The University of Calgary paid a ransom in bitcoins amounting to $20,000 after a recent ransomware attack on its computer systems. [According to the university](http://www.ucalgary.ca/utoday/issue/2016-06-08/university-calgary-makes-significant-progress-address-systems-issues), the staff was able to isolate some of the affected machines and was working to ensure its systems are operational. University Vice President of Finance and Services Linda Dalgetty said that the cyber-attack that crippled multiple systems on May 28 leaves no indication that any personal data was released to the public. She also added that the officials agreed to pay the ransom to ensure critical systems could be restored, but it may take some time for the school’s IT staff to apply the decryption keys to the infected machines.

“As part of efforts to maintain all options to address these system issues, the university has paid a ransom totaling about $20,000 CDN in bitcoins that was demanded as part of the ransomware attack,” Dalgetty explains. She also added that while paying the ransom was not exactly the “proper” course of action, the university could not risk losing critical data. “We are a research institution, we are conducting world class research daily and we don’t know what we don’t know in terms of who’s been impacted and the last thing we want to do is lose someone’s life’s work,” she added.

**[**[**How does ransomware work?**](https://www.trendmicro.com/vinfo/mx/security/definition/ransomware)**]**

University officials are not sure about the source, or if it was done by one person, a group, or whether it’s local or international. Previously, the university suffered a data breach but this attack was different because it encrypted the school’s email server. “What we do know is that when we first identified the encryption, we did get a ransom note, so that’s how we knew it was ransomware. And we also knew that it was likely someone external who had planted that ransomware,” Dalgetty said. The university has been working double-time for more than a week trying to address the attack that affected the school’s email, Skype, wireless networks and other services. Meanwhile, users with university-issued computers were advised to keep them shut down while the systems remain under threat.

While Dalgetty claims that the university was able to confirm that the decryption keys work after paying the ransom, the school also acknowledged that ransomware is indeed becoming an increasing problem and that it is “a disturbing global trend of highly sophisticated and malicious malware attacks against organizations, including NASA, law enforcement agencies, and large health care institutions”.

**[**[**Defending against ransomware**](https://www.trendmicro.com/vinfo/mx/security/news/cyber-attacks/ransomware-attack-holds-hollywood-hospital-records-hostage-for-3-6m)**]**

The recent string of ransomware attacks highlights the risk involved in paying the ransom. The FBI has issued an advisory for users and businesses to decide against paying any ransom. “Paying a ransom doesn’t guarantee an organization that it will get its data back—we’ve seen cases where organizations never got a decryption key after having paid the ransom. Paying the ransom not only emboldens current cybercriminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals,” says FBI’s Cyber Division Assistant Director James Trainor.