Announcer:

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

Emily Yeap:

For cybercriminals, stealing your personal information and money through online scams has become big business. The growth of social media use has resulted in even more scams, according to recent reports given to the Federal Trade Commission. More than one in four people who reported losing money to fraud in 2021 said it started on social media.

In 2021, more than 95,000 people reported about $770 million in losses to fraud from social media platforms. Those losses account for about 25% of all reported losses to fraud in 2021 and represent an eighteenfold increase over 2017 reported losses. I'm Emily Yeap.

My guest today is Dr. Xiang Guo, assistant professor in the Department of Information Technology and Cybersecurity at Missouri State University. He joins me to shed more light about online scams.

Xiang Guo:

Online scam has its own unique characteristics. Primarily it's because when people browse on the internet, they treat the internet a little different than they're doing normal face-to-face interactions. So there are a couple things online, you don't see where the other party are, and then you're basically being presented with limited information. Unless you understand the technology behind it, sometimes you don't know whether a website is real or not, whether a message is real or not. So that makes it very challenging for normal people to be able to distinguish whether this is a real email or this is a phish, or somebody trying to steal my personal information, or they're just trying to be helpful. So I think that's the primary reason why we see a lot of online scam, because they're targeting at the human weaknesses that we do not have the add-on layer of verification in online communications.

Emily Yeap:

Guo highlights a few types of online scams.

Xiang Guo:

There's a couple categories. So, the first category is what we call a phishing campaign. It's where the bad people, they're trying to gather information about the target. Instead of shooting random emails – I'm sure we all get email from a rich princess trying to transfer money and those kind of things – those are old, those are basically generic emails they're trying to target. But the phishing campaign is different. They're more targeted. So, instead of going off random stuff, they actually study you. So they look at your social media posts, they look at your friends, they look at what you do, and then they start craft all the emails that target at your workspace.

One example we have seen in the College of Business or other departments too, every now and then we'll get a random email coming from my department head. It'll have the same name, it will have the similar email addresses, and then you will just say, “I need this particular thing done in an urgent manner. I’m meeting with the clients, I cannot talk, please do that.” So, when they figure out your organizational charts, they know who the leaders are. Then they're trying to impersonate that leader and then trying to trick you to click on the links or do whatever they told you to. So this is harder to combat cause when you're in busy times, when I'm teaching classes, all of a sudden, I get email from my dean, how do I respond? I don't have enough time. They're trying to create the urgency. So that's one type.

The other type was the fake website, fraudulent links. So they send you an email that appear to be coming from your bank, ask you to reset your password. And then of course we're concerned about financial records and those kind of things. So we click on that link instead of thinking whether I should or not. And then when you click on that link, they build up a fake website, having all the graphics, it's easy for them to replicate, because all the materials are online. And then you go to say, Bank of America, but it's not a real website. It's a fake website. But if you don't know what you're looking for, and then they had a box to input your username, password. Every time they’re going yo say it's wrong because they're trying to gather the information. So that's another type of scam.

And then a third type is basically trying to scare people to do certain things. We heard about ransomware. In ransomware, they lock down your computer. They display a message on your screen saying, all your data will be erased within five minutes, unless you send me 0.01 bitcoin and those kind of things. And then there's a real ransomware. There's also another type it's called scareware. It's not a real thing. They basically showed you a picture and say, “Hey, you got hacked and if you click on this link, we'll help you.” And then people are not suspecting. They were just like, oh my gosh, I need help. I need to get out of here. So they click on that link and then through that, they either do some other malwares on your systems or they ask you to pay.

Those are the general types. There's more advanced tactics out there. But the thing is, they're trying to target at our human intrinsic weaknesses, right? We want to be helpful. We want to help each other out. When we are facing emergency, we go back to our instincts. We don't have time to think. So, I guess they're targeting to make you feel like this is urgent. I have to get it done. And then you reduce your reasoning skills. You don't look for signs. You don't look for the indicators and then you just fall for the traps.

Emily Yeap:

That was Dr. Xiang Guo, a cybersecurity expert at MSU. Tune in next Tuesday as he explains how to protect yourself from online scams. 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.