

Amanda Lindsey: My name's Amanda Lindsey, I am an information security analyst with Pfizer. Well, with me, especially, I'll think phishing, because that's usually my wheelhouse. I analyze everything from who sent the email, who received the email, what location they're in. If I can get a copy, analyze the headers, which is the information that tells you where are the different places it bounced from.

[00:00:30] What's the link? Where would I go if I clicked it? Is it where it'll take me to a site that wants my login information, so it can actually take over my account? Is it a pretend banking one, which actually could steal my banking information, but also steal my money in the bank account? Is it a bad attachment that can actually put something on the computer and then open a doorway to the network?

[00:01:00] My ultimate cyber job, it's pointing towards threat intelligence. There was a gentleman named Hushpuppi. He made millions from compromising business emails and diverting funds through wire transfers, because that's part of business email compromise. You take over the account, pretend to be the CEO and say, "Hey, you need send money to this bank account instead of your normal one that you send the money to." [00:01:30] Now, Russia's getting into it. And of course, ransomware. That's the big way that a lot of them get in is a phishing email, and I kind of want to look into that, why people click the links, why people open the attachments.

Just asking questions. Always being ready to learn. Just wanting to dig a little deeper, not just being, "Okay, this information's good enough to close [00:02:00] this ticket." Try to dig a little deeper in saying, "Okay, why did the person click the link?" Or, "Why did this go off? Why did this alert come through?" I honestly want to say part of it is because I'm on the spectrum myself, because I hyper-focus. I'll put my headset on, listen to stuff while I'm digging into stuff/ my mind's always thinking. That's why sometimes [00:02:30] when I'm speaking my thought process kind of will change and then I'm like, "Okay." I stopped what I was speaking about, so I have to make sure, normally, if I'm speaking to a group, I have notes. But having that thought of my mind always thinking. I'm always thinking.

The moment that made me really want to get into cyber, I was towards the [00:03:00] end of my master's, lost both of my grandparents that I was very close to. They were pretty much my parents, because my mom was a single mom and she had to work nights and go to nursing school during the day, so I was very close to them. Lost both of them in six months, determined in that time point, I'm going to do whatever I can to get my foot in the door to get into cyber. Because I was like, "This is what I've gone to school... I'm almost done. Let me finish it." I honestly considered quitting my master's degree during that time [00:03:30] because of the stress, and then working and then also having, at that time, a toddler, as well as a school aged child on the spectrum. And as soon as I got my master's done, it was like a month later, I actually got my foot in the door in cyber.

Certification, possibly introduced them to the CompTIA. Security+. [00:04:00] Another big thing I encourage is labs, is where people get an old laptop from somebody, reset it with like Kali Linux, and learn about the tools that the bad guys use. Like, "Oh, this is a password cracker. How does it work?" There's also a lot of great people I follow on... There's great people on LinkedIn and social media that help push [00:04:30] introductions to cybersecurity. Some of them actually have trainings that are pay what you want, pay what you can.

I would recommend, first thing first, if they're in school, look for a good cyber program that's more than just okay, read a couple chapters, take a quiz. I liked the Western Governors because it was competency based. You couldn't pass a class that you were in until you showed, either by [00:05:00] passing the certification or through task stream, which is where you submitted your task for the scenarios, that you had an understanding of what was going on and what was asked of you.

The way I know I'm doing my job is our users are protected. If I bring up information such as, "Oh, this is a potential [00:05:30] threat", such as there was a issue of what is called a drive-by download. This is when you go and download something... You need to edit a PDF and most of us don't want to pay for an Adobe subscription. There was maybe, "Oh, a free PDF editor." You downloaded that, but what comes along with it is malware. And while looking at this one incident of this, I looked at it [00:06:00] and remembered that the IP was related to this malware, this free PDF download malware. So I started digging and determined 1600 machines had this potential issue. This led to where I had to call somebody, because it was night shift. My boss had to call his boss and it went up the chain, but because of that, that potentially prevented [00:06:30] a major infection.

A typical day for me starts by reviewing what's in our queue, see if there's any that I can grab and assign to myself and start working them, as well as looking over the inbox, what's been patched, what's come through overnight that might be a major incident, the news that's [00:07:00] gone on in the world of cybersecurity. I just kind of get a deep overview of that. Then we have our morning meeting that kind of goes over what happened yesterday in the night shift, going over previous events that were closed, making sure that I have a cohesive understanding of what the other analyst was doing when they closed the ticket. Review what's in our sim, see if there's any major events. Possibly also work with other teams, [00:07:30] such as threat analysis, messaging, security. And also myself, I'm also working on documenting and changing the operating procedure for different kinds of tickets.

I want to know more about, "Okay, so they got a phishing email." Most people see it an email and be like, "Oh, link's blocked. They didn't click it. All right, fine," go on. Me, I want to dig deeper. [00:08:00] Is this tied to any known campaigns? Why was this flagged? Who else got this? Who's the sender? I like to get a full understanding of everything and then try to dig into what's going on.

If you're a true crime person, you're going to like the forensics side of cyber. The defenders. The who, what, where, when, why. [00:08:30] If you always were that one that loved playing Clue. If you were that one that tried to figure out... If you hear stories or news cases of this company got breached and you always were like, "How?" That's cyber.