Announcer: The Missouri State Journal, a weekly program keeping you in touch with Missouri State University.

Emily Yeap: Online scams have been costly to Americans, especially in the past year. A recent report from the Federal Trade Commission finds U.S. consumers lost nearly three quarters of a billion dollars in 2021 to online scammers. I'm Emily Yeap.

Last week on the Missouri State Journal, cybersecurity expert Dr. Xiang Guo discussed several types of online scams. Guo, an assistant professor in the Department of Information Technology and Cybersecurity at Missouri State University, is back with me again today to offer some tips and advice about protecting against online scams.

Xiang Guo: Awareness is key. You don't have to know a lot of IT to be able to protect yourself. So there's hope. People just think, "Oh, no matter what I do, I cannot be helpful." No, it's not the real case. The real truth is that there's certain steps you can take to protect yourself, your family, your friends.

The first thing is that you should never click on any links on your email. You always go through the official website, especially when it's coming from your bank. You get an email from your bank, don't click on the link. Go to the bank website. You know where to go, and then when you go there, look for indicator.

Normally, those website will have a green padlock to show that's an encrypted site that's real. Look for those things. Have a antivirus software installed on your system. Any reputable vendors will be able to do that. They will monitor your traffic. They will show alerts. They will scan your files.

No matter what you do, have a paid version professional antivirus software installed. They're going to take care of 90 or 95 percent of the normal threats. Also, do not download anything from your email. If you send the email attachment to your friend, let them know through other means, either text messaging or call them and say, "I'm going to send you a file, and then you know that's from me." So practice those generic steps, going to minimize your chance that somebody trying to fool you.

Emily Yeap: It's important to limit what you share on social media.

Xiang Guo: Do not overexpose your personal information on social media. We all share pictures on Instagram, Facebook, on Twitter. It's fun to share that between friends, but then you need to understand, internet is not your private channel. If you share the information on the internet, it's the equivalent to posting that in the city hall.

You don't want to show your family address, your date of birth, or birthday party to bunch of random people. Normally, we don't want to do that. But we want to post it on Facebook because I have friends on Facebook. But also know that other people you don't know or have no idea can also see this on Facebook or any social media site.

You probably want to be a little bit more mindful because every picture you post expose some aspect of your life. That's how the phishing campaign or spear phishing happens. They look at your social media, they know who you are, and then your daily routines, they know you're working in this institution. You always go here and do those things.

That's what we call cyberstalking, right? When you give them more handle, and then when they come for you, it's hard for you to tell. If you do have to use social media, make sure you check the privacy settings. Limit that to only your friends, and then be careful who you be friends with.

There are certain things I will never post on my social media. My personal information, like social security numbers, that should never be posted anywhere. You should never even write them down because that's a risk. Your date of birth, birthday party photos because then when you do that, they figure out your date of birth.

If you look at online verification, they need to know your identity. They know your name, and then if you had to pay taxes, that's public record where you live. Your date of birth, that's something you can disclose. If you do that, and then they know who you are, where you live, and then they can get some other information from other channel, and then they can piece out a fake identity. A lot of people don't think their personal information values a lot. It actually values more than what you think.

Emily Yeap: Make it a point to segment out your life.

Xiang Guo: You want to use different type of account for different purposes. You want to make sure your professional life is separate from your personal life in term of your email you use or bank accounts and those kinds of things. I only use my school email dealing with university stuff. I don't use that for anything else, and only use my personal professional email dealing with my professional activities, LinkedIn, professional networking.

Then I have a shopping email for Amazon or any online shopping because that's different tiers. The financial email I use, I never share that with anybody. There's no way for somebody to know what email address I use with my bank. If you do that, you basically migrate your risk. You don't put all eggs in the basket, so to speak.

Oftentimes people want convenience, use one account across the board. But your bank may have high level security, but a online game may not, and then if you share the account between both and then the game got compromised, they going to try that with everything else. And then if you put all your stuff in the same account, then you going to have a whole lot more trouble in the future.

Emily Yeap: That was cybersecurity expert Dr. Xiang Guo from MSU. I'm Emily Yeap for the Missouri State Journal.

Announcer: For more information, contact the Office of Strategic Communication at 417-836-6397. The Missouri State Journal is available online at ksmu.org.