00:09 **Producer**: And now, without any further delay, let's begin today's event entitled Cybersecurity and You, helping secure your home for work and your family. I'd like to introduce your presenters for today. And they are Jay Wiley, Administrative Vice President and Deputy Chief Information Security Officer with M&T Bank, and Kristopher Meyer, Threat Intelligence Officer with M&T Bank. With that, Jay, the floor is yours.

00:33 **Jay Wiley**: Hey, thank you. I just want to say a good afternoon to everyone. Hope everyone is doing safe, and your families and your staffs are doing well. Kris and I both appreciate the opportunity to talk cybersecurity to you in this afternoon. Of course, it's something that's near and dear to our hearts, so we're glad to be able to try and share that with you. A brief bio on myself. I've been with the bank about five years. Prior to that, I came from another larger financial institution called the Internal Revenue Service, where I was in cybersecurity as well. And then before that, various cybersecurity assignments, as well as years in the US Army as an Intel officer. Kris, if you wouldn't mind giving us a brief bio of yourself.

01:20 **Kris Meier**: Sure, thanks, Jay. Good afternoon, everyone. My name's Kris Meyer. I've been with the bank about three years as a threat intelligence officer. Before that, I worked in the healthcare space, did a lot of cybersecurity architecture work. And before that, a great deal of consulting in the small and medium sized business, IT and security space. I'm with a large company in the financial space today, but I've got a lot of understanding in the small and medium sized business space too. And I know we've got a lot of buried attendees here. Hopefully we'll be able to address any questions you have, regardless of where you're coming from.

And I'm going to step right into our first slide, and we'll get started. This unprecedented time has kind of presented us with a bit of a target page landscape for bad guys. And that's really the case fora couple different reasons. And my job here, and my team's job here at the bank is really to help our broader cybersecurity team, as well as our business partners and technology partners understand what the risks are out there. What the bad guys are doing, what tools they're using, and how they're targeting us. And what we're seeing is not so much a dramatic increase in the number of threats that are out there, but a shifting of focus for those threat actors that are doing bad things. So, if you had one group of bad guys that were doing a lot of phishing, it's not that they've increased their phishing, it's that they've pivoted their phishing attempts, and has started to use COVID-related a phishing campaigns. We're seeing a lot of CARES Act and PPP related phishing campaigns as well. And obviously, this environment has presented a number of issues where we've never worked together in a home before. And so, we're mixing a lot of devices. We've got networks with corporate technology, with home technology. Kids are doing homeschooling. We've got voice assistance, and all this stuff on the same network. And all that creates a lot of new complexity, and new potential issues that we're going to start to walk through today. I will hand that next slide over to Jay, and we'll start down that road.

04:13 **Jay Wiley**: Thanks, Kris. There's a quite a bit that each one of us can do, that some of the question out here is what can I do about the cybersecurity understanding of the vulnerabilities? How do we protect against those? And what I hope you find is that a lot of this is not revolutionary things. It's a lot that we can do ourselves, and we just have to know what it is, pay attention to it, and then take action. I think the final thing I would say about this is a lot of what we're going to say here is actually free, which is a great price to pay. A lot of things you can do don't cost money, and it's going to help your defensive posture.

What we want to do is understand what your exposure is. Where are you particularly vulnerable. And you can see on the chart there are four main areas. Number one, anything that's attached to your network could be vulnerable. Now, the trick here is to think about all the things that are on your network. Yes, we know you've got a laptop. You've got a cell phone. But what about your TV? What about your home assistant device, those devices like Alexa, or Siri, etcetera? Perhaps you have a refrigerator, that's a smart refrigerator that keeps track of your groceries, etcetera, etcetera. If it has an IP address, and it's on your network as well. Think about all of those devices, because the things we're going to talk about. then apply to all those devices on your network. Another aspect of this is, do you share some of your devices? Maybe you have a family tablet, and everybody uses a tablet. But you might also use that to log in to check your email, or something at work. You have to remember that with multiple people using that, we've got to be aware of what's going on. Maybe one of the kids used it to download some software, and that could potentially be vulnerable as well. You got to think about your router. That is the access point to your network. We all have them connected to the cable box, or what have you. And that is the point of entry to your network. And there's some things we can do around this to get your router more hardened, and make it harder for somebody to get in to your network. The last thing I would say then is a lot of us do use cloud services. And what we mean by cloud services is something like this on the Internet, and you're taking advantage of it. One of the things is there's Office, which is a Microsoft Suite add-in on the network that you can utilize to do your work preparation, your PowerPoint presentations. You have things like Gmail, which is your Internet mail. Those things are out there, and there are these cloud services. You need to be aware of all the ones that you are using, and hopefully that they're a robust service that you're using. And it's not, let's just say, a weak one, or a vulnerable service. So when you take a look around this, you get a whole view of where you could be vulnerable from your network. And how it's configured to all the devices that are on there, to who's using them, and then any other third-party services. So, let's go on and talk about some things that we can do to secure your home network. And Kris and I, we'll split some of these.

I'll start at the upper left, which is keep all networked devices updated. And what I really mean there is keep all your devices updated. Some statistics from a couple of years ago, just to highlight how keeping your systems updated has a lot of weight 70%, thereabouts, of attacks, use known vulnerabilities that you could have patched. So, you're going to knock out three-quarters of what you might. be vulnerable to just by maintaining your software up-to-date. Another key stat, nearly 90% of successful attacks only use basic techniques. Meaning, they just had to take advantage of this, they just had to do that, it wasn't that hard. So, again, if you're updating your software and keeping it up-to-date, then you're knocking out nearly nine-tenths of those successful attacks. Because they only use the basic techniques and our patches would account for that. One thing you can do, too, is ensure that that update mechanism on your devices, your laptops, your phones, etcetera, are set to automatically receive those updates. And that way you don't necessarily have to think about it. They release them, sometimes ad-hoc when they need to, if there's a really scary vulnerability out there. But generally, they do it in a weekly pattern or something like that. So, if you have that turned on, then you don't even have to think about it, if you'll get up-to-date with the latest software, and you should be okay on that. Another thing you need to do in terms of keeping your devices updated is. we recommend that you should run an anti-virus solution on there. Whether it's your phones, your laptops, it can be Mac, it can be Windows. There are anti-virus solutions out there that you can investigate, research and then utilize those. And the last thing I'll saying on the terms of devices is use passwords on all your devices and your apps. You don't want to just sit something down and have somebody come along and be able to pick it up and then do something on

your behalf that you wouldn't want them to do. And having said about having some passwords on your devices, that you need to make them strong. Now, we all understand that sometimes those things can get a little out of hand, they can be hard to remember. But one of the key things you can do is always change the default password that comes on your device, especially on your routers. We just talked about your home router being the primary entry point. So, if you go on there and you change that, because here's the thing, a lot of those are pretty standard and pretty well-known. For instance, it might just be a username of admin and a password of admin. And I know this, the bad guys know this. And so, if you don't change that default password, I can just come right along and in the first ten seconds, guess that and, who knows, am I successful or not? But change your default passwords. Then you want to use something that's strong, that's unique. It can be longer than not. That, of course, starts to draw you into the situation where, okay, how do I remember that? Well, one of the things you can do is use a password vaulting solution. It's a piece of software, it's an app that you can get for your computers and/or for your phones, where you can actually store all those into that vault. Thereby you only have to remember the one that locks into your vault. It's like having a safe, if you will, a software safe for your password. So, there's a recommendation there to help you store those so that you can make them strong and unique. And then you only have to remember the one to get in there. And so, with that, let me turn it over to Kris, take a couple of the other topics.

11:56 **Kris Meier**: Thanks, Jay. So, on the securing your router topic, a lot of what Jay's already kind of gone. through for your normal network devices is definitely in play for your router. And if you think your router, that's your entry point into your network. So, it's probably one of the most critical pieces of hardware on your network, yet, it's not ever one at the top of our list, for maintaining anyway. Because, generally speaking, we buy it from an online store or big box store, we set it up, we've got connectivity and we kind of forget about it. And what makes routers in particular rather difficult to keep. up-to-date is a lot of the ones that are sold really have a pretty short shelf life as far as portability is concerned from the vendor. And so, what I like to recommend in this space is get a router that has a one, two, three-year commitment from the vendor to receive updates. And preferably automatically update itself in the middle of the night. And I can't recommend specific vendors, but there's a lot out there that have that capability. And it takes it off your mind, it keeps them up-to-date. And again, it's that critical connection between all your devices that. you care about with all your data on it and the rest of the outside world.

Like Jay said, obviously true as well, those administrator accounts - change those passwords. When you're setting up home Wi-Fi, make sure to set a strong password there, especially if you're in a really populated area where your home Wi-Fi network can be seen by others. I know that I'm in the city of Buffalo and I can probably see of my neighbors when I when I open up my laptop. And so, you want to make sure that you're setting a strong password there that only you and your family now. From the administrative account side, too, in addition to setting a strong password, I like to recommend turning off any remote administration capabilities. A lot of routers have this. Where, if you're traveling and away from home, you can remote in and make changes. Quite frankly, the scenario where you need to do that is so seldom that I just recommend people turn that off. Because having that on opens you up to a lot of different attacks from the Internet side.

And then the last thing I'll recommend, and this is more for folks who are a bit more technical, is many routers today have this concept of home network and guest network. So, if you have family and friends over and they need to use your Wi-Fi, you have this separate guest network that you can provide to them. And that's a great idea for folks that are traveling into your home. But it's also a really good idea

for devices that you want to have around because they're convenient, but maybe they're not updated all the time. Maybe you don't trust them as much. And so, you think about all these internet of things (IOT) type devices, security cameras and voice assistants and home speakers and all this stuff that kind of falls into this almost secondary category from a trustworthiness and security standpoint. For those more technical folks, I like to recommend leveraging those guest networks there. Because it creates a bit of an air gap or firewall between your home laptop, your corporate laptop, and then all these other devices that you might not trust quite as much.

And then on the topic of backups, this comes up in pretty much every cybersecurity conversation but keep good backups. And what I also like to recommend here is keep backups in a way that creates an air gap. Meaning if your backups are online and easily accessible from your home or. work machine, then the bad guy can get those backups. Too, and what we have seen in a lot of recent ransomware-based attacks is, that once the bad guys get in. They hunt around for those backups, try to delete those first, and then launch their ransomware attack. Thought process being that if you could recover, you're less likely to pay the ransom. And so, the bad guys have started to understand that. And so, whether that is an on-premises or cloud-based backup, I recommend encrypting those transmissions. Encrypting those files that rest, and also making sure that that's air-gapped a bit. Not easily accessible from your home machine, and that may be use a separate account and password. Maybe it's an offline backup that you can't really access directly, there's a number different ways to accomplish that. But I think that's probably the biggest thing you can do to protect yourself from all the ransomware attacks that are out there today.

And with that, I think we've got a poll coming up here. So, we are going to engage everyone in the audience, hopefully get some responses here. So, the question for the group is, how do you remotely access your work email when away from your corporate laptop? So, another corporate device such as a phone or tablet, a personal device with a dedicated corporate mail client. A personal device with an email client, used for both personal and business use. A personal license-accessed email host on the Internet, like a cloud-based service, or no remote access. And we'll give everyone a second or so to respond before we look at the results, I'm curious to see. All right, let's, sorry Jay, go ahead.

18:02 **Jay Wiley**: Yeah, I was just going to say, I think a couple of those, I use the first couple, I think. And we'll get to talk about that here in a minute.

18:12 **Kris Meier**: Yeah, sure, take a look at these results here. Another corporate device such as a phone or tablet, that's great. So, that's my preference personally. It's not always the most cost-effective solution of course. But I find myself I'm liking the mental break point as much as the technological one. When I pick up my corporate phone, I'm in a little bit of a different mindset than when I pick up my personal phone. And so, while it kind of stinks at times to carry around two devices, that's my own personal preference. Great, all right, well thank you for your responses, that's awesome. And so, I will turn this back to Jake, kick us off on this slide?

19:14 **Jay Wiley**: Yeah, thanks, Kris, so you can see here, some of the steps you can take to secure your business information. And that kind of follows on from the question that we just asked relative to the polling question. How do you access your email? And our going-in position is that you need to use business equipment for business. We all know there are ways that you can utilize personal devices in the conduct of your business. There's a term that you may have heard, bring-your-own-device, in fact, that is what I do. I have my own personal cell phone that I use in lieu of a corporate-provided one, and I use

that for business. However, what we have done is used what we call a mobile. device management application. And that application is just like a safe container on my phone. That restricts the access and the use of the business information to that container. The information, I can't bring it out of there onto my personal phone. Somebody can't really get from my phone and jump into that container. Because we have our corporate controls around that to prevent that from happening. That's one of the things that you want to do with respect to that, try to keep business equipment for business. And if you have a personal or a bring-your-own-device policy. Make sure that you use some mobile device management software to keep those separate.

That goes back to the email question. Where if you're connecting just straight on from your personal device or personal laptop, and you go and access your mail. There are some concerns there There are concerns that there's an access path from your phone into your email. situation. And that could be corrupted, or taken advantage of, and then there's also a data aspect of it. In terms of now you've brought company or corporate data down onto your personal device. And if you're the CEO, you know how you're handling your own information. But maybe it's one of your employees. And now all of a sudden, how do you put some control around your own business data? And ensure that that doesn't get somewhere you don't want? So, you can use personal devices as a bring-your-own-device. But make sure that you have some sort of control in place to try to restrict the vulnerabilities there. And also restrict the potential loss of data there.

On the previous slide, we did talk about password-protecting your devices and applications. But in this case, what I'm trying to talk about is, make sure you lock your device before you walk away. A lot of us sometimes get up, it's a coffee break and I'll go pour myself a coffee, or it's a bio-break, etcetera. Go ahead and hit that Ctrl Alt Delete in the windows lock your screen, so that somebody can't come along. It's even more important now that we're working from home. Maybe your children or your pet isn't going to come and log on. But if you were in a public space, maybe, and accessing the network from there. Somebody else, a bad actor could come along. So, it's just a good security practice to make sure you lock your device before you walk away and don't leave it unattended. Now, what's unattended? Obviously, you don't want to leave it, if you're at the restaurant, you don't want to leave it on your table when you go to the restroom. But there's also things like don't leave it in your vehicle. A lot of us believe that we're going to put it in our trunk and it's safe. But the bad guys, they know these things, they learn these things over time. And so, in this case, they could just break into your car, go through the back seat and they're in the trunk. That's not as secure as you think. Our policy is if you've got a corporate device, you carry it with you wherever you're going. And of course, that can be inconvenient sometimes. So, you just got to do a little thinking ahead. Don't drive your car with your corporate laptop down to the ballpark, and then leave it in your car, so think about that. You want to avoid the use of USB drives, that's a huge vector of inserting malware into your environment. You can't get around it, but at least have the mechanisms in place. Certain people will authorize that because of their business use. But in general, we discourage or don't allow the use of USB drives because of the high vulnerability.

24:02 **Jay Wiley**: Then the threat vector that that can introduce into your environment. Then Kristopher, let me turn it back to you.

24:10 **Kris Meier**: Yeah, sure, so I'm going to start by talking about you know, sticking with third party services. But the one other thing I just like to add to your last point, Jay around password protecting applications on mixed use devices is, it's not only a cybersecurity kind of thing. It's really a data-

protection kind of thing. And so, I mean, by that is anyone who's got small children. at home know that you've got games on your personal phone. You also might have your corporate email. And in from experience, I can say that it's nice to have a password on your corporate email, so that things don't accidentally get deleted. And so, it's just another little safeguard to have in play on the third-party services side.

So, I guess optics into this world vary by the size of company that you're at. So, if you're on the small or medium sized business side, you've probably had a hand in or at least awareness of the negotiation of these third-party service contracts. So, whether that's a file sharing or storage service or a backup service or email or you name it, you might have some visibility into that. Those of us who work at larger organizations are sometimes. just given a list that says use this one web conference vendor or this one file sharing service. And sometimes maybe that service isn't as flexible as we need it to be and the temptation is to use another service. And I think that's all the more front and center when you're at home. Because especially if you're in a mixed user, bring your own device type of environment, you might have some of those other services loaded there that you use in a personal manner. And so, there's certainly some temptation to just use that service that is easier, that you might use on the personal side. And I guess what I want to kind of reinforce for everyone is there is a lot of process that goes in to the conversations in and around onboarding a new service provider, and there's a lot of reasons as to as to why. One ends up as the recommended provider at a company and that's because of a range of different issues So, they might have better data privacy guidelines, data retention guidelines. You name it. And so, all that to say extend some trust and use the services that are provided to you by your company, understanding that kind of all that legal and privacy work has gone on in the background to kind of that. And then the last one that I wanted to mention, and this is a pretty, short topic, but I think it's important, especially when we're working at home. We don't necessarily have the same kind of mindset in and around physical documents. And so, if you can print from home and you might do that and you might just throw them in the recycling bin whereas if you're in the office, you know to put that in the shred box. And so, what I recommend is if you have a home shredder, please use it. If you don't, some companies are recommending - hey, keep those safe, put them in safe and then when we do all come back in the office, shred them then. Any kind of option is good just as long as you're kind of trying to keep the same mental mindset that you would in the office as you would get at home now in this modified work environment.

27:57 **Jay Wiley**: Hey, Kris. I think that's a good point that you make in that. Yes, we are all working from home, but you do need to bring some of the mindset to your space. Whatever your work space is at home, that's what we're talking about. Just bring that work environment mindset to that area as well. You don't necessarily leave things laying out. You might put them away in your drawer, filing cabinet, etcetera. You might dispose of them this way that way and all those kinds of things, and just treat it in the same mindset, and then that'll go a long way to helping you out at home.

28:38 **Kris Meier**: So, a couple more topics extending on our previous slide. So, I wanted to specifically talk about secure teleconferencing. I think it's probably safe to say we're all using teleconferencing, I think we're also using it more than we ever have before. And with that comes some learning curves, of course. And I think that this is a technology that not everyone kind of considers the privacy and cybersecurity ramifications of the usage, because it's air quotes here just a "teleconferencing solution". I talked to someone, and it's over.

What I want to reiterate, it's kind of to my earlier point on the third-party contracts and third-party service provider side, use what your company has already vetted and approved, because there are components that, but do have a privacy and cybersecurity concern to them. So, the call might be recorded. The screens might be recorded. The web conferencing software might have file sharing capabilities or whiteboard capabilities or chat or something else to kind of enhance the usability of that product, but also opening you up to data loss scenarios. So, make sure you understand if I'm in this web conference with vendor X, is what I shared being recorded, is that file I dropped in there going to stay around for a year or is it gone after the conference call ends? Understanding all those components and sticking with the approved vendors for your company is really important at this time.

And then phishing is always a topic on any cybersecurity briefing that that you've all attended in the past, I'm sure. But what I want to reiterate here is the unfortunate truth is this is probably just about the most hostile environment for phishing right now. Everyone's a little bit more stressed out. Everyone's a little bit more on edge. Everything is a little bit more time sensitive. You're trying to react quicker. You're probably distracted at home if you've got kids home schooling and a partner at home, as well. It's just a much different environment. And so, all of that blends together and kind of a perfect scenario for you accidentally clicking on something you didn't mean to click on. And so, if I could have people take away anything from this, I would say take a breath. Think before you click and try to separate yourself from all that other stuff that's going on, because it really is that perfect storm, so to speak for the bad guys and they know it from a phishing standpoint.

31:36 Jay Wiley: Hey, Kris, I think it's time for another polling question. So, let's review that if you don't mind. So, what would your action plan be if you were discover something suspicious in your corporate device or email, etcetera. So, option A, we have a documented business level plan to follow. A formal plan that you practice how to enact. Option B, we would call our security administrator to take action. Option C, you would call a colleague who maybe knows something about computers. I don't know anything, I'm in finance, let me let me call someone who knows a little bit more about that. Or D, our favorite option is, what plan? [LAUGH] And so you guys go ahead and take a couple seconds to put in your polling answers, I'd appreciate it, thank you. Hopefully that wasn't you, Kris, that just clicked "what plan," because I know better.

32:45 Kris & Jay: [LAUGH]

32:28 Jay Wiley: So, let's go ahead and see what the results look like at this point. Great, if you look at that we're talking nearly, what is that, almost 75% have a have a business plan to follow or do have some sort of identified staff to help you take that action. And that's what we would encourage. You really have a "plan"? It doesn't have to be this first one that's really documented, and they practiced it and it's codified, those kinds of things. That's desired, but just depends on the size of your company and the amount of resources that you have. But at least if you have a "plan", you know what to do when things go wrong, then that's going to make your response just that much better. And speed of response is one of the key criteria that we look at, because then you're able to cut off the potential damage a lot faster. And in cybersecurity one of the things we look at is that sometimes a lot of these things go undiscovered for quite some time. And that allows those bad, bad guys to do some damage. So, thank you for your participation in that. And I'm really encouraged to see that a huge majority kind a have a plan and have people they can reach out to. So, if you feel like you've been victimized, there are some things that you should do, can do. And you can kind of put this in your plan. But like I said, speed of

action is really critical. So, act immediately. If you've got some financial issues, you contact your bank. In this case contact M&T or Wilmington Trust, and we've got resources that we can bring on to that particular problem. If it's identity theft, for instance, maybe someone's gotten your credential or something. Report it to your local police department, they can help with that because there's lots of things you can do. Besides your bank, you can call your credit card companies, freeze your accounts, etcetera. If it's business related, hopefully you either have a department or you got some staff or a member who handles your IT and work with them to get those things cleaned up. And now, if it's your personal stuff, then it gets down to. trying to find out experts who can help you solve the problem. That's not quite as easy to do that. But I think we all kind of have an idea of some folks in our families and our sphere of influence who know quite a bit about personal equipment and IT and stuff, and they can help. I know personally, I'm sure it's the same with you, Kris, is that my family tends to reach out to me in those kinds of things.

So, do that. If you notice now, we've talked a little bit about phishing, and we've got some questions on social engineering, so we'll get to that. But if you think that you have a phishing email or a fraudulent email, you can contact us at the phishing@mtb.com mailbox, and you see that on your slide. Anything related to your account, and you can see our contact numbers that you can contact us, and then we'll get our escalation focus on that and get those situations resolved. And so, thank you for the time. That's the prepared remarks that Kris and I had. If you want to learn more about some of these things that we've talked about, we've set up a cybersecurity microsite at the address that you can see here (www.wilmingtontrust.com/cybersecurity). Hopefully we covered some items of interest. But what we really did want to get to, and what hopefully is maybe the most fruitful, is the question and answer session, which we'll handle right now.

36:55 **Kris Meier**: Yeah, and I'll take the first one. Jay, you can take a sip of coffee here. The first question I have is, what about backing up to an external disk - the USB drive I'm imagining here. So, I think this is a kind of a good option. I will give a couple tips or caveats to doing so. So one is, I wouldn't leave that guy plugged in all the time. So, to my earlier point about, how do you best protect against ransomware? It's creating that “air gap” between your machine and the backups. And so, I would do the backups and then don't always leave that drive plugged in. Lock it in a safe, physically secure it. I'd also recommend encrypting that drive. Because if you back that up, those drives today are very small and can get lost or stolen rather easily. And so, I would encrypt that disk at rest, keep it in a safe place, and not leave it plugged in all the time. And then the last thing I would say there is that you can kind of have the best of both worlds if your risk tolerance is such that you can trust an online backup service. And you've vetted that they are doing all the security that they should be doing. I know that a number of those services support the online backup function, as well as a local backup. And a major benefit of having that local backup is speed of recovery. Because that recovery time is always going to be quicker with a physically plugged in thing to your computer versus you downloading files through your internet connection. That's a great question.

38:39 **Jay Wiley**: Thanks, Kris. Hey, so I've got one that's come in, and it's what about accessing your corporate virtual personal computer via your personal laptop. And I'm not sure that this topic, we actually brought it up, I think meant to. But what you would want to use there is a virtual private network or VPN. And what that does is that establishes a secure connection from your network to the network that you're reaching out to, in this case, your corporate network. And in fact, I am doing that right now as we speak. I'm on my own personal computer, desktop computer, and I've established that

virtual private network connection to my bank's enterprise network, and then I am displaying my virtual PC. So, you want to make sure that that's a secure VPN, because then that protects all that information flow from your home back to the corporate enterprise, so that nobody can see it or get into it. And that's how you'd want to do that.

39:45 **Kris Meier**: Thanks, Jay. I'm going to ping you back on that one with the next question. The next question is, how safe are public Wi-Fi options, coffee shops, etcetera? And how do you remain secure when you're working away from home? So, when we all can leave our houses again, that's a question that constantly comes up for us on the cyber side. And so, I think answer number one is that corporate VPN. And so, while it doesn't eliminate all the risks associated with a public. Wi-Fi option, it does eliminate some. And so that virtual private network technology creates that end-to-end encrypted connection between you, and your laptop, And your company network and kind of shields you from some of the other stuff that might be happening on a public Wi-Fi hotspot. And then the other thing I'll say is many cell plans have high data caps today, or even unlimited data caps. And when available, you've got a decent signal - that's always my recommendation, personally - is a hotspot to your phone, and use that versus public Wi-Fi. So, it's always the safest option. And nowadays, especially if you're in a major city, the speeds are almost the same as you'd get from public Wi-Fi as well.

41:07 **Jay Wiley**: Kris, got a question here. Let me pose it to you, if you don't mind, put you on the spot.

41:12 **Kris Meier**: All right.

41:13 **Jay Wiley**: Will scanning a USB thumb drive with an antivirus scanner confirm that it is safe to use?

41:21 **Kris Meier**: I guess the answer is yes or no. So, it's going to give you the same amount of confidence, as it would your normal PC. So, meaning if I scan my home PC, or my work PC, and I scan USB drive, I'm going to have the same level of confidence that I have in those results because the technology doesn't really differ in that respect. What I will say is that antivirus technology, in general, is a constant cat and mouse. So, the companies that provide antivirus are constantly chasing the bad guys, and the bad guys are constantly trying to evade detection. And so, no technology on the market ever has 100% security, and that's why we talk about all the different kinds of security. So, in the cyber side of the house, we call that layered security model, meaning, I've got a really good credential. Well, they get my credential, now I've got two factor. And I've got antivirus, and I've got a strong Wi-Fi password, and I've got all these other things that mitigate any of the residual risk. And so hopefully, I answered that question enough.

42:36 **Jay Wiley**: And I would say, there's a business, or a corporate aspect to that as well. And what we have chosen to do is utilize a known vendor. And we use approved USBs that are capable of being encrypted, because we don't want to lose our data. So, from a business perspective, there's a way to set that up, so that according to your risk appetite, that you may be able to use a preferred type of USB that meets your own risk appetite, and controls that then you can use that, and make that the approved one at a business. Here's another question that has come in. For routers provided by the Internet provider, can you still protect yourself? Yeah, I think that the things that we've talked about. In other words, my router is from company x and they gave it to me when I signed up for the service. I went in and did some of those things that Kris had talked about earlier. Things like putting a strong password on there, changing from the default as well by doing things like. not broadcasting my network main, how it comes out, and it can be whatever, John Smith Internet. And that's a broadcast that you drive down the street,

you could see that that's “John Smith internet.” Lots of things like that. Turn off your remote access. Yeah, even though the router is provided by your Internet provider, the steps you can log on to take. Because you do have administrative control over that router, despite the fact that your service provider gave that to you.

44:33 **Kris Meier**: Thanks. So, the next question here is, is there a risk in connecting your work email account on personal devices, such as personal laptops or desktops? So, what I'll say is the information on the device is only protected by what you've put in place there. And generally speaking, on a corporate controlled asset, if you've got a cybersecurity partner, you've got an IT department. You've got policies and programs, and all these other controls in place on that corporate laptop that you may or may not have on your home machine. So, I think it's probably fair to say that most times, machines don't have the same level of trust, as a standard corporate machine does. And so, what I recommend is if your company policy is such that you can access information from home machines, don't download that email. So, if you're checking your email, I think webmail is much safer option. Because those messages don't get downloaded as a whole to your home machine. You're just kind of accessing them temporarily. And then extending that beyond the laptop scenario into a mobile device, or tablet kind of scenario. I'm a big proponent of setting those application level passcodes. So, you might use your fingerprint, or a pin to log into the device. But then you have to reauthenticate to open that email client. I think that's a really nice safeguard. And the last thing I'll mention is working with your cyber and IT folks. It's also possible to keep the email on those tablets and phones in a small encrypted container. So that if something does happen to that device, that data is protected as well. So, there's a lot of things that you can do to mitigate some of that risk. around accessing it from an “untrusted device”.

46:46 **Jay Wiley**: So, while I take the next question, I'm going to go back here to the previous slide. Just so if anybody wants to takedown the phishing address, or any of the phone numbers to contact us, I'll leave that up to you, while I address this next question. So that you can get a chance to copy that down, in case we moved a little too quickly through that the first time. So, the next question is, if a computer has been infected, you take it off the network. You scrub it, you try to clean it up. And it still shows that the malware is there, can you use it, or should it be scrubbed further? And I would say yes. If you've got a known malware on that system, you should totally take it back to bare bones. In other words, clean off the hard drive back to nothing, and reload everything up from scratch. That's really the only way that you're going to get a high level of confidence that nothing is still there. Anything less than wiping it out, that just kind of leaves that doubt in your mind. So, the recommendation there is wipe it and rebuild it. Now, one of the things you can do in advance is have a known, good software image. You got that one CD or DVD that has your operating system image just as you like it, and then that makes it faster to rebuild those machines. So, yeah, I would say you got to scrub that thing and get it back to ground zero, and then reload it if you've got malware on it. And that's, whether it shows that you might have cleaned it or not, just wipe it, just don't even take the chance.

48:36 **Jay Wiley**: Kris, if I could ask you, would you talk a little bit about executive impersonation, social engineering, and some of those concerns. What's to watch out for there?

48:46 **Kris Meier**: Yeah, sure, thanks, Jay. Yeah, that's a topic that is of heightened concern, I think, to myself and my team. We're trying to get the word out on that, so I'm happy to talk about it here. Obviously, we're in a much different environment now. And what I've noticed, in my own day to day, is I get a lot more calls from numbers I don't know, because people are calling from their work cell phone or

their personal cell phone. Speaking from experience here, during the first couple weeks of quarantine, certain cell providers in this area worked much better than others. And so, people were constantly swapping back and forth to get better audio quality on the conference calls and stuff like that. And that creates an environment where it's really difficult to validate the person on the other end of the phone sometimes. And it opens you up to some of that social engineering that might not have happened before. Because if you're sitting in a corporate office, and you're looking at your corporate phone, you can tell with a high degree of certainty that that name calling is probably the name that's on the other end of the phone. Unless someone's sitting in an office building, and then you got other problems, most likely.

And so, I think that the biggest thing I can do is reiterate, validate on a known good number, the person on the other end of that email or phone. And so, what I've taken to doing is, if I don't interact with that person on a day to day basis, I can't tell their voice. So if Jay called me, I'd know it's Jay, and I know all his numbers. But if someone in a different business line is reaching out to me for some advice, and I've not interacted with them before, and they're calling from a personal cellphone, I've just taken to saying, “hey, can I call you back at your office line?” No problem, I'll connect that way, and it’s a quick validation thing that I can do before we get into talking about a sensitive topic. The same thing for email. One thing I'll point out is that fraudsters, a lot of times, will doctor the footer in an email, such that they'll change the callback number to one of their own. And so, when you're validating that request from the CEO, actually came from the CEO, call that person back on a known good number, don't rely on the email footer. And I think, like I said, I think it's all the more important tin the current work environment.

51:11 **Jay Wiley**: Yeah, thanks, Kris. I think I would just add really quickly, we talk about two things that folks in this realm of social engineering and executive personation, they try to use a sense of urgency, they try to get you to do something now, it's got to be done now. We need to answer the CEO now. We need to send this money wire over here now. Those kinds of things. And when you have that sense of urgency, that's something that's kind of raises the hairs on the back of your neck - it gets your “Spidey Sense” up. The other thing is that they're kind of preying on your ability to do your job. We all want to do our job. And they're like, “hey, you might be not doing your job,” or, “you'll be letting me down if you can't get this done,” sort of thing. So those are the two telltale approaches that they try to use in this realm to get you to just kind of blow through any of those “Spidey Sense” things that you've got going off in your mind.

So, another question here is, should you require home devices connected by VPN to have approved antivirus running? Well, I'll tell you that we do a check here at the bank for anyone who's attaching to our network by VPN, obviously, that they have the latest updates running, from an antivirus perspective, anti-malware, etcetera. And so, that is a precondition to connecting to our network. If you're a big corporation, you've probably had that setup, or you have that capability, and it's not too hard. But if you're smaller, then that presents a little bit more challenge. But really, the answer is yes. To some level of certainty, you need to make sure that those things connecting to your network are in a state that you would want them to be in.

53:16 **Kris Meier**: The next question I'll take is, how does multi-factor authentication help? So, I'll take a quick step back, and we say two-factor or multi-factor all the time, I just want to make sure everyone on the call understands. And so, when we say multi-factor, what we really mean is something you know, and that's traditionally a password, and then something you have, and today, that can take on a lot of

different forms. It used to be that we all, especially in the cyber security realm, carried around these hardware physical tokens with a number on a little digital screen that changed every minute. And so, if we had to authenticate to our email or VPN, we'd put in our username, our password, and then that number on the screen, and that was a secondary check. Nowadays, that second factor can take on a lot of different forms. I've got watches that pop alerts, that I can hit a button and fingerprint, and codes that are texted to me, and apps that do it. And so, there's a lot of different ways to execute on that, some more user-friendly than others. But what that gives you, from a protection standpoint, is if your password is compromised in some way, and someone goes to log into your account, without that second factor, they're in. So, if they're logging into your email, and they know your password, they have access to your email. With that second factor, they also have to steal your phone or your watch or that little hardware token - however you're getting that second factor, and that presents, obviously, a much more difficult problem. And it also gives you, as the end user, a bit of an early warning indication that maybe you've got a problem with your password. Because if you see that alert, and you didn't initiate it, you can assume that somebody's guessed your password, or gotten access to it, and it allows you to quickly change that before there's any breach of your information.

55:22 **Jay Wiley**: Cool, Kris, and as we get here, near the top of the hour, I'm going take the last question. And the question is, how do I create a guest network from your internet service provider that you have at home. And so, typically, that's just going to be a tab that's on your router interface. And when you log into your router, it should give you the option there to enable or disable the guest network. And so, you would enable that, you can name it whatever you want, set up the security parameters as you want. And then, having established that guest network, then you come back out and you take your devices that you want to be on that, let's just say you have a network thermostat on there, you would attach it to that guest network. So, you're not just signing up for, as I said earlier, John Smith network, you want that for you and your business connection. And then, John Smith guest network, you could attach your TV to it, and your thermostats, and those kinds of things. So that's an option inside of your router interface, to be able to enable that and configure the guest network.

56:42 **Producer**: Okay, well, with that, gentlemen, Jay and Kris, I do want to thank you for a great session today. Thank you, ladies and gentlemen for joining us today. If we didn't get to your question, we will follow up post-event. You will also receive an email with post-event assets. Finally, we do have a very short survey for you to fill out upon exiting, and we do appreciate your feedback. Again, thank you for your participation, and have a great day.