Sarah Pavelek: Hi, I'm Sarah Pavelek.

Raj Patel: And I'm Raj Patel. Welcome to the second edition of our Alumni News podcast.

Sarah Pavelek: We're partners in Plante Moran's cybersecurity practice, and today, we're going to talk about cybersecurity and how it might affect you personally. You might think you know how to protect yourself from cyberattacks, but hackers are always finding new ways to gain entry to personal information.

Raj Patel: We've been hearing about cyber horror stories for years. Everyone knows a story about somebody falling for a phishing scam. If you haven't been scammed yet, you might think you're safe, but the reality is if you don't stay vigilant, you might be the next target. Keep listening to hear three surprising things every technology user needs to watch out for. Plus some of our most eye-opening stories from the field.

Sarah Pavelek: The first thing that everybody should watch out for is increasingly sophisticated phishing scams.

Raj Patel: Phishing scams are not new. We've seen these emails for years. What's changed is how smart the hackers have gotten with phishing. In the old days, they would send mass emails and see who was going to click on the links. And they would try to get your credentials, your passwords, your login IDs. Today, they've gotten smarter — they target individuals. They might target a CEO or CFO or a family member, and they're going after your money. Most of these email scams ask you to wire money or ask you access to your financial data. Stay vigilant. If you get an email asking for your password, or phone call or text message asking for a password, never give it out. And secondly, if you're asked to transfer money, wire money or give it access to your bank account details, wire, email, text or a phone call, do not provide that information.

Sarah Pavelek: And I think one thing to remember too is these scams are not just over email now. They can also be over text message as well. And some red flags that you can look out for when you think you might have received a phishing scam is look at the email address and look at the text within the body. It could be from a company or a friend that you trust, but if it has a generic greeting such as, Dear Sir or Dear Madam, chances are it's probably not from who you think it is.

Sarah Pavelek: You want to look and see if the email address or the company name is spelled incorrectly or if it comes from a public domain such as, Gmail or Google. Check out for bad grammar. Oftentimes, these phishing scams don't have proper grammar within the text of the email or the text document. If it contains an attachment, that's also another red flag that it could be a phishing scam. And I think one of the most important things to remember is if you receive a message that's designed to make you panic, if it immediately instills panic in you, stop, think about it, and then call or separately email the company or the person that you received the message from.

Raj Patel: Sarah gave you great pointers on what to look for in an email. In addition to that, if you get an email that's suspicious from a friend or from somebody at work, you should call them back and verify. Did you mean for me to wire that money? Did you mean for me to give you these credentials? Similar with a bank, call the bank back. Do not just respond to the email — take a step back. That extra step is going to help you and protect you.

Raj Patel: Many of you know me; I love technology, and I'm very tech savvy and, in my home, we have a number of different smart devices that we have put in our house, whether it's the doorbell or it's the temperature gauge or it's the automated blind set we have in our homes. But also, I'm also concerned about the security of these smart devices. What we've done at our house is we have two networks. One is a private network where all these devices connect and they're not connected to the internet. And we have a second network where we go to the internet and that helps us protect these devices. It's inevitable that you will have these technologies in your homes, in your businesses, but there's ways to protect it.

Sarah Pavelek: And these devices are everywhere. They're in our homes, like Raj mentioned. They're in our cars as well. Anything these days can be connected —we've got TVs, refrigerators. One of the scariest things that I've heard are dangers attached to baby monitors and cameras in your home. There was a recent story about one of the Nest camera systems that a family was using for a baby monitor. And the monitor was hacked. A new mother and a father woke up in the middle of the night to a stranger's voice in their baby's room. When they turned the light on in their room, the stranger said, turn the lights off, I'm in your baby's room and I'm going to kidnap your baby. When they rushed into the 4-month's-old room, he was still sound asleep. The hacker had gained access to the baby monitor over the Wi-Fi network, and could see the baby in one room and the parents in a separate room. Again, it's something that you didn't historically think about with but with all these devices connected to our wireless networks, it creates vulnerabilities to an attack.

Raj Patel: One other thing to remember also is when you install these devices, they come with passwords to configure them and always change those passwords. Do not leave those passwords as they are because every person that bought that device knows that password.

Raj Patel: One of the things I like about my job is I get to travel. I travel to cities around the US and to cool places around the world. When I'm on the road, I always am conscious about protecting ourclients' data. The first thing I make sure is that my laptop and my phone is always safe. When I'm in a hotel room, I make sure it's locked up in the safe and not sitting out. The second thing I'm also vigilant about is how I connect to the internet. I will not use the coffee shop Wi-Fi, airport Wi-Fi, or hotel Wi-Fi because I cannot trust who set their Wi-Fi up and what are the security controls around it. What I have is I have my own data access point, and I

take that with me and I only connect to the internet using that point. I know it's secure and it's safe. That way I'm making sure when I'm on the road, I'm protecting our clients' data and my data.

Sarah Pavelek: And I don't know about you, Raj and the rest of you, but when I travel, inevitably, my cell phone battery is always running low at some point in time. It's very common for most of us to plug into a charger in the airport and we don't really even think twice about it. This is one of the newest cybersecurity scams out there and the technical term for it is called juice jacking. What it is, is when you plug your phone using the USB wire, when you plug it into a USB port in a public area, that USB port could be compromised. Once you plug it in, malware can be installed on your smartphone and that compromises your data. There's an easy solution to this and one that I tried to remember every time I'm traveling is avoid charging via the public USB ports. Just take your charger that you can plug into an electrical outlet and use that. Electrical outlets don't allow data transfer, and this is one way that that could help keep you safe from one of these newer risks.

Raj Patel: Also, when I'm traveling with my family on vacation or when I went on my sabbatical, I unplug my cable and my Wi-Fi box at home. I also unplug my home computer and that gives me safe of mind that no one's going to be able to get into anything at home or my computer at home. It's an easy step to protect yourself while you're on the road.

Raj Patel: Thanks for joining us for the second edition of Alumni News podcast. We hope you enjoyed it and found our advice helpful. I love connecting with alumni, so feel free to reach out to me with any cyber-related questions.

Sarah Pavelek: If you have any questions or want to talk about cybersecurity, you can find both of our contact information on this page below the podcast player. Thanks for listening and stay safe.