Scams, Hackings, Distractions and Downright Dishonesties (11/13/17)

Welcome back and thanks for attending the first meeting of the season of the PebbleCreek Computer Club. After today the next meeting will be ***Monday, January 8th, 2018 at 4:15 PM*** *and every Monday thereafter for about 15 weeks. Hope you decide to continue attending.*

"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. *(This handout is similar to last year's with several 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. Here goes:

Phishing (sic) Scams

These typically come to you in an email or possibly as a pop-up window. At first glance they often look and sound official. 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. Under this scam, a retailer may tell you you've won a "shopping spree" or a free laptop (from Target, Best Buy or Wal Mart). You didn't! They want your email address and other relevant information.

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.

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 the lower left hand corner of your screen, the actual link that will be activated 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 checker might stop the connection. Don't chance it.

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. 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 a lot of 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 ! or %. You might also want to email your contacts and say that it wasn't you who did this. Characteristics of these hacker-generated emails are: No subject, email not signed, email contains a link that makes little sense and the body of the email is sketchy, at best. Exhibiting at least three of these items is a dead giveaway.

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.

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 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." 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". Click on the Applications Tab (Windows 7) at the top. Then find a reference in 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 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 with 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 my Malwarebytes should be eliminated.

There is another of these scams that recently came to my attention. A person was trying to pay 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 for over 600 days 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

NOTE: If you happen to call the number and give them control of your computer this note is relevant. You're talking to them on the phone and they have control of your computer. When they ask for lots 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 bad guys. So before you hang up, shut off your computer to sever their access. By the way, such a password can be broken but it's a major hassle.

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.

It is never a good idea to let anyone, whom you don't know, have access to your computer. 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 legitimate such as “Security Shield 2017” 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.

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. With Win 10, if your machine is on, hold down the shift 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 or 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)

Cold Calls

Some scams start with a cold phone call. The caller with say something like, "I am from Windows (they are usually careful not to say they are from Microsoft) and we 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. Scam!!! If you happened to agree to payment, call you credit card immediately and refute the charge.

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 can'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 a lot of 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. 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, I 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.

Call 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 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.

Also another recording says they are from the IRS and you owe. A lawsuit will be filed against you if you don't call the number back. Ignore this one too. It may be made to look more real because you caller ID might even display a Washington DC area code. The IRS never calls or emails. They always use the US Mail.

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 "ccsetup536.exe" which seems right…"cc" for CCleaner, "setup" for the action and "536" 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 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 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 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 of all 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 (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 we’ll guarantee to fix your problem and give you two years worth of support. Run the other way! First of all, that's WAY too much money and secondly, you pay with 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 and are scammers. A variant of this is the cold call scam described earlier.

Why do People Do This?

The answer is almost always **money.** Every one of these scams is designed, some how, 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. 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. First 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 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. 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 red light 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 535-7791

One Last Item - In September of 2017 a very popular cleanup program called CCleaner was infected with a real Malware Trojan. This meant that if you installed this, it planted some bad software in your machine. Since this is a program I have believed in for a long time, I looked into it in detail. It was only in version 5.33 of CCleaner. After that it was fixed by the source of the program. Current version (at this writing) is higher than this, e.g. 5.36. If you skipped 5.33 there was no problem. For example, if you had version 5.29 installed and you upgraded to 5.36 you skipped the bad one. If you did install version 5.33 or if you are not sure, you must run an up-to-date version of Malwarebytes AntiMalware. That program will identify the Trojan and remove it. I had it on my machine and MWB fixed it.