

# Data Protection is Everyone's Responsibility

February 23, 2021

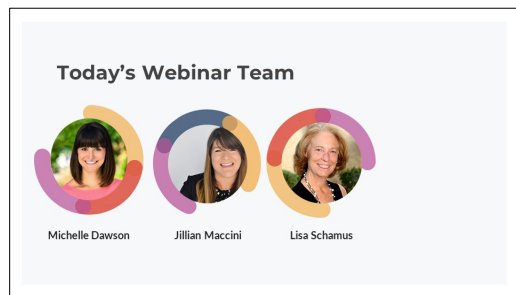
## Transcript

### Slide 1



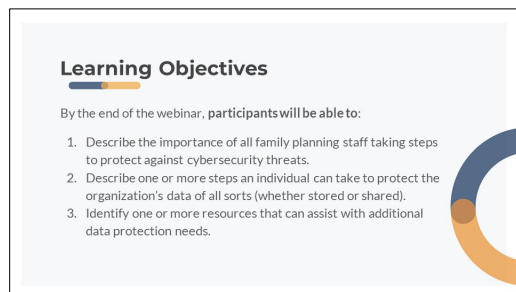
Lisa Schamus: Hello, everyone. This is Lisa Schamus from the Title X Reproductive Health National Training Center or RHNTC. And I'm delighted to welcome you all to today's webinar about data protection. I have a few announcements before we begin. Given the large number of participants, everyone on the webinar today is muted. We do plan to have some time for questions at the end of the webinar today. And you can ask your questions using the chat at any time during the webinar. A recording of today's webinar, the slide deck, and the transcript will be available on [rhntc.org](http://rhntc.org) within the next few days. This presentation was supported by the Office of Population Affairs or OPA, and Office on Women's Health. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of OPA, OWH or HHS. As we begin the webinar, we want to acknowledge that many challenges that Title X providers have worked through the past year and continue to work through in order to provide essential health care services. The RHNTC admires your dedication to your clients and the critical mission of the Title X program. So, thank you. And as more people are working from outside of traditional offices in response to some of the challenges that we're facing today, the content of this webinar is ever more relevant.

## Slide 2



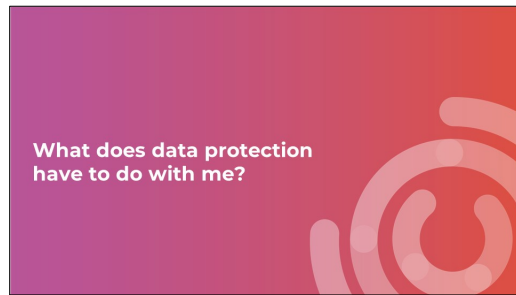
I'd like to briefly introduce our webinar team. Our lead presenters today are Jillian Maccini and Michelle Dawson. Jillian has nearly 10 years of experience as a trainer technical assistance provider. This includes her work on health IT and telehealth as the project director of HITEQ or Health Information Technology Evaluation and Quality Center, as well as a trainer, reviewer and analyst for HRSA's Bureau of Primary Health Care's Uniform Data Set or UDS data reporting, and as a Patient Centered Medical Home or PCMH-certified content expert. Michelle Dawson will be facilitating our question and answer. Michelle provides training and technical assistance to health care providers and health services organizations and specializes in curriculum development and distance learning. Jillian and Michelle are both training in technical assistance providers for the Reproductive Health National Training Center. And with that, I'd like to turn things over to Jillian to get us started, Jillian?

## Slide 3



Michelle Dawson: I think I'll do the learning objectives while Jillian gets her audio online. And so, we will start here for the day. Thank you, Lisa, for that lovely introduction, and welcome, everyone. It's a delight to be here with you today. And I hope that everyone's going to come away from this session with a greater understanding of how and why data protection is everyone's responsibility. Specifically, by the end of today's webinar, our objective is that each of you will be able to, one, describe the importance of all family planning staff, taking steps to protect against cybersecurity threats. Two, describe one or more steps that an individual can take to protect the organization's data of all sorts, whether stored or shared. And three, identify one or more resources that can assist with additional data protection needs.

## Slide 4



Michelle Dawson: Jillian's all set. I'll pass it to her.

Jillian Maccini: Yes, thank you so much. And thanks for helping me out as my computer very suddenly restarted, which is so apropos for this webinar. I'm going to ask Michelle to keep running the slides just in case it happens again. Hopefully that's all right. So, let's go ahead and get started. We'll start by answering the question what does data protection have to do with me, particularly if you use a third party vendor or contractor for managing or storing your electronic records and data, it can feel like it's their job. However, there is much more to it. Next slide.

## Slide 5



In today's webinar when discussing data protection, we're talking about taking measures to secure information stored on your computer, your device, your network and other accounts. Data protection includes the actions and processes that each person takes to protect private information. And this is all private information, whether PHI or grant information or even just your emails and communications. Taking steps to protect data is the first step towards ensuring privacy. Privacy is only possible when information is protected. This is why our mantra for today's session is data protection is everybody's responsibility.

## Slide 6

Key Terms	
<b>Device:</b> Computer such as laptop, desktop, PC, or Mac; smartphone such as iPhone or Android, or other things that conduct activities electronically, such as smart TVs, smart coffee makers, or smart vacuums	<b>Operating system:</b> Manages all of the software and hardware on a device, coordinating to make sure each program running on the device gets what it needs
<b>Hardware:</b> Refers to the actual device or components of the device, such as a computer or smartphone, as well as the wiring, circuitry, and other physical pieces within the device	<b>Software:</b> Refers to programs or applications used by or on an electronic device

First, we need to be sure we're all on the same page with a couple of terms in order for the remaining discussions to be clear. So, stick with me if this is a review for you. First, when we say device, we mean the obvious like computers, laptops, desktop PCs, or Macs. When we say smartphones, these are devices and they might be iPhones or Androids. But it's also all other things that conduct activities electronically. Critically, this includes all things that connect to the Internet, such as smart TVs, smart coffeemakers, smart vacuums, etc. So, not only the things you sort of actively use to connect to the Internet in the traditional sense, but it's also truly all things connected to the Internet. So, when we say device, think about that really expansive definition. And next, an operating system is what manages all of the software and hardware on the device coordinating to make sure each program running on the device has what it needs. The most familiar operating systems may be Microsoft Windows, typically used on PCs. Macs have their own operating system known as macOS. As do smartphones, such as iOS for iPhones. Other devices like your Roomba smart vacuum or your smart refrigerator also have operating systems of their own. Hardware, this refers to sort of the physical device or components of the device that's wiring, circuitry, things, physical aspects within the devices that are part of the device. And then software refers to programs or applications used by or on an electronic device. For example, Microsoft Word, Microsoft Excel, Adobe Acrobat Reader. All of those are software programs. Smartphones have software both in the form of the operating system, as well as apps on the smartphone, for example. And then smart devices, again, have software of their own, the thing that makes them run, the things that makes your Roomba run or your Google Home run or any of that. That's software of its own as well.

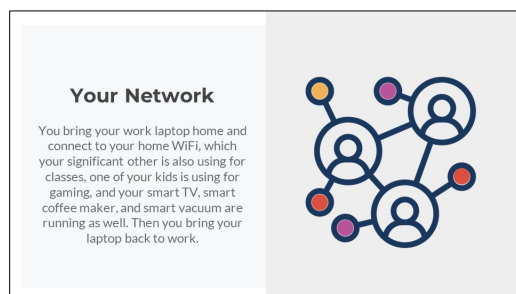
## Slide 7

Key Terms Continued	
<b>Cloud:</b> Using "the cloud" or "cloud storage" refers to using remote servers to conduct a task or to store information. <i>Tip: Something may be "in the cloud" if it requires the internet to access.</i>	<b>Local:</b> Doing or storing something "locally" refers to doing or saving to your own device or servers, without transmitting it to remote servers. <i>Tip: Something is "local" if it doesn't require the internet.</i>
<b>Browser:</b> The software application on a device that is used to access the internet. Common examples include Chrome, Safari, Firefox, Edge (formerly known as Internet Explorer).	<b>Network:</b> All devices connected together through a central node. This can include local area networks where multiple devices can access each other, typically through WiFi or Ethernet cables, such as multiple computers connected to shared printers and servers.

When we say the cloud or cloud storage, this refers to using remote servers to conduct a task or store information. So, for example, when using email online, such as Gmail, that uses the cloud to transmit or store information. They're stored on the server of the email provider, not on your own computers or servers. And so, this might very well be true of data you collect in your organization as well. It might be

stored on a third party server on the sort of vendors server and that's considered in the cloud. Something may be in the cloud if it requires Internet to access. Local, doing something or storing something locally refers to doing or saving to your own device or servers without transmitting to remote servers. So, a tip is something is local perhaps if it doesn't require the Internet. If something saved on your laptop, so you can open it without connecting to the Internet that's being saved locally. And then a browser, I'm sure everybody knows this, but just in case. This is the software application on a device that's used to access the Internet or the application that you use to access a given web page. This might be Chrome, Safari, Firefox, Internet Explorer. Those are all browsers. And then network, this is all devices connected together through a central node. This can include local area network for multiple devices can access each other, typically through WiFi or ethernet cables, and at home or at work. It's also anywhere you bring your device and connect to that shared central node. And this might be WiFi at a coffee shop, connecting to the Internet at the library, etc. Next slide.

## Slide 8




So, let's say you bring your work laptop home and connect to your home WiFi, which your significant other also uses for classes, one of your kids is using for gaming, and your smart TV, smart coffeemaker and smart vacuum are running on as well, then you bring your laptop back to work. In this example, there are at least six devices laptops, phones, gaming consoles, and smart appliances running on your home network. Each with its own operating system hardware and each potentially connected to other networks. So, let's do a quick poll and we will launch that poll now, where we're going to ask which of the following devices are connected to your home or work network? So, you as a participant in this session today, which of the following devices are connected to your home or work network? Meaning they're connected to the Internet or WiFi at your home or work, gaming devices, smart coffeemaker, robot vacuum like a Roomba or Shark, smart TV, smart thermostat like a Nest, smart outlet that allow you to control your lamps from an app for example, smart doorbell or door locks such as a Ring, smart speakers such as Alexa or Google Home, or other devices that are connected to your network. So, select all that apply, and we'll give it just a couple more seconds. And then we can go ahead and share what we see here. Okay. So, 80% of participants have a smart TV. About 50% of have a gaming device. About 50% have smart speakers. And then smart doorbells like a Ring or something like that are common as well. So, these are all things that are on your network that you might not normally think about. You may think about, "Okay, my laptop, my partner's laptop. And that's kind of all we run on our network." But all of these other things that we just pulled on are part of that as well. And this example really shows how our work and our lives are sort of a wide web of devices, networks and so on. Each of which can be a vulnerability to protecting your organization's data or information. Next slide.

## Slide 9

### Your Network


You bring your work laptop home and connect to your home WiFi, which your significant other is also using for classes, one of your kids is using for gaming, and your smart TV, smart coffee maker, and smart vacuum are running as well. Then you bring your laptop back to work.



## Slide 10

### Impact of the Pandemic

- We are more, necessarily, spread out these days, more likely to be working from different locations.
- We are perhaps less in touch with our IT support, as we may not be co-located or may be hesitant to have them come in.
- We may be sharing networks with more people in our households, as children, partners, roommates, and others may all be working remotely.



So, the importance of data protection (we can move forward) during the pandemic has had important implications for data protection in that we're more spread out these days and perhaps working from different locations. Maybe less in touch with IT staff and maybe sharing networks with more people in our households, for example, who might be working or learning remotely. This can result in additional vulnerability or exposure. As a CNBC article from 2020 put it, the surge in work from home arrangements increase the opportunity for cyber attacks. When the pandemic first tick, companies that went from maybe 10% of their workforce working from home went to 90 or 100% working from home, and found that their systems were not designed to take on the increased load to get folks up and running with work from home or remote access to what is needed. The focus was on availability and getting the people the tools and data that they needed to work remotely rather than security. A cybersecurity expert added that with the mass shift to remote workforces, the corporate perimeter has been broken. This is compounded by the reality that most home networks are insecure. And household smart devices are vectors for attack. Next slide.

## Slide 11

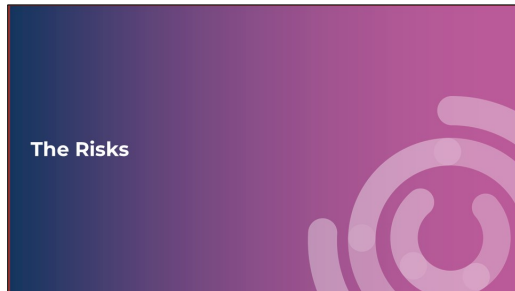
### Impact of Increased Data Collection + Sharing

- Like many things, providing family planning services involves data collection and sharing that has become increasingly granular.
- Regardless of data collection mechanisms (EHR, database, etc.), the need for security of storage and sharing remains.
- Regardless of "ownership," vendors, or type of organization, the need to protect sensitive information remains.



Like many jobs and activities, providing family planning services to clients involves data collection and sharing has become increasingly granular. And again, this is both the collection, the storage and the sharing. So, it's not only the sharing, it's all of those things. Regardless of data collection or storage mechanisms, whether it be an EHR, or a database, or anything like that, the need for security of storage and sharing remains, as each connection is a potential vulnerability to even third party databases. So, specifically, regardless of ownership or where the data resides, for example, whether it's on the cloud or locally, and regardless of vendors or type of organization, the need to protect information remains.

## Slide 12



## Slide 13



So, what are the data protection risks? Ransomware in which files are encrypted and then a ransom is demanded to restore access, accounts for about, is up 90% during the pandemic, according to a 2020 report. Ransomware attacks are complicated by demand for cryptocurrency, which may be unfamiliar and more difficult to track, and really not knowing if data can or would be restored, even if the ransom were to be paid. So, even if your data is not stored locally, meaning that it's stored on the vendor servers or remote server, your network and devices can still be a vulnerability because your login information or other access to those remote servers can be gained through your network. And we'll talk about that a little bit more in a moment.

## Slide 14

### Ransomware in the News

In Oct. 2020, a cyberattack devastated the University of Vermont Medical Center's IT systems. The first indication of the attack was when various applications stopped working. There was no overt message, so for several hours it was not identified as malware.

["We got taken down": UVM Medical Center says cyberattackers were likely](#)



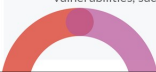
So, this story was in the news quite a bit, and I'm sharing details here from the Burlington Free Press. In October of 2020, a cyber attack devastated the University of Vermont Medical Center's IT systems. The first indication of the attack was when various applications stopped working, sort of just seemed to stop working. There was no overt message. There was no clear sign that this was malware or ransomware. And so, for several hours, this was not identified as malware. After about two hours, investigators found a file with the contact information for the attackers. There was not a clear ransom demand, but it was assumed that if they contacted the information provided, there would have been a ransomware demand. At that point, the hospital realized that it was a malware-ransomware situation and moved immediately to cut off access to its systems and the Internet. By cutting off access, the medical center was able to prevent malware from infecting vendors and other hospitals, because remember, accessing one link in the chain provides access to the whole network. So, it prevented it from infecting those vendors and other hospitals in the UVM Health Network. And the hospital also took Epic, its EHR system, offline. The cyber attack had two major impacts. First, the malware encrypted the files and data behind all of the hospital's infrastructure and applications on its servers. Second, the attack deposited malware on more than 50, I'm sorry, 5000 computers and laptops used by the hospital. So, remember, it did all of these things without anyone noticing and before it demanded anything. The hospital had to move to paper for nearly a month. Next slide.

## Slide 15

### Ransomware Transmission

The malware that takes a system ransom can be transmitted in a number of ways:

- E-mails posing as legitimate business or including tempting links
- Malware acting as legitimate update requests
  - Phony anti-virus programs patches and updates
  - Phony Windows system updates
- False "You've got a virus" notifications
- Gaining access by exploiting known network or security software vulnerabilities, such as unsecured devices or code vulnerabilities

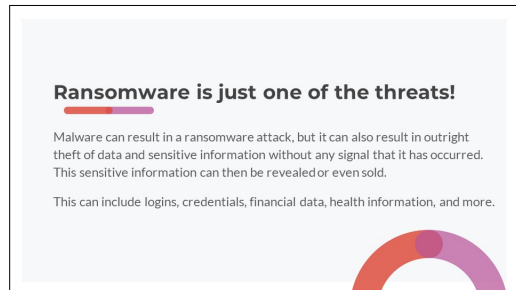


Ransomware can be transmitted a number of ways. It can be emailed posing as legitimate business or tempting links, we'll talk about that in a little bit. It can be Trojans acting as update requests. So, one of the things that we'll talk about today is the importance of updating all your operating systems and software regularly. But it's important to make sure we're doing that in the most legitimate way possible so that we don't fall for these Trojans acting as update requests. Also, antivirus program patches and updates or faux antivirus program patches and updates or false "You've got a virus" notifications. I think we've all gotten that pop up when we went to a website that we thought was legitimate. And then you



get a pop up on your screen that says you have a virus click here. That type of thing can be how this gets installed on computers or in networks, or by gaining access through exploiting no network or security software vulnerabilities. This is when we're using a software that actually has a backend vulnerability and the malware is allowed to sort of infiltrate everybody who's using that software. Next slide.

## Slide 16



Ransomware specifically involves taking money. But really that's just one type of cyber attack, and really just one reason that there may be a cyber attack. There are many other types of attacks for which malware is used. These include destructive attacks in which data or networks are just destroyed, sort of just for the fun of it or for malicious intent, whatever that is, or what's called island hopping, where attackers exploit the weaknesses of smaller organizations in order to move laterally and target larger organizations who may be vendors or service providers for smaller organizations. So, really, this island hopping is sort of what we talked about before where a bad actor may not be going after your organization, but maybe going after all organizations who use a certain vendor or software so that they can attack that vendor and software, for example. Also, being an organization that may have money, may have sensitive information, or that people oppose for some reason can increase the likelihood of being targeted by cyber attacks. And remember, you might not even realize that an attack has taken place. The malware may not be immediately apparent, and there may not be anything clearly stolen or broken, as we talked about in the UVM examples.

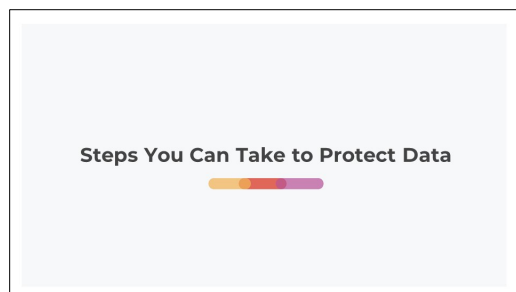
## Slide 17



So, what examples of hacking or cybersecurity breaches have you heard about? Please chat in. And I'm certainly not asking you to name names or share anything terrifying that has happened to you. We're really want to hear some examples of what you've heard of, of security breaches, and how that played out. So, please chat those in and we'll keep an eye on the chat. So, somebody said the city of, so, a city had an issue. Yeah, the Experian breach. That's a good example. There's a been a number of retailer breaches. We think about the Target breach or the Home Depot breach. A number of cities that have

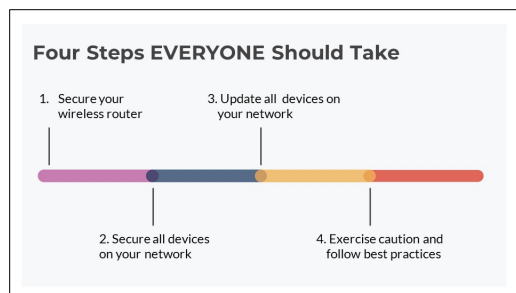
been mentioned, they had to pay for those ransomware. I think we heard about Baltimore in the fall, I believe it was, was locked out of their systems for many weeks. Some hospitals have had their data breached multiple times in the past couple years. There was a time where PlayStation servers were hacked and couldn't get online for about a month. Wow. A local factory had a ransom demand. A university in Colorado, county government, Blue Cross Blue Shield. Somebody's university had to move to a double ID system due to a university wide data breach, yeah, absolutely a two-factor authentication. We're not going to talk about that today. But that is a great tip. Great, thank you all for chatting those in. Let's go ahead.

## Slide 18



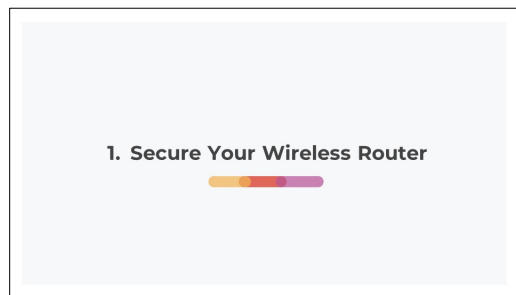
So, hopefully, we've persuaded you that the cybersecurity threats exist. And those examples that you all just shared really demonstrate how much we've all seen these in real life. And hopefully, you agree that protecting against these things is critical. So, let's talk about those steps that everyone can take.

## Slide 19



So, we're going to talk about each of these four steps one by one. It's going to be secure your wireless router, secure all the devices on your network, update all the devices on your network, and then exercise caution and follow best practices.

## Slide 20



So, first, securing your wireless router. Let's talk about that.


## Slide 21

### Router Software and Password

Be sure the router software is up-to-date and password has been changed.

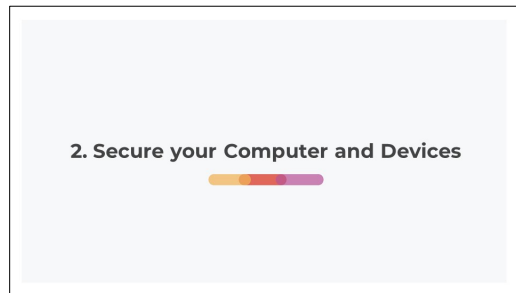
- If you know your admin login for your router, then use that to log in to your router settings. Once logged in, check for software updates and update the router password, so it is NOT the default password.
- If you do not know your admin login, then first, find the brand name on the side or bottom of the router itself. Then, search the internet for updates (e.g., "update netgear router"). Opt for the brand's website over other options.

Be sure the WPA2 data encryption is set as your security type. This can be updated in the router settings and can be checked in Network Properties on your computer by going to Wireless Network Properties and looking at "Security Type."



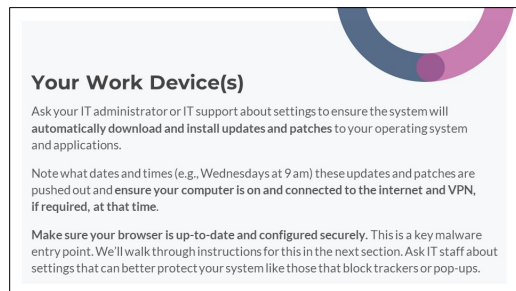
To be sure that router software is up to date, you want to start by finding the brand name of your wireless router by looking at the side or the bottom of it. Pick up your wireless router that you have to reset when you have storms, like we've all had in the past couple weeks, and look at the sort of side or front of it. And there should be information about how to actually log in to the router itself. If there's not and usually what it is, is it's sort of a web page and then an admin login and password. If there's not a web address on the router itself, then you can start by searching for how to update it. Search for update NETGEAR router, or you can go back to the manual if you have that or reach out to your service provider. For example, if you have your router through Spectrum or Comcast, you can reach out to them specifically. You want to be sure that you are not using the default password for your router. Often, routers come with a preset password which may be printed on the side or bottom of the router. Usually it's like two words and three numbers. If you're still using that password for your WiFi network, it's time to change it. Use the router address, again usually written on the bottom or side of the router, and log in with the current username and password. Once you're logged in to the router, you'll have the option to change the password. And really, we recommend changing this password somewhat regularly as well as the name of the network if that's possible. You want to be sure that WPA2 data encryption is used. This protects from eavesdropping where bad actors can sort of monitor traffic on your network. Check this by going to your wireless network properties on your computer and looking at security types. And you can see in the screenshot here, that orange box is the properties. And if you click on that and scroll down to security type, you'll see if it's WPA2 as your security type. If it is not currently set to WPA 2, then you need to change your settings on your router. So, as discussed, you'd log in to your router to make that change. This isn't something that you could change in your WiFi settings on your computer directly. And these are just initial steps. At the end of this presentation, we'll provide a link to a piece that provides several more tips and more guidance on securing your network.

## Slide 22



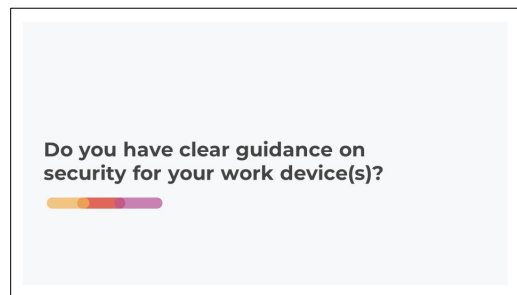
Securing your computer and devices. We can go to the next slide.

## Slide 23



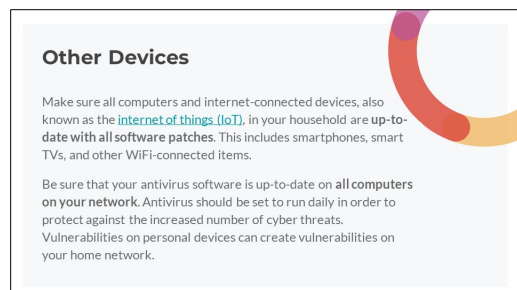
So, you want to make sure that you ask your IT administrator and IT support about settings to ensure the system will automatically download and install updates and patches to your operating systems and applications. And it's also really important to understand when this happens, does your computer need to be on? Does it need to be awake? Sort of what can you expect? Does your computer need to be restarted? So, for example, is it that your patches are pushed out by your agency at 9:00 AM every Wednesday, and therefore your computer needs to be on and awake at 9:00 AM and is going to need to be restarted after those patches are pushed to it. You may have a snooze option that you get to use a number of times. But making sure that you understand when those happen and what you need to do. And then making sure your browser is up to date and configured securely. This is a key malware entry point. We'll talk about instructions for this in the next section. But it is really important to ask IT staff about settings that can better protect your system, such as those that block trackers or pop ups. And making sure that you are following whatever the work guidance or the IT administrator guidance is. I know for us, it's a real pain. My computer restarted right before this. And I think that was related to a patch that we got. But making sure that those go through is critical for protecting our information. Next slide.

## Slide 24



So, do you have clear guidance on security for your work devices or what's expected? What does that look like for you? So, someone chatted in at some point, "Can you address hotspots?" Tell me more about what you mean? And I'm sure we can. So, do you have clear guidance for your work devices? When those need to be on, whether it needs to be connected to the Internet? That type of stuff. All right, I've got one yes. And if not, what do you feel like you don't know? Okay, I've got one no. We're at 50-50 at the moment. And so, if you don't know, and the question is really do you know when your patches and updates are released, do you know if you need to be connected to the VPN in order to get those things, that type of thing. So, if you do know, that's great. If you don't know, this is definitely the chance to speak to your IT administrators about what exactly is needed for your work devices and what needs to happen to make sure that that stays up to date. Do you need to connect to the VPN? Do you need to remain connected to the WiFi, that type of thing? Next slide.

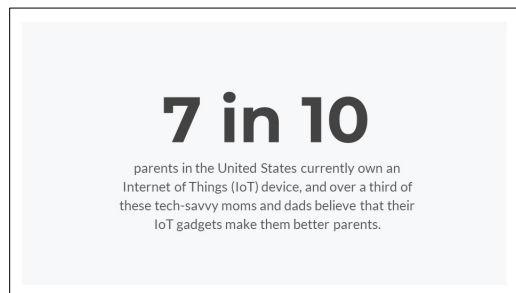
## Slide 25



So, let's think about all the other devices that need to be updated as well. Think back to our earlier discussion of devices. Remember that this includes all Internet-connected devices on your network, computers, smartphones, gaming devices, smart TVs, WiFi connected printers, robot vacuums, and everything in between. These all come together to create what is called the Internet of things or IoT. So, if you've ever heard the term IoT devices, this is what it's talking about. There has been an increase in IoT-based cybersecurity attacks. One really good example is the Ripple20 attack, which you can Google or there will be a link in the notes on the slides that use Internet of things devices in order to attack networks. And consequently, the security of all IoT devices is needed to protect information on your work computer. Again, we'll talk about how to update these in the next section. Smart kettles, smart coffeemakers, smart refrigerators, these are all potential vulnerabilities. You really should be sure that all IoT devices are updated regularly. And again, we'll talk about that a little more in the next section. And then the other thing to be sure of is that you are updating your antivirus software on your computer, as well as all other computers on your network. So, this might include your computers that

your partner is using, or any children are using for schooling, things like that. Some kids got laptops from school. Some kids are using laptops way more now than they ever had before. So, running that antivirus on those maybe daily in order to protect against the increased number of cyber threats that we're experiencing. And it's important to remember that vulnerabilities of personal devices can create vulnerabilities on your home network, which then can be brought into work if you bring your computer back into work and connect to that network, for example. Next slide.

## Slide 26



So, let's dig more into this Internet of things. So, when thinking about the Internet of things, or IoT, as I said, in addition to those smart devices that we already talked about, there are many, many more examples. For example, 70% of parents in the U.S. currently own an IoT device sort of related to their kid. And over a third of these tech savvy moms and/or dads believe that their IoT gadgets make them better parents. While they may very well be, really many IoT devices are super convenient, they also introduce more vulnerability to the network.

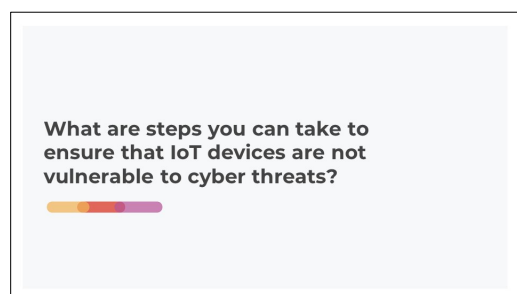
## Slide 27

<b>Which of these are Internet of Things (IoT) devices?</b>	<p>Jean has a new baby. Among the things that Jean brought home in preparation for the baby's arrival include:</p> <ol style="list-style-type: none"><li>1. An electronic wipe warmer</li><li>2. A sleep sensing/biofeedback onesie</li><li>3. A bluetooth bottle warmer</li><li>4. An automatic dimmer light</li><li>5. A stuffed animal that can record and play back voice messages that can be sent over the Internet</li><li>6. New iPhone app to track feedings</li><li>7. WiFi baby monitor</li></ol>
---	--

So, which of these are Internet of things devices or IoT devices? So, in this example, Jean had a new baby. Among the things that Jean brought home in preparation for the baby's arrival, they include an electronic wipe warmer that can be turned on and off with a button on the front and has automatic shutoff. They include sleep sensing or biofeedback onesie that sends data to a smartphone app. They include a Bluetooth bottle warmer that can be started or changed from a smartphone over WiFi, an automatic nightlight that can be changed based on the time of day, letting baby know when it's time to rise, a stuffed animal that can record and playback voice messages that can be sent over the Internet, a new iPhone app to track feedings, and a WiFi baby monitor. So, let's do a poll. Which of these are IoT devices or are part of the Internet of things and select all that apply. And while everybody's answering that, I'm just going to address one question that came in through the chat. So, a question came in through the chat, advice for a small nonprofit with no real IT department, how can we remain as safe as

possible? Definitely all of these tips that we're talking about here, we may be talking about them for home and office, they are certainly applicable for both. So, anything that we advise that you would do at home also could be used in a small office, or something where there's not an IT staff. And there are also going to be a number of resources that we're going to share at the end. So, let's see. What did folks say were the Internet of things devices. Okay, so number two and number seven were the big ones that were identified. That is two of them, for sure. So, two is correct. The sleep sensing onesie sends biofeedback information over Bluetooth. So, this is indeed part of the IoT. The electric wipe warmer that can be turned on and off of the button on the front and has an automatic shut-off. That's electric, but it's not connected to the Internet. So, that is not part of the Internet of things. But the sleep sensing biofeedback onesie is part of the Internet of things because it shares information back and forth. The Bluetooth bottle warmer that can be started from a smartphone. Yeah, that's correct. That is an IoT device. It sends information when the bottle is ready for example. The automatic nightlight is programmed and sensing, but doesn't connect to the Internet specifically and doesn't send or receive any information, so that is not IoT. The stuffed animal that parents, grandparents or others can send recorded messages is indeed an IoT device because it sends and receives these voice messages over the Internet. Note that if the stuffed animal just recorded things directly to like a tape inside like Teddy Ruxpin when I was a kid, then that would not be IoT. That would be just stored locally. A new iPhone app for feeding is not IoT because there's no device sending information. It's just storing information on the smartphone. You or Jean as the person is just entering the feeding. So, it's just the smartphone itself. It's not an IoT device separate from that. And then the WiFi baby monitor is IoT because it's transmitting information, video feed, in this case, via WiFi to monitor downstairs, for example. And so, again, remember, it's not just baby stuff. By the end of 2018, more than 23 billion devices were connected to the Internet worldwide. Many of these IoT devices feel so distant from a computer, it can be hard to understand how they can put us at risk, particularly smart devices that perform a simple function like a smart coffeemaker, for example. These are IoT devices as well that connect to your home network. Next slide.

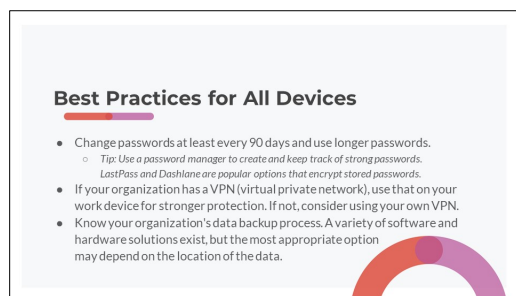
## Slide 28



So, we haven't discussed this yet. So, this is really just a baseline knowledge check. So, don't worry if you don't know the answer. But the question is, select all that apply, what are the steps that you can take to ensure IoT devices are not vulnerable to cyber threats or to protect any IoT devices against cyber threats? And again, you may not have any of these, but it's worth knowing as they become more and more prevalent. So, register the device, keep the software updated, turn the screen off and camera off so it's not recording you. Read the reviews online to see what others say, and/or unplug it when it's not in use. So, which of these are ways to minimize vulnerabilities from IoT devices? Okay, let's see what we got. Yeah, so one register the device, yes, definitely, because that's how you get your automatic updates. And we'll talk a little bit more about that. Keep the software updated. Yes, definitely. I see 94% of people got that. That's great. Both of those are absolutely key. Number three, turn off your screen or

camera so it's not recording you. No, this actually doesn't make it less vulnerable to cybersecurity. There might be other good reasons to do that. But it's not specifically related to minimizing the vulnerability of that tool. So, that's a distinction that's important. Number four, read the reviews online to see what others say. No, this isn't a best practice because who knows who those other reviewers are, right? We hear all these stories about these sort of fake reviews on Amazon or wherever. And so, similarly, in this situation, those are not necessarily a source of truth for us. And then lastly, unplug it when not in use. Yes, absolutely. And we'll talk about that in a moment. And just a couple other tips are to stick with known manufacturers and Googling those manufacturers to make sure that hasn't been anything in the headlines, where they've been breached or anything like that. You want to avoid purchasing those smart devices from lesser known makers, who are less likely to properly invest in security measures. Remember, your average stuffed animal company is not super invested in security. So, that Internet connected teddy bear comes with sort of additional risks. And we'll talk about a couple other best practices in a moment. We can go to the next slide.

## Slide 29



So, best practices for all devices, all situations is to change passwords regularly. Every 90 days at absolute minimum, more like 30 or 45 is even better and to use longer passwords. A couple more characters can increase the time required to crack your password from seconds to hundreds of years. So, adding four more characters to your password can make that change. A secure password that mixes title cases or capitalization in lowercase and uses a mixture of characters and symbols is key. And default passwords as we talked about with the routers are way too easy to find. You can actually find default passwords for most common router types just on the Internet, just for the Google search. I know these passwords can be really hard to remember. We've got a million passwords for everything we use every day. And so, a couple tips are to use a password manager to create and keep track of strong passwords. LastPass and Dashlane are popular options to encrypt stored passwords. Encrypted means that the data has been converted to code such that if someone were to hack in and get that data, it would still be scrambled or unreadable. So, when we say encrypted, it means that even if somebody can get into it, typically they're still not able to actually access the information. So, using a password manager makes the management of all these passwords much easier. If your organization has VPN or a virtual private network, use that on your work device for stronger protection. And what that does is it sort of cordons your computer off from everything else that's on the network because you're running your traffic through that VPN rather than through that network that's sort of being shared by everybody. If your organization doesn't have a VPN, consider using your own VPN. You can find reputable providers online. And there are some affordable options. If you need to work in a public location and are accessing sensitive information, you should always be using a VPN. To find those reputable technology vendors of any sort online, you're going to want to start by using websites such as CNET or Consumer Reports. So, websites that are legitimate and have a long history of reviewing and verifying software, you don't necessarily want to do just a standard Google search for those. And so, again, that's CNET, so C-N-E-T, or



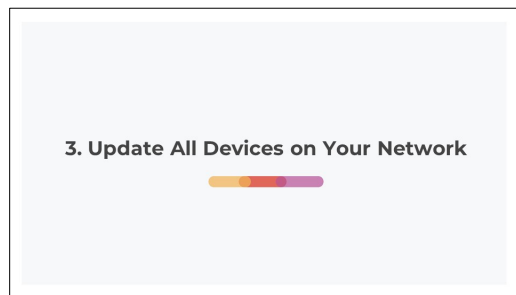
Consumer Reports are two good places to start. And also know your organization's backup processes. A variety of software and hardware solutions exist, but the most appropriate option may depend on the location of the data. If you're a very small organization, you still want to make sure you're backing up your data, even if it's just on your own local external hard drive on a daily or nightly basis for example. This makes it so if you are locked out of your device, you're attacked by ransomware or a destructive attack, you can still access that information. Next slide. So, shared networks. I just gave a couple of tips and thoughts about shared networks.

## Slide 30

<b>Shared Networks</b>  Nylah just moved to a new place, so while waiting for the cable company to come and set up the internet, Nylah goes to a nearby coffee shop to get some work done. Nylah feels like there is no sensitive data on her laptop, since she doesn't keep client spreadsheets on it and uses a third-party vendor for client data.  As such, Nylah feels comfortable logging on to her computer and then logging onto the WiFi, so she can send a few emails, get some paperwork done, and check the client schedule for the day.	<b>What should Nylah do?</b>  <ol style="list-style-type: none"><li>1. Go ahead, there is no sensitive information being exchanged.</li><li>2. Just stay under an hour, so a hacker doesn't have time to infiltrate.</li><li>3. Look around and see if anyone else is on their laptop. If no one else is, then there is no risk, so she can go ahead.</li><li>4. Confirm the name of the WiFi network with cafe staff, connect, and log into VPN before anything else.</li><li>5. Don't use the public WiFi, just wait for the internet to be installed at home.</li></ol>
--	--

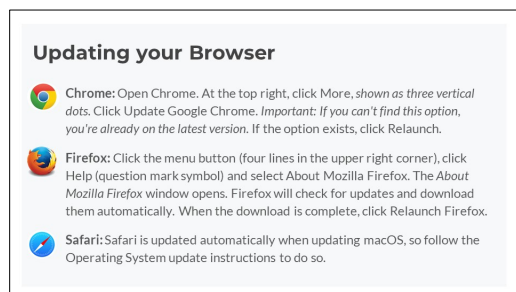
And so, let's look at this example. So, Nyla just moved to a new place. And so, while waiting for the cable company to come and set up the Internet, Nyla goes to a nearby coffee shop to get some work done. Nyla feels like there is no sensitive data on her laptop, since she doesn't keep client's spreadsheets on it and uses a third party vendor for client data. As such, Nyla feels comfortable logging into her computer and then logging on to the WiFi so she can send a few emails, get some paperwork done and check the client schedule for the day. What should Nyla do? Should she go ahead? There's no sensitive information being exchanged so there's little risk. And we're going to launch a poll for this. It should be fine for her to check her email on the public WiFi and logging into the clinic scheduling system is okay too. Just stay under an hour so the hackers don't have time to infiltrate. Number three, look around and see if there's anyone else who's on their laptop. If no one else is and there's no risk, so she can go ahead. Confirm the name of the WiFi network with the cafe staff, connect and then log in to her VPN before doing anything else. Or lastly, don't use the public WiFi just wait for the Internet to be installed at home. So, which of those is the best way to go? And while we're waiting for that, I see somebody asked which devices were IoTs. You will see that on the slide, but it's basically everything that shares information via the Internet. Mary, that's an answer to your question. And Chris said, you can use a mnemonic or acronym of sorts for a password. And that's a great tip as well. So, everybody got the answer right. So, at a minimum, Nyla should do number four, which is to confirm the name of the WiFi network and the password with the cafe staff before connecting to make sure she's not connecting to a spoofed network or something that has named itself something similar so as to get people's information, and then using that VPN before doing anything else. And then in a perfect world, we wouldn't use the public WiFi, we would just wait for the WiFi to be installed at home. But number four follows the best practices. Next slide.

## Slide 31



So, update all the devices on your network. And again, remember that all the devices on the network are potential entry points for bad actors. So, keeping all of those up to date minimizes the vulnerability for all devices. We're going to buzz through the next couple of slides, but they have important information for your reference.

## Slide 32



So, the next slide, most browsers will alert you when your browser needs to be updated. So, the key is to go ahead when prompted for updates in your browser. This often shows up in the upper right hand corner of the browser or when you launch the browser, it will say there are updates. Next slide.

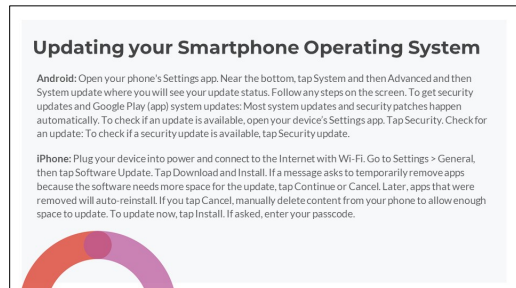
## Slide 33



What happened there? Updating your operating systems. So, updating your operating system for your work computer, that might be done by central IT support. And again, the key there is to discuss patches or updates that are pushed out on a regular basis. But remember, it's critical to keep everything on the network updated. And so, check for those updates using these tips. And again, you'll be prompted for

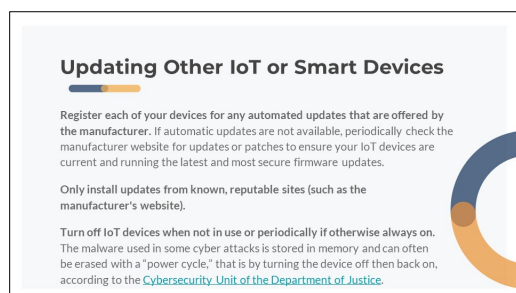
these updates in most situations. But these tips here can make sure you are up to date now and can keep you up to date. Next slide.

## Slide 34



And again, smartphone operating systems will usually be prompted to automatically. We've all seen that pop up that says XYZ update will be made tonight. You'll want to make sure that you're connected to power and WiFi regularly to be sure that this happens. Sometimes you have the option to put off an update, but doing that does create a bigger potential vulnerability because security patches are sent through those updates. And similar with apps, all of the apps on your smartphone when you get those updates for those apps, those typically have security fixes as well. The only trick that can sometimes happen with your smartphone operating system is that you might get a message asking you to temporarily remove apps because you don't have enough space. And you can just allow that and they'll uninstall and reinstall automatically. Or you can click Cancel to manually delete content and make space, but it is important to actually do that. So, Chris asked how can people tell if an update request is legit? So, you can actually go follow these steps that are on the screen. So, rather than just clicking OK, on any pop up that you get, you can follow the update instructions on the screen here. It actually tells you how to go into the system and check for updates manually rather than just clicking OK on anything that pops up. So, that's how you would know it's legit. Good question. Next step. I'm sorry, next slide.

## Slide 35



For all the IoT devices that we discussed, they need to be updated as well. You'll want to register each of these devices, which you may have already done when you were setting it up. For example, if you have a Roomba or something like that, you had to make an account for it. That is registering it. If you have a Roku or smart TV, similarly, you had to register it when you set the whole thing up generally. If not, then you can go to the manufacturer's website to update and actually search for updates on their website. And sometimes you just have to put the serial number in from your device. The other thing to note is it's also a best practice to turn off IoT devices when not in use, or at least regularly, so as this power cycle

can clear the memory. So, for example, if you have a smart coffeemaker, you may want to turn it off or unplug it after your morning coffee and then plug it back in at night rather than leaving it on all the time. This is true, whether you're working at home, in an office, in a clinic, etc. Next slide.

## Slide 36



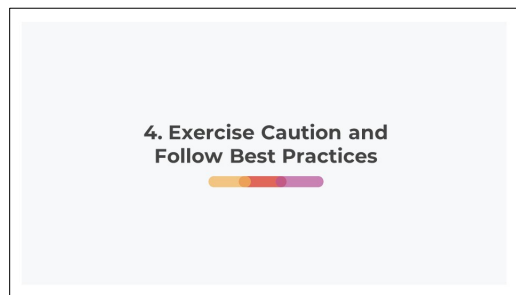
So, let's use the example of the Internet connected stuffed animal that allows loved one to send voice messages. When you purchase or receive it, you first want to look at the information that comes with it for registration information. You want to register right away. If that ship has sailed, which it has for many of us with many devices, then take a moment to figure out who the manufacturer is by looking at the tag or the box or something like that. Go to their website and check for software updates. And then at the very least, unplug it or completely power it off regularly. As mentioned on the last slide, the Justice Department has said this can thwart attacks. This also has the additional benefit of making it so that particular device is less active, so, there are less active and open devices on your network, each of which again can act as an entry point. If all of our smart devices are on all the time, then that can be 10, 20 or more devices on the network, each a potential vulnerability. And remember, if someone can get into your WiFi network through hacking your baby monitor, then they can potentially access all of the other devices and information on your network, including logins, sensitive patient or client information, grant information, financial information, etc. Next slide.

## Slide 37



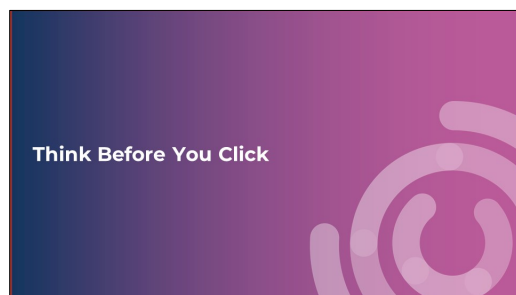
So, how could you set up reminders to check these things regularly. This is one of the potentially less exciting parts. But generally, you want to make sure these things are done at least quarterly every 90 days, as we said. And so, you could do this with anything else that you do quarterly. You could just set a regular appointment in your calendar. You could do it every time the seasons changed on the solstice, you could spend a little time on your cybersecurity updates. Making sure that you have something consistent really makes it easier to do it. Next slide.

## Slide 38



And so, the fourth and last thing is what we've covered so far is really just what each individual in an organization can do to protect the organization from cybersecurity threats.

## Slide 39



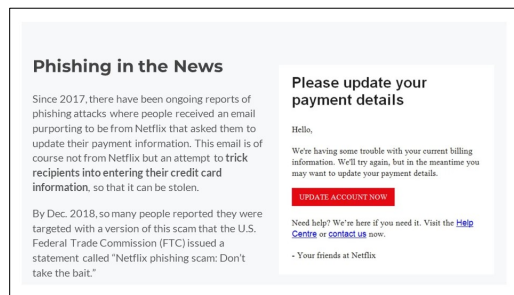
There's also a number of sort of cautions that we should all take and best practices that we should all take. And these can all be summarized by think before you click as the next slide says. Next slide.

## Slide 40



So, phishing attacks we mentioned briefly earlier, phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. This is usually performed through email, but also can be done via text or social media as well. It usually involves getting the recipient to open a fraudulent link or attachment. And the goal is to steal confidential information or to install malware on the victim's device. In 2020, there were many examples of phishing attacks that were COVID-19 related such as masquerading as being from the CDC or phony test results to get somebody to open those emails. Next slide.

## Slide 41



So, one example of phishing in the news. Since 2017, there have been ongoing reports of phishing attacks, where people received an email purporting to be from Netflix to update their payment information. And it was so pervasive that by the end of 2018, the FTC released a warning about it. This is just an example of how individuals can be targeted and duped. And note that this might have been just steal credit card information, but it also could be that when you click that update account information, it actually just downloads malware to the computer. A number of things are possible through this type of phishing email or targeted phishing. Next slide.

## Slide 42



So, a more specific example is spear phishing, which is phishing, but even more highly targeted. Spear phishing targets individual organizations for infiltration. In one example from a newspaper in I believe it was Florida, someone sent an email to a city department that made it look like it was from a current construction contractor working with the city. The email requested payment for services via EFT. While the email was phony, the underlying invoice was legitimate. So, this misdirected legitimate funds to an illegitimate account. We've also seen things like this with the DNC email hack that was a spear phishing attack, and has also been done to famous people and released some information from famous people, etc. And again, in this situation, no one knew what had happened because the invoice itself was legitimate. It just had them transfer the money to an illegitimate account, so nobody even noticed until that contractor asked for the real payment. Next slide.


## Slide 43

### Stop Phishing Attacks

Call or otherwise confirm the sender before you click.

Look for consistency. For example, if an email is titled RE: Your budget question, then there should likely be an email thread below that this is a response to. Similarly, if you get a test or vaccine reminder from CVS, it should be from the same address as previous communications. Double-check for consistency before clicking.

Even better, **don't click at all** and instead go to the site or account and log in, and then confirm the information there.



So, to stop phishing attacks, the best practice is to call or otherwise confirm the sender before you click. Also, be suspicious of unsolicited phone calls, visits, emails, etc. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company. Don't provide any personal information or information about your organization, unless you're certain of a person's authority. Don't reveal organizational or personal information and don't respond to email solicitations for this information. Don't click on links sent in emails. You can always go and follow up with the person it purports to be from and provide that information if need be. But just clicking on a link in an email without verifying that first is that real phishing issue. Don't send sensitive information over the Internet before checking a website's security and pay attention to the URL or address of a website. Look for URLs that begin with HTTPS. Next slide.

## Slide 44

### Make Good Cyber Choices

- Do not use personal email account to send or receive company emails.
- Don't forward work emails to personal email accounts.
- Do not send or share data through personal file sharing tools (e.g., a personal Dropbox account).
- Do not discuss organizational matters through or on social media.
- Be sure to use a secure, encrypted connection like a VPN when communicating or accessing client or client data.
- Make sure work devices such as your computer and/or smartphone are secured in the home at all times.



Just generally use good cyber choices. Don't use your personal accounts for work. Don't send data through personal file sharing or email or via social media. Make sure that your devices are secure, physically secured at home. Next slide.


## Slide 45

### Educate Those Around You

Every member of your household, internet-connected device, or wireless connection is a **potential entry point** into the organization's network.

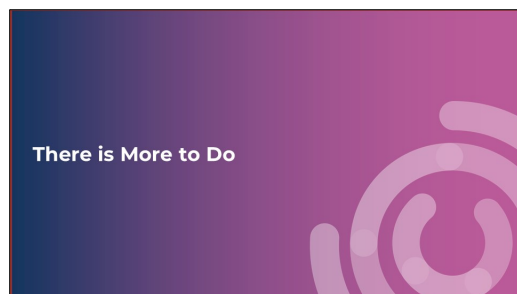
Talk to those in your household about how important it is that your **network provide a safe and secure place** for you to conduct your work.

If you have shared your password for your wireless network with family and friends, change it. **Update the password and then confirm with people that their devices and systems are up-to-date before passing out the new password.**



And then one last thing. I've stressed a number of times that the network is everybody in your home. So, every member of your household, every Internet connected device, and every wireless connection is a potential entry point into the organization's network if not actively protected and trained. If you have shared a password for your wireless network with family, friends, visitors, guests, then change it, not because you mistrust them but because they could be using compromised equipment on your network. You can create a separate guest login in lots of routers and things like that. That is an option if you want to be able to provide people the WiFi. So, do update that and then confirm with people that their devices and systems are up to date before passing that new password out. Next slide.

## Slide 46



So, what we've covered so far is really just what each of us as individuals in an organization can do to protect the organization from cybersecurity threats. Of course, there's much more to be done. These additional components include privacy and security policies that further protect the organization as a whole, ensure the continuity of services and access to records and comply with regulatory requirements. Those are all essential as well. Next slide.

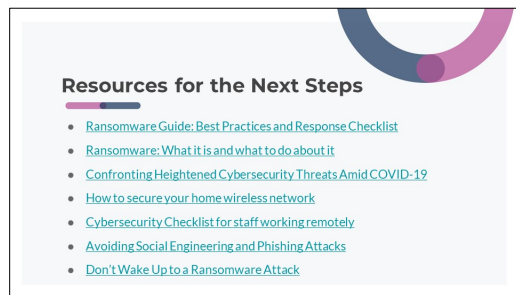
## Slide 47



None of what we've discussed here replaces the need for strong organizational policies and ongoing compliance with regulatory requirements. There are additional steps needed to fully protect data in order to ensure privacy and security. And it's critically important that IT be aware of some of those best practices. Cybersecurity and Infrastructure Agency, also known as CISA has some very helpful ransomware guidance that provides detailed actionable information on preventing and responding to ransomware. And unfortunately, security incidents do happen. These things happen even if we do everything we can. So, understanding how to respond when it does happen is also really important.



## Slide 48

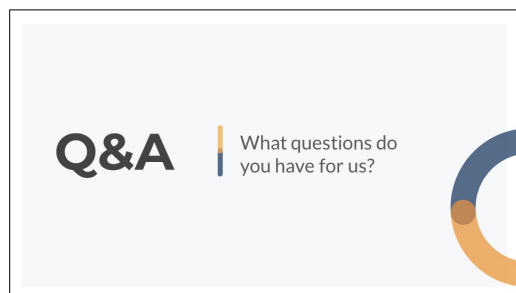


So, resources on the next slide, and you should have received these slides before this presentation, and you'll receive them again after I believe, and many of these help with those other things as well.

Resources for next steps:

- <https://hackablepodcast.com/episodes/internet-of-toddlers>
- <https://arstechnica.com/information-technology/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments/>
- <https://nymag.com/intelligencer/2018/05/why-using-smart-wearable-baby-monitors-was-a-mistake.html>
- <https://www.techdirt.com/articles/20170228/05292336807/smart-stuffed-animal-company-leaves-voice-other-data-millions-publicly-exposed.shtml>

## Slide 49



So, I think we've got time for a couple questions. Michelle, do you want to queue those up or Lisa, was it you? I apologize.

Michelle Dawson: Yes, absolutely. And so, our first question is with regards to hotspots. And the person said, "I don't have a WiFi router, so I use a mobile phone hotspot for Internet. How does that impact security?"

Jillian Maccini: So, it's good in that it's private. But again, it requires keeping that updated. So, just like you have to keep your phone updated and your apps on your phone updated, that becomes all the more important if you're using your phone as the hotspot to be connected to. But I will say if I'm out in public, I hotspot on my phone as being better than public WiFi. So, if you're looking for a scale, that might be helpful.

Michelle Dawson: Our next question is, "Is there something bad about forwarding an email from work email to home email, if we verified the sender?"

Jillian Maccini: Not necessarily, no. As long as you know what it's from, the content, and it's not breaking any rules around disclosure or things like that, that's probably fine. Keeping things separate is good in a number of ways. But you're probably not creating a security issue if you know where the email was from and you know its content.

Michelle Dawson: Thank you. We have one minute, so if you have questions, very quickly.

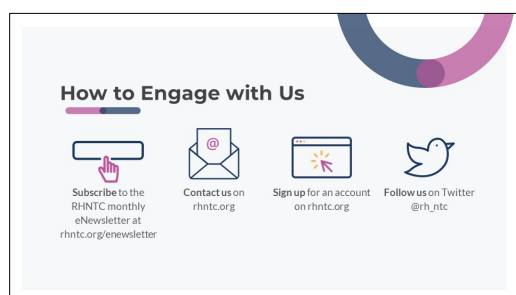
Jillian Maccini: Sorry, I closed the chat. And so, I will go back to one other question that ... So, I had mentioned earlier that one of the ransomware, one of the ways that ransomware can happen is through fake alerts that you get.

Jillian Maccini: And so, then somebody said, "How can you tell if an update request is legitimate?" Great point. One, you probably have seen many of these things before. So, if it looks different, or if it's flashing, or if it's really aggressive, Microsoft and Mac are not known for making super aggressive flashing things. That might be sort of a red flag. Let me check and make sure that this is legitimate.

Jillian Maccini: And also, if it's happening when you go to a specific web page or something like that, that's a red flag that it may not be legitimate as well. These things are generally going to happen. You're going to see them in the normal places that you see them. And again, you can sort of avoid all of that altogether by just going through those update steps that we had on the slide.


Lisa Schamus: Great. Well, I think that we're just about out of time. So, I wanted to go on to the next slide. And thank you all for joining us today. And I hope you'll join me also in thanking our speaker.

## Slide 50



Lisa Schamus: As a reminder, we will have the materials from today's session available within the next few days. And if you have additional questions for the RHNTC on this topic, please don't hesitate to email it to us at [rhntc@jsi.com](mailto:rhntc@jsi.com).

## Slide 51



rhntc.org

**THANK YOU!**

Please fill out the evaluation form  
after the webinar!

**CONTACT US**

[rhntc@hpi.com](mailto:rhntc@hpi.com)

This webinar was supported by the Office of Population Affairs Grants PPTA000020, TPAH000006 and the Office on Women's Health Grant A574N0000-90-00-000. The views expressed do not necessarily reflect the official policy of the Department of Health and Human Services nor does mention of trade names, commercial products, or organizations imply endorsement by the U.S. Government.

Lisa Schamus: And our final slide is just an ask that you please complete the evaluation today. A link to the evaluation will appear when you leave the webinar, and then we'll also email it to you after the webinar. We really do love getting your feedback and we use it to inform future sessions. So, thank you all so much for joining us. And that concludes our webinar for today.