Scams, Hackings, Cons, Distractions and Blatant Dishonesties (11/13/23)

*This document was written for the first meeting of the season of the PebbleCreek Computer Club – **November 13, 2023,** EN Ballroom, 4:15**.** After this first gathering, the next session is scheduled for **Monday, January 8th, 2024 at 4:15 PM** and every Monday thereafter through March. Always EN Ballroom at 4:15.*

Although this write-up is very similar to previous year's descriptions, many of the details have been updated.

"Trust everybody, but cut the cards". These words of Finley Peter Dunne may be especially applicable to computers these days. As I have frequently said, a little paranoia is good, but don't get carried away. Below are listed some problems, scams and dishonesties that you may encounter working with your PC. Some involve Internet interaction; while others may involve phone calls. *(This handout is similar to last year's with several major modifications to include some new scams I have become aware of, several of which have been attempted on me.)* The more you know about these things, the less likely you are to be entrapped by them. They range from the blatant to the subtle and, perhaps, are best described by example.

Those of you who have been in the Computer Club before know that I create these write-ups or handouts, pretty much from scratch, using primarily my own knowledge and experience. I'm going to make an exception in the first section of this document. There was a complete section in the Wall Street Journal on 9/9/21 entitled "Cybersecutrity". Even though it is over two years old, it contained many articles of interest, but the one most relevant to this topic described why scams often work. I'm going to paraphrase the content of that article below. Keep these ideas in mind when you go through my examples that follow. See if you may be guilty of any of these thoughts.

Our Brain as a Cybersecurity Risk (from The Wall Street Journal 9/7/21**)**

Loss Aversion – People find the pain of loss much greater than the joy of gain of equivalent value. This means that if we are presented something as a potential loss, we are willing to take a risk to try to avoid it. If it is presented as a possible gain, we are OK with taking the safer option. Scammers, therefore, often claim there is a problem with something like a bank account, an Amazon order or an email password. The "solution" involves clicking on a fake website. See Phishing (sic) below.

Authority Bias – Most folks in our generation were trained to trust figures with power or authority. If we get an email purportedly from a bank, government agency or Internet Service Provider, we often don't bother to check the actual source of the email (email address of sender). The sender email may be something strange. That is a dead giveaway.

Urgency Bias – This is an emotional thing. How many times have you interrupted a face-to-face conversation to answer a ringing phone? That's an example of urgency bias. Scammers often pose some kind of deadline that plays on this weakness. A fake email may say something about your credit card will be suspended immediately unless you act quickly. Some will show a (fake) countdown clock

Halo Effect – We have a tendency to respect well-known brand names. Scammers often use an official looking logo in their attempts to dupe us. This could be a bank, credit union or retailer (e.g. Amazon).

Present Bias – This is similar to the Urgency item above, but this one essentially states that we are more concerned about the "now" than we are about the "future".

Availability Bias – We tend to make good judgements on what we've seen before. If something is novel (according to this article), we tend to be more likely to believe it. (Dan's comment: if I can familiarize you with many of the scams that are out there, you will be less likely to be taken in by them).

Illusion of Invulnerability (sometimes called the **Optimism Bias**) – This is the (mistaken) belief that bad things won't happen to me. Scammer manuals (there must be such a thing) probably list a target audience. This could be why phone numbers and emails in a zip code with many seniors, may get more than their share of fraud attempts.

Now let's get on with some of my descriptions of the kinds of thing you might run into.

Phishing (sic) Scams

These typically come to you in an email or possibly as a pop-up window. At first glance, they often look official and very legitimate. They may appear to come from a bank, broker or a reputable retailer – complete with a logo. They typically tell you that your account is messed up (perhaps your assets frozen) and the only way to clear it up is to verify your password, user name, address, etc. Don't! Usually, the more information they ask for, the more crooked it is. This is an attempt to get you to voluntarily provide the secret access information. In another form of this scam, a retailer may tell you you've won a "shopping spree" or a free laptop (from Target, Best Buy, Amazon or Walmart). You didn't! They just want your personal information, so don't fill out any "forms".

Just remember: No reputable institution, such as a bank, will ever notify you of a problem by email. Ignore them! If you want, call the bank and tell them about it. Nothing is likely to come of it, however. If you fall victim to a Phishing scam, you must call the bank and tell them (see **Final Thoughts about Scams** on the last page of this handout).

A variation of this scam is to tell you that due to some problem, your email address is being deactivated unless you supply your password, etc. Don't respond. I have seen these using the Cox, Comcast, CenturyLink and the Hotmail logo.

Also, you may get an email that says you have been charged for something. This may be computer security or a two-year service plan. I've seen this one use the McAfee name, Amazon or Best Buy. This email can be made to look like a "paid" invoice. It then concludes by saying if you don't think you made this charge, you should call a number that is in the email. Remember two pretty hard and fast rules; 1) if you're pretty sure you didn't make the charge, just ignore the email and don't call the number and 2) under NO circumstances should you let anyone you don't know personally EVER, EVER take control of your computer. See Refund Scam on Page 7.

NOTE: Here is a trick that may be helpful. A phishing scam often contains a link to click on (e.g. verify your profile information by clicking here - www.wellsfargo.com/profile). Before you ever click on a link in a suspicious email (or anywhere else for that matter), hover your mouse pointer over the link but don't click. When you are pointing at this link, there will appear in either the lower left-hand corner of your screen or right above the mouse, the actual link that you will be directed to if you were to click. If the link that appears in that little window is exactly the same as the one you're hovering over, there is a chance it is legitimate, however, the link that appears will likely be altogether different. This is evidence of a deception. The actual link might contain a two-character domain code that tells you that it would direct you to a foreign country. Bad news! When in doubt, don't click. If you accidently click, a good virus or malware checker might stop the connection by saying the page you are trying to open is questionable. I wouldn't chance it.

Look for grammatical, punctuation and spelling errors too. This is another indication that the sender is not a native English speaker. Reference further points on this matter at the end of the next paragraph of this write up.

Email Hacking

Web-based email addresses, such as @yahoo.com, @gmail.com, @aol.com, @hotmail.com or even @msn.com are especially vulnerable to hackers. When this type of account is hacked (your password broken), typically the bad guy will send out an email to everyone in your address book…looking like it came from you… that frequently contains a virus in the form of an infected link reference. The email may just say, "I need a favor". That favor usually asks for a gift card to be purchased as a gift for a friend. If the email contains a link, their objective is to get the recipients to open the link in the email and infect that recipient with a Rogue Virus. (See **Rogue Virus** later in this write-up). If this happens to you, likely you will get many phone calls from folks in your address book asking what is going on. Your main recourse is to change your password to the web-based email. Make your password difficult to guess by incorporating a special character in it like a "$", "!" or "%". You might also want to email your contacts and say that it wasn't you who did this. *Four characteristics of a hacker-generated emails are: 1) No subject; 2) email not signed; 3) email contains a link that makes little sense: 4) the body of the email is brief, contains grammatical, spelling or punctuation errors. Exhibiting at least three of these items is a dead giveaway.*

When the hacker got into your email, he/she likely made a couple of changes that you must undo. First, they probably turned on "Auto Forwarding" to automatically forward YOUR incoming email to a similar email address that they, the hacker, created. An example would be, if your email is computerguy@gmail.com, they might create computerguy759@gmail.com to which yours are sent. This means that when people answer the bogus email, their reply doesn't go to you, but rather goes to the newly created email. You may only notice this by the fact that you haven't received any email since the hack. Once you turn off auto forward, you must also make sure that the bad guy didn't create any message rules. If they did, delete them.

Variant of this hack job is to send an email that says you are stranded in …some country… without a passport and you need money… or you have been detained by authorities in …some country… and need bail money. Most of my friends don't travel to the Philippines on the spur of the moment and then contact me for money…ha. It's hard to believe some folks actually fall for this.

Facebook Message Scam (Sometimes called Facebook Lottery)

This is kind of a cross between a phishing and a hacking scam. I personally experienced this one on September 16th, 2018. Here's how it works. You may be asked on Facebook, by someone you know, to be friends. In this scam the friend request often comes from someone who is already marked as a friend. That's an indication something is wrong. In any event, you will get a text message through Facebook, appearing to come from one of your friends, that says, "How are you doing?" Your typical response would be "Doing great, how about you?" The next message will come back saying that they have some fantastic news to share with you. Naturally, you will ask what it is. The paragraph below is an exact response (including errors) that I received after the how-are-you-doing exchange:

> "have you heard about the good news from Facebook about the Ceo of facebook Mark zuckerberg to help Cancer,Glaucoma,Pacemaker and diabetes ,Deaf,Retired,Disable and some facebook users in conjunction with the federal government Grant and PCH?"

I have often warned folks about written exchanges that have grammatical, punctuation or spelling errors. There are all kinds of red flags in the above. First word not capitalized. Facebook capitalized once and then not. Proper name Zuckerberg not capitalized. CEO written as Ceo. Words like Pacemaker, Deaf and Disable (which probably should be disabled) and Grant were capitalized that shouldn't be. Notice, too, the improper use and spacing of commas. In addition, it's a little strange to think the federal government is working in conjunction with Publisher's Clearing House (PCH). And to top it off, the whole sentence is awkwardly written. It is quite unlikely that someone who is paying attention would make this many errors accidently. Probably not a native English speaker.

Anyway, I played along and the next message said they received $800,000 and happened to notice my name on the unclaimed money list. I was told to text 1-256-405-4751 to initiate my claim on some big money. Since I was sure it was a scam, I texted back a question that only my friend knew the answer to - saying, if this is really you, please answer my question. The response I got also contained errors. It was:

> "Are you kidding me? You need to trust me its is real me and legitimate. You don't need to nervous about this."

Improper use of "its" and no "ly" on the end of the word real. Missing the word "be" in front of nervous.

I'm not sure what would happen if I texted that number, but it would likely try to ensnare me in some scam where I would be asked to put up some token front money to receive my "prize". I didn't want to find out.

At this point, I quit texting and called my friend on the phone. He confirmed it was not him. I suggested he change his Facebook password.

If you search the Internet through Google for "Facebook message scam", you will get a multitude of hits explaining variants of the scam described above.

Bottom Line: Facebook can be a dangerous place as it is full of personal data. Beware of a friend request from someone who is already marked as a friend. If you are a member, don't post too much really personal information. Be very careful about exchanging information with someone or some website where the communication seems out-of-character with the situation. Ask yourself if the information seems unusual or is too good to be true. By the way, Facebook claims they are working on this.

Facebook Help Scam

Facebook is a free website. There are sections in the Facebook website that offer suggestions on how to fix problems you might encounter. However, THERE IS NO FACEBOOK CUSTOMER SUPPORT PHONE NUMBER where you can talk to a real person. Notwithstanding, if you type Facebook Customer Support into Google, you get many hits. Your Internet search may even yield a phone number, one of which is 650-543-4800. This is a California number that is NOT Facebook. If you call it, the person may answer the phone "Facebook Support", but they are a third party. Don't believe what they tell you and don't give them control of your machine. And whatever you do, don't pay them. See following paragraph.

I called one of these numbers last year just to see what would happen. When I explained a Facebook problem, they quickly told me I had been hacked and asked me how close I was to a Walmart or Target Store. They then proceeded to tell me my network wasn't secure (he said the hacker was someone in Nigeria - amazing how many smart people are in Nigeria) and that I needed to go to Walmart and buy a $50 iTunes card or Apple Gift Card. Now I was really confused. When asked why, they said I would read them the iTunes card number to show good faith (of which I had very little at this point). They said Facebook is free so the $50 they took would be refunded back to me immediately (This is clearly a test of gullibility). The guy was actually willing to stay on the phone with me while I went to Walmart. When I told him I lived in a rural area and Walmart was 50 miles away, he gave me his name and a (New York) call-back number and said to call him when I got the iTunes card. I hung up and never called back. I looked up this scam online and found a video that explained exactly what they were trying to do.

Scary Pop-ups (Very Common)

Another ploy by the bad guys is to generate a pop-up screen, which looks official, that says there have been viruses detected on your machine and you should call the free 800 number for help. It may even be accompanied by an audio warning (played loud) that says, "Your machine is infected. Do not turn it off. Call the number shown. Your credit card numbers and bank accounts have been compromised." The warning may even state that in an effort to save your machine, Windows will be disabled (It won’t be). You may be tempted to call it since you could experience difficulty in getting rid of the pop-up. Don't call the number. This is just a variant of the cold call approach described below. Here is how to get rid of that message. Press the **Ctrl-Shift-Esc** keys at the same time - i.e. hold down Ctrl and Shift with one hand and tap the Esc Key with the other hand. This will bring up a window labeled "Task Manager". (Another way to get to the Task Manager is to right click the mouse on a blank area of the task bar (revealing a menu) and left clicking on the words Task Manager) Make sure the "Processes" tab at the top is chosen. Under the Apps heading find the list that describes the error message pop-up, highlight it and then click on "End Task". The window should go away. The reference line may refer to your browser, such as Internet Explorer, Chrome or Edge. This is because the pop-up you are seeing is coming through the browser. If this doesn't work, go ahead and manually turn off your computer by pushing and holding the power button. When you reboot the message should be gone. In spite of the warning**, there is NO danger in shutting off your machine**.

One variant of the scary pop up is to display a close replica of the "famous" Blue Screen of Death (BSOD). It is the same color as the real BSOD, but it gives a phone number to call. It may also even "speak" to you saying that virus activity has been detected and for your own protection, you should call a certain toll-free number. Don't call it and if you do, be sure you don't give them control of your machine. Also, the dead giveaway is when they ask for money.

By the way, the real BSOD doesn't give a phone number but rather tells you a couple of things to try including removing recently installed hardware. If you get the real BSOD, turn off the machine with the on/off button (hold it in for 5 to 7 seconds and your machine will shut down) and reboot.

Just to be sure that nothing has infected your machine, after you see one of these pop-ups, you should run Malwarebytes AntiMalware. If there was some residual from the pop-up, this program will find it. Anything found by Malwarebytes should be eliminated or quarantined.

There is another of these scams that recently came to my attention. A person was trying to pay AZ real estate taxes online. During the course of this transaction, there was a popup that said there was a problem and to call a certain 800 number. The pop-up was actually a scam but appeared at such a time that it looked, as always, fairly legitimate. The person called the number and was told they have had a virus on their machine for over 600 days (now that’s a streach!) that was preventing them from doing what they wanted. The person on the phone said for $200 they would fix it. RED FLAG! It was a scam and they hung up as they should have. An inevitable ploy of these people on the phone is to scare you with a threat of credit cards or bank accounts being compromised

IMPORTANT NOTE: If you happen to call the number and give them control of your computer, this note is relevant. You're usually talking to them on the phone and they have control of your computer. When they ask for large amounts of money, you may realize that it's a scam and hang up. The problem is, after you hang up, they still have control of your computer and may vandalize it because you didn't pay. This may be in the form of adding a password that only they know. A return call might be made to you trying to hold you hostage until you pay them. Remember, these are really bad people. So, before you hang up, shut off your computer to sever their access. In many instances, such a password can be broken but it's a major hassle. Installing software as described in this paragraph is sometimes called "ransomware".

One more thing (I sound like Lt. Columbo), if you voluntarily pay them with a credit card and then realize that you shouldn't have, call the credit card company immediately. Tell them you want to dispute a charge and most credit card companies will see that it is a payment headed for another country and block it. Some card companies will actually call you when the charge is initialized because they know it's questionable. If the scammer installs software, even if it is useless, and gives you a bill of sale, that can make it very difficult to get your charge reversed.

Scammers know that many credit cards are "looking out" for their cardholders. As a result, some ask for payment in the form of prepaid cards such as iTunes or Apple Pay cards or by money order. If you do this, it is impossible to stop payment after the transaction is complete and the victim has no credit card corporation to back them up. So, if you are talking to someone and actually believe they are helping you (not likely) you can realize immediately that it is crooked if they ask you to go to Walmart and buy an iTunes card and then read them the number. Put them off somehow by saying you have to check with your IT department and then hang up. Never pay!

One thing to always keep in mind is that ***It is never a good idea to let anyone, whom you don't know personally, have access to your computer***. I can't say that enough. Just realize that scammers are everywhere.

Rogue Virus

This is a program that likely comes to your machine by visiting an infected website. The typical Rouge calls itself something that looks real such as “Security Shield 2023” or “AntiVirus Security Pro”. These are misleading names because the programs are frauds. What they do is pretend to scan your computer and tell you how badly you are infected…and for only $149.95 or more… they will fix you. No real virus checker will EVER install itself and then scan without being asked. What this amounts to is pure and simple extortion. This type of infection has been called ‘scareware’ because their idea is to frighten you into thinking that you need to buy their (worthless) software. If you buy it, symptoms will go away for a while. But you have paid a blackmailer. Who knows where it will end? Some of these programs may even describe themselves as "Microsoft Partners"... wrong! Don't be fooled. There is one category of Rogue that locks your screen and says the FBI needs you to pay a fine. Variants of the FBI virus are the "Department of Justice" virus, the "Homeland Security" virus and the "ICE" virus. These have been around for years.

There are several courses of action that can deal with this type of virus – the two most effective are: 1) doing a System Restore to a point before you had the virus or 2) by running an updated version of Malwarebytes Anti Malware. Some of these viruses are so clever that they will disable your ability to update and/or run Malwarebytes. This is where you may have to boot into Safe Mode (tap the F8 key during boot in Win7) and then install or run Malwarebytes. In some extreme cases, it may require you go into DOS to fix it. The F8 trick does not work in Windows 10 or 11. With Win 10 and 11, if your machine is on, hold down the Shift Key and then hit restart. It will give you an option to go into safe mode.

I've even seen a variation of this category of virus where they put some very nasty porn on your screen that you can't get rid of. The idea there is that it will embarrass you to the point where it is easier to pay the fee than it is to explain to some potential helper that you weren't really viewing the obnoxious websites.

There is another one where you get a message on your screen that your version of Windows has (or will soon) expire. This has to be removed and in most cases can be done so by running Malwarebytes AntiMalware. This license-is-expiring scam can also be in the form of a recorded call - see below.

The Internet is a virtual limitless source of information about virus removal. Do a Google Search of the Rogue name and add the word “removal” to it. The result will likely suggest a good method to get out of your dilemma.

If you are really frustrated and want telephone help, you also need to be very careful. Telephone numbers that you get from an Internet search may be to some less-than-legitimate outfit. You may get through to a person, they will be polite and full of "promises" and then they will ask for a high fee. Don't pay it. You are way better off calling a knowledgeable friend. (See "Calling Microsoft" section below)

Phone Calls with No One There

A very common situation these days is where you get a phone call - either on a land line or a cell phone - and when you answer no one is there. Research has revealed that this is a way to verify that the number indeed reaches a live human. It is robo-dialed. A computer just dials every number combination. Those that are answered are live numbers and can be sold (to scammers) so they don't waste their time with dead of unassigned numbers. The best strategy for you is to not answer numbers or area codes that you don't recognize. If it's important, they will leave a voice mail. In addition, you can usually predict that any call coming from some 8xx area code is likely a scam. You should certainly not answer those.

Cold Calls (claiming to be from Windows)

Some scams start with a cold phone call. The caller will say something like, "I am from Windows (they are usually careful not to say they are from Microsoft. However, lately they have gotten more aggressive and will actually TELL YOU they ARE from Microsoft.) and they have monitored some suspicious activity on your computer". They don't really know that you have a computer. They are just guessing. They figure by the zip code or phone exchange that you likely have a computer. They will act helpful and want to connect to your computer and take control of it to diagnose the problem. At this point, your only problem is that they are on the phone. Please don't give them control of your machine, don't believe anything they say (including the guy's name - too many of them are named Bob) and for goodness sake don't pay them anything!! They may offer a five-year support contract for $299 or more. Scam! If you happened to agree to payment, call your credit card immediately and refute the charge.

I even encountered one instance where the bad guys were so greedy, they wanted $2000 for the contract. They were also extremely blatant in that they wanted access to the "mark's" bank account to do a direct debit. Wow! There are several red flags here that it should scream fraud. If one happened to fall victim to this, the process of undoing it can be severe. It would mean cancelling your bank account and often putting yourself at the mercy of the bank. I have to say it one more time: **Don't ever let an unknown person have access to your computer - regardless of who they SAY they are - not EVER!**

The caller may say they are "A Microsoft Partner" and they want to improve your computer's performance. The bottom line is they always want to take control, they always run some bogus software showing you how bad off you are (you're not!) and they ALWAYS want money. Hanging up on them is the best approach, but if you must talk to them, ask them point blank, "Are you with Microsoft?" They usually don't say yes, because they are not. Then ask what company they are with and where is that company located. It might be "iyogi", based in Gurgaon, India. They employ many scare techniques to get you to pay… Avoid this.

No reputable company will ever call you at home. They may even give you an 800 number and ask that you call them back. Easiest thing is to hang up and don't call them back. Don’t fall for it. String them along to have some fun, but don’t ever, ever pay them or allow access to your computer. Sometimes I play SO dumb that I can't follow their instructions. They may ask me to hit the Windows Key. I tell them I have old-fashioned windows that don't have locks on them. My door has a lock, but now my windows, so no key is necessary.

If you happened to give them control of your machine, turn your machine off and back on. Connection with them will be lost and you should be OK. If you did give them control, I would run a scan with a program like Malwarebytes AntiMalware to make sure nothing was "planted" on your machine.

I, personally, have received several of these calls. Sometimes, instead of hanging up, here are other ways to put them on the defensive (Just for fun - yes, I have a weird definition of fun). When they tell me my computer is infected I asked them how they knew my phone number. They have no answer since these calls are placed at random. Sometimes I ask them to tell me which of my several machines is infected by giving me the IP (Internet Protocol) address of the infected machine. They can't do this either. I have actually succeeded in getting these people to hang up on me. I regard that as a victory. When I recognize a scam number on caller ID, I sometimes answer and pretend I don't speak English.

Cold Call (or email) Refund Scam

This is one I first encountered in September 2018, but it is still around today. It seems there is no bound to the creativity and ingenuity of these folks who are after your money. In this approach, a live caller (with a heavy accent, of course) tells you they are with Windows and Mac (now that's versatility) and they are calling you about the $300 refund to which you are entitled. You answer something like, "Oh really?' They go on to say that you paid $300 for your Windows license and you were overcharged. They are calling to get the refund to you. I've been called with this one several times, but I never go far enough to see what happens. I would imagine that they want a credit card number, to which they will apply the credit. That pretty obviously a bad thing, so don't fall for it. Tell them to mail you a check.

In addition to the credit card method, above, here is another way the refund scammer will try to trap you. Let's say they are offering a refund of $300. It can be for any bogus reason. After you give them control (don't), they will ask you to sign into your bank account so they can issue the refund. While in the account, a window will pop up and the bad guy will ask you to enter the figure ($300). When you type it, they will type in a third zero (claiming that you accidently did it) to make the refund $3,000. They will then tell you that the figure cannot be undone and they issued the $3,000 refund. That will show as pending in your bank account. They will then tell you that YOU OWE THEM $2,700 (3,000 minus the original 300) and you should wire them that amount. At this point you should say thanks for the money and hang up. If you were to wire the money you would be out the $2,700, and of course the pending refund would fall off your account without taking place.

The calls I have received showed a caller ID of Spartanburg, S.C. Obviously, you can choose not to answer and call from an unknown location. (Sometimes the caller ID actually shows "unknown"). I have tried several approaches to put them on the defensive (some mentioned above). I asked them where they are calling from. One caller said, Las Vegas. I asked what the weather was like. That person told me to have a nice day and hung up.

I told another caller that I never paid $300 for my license. They insisted that I did and wanted to proceed with the refund. I insisted that I didn't pay because I stole the machine that I was using. That got them to hang up.

A variation of this scam that I have been told about is using the Cox name. In this situation, the caller says that they know that your service (provided by them) hasn't been up to par and they would like to give you a "good will" credit. Regardless of who the callers says they are, the procedure they use is always similar. Be on guard.

Yet Another Cold Call Scam

Recently, I received another cold call with the caller ID reading Jamaica. I instantly thought "scam", but I answered to see if this was a new approach that I should know about. The person (again, with heavy accent) said they were from the "Unclaimed Funds" Department and there was something in my name for me to claim. When I asked what it was, they said it was "5.5 Million Dollars and a brand-new car". Wow, they weren't kidding around. When they wanted a deposit from me to assure good faith, I hung up. You could also tell them that you just bought a new car and you really didn't need the money – they should give it to someone else.

Calls with a Recording

Still another cold-call approach is to phone you and when you answer there is a recorded voice that says something about Microsoft has been notified that your version of Windows is about to expire (or has expired) and you should call a number to get it fixed - for a price, of course. You can safely ignore this call as Windows doesn't ever expire. This is even true if you upgraded from Win7 or Win8 to Win10. Just for fun, I once called the number given and they had me go to the "Services" area in my computer. This is a place where most folks never visit. They showed a few things that were totally normal and correct and said, "See, that's evidence that your version is about to expire". My response to them can't be written here, but you certainly can ignore the recording.

> A variation to your-Windows-has-expired scam is where the caller has you open the command prompt by hitting the Windows Key and the R and then type "cmd". Then they will ask you to type "assoc" and hit enter. This command lists the application and class associations of system files. The one that the scammers always focus in on is the association for .ZFS files—a long class identifier (CLSID) string. CLSID stands for Class ID and makes reference to the computer's registry, which is way too detailed to discuss here. The point is, the long number that follows is the SAME ON EVERY COMPUTER. The scammer will TELL you it stands for Consumer License Support ID and he will recite it to you like it is a unique number.

Then he will say something like, "since I know that number you should trust me". Total BS. If you stayed on the phone with the crook for this long, tell him you have a different number. When he wants to connect to you and illustrate your dastardly fate, tell him you'll take your chances with an expired license. Remember - A Windows License never expires.

A good description of the above scam is found at https://arstechnica.com/information-technology/2017/01/take-your-sweet-time-how-i-scammed-a-tech-support-scammer-for-nearly-two-hours/

There are two other recording scams that I have experienced - one says they are from the IRS and you owe; the other says they are the Social Security Criminal Division and your Social Security will be cut off. In the IRS scam they indicate that a lawsuit will be filed against you if you don't call the number back. The Social Security scam also asks you to return a call to a certain number. Ignore both of these. It may be made to look more real because your caller ID might even display a Washington DC area code. Neither the IRS nor Social Security ever call or email. They always use the US Mail. I once called the indicated number and they said an agent was being sent to arrest me. I replied that I'd leave the light on for them.

Another older variation is a call from "Rachel", from card-holder services, who says there is no problem with your credit card, and due to your good payment history, the company calling wants to offer you a lower or zero interest rate on your credit card balance. This is just a come-on. First of all, if you press "one" to talk to a representative (I've done it just to see) you could be 45th in the queue. Secondly, when you do get a real person on the phone they ask you your credit card number. I usually respond by saying, "You called me. You should know my number." They immediately get angry. Don't connect to them. By the way, if they say, "Hit 'three' to be put on the do not call list", don't do it. That just verifies that you are a live prospect, so they will likely keep calling.

I've also found that if you call one of these numbers back and you block your caller ID, so the person on the other end doesn't see YOUR number, they won't answer. On an iPhone you do this by dialing *67 before dialing the number. It's probably easier not to call back.

Distractions

This greatly resembles the “bait and switch” approach used by retail stores. In this scenario, you may go to a very good website such as www.filehippo.com to download a free program. Sometimes getting that program to start downloading takes as many as three or four clicks on the correct buttons. You may be looking to download CCleaner for example, which has a very good free version. During the series of clicks, you may be offered a pay version in such a way that it makes you think the free one is worthless. It might say “no support” next to the free one. Well, that’s OK. Also there may be larger download buttons to click on that seem right. In the end you will get a window that opens to Run or Save the file. Make sure the program name in that window is, in fact, the program you were targeting. Example: CCleaner's program is named "ccsetup586.exe" which seems right…"cc" for CCleaner, "setup" for the action and "586" for the version number. If the program is something like "downloadhelper.exe", you likely clicked on the wrong button. Also, if you look closely near the "clickable" button, many times the wrong one will have the word "advertisement" next to it. These can lead to trouble if chosen.

Beware of buttons that say “Free Download” and “Free Scan”. These both may be true, but once downloaded or scanned, no correction is done to your computer without paying. When in doubt, Google the software you are looking for. There are many websites that review these items. There is an awful lot of very effective free software available. This is why I, personally, shy away from pay virus checkers such as Norton, McAfee or Kaspersky.

Also be careful as you are installing a new program. Often there are several screens or windows that require you to click on "next" or "continue". Take your time and make sure you are not agreeing to let them install an unwanted program and change something like your home page or your search provider.

Calling Cox, Comcast or Century Link (or any Internet Provider)

Cox and Century Link (Comcast in other cities) employees often earn an A+ for patience and politeness. Maybe one call in ten that is made to them is actually warranted. The other nine involve situations that could have been resolved without them. Since they are only concerned about their service, they are not sympathetic to folks who have installed their own routers, solar panel monitors or Magic Jack Boxes. When they find out you have any of these devices, they will want to talk you through removing them to verify that their service is OK. There will be a future handout entitled If you Cannot Connect to the Internet. Depending on their level of frustration the person on the phone may try to set up an appointment for a technician to come to your house or they may suggest you call

Microsoft. Many issues are resolved by rebooting the modem and the router (in that order). Reboot means power down and then power up. If you do schedule a technician visit, be aware that this will be something you have to pay for it if it winds up being NOT their fault - which is common.

Calling Microsoft (or HP or Dell, etc.)

Microsoft actually does have telephone support (honest), but be careful. Their real phone number is 800-642-7676. First, calling Microsoft should be an absolute last resort. Secondly, some phone numbers you get off the internet may say Microsoft Support – but they are not REALLY Microsoft. The same is true of other companies. This is like Jake's Auto Shop saying "Chevrolet Repair" where he does everything to make you think he is a Chevrolet Dealer – when, in fact, he is an independent, or worse, a crook. Microsoft Support could be of this ilk. Here is how you can tell. You place a call; they listen to your problem; they might even use a remote connection (with your permission) to take control of your computer to diagnose the problem (sounds good so far) and then… they say they can see the problem and they would be glad to fix it for some exorbitant fee. They will say something like for $395 (or more) we'll guarantee to fix your problem and give you two years worth of support. Run the other way! That's WAY too much money and be warry of the "guarantee" of fixing it. If you pay and they don't fix it, guess what? No refund. You could actually buy a new computer for what they want to charge. These folks may work out of a boiler room (background noise can be heard) and are scammers. A variant of this is the cold call scam described earlier.

Texting Scams

This one plays on your urgency bias. You see a text and, right away, think, "This must be important". A bogus text may contain a website link and explains that you need to go to that link to reactivate a credit card or correct a charge that the text claims you made. It could reference the delivery of a package that you didn't order. Instead of taping on the link provided, go to your bank website, credit card site or Amazon, in your usual manner, to see if the referenced charge appears. Chances are it isn't there, meaning you can ignore the text.

Clickbait

Although not technically a scam, this certainly falls under the category of distractions. As you search the Internet, especially if you are on a news page or financial page, it seems there will be an endless supply of "come-ons" that are meant to peak your curiosity. The heading of this area can say "Around the Web". These will be in the form of pictures with captions like "The 10 Most Dangerous US Cities", "What Celebrities from the 80s look like now", "You Won't Believe This Weight Loss Secret" or "Most Men will fail this Quiz". When clicked on, these will take you into a slideshow that often displays what was advertised. Occasionally they will take you on a lengthy set of pages that will eventually get you to an unsatisfying conclusion. The purpose of these "clickbait" sights is to plant tracking cookies (to be explained in a later write-up) that report your Internet habits to a third party. Suffice to say most are undesirable.

I did an experiment where I ran a cookie-clearing program to make sure I had no tracking cookies. Then I went to a clickbait site and only looked at a few slides. I then ran the cookie-detecting program again and it found over 1000 tracking cookies. This happened in a matter of minutes by visiting one of these sites. This essentially told me two things: 1) Avoid these clickbait sites and; 2) it is necessary to have a cookie-cleaning program that is run quite often.

There is an area in all Internet Browsers (Edge, Chrome, Firefox, etc.) where you can activate or deactivate "Extensions" or "Add-ons". These, too, will be discussed in detail in a later write-up. In general, add-ons can slow down browsing so having few or no add-ons was my usual recommendation. With the exploration of clickbait, however, I have found one browser extension that is worth having. It is called "Malwarebytes Browser Guard". Having this installed and activated on whichever browser you are using will minimize the displaying of clickbait ads. This extension is free and can be activated when you install Malwarebytes Antimalware (a very desirable program to help keep you clean) or can be installed by typing "Malwarebytes Browser Guard" into Google and following the instructions.

Why Do People Do This?

The answer is always **money**. Every one of these cons is designed, somehow, to get money out of someone, somewhere. If they can get you to buy a worthless product, or subscribe to a less-than-stellar service, they have succeeded. Most people doing this are off shore and may speak with a heavy accent. Many credit card companies are aware of these scams and will sometimes call you if you try to pay for one. They will say something to you like, “There has just been a charge authorized on your card to Kazakhstan” and ask you if you really want to go through with it. It’s best if you don’t authorize it, but this is a chance to stop it.

Even legitimate companies selling products like Norton, McAfee, and Spyware Doctor delight in giving you the convenience of automatic renewal of your subscription on your credit card. I personally don’t think this is a very good idea. Rather, let the computer remind you that your subscription is about to expire so you can proactively pay for it – if you want to. Many who agree to automatic renewal, forget about it and then realize that your card has been debited too late to get your money back.

Final Thoughts about Scams

If your email has been hacked, it is not likely that anyone is after your bank account. If you get a virus and cure it, you are not likely to fall victim to identity theft. However, if you pay a scammer, either a cold-call person, by calling a number in a phishing scam or succumb to virus scareware, you need to contact your credit card company as soon as you can. Although the perpetrators are likely content with the money you voluntarily gave them, there is a distinct possibility that the credit card number you provided can end up in the wrong hands (it is actually already in the wrong hands) and sometime in the future other charges may appear. If you pay the crook with a gift card, that is a non-reversible transaction, so the money is likely lost. Danger also may lurk if you provide private information to an unknown person about your banking information (Phishing).

Some people are reluctant about conducting any financial transactions (making a purchase or paying a bill) online because of fear of their credit card number or bank account number being compromised. Generally, this is not a problem unless it's a scam. Look at the address line in your Internet browser (Also called the Uniform Resource Locator (URL) line) you will see it begins with the letters "http" - standing for Hyper Text Transfer Protocol. When you are on a page displaying your bank balance or showing a field that is waiting for a credit card number to be entered for a purchase, there will be an additional letter following the http. It will be "https" where the "s" indicates a secure website. Visit www.amazon.com and you will notice no "s" until you get to the screen where you are going to enter your card number to make a purchase… then the "s" will be there. Go to the website for Wells Fargo Bank or Charles Schwab and there will always be an "s" there. Remember this last paragraph refers only to transactions that you are doing on purpose.

In my opinion (IMO) you should feel pretty confident that the information you provide to an "s" website will be safe. You are probably in more danger by letting your physical credit card be taken out of your sight when you are paying for a dinner in a restaurant. The card could be easily copied at that time.

I've also heard people say that you should cover your computer's camera. IMO this is a little extreme. It is very unlikely that you will be spied on in this manner. Think about it - why would a stranger do this. Also, a light, near the lens, will glow when the camera is on. If your camera has the light on for no reason, it could be worth looking into why. Putting duct tape over the camera is a little too paranoid.

Dan Phelka 623-535-7791

Don't get trapped by a phone call!!

Disclaimer

I've done my best to describe and outline as many scams as I have seen, experienced, read about or been told about. New ones are surfacing every day. This write-up is, therefore, by no means all-inclusive. I hope that it alerts you to the type of cons that are out there - many of which you will encounter. A little caution if always wise. Beware of things too good to be true or charges that are exorbitant. If you could buy a new computer for what the bad guy wants to charge you, it's almost guaranteed to be a fake. When in doubt, do a search of the Internet using Google or DuckDuckGo. The advantage of DuckDuckGo is that they will not track you the way Google does.

Addendum to Scams Write-up (11/13/23)

I'll start this addendum with a phrase I used several times in the other write-ups (I can't say it enough):

"**Don't ever let an unknown person have access to your computer - regardless of who they SAY they are - not EVER!**"

Now that I've got that out of the way, let me share two recent experiences that other PC residents have lived through because they didn't follow the above advice. By the way, these people felt very bad after it happened but that didn't mitigate their misery.

Supremo

One person was seeking help in getting a printer installed. They did an Internet search and one top result gave a number to call that presented itself as HP Support – it wasn't. Searching the Internet always brings back a list of "hits" on the words you used in the search. The search provider however takes payment to present "ads" above more relevant results. This person called the number and got a "seemingly" very knowledgeable and polite person. The first thing the phone person did was asked to control the victim's computer. To shorten the long story, after the bad guy got control, he proceeded to explain that things were wrong (they weren't) that prevented the printer from installing. He wanted payment to clear up the "fake" problems. Realizing this was a possible scam, the victim hung up the phone but didn't immediately turn off the computer. Still connected, the scammer loaded a software program called "**Supremo**". This is a program that executes at startup and allows access to the computer by a remote person without further permission. This is very dangerous and can be spotted by an entry in the System Tray – on the right side of the taskbar just to the left of the time and date. The Supremo.exe has to be deleted using Window Settings under Apps and Features or in the old Control Panel under Programs and Features.

Supremo is a legitimate program that can be very useful, but unfortunately can be abused by scammers. It is very helpful if you are in one location but have a computer at another location that you need to access. If, however, it is secretly loaded on your PC, some unknown person can access that machine. They can wreak much havoc by gleaning information that you have stored in your browser or elsewhere, like passwords and credit card information.

Other programs that provide this function are "**Any Desk**" and some settings in "**Team Viewer**". If the scammer had you use any of these programs, I would uninstall them as soon as possible. Go to the Control Panel, display it in small icons view, click on Programs and Features and then sort this list by Date Installed by clicking on the column heading. It one of these programs was installed recently, that's all the more reason to remove it.

If you legitimately use Any Desk or Team Viewer, make sure that the settings are such that only you, with knowledge of a password, can access the machine. Just be suspicious if you don't use either and they were installed recently.

Lock My PC

This is another legitimate program that has been abused by scammers. When used properly, it allows the computer owner to add a level of security above what Microsoft provides.

However, this can be installed on your computer remotely, if you give control to a criminal and then hang up the phone but don't disconnect from the Internet. The next time you boot the request for a password will come up before the Microsoft PIN or password request. The crook has your computer locked and they often call back a want a ransom payment. Instead of paying the ransom, there are two approaches to this. Seach Google for "Lock My PC" and follow the instructions (you will need a second computer that is not locked)