Read the following articles:

* <http://www.cbc.ca/news/technology/ransomware-europe-russia-ukraine-petya-bitcoin-1.4179683>
* <http://www.cbc.ca/news/canada/toronto/oshawa-hospital-cyberattack-1.4114758>
* <https://www.thestar.com/news/canada/2017/05/13/ontario-health-ministry-on-high-alert-amid-global-cyberattack.html>

**Ransomware Basics**

1. What is a ransomware attack?

Ransomware is a form of [malware](https://www.csoonline.com/article/3295877/malware/what-is-malware-viruses-worms-trojans-and-beyond.html) that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

1. How does ransomware work and what does it affect?

There are several vectors ransomware can take to access a computer. One of the most common delivery systems is [phishing](https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html) spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in [social engineering](https://www.csoonline.com/article/2124681/social-engineering/what-is-social-engineering.html) tools that trick users into allowing administrative access. Some other, more aggressive forms of ransomware, like [Not Petya](https://www.csoonline.com/article/3233210/ransomware/petya-and-notpetya-the-basics.html), exploit security holes to infect computers without needing to trick user

1. How could you be affected by a ransomware attack?

You could be affected by a ransomware attack by having a random email in your inbox or junk or etc. By clicking that email you could get that ransomware inside your computer and a message will pop up on your screen and the message will be along the lines of “this computers files are now encrypted pay \_\_\_\_\_\_\_ amount of bitcoin and you can have your files back.

1. How can you protect yourself against a ransomware attack?

You can protect yourself against a ransomware attack by wiping the computers that were affected of that ransomware attack.

**Canadian Attacks (In The Past)**

1. What was affected in Canada in the articles above?

The cyberattack has paralyzed computers and networks around the world, including the ones that run Britain's hospital network, Germany's national railway and scores of other companies and government agencies worldwide.

1. How badly was Canada affected?

Canada was not affected that bad because the files of that day were the only files that were gone forever but all the other files are safe because of the daily backup that the buildings use on a daily bases.

1. What other countries were affected?

Germany, Britain and some other countries in Europe.

1. Where did the attack come from?

Attacks like this one happen when a type of software seizes control of a computer, encrypting its contents and rendering them inaccessible.

"The vehicle that the malware going from one device to the other is spam. The most common way that they do that is via a link in an email," said Atty Mashatan, a professor at Ryerson University's School of Information Technology Management.

1. Why was the attack started?

Attacks like this one happen when a type of software seizes control of a computer, encrypting its contents and rendering them inaccessible.

"The vehicle that the malware going from one device to the other is spam. The most common way that they do that is via a link in an email," said Atty Mashatan, a professor at Ryerson University's School of Information Technology Management.

"It looks as if it's from someone you know, in your contacts. You click on it, and bingo. The actual malware, the file, is downloaded."

The perpetrators then demand hundreds or thousands of dollars to unlock the victims' computers — essentially holding the documents, photos and other items on the computer for ransom.

"This one wasn't really a targeted attack at all," Mashatan said. "They usually run this campaign and hope to infect as many devices as they can."

1. How was the attacked stopped?

All the computers were wiped of all the files and the virus on that same day that the ransomware attack.

**Canadian Attacks (Present Day)**

1. Google “ransomware attack Canada 2019” and research an attack that occurred in the past two months.
   1. Summarize the attack in a paragraph that describes: who, what, where, when.

ransomware" cyberattack that's hit 150 countries in recent days.

Lakeridge Health — one of Ontario's largest community hospitals — said it appeared the ransomware threatened its computer system, but a spokesman said the facility's system was able to deflect the attack.

"Our antivirus software contained the attack and so while we've had to reset some of our systems we weren't affected in the same way that other places were," said Lloyd Rang.

"Patient care wasn't affected and neither were any medical records or health records breached in any way."

The warning screen from a purported ransomware attack, as captured by a computer user in Taiwan, is seen on laptop in Beijing. The attack locked up computers and held users' files for ransom at a multitude of hospitals, companies and government agencies around the world. (Mark Schiefelbein/Associated Press)

The cyberattack has paralyzed computers and networks around the world, including the ones that run Britain's hospital network, Germany's national railway and scores of other companies and government agencies worldwide.

On Sunday, officials and experts urged organizations and companies to update their operating systems immediately to ensure they aren't vulnerable to a second, more powerful version of the malicious software, dubbed "WannaCry."

Matthew Tait, a cybersecurity expert and founder of U.K.-based Capital Alpha Security, told CBC News Network that "a number of" organizations and individuals in Canada have been affected, but that many of them haven't been forthcoming with that information.

"This is a global attack," Tait said. "This has affected all countries and Canada is no exception there."

A spokesperson for Public Safety Minister Ralph Goodale said the government doesn't comment on specific threats, but that the Canadian Cyber Incident Response Centre is focused on protecting vital systems outside the government, including hospitals.

Meanwhile the Communications Security Establishment, a Canadian intelligence agency, said in a statement Saturday that the federal government's computer networks do not appear to have been affected by the attack.

"The vehicle that the malware going from one device to the other is spam. The most common way that they do that is via a link in an email," said Atty Mashatan, a professor at Ryerson University's School of Information Technology Management.

"It looks as if it's from someone you know, in your contacts. You click on it, and bingo. The actual malware, the file, is downloaded."

The perpetrators then demand hundreds or thousands of dollars to unlock the victims' computers — essentially holding the documents, photos and other items on the computer for ransom.

"This one wasn't really a targeted attack at all," Mashatan said. "They usually run this campaign and hope to infect as many devices as they can."

She said it's important for everyday people to remain vigilant to prevent these attacks from spreading.

People should keep their computers' operating systems up-to-date, she said, because the latest updates often patch up security holes. People should also avoid clicking on suspicious links.