Midland Computer Club

Midland Michigan

BITS AND BYTES

OCTOBER 2021

https://mcc.apcug.org/

ARTICLE INDEX

GENERAL CLUB MEETING
VIA ZOOM

Wednesday, October 27, 2021
6:00 P.M.

Cautionary Tale about Free VPNs

By Joel Ewing, President, Bella Vista Computer Club
April 2021 issue, *Bits & Bytes* — www.bvcomputerclub.org — president (at) bvcomputerclub.org

One of the caveats in the VPN article in the March 2021 *Bits & Bytes*, also mentioned at the March General Meeting, was that free VPN services were not recommended. As if on cue, see the following article recently published by Malwarebytes Labs on "21 million free VPN users' data exposed."

A hack of several free VPN services revealed that not only were some services collecting user activity logs in contradiction of their advertised policy, but some were also collecting email addresses, passwords that were not encrypted, IP addresses, mobile device models, and IDs.

The whole point of using a VPN with mobile devices is to avoid exposing non-encrypted data when using a public Wi-Fi network; but if that data would have been non-encrypted on a public Wi-Fi without VPN, then with a VPN service, it is still exposed non-encrypted within the server of your remote VPN service. In addition, if the service also requires a special app to be installed on the mobile device, then that app will also see any non-encrypted data before it is sent to the VPN service and potentially have access to other data on the mobile device. Thus, a free VPN service is much more likely to be tempted to exploit their access to non-encrypted data if that is their only way to profit from the free service.

One of the reasons for distrusting the security of a public Wi-Fi network is that you can never know whether or not it is supported by secure hardware or whether that hardware is configured correctly to at least make it as secure as possible. Because of the limited number of users on one Wi-Fi network, the motivation to expend much effort to hack that one network is not high. But, if it shares an exposure common to many other Wi-Fi networks using similar hardware, it could be at risk. Furthermore, the users have no way of knowing the details of a particular public Wi-Fi node, so it is wise to err on the side of caution. A VPN service, on the other hand, may have hundreds of thousands of users.

The possibility that a free VPN service may be engaging in questionable behavior and be holding sensitive user data on its servers makes it an extremely attractive target for hackers and data thieves, who can justify spending much time and effort to break in. That makes any collection of sensitive information by a VPN service a more serious concern. One of the suggestions made is that you should look for reviews of a VPN service by known and trusted organizations before deciding on a VPN service. One of the interesting things that this data leak revealed was that there were several differently-named free VPN services that all appear to be run by the same company. These were all supported by mobile apps that were gathering inappropriate data, combined with the attempt to disguise the company's true identity, suggest that this was a deliberate attempt to engage in unethical behavior.

Caveat Utilitor

Don’t Let Your Identity be Compromised!

By Jeff Wilkinson, President
Sun City Summerlin Computer Club — https://www.scscc.club — president.scscc (at) gmail.com

We should all be cautious answering those seemingly innocuous questions posted on social media sites such as “*What Year Did You Graduate High School,*” or “*What City were you Born in,*” “*Can you remember your childhood phone number*?” or “*Who was your first-grade teacher*?” and on and on. These interesting questions appear harmless and appealing as you develop friendships and reminisce with old and new friends on social media, but beware! Many of these answers can be used to answer or reveal security question answers you chose when you set up accounts at your bank, utility company, etc. For example, when you forget your password, as happens all too often, you will be asked to answer security questions from when you initially

set up your account, in most cases some time ago! In addition, answers to these types of questions posted on social media or quizzes can be used to build a profile on you with the information needed to open a new account!

Keeping your identity secure on social media is essential to your financial and personal safety. Unfortunately, identity theft is evolving, with thieves using the latest technology to move from credit card counterfeiting to checking and savings account takeover. A May 2020 study by Javelin Strategy and Research found account takeovers — identity theft where a criminal gains unauthorized access to an online account belonging to somebody else — are trending at the high loss rate, up a staggering 72 percent over the prior year.

Remember that when you first create a social media account, you provide personal information such as name, age, email address, etc. And I venture to guess that most of us have never read the small print terms of service provided by the host. As you traverse the various pages, forums, postings, etc., data mining creates a profile of your behavior, likes, and dislikes. This information is often monetized by the host sites you visit, meaning sold to third parties. Facebook collects data from all devices you have installed their app on. The language used and time zone can include your device location, data provider, or internet service provider. Data on sites you like or visit via a link on Facebook is also collected.

What can the consumer do to protect themselves?

- Keep your software up to date
- Log out of social media sites when finished, particularly when in a public location or using a public computer
- Use two-factor authentication wherever possible.
- Used strong passwords - keep track of them with a password manager
- Use a screen lock on portable devices
- Don’t conduct business or share critical information on public Wi-Fi
- Put a credit freeze on your accounts with credit bureaus. Equifax, Experian, Innovis, TransUnion
- Protect your social security number – only give it out when absolutely necessary
- Be aware of billing cycles – if financial information is late or doesn’t come, follow up
- Be cautious of participating in viral memes such as “name your most memorable concert.”
- Set strict privacy settings on Facebook, Twitter, Pinterest, Instagram, and LinkedIn

If you are a victim of identity theft, report it to the FTC online and create an account to create a report and generate a recovery plan. You will gain access to recovery plan updates and prefilled form letters to send to creditors. You should also report medical identity theft to Medicare’s fraud office and tax identity theft to the IRS.

It should be clear that you want to avoid this, so a little awareness and preventative steps can help prevent potentially serious problems.

Dan's Desk

Don't Respond to Potential Scams

By Dan Douglas, President, Space Coast PCUG, FL
April 2021 issue, *The SCPCUG Journal* — www.scpcug.org — datadan (at) msn.com

PLEASE PRINT THIS OUT AND PASTE IT NEAR YOUR PC AND READ IT BEFORE RESPONDING TO ANY POTENTIAL SCAMS.

Unfortunately, I have seen a dramatic increase in people seeking help after being scammed on their computers. Unfortunately, this includes some of our SCPCUG members. So, this month, I would like to share some precautions you can take to minimize your exposure to getting scammed on your computer.

Let's look at the most common ways of enticing people to fall for these schemes:

1) Phone Calls - Receiving or placing a phone call, supposedly from or to some recognizable, well-known/ trusted organization, such as Microsoft, Dell, Amazon, HP, etc.

Prevention and best practices to avoid falling victim:
If you want to contact an organization, go to their official website and click on the contact us link. Do not search for contact info. Scammers pay to be listed first on common searches and will act as if you are calling the real company. I've seen this many times with people trying to call HP for printer issues or supplies. They do a web search and call the first number that comes up, and the person convinces the caller that their printer may need an update, and if they give them remote access, they can check it out, and then it is game over.

It is extremely unlikely you would ever receive a phone call regarding your PC or any activities you perform.

My advice is to immediately hang up on anyone claiming to be calling from one of these organizations.

2) PC Messages - Receiving a screen message on your PC that informs you - take your choice - you have been hacked, you are in danger of losing your banking passwords, your PC has been used for illegal acts and will be reported to the FBI, your IP address has been traced, etc. The message usually states to not turn off your PC and to call some number immediately.

These are commonly delivered through your browser (Edge, Chrome, Firefox, etc.) but can be cleverly designed to hide where it originated from or look exactly like common company messages by using their logos and copies sections from their actual web pages.

Prevention and best practices to avoid falling victim:
Ignore the message – do not be scared or worried. Instead, immediately force your computer to shut down completely (NOT sleep) – pull the plug if you need to. The scammer will usually disable many of the common ways to close the program/browser normally, such as preventing you from clicking on the close X in the top right-hand corner, so forcing the power off may be the only way. Usually, the scam will not permanently infect, corrupt, or access any of your information if you shut it off immediately. Download the free version of Malwarebytes from www.malwarebytes.org if you want to be sure all traces are removed. If you let the scammer have remote access to your PC, you may need to change your accounts (credit cards and financial) and their passwords to be safe.

3) Email – Opening an attachment or clicking on a link embedded within an email can launch any one of many forms of 'attacks.'

Prevention and best practices to avoid falling victim:
The first thing that I always do when I get an email that may be suspicious is to check the sender's email address. Your email program may always show this address, or you may need to hold the mouse over the name to see the actual email address that was used to send the email. Anything that doesn't look normal, such as a domain name that is not the same as the company name, or a sender ID that looks made up, such as dsae12345@ myname.com, I would delete/flag that email as junk and report it as a phishing email. Phishing is where the scammer tries to get you to log on to a website that looks like a legitimate one but really captures your login information – common ones are banks, PayPal, and Amazon. Never open an attachment without checking the sender's email address first. Malwarebytes is a good program that may be able to block many scam programs before they are active if you are using the premium version.

I Was a Fool, So You Don't Have to Be

By David Kretchmar, Hardware Technician
Sun City Summerlin Computer Club — https://www.scscc.club —dkretch (at) gmail.com

I don't necessarily think of myself as a fool, but I did a foolish thing a few years ago. I bit on one of Motley Fools' ubiquitous teaser internet ads promoting the best new emerging technology stocks that were about to "explode." I paid (I think) $29 to Motley Fool to get the names of the stocks. Motley Fool sent me the names of several mostly small and pink sheet stocks. Most pink sheet companies are highly speculative, have little or no earnings, and are low-priced penny stocks. For many pink sheet stocks, a price appreciation up to one penny would be wildly profitable, but well over 90% of these stocks appeared worthless.

The Motley Fool
MAKING THE WORLD SMARTER, HAPPIER, AND RICHER

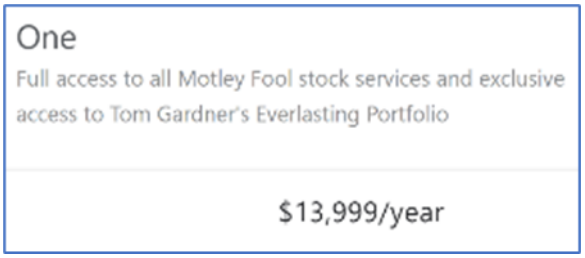
I wonder if they are buying shares before they recommend them and running the shares up and then maybe even shorting them or just taking advantage of people willing to pay for their information. Their expertise seems to be selling themselves, not researching companies.

The Motley Fool's website is self-described as "A wide-ranging investment resource that intended to "educate, enrich, and amuse individual investors around the world." The site includes discussion boards, quotes, data, and of course, stock-picking advice. Many of the articles are voluntarily contributed by various individuals. Unfortunately, I suspect that many have taken a position in the stocks they are now pumping, not unlike the Motley Fools, with hopes of profitable dumping.

Upsells

If you are not satisfied with the advice provided according to your original subscription, the Motley Fools will offer you "better" subscriptions, such as:

Or:



A Foolish Website

I am not new to the stock market; I focused on security analysis in college and have been doing my own research for over 50 years. Almost everything I have seen from the Motley Fools is absolute garbage. I highly recommend not using their website for any information except maybe for the entertainment value of how foolish it is. Often there are contradicting opinions on the same stock on the same day!

There is way too much advertising on the Motley Fools subscription website. This site is without transparency and, therefore, of questionable value for investors. Suppose you want to be successful, and actually be one of the rare investors who make money relying on the advice of others. In that case, you need to receive information from people whose own investing/trading results you can clearly see. There are several dozen articles every day, and I believe no one could construct a good trading strategy based on the hundreds of stocks they say are "ready to explode."

The Motley Fool's subscription website is a mess of marketing. Most of the articles provide virtually no actionable information, except pitches for more expensive Motley Fool newsletters. Occasionally there is a well-written article that contains decent information, but this is rare.

To be fair, I do agree with their philosophy that a buy and hold strategy, not trading, is the path to real wealth accumulation. They deride ALL short-term trading dogmatically but make tons of picks, some work, others totally fail. Also, they advise not to bother trying to time the market; just spend time in the market holding your winners and trimming losers. So there – in this paragraph, I've reflected virtually all of the sound advice you are likely to glean from the Motley Fool website – and it was FREE!

Can they do 5X better than the market?

It is inconceivable that The Motley Fool could beat the S&P 500 by over 500%, as they claim in their current advertising. Most professional money managers and advisors have difficulty equaling the performance of the market averages. Those who are considered investment geniuses, such as Peter Lynch and Warren Buffett, could beat the market by a few percentage points a year. Anyone able to beat the market averages by 500% would be able to amass great wealth investing and would not have to sell a tout service.

Even the free offers are less than worthless

Almost every day, I see Motley Fool teaser articles on sites such as Yahoo Finance, and often the headline is misleading. The article provides just a superficial discussion of a stock. Usually, the article ends stating the stock discussed is OK (or bad), but the Motley Fools knows ten stocks that are better, which they will provide to you if you just furnish your email address. I have done this several times (providing my "junk" email address) and have never received the information the Motley Fools promised. Instead, they bombard my mail account with worthless spam. I suspect they also sold my email address since I also started receiving spam from unknown companies.

The sports betting scam

When I worked as a Special Agent in a former life, I was involved in investigating an off-shore sports betting site. The owners of this site quickly discovered they could make more money selling gambling advice, also known as tout services, than from the bets themselves. The profit on sports bets was about 5 percent – (10% of losing bets), similar to on-shore bookies and casino sportsbooks.

Say Boston was playing New York, they would tell half their new subscribers (or potential subscribers) to bet on Boston, and the other half New York. After the game, half of their customers would feel their handicapping might be good, and the other half would probably quit. The subscribers who stayed would tell half of them to bet one side of a game and the other half to bet the other side. Again, half of their customers would think they were great, and the other half would have their doubts. After doing this once or twice again, they would have a smaller pool of customers who thought they were geniuses and would pay big bucks for their next tip.

Conclusion

The Motley Fool and many other stock picking services operate similarly to the sports tout scam. But, at least they are no fools; only people who buy their services are.

It's Called Clickbait, and You Need to Learn to Avoid It

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://www.ckcs.org — lextown2 (at) gmail.com

I was eating yogurt as I was reading stories about one growing danger on the Web: Clickbait. What I read made me pause and put down my spoon.

It turns out that plenty of us are clicking on email links or Facebook postings sent to us from unknown senders. Unfortunately, this can lead to malware and trojan horses infecting your computer.

The practice is called clickbait. Someone you don't know sends you an email or a Facebook posting. It contains a link. You click on it.

Catchy and provocative headlines are usually a dead giveaway that you're being targeted by clickbait.

Clickbait often contains these qualities:

- Headlines that appeal to your strong emotions, such as humor or outrage
- Headlines designed to grab your attention, leaving you wanting more information
- Headlines that tell you nothing about the content of the article
- The headline is too good to be true
- Content that encourages you to share the item with someone else on Facebook
- Funny images or video

Examples of clickbait headlines include:

87–Year–Old Trainer Shares Secrets toLosing Weight

When You Read These Shocking Food Facts,You'll Never Want to Eat Again

Stop Eating Chicken Breasts Immediately

Here's the scary part. A study of 7,804 students by the Stamford Historian Education Group revealed that more than 80 percent of middle school students believed an ad was an actual news story. This, despite the fact that the ad was clearly marked with the words, "sponsored content."

The point is to teach people to recognize clickbait and to avoid it. It's not worth your time.

Free IQ tests and credit score checks often ask you to fill in personal information. Unfortunately, you don't know that the website collects your personal details to build a profile on you. Once you submit this information, you'll be subjected to scams and even more links to dangerous websites.

Clickbait links open the door to more spam and potential malware, adware, spyware, viruses, worms, trojan horses, and the real possibility that someone could take over control of your computer. Just say no by refusing to click on links you aren't sure about.

The DealDash (Penny Auction) Scam

By David Kretchmar, Computer Technician
Sun City Summerlin Computer Club — https://www.scscc.club — dkretch (at) gmail.com

If you watch much TV or surf the internet, you've seen ads promising products as much as 95 percent off retail at DealDash.com or other penny auction sites. DealDash advertises itself as offering fair and honest auctions, but is it really? Millions of people have signed up for a chance to buy items at penny auctions at a fraction of the retail price. Who wouldn't want to buy a new iPad for $30? But think about it; who would want to sell that iPad for $30 when it cost several hundred dollars wholesale? It is worth noting that the "penny" in penny auctions refers to the bid increments, but your actual cost could be many dollars.

Consumers are buying more items online every year and appreciate the convenience, selection, and often substantial cost savings. So, these penny auctions would appear to be an extension of that money-saving online buying concept.

Most consumers are familiar with online auctions at sites such as eBay, where interested individuals bid up the price of an item until time expires. The high bidder at the end of the auction wins the item at the winning bid price.

However, another form of online auctions, internet penny auctions, has expanded in recent years. While some of these sites are *technically* legitimate, many of their business practices are questionable, and most consumers would be better off avoiding them altogether.

How penny auctions work

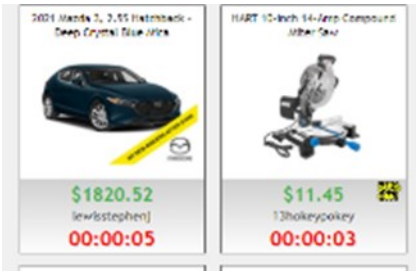
In some ways, online penny auctions are internet bidding sites that share some similarities with legitimate auction sites like eBay. However, the BIG difference is that consumers who bid on penny auctions must pay for each bid they make regardless of whether they win or lose the auction.

Generally, anyone interested in bidding in a penny auction must pay a registration fee before gaining access to bidding. While not required by all penny auction websites, this fee is often described and charged in what many consider an underhanded way. For example, it is typical for a consumer to make a query regarding online penny auctions. If the consumer provides credit card information, that credit card is immediately charged $60 - $99 as part of the registration process. Often consumers provide credit card information without realizing they are authorizing any payment.

An Auction Example

As stated above, penny auctions' business model immediately charges anyone furnishing them a credit card number of at least $60, which buys 100 bids.

Most new bidders bid on one or two auctions, lose their 100 bids ($60), and quickly realize getting a bargain wasn't as easy as it looked. These sites count on the addictive nature of *almost* winning an auction, maybe losing by a penny or two, to encourage a percentage of bidders to buy more bids. Sometimes a substantial discount is offered - i.e., if you sign up right now, you can get 200 bids for the same $60.



Penny auctions usually allow losing bidders to apply at least part of the money spent on bidding towards buying the product at *their* retail price.

However, penny auction sites, including DealDash, often substantially overstate the retail price of items, so buyers are usually either overpaying or perhaps getting completely ripped off.

How the Auction Works

The bidding for an item typically begins at $0 and then increases by one cent each time someone bids. There is a countdown clock that restarts every time someone places a new bid. Some websites even allow users to set up automatic rebids if they are outbid. The total price of the item “won” is determined by the number of bids, so you could end up paying well over the retail value of the item you’re bidding on. Generally, you have also lost the money spent on the used bids if you lose the bid.

Let’s say the auction is for a new computer with a stated retail value of $599. The bidding starts at $0, increases in 1 cent increments, and one “lucky” bidder “wins” the computer for $30. The winning bidder is given credit for the bids he has “spent” at $0.60 each. It is not unusual to see individuals bidding hundreds of times, so if the winner in this example bid 300 times, that winner paid $180 for their 300 bids, if each bid cost $0.60. Still, this does not seem like a bad deal for the winner; $180 for a $599 computer, even if it is a system, you could get on Amazon for $399.

If a penny auction item sells for $180, the auction site has received 18000 incremental 1 cent bids, which cost the bidders as much as $10,800! Penny auction sites often promote themselves as “social media” buying and stress the social nature of their sites. What they don’t advertise is how addicting these sites can be. $10 gift cards can go for over $20 when bidders’ egos apparently overrule all common sense. And I can virtually guarantee that YOU will not get that computer for $180.

An individual cannot determine which penny auction sites are “legitimate.” Some state attorney generals have found that some penny auction websites use “shills” that automatically outbid people, making it virtually impossible to win items at a reasonable price. Some of these shills are software programs that show a fake username to persuade consumers that they are bidding against a real person. As a result, several penny auction sites have disappeared, never shipping items won. Other sites have sold financial information about users or put additional charges on credit cards without permission.

Conclusion and Recommendation: Avoid Penny Auctions

While online penny auctions may sound like an attractive deal at first, consumers should be very wary before handing over any money or credit card information. It is doubtful that consumers will save any money by using the service to purchase goods, and much more probable they will be ripped off.

Those Pesky Car Warranty Calls

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://www.ckcs.org — lextown2 (at) gmail.com

Nearly every other day, I receive an obnoxious voice mail: Your car warranty has expired. This is the final call. If you don't respond now, you will get no extended warranty coverage.

Those calls go to my iPhone's voice mail without bothering me because the robocall slayer software known as Nomorobo recognizes this is snake oil and keeps my phone from ringing.

Now, NPR has dissected the calls and given us an inside look at what's really going on.

It turns out if you pay for this service, it covers very little, according to NPR's Planet Money. If you paid a monthly fee, the company claimed to cover your car bumper to bumper. But it turns out the warranty was worth about as much as the paper it was written on. Furthermore, this was all promoted in a very deceptive way, says the NPR article.

The piece notes the contracts sold were legal. But if you tried to cancel the service, your patience was taxed to the max.

NPR says the standard operating procedure was to force customers to talk to six or seven people to cancel. Then, while speaking to that individual, the company would purposely terminate the phone call. Then the customer had to go back through the process all over again to try and cancel their service.

It turns out despite all this, the company called U.S. Fidelis was doing very well. According to NPR, "One of the owners spent $26 million building a mansion with a bowling alley and all these secret rooms and this weird walkthrough shower that was kind of like a car wash for your body."

By 2007 or 2008, the complaints began piling up. Since word was getting around that U.S. Fidelis customers were quite unhappy, the company turned to a new way to promote itself: robocalls.
By one estimate, U.S. Fidelis sent out one billion robocalls pitching its product – in just ten months.

As tempers flared and unlucky recipients of these phone calls fumed, more than 40 states began going after U.S. Fidelis and its robocalls. NPR reports U.S. Fidelis was banned from robocalling. In addition, dozens of news articles, TV and radio news reports, and Internet news stories blasted the company. Finally, U.S. Fidelis customers vented during news interviews. They were red hot angry.

Tales of families sitting down for a nice evening supper interrupted by these robocalls surfaced.

Folks who could hardly afford to buy these so-called "extended car warranties" were spending hard-earned dollars.

Eventually, the company went bankrupt.

So that's the end of the extended car warranty robocalls, right? Not. Exactly.

NPR reports, "It's been ten years since US Fidelis went bankrupt, and now these auto warranty calls are back with a vengeance. But unlike with US Fidelis, many of these calls do not name the company calling you. So, while the federal government tries to figure out who exactly is calling, you will continue to be robocalled and asked about your car's extended warranty."

Read and hear the NPR story here.

More stories:

FCC - Combating Spoofed Robocalls with Caller ID Authentication

FTC says hang up on car warranty robocalls

Car Warranty Scam Robocalls: Here's Why You Get So Many (And How to Stop Them)

Tricky Spam Emails

By Jim Cerny, Forums Coordinator / Instructor, Sarasota Technology Users Group
www.thestug.org — vp1 (at) thestug.org

You probably are all aware of those awful spam emails that come to you in your inbox. But recently, I had a very sneaky and tricky spam email that appeared to come from a friend, and I need to tell you about it so you can be very careful.

First, I received a brief email from a friend of mine who was also listed in my contact list, but I found out later that the source email address was not really his. It “looked” like his, even having his wife’s first name in it, but it was NOT his email address; it was from a different email provider, which he never used. Yes, that was tricky all right, but later that week, I received one even worse. The email sent to me appeared to come from another friend and, being very careful, I “hovered” my mouse on the email address, and it did show his actual email address, exactly as it is entered in my contact list! But it was NOT from him.

Fortunately, I called him, and he confirmed that someone had “stolen” his email address and was using it to try to get gift cards from people.

So, in addition to the usual email precautions, I would like to offer these to help you from being scammed

+ Brief emails from a “friend” that say something like “Can you help me?” or “Can I ask a favor?” are clues that they are bogus. Call your friend to confirm if they really need your help. As they say, if it was really urgent, they would have called you, not sent an email.

+ If you do reply to such an email by mistake, you will get a follow-up email with a sad story and an urgent request for something like a “cash card” or donation. Don’t do it!

+ Do not reply or provide ANY personal information in ANY email. Emails can be forwarded to anyone anywhere. Valid email addresses are traded like stolen credit card numbers.

+ Do NOT send money or credit card information in any email. Instead, use your online banking to pay bills.

+ THINK – did the email text really appear to be something your friend would write to you? If there is the least bit of oddness about it, call the person.

How do these scammers get started? Our neighborhood has a directory provided to all residents, which includes phone numbers and email addresses. Many people purposely do not provide their personal information in such a directory. Once you get an email address, I suppose it is possible to tap into some emails sent by that address and thus obtain many more email addresses.

Finally, it appears a scammer can send an email that appears to come from someone else’s address, and yet they still receive replies to the scammer’s email inbox. How they do this, I have no idea, so be careful.

One final story – I was at the Walmart customer service desk when an older man was requesting a money transfer to his son, who needed money quickly. The Walmart people knew right away that it was a scam and refused to fulfill his request. The man was angry, but it was the right thing to do. He wanted to send “his son” several thousand dollars!

Dan’s Desk

Backing Up

By Dan Douglas, President, Space Coast PC Users Group
The Space Coast Journal — www.spcug.com — datadan (at) msn.com

We’ve discussed the subjects of performing backups recently at our meetings, so I thought I would update the article I wrote on the topic back in 2018.

Two types of files are required to be backed up. There are your personal files, normally stored in the following folders under your login account in Windows: Desktop, Documents, Downloads, Favorites, Music, Pictures, and Videos. Each user that has an account on a PC has their own set of these folders. If the user only uses the programs that come with Windows or has a standard set of programs that they add to Windows that are can be easily re-installed either from a DVD/CD backup or a download file, then that makes backup and recovery much easier. The other type of files to be backed up would be the Windows System Files. These include the Windows Operating System itself plus all of the programs/ apps, files, and data used by those programs/apps.

If you have all of your personal files backed up and you have the files required to reinstall your programs, then you can easily get a replacement PC or hard drive restored completely.

Just about every PC user has heard that they should back up their PC, but based upon what I've seen, only about 20% have an active plan in place.

The reasons that I've been told that users do not perform backups regularly are along these lines:

I don't know how to set it up
It will slow down my computer too much
It's too costly
I forget to do it

None of these are acceptable excuses anymore!

Let's go through these one by one and see how to address the issues.

Setting up your backup
In Control Panel, under every version of Windows since Vista, there is an app named Backup and Restore or Backup and Restore (Windows 7). This app is suitable for 99% of the user community.

This app lets you pick a target location for where your backup will be stored either on a local drive or a network storage location, which can include cloud storage. A schedule can be set for what frequency you want to use for creating your backups – daily and what time of day or weekly by day of the week and time of day or monthly by day of the month and at what time of day. You can also determine if you want just your file libraries backed up or the whole disk(s). In both cases, a System Image will always be created as well. The System Image can be used by a restore program to exactly duplicate your hard drive onto a new PC or a new hard drive. The retention period can also be set for how long to keep a backup for or you can allow Windows to manage the space and to automatically replace the oldest backup with the newest.

Selecting the best time to perform your backup When you select the time of day to run the backup as described in the previous section, you must pick a time that will be when your computer will be powered on. The backup program cannot power on a PC that is turned off to perform a backup. So if you use it each Sunday at 7 pm, make sure you leave your PC on every Sunday evening. A backup that runs when you are using the PC can impact your responsiveness and will take longer to complete than running at a time that no one is using the PC.

Cost of running the backup
Since the backup program is included with every copy of Windows, there is no software cost. In addition, almost all external backup drives include a backup program of some sort. Cloning/backup software from Macrium is also recommended. The only cost is that of providing a backup drive, either as a local hard drive or a network-accessible location such as a Network Accessible Storage (NAS) or cloud storage. This drive can be used for other purposes so even that cost can be split across other activities. An external 5TB USB 3.0 drive can be bought for less than $130 lately, so that's cheap insurance for not losing all of your data.

Set it once and it's automatic
As we saw in the sections above, once you set up the backup program, it will run automatically as long as the backup location is accessible and the computer is turned on at the scheduled time. Perhaps a repeating calendar reminder note will help make sure that you are always protected!

Restoring from a backup is best suited to situations where your hard drive is damaged and some files can no longer be accessed or the system won't even boot up. I've seen a lot of computers recently, where the owner complains of poor performance and upon investigation, I've been able to determine that it was a hard drive failing that was causing the lack of responsiveness. The hard drive would sometimes retry reading a file hundreds of times before either being successful or unsuccessful. This causes the hard drive to fall behind in any other requests for data and therefore the whole system slows down.

The File History app, which was introduced in Windows 8, is the best program to use for restoring individual files. Every time a file is created, changed, or deleted a copy can be written to the file history backup drive. This drive can then be used to restore a previous version if required. This is a great recovery tool if you are ever a victim of a ransomware attack where your personal files are encrypted. You can add additional directories to be backed up in addition to the normal set of personal file folders.

The option of Save copies of files specifies how often File History runs automatic backups. The default is hourly, but you can set the frequency to 10, 15, 20, or 30 minutes; 3, 6, or 12 hours; or choose to back up files once a day. Please note that a new version is created only when at least one item has changed in the file. The Keep saved versions option specifies how long to keep the backups. By default, these are kept forever, but you can also select 1, 3, 6, or 9 months, or 1 or 2 years. If your backup drives are tight on space, you can select the “Until space is needed” option and risk losing older backups quickly.

The best approach is to use the Backup and Restore program regularly, perhaps just using the System Image backup function, together with File History to fully protect all of your important files and folders. That way you will be protected against both hardware failures of the hard drive as well as accidental deletion or corruption of important documents.

Don’t pass up the free cloud storage from Microsoft, Google, and others that can supplement what you backup to a local/network drive. Cloud storage is impractical for full drive/image backups due to the extremely long time that it would take to do a full recovery over the internet, but for individual files, it’s great.

How Do I Remove a Virus from My Browser?

By David Kretchmar, Computer Technician
Sun City Summerlin Computer Club — www.scscc.club — dkretch (at) gmail.com

Our computer operating systems have become more secure, so developers of malware have turned their attention to a more vulnerable target, our web browsers.

Chrome, Edge, Firefox, Safari, and Opera are the browsers most of us use to connect to the Internet. All of these browsers can be infected by a redirect virus, despite their built-in security.

Redirect viruses, also known as hijackers, can make your online life very difficult In this article, I’m going to describe the process of acquiring, identifying, and removing an infection from your browser. I’m going to focus on Google Chrome; the techniques are similar, yet slightly unique for each browser. Most users should be able to use the described procedures on their own systems, with small variations depending on the browser and underlying operating system (Windows, Apple, or some flavor of UNIX/Linux).

Redirect viruses can come from several sources.

Extensions

Hijackers can sometimes be “Trojan Horsed” in with browser extensions; extensions are small programs for a browser that serve the desired purpose, such as weather, price comparison, coupons, or productivity tools. If you install these extensions, you could unknowingly grant them the ability to influence your browser settings or change your preferences such as your home page or your default search provider.
Extensions are usually the first place to examine if you suspect you might have an infection.

Spam emails

On at least a weekly basis I receive an email telling me that my account at Amazon, Facebook. eBay, PayPal, etc. have been frozen due to suspicious activity. The email contains a link to click on to resolve the problem. In reality, if I clicked on the link provided, my problems would be just starting. If you receive an email informing you of a problem with, for instance, your Amazon account, access your Amazon account the way you would normally if you think there might be a problem.

Social Media

Links from your Facebook or Twitter feed could also be rerouted in phishing, redirects, or browser hijacking. Facebook is notorious for allowing questionable items to appear in your feed. Some bad links might be posted by unsuspecting Facebook friends who find it easier to copy and paste or just click Share than to vet an item. And no, Costco is not going to send you a $50 voucher if you just take this survey revealing all sorts of personal information.

Free software downloads from unreliable sites.

Hijackers can get added along with free software downloads. Often web sites will offer a desirable program but try to trick the user into downloading malware. Always look at the address bar to make sure you are downloading software from the legitimate provider's site.

Without realizing it, you could lose control of your browser by clicking on the wrong link on the wrong website.

Do I have a browser virus?

A browser virus on a PC or Mac is a browser hijacker that targets your browser. This type of malware is used to generate web traffic and collect information.

How do you find out if your browser has a virus? Here are the main symptoms:

- Your homepage redirects to a website different from what you expect.
- Unwanted extensions appearing in your browser (you might see icons at the top right side of your browser).
- Ads show up more often than they should, usually in unexpected places.
- Pop-ups and banners that advertise fake updates or software regularly appear.
- The link you click in search results redirects to dubious or possibly malicious websites.
- Your browser performance decreases dramatically no matter where you go on the Internet.

A virus can also ask you to update a program such as Adobe Flash Player or download any other tool (program) that would help you fix the problem it is creating. These warnings don't always mean that you have issues with the browser but should be suspect.

If you notice any of these signs, your computer browser is possibly infected with a virus.

Potential risks of a browser virus

As a browser hijacker, a pop-up virus is categorized as a potentially unwanted program (PUP). Once the malicious program attacks your computer, it starts modifying browser settings. For instance, it changes the default search engine and homepage, without asking for your permission.

The most serious problem created by having this virus is the ultimate invasion of your privacy; secretly harvesting as much of your personal information as possible to engage in identity theft. Some browser viruses are all about collecting personal details (IP address, location, searches, etc.) and sharing them with third parties. This may cause serious problems related to privacy and data security.

How to get rid of the browser virus

Delete unrecognized extensions

1. Go into your browser settings (in Chrome it is the three perpendicular dots at the upper right side of the browser).
2. Click on the Extensions tab.
3. Look for any extensions that shouldn't be there. If you find anything, select it and hit the Uninstall button to remove it.

Check your homepage and search engine settings

These settings appear in the settings area of your browser. In Chrome go into the browser settings and click on Settings. Make sure your homepage and default search engine are correct.

Additional things to check

1. Go to the Applications or Applications and Features folder and find any suspicious software. It may disguise as the desired application, so search for anything you don't remember downloading. Also, note the install date to identify possible problems and look at the last program you downloaded before noticed problems.
2. Check your Downloads folder for items recently downloaded from the Internet for clues about the possible problematic vector that has introduced the malware into your browser.
3. Once you detect the malware, drag it to Trash and empty it, or delete it and then remove it from your Recycle Bin.

Get rid of every trace of malware

After the above steps, download and perform a Malwarebytes scan as well as a full scan with your installed virus protection to make sure no harmful PUPs are left on your system.

Conclusions and Recommendations

To avoid getting browser viruses, pay attention to the websites you visit, files you download, and apps you install. Avoid using third-party software downloaders and installers - they usually include PUPs. Never ignore the warnings if your browser alerts you that a website is not secure.

Still, it's always better to prevent the problem than to try to deal with it. Browse wisely!

Interesting Internet Finds March 2021

Steve Costello
scostello AT sefcug.com

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members. The following are some items I found interesting during the month of February 2021.

PSA: Gmail Has Your Old Chat Logs From Google Talk (And Hangouts
https://www.howtogeek.com/711404/psa-gmail-has-your-old-chat-logs-from-google-talk-and-hangouts/
Did you use Google Talk and or Hangouts? If so, your logs are still stored in your Google account and taking up space. Check out this post to learn how to access and delete them.

Megapixels Explained – Cyn Mackley
https://cynmackley.com/2021/02/01/megapixels-explained/
Do you wonder what megapixels are? Cyn Mackley provides an informative explanation of megapixels that is not too technical.

How To Set Up Voicemail On Google Voice
https://www.online-tech-tips.com/google-softwaretips/how-to-set-up-voicemail-on-google-voice/
This post explains how to set up voicemail on Google Voice. If you don't have Google Voice yet, it also explains how to get started with Google Voice. (I have been using Google Voice for years.)

Google Meet Adds Green Room To Test Video And Audio Quality
https://www.makeuseof.com/google-meet-video-audio-quality-test/
I belong to a group that has started using Google Meet instead of Zoom for online meetings. When we first started there was a lot of time spent making sure our audio and video were working correctly. Recently, on the day of the February 2021 meeting, I saw this post. Using the information in this post, I checked out my audio and video, making sure everything was working correctly before the meeting.

How Often Should I Reboot My Computer?
https://askleo.com/how-often-should-i-reboot-my-computer/
Leo Notenboom answers this recurring question. As with most of his answers, there are pros and cons discussed. (Note: I leave my desktop on 24/7 unless there is a problem or software update. I turn off and unplug my laptops when they are not in use.)

Are VPNs Illegal?
https://www.addictivetips.com/vpn/are-vpns-illegal/
I know some users are concerned about the legality of VPNs. If you are one of them, check out this post. (I use a VPN whenever I connect to public wi-fi on my phone and other devices. I do this for safety and privacy, not to get around geographical restrictions.)

Google Storage Changes Coming In June
https://davescomputertips.com/google-storage-changes-coming-in-june/
Do you use Google's free storage? If you use Gmail, I am sure you do, whether you know it or not. This post has the information you need to be aware of about changes coming after June 1, 2021. I suggest you read this post and make your decision(s) before then.
****