Computer threats and countermeasures in modern world

Pauli Mäkelä
The thesis examines computer threats and countermeasures on modern world focusing on the use of personal computer and mobile devices. As the issue is wide and complex such a focus is justified for this thesis.

The impact of cyberattacks and cybercrimes is significant for computer users and through them to businesses and society. Some estimates suggest that the damage related to cybercrime is growing rapidly and is projected to be USD 6 trillion globally in 2021.

Six main types of computer attacks can be identified: backdoor, virus, denial of service attack, distributed denial of service attack, browser hijacking and eavesdropping of man-in-the-middle attack.

Individual PC and mobile device users operate in different systems and are using different operating systems and vulnerabilities vary accordingly. The thesis looks systematically at the vulnerabilities and countermeasures in different situations. It is important to note that some studies suggest that some 70% of computer attacks originate from emails and their attachments.

The computer threats and vulnerabilities are a serious issue in the modern world which is increasingly relying on IT-solutions in providing services for businesses and public and in the transformation to the digital economy and society. The damage caused by cyberattacks and crimes is already very high and on increase.

At the same time the cyberattacks and cybercrimes are slowing down and impeding the digitalisation and all the efficiency gains and other benefits it can bring about. Also risks to security are evident and felt already.

The stakes are high, the awareness is still low and available countermeasures and knowledge of them is not fully utilised.

Keywords
computer, threats, countermeasures, cyber security, cyberattacks, cybercrime
# Table of contents

1  Introduction .........................................................................................................................1
1.1 Research questions .............................................................................................................1
2  Theoretical Background .......................................................................................................3
   2.1 Types of vulnerabilities ....................................................................................................2
   2.2 Systems at risk .................................................................................................................6
3  Countermeasures ..................................................................................................................12
4  Case studies ........................................................................................................................15
5  Discussion ............................................................................................................................18
References ...............................................................................................................................20
1 Introduction

When talking about computer security the main objective of any countermeasures is that users protect their own PC’s from outside threat.

Outside threat usually coming from cyber criminals who try to steal and damage the software’s and hardware’s of your computer. Hackers try to steal your sensitive information and then use it for personal gain.

This is the major problem in the IT sector causing all kinds of threats, problems and costs in businesses, public administration, security and individuals. Some indication of the magnitude of these problems are presented below.

![Motivations Behind Attacks (January 2019)](image)

**Figure 1** Motivation behind cyber attacks

Cyberattacks cause all kind of harm, loss and costs, both to PC users, businesses and society. Due to the nature of these attacks the available data of assessing the impact is insufficient. US government has estimated that malicious cyber activity cost the US economy alone between USD 57 billion and USD 105 billion in 2016 and spill-over costs are much higher.

Across the industry assessments have concluded that in 2019:

- Some 24000 malicious mobile apps are blocked every day
- 71% of cyberattacks with spear phishing emails
- in 2017 20% of attacks came from China, 11% from the USA and 6% from Russia
- in 2017 61% of victims were businesses under 1000 employees and of all tacks 18% took place in the USA
• Average cost of a malware attack on a company is USD 2.4 million out of which information loss represents 41%
• Damage related to cybercrime is growing rapidly and is projected to be USD 6 trillion in 2021

The estimated impacts presented above demonstrate that computer security and cybercrime is a serious issue for our societies. As threats and cybercrime are increasing rapidly there is no time for complacency. For instance, while three quarters of companies have over 1000 sensitive files, 21% of all files are not protected at all and 41% of companies having over 1000 sensitive files including credit card numbers and health records left leave these files unprotected.

Computer security includes different protection mechanisms. These mechanisms include access control, which helps the user to protect his/her computer. An example of access control is username and password. These two security factors help users also to protect against harmful files, which could be downloaded from the internet.

Access control also includes physical aspect. Harmful files can be downloaded from the internet, which could, for example, slow down the computer. An external user can also hijack computers. Thus, it is important for a user to protect his/her computer from harmful files and users by using a good protection mechanism.

1.1 Research questions

The idea of this thesis is to find out what kind of security threats there are. In addition, the main idea is to examine what kind of countermeasures people can use to protect their personal computer(s).

Due to the complexity and continuous developments related to IT security issues this thesis is focusing on security issue related to the computer and mobile device use of the public.

In addition, the impacts of security risks are being looked at to the extent they can be estimated and covered.
2 Theoretical Background

Vulnerabilities are a path that a hacker or a criminal may use to gain access to someone’s computer. Hackers and criminals try to find an opening on the security mechanism and then try to utilize it. If a hacker or a criminal finds an opening, he/she tries different methods to gain access to the system. These methods may include sending viruses through emails or different web pages and then use the opening for his/her purposes. Other mechanisms also exist, and hackers and criminals are continuously developing new ways of attaching personal and mobile devices. This poses a specific challenge to those trying to deal with the IT security issues as there is a continuous and evolving race between those responsible for IT security and hackers and criminals.

If these problems aren’t solved it leaves an unprotected area in the computers system. A hacker may then use this area to gain access to the computer. Once in, a cyberbully can steal sensitive information or cause other harm to the computer user.

2.1 Types of attacks and vulnerabilities

Backdoor is a method in which a hacker tries undetected to gain access to someone’s computer by bypassing the normal security mechanisms. If the hacker manages to get in, he/she tries to use the computer in his/her advantage. This means that a hacker tries to find vulnerabilities which he/she can use to gain access to files and other sensitive information on the computer. The cyber bully might target different software’s. These software’s might be out of date which the hacker could use to get in. One good example of these programs is zero-day attack. When a problem occurs in a software it might take a while for the user to repair this flaw. During this time, the hacker has infected the computer and installed harmful viruses. (TechTarget 2019.)

Backdoor attack contains different types of malicious software’s (malwares). This cyber bully may use these malwares to harm the computer. These malwares have multiple tasks. For example, hackers use malwares to harm the computer and steal sensitive information. They also use them to bypass access control, so they could take the computer over. Some of the symptoms of malwares are:

1. Changes the usage of the processor from normal to high
2. Slows down the usage of browser
3. There could be some problems with internet connection
4. Computer may get stuck
5. Sudden loss of files or the files may be modified
6. Abnormal activity on your computer.
If a backdoor is installed it has some negative effects on a user’s computer. Once installed, a hacker can access your files on your computer. He/she can create, delete, edit or copy them. It is also that your computer’s hardware devices are affected. Hardware devices include central processing unit (CPU), main memory and a power supply unit. Once affected, a hacker can, for example, shut down your computer if he/she wants to do it. If your computer is affected it is possible that the hacker tries to steal your personal data, passwords, identity details and valuable documents. The hacker can also track your activity on your computer and check your web browsing history. A backdoor can also infect your files, damage your computer or corrupt your applications. Your infected computer may underperform, run slowly and even crash. The hacker might install new programs without you noticing them. Once you start your computer these new programs may open immediately without you noticing it. It might also be possible that a backdoor is designed in a way that it is impossible to be removed. This creates an additional problem for you as once it is installed it cannot be removed and more radical measures are needed to overcome the problem. (Comodo Antivirus 2018)

**Virus** is one type of malware. Typical feature of viruses is that it can make of copy of itself. Once the virus multiplies, it can spread through the computer without the host noticing it. Viruses may spread through attachments sent through emails or through files which the user has downloaded from the internet. Additionally, viruses can spread is that the user visits sites, which are infected. Hackers may also use adverts to spread viruses. Once a user clicks an advert, the computer becomes affected.

The purpose of viruses is typically to delete or modify files on a computer. They can also be used to stop programs from working or to block the computer doing basic tasks. These tasks might include installing or removing programs, backing up data or the ability to change screenshot when the user wishes. Some viruses can even wipe out the entire information on the hard drive. Viruses ma also lay dormant within a computer and go unnoticed for some time. Once a certain program is opened these viruses become active. It is also possible that a virus starts operating once an infected file is downloaded. (TechTarget 2019; DaBoss 2013.)

Viruses might be difficult to notice because they are designed not to raise alarm. Some of the symptoms of viruses include users to get some random pop-up windows. These pop-ups might encourage you to visit random websites or download infected files. Another symptom can be that your homepage on your web browser has been changed. It is possible that this new homepage is a harmful website which is infected with viruses. Once you
open your web browser you are instantly taken to this site and your computer gets infected. A hacker might get a change to take over your emails. Once take over, this hacker starts to send random emails to random people. This way this hacker has an opportunity to infect other systems as well. Furthermore, your computer’s hard drive could get damaged. Because of this, your computer might crash or freeze more frequently. It is possible that once you shut down your computer you may not be able to open it again. Because of viruses’ new programs can be installed without the user ever be aware of it. These programs may start randomly. A virus can might change passwords on the computer. Because of this, you may not be able to sign in on your computers account. (Norton 2019.)

Another way for a hacker to inject a computer with viruses is by browser hijacking. The cyber bully checks which browser the computer user is currently using and tries to change modify the settings. The hacker might try to change homepage of that browser. Once the user starts the browser the browser is directed to a page which is infected by viruses. After this the viruses spread across the computer. (TechTarget 2019; Norton 2019.)

Some of symptoms of browser hijacking are that when visiting different websites these sites work very slowly. This user might notice that the web browser has some toolbars which he/she has never installed. When searching information from the internet, the web browser always directs the user into different website. You will start to get multiple pop-ups which might advertise something. (Norton 2019.)

**Denial of service attack (DoS)** is a type of threat where a cyber-bully attacks to a computer and prevents users to gain access to it. What a hacker does is that he/she floods the server or system which would cause the computer to be busy. This makes the computer impossible to use. DoS can include different types of attacks. (TechTarget 2019.)

**Distributed denial of service attack** is a type of attack where a single system is attacked from multiple sources. This type of attack targets, for example, a server, and then it would overload it and cause the system to be on hold. Because the incoming messages are ongoing the system would eventually shut down or crash. Distributed denial of service attack may be caused by a single hacker or even an organized crime gang.

Distributed denial of service attack starts by seeking any kind weak spot in a system. This type of attack can even search multiple vulnerabilities at the same time. Once it has found the most vulnerable spot it will take those parts over. When the taking over is complete it will either infect the system with malwares or it tries to bypass the access control. By passing access control means that a hacker tries to guess the default password. A system
which is under someone else control is called a zombie computer. When a computer is completely someone else’s control it allows the attacker to send viruses through the internet. This way the attacker can infect other systems which are on the same internet. (TechTarget 2019.)

(Distributed) denial of service attack could have the following symptoms on someone’s computer. A user’s internet connection is slower than before. Because your internet connection is slower you may have difficulties accessing on files stored on the internet. It is possible that you may have difficulties accessing different websites. You may also start to get more and more spam email. (TechTarget 2019.)

Eavesdropping or man-in-the-middle (MITM) attack is a type of vulnerability where an actor is, without a permission, listening a conversation between different parties. Eavesdropping can be done by listening telephone conversation or checking sent emails. Eavesdropping could be, for example, be used while a user is using Skype. PC and laptops could have microphones attached to it. While a user is using this microphone, a third-party member could be listening what the user is saying. PC and laptops could also have microphones built internally. A user can use this microphone, as well.

While eavesdropping, a third-party actor tries to find out sensitive information which he/she could use for his/her personal gain. MITM can occur while user visits sites which requires him/her to login. User’s tries to login to the site by using authentication. An example of this kind of site could be a financial site where an attack could gain sensitive information.

A hacker may also gain access to sensitive information by checking the public and private keys between two different parties. Both keys use different kind of algorithms to convert text into readable and unreadable form. Public key is made public and it can be accessed by anyone. If user A wants to send a message to user B, user A uses the public key to encrypt the message into unreadable form. User B then can decode the message with the private key. Private Key is only shared between parties who wish to send messages to each other. (TechTarget 2019; Corondo 2018.)
In a normal flow, if a user wishes to access a website the client connects to that site’s server. If the connection to the site is successful, the user sees the content of the site. On the man-in-the-middle flow, a hacker tries to insert him/herself in-between the flow of traffic between client and server. If he/she is successful he/she can inject the flow of information with false data.

**Figure 2** How Man-in-the-Middle attack works.

**Figure 3** An example of Man-in-the-Middle attack.
In a normal situation, different users can exchange information by using their public and private keys. Public key is used to change text into unreadable form. A hacker may block the real public key and replace it with a fake one. With the fake public key, the hacker makes different users believe that they are talking to someone trustworthy. The hacker can send them injected files and a user thinks that this file isn’t harmful. Once he/she opens the file his/her computer is full of viruses.

Another type of threat is called **spoofing**. A hacker tries gain access to a computer by masking the threat as a safe information. Spoofing can be used in different ways. In email spoofing, a hacker disguises an email in a way that a user thinks that it can be trusted. This type of email can contain links to harmful sites. It can contain harmful attachments. (Mack 7 June 2018, Forcepoint 2019.)

With spoofing, a hacker might try to fool different computer users. For example, a hacker may send a misleading email to a user. A hacker sends an email to user saying that he/she has made a purchase from Amazon. Without questioning the genuineness, the user might click on the attached link on the email. Right away the user is transferred on a false website and is required to log in. Once the user logs in his/her credentials are lost. Hackers may use names of big well-know companies to lure computer users. (Malwarebytes 2019.)

### 2.2 Systems at risk

Security risks related to individual uses are different in different IT systems. This chapter aims at identifying main risks related to different user systems and interfaces.

**Personal computer**

The issue of computer threats to public emerged when the personal computers became common as a working tool in work places and in households. Initially, they emerged as viruses attaching PCs and causing problems in using and storing files and data. When the use of internet expanded and integrated into the use of PCs also the vulnerability of PCs to computer threats became more complex and versatile. The following examples of threats can be mentioned as most common threats of today.

Backdoor is a virus, which tries to use the flaws and vulnerabilities in a computer to gain access to personal information. Backdoor can be used remotely. What this means is that the hacker does not need to have the user’s computer to gain access to user’s computer.
Once the backdoor virus is installed, the hacker can take over the monitor and keyboard of the user's computer. Once these two components are under his/her control, the hacker can use his/her own computer to gain access to the sensitive information.

An example of backdoor is virus called **FinSpy**. After the virus is installed, the hacker can gain access to the sensitive information once the user connects the computer to the internet. The hacker also tries to change the settings for the firewall and other security setups.

**Mobile devices**

Increasingly, mobile devices such as laptops, tablets and mobile smart phones are replacing the traditional use of PCs. This has led to specific challenges of threats of mobile devices.

Mobile users are in slight disadvantage when comparing to PC users. PC might check their emails once a day, but mobile users could have their emails attached to their phones. Once an email arrives, the phone makes an alarm and the user checks the email instantly several times a day. This multiplies the possibilities for attacks and makes protection more challenging. Same holds for all kinds of other usage of mobile devices though specific apps.

One example of problems on mobile devices security is called **Data Leakage**. While downloading different apps, the user usually allows the information on his/her phone to be shared. Once the download begins, the personal information is sent to remote servers. Hackers can try to gain access to the servers and steal the information from there.

Unsecured Wi-Fi connections can be dangerous for mobile users. This type of Wi-Fi connections does not have any passwords which allows any hacker to gain access to someone's phone. It is important to remember not to use any confidential or personal services while using an unsecured Wi-Fi. These kinds of services use, for example, banking and credit card information.

Network spoofing is one method, which hackers could use to gain sensitive information. When using this method, attackers set up fake access points. Fake access point means connections, which look like Wi-Fi connections but are actual traps. These kinds of traps can be found in coffee shops, libraries or airports. Hackers name these access points with a common name.
If a user uses a Wi-Fi at a coffee shop, cybercriminal could name his/her fake network, for instance, as “Coffee Shop Wi-Fi”. This way the hacker encourages a user to use his/her fake address.

Sometimes the fake Wi-Fi might require the user to create an account to gain access. If the user decides to create an account with an email, which he/she uses for other services, this allows the hacker to gain access to sensitive information. Wi-Fi users should not give any sensitive information while using unsecured Wi-Fi. If account is needed, then the users should create a new email and use that just for this Wi-Fi connection.

Phishing Attacks may cause problems to people who use mobile devices. A Phishing Attack is a threat where people get harmful viruses through email. Hackers send spam emails in a hope that email users would open them and then viruses would spread through the device. These spam messages could be named in such a way that different users believe that these emails are important. These spam messages could be, for instance, a request from their bank. The message could hold a link to a website and the bank might request the user to click the link.

Spyware is s specific program which mobile user are worried about. Spyware is not a malware which mobile users are most worried about. However, it can keep track of the areas where the user moves and keep track the most recently used and downloaded applications. In order words, spyware tries to spy your internet usage and tries to steal the data. (Kaspersky 2018.)

Spyware is designed to harm the user’s electronic devices without them noticing it. If a spyware is installed successfully then it tries to gain access to user’s sensitive information. Sensitive information could be your credit card or bank account information. It is also possible that a hacker could steal your identity by using a spyware. In addition, spyware could keep track on your passwords and keep track on your mobile usage. Here are some examples of the types of spyware:

- Adware. This type of spyware keeps track on your browser history and downloads. It also tries to predict what your future downloads are going to be. It's also possible that adware tries to show advertisements of the products which you buy.
- Tracking cookies. This spyware keeps track of your web activities.
- System monitors. This kind of virus keeps track what you do on your device. It can record the websites that you visit, the application which you run, or emails that your read.
Different operating systems and their combinations

There are 3 main computer operation systems in use globally. There are Windows of Microsoft mainly used in PC and office surroundings, Apple operating systems mainly for PCs and mobile devices and Google based systems focusing on mobile devices.

The computer threats, their occurrence and counter-measures vary depending on the operating system. They are in general similar, but each have their specific features. Some of these specific features are presented in the following.

Windows users face some specific problems when trying to protect sensitive information against hackers. Some reasons for this are:

1. File and share permissions. In Windows, this is one of the biggest vulnerabilities. Files can share everything with everyone. Windows users can easily create and share files with anyone across the internet. The files that are shared can have a strong authentication. However, it is also possible that admin usernames and passwords are so easy to search that the hacker does not have any problems hacking it. In addition, with the sharing possibilities the hacker can then reach easily other users.

2. Only basic firewalls set. Windows computer might have a free firewall option available for its users. This free firewall does not give the best protection to its user. To prevent the hacker hacking the computer it might be a good idea for the users to buy a better firewall. This is not often done, and vulnerability remains.

3. Weak passwords. The computer user might set a password on the admin users, which can be guessed and searched easily. Another vulnerability problem related to passwords is that the user might not set a password when the computer is at sleep mode or at screensaver and forgets to log off. Once the users log in the computer might not ask any password and the desktop appears immediately. This offers to another person the access to the computer while the main user is away and creates a risk for misuse.

Interfaces between mobile and fixed devices

Computer users are increasingly using PCs and mobile devices in an integrated fashion which poses some specific risk and vulnerability issues.

Careless use of mobile devices might open a possibility for hackers to get access to PC and to wider network with PC attached to it. And vice versa.
LAN networks

Local Area Network (LAN) is a network where two or more computers are using the same network and are connected to each other. The range of a LAN connection is less than one kilometer and it can be used on buildings or offices.

One important aspect of LAN networks is that you have a clear understanding of the network. This means that you know, for example, the vendor, basic configuration of firewalls and you know the amount of people using your network.

Once you have a basic idea of the network, you might encounter some vulnerabilities. You could find out that the firewall settings are incorrect. You find out that the password, which you use, is not correct.

As important as it is to protect your network from hackers, bots and viruses it also important to protect your LAN network physically. If your physical security is weak it can be an easy target for a hacker to take an advantage of it. For example, this hacker could install a wireless router to your LAN network and then use it to harm your devices.

Additional problem with LAN networks could be that these LAN users might use a network which does not have a password. It is quite easy just to plug in the modem and start using it. One possible security method which user can use is called Media Access Control (MAC) address. In hardware’s, MAC address work as an identification. This helps the users to tell which hardware which is. Even though MAC address cannot be changed, and it can be easily hacked, it can work as a first layer of security. (Networkworld 2018.)

3 Countermeasures

The countermeasures against different types of attacks and vulnerabilities are presented and analysed based on the literature survey and knowledge gained during the studies. Any further questionnaire to selected IT-managers would not result additional information as countermeasures are being very widely covered in literature. Furthermore, the picture is constantly changing due to the race and dynamic nature of the challenge. It should also be noted that some countermeasures are protected by the intellectual property rights and are not disclosed in detail because of the protection against hackers and criminals.

The analysis is structured in the way the vulnerabilities are being presented above.
**Backdoor**

A backdoor may be difficult to notice. There are a few ways which can help the user to detect a backdoor. An antimalware can help a user to remove a backdoor from his/her computer.

Antimalware can help a user to prevent backdoors to be installed on the computer. Antimalware scans the data coming from the network and blocks anything which seems suspicious. Antimalware can help its user to do these:

- Antimalware can prevent users visiting on sites which are infected by backdoor or other viruses
- If the user has two or more devices, then antimalware can protect those if one device is affected
- It can keep track on how many times a computer has been affected. It can also show the time it takes to get rid of the backdoor.

**Virus**

Hackers try to gain access to different computers. By using different viruses, hackers try to infect the computer to gain the sensitive information from different users. The first thing a computer user should do is to install an antivirus software on their computer. With the help of this software, different users can scan their computer and find out if their computer(s) contain any harmful viruses. Users should use an antivirus software that they can trust and keep it up to date.

It is also possible that a hacker tries physically gain access to your computer. This attacker may use some software to gain access to your computer. Once in he/she may inject your PC with viruses. For this purposes PC users should create a strong password to protect against hackers. These passwords may be used while trying to download a program to your computer. This final step conforms that the user is sure that he/she wants to download the file.

Different PC users should be careful when using emails. Email is one important way which hackers can spread viruses. Even though good antivirus software’s may be aware which emails cannot be trusted, it is a good practice not to open links or attachments that you do not trust.

Sometimes PC users may get different pop-ups when they visit different sites. It would be a good practice to prevent these pop-ups. These pop-ups may contain different viruses,
such as spywares or adware’s, which may overload your computer and then damage your PC.

An additional good practice would also be that the user turns on the User Account Control (UAC). This way any changes cannot be made without a permission from the administrator.

**Browser hijacking**

Browser hijacking is a type of malware that tries to change web browser settings. These changes are made without the user’s permission. This virus tries to readdress the user’s browser to websites that the user would not normally visit.

Once the malware has an effect, the hacker tries to change the default browser. For example, if the user is using Google Chrome the hijacker might try to change the default browser to Firefox. This attacker may try to change browser’s homepage, which would cause the webpages to load slowly. This hacker might install some toolbars and he/she may try to generate different pop-ups. These pop-ups could be some advertisements from different sites.

The idea of these browser hijackers is to send misleading advertisements, so he/she gets revenue. For example, the attacker could change the browsers homepage into a website, which the hacker could have created him/herself. Once there, the hijacker might offer the user different links to other websites. The hacker does this because he/she wants to see what interests the user. This way the attacker can collect the data and then he/she can sell the information to different parties for marketing purposes. The hijacker can also try to steal sensitive information such as users banking information. (TechTarget 2018.)

To remove the effects of browser hijacking, users can do these measures:

- Checking the current add-ons, plug-ins and extensions and removing any suspicious or unnecessary programs.
- The user should reset the browsers homepage if he/she suspects that the homepage has been changed.
- The users should be careful when visiting different websites and delete their browsing history if they think that they visited any suspicious websites.
- The users should be careful not to download any software’s which they do not trust.
- Users should check that their antivirus program is up-to-date. This way users can be notified if they are about to download an untrusted software or visit a suspicious website.
(Distributed) Denial of service attack (DDoS)

One way to protect your system against Denial of service attack and DDoS is to prepare an incident response plan. This plan helps companies to deal with the aftermath of a cyberattack. Incident response plan helps the personnel to address the important areas. These areas include limiting the damage on the company. It also helps the company to implement the plan as soon as possible. This plan should be implemented as soon as possible. (TechTarget 2018.)

These steps help to complete the incident response plan:

1. Preparation. First step should include the preparation for potential incidents. Different computer user(s) should be ready in case of DoS
2. Identification. The staff of a company should try to determine whether the attack is a denial of service attack
3. Containment. The staff should try to isolate the systems which are already damaged by the attack
4. Eradication. The root of the attack should be found and then removing the affected systems
5. Recovery. Once the affected systems are removed the staff should try to fix the problem. Once the threat is gone these systems can be returned to normal.
6. Lesson learned. The steps which were taken during this plan should be recorded. If a similar attack occurs those documented plans can be used again.

Eavesdropping or man-in-the-middle (MITM)

Man-in-the-middle attack is a scenario where an outsider is listening conversation between two or more people. These conversations may happen through emails. These different people send messages to each other and a hacker tries to get the information out of these messages.

Spotting a MITM can be hard. It is important for network users not use any public networks. Public networks might not have a password. Because of the lack of password, public network user(s) can be an easy target for a cybercriminal.

One countermeasure against MITM is to use intrusion detection system (IDS): IDS helps users to monitor their network. If someone tries to get in or hijack your network, then IDS give an alert. It is possible that the IDS can act if it notices suspicious activity in the system. IDS can act if it notices that malicious programs are sent from questionable IP-addresses.
Intrusion detection system varies and therefore can offer different detection systems for its users. For example:

1. A network intrusion detection system (NIDS). NIDS offers a detection between different point(s). For instance, you can set up NIDS to a network which is used at home. This way you can check what is happening inside your network. You can also monitor traffic which comes outside of your network.
2. Anomaly-based intrusion detection system. In this type of IDS, the administrator sets different rules over the network. These rules can allow or block someone from the network. These rules may determine accesses points of the network. If an intrusion is detected, then this IDS compares the changes in the network to the rules. If something is detected the threat is deleted.

Spoofing

Spoofing is a situation where an outsider tries to gain sensitive information over the internet. This person listens conversations between different end points. These conversations may happen, for example, through email or skype. Spoofing can also happen when a user visits a website. For example, if a person wishes to login into his/her email a hacker may send a false website to this user. Once the user logs into the email account, the hacker gains access to sensitive information.

To prevent spoofing:
- You should use two-factor authentication. A username and password may not always be enough to protect your different accounts. A person could also provide a phone authentication as well. When login into an email account, a user can provide the usual username and password. And then enter a code which he/she gets from his/her phone
- A user should check the sites which he/she visits
- User should avoid giving sensitive information on the internet
- The person should avoid clicking email links or attachments which he/she find suspicious.

4 Case studies

This first example of a case study is from Cyber Crime & IT Fraud. The case study explains, in quotes, what cybercrime is. The case study also explains how computer(s) are used as weapons to commit crimes. Some of the examples are cyber terrorism and credit card fraud. Sometimes a computer can be target. Once the computer is hijacked it can be used to attack other computers. In the first section, the case study gives a few dates. It shows that the first recorded cybercrime happened in 1820. The first spam email was done in 1978.
The case study gives the types of cybercrimes. Some of the cybercrimes mentioned are:

1. Hacking (credit card)
2. Identity theft
3. Computer vandalism
4. Online fraud
5. Phishing

To prevent these types of attacks users should use countermeasures. The types of countermeasures are:

1. Firewalls
2. Operating systems should be up-to-date
3. Computers should have anti-virus programs up-to-date
4. Using strong passwords

This case study also shows the drawbacks of ransomware. Ransomwares may cause a company to lose data. Even if one device within the company gets affected it can be the cause of several blackouts. The company should keep the firewalls up-to-date. The employees/employees should be careful with emails. Companies should take back-ups of their data and secure those files.

Companies may face internal threats as well. These internal threats can be that a cybercriminal managed to get hold on credentials of a worker. There might be a worker within the company who intentionally injects the company's system with viruses and other harmful data. It is important that staff do not lose their credentials. With the credentials anyone can bypass the security measures. Workers have user account while working on the company. With this user account the worker can access to company's sensitive data. To prevent against these threats the company should implement multi-factor authentication.

These multi-factor authentications include a swiping card and a pin. If a worker wishes to enter a room where sensitive data, he/she must swipe a card in a card reader. After the card swipe the worker must enter a pin. The user might have to enter a password if he/she wants to enter the company's website. These passwords can be used only once. Once the worker signs in into the websites the pin expires immediately. These pins might be sent to requested phone or email.

The case study shows that a company can also do some staff training. The staff training may include some learning on using different passwords. Staff is suggested not to use any external passwords. This means that they should not use passwords which are being used in their personal emails. They should not use same passwords. It would be important that the worker knows about malicious emails and attachments. They should also be aware of malicious files and common file types. Common file types are, for example, .doc and .docx. When sending a word document these two should appear. When dealing with
pdf files .pdf shows a user that a file was sent on pdf format. Knowing these the company may protect against malware delivery.

This case study also shows examples where there were not enough protection mechanisms. First incident shows that there was a person whose Gmail account was hacked. The hacker sent a payment to the customer saying this person should pay 15k dollars to given bank account. Without knowing that this person was paying the amount to false bank account. The customer lost all the money.

Same type of incident happened to another client. This client email was hacked and then received a note that 3000 should be paid. There was an invoice sent and this client paid the requested amount. The invoice included the required bank account number. This bank account was fake. The client lost the money. (Hutcheon February 2018.)

Second example of a case study is from Cyber Case Studies: The Traditional Security Nexus. This case study begins with an introduction explaining how more people are depending and using online services. Because of this cyber security issues have become more and more important. Because of the increase of information online cyber criminals have learned to take advantage of the situation. They have learnt to use this information for their personal gain. The case study points out the increase on devices which people use to connect to the internet. These devices can be used, for example, either at home or work. These devices are not just pc, laptops or tables. There are devices, such as smart thermostat and fire-alarm, which can be controlled remotely.

The case study shows few areas which should be protected. One of these is called Personal protection. This area explains how different sites have started to collect information on the people who are registered. These sites can be site such as social networking sites and social media sites. If these sites have a lot of people registered that could mean that there is a lot of information collected. This information can be used, by cyber criminals, to blackmail people or use their identity. The case study gives a few examples. For example, an unknown group of terrorists was able to hack to Sony Online Entertainment. The hackers were able gain information from the CEO of Sony Online Entertainment. They gain information about tweets and sent a false tweet to American Airlines. The tweet said that one of the planes would contain a bomb.

The possible countermeasures against this could be to limit the amount of shared information. Another way could be to limit the amount people who can view your profile. These could be done by asking permissions from the user. The social media users should be
made aware about the information which is made public. This way the users can try to limit or change the information shown on their user profiles.

The case study gives more examples from different areas of protection. One of this area is called Information Security. This area explains how sometimes protecting your computers with the best protection system is not enough. The personnel need to consider other devices as well. These devices might be phones and printers. Hackers might gain access to company's printer and discover what a staff member have just printed. Mobile phones have cameras and microphones which a hacker can gain access to. This way a cyber-criminal can eavesdrop conversations or take notes from camera pictures.

To prevent these attacks the staff could make sure that all devices are up-to-date. The microphones within the phone could be switched off. Another way is not to take your phone when having a meeting. They can also cover the camera with a tape.

A third case study is called Personnel Case Studies. This case study focuses on the inside threat. Personnel must take different security assures when they are working with company's sensitive information. Cybercriminals try to target these kinds of workers. (OSCA 2014.)

5 Discussion

This bachelor's thesis is looking systematically at the computer threats and counter measures in the modern world. The issue is becoming ever so important when the digitalization of our economy and society is advancing, and these threats pose more and more economic, security, privacy and societal risks. In other words, computer risks are related to almost all aspects of the modern life.

This thesis focuses on attacks, risks and counter-measures of the individual computer uses and is not presenting and analysing directly for instance business-to-business computer risks and risks of maintaining public services and records. This focus was chosen due to the complexity and the dimension of the issue and the limits of the scope of the BSc thesis.

And this thesis is based on the information available in the literature and related articles and information sources. Conducting a questionnaire and/or interviews was considered but it was concluded that these would not bring much added value. Since the nature of the issue is very international, collecting additional information would be a challenge as
there is not much appetite to disclose publicly the sensitive and confidential information and rapidly changing environment for computer threats the thesis is based on the literature survey. And besides, there is already much and up-to-date information available for such a thesis.

Based on the work and analysis done following conclusion can be drawn:

- Major risks of computer attacks of an individual PC user are related to connecting to the unsafe and risky internet sites, making unsafe and risky payments through internet and opening unknown and risky attachments to emails. Users should be careful when connecting PC or mobile device to a public Wi-Fi.

- The consequences include viruses causing malfunctioning of the PC, computer hijacking, fraud payments and stealing information such as personal data. Credit card details and identities are being stolen. The users should be very prudent not to provide any confidential information such as bank account details, credit card information nor personal details to anyone without being sure that it is safe, and risks of misuse do not exist.

- The risks are similar when using PCs or mobile devices with specific features depending on the device and operating systems. Mobile users should be careful when attaching their email address to their phone. This makes the phone an easier target for a cybercriminal.

- The individuals using computers should be aware of risks of computer attacks and when using their PCs behave in a responsible and precautionary manner making sure that the protection is up-to-date all the time and avoiding any use which is suspicious and unknown.

- There are at least 6 major types of computer threats related to the individual computer use where threats and countermeasures are specific. The landscape is very dynamic and there is a race between the threats, their identification countermeasures.

- It is difficult to get any comprehensive information on the damage and costs related to the computer threats and attacks. Often, they are criminal and international and global by their nature and statistical and complete information does not exist. However, anecdotal evidence suggests that the economic, security and fraud impacts are significant and on the rise. Overall, some estimate suggests that the damage related to cybercrime is going to rise to some USD 6 trillion in 2021.

- The computer risks and attacks are one factor which limits the possibilities for further digitalisation of the economy and society with all the efficiency gains and benefits it could bring about. That is why it is important to fight against them with all necessary national and international co-operation and measures. The IT-companies have a special responsibility in the fight being best placed to prevent computer risks and attacks when designing and maintaining hardware and software.

- The fight against computer risks and threats requires intensive EU and international co-operation and rule setting. The phenomenon is international and global and criminal organisations and hackers operate globally, and thus the response
also needs to be global. Key players are governments, IT-companies but also law enforcement authorities and police. All these needs to have a knowledge and expertise and tools for addressing risks and threats.

- If not properly and effectively managed computer risks and threats can become a major national and global economic, social and security risk and prevent the digitalisation process.
References


Youngupstarts 2016. 9 Types of computer viruses that you should know about – and how to avoid them. URL: http://www.youngupstarts.com/2016/04/14/9-types-of-computer-viruses-that-you-should-know-about-and-how-to-avoid-them/. Accessed: 02.05.2018