‘Good cyber hygiene’ part of digital lifestyle

University of Wisconsin-Oshkosh’s Cybersecurity Center of Excellence directors Jerry Eastman, left, and Michael Patton, in mask, are pictured Dec. 7 in the new center located at the Culver Family Welcome Center, 625 Pearl Ave. The center is run with help from Wisconsin Cyber Threat Response Alliance intern Sean Cannon, back left, and volunteer Thomas Barrett, bottom right. DAN POWERS/USA TODAY NETWORK-WISCONSIN

New UWO program wants businesses, community to get defenses up

Katy Macek Oshkosh Northwestern
USA TODAY NETWORK – WISCONSIN

OSHKOSH – If your home was burglarized, University of Wisconsin-Oshkosh information systems professor Michael Patton bets you’d tell people. When it comes to our information being burglarized, though, people are surprisingly quiet.

“If there was someone in your neighborhood breaking into houses, you would tell your neighbors,” Patton said. “That’s what’s happening in the cyberworld, but we don’t tell anybody.”

He is hoping the University of Wisconsin-Oshkosh’s new Cybersecurity Center of Excellence, which opened in September, can get people talking. Patton directs the new center with Jerry Eastman, president and founder of Wisconsin Cyber Threat Response Alliance.

The center is not only a place for UW-Oshkosh students studying

See PROGRAM, Page 5A

Program

Continued from Page 1A

cybersecurity but also, Patton and Eastman hope, a resource for individuals and small businesses to learn, train and better understand cyber threats before they happen.

"Cybersecurity is your ability to control, to an extent, the data that is out on the internet," Patton said. "We realize everyone's at a different phase in that journey."

The Cybersecurity Center of Excellence is about helping people at every phase, from the most basic, like how to connect safely to the internet, to hands-on training and cyberattack simulations that prepare organizations for what to do when — not if — it happens to them.

Center simulates real world: "We have some dangerous stuff in here."

Eastman leads the cybersecurity center, a room on the second floor of the Culver Family Welcome Center, 625 Pearl Ave., that is filled with clusters of computers and servers. He, Patton, a WICTRA intern and volunteers runs the center. Corporations donated much of the equipment.

It operates on a standalone network cut off from the rest of the university, which Patton said allows them to role-play real cyberattacks.

"We have some dangerous stuff in here," Patton said.

They can run every scenario from what happens in the moment an attack occurs to how management responds and helping business owners create and/or understand IT Disaster Response Plans. Patton said the idea is to expose them to things like a ransomware attack in a controlled environment, where they can learn how to respond to it before having to actually deal with it.

"We are here to elevate everyone's education, whether it's making people more aware of what it means to turn on technology and use it, all the way to high-end professionals who would like to have real-world experience," Patton said. "It's better to have dealt with a ransomware attack in a space like this than your actual organization."

Cyber threats are becoming more prevalent every day. Amanda Knutson, a supervisory special agent for the FBI-Milwaukee field office who manages the state's cyber task force, said they receive "nonstop complaints from individuals and companies" about scams, ransomware attacks, computer intrusions and data breaches.

The FBI's 2020 Internet Crime Report found that the American public in 2020 reported 791,790 complaints through its Internet Crime Complain Center that resulted in losses exceeding $4.1 billion. That is a 69 percent increase in complaints from 2019.

"We have been able to get by, most of us, thus far relatively unscathed," Patton said. "That is going to change drastically in the next few years, which is why we felt the need to get something like this (center) set up."

Fortunately, though, there are simple things everyone can do to be more cyber-savvy, much with just a change in mindset, Patton said.

"So much of cybersecurity is free, it's just changing your behavior," he said.

FBI agent: Keep "good cyber hygiene"

Patton himself was a victim of hacking over "something simple and stupid," he said.

He didn't have two-factor authentication set up on his Facebook account. A hacker guessed his password, changed it and then turned on two-factor authentication so Patton couldn't get back in.

His story is not unusual. Knutson said one of the biggest misconceptions about cybercrime is that people don't believe it could happen to them.

"People think it's always going to be somebody else's issue," she said.

Knutson recommends individuals and businesses practice "good cyber hygiene." The first step: Simply being aware of the many forms of cybercrime from spoofing and phishing attacks to charity and disaster fraud, advance fee schemes and more.

After that, she said there are basic measures to stop hackers from getting into your digital accounts, similar to locking your door and installing a security camera to stop physical theft:

- Create long, complex passwords, preferably 12-plus characters using a non-dictionary word.
- Turn on two-factor or multi-factor authentication (so hackers can't take over an account and lock you out, as Patton learned).
- Don't do anything using sensitive information on public Wi-Fi networks, which are generally not secure.
- Don't click on links or open attachments from unprompted emails, especially from people you don't know.
- Be wary of people asking for your personal information, especially via text or email.
- Wipe all devices before selling or tossing them.

"The average criminal wants to make the score as easy as possible," she said. "The more defenses you put up, the less likely you'll get hit."

Knutson shared an example of someone closing on a house and then receiving an email with instructions for wiring funds. Even if it seems legitimate, she recommends calling your contact directly before opening or following through.

"You cannot take the chance that somebody's intercepting that email," she said. "People lose their life savings thinking they're putting a down payment on the house."

Businesses have to maintain, invest in cybersecurity

It's equally important for businesses to follow cyber hygiene: Knutson said every organization should have an incident response plan that includes what to do if they become a victim and identifies all types of incidents that are possible and what steps to take.

"The organizations that are the most secure are the ones that have an executive management level that understands the importance of cybersecurity, prioritizes it and puts their money where their mouth is," she said.

Knutson recommends businesses keep software updated, use strong passwords and network firewalls, intrusion detection systems that warn of malicious behavior and regularly back up their data. Securing routers, encrypting all company devices and wiping those devices before disposing of them are also vital.

Knutson also recommends filtering email so employees are less likely to even see phishing emails and "white listing" employees who have access to sensitive information. A mirror to black listing, white listing means, by default, denying everyone certain points of the network and manually selecting only employees who can access.

"White listing is more difficult because there might be a time when you're blocking legitimate traffic, but it is more secure," she said.

The city of Oshkosh learned its lesson about phishing scams the hard way when it fell victim to a ransomware attack in February 2020. Tony Neumann, the city's information technology division manager, said the ransomware was activated by an employee who clicked on a link in a malicious email. It took down workspaces and servers.

"It's an eye-opener, especially when it hits close to home," he said.

Fortunately, the city had manual documentation, backups and cyber liability insurance that lessened the blow.

He said the city learned from that experience; it added more IT staff, hardened its network security and implemented a phishing training program to educate employees.

Training is one of the best things employers can do to educate their workforce, Knutson said.

That, Patton and Eastman hope, is where the Cybersecurity Center of Excellence can come in.

Center hopes to provide outreach for businesses, community

Unless you're planning to live in seclusion somewhere, Patton said its difficult to avoid a digital lifestyle. But you can learn how to responsibly engage.

"We live a digital life ... you are never 100% safe," Patton said. "The goal is to be aware of the dangers, know how to deal with them and be prepared, should something happen."

The Cybersecurity Center is a resource for students in UW-Oshkosh's Information Systems program with a cybersecurity emphasis. The university also has three different cybersecurity courses and a cybersecurity club that can use its services.

Eastman said one goal for the center is to give those students real-world experience, not only through role-playing scenarios but also by working directly with local businesses that experience cyber threats. He hopes the center will eventually establish itself as a place where those businesses can turn to for resources.

Eastman added they want to be a funnel that turns out students with a heightened awareness of cybersecurity,

See PROGRAM, Page 8A

Program

Continued from Page 5A

by partnering with local school districts.

"We want an integrated training pipeline from K-12 through businesses," he said.

The center is not in competition with cybersecurity firms large companies hire to protect their systems, but Patton said instead is hoping to complement those by acting as a resource, particularly for small businesses that can't afford their own IT department.

It's only been operating a few months, but Patton and Eastman have big plans for the center.

They hope to offer seminars and training as well as hands-on simulations to anyone who is interested. They are also partnering with the university's Women's Center for a "Women in Cybersecurity" speaker series.

"We have lots of really big ideas and visions, we just need time to get it rolling," Patton said.

The most important thing, though, is just to get people talking. Patton said most people are embarrassed to admit they've been a victim to hacking or cybercrime, but the reality is just about everyone has been.

Hiding it doesn't stop the bad guys. In fact, Eastman said, cybercrime is well organized and the criminals are communicating with each other about easy targets and places to avoid.

What everyone else really needs to do is follow the same model.

"If you're willing to speak and tell people," Eastman said, "that's how you can get back at the bad guys."

Contact Katy Macek at kmacek@thenorthwestern.com or 920-426-6658. Follow her on Twitter @KatherineMacek.