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

Emily Yeap: While the field of cybersecurity is advancing daily, cyberattacks are still a huge threat. In 2018, hackers stole half a billion personal records, a more than 100% jump from 2017. October is National Cybersecurity Awareness Month. This year's theme is Own IT. Secure IT. Protect IT. It emphasizes personal accountability and the need to take proactive steps to secure your personal information. I'm Emily Yeap.

My guest today is Dr. Richard Johnson, professor of information technology and cybersecurity at Missouri State University. He joins me to discuss data breaches and protecting yourself online.

Richard Johnson: We are hearing more about data breaches. U.S. laws are changing, over the last 10 to 20 years, requiring companies to report data breaches where they weren't before. But, they are becoming also more common just because of technology – the technology to actually dig into somebody's computer, they're getting better. The number of hackers is increasing. The number of devices connected to the internet is increasing, so all these factors means that there are more data breaches.

Emily Yeap: In a data breach, the types of information stolen may include names, dates of birth, email addresses, social security numbers, banking details and more. What do you do if you're a victim of a breach?

Richard Johnson: Contact the three major credit reporting agencies: Equifax, Experian and TransUnion. Freeze your credit report, which means nobody can open up any new lines of credit under your social security number, under your name, until you unfreeze it. Contact the credit card company or the bank immediately if you see some kind of suspicious activity on your statement. Check your transactions frequently. You've got to take action quickly, you don't wait two, three days, a week or two, to follow up with the bank. For some reason you've got good reason to believe your social security number has been stolen, you need to contact the IRS. That's very important to do that. The last thing is if you feel like somebody is getting into your bank accounts or credit card accounts, change your passwords immediately.

Emily Yeap: With no surefire way to avoid a data breach, how can you protect yourself online?

Richard Johnson: First of all, you need a mindset of got to protect my personal information – your phone number, and your address and your date of birth. You don't want people to know all those things, because hackers use every piece of information about you.

Emily Yeap: Another key step is to use complex passwords.

Richard Johnson: If you are a student at a university or you work for a company and you have passwords to get into the organization's computer systems, and they always tell you, "Well, you have to have a complex password." The requirements are really not that great, you have to have upper case letter, lowercase letter or maybe a number and a special character, and it has to be at least eight characters long. To be kind of ridiculous, some people might say, "Okay, my password is going to be password with a capital P, one, two, three, because that's really easy for me to remember." And then you have to have a password for where you bank, so I think I'll use password one, two, three." Oh, maybe you'll add an exclamation mark. You need better passwords than that, but the problem is it's a matter of convenience versus security and we tend to want convenience more than we want security.

You want to avoid words, because they're very easy to guess because the hackers actually have programs that can go through millions and millions of variations of different kinds of passwords with dictionary words in a matter of seconds trying to get into your account. Ideally what you want is a password like capital X, seven dash nine, four, six, X, Y, A, N. A very difficult password to guess, but are you going to remember that password? No, you're going to write it down and put it in your purse or your billfold and then you lose your purse or your billfold and somebody has your password. There are password managers where you can come up with one very difficult password for somebody to guess to get into the password manager, and then you can make up all kinds of random passwords for all of your accounts and you don't have to remember them. You just have to remember the one complex password.

Emily Yeap: If your identity has been stolen, make a police report.

Richard Johnson: That makes it official. If you don't file the police report, then your legal recourse may not be there in the future. You need to say, "Hey, somebody stole my identity," and they will file a report and then you can use that as future leverage to make sure that you're not held responsible.

Emily Yeap: That was Dr. Richard Johnson, professor of IT and cybersecurity at MSU. I'm Emily Yeap for the Missouri State Journal.

Speaker 1: For more information, contact the Office of University Communications at (417) 836-6397. The Missouri State Journal is available online at ksmu.org.