Answer the following questions.

1. What is a ransomware attack?

A cyber-attack that locks users out of their files, to make money from the hacking.

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

Software that locks up computer files with almost unbreakable encryption, then the user demands a ransom for the release of the files. It can affect everyday life if it hits public places such as: Hospitals, government offices, major multinational corporation, and banks. This is because it effectively shuts down the system that we use at these places, which more likely than not have to be closed down because of these attacks.

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

Oshawa hospital Lakeridge Health, many Canadians and countless Canadian organizations were hit by these attacks. Public Safety Committee had to focus on protecting systems even outside the government from ransomware attacks.

1. How badly was Canada affected?

Only one hospital, some government offices, many organizations, and some Canadians were affected, which is a problem, but in comparison to other countries that were attacked, we were not hit as hard.

1. What other countries were affected?

* Ukraine
* Russia
* U.S.
* Much of Europe

1. Where did the attack come from?

The attacks are thought and look to have come from Ukraine, but the true origination of the attacks is unknown.

1. Why was the attack started?

The attack was to make the hackers money, $300 per computer to unlock the files were demanded, more so in bitcoin to presumably cover their tracks and be untraceable.

1. How was the attacked stopped?

The attack on vital systems was halted because of a safety protocol they put into effect before the attack, where the buildings would disconnect from the internet for a short while, as well as updated operating software and other updated software also protected them. A new patch for the OSs was rolled out to prevent a potential second more harmful attack.

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

We could have our computers stealthily hit by malware, and unknowingly have our files encrypted and held hostage, which would either cost a lot of money to undo, or a lot of time to decrypt, in the chance we know how to do that.

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

This software spreads mainly through spam e-mail links, which is an easy issue to deal with, either;

1) Don’t open spam mail

2) Don’t click links in spam mail.

3) Identify if the e-mail is in fact 100% the correct address it was supposed to come from, then carefully read the e-mail and check for correct information or if it sounds like who it was to come from, check if the link is a trustworthy website, then and only then should you click any inserted link.

It can also be from shady torrenting/pirating websites, so to prevent this,

1. Purchase the actual product
2. If you cannot purchase it, don’t torrent or pirate software