# Audio file

[Your Recording 1.wav](https://1drv.ms/u/s!AOIiJgTgFDd_hxo)

# Transcript

She can really say June 1, 2023, comments, suggestions, questions welcome anytime. Audio recording of this session and then before file be available later today when you get the PDF on this computer club site, you can click on that link and have an MP4 file that you can either view or download and adjust volume, rewind, pause, have a good time. So audio recording is in progress. It's a warning to you if you want to say something not preserved posterity. Let me know. Sighting is required. We, members of the charter club sponsor net CIG, some City Community Association by law. So I'm still making an offer to anyone that would like to be a presenter, like if you've discovered. Something in the cyber security realm that you think would be of interest to the membership. We can do that. We can do that if you've gotten the e-mail from the computer club. The I device is SIG is going to be renamed into the Apple Users Group, CIG, so that will cover. The thing is that. What's covered by I devices before, and you know the iPhone, iPad, TV, Apple TV, those kind of things. You can actually join the apples users group sick now on the web app. Yeah, computer club website. And the first meeting will be held. In the atrium in September 8th. Until then, I devised this topics will be covered in the Mac users group the mug, so they're getting to be more blended. Yeah, getting to look more like. So we can do some things in the back users group. That are device related, but anything security, cyber security related, we'll try to cover, we'll cover here in the cybersecurity, say some recent presentation postings. The NRO did a town hall in the ballroom recently. By 12, that has been recorded. The slides are synced up, and that presentation you can view downline load, rewind, adjust volume, just size, pause, review all those kind of things by clicking on the green link and again. Maybe 4 file that you can either view or download the computer club also recently held yet another inquiring minds presentation May 16 and if you click on the green link here you will actually be able to downline load that one. Which was about. Technology in the healthcare sector. There are a lot of other really good computer and cyber related. Resources in Sun City, the self-defense Club has a self and home security SIG and they have given several presentations and most of those are posted on their SIG website. They're club site, cybersecurity and old older Americans telephone scams. Warnings from the FCC the current issues club has done several presentations that are again recorded. They do something called background sheets where they do intensive research before the meeting and then have general discussion at the current issues meeting once a month. Some things that they covered in the past that. Like big, relevant consequences of disinformation, misinformation, and they topic, called cybersecurity, the Investment Education Club. Again, cyber is getting cybersecurity is getting really ingrained in just about everything you do. Some of the examples for the investment. Education clubs are cryptocurrency and blockchain, and then the computer club. Obviously if you go to the education tab on the computer club, you can see some past presentations that were recorded and you can view those and several of the CIGS recorded and or offered their presentations. As files that you can download some of those things are really, really, really interesting. Internet of Things. Sig is something that I think is a hidden treasure that is not utilized enough and they do a lot of information, you know, a demonstration of 3D printing. And, you know, got traveling with electronics. Very interesting and. And for one, we do. Remind me and maybe others about what GPT stands for. It's it's fancied about and hardly ever expand on what GPT is an acronym for and it is generative pre trained transformer. So ChatGPT has taken the Internet with all the questions and answers and made that. Into training into a transformer so that something they call it artificial intelligence is really a regurgitation of human intelligence captured and played back. Depending on what users ask. And it was a. There's been a lot of fear mongering about artificial intelligence. Is it gonna make humankind extinct? And you know it it's, you know, complete gambit. But it's it's this. Let's let's do some positive thinking. GBT and Autism is a really interesting. Effort put forth autistic children are and adults as well are more apt to bear their souls and get over their hurdles with autism by using something artificial intelligence that speaks more like them also. Recently, May 21st, 2023, age 60 minutes episode was really interesting. They talked about cybersecurity and targeting seniors A10. Vegan dollar loss in last year, according to the FBI report. Take that to mean that most people that get scammed with cyber crimes do not report, so this is just the reporting $10 billion. Taken from ours. Citizenry that if it was anything else, would be a national crisis, but we just don't seem to. Put enough effort to that. Enough awareness, enough preparedness, enough understanding, and that's what the cybersecurity really endeavors to do. Yeah, very few losses are reported. People are just embarrassed, and everyone, everyone is vulnerable. Why is it not a national cars? It's and yeah. So yeah, we do a lot for our personal security and the security of our home and cars. We have doorbell cameras, we have alarms with the cars, all those kind of things, but we're more likely to be scammed from afar. We're free hardware that we set up that's probably not gonna do us any good when we get scanned by any cyber LAN. Yeah, artificial intelligence, a lot of available apps that can be deployed by script kiddies, social engineering, you know. So it's really interesting to see how AI has helped social engineering I AI's come up with some really good plausible. Screw ups to. Play to get us to give up our personal information or our credit card numbers or banking information. So yeah, please help. Please help if you are a victim of a scam, reported, reported. If you go to that town hall. You can see. The methods of actually reporting it, including local law enforcement. Some current issues if you have a Dish Network subscription. Dish Network was hit by ransomware. They were kind of quiet about how they responded to this effort. Some people are now speculating that they actually paid their ransom in order to get their data of their customers back. There's something called Ghost Touch and the ability to access smartphones by putting a electronic device under a restaurant table, for example. And then you've seen people come into restaurants. The first thing to do is take out their phone and put it on the tabletop in the restaurant. If one of these devices is under that. They will talk, they can get access to that phone as it's just laying there untouched by human hands and they able to get under that, that, that's, that's just where we're at now. 18 has admitted to hacking 60,000 directing accounts, granting is.

What are you doing? You still there?

Sorry. Yeah, Team hack 60,000 drafting accounts got draft king is. One of those bedding sites, and yeah, they actually would go in. And do credential stuffing. So if you have reused your password that you use on drafting, chances are they were able to get into your account and what they do is add a new payment method and then start with long funds out of. If these draft can accounts, you know 60,000. It's a pretty good number. Some Android devices are actually being shipped from the factory with malware already loaded in them, and it's Android devices and not just Android smartphones, Android smart tablets and even smart TV's running the Android operating system. Hilt with ransomware as they come out of the factory since shrink wrap some of the TV's that you smart TV's have this infection that you can get off of Amazon and quite a few others are those. Malware phones back to a control and command and Control Center, and it's being shut down. But as soon as if one of them is shut down, another one pops back up. They just have, you know, so many potential devices out there that they can use to scam us and get our. Congress reports intelligence agencies report that the FBI has misused the surveillance tool that they've got as part of the FISA court. After the Patriot Act. So, but in direct violation of section 702 in the FISA. In fact, this is something that is interesting to read. And again, the green link will bring up this PDF. It's actually a joint cybersecurity advisory from just about all of our intelligence agencies, including quite a few from overseas about the pupils Republic of China being states. Blocker cyber actor. Other issues Twitter and the European Union, they are threatening to drop out of a voluntary agreement with the GDPR regulation enacted in the European Union. The GDPR regulation is to increase the privacy of the European Union. Ireland's Data Protection Commission has taken the effort in the. Well, they're citizenry to sue or find beta and €1.2 billion, and which is a huge fine. Even if they were to win that court case, I doubt if that they would ever have to pay. And what they contend it is the private information of European unions. Users were transferred out of the European Union without approval. So this is going to be an interesting fight. And is this a? Enhancement to European Union members, users or a judgment. Recently, Indiana, Iowa and Tennessee have passed comprehensive privacy laws. That's eight states now total. You see, Texas is not on that list. There are just so many fines and ransomware incidents that come up in the last couple of weeks or not even going to go. Into that but. The barcode e-mail security gateway which is used by quite a few very large corporations, has yet availability that allow e-mail to be sent. Why do we care? Because a company that we have trust in might have had their e-mail administrator taken over and when they will send out something not on behalf of a this agency or company, that corporation that we trust but. Something that's really interesting, I've recommended brave one. I recommend having several browsers in your. Open anytime and you have various security levels for each of those browsers. Brave was one that typically comes out-of-the-box with enough security enhancements to be worthwhile, but you can add a lot of security enhancements, extensions, those things to brave as well. Brave as what? Working with something they call OTR that's off the record off the record is a chat program used by Snowden, you know, so it's very secure end to end encryption. So off the record in journalism parlance is, you know, you can't take notes on this. So you know, off the record what will happen. Is the website itself will suggest that the browser should forget anything. This website is about to present to the user using that browser. So completely forget anything from now on, all of the things that are needed to maintain state in a browser. Are actually stored now in a clean temporary area. A new clean temporary area, so there's no history, no cookies, no data is written to disk. It's a very secure way of visiting a site. It actually hides it from the device. So your Mac or windows. What don't know about it? What is intended for is, I think, of domestic abuse in partner relationship. One of the partners that's being abused would like to get some advice on how to proceed. If they shut off their browsing history totally like you can do. Or some browser it might hide too much and give suspicion to the abuser, so we don't want that. We also don't want to hide too little, so you know abuser can go and find out history from the browser and after the site visit you know it's going to delete cookies and permissions and all those kind of things. As happens now with secure mode or whatever, the device thing to so yeah, so it's not going to delete the history and caches, which again would probably raise suspicion on the users. Also it will have a quick exit button method so. You know, if the user comes in to the room during the middle of this, you know there's a method of doing quick exit and cleaning up. After that the site will define the methods, not the browser, so you know it's that's the way it should work. The site will actually want do you want. Off the record. Method enabled and the user must approve. So if you think about it, this gets around some of the other things that might go amiss with having this kind of capability in a browser, and that OTR is then tied to that site only. So the other browsing tabs that might be open in brave. Still exists, so again, we'll lessen these suspicious behavior that might lead to investigation. So yeah, there's no suspicious gaps. If you're into. They actually will put a request OTR and the HTML header. There's some debris, some preloaded OTR partner size primarily. Sites to help with abuse victims. There's no protections for brave extensions. Any spyware on the machine, any network sniffers, any operating system logs, any crash logs, any memory harvesters which a lot of spyware does. So this is not written to this. But it is printing to memory and in a memory harvesters can find this information as well. So brave 1.53 is when this OTR session will be available. Some things about passwords and you know. Again, our highly recommend we just forget using passwords and go instead to pass phrases, pass phrases or more secure you know for. Normal sites, normal things, you know password manager is is recommended. But for science that have financial. Impact, IE banking, brokerage, online shopping go to pass phrases and write down a hint for the passphrase. Don't put it in a password manager. There is a lot of. Effort to secure password managers. But there's always a way. There's always a way, some recent. Reminders of you know why passwords might be not. The best method and pass phrases over overcome that Donald Trump's pet Twitter password was your fired for a while, and then it was published, and then he changed it to maggot 2020, exclamation point, Perris Hilton. T-Mobile account was Tinkerbell Zuckerberg. Pass accounts have all been, you know. Cutro had published a picture that had a sticky note on her computer that had her password written down. Even Williams and the Reese of Foursquare and celebrate sell agate with lots of celebrities had their photos. Walking into because they use weak passwords. Apple and AI. AI is so far not a player in the artificial intelligence space, and because of that they have an internal ban for their employees that they can't use any artificial intelligence platform because other companies have used artificial intelligence to do programming enhancements and. Debugging and marketing and those kind of things and you know those are now captured out in the wild and available for anyone and everybody so. And a lot of companies are. Garbing up artificial intelligence companies by acquisition. Apple does have some kind of. Play in the artificial intelligence. If you have an Apple TV, there's something called Bobcat that does artificial intelligence to do viewing, recommendations and stuff. Some scams that have been brought to my attention lately. You know someone behind you at an ATM will distract you and. They throw money on the ground and they, you know, tap you on the shoulders. And is that your money? Did you drop that? And as you bend down to pick it up, they will swap out. Your ATM card with a counterfeit one and then you know, run away so. We need state. They're just all kinds of things out there. Remember to shield when you're entering your. And because some of these ATM machines have a attackers camera in addition to the bank's camera, that will view the keyboard as you're typing it in. So you secure ATMs, inspect those ATM's for you for. Using withdrawals and beware of any strangers in the area and onto your accounts. You know something to do. I suggest daily. And enable transaction alerts and keep that card secure and. You know, be more aware. Something that you might. Buying handy is you need if you need to quickly clear your browsing history for whatever reason. In Windows control shift and delete as a three. He sequence will do that quick look here and in the Mac command shift. So passwords again, it's not passwords, it's passphrases. And there's no brute force used to be the effort to find your pass phrase. But now it's social engineering. You know, you need to cancel your subscription or we've canceled your subscription and you need to log in. And and give us your password and you know those kind of things. Some people are really. You wouldn't believe how easily they're scammed by a phone call and, you know, going ask that, you know, we'll give us your password and we'll fix that for you. Asus router on May 16th. The Asus router actually issued A firmware update that was in error on most of those routers that got got that firmware update and applied. It actually could have gotten a subsequent firmware update. Because they have a fail safe method of. If the firmware update does not work. So if you have one of those and they're on the Bay 16th, you had some trouble getting on or getting back in. If you keep keep it powered up eventually it should have resolved itself. The actual cost was broken figuration. File TPP link we talked about this a couple of sessions ago. They have a firmware update but because a lot of IoT devices are this way, most users did not were not aware that there was a firmware update available. Even very savvy Cyber users were not aware that the firmware update was available and doing firmware updates for IO T devices automatically has fought. There's there's a downside to this, and that downside is that firmware. Have a malicious backdoor planted into it. Shifting gears, what are we talking about here? And or a lot of people use Android because they could take anything they want and put it on there as opposed to the iPad and iPhone, which are highly controlled by Apple, making sure that the applications you load are only from that Apple Store Android you can download, load anything from anywhere. Ohh Google because of that has put something called Google Play protect on their Google Play store and even with this protection in there's several 100. Applications found every month that have malicious code in them, so this is something that will help you protect the applications. That you have. Loaded from the Google Play Store and the. Real benefit here is if that application has later been taken over by someone who makes it into a malicious app, this Android setting will help. And again this. Is a screen shot of play protect on the Android or Google Play store for the iPhone? Is is good advice and we've done this before and you know for. To reiterate, consider using the mail privacy protections that are part of the new iOS. Installation and iPad or OS as well. What mail privacy protection does is hide your IP address so trackers are less app or. Able to track you if prevents senders from seeing if and when that e-mail is no open. When I send out the e-mail to as an invitation here, I can actually see when users open it I can see when users actually click on the link. A lot of users. We know, but a lot of users click on the link before it's time to hold the zoom meeting with Apple protect. You're not. The sender is not able to detect all these things. So on the iPad iPhone device, go to settings, mail and then privacy protection and toggle. There are hidden files in both the Android and iPhone and for. If you want to find out what some of those hidden files might be on the Samsung, you can go to settings and you know well for the Android devices you can go through the settings that are going to be here and will be part of. The slide deck. For the iPhone, you can do it a third party explorer on your computer back or Windows PC. Attacks that iPhone to a computer by USB and go through and find the hidden files that way as well. With iTunes backup, which is not pulling it down, working for getting iTunes back up over into the Finder on Mac OS. You can use the terminal app on a Mac that's connected or synced up with your iPhone. This is a setting that you can use in Finder on the Mac to prove that. You can also jailbreak your iPhone iPad, which is very much not recommended. He passed yet another password manager. That's that we're going to talk about. This is it's a vulnerability that so far has been unpatched. So it's an exploit you can actually retrieve the clear tax master password from a instance. Of Keepass on a device. So the master password is stored in memory. There is now a method and the method is well known to attackers to retrieve the clear text master password. Remember how password managers work, all your passwords are kept behind the vault. And that will you access by entering a master password. All that clear text password is available through very detailed and. Strict methods in order to get this, but it is possible the something that should be emphasized now this requires access to the memory of the machine that you have the password, Keepass master password manager held on. But it is possible to retrieve the master password. In clear text from memory and this happens even at the data place the vault is locked. And there's many ways to get access to memory. You can have a process dump and mirror is actually in the swap file as well. And when you hibernate to Windows machine, the memory is written to disk and then that disk is available to attackers. So yeah, this will work on Windows Mac. OS and Linux, so this version and older are keypass are vulnerable. A safe 2.54 should fix this issue, but it's even if you update keypass that master password still might still be available in memory if you have it rebooted your machine. So yeah, beware of any apps that can access or dump memory. There's something called Telly TV, which is a interesting thing we've talked about that last time. Basically what they said is the 1st 500,000 people that register will get a Free TV, big screen TV, O LED TV. Look at the size this TV actually comes with the sound bar, and so the big TV, then a. Sound Bar then then. Another screen below like 9 inches displays ads. 24/7. So you know the ads aren't in the content. The ads are displayed in a. If you get one of these and it sounds enticing, it actually, you know, claims to have well it does have ability to do video chats with your family. So it has a camera and a microphone and a speaker, and it has motion detectors, so you can set it up to alarm for like a burglar. Or but if you think about this and. Think about this hard. If you look at the terms and conditions, we're going to collect all information about the audio, video content and watch the channel to view and the duration of the viewing sessions. If you look at just about any smart TV, you're going to see, that's they do that as well but but but but this if you. No intelligence agency on the planet in history could design A better surveillance camp device than a telling TV. So, you know, shifting gears again, you know, reiterate this again trying to raise awareness and preparedness and understanding for Wi-Fi, strong encryption, strong encryption. You know someone sitting out in the driveway with a. Wi-Fi access point can see the traffic going in your house. If it's not encrypted. If it is encrypted, they can see who and where it is going because that header. Who descended to and who to receive it from? It can't be encrypted because it has to be in the clear. So yeah, use strong encryption up to the Max that all your devices get to use the lowest common denominator, common denominator, and so the encryption method use a strong pass phrase to set up that encryption. Review where you actually place the Wi-Fi access point in your home center so center is away from Windows and away from people roaming around outside. Higher up is better because there's less interference, typically higher up over bookcases and those kind of things, and avoid high interference. Objects like what cases, aquariums, those kind of things? I think it's really important to do an inventory. So every so often go to your wireless access point and ask you what devices have you associated with in the past and make sure all those devices are devices known to you. There's something called bandwidth. Three were, you know, a neighbor might be enhancing the amount of bandwidth that they use. And they can. Still your bandwidth because if you think about how most of us are laid out, we have a common utility app. Or home, you know that shared by our neighbors, you know, check your channel for speed and think about scheduling down that loads in the evening when maybe that paper with a lot of bandwidth use. Isn't using it. Google One is a pretty good VPN and VPN virtual private network. I've kept iterated over and over again. This is not a security panacea. Turning on a VPN using a VPN is not going to do that much for enhancing your cyber protection, but Google VPN. Has enhanced their ability to do some features that might sway you to you. At least review the Google One as a. This is something that I want to really emphasize. Android devices are now being known to be susceptible to a brute force fingerprint attack. We're going to talk again momentarily about how iPhone users are getting their whole digital life. Ruined by someone running up and grabbing their iPhone out of their hand while it's unlocked and then going around the corner and resetting the passcode and, you know, going those ways. If someone can get hold of your Android device, you might think. Excuse me, Sir. It was locked and then, you know, they don't have my fingerprint to unlock it. But now they don't need your fingerprint to unlock it. There's something called a brute print. I fingerprint brute force for the fingerprint, so this brute force trial and error crack to crack a code key or password to gain access to the. Android phone protected by a fingerprint reader. It's can now be overcome. So in in. Yeah, there's two vulnerabilities here. Something called cancel after match, fail and match after a while, which you know makes sense for the good geeks up on us. But for a lot of us it doesn't. But there are two vulnerabilities, and these two vulnerabilities are inherent in every. Android distribution, so you know that's that's the bad part. So you know this biometric data on the fingerprint sensor that's serial peripheral interface is inadequately protected and that's the attack vector that we're using. It allows for men in the middle and to hijack fingerprint images once you. Authenticated with your fingerprint again. For the geeks, this is how that attack works. This attack does unlimited number of submissions and that's you know, that's that's the bad part. And you know, until they target's fingerprint is matched and the device is unlocked. You do need physical access to the device because the attacker has to take off the back in order to connect a PC card. To the device and then it. We'll go through. A long list of fingerprint databases that are easily available on the Internet. There's academic academic data sets that have a large trove of fingerprints. There's biometric data leaks, the equipment costs $15, and this is effectively what we're dealing with. So again, this is attack after they have stolen your Android phone, much like the users of iPhone have to be worried about someone snatching the phone out of their hand or out of the purse or. Out of their restaurant. Take people talk while it's unlocked, but they have could have gotten. The unlock code, the PIN code by other means, so yeah. They manipulate the false acceptance rate, which you know most of us are that have dendroids that don't have this PC card connected to kind of rely on. So this is the flaw that they overcome so they can brute force that device. Some of these attacks take many hours, but you think about the game of many hours of effort. You know, having a person's financial life. Our smartphones have everything known about us. They know more about us than we do. So again, you know flow chart. This is the. Section of code that's actually part of the vulnerability. And like I said, this is currently now all Android. Systems from Google, Android or central to this. This is again more detailed. This time it works. These slides will be available available later so. This is a lot of effort that has gone into making sure that you know somebody just doesn't take your fingerprint and you know Scotch tape and then make a rubber copy of it and use that to unlock your phone. There are these sensors have capacitive electrical integrity. Compared to the optical, obviously some ultra thin technology and using ultrasonic to make sure that it is a live fingerprint and not something you know or clone or those. This is how long it typically takes to break in the Apple phones. There at the bottom are now limited to. The number of attacks that they they will accept before shutting down. All tested and devices Android devices are successful. iOS normally has five is the limit actually. Under this probability they're up to 15 attempts. Fingerprint data on the I I devices is encrypted so that that is a method. For protection time to attack, you know, from three hours to 13. Typically, fingerprint readers on Android devices are either side mounted, back, mounted, or under the display. And this is the press that's been out basically about this. I devices are typically safer because the fingerprint database is encrypted. But, but there's been experiments, typically in an academic environment where someone will take their I fingerprint protected iPhone. And we'll pass it around to, you know, students in the classroom. And chances are, like, I think the last thing I heard about done this 60% chance that it will be unlocked because the fingerprint was close enough. So Android protections the older devices and older Android installation are. Distributions are worse, vulnerable to this than the newer ones. Switching gears again, OOPL PYPL, which is a Python package across repository, has disabled new registrations and uploading a new projects because they have an unmanageable flood of malicious codes that that's. Really, really bad. Android has something called I Recorder. That's a screen recorder and it's now being reported. You know when it first came out and was in the Google Play Store. It was a actual good spring recorder, but now it has turned that screen recording, capturing the. Get on your screen and turn that into malicious purposes. It still is a good screen recorder, but that screen recording is then packaged up and sent to the attacker. He's been subsequently removed from the Google Play Store, but if you have downloaded it before and you still have it loaded on your Android by, you're announced susceptible to having this screen recording. Take over your screen on Android. Android 11 and up, we're up to Android 14, is actually in beta. Test out 13 is the current release. If you do app Hybrid Android will. And we start all over in Android 11 and you have a method that prevents some apps like this app recorder from being held to or. Changed from malicious uses and what's called is app hibernation. So if you haven't used an app in several months, they will go through that app and not remove it, but they will remove all permissions off of that app. Super VPN was one of those VPNs that claim yeah, we don't log anything at all. So if law enforcement comes in looking for our. VPN logs for our users. We don't log anything, so they'll go away empty handed. That was the claim, but actually they forgot that to protect their logs and it was actually found open open container on the Internet. So not only were there lying about not doing any logs. They had their. Logs available to anyone on the Internet. This is what we're living in now. So that py Pi, you know, I don't do Python library so I don't need to follow but you know worry about that. In order to mitigate that, this library has gone through efforts to purge the IP address of their users, you know. And why are they doing that? Why are they? You know, purging records? And why are they going through the efforts now to encrypt the IP addresses from now on? And they saw that they use for encryption is not stored. And you know why are they doing this? Why, why, why? And the reason they're doing this is the Department of Justice has issued A subpoena to them. For users and their associated IP address. This is discerning, you know, it's actually something that came up on our phone. You know, the Amazon driver chat, this is a message from your Amazon delivery driver, I don't know. For sure, if this is actually a scam or this is actually. The Amazon driver, because a.co is actually registered to Amazon. But then I'm yeah, I didn't do this. And so far I've gotten all my apples Amazon stuff. This is really, really discerning and want to really, really emphasize that this is not. Good, this is something sent out by Intuit and you know, it's standard. We've we've seen all this before, you know, I know your password. If you don't give me Bitcoin, I'm going to laugh at all your contacts. Yeah, that's not the thing that's discerning here, the thing that's discerning here is. Who it's from. And it really is from Intuit. What does Intuit do? Intuit sells TurboTax. That sells mirror, which is a personal finance application. They have quicken, QuickBooks. They do credit karma, they have MailChimp, they have all of this information about us, and their account has been taken over this, this and you know, it's used for spam. But what else could it have been? As for what else could it have been used for, Intuit has had some. Legal issues in the past, they claim that you know, TurboTax was actually a free file when in fact, you know, they were trying to lure you in and. Get you onto the paid version. So Intuit has had major password issues. They had quick and for a while down Quicken they sold Quicken. Sometime later Quicken then got sold to yet another one, yet another one and some users that are using the old Quicken are getting into the. Intuit is not really. Deep access, good control of their Intuit passwords. This hope was a wake up thing. PayPal, we talked about PayPal some months ago. And the capability of any seller sending a invoice to the buyer by using the PayPal mail delivery system. So this invoice actually comes from PayPal, but the invoice has been doctored to steer you to another phone number or another web address, another link, and if you call that phone number. Click on that link, you're not going to PayPal or the seller. You actually go into an attacker. You know this. We talked about this before. It's really, really discerning. But recently PayPal has a lot of. Money flowing through it. There's pretty wealthy. You can do things with PayPal, like do peer payments. You can do money transfers. PayPal has a mobile app and access to the web, you know. And yeah, this is going to be susceptible to phishing and identity fraud, so some recent PayPal incidents. The attacker places an order and they will use a fake or non existent physical address and then they will watch PayPal and say we couldn't deliver your package to the seller because physical address doesn't exist. So the attacker wanted that and they say oops. Yeah, my mistake. Use this address to deliver that package instead, and then they give them, you know, either their mule or their. Delivery address and now they have the. Merchandise and then after the shippers delivered to this rerouted address, and now I'm control of the attacker. The attacker will then ask for a refund from PayPal. And yeah, say, you know, it never got delivered on all the money back. And since it was rerouted, there's no proof of delivery, so the. You know the attacker, you know, gets double. Revenue for its efforts. Because of that, it's not protected by solar protection. Solar protection is something that PayPal has pioneered. And you know, is a good method. So we talked about the fake invoice, you know, but. Bring that up again. Another attack is to overpay and then ask for a refund of that overpayment. So you buy something and and overpay. Or you claim it, overpay, and then the overpair. The attacker will use the. Your rank to get that overpayment back. And you can also use my preferred shipper as opposed to Paypal's. So you know just about anything now and you know this was a. Strong point emphasized in that town hall for the NRO fraud group. Watch for, you know, generic greeting, dear user. Dear customer, whatever bad grammar that bad grammar used to be the tripping point. But with artificial intelligence out there now, using the grammar on the phishing attack. Will be better than, you know. So yeah, more real than real. Investigate any attachments before you open them. Anything that requests personal information that doesn't need that personal information to be as. To the department. Any payment request, any payment request, any payment request, all our money is ones and zeros now and it's transferred by. Use on PayPal and used goods and services as a payment method as opposed to some of the others like. Family and friends and things. That has safeguards of the. Take down safeguard program. For PayPal, use a strong pass phrase and multi factor authentication and monitor that PayPal account. Think about our mobile device and before we get into this iPhone thing, you know. We have reliance on the hardware. We have reliance on the operating system. We have Android or. Uh Apple relies on the apps that we've loaded apps, other amps that we've not loaded, and then malware. This, again, is important. There's now something a fishing camp, and it's actually the fishing kit is called file archivers in browser and this is pretty sophisticated and it's fairly new with this fishing kit will do is emulate. In fake Winmar, which is a archive method or File Explorer on Windows Machine, it will actually emulate a fake, fake, fake, fake, fake File Explorer window in your browser. So if you're not paying attention, you will see what it looks like, a Finder window or File Explorer window or. When more windows inside your browser and the attackers are using this now they have control of that site in the browser. And they can turn anything, anything, anything into a dot zip file and dot zip for the. Most of us. Know dot zip is usually a compressed archive, but recently Google for whatever reason decided that they would make 2 new. Well, actually make 4 new top level domains. So now you can register your website with the name of whatever dot zip Google claimed when they created that. That will newer users that want something zippy to use the dot zip as the domain. Tuple domain as part of their name. But you know those of us who are used to having zip as a compressed archive and zip is also heavily used by security researchers, you know, to zip up malware and send it so you know they're just now trying to trick the user into clicking on. Click on way too much. We don't need to do that, especially if we're used to clicking on things. You know, like setup dot zip to down on those packages in the past so you know this is something, you know, a real. Good method for getting. The users to click on something that we should click on. Don't you know this is a screenshot of the File Explorer inside the browser? It's not a File Explorer window from windows. A actual now this fishing kit will actually send back to the browser this fake surety scan. We we scan that zip file and it's it's good to go, you know, go ahead and have a good time. And this is again ice screenshot for the archivers and browsers. So you know. We click on the PDF to Redick. Redirecting story to a credential stealing page. We've talked about that before and many, many times. Click on this file link to download the malicious file. Something you can do is. Reason this happens or tricks a lot of people is windows typically is not set up to display file exchanges. That is a something that most of us need to address, and they will actually give because of that. The real file extension is typically not seen in. File Explorer window. Other thing that's really bad, really bad I think is Windows search, IE the search box next to the start button actually will search the web if it can't find it on your computer. So if you type in something like a zip file that the attacker is trying to get you to click on, you won't have it on your computer. Luckily, but it will typically might find an app on the web because it will use a web search. This is 2 vulnerabilities that allow this effort to go through. So that's if domains are potential for abuse, that is a message of today. One of the message of today and also they have dot MOV for movie domain Google has. They came up with. The other ones that dad and not PhD improv and. You know those kind of things? This is, you know, there's what's. What's the difference between these two links? And, you know, at first glance, they look pretty similar, but the second one will not be. Second one will not be helpful and you can also the attackers will use Unicode characters and what will look on your computer to be a forward slash is actually an Unicode, not a forward slash. So it is not interpreted by a browser as a separator in the. So some suggested changes is you can actually disable web searches in Microsoft Edge by going to the settings and making sure that search the web is it's disabled. Disabled web search in Windows search is something that would be a. Good win, but unfortunately the only way to currently do it and they're looking at doing this is by doing it rich edge rich edit hack or using group policy in the windows deploy. Some suggestions for making sure that the true extension for Windows is loaded or displayed is go through the File Explorer settings here. This isn't really security, but it is a hassle. You know you get a news article that looks really good, but you. Know they put. Up an overlay in order to view this article, you need to strive or send us money or whatever, and you know it's hard to dismiss that overlay. But there is a behind the overlay. Browser extension that you can load to most browsers and then you know if when that overlay comes up. If you do command shift X on the Mac OS or command or control shift X on Windows that overlay will be removed and you can read the article. So air tags. We talked about air tags before and you know the controversy is, should those air tags beep or not beep if you use air tag to track your dog or your bicycle or you know those kind of things maybe beeping you know would be good. Trying to find your lost bicycle. Maybe beeping would not be good if you use it to track your car. If it is stolen. If it is stolen. Please don't find law enforcement and have them go after the stolen automobile. Do not go after it yourself. There's been instances on the news. You know, fatal shootings because. Trying to track down stolen automobiles. Oauth has a vulnerability. Oauth is what we use for when we see sight that says would you like to log in with an e-mail address or would you like to use Facebook or Google or some other site that knows who you are already and you know I don't do that. But you know it, it is a convenience. A recent vulnerability has been found that allows credential leakage, so this is another method of gaining users credentials. And basically this is how you know things work. You want to go to a site and you know, say, you know, I'd like to log in and the site will say, would you like to log in to Facebook? And so you send any of the browser sends a message to Facebook and said, you know, I need proof of who I am from you. To tell the random side I'm going to and the reply will come back. It'll tell random site you know your credentials are secret. 123 So now you go to the site and said Facebook told me the secret that you're looking for is secret 123. And so then the site. We'll go to Facebook and says, who is? This guy and pancreas. Come back. You know it's john@gmail.com. So that's how that works. Again, not really cybers related, but something that. Might be useful is view the history of your house. Google has been doing mapping, driving around in their cars and taking St. views for a long time. And you know, if you want to see what your house look like last year or before it's painted or whatever. Potentially if you go to the. In Street View that you're looking for, if you click on see more dates you actually see if previous dates have been captured in the Google map and see what they. House look like or the building site or whatever. Google is testing AI boosted search trial. It's going in search labs. You need to sign up. I've signed up and not gotten in so far, but it looks to be a interesting. Enhancement to Google search. Other current issues. That I went through today before the meeting and found out. All of the current. Browsers that I use and the current version I recommend highly for any site web browser that you use to go to financial sites. First thing you do before you use that is to check for the current version. Some alternative browsers if you're looking for yet more browsers. Epic has security and anonymity as a selling point. An anonymity is it's. Usually one where requires some knowledge to get. In and then. Maxtron is a feature Rich browser has a lot of bells and whistles. And answer us all on Google Chrome is for lightweight. Browser if you're running on a. Low powered Linux machine and torch quickly torches your history, so if you're going around size that maybe you don't want other people know about. So we've said that I've said that we're going to do personal devices as part of the cybersecurity safe things that don't fit in strictly into the cyber realm. This is important. This is an iPhone attack. The iPhone snatching your iPhone out of your hand and running out the door and resetting it is much worse than you know home burglary, because they have now your entire financial life on that iPhone. Your photos, all those kind of things. It takes about 18 seconds to reset your password after they run out the door. In your iPhone, iPad and Mac. You know those are. Of action not typically move, but you can be, you know, laptops. You know you have your key chain that has your banking apps and financial shopping. You know, all your contacts, messages, photos, your entire digital life is on that iPhone that's now been. Kicking out of your hand and run away, they will change the Apple ID password, so if you go to your backups on your Mac and password change, you can't get to them. If you have set up a recovery key, which is good practice that typically that recovery key if it's there, they'll reset it. If it's not there, they'll set it. So you know. You can't convince the recovery key is apples proof of identity. So if you don't have the recovery key, you can't prove to Apple that that Apple ID is intact. Really you you could show up with a lawyer at Apple headquarters with a passport, with your birth certificate. You're not gonna let you in. That is you're apples. Proof of identity, that recovery key and that recovery key is gone. It's been reset. It's been set. Find my doesn't work iCloud backup to get your data back from your back. Not going to work. iCloud access to get your data back from PC is not going to work. If you're if, if you go to this top grain length, you'll see that we've done more expounding on this attack couple months ago now and also as part of that presentation, you know how past these work and those kind of things and. If you go to. The link here after you do see I. Say excuse me, say log in with your resident ID, you'll see some other cyber security presentations that cover that and other things. So how could you prevent this or not prevent it? How can you? Slow down this or yeah potentially prevent. You can use. An iPhone protection called Screen time Screen Time is actually deployed for allowing your phone to be used by kids or grandkids. Their partners or whatever, but you want to limit those kids and grandkids so they can't use this device when it's bedtime, when they should be asleep. So it was. A preventative measure set up for that design providers, but it is if you're competitive measure and effectively what you can do is go through the screens. Here and set up so that during certain hours, like when you're out and about and might have your iPhone snatched from your hand or stolen off your table top if those hours are set up to during screen time, those attackers will not be able to change those settings for you.

OK.

So in if you have this and it's in your position and you need to change those things, you can turn screen time off and then do the save and then turn screen time back on. So this is a protection method that. Really should be considered. It's not the not the only measure for the. So you know both. The iPhone and the. Android, you know, think about this. You know it's a constant connection to the Internet. So the Internet and all the people in the Internet, the all 5 billion of them, you can see them, they can see you. It's almost a constant connection. Unless you pull the battery out or turn it off. It contains your laugh information, all the message you sent, all the photos you viewed, all the photos that you've been sent and yeah. Can deliver all that information and candle receive information. News. All those things 24/7 we live with that thing attached to us and wait. Are they after me? Yeah, they're after that Apple ID that it's tied to the keychain. It's tied to your bank accounts. You can actually gather evidence, and you probably haven't thought about this, but actually, if you know you suspect this scam, call. You can play along, which is highly discouraged and gather evidence to give to law enforcement later. How do you do that with the screen recorder on your smartphone or smart tablet? Not all apps allow screen recording like YouTube and other things that don't want the screen recorded, but most of them do. Total considered that Speaking of devices Amazon is working on polarized sunglasses with Alexa built in. So as you're walking around with your polarized sunglasses outside, you can listen to audio books. You can listen to newscasts. You can adjust the volume up and. Down, you know, if you go by. Someone mowing their yard and you know, listen to all the books. Turn the audio up until you go buy. So for iPhones as screen recording the Control Center so you can quickly get that going. You know if you get a scam call and once record it. So this is how this works to play. A little movie here. You see, you get a countdown. And then once the countdown is complete, you get a stop and then you when you get a stop it will actually have. That restraint recorded and. You can then stop and then put it into your photos album. We talked about. Previously and it's on the Computer Club home page about securing IE patching your iPhone, iPad devices. That is such a serious vulnerability that the US government agency in charge of security has informed all federal civilian. Executive branch agencies to patch their Apple devices with that patch by June 12. All those things patched if you running Mac OS because you think it is immune from attack. The Golan cobbles strike therein. Has been modified to attack Mac OS. There's something called Max Stiegler Max Steeler is. Malware, it gets owned your Mac or your Apple device and steals access to your iCloud key chain that has your credit card data. Any cryptocurrency wallets that you have any past browser cookies that can be reused. Access sites Max Steeler has the that we dot MG as a Download file. So you need to keep those devices update and only pumped off from trusted sources. After that came out, there's something called Atomic Max dealer that again, you know steals your key chain all. The things that. Backs feeder did and it's down on mode. Files are listed here. So more and more things are targeting Mac OS, so don't be complacent and keep things up to date. Only install from trusted sources. Google has now. Announced an Android bug bounty program. This will help keep some Android apps. That are protected the. But bounty goes up. You know, 3025 and $20,000 if you're not a programmer with artificial intelligence, you can bang, you know, be one and you know, artificial intelligence can be used by anybody to find vulnerabilities in applications. So you can use artificial intelligence capabilities for attacking programs to potentially find a bug in. Software and get a pretty hefty award for that thing and you didn't do it. You're artificial intelligence scattered in. Windows now has something called phone link and phone link before worked pretty well with Android devices. As with the very recent instance of Windows, now it works with. IOS so your Apple phone so you know if you're working at your computer, your Windows computer and you have your iPhone not handy in your pocket or an extra room, you can actually use phone link to answer your send messages or do anything that that you want, that you would do on your iPhone and actually be done. In phone like applications inside of Windows. Vulnerability that we're we're not dealing with and the vulnerability is once a small or an IO T device is implemented. Getting the updates out by firmware or problematic. And in this case the firmware update for a. Asus router is good. I mean they say there's a firmware update. Actually after the first update you can turn on auto firmware updates and it will update automatically. So that's the good part of being able to do. Firmware updates autonomously, so you don't have to check the bad thing about it if you have an HP model listed here. HP sent out a firmware update to all of the connected printers and the update was to enhance the detection for using a non HP link. Ink cartridge. That firmware had an error in it and now anyone who has a 920 E HP printer cannot use it for anything other than a boat angler cause the firmware is. Reloaded and that will firmware it was not. We keep saying those you know, type in this letters in order to prove that you're you. Know a human and not a. Robot that's captures are pretty good and discerning whether you're actually a human or a robot. But attackers that want to break into size protected by captures saying you know we can't beat this. So how whatever whatever going to do well, we're going to apply those humans to use. To break into CAPTCHA services. Classmates, classmates long time ago. Yeah, I I signed up. They they really pushy class space was later purchased by my life. And if you want to get scared as hell. Look at what? My life knows about you. But you know this, this is just. I don't like like this. You know, they send the thing recognizing anyone in this photo. And guess what you have to do to severe that. Vote View a link? Yeah, don't do that. Please not do that. Really, in the little high note, you know if you have electric vehicle, you think about it. You know if you break down the road, you have a gasoline there hold tight, duck triple. A comes out and brings your gas can. What are they going to do? If you have electric vehicle, they pick you up and take you to a charter station. Ohh that's it for running way over. I apologize for that. This should be. Posted later and you can review and.

John yes, Brady, one of your presentations you mentioned investigate attachment. Can you go into? How you recommend us to investigate attachments?

Yeah, that that's a good question and doesn't have a good answer because attachments can be PDF documents, they can be, you know. Just about anything, any of any type of file can be sent as attachments you think about when you send e-mail to anybody and you know you want to do an attachment, you can pretty much pick anything on your computer, on your device and include that as an attachment. So that's why it was sort of a generic thing, you know, investigated. Actually, it's really depends on what the attachment is. You know whether it's a PDF file, whether it's a movie, whether it's, you know, just, you know, just, you know, too many. Options there to say you know this is the definitive put on that Pi hat. Do you know you? You've got some awareness now of things that can't happen and then you know. Do some preparedness. If you know if any. If you have any suspicion. Don't let you know do I don't bound investigation I you know. Ruler sent that link to you, called him up and say, did you send this to me? A lot of. Times, they will say, I could blissfully unaware of any attachment I sent to you. And you know, we want to. That's the kind of investigation I guess. I mean does that make sense? It didn't answer your question at all. But you know it's it's. It's just, yeah, too complex a question to say, yeah. 123. OK. Usually the best thing is to investigate Alabama. You know who sent this to you? Do you trust them? And even if you trust them, verify that. Yeah, they really did send that because you know. It's happened to me almost on a daily basis. You know, you get someone that you know, or at least you sent e-mail for. You know, please, you know, open this or please look at this or have you heard about this? That's the one I get the most and those kind of things and typically their e-mail account has been taken over. They're not really sending it anyway, so you know, contact them out of band, IE other methods, not e-mail, and typically find out that, yeah, mostly unaware of any attachments I sent to you. So yeah, delete it. And if they did so, that's that's the best thing I've. You should really click on. That and go that way. OK, attendance is much. Appreciated on these zoom sessions. I know a lot of people you know want to view them later in the evening or whatever and go that way. So aware of that, but attendance on the zoom session is important to me and is appreciated, so we'll do this. A couple of weeks.