Backups & Data – What You Need to Know

CyberAware Podcast: Season 2, Episode 5

Nathan: Hey, everybody. Welcome back to the cyberware podcast, today we're going over our fifth episode, which is data and backups. My name's Nathan, your resident cybersecurity expert. And I'm joined here by Ham.

Ham: It's so great to be back again here at the recording studio.

Nathan: I agree. All right, so let's get into it.

Ham: Dude what is a backup?

Nathan: More or less data backup is, your data itself and it's being stored elsewhere so that it can be restored to its original state.

Ham: So you have, how do I put it a wall? Right? And then if something breaks through that wall, and then you have a second line of defense where, oh, no, your stuff is gone, but wait a minute. I have all my information that's been backed up.

Nathan: Data backup comes in many shapes or forms today. We're going to be mainly talking about, external and cloud.

Ham: I get it. Everyone's got is like on the cloud already, but like, what's it really mean?

Nathan: What do you know about the cloud? What do you use cloud wise?

Ham: Well, Nathan let me you. I know very little about the cloud. All I know is that when I save on Microsoft it goes up into the one drive and I'm like, nice it's there forever now.

Nathan: Fair enough. So are you one of the people who pictures cloud – Like when people think cloud, they think, it's just up into the atmosphere. It's gone. Just in the cyberspace.

Ham: Not really, I think there's definitely a point where it, like it floats and it hovers. Cause you know, when we talk about the worldwide web it's stays in one particular spot.

Nathan: Yeah, you're getting there so like the cloud itself refers to softwares and services that run on the internet. So as you're saying, worldwide internet kind of same thing, instead of something being locally-based on your computer these things are cloud services. So there's stuff that runs on the internet. So this could be, you know, Google drive one drive your apple photos the whole online cloud kind of thing.

It's that whole thing, for us on campus here, students, faculty, staff, all of us, actually, we have like Microsoft OneDrive and we use that for free. I use it all the time. I don't know if you use that for classes or whatnot.

Ham: Yeah.

Nathan: Uh, we're going to be talking about that a bit today as well. Pros, cons, why we use that. So, yeah, I mean, going back on what you said what kind of online services do you, you use?

Ham: Personally? Well, mainly I'm huge on the Google. So I ride Google till I die. like just the whole, like how like Google docs, Google, all that just works.

For example, I can go to say the state fair, right? I'll take a couple of pictures on my phone and all those photos are saved within the cloud somewhere. And I can go onto my computer and say, Hey, I want to upload this.

Nathan: Now have you ever had to rush an assignment. And you finished it on your phone, somewhere you probably shouldn't be writing your assignment.

Ham: Not necessarily. I'll try to do my homework mostly at home.

Nathan: Well, that's living the beauty of it. Firstly, I have experienced that, you know, the beauty of the cloud access anywhere. Anywhere you have internet, that's kind of the catch right there. If you have internet, these things will take you wherever you need to go.

And disaster recovery, if you have everything on your computer, on the cloud, you spill coffee.

Ham: Got the cloud it's right there.

Nathan: Exactly.

Ham: I actually have a great story about this. 2019, me and my dad, we decided to go to Yellowstone National Park. Right? Beautiful, beautiful place.

By the way, a hundred percent would totally recommend to go three or four times again. But we were, we were chilling in front of the sulfur pit and I had my phone out and I was like taking pictures and I dropped my phone in the sulfur pit.

Oh, of all the places the sulfur pit feels real bad.

Nathan: Did you ever get it?

Ham: I mean, gone, it was disintegrated in 10 seconds. Gone. Absolutely just dust.

Nathan: The saving grace though?

Ham: The saving grace. I had all my photos saved onto my cloud and all the photos that were on my old phone transferred through to my new phone.

Nathan: Yup. I mean, talking phones in general, I personally take a lot of photos and just as kind of keepsake stuff like that. If my phone were to get destroyed, I get a new phone. I sign in, download the 3000 cloud photos I have everything that I have on it contacts photos. That's a big one. Any of your other information? I, do you have any that I'm missing out?

Ham: I think that's really it. I mean, I don't save any passwords on my phone.

Nathan: As we talked about in previous episodes, that's a good thing. But yeah, access anywhere and disaster recovery, that's a big one in case your phone gets run over, you drop into the lake. I've done that. Or sulfur pits, as you were saying.

Another, another big thing is low cost. Yeah. It's not like you're spending hundreds of dollars. I mean, maybe from a company standpoint, but a personal standpoint, you don't need to spend a ton of money. As I was saying, you know, with us in one drive, you have school free.

Ham: A hundred percent

Nathan: Your OneDrive is your OneDrive. I think we have up to a terabyte of space that we can use.

Ham: Holy moly.

Nathan: Yeah. I have actual physical hard drives. That have that much room

Ham: Yeah.

Nathan: Versus free cloud. It's free for us, it's yours while you're here. Yeah. So I definitely recommend using it because it's, even if you have your own stuff, I'd still recommend having that as well.

Ham: It's a really great tool that you could just have it as a free accessible resource that you're able to use at school.

Nathan: I don't know what at school would have been like 10 years ago. Your USB

Ham: USB flash drive that held 32 gigabytes. That was it.

Nathan: And that's, you had to carry that thing with you.

Ham: And if I lost it, my homework was gone.

Nathan: Going back to just some of the pros, just cloud in general, scalability. You know, like with cloud, how much room you have, how much room you need.

Ham: Sure.

Nathan: If you need more, you can get more with the cloud. You can kind of work with how much you have. And then another thing as you, again, with security is it's online. It's not like you leave your laptop out or you leave your USB or your hard drive in your backpack or on your desk and you turn away for a second.

Security wise. I mean, it's pretty good. As long as you keep your devices locked and whatnot.

All right. Coming off cloud, you know, the other kind of external storage devices, you got hard drives USB, stuff like that.

I personally have a hard drive as well, and I carry that thing with me. I just can pull it and bring it with me. You can get some pretty big, hard drives, which is a good thing. Uh, performance. They're there, it's physical. No internet needed. It's just right there.

Ham: You plug in, you go,

Nathan: You plug and go. You got a computer, you got your hard drive. You're good to go.

One of the downsides though, one of the biggest things that you have with that thing gets broken. You're kind of toast.

Ham: Yeah, that's true. Like a good example at home. Right. So at my gaming station, I have an external two terabyte for my separate games and music that I've downloaded.

Nathan: Okay.

Ham: And there was like three months ago. I accidentally uninstall like unplugged it before doing the whole, like step-by-step safe to unplug and it corrupted the whole everything. And I was like, Crap. All my stuff is gone. This is awful.

Nathan: Did you have a backup at all?

Ham: I did not.

Nathan: Now moving forward.

Ham: I'll definitely have a backup.

Nathan: Backup your devices. You never know what's going to happen. You know, something might break whatnot and instead of you losing everything that you've had on that. Yeah. You can at least have that saving grace.

Ham: 500 gigabytes worth of games, yo!

Nathan: Yeah. That's so bad. Yeah, exactly.

Ham: Re-install them. Oh my gosh.

Nathan: But yes security wise if you have your hard drive left out on your table, what stopping someone from just grabbing and going?

Ham: That's true.

Nathan: With cloud I got my password protecting that. It's my account, my password.

Ham: Yeah.

Nathan: Some hard drives some external storage devices have that. Other times you just plug it in and you can access it.

Ham: That's true. That's how mine were back way back in like middle and high school.

Nathan: moving on though, types of data, there's many types of data.

You know, we got public data, internal data as well as confidential data. I don't know if you want to take any stabs in the dark at what any of those would mean.

Ham: You know, I honestly don't really know, but I'm guessing like public data is stuff that is readily available.

Nathan: If you were to search me up online, what do you think you could find.

Ham: Probably your Facebook, Twitter, Instagram.

Nathan: LinkedIn. You can find your jobs. There could be pictures of me online. There could be, as you're saying with Twitter or your Instagram, some of that stuff is what you can immediately find a first name, last name, maybe your job, maybe where you grew up, maybe your high school or your college you attend.

Ham: Yeah.

Nathan: Most of that is public data.

Ham: Say you're going in for a job interview. Hey, let's start with this guy. Social media. See what he's about?

Nathan: Oh, I can guarantee with any interview they're going to vet you. Yeah. It's easy to search a LinkedIn or an Instagram, even with college kids.

Ham: Oh my gosh.

Nathan: And I think we talked about in our first episode, what are your posting online?

Ham: Yeah.

Nathan: You know, it's a good representation of who you are behind the scenes is what your Twitter, what you're posting on your Twitter. Twitter can get pretty wild.

Ham: It, you know, I'm on Twitter daily and it is insane.

Nathan: Some of that stuff is public and an employee or potential employer. They can find that stuff, what they can do with a quick Google search of you

Ham: Done.

Nathan: on the other side of things, internal only data is different, you know, that could be things like business plans or stuff that only a select few sure can actually access. Maybe internal personnel of a company. I can't just go online or walk up and there'll be like, yes, here you go.

Ham: Yeah.

Nathan: You need somewhat of permission actually to view that kind of stuff. And then the last one, we have confidential data.

Ham: I'm guessing it's like, this is my stuff. No one else's.

Nathan: Yes. I mean, can you think of something that I probably couldn't find on you? If I search your name?

Ham: I have no idea.

Nathan: What about your social?

Ham: If you'd definitely search like my Facebook or like Twitter probably.

Nathan: Your social security.

Ham: Oh, absolutely not. Social security. Absolutely. My medical records, no way.

Nathan: Yup. Legal files. It's specific authorization or clearance to actually view this kind of data. And this can tie in with students, even here at, at our school, students have certain rights student privacy rights, what can, and can't be public information.

Ham: Yeah.

Nathan: So, you know, I could maybe find a student's name, but I might not be able to find their address or their phone number.

Oh, that's going to be protected, you know? Things like HIPAA and

Ham: yo the HIPAA, it was always listening. I used to work at a nursing home a couple of years ago and you know, the same thing ties over there.

Nathan: Yup.

Ham: It was probably one of my favorite jobs of all time. Cause like the residents made that job so much fun and I'd want to tell stories about them to my family.

Nathan: But you can't talk about it.

Ham: I can't talk about it. You're not allowed to talk about patients, not even names or anything like that.

Nathan: Patient data, as you know, in hospitals or student data or what. Data comes in all sorts of sizes, shapes and sizes.

Ham: Would this kind of tie into like when the Sony PlayStation hack happened when like credit card information got stolen.

Nathan: Yup. Yeah. Another one that I forgot to mention off the top of my head, restricted data. You go to take a crack at that or no.

Ham: You know, I honestly have no idea.

Nathan: All right. So restricted data is data that's like proprietary information on research or data protected by state and federal regulations, things like that. If we're talking about Manhattan project for back in the day, that would be an example of restricted data, I guess.

Nathan: I was trying to find a good example. Yeah. That one.

Ham: Oh, okay. Wait a minute. I'm bringing in a memory from like ages ago. Wiki leaks, if I remember? In my boomer brain of mine, as I'm 26 years old, I remember all this information.

Like military information got leaked, leaks about different political positions and powers got leaked, all the dirty stuff that they did. The background under the table, money handling, all that stuff was leaked and crazy.

Nathan: Yeah, that would tie in. I mean, we kind of went down the rabbit hole there with data. I think that's about all we need to cover today. Some of my main takeaways that I have here, as we were talking about earlier for people at school. Our cloud one drive guys, can't recommend it enough. It's useful it's free as a student perspective I use it all the time. If you're not backing, I would suggest starting backing up. If it's something that you're going to be mad, if you lose, back it up.

Ham: Back it up.

Nathan: How about you? Any takeaways?

Ham: I'd say probably my biggest takeaway is like actually learning what the cloud really is versus like, oh, it's just my data up and the sky somewhere. It's actually in a position where it's safe, secure, and I can always access it if needed.

Nathan: I'm glad that we could maybe shed some light on exactly what it is and go a bit more in depth today about, you know, how the is useful, what exactly.

Ham: Yeah. It's always a great, great time coming in here and learning about this so much because I'm just an average Joe kind of guy. Granted, I play a bunch of games in my spare time, but even still.

Nathan: I mean, some of this stuff I'm researching, I'm learning at the same time, you know, as you are. So it's fun just to learn together. So again, thank you everyone for joining us on our fifth episode here, the cyber podcast. And thank you again, Ham for joining me today.

Ham: Dude. Thanks for having me as always.

Nathan: No problem. I guess we'll pass it off to mercy for the news.

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 today. Craigslist customers, stormed with emails containing malicious links. Attackers hijacked Craigslist's internal email system in early October, 2021, and exploited a security flaw to execute a phishing scam that affected the platforms users.

According to the report from an email cybersecurity platform called Inky, their attack has phishing email warns users that their ad or listing has been flagged for inappropriate content.

It also asked users to click on a link to a form with more information about the issue, within 24 hours.

That fake email also displays Norton and Microsoft logos at the bottom to trick users into thinking it's an authentic message.

If you use Craigslist, be aware of phishing attempts and do not interact with suspicious emails. Our second news update today, another major SMS scam targeting millions of Android users.

A trending scam called Altima SMS discovered by the security firm Avast, is affecting Android users. It is said to have begun in May, 2021. The scam campaign includes various malicious Google Play apps in disguise like keyboards, QR code scanners, video, and photo editors, spam call blockers.

Camera filters and games. Most of the fraudulent apps are downloaded by users in Egypt, Saudi Arabia, Pakistan, the UAE, Turkey, Oman, Qatar, Kuwait, the US, and Poland.

If a user downloads, one of these malicious apps, their location and personal information is gained. Then the users email or phone number are used to sign up for a premium SMS subscription of about $40 per month.

Depending on the country or mobile carrier, while some apps have been taken out by Google, Android users should be cautious of this scam and follow these tips when downloading or purchasing new apps.

Check their reviews, check the app permissions, avoid entering personal information, like your phone number and only use official app stores.

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