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 type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

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

Ransomware is a type of malicious software that blocks a user’s access to a system or data by encrypting it until the victim pays a fee or ransom to the attacker.

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

I could click on a link from a person trying to put ransomware on my computer.

1. How can you protect yourself against a ransomware attack?
2. Ensure your Operating System (OS) is up to date
3. Download up-to-date security programs
4. Make sure all your devices have password protection
5. Create difficult passwords
6. Beware of phishing emails

**Canadian Attacks (In The Past)**

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

Oshawa hospital was hit by a ransomware attack and also many other companies and people.

1. How badly was Canada affected?

It affected lots of people and businesses

1. What other countries were affected?

Over 150 countries were affected.

1. Where did the attack come from?

The attacks origin is unclear but it used leaked NSA code and started in Ukraine and Russia and spread from there.

1. Why was the attack started?

It was probably started so the attackers could make money.

1. How was the attacked stopped?

As the attack spread and people found out about it they stopped clicking the links.

**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.

On May 7th 2019, most of Baltimore's government computer systems were infected with a new and aggressive ransomware variant named RobbinHood. All servers, with the exception of essential services, were taken offline. In a ransom note, hackers demanded 13 bitcoin (roughly $76,280) in exchange for keys to restore access. The note also stated that if the demands were not met within four days, the price would increase and within ten days the city would permanently lose all of the data.

As of May 13, 2019 all systems remained down for city employees. It is estimated that it will take weeks to recover. According to Mayor Jack Young, US Federal Law enforcement continue to investigate the attack.

The attack had a negative impact on the real estate market as property transfers could not be completed until the system was restored on May 20th. However, the restoration of all systems was, as of May 20, 2019, estimated to take weeks more.

Baltimore was susceptible to such an attack due to its IT practices, which included decentralized control of its technology budget and a failure to allocate money its information security manager wanted to fund cyberattack insurance. The attack has been compared to a previous ransomware attack on Atlanta the previous year, and was the second major use of the RobbinHood ransomware on an American city in 2019, as Greenville, North Carolina was also impacted in April.