**ICS3U1 – Ethics**

**PART 1: Review Ethics - Answer the following questions based on the reading.**

1. What are values?
2. What are ethics?
3. What is hacking?
4. What is piracy?

**PART 2: Piracy – Choose one of the articles and complete the table.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Article Selected**  **(circle choice)** | **Give some examples of Intellectual Property?** | **Why is important or necessary to protect original works or ideas over the Internet?** | **What are consequences of being caught using someone else’s intellectual property?** |
| Know the Do’s and Don’ts of Copyright laws  Software Piracy and the Law  The Risks of Piracy |  |  |  |

**PART 3: Phishing - Choose one of the articles and complete the table.**

|  |  |  |
| --- | --- | --- |
| **Problem Selected**  **(circle your choice)** | **Description of the Problem** | **What signs should you watch out for?** |
| Online Swindlers  Fox News: Phishing Email Scams  Hotel Wi-Fi Scams |  |  |

**PART 4: Viruses – Watch the video “Malware Fundamentals” and answer the following questions.**

1. What is malware?

Malware (malicious software) is a collective terms for threats including viruses, worms, and Trojans. It is designed to be installed as discreetly as possible.

1. Give a short working definition of each of the terms:
   * 1. Computer virus

Designed to infect objects on a disk, and travel automatically between computers. It is oftene triggered by an individuals action, such as clicking on an affected email attachment.

* + 1. Computer worm

Spreads, automatically. Instead of writing its code to multiple objects on a disk, it installs itself once and then looks for another computer to infect. Some worms, such as email worms, require the action of an individual in order to spread. Other worms, such as network worms, spread without the need of human interaction.

* + 1. Trojan horse

Trojans are often downloaded in the expectation that they will perform a useful function. Instead, it carries out a harmful operation on the computer without the victim’s knowledge or consent. Troajsn may be downloaded silently on a computer when the victim is visiting a webpage that is compromised and contains malicious code. The code runs automatically when the webpage is visited. Troajsn don’t self replicate, but rely on a connectivity provided by the internet.

1. Give some examples of what malware tries to accomplish.

Discovering a victim’s confidential data, including passwords. This information may be used to steal money from a victim’s bank account, or the information can be sold to other criminals. Intellectual property can also be stolen to make money. Malware can also be used to carry out attacks on specific organizations and send thousands of spam emails. Extorting money, which involves decrypting the data with a password, and asking for money to decrypt it. This can occur in the form of an anti virus scam, which makes the victim believe that they do not have adequate protection. They are asked to download and pay for removal of malware that isn’t on their computer. They may see popup windows that indicate the presence of malware.

1. Describe things you can do to secure your computer against attack.

Use antivirus solutions, which search for snippets of code that identify a known virus or Trojan (known as a signature). Using Kaspersky Proactive Technologies, which include heuristic analysis, sandboxing, application whitelisting, and behavioural analysis, protect the user from malware. These technologies can even detect malware without a signature.

**PART 5: Journaling – Answer the following three questions.**

1. How costly is damage done by computer viruses? Search for reports that summarize the impact both in terms on dollar value and the number of people affected. Why do you think good estimates of damage may be so hard to generate?

In the past two years. 16 million US households have had a serious computer virus, 8 million have had spyware problems, and the estimated total cost to households affected by these problems was 4.5 billion dollars. Computer viruses cost businesses 55 billion dollars each year. Accurate estimates of damage may be hard to determine because much of the damage may not be known to be due to malware. As a result, such damage would not be reported and identified as damage done by a virus.

1. If someone is found guilty of writing and spreading computer viruses, what type of punishment do they typically receive? What do you think should be punishment for writing a virus that affects millions of computer users around the world?

Those found guilty of writing and spreading computer viruses typically face imprisonment for up to forty years in some very serious cases, fines, or both. This is generally the case for all forms of cyber crime. I believe that long term imprisonment is an ineffective method to turn criminals into responsible citizens. I believe that a suitable punishment for a criminal who is responsible for a virus that affects millions of computer users would be for them to pay fines to compensate for as much of the damage as possible, and/or to be given a mandatory sentence to community/public service. For example, they could volunteer in a Community Supported Agriculture farm (CSA) or in the army for peacekeeping purposes. This would be more likely to instil a sense of civil responsibility and belonging within a community.

1. Do some research into the distinction between white-hat and black-hat hackers. What activities are clearly black-hat activities? Clearly white-hat activities? What activities fall into a gray area? How do you feel about these gray-hat activities? Can you come up with a definition of an ethical hacker? Does a career as a white-hat hacker sound attractive to you – why or why not?

Black hat hackers violate computer security for personal gain or simply for maliciousness. They are criminals performing illegal activities that cause harm. This could include using a botnet to perform DDOS attacks against certain websites, or to steal confidential information from an individual to use against them in any way. White hackers use their hacking abilities for legal purposes that do not cause harm. For example, a white hacker may be authorized by an organization to compromise their systems, so that they may tell the organization about it. This allows the organization to improve their defences against black hat hackers. Some activities fall somewhere in between the black and white hat areas. For example, if someone compromises a computer system without permission and inform the organization about the problem they found. They did not ask for permission, which can be seen as unethical, but they informed the organization so that they may improve their systems.

I feel like gray hat activities are still irresponsible and unethical because they can result in misinterpretations of the hacker’s intentions and potentially cause some harm. An ethical hacker would be anyone who hacks for purposes that do not cause any harm at all. They may be the typically white hacker who uses their skill to inform organizations and developer about a problem with their software systems, or even someone who hacks without permission just for fun, but does not take advantage of other’s information or cause any trouble.

I love solving challenging problems, whether it be in math class, physics, or breaking into someone’s WIFI (yes, I do that sort of thing sometimes). In that respect, a career of hacking without the risk of punishment is an attractive and exciting options for me, even though I am not the best with computer programming.