



**BRNO UNIVERSITY OF TECHNOLOGY**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

**FACULTY OF ELECTRICAL ENGINEERING  
AND COMMUNICATION**

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

**DEPARTMENT OF FOREIGN LANGUAGES**

ÚSTAV JAZYKŮ

**CYBERCRIME: CONCEPT,  
DETECTION AND PREVENTION**

KYBERKRIMINALITA: KONCEPCE, ODHALOVÁNÍ A PREVENCE

**BACHELOR'S THESIS**

BAKALÁŘSKÁ PRÁCE

**AUTHOR**

AUTOR PRÁCE

**David Tureček**

**SUPERVISOR**

VEDOUČÍ PRÁCE

**Mgr. Ing. Eva Ellederová**

**BRNO 2019**



# Bakalářská práce

bakalářský studijní obor **Angličtina v elektrotechnice a informatice**  
Ústav jazyků

**Student:** David Tureček

**ID:** 185919

**Ročník:** 3

**Akademický rok:** 2018/19

## NÁZEV TÉMATU:

### **Kyberkriminalita: koncepce, odhalování a prevence**

#### **POKYNY PRO VYPRACOVÁNÍ:**

Vymezte koncepci kriminality, její historický vývoj a charakterizujte její typy a aktéry. Na základě rešerše literatury analyzujte různé způsoby odhalování kyberkriminality a diskutujte nejefektivnější opatření zaměřená na její prevenci.

#### **DOPORUČENÁ LITERATURA:**

- 1) Clough, J. (2010). Principles of cybercrime. Cambridge: Cambridge University Press.
- 2) Chawki, M. et al. (2015). Cybercrime, digital forensics and jurisdiction. Berlin: Springer.
- 3) Geers, K. (2011). Strategic cyber security. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.
- 4) House, N. (2017). The complete cyber security course. Volume 1. London: StationX Ltd.
- 5) McQuade, III, S. C. (Ed.). (2009). Encyclopedia of cybercrime. Westport: Greenwood Publishing Group, Inc.

**Termín zadání:** 4.2.2019

**Termín odevzdání:** 28.5.2019

**Vedoucí práce:** Mgr. Ing. Eva Ellederová

**Konzultant:**

**doc. PhDr. Milena Krhutová, Ph.D.**

*předseda oborové rady*

#### **UPOZORNĚNÍ:**

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

## **Abstract**

This bachelor thesis deals with the concept of cybercrime. It begins with a description of the historical development of cybercrime and computer technology relating thereto. Then it continues with giving reasons for cybercrime and describes cybercrime from a more practical point of view while analysing various cyber threats and attackers, including illustrative examples. The theoretical part concludes with a chapter concerning the prevention and detection of cyber threats. The purpose of the practical part is to demonstrate the impact of a simple Denial of Service attack.

## **Key Words**

cybercrime, cyber threats, virus, malware, Internet, Deep Web, antivirus, Denial of Service

## **Abstrakt**

Tato bakalářská práce se zabývá koncepcí kybernetické kriminality. Začíná popisem historického vývoje kybernetické kriminality a s ní související počítačové technologie. Práce dále uvádí důvody, proč ke kybernetické kriminalitě dochází, a popisuje kybernetickou kriminalitu z praktičtějšího hlediska, přičemž analyzuje různé typy útoků a útočníků včetně názorných příkladů. Teoretická část práce je zakončena kapitolou věnující se prevenci a detekci kybernetických hrozeb. Účelem praktické části je ukázka jednoduchého Denial of Service útoku.

## **Klíčová slova**

kybernetická kriminalita, kybernetické hrozby, virus, malware, internet, Deep Web, antivirus, Denial of Service

Tureček, D. (2019). *Cybercrime: Concept, detection and prevention*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. 2019. 50 s.  
Vedoucí bakalářské práce: Mgr. Ing. Eva Ellederová.

## Prohlášení

Prohlašuji, že bakalářskou práci na téma *Cybercrime: Concept, detection and prevention* jsem vypracoval samostatně pod vedením vedoucí bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne .....

.....

David Tureček

## **Poděkování**

Tímto bych chtěl poděkovat vedoucí mé bakalářské práce, Mgr. Ing. Evě Ellederové, za božskou trpělivost a cenné rady, které mi v psaní téhle práce nesmírně pomohly.

# TABLE OF CONTENTS

## THEORETICAL PART

<b>1</b>	<b>INTRODUCTION</b>	<b>9</b>
<b>2</b>	<b>HISTORY</b>	<b>11</b>
2.1	Early history	11
2.2	1960s and 1970s	12
2.2.1	Misuse of phones and computer sabotage	12
2.3	1980s	13
2.3.1	Arrest of Captain Zap and the hacking of Kevin Mitnick	14
2.3.2	The first worm hits the Internet	15
<b>3</b>	<b>CONCEPT OF CYBERCRIME</b>	<b>17</b>
3.1	Malware	17
3.1.1	Worms and viruses	18
3.1.2	Ransomware	19
3.2	Phishing	21
<b>4</b>	<b>REASONS FOR COMITTING CYBERCRIME</b>	<b>24</b>
<b>5</b>	<b>CYBERCRIME IN PRACTICE</b>	<b>28</b>
5.1	Deep Web and the Darknet	28
5.2	Internet black markets	30
<b>6</b>	<b>MEASURES TO PREVENT A CYBER ATTACK</b>	<b>32</b>
6.1	Password protection	32
6.2	Safe internet browsing	34
6.3	Antivirus and firewall	35
6.4	Corporate protection	36

## **PRACTICAL PART**

<b>7</b>	<b>DENIAL OF SERVICE</b>	<b>37</b>
<b>7.1</b>	<b>Simulation of a DoS attack</b>	<b>38</b>
<b>8</b>	<b>CONCLUSION</b>	<b>43</b>
<b>9</b>	<b>LIST OF REFERENCES</b>	<b>44</b>
<b>10</b>	<b>LIST OF FIGURES</b>	<b>50</b>



# 1 INTRODUCTION

With the swift growth and spread of information technology, computer and the Internet have become nearly omnipresent, which lead to the creation of a new platform for potential crime commitment. Cybercrime, or computer crime, can be thought of as a rather new concept of crime. The first occurrence of an offence committed by the misuse of technological advancement that could have been considered cybercrime dates back to the 19<sup>th</sup> century, but cybercrime as we know it now, dates to the 1970s (Fell, 2017). Nowadays, it is a much more serious issue and has a wide variety of forms when compared to even a couple years ago. In order to understand the nuances of cybercrime one should firstly get acquainted with the meaning of crime and cyberspace; from which the expression cybercrime is derived.

Crime, in its purest sense of a word, is an action that is perceived as an offence that is punishable by law. Throughout the ages, what is considered as a crime has always been an ever-changing matter. According to the Council of Europe (2015), it has also always depended on the time period and place, which is crucial when it comes to cybercrime, since for example; many African states have not yet adopted minimal legislation practices to fight cybercrime, even though cybercrime is a wide spread issue in the country.

Lilemose and Kryger (2015) report that cyberspace is a term coined in the late 1960, even though the original meaning of the word has barely anything common with the meaning it has now, cyberspace can be simply understood as an imaginary environment on which computers and the Internet network operate.

Finally, we can define what cybercrime really is: cybercrime, in its earlier years called “computer abuse”, is essentially any criminal activity that has been committed with the use of a computer, or any device that is capable of connection to a network (McQuade III, 2009; Rouse, 2018). This is a very basic definition of what cybercrime encompasses.

The aim of this thesis is to describe the concept of cybercrime including its nuances and to carry out a simulation of a Denial of Service attack. The first chapter of the practical part of this thesis will outline the most important developments that happened throughout the history of cybercrime along with the development of computer technology, which I feel is vital in order to understand the technological context of cybercrime. This chapter will also include examples of one of the most notorious criminals from the historical perspective.

The purpose of the second chapter of this thesis is to provide the comprehensive definition of cybercrime, examine its different types and give reasons why the particular type of cybercrime is as popular and widespread as it is, which will serve as an important base for the following chapter. This chapter will also include examples of how phishing and ransomware may look like in real life as well as practical tips on how one should defend against such threats.

The following, third chapter, will explain why cybercrime is so popular. This chapter will consider the victims of cybercrime, showing that they are not only larger corporations, but also smaller businesses suffering from great losses due to their negligence. At the end of the chapter, a reader can find an illustrative example of how a cybercrime attack might look like.

Next chapter concerns the practical side of cybercrime, describing how exactly is it possible for average people to buy illegal goods through the Internet black markets.

At the end of the theoretical part, I will discuss the most effective measures of preventing cybercrime that the average users should undergo and the precautionary measures that companies should take in order to avoid becoming a victim of cybercrime. This chapter will also focus on what companies and average users usually overlook and underestimate.

Finally, the practical part of this thesis shows a simple example of a Denial of Service attack, using two computers and a router. The purpose of this example is to demonstrate the impact of such attack.

# **Theoretical part**

## **2 HISTORY**

This chapter deals with the history of cybercrime including examples added for greater understanding of the matter. The history of this topic is very rich and to provide a detailed survey would extend the scope of this thesis, therefore the following text will outline the most important events in the historical development of cybercrime.

### **2.1 Early history**

The history of cybercrime begins in 1878, with a group of teenage boys, working for the first telephone company. At that time, in order to establish a phone connection between the callers, the operators working at the phone company, had to connect them manually. Even though the work was simple, it needed someone that would have a lot of energy and dexterity to quickly connect callers together, that is why they hired mainly teenage boys. This idea proved ineffective soon after, since the teenagers, working as operators, were more interested in hacking the system, finding out how it works, rather than to actually do their job. This resulted in them messing with the callers, disconnecting their calls and connecting complete strangers together. In contrast to actual modern cybercrime, this was just a petty crime that did virtually no harm to anybody (Garber, 2014).

From the historical background of computers, it is necessary to realize that the computers as we know now are a relatively new invention because when cybercrime was still in its infancy, personal computers were non-existent, instead, there were mainframe computers, first invented during the 1940s and 1950s (Murdock, n.d.). A few years later, mainframe computers were only at larger institutions and were beginning to be put into several universities (McQuade III, 2009). The Internet was also nowhere near as ubiquitous. The basis for the Internet, the Arpanet, was put into use in 1969, with the focus to send scientific research data among selected universities, by connecting the universities' mainframe computers together. The data were sent through the network in small units called packets, which is the same way it works now (Rouse, 2017; McQuade III, 2009). In the 1950s and 60s, technology enthusiasts at the MIT laid the foundation to what is now being called a "hacker". Brunvand (1996) points out that sharp students of the MIT were naturally drawn

to explore and fiddle with the phone switching network and eventually the computers at the MIT Artificial Intelligence Lab.

## **2.2 1960s and 1970s**

At the beginning of the 1970s, computers and the Internet were starting to become progressively mainstream. This was the time when investigators began to examine the concept of cybercrime, or computer crime, since this time marks the first occurrences of computer sabotage, manipulation and espionage (Clough, 2010; McQuade III, 2009). These early computer crimes frequently involved actual physical damage to the hardware itself as distinct from long-distance manipulation of today. Among the more notable examples are student riots in Canada which happened in 1969. Kabay (2008) reports that the riots culminated into a fire which broke out on the grounds of the Hall Building, which led to destruction of computer data and university property, totalling \$2 million. Another example of a physical attack on a computer can be found in 1970, where a bomb, which was planted in Sterling Hall, on University of Wisconsin campus, resulted in devastating \$16 million worth of data.

### **2.2.1 Misuse of phones and computer sabotage**

Computer crime was starting to get a more serious treatment throughout the 1960s, although many crimes still only consisted of theft, sabotage or fraudulent transfer of electronic funds, due to the still limited availability of computers in everyday life, as Clough (2010) points out. Cybercrime has never been strictly tied to the use of computers. The late 1960s also mark the rise of so-called “phone phreaking”, which is a slang term for the exploitation of phone systems i.e. the criminal can gain access to a phone system and exploit it in order to gain access to international calls or voicemail. In practice, when a phreaker uses one of the phone system’s services, it is run through a multiple of phreaked phone lines, thus making them very hard to trace and consequently costing the actual owner of the phone system a lot of money (Foresee, n.d.). Kovalchik (2008) gives a notorious example of phone phreaking that occurred, when a US Air Force soldier and a computer programmer, John Draper, also known as Captain Crunch, was able to make free phone calls by using a toy whistle from a cereal. The whistle emitted a sound at a frequency of 2600 Hz, which is the same frequency

the AT&T phone company used for communication among its switches. Once the telephone heard the sound emitted from the whistle, the telephone considered Draper's call to be from an official operator, meaning that his call became free of charge.

As the time passed, more cases of computer crimes started to occur. Kabay (2008) describes the 1970s story of Albert the Saboteur whose infamous name is associated with an interesting case of computer sabotage. The National Farmers Union Service Corporation of Denver suffered \$2 million worth of damage throughout 1970–1972 due to fifty-six disk crashes. Experts thought the crashes were happening due to power fluctuations, but were eventually proven wrong, after installing surveillance cameras, which caught Albert, a night shift operator, sticking his car key into the computer. He had been doing this repeatedly over two years.

Another computer-related criminal from the 1970s, Jerry Neal Schneider, was responsible for a prime example of an impersonation computer crime. Jerry was a social engineer and a security consultant who obtained parts by scavenging from Pacific Telephone and Telegraph's (hereinafter referred to as PTT) dumpsters. During this scavenging, he built up a collection of PTT documents including invoices and training manuals. After a few years, he reportedly knew more about PTT's procedures than its own employees. By collecting valuable information from the invoices and manuals, Jerry was able to impersonate the company staff and gained vital information about ordering procedures. He then proceeded to abuse such information to order various equipment that he then proceeded to steal from the company's usual drop-off point. Jerry went as far as to have its own warehouse full of stolen equipment. He later became a computer security consultant, after he served his inevitable prison sentence (Becker, 1980; Kabay, 2008).

### **2.3 1980s**

As the years went by, it was only natural to see the popularity of computers and the Internet to grow exponentially. Obviously, this fast growth was followed by many more cases of computer abuse, which finally forced the state and federal government to build the first legislative pillars by passing the first laws against computer crime.

In 1984, Ronald Reagan signed into law the first revision of the U.S. criminal code, extending the jurisdiction of the United State Secret Service over credit card fraud and

computer fraud. This action is then followed in 1986, when the congress passed the Computer Fraud and Abuse act, which officially makes it a crime to break into computer systems (Focus Training, 2016; Comprehensive Crime Control Act of 1984, n.d.).

### **2.3.1 Arrest of Captain Zap and the hacking of Kevin Mitnick**

In 1980, Ian Murphy, also known as Captain Zap, hacked into AT&T computers with the help of his accomplices. By hacking into the computers, Murphy was able to change the internal clock of the computers, which activated late-night discounts for people who were using phones in the afternoon, and conversely deactivated the late-night discount for people who were making phone calls at night. Due to these actions, Murphy underwent a trial and was historically the first person to be convicted for hacking (Murphy, 2011).

Kevin Mitnick is a very controversial, and arguably the most important figure from the history of computer crime. Before even reaching the age of eighteen, Mitnick had already had some experience with being a cybercriminal by phone phreaking and breaking into computer networks (Greene, 2003). A major company dealing in computer industry, Digital Equipment Corporation, became a victim of Mitnick's hacking because a group of hackers that he had been in contact with challenged him into hacking one of the company's computers. He accomplished this task using social engineering. Disguised as Anton Chernoff, Mitnick simply called the company's system manager with the problem that he could not log into the system. Mitnick was convincing enough for the system manager to just let him choose new login and a password, and then proceeded to steal the source code of the VAX VMS operating system. Mitnick's actions landed him into prison for one year, with three years of supervised release, although this sentence did not put a stop to his actions (Kevin Mitnick, n.d.). Mitnick continued with hacking, which lead to him being persecuted by the FBI, making him the first hacker to have his face on an FBI "Most Wanted" poster (Delio, 2001). Mitnick was persecuted for two years, but he made a mistake of leaving an insulting message on one of the computers and a voice-email, which belonged to an Internet security expert, who ended up helping the law enforcement. Mitnick was then imprisoned again, in 1995. In 1999, he was convicted in the federal court and sentenced to nearly four years in prison for several counts of wire and computer fraud, although was released in 2000 under a three-year parole, which restricted his access to computers (Kabay, 2008).

At present, Mitnick runs the security firm Mitnick Security Consulting, LLC which helps test companies' security strengths, weaknesses and potential loopholes. He is also a global bestselling author of books *Art of Intrusion: The Real Story Behind the Exploits of Hackers, Intruders and Deceivers* and *Art of Deception: Controlling the Human Element of Security* (Mitnick Security Consulting LLC, 2019).

### **2.3.2 The first worm hits the Internet**

The Morris Worm is talked about as the first malware that tried to take over the Internet. It was created by Robert Tappan Morris, and was released on the Internet on November 2, 1988. It is estimated that the worm affected 5% of all computers through the Internet. It should be noted that at that time, Internet was nowhere near as widespread as it is now, so 5%, while a big number, it is still not as tragic in comparison to today's standards. The worm also affected only computers running on the UNIX operating system.

Computers affected by this worm got often extremely slow, and the worm was also able to cause power outages. It spread itself onto other computers by cloning itself and sending itself through Sendmail, an email transfer agent through which it is possible to send and receive email, the worm misused this feature and continued to spread itself, which resulted into the creator of the Worm, Mr. Morris, being arrested for five years, and fined \$250,000. The Morris Worm helped the creation of CERT Coordination Centre, which was designed to fight with threats to the Internet. The worm generally served as a wake-up call for things to come, and a realization that Internet security should not be taken lightly (Morris Worm, n.d.).

With the emergence of the World Wide Web, computer abuse of the past years evolved into cybercrime like we know it now. Nowadays, computers networks talked about in the historical books have transformed into what we currently call information systems, with larger corporations often creating their own information systems, which are then connected to the Internet. The development of technology has been very rapid in the past few decades and there are very few signs of it slowing down. It is also necessary to understand that in the past, the count of potential victims of cybercrime was in thousands, but now is in billions (McQuade III, 2009; Clough, 2010).

Aimoto et al. (2018) inform that in 2017, there were more than 1 billion web requests analysed by Symantec, which equals to a 5 % rise from 2016, but the more important statistic is that one in 13 these web requests led to malware, a 3% increase from 2016. Another example are attacks on mobile phones, which have increased by 54% with over ten thousand new variants of malware, compared to just last year. There has also been an increase in ransomware, a type of an attack which blocks the user's computer, the computer will stay locked if the user does not proceed to send a certain amount of money to the hacker's address. Since 2016, there have been 46% new ransomware variants, with hacker asking for more money on yearly basis. And finally, an increase in overall vulnerabilities has recorded a 13% increase, compared to 2016. From the information stated above, we can clearly tell that cybercrime has been on the rise on yearly basis.



### **3 CONCEPT OF CYBERCRIME**

To conceptualize cybercrime as a whole is a rather difficult task, since it is a very broad topic. The simplest definition of cybercrime can be understood as any crime committed via any device, either against a person, person's information or other device. This chapter entails the most known types of cybercrime, with a specific aim on crimes that can be encountered rather commonly in everyday use of the computer and the Internet.

Although the most frequently encountered cybercriminal activities usually only harm the victim's user experience of the computer, or the hardware itself, it is still necessary to understand that there exist some rather extreme cases, that go beyond impairing the user's experience and are still classified as a cybercrime to a degree. One of these cases being child pornography. Nowadays, as Clough (2010) points out, the production process of child pornography has been greatly sped up by the new technology and what is even worse, the Internet has allowed such people to distribute the material very easily. Criminals who want to view such materials can connect with other criminals through various forums or imageboards<sup>1</sup>, or the directly purchased from somebody via the Internet's black market. The other case which people usually not link together with cybercrime is the enticing of hate and terrorism. The United Nations Office on Drugs and Crime (2012) reports that the Internet is often used in order to promote and incite terrorism by the means of spreading hateful propaganda, recruiting (especially vulnerable minors) and by using the Internet as a financing or a training tool.

#### **3.1 Malware**

Malware is a common term used when describing a software that was designed with the malicious intent of harming either the computer's system, network or the user's data, hence the name malware; a portmanteau of "malicious" and "software". There exist many different types of malware, some of which work in conjunction with social engineering, with the purpose of not only destroying the user's data but also stealing them.

---

<sup>1</sup> Imageboards are a type of Internet forums where the users communicate with each other mostly by posting images, with the ability to also use text-only posts. Imageboards do not require the users to register or give any information about themselves, therefore the posting is done anonymously. This has led many criminals to use such sites to not only look for child pornography, but to also distribute it. The most notorious imageboard nowadays being 4chan.org.

Many users become affected by malware while browsing various websites or downloading software. A regular visitor of the Internet is affected by simply not paying enough attention to the sites they visit, hastily downloading software, or viewing random emails, without doing any research or paying much attention. Once the computer gets infected, the malware can either reside in the user's computer unnoticed, and proceed to continually collect data, or it can make the user's experience of the computer very unpleasant. The way the malicious software behaves depends on its type.

The term "malware" is also very often misinterpreted for a specific kind of malware, which is the virus or the worm.

### **3.1.1 Worms and viruses**

Nearly every computer user is familiar with the term computer worm or computer virus, but very few actually know how viruses and worms operate, or how dangerous they really are.

Experts from the cyber security field at Symantec (n.d.) describe the computer worm as a self-replicating software that can replicate itself without any human interaction and consequently causes harm. As mentioned in the previous chapter, the computer worm, sometimes also called a network worm, not only replicates itself on the user's computer, causing major slowdowns, but can also spread throughout the entire computer network. By exploiting security deficiencies in the computer's system, a worm can harm the computer by corrupting user's files, slowing down the computer's network or attaching itself to an email client and continue to spread itself into others. One of the more unpleasant actions the worm can commit is to create a backdoor for the worm's creator. Your computer then becomes what is called a zombie, allowing the creator of the worm to access your computer freely. Worms are arguably more dangerous than viruses since they are completely autonomous and can attach themselves to parts of the operating system which the average user cannot usually reach or even see, but often just keep on spreading throughout the network (Computer Worm, n.d.).

Viruses are very similar to worms in that they also possess the ability to replicate themselves, but they require the user's input to get into the system, since they usually attach to other programs (Symantec, n.d.). Oh (2015) informs that an example of how one can get infected by a virus is by downloading software through the Internet, from suspiciously looking

websites. In my personal experience, I have been affected by many viruses when using the computer as a teenager, most often by illegally downloading videogames from the Internet. While illegally downloading any software from the Internet, it is very likely for the average user to not only get the desired software, but also a virus. By installing the downloaded software, the virus will usually install along the downloaded software completely unnoticeably, infecting user's computer. Mitra (2017) analyses many different damages that viruses can cause, such as corrupting hard disks, deleting files on the computer, noticeably degrading computer performance or displaying unwanted messages. One of the more devastating viruses is the Boot Sector Virus, which the security experts at Kaspersky (n.d.) describe as a virus which can infect the boot code<sup>2</sup>. This action may result in the inability to start the system since the virus will be executed before Windows can boot.

### **3.1.2 Ransomware**

Ransomware is a malicious software which encrypts your files, making them completely inaccessible – at least until the victim of the attack decides to pay the ransom, in order to get access to the files (Symantec, n.d.).

Users are usually affected by ransomware through downloading unknown attachments from seemingly harmless emails, or by simply browsing the web. While browsing the web, the user's computer connects to many various sites in order to, for example, show the video content of the site, bring up a pop-up window, or display advertisements. Torres (2018) observes that cybercriminals have unfortunately taken advantage of the Internet advertisements, where a user can get infected by clicking on a malicious advertisement, or by doing virtually nothing, since such advertisements can run the malicious code by just simply being present on a website which hosts said these advertisements. This phenomenon is aptly named Malvertising.

When users get infected, they are not able to access their files and most often than not, they will have to pay the ransom within a certain period of time. The clever thing about ransoms is that the cybercriminals behind the software usually do not demand unrealistic or very high amounts of money. In 2017, more than 200,000 computers around the world were attacked by a ransomware called WannaCry. If a user was affected, they had to pay

---

<sup>2</sup> The boot code is an instruction set which the computer follows in order to start the computer system properly (Computer Hope, 2017).

around \$300 in Bitcoin. They had to pay the sum within three days, otherwise all their files were deleted. The fact that the ransom is only a few hundred dollars may force companies or even families to pay the price instead of risking loss of all their files (WannaCry, n.d.).

Even though the outcomes can be very devastating, as in the case of any other cyberattack, protecting against ransomware is rather easy. Good antivirus software, which should be an essential part of everybody's computer, will do most of the work; however, from the user's side, prevention should be thought of as well. An important measure that many users do not take is to regularly backup their sensitive files and documents, either to the cloud, or to an external disk. In case of a ransomware attack, the users have all their data safely stored in a safer place and can recover them easily.

Ransomware can also be combined with phishing by which I was personally affected while writing this thesis. While searching for a practical example of a ransomware attack, I have stumbled upon an email in my personal spam folder, titled with my email address and a password I have not used since 2008. The email started with: "Let's get straight to point. None has compensated me to investigate about you. You may not know me and you're most likely wondering why you're getting this e mail?". While reading this, the average user can get tense since it does not look like it was written by a computer, but an actual criminal. The email then continued that he had installed malware on a website I had registered at. The malware then got into my computer, which started working as a "Remote control Desktop with a keylogger which provided me with accessibility to your display screen as well as webcam". The attacker's software then apparently recorded a "sensitive video" of my person. The program also gathered all the contacts from my email and Facebook. The attacker presented me with two choices: I can either ignore his email, which will cause him to release the footage, or I can pay him \$977, to which he will respond by deleting the footage. At the end, he informed me that resistance would be futile and informing the law enforcement officials would be pointless, since he could not be tracked. Also, there was the possibility to ask for a proof, by replying to his email with a specific message: "Yea!". He would then send me and other 15 people from my contact list an excerpt from the video. However, he then follows this statement with "please do not waste my and your time by responding to this email message".

By quickly reading through this mail, one can get the impression that this is a huge problem and if the addressee does not pay, he would get in trouble. However, there are many hints throughout the email which can be followed to recognize it as a prime example of a typical

phishing scam. First of all, the information which scares many people most, is how the attacker knows the person's password? In fact, it is very easy to get a random person's email address and a password. Many websites have been hacked and many contact details of random people have leaked out, therefore the attacker can easily browse through thousands of contact details and randomly choose his victim. The other determining factor in this email is the complete lack of personalisation. Even though it states that he has access to all my contacts and even to my Facebook, he should also have access to my name, my location, my phone number, but all of this is missing from the email. Last but not least, a simple google search for this similar kind of email shows that there are many such emails that are alike, with only slight changes.

### **3.2 Phishing**

Needless to say, the average computer user, not even the most curious one, would not just download an unknown attachment from a suspiciously looking email, that came from an email address that the user does not know. Cybercriminals know that obtaining somebody's data is not easy, however, one of the more frequent cyber-attacks almost every Internet user has experienced takes place in a similar way and it is called "phishing".

It might be assumed that cyber criminals are not foolish, and they realize the fact that people have been taught not to download or open unknown email attachments, just as they were taught not to enter unfamiliar cars with strangers in them.

During a phishing attack, the attacker is trying to catch a gullible, or uninformed user through an email, serving as a "bait" that is sent to the user's address. The emails sent from the attacker are often masterfully disguised as an email from an insurance company or a bank, the email body usually having the same design as the official email from a bank with the address that the mail was sent from, often being almost identical to the official bank's email address. "Almost" is the crucial word since the email is not the deciding factor whether the email sent from a bank is legitimate or not. Fortunately for the average users, a lot of phishing emails are trying to be too advanced with attackers trying to personalize the email to, for example, the addressee's country. This, unfortunately for the attackers, commonly results in a very credibly looking email written in an incorrect Czech language, which even the most gullible person would not trust. Another typical example is an email containing the message that the user's yet unknown uncle has died in Switzerland, therefore it is important for the

user to tell the sender his contact details or even provide his credit card information so that several thousand euros could be sent to him as a part of uncle's heritage. In theory, it might seem completely crazy, though in reality cyber criminals would not tirelessly send similar emails if the success rate was zero percent. In general, it seems ludicrous that phishing still works nowadays when everybody knows that banks or any other services will never ask for a user's password, and that getting several thousand euros without any effort sounds too good to be true. Again, this is happening because it works, and it works because not everybody is as sharp and as careful as they should be while using the Internet.

Thankfully, protecting against these cyberattacks is just a matter of understanding and awareness and there are a few rules everybody can follow in order not to be affected by a phishing attempt, as CShub (2018) reports. Phishing emails themselves are not harmful, harmful are the actions of the addressee, therefore it is advised not to click on any suspicious buttons or hyperlinks<sup>3</sup>. Various buttons and links which can be interacted with usually lead to a completely different web site from what it may seem at first sight. The user can simply check where a button or a text link leads by hovering the cursor over it, displaying the path to which this hyperlink or a button will lead to after clicking on it. Phishing emails also try to convey urgent messages, forcing the victim to act recklessly without paying any deeper attention to the content itself. It can either be a proposal to withdraw a prize within a limited time or a warning that the user's bank account will get closed if his contact details will not be provided in time (Cyber security hub, 2018). Erb (2018) warns that during the tax season in the United States, it is especially popular for the attackers to make their phishing attempts look like they were sent from the Internal Revenue Service, taking advantage of taxpayers. The Internal Revenue Service had to issue a public warning, since phishing attempts became more rampant (IRS, n.d.). Lastly, an officially looking email with severe spelling mistakes, or a blank email with just a file attached poses an obvious threat and should be discarded immediately.

One of the more recent examples of a successful phishing attempt happened at the end of 2018. Uconn Health, a branch of the University of Connecticut responsible for clinical care, was recently affected by a successful phishing attempt which resulted into exposing its patients' data, threatening 326,000 individuals, as Matthews (2019) reports. In the official statements from Uconn (n.d.), it is stated that the attacker got access to Social Security

---

<sup>3</sup> An interactable part of a text which will forward the user to another document or website.

numbers, of which 1,550 could have been exposed, names, billing details and medical appointments.

Apart from the attacks mentioned above, there exist many more different types. The practical part of this thesis focuses on a Denial of Service attack, known mostly as DoS.

## 4 REASONS FOR COMMITTING CYBERCRIME

According to Clough (2010), there are three factors which determine the likelihood of crime happening, the first one being a count of motivated offenders. Needless to say, the Internet is used on daily basis by many people across the entire globe; in fact, the total count of Internet users is over 4 billion, with 49% of users being in Asia (Miniwatts Marketing Group, n.d.). Hypothetically, there is a possibility for one user out of all four billion users to commit a crime that will affect the other four billion users. This is a huge pool for criminals, a pool of potential offenders and victims that has never been seen, especially when we take into account the availability of fitting possibilities to commit the crime, which is the second factor according to Clough's (2010) theory on why crime happens. It is only natural to assume that crime has always been a local matter. If one is to commit a crime in the Czech Republic, the crime will fall under the Czech jurisdiction and will be dealt with accordingly. Since the arrival of the computer and the Internet, people have an opportunity not only to connect and communicate with others all around the world, but also to harm them. The European Commission (2012) affirms this by stating that cybercrime is regarded as a low risk – high reward activity with no natural or set borders. Finally, Clough (2010) identifies the factor which describes the reason why cybercrime is such a widespread issue, which is the shortage of competent ways of protection.

It is only natural to assume that cybercrime would be very popular, since it is regarded as a highly profitable activity with virtually no risk when compared to other types of crimes, considering that for example thousands of Americans are being hit with cyber-attacks every year, yet a very small percentage of these attacks gets reported and when they do, the local police can do very little about it, since they are ill-equipped and even though the FBI has the ability to help, it simply cannot afford to deal with smaller crimes (Grimes, 2012; Johnson, 2018). To put things into perspective, we can examine and compare a traditional crime versus a cybercrime. The FBI's Bank Crime Statistics (2011a) from 2010 reveal that there have been slightly over five thousand bank robberies which in total, caused the damage of \$43 million, with slightly over \$8 million recovered. The statistics further show that during the robberies, 106 people were injured and 16 were killed, since the robbers used firearms in more than thousand cases and threatened with one in almost half of the cases. If we take a look at the statistics from the same year, but from the perspective of cybercrime, we can clearly see a huge difference between these two types of crimes. The FBI (2011b) reports that in the same year, more than three hundred and thousand people were affected by



cybercrime, resulting in the loss of \$1.1 billion. Bill Hinerman (FBI, 2011b) remarks that “anybody and everybody can potentially become a victim of Internet crime. The most heart-breaking aspect is, we practically can never get the victims’ money back”.

In reality, it is not very easy to be completely secure if a company or an individual does not put enough time and effort into securing themselves. Unfortunately, many individuals and companies, especially smaller businesses, do not protect themselves due to either lack of knowledge, resources, or thinking that by virtue of their smaller size, they would seem like an insignificant target compared to other, larger companies and businesses. This has proven to be a huge misconception (Amerding, 2015). There is no doubt that hackers are committing cyberattacks just to prove something to themselves by trying to breach into larger corporations; however, the majority of attacks are against smaller businesses. The Small Business Committee (2015) reports, that in reality, 71 % of cyber-attacks are aimed at businesses with fewer than 100 employees. This proves that most hackers do not consider hacking as a mere recreational activity or competition amongst their peers as they did in the past, but they hack with the intention of stealing contact information, credit and bank account data and many other forms of intellectual property for the purpose of financial gain. McCracken, President of the National Small Business Association commented on this issue by explaining that: “Many small companies are not in a position to have a dedicated IT department, and many either outsource IT functions or assign such duties to an employee with other responsibilities—often the owner him/herself” (Small Business Committee, 2015). Unfortunately, two years later, things do not seem to look any better for smaller businesses. Ponemon Institute LLC (2017) shows that out of all represented companies in the study, 51 % have experienced either a successful or unsuccessful cyber-attack and what is even more disturbing, only 21 % of companies claim that their ability to defend against cybercrime is very effective, which overall results into a 6 % increase in cyberattacks and 4 % increase in data breach compared to the last year, with phishing or social engineering being the most common type of an attack. It does not mean there are not enough effective tools for an individual or a company to protect themselves; this issue was only widely present in history as outlined in the first chapter. As a matter of fact, there currently exist highly advanced tools that can protect against the vast majority threats, and even predict certain devastating types of attacks almost two years in advance, through the help of machine

learning and AI<sup>4</sup>. The main problem is simply the lack of knowledge and caution when handling sensitive data as the above-mentioned statistics about the most common type of an attack suggest.

There are many tools that can be used by individuals and companies in order to protect themselves as much as possible, but on the other hand, there are effective tools that hackers can also use to keep themselves safe and, above all, anonymous and private. The difference between being anonymous and private on the web, is that when a user is anonymous, nobody can know who the user is, but can they see what the user does. When a user is private, no one can tell what they do on the web, but they can reveal the user's identity. Anonymity plays an essential role in cyberspace and is arguably the most effective weapon in cybercriminal's hand. Hypothetically, the notion of being anonymous on the Internet might sound tremendous, but users must actively try to stay anonymous. If average users use the Internet without any protection and tools that make them anonymous, and search for things they are interested in with the help of Google through a regular web browser, it is safe to say that each of the users' steps are being tracked and monitored. The information gained is then used for personalized advertisements, personalized search, and probably many other things that the average users would not like if they found out. It is then only natural that you want your own privacy when browsing the web, and even though it has been getting progressively harder to stay anonymous and private, it is still possible to a certain degree. The dangers of anonymity and privacy are then obvious, since people can take the advantage of being anonymous and can harm others.

Cybercriminals are often able to hide information about their location and IP<sup>5</sup> address by using many tools, such as Proxy servers and Virtual Private Networks. As an example, a typical cybercrime would look approximately like this: a cybercriminal searches through the Internet for random personal email addresses, they then proceed to send many phishing emails, disguising themselves as a credit card company and if lucky, somebody that is uninformed and gullible enough will give them their credit card information. The criminal does all of this while staying as anonymous and as private as possible. After gaining necessary information, whether the victim's personal or credit card information, the criminal

---

<sup>4</sup> AI stands for Artificial Intelligence. There are two forms of AI, the first being weak AI, which is designed to deal with specific tasks and the other one is strong AI, which is able to solve different tasks on its own by learning and adapting.

<sup>5</sup> IP address is short for Internet Protocol address. IP address serves as a label which automatically assigned by the Internet provider to any device connected to the Internet. (IP address, n.d.)

then can proceed to misuse the information to steal money from the victim or more likely, sell the information locally, or on the Internet. In most cases, selling such sensitive information is not done through a usual bank transfer, since bank transfers are neither anonymous nor private. As a result, the offenders most often sell the obtained information for cryptocurrency<sup>6</sup>. There also exists a “private and anonymous” version of the Internet. Personal or credit card information obviously cannot be easily sold or purchased on the “regular” Internet, since it is regarded as an illegal practice and would be punished almost immediately. More information about where on the Internet most of the crime happens are detailed in the following chapter.

---

<sup>6</sup> Cryptocurrency is a form of virtual currency. Cryptocurrencies can be obtained either by mining (solving complex computational problems) or by buying them on one of many cryptocurrency exchanges. Cryptocurrencies are stored in virtual crypto wallets, each of them having a set address and due to the decentralized aspect of cryptocurrencies, each wallet and transaction can be freely inspected. Most popular cryptocurrencies used by cybercriminals are Bitcoin and Monero, with the latter being completely anonymous (amount of Monero one has in a wallet can, as well as the transactions themselves, cannot be viewed by anybody) (Frankenfield, 2019)

## 5 CYBERCRIME IN PRACTICE

Just as there is Yakuza in Japan, or Triad in China, cybercriminals also have their own groups, organizations, hideouts, platforms and specific practices. This chapter will present a closer look at the practical side of cybercrime, various online black markets, which make it possible for anybody to buy drugs, weapons or personal information.

### 5.1 Deep Web and the Darknet

One might think that the Internet is a large playground where anybody can access everything. This, in theory, is true, although, for the average user, more than 90% of the entire Internet is hidden, and cannot be found or accessed by using any search engine through any of the mainstream web browsers, Mae (2018) remarks. The part of the Internet, which can be accessed by googling something, or typing a specific web address, like <https://www.google.com>, is called the surface web. The other part of the Internet is called the Deep Web. The Deep Web is the rest, i.e. any content that cannot be accessed by a search engine and usually requires to log in or is locked behind a paywall<sup>7</sup>. Schober (2015) implies that one can image the entire Internet as a giant iceberg, with only a little tip being shown above the water, which represents the surface web, with most of the content being submerged under the water; the Deep Web. In practice, the content of the Deep Web can be science journals, which the user has to pay for in order to access them, government databases, videos on subscription based sites or messages on social media – this is the content that cannot be simply accessed by googling, or typing a specific web address. The terminology, however, can be very confusing, since many people mistakenly assume that the Deep Web is something exclusively sinister and illegal while it just characterizes everything which is hidden. The proper terminology for the darker part of the Internet is the Darknet (or Dark Net) (Brightplanet, 2014).

---

<sup>7</sup> Access to the content is restricted, and the user must pay for the content. It is usually a one-time purchase or a reoccurring subscription-based system.

If the small portion above the water, in the iceberg analogy is the surface web, and everything below is the Deep Web, then the part at the very end is the Darknet. The Darknet symbolizes a part of the internet that can be accessible only by using TOR<sup>8</sup>, which is an acronym for the onion router.

When browsing through the web using any of the mainstream web browsers, like Google Chrome or Mozilla Firefox, the process of connection to a site is very simple. A user can type a domain, like *www.google.com* into a browser, the browser will then follow with a *handshake*. During the handshake, the client side, in this case, the user, will send a packet to the server, in this case, google, to ask whether the server is ready for a new connection and if so, the connection will be established, and the client can communicate with the server (Three-way Handshake, n.d.). On the other hand, when using a browser like TOR, the connection process becomes a more complex. Nigam (n.d.) explains that TOR uses the onion routing technology, which is different from how a regular browser handles connecting to a website. When connecting to a website using TOR, the connection between the client and the server is maintained between different nodes, simply put, there exists a middleman in the connection. During a regular connection through Google Chrome, when the user tries to connect to *www.google.com*, the network traffic between the client and the server can be monitored and ultimately traced back to the client's IP address – which then can be used to identify a specific computer. When using TOR, the user's connection is under many layers of encryption and it does not go straight to the server the user is trying to connect. Instead, the connection hops between various servers each of them peeling back the encryption layers just enough, so that the one server would have sufficient information as to where to travel next. Each server would therefore have a key to the specific layer, with the client having keys to each of them. For example, suppose that someone would try network sniffing<sup>9</sup>: At the beginning of the connection, the sniffer would only acquire the address of the first server and an encrypted message. Similarly, at the end of the connection, the sniffer would only be able to see the end server contacting another server without any information about the client himself. This is how TOR browser provides anonymity through the usage of onion routing.

---

<sup>8</sup> TOR is an acronym for the onion router. TOR is a browser which uses the onion routing technology in order to stay private and being able to connect to websites to which a normal browser would not be able to connect (Tor, n.d.).

<sup>9</sup> Network sniffing is a term describing real-time monitoring of packets, flowing through a computer network. It can be done by using specific software, for example, Wireshark (Securebox, n.d.).

## 5.2 Internet black markets

The most infamous place that could be found on the Darknet was a marketplace called Silkroad. Silkroad launched in 2011, with a man named Ross Ulbricht as its creator. In order to access Silkroad, one had to use the TOR browser (Norry, 2018). Babka and Willis (2018) point out that Ross's theory behind Silkroad was to create an entirely free market, where people would be able to buy nearly anything – from drugs, fake IDs to guns. Ross had very libertarian beliefs and by creating Silkroad, he ultimately wanted to let people buy items which were prohibited by the state, completely securely, without the need to negotiate with dangerous gangs in order to buy guns, drugs or get caught by the authorities. Even though Silkroad was a free market, the purpose was to only provide goods without any history of harming anybody, meaning that one should not be able to buy stolen data, credit card info, child pornography, or weapons of mass destructions. Norry (2018) addresses that originally, it was not possible to buy any kind of firearms, this rule was relaxed only due to Ross's belief that the firearm regulations made it increasingly harder for people to have the option to buy a firearm legally – and would rather resort to buy them through a more dangerous way.

Babka and Willis (2018) add that from the user's perspective Silkroad was a very safe site. People had the certainty that everybody would get paid. All the transactions were made through bitcoin, which made it secure, anonymous to a certain degree and ensured that it is impossible to use counterfeit currency and obviously, there were no taxes on any of the goods. Silkroad also had a rating system in its place where people could rate different vendors and quality of their goods.

Norry (2018) remarks that Silkroad ceased to exist in 2013 due to an FBI investigation, and Ross Ulbricht was arrested. It is estimated that over Silkroad's lifetime, more than \$1 billion flowed through the market. Unknowing to Ulbricht, he was communicating with an undercover FBI agent, which helped the FBI to catch him at his house, with his laptop being logged into Silkroad as an administrator. The FBI also found millions of dollars in Bitcoin on his laptop. Ulbricht was sentenced to double life in prison plus forty years, for operating the Silkroad marketplace, Ross was also accused of hiring hitmen, although no evidence exists of murders being carried out (Freeross, n.d.). Even after all these years, there are still people who fight for Ross' freedom, with over 155,000 people having signed an online petition, many believing that the investigations were riddled with corruption, unproven

allegations, evidence tampering and privacy violations against Ross Ulbricht's person (Change, n.d.).

There are several other markets, many of which only stood online for a short period of time, with notable exceptions being AlphaBay and Dream Market. According to Wikipedia (n.d.), after Silkroad, AlphaBay was the most popular darknet marketplace, having over 400,000 users in its prime, but unlike Silkroad, AlphaBay did not have such strict rules, although it worked on the same principle. AlphaBayMarket (n.d.) reports that all the goods could only be purchased via cryptocurrency and one could purchase almost anything; the offer of goods ranged from drugs, unlicensed guns, to stolen credit card information and other financial data. Richard (2017) remarks that AlphaBay was online from 2014 and ceased to exist in 2017, with its creator being arrested and later found dead in his prison cell, after he committed suicide.

Dream Market is currently the longest running Darknet marketplace, running from late 2013 until now. The Dream Market works as the other markets mentioned above, and any goods can only be bought using cryptocurrency. The top selling goods on the Dream Market being drugs (cannabis, ecstasy, stimulants, psychedelics), digital information, but also e-books and various counterfeits. As an example, in February 2019, a hacker called Gnosticplayers posted a batch of stolen data, with previously posting two batches from various data breaches. All in all, Gnosticplayers has been using the Dream Market to sell personal information of 839 million users. The hacker got the data from hacking various websites, like a GIF hosting service GfyCat, real estate site StreetEasy, or mobile payment service Onebip, amongst many other (Jason, 2019).

## **6 MEASURES TO PREVENT A CYBER ATTACK**

For an individual to stay protected against cyber threats, one should follow certain practices when it comes to cyber security. An individual can make their own computer, data and home network secure for free. Moreover, the process to ensure high cybersecurity is not needlessly difficult as it mostly requires only general understanding of common threats.

### **6.1 Password protection**

Password protection is the most common way for an individual to have a protected access to their devices, software and data. A password is required in nearly all electronic devices that can store any form of sensitive data – whether it be emails, mobile phones or cloud storages.

Even though users use passwords as means to protect outsiders from accessing their precious data, still, many people choose to use extremely weak and unthoughtful passwords. Wang et al. (2018) state that it is very common among people to simply reuse their passwords for various services or slightly modify it, even when it comes to services which store more sensitive information – like emails. He further adds that people continue to use passwords that have been leaked during data breaches.

SplashData (2018) indicates that the most popular password nowadays is ‘123456’. This simple string is leading the chart of most common, and at the same time, worst password that people use on the Internet. The theory behind why people use this is very simple; ‘123456’ is very quick to type on a keyboard or on a mobile phone and is very difficult to forget. Gartenberg (2018) reports that in October last year, a famous rapper and producer Kanye West had a televised meeting with Donald Trump, during which West pulled out his mobile phone and proceeded to unlock it by typing ‘000000’, under the sight of many television cameras. Nopsec (2017) informs that one of the bad habits that users often do is to use a password which is the same as the user’s login name or for worse, using a default password with which a certain device came. For example, network routers usually come with a default combination of ‘admin’ as a username, and ‘admin’, or ‘password’ as a password. Many people unfortunately do not bother to change the default setting on many devices or services. Nopsec (2017) further emphasizes that the most common practices that hackers use to get into somebody’s account are password guessing and cracking. With password



guessing, one can imagine that it is not very difficult to get into most people's online accounts with such passwords as mentioned above. The redeeming part for users who adopt such bad practices is that in some cases, accounts get locked after many failed attempts while entering a wrong password. Another fortunate thing is that many services also require a login name, which on one hand, brings another layer of protection, but on the other hand, many websites have suffered through a data breach, leaking out a great deal of password and username combinations. This can be combatted by simply changing the password, but as mentioned above, many users do not bother with such actions and continue to use their old passwords.

Franceschi-Bicchierai (2017) suggests that the best way how to create a password is to use a combination of uppercase and lowercase letters, various signs and number and with the length of preferably more than 8 characters. Ideally, a strong password looks like this: 'iJ-mG1!h@0,kas'. Naturally, no person would ever remember a password like this, especially when it is advised to use a different one for each service or device. Fortunately, password managers are available on many systems to help users with their passwords. Password managers create a unique and strong password for every website a user chose to use. The password manager then fills out login forms with the password it has created. A user will only have to create and remember a single password that he will then use to log in to a password manager of his choosing, in order to gain access to his passwords.

Just as password managers can help users to safely log into applications and services on various devices, there are also safer ways to log into a device itself. Nowadays, nearly every modern phone and laptop is equipped with a fingerprint sensor, some mobile devices even have a special face unlocking mechanism. Apple (2017) explains that their face recognition technology, which uses a 3D depth sensor is twenty times more secure than unlocking a device with a finger, meaning there is only one in a million chance that the face recognition software could be tricked, compared to one in fifty thousand with the fingerprint sensor. Face recognition technology which other manufacturers use on their devices is, according to Clover (2017), less secure, due to using only 2D scanning with no depth.

## 6.2 Safe internet browsing

As outlined in the chapter regarding malware and other cyber-attacks, a lot of problems can be solved by having basic knowledge about what is and is not dangerous. Stewart (2018) informs that while browsing through the Internet on daily basis, regular users are not that likely to get attacked or infected by any form of malicious software. A problem may arise when the user chooses to visit websites with adult content, various file sharing sites, illegal streaming services and social networks. In general, Stewart (2018) advises to not download any software from above mentioned websites, since the user never knows what he is truly downloading and may get infected by malware. Another issue is that the Internet is full of advertisements, especially on adult and illegal streaming sites. The content hosted on these sites is usually free, therefore the only way for them to make money is to cover their websites with ads and various other pop-up windows<sup>10</sup>, with likelihood that the user, viewing these ads may get infected by malware, through malvertising.

In order to stay safe, it is not only necessary to think about how a user would use the Internet, but also how a user would connect to it. Many people connect to the Internet in coffeeshops, malls, restaurants, airports, etc., through using public Wi-Fi. Dolly (2019) warns that there is a possibility for a third party to inject itself in the middle of you and the connection point, causing your data to go through somebody else and not straight to the connection point. For this reason, it is not advised to use public Wi-Fi for anything else other than basic searching, since the middleman could potentially harvest any sensitive data, like credit card information or a home address from the user's network traffic. If a situation occurs in which the use of public Wi-Fi is unavoidable when handling sensitive data, Dolly (2019) recommends using a VPN<sup>11</sup>.

---

<sup>10</sup> A pop-up window refers to a new browser window that appears either by clicking on a hyperlink or automatically upon visiting a certain website (Beal, n.d.).

<sup>11</sup> A VPN is a tool which enables the user to hide his real IP address and encrypt data transfers. This tool is provided by e.g. NordVPN or TunnelBear (WhatIsMyIP, n.d.).

### **6.3 Antivirus and firewall**

Whether the users are not as knowledgeable as they should be, or simply not careful, antivirus software is in most cases the last line of defence and should be mandatory on every computer.

The purpose of antivirus software is to search and destroy malware. Buffered (n.d.) describes an antivirus as a program which scans the computer's system, any inserted removable media, visited websites or files the user chooses to download from the Internet. During the scanning process, the program is looking for virus signatures, which can be imagined as digital footprints of a virus. The "footprint" is comprised of unique bits of code, strings of numbers and characters (Virus signature, n.d.). Yusuf et al. (2017) report that most viruses available on the market use heuristic-based detection<sup>12</sup> in order to compare the signatures of already known viruses against a potential threat - this approach to scanning gives antiviruses the ability to detect brand new viruses and even those, who have been disguised and released as new. Unfortunately, "this method may sometimes cause that the antivirus may detect an uninfected file as infected", Yusuf (2017) adds. On the market, there are currently many options when it comes to choosing antivirus software. The consensus is such that even though many companies offer a free version of an antivirus solution, they are most often not as robust as their premium counterparts, mainly in the swiftness of detecting non-automatic scans and updates, and a lack of a powerful firewall (Buffered, n.d.). An example of an antivirus which provides a free version, as well as a more premium solution, is Czech antivirus software called Avast, with the free version being sufficient for most average users.

As an antivirus solution could be understood as software which defends the computer itself, a firewall provides security for the network (Comodo, n.d.). Whereas the antivirus actively prevents threats, in the form of infected files, the firewalls protect the network from infected packets.

It is also very important to note that keeping every piece of software installed on any device should be updated frequently, due to companies releasing various bug fixes for their software in order to keep it as secure and functional as possible.

---

<sup>12</sup> An approach with no certain algorithm, often requiring a non-optimal, or logical practical method (Heuristic, n.d.).

## **6.4 Corporate protection**

As mentioned in previous chapters, companies of any size are targeted frequently, since a big reward is always waiting for the attacker. Cybercrime prevention in smaller or larger corporations should be no different than what an individual user at home should do. Truesdell (2018) recommends one of the most effective weapons against many forms of cybercrime, and that is awareness. Employees should be schooled accordingly in order to have a general understanding on what they can or cannot offer to do with their company computers. Therefore, every employee should have enough knowledge of phishing and the impact of accidentally downloading an infected file. Tyler (2018) also recommends forcing employees to properly sign off all their services and accounts, in case there would be anybody willing to sabotage the company, or the employer.

From my experience of working at a mid-sized corporation, where I was using the computer on daily basis, I can safely say that the company and all my data were very secure. A new, strong password for Windows and email login was generated every month for each employee. Employees were schooled about basics of cyber protection and assured that nobody from the company would ever ask them about their password. We had a strong and safe network infrastructure where nobody could visit an inappropriate website, since nearly all of them were banned. No employee was able to install anything without the permission of an administrator, Our internal database that all of the employees used to work could be only accessed from the work computers and not from home and when it came to home-office working, each employee had to speak with the IT department in order to gain privilege to the database from his personal computer – and only for the duration of the home-office. All the files were automatically backed up to the cloud; therefore, when any employee needed to move to a new PC, the only thing he needed to do was to just login. The company was backing up the files for three reasons: firstly, for the sake of convenience; secondly, due to the security of having all of the files backed up elsewhere so that in case of any hardware damage or accidental deletion, the files would not have been lost. Thirdly, due to all of the files and documents being on the cloud, no employee ever had the need to use any removable media, like USB drives, which may get infected by malware at home and then spread to the company's computers.

## Practical part

### 7 DENIAL OF SERVICE

Clough (2010) describes a Denial of Service (hereinafter referred to as DoS) attack as an attack that aims to overwhelm the network with huge traffic, slowing the network down or even rendering it completely unusable, therefore denying service. Although DoS only uses a single machine, there also exist a more dangerous variant called a Distributed Denial of Service (DDoS). As the name suggests, the attack is carried out from more than one device connected to the Internet. The attacker usually gets access to a wide range of devices by infecting them with malware, which allows him to hijack the device and use it to cause harm. This hijacked device then becomes a bot, a larger group of these devices is described as botnet (Imperva, n.d.).

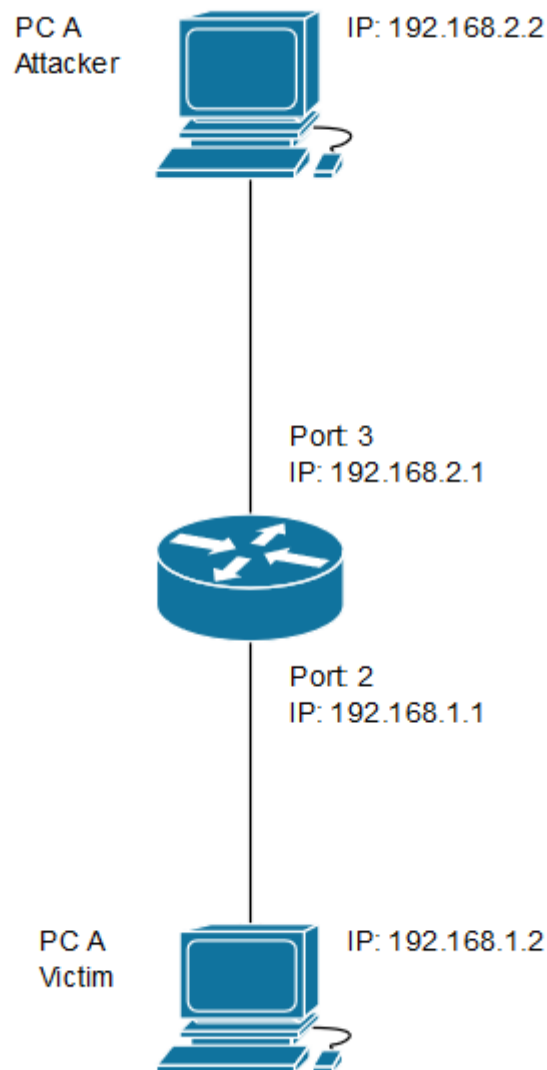
There are many various techniques that can be used in order to overwhelm the network, this practical example uses a method called ICMP<sup>13</sup> flood. Clough (2010) describes ICMP flood as an action which utilises pings, bite sized signals used to test whether a computer B can be reached from a computer A. The attacker, however, can cause the victim's computer to slow down noticeably and even cause the server or computer to crash, by simply overwhelming the victim's computer with enormous quantity of pings.

---

<sup>13</sup> Internet Control Message Protocol is an Internet protocol used by network devices for sending small information messages (Internet Control Message Protocol, n.d.).

## 7.1 Simulation of a DoS attack

The simulation is run locally between two computers and a router (see Figure 1), so at first, it is needed to set the IP addresses and the default gateway on each computer manually, through the operating system's interface. For the sake of simplicity, it is also necessary to turn off a firewall on both devices since it blocks ICMP requests by default.



*Figure 1.* Network topology.

After everything is done locally, it is time to generate the packets. In order to do so I decided to use Ubuntu operating system as a platform, and trafgen<sup>14</sup>, a network traffic generator. This process can be also carried out using a Windows PC, though I do feel that if given the choice,

---

<sup>14</sup> Trafgen is a part of a networking toolkit for Linux called netsniff.

using almost any Linux distribution is faster and easier for most tasks.

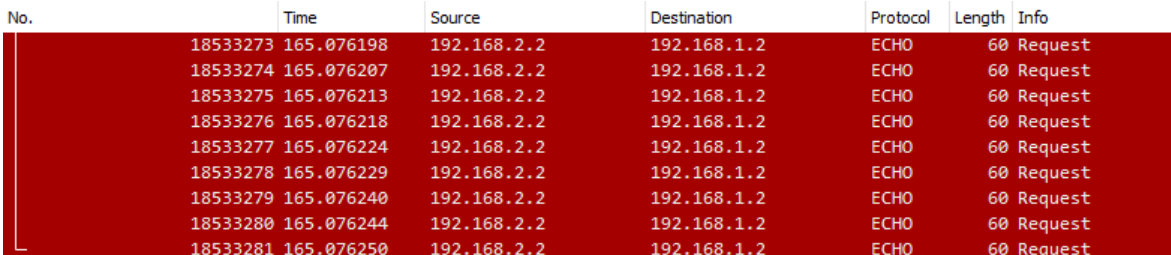
Trafgen will generate echo packets, but first it is needed to configure it properly so that it would know where to send the packets. The configuration is done by creating a simple configuration file, with a script, which will serve as a set of instructions for trafgen to read.

In this case the script looked as follows:

```
{  
  eth(da=28:D2:44:35:80:26),  
  ipv4(daddr=192.168.1.2)  
  udp(dp=7),  
  "test"  
}
```

The first line of the script sets the MAC address<sup>15</sup> of the destination, whereas the second line sets the IP address of the destination, in our case, the destination is PC A, the victim's computer as illustrated in Figure 1. On the third line, there is a destination port *dp* set to "7", meaning that trafgen is going to generate "echo", a small packet into which a user can write a simple text, in our case "test" (Auditmypc, n.d.). From this point, everything is ready and by calling the script, PC B will start to send the packets. The packets will flow indefinitely, if not terminated by the attacker.

On PC A, we can observe the packet flow from PC B by using a network sniffing tool, in this case, Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
18533273	165.076198	192.168.2.2	192.168.1.2	ECHO	60	Request
18533274	165.076207	192.168.2.2	192.168.1.2	ECHO	60	Request
18533275	165.076213	192.168.2.2	192.168.1.2	ECHO	60	Request
18533276	165.076218	192.168.2.2	192.168.1.2	ECHO	60	Request
18533277	165.076224	192.168.2.2	192.168.1.2	ECHO	60	Request
18533278	165.076229	192.168.2.2	192.168.1.2	ECHO	60	Request
18533279	165.076240	192.168.2.2	192.168.1.2	ECHO	60	Request
18533280	165.076244	192.168.2.2	192.168.1.2	ECHO	60	Request
18533281	165.076250	192.168.2.2	192.168.1.2	ECHO	60	Request

Figure 2. Wireshark interface – packet flow.

In Figure 2, we can see a screenshot from the Wireshark's interface. It shows us the end of the packet flow. It is observable that in a very short time, no longer than two minutes, PC A received 18533281 packets.

<sup>15</sup> Media Access Control address is a unique address assigned to a hardware network controller (MAC address, n.d.).

Wireshark also shows the source of these packets, its destination and the used protocol. Wireshark allows us to inspect each individual packet further, allowing us to see the packet's details.

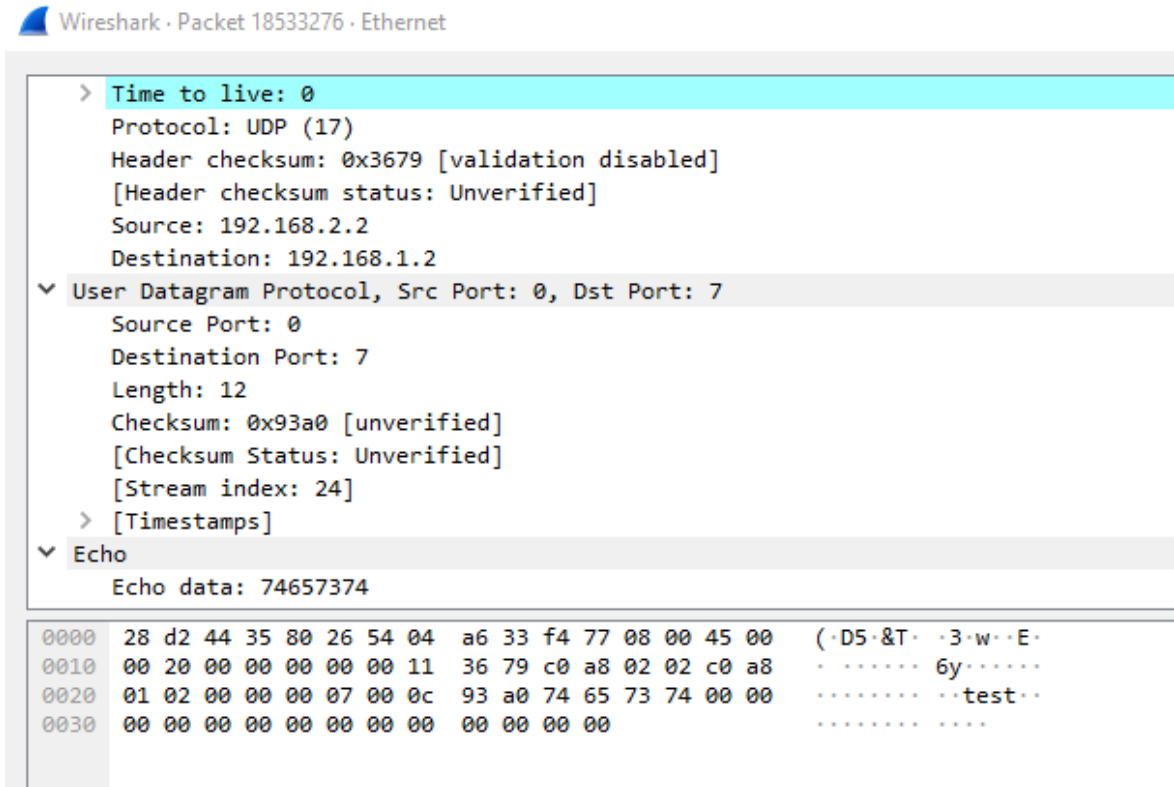


Figure 3. Wireshark interface – packet detail.

In Figure 3, the detail of the packet shows further information, including the short text that is written in the configuration file for trafgen (“test”). On the other hand, the attack can be observed from a broader perspective in Figure 4.



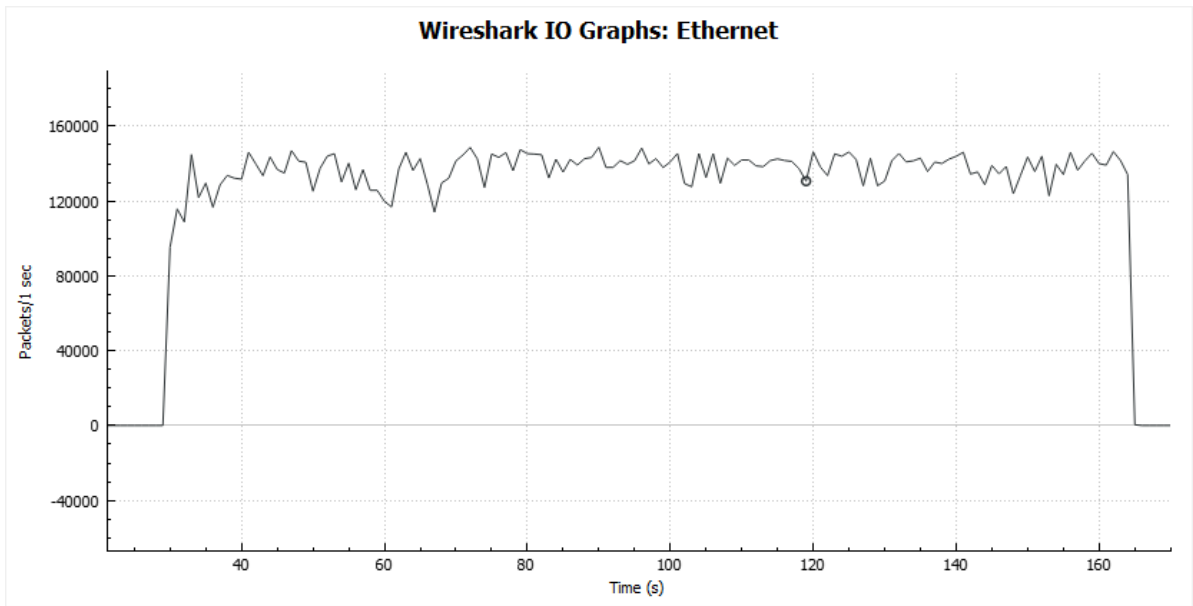


Figure 4. Wireshark interface – graph of the packet flow.

As stated earlier, a DoS attack may hinder the user experience of the victim’s computer as shown in Figure 5, where the connection from PC A to PC B is getting interfered by the attack.

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

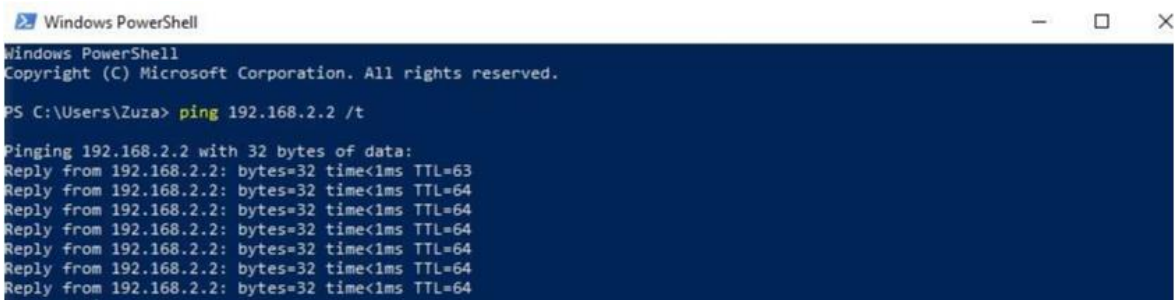
PS C:\Users\Zuza> ping 192.168.2.2 /t

Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.2.2: bytes=32 time=1031ms TTL=64
Reply from 192.168.2.2: bytes=32 time=12ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.2.2: bytes=32 time=10ms TTL=64
Request timed out.
Reply from 192.168.2.2: bytes=32 time=9ms TTL=64
Reply from 192.168.2.2: bytes=32 time=10ms TTL=64
Request timed out.
Request timed out.

```

Figure 5. Ping from PC A to PC B – under attack.

After starting the packet flow from PC B, PC A became completely frozen and unusable due to the large packet flow, which overburdened the CPU. Therefore, the PC A was unable to even perform a simple ping command, which would send 4 requests to PC B, testing whether it can be reached through the network by PC A. The command had to be modified adding /t to the end of the command, so that PC A would ping PC B indefinitely.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Zuza> ping 192.168.2.2 /t

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time<1ms TTL=63
Reply from 192.168.2.2: bytes=32 time<1ms TTL=64
Reply from 192.168.2.2: bytes=32 time<1ms TTL=64
Reply from 192.168.2.2: bytes=32 time<1ms TTL=64
Reply from 192.168.2.2: bytes=32 time<1ms TTL=64
Reply from 192.168.2.2: bytes=32 time<1ms TTL=64
```

*Figure 6.* Ping from PC A to PC B - not under attack.

From Figures 5 and 6, it is easy to spot the difference in communication between the two computers when they are under a DoS attack and when they are not. Figure 5 shows that the ping requests were mostly not even able to reach their destination and if they managed to reach it, there was a significant delay when compared to Figure 6, which shows a clean flow with little or no delay.

In practice, DoS attacks can be prevented rather easily. As Weiss (2012) informs, the attack can be simply stopped by blocking the IP address of the attack's origin. Firewalls usually block various ping requests natively or can be configured to do so. The problem arises when the victim is under a DDoS attack. The effect of DDoS is the same as of a regular DoS – the intention is to flood the victim's network, causing it to crash, or slow down. As an example, in 2017, a DDoS attack affected Swedish transportation services, crashing an IT system which monitors location of trains. This caused a disruption of various services and the delay of trains, as Barth (2017) reports. Although similar, the effect of a DDoS is much stronger than of a regular DoS and as such, it is also very difficult to protect against. Since the attack is distributed (meaning more than one origin), it is impossible to block all the attacked IP addresses. Weiss (2012) remarks that many victims act when under a DDoS attack in collaboration with their Internet provider, who can reroute the incoming traffic. Although it stops the attack, it also causes the traffic from regular users to be rerouted as well, thus denying access to a certain service. Rubens (2018), however, advises fewer extreme solutions to the problem. One of those solutions is to spread out the servers, on which a certain service runs, across multiple datacentres – the datacentres should differ geologically and should also be connected to different networks. In case of a DDoS attack, the effect of it will not be as fatal and can impact only a part of a service. One of the most effective solutions is, however, to use a specialised solution, distributed by cybersecurity vendors such as Arbot Networks, or Cloudflare, which blocks the DDoS attack before it can hit a firewall.

## 8 CONCLUSION

Cybercrime is a very wide topic which has been covered by a large number of sources. The aim of the thesis was to discuss the crucial issues of cybercrime, give relevant examples of cybercrime and suggest most effective measures to prevent it.

Looking back at the history, it is quite interesting to see just how quickly technology has progressed as well as crime misusing it. Around fifty years ago, there were people interfering in telephone communication using a whistle, then, an old, night shift operator became famous for sabotaging equipment worth two million dollars with his car keys. Nowadays, many forms of cybercrime happen on daily basis. Whether it is people from across the world trying to scam strangers through phishing, or a hacker stealing personal data from large companies and selling them on a marketplace hidden from the ordinary people. But then again, why should people not commit cybercrime? From the moral standpoint, it is wrong to steal from people or destroy something that somebody worked on. But from the purely practical point of view, there is a little chance that a skilled cybercriminal will be caught, therefore, it is almost impossible to prevent the people who do not value morals and want to get rich from committing cybercrime.

The theoretical part describes mostly threats which can directly affect almost anybody – from single users to larger companies, but it mostly concerned data or money theft. For this reason, it was necessary to inform the reader about another very common threat, which is the DoS attack. The purpose of the practical part was to simulate such an attack and to show how devastating it could be. In this specific example, not only the network, but also the victim's computer suddenly became incredibly slow, to the point of being inoperable. Now, it is necessary to examine it in a broader perspective. In real life, DDoS attacks can hinder big corporations from providing various services for many people, thus resulting in loss of earnings due to network congestion as noted in the example from Sweden.

There are many more aspects concerning the topic of cybercrime than this thesis dealt with, such as different types of malware, exploration of the Deep Web and emerging trends including machine learning for not only fighting the cybercrime, but also for committing it. One is left to wonder what the future technology will bring us, and to be relevant, what ways the people will find to misuse approaching technologies.

## 9 LIST OF REFERENCES

- Aimoto, S., et al. (2018). *Internet security threat report. Volume 23*. Mountain View: Symantec.
- AlphaBay. (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from <https://en.wikipedia.org/wiki/AlphaBay>
- AlphaBayMarket. (2016, November 1). What felons can find on AlphaBay market. Retrieved from <https://alphabaymarket.com/what-felons-can-find-on-alphabay-market/>
- Apple. (2017, November). Face ID Security. Retrieved from [https://www.apple.com/business/site/docs/FaceID\\_Security\\_Guide.pdf](https://www.apple.com/business/site/docs/FaceID_Security_Guide.pdf)
- Armerding, T. (2015, January 12). Why criminals pick on small business. Retrieved from <https://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html>
- Auditmypc. (n.d.). UDP 7. Retrieved from <https://www.auditmypc.com/udp-port-7.asp>
- Babka, J., & Willis, P. (2018 January 29). How YOU can help #FreeRoss Ulbricht of Silk Road. Retrieved from <https://downsizedc.org/silk-road-amicus/>
- Barth, B. (2017, October 13). DDoS attacks delay trains, stymie transportation services in Sweden. Retrieved from <https://www.scmagazine.com/home/security-news/cybercrime/ddos-attacks-delay-trains-stymie-transportation-services-in-sweden/>
- Beal, V. (n.d.). pop-up window. Retrieved from [https://www.webopedia.com/TERM/P/pop\\_up\\_window.html#](https://www.webopedia.com/TERM/P/pop_up_window.html#)
- Becker, J. (1980). Computer crime. Career of the future. *Computer Careers Magazine*, 1, 12–15. Retrieved from [http://www.haftofthespear.com/wp-content/uploads/2011/02/Becker\\_1980\\_Computer\\_crime\\_career\\_of\\_the\\_future.pdf](http://www.haftofthespear.com/wp-content/uploads/2011/02/Becker_1980_Computer_crime_career_of_the_future.pdf)
- Brunvand, E. (1996, October 15). A little bit of hacker history. Retrieved from <https://www.cs.utah.edu/~elb/folklore/afs-paper/node3.html>
- Buffered. (n.d.). What is an antivirus? Retrieved from <https://buffered.com/glossary/antivirus/>
- Change. (n.d.). Clemency for Ross Ulbricht, Serving Double Life for a Website. Retrieved from <https://www.change.org/p/freerosspetition-we-see-potus-s-clemency-for-ross-ulbricht-serving-double-life-for-a-website-realdonaldtrump-free-ross>

- Clough, J. (2010). *Principles of cybercrime*. New York: Cambridge University Press.
- Clover, J. (2017, December 8). Face ID in iPhone X vs. 'Face Unlock' facial recognition in OnePlus 5T. Retrieved from <https://www.macrumors.com/2017/12/08/iphone-x-vs-oneplus-5t-facial-recognition/>
- Comprehensive Crime Control Act of 1984. (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from [https://en.wikipedia.org/wiki/Comprehensive\\_Crime\\_Control\\_Act\\_of\\_1984](https://en.wikipedia.org/wiki/Comprehensive_Crime_Control_Act_of_1984)
- Computer Hope. (2017, October 2). Boot code. Retrieved from <https://www.computerhope.com/jargon/b/bootcode.htm>
- Computer worm. (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from [https://en.wikipedia.org/wiki/Computer\\_worm](https://en.wikipedia.org/wiki/Computer_worm)
- Council of Europe. (2015, May 11). The state of cybercrime legislation in Africa. Retrieved from <https://rm.coe.int/16806b8a79>
- CShub. (2018, October 31). 6 ways to identify phishing attack emails. Retrieved from <https://www.cshub.com/attacks/news/5-ways-to-identify-phishing-attack-emails>
- Delio, M. (2001, June 2). The greatest hacks of all time. Retrieved from <https://www.wired.com/2001/02/the-greatest-hacks-of-all-time/>
- Dolly, J. (2018, January 9). Why should you never, ever connect to public WiFi. Retrieved from <https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-wifi.html>
- Erb, K. P. (2018, December 4). IRS Warns on surge of new email phishing scams. Retrieved from <https://www.forbes.com/sites/kellyphillipserb/2018/12/04/irs-warns-on-surge-of-new-email-phishing-scams/#4de3e6984b24>
- European Commission. (2012, April). Fighting cybercrime. Retrieved from [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/cybercrime\\_fact\\_sheet/factsheet\\_cybercrime\\_v.03\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/cybercrime_fact_sheet/factsheet_cybercrime_v.03_en.pdf)
- FBI. (2011a). Bank crime statistics 2010. Retrieved from <https://www.fbi.gov/stats-services/publications/bank-crime-statistics-2010/bank-crime-statistics-2010>
- FBI. (2011b). Internet crime report. Retrieved from <https://www.fbi.gov/stats-services/publications/bank-crime-statistics-2010/bank-crime-statistics-2010>
- Fell, J. (2017, March 13). Hacking through the years: a brief history of cyber-crime. Retrieved from <https://eandt.theiet.org/content/articles/2017/03/hacking-through-the-years-a-brief-history-of-cyber-crime/>

Focus Training. (2016). The secret history of cyber-crime. Retrieved from <https://www.informationsecuritybuzz.com/articles/the-secret-history-of-cyber-crime/>

Foresee. (n.d.). What is phone phreaking? Retrieved from <http://www.foreseegroup.co.uk/2016/08/12/what-is-phone-phreaking/>

Franceschi-Bicchierai, L. (2017, November 22). How password managers work and why you should use one. Retrieved from [https://motherboard.vice.com/en\\_us/article/59yv5x/how-password-managers-work-and-why-you-should-use-one](https://motherboard.vice.com/en_us/article/59yv5x/how-password-managers-work-and-why-you-should-use-one)

Frankenfield, J. (2019, February 12). Cryptocurrency. Retrieved from <https://www.investopedia.com/terms/c/cryptocurrency.asp>

Freeross. (n.d.). Free Ross Ulbricht. Retrieved from <https://freeross.org/>

Gartenberg, Ch. (2018, October 11). Kanye West's iPhone passcode is 000000. Retrieved from <https://www.theverge.com/tldr/2018/10/11/17964848/kanye-west-iphone-passcode-trump-iplane-apple-meeting/>

Garber, M. (2014, September 19). When phone operators were unruly teenage boys: Before they were women, they were swearing, wrestling, beer-drinking pranksters. Retrieved from <https://www.theatlantic.com/technology/archive/2014/09/when-your-friendly-phone-operator-was-a-teenage-boy/380468/>

Greene, T. C. (2003, January 13). Chapter One: Kevin Mitnick's story. Retrieved from [https://www.theregister.co.uk/2003/01/13/chapter\\_one\\_kevin\\_mitnicks\\_story/](https://www.theregister.co.uk/2003/01/13/chapter_one_kevin_mitnicks_story/)

Grimes, A. R. (2012, January 10). Why Internet crime goes unpunished. Retrieved from <https://www.csoonline.com/article/2618598/cyber-crime/why-Internet-crime-goes-unpunished.html>

Heuristic. (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from <https://en.wikipedia.org/wiki/Heuristic>

Imperva. (n.d.). Botnet DDoS Attacks. Retrieved from <https://www.imperva.com/learn/application-security/botnet-ddos/>

Internet Control Message Protocol (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from [https://en.wikipedia.org/wiki/Internet\\_Control\\_Message\\_Protocol](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol)

IP Address. (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from [https://en.wikipedia.org/wiki/IP\\_address](https://en.wikipedia.org/wiki/IP_address)

IRS. (n.d.). Tax scams / Consumer Alerts. Retrieved from <https://www.irs.gov/newsroom/tax-scams-consumer-alerts>

- Jason. (2019, February 25). Hacker selling third round of stolen databases on Dream Market. Retrieved from <https://dreammarketdrugs.com/hacker-selling-third-round-of-stolen-databases-on-dream-market/>
- Johnson, T. (2018, March 13). Get hit by Internet crime? Good luck getting help from some local police. Retrieved from <https://phys.org/news/2018-03-Internet-crime-good-luck-local.html>
- Kabay, M. E. (2008). *A brief history of cybercrime*. Norwich: School of Graduate Studies.
- Kaspersky. (n.d.). What is a Boot Sector Virus? - Definition. Retrieved from <https://usa.kaspersky.com/resource-center/definitions/boot-sector-virus>
- Kevin Mitnick. (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from [https://en.wikipedia.org/wiki/Kevin\\_Mitnick](https://en.wikipedia.org/wiki/Kevin_Mitnick)
- Kovalchik, K. (2008, August 30). True crime: John Draper, the original whistle blower. Retrieved from <http://mentalfloss.com/article/19484/true-crime-john-draper-original-whistle-blower>
- Lilemose, J., & Kryger, M. (2015, August 24). The (re)invention of cyberspace. Retrieved from <http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/>
- MAC address. (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from [https://en.wikipedia.org/wiki/MAC\\_address](https://en.wikipedia.org/wiki/MAC_address)
- McQuade III, S. C. (Ed.). (2009). *Encyclopedia of cybercrime*. Westport: Greenwood Press.
- Matthews, K. (2019 February 2). Incident of the week: UConn Health phishing attack exposes patient data. Retrieved from <https://www.cshub.com/attacks/articles/incident-of-the-week-uconn-health-phishing-attack-exposes-patient-data>
- Miniwatts Marketing Group. (2018). Internet world stats. Retrieved from <https://www.Internetworldstats.com/stats.htm>
- Mitnick Security Consulting LLC. (n.d.). About Kevin Mitnick, CEO, team leader, and chief white hat hacker. Retrieved from <https://www.mitnicksecurity.com/about/kevin-mitnick-worlds-most-famous-hacker-biography>
- Mitra, A. (2017, March 7). Worm vs virus vs Trojan. Retrieved from <https://www.thesecuritybuddy.com/malware-prevention/worm-vs-virus-vs-trojan/2/>
- Morris Worm. (n.d.). In *Techopedia*. Retrieved from <https://www.techopedia.com/definition/27371/morris-worm>
- Murdock, E. E. (n.d.). *History of Computers in Education* [HTML Document]. Retrieved from <https://web.csulb.edu/~murdock/histofcs.html>
- Murphy, I. A. (2011). Captain Zap. Retrieved from [https://hackstory.net/Captain\\_Zap](https://hackstory.net/Captain_Zap)

Nigam, P. (n.d.). Onion routing. Retrieved from <https://www.geeksforgeeks.org/onion-routing/>

Nopsec. (2017, August 9). How hackers exploit weak passwords. Retrieved from <https://www.nopsec.com/weak-passwords-exploit/>

Norry, A. (2018, January 29). The history of Silk Road: A tale of drugs, extortion and bitcoin. Retrieved from <https://blockonomi.com/history-of-silk-road/>

Norton. (n.d.). What is a computer virus? Retrieved from <https://us.norton.com/Internetsecurity-malware-what-is-a-computer-virus.html>

Norton. (n.d.). What is ransomware? And how to help prevent it? Retrieved from <https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html>

Ponemon Institute LLC. (2017). *2017 state of cybersecurity in small & medium-sized businesses (SMB)*. Traverse City: Ponemon Institute.

Richard. (2017, July 16). AlphaBay seized by feds, admin commits suicide in Thai jail. Retrieved from <https://darkwebnews.com/alphabay/alphabay-gone/>

Rouse, M. (2017). ARPANET. Retrieved from <https://searchnetworking.techtarget.com/definition/ARPANET>

Rouse, M. (2018). Cybercrime. Retrieved from <https://searchsecurity.techtarget.com/definition/cybercrime>

Rubens, P. (2018, June 26). How to Prevent DDoS Attacks: 6 Tips to Keep Your Website Safe. Retrieved from <https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.html>

Schober, S. (2015 January 27). Deep Dark Web of the Internet iceberg. Retrieved from <https://scottsschober.com/deep-dark-web-of-the-internet-iceberg/>

Securebox. (n.d.). Network sniffing. Retrieved from <https://securebox.comodo.com/ssl-sniffing/network-sniffing/>

Small Business Committee. (2015, April 22). Small business, big threat: Protecting small businesses from cyberattacks. Retrieved from <https://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=398099>

SplashData. (n.d.). The top 100 worst passwords of 2018. Retrieved from <https://www.teamsid.com/100-worst-passwords/>

Stewart, Ch. (2018, June 25). How to browse the internet safely. Retrieved from <https://hackernoon.com/how-to-browse-the-internet-safely-d84e59d56057>

Symantec. (n.d.). What is a computer worm, and how does it work? Retrieved from <https://us.norton.com/Internetsecurity-malware-what-is-a-computer-worm.html>



- Three-way Handshake. (n.d.). In *Techopedia*. Retrieved from <https://www.techopedia.com/definition/10339/three-way-handshake>
- TOR. (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from [https://en.wikipedia.org/wiki/Tor\\_\(anonymity\\_network\)](https://en.wikipedia.org/wiki/Tor_(anonymity_network))
- Torres, G. (2018, April 10). Malvertising: attack of the ads. Retrieved from <https://www.avg.com/en/signal/what-is-malvertising>
- Truesdell, G. (2018, January 12). 7 cybercrime prevention tips for modern businesses. Retrieved from <https://www.advantageservices.net/blog/85/7-Cybercrime-Prevention-Tips-for-Modern-Businesses>
- Tyler, A. (2018, June 13). 10 essential steps for preventing cyber-attack on your company. Retrieved from <https://www.itproportal.com/features/10-essential-steps-for-preventing-cyber-attacks-on-your-company/>
- UConn. (n.d.). Notice of Data Security Incident. Retrieved from <https://health.uconn.edu/securityincident>
- United Nations Office on Drugs and Crime. (2012). *The use of the Internet for terrorist purposes*. Vienna: United Nations Office.
- Virus Signature. (n.d.). In *Techopedia*. Retrieved from <https://www.techopedia.com/definition/4158/virus-signature>
- Wang, Ch., et al. (2017). The next domino to fall: Empirical analysis of user password across online services. Retrieved from <https://people.cs.vt.edu/gangwang/pass>
- WannaCry. (n.d.). In *Wikipedia: the free encyclopedia*. San Francisco: Wikimedia Foundation. Retrieved from [https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)
- WhatIsMyIP. (n.d.). What is a VPN? Retrieved from <https://www.whatismyip.com/what-is-a-vpn/>
- Weiss, A. (2012, July 3). How to Prevent DoS Attacks. Retrieved from <https://www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html>
- Yusuf, M., et al. (2017). Review of viruses and antivirus patterns software & data engineering global journal of computer science and technology: C review of viruses and antivirus patterns. Retrieved from [https://www.researchgate.net/publication/322552067\\_Review\\_of\\_Viruses\\_and\\_Antivirus\\_Patterns\\_Software\\_Data\\_Engineering\\_Global\\_Journal\\_of\\_Computer\\_Science\\_and\\_Technology\\_C\\_Review\\_of\\_Viruses\\_and\\_Antivirus\\_Patterns](https://www.researchgate.net/publication/322552067_Review_of_Viruses_and_Antivirus_Patterns_Software_Data_Engineering_Global_Journal_of_Computer_Science_and_Technology_C_Review_of_Viruses_and_Antivirus_Patterns)

## 10 LIST OF FIGURES

<i>Figure 1.</i> Network topology. ....	p. 38
<i>Figure 2.</i> Wireshark interface – packet flow. ....	p. 39
<i>Figure 3.</i> Wireshark interface – packet detail. ....	p. 40
<i>Figure 4.</i> Wireshark interface – graph of the packet flow. ....	p. 41
<i>Figure 5.</i> Ping from PC A to PC B – under attack. ....	p. 41
<i>Figure 6.</i> Ping from PC A to PC B – not under attack. ....	p. 42