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?
   1. A ransomware attack is a type of malware, in which software enters the computer and holds the files and data of the computer hostage until a ransom is paid for the files. If the fee is not paid in the required time, all the files of the computer become deleted. This kind of attack takes massive advantage of PC vulnerabilities, and acts as a Trojan or worm upon entrance.
2. How does ransomware work and what does it affect?
   1. What the ransomware does is that it takes the computer files and data hostage, and then with the files and data, it declares a sum of money needed to be paid to return the stolen files and data.
3. How could you be affected by a ransomware attack?
   1. I could be affected by a ransomware attack since if an attack does take place, all my student working files will be encrypted, and all my hard work from school will be gone, **gone!**
4. How can you protect yourself against a ransomware attack?
   1. Protecting yourself against a ransomware attack is fairly easy, you must be careful on the links you click on, and make sure the emails you receive are from people you know, and recognize.

**Canadian Attacks (In The Past)**

1. What was affected in Canada in the articles above?
   1. Mainly hospitals in Canada were affected as the result of the ransomware attack. However, hospitals weren’t the only ones affected, businesses and casual family computers were also affected, and in a result tens of thousands of dollars have been lost from all these three sectors.
2. How badly was Canada affected?
   1. According to the Canadian Internet Registration Authority (CIRA), Canada has reported a 40% increase in victims of cyberattacks and malware. It also states on the several attacks on the Hospital in Oshawa suffered a minimal loss of information as the backup provided by the hospital restored the previous information. However, information of worth of one and a half day had been lost, and several machines were shutdown resulting in the risk of many patients. On the national scale, it is said that Canada has up to 600 000 people threatened and possibly vulnerable to future attacks. On the business level, in the past 12 months, 250 to 499 employees were affected further increasing the percentage by 66% of attacks from last year.
3. What other countries were affected?
   1. There were as many as 100 other countries that were also affected including Great Britain, which was forced to close wards and the ER and deny patient entry.
4. Where did the attack come from?
   1. It is believed these attacks came from Russia and were intended attacks towards businesses and the health sector.
5. Why was the attack started?
   1. The attack was started probably by criminals in order to gain large sums of money from each computer affected by taking its files hostage. It is estimated that before all the infected computers’ files are wiped out, one billion dollars US will be exploited by the creators of the malware.
6. How was the attacked stopped?
   1. The attack was stopped when the hospital shutdown it’s system and loaded up the backup it had stored, however in terms of other businesses, they were not as lucky and had lost millions of dollars’ worth of information. This has led to the systematic panic and raised awareness towards the growing malware problem.

**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.
   2. A recent attack hit a dental office in Toronto, Ontario on November the 7th targeting the offices’ files and partially damaging them. The hacker, who maintained communication with the dental office says he demanded 15 Bitcoins ($165 000). It has been determined that the malware used in the attack was the *Ryuk* virus, this same virus has been used in targeting 3 hospitals in Ontario, and other medical facilities in Australia, and Alabama, the malware is used to infiltrate a system and then hide to find vulnerabilities in that system. It is believed that this malware was developed in Russia and can be accessed in the dark web, coming at the cost of $200US with monthly “maintenance costs”. The dentist running the office says he felt like it was a “violation”. This shows us the power of malware today.