on signature-based malware detection alone to keep your system safe—you're not really safe.

Is Windows Defender good enough?
Maybe you're using Windows Defender because your computer came with it preinstalled. It seems fine, but you've never looked at other options. Or maybe you have Windows Defender and your computer somehow got an infection anyways. Either way, here's something to consider: Defender is one of the most targeted security programs by cybercriminals. And there are whole categories of threats that Windows Defender doesn't protect against.

The majority of threats detected today are found using signature-less technologies, but there are several other methods of malware detection that, when layered together, offer optimal protection over Windows Defender. Malwarebytes Premium, for example, uses a layered approach to threat detection that includes heuristic analysis technology as just one of its components. Other major components include ransomware protection, web protection, and anti-exploit technology.

Do Mac and mobile devices need anti-malware?
In 2019 for the first time ever, Macs outpaced Windows PCs in number of threats detected per endpoint. Over the last few years, Mac adware has exploded, debunking the myth that Macs are safe from cyberthreats. While Macs' built-in AV blocks some malware, Mac adware has become so aggressive that it warrants extra anti-malware protection.

Meanwhile, Mac's mobile counterpart, the iPhone, does not allow outside anti-malware programs to be downloaded. (Apple says its own built-in iOS protection is enough.) However, there are some privacy apps, web browser protection, and scam call blockers users can try for added safety.

As for Android, malware attacks from threats, such as adware, monitoring apps, and other potentially unwanted programs (PUPs) are more common. At best, PUPs serve up annoying ads you can't get rid. At worst, they'll discretely steal information from your phone. Also, because the Android environment allows for third-party downloads, it's a bit more vulnerable to malware and PUPs than the iPhone. So we recommend a good anti-malware solution for your Android device as well.

How can I remove malware?
Malware detection is the important first step for any cybersecurity solution. But what happens next? If you get a malware infection on one of your devices, the good news is you can easily remove it. The process of identifying and removing cyberthreats from your computer systems is called "remediation." To conduct a thorough remediation of your device, download an anti-malware program and run a scan. Before doing so, make sure you back up your files. Afterwards, change all of your account passwords in case they were compromised in the malware attack. And if you're dealing with a tough infection, you're in luck: Malwarebytes has a rock-solid reputation for removing malware that other programs can't even detect let alone remove.

If you need to clean an infected computer now, download Malwarebytes for free, review these tips for remediation, and run a scan to see which threats are hiding on your devices.

How do I protect against malware?
Yes, it's possible to clean up an infected computer and fully remove malware from your system. But the damage from some forms of malware, like ransomware, cannot be undone. If it's encrypted your files and you haven't backed them up, the jig is up. So your best defense is to beat the bad guys at their own game—by preventing infection in the first place. There are a few ways to do this. Keeping all devices updated with the latest software patches will block threats designed to exploit older vulnerabilities. Automating backups of files to an encrypted cloud storage platform won't protect against ransomware attacks, but it will ensure that you needn't pay the ransom to retrieve your files. Training on cybersecurity best practices, including how to spot a phishing attack, tech support scam, or other social engineering technique, also helps stave off insider threats. However, the best way to prevent malware infection is to use an antivirus/anti-malware program with layered protection that stops a wide range of cyberthreats in real time—whether it's a malicious website or a brand-new malware family never before seen "in the wild."

But if you have antivirus already and threats are getting through, maybe it's time to move on to a program that'll "just fix your computer" so you can stop worrying about malware detection and start…participating in distance learning classes? Ordering groceries? Having your virtual doctor's appointment? Developing a vaccine? Literally anything else. SHARE THIS ARTICLE. (Updated August 25, 2020, Malwarebytes Newsletter, August, 2020)

FINDING INFORMATION ON THE NET

Most information is found on the Internet by utilizing search engines. A search engine is a web service that uses web robots to query millions of pages on the Internet and creates an index of those web pages. Internet users can then use these services to find information on the Internet. When searching for information on the Internet, keep the below things in mind.

Surround searches in quotes
If you are searching for a specific phrase, such as computer help, place quotes around the phrase to get results for that exact combination of words. For example, type "computer help" as your search criteria to match pages where those two words appear together.

This trick can also be used in parts of your search query. For example, Microsoft "computer help" would search for anything containing Microsoft and that also has computer help together.

You can include multiple quoted phrases in your search. For example, searching for "Microsoft Windows" "computer help" would give results for pages that contain both of those exact phrases.

Be aware of stop words
Any search engines will strip out common words they refer to as stop words for each search that is performed. For example, instead of searching for why does my computer not boot, the search engine would search for computer and boot. To help prevent these stop words from being stripped out, surround the search with quotes.

Tip
If stop words are not important, don't enter them into your search.
Familiarize yourself with Booleans
Many search engines allow Boolean logic operators to help filter out bad results. Although common Booleans include "and", "or", and "not," most search engines have replaced these keywords with symbols. For example, to find computer help without results containing Linux, you would type computer help -linux. The "-linux" tells the search engine to exclude any results containing the word Linux.

Know what features are available
Many search engines allow for additional syntax to help limit your search strings. For example, Google enables users to search for links to a particular page by typing "link:" and other keywords at the beginning of the search query. For example, to see who is linked to Computer Hope, you'd type: link:https://www.computerhope.com in the search box.

SEARCH ENGINES

A search engine is software accessed on the Internet that searches a database of information according to the user's query. The engine provides a list of results that best match what the user is trying to find. Today, there are many different search engines available on the Internet, each with its own abilities and features. the most popular and well-known search engine is Google. Other popular search engines include AOL, Ask.com, Baidu, Bing, DuckDuckGo, and Yahoo.

How to access a search engine
For users, a search engine is accessed through a browser on their computer, smartphone, tablet, or another device. Today, most new browsers use an omnibox, which is a text box at the top of the browser. The omnibox allows users to type in a URL or a search query. You can also visit one of the major search engines' home page to perform a search.

Baidu
Incorporated in January, 2000, Baidu is a Chinese technology company that provides Internet services and products. They are considered to be the Chinese equivalent of Google. Baidu serves over 75% of all searches performed in China, making them the second-largest search engine in

the world. The first Chinese company to be listed on the NASDAQ-100 stock market index, in 2017 Baidu's equity was approximately $120 billion. According to Alexa, Baidu is the world's fourth-most visited website. (www.computerhope.com, Updated 06/02/2020)

U.S. CENSUS AND ELECTIONS

The U.S. Census is very important for all of us as family historians. We trace our ancestors back from the latest census in which we can find them decade by decade. Although we can find our female ancestors in earlier census records, their maiden names are not included, and this presents many challenges as we try to trace the family lines of these ancestors. Marriage records are not always easy to find. In addition, the U.S. Census records before 1850 only include the names of the heads of house. The immediately preceding decades give information about males and females and some information about ages. The earliest Census records group the genders together, and it is difficult to identify those who were not heads of house unless we are able to find marriage, church, or will records that identify those who are grouped together.

2020 is a very important historical year. This is the 75th anniversary of the end of World War II. The war in Europe ended on May 9, VE Day. On August 14, --Japan accepted unconditional surrender terms, VJ Day , and on September 2, the Japanese sign ceremonial surrender terms aboard the U.S.S. Missouri.

The year 2020 is the 100th anniversary of the 19th Amendment, which resulted from the strubble and work of women of the previous century. Most women were able to vote when the amendment was approved, but some black women in the south were still denied the vote until the Voting Rights legislation past in the 1960s. States determine the rules for elections, and literacy tests, poll tax, and other prohibitions made it impossible for these women to vote.

Census records are very important for other reasons than tracing our ancestors. The number of U.S. Representatives in each state are determined from the previous Census, and some federal funds are distributed to the states according to the reported populations. 2020 has presented some additional challenges for the U.S. Census. Many of us were able to register for the Census online, and the spelling and writing errors that we have found in some earlier handwritten Census records should not be difficult to read in the future. However, the pandemic presents some significant problems for those who could not or did not complete their Census forms online. We would like to think that everyone has an opportunity to be included in these records.

From 1850 to the beginning of this century, the information provided in the Census increased. In 1850, the names of all people residing in a household are given for the first time. The 1880 Census provides the birthplace of parents of the people including, helping us trace them back to places from which they emigrated. In 1900, we are able to see how many children a woman had had and how many of them were living at that time.

This is the 60th anniversary of the election of the first Catholic President, John F. Kennedy. I cast my first vote in that election and have voted in 14 Presidential elections since that time. I have voted in two states, Missouri and Illinois. In 1860, I voted by Absentee ballot in Ohio where I moved in September because my legal residence was still at my parents' home in Missouri.

I have been listed in 9 U.S. Census records, but I have not found myself in any of these records yet. We have not been able to find my family in the 1940 Census, and the 1950 Census will not be published until 2022, 72 years after this Census was taken. I have lived in Oklahoma, two cities in Kansas, five cities in Missouri, one city each in Florida, Ohio, and Illinois. We have much better records now because of technology, but if I had lived 100 years before, it would have been extremely difficult for future generations to find me in each census.

Marjorie Slavens, Editor