Cybersecurity 313 Podcast Episode No.10 with Shaun Bertrand

Announcer 0:01
This is the Detroit Mercy Cybersecurity 313 Podcast.

Tamara Shoemaker 0:07
Hello, this is Tamara Shoemaker, the director for the Center for Cybersecurity and Intelligence Studies at the University of Detroit Mercy. And I am excited to introduce Shaun Bertrand from CBI. He has an enthusiasm for cybersecurity that is contagious. And we've run into each other at several occasions, one of them being GrrCON, which is the greatest thing out in Grand Rapids. But we brought Shaun here because he has a great background, and he has a really good take on the kind of things that we're talking about in this podcast. And so I want for you as the audience to get a feel for who Shaun is, and have him explain who he is, and a little bit of background about the company that he worked for. And then we'll go ahead and try to educate you guys on some few tips and tricks to help keep yourself safe. So Shaun, take it away.

Shaun Bertrand 0:51
Well, thank you, Tamara. You know, the best way I describe myself is a extremely passionate individual as it pertains to cybersecurity. I've been in the industry for a long time. Judging by the gray hairs here, about 20-25 years, I started off doing this stuff before, ethical hacking was a thing. It was more or less a concept and theory. And back in the day, the stereotype on hackers had a different meaning than it does today. Right. But I stuck to my guns, extremely passionate, got involved with a company called CBI. And 18 years ago, I started at CBI and it was this small company talking about cybersecurity at a time when it wasn't really an in demand service as much as it is today. And so I helped with a number of others accelerate the organization's pursuit toward cybersecurity. And so today we're about 150 people, I run a number of different teams as the SVP of security programs, and you know what I like to invest though... I like talking to friends and family and other people, where we can just give them some guidance and some insight into some best practices. So I'm looking forward to the conversation here today. Thanks for having me.

Tamara Shoemaker 2:04
Well Shaun, we're really looking forward it too. CBI has been an amazing supporter of some of the things that we're doing at the university and in the center and my main push to nausia level with cyberpatriot in the K through 12 stuff bringing up the kids. And so we've run into a lot of things. Your folks at CBI have been amazingly supportive of that. I think your chief executive officers a couple of days after he arrived, he showed up for my summer camps to help out, do you guys have all been amazing you serve on my board of advisors, all that kind of good stuff. So this is sort of a good friends talking about stuff that we love to do. And again, like you said, the audience that we love to take care of the most are those ones that not necessarily other folks, while we hang out with all of our security friends, right. And we talk about the kind of Oh, how things are going, and how things maybe haven't changed quite as much as we'd like to in the years that we've been in it. And the same problems keep coming up what we really

need to talk about and address some of the thoughts that the regular folks out there need to talk about and need to hear about. And so what do you think that some of the main priorities we need to focus on in cybersecurity would be?

Shaun Bertrand 3:07
Yeah, oftentimes the consumers, the people are just as much at risk as the organizations and the corporations. And we'll talk about that a little bit later. But when I sit down, and I talk to my family and friends about the areas that you need to focus in on, I really try to drive home the fact on probability and realism. You know, some of the things that we hear in the media are very important, and we need to build some best practices and defenses in our personal lives. But other things, you know, one in a million shot of kind of going down, let's not focus on that, because everything we hear in the media is based on a lot of fear, uncertainty and doubt. So when I talk to people, I say, there's two things you should be most concerned about. Number one is phishing attacks, corporations and people, it's the number one most widely used attack that the bad guys are going to use to break into your environment, your computer, your world is a phishing attack. And we're all generally familiarized with kind of the concepts of phishing. But oftentimes, we don't really know exactly what to do, what to look for. We'll talk through some of that today. The second area that is of concern are vulnerabilities on your computers and your mobile devices, and all your smart home technology as well too, right? Your smart thermostat, your Amazon devices, all of these things have vulnerabilities on them that can allow these malicious hackers to gain access into your personal lives to the point where you don't want them to, right so those two areas are where we see the best opportunity to educate and enable people to build better awareness and recognition of some red flags to look out for and some best practices to follow.

Tamara Shoemaker 4:47
So I totally agree with you. And the thing I think that's a little scary about that is that phishing has been around since the beginning of time practically and cyber and so is vulnerability, right? So these are things that are too Just inevitable in the systems that we use, but with a few tweaks, we can make sure that we're safe. And I like what you said about sort of general practices. I mean, it's one of the things I preach like crazy, both of my cyberpatriot kids and to the senior citizens that we talked to about some good easy things that you can do and look for, that can keep you safe. And can you expand on that a bit about like the phishing episodes, and...

Shaun Bertrand 5:24
Absolutely, the first thing I try to educate people on is one of the main principles to look for in a phishing attack. And it's called F.U.D. Fear, uncertainty and doubt, these bad guys, they're trying to instill some fear, uncertainty or doubt, to provoke you to do this thing to open this email to click on this link to open this attachment. Alright, so the first thing you should ask yourself, Is there any F.U.D.? Is there any fear, uncertainty and doubt? And are there any other ways that I can validate the authenticity of this email without clicking on the link or opening the attachment as an example, all the COVID related attacks that we see a lot of things we see with the CDC and an even attacks

against organizations where they're impersonating some communication on new workplace policies? We see a lot of stuff there. And one of the first things I look at is the opportunity to validate is this. Is this really coming from...? Can I call human resources? Or can I do this thing to you know, better understand who this is? Same thing with the bank, when you get an email, a phishing email, a lot of these are based on financial perspectives. Rather than clicking on the link, if you got a suspect, a phishing attack, open up Google, go to the Contact Us page of the bank itself and call them and validated through there. So that's one of the ways we see is being able to validate the authenticity and look for a little bit of that fear, uncertainty and doubt.

Tamara Shoemaker 6:51
For the most part, people fall for a lot of this stuff, and not just with fear, because fear is definitely one of them. You know, the minute I get something says IRS, I'm like, Oh, no, not again, no. Quick, I gotta get these guys off my back. Right. Yeah. But also, the other piece, I think that a lot of folks end up happening is they're, they're just good citizens right there that feel like, hey, somebody's asking me to do something. If somebody took the time to send you regular mail with a stamp on it in the whole nine yards, it was probably something official. While there are some spam stuff that happens with regular mail. It's not quite as prevalent as it is now. Because it's so darn easy for everybody to get a hold of everyone. Right is Yeah. And so I think sometimes that people are trying to do the right thing while they're doing that. But like you said, the easy part is to just validate where it's coming from, right. And some people say they can just hover over the site and say, Oh, well, we know that is there that isn't, is that a good suggestion, Shaun?

Shaun Bertrand 7:43
it's not a bad suggestion, because some of the old school attacks that we've seen for a while that aren't really too advanced, still leverage those principles where there is a hyperlink. And that hyperlink says one thing in the email, but if you hover your mouse over it, it shows you the true URL. So it's one of many things you can do you know, another thing that you can do is look at the domain, the source email that it's coming from, you know, oftentimes, we see this thing called a typo squatting attack. It's a fancy term for the fact that if I wanted to try to pretend to be, let's just say, online banking provider, who's already got an online banking provider.com domain, there's nothing from stopping me from purchasing a domain that looks just like their domain. And maybe I substitute, you know, an L for an eye. So it looks very similar. But unless the trained eye is really looking that's called typo squatted attacks, and so so another red flag you can look for is looking at that domain and the source and see if there's any red flags there that call out the fact that this is indeed a phishing attack.

Tamara Shoemaker 8:47
I truly love your very simple way of doing it as far as verifying it right. So I mean, that's one of the things that I do for sure is I don't ever clicked on anything, I definitely go with my bank sends me an email, I think my bank sending medium mail, I just go straight to my bank, on the web, no following any links and go in and check to see if they've left me

a message because that's where they're gonna leave me a message is in our secure account. Exactly. Yeah.

Shaun Bertrand 9:11
So you know, anything with text messages, right? We hear smishing attacks, those are a lot more prevalent today than they are...

Tamara Shoemaker 9:18
A lot more. I'm getting a ton now that it's political season.

Shaun Bertrand 9:21
Oh, my gosh, don't get me started.

Tamara Shoemaker 9:23
Right. It's amazing how many people want parts of our money? Don't worry, I'm broke.

Shaun Bertrand 9:29
Don't bother me. I have nothing to give.

Tamara Shoemaker 9:31
That's right. I've given all I can. But we're still there. So you know, you have to be careful. And that's a really, really easy way to do that. I think that's a nice straightforward way. You either pick up the phone or you go directly to the actual website, login and find out if they sent you something. And it's just that easy. You can avoid any of those kinds of things. What about the vulnerabilities that are inherent in all of our connected devices? What do we do about that?

Shaun Bertrand 9:57
That is a great question and there's no silver bullet answer. But there is a best practice that we can leverage. You know, every time we see an update happen either on a Windows device or an Apple device, and we have to restart or schedule a restart. What I will tell you is it is worth it, let those things do what they do, and you get an update on your phone from either Google or Android or iOS, get that update installed as soon as you can. That's first and foremost, because there is a time that the malicious adversaries are working to kind of basically weaponize the exploits against those devices. So the sooner you patch your device, the more protected you are against these future inevitable attacks that are going to occur. So update your devices. Now, when we talk about devices, there's two perspectives, there's the operating system, and then there's applications on these devices, right. So the operating system is generally the easier part you get a notification from Windows or Apple or iOS. And it's easy, but the application side sometimes isn't that easy. On your phones, you generally have your application set to auto update, and you should, that's what you should do keep your applications and an auto update. Some computers don't have that luxury Windows devices specifically. So I recommend a couple things. Number one, once in a while, go into your add remove programs and just remove what you don't use anymore. You'll see there is a long laundry list in most people's add remove programs, that you can clean up

some space on your computer. But also, as we say in our world, reduce your attack surface. That's fancy language for if this isn't a vulnerability anymore, because I removed it, there's that much less attack surface that the bad guys have to work with. So get those applications off there if you don't need them, and then update the ones that are more prevalent than others are more popular. And what I tell people is focus on things like the office suite, Java, Adobe, you know, things of that nature, make sure you keep those technologies up to date, as best that you can in those applications.

Tamara Shoemaker 12:00
Because most likely, those are the ones that folks are going to go after right, the vulnerabilities in those larger systems and those ones that they know people are depending on right, and that a much larger number of people have those on their stuff. But I'm loving the what you just said. So basically good housekeeping, right, now in and make sure you clean stuff out, you know, clean that closet out, you know, if you're not using it, why is it in there, you know, and like you said, making your attack area, your surface much smaller. And like you said, some of these world well known places are right on making sure that their security is up to date, because they do not want any kind of problems on their customer base. And so you can depend on that. That's a really good suggestion. And this is not something that takes a huge amount of skill, you know, on our phones, our apps and in our PCs and stuff, you just like you said, you just have to go to the settings and go to apps, and it's got install or update. Right. So this isn't some major technical issue.

Shaun Bertrand 12:56
No, it's not. And I think there's the other area that we didn't touch upon too much. But we should, or all these fancy technologies we have in our house, you know everything from your modem and your router to your smart thermostat. And the other. I'll give you the cliff notes version on what I feel is the best, you need to update these devices too. And sometimes they're a little harder than others trying to log into your router, you'd have to go to Google and learn how to do that. But please do it's not that hard, you can update what's called the firmware, which is just the software on the device relatively easily. However, you know, most home wireless networks and home networks, they offer the ability to basically split your network into an untrusted network and a trusted network. Okay, and there's a benefit there that is traditionally called a DMZ, a demilitarized zone. So in the untrusted network, this is what I do at home on my untrusted network, I have all these IoT technologies, my smart devices, this that all these things, I don't trust that Well, all right. And then over here on the trusted side, I have my computer, my desktop and the other devices that I use, but I trust. And the goal there is that one can't talk to the other. Okay, so if anything becomes compromising your untrusted environment, it cannot get here. And that is very important. So it's relatively easy to set these things up, you might have to consult Google a little bit. But overall, you should put all of those new technologies I just went to Home Depot the other day and saw a Smart Water Heater. And I'm thinking to myself, well, why why would I need a smartwater here? And I was thinking, well, it could talk to the thermostat and it could give me some good data and it's like, Alright, I can see a use case but there's nothing that's untouched now.

Tamara Shoemaker 14:40
Don't do that around my husband, please don't we then the next thing I'll have in my toilet, we'll be doing it and everything else. I mean for us. He's into tech just for the sake of tech. But that was a really good a really, really good piece there that we really need to make sure that we focus on that, you know, you have the things that you don't trust and you don't want to have a line of infiltration right into your actual trusted stuff like your PC and the things that you do you're banking on and all that kind of good stuff, right? Oh, the thing is, is that in industry, and all over I mean, it's like, for instance, that really, really big target incident that they had a couple of years ago at Christmas time they came in through the HVAC systems.

Shaun Bertrand 15:18
That's correct.

Tamara Shoemaker 15:19
Yeah. So, you know, Who woulda thunk it? Right. So I mean, like you said, now that we have all these things that are connected, it makes sense to keep those on the outside and the other on the inside. And that doesn't mean that we're using a whole different system or anything. It's just use the guest part would be for things like your TV, and all the other things that are trusted, and then your one with a good hard password, and much more software or much more firewalls and all that kind of good stuff on it would be the inside one where you're doing all your trusted banking, and you're working and all that. That's perfect. I mean, especially now with everybody home working, right.

Shaun Bertrand 15:54
That's the important thing. That's what we're emphasizing.

Tamara Shoemaker 15:57
And kids going to school, too.

Shaun Bertrand 15:58
Yeah, exactly. It goes around my untrusted network right now my two twin boys, you know, who are eating up a lot of bandwidth on a daily basis with video conferencing and other. Yeah, a trusted network. And that's a lot of the advice that we're giving our corporate customers as well. Its let's disseminate this language down to the consumers so that they can protect their home networks given that remote workforce.

Tamara Shoemaker 16:19
And it makes just so much sense. And the other thing too, I think that maybe you talked about was that all of those things also need to be updated as well. And so if they're not trusted network, it's okay that you put it on automatically update or do whatever it does, because it's not going to be able to touch anything else is going on in your actual computer and that kind of stuff. I for the longest time blamed my cat, for turning the TV on and off is the bizarre thing. Every once in a while we would come out of the bedroom in the morning, and one of the TVs and another part of the house would be just turned

on. And we didn't know what it was, until one time it happened with us. While we were around. The TV was updating itself.

Shaun Bertrand 16:57
No kidding. Yes. all over the night... Yeah, it just stayed on after it updated. And it had a little question on you know, do you want to restart or whatever it was that it did, but it was letting you know that it had just updated itself. But the first couple of times it happened. I'm thinking dang those cats.

I liked you're blaming the cat first. Blamed the pet first.

Tamara Shoemaker 17:16
It wasn't on animal channel. So I knew there was something else up.

Shaun Bertrand 17:22
Classic.

Tamara Shoemaker 17:23
But for a long time. It took us a while before we figured out what it was, but it was updating itself. But again, that can be a bit scary if you're not in control of that.

Shaun Bertrand 17:32
Oh, absolutely.

Tamara Shoemaker 17:33
And you're inside, then you're okay, right. I mean, we talk about that in cybersecurity all the time, right, sort of how you have different zones and how you have separation of duties, and separation of access, and all that kind of good stuff. So this is a really good home suggestion for folks. Because as we're adding more and more of these IoT's, we're also increasing the vulnerabilities that we're putting in our homes. And like you said, Now that we're all working from home and stuff, we really don't want any of that kind of stuff to happen with anything that we're doing with work, and then have some kind of long range effect on our careers and our livelihood, all that kind of good stuff. Right. And just for the companies, I mean, you know, we want them to stay in business. I don't want to be responsible for having had something happened in my own home that caused the university to go down.

Shaun Bertrand 18:16
Absolutely. Yeah, there's that sense that we need to take a little bit more prioritized approach to home security and personal security than we ever have. It can affect our future careers and all the people that we're connected with business wise, and friends and colleagues. So...

Tamara Shoemaker 18:31
So that brings up a good thing. Like you said, one of the things that we do is we see a lot of things in the past that get us a little nervous, a little scared and make us really

leery about, oh, gosh, I can't take care of cybersecurity on my own. It's just too complicated and too hard. And one of the things that I know that's out there like crazy right now is this ransomware stuff. And I always joked earlier in my career, not lately, but earlier in my career, well, they never going to come after me because I don't have anything they want. That was before I started to realize that they're going to go to the one that's the least protected to get to what they need to get to. And I was probably one of the least protected right? So I was that what am I a husband always says you don't have to outrun the bear. You just have to outrun your buddy.

Shaun Bertrand 19:13
The person behind you. That's right.

Tamara Shoemaker 19:16
So even though I don't have much that they might want, in this day and age, that's not exactly the only thing that you need to worry about. Right?

Shaun Bertrand 19:24
Yeah, you know, first of all, let's define what ransomware is. ransomware is essentially a virus that is designed to lock up your computer or your most important files. And only give those back to you after you pay these malicious hackers a ransom right. And this is a very well operationalized business model that these bad guys have going for them. As some insight to this attack. The way you pay a ransom is through this thing called digital currency or Bitcoin. And all you really need to know is it's a anonymous currency and most people don't I talk to you have no clue on how to pay Bitcoin. So these bad guys actually have a call center that you can call and they will walk you through how to pay the ransom to make it as easy as they can on you. And then people also talk to me and they're like, what are the chances that if I pay the ransom, I'm looking at my files back. It's like 99%. Do you know why there's a business model and of level of integrity that they have to adhere to? Because if they stopped giving the files back, people would be less inclined to pay the ransom down the road, right? It's absurd. And it is a threat to consumers Tamara, it's a big threat. You know, people say I don't have anything thereafter. What would you do if I locked up all your pictures and videos that you've had over the last 20 years, infiltrated your computer to know that I could get all of that locked up. And that's a big deal. There's a price tag that people are paying for that. And there's certainly some best practices that we can follow. But it's a real threat. It's something that consumers need to be aware of, both in the workplace and at home.

Tamara Shoemaker 21:04
From what I understand. It used to be we only thought of big corporations of being people that they want to get but what they're doing now, because they have business standards for this, they have large groups of people working on this together as companies, right. And so it's okay, if they're only getting a small amount from a lot of people, because it adds up, right, what to understand and the research that I've read before, this kind of crime is outpacing the drug crimes, that cyber crimes are taking more revenue from us than the drug crimes are.

Shaun Bertrand 21:33
This is a billion dollar industry, and maybe soon to be trillions. I mean, it is unbelievable. 20 years ago, when I got into this thing, you saw companies getting hacked from people that just wanted to show off, they were showing off and they were like, cool, look at me, I earned some stripes on maybe. But since then, the transformation that we've made into this monetized kind of commodity based hacking, from ransomware, to blackmail, to extortion to these things called denial of service attacks. It's unprecedented. And I don't think we've reached a plateau yet.

Tamara Shoemaker 22:06
It's all big business now... we have to learn how to protect ourselves from me. So what are some of the things we can do?

Shaun Bertrand 22:13
Well, with ransomware and phishing, they go hand in hand. First, let's connect the dots generally speaking, a ransomware threat to a consumer and often a business is going to arrive in a phishing email, not always, but a lot of the times, and if it doesn't capitalize on phishing, it's going to likely capitalize on a vulnerability on your system. All right, and again, not hundred percent those who but generally speaking, those are the two major ways that you're going to see it. So all the principles that we mentioned beforehand with the phishing hold true here, especially with malicious attachments. You know, one thing we see what's weaponized a lot are Office documents, Excel documents and Office documents, you get something from somebody that you don't know, or in some cases, even somebody that you do know. And you generally don't get this kind of attachment or email again, let's validate the authenticity, not by replying to the email, but reaching out and calling this person or finding a different way to communicate and see. Also, we talked about the importance of updating your systems, people still ask me today's anti virus worth it? And the answer is yes. All right, it is possible. For groups that I run, we run an ethical penetration testing team at CBI and we have abilities to bypass some of these technologies. But it does do a good job at identifying a lot of these threats. ransomware included. You know, a lot of people don't know, on a Windows system, if you're running Windows and Mac has some similar functionality. They have a ransomware protection option that you can enable, you can check a box and it will prevent the ransomware from infecting other files on your computer that goes a little bit beyond the traditional antivirus. But, you know, understanding those controls and some of the features that you have are another good step to making sure you're not affected by this very probable and viable threat that's going on.

Tamara Shoemaker 24:02
I was blown away. You saw my reaction, right? We're talking to each other through zoom so we can see each other even those will be a podcast. And when you said that, folks, they're still asking whether or not they need their security tools. Yeah, I'm just blown away. Right. So it's like some of these things just haven't changed, right? It's like, Oh, well, I don't really need all that junk, do I? And I'm like, Ah...

Shaun Bertrand 24:24

Now more than ever.

Tamara Shoemaker 24:25
Yes, Yes, you do. And they are improving at all. They also are adding things like password managers, and they're also adding two factor authentications in with all that. So you've got all these tools at your disposal, but you have to use them. You know, one of the other reasons I know that they also like you were saying you're getting a file from somebody that you don't normally get files from and all that kind of stuff and you think well but it's from you know, Sam and I know Sam or whatever it's like, does it hurt to send Sam a separate email saying Sam did you...

Shaun Bertrand 24:56
A test message. Yeah, because guess what, Sam's account could have been compromised. And again, bad guys that are sending you that.

Tamara Shoemaker 25:03
You know, I don't know how many times I'm faced with when I'm talking to my K through 12 kids on these subjects. And when I'm talking to my older generation, right, my senior citizens and stuff, and I'm asking them, do they pay any attention when they download all these lovely free apps? are they paying any attention to what permissions they're giving those apps?

Shaun Bertrand 25:21
True.

Tamara Shoemaker 25:22
And they're like, what permissions?

Shaun Bertrand 25:24
What does that mean?

Tamara Shoemaker 25:26
You know, I'm like, okay, I mean, I get that you don't want to be reading all of, you know, this huge contractual language that's difficult to understand. But there are a few things that when you load something, it'll ask you about whether or not you want to do and I'm always amazed at the amount of free software that asks for things like my contact list, correct?

Shaun Bertrand 25:47
Or access to your microphone, or your camera...

Tamara Shoemaker 25:51
Or your location. And it's like, wait a minute, I just downloaded a flashlight app. Why do you need my stuff? Yeah, I don't need that for that kind of a service. Thank you very much. But I don't need to track me while I'm trying to find my way around in my house with my flashlight.

Shaun Bertrand 26:05
Privacy is a big thing, though. Right?

Tamara Shoemaker 26:07
But I'm just saying, you know, the things that they are asking for are ridiculous. And so you know, many times I often tell the kids and the older people, it's like, you know, maybe you can pay the dollar 99 for the version. That's not asking for all of your personal information. You know, I think that that buck 99 is probably worth it. If you're going to be a tiny bit safer. You know, you get what you pay for sure. When you're not paying for it. I think you get a lot of undocumented help, that maybe you didn't really ask for.

Shaun Bertrand 26:34
You might not have signed up for that undocumented?

Tamara Shoemaker 26:37
No. And that's a difficult thing. Because everyone's trying to... Oh! that's so fun. And it's free. You know, I might as well do all that. Is there anything else that you can think of that we can tell folks that are listening that can help them now, like you said, Now more than ever COVID it's got us all, working virtually and living virtually. And it's kind of scary out there in this.

Shaun Bertrand 26:58
I think a couple points that I'd like to drive home, it has to do about passwords, right? Something that we've heard a lot about, and it's very hard. We've been told over the years, we should have something uppercase, lowercase numeric, special characters, it should be eight characters or more. It's a lot of complexity for people. And one of the things we try to drive home is you should use unique passwords on different sites, right. So if an attacker compromises your Netflix password, somehow, that's the same password you're using for online banking, guess what, it's going to be a bad day for you. So what we have really shifted away from is, instead of all these uppercase, lowercase Numerix, we want something that is longer. Okay, we want a password that we actually call a pass phrase. All right, so think of something like all rocks roll down the hill today, it's pretty easy to remember, don't use that, by the way. But that's what we're talking about is having something that we can remember that still, because a longer password is harder to crack, you know, passwords are stored in an encrypted form. And it's possible to try to break that encryption if you're using a weak password. Another example is never use seasonal words, in your passwords, we see a lot of fall 2020, exclamation mark or summer 2020. It's funny when I give security awareness training in person to large audiences. When I say that I see like 10 people put their head down, like oh, my goodness, that's my password, gonna change that when I get back. So you know, make these passwords longer. And then as you mentioned before, Tamara, are a great point with password managers. There's no way we can organize all of these passwords. It's risky. If you do it on your computer, with like a notepad file or something, there's risk and doing it on paper and putting it in the safe a little bit. I actually kind of

like that a little bit more sometimes. But bottom line is there's tools and technologies that help you with this. I don't get compensated, but things like LastPass. LastPass is a good tool. It'll basically control all of your passwords in a secure way, with one master password. And that brings me to my next point, you cannot simply have on LastPass one, just password you have to use what's called two factor or multi factor authentication. When my family and friends come to me and they say what's the most important thing I can do? This is my answer. two factor authentication. So what is that? Since the dawn of proving we are who we are, there's been three ways that we've done that. What we have, what we know, and what we are, okay. So what we have might be an ATM card, what we know would be a password, and what we are things like biometrics, right fingerprints and Iris scans and all the cool Mission Impossible stuff, right? Only when you combine two of those three, does that equate to a secure authentication or a secure process right? You use two factor every time you go to the ATM When you go to the ATM, you have your ATM card, you put it in, and what you know is your pin. Without any one of those alone, you can't get money out of the bank. That's two factor authentication. There's not a site in the world now, that really doesn't support two factor. There is a few of them out there. But basically every online banking platform, Facebook, LinkedIn, all your personal sites, the best thing you can do is go out there. And it's pretty simple. Nowadays, you register, you usually get an app on your phone. And when you log in with your username and your password, next thing is you get a pop up on your phone, and it says, Do you approve of this login? And if you just logged in, you would click Approve. And that's it. If this pop up, occurs at two in the morning, when you're sleeping, or when you didn't log in, you should not click Yes, you should click No, I did not log in. But it's a great way to really secure yourself use unique passwords that are longer and enabled as two factor authentication on everything that you have. Those are really important topics.

Tamara Shoemaker 31:03
Well, and I think that you hit on the fact that it's not a complicated issue, right. So that everybody's offering it, you know, all the places that you really need to have really, really secure like your banking and your work logins, and maybe your larger accounts that have a credit card attached to them, in some way, shape or form. But it's much easier. Right? You and I probably remember the day when we had a little...

Shaun Bertrand 31:25
Key fob.

Tamara Shoemaker 31:27
Right! That would send a secret code to you. So that was a little bit more complicated, right, setting it up and getting the key fobs sent to you and all that kind of stuff. But now, like you said, because we're all using our cell phones, you just give them the cell phone number one.

Shaun Bertrand 31:39
Yeah. And this is what you have. That's essentially like your ATM card kind of.

Tamara Shoemaker 31:43
Yeah, absolutely. And then you get that text, and it's no big deal. You get Yep, it was me and you're good to go. And but now you know for sure. Like you said, somebody is not going to be able to get in there without that.

Shaun Bertrand 31:54
That's right.

Tamara Shoemaker 31:54
And the password thing. I'm just like, do you need security software? The question of do you have good passwords is just cracks me up that it's still one of the number one ways that people get busted. And when I'm talking to the camp kids and all that kind of stuff, I have all these crazy videos about how bad people are at this, you know, 123 is their password that the computer may have come up with and all that kind of good stuff. But surely it's not as complicated all that, and I loved your explanation about a phrase, you know, think of a phrase that you can remember. And that's a really cool way to do it. And then like you said, if you've got hundreds of passwords, like we all do, using a password minder is a great idea. And there are tons of them out there. And even our security software is bundling those things in together. So it comes with so you know, it's really not as complicated as it used to be. So there was there easy things to think about. I truly appreciate you giving us all your words of wisdom here, your many, many years of experience in the field, working with large enterprises, small and medium businesses, all kinds of different sizes, keeping them safe, and being able to talk to some of our folks and keep them safe is really important to us here at the University of Detroit Mercy and at CBI and really, really glad that you took the time out to share that with us.

Shaun Bertrand 33:05
Thanks for having me. You know, it's really important. We enable the community in any way that we can and we have a ways to go but with some of these measures, we can really improve our security and cybersecurity hygiene. And I'm honored to have had the opportunity to talk to the audience today. Thank you Tamara.

Announcer 33:23
You've been listening to the Detroit Mercy Cybersecurity 313 Podcast. If you would like more information on today's discussion, please contact Tamara Shoemaker by emailing shoematl@udmercy.edu. And please plan to join us again for the next edition of the Detroit Mercy Cybersecurity 313 Podcast.