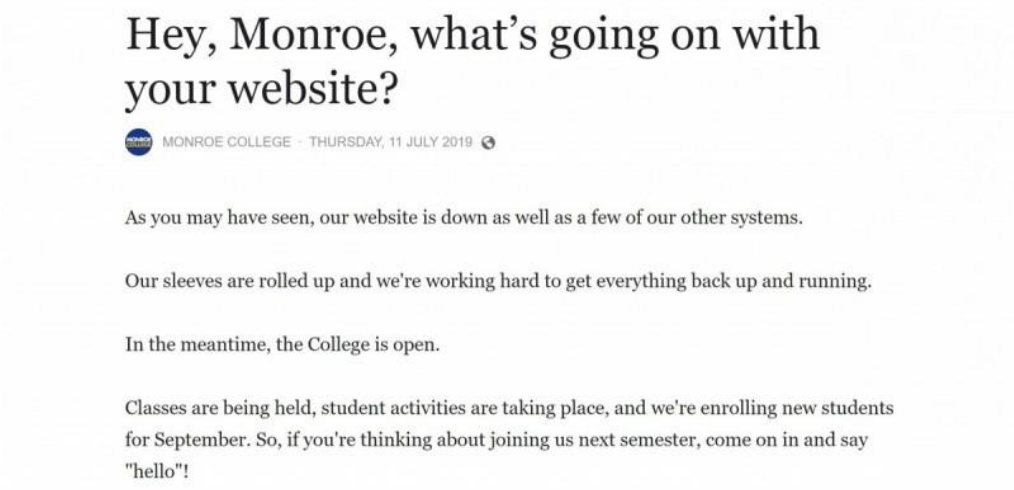
INSIDE HIGHER ED

Hackers Demand $2 Million From Monroe

College's IT system was attacked by hackers demanding $2 million in Bitcoin. Experts warn that other institutions are vulnerable to similar attacks.

By Lindsay McKenzie

July 15, 2019


Hey, Monroe, what's going on with your website?

MONROE COLLEGE · THURSDAY, 11 JULY 2019

As you may have seen, our website is down as well as a few of our other systems.

Our sleeves are rolled up and we're working hard to get everything back up and running.

In the meantime, the College is open.

Classes are being held, student activities are taking place, and we're enrolling new students for September. So, if you're thinking about joining us next semester, come on in and say "hello"!

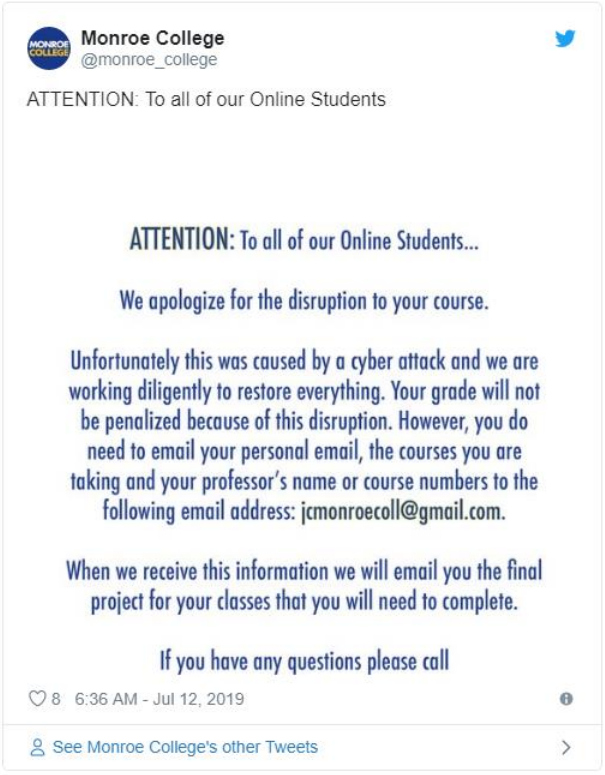
A cyberattack disabled many of Monroe College's technology systems and platforms last week. Students and faculty and staff members were locked out of the college's website, learning management system and email, with hackers demanding payment of around $2 million in Bitcoin to restore access.

Marc Jerome, president of Monroe College, a for-profit institution in New York City, confirmed the cyberattack in a statement July 11. "Our team is working feverishly to bring everything back online, and we are working with the appropriate authorities to resolve the situation as quickly as possible," he said.

“In the meantime, Monroe continues to operate,” said Jerome. “We’re simply doing it the way colleges did before email and the internet, which results in more personal interactions. As we have done throughout our 86-year history, we are coming together to assure that our students, faculty and staff are well served."

Jackie Ruegger, executive director of public affairs at the college, said in an interview Friday that the institution did not know who had orchestrated the attack. She said the college is working with local law enforcement officials and the Federal Bureau of Investigation. She did not comment on whether the college plans to pay the $2 million ransom.

Despite the college’s learning management system, Blackboard, going down, students continued to attend classes last week, handing in homework on paper, said Ruegger. The college’s online students have been advised to contact the college through their personal email accounts.



Over the weekend, the college's main website came back online. The college has not publicly shared whether access to its IT systems has yet been restored.

Jared Phipps, vice president of worldwide sales engineering for cybersecurity company SentinelOne, said these types of attacks have been linked to a small number of sophisticated criminal groups.

"They scope out the size of the organization and its ability to pay the ransom," said Phipps. "They're determining your pain threshold."

Earlier this year, Grinnell, Oberlin and Hamilton Colleges were subject to a ransomware attack on their admissions systems, but the hackers demanded just a few thousand dollars, which was later reduced to $60. Local governments, police departments and health organizations have also recently been attacked. In Baltimore, for example, the city government has refused to pay hackers after a cyberattack earlier this year, opting instead to rebuild its systems at a cost of over $18 million. The hackers originally demanded $76,000.

Typically these attacks start with a phishing email -- an email disguised to look as if it is from a trusted source, said Phipps. If someone unwittingly clicks on a link in a fraudulent email or enters their personal log-in information, hackers can install malicious software known as ransomware, which will encrypt and block access to the users' computer files. The hackers then demand money for the encryption key. If there are no backups of the system elsewhere, institutions are left with few options, said Phipps -- rebuild or pay.

Attempted ransomware attacks happen every day, but it is difficult to gauge how many of the attacks are successful, as "nobody is required to disclose it,"

said Phipps. “If nobody’s personal information is lost, you don’t have to disclose,” he said. Information from cyberinsurance companies suggests, however, that attacks are on the rise, and many organizations are choosing to pay because they aren’t able to restore their systems from backups, he said. Ben Woelk, information security office program manager at the Rochester Institute of Technology, said that successful attacks in higher education at the institutional level are unusual as attacks are “more often targeted at specific individuals, and the ransom demands are nowhere near as high.”

Both Woelk and Phipps agree that the attack on Monroe is notable because of the large ransom the hackers are demanding from the college. “This is the highest amount I’ve seen in higher education,” said Phipps.

Ensuring institutions have isolated backups so that systems can be restored if they become compromised is critical, said Woelk. Software that monitors unusual computer activity and filters out suspicious email is also useful, but the most important defense against a ransomware attack is education, he said.

“You need to train your community to recognize anything suspicious and report it ASAP,” said Woelk. In the past few years, many colleges have started to use simulated phishing programs -- deliberately sending fraudulent-looking emails to faculty, staff and students to see how they respond. Previously, many institutions were unwilling to take this approach because they didn’t want to “trick” their community, but it’s increasingly seen as necessary, said Woelk.

Michael Corn, chief information security officer at the University of California San Diego, said crippling ransomware attacks like the one Monroe College experienced are the “exception and not the rule.” Nonetheless, Corn

said higher education institutions should be doing more to prevent and prepare for these kinds of attacks.

At his institution, Corn has encouraged his colleagues to think through how to respond to a crippling cyberattack just as they would for an active shooter situation or an earthquake as part of their “all-hazards” emergency operations planning. “We’ve carried out a drill asking how we would respond to this. That kind of planning makes me feel much better about our preparedness and raises awareness,” he said.

Corn said that his institution has agreed that it would not pay a ransom in the event of an attack. There is no guarantee that once you pay, the hackers will give you a working encryption key, said Corn. And paying up might indicate that you’re an easy target for future attacks, he said. He acknowledges, however, that there are data -- medical records, for example -- that might make the institution think differently. “It’s a decision we’d have to make in the heat of the moment.”

Read more by Lindsay McKenzie

https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack?utm_source=Inside+Higher+Ed&utm_campaign=af9a6d96b1-WNU_COPY_01&utm_medium=email&utm_term=0_1fcbc04421-af9a6d96b1-199133009&mc_cid=af9a6d96b1&mc_eid=6f67a838c9