BobbyTheIntern

[00:00:00]

[00:00:00] **G Mark Hardy:** Hello and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G. Mark Hardy. I'm your host for today, and we'd like to welcome you to the show. We'll be talking about, well, what do we do with new hires and people who are fairly inexperienced with IT, but yet get access to our systems. If you're new to CISO Tradecraft welcome, please go ahead and follow us on LinkedIn. If you haven't already or subscribe to us on your favorite podcast channel. If you're watching us on YouTube, great, please click subscribe. That really helps us out a lot. Didn't realize why people kind of did that before, but Now that I'm in this side of the camera, I realized it really does help.

So if you go to YouTube, CISO Tradecraft, that will help us out a lot. Well, now that we're into summer, and this usually means [00:01:00] one thing for a lot of organizations, new hires and organizations will recruit fresh college graduates or even students in between terms as schools let out. And so some of us will hire new talent whose modus operandi is ready, fire.

But we'll affectionately call that young person Bobby the intern. Now, before Bobby the intern can create havoc on the company network, how about we train that poor kid on what he's supposed to be doing and, more importantly, on what he's not supposed to be doing. And that'll be the focus of today's show. But first, let's hear from one of our sponsors.

As a security leader, it's your job to provide advice to leadership on cyber risks and concerns. How do you answer your board when they ask, is the software we use safe? How do you measure cyber security performance and what types of risk does AI create? On our next episode, number 141, join us for a conversation with Chertoff Group Cyber Experts David London and Adam Iles.

The Chertoff Group helps organizations achieve their business and security objectives in a complex risk environment. Learn [00:02:00] more at www.chertoffgroup.com

[00:02:02] **G Mark Hardy:** Back to their show. One of the challenges that we face as a cybersecurity leader is keeping our organization security culture.

According to KnowBe4 quote, security culture is defined as the ideas, customs, and social behaviors of a group that influences its security.

Now, when I taught at SANS, we used a diagram from Dr. Lance Hayden's book, People Centric Security, and it showed an iceberg with behaviors and artifacts above the waterline and beliefs, values, and assumptions below the line. And like an iceberg, a majority of security culture is out of sight. And also like an iceberg, it takes a lot to move it.

My fellow SANS instructor, Lance Spitzner, wrote that some of the most common indicators of a strong security culture include. People feel safe reporting incidents, even if they caused it. People include security as part of their job description. Employees correct and help their coworkers to be more secure.

My shared belief that security [00:03:00] plays a strong role in your organization's success. And. People feel comfortable asking your security team questions. Does that describe the culture at your organization? If not, perhaps you have a little bit of work to do. I recently did a security awareness training for a number of senior executives, and one of the responses I got back was someone who said, this is so much better than what I've seen in other places where it's sort of a gloom and doom and fear.

Because what I put out is that, hey, we're all human. If you make a mistake, Let me know. We can fix it pretty quickly. Don't hide it. It's only going to get worse. And so we'll work together. There's no permanent record on you like it was back in high school. And as a result, let's just go ahead and team up.

And people respond to that message. Of course, you need to be sincere about it and not keep your sort of a secret little list of people. They say, if you screw up once, okay, it happened. If you screw up a second time, yeah, maybe it's appropriate to do a little bit of remedial training. Now, if a person screws up month after month after month, maybe it is time for that conversation to say, you know, [00:04:00] there are jobs around here that don't require a computer.

Floors need to be swept. Toilets need to be cleaned, et cetera. Anyway, we'll go back to the idea of security culture, and it's about making the entire organization resilient. To cyber threats. And part of achieving this outcome is building a culture that promotes security vigilance. And that begins from day one.

Let's go over the basics that everybody in the company needs to know.

Let's start with something that grabs their attention. Start by showing a picture of the company's core product. This could be the Amazon shopping website, Netflix homepage, a picture of the latest Tesla vehicle, or the latest iPhone, depending on whatever your company happens to make. And this picture should be something that brings pride in the brand of the company.

You might ask, what do customers think about when they see this product? Should be good feelings and knowing that it's something that's valued now, take that same picture, maybe add animation. So you start to see things like third party data loss, [00:05:00] ransomware, phishing, denial of service attacks, intellectual property loss, compliance violations, loss of customer data.

And if you knew, That these things frequently happen at this company. Would you as a customer still want to buy that product? So you want your people to see that cyber incidents harm the brand. They decrease future sales and they do cost money to fix.

So then what is cyber security? We assert that cyber security is the business of revenue protection.

Now, that should make sense to you, but what is revenue protection all about? Most everything that an organization does relies on software and the data behind the software. For example, without software and its data, most organizations would be unable to send email, collaborate, record customer sales, send invoices, document accounting expenses, and execute banking transactions.

Revenue protection focuses on ensuring that the business understands, manages, and mitigates the risk of data being disclosed, altered, or denied. These [00:06:00] three items map back to confidentiality. Is it being disclosed? Integrity? It's been altered. Or availability? Is it being denied? The CIA triad we learned early on in our cybersecurity careers.

Well, now that we've kind of defined what cyber security is, we need to understand how that's achieved. And good cyber security comes from executing cyber practices, commonly known as cyber hygiene. And typical examples of this include, but they're not limited to, security awareness training, risk assessment and risk management activities, application security and vulnerability management activities business continuity exercises, disaster recovery, incident management in response, audit, compliance, and control activity. See, these practices ensure that organizations understand, manage, and mitigate the risk of their data being disclosed, altered, or denied. Now that our

new hires have a good understanding about what cyber is about, and what do we want them to focus?

The 2023 Verizon Data Breach Report, [00:07:00] which is one of the largest studies on how bad actors break into companies, says that the three primary ways in which attackers access an organization are stolen credentials, phishing, and exploitation of vulnerabilities. Let's start with those three things and give helpful advice on each to our new hires.

Start with stolen credentials. If you log into any IT application with just a username and a password, you're doing it wrong. Because without a whole lot of detail, here's a few reasons why. People choose obvious passwords. They reuse passwords. They typically write them down. Typical, you know, yellow sticky on the bottom of the keyboard.

When somebody leaves the company or changes their role, The passwords aren't always revoked. Now, I had a situation where one of our interns this past month, we're talking to him and he said, Hey, I need to get a copy of such and such. And, okay, fine. Well, I'm using this guy's account and password. Really?

Oh, yeah. I mean, we share it all the time. Well, why didn't you tell IT that you guys need some more [00:08:00] resources? We could get them for you. Now, here are these fairly junior people. Smart as all get out. No question about that. That don't understand the concept of cyber hygiene. And not only do they not just have a single password, but it's being passed around like a party.

And I was like, no, we had some specialized training. We sat everybody down and explained why that was a bad idea. And again, a little bit later, one of the interns contacted me and says, Hey, can I get the admin password? I need to go ahead and assign some rights here. It's like, no, you can't get the admin password.

Nice idea, but we got to help people understand that there are systems installed for a reason. Now, if usernames and passwords are wrong, what does good look like? Out of the world of modern identity and access management, and we often will hear the term zero trust. Well, first of all, one of the things we can use is Single Sign On (SSO).

It's one password that people need and access multiple enterprise applications. They're all federated and therefore that credential is trusted across these different [00:09:00] places. Great. Now, since we don't want one guessable

password, we want complex passwords or phrases. Now, I suggest that something more than 15 characters is long enough at this point in time.

Teach users to create past phrases. Something like, My favorite book to read is Lord of the Rings, or the little girl went to the store to buy some food for her cat, or better yet, show them how to use a password managing tool like Bitwarden or LastPass, or there's a whole class of companies that are out there that do that, which means you memorize one password, and then it can maintain and even generate a lot of complex passwords. Google will do that for you. Do that in Google Chrome. The problem, potentially, with storing it in Google Chrome, using Google Chrome's browser, is what? To access those passwords, all you need is a device password. Well, on my laptop, I've got a pretty long login.

But you know what? On my cell phone, it's da da da da da. Go ahead and hit the pin in there. And all of a sudden, that's all that stands [00:10:00] between you and somebody who's got five minutes with your phone and you're not there, harvesting a whole bunch of your credentials. So you got to think carefully about how you do that.

But the whole idea is length is better than complexity. The whole idea. Of uppercase lowercase numbers and special characters and changing many 30 days little homework assignment. Go look back up You'll find that that was back from the days of the pdp 11 when that's about how many Times it would take to search the entire space of eight characters With upper lower number special characters giving you about 80 some odd different variants.

Take that to the eighth power and then look at the instruction speed on that computer. It would take about 60 days to try them all. So halfway through is 30. Yeah, that's probably a good safety point. We still do that. And I still see password policies where you need all these crazy complexities. Best idea would be say, hey, that's fine.

As long as user doesn't have to remember it. If using an effective password manager, have a big long password and it can be nothing but words. But don't make them verses out of a song or something else. But they [00:11:00] say something that people come up and it's absolutely unique to them that they'll remember.

And then let the password manager remember 20, 30, 127 character complex password string, and then it works out pretty well. So once we help them understand about password management, and if you don't have a password

manager, but the importance of length over strength on passwords, talk to your new folks about multifactor authentication or MFA authentication requires to use something like a YubiKey, an authenticator app, or even an SMS code to log in after typing in their password. Now we want to make sure that they know how to use it and that they know that they need to use it because your organization should require that in all your applications. Also, you want your employees to turn on MFA and their personal stuff. For example, turn on MFA on your LinkedIn account.

But wait, that's my personal LinkedIn account. Yeah. But do you identify yourself as an employee of this company? Well, then if somebody were able to get into that account, they could impersonate you, make all kinds of [00:12:00] postings. And since you're viewed as a representative of the company, any malicious postings could harm our brand and that's not good. It's not career enhancing either. Okay. We've done single sign on, complex passwords, MFA. Is that enough? MMM, actually we can do one more thing. Conditional access. See, we rely too much on people spotting phishing attempts. And the reality is that pretty much anybody can be phished.

That was my point a little bit earlier about when you're trying to help people understand your security culture, recognize that everybody can make a mistake. Just don't make a lot of them, but make it so that if you make a mistake, Hey, I screwed up, let people know. But in some safeguards, if you add in to say that even though you have the correct password and the MFA passcode, if you don't come from a corporate managed machine, sorry, you're not allowed to access the system or network.

And this could be done with solutions like Microsoft Azure Active Directory or Zscaler. I do that and with all our employees, they have to come in on a managed device. [00:13:00] If it's not a managed device, can't come in. But I want to check my email and bring your corporate phone or bring your corporate laptop.

But I'm on vacation. Well, then be on vacation. All right? I carry two laptops and two phones. I've done that for literally decades. Did that in the military when you had to have your military one. And now I just do that with the client stuff. And you get used to it. You might end up with one arm longer than the other, but yeah, you'll survive.

Now, if we can do these things and teach people about them, then we have significantly reduced the risk of stolen credentials in our environment. Now, one more thing, just remember that credentials don't only belong to humans.

Credentials can also belong to software. So don't lose credentials by allowing developers to store valuable things such as passwords, tokens, or API keys into source code repositories or GitHub or binary object repositories or shared folders and things such as that.

Take a quick pause here for a brief message from one of our sponsors. Can you answer the question, are we protected? Introducing Prelude Detect. Prelude [00:14:00] Detect is a production scale, continuous testing platform that gives organizations assurance that they're protected against the latest threats. They've correctly prioritized their critical vulnerabilities and their defensive controls work exactly as expected.

And if not, Prelude's integrations with defensive controls, such as CrowdStrike, create an auto hardening defense. Get started for free or request a demo at www.preludesecurity.com Again, that's preludesecurity.com. Now back to our show.

Next, we need to teach our employees about phishing. Remember, not everyone has the same understanding of technology. So start with the basics, create a hyperlink that says www.google.com. Okay. Now what happens if someone clicks on this link? You'd expect them to go to Google.Com right? Now what happens if somebody edits the link and points it to a MaliciousWebsite.Com but doesn't change the text that appears on the front, doesn't go to Google.

So you can highlight a URL in Microsoft Word, hit [00:15:00] control +K to show where the link actually goes or on a Mac it's command +K, but it's a helpful feature since marketing folks will also shorten a really long URL found a website. I just put the word link over it or click here on top of it. Now, understanding that URL links can be used to trick you is how some attacks begin. You see, bad actors are not going to type, click nefariouswebsite. com in an email they send you. They're going to send you an email that links to something you're familiar with. It could be UPS packages, Zoom invites, addition to a Slack group, your company name with a typo.

We've been getting a lot of DocuSign requests lately that look like a DocuSign, but you click on it, and then it takes you to a place saying, oh, you need to log in. With your Microsoft ID and password. It's not really a Microsoft site, but it sure looks a lot like it and things such as that. And so what we want people to do is notice if something that they get is normal or not.

And the way you can tell if it's an email is normal if it [00:16:00] comes from an external email address. For example, Okay. If you work at Walmart and your

email is John.Doe@walmart.com, and you get something from walmart.de or walmart.xyz or a Walmart dot, any one of the 1400 plus top level domains, because I don't think they've bought and bought every last one of them, then that's not an internal email.

Now, it could be blocked and detected at your gateway. There's a lot of rules. For example, I use Microsoft 365 and we can identify that for spoofing and if somebody. Says, let's say, you know, Joe Wilson is your CEO or Nancy Johnson is your CFO and you get nancy. johnson at somelookalike. com. Yep, it's going to flag that or something comes in.

It doesn't pass the DMARC, DKIM, or SPF framework checks it'll look for that too. But if you're getting an email from UPS and you're really expecting a package from UPS. Don't click on a link, just log in to ups. com and search there for your package or drag your mouse and copy the package name or the tracking [00:17:00] number and drop that into the web browser when you go to that website because it's significantly reduce the risk of clinking a bad link.

It's going to get you the same place if it's legit. Now, according to this year's Verizon data breach report, 83% of breaches involved external actors. Five out of six, 74% of breaches involve humans, either through social engineering errors or misuse, meaning probably the rest of them is going to be technology 50% are socially engineered.

Their incidents involve pre texting believable story that someone comes up with it. You get suckered along. You wouldn't do it if you didn't realize they weren't lying to you. 24%. of the breaches involve ransomware and 49% involves stolen credentials. See, a lot of organizations today are putting a warning banner on the top of their emails to help people understand when emails originate from outside the company.

And if you see a warning banner or you see an external email address, stop and ensure that you're dealing with legitimate correspondence from before you continue. If it's an email you're expecting, it's probably okay. But if it's [00:18:00] unexpected, and I want you to click on a link, or open an attachment or call Microsoft right away.

That's a bit sketchy. I've got some pushback in some organizations. We added that and he's actually like, well, why do we need to do that? I deal with external people all the time. I'm aware of that, but not all employees do. And maybe we have to kind of structure it out because if somebody is in sales, they're going to be dealing with external all the time.

But if you're internal on accounting, you might not ever be talking to somebody unless you're receiving invoices. But if you're on a dev team, you're probably not dealing with a lot of external messages. And so as a result, these things are very, very valuable. Now, here's a little rule of thumb to go ahead and teach your folks.

If an email creates an emotional response, Because it wants you to click on a link under attachment urgency or bad things are going to happen very soon If you don't that's really really sketchy report these The cyber security incident response team, you should have set up an outlook, a little button that says report phishing takes only a second for users to do so.

Of course, you need to set that up in advance on your end if you're a security leader. But here's [00:19:00] why we want everybody to report phishing emails instead of, well, just deleting it. Let's say three people get sent a malicious email. One clicks it. One deletes it, and one reports it. Now, if someone reports a malicious email, we can look into it.

A copy gets sent to Microsoft if you're using 365. They can go ahead and look for similar emails and say, yeah, that's a whole part of a campaign. There's something that looks just like that that's in somebody else's mail. They haven't looked at it. Let's go pull it right out. And so they can actually delete messages before they ever get delivered.

Now, if somebody's fast on the inbox, they might have already opened it. And if there's malicious stuff in there, you get an alert saying, warning, user has opened something that had malicious content. We couldn't get it in time. It's better than doing nothing. Now, if you have people who click on these things and look further, we can do an investigation.

You can do kind of a link analysis. Hey, this person, this person, and this person, they all got the same email. This person reported it. This one didn't. All right, let's go ahead and you can make sure that gets thrown away. This one opened it and activated something. So that might be where [00:20:00] the problems are coming.

So the whole idea is we want to stop cyber attacks before they really get started. It takes a little while, not a very long while, but for lateral movement to start. About an hour on average between when an initial endpoint is compromised and someone starts to move sideways. So if you can respond in that golden hour, you're able to go ahead and really reduce the likelihood that somebody.

One of your employees, one of your interns who clicked on something has introduced a problem that you now have to deal with on a big order. Now, if you get an email that looks beyond simple phishing. We recommend having users contact the cyber department. Start a conversation if you see a business email compromise where someone's trying to change payment information on one of the company's suppliers.

And they're not going to give up after a single attempt. There's a lot of money to be made. I've seen some of these companies that are targeted. These attackers do a lot of homework. They do a lot of research. Why? Because there's a big pay bay on the other end of it. And so what happens is, is that If they can get into somebody's email account, probably through [00:21:00] phishing, because you don't have MFA turned on.

And so someone falls for a phishing email, they say, enter in their ID and their password, but give it up to the bad guy, and they say, okay, here's your DocuSign, or here's your whatever. They think nothing of it, but the attackers will often do that as a login late at night. Go ahead and read the inbox, read the outbox, and then log back out.

You know, try not to leave any tracks. When they start to see contracts or payment terms or things like that, once a contract goes out, I saw this one of our clients that evening, the attackers logged in, sent a Chaser email to the client saying, Oh, by the way, here's a new banking information. Please make sure you're sending their payment.

They're sent it and then deleted it from the outbox. And then this happened three different times. And so eventually the customer is not getting their stuff because the company isn't getting paid and the customer called up saying, Hey, where's our stuff? We paid you and said, no, where's our money. You didn't pay us.

Well, we paid you. No, we didn't. Yes, we did. Well, where did you pay? Well, we paid there. We said, pay there. No, you said. Oh, yeah, all could have been avoided with multi factor authentication [00:22:00] because that stolen credential when someone tries to log in, by the way, because they were so good about deleting the emails and eventually when they're done with that account, they scorched it, they wiped out this person's sent folder for almost a year, but I was able to get it.

Information from the other end of the correspondence. And what we found out is not naming any names here, but, uh, IP addresses went to Lagos, Nigeria and nothing against folks in Lagos, but, I don't know, a hundred thousand us dollars

goes a long way there. Probably spends a little bit better than it does in New York city.

And so would that be worth. Time and energy and effort and patience to attack somebody. Yeah. And so what you want people to understand these scenarios of BEC, business email compromise. And then what I do is in my contracts, I make it part of the contract. I said, this is the payment information. It's in the contract.

Any change to the payment information must be signed by both parties in advance before it's approved. So if somebody ever were to get in [00:23:00] to one end or the other and try to change the payment information and the other party knows, Hey, Contractually, I can only pay account A, but they're saying pay account B.

Let's get them on the phone. You're making it much more difficult for an attacker. And if they do pay B, and they can't say, well, somebody pretended to be you, and they faked us out, they say, well, look at the contract. What does the contract say? Oh, it says that if we send it to somebody else, we're on the hook for it.

Cynthia, I was trying to protect you. So most companies only make that mistake once. I'm trying to help you make that mistake zero times. Okay, the last way that bad actors get into companies is by exploiting vulnerabilities in software. Now if you want to have developers build a secure website, they need to do at least three things.

One is they have to patch their software and keep it patched. Software age is like, well, milk, not white wine. It doesn't get better with age. And over time people discover vulnerabilities. And if you're using an obsolete package, the problem is, is that a lot of that updated version will have [00:24:00] similar code and they'll patch it up here.

But they won't patch it here. So an older version of PHP or even operating systems. I love Windows XP, but there's still code in XP that's used in Windows 11. Go ahead and change your network information around and you'll notice that that was the same screen you saw in 2001. And who knows, it might have been there from Windows 95.

They haven't updated the code. But if they had found a problem in it and they patched it. They're not going to patch the earlier versions. So make sure patch software at all levels, OS, the middleware, application tier, etc. And once that's

done, you want to make sure you have a good, solid configuration. The Center for Internet Security, cisecurity.org, has benchmarks. And these benchmarks, which you can download, will help you give guidelines for how to secure your applications. See, operating systems and web servers and other things have some pretty bad defaults from a security perspective. They're designed to work when you take them out of the box.

So, turn that stuff off. Some vendors have gotten better. If you get a home router, remember we used to get the [00:25:00] Linksys routers and... 192. 168. 100. 1 and Admin, Admin. That was your login for everyone on the planet. Now, you may still have a login of Admin, but you get more complex passwords. I know that cable modems that I get here from this company here, word, digit, word, digit, word.

Okay. Length greater than, not uppercase, lowercase, number of special characters. But the whole idea is each one's a little bit different. So there's no master key that's out there. So what's that? We've gone ahead, we've patched the software, we have good configurations. And then finally, if you have custom code on your website, make sure that somebody's checking that.

You've got static, dynamic, or interactive security testing. SAST, DAST, or IAST if you pronounce it that way, or Software Composition Analysis, SCA, scanners. These, we're not going to spend a lot of time on these, but if you want to learn more, we already have talked about it. So check out episode number 35.

Setting up an application security program or episode number 94, easier, better, faster, and cheaper software. See, the [00:26:00] point is, if something is accessible to the internet, it needs to be secure. Now, even if something is internal, it still needs to be secured. For example, we often hear developers say, Well, I'm not worried about patching something because it's behind the firewall, or it's on a system that uses MFA.

And in response, ask, Is this system frequently used by developers or admins? Well, yes, it is. Okay, so if I successfully phished one of those employees, and ran a simple command like netstat to see where the developer admin was currently logged into. Would I see access to this system? Um, well, yes, you would.

They spend most of their time on it. Now, if I saw that someone had current access to the system, and I did a simple scan and saw the system was version XYZ, which had a remote code execution vulnerability, and it hasn't been

patched, do I really need their login credentials? Not really. I don't need to phish them for it.

I'm in. [00:27:00] It's okay then. So it seems like something we should patch, right? So using this type of questioning gets people to understand how the things that they've been taught about security may not actually be good enough. They need to have an attacker mindset. The offense informs the defense to see how things can be harmed.

And that's really the whole focus of threat modeling, which we'll leave that for another day. Verizon attack methods of stolen credentials, phishing, and exploitation of vulnerabilities, We should also highlight a few more attacks for our new hires, or Bobby the Intern, as I think we're calling them. First or third party applications.

See Bobby, please don't sign this organization up for free tool without going through our internal procurement process. Well, why it's free? See new hires think they're adding value when they're creating efficiencies. They want to use things like ChatGPT to get quick answers, grammarly to get better sentence structures, or Otter AI to take notes in meetings.

And these can be good things. [00:28:00] However, they also come with risks. Chat GPT has had data breaches. When you give grammarly access to your sensitive data, that's in your document. You don't know what it does with it, and Otter. ai and its peers could retain all of your information that you upload to it for improvement, for study, etc.

But this is how the AI models train. They learn from you. So let's make sure we get these enterprise level licenses and contracts with these services in place. To protect our organization. These are superior to personal licenses or freeware licenses, which most consumer grade products default to. When we go through these processes, we also create an inventory.

So we know what's running in our enterprise. And that way, if some vendor like Otter AI reports a serious security breach. We can see who's using that application, who has connections with the app, so we can get an official response as to what was compromised and put a limit around what our risk is. And additionally, we can create disaster recovery plans for these services so we can continue as a business when they're not in service.

If we're dependent on an app and we [00:29:00] don't even know about it because somebody's paying for it with their corporate credit card and they're

building 74. 99 a month as a taxi because they don't need a receipt to cover this Azure or some other vendor, That's bad behavior. That means we're not communicating to them effectively the risks and we're not giving them the tools they need or that they think they need to get their job done.

So come with some of that's on us. But it's also important that once they know that, that you've communicated it, it's on them as well to make sure they do it right. So please, please, please ensure that your people procure software the right way to keep the organization safe. And don't forget to teach your new hires that you should not plug untrusted devices into equipment.

For example, you find a USB drive laying around, it's on the floor in a building or in the restroom or in the parking lot, road apples, as we used to call them when we did security testing. Don't pick it up and plug it in to see what's on it. If you get offered a free mouse or a USB fan at a conference when you're walking around like a trick or treater at RSA or Black Hat and grabbing all the stuff off the desk, careful what's on them.

They may [00:30:00] not always be what they seem. They might already have malware on them. A picture frame that has rotating pictures. It's basically jpeg jpeg That's nice. These have come right out of the factory with malware built into them a feature, right? So you want to be very careful when you travel a lot of people plug their phones into wall charges or Charge at the station there at the airport or other public places But is there more than just five volts on the other end of that cable or is it something harmful?

FBI put out a warning last month on juice jacking. It's been around for a little while, but it basically means that that Typical USB cable, whether it's USB A or C, has data as well as power in it. Now I've got a little thing. It's probably got a trademark on it. I came up with the idea of the USB condom, but it's basically passes the USB in this side and only lets the power go out the other side.

And you can buy these things for fairly inexpensively, have them print up with your name on it and give those away. Now those, I think would be useful things to give away at trade shows where they actually go ahead and they filter out the data. But unless you bought it or know where it's coming [00:31:00] from, or you've tested it, you want to really be careful about that.

We see a lot of people using QR codes. They use them in stores and restaurants. You'll see them on walls. You see them in magazines and things like that. So little stickers on the wall. Let's see what they are. QR code basically is turns into being. A bunch of characters. Often it's a URL. It just takes you to a website.

Unless you use an app that screens these codes, you can't know in advance if these links are malicious. So if you're in a restaurant like, I don't know, Chick fil A and you see a QR code sitting on a card in the table or whatever, you can just open up your camera application and scan the link. Go to the App Store and look for the Chick fil A app.

If you want to do it that way, that way you can see the official site with millions of downloads. Now I found a tool and you can look for it. I'm not going to pitch any particular brand here. That what it is, is I don't use my camera application. This is actually a QR scanner tool. And I hold it over the QR code and then it says this is a destination.

It sorts it out and then it says trusted, safe, unsafe, or I don't know. A lot of these things will go to [00:32:00] shortened URLs. And if you're familiar with the concept of a shortened URL, it's just a redirect. Where you go to something that's just fewer characters. So otherwise you don't have this big, huge, complex QR code.

And then that redirect takes you to where you're going. One of the first ones was bit. ly very popular. I like the idea. I've used it a lot. But the thing is, is that how often do you do business with Libya? Technically that's the ly. And so as a result, if you have a domain, that's a bit. ly, blah, blah, blah, blah, blah, show you a little trick.

Put a plus sign at the end of it and then enter it in your browser and that takes you to the control page for the person to set that up. It shows you exactly where it goes to as well as other things like that. Not everybody does that, but the danger of shortened URLs are is that you have to go here and then bounce over to the other one.

So again, help people understand that there is a potential risk there. One final thought for all your employees. Users have the ability to delay when desktop patches are done. Ideally, you have automatic patching enabled, and it restricts what delays users can [00:33:00] choose. We use that where you've got to get your update, you've got so many hours, I'm busy, I'm working on a big project, I get that, you're working on a project, but you've got to sleep at some point, so we're going to give you at least 24 hours, which you have to apply the updates, or it's going to just reboot on its own, that's what Microsoft does.

If you don't, if you don't have that capability turned on with the automatic patching, And restricting these delays where people can delay, delay, delay, teach your employees how to look for patches and update them quickly. Okay,

control, escape, bringing up the little Cortana thing and UPD updates. And then just check for updates.

If you're in Microsoft 365, any of the applications, Alt F D R U. File account, update, update now. I don't know why they got those letters, but that's what happens to be in the shortcuts. I love keyboard shortcuts because, well, been around for a while. And so why use a mouse when you go quickly?

But the whole idea is, is the updates that happen for Windows aren't necessarily updates that happen for your Microsoft 365 apps. And they're not [00:34:00] the updates that take place for your browser. And so if your user's updating your Chrome browser, it only takes a few seconds to apply. But you have to restart the browser for that update to take.

So even though you can make a policy that says, Hey, it's a controlled app or running it, and we push out the updates unless somebody reboots it. So what happens? They leave the browser running for day after day, sometimes weeks on end. It'll never gets updated. One of the things you can do, I use Chrome a lot, is that you can set it so that when it restarts, it says, bring back all of the old windows that I had before.

Now, that makes it a little bit easier to apply a patch or reboot like that. The only thing is you will not get back. You're incognito windows. And while I like to do incognito, in fact, I'm recording this on an incognito window, mostly because as a force of habit I've had, when I closed down my browser, I got no cookies left over.

I got no history left over. It's nice and clean and nothing ever builds up. Plus it doesn't give you necessarily any security. It [00:35:00] doesn't keep apps from breaking out of incognito mode, but it does really limit what gets tracked out there. That plus a cookie tracker. Or cookie limiter goes a long way toward making the browsing experience, not any more or less convenient, but a lot less of a concern for folks.

So make sure that they update their browsers on a regular basis, because some people just don't feel like it. They're going to get around to it and they never get around to it and things like that. There needs to be a little bit of accountability there. That's a lot more things you could teach your new hires about security and things like proper data classification, how to use a virtual private network, backing up their software, or backing up your tools to services of daily or monthly backups.

You're keeping your data synchronized between the cloud and your hard drive. Again, a lot of applications today do that automatically if you're using OneDrive or the like, and Microsoft has that built in, but you got to turn it on. Not everybody has it turned on. What you want to do is help them understand [00:36:00] things like acceptable use policies.

What are you allowed and not allowed to do? These rules are here for a reason. Data privacy requirements. Don't just send social security numbers. Don't just send credit card numbers by email and things like that. Secure file sharing. All those things are important. However, you don't have time to present everything in this one session.

People will glaze over. They'll run out of time. And besides, They're only there for the summer, perhaps, as an intern. You can't spend the whole summer teaching them about security. So show where employees can go ahead and find guidance, where they can get information if they have questions. It might be on an internal website.

You might have a group email for help or whatever, but remember, if your new intern, your new hire feels like you have a friend in cyber, ask questions and that's a good thing. All right. Hopefully I've given you enough to think about in terms of how to orient your new employees. or short term employees for being able to do the right stuff.

Most of this is things you probably already covered, but it's a matter of organizing it. What I found is very helpful is, I use PowerPoint. I used to do a lot of death by PowerPoint. We don't use it in this show. We haven't not yet, but [00:37:00] you never know. But what I found out is with PowerPoint is you can set it up where you can have a little talking head in the bottom right hand corner and then go through your PowerPoint slides and now it's as if you're sort of with the person, but you get to see the slides.

So if you can't be with somebody directly, You can then communicate it that way, but find different ways to communicate your information out there. Don't just be boring. There are excellent tools out there. There's many companies out there that will have learning management systems, LMSs. They'll also have tracking so that if you have hundreds or thousands of employees, you don't have to keep a spreadsheet.

It's who watched and who didn't watch it. Take advantage of those tool sets. Remember, every organization has their own unique requirements and just

grabbing something off of a wishlist. All right, fine. There you go. Watch this thing. And there's your 30 minutes of security awareness training for the year.

We used to do that in the military. We had 30 minutes a year. That's not enough. And you got to realize that it's not enough. So make it a game, make it entertaining, make it enjoyable, but make it non confrontational. You want people to feel that they're part of a team that's going ahead and [00:38:00] defending the enterprise.

So hopefully you found enjoyed learning about this and want to thank your listeners for You know, sharing this content on LinkedIn, let other people know forward link or whatever like that. Also, if there's something you want us to talk more about, let us know, you can send us a comment by going to see so tradecraft.

com or send us a message on LinkedIn or follow us there. I said, and that way you can communicate back and forth. Now, some of our. Episodes are inspired by viewer comments and recommendations. And who knows one of these upcoming episodes, you can say, Hey, that was my idea and they're using it. Okay. So anyway, thanks again for listening or watching, and please don't forget to check out our sponsors.

We're glad we can support you on your journey to becoming better at CISO Tradecraft. Until next time, this is your host, G Mark Hardy. Have a wonderful day and stay safe out there.