INSIGHTS REPORT

Protecting Your Campus in the AI Era

THE CHRONICLE OF HIGHER EDUCATION

sponsored by verizon

Explore strategies for protecting your campus in the AI era

Generative AI enables remarkable access to information for students and faculty, while unlocking new opportunities to streamline college operations. But it also puts new stress on your campus communication infrastructure. Maximizing the benefits of AI while minimizing any potential downsides is an ongoing challenge for any institution. That's why a reliable, fast, agile and secure communication and IT network is more important than ever for today's colleges and universities.

Ultimately, networks are about serving your community better by enabling and inspiring learning—while reducing the possibility of slowdowns, outages, or other issues. With the right network, your institution can:

- **Handle higher data volumes**
  AI, virtual reality, social media and other bandwidth-hungry applications can raise network traffic to the breaking point. A strong network can adjust to spikes and lulls, providing users with reliable, always-on connectivity.
- **Take control of cybersecurity**
  AI is supercharging cybercriminals, enabling new threats and scams at scale. A secure network and cybersecurity solutions can serve as an effective frontline against these threats.
- **Be ready for the future**
  An agile network lets you evolve quickly to meet evolving needs of your community and address new challenges.

At Verizon, we offer a wide range of advanced, proven networking options—including private wireless, fixed wireless access, SD-WAN and more—designed to meet the needs of educational institutions. We're pleased to support this special report from The Chronicle of Higher Education, "Protecting Your Campus in the AI Era." You'll find plenty of insights about how to keep your campus safe and productive while leveraging AI and other emerging technologies.

Want to know more about Verizon solutions for higher education?
Visit verizon.com/highereducation.

Patty Roze
Vice President, Public Sector Sales, Verizon

verizon

TABLE OF CONTENTS

Protecting Your Campus in the AI Era

By Jeffrey R. Young

4 INTRODUCTION

7 DEEPFAKES, AI-POWERED MALWARE, AND OTHER NEW THREATS

11 HARNESSING AI TO IMPROVE SECURITY AND BETTER EDUCATE USERS

15 NEW PRIVACY AND INTELLECTUAL PROPERTY CONCERNS

19 CONCLUSION

Contact CI@chronicle.com with questions or comments.

Protecting Your Campus in the AI Era was written by Jeffrey R. Young and underwritten by Verizon. *The Chronicle* is fully responsible for the report's editorial content.

Cover image: iStock

ISTOCK

A horde of AI bots might be attacking your campus's computer network right now.

The same generative artificial-intelligence technology behind friendly personal assistants advertised by Google, Microsoft, OpenAI, and other major tech companies also powers new tools that make malicious hacking more user-friendly than ever.

"Bad actors are basically playing general to an army of bots," says Isaac J. Galvan, community program director for cybersecurity and privacy at Educause, a nonprofit that supports technology at colleges. "They can get access to dozens or hundreds" of autonomous AI agents, he adds, which can try to send malware, or harmful software, to infect computers on a network with viruses or give hackers access to sensitive data.

The stakes are high, as students, faculty, and staff members are more reliant than ever on campus networks to go about their daily learning and work. Last March, for instance, a sophisticated cyberattack at the University of Winnipeg led officials to shut down the campus network to make repairs, forcing professors to cancel classes and postpone final exams.

Cybersecurity has long been a top concern of campus IT officials. But new AI tools are making

"Bad actors are basically playing general to an army of bots."

the task of securing networks more complicated, many experts say.

"The floodgates are open, and people are having to quickly adjust to the new generative-AI onslaught," Galvan says.

Most campuses haven't done enough to respond to new AI threats, though, according to a survey of college IT leaders released this year by Educause. It found that only 9 percent reported their institution's policies for cybersecurity and privacy adequately addressed AI-related concerns.

Meanwhile, cyber intruders see colleges as tempting targets. Most campuses support thousands of users of a wide range of ages and comfort levels with technology. There's also a diversity of valuable data for bad actors to thirst for, including personal information that could be used for identity theft and also specialized research data.

While generative AI gives bad guys better tools than ever, it also brings powerful new ways to protect networks from intruders.

"We do research that is classified," notes Luiz A. DaSilva, a professor of cybersecurity at Virginia Tech. And yet the ethos of the scientific method prizes sharing data rather than sealing it up. "Universities tend to be very open," he adds. "We want to collaborate with others and other organizations." That makes campus cybersecurity more challenging than at, say, a corporation.

It turns out that the biggest vulnerability on campus when it comes to AI are users themselves. For one thing, students or professors might get tricked into giving away their passwords, as AI makes so-called phishing schemes more believable. And when users on campus try free versions of ChatGPT or, say, the popular Chinese chatbot DeepSeek, the companies often grab the data for use in training their language models — or who knows what else.

"You're tempted to put the Excel workbook right into ChatGPT, but depending on what's in that information, you might have just created a security incident unintentionally," says Galvan, of Educause.

There is some good news amid the AI challenges, though. While generative AI gives bad guys better tools than ever, it also brings powerful new ways to protect networks from intruders.

Campus tech leaders increasingly employ powerful AI tools to scan campus networks for unusual activity and automatically spring into action when something seems amiss. It's the same approach used by banks to lock a credit card if, say, an unusual charge is made in a city far from the cardholder's home.

At Arizona State University, for instance, such AI-powered tools can now detect if a given professor's account is suddenly accessing files at midnight — a time when that user rarely logs on — and shut down access.

"To survive, cybersecurity must evolve. To win, it must innovate."

"Expecting human beings to comb through all that data and find those needles in a haystack is unrealistic," says Lester Godsey, chief information security officer at ASU. "But AI is particularly good at finding those needles."

And many campuses are using AI to improve the training opportunities they give students and faculty to avoid getting cyber-scammed, and they're tapping students to help protect networks in new ways. Colleges are also increasingly teaming up to share best practices, joining collaborative efforts like the Commonwealth Cyber Initiative, which is led by Virginia Tech.

It's cliché to say that cybersecurity is a game of cat and mouse — of constant sneak and pursuit, where the cybersecurity professionals may briefly gain an edge, only to be thwarted by clever new thrusts for the cheese.

Could something fundamentally new happen when AI cats and mice join the landscape?

"Defensive tools and strategies from previous time periods were not built to protect against current AI-driven cyberattacks," wrote Amit Ojha, vice president for digital technology for the fashion brand Spanx, in a recent op-ed in *The National CIO Review*. "To survive, cybersecurity must evolve. To win, it must innovate."

This report will consider the pros and cons of AI in securing campus computer networks, and look at innovative new approaches that could, possibly, alter the balance of power for cybersecurity in higher education.

SECTION 1

Deepfakes, AI-Powered Malware, and Other New Threats

ISTOCK

Not long ago, cybersecurity professionals rolled their eyes at users who fell for phishing attacks. The solicitations in emails or text messages were usually clunky and clearly suspicious, yet gullible students and even faculty members regularly took the bait, clicking on links that infected their computers rather than delivering a promised cat picture, or that tricked them into giving away their passwords.

In the age of generative AI, however, fewer experts are laughing, since new schemes look and sound eerily realistic.

Consider new types of phishing schemes that use AI to impersonate the voice of someone known to a user via a phone call or voicemail, a strategy known as "deepfake vishing" (that last word is a mash-up of "voice" and "phishing").

Professors are ripe targets for these attacks because many of them have posted plenty of clips of their voices on college websites or on YouTube that cyberattackers can sample to train an AI model. Free or low-cost AI tools can now accurately mimic a person's voice after being given just a short clip of a person talking.

"Imagine that a professor has a bunch of courses online — that's a lot of data that could be used to fake a voice message from the department chair that says, 'Hey could you send me this information?'" says Giovanni Vigna, a computer science professor at the University of California at Santa Barbara. He notes that he taught a cybersecurity

"Imagine that a professor has a bunch of courses online — that's a lot of data that could be used to fake a voice message from the department chair that says, 'Hey could you send me this information?'"

course online that's still freely accessible, and that if someone heard a voicemail that parroted his distinctive Italian accent, they could be easily fooled.

The professor knows such vishing attacks are possible because he recently crafted a fake voice message himself. "I participated in a hacking competition where we had to reproduce the voice of the professor who wrote the challenge in order to break into the system and win the flag," he says. And it turned out to be pretty straightforward using free open-source tools. "We just took a recording of this professor, and we synthesized something."

Some AI-powered scams now even fake video calls, with attackers posing as a user's friend in a Facetime call, with a realistic-looking computer-generated likeness saying they're having an emergency and need money wired, stat.

AI is also making phishing scams sent via email and text message more realistic — and more personalized. Cyber attackers who sample a user's public social-media posts or illegally gain access to personal text messages or email histories can train AI models that mimic a user's writing style and make it possible to drop in personal references in their attacks.

Cyberattacks that use "social engineering" — the way a con man might play a mark through psychological trickery — have been around for years, but until recently these scams had to be crafted by humans rather than bots. Vigna worked for a company a few years ago, for example, where the office manager got an urgent email that appeared to come from her boss asking her to buy 40 Amazon gift cards for an event and send the codes. (She started to purchase the cards, but then reached out to ask her boss a question about the request, only to learn he had no idea what she was talking about.)

The rise of AI tools, though, not only makes the scams more convincing, but easier for bad actors to automate and target more users.

"Scale" is the word that many cybersecurity experts use to describe how AI changes the threats that campus networks face. Automation is AI's superpower, after all, meaning tasks that once took a gang of criminals can be done by one criminal guiding bots.

And experts say that automation is leading to what is being called "malware as a service," where even someone without any computing knowledge can hire a provider from the dark web to do things like launch phishing attacks or attempt to steal user identities for a fee.

"There are illegal companies that will provide you with statistics on how well your malware is doing," says Darren Hayes, an associate professor and director of the cybersecurity program at Pace University.

And thanks to AI, these malware systems can automatically adjust their approaches as they go, refining their attacks based on past experiences without human intervention.

What's worse, some illegal providers now offer "ransomware as a service," says Hayes, meaning that they use AI to launch an attack against a

college or other organization and seek hefty fees to restore access.

Perhaps because AI has made it so much easier to stage ransomware attacks, they are on the rise nationwide at all kinds of organizations, including at colleges. Forty-four percent of data breaches between November 1, 2023, and October 31, 2024, involved ransomware, up from 23 percent the year before, according to a major report on data breaches by Verizon released in April. The study did note that fewer victims of these attacks paid the ransom, with only 36 percent forking over the money compared to 50 percent the year before. Meanwhile, a recent cybersecurity report from Trustwave Holdings found that in 2023 there were 352 ransomware incidents at educational institutions.

Thanks to AI, these malware systems can automatically adjust their approaches as they go, refining their attacks based on past experiences without human intervention.

To illustrate just how damaging these attacks can be, in 2022 a small private college in Illinois became the first higher-ed institution in the nation to close its doors for good because of a ransomware attack. The 157-year-old historically Black college, Lincoln College, said in a statement that a 2021 breach "thwarted admissions activities and hindered access to all institutional data, creating an unclear picture of Fall 2022 enrollment projections." Even after paying a ransom to restore access to its data (officials did not disclose the exact amount but said it was less than $100,000), the college was not able to recover.

The spread of cyberattacks due to AI has come at a tough financial time for many colleges. It seems like every day colleges face new challenges from Trump administration policies that threaten federal research funding, limit international students, or challenge institutions' tax-exempt status. In any tight budget period, says Hayes, of Pace University, "IT is sometimes one of the places to get cut."

Marshall University, in West Virginia, is one of many institutions facing budget restraints that have kept it from buying the latest tools when it comes to protecting their campus networks. Because of a deficit, the university is operating under what it calls a "Save to Serve" ethos to try to get the institution profitable by 2027.

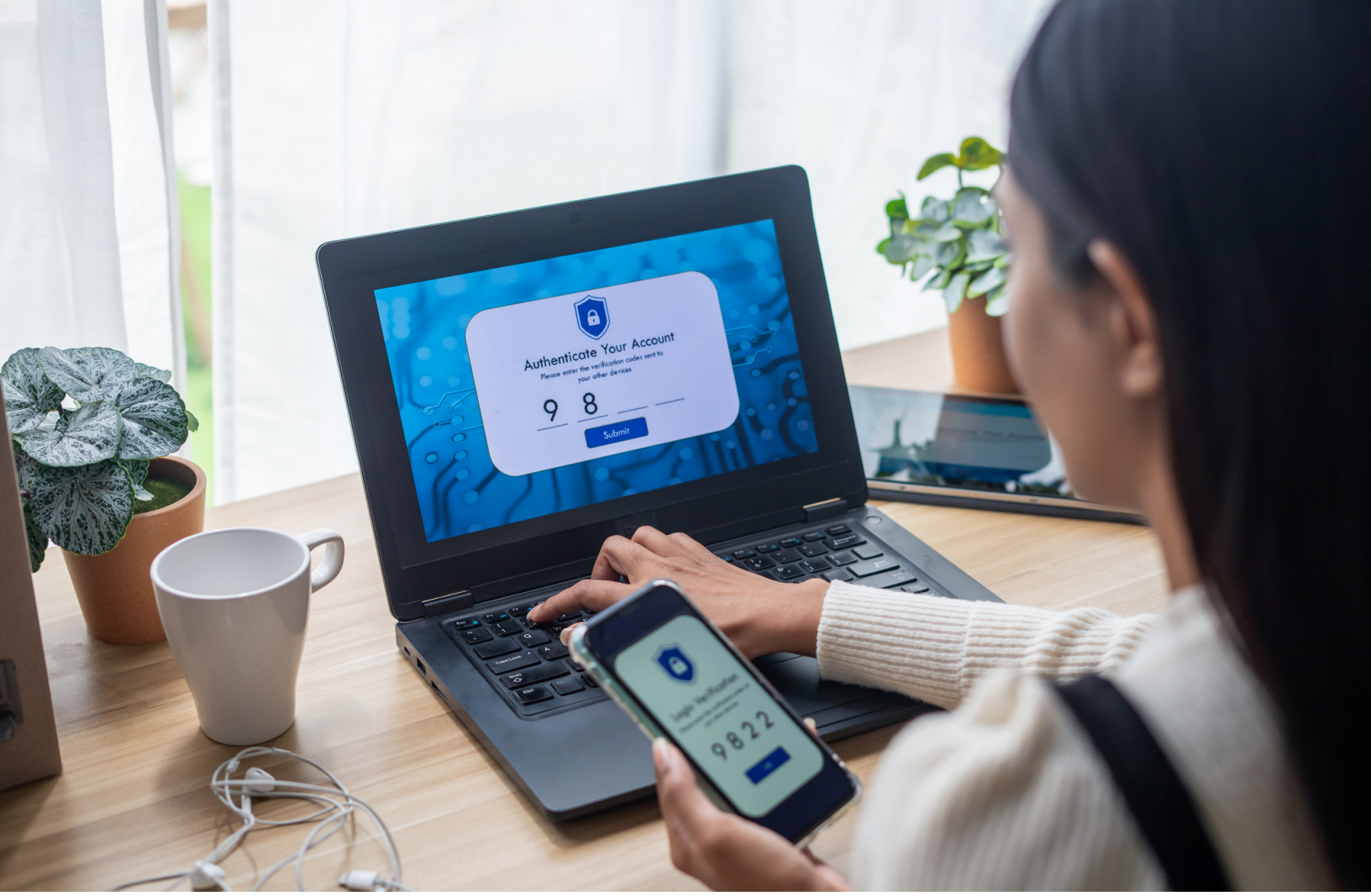
"We call it getting scrappy," says Jodie Penrod, Marshall's chief information officer. "We do the best that we can with what we have."

In cybersecurity, that means using AI to help IT staff be more efficient. For instance, officials are testing a way to use AI to sort through network logs, looking for patterns to help prevent attacks. There are off-the-shelf tools to do that, but they are out of the university's budget, so they have to build their own. "It's not going to have all the bells and whistles, but it's going to help you get something done," says Penrod.

New AI-powered network attacks make such innovation essential, Penrod adds. "By our latest metric we're getting about 100,000 hits every 10 hours on our network. With AI we're just going to see [attacks] increase exponentially."

SECTION 2

Harnessing AI to Improve Security and Better Educate Users



ISTOCK

As AI makes phishing attacks more sophisticated and prevalent, many cybersecurity experts say educating users in how to detect them is more important than ever. Thankfully, AI is helping to improve those education efforts.

In some ways, the bar for cybersecurity training was pretty low. The norm at colleges and many other organizations has been to require users to watch a training video on phishing scams and call it a day. You may have seen one of these educational videos — or just fast-forwarded to the end of the video to check a box. "A lot of training videos that are mandatory out there are pretty poor," notes Hayes, of Pace University's cybersecurity program.

Colleges are increasingly adding simulated exercises that force users to confront phishing scenarios in a more engaged way that has proven much more effective, Hayes says.

One example is at Cornell University, where an AI-powered system sends all campus users a tailored phishing email from a forged address at least once each quarter. Think of it as the cybersecurity equivalent of a fire drill. Users who click on the fake phishing scams are coached to be more discerning in the future. And the goal is to get students and professors in the habit of reporting phishing emails to campus officials by pressing the "PhishAlarm" button in the campus Gmail system when they see anything that looks suspicious.

"Successful reporting of that message via the PhishAlarm report button results in a pop-up congratulations note," explains the online instructions for the simulation program. "There is no punitive action for clicking links in a phishing

simulation, but each response provides information to the IT Security Office about which attacks are most likely to be successful."

And new insights from behavioral science could further strengthen these kinds of simulations, argues Cleotilde Gonzalez, a research professor in the department of social and decision sciences at Carnegie Mellon University.

"What we want is to maximize the learning of the end users and challenge them to do difficult cases," says Gonzalez. In an experiment, she and some colleagues presented phishing email scams to users that were more and more challenging, and used AI and cognitive-behavioral modeling to help predict what a user was most likely to fall for. The goal is to maximize the chances that when users get a scam, they can detect it even if it comes in a novel form or approach — which is key as AI makes new kinds of scams possible. "We need better training paradigms," she adds.

Hayes, of Pace, argues that education about phishing needs to start even before students get to college. Some high schools, he says, are using free online course materials from Khan Academy or other sources to educate students about phishing threats and the importance of changing their passwords frequently.

Many colleges, though, don't even mandate old-fashioned training videos, much less AI-powered phishing simulations. A new survey of campus chief technology officers conducted by *Inside Higher Ed* found that only 26 percent of respondents said that they require cybersecurity training for students.

These days more colleges are fighting AI with AI when it comes to defending their networks. As malicious hackers enlist armies of bots to attack campus systems, cybersecurity officials are bringing their own AI bots to the battle.

College cybersecurity leaders say that tools colleges already use to protect networks are adding AI features to do things like more sophisticated virus scans of any file coming in via campus email. Rather than simply look for files that match known malware, for instance, it is becoming common for scanning tools to consider a range of factors. "Attacks these days are constantly changing," says Godsey, of ASU. "We can leverage AI in the back end to look at an attachment more holistically."

In fact, one of the biggest wins from AI might be building networks that can "heal" themselves before any attacker can exploit a security hole.

And off-the-shelf tools like CrowdStrike and Microsoft Defender increasingly use AI in detecting threats to networks based on patterns, and even feature optional AI agents that can take preventative actions without having to check with a human staff member, within preset parameters.

In fact, one of the biggest wins from AI might be building networks that can "heal" themselves before any attacker can exploit a security hole, says Vigna, of UC Santa Barbara. He is getting ready to participate this summer in the AIxCC Cyber Challenge, sponsored by Darpa, an independent research and development agency within the Department of Defense. Teams will be provided software they've never seen before and tasked with using AI to find and patch flaws in the code without human help. The winning team will bring home a $4 million prize.

"Scale and speed are really the name of the game at this point," says Vigna. "Humans have been in the loop, and they are slow" at software patching.

But isn't there a danger that AI bots trying to heal a network could accidentally cause new glitches? Vigna believes the bots are up to the task, and he points out that they always report back to humans about what they've done so someone can check their work.

Many college leaders are also increasingly tapping into a powerful resource unique to educational environments — students.

Several colleges across the country are setting up student-run security operation centers, or SOCs, on campuses to help protect their computing environments.

One of the latest examples is at Miami University, where this summer officials are converting a former conference room into a dedicated space where student employees will take shifts monitoring the campus network for security threats and responding when they see trouble. The room is adjacent to where more-experienced campus IT officials work, so they can step in when larger issues emerge.

Student workers will gain real-world experience in a growing profession in which there is a shortage of qualified talent, says David Seidl, Miami's vice president for IT and chief information officer. And they will also help develop strategies for using AI to better secure networks.

The plan is to mount large IT panels on the walls with real-time information about the campus network, aiming to give the room the look of something out of a Hollywood spy movie. "You want it to be a cool experience for students," says Seidl. Four student workers will staff the facility by the fall, with the hope of expanding to six, if donors can be found to fund new positions.

Auburn University, Louisiana State University, Oregon State University, the University of Cincinnati, and the University of Nevada at Las Vegas are among other colleges that have set up similar student-run SOCs to monitor campus networks.

And AI chatbots are also making it easier and faster for colleges to give answers to students and professors who need to do things like reset their passwords or ask about a suspicious email.

That's true at Arizona State, which serves one of the largest populations of learners in the country with more than 150,000 students, about half in person and half online.

"We have a bot now that can answer a lot of those questions for our helpdesk," says Godsey, the chief information security officer, who adds the tool just went live this spring and is essentially a chatbot trained on internal documentation and even curated logs from help sessions by humans and users on the university's internal messaging channels. (Any identifying information is removed to protect user privacy). Though the university had a similar chatbot in the past, the new one is custom-built. "And we've already noticed a reduction in the sort of feedback" that human employees need to weigh in on," he adds. "In some instances it might just be shaving a minute or two off every engagement, but because of the volume, you start seeing significant savings and efficiencies over time."

SECTION 3

New Privacy and Intellectual Property Concerns

ISTOCK

As more professors experiment with AI in teaching and research (18 percent of college instructors called themselves frequent users in one survey last year), college tech officials are making a nuanced pitch: Please try tools like ChatGPT, but for the sake of federal law, do it carefully.

A key risk is keeping sensitive information private when using AI chatbots. Student information that professors routinely handle, such as student grades and even class rosters, is protected by the Family Educational Rights and Privacy Act, or FERPA, so colleges can't disclose that without student consent. Meanwhile, the business model of the free versions of many AI chatbots is to ingest any information that users type into the system and use it to further improve their models. And it's possible that if information typed in by a professor gets into a model, it could be revealed to other users. So a careless professor could easily run afoul of federal law.

At the University of Pittsburgh, the website for the University Center for Teaching and Learning puts it this way: "If the information is not already public, it should not be put into a free gen-AI platform."

Many colleges also support faculty members working with patient-related data covered under the Health Insurance Portability and Accountability Act, or HIPAA, which mandates that the records be kept private.

"I don't think people think a lot about protecting their own data," says DaSilva, of Virginia Tech.

Some colleges are signing contracts with tech companies including OpenAI, Google, and Microsoft so they can provide these AI chatbots to students, faculty members, and staff where the companies promise to keep all user information private.

One of the first colleges in the United States to jump in was the University of Michigan, which since 2023 has operated UM-GPT and other customized AI tools on a website available to its users.

The university's chief information officer, Ravi Pendse, says that ever since he first tried ChatGPT, he felt that "generative AI was going to be the most impactful tech of our generation," and he expects AI to rival the internet at how it could change many facets of daily life. "But," he says, "we have to use it responsibly, ethically, and legally."

"I don't think people think a lot about protecting their own data."

So the university has made a big investment, dedicating "two or three staff members" to build tools for use on campus, and paying for licenses with several different AI companies, Pendse says.

One tool the university developed, called U-M Maizey, is designed for researchers on campus to have a user-friendly way to bring generative AI into teaching and research.

On the research side, Pendse hopes that AI will help advance innovation in science, pointing to a project at the University of Toronto where AI helped scholars find a nanomaterial that is stronger than steel, by combining substances that humans hadn't thought to put together. And if professors use U-M Maizey, Pendse says, they know their intellectual property will be protected. The tool offers what is called a "temperature" setting that allows researchers to adjust the "output-randomness" of the AI model, according to the U-M Maizey website. A high-temperature setting leads to more out-of-the-box results, though in some cases those might be too outlandish or unworkable for actual research. A low-temperature setting results in more conservative answers that have a "high probability of being accurate."

For teaching, the university has integrated the Maizey tool into its course-management system, so that professors can access it easily. Maizey allows instructors to upload their teaching materials into the AI tool and ask it to generate quizzes for students or let them ask questions of the material using a chatbot interface. Copyright issues have emerged as professors have started to use the tool, however. When a professor wanted to upload a 750-page book into the system to let students ask questions to test their understanding, Pendse pointed out that the use could run afoul of the publisher's rules.

A couple of other universities have set up similar AI hubs for campus users, including ASU, and other colleges are signing contracts with AI providers to offer campuswide access in ways that protect privacy and intellectual property. A survey of college tech officials last year found that 20 percent of colleges have collaborated with AI companies, with another 32 percent considering such arrangements.

Pendse says that Michigan plans to make its AI tools available open source so that other colleges can easily offer similar services. Michigan also hopes to offer a service to colleges to help them install the AI tools, and to make the fee low for colleges but higher for corporate users.

Some college officials worry, though, that AI will open a new digital divide on campuses, with some being able to afford the tools and others getting left behind. “How are we going to make sure everybody has access to the tools?” asks Galvan, of Educause.

Most campuses haven’t even set up rules of the road for using AI, much less offer their own AI services. Only about 39 percent of campuses have an acceptable-use policy for AI, according to Educause’s AI Landscape study, which is subtitled, “Into the Digital AI Divide.”

The secret to success will be for colleges to work together to bring in AI, argues Michael Zastrocky, executive director of the Leadership Board for CIO's in higher education, a nonprofit group supporting campus technology.

“The more we share and help each other, the better, and that’s something unique to higher ed,” says Zastrocky, noting that colleges have a culture of sharing detailed information about best practices in technology, rather than treating innovations as business secrets.

One of the latest examples of that spirit is being led by the University of California at San Diego.

Rather than pay licenses to OpenAI or another model on the cloud, the university installed the open-source Llama AI model released by Meta and runs it on a data center on campus, giving officials full control of the data. And the price to offer the service to campus users, on a website it calls TritonGPT, is roughly a tenth of the cost of working with OpenAI or Google, says Vince Kellen, UC San Diego’s chief information officer.

Some college officials worry, though, that AI will open a new digital divide on campuses.

And the university has partnered with other campuses to share the system. That includes working with San Diego State University and community colleges in California through a collaboration called the Equitable AI Alliance.

“The mission is to democratize access,” says Kellen.

So will AI ultimately make college networks more vulnerable, or more secure?

Vigna, of UC Santa Barbara, argues that AI will turn out to be a win for campus cybersecurity, since bringing greater scale to defensive systems will make networks so solid that they will be able to withstand the greater barrage of attacks enabled by AI.

"Think about soccer," he says. It's already extremely difficult to get a ball past a goalie, and AI essentially allows multiple goalies at once, as bots can help detect attacks and automatically patch software holes. In his view, "that really helps defense more than the attackers."

But putting in these AI goalies comes at a cost.

"We aren't spending less money each year on cybersecurity and cyber threats, we spend more each year," says Zastrocky, of the Leadership Board. These days that is hard for colleges of any size, but especially smaller ones who have struggled to afford the latest tools.

He argues that AI is just the latest technology that campus officials have to adjust to, as they have for previous innovations. "We have to get smarter than the bad guys," he says. "We're getting closer to having a better understanding about how to thwart attacks that are caused by AI, but we have to work hard to prevent catastrophic events that can take place with AI."

Kellen, at UC San Diego, believes that AI will be a net positive because he sees more and more mainstream networking and computing tools — even routers, laptops, and cellphones — beginning to add AI features to prevent attacks. "AI at the edge is here, the products are shipping," he says, "and that AI is going to be able to detect threats and better prevent it from attacking you and spreading." He predicts that such tools will be common within a year or so, and that any added costs will likely be "worth the ROI" in terms of protecting networks. "If I have 1,000 routers and network switches, I'm going to have 1,000 little language models all looking for attacks."

"If you raise the barrier to entry for cyberattackers, the cyberattackers become fewer — they become well-funded, but they become fewer, and then their targets become very select," Kellen adds.

"We have to get smarter than the bad guys."

No one *The Chronicle* interviewed for this report appeared worried that putting intelligent agents in every device and network switch would lead bots to attempt to take over the world, as Skynet did in the *Terminator* movies.

"The large language models that power today's AI are remarkably limited," says Kellen. "Generative AI is not proficient in all the things that make us human. It has no self-awareness. It has no agency. It has no self-determination. It has no sorrow or loss. It has no motivation."

Plus, adds Vigna, of UC Santa Barbara, these AI models are being used in "very constrained and very well-defined ways." As he puts it: "It's not like

it's able to directly break into your bank account."

One longtime expert in cybersecurity, Alex Stamos, recently discussed this question on an episode of the podcast *Search Engine*. He's the chief information security officer at SentinelOne and a lecturer in computer science at Stanford University.

"Something I tell my Stanford students is that security is an incredible field to get into, because it's the only part of computer science that gets worse every year," he says, meaning it's full of new challenges. "Every part of CS just magically gets better — like graphics, and compute [the hardware and software it takes to make fast calculations], and storage. But systems get more complex, less understandable, and more important every day, and as a result systems get less safe. And there's more desire for people to break them and more need to make them safe. And I think AI has just massively multiplied that."

THE CHRONICLE
OF HIGHER EDUCATION

1255 23rd Street, N.W.
Washington, D.C. 20037
202.466.1000 | Chronicle.com