The Hoya
Since 1920

Howard University Ransomware Attack Prompts Georgetown To Take Additional Precautions

September 16, 2021 by Sarah Conner (https://thehoya.com/author/sarah-conner/)

Georgetown University urged community members to take precautions against potential network breaches Sept. 9 after Howard University fell victim to a ransomware cyberattack that forced the college to suspend all classes for four days.

A ransomware cyberattack struck the Howard network Sept. 3, disrupting the university's systems and forcing its information technology team to take the systems offline to address the attack. In response to the hack, Georgetown University and the FBI provided (https://www.nytimes.com/2021/09/07/education/howard-university-ransomware.html) assistance to Howard's IT department.

While Howard was able to restore some services, like its WiFi, and resume instruction, the ransomware attack remains an ongoing threat, according to a Howard University spokesperson.

"Our IT team continues to work diligently, night and day, to bring our systems back online, and as a result, WiFi has been restored across campus, face-to-face classes resumed on September 8th, and online class instruction resumed as of September 13," a Howard University spokesperson wrote in an email to The Hoya. "We have a long road ahead, and a dedicated team of professionals continue to monitor the situation and address outstanding issues as they are identified."

@howard1867/INSTAGRAM | A Sept. 3 ransomware attacked forced Howard University to suspend classes for four days while the university worked to restore its systems.

Before the attack, Howard students were required to use two-factor authentication any time they log in to access university servers. After the hack, Howard also announced new password requirements for students and faculty Sept. 13 after the attack. Georgetown has enacted similar rules for students in the past, including requiring community members to update their passwords June 1.

While Georgetown was not the victim of a cyberattack, the university has taken additional precautions to protect the university against a similar attack, according to Judd Nicholson, Georgetown vice president for information technology and chief information officer.

"UIS has taken a number of steps to prevent such attacks against the Georgetown network, including increased network monitoring," Nicholson wrote in an email to The Hoya. "Because of security concerns, we do not release specific details about these precautions."

Ransomware attacks in Washington, D.C., have increased in recent years. In 2016, Georgetown MedStar Hospital was the victim (https://www.washingtonpost.com/local/likely-ransomware-cyberattack-still-crippling-medstar-health-computers-at-some-hospitals/2016/03/30/a82c9fa8-f687-11e5-8b23-538270a1ca31_story.html) of a cyberattack on patient records and email databases. In May 2021, the Metropolitan Police Department suffered (https://apnews.com/article/police-technology-government-and-politics-1aedfcf42a8dc2b004ef610d0b57edb9) a cyberattack by a Russian ransomware syndicate. In both attacks, hackers demanded monetary compensation to restore the operating systems; however, neither victim paid the ransom.

The motive behind the Howard attack is unclear, according to Clare Sullivan, visiting professor at the Georgetown University Law Center and executive director of the Cyber SMART Research Center, a collaborative technology research firm at Georgetown University.

"Usually money is demanded and economic advantage is often the motivation," Sullivan wrote in an email to The Hoya. "However, there can be other motives such as to cause damage or to show power. The latter are more likely to be motivated by a grievance, sometimes by a disgruntled applicant or student or employee; or by someone just wanting to cause disruption and observe the ensuing chaos."

If Howard is blackmailed for monetary compensation, administrators will have to make a difficult decision, according to Eric Burger, a Georgetown computer science research professor and member of Cyber SMART.

"They're going to set the price such that Howard can pay," Burger said in a Zoom interview with The Hoya. "If they say half a million dollars, or $100,000, then Howard is in a really tough spot: Are we going to spend a week rebuilding our systems or are we going to pay?"

Though there is no evidence any personal information was stolen during the attack, Howard considers the hack an ongoing threat and will continue to work with the FBI to restore the university's system capacities, according to a Howard University spokesperson.

While ransomware attacks may happen again in the future, practicing individual cyber safety remains the best way to combat potential threats, according to Sullivan.

"Always keep in mind that your personal information, particularly your identity information, is valuable, dont disclose it unless you know to whom you are disclosing it, how your information will be used, and how it will be protected," Sullivan wrote.