Expert: COVID-19 is giving cyberattackers an opportunity to hack universities

July 20 2020, by Alicita Rodriguez

Credit: CC0 Public Domain

In July, the University of California, San Francisco paid $1 million to hackers who stole data from the university's School of Medicine and threatened to publish it. Michigan State University and Columbia

College Chicago were also recently attacked. This past January, Regis University in Denver paid a ransom to hackers. Are colleges and universities being specifically targeted by cyberattackers? We asked Joseph Murdock, cybersecurity expert and faculty in the Business School, for answers.

What is Ransomware?

"Ransomware is a type of malicious software (malware) that is designed to encrypt your data files," Murdock explains. "Once encrypted, it will then ask for a ransom to be paid in something hard to trace like Bitcoin or some other crypto-currency. If you pay the ransom, the attacker will typically send you the key to decrypt your files."

The reason ransomware is on the rise is because it works. "It is estimated that in 2018, ransomware was an $8 billion industry for attackers," Murdock said. Hackers are not specifically targeting educational institutions. "In 2019, the education sector only attributed 5% of overall ransomware attacks, so it is a relatively small segment," Murdock explains. Government and manufacturing are the two top segments hacked by cyberattackers. The reality is that hackers are just going after large computer systems at organizations that can pay large ransoms—universities included.

Don't Click on Phishing Emails

Of course, the more people use a system, the greater the chances are of successfully infiltrating it. "According to the 2020 Verizon Data Breach Investigations Report (DBIR), 94% of malicious software enters an organization via email," Murdock said. Murdock points out there is a simple solution to help protect all organizations, including universities, from hacking. "Training your users to be able to spot malicious emails

(phishing emails) and not respond to them or click on any links is very crucial," he said.

With so many students, faculty, staff, and alumni relying on university email accounts, there are ample opportunities for hackers to infiltrate a university computer system. "Due to so many malicious attacks coming successfully via email, user awareness training has a huge impact on how secure an organization can be," Murdock said. For those who may have forgotten how to recognize phishing attacks, the Office of Information Technology has some valuable tips (see box below).

COVID-19 Pandemic Increases Ransomware

Unfortunately, the pandemic has turned into an opportunity for hackers. "Since the start of the current COVID-19 pandemic, an uptick in malicious emails has been seen with related subject lines," Murdock said. "People are hungry for information about the pandemic, so these emails may have a higher success rate than the typical phishing email we are all used to."

The health crisis has also inadvertently created more opportunity for cyberattacks to be successful. "You have many workers that have had to transition to working from home, which has created a strain on IT departments to support these remote workers and their home computing devices, which may not be as secure as the equipment maintained by the organization," explains Murdock. More people working from home basically creates "an additional path of entry for attackers."

Due to the pandemic and the increase in students, faculty, and staff working from home, universities will need to be more careful now than ever before. "If the trend of successful ransomware attacks on universities continues, I imagine the attacks will become more common as attackers will see they can exploit this segment successfully,"

Murdock said.

More information: 2020 Verizon Data Breach Investigations Report: enterprise.verizon.com/resources/reports/dbir/

Provided by University of Colorado Denver