Risks 101: Check & Protect

CyberAware Podcast: Season 2, Episode 6

Nathan: All right, everybody. Welcome back to the CyberAware Podcast. Today, we're going to be going over episode six. What is risk assessment? My name's Nathan. I'm joined here by my cohost.

Ham: Dude, it's Ham. Welcome back. We are here once again in the studio talking about the risk assessment.

Nathan: All right. Just off the bat, risk assessment. What do you know?

Ham: Nathan, I'm going to be honest with you, man. I'm trying to look at these notes that I was given today. And uh let me tell you, I don't know anything.

Nathan: Yeah. Fair enough. It encompasses identifying and analyzing and responding to risk factors that could be in your life or in your business. Things like that.

Ham: Sure.

Nathan: Risk management means controlling the outcomes, and you're prepared. Acting proactively rather than reactively to things that may happen.

Ham: Yeah. Now I got to ask, what is a risk?

Nathan: Risk? I mean, think about it. Just from a personal standpoint, do you have things that could get stolen?

Ham: At home, yeah, my computer or the fact that I don't leave my car locked whenever I leave it.

Nathan: Uh As you're saying though, with risk, you know, that's the example of risk, I mean, from a cyber standpoint as well. What do you have online? We talked about this first episode.

Ham: That's true. There's so much stuff that's online, you know, you can go onto Facebook, Instagram, Google Plus, Twitter! It's all there, all that stuff is available.

Nathan: And on top of that, even more, you game a lot.

Ham: Yeah. I game all the time.

Nathan: You have credit cards, you have in game items, you have your accounts in general, how many hours you put into a certain thing?

Ham: Thousands.

Nathan: Anything that has value to you. From a personal standpoint, it could be your own data, it could be your own belongings. From a company standpoint, same thing. It could be data and it could be physical things as well. Anything that has kind of a value to it, or a potential to be a risk, potential to get stolen, potential to be destroyed. I mean, some of these things, if they got lost or stolen or ruined, cause an impact on you.

Ham: Oh, I'd be really sad. If my League of Legends account got banned, I'd be so angry.

Nathan: Yep. Taking inventory on those kinds of things, that's one of the first things about risk assessment that we have.

Ham: Going back to the League example, right? Like I've been playing League of Legends for 11 years now. And it's been a great time. I'll, I will just put that out there, like shout outs to Riot and all them. But, um, I've spent over $3,000 on that game. Granted that's over 10 years. Like, I get it. Riot has owns my soul at this point.

Nathan: Fair.

Ham: And if my account gets lost, hacked, banned, that's three K down the drain.

Nathan: We won't talk about hours.

Ham: Countless hours.

Nathan: 10 years, you put into that.

Ham: Yeah.

Nathan: Talking from a cyber standpoint, risk assessment, that's included. We have our own things that are important to us of value in that sort of way. Risk assessment, it's not just for companies or just organizations that need risk assessment. It can be taking inventory of your own life.

Ham: It could be anything

Nathan: It could be your cars. Your house. It could be what valuables you have, your family. Risk assessment is for finding where you're vulnerable and proactively, not reactively, prepping for if something where to go wrong. You have holes in your boat, figure out where these holes are and how you can patch them, how you can plug these holes basically.

Ham: How to fix it.

Nathan: Not everything can be fixed. And in that sort of sense, it's when you have a plan in place for if something were to happen, how you can proactively fix it.

Ham: Yeah. So Nathan, if I wanted to, you know, say I'm going home tonight, it's the weekend. How how would I make sure that I can assess the risks that I have and make sure that I'm safe.

Nathan: So on simple, simple terms, a risk assessment process. It boils down into identifying risks, assessing these risks, controlling them, and then reviewing the controls. So, identifying a risk. Where you're vulnerable. What are the risks? And then assessing them. Why these are risks, how big of a risk it is. Some things might be bigger than others.

Ham: That's true.

Nathan: Your League account compared to, let's say, a hard drive or something. Identifying, this takes precedence over this one. Controlling the risks. How many holes you have in your boat? And if you can fix them, do it. Again, you can't, you can't fix everything. Have a plan in place. If something goes wrong, instead of you running around like a chicken with your head cut off. Take steps in order to better protect yourself.

Ham: How would I go about protecting that? What are those steps?

Nathan: I might suggest on just a physical level, lock your car at night.

Ham: Sure. Okay. Understandable.

Nathan: You know, don't leave your hard drive sitting out on a table. Safe clicking. In our first episode where we were just talking about security in general, a lot of those safe practices tie into risk assessment. You know, this could be from a company standpoint, teach your employees how to be cyber aware.

Ham: Yeah.

Nathan: Teach students how to be cyber aware. You know, at your home, teach your kids, if they're on the internet. Safe clicking, safe searching.

Ham: Absolutely.

Nathan: That sort of thing. Taking inventory, you got possessions, you got valuables. It also can be from a larger standpoint, just of everything in your life.

Ham: Like you were saying, lock my car at night. Make sure everything is locked up, closed, and nobody can get in, right? Or if you're at school, don't leave your hard drive out on the table where if you turn away to talk to a buddy, out of nowhere [00:05:00] comes, you know, Johnny McThief over here comes over, steals your hard drive. And next thing you know, it's gone. Say, someone tried to access my Twitter and I have two-step verification.

Nathan: Vulnerability reduction. You already have taken proactive steps.

Ham: Sorry to cut you off. I have multiple authenticators on my phone for many of my accounts.

Nathan: If you didn't have those authenticators, you'd be more vulnerable. Whatever sites, whatever accounts, those are linked to would be more vulnerable. Take steps in order to better protect yourself. Two step verification, don't give your password out to your coworkers, don't open up phishing emails that you get. It just ties into the whole mindset of being cyber aware.

Ham: Dude, okay. I'm going to go off on a tangent really quick. You know how we talked about fishing and I think, I think , episode one, I can't remember.

Nathan: Okay.

Ham: I got the Adobe Flash email that we talked about, you know, how they canceled Adobe Flash?

Nathan: Yeah.

Ham: Yeah. And I got an email for it. I was like, wait a minute. I remember this.

Nathan: So it was for Adobe Flash? Do you remember what it was asking?

Ham: I can't remember, but I saw that like the old Adobe Flash logo and I was like that's not real. This is fake. What do you mean? Are you kidding? I just ignored it, I didn't even click it.

Nathan: You knew better though! Looking back if you hadn't heard about how –

Ham: Oh, I would've definitely clicked. I would have one hundred percent clicked it. Like, Adobe Flash out of date? Absolutely! Sign me up! But like remembering the podcast that we had, like, a couple of weeks ago, I was like wow!

Nathan: That that could have been a risk to your computer. If you had downloaded the fake Adobe.

Ham: So sad.

Nathan: Yeah. Some of my main takeaways , do a risk assessment. It can be just on you and your workstation. It could be company-wide, it could be you at home, you and your family, you and your physical belongings, cyber. Know where you're vulnerable. It's just good to keep a good eye out and remain aware.

Ham: A couple of my takeaways are, you know, taking those steps that you need to be safe against these risk factors that can come around at any point. Two step authentication. I recommend it to literally everybody. It doesn't matter what you do, if it's available, use it.

Nathan: Yep.

Ham: It is so powerful.

Nathan: Well, thank you again, Ham for joining us on this episode!

Ham: Dude, thanks for having me. It's always a pleasure to learn so much.

Nathan: Well, I think that wraps it up for our episode six. Thank you again to all of our listeners for tuning in for this episode. And we'll pass this off to Mercy.

Ham: GG's everybody.

Mercy: Hey, everyone. Mercy Ayesiza here with the news, a student expert on the information security team. I'll be updating you with what's going on in the cybersecurity world. Before I get into the headlines, please make sure to subscribe to our podcast.

Our first news update, malware hides in Google Chrome as legit Windows application. Researchers from Rapid7, a cybersecurity company, recently discovered an ongoing malware campaign that was using Google Chrome as a disguise to infect multiple Windows systems without being detected by Windows security defenses. One of the researchers mentioned that the malware's goal is to collect sensitive data and steal cryptocurrency from the infected PC.

The malware takes effect when a user visits a malicious website and is persuaded to act on a false Google Chrome update, which then infects the machine. The malware can bypass detection by imitating a major Windows operating system utility. Be aware of malware scams and always double check that you're only downloading official updates.

Our second news update today, more than one billion face prints to be deleted by Facebook. Facebook announced on November 2nd, 2021, that it will be dropping its facial recognition system and deleting over one billion face prints. With Facebook's facial recognition, the software can automatically identify people in uploaded photos and videos by tagging names and linking their accounts if they are registered for the feature. Jerome Pesenti, the VP of artificial intelligence at Facebook, said, "Users who have opted into our facial recognition setting will no longer be automatically recognized in photos and videos and we will delete the facial recognition template used to identify them."

The company hopes that this tremendous change will be able to enhance privacy, transparency, and control for its users. And that wraps up the news for this week. Thank you for listening to the CyberAware Podcast. We'll see you next time.