Three cyberattack trends affecting higher education to look out for in 2025.

INTRODUCTION

Security, administrative, and academic leaders in higher education will need to focus on a wide range of cyberattacks in the coming year.

There are three notable trends to watch for:

1. Cyberattacks targeting supply chains of colleges and universities.
2. Attacks leveraging the power of generative artificial intelligence (GenAI)
3. "Insider threat" attacks by bad actors who become illegitimately employed by higher ed institutions

Higher ed leaders who effectively detect and prevent these three types of attacks will make significant progress in strengthening cybersecurity this year.

CYBERATTACK 1: SUPPLY CHAINS

In 2025, cybercriminals will increase the number of cyberattacks aimed at supply chain networks of vendors, suppliers, contractors, and customers associated with colleges and universities.

To a growing extent, cybercriminals are finding an abundance of "open doors" within supply chains and steal sensitive information and generate revenues.

Frequently, they start by attacking a third party in the supply chain to establish a foothold because these entities are often smaller in size and resources than colleges and universities. Once inside, they eventually go after the larger target. The higher ed institution which has an abundance of sensitive employee and student data as well as intellectual property.

Tip:

Conduct thorough due diligence on third party suppliers with whom your institution shares its most sensitive data. Identify cybersecurity controls they have in place. Ensure they have widespread encryption, use multifactor authentication, and require complex and long passwords.

If you find your supply chain business collaborator unwilling to share enough information to satisfy the level of security risk you need, it might be best to stop sharing information and find a more cooperative vendor.

CYBERATTACK 2: MORE COMPLEX AI-DRIVEN CYBERATTACKS

It's no surprise there will be more new types of cyberattacks than ever launched in 2025 that leverage the power of GenAI. Cybercriminals will use the technology to unleash a barrage of newly configured crimes including AI-powered malware, AI chatbots, AI-fueled identity theft, AI-enabled web and voice-based attacks, and AI-generated phishing emails and text messages (vishing). It will be noticeable this year how much more convincing, harder-to-detect, higher in number, and more automated these attacks will become.

Tip:

Use GenAI to quickly and accurately detect these cyberattacks. Take advantage of the productivity benefits of AI automation to streamline cybersecurity tasks.

The more you use AI to fight cyberattacks more efficiently, the more likely you are to bolster cybersecurity.

NEW TYPES OF AI-POWERED PHISHING CYBERATTACKS

This year, you'll notice that cybercriminals are launching relatively new types of AI-fueled phishing attacks. One is called "hybrid phishing." In this scenario, a bad actor will, for example, send an email to a higher education administrator or professor. The email will contain a phony bill from a well-known company saying that states the target victim was charged $1,000 (or some other amount) for a recent purchase.

But that transaction never happened. In the email, there will be a sentence worded something like this: "If you had an issue with this charge, please call this phone number: xxx." The ploy aims to lure target victims into placing a voice call questioning the bill, then tricking them into releasing sensitive information such as a password.

Tip:

If you get an email indicating you paid for something you're not aware of and there's a phone number included , don't call the number and don't respond to the email. That's a red flag that you actually received a hybrid phishing cyberattack.

DETECTING DEEPFAKES

Like 2024, GenAI-powered deepfakes will continue to be a major problem within higher education institutions this year. Deepfakes are created videos or audio recordings showing someone doing or saying something that never happened. A deepfake aims to intentionally cause the target victim harm often by stealing their sensitive personal credentials or coaxing them to click on a link that unleashes malicious software. The goal is often to disrupt or halt a victims' computer network from functioning; or, impair several computers and networks across the university.

Be especially vigilant to spot audio deepfakes, which are becoming more widely used because they tend to be more difficult to detect than video deepfakes. Decision Market Research finds that from 2024 through 2033 the annual global growth rate for voice deepfakes is projected to be 37.6% and will total $79 million this year (34% in North America).

Tip:

If you receive a phone call unexpectedly from someone you know asking you to take some action urgently, stop. It's probably an audio deepfake. If the person's voice seems in any way odd in tone or not quite how they usually sound or speak, that's a red flag you're the target of a deepfake.

CYBERATTACK 3: INSIDER THREATS

Fueled in part by the growth in remote working, there will be more insider threats in 2025 that lead to cyberattacks against higher education. In one likely scenario, for instance, IT workers from North Korea pose as Chinese and Russian IT freelance contractors searching for remote working job opportunities. Their aim could be to obtain employment under false identities in U.S.-based colleges and universities.

Operating as employee "insiders" in these organizations, they could likely steal sensitive data and/or money, demanding ransom payments from the college or university that hires them. These cybercriminals may be focused on stealing money or cryptocurrency along with gathering weapons of intelligence to fund North Korea's military operations.

Alternatively, these bad actors can steal the identities of legitimate U.S. citizens to become employees of colleges and universities in order to obtain sensitive information and benefit financially.

Tip:

If you receive a job application from an IT worker claiming to be in China or Russia, be sure to do a thorough background check to verify the applicant is from China or Russia and not North Korea. For better transparency, an in-person or video interview should be required before hiring. Once hired, if the IT worker asks to use a personal laptop PC or won't enable their video during a Zoom call, that's a red flag it could be a cybercriminal.

Monitor employees' online behaviors for abnormal activities such as multiple login attempts, unusual working hours and requests for privileged access to sensitive information.

Throughout the year, other major cybersecurity trends will be shared.

QUESTION:

What do you think are the three biggest cybersecurity trends to watch this year and why?

Please include your thoughts in the comments section.