The Wild World of Cybercrime

CyberAware Podcast: Season 2, Episode 9

Nathan: All right, everybody welcome back to the CyberAware Podcast. My name's Nathan, and today for our ninth episode, we're talking about cybersecurity crimes and I'm here joined by my co-host.

Ham: Dude, it's Ham. Back in the studio as always! This episode is going to be wack.

Nathan: It's fun. Throughout the seasons so far, we've talked about different types of crimes, today we're just going to go a bit more in depth. Just starting here, cybersecurity in general, crimes. Off the top of your head, what you've learned so far, what kind of crimes can you think about?

Ham: People stealing your information.

Nathan: Identity theft.

Ham: I don't know, hacking potential accounts. Hacking your Facebook, Instagram, Twitter, even your LinkedIn. They can learn so much about you! Going towards bigger company wise, you have security leaks.

Nathan: Yeah, cyber espionage. Cyber bullying, one not many people think about.

Ham: A huge epidemic, by the way.

Nathan: We have phishing, you have malware.

Ham: Oh.

Nathan: Like we talked about in a previous episode, crypto jacking. Mining your cryptocurrency without your consent on your device. And then also credit card fraud and identity theft like you were talking about. And I'm sure we're missing a ton more, but cyber crimes in general kind of break down into three categories. So we got crimes in which computing device is the target and that's, for example, gaining network access. And then we have crimes in which the computer is used as the weapon.

Ham: Yeah.

Nathan: So for example, DDoS attacks. Anyone who's listening who doesn't know what a DDoS is, it stands for denial of service attack. And more or less your network is fried. It overloads it and it just kind of kaputs.

Ham: Yeah, it shuts it down. You know, that happens so much when I'm playing Rainbow Six, right? Like we'll be playing, we'll be mid ranked match, and next thing you know, the server gets a DDoS'ed and the whole game shuts down.

Nathan: Yeah. And then lastly, we have crimes in which the computers use as an accessory to the crime. So for example, using computers to store illegally obtained data.

Ham: Oh.

Nathan: So yeah, it breaks down into those three for the most part, but computers can be used in many ways for crimes.

Ham: Okay.

Nathan: You know, with the internet and how big the internet's gotten, World Wide Web, the whole nine yards, the volume of cyber crimes and how much they've increased, and how fast they're changing. Because it's – criminals no longer need to be physically present when committing a crime.

Ham: Yeah, that is so true.

Nathan: Going back onto the DDoS attacks, you could be playing Rainbow against someone who's on the other side of the country or the other side of the world.

Ham: Yup.

Nathan: They could just completely kaput your network, as you were saying, fry your router.

Ham: Yeah.

Nathan: And that kind of stuff is just nuts and that goes into it. Crimes have just become so accessible in this sort of sense.

Ham: Yeah. This is insane. Cause you know, it happens all the time. It's an everyday thing, it just happens at almost every moment.

Nathan: Yeah. The internet speed and the fact that you can remain anonymous in these kinds of cyber crimes and the lack of borders make these kinds of crimes, just so easy to carry out and kind of hard to track.

Ham: Yeah.

Nathan: Compared to regular crimes, if someone's breaking into your house, they have to physically break into your house versus they could be halfway across the world. There's no borders, there's no, it's just, it's kind of –

Ham: Like an old west kind of style.

Nathan: Yeah, I mean, there's rules in place like we have now, but you know, there's a lot of types of crimes. As you're saying, ransomware, fraud, money laundering, stalking, cyber bullying. And most of these are punishable.

Ham: What are the penalties for some of these cyber crimes? Like what's the worst thing you could do and get punished for it?

Nathan: I guess, whistleblowing.

Ham: Yeah!

Nathan: I'm not going to name drop, but I'm sure you can probably think of a pretty famous whistleblower. If they came back to the U.S.–

Ham: Oh, my gosh.

Nathan: Yeah. So that's kind of espionage, treason. It's pretty highly considered a bad thing to do. For everyone who doesn't know what cyber espionage is, it's involving a cyber criminal hacks into a system or networks. Basically just leaks or accesses confidential information by maybe a government or an organization. And it can include every type of cyber attack. You could destroy data, gather data, steal data. And nowadays, countries are hiring hackers just to hack other countries.

Ham: Wild.

Nathan: Cyber espionage can come in many ways shapes and sizes. That could be an employee who leaks inside data or who willingly leaves something vulnerable for someone to steal. Someone wants it, someone offered money for it. And cyber espionage, that holds a big fine. With crimes in general, it's the thing with regular crimes. Loitering is going to be less than assault, you know what I mean?

Ham: Yeah.

Nathan: Some are taken more or less seriously. We have things like credit card fraud and identity theft.

Ham: Oh yeah.

Nathan: With identity theft, someone uses your identity. So someone could be posing as you online, and that sort of thing is scary to think about.

Ham: Yeah.

Nathan: And someone's posing as you online, committing cyber crimes, things like that. It can turn into a whole mess.

Ham: Yeah.

Nathan: Credit card fraud occurs when somebody uses your credit card or your credit card number when it's not theirs and without your permission.

Ham: Thank goodness I don't save any of my credit card information to literally anything.

Nathan: Again, good thing you don't save anything online. But as we were talking about with the internet iceberg episode – data leaks, that kind of thing.

Ham: Yeah.

Nathan: Think about how many websites you put your credit card number, your address, without a second thought about, "Huh – I wonder how secure they are?" Your credit card, it's probably on the dark web somewhere.

Ham: Oh, easily.

Nathan: People can buy credit cards from the dark web. They can buy thousands of credit cards for 20 bucks or something like that. Pretty cheap amount, they're not going to use all of them right away. Some of them might not work, some of them might. They might use this one now, one five years down the line and test the waters. And then all of a sudden you might, you might get an alert one day that, oh my gosh, you've had $700 on your account spent.

Ham: 700 smack-a-roos?

Nathan: That's a pretty big one, and that's just on the low end. Credit cards are everywhere nowadays and credit card fraud can occur from anyone who, someone might look at your receipt, or even employees might swipe your credit card number while you're there. Gas stations, I don't know if you've seen, when you swipe your card, you insert it into the little slot.

Ham: Oh yeah.

Nathan: Sometimes people put fake readers over that that blend in.

Ham: And you know what, that brings a really great point. For the longest time – it wasn't until late 2020, I think December, I decided to finally get a debit card.

Nathan: Okay.

Ham: And otherwise I've been paying with cash for everything. I'd go to my bank, physically take out money, and go buy whatever I needed to.

Nathan: I agree with you. If I could pay for everything in cash, I would. But then you have credit and you need to buy things in life.

Ham: Yeah, I guess. Grrrr!

Nathan: Go world. With you getting it now, even for someone who's new to this, if you don't know what you're putting your credit card on site wise, don't do it. You know, it's just good to think about. Know what you're doing. Check your accounts, check your accounts.

Ham: Daily.

Nathan: Daily. It's a good thing to do. Set up alerts, set up multi-factor. That's your money, that's your savings. That's you.

Ham: That's your life.

Nathan: Credit cards made up a total of almost half a million reported instances of fraud in 2020. It's nuts how much credit cards are used for theft. Cyber crimes in general have been jumping through the roof up to like, I don't know the exact number – I did a paper on it for one of my classes last year, it's like in the billions upon billions of dollars how much cybercrime costs the world a year. It's the largest crime ring that you can possibly think of, out of anything. Nothing compares to how big just cyber crimes in general are.

Ham: That's wild. I had no idea.

Nathan: It's crazy to think about how much it's changed. And then we have cyber bullying, which not many people think of. And cyber bullying boils down into a lot more than calling someone ugly over the internet. It can be just intimidating, threatening, abusing, or harming content that's offensive to another person on the internet.

Ham: Yeah.

Nathan: And the thing is, someone doing it in person versus online – again, anonymous.

Ham: Yeah.

Nathan: Even in some cases nowadays police can get involved, FBI can get involved on all these sort of things. Like it's a real issue. Harassing phone calls even count.

Ham: Oh, good. Tell them to stop calling about my car's extended warranty.

Nathan: I actually just had a call earlier. I wouldn't call it cyber bullying, but just scam calls in general. We didn't even talk about scam robocalls. Within five minutes today, I had six

calls from six different numbers. I answered it and they asked for a random name and were talking about senior banking insurance. Clearly, clearly scum.

Ham: Oh, a hundred percent.

Nathan: Trying to scam someone old. And I told them, "Not my name, not a senior." Hung up immediately. Called all six numbers back to see if they'd answer – "this number is not in service." What they were doing is just – brand new number, call someone, brand new number, call someone, brand new number. And untrackable number.

Ham: Ugh!

Nathan: It's, oh it's gross.

Ham: That's disgusting.

Nathan: Everyone has gotten the scam calls. I'm hoping our phone carriers will do something about that soon enough.

Ham: We're hoping.

Nathan: Take them off from coming through. It's insane.

Ham: Yeah.

Nathan: And going off of cyber bullying though, we have cyber stalking. This sort of thing can be dangerous at times. Cyber stalking is using technology to harass or frighten someone. And stalk them. Learn about them, whatnot.

Ham: Oh yeah. And that is so, it's so bad, especially in this day and age. It's so disgusting how people will go to great lengths to find you, learn where you live, and go the extra mile to potentially do something super harmful to you.

Nathan: Know what you're doing online, what your presence is, your footprint, your online footprint. There's scary people on the internet.

Ham: Yup.

Nathan: And stalking I think goes as a gross misdemeanor, but that can go way up depending on how bad it gets. Felony level too I'm sure.

Ham: Absolutely. And you know, it could even happen just, say you have a friend. Say on campus, right? And they don't really want to be your friend, they want to be super harmful to you. You'll add their Snapchat, Facebook, all that such. You know, on Snapchat you have your Snap Map.

Nathan: Oh my gosh.

Ham: And it's available. They can know exactly where you are at the exact point.

Nathan: I don't have Snapchat. I used to, haven't in a while, a few years. The Snap Maps – that's so invasive. I can see where you are to a foot the last time you logged in. You can see where everyone is. You can see everyone across the world where they are. That's scary! And you can turn it off, but like –

Ham: Is it really off?

Nathan: Is it really off?

Ham: "Haha, just kidding, we literally have binoculars all over you, man."

Nathan: Not trying to harass, but that's an invasion of privacy if I've ever seen one.

Ham: It is.

Nathan: Cyber crime has gotten big over the past few years and, just knowing how much danger it can be is a pretty good thing to be aware of. But these are just some of the ones I wanted to talk about.

Ham: Yeah. And you know, we got to say Nathan, I think it's time we should wrap this up here. What are your three takeaways here from this episode?

Nathan: Know what you're doing on the internet. I definitely would say, know what your footprint is. Your internet footprint. If you want to, do a quick search on yourself, see what you can find.

Ham: Yeah.

Nathan: Check your bank accounts. They can be vulnerable. Just be smart, be secure, and be aware.

Ham: Absolutely.

Nathan: And how about you on your end? What are some of your big takeaways?

Ham: I say the big takeaway is knowing how deep cyber crimes can really get from just the starter level to all the way down. I had no idea that any of that existed being yet the common Joe, just chilling, hanging out here. I'm learning so much, you're teaching me so much, and we're learning together. And this has been a fantastic, fantastic time.

Nathan: Well, again, thank you for joining us on today's episode.

Ham: I can not thank y'all enough.

Nathan: No problem. All right, thank you to all the listeners for tuning in today, 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. Today's highlights are –

Major wind turbine manufacturer hit with a cyber attack. A big data breach hit Vestas Wind Systems, a Danish owned wind turbine company, on November 19th, 2021. This led to some of their IT systems to be shut down. The company, which services wind turbines in the U.S and Canada, is worth about 34 billion dollars. Vestas has not yet disclosed the total damage from their attack, but it has mentioned that some data has been compromised. Vestas has, however, mentioned in an update that the breach hasn't heavily affected their service, manufacturing, and construction processes.

Our second news update today – 1.2 million customers affected after GoDaddy's most recent breach. Major internet domain registrar GoDaddy suffered a cyberattack after email addresses, database login credentials, and customer numbers were legally accessed by a cyber criminal. The cyber attack is said to have initially began on September 6th, 2021, and was noticed clearly on November 17th, 2021 when the attacker used a stolen password to gain access to the company's WordPress hosting environment. Recently, GoDaddy has experienced cybersecurity incidents, this being the fourth major incident since early 2020.

Our third news update news today – be aware of scammers using phony TSA PreCheck sites during the festive season. TSA PreCheck helps travellers get through the airport screening quicker. But, a trending scam is taking advantage of customers through emails, asking them to renew their TSA PreCheck memberships for twice the regular fee.

When users click on the link in the fake emails, they're taken into fake TSA renewal websites with persuading ".com" domain names and asked to proceed to pay with no guarantee of the renewal. Please be careful what website links you click on and be wary in inputting personnel and payment information. For genuine TSA information or websites, please visit the Homeland Security website.

And that wraps up the news for this week. Thanks for listening to the CyberAware Podcast. We'll see you next time!