Basics of Cybersecurity

CyberAware Podcast: Season 2, Episode 1

Nathan: All right, everybody. How's it going? Welcome to season two with the CyberAware Podcast. My name's Nathan Sloneker. I'm a student on the information security team at Minnesota State University, Mankato. And I'll be your resident expert on all things cybersecurity. And I'm here joined by Ham.

Ham: Hey, what's happening guys. I'm, just your regular average everyday guy, but you know, I'm also a guy who loves to game. I work here on campus in the CSU as part of their kitchen and, it's great to be a part of this team, man.

Nathan: Welcome aboard. All right. So for our first episode today, we're just going to be talking about the basics of cybersecurity and just starting off you Ham, what do you know about cybersecurity?

Ham: You know, Nathan? I don't really know a whole lot about cyber security, but I make sure to keep. My password's tightly-knit over 14 characters. Surprisingly. I can remember that stuff. I travel a lot, so I don't try to like jump on open wifi. Who knows what could be on those, like wifi bands, try and sneak in some of your information, right?

Nathan: As far as tips go, those are very good practices to have. I have a few friends here who, you know, or even, I know people who have the same password for their bank account, that they do their Instagram stuff like that. Some of the stuff they're going to be talking about is why you probably shouldn't be doing that sort of stuff.

So just starting off here, for anyone who isn't familiar with, what cybersecurity is, it's the practices of just protecting, computer systems, networks, things like that, all things cyber, and it important again. How much stuff runs on the internet nowadays and technology, all that sort of stuff.

Backbone of all that is cyber security. And, as for our message, for our team in general, it's being cyber aware that's our message that we're going to be pushing out this whole season is what it means to be cyber aware. And on another question for you, ham, is that when you think of cyberaware, what do you think of, you already had good examples, but are you familiar with our message?

Ham: Not really Nathan, to be fair with you, like just being cyber aware is something that I tried to learn a little bit more in high school to see what was really there. But in reality, I really don't have any clue what's going on.

Nathan: Okay. Yeah. So being cyber aware, as we said, it really falls back on the safe cyber security practices, knowing what you're doing, being smart in what you're choosing to do, what you're clicking, all things like that.

Some of the things we're going to be covering in this episode are just that. For our backbone to be cyberaware as our main message, which is the four P's of cybersecurity, which has passwords, patching, phishing, and protecting your devices. Are you familiar with any of those?

Ham: I'm really aware with phishing because like just how people go and just try to like, go for those. I'm going to say key words, like when you're signing on to like a wifi okay, what's your password. Or it could be, you got to sign in like a birth date, like what's your birth date? And that's just one piece of information that they could use to try and snag something of yours.

Nathan: All right. Just going off some of the things with the four P's ham, have you again, you're you said you're familiar with phishing. What is phishing do you have, and have you ever experienced it?

Ham: I've experienced phishing a whole lot. I'll get emails left and right. Asking for a reset password. Even in this day and age where everything's online. We were ordering stuff online, Amazon, you name it, you're entering passwords, left and right. You're getting emails from everywhere.

Right. It's people are so. Destructive trying to get your information. They'll go to great lengths to do anything.

Nathan: Let me tell you this. So last week I actually had a, we had someone, a phishing email. I found its way to a couple employees on campus and we had a, it came through and with me being on the security team, I investigated, I go into the VM, a virtual machine.

Yeah. Yeah. And I click on the link and go see what's going on. I'm not kidding. This was the most legitimate site I've ever seen. You clicked on it. It was branded purple. Oh, the whole thing. And it just, all it said was enter your password. And me being the jokester, I just typed in some random words and it just said thank you , That's it.

They want you to log in and just said, thank you. But I mean, most legitimate phishing email I've seen today just with how the branding looked on it and think people are getting sophisticated with it. You might have the odd one where you get something you're like, really? This is the best you can muster up? but we've been having, yeah.

I genuinely. Impressed with what I saw last week. And it just goes to show, with how far some of these things can come when it comes to other things, phishing, there's a, an example that we'll talk about later called whaling it's it's kind of a variant of phishing. There's like spear phish, and you're going for select people, wailing.

You're going for the top guy. You're going for the executive. You're putting in the effort to make it look really legit and I mean this was just not on the same level of any sort of way, but this is just goes to show you how sophisticated some of these things are starting to get and how methodical and thinking people are with, okay, how can we get this?

How can we attack someone with this? It's not just throwing something at the wall and seeing if it sticks.

Ham: Oh, it's so crazy. Like imagine someone taking the time and the effort to really make a webpage that's so branded perfectly like just to the Minnesota State University, Mankato brand itself, the purple and gold, everything like you were saying, like that blows my mind that someone would go to great lengths to try and make something like that happen.

Nathan: And it's crazy. It's not just Mankato, we're not just the only people is having to it's happening to ton of companies, ton of other colleges, even your home, whatever it could be. Okay. This kind of looks like my provider of some sort or whatnot, and this doesn't even get into phishing where you might have something like phone calls.

Yeah. The robo calls that everyone receives a million times a day in today's world. So yeah, and then another thing that I thought we should cover is patching. Are you familiar with what patching is? I know about like patching my games. That's really, that's pretty close, patching, just fixing improvements on anything that's broken, or anything that might be out of date, stuff like that.

So patching is one of the things that we also recommended and that kind of just follows in the same. Keep your devices up to date and we're going to be covering just kinda the, top what vulnerabilities can happen. And why that's one of them,

Ham: that's a great, that's a great topic to talk about because my old laptop that I have is still runs on windows 98, and it is a beef of a laptop. But let me tell you, I don't, the amount of viruses I think probably has, is incredibly high, but just because like I was a young kid back then, I didn't know what to look out for. And now like now my like home-based computer. I only visit YouTube Facebook, Twitter.

Nathan: I don't know. I don't know if you've ever had a Mac before. Are you familiar with Adobe flash?

Ham: A little bit.

Nathan: I don't know if you recently heard that actually went out of date. Like they're not supporting it anymore.

Ham: Wait, are you talking about the original Adobe flash that would run like flash games?

Nathan: Yup the original Adobe flash and it actually is like a hot spot for like malware and viruses. Now people have their update, your Adobe flash. We have, there's a one, malware that's associated with it called Shlayer. Interesting. I've never heard of that. And it's one of the, we get that, just through our email, our alerts, we have that, every other week we have at least one of those come in cause someone.

Has something, they still have Adobe flash on the computer. So for anyone who's out there that has Adobe flash get rid of it. Okay. It's not supported, not needed anything like that anymore.

Ham: I can't play club penguin anymore.

Nathan: Nope. All right. So yeah, just backing off safe cybersecurity practices. So you were you earlier, you were covering what you do in your own time. Do you notice anything that you see other people do that you're like, why, why do you do that?

Ham: Oh, all the time. Like if I'll, I'll go down to the coffee hag here in Mankato and like, yeah, they got a free, they got free wifi down there, but like, I'm going to be honest with you.

When I go down in there, I just jumped right on my phone. I do all the stuff from my mobile device because it's tagged to like my LTE, my 4g network. And I don't need to worry about anybody being on the same network as me because like people who are like super, super smart. And like, know, all this computer savvy stuff, if you're on the same network, people will find ways to wiggle their way into your system and they'll find ways.

Nathan: You can fairly easily find out who else is on your network. But yeah, just with a wifi in general, the free wifi that you're talking about, coffee shops, airports. Oh, airports. Don't if you see free wifi, don't use it. Not a good idea.

If it's not password protected, you have no idea what sitting on the other end of that network. Safe clicking, know what you're getting yourself into and know what you're clicking on, know what you're going to be searching, know where you're going. Okay. Don't just randomly, okay. Yeah. Let's click, let's go.

I'll log into this wifi. I'll click on that link. Just a horrible practice overall. No. And just be mindful of what you're doing and that'll keep you safer. Cause that click could accidentally download something on your device or that click could log you into a wifi network. That's unsafe.

Ham: Yeah, that actually brings me to a really good story. When I was really young, on one of my older, older laptops that I used to have I was on YouTube and I was just, scrolling, watching through videos left and right left, right, blah, blah, blah. And I went down this huge rabbit hole.

And then onto this video that I was like super interested about, I was like, click this link and it'll, give you a coupon code, blah, blah, blah. And me being the dummy that I was, I clicked on that coupon link a little bit. I know. Downloaded the Trojan virus onto my laptop. Fun. And it was completely unusable after that.

Nathan: It, yup. That's just backs up to safe, clicking, , sorry to hear that that happened. I'm sure it's been a learning experience though.

Ham: It really was.

Nathan: yeah, just even off the wifi and stuff. Do you, I'm sure you game a lot. I take it.

Ham: Yeah I game a lot and, I got a VR set. Okay. Virtual reality. Little did I know is that those VR systems don't have any malware or like antivirus protection inside them, yeah, I didn't know that either.

So little did I know that people were able to like trace my location through the headset? Yeah, actually literally, literally it was the scariest moment of my life. It got to a point where I was chilling. I was on VR in a game called VR chat. Right? Yup. And I was chilling in with this world with a bunch of people and I got it.

I like, my computer just started pinging me left and right. I was like, what the world's going on? So I left my head set up and I see like these Xs all over my screen. I was like, oh my gosh, what is going on on your computer screen? My computer screen. So I had to lift up my headset and I just kept hearing these pings .

And there were error messages all over my screen. And I was like, what in the world's going on until my VR set blacked out and it just died. And I was like, wait a minute. What's happening? Okay. So I immediately shut, I hard turned off my computer. Okay. I was like, I'm not going to go back on my computer for a couple of days. And I just left it alone.

Nathan: Okay. And when you turn it back on, it worked. It worked just fine, everything worked. So, yeah, with the four P's of cybersecurity, we have patching passwords phishing and protecting your devices. So passwords itself pretty simplified, , have a good password. Don't share the same password, everything, , most passwords nowadays you'll see the weak medium strong.

Always have a strong and double, the strong is my double it, so I'm, I, , always don't have the same password that you have for your Facebook that you have for your bank, that you have for your email. I myself have different passwords for everything and they're 25 plus characters long and just jibberish, absolute gibberish.

And I have a, I had a few buddies. I mean, one of my buddies the other week, actually last week itself, one of my friends from back home actually had his, his work email got like. Hacked in a way. And we found out that it was from somebody in Ukraine is where it was located. It could have been a VPN, but we just saw Ukraine.

I was like, Hey, what password is this for? And he told me, oh, I have this password for my work, not my bank account, but I have it for my Instagram and this. Okay, go into your email, find all the accounts associated with that email and that profile, go change your passwords immediately.

And this is for anyone who's listening with your passwords. If you have the same password for anything, don't if I could recommend anything, take an hour out of your day, go through and just change all your passwords, , put them somewhere only that you know, where they are and just go through, take an hour, change all your passwords on everything.

And that way you'll know it'll be safe. No one else can have that sort of thing. Cause as I was saying password stuff, they get leaked.

Even your credit cards. It could, someone could have bought in your credit card off the deep web auction. Years ago, and they're just waiting until they actually need to use it. You're one of a thousand that they ended up getting and it's just, yeah, just protecting your password, having a good password, all that.

Keep your stuff updated, change your passwords frequently. Always a good idea. Okay. And next, for the four P's we have protecting your devices, ham, what do you do to protect your devices?

Ham: I try to take, the average everyday guy approached everything like. I got my phone, I got my computer, I got my tablet.

I have all these things and I have different passwords for each device smart. So like, even though on my phone, like really in reality, I just shake it and I turn it on because I'm the only one who touches my phone. I never leave it anywhere. I don't go anywhere without it. And it stays in my pocket, , as for like my computer and my tablets.

Yeah. They're linked to my Microsoft account, but I have different passwords for each of them just in case. If anything happened.

Nathan: Okay. And just the thought process for a year. Do you have like a four digit password on your phone or what? What kind of security do you have on your phone? ,

Ham: Honestly, nothing really.

Nathan: Okay, if I were to ask you, what kind of things do you store on your phone that you might not think of? , do you have social media? I do, emails. Yep. Student. , just personal email any banking information? No, no banking apps. Nope. Okay. That's smart. Do anything else that you can think of that you have on there that I overlooked or you have contacts?

I got my contacts, messages. Okay. Now how about you? Do you play on a PC laptop? A PC. Okay. What, how about the PC. How much, how much stuff, important things do you think you have stored on there? I, you know, probably 80%, probably really important things are on my computer. Yep. And just going off of that, if that computer became vulnerable.

Or I would be in detriment. Exactly. So, yeah, just going back off the protect your devices, if you just want to take, take a minute and think about everything that you have stored on your phone, your computer, your tablets, how much are your stuff? Oh, I have my banking information. My Amazon, oh, well, my Amazon's tied to my credit card, my Netflix account, or, you know, my Facebook has my contacts, my address, where I went to college, all these things.

It could be just found vulnerable. If anything were to happen to your devices, so just keep protecting your devices, keeping your devices, just up to date. Make sure it goes off of the

four P's of cybersecurity, all that stuff. Keep them up to date, keep them secure. Don't be just giving your password out to anyone don't just lend anything out whenever, stay smart.

Cause again, just do a thought, just take a minute and think about everything that you have on these devices. And you'll be like oh my, I have a lot of important stuff here

Ham: Exactly and there's one thing, you have a Mac or a PC ?

Nathan: I have a Mac a Dell and a PC.

Ham: Okay. So you got them all. When you're like, when you're logging onto a website, say Amazon, for example, right? And Google says Hey, do you want to save this password for this website? Never. Never. Absolutely not.

Nathan: I agree with you there.

Ham: Like Google, why are you trying to save my stuff? I don't want that. This Is my information.

Nathan: No, a hundred percent agree. I don't save passwords, not a fan of it. I know my password. I don't need you to know my password. I know some people are lazy and just like, eh, you know what? I don't want to type this in every time or don't save it better practice that way, after typing it in five times, he usually can depending on how long it is memorize it pretty quick.

Alright. We start talking about personal security. Now we can talk about businesses and small businesses and, one of the biggest vulnerabilities do you, I, if I were to ask you, what do you think the biggest vulnerability that most businesses have is.

Ham: Honestly, I would have no idea to be fair. I'll keep going to the example of open wifi. Yup. Who knows, , some person you're in, , some hacker guy could hacker-man his way into it and be like, now he's in the network. And he is, finding all the credit cards that have been stored through the, the card swiper or there, or if they're new to the business, they'll have the like the apple scan or whatever, it's called.

I'm not, I can't remember what it's called, but like all that information. Goes to the phone and then that gets saved into their database.

Nathan: That is a great example, what I was going to say or what I personally believe in what is usually the biggest vulnerability people.

Ham: Oh, okay.

Nathan: If you think about it, as you were talking about, the the hacker man, quote, unquote, all this sort of information, and it comes back to even phishing.

If you're trying to fish, you're phishing. someone Not a machine, not anything. It's the person who click on that, make it vulnerable. Yeah. Or, someone, oh yeah. I'll hold the door for you and you can get in, if, depending on who we have in future guests. I know a story that if we have a certain person, they might tell, so that'll be pretty fun when they're here.

But yeah. As far as I can say, People are sometimes the biggest vulnerability and it's not like we mean to be, it's just, we, people are trusting most of the time. So, when it comes to, okay, that looks legit, I'll click on it. Or, y'all hold the door for you or yeah. , here's what you need.

What do you, I can help you out here? And that just falls into security awareness and just going back onto the cyberaware again, if you can big, small, however, even within your family, Cyber aware, do you know, just teach people, and teach everyone that you can about the dangers of the internet and the internet can be a great place.

It can be a fun place. It's just be smart with what you're doing. And when it comes to, businesses, big, small, training people and just teaching them about, , how to be safe and how to be, just on top of everything they're doing and just be aware of anything that could be going on.

Always a great thing. So, safe practice. Always, always, always going to recommend that. And when it comes to, businesses, big and small, some of the issues that it has with security, who do you think has more funding for security?

Ham: Definitely bigger businesses.

Nathan: Exactly. Yeah. So that's actually, , we're going to cover that in our later episodes is a big attack that I'm sure you've heard of ransomware.

Ham: Yep.

Nathan: Yep. So we're going to be covering just kind of how the businesses themselves can, tie into ransomware. All right. So yeah, just going off as I just talked about ransomware threats in the cyber world , how about you, can you list any off the top of your head that you can think of?

Ham: Oh gosh, I'm trying to just think,

Nathan: you've mentioned phishing, phishing. Hackerman you mentioned hacking.

Ham: I remember the leak, the leak information of the PlayStation network. If you remember that many years ago, there was

Nathan: what was Xbox lizard squad.

Ham: yeah. Yeah. I remember that over that, ah, man, that was rough.

Then there was the security dump of Facebook when that happened. Oh gosh. Like these big, it doesn't matter who you are. It's everybody's at risk.

Nathan: I've had one of the people who I've learned from telling me for, it's not a matter of if it's a matter of when, when it comes to your vulnerable, everyone will, at one point, it's not a matter of if it's when, so yeah, just going off what you said, you covered hacking phishing.

So other big ones, as I said, ransomware, credit card fraud. I mean, have you ever been a victim of credit card fraud in any sense or know someone?

Ham: No, not that I know of.

Nathan: Okay. Anyway, continuing on. So as we said, we covered, , the types of threats in the cyber world, hacking ransomware, phishing, fraud, as I said, credit card fraud, big one nowadays.

Another one cyber-stalking big one, someone finding your address and all things like that, that could tie into it a little bit. Just the same sort of sense.

Ham: Like DDoSs attacks and. And having someone know your location literally to a T.

Nathan: Yup. Okay. For anyone who doesn't know a DDoSs, it's a denial of service. So basically I can fry your router more or less, or your wifi.

Ham: My favorite.

Nathan: Yup. So if anyone has your unit, your network information, your IP, stuff like that. And for a big thing is DDoSing happens a lot in video games for anyone who doesn't know if they get you in a network or they're in the game with you, they get, you guys are linked through the game, , your networks are paired because you're playing together. They can then use that to basically boot you off through your wifi or, boot, your internet, whatever you have. And then you will be obviously off the internet. Your internet went down. Game's going on, but you got kicked.

Ham: Yeah.

Nathan: So yeah, DDoSs, denial of service. And another one social engineering, as I said, people will social engineer, their targets know who they're looking into, , who they're going for. And as I said, people are trusting, they might try to get this information from you.

You might not expect anything from it. And then bam. Vulnerable!

Ham: Boom. It happens.

Nathan: And then we already covered whaling earlier it's going for the top executives, stuff like that. And this can tie in, here's another one called spear phishing. Where it could be okay,

I'm taking this person, this person, this person, and then whaling is. I'm top dog, I'm going right for. We're going right for, the top of the line, who's at the top of the food chain here.

Some of the top vulnerabilities in our daily lives that we can handle as I said, one of the biggest vulnerabilities is usually people when it comes to technology. And even going off, just the four P's that we were talking about earlier is patching. So things like old devices out of date devices.

Always can be vulnerable, keep your things up to date. Always, always keep things. Up-to-date apps, devices that you have, all the time. As we also said, goes and ties into the patching and you with the four P's out-of-date devices, old devices, keep your stuff up to date. And when it comes to old devices, certain things like mac's I think having an expiration date, we're past a certain age that they can't actually get any more updates or they can't, , get the new big sir update.

Ham: Sure.

Nathan: And then another big vulnerability is zero day vulnerabilities. I don't know if you're familiar with that?

Ham: I honestly have no idea what zero day vulnerability is actually at all.

Nathan: Zero day vulnerabilities are something that , like a provider might be aware of and the customer might be in the dark about it. And the provider has known about it the whole time and might not say anything, and the longer it goes on just the bigger issue that it could be. So yeah, that can be a pretty big, , issue when it comes to some big developments or some big software that.

Ham: Interesting.

Nathan: That's how we never knew. Or we didn't know about it. They might've known about it, but just kept in the dark

Ham: That's fishy. Yeah. That's some fishy stuff.

Nathan: So, yeah, I mean, that's just a general cybersecurity guys, , and just being cyber aware if you want to have some more tips on that, just check out our website or just tag along in later episodes.

Cause we're going to be talking about more of these kinds of issues. so yeah, big takeaways from this episode, and just being cyber aware. Being smart on what you're doing on the internet, making sure people that, , are being smarter than the internet, that ties into, having a good password, safe, clicking, all that sort of thing.

How about you? What, what would you recommend for, some viewers.

Ham: I say the three big takeaways for myself is like, make sure, what you have, make sure your information is safe. Being aware, like passwords is a huge thing for me. Like I have a different password for just about everything that I logged into.

You know, patching, make sure your stuff is up to date, making sure everything's ready and ready to go. and honestly, I didn't know about like the, the term of whaling. I thought that was crazy. And they all people going for the top dogs that's mind blowing to me.

Nathan: Yup. It's interesting stuff. What, what kind of attacks, and we only covered a handful there's so much more out there that we can cover in later episodes, but this is just some of the main ones that we wanted to bring up this episode. So, yeah. For anyone again, with the website, just go to mnsu.edu/cyberaware, for more information on that sort of thing.

Again, Ham, thank you for joining me for this first episode and thank you for everyone. Who's listening!

Ham: Dude. Thanks for having me on this has been such an honor. Thank you.

Nathan: I'm glad to have you. And now we're just going to pass it off to Mercy for the current news

[Music]

Mercy: First update today, gamers be aware. Malware hunts epic and EA origin accounts. A new malware in the hunt today is BloodyStealer that swipes data, including cookies, passwords, bank card information saved in web browsers, screenshot login, memory and application sessions. Third touch made by Kapos, a big demand on the dark net for stolen game accounts that are going for a very attractive price. Gaming accounts are clearly hunted by cybercriminals. So if you want to enjoy gaming peacefully and not worry about your ingame credit, or accounts being gone, make sure you protect your account with two factor authentication and use our reliable security solution to protect your devices.

Our second update today.

Emails chat logs, leaked online from a far right militia link to the U S Capitol riot. Emails, chat logs, membership records, donor lists, and other files were leaked by a group called oath-keepers. These also admitted they're real in the January 6th storming of the U S Capitol. Some ofthe data leaked online was 160 of the U S government and military email addresses.

Our side news added today is TangleBot malware aiming at Android devices cyber-security

company called Cloudmark has recently identified a new malware that can take over a victim's mobile phone through SMS. The way this would work is you get a text message. A link. Once this link is clicked, you read a receipt to a website asking you for an Adobe flash update. This malware also has the ability to take over your devices functions that may include a contact lists, your phone history, camera and microphone, along with the ability to use the internet, be aware and avoid clicking links from numbers. You do not recognize.

Another malware on the hunt called "Shlayer" has the same ability to ask you for an Adobe flash update. And once this is clicked, it has access to your browsing history and may also pave way for other malware to be downloaded on your device. And that wraps up the news for this week. Thank you for listening to the cyber podcast. We'll see you next time.