

CYBER SECURITY

Home user's perspective

Mikko Ikonen

Bachelor's Thesis of the Degree Programme in Business Information Technology
School of Business and Culture
Bachelor of Business Administration

2014

Lapland University of Applied
Sciences
Degree Programme in Business
Information Technology

Author	Mikko Ikonen	Year	2014
Supervisor(s)	Juha Meriläinen		
Subject of thesis	Cyber Security - Home user's perspective		
Number of pages	52		

Cyber security is important to understand for home users. New technology allows for new cyber threats to emerge and new solutions must be considered to counter them. Nearly every device is connected to the Internet and this opens new possibilities and threats to cyber security. This Bachelor's thesis explores the different aspects of cyber security and suggests solutions to different cyber security issues found.

The different aspects of cyber security under research here include personal privacy, mobile devices, personal computers and online services. Each aspect is analyzed for potential cyber security issues and solutions are presented on the basis of the analyses.

The cyber security issues and solutions are presented with the home user being in the focus. This means that the issues discussed will avoid difficult technical terms and provide explanations when necessary. Exploratory research is used as the main research approach through literature review of relevant literature and articles.

The findings in this Bachelor's thesis indicate that there exists no perfect protection against cyber threats. Protection is not only technological as the human component is equally important. Human vulnerability is often exploited by modern cyber-attack. These threats are mitigated by both personal action and technological solutions. There do exist threats that can compromise cyber security without human interaction but the human is most commonly the culprit of the incident. The criminals behind these attacks are highly skilled and able to fool most home users into compromising their cyber security.

Key words

Cyber security, threat, vulnerability, privacy

CONTENTS

ABSTRACT

FIGURES AND TABLES

1	INTRODUCTION	5
1.1	Background and motivation	5
1.2	Scope, objectives and research questions.....	5
1.3	Methodology and limitations	6
1.4	Structure of thesis	7
2	CYBER SECURITY	8
2.1	What is Cyber Security?	8
2.2	Role of the user	9
3	PERSONAL PRIVACY	10
3.1	Identity Theft.....	10
3.2	Mobile Devices	11
3.3	Online Tracking.....	15
4	THREATS AND SOLUTIONS.....	19
4.1	Mobile Security	19
4.2	Personal Cyber Security	21
4.2.1	Malicious Software	21
4.2.2	Scamming and Phishing.....	24
4.2.3	Passwords.....	26
4.3	Computer Security	29
4.3.1	Anti-Virus Software.....	29
4.3.2	Automatic Updates	36
4.3.3	Firewall.....	41
4.4	Network Device Security.....	45
5	CONCLUSIONS	47
	REFERENCES	49

FIGURES AND TABLES

Figure 1: Flashlight application for Windows Phone	11
Figure 2: Windows Phone security features.....	13
Figure 3: Find My Phone feature demonstration (Microsoft, 2014a)	14
Figure 4: User Agent information (What's My User Agent, 2014)	16
Figure 5: Example spam E-mail.....	22
Figure 6: Fake Microsoft lottery.....	25
Figure 7: Fake Facebook notification.....	26
Figure 8: Microsoft Security Essentials	30
Figure 9: Avira Free Antivirus.....	31
Figure 10: Avast Free Antivirus.....	32
Figure 11: Avast statistics	33
Figure 12: Avast for OS X (Bradley 2012).....	34
Figure 13: ClamAV Graphical User Interface	35
Figure 14: ClamAV command line scan.....	35
Figure 15: Windows Update settings	36
Figure 16: Windows Update.....	37
Figure 17: Detailed Windows updates	38
Figure 18: Ubuntu Software Updater	39
Figure 19: Ubuntu update settings.....	40
Figure 20: OS X Updates (Apple 2014a)	41
Figure 21: Windows Firewall main window	42
Figure 22: Windows Firewall allowed programs.....	43
Figure 23: Windows Firewall Advanced Security	44
Figure 24: Iptables default policy	45

1 INTRODUCTION

This chapter discusses the background of this thesis topic along with motivation, objectives and structure of the thesis. The scope, research questions and methodology are also discussed.

1.1 Background and motivation

Cyber Security has become increasingly important to the normal everyday user. The increased opportunities granted by today's technology also bring about new security concerns that must be taken into account. Home user's need to be aware of the risks involved in using today's cyber technology where an increasing number of the everyday items they come in contact with are connected to the Internet. As everything is moving to the internet, it opens new ways for criminals and government officials to compromise the user's cyber security and privacy. This thesis focuses on these issues and their solutions. The motivation of this thesis is the need for cyber security strategy for home users which can be read and understood by anyone. Personal interest in the topic also influenced its selection.

1.2 Scope, objectives and research questions

The scope of this thesis research is narrowed down to include home user cyber security. The thesis research focuses on recent cyber security issues and countermeasures for home users. This research excludes corporate users as they are not within the framework of this Bachelor's thesis, but will include discussions of some cyber security from corporate information systems' point of view in order to find security practices that could be adapted for home users.

The scope has also been narrowed down to include only the basic definitions of cyber security threats as the research is focused on their implications and not their technical aspects. The research work is fully theoretical, thus it does not contain any practical implementation.

The objectives of this thesis are, firstly, to describe the aspects of modern cyber security with emphasis on the importance to home users. The second objective is to describe current cyber threats that affect home users and how to protect against them. The third objective is to suggest a strategy based on the findings, to aid home users to avoid potential security concerns.

The following questions were defined for this thesis in order to achieve the objectives of this research.

1. What are the latest threats to home users in regard to cyber security?

This question aims to answer what cyber security threats home users and their information systems face in today's world. The knowledge to answer this question is based on analyzing relevant literature.

2. What is the impact of these latest security threats on home users and how could these threats be avoided?

This question seeks to find out how the latest security threats have impacted on home users and what measures are available to protect against them. This question can be answered by analyzing literature and studying existing security solutions.

1.3 Methodology and limitations

This thesis research uses the qualitative research method due to it being suitable for fully theoretical research work. Glenn (2010, 96) states that qualitative research is exploratory and thus creates hypotheses. This led to this research work also using exploratory research because it is the most suitable approach for this kind of research.

Exploratory research was chosen because this thesis research requires acquiring knowledge about topics that may not be clearly defined. (Sachdeva 2009, 14.) The exploratory research approach is complemented by qualitative

research methods with the focus on literature review as exploratory research alone can provide only insights and not conclusions. (University of Guelph 2014.)

The limitations of the thesis research are the ever changing cyber security threats and vulnerabilities. Not all vulnerabilities are documented and new ones may be found at any time and this research cannot discuss undocumented issues which were not public knowledge at the time of writing. Exclusion of corporate users could be considered as a limitation, but the scope still allows some aspects from the corporate world to be incorporated in this thesis research.

1.4 Structure of thesis

The thesis is structured into five main chapters. The second chapter focuses on general aspects of cyber security and the role of the user in it. Privacy of the user is discussed in the third chapter. Fourth chapter is focused around the different cyber security threats the user might face and how they could solve or mitigate them. Fifth chapter concludes the findings of previous chapters and proposes ideas for better home user security.

2 CYBER SECURITY

This chapter defines and explains the concept of cyber security and its various aspects. Role of the user in the context of cyber security and the problems with their personal privacy are also discussed.

2.1 What is Cyber Security?

Cyber security is very close to traditional information security by definition. The only difference is that cyber security focuses on cyberspace instead of including physical security. IT Governance Ltd defines cyber security as the protection of networks, systems and information in cyberspace. (IT Governance Ltd 2014.) Cyberspace, according to Limnéll, Majewski and Salminen (2014, 29) means the artificial world created by humans which contains the internet, social media, computer networks and systems and even Smartphone software. Regarding the definition of cyber security, Limnéll et al. (2014, 30-31) also point out that the word "cyber" was made to represent the protection of information also during transit and not just a term for protection of stored information as was the case with information security. They also consider the word "cyber" to better describe the cyberspace in today's world when compared to other terms Limnéll et al. (2014, 30-31). This is related to the general confusion on what cyber security is in relation to other terms such as information security.

The three domains of information security can still be applied to cyber security. These are confidentiality, integrity and availability. The three domains according to Järvinen (2012, 10) can be defined as follows: Confidentiality means that information like e-mails and personal information must remain confidential when necessary. The information must be available only to authorized personnel and access to it be restricted for example by passwords, access rights restrictions and encryption algorithms. Integrity is defined as the information not being allowed to change during its processing and usage. Only authorized changes are allowed. E-mail viruses are one example of the loss of integrity. Finally,

availability means that information must be available when needed while this is not always easy due to hardware and software faults. (Järvinen 2012, 10.)

A frequently asked question is who the people who seek to breach cyber security are. Criminals and government officials each have their own agendas on why they would like to get an average user's information for themselves. Reasons behind these actions range from national security to profits through personal information. This topic will be discussed further in the chapter to follow.

2.2 Role of the user

Today nearly everyone owns some kind of device that is connected to the Internet either at home or at work. Consequently, cyber security is also very important for these people and this also leads into problems. Järvinen (2014, 174) points out that most Finns are of the opinion that the best protection against international espionage is their own insignificance. While this is true in the case of espionage, cyber criminals do not make any difference between geographic locations. Järvinen (2014, 179) further points out that the common misconception for Finns is as follows: "I don't have anything to hide". However, everyone has financial, medical, relationship and password information that they would want to keep secret. This belief of insignificance further leads to cyber security not being only a technological issue but the user also playing a major role in it. Limnell et al. (2014, 13-14) state that as people become increasingly dependent of cyberspace, so does increase the safety requirement of it. It is also pointed out that cyber security is not only for a small group of experts, but it involves everyone and everyone is also responsible for it. Cyber security is also a strategic and political concept, and not just technological. Limnell et al. (2014, 14.)

3 PERSONAL PRIVACY

This chapter will discuss the various means of how users can be tracked, how information can be acquired and what can result from it.

3.1 Identity Theft

Identity theft is one of the major risks to personal privacy. There exists two kinds of identity theft according to Järvinen (2012, 256-258). First is assuming identity of another person for parody or anonymity purposes with no specific goal to harm this person. This type of identity theft is not illegal and authorities have little power in stopping it. It also causes little damage to the victim apart from mental malaise. It is considered illegal only if the fake identity is for example used to insult the real owner's honor, or spread information protected by the privacy act. This information is based on Finnish legislation. (Järvinen 2012, 256-257.) Legal limitations may vary depending on country.

The second, more dangerous form of identity theft is the intent to do fraud by assuming some other person's identity. Personal information can be acquired from social media or public registries, and credit information can be stolen from users. Together these form the foundation for fraud by assuming the identity of the victim. The fraudster can for example place orders, do payments or even open a new mobile number with the stolen identity information. The fraudster can also use the stolen identity to contact the friends of the victim in an attempt to steal even more information or fiscal assets. This can be very devastating for the victim as cleaning up his or her name and credit history is a difficult and time consuming process. This type of fraud is considered illegal. (Järvinen 2012, 258.)

3.2 Mobile Devices

Mobile devices are one group of devices many might not realize to be such a potential source of information. Phone calls, messages, E-mail and social media are all tied to modern mobile devices and users carry them with them always. Since they are always with the person carrying them, they are easy to steal or forget somewhere. Risks to privacy then arise from losing the device to another person or having the calls be eavesdropped on. The mobile phone contains its owner's personal life in a miniaturized form. Järvinen (2012, 30.)

Further issues to privacy arise from the endless supply of different mobile applications that are available at the respective application stores. Users should always read what information the application will collect and refuse installation of software with questionable privilege requirements. (Järvinen 2012, 55.) Figure 1 below shows a real world example of a flashlight application for Windows Phone devices which requests suspicious privileges.



Figure 1: Flashlight application for Windows Phone

The figure reveals that the application is requiring more privileges than what a flashlight application needs to function. The application would need only video and still capture to access the camera flash in order to function. Everything else is unnecessary. It can be assumed that the remaining requirements are tied into advertising to profit from the free application. There exists non-profit variants of this application that do not require anything but the one required requirement.

Järvinen (2014, 296) points out two examples where applications collected more information than what the users were aware of. Application called Brightest Flashlight Free collected information about users and forwarded the information to advertisers. The application had been downloaded over 50 million times. The second application is the popular mobile game Angry Birds. The advertiser partner of Rovio the developer of Angry Birds used a user profiling system for targeted advertisements. The system collected information about the users and there is suspicion that the US National Security Agency may have gained access to the collected information as well. (Järvinen 2014, 296.) These examples reveal that applications are able to collect information about users and that the information collection could be avoided by not installing them.

There are methods to improve personal privacy of mobile devices. Most phones carry numerous security features that commonly are left unused. Most basic protection comes from the subscriber identity module (hereinafter SIM). Most commonly known as the SIM card. The personal identification number (hereinafter pin) and the personal unblocking code or PIN unlock key (hereinafter puk). They are not made to protect the phone, but to protect the mobile subscription on it. Both are features of the SIM card. The pin code is a numeric password which is used to unlock the phone when it is powered on with the SIM card in it. After three failed attempts to enter the correct pin code the puk code will be required to unlock the phone. After 10 failed attempts to enter the puk code, the SIM card will destroy itself and it cannot be recovered after that. (Järvinen 2014, 40-41.) It is possible to disable the pin query which is not recommended. The protection provided by the SIM card is still limited however as the card can be removed.

Järvinen (2012, 41-43) states other methods to protect mobile information as follows: First method relates to the SIM card. It is possible on some mobile phones to lock the phone if the SIM card has been changed. The phone would then query the security code or password. The feature is not available in all phones but the functionality can be achieved through 3rd party security software. The same security code can be used to secure the touch screen thus preventing unauthorized use and accidental interaction inside a pocket. The second method is the possibility to use a figure password for the screen. The same password will also function like the administrator password of computers. The password protects the phone management settings such as firmware update and resetting data counters. Third method is remote locking which is another safety feature that is available either in the phone operating system itself, or as a 3rd party service. It allows locking the phone through the internet or with a text message. Remote wipe is related to remote locking, but wipes the personal information on the phone instead of locking it. Figure 2 below shows the security features built into Windows Phone mobile phones.



Figure 2: Windows Phone security features

It can be seen from the figure that Windows Phone devices can be remotely located, locked or wiped with no 3rd party software needed. Locating the phone was tested for this Bachelor's thesis and the following figure 3 fabricated from Microsoft (2014a) illustrates what the website looks like after issuing the command to find the phone.

Find My Phone

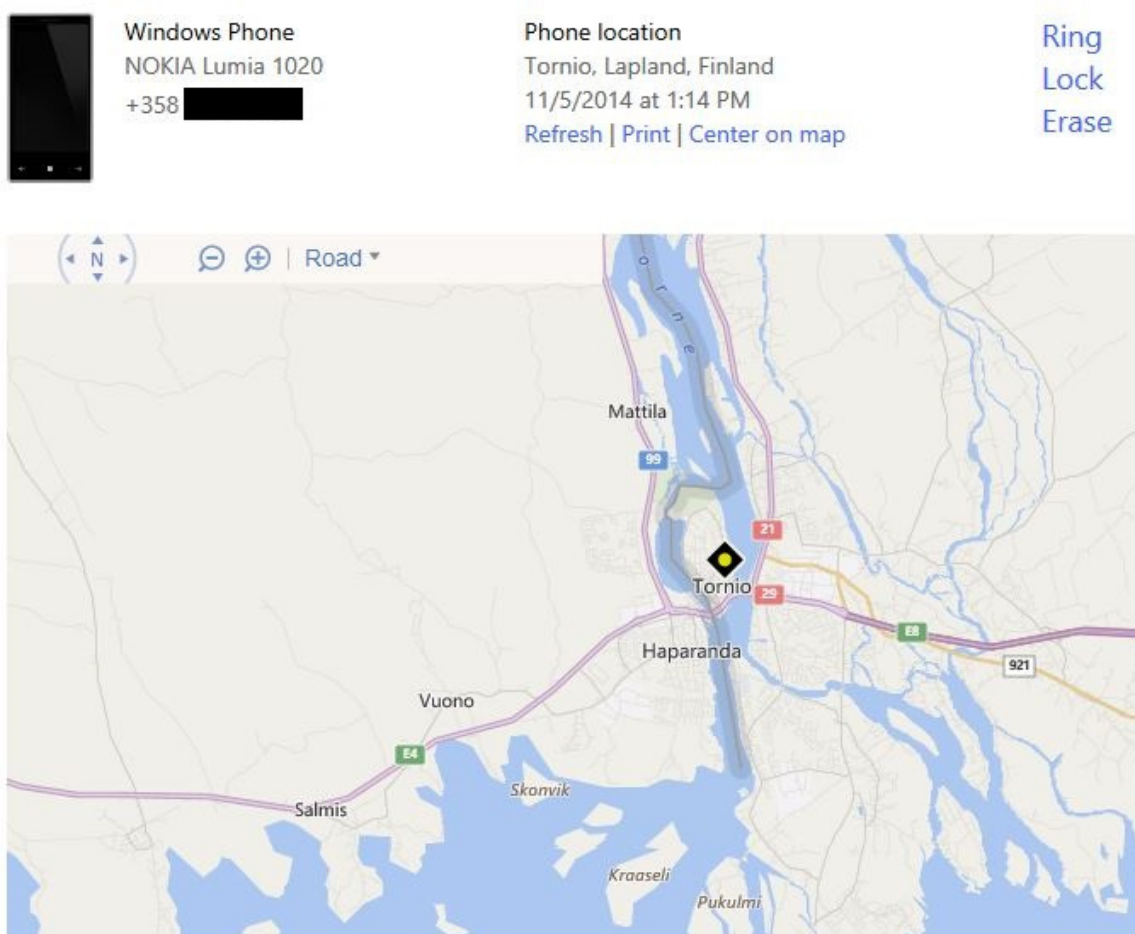


Figure 3: Find My Phone feature demonstration (Microsoft, 2014a)

The mobile phone can be accurately located from nearly anywhere in the world as the figure shows. The map can be zoomed in and out and spans the entire world. E-mail was also sent to the registered address with a link to the map.

All of these features provide good protection against outsiders accessing the information in mobile phones, but they have to be used if they are to be of any use. Many users do not use any of the security features and leave the pin number to the operator default which is commonly 1234 or 0000. These default pin numbers are the two most commonly used pin numbers according to Muller (2011.)

3.3 Online Tracking

Tracking on the internet is very common and is usually harmless, but there are still risks to personal privacy. Järvinen (2010, 161) states that everything done on the internet leaves a trace. Users are commonly told how every action can be investigated and analyzed but this is not true. No individual party can access all the different traces due to the wide spread of them. Järvinen (2010, 161.) The decentralized nature of the traces thus makes it hard to identify any single user.

There exists multiple traces which users leave behind on the Internet. IP address is one of the most common traces left behind by the user. According to Crawford (2014), IP address is a unique identifier for every device on a network. The IP address is essentially the address of a device on the Internet. There are static and dynamic IP addresses. Dynamic ones are the common ones used by everyday users. Static addresses do not change, while dynamic addresses do. Järvinen (2010, 164) maintains that IP address alone cannot be used to effectively identify anyone. It is possible to assume what organization the user is from and determine roughly the geographic location, but IP address might change so different user gets the same address later on for example. To help identify users, tracking cookies were developed. (Järvinen 2010, 164-165.)

Cookies are files stored on the device by the web browser. Cookies hold information relating to certain visited websites. The purpose of cookies is to identify a user when they revisit a website. (PC Tools 2014.) Järvinen (2010, 166) states that cookies are harmless and beneficial for the user. Since the

remote server that creates the cookie, they cannot know anything more about the user than what they already know. The more concerning part about cookies is if they are poorly implemented and contain partially confidential information instead of numerical identifiers. If such cookies were lost to a malicious party, the personal information included with them could be revealed. Third party cookies which are used by advertisers can show what websites the user has visited, but are not able to collect any personal information. (Järvinen 2010, 166-169.)

Cookies are also used for analytics and targeted advertisements. Large online services are interested in knowing usage statistics and how these statistics could benefit their advertising. The analysis can include country and city, popularity of certain pages at certain times and the information concerning how the user came to visit the site. (Järvinen 2010, 175-176).

Other information about the user can be acquired through the use of header. The header is transferred to the web server in a field called user-agent. This is done when navigating to a web page begins. The information in user-agent contains the used operating system and web browser. Figure 4 below adopted from What's My User Agent (2014) shows an example that shows the user agent information.

Analyze User Agent String

Elements of Your User Agent String:

Mozilla/5.0	Mozilla version 5.0 Originally indicated the Netscape web browser, now a generic term which most modern browsers use
Windows NT 6.1	Windows NT version 6.1 Windows 7 (or possibly Windows Server 2008 R2)
WOW64	WOW64 version 64 bit Windows-On-Windows 64-bit. A 32-bit application is running on a 64-bit processor.
rv:33.0	rv:33.0
Gecko/20100101 Firefox/33.0	Gecko version 20100101 Firefox/33.0

Figure 4: User Agent information (What's My User Agent, 2014)

The figure reveals the user-agent information of an example computer. Browser information and operating system has been identified by the website.

Preferred language of the web browser is also sent to make it possible for websites with international content to adjust automatically. JavaScript is used to gain further information such as screen size and color information, time zone, size of the browser window and installed fonts. The header will also forward the address of the last page visited when a user clicks a link on a website and is forwarded to another web page. This is called referer information. The original developer misspelled the name and it is difficult to change now that it is standardized. Web bugs or clear gifs are yet another method of tracking. They are one pixel sized transparent pictures which are loaded from other servers thereby causing a log entry when the page containing the web bug is loaded. The log entry contains the IP address of the user and the web bug may also deliver cookies for future identification of the user. Web bugs can also be embedded onto e-mail messages for the example advertisers to know if their e-mails have been opened or not. The web bugs do not need to be sized one pixel. They can be a logo or any prominent picture on a web site or e-mail. (Järvinen 2010, 176-182.)

The uses of JavaScript were discussed previously in this chapter. However, in addition to the uses discussed, JavaScript has further uses. It can be used to read the clipboard where copied material exists when the command is issued on Windows operating systems. This feature is available in Internet Explorer. It will by default ask the user's permission to use the clipboard, and the feature can also be turned off in the settings. It is also possible to determine previously visited addresses, but this is a slow process. (Järvinen 2010, 183-185.)

When all the information collected through these different methods is combined, it is possible to draw a quite clear picture about the user. Richmond (2013) states that this process is called "Web based device fingerprinting" where the information is used to create a cookie-free unique identification. Järvinen (2010, 185) points out that this form of tracking is difficult to detect and also makes

opting out of it very hard. Järvinen (2010, 185) further points out that through the device fingerprint the same user can be identified very reliably even if their IP address were to change and usage of cookies were forbidden.

There are ways for users to make it more difficult for outside parties to identify them and collect information. One of the easiest and also free solutions is a browser add-on called Adblock Plus. It blocks advertisements that it categorizes as "annoying" while keeping certain acceptable advertisements visible. It can also be used to disable tracking done by websites and to block malicious domains that are known to spread malicious content. Social media buttons can also be disabled and it also offers typo protection to prevent navigating to malicious websites by mistyping a safe website's address. (Adblock Plus 2014.) Järvinen (2010, 194-195) also points out two services where users can opt out of tracking cookies, i.e. Network Advertising Initiative and Targeted Cookie Opt-Out.

There exists other solutions too but the examples presented in this Bachelor's thesis were primarily selected due to their ease of use. This does not diminish the value of other solutions in any way however. Everyone is free to use what solutions they want to. No solution may provide perfect protection though. There exists no such application or browser add-on which would make someone truly anonymous. A lot of information collected is used to provide improved and targeted service towards the user, but it is each one's own choice whenever he or she want to provide this information or attempt to prevent it from being gathered. The solutions exist to provide the user with this choice. There are some malicious intentions too on the internet, but majority of the information collection is for common benefit.

4 THREATS AND SOLUTIONS

This chapter discusses the more active and targeted cyber security threats in comparison to what has been previously discussed in this thesis. Users might face these threats when interacting in the cyberspace. While the previous chapter focused on privacy and passive issues such as information collection, this chapter discusses active threats with the intent on harming and compromising the user. It will also discuss how to protect against such threats.

4.1 Mobile Security

As indicated in the previous chapter, mobile devices contain lot of personal information and provide much easier opportunity to profit through them. Felt & Wagner (2012, 169) state that consumers would say phones were not computers and experts would say that they are. Phones are like computers though and are vulnerable to malware for example. Money is what criminals are after and the phone is where the money is in this context. Järvinen (2012, 53) points out that phone malware could cause much greater damage than one in a computer by for example making calls to a number that charges money and then publishing all the personal information of the unfortunate victim. Work related files could also be sold to other companies.

Mobile malware can be categorized into four different major categories according to DuPaul (2013) as follows: First is Spyware and Adware. These are installed without user interaction by being disguised as a harmless application or by infecting other applications the user is downloading. The aim of these type of malware is to collect personal information and transfer them to a third party. They may also gather information about the device in order to allow easier deployment of future attacks.

The second category is Trojans and Viruses. These infect devices the same way as in the first category. By software that seems harmless. These types of

malware are capable of taking more direct control of the device by hijacking the browser for example or by sending texts and capturing login information.

Viruses are the more severe form of the two and they can even access the system files. This could create irreparable damage for the user.

The third category is phishing applications. This contains all the tools fraudsters use in the mobile world. They range from mobile phishing sites to mobile applications with Trojans in them. Infecting otherwise safe applications is also not unheard of. The aim of the phishing is to gain personal information or money through stealing login credentials or through other means.

The fourth category is bot processes. They are hidden processes that can be activated by remote order and remain hidden from the user. Their capability is currently limited, but they are expected to develop to be more dangerous in the future.

According to Järvinen (2012, 54), the fact that mobile phones are tied to the official application marketplaces is a good security feature. While it limits the choice for the user, it also improves security. Applications are checked before they are released to the application marketplace. Majority of mobile phones forbid installation of software from 3rd party sources by default. (Järvinen 2012, 54.) Mobile anti-virus software is also available depending on used platform and it is highly encouraged to be used. Users should install such security software as malicious software is becoming more and more common. Users also tend to install applications without reading reviews or what permissions they are giving to the software.

Terms of service or license and privacy policy texts are also ignored as they are usually long and therefore take a long time to read and to understand. These actions allow malicious content or unwanted information collection to take place in the mobile device. According to Sauro (2011) license agreements are also not read because using the software requires accepting the license meaning there is no choice for the users if they want to use the software.

4.2 Personal Cyber Security

Personal cyber security in the context of this subchapter means any risk or threat for the user that may arrive through cyber space. These include for example viruses, scams and phishing. Solutions are also presented which will help reduce the risk of compromising one's cyber security.

4.2.1 Malicious Software

Computer viruses, Trojans, worms and similar are still common in the cyber space and will most likely continue to be in the future. Malicious software such as these often rely on two methods of interaction with the host device. These are subterfuge and causing rapid damage that can be visually seen on the computer operating system. The more subtle actions of such software include capturing key strokes to steal login information and sending spam messages using the computer. They may also add the computer to a botnet where it can be used to do denial of service attacks for example. Users may not notice these actions till their service provider notices the malicious traffic and sends a notice to the user. The non-subtle software may destroy system files, prevent certain software from working, or even encrypt all files and demand payment for the decryption key. This "ransomware" has been popular for some years already and recently they have been localized to look as if they were coming from a local law enforcement agency.

There are many methods how these malicious software, or malware as they are also called, find their way into the computer. Järvinen (2012, 181-187) suggests some potential methods discussed below.

First method, i.e. the E-mail, is the classical method for many viruses to infect computers. Users are often fooled by interesting and relevant content to open malicious attachments. In some cases there may also be a link to a site where the user is further tricked into downloading and installing malicious software. Tricking the user is a major factor as users have learned to be cautious about

unknown E-mail attachments and no longer open them so easily. This is why modern spam appears to look like something important to the user. (Järvinen 2012, 181-182.) Figure 5 below depicts a spam E-mail which had virus attachment on it.



Figure 5: Example spam E-mail

This message is a fake court hearing request with malicious attachment. While this example does not follow the interesting or relevant content practice, someone somewhere is still going to open that attachment and risk their computer. In this case Windows Live Mail application automatically removed the malicious attachment but very often web-based mail services have very limited virus protection or none at all.

The second method is compromised web sites which will infect computers that have vulnerable browsers or browser add-ons. The malicious software can be downloaded and installed onto the user's computer with no interaction required from the user. This makes this method dangerous as the user will not know that the website has been compromised. A subset of this method is websites that

are built to infect computers. (Järvinen 2012, 183-187.) Websites that deliver illegal or otherwise questionable content are popular for this method.

The third method is browser add-ons. Malicious add-ons may have partial control over the browser and may thus capture passwords, deliver additional advertisements or manipulate what web sites the user is navigating to. These add-ons also commonly change the home page of the browser and may also select different search engine to be used. (Järvinen 2012, 187.) Toolbars are very common form of such add-ons, but there exists also invisible ones that can only be seen in the list of installed browser add-ons.

The steps required in preventing most infections are simple and there are many similar lists available on the internet. United States Computer Emergency Readiness Team (2012) recommends usage of anti-virus software and firewall. They also recommend not running unknown programs or opening unknown e-mail attachments. Users should also keep the operating system and all applications up to date and disable or uninstall unneeded browser add-ons. (United States Computer Emergency Readiness Team 2012.) Not using an administrator account in everyday computer use will also help prevent some infections as the normal user account generally does not allow installation of software or changes to system files.

In case of infection there are ways to attempt solving the issue if the currently installed security software is not able to remove the malicious content or if there is no such software installed. F-secure provides a free to use online scanner which can remove most viruses and other forms of malicious software and they also provide instructions to remove ransomware if the user has fallen victim to that (F-Secure 2014.) In the event that payment is demanded in any form to remove the malicious content, it is not recommended to pay. This is nearly always a scam and will not actually remove the infection. Such extortion is popular method for criminals to make money and helping the user is not in their interests.

Users should also be aware that there exists fake security software which will claim there are problems in the user's computer and often require payment before these problems are fixed. This also falls into the category of scam and these types of software may actually infect the computer with other malicious software. These software are often categorized as scareware. (Järvinen 2012, 215-217.)

Protection against malicious software can be difficult due to the different aspects involved in it. For example, everything needs to be kept up to date, anti-virus software should be used and it is recommended to do the virus scan regularly. Many home users may not be aware of all these different pieces that form the overall cyber security for them while their actions also play a part as they use e-mail, online services and browse the internet. Yet one weak link in this chain may compromise them.

A majority of malicious software target Windows users due to its popularity but this does not mean Linux or Mac OS X are completely safe to use either. Harrison (2014) points out that malware for Mac do exist but they are few and that the Unix-based architecture of OS X itself makes it more difficult to infect it. However, it can be infected though. Concerning Linux, Wallen (2010) maintains that there exists malicious applications and root kits for Linux and that the latter can be very difficult if not impossible to remove once an infection has occurred. Both operating systems are safer to use than Windows machines, but there is no guaranteed safety there either.

4.2.2 Scamming and Phishing

Various scams and phishing attempts are also a never ending menace to the user. E-mail is the most common method used in spreading them. Promises of money, love or very cheap products are in this case too good to be true. Many internet advertisements are also scams along with claims of having won something or being the thousandth user visiting. (Järvinen 2012, 162-167.)

Common sense is the best protection against scamming. Thinking about the situation often results in the scam becoming obvious. Järvinen (2012, 159.) Figure 6 below reveals example title of a fake lottery.

The image shows a screenshot of an email header. The main text is "CONGRATULATION!! You've Won The Lottery." in a blue font. Below it, in a smaller black font, is "MICROSOFT LOTTERY (info@condomtsq.org) Add contact". The email address "info@condomtsq.org" is clearly a misspelling of "info@microsoft.com".

CONGRATULATION!! You've Won The Lottery.
MICROSOFT LOTTERY (info@condomtsq.org) [Add contact](#)

Figure 6: Fake Microsoft lottery

The figure shows a very poorly done scam E-mail title where the user is told they have won the Microsoft lottery. The sender address doesn't look like Microsoft official address which alone is suspicious.

Phishing is different in the regard that they are usually targeted meaning they are for services the particular user is using. They usually attempt to get login credentials or credit card details by using fake websites that look like the ones belonging to the real service. Banks and payment services such as PayPal are very popular topics to phish with. (Microsoft 2014b.) When it comes to the targeted phishing, users should remember that banks and other internet services never ask login or credit card information over e-mail or by any method. These types of requests are nearly always fake and are attempting to steal information from the users. The fake websites may look just like the real one, but the address of the site will give it away. The following figure 7 will show an E-mail phishing attempt of Facebook login credentials.

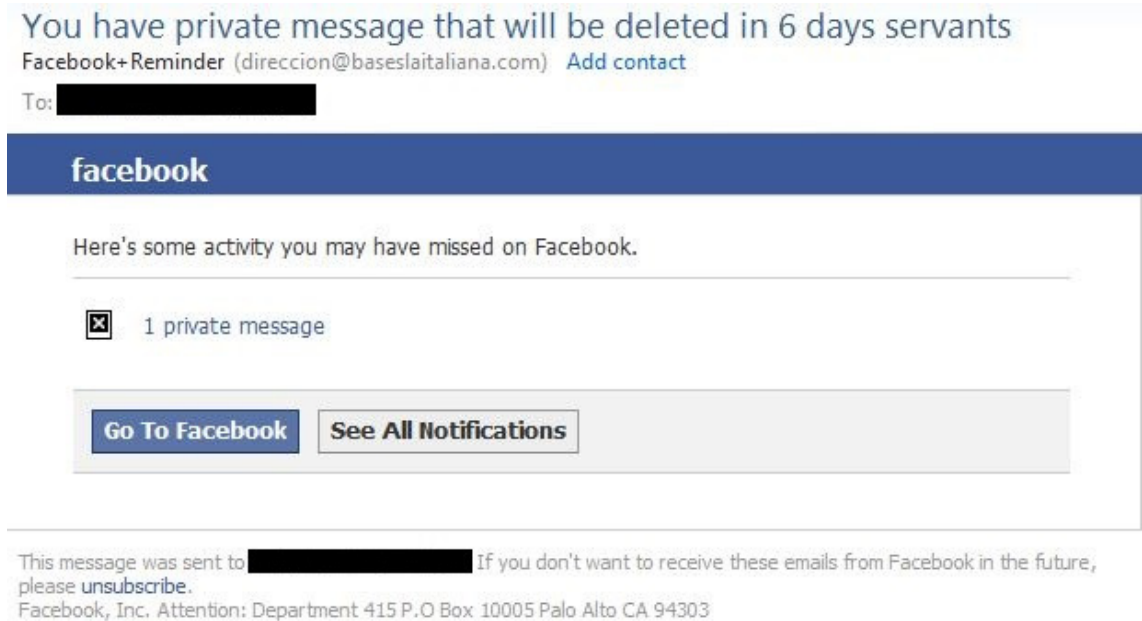


Figure 7: Fake Facebook notification

This is a skillfully done fake notification where all buttons and links take to a fake Facebook login page. The fraudster would steal the login information should the unsuspecting user try to enter them there. The phishing attempt in this case can be identified by the strange title and sender address. The address this message was sent to does not have a Facebook account associated to it which shows that these attempts are not targeted but attempt to benefit from the widespread popularity of the service.

4.2.3 Passwords

Passwords are the bane of nearly every user. A password is required for nearly everything and keeping track of them can be difficult. (Granger 2002.) There exists so many different services where users have passwords and this leads to problems with cyber security as the users do not use good password practices. While different password for every service is encouraged, it is still very common for users to reuse same passwords everywhere. Loss of account at some online service may therefore enable further loss of accounts and personal information.

It is said that the current password guidelines that are repeated everywhere do not make sense in all situations. The common guidelines for example say that passwords should be between 8 and 15 characters and contain special characters and numbers. Also the password should not be written down anywhere. The requirements can be considered to be so strict that not even their creators can follow them all. (Järvinen 2012, 113-114.) For home users there is little harm in writing down on paper the most important passwords. That after all is the place where no cyber-criminal can never gain access to it. It should still be kept safe from burglars though. Length of the password does increase the time it takes to guess it through brute force attack but there is some room for common sense here as well. Järvinen (2012, 116) states that adding one normal alphabet character to a password multiplies the password breach time by 28 times. He also states that adding a special character multiplies it by 20 times. This results in adding one normal character from a to z being more secure than adding one special character. The 28 times multiplier is including Scandinavian specific characters such as 'Å', 'Ä', and 'Ö'.

Regular changing of passwords could be considered excessive too in the context of home users. Järvinen (2012, 116) points out that it is highly unlikely for passwords to be revealed without the user knowing. Even if this does happen, the attacker will be able to utilize the advantage provided by it very quickly, thus invalidating the added protection of password changing. Continuing misuse usually happens only within family through current or former spouse. Online services are usually good at identifying misuse from foreign locations and locking such accounts. February 1st is the national 'change your password day' which is a good day to change all passwords. (Järvinen 2012, 116-117.)

Services can be grouped by importance. Most important services would get the most secure passwords which would be changed when it feels necessary. With least important services there would not be any password changing at all unless there was a proper reason for it. (Järvinen 2012, 118.) Good reason would be

for example the "change your password day" which would still have all passwords changed once per year by minimum.

Password managing software can also be used to store passwords. Usage of such program requires only remembering the master password which allows seeing all passwords stored in the program. This eliminates the need to remember all passwords for different services but also poses a risk. It will be difficult to remember passwords that do not need to be written manually. The master password itself could be forgotten or it could end up in wrong hands. As the program is not on a foreign computer, it is still needed to remember the passwords when on such computer. Web browsers also provide the functionality to store passwords and fill login information automatically, but by default the list of passwords is not protected by any way and anyone using the computer could view all the stored passwords. Therefore it is critical to define a master password that prevents viewing the list without first inputting the password. (Järvinen 2012, 130-133.)

What to avoid when creating passwords is still the same. No dictionary words or obvious alphabet to special character conversions i.e. cash -> ca\$h. Not using the username as password or typing it backwards. Rows of characters and numbers from the keyboard are also bad passwords. Automated breaching tools and educated guesses make these trivial to breach. Names of pets, family members and birthdays or other dates of important events also make poor passwords as for example social media makes it easy to find such information. Järvinen (2012, 118-119.)

Password reset mechanisms are unfortunately weak security wise. According to Järvinen (2012, 128), security questions are easy method of break in i.e. they provide generic and easy to guess default questions and answers to those can commonly be found in the social media. The usual names of pets, middle names and school names are common sight in most security questions. Nothing forces the user to stay in truth with the security answer though. The best security then is to make incorrect answers to security questions that only the

user remembers. These answers cannot be found in the social media and thus provide actual protection to the password. (Järvinen 2012, 128-129.) Strong password for e-mail is also important as that is where resetting passwords for other services takes place. Attackers could reset passwords for all services tied to an E-mail account should they get access to it and know what services are used with it.

4.3 Computer Security

Securing the personal computer is a very important step for any user. Computers typically store personal files and are used to access sensitive information such as financial information through online banking. This is why it is also important to understand the importance of security software. According to Järvinen (2012, 180), malware also spreads through online services and web browsers which makes used operating system irrelevant in terms of security. This in turn makes the use of anti-virus and anti-malware software additionally more important.

4.3.1 Anti-Virus Software

Anti-virus software is designed to detect and remove malicious software such as viruses and Trojans. They also act as passive protection from them by preventing infection. (Criddle 2014.) Anti-virus software is available for all three major computer operating systems which are Windows, Linux and Mac OS X. Majority of the offered software is for Windows users but there is need for this software on the other two platforms as well. This Bachelor's thesis will introduce some of the popular free to use anti-virus software for the three platforms.

Microsoft Security Essentials is a free anti-virus program for Windows computers which is included in Windows 8 computers under the name Windows Defender. For Windows Vista and 7 it must be downloaded separately. There is no registration required and the install process and usage is very simple. It is also quiet in the sense that there is no intrusive pop ups or the like unless there is a problem. (Microsoft 2014c) Figure 8 below depicts the main view of the program.

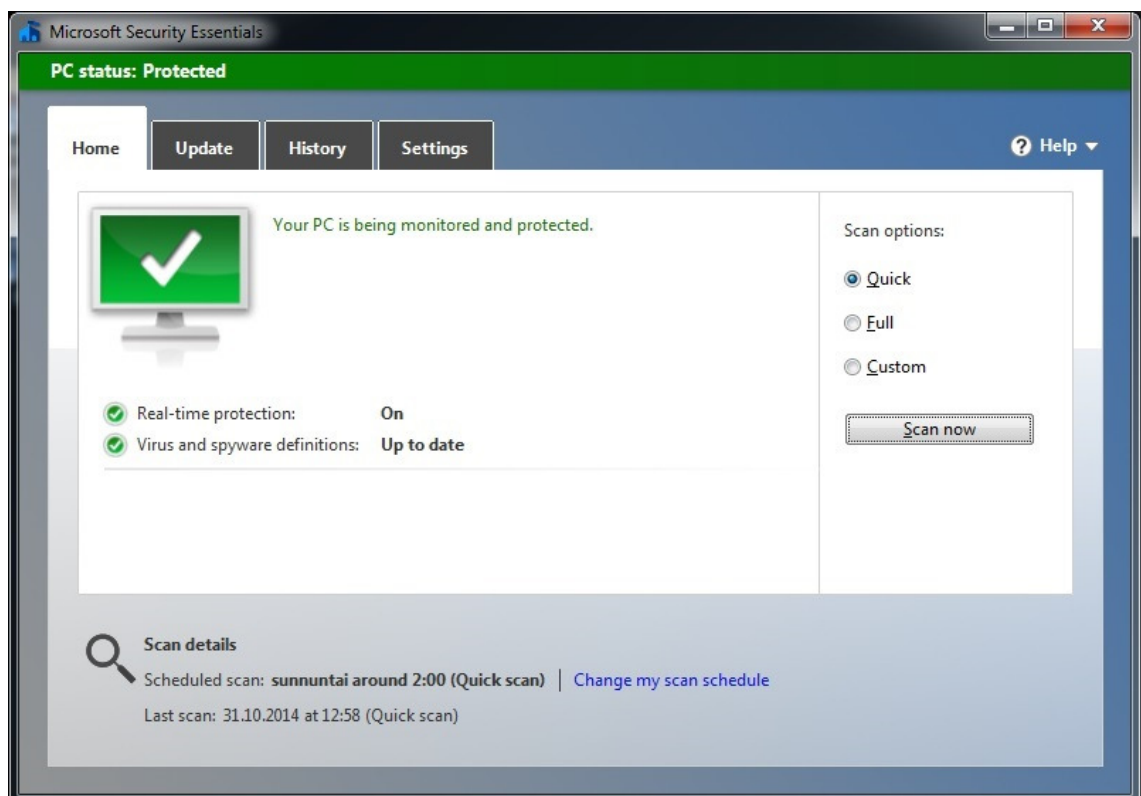


Figure 8: Microsoft Security Essentials

The program looks very simple and is very easy and simple to use. The price of simplicity is the lack of certain kinds of protection that is present in more complex solutions. The program updates itself through Windows Update which requires correct settings for updates to download and install automatically in order for the program to stay up to date without user interaction. It is also possible to manually check for updates and install them from within the program.

Avira Antivirus is a commercial anti-virus program which provides features such as firewall, mail protection and web protection. It also has protection for Android devices and social media. Many of the features are restricted to the commercial version but the free version still offers basic protection from malicious programs and web sites. It is available for Windows, OS X, Android and iOS. (Avira 2014.) Linux products are to be discontinued in 2016 and thus have been excluded from this Bachelor's thesis. Figure 9 illustrates the main window of the program on a virtual Windows XP system.

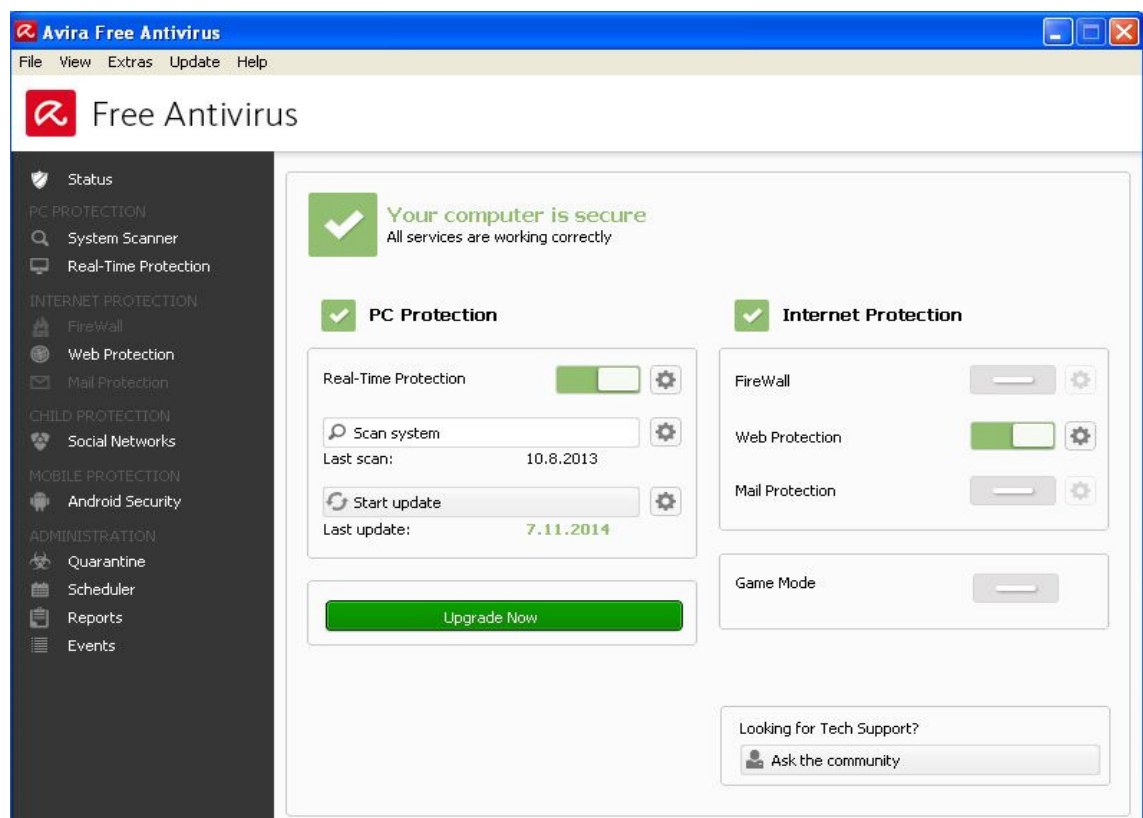


Figure 9: Avira Free Antivirus

This program is also simple in looks and the features not available in the free version are grayed out. The figure is also an example of bad virus scanning practices where the last scan was done over a year ago. This test system is online rarely and, therefore virus scans are so infrequent. The program is also notorious for pop ups to advertise the commercial license and also for the pop up scan window. Updates happen automatically without user interaction.

Avast is another solution with a free option and a commercial license option. It is available for Windows and Mac OS X systems and also for Android devices. There exists Linux versions too but they are not actively marketed and are not visible on the web site. The free version provides protection against malicious software, home network security and browser cleanup. Other features such as firewall and active protection against fake websites in banking are only in the commercial versions. (Avast 2014.) Main window of the Windows version can be seen in Figure 10.

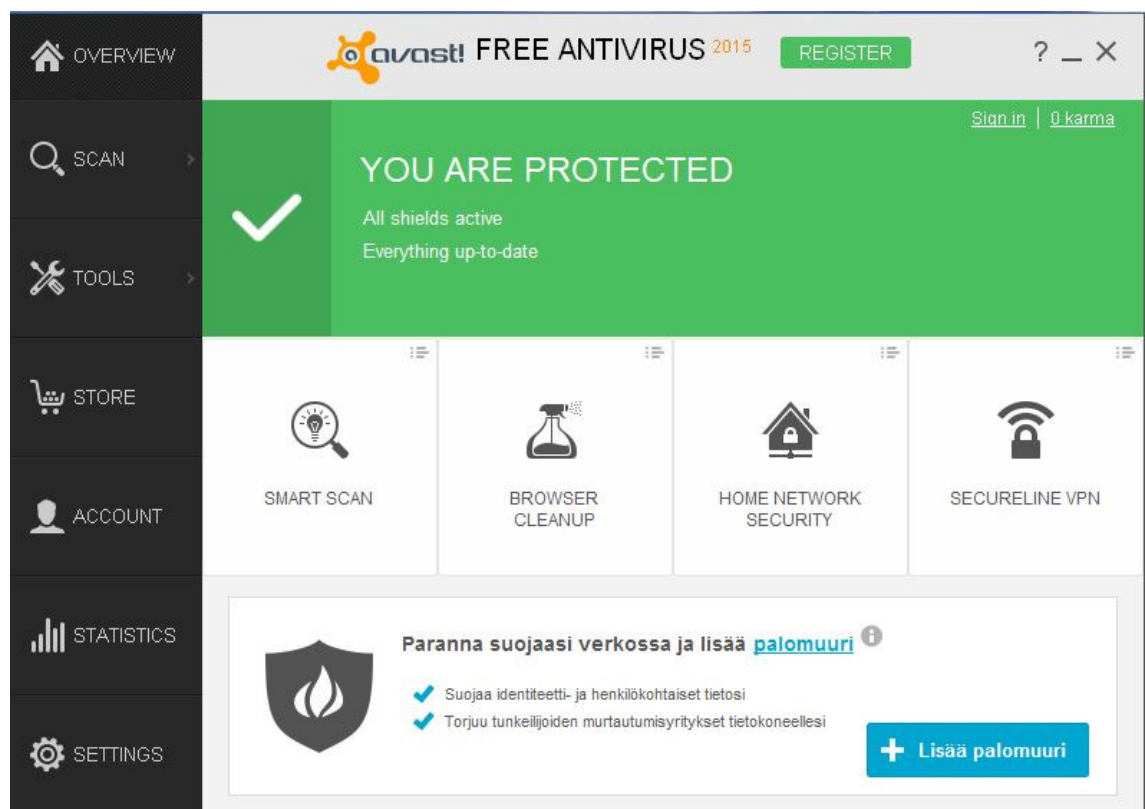


Figure 10: Avast Free Antivirus

The main window of the program is simple in looks and is easy to use like the other programs presented here. Other views have been collected to the menu on the left to make them visible should the user need to use them. Updates happen automatically and can be configured if different behavior is desired. The program advertises paid features like Avira does. The figure also displays an advertisement in Finnish to add the firewall to the program which is a feature in

the commercial version. The program also collects statistics and figure 11 reveals that view.

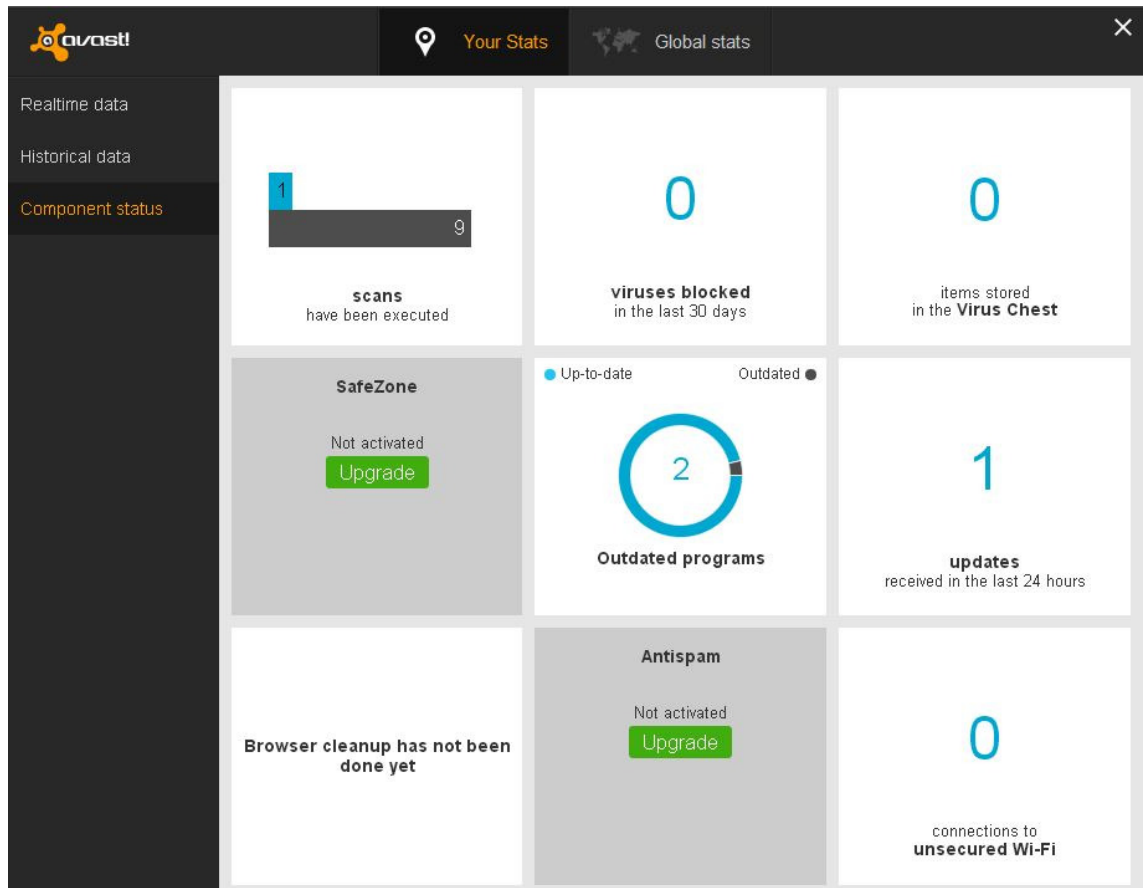


Figure 11: Avast statistics

The figure reveals an interesting statistics view, that shows completed virus scans compared to world monthly average which in this example is 1 monthly scan to a world average of 9. It also shows out of date programs and update and virus related information. Unsecure Wi-Fi connections are also displayed.

The OS X version of Avast looks different from the Windows version but offers similar features. Figure 12 from Bradley (2012) shows what the program looks like.

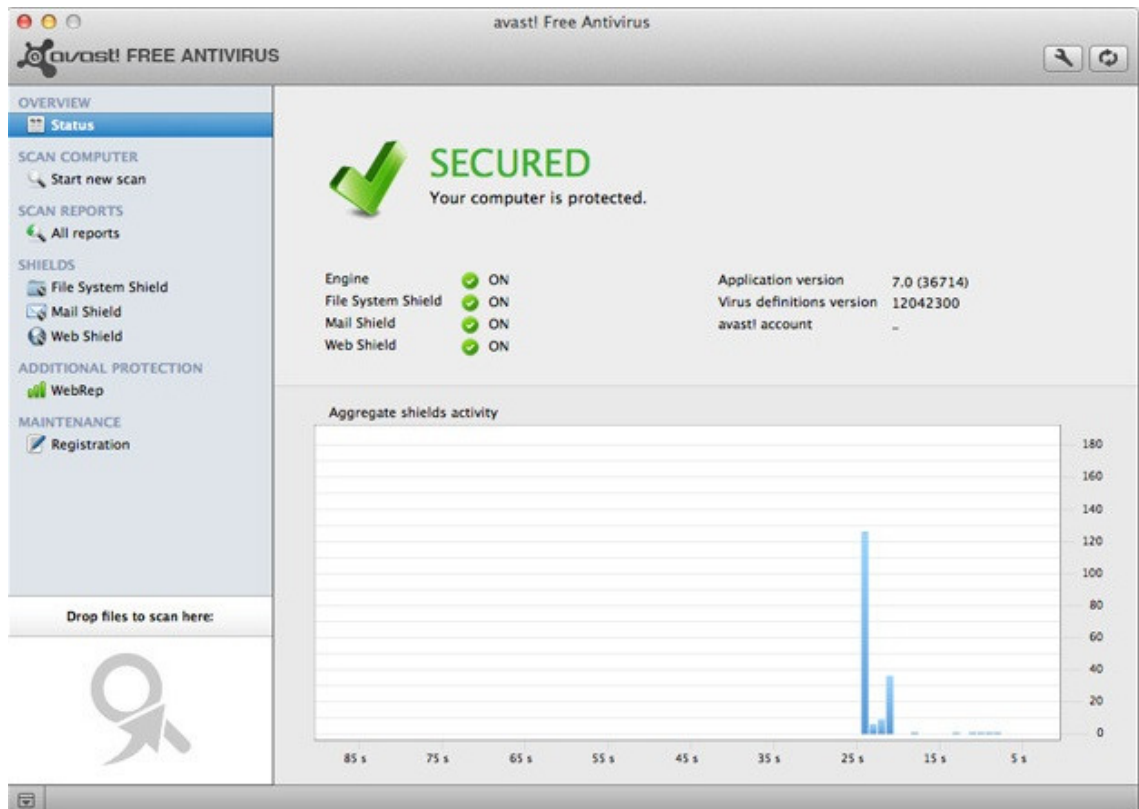


Figure 12: Avast for OS X (Bradley 2012)

The program continues the trend of simple looks and ease of use. There are also new features like dropping files into the indicated area to scan them.

ClamAV is an open source anti-virus program available for all three major computer platforms along with BSD and Solaris. It offers only basic features but is free of charge with no commercial license. (ClamAV 2014.) This Bachelor's thesis will present only the Linux version of this program. Figure 13 below depicts the minimalistic graphical user interface on Ubuntu Linux.

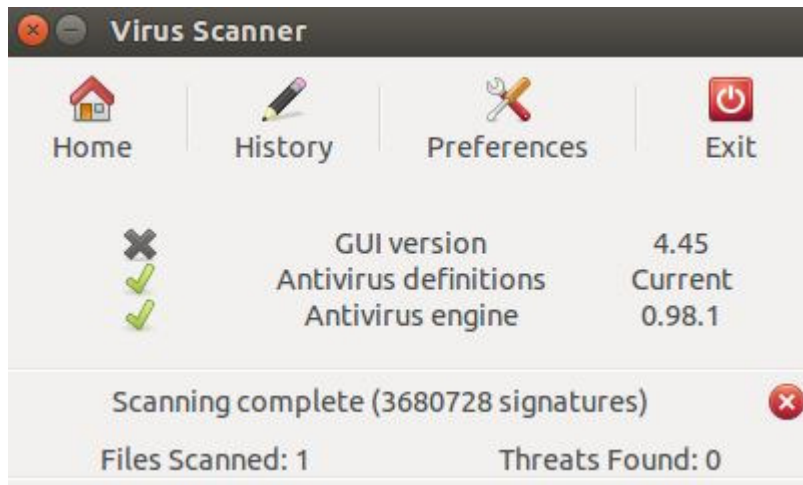


Figure 13: ClamAV Graphical User Interface

The graphical user interface is simple and does not offer much in features or visual aspects. Drag and drop scanning of files can be done once the scan information section at the bottom part of the window has been closed. Updates are done from the command line and scanning can also be done from there as Figure 14 shows.

```
mikko@mikkoub-VirtualBox:~$ clamscan
/home/mikko/.xsession-errors: OK
/home/mikko/.bash_history: OK
/home/mikko/.ICEauthority: OK
/home/mikko/.bashrc: OK
/home/mikko/.xsession-errors.old: OK
/home/mikko/examples.desktop: OK
/home/mikko/.Xauthority: OK
/home/mikko/.bash_logout: OK
/home/mikko/.profile: OK
/home/mikko/.dmrc: OK

----- SCAN SUMMARY -----
Known viruses: 3675212
Engine version: 0.98.1
Scanned directories: 1
Scanned files: 10
Infected files: 0
Data scanned: 0.01 MB
Data read: 0.01 MB (ratio 1.50:1)
Time: 8.475 sec (0 m 8 s)
mikko@mikkoub-VirtualBox:~$
```

Figure 14: ClamAV command line scan

The virus scan on Ubuntu is very short. Only 10 files were scanned by the default scan. While the scans can be initiated easily from both the graphical user interface and the command line, the program does not feel user friendly when compared to commercial products.

4.3.2 Automatic Updates

Keeping the operating system up to date is important as the patches will fix security vulnerabilities and address other issues with the operating system. Same is also true for any other programs or browser add-ons used. Updates are often frequent and all three major operating systems can be configured to check for updates automatically.

Windows operating systems offer automatic updates with settings to install automatically or informing that updates are available. (Microsoft 2014d.) Figure 15 shows the update settings of Windows 7 operating system. The window looks similar on Windows Vista and Windows 8 as well.

Choose how Windows can install updates

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

[How does automatic updating help me?](#)

Important updates



Install updates automatically (recommended)

Install new updates: Every day at 3:00

Recommended updates

Give me recommended updates the same way I receive important updates

Who can install updates

Allow all users to install updates on this computer

Microsoft Update

Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows

Software notifications

Show me detailed notifications when new Microsoft software is available

Note: Windows Update might update itself automatically first when checking for other updates. Read our [privacy statement online](#).

Figure 15: Windows Update settings

Updates can be scheduled to install at any desired time and that the recommended option is to install them automatically. Recommended updates can also be included in this installation and this has been enabled for the operating system used in the figure. Microsoft categorizes updates into three different categories. Important updates, recommended updates and optional updates. Important updates are security and reliability updates while recommended ones are general software updates (Microsoft 2014d) Figure 16 depicts the update window when new updates are available.



Figure 16: Windows Update

Windows will automatically select important updates to be installed as can be seen in the figure. It will also notify when updates were previously installed and when the most recent update check was. Clicking on the important updates row will open a window where specific update list is shown. Figure 17 shows this window.

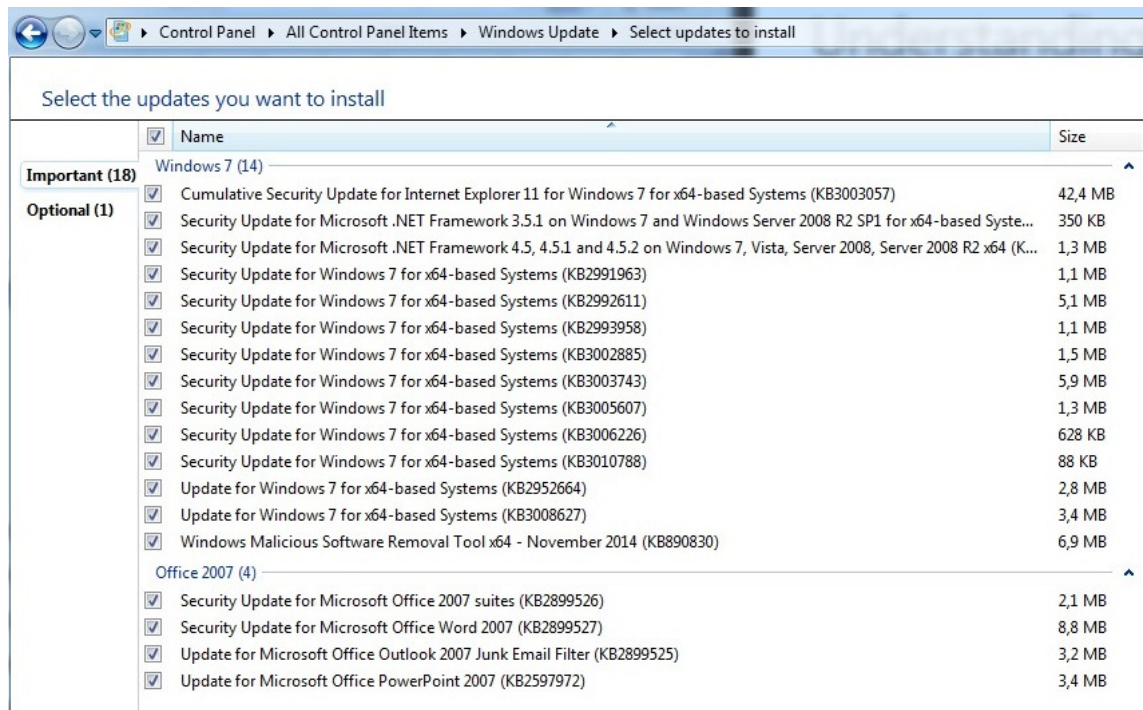


Figure 17: Detailed Windows updates

Updates are categorized by importance and also by products within the categories. Each update has a KB number associated to it. It acts as an ID number to tell different updates apart. More information about a specific update can also be found on the Internet with the KB number. Updates can be selected and deselected freely in this window.

Linux updates operate differently from Windows ones. Due to the centralized nature of Linux applications, the software update program will update both the operating system and all installed applications on the computer. On Windows operating systems the Windows Update can only update Windows itself and any installed Microsoft products. The different Linux distributions offer different solutions for update management and features described in this Bachelor's thesis may not be present in other distributions. Most distributions follow the same principles as in Ubuntu. Software Updater of Ubuntu Linux is shown in Figure 18.

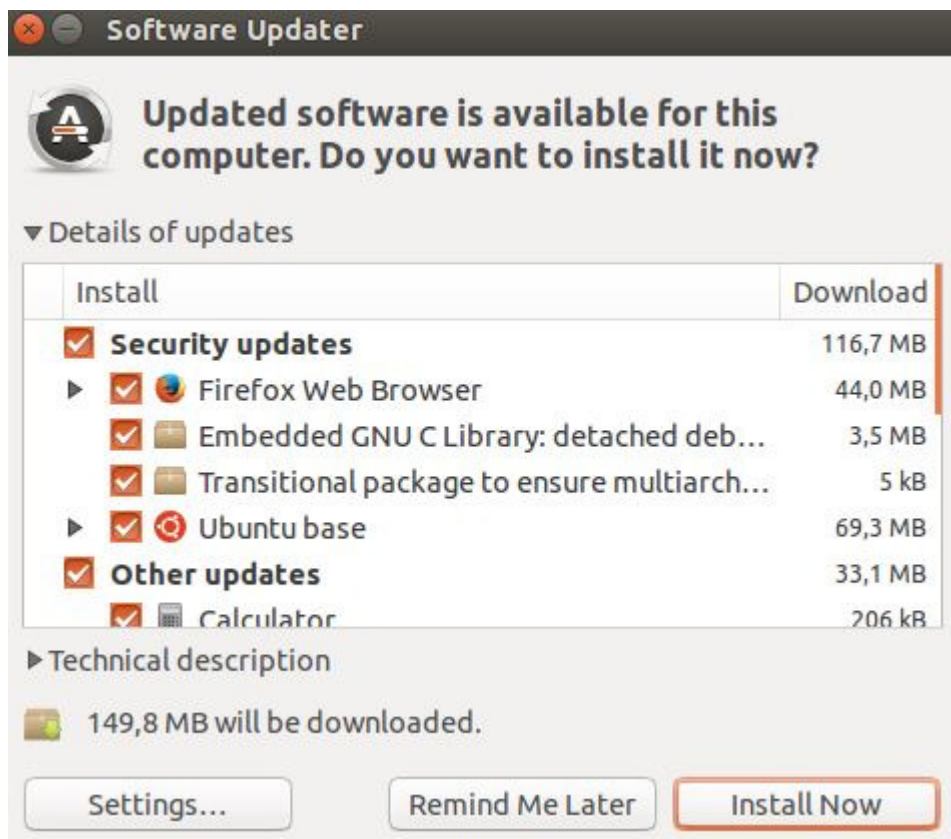


Figure 18: Ubuntu Software Updater

Ubuntu Software Updater is very easy to use and categorizes updates by security and other updates. Command line can also be used to update the system. Updates can be deselected freely like on Windows operating systems. Update checks can be scheduled like on Windows and they can also be installed automatically. Figure 19 illustrates the update settings of Ubuntu Linux

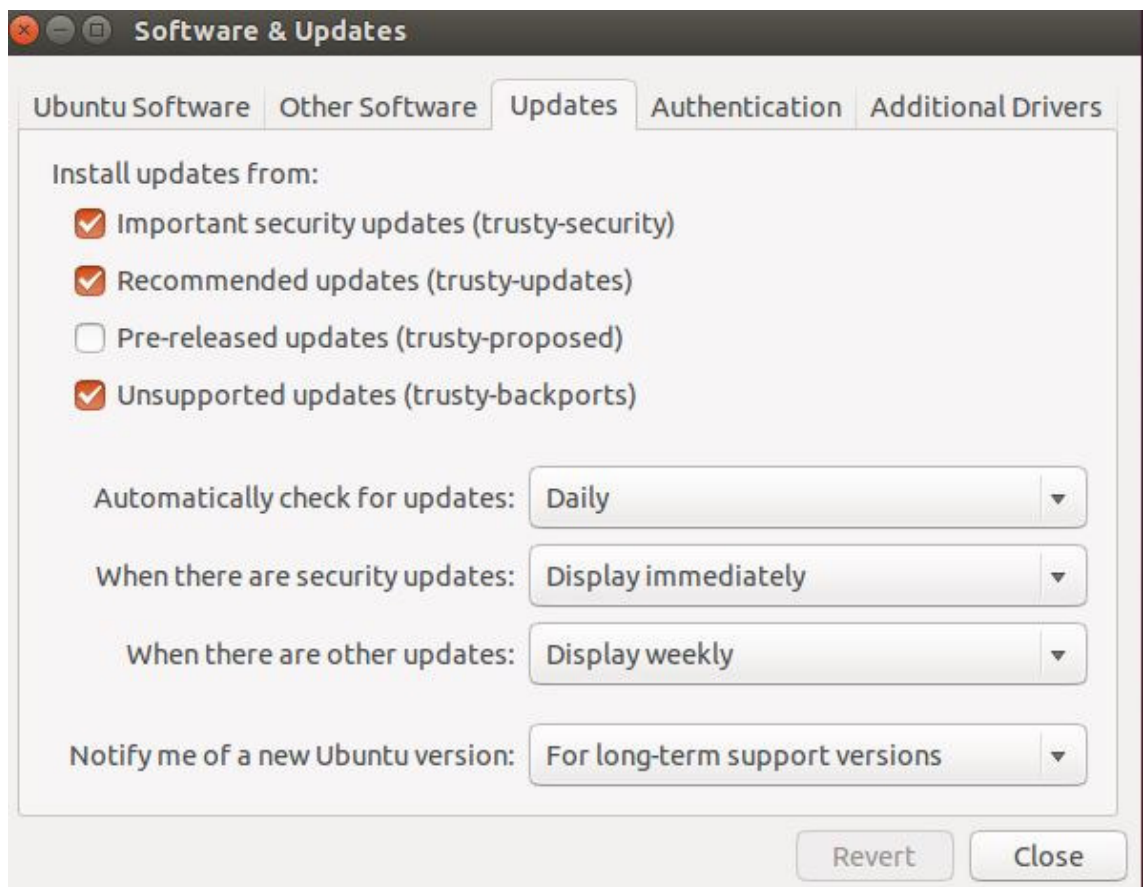


Figure 19: Ubuntu update settings

The update settings show different update repositories for the different categories of updates. The settings displayed are default values that have not been altered in any way. One difference from Windows is the notification of new operating system releases where either long or short-term support versions can be selected.

Mac OS X operating system offers a similar method of updates as Windows does. Updates are offered for the operating system itself and to products acquired from the Mac App Store. The OS X Yosemite can automatically install updates overnight or manually by the user if the automated feature is not used. (Apple 2014a.) Similar scheduling features are available when compared to Windows and Linux. Figure 20 from Apple (2014a) shows the Mac App Store where updates are managed for the latest OS X versions.

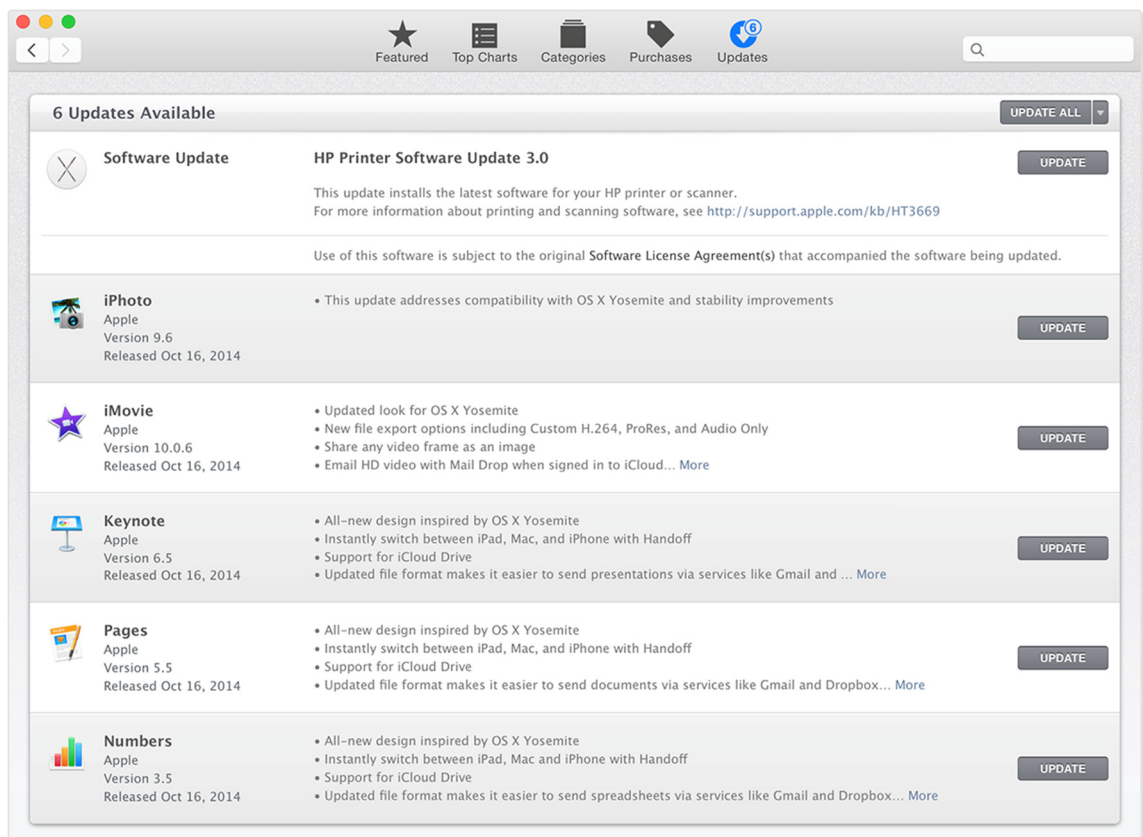


Figure 20: OS X Updates (Apple 2014a)

The updates page shows updates for the operating system and applications from Apple. Software not from Mac App Store must be updated separately. Standalone installers are also available for situations when there is no internet connection or if updates need to be downloaded with another computer.

4.3.3 Firewall

Firewalls filter undesired incoming connections to the computer. Depending on content of the IP package and the rules of firewall, traffic is either let through or blocked. There exists two types of firewalls. First is software firewalls which are either built in to the operating system or installed as separate application. Second is hardware firewalls that for home usage are for example in consumer internet routers and wireless access points. (Järvinen 2012, 189-190.) Only one software firewall can be in use at a time. Multiple different firewalls will compete with each other and will cause problems or prevent the protection firewalls provide. Hardware and software firewalls can be used together as they exist at

different points in the network therefore they do not do filtering at the same time. It is recommended to use both hardware and software firewall as this provides a double layer of protection against malicious incoming connection attempts.

According to Järvinen (2012, 190) Windows, Linux and OS X computers all have built in software firewall. There are also third party software firewalls available for all three types of operating systems. This Bachelor's thesis will present the built in firewall solution on Windows, Linux and OS X.

Windows Firewall is in all modern Windows operating systems and is on by default. Recommended settings are to have it on for all network locations and connections and to have it block all inbound connections unless separately allowed (Microsoft 2014e). The Windows Firewall has a simple user interface and settings can be changed easily. Figure 21 shows the main view of Windows Firewall on Windows 7 operating system.

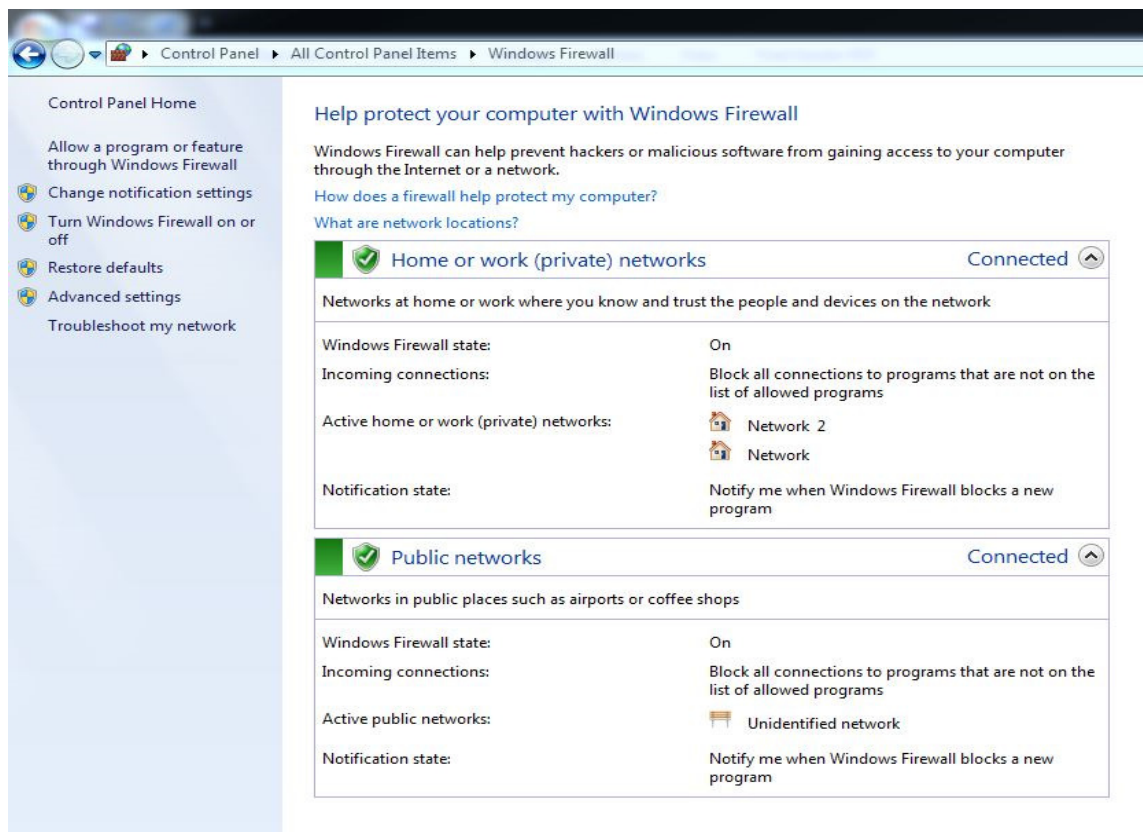


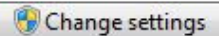
Figure 21: Windows Firewall main window

In this example the firewall is on and is set to block all incoming connections that are not in the list of allowed programs. The list can be adjusted in a separate window which is depicted by Figure 22.

Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

 Change settings

Allowed programs and features:

Name	Home/Work (Private)	Public
<input type="checkbox"/> Windows Collaboration Computer Name Registration Service	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Windows Communication Foundation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Windows Firewall Remote Management	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Windows Live Communications Platform	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Live Communications Platform (SSDP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Live Communications Platform (UPnP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Windows Management Instrumentation (WMI)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Windows Media Player	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Windows Media Player Network Sharing Service	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Windows Media Player Network Sharing Service (Internet)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Windows Peer to Peer Collaboration Foundation	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Windows Remote Management	<input type="checkbox"/>	<input type="checkbox"/>

Figure 22: Windows Firewall allowed programs

The list can be adjusted by clicking the button "Change settings" which requires administrator privileges. Any programs not in the list can also be added by clicking the 'Allow another program...' button. Ticked box indicates that the program is allowed by the firewall.

Windows Firewall also provides an advanced view that is less user friendly and geared towards experienced users. It allows more control over the firewall. Typical home users should not need to use this view. Figure 23 reveals the advanced view.

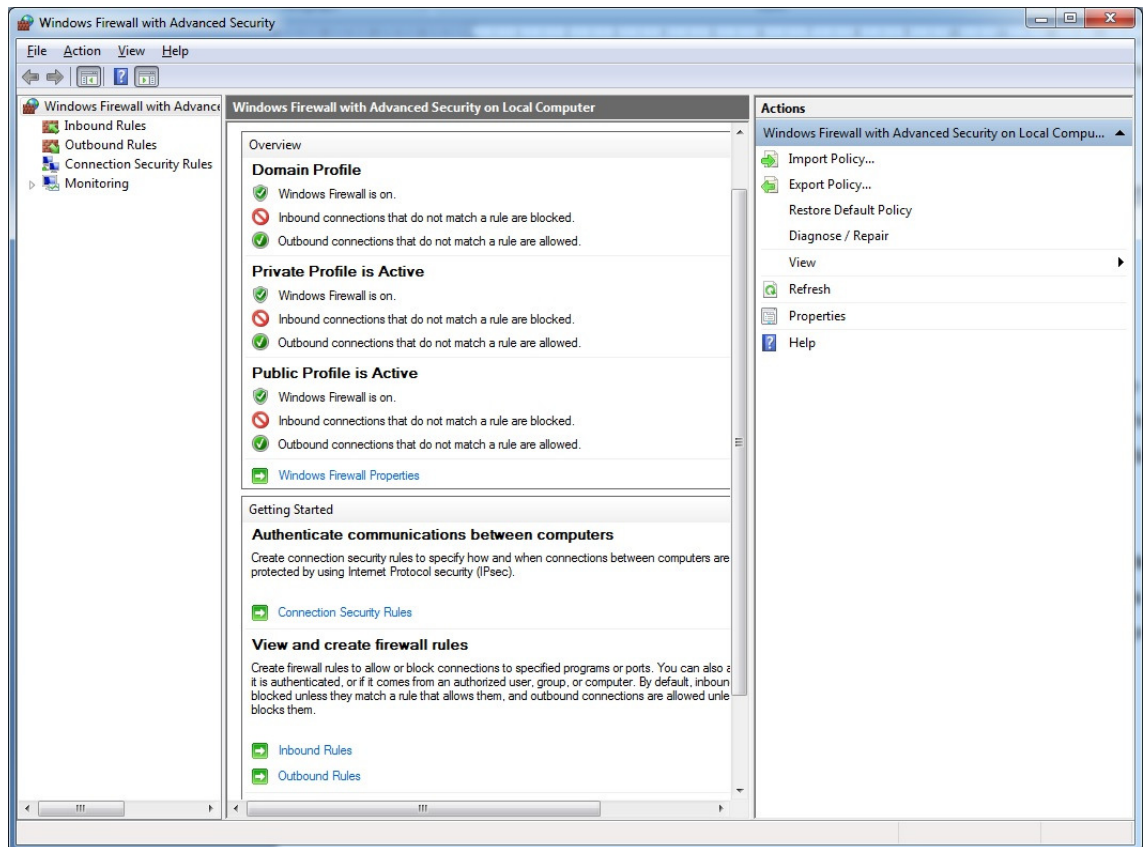


Figure 23: Windows Firewall Advanced Security

Like the name suggests these advanced firewall settings are not for the average user. The advanced security view provides the same functionality as the basic one along with its own advanced features for fine tuning and logging for example.

Linux operating systems commonly have firewall utility called iptables pre-installed. The program uses three different policy chains to control traffic. These three are input, forward and output. It is managed only from the command line and allows various security configuration on what is allowed to connect and what is not. The default behavior is allow all connections. (Brown 2014.) The default policy set on a virtual Ubuntu Linux can be seen in Figure 24.

```
mikko@mikkoub-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Figure 24: Iptables default policy

The command 'iptables -L' lists the current rules. The program is not user friendly for the everyday user who is not comfortable with console commands. The application is also more useful for servers rather than home computers.

Recent Mac OS X operating systems have an application firewall included. Connections can be controlled based on applications for easier management. It is also possible to block all incoming connections or allow signed software to connect. Stealth mode is also supported where the firewall will prevent responses to probing requests. The limitations of the application firewall is it being designed only for common internet protocols. This restricts the features available to it. Earlier firewall implementation called 'ipfw' still exists and can be accessed through the command line. (Apple 2014b.)

4.4 Network Device Security

The network devices such as routers and wireless access points also contain configuration options and features that affect cyber security. According to Pinola (2014) the router is the first device between attackers and home devices. This is why it's important to configure the router properly.

There are multiple steps in ensuring that the network device is secure. Every router and access point comes with login credentials to access the management user interface. The password for this must be changed from the default one to prevent outsiders from accessing the configuration options. In

some models the username can be changed too and it should be changed if possible.

With wireless access points it is also important to change the name of the wireless network from the default one. Many access point models name the default network after the manufacturer which will immediately tell outsiders what manufacturer access point is used. Improved security modes such as WPA2 are also encouraged to be used with a secure password. Other features such as Remote Administration and Universal Plug n'Play should also be turned off as both give more possibilities for outsiders to try access the network. (Pinola 2014.)

The device firmware should also be kept up to date as new firmware typically fixes security vulnerabilities that may allow attackers access to the device. Third party firmware could also be considered as the two popular open source firmware like DD-WRT and Tomato provide much more security features and are updated more often. (Pinola 2014.)

As was previously discussed the devices come with their own firewall which should be used in combination with a software firewall on the computer. Depending on model there may also be possibility to enable Stealth Mode which will prevent the device from answering to ping requests making the devices within the network appear invisible.

Common misconception about the network devices is that they are just boxes that shouldn't be touched after they are up and running. Instead it is important to check up on them regularly for updates and to make sure the settings are correct. While the user interfaces might be barebones and not user friendly it is well worth the time to go through them.

5 CONCLUSIONS

Internet has made it possible for many of the cyber security threats to become successful to the extent that they are today. This must be taken into account when considering the security of the home user. The Internet is not going away and technological advances are continuing to tie it into more devices and thus add cyber security threats to the users. For the home user it is important to know that cyber criminals attempt to exploit them with any ways imaginable and that time and place do not make anyone safe from cyber-attacks. Common sense and usage of the provided technological security solutions will carry anyone far but there is never perfect protection against everything.

As the internet is the source of all threats to cyber security, this makes countering them difficult. E-mail carries malicious attachments, phishing attempts and web sites can be compromised to infect anyone visiting them. Even the virtual 'you' can be lost to attackers and be used to target other people. This potential loss of identity makes it very difficult to identify fraudulent content from real one.

Different computer and mobile operating systems do not provide security by themselves anymore. Online threats can risk any operating system through the applications installed on it. While Linux and Mac OS X operating systems are still considerably safer than Windows, there is still need to consider cyber security on those platforms as well. Rarity of the operating system does not provide protection despite the fact that it is still commonly believed.

This Bachelor's thesis explores the different personal and technological aspects of cyber security. It is important to understand both the user and the technology. The two together are the foundation of cyber security. Thus the strategy for home user security is both personal and technological. Not believing everything seen on the internet is the most critical point. The various scams and phishing attempts along with virus e-mail attachments are commonly made to look interesting. E-mail attachments are not to be opened and expected attachments

should be virus scanned before opening. Lottery win notifications and cheap deals or promises of profit are to be ignored. No links are to be clicked if some service appears to be notifying about login credentials or credit cards.

The technological side of the strategy involves usage of anti-virus and firewall software. It is essential that these are kept up to date along with the operating system as well. Passwords are recommended to follow common security practices by being complex enough yet easy for the owner to remember. Advertisements can be blocked which will aid in personal privacy and also mitigate risks of malicious advertisements. Network devices should be regularly maintained and be properly configured.

It can be concluded that security solutions need user interaction to provide the best protection. While many applications and operating systems provide automatic updates and virus scans it might still be necessary for the user to configure the automation. Various privacy and security features of applications and mobile devices may not be enabled by default and need to be turned on manually. The security software itself may not even be installed and will need to be acquired separately. This means that the user has major responsibility and a wide variety of actions to take in securing their devices.

Many applications are easy to use and configure and there exists guides for more complicated tasks. It is the user's responsibility to take matters into their own hands and take the necessary steps to ensure they are secure in the cyber space.

REFERENCES

Adblock Plus 2014. Adblock Plus - Features. Referenced October 27, 2014
<https://adblockplus.org/en/features>

Apple 2014a. Update OS X and App Store apps on your Mac. Referenced November 12, 2014
<http://support.apple.com/en-us/ht1338>

Apple 2014b. OS X: About the application firewall. Referenced November 17, 2014
<http://support.apple.com/en-us/ht1810>

Avast 2014. Avast 2015 is here, and it's free. Referenced November 10, 2014
<http://www.avast.com/en-eu/index>

Avira 2014. Download Avira Free Antivirus 2015. Referenced November 7, 2014
<http://www.avira.com/en/avira-free-antivirus#>

Bradley Tony 2012. Avast Offers Free Security for Mac OS X. Referenced November 10, 2014
http://www.pcworld.com/article/254645/avast_offers_free_security_for_mac_os_x.html

Brown Korbin 2014. The Beginner's Guide to iptables, the Linux Firewall. Referenced November 17, 2014
<http://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/>

ClamAV 2014. ClamAV is an open source antivirus engine for detecting trojans, viruses, malware & other malicious threats. Referenced November 11, 2014
<http://www.clamav.net/index.html>

Crawford Stephanie 2014. What is an IP address? Referenced October 23, 2014
<http://computer.howstuffworks.com/internet/basics/question549.htm>

Criddle Linda 2014. What is Anti-Virus Software? Referenced November 7, 2014
<http://www.webroot.com/us/en/home/resources/tips/pc-security/security-what-is-anti-virus-software>

DuPaul Neil 2013. Common Mobile Malware Types: Cybersecurity 101. Referenced October 23, 2014
<https://www.veracode.com/blog/2013/10/common-mobile-malware-types-cybersecurity-101>

Felt Adrienne Porter & Wagner David 2012. The Mobile Problem. In Markus Jakobsson (ed.) Death of the Internet. Hoboken: John Wiley & Sons Inc. 169

F-Secure 2014. Removing 'Police-themed' ransomware. Referenced October 29, 2014

http://www.f-secure.com/en/web/labs_global/removing-police-themed-ransomware

Glenn Jerome Clayton 2010. Handbook of Research Methods. Delhi: Oxford Book Company

Granger Sarah 2002. The Simplest Security: A Guide To Better Password Practices. Referenced November 3, 2014

<http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices>

Harrison Andrew 2014. Best Mac antivirus software 2014: 6 Mac internet security suites tested and reviewed. Referenced November 7, 2014

<http://www.macworld.co.uk/feature/mac-software/mac-antivirus-internet-security-software-malware-review-3523842/>

IT Governance Ltd 2014. What is Cyber Security? Referenced October 13, 2014

<http://www.itgovernance.co.uk/what-is-cybersecurity.aspx>

Järvinen Petteri 2010. Yksityisyys - Turvaa digitaalinen kotirauhasi. Jyväskylä: Docendo Oy

Järvinen Petteri 2012. Arjen Tietoturva - Vinkit ja Ratkaisut. Jyväskylä: Docendo Oy

Järvinen Petteri 2014. NSA - Näin meitä seurataan. Jyväskylä: Docendo Oy

Limnell Jarno & Majewski Klaus & Salminen Mirva 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy

Microsoft 2014a. Find my Phone. Referenced November 26, 2014.

<https://www.windowsphone.com/fi-fi/my/find>

Requires registration

Microsoft 2014b. How to recognize phishing email messages, links, or phone calls. Referenced November 26, 2014

<http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx>

Microsoft 2014c. Get free virus protection with Microsoft Security Essentials. Referenced November 7, 2014.

<http://www.microsoft.com/security/pc-security/microsoft-security-essentials.aspx>

Microsoft 2014d. Understanding Windows automatic updating. Referenced November 12, 2014

<http://windows.microsoft.com/en-us/windows/understanding-windows-automatic-updating#1TC=windows-7>

Microsoft 2014e. Firewall: frequently asked questions. Referenced November 14, 2014

<http://windows.microsoft.com/en-us/windows/firewall-faq#1TC=windows-7>

Muller Rudolph 2011. Do you have a weak password or PIN? Referenced November 26, 2014

<http://mybroadband.co.za/news/security/31546-do-you-have-a-weak-password-or-pin.html>

PC Tools 2014. What are browser cookies? Referenced October 23, 2014

<http://www.pctools.com/security-news/what-are-browser-cookies/>

Pinola Melanie 2014. The Most Important Security Settings to Change on Your Router. Referenced November 20, 2014

<http://lifehacker.com/the-most-important-security-settings-to-change-on-your-1573958554>

Richmond Ben 2013. How "Device Fingerprinting" Tracks You Without Cookies, Your Knowledge, or Consent. Referenced October 27, 2014

<http://motherboard.vice.com/blog/device-fingerprinting-can-track-you-without-cookies-your-knowledge-or-consent>

Sachdeva J.K. 2009. Business Research Methodology. Mumbai: Himalaya Publishing House Pvt. Ltd. Referenced November 25, 2014

<http://ez.lapinamk.fi:2054/lib/ramklibrary/reader.action?docID=10416021>

Sauro Jeff 2011. Do Users Read License Agreements? Referenced November 26, 2014

<https://www.measuringu.com/blog/eula.php>

United States Computer Emergency Readiness Team 2012. Home Network Security. Referenced May 21, 2014

<https://www.us-cert.gov/Home-Network-Security>

University of Guelph 2014. Exploratory Research. Referenced May 21, 2014

<http://www.htm.uoguelph.ca/MJResearch/ResearchProcess/ExploratoryResearch.htm>

Wallen Jack 2010. Myth Busting: Is Linux Immune to Viruses? Referenced November 7, 2014

<http://www.linux.com/learn/tutorials/284124-myth-busting-is-linux-immune-to-viruses>

What's My User Agent 2014. Analyze User Agent String. Referenced November 26, 2014

<http://whatsmyuseragent.com/Analyze/>