TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technology

Dineta Mahno A143652

DESIGN OF CYBER SECURITY AWARENESS PROGRAM FOR THE FIRST YEAR NON-IT STUDENTS

Master’s Thesis

Supervisor: Truls Ringkjob

Master of Engineering

Tallinn 2017

Author’s declaration of

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Dineta Mahno

02.01.2017

Abstract

The world becomes increasingly interconnected. The internet importance growth with each year and plays a very important role in our life. We work, we learn, we play online. This technology brings advantages and makes our daily life easier and at the same time it also adds extra risks to our personal and business information. This is especially true for students, who spend a lot of time online. In the universities we teach students to be a good specialists and to perform their jobs in accounting, sales, law, medicine, engineering and so on, but lack to teach them the basic knowledge about the risks to the systems making them the perfect target to the attackers. There are many simple ways that these risks can be reduced and it all starts with cyber security awareness.

In this paper, the author will show the need for cyber security awareness program for students in the university and will design a cyber security awareness program for the first year non-it students.

This thesis is written in English language and is 46 pages long, including 6 chapters, 22 figures.

Annotatsioon

Maailm muutub üha enam omavahel seotuks. Internet mängib väga olulist rolli meie elus ja ta tähtsus kasvab igal aastal. Me töötame, õpime ja mängime online. Ühelt poolt see tehnoloogia annab meile suured eeliseid ning muudab meie igapäevast elu lihtsamaks. Kuigi samal ajal võrgus olles riskime me koguaeg oma isiklike ja ettevõtte andmete turvalisusega. See risk on eriti kõrge üliõpilaste seas, kes veedavad palju aega internetis.

Ülikoolides me õpetame üliõpilasi, et nendest saaks head spetsialistid. Koolitame neid, et nad oskaksid teha oma tööd raamatupidamise, müügi, õiguse, meditsiini, inseneri ja muudel erialadel. Aga samal ajal unustame õpeta neile interneti turvalisuse riske mille pärast nad saavad ideaalseks sihtmärgiks ründajatele. On palju lihtsaid viise, et neid riske vähendada ja see kõik algab küberturvalisuse teadvustamisest üliõpilastele.

Kui õpilased on korralikult haritud küberturvalisuse riskide kohapealt, siis nende teadlikkus tõuseb ja nad teevad vähem vigu. Samuti väga oluline, et neid harides saavad nad oma teadmisi jagada perekonna liikmetega. Ettevõtted saavad üliõpilaste teadvustamisest suurt kasu ja minimaliseerivad riske.

Selles töös autor näitab, et tudengitel on reaalne vajadus õppida küberturvalisuse aluseid ülikoolis ja luua arvuti turvalisuse õppekava esimese aasta mitte-it erialade üliõpilastele. Programm on loodud, et anda üliõpilastele põhilisi teadmisi, kuidas tagada enda turvalisus internetis ja võrgus. Tööandjate vaatenurgast suurendab see oluliselt tööturule siirduvate noorte kvalifikatsiooni.

See lõputöö on kirjutatud inglise keeles, on 46 lehekülge pikk ning sisaldab 6 peatükki ja 22 joonist.

List of abbreviations and terms

CIO Chief information officer is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals.

HR Human Resource are the people who make up the workforce of an organization, business sector, or economy.

IDS Intrusion Detection System is a device or software application that monitors a network or systems for malicious activity or policy violations

IP Internet Protocol is a set of rules governing the format of data sent over the Internet or other network.

IT Information Technology is the application of computers and internet to store,study, retrieve, transmit, and manipulate data,or information, often in the context of a business or other enterprise

PC Personal Computer is a general-purpose computer whose size, capabilities, and price make it feasible for individual us

TCP The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called TCP/IP.

VPN Virtual Private Network is a technology that creates an encrypted connection over a less secure network

Table of contents

List of Figures

1 Introduction

Today computers and Internet play a very important role acting as a platform for communication, trading activities and sharing resources and information in the businesses around the world. The internet has slowly taken over every aspect of our lives such as social networking, shopping and even critical infrastructure such as banking, transportation, law enforcement, emergency services. In our country all governmental, industrial, and economic systems depend on computer networks. And as larger amounts of sensitive data are being transmitted and stored electronically, and as more databases are being connected to the Internet, the need to secure grows more and more every day.

In the universities we teach students to be a good specialists and to perform their jobs in accounting, sales, law, medicine, engineering and so on, but lack to teach them the basic knowledge about the risks to the systems. There are many simple ways that these risks can be reduced and it is all starts with cyber security awareness. If students will be properly educated about the possible threats of the online technology, the risks that could affect them would be minimized. Also very important that being educated about this risks they can also share their knowledge to their families. And of course the companies will only benefit from this by achieving the minimum risks of getting human error during the working process.

The goal of this research to prove that there is a significant need for students to be educated about cyber security risks and to design the computer-security education curricula for the first year non-it students. The program which should be intended to give students the basic knowledge how to stay safe online and will help to be a more better specialists who are able to reduce internet risks while working in any kind of organization. The outline of the remaining part of this work is highlighted as follows: Chapter 2gives the description of the problem we are facing this days. Explains the purpose of the work and why we deal with the first year non-it students. Chapter 3 introduces selected research methodology like convenience sampling and case study. Chapter 4 gives the overview of survey analysis and introduces the analysis of case studies. Chapter 5 introduces description of the designed course

2 Situation and problem analysis

2.1 Problem and purpose

The world becomes increasingly interconnected and the Internet importance growth with each year. Huge amount of sensitive information stored and transmitted across the network which forced the companies to pay more attention to the security of their IT infrastructure. Imagine that you are the owner of the company. You have invested a lot of money to secure your IT infrastructure, have hired a good specialists to you IT department to operate them, but one day you have got to know that you were hacked. You can ask yourself: How was it possible? I have the best security equipment and team. And the answer for this question is very easy: no matter how good you protect your infrastructure on the technical level there is always exist the biggest security gap: The User. One who is doing every day job by running applications, visiting web sites, managing emails and so on and even do not think about the process.

According to the Symantec monthly threat report the number of cyber-attacks and threats that Internet users are exposed to has noticeably grown. “On the Figure 1 we can see that the email malware rate increased in November, jumping from one in 158 emails in October to one in 85 emails. The global spam rate increased for the third month in a row, to 54.3 percent, reaching the highest rate seen since March, 2015. The phishing rate increased in November, up to one in 2,621 emails.” [1]

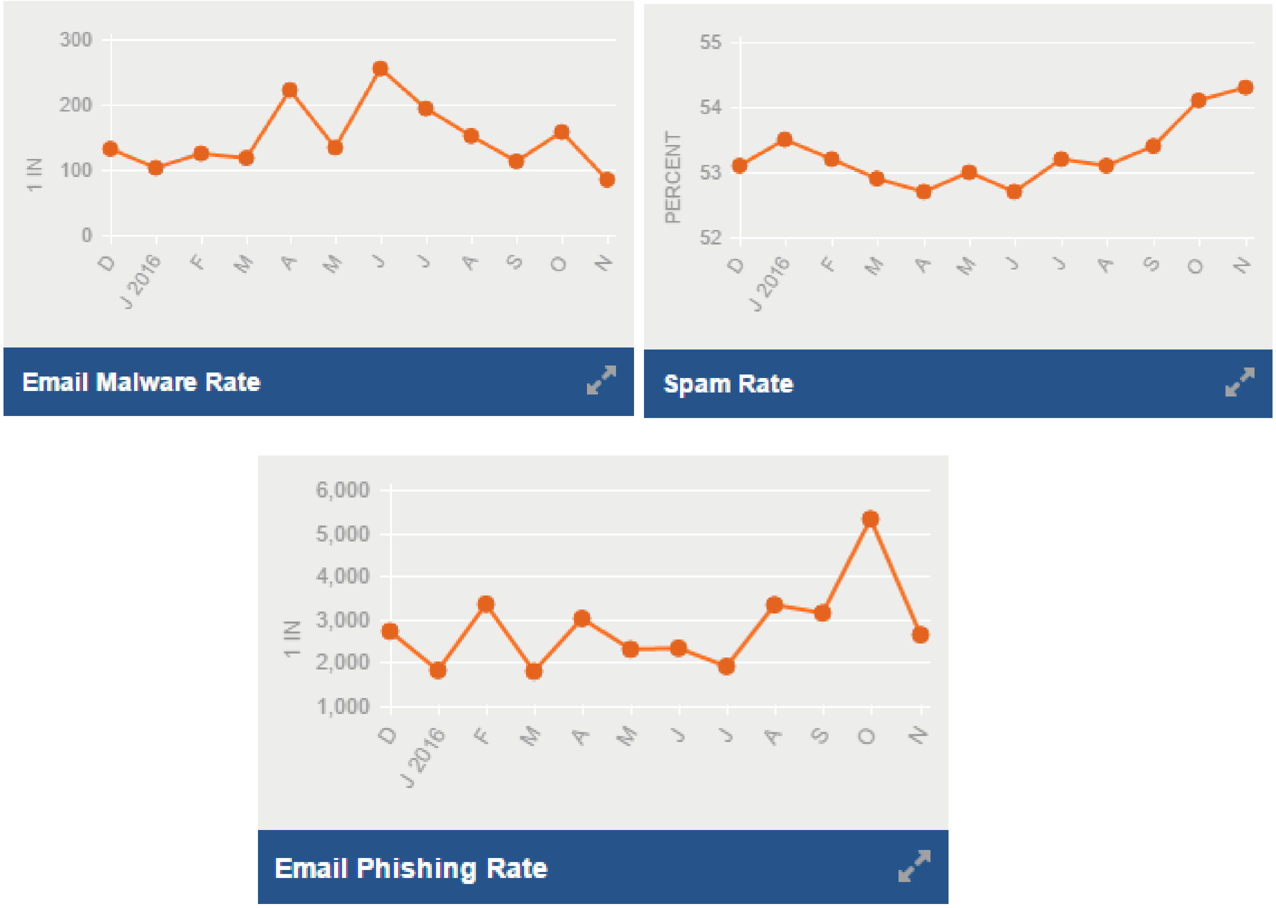


Figure 1. Malware, spam and phishing growth in November 2016 (Symantec, 2016)

To protect from threats even the best security technology and staff in the world can not help unless employees lack the basic knowledge about the risks to the systems they are working with and do not understand how to defend these systems to safeguard data and protect company resources, how to act in the situations when attacker call them, how to identify malicious emails and so on. Some companies invent their own security awareness programs, some organize an awareness training but in spite of this there is still a need to teach a first year non-it students security principles in the university. Cybersecurity awareness is not just a knowledge what are the threats. It is the knowledge combined with different practice of attitude that teaches how to take right steps to minimize the impact of this threats and to protect our information assets. If students are aware about online threats, the risks that could affect them would be minimized.

First of all students will know how to protect their own private sensitive information and secondly organizations will benefit from this, because it will allow to minimize the risks of getting human error during the working process, the error that could be a critical for organization.

Students have to understand that no one can secure them as along as they will not study to secure themselves. Every Internet user has a role in protecting his part of cyberspace, including the devices and networks he or she uses. Our actions have a collective impact and when we use the internet safely, we make it more secure for everyone. „If every user would be educated about cyber security and how to implement all this different security practices, the digital world will become more safer and more resistant from attacks and more resilient if an attack occurs“. [2]

That is why the purpose of this work to prove that there is a significant need for students to be educated about cyber security awareness and to design the computer-security program for first year non-it students.

2.2 Target group

Cyberspace is shared space and we all have responsibility to secure it. There is a proverb: “Forewarned is forearmed“ that can be used in cyberspace with the meaning: more you know about the cyber risks and be aware of the threats, more you know what to do about them. And it is especially important for students who involved in higher education.

First reason is the dependence of the higher education on the internet. Students use the benefit of this technology for making researches, writing papers, performing presentations, communicating with teachers and other students, and so on. They are enrolled in online programs and classes. And if they are not aware about cyber security they can become a perfect target to attackers.

Second reason, they reach the age of majority at 18. “The age at which a person is considered an adult, with all the attendant rights and responsibilities of adulthood who is liable for their own actions, such as contractual obligations or liability for negligence. Also a parental duty of support to a child ceases when the child reaches the age of majority.” [3]

Third reason is future employee or trainee. This reason is very closely linked to the age of majority. School education is complete till this time and students start becoming self dependent. This becomes a reason why after the first half of the first year of studies they start to search for a job and begin to work. On the third year of studies the trainee course for students is mandatory. It means that they become an employee at least for 4 month. And as there is currently a lack of awareness amongst students due to the absence of education that is readily available to them they become the weakest link who can be used by attackers.

The fourth reason, let’s call it young teachers. Students go to university to get an education. “The purpose of education is to share our knowledge with others. A great teacher can impart a deep understanding of a subject to students effectively and with passion and hope, in turn, that in doing so those young people will be inspired to teach others.” [4]

Awareness about cyber security risks is also a knowledge and the students are the perfect way to share it. They belong to the age group that can teach younger ones like brothers and sisters and also to be a good teachers for the older people, like parents, grandmothers or grandfathers.

3 Methodology

In this study will be used boths research methods: qualitative and quantitative research. Qualitative research provides insights into the problem. Quantitative research is used to quantify the problem by the way of generating numerical data or data that can be transformed into useable statistics. [5] Along with survey questionnaire that will be given out to students for the statistical results of the findings in the study, there also will be an interviews.

In order to prove that there is a significant need for first year non-it students to be educated about cyber security awareness and to design the computer-security program, we need to (1) use case study to understand if there are a consequences of lacking cyber security awareness amoung students, (2) to get the general picture of student's knowledge about cyber risks and online threats and (3) understand student's expectations from university course for the program better design.

3.1 Data collection and analysis

3.1.1 Student's knowledge and course expectations

To collect data about student's knowledge and course expectations author will use convenience sampling. This is a fast, easy and cost effective method of data collection. This type of sampling is done by creating a questionnaire and distributing it to our targeted group. The best way to measure the understanding of the risks that system can bring is with survey. To prepare a questionnaire author is using online survey. For this purpose was chosen site www.surveymonkey.com. This site provides storage and analysis for surveys. This way of collecting the data was chosen because SurveyMonkey is very easy to use and there are available different formats for asking questions like multiple choice, true false, open-ended. SurveyMonkey provide you with a link to the survey that is the best way to use because you can post it to any resource that will help to cover as much participants as possible. Also this site allows to select a number of filters for the collected data and information which is provided for each question shows the percentage of participants who has responded.

There have been designed a “Cyber security awareness” survey to ask how students will respond to the specific cyber security related questions. The survey is anonymous and distributed in a closed group for students in Facebook. This is a special group for student community, where students from different universities share the materials and discuss any topic related to any subject in any university of Estonia. As the survey will be anonymous it will help to receive honest answers because students will not be worry to save their face, because our goal is to focus on what, and not who. Second it will give us a general picture among universities as there are will be answers from the students who present different universities and faculties. Third author explained that this a knowledge control and asked do not search in google, but for some type of questions to answer honestly: yes or not. Survey consists of 19 questions (see Appendix A) and conditionally can be devided into two parts. First part will help to collect general information about participants: university, faculty, work experience and will evaluate their security awareness understanding based on their answers to the questions. The second part consist of questions that will help to know what students think about teaching methods and if they in general are interested in taking cyber security awareness course. The answers will help to understand the needs of students, their expectations from the course and will help to design a program that will be really interesting for the first year non-it students.

Survey consist of questions such as multiple choice, multiple select, general “nominal” and open questions. Multiple choice will ask students to select one of the options. Multiple select questions will give the students an opportunity to select as many options as they think right. Discrete questions with the opportunity to answer “Yes/no” will give us a simple count, do the students know something or want something. Open questions will ask students to type their own opinion. Survey should take about twenty minutes to complete.

3.1.2 Sample cases

In the research about knowledge and opinion about teaching methods will be used students who come from different universities and from different faculties. The companies who are agreed to be used in the research are two types: (1) small-size business sales company “A” with the 25 employees and (2) big companies:

- IT company “B” with 255 employees
- Retail company “C” with more than 500 employees around Estonia

Company “A” is a young sales company. The age of employees varies from 22 to 33 years old. IT services they buy from the IT company.

Company “B” is an IT company. The age of employees varies from 19 to 45 years old. The company does not have their own awareness program and they never organized a training about cyber security awareness. During year 2015 and first half of 2016 company have hired 43 new employees. Seventeen new employees belong to the first year students.

Company “C” is a retail company. The age of employees varies from 23 to 65 years old. The cyber security awareness training was organized in September 2014. During the year 2015 and first half of year 2016 company have hired 30 new employees and offered a 10 trainee places.

3.1.3 Consequences of lacking cyber security awareness

In this part of research author will use case study method. This method of study is very useful because it gives opportunity to test the survey results by using them in real world situations. First case study is to test employees from company “A”. The threat is an attacker in the company or by other words a social engineer. Social Engineering uses human error or weakness to gain access to system. The company is small and they do not have their IT department. They use third-party managed IT services. According to the contract the IT guy from this company comes at the office once time in a month to check the employee PC-s and server room. The best way here to see if the employee know what is social engineering and they know how to act in case of such attack is to introduce me as a new employee of IT company who came instead of sick one.

Author will ask employees to use their computers to control their security settings and will use a memory stick. Author justify it by the fact that the management decided to use another antivirus program that author need to download to each computer. This simple manipulating will give us a picture how employees will act if they see a stranger in the office and especially how easy they will give an access to their computers where can be a sensitive data.

In the case studies of company “B” and “C” the most effective way to analyze the situation caused by lack of employee’s knowledge in cyber security is by interviewing the IT department CIO. In the both companies “B” and “C” there are were already real cyber incidents during year 2014 - 2016. In company “B” the incident have happened in the April 2016 and was presented by e-mail with a malicious attachment.

In the company “C” the first two cyber incidents were in year 2014. The cyber security awareness for employees was organized in the same year. The incident in 2016 have happened in February 2016 and was presented by e-mail with the malicious attachment.

4 Analysis

As Clint Eastwood once said, "If you want a guarantee, buy a toaster." The only secure system is one that's unplugged, turned off, and in a locked room. Since it's not practical to leave our systems turned off, we need to understand the risks to our systems and prepare ourselves to defend them. Preparation begins with understanding — and that's where awareness comes in. [6]

4.1 Case study

We are responsible for what we are doing and we have to understand that every our decision to do something or not to do, have the consequences. Case study are represented by example of 3 companies and based on two types of attacks: social engineering and malicious attachment in e-mail. After analysis we have a clear picture of consequences of lacking cyber security awareness among students.

4.1.1 Social engineer in company "A"

The results of social engineering attack in a company are represented by human based deception. After introducing myself as a new employee of IT company, I explained that the guy who usually comes is sick and I will be instead of him. Surprisingly, but all 19 employees who were at work this day, no one have asked any provement from me. They just trusted me. Another fact they work in sales company. In their computers, they have a sensitive information like client lists, customer databases, financial details, the company deals, their pricing information, design of their new unique products that they plan to sell in the market and they have let me to use a memory stick. After I said that I need to download new antivirus from memory stick and this will take around 30 min, only 4 employees from 19, stayed near me at least to watch what I am doing. The other 15 just let me to be alone with their computer and were not interested what else I could do with memory stick. It is a small-size business, they do not have any security policy and as a result we can see that 19 employees are a potential danger to company data due to the lack of knowledge not only about social engineering but about cyber security in general. Employees can not even imagine that such simple attitude as trust, ignorance or carelessness can cost their company not only financial lost but what is most important the lost of reputation. And as a reason it can cost them their job.

4.1.2 Malicious e-mail in IT company "B"

The malicious e-mail in company was send in April 2016. The financial damage for the company was around 7, 000 euro. In the incident were involved 27 employees. Among this 27, malicious attachment was opened by 10 employees who are all working students. On the Figure 2 we can see that 2 students are from HR department, 3 students are from accounting department, 1 from sales department, 1 is company assistant and what is most surprising that 3 students are from IT department.

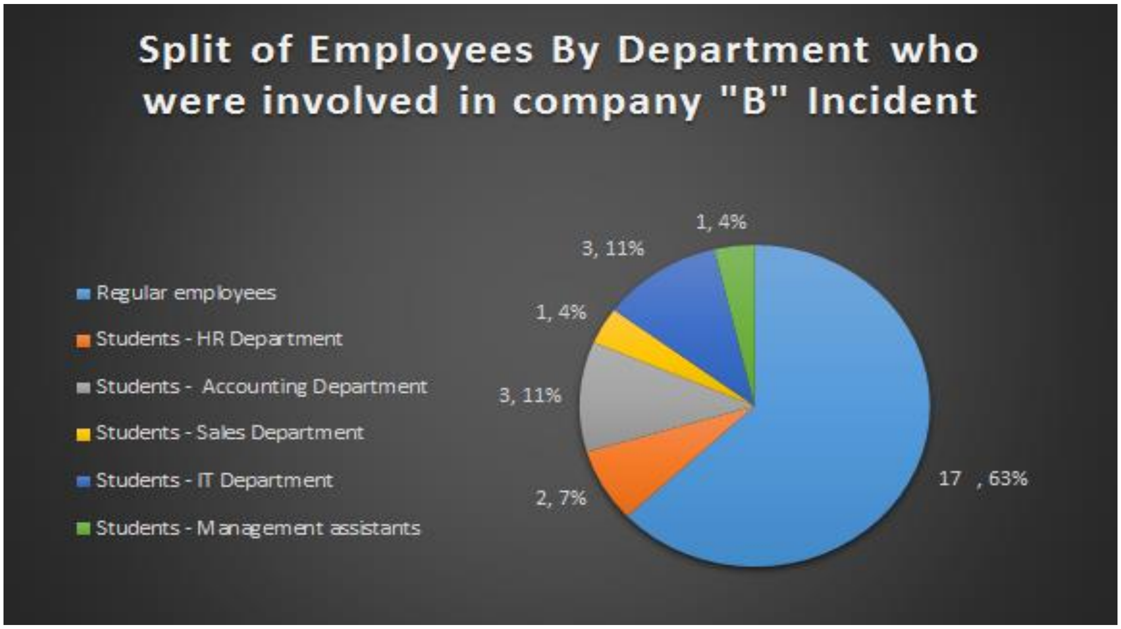
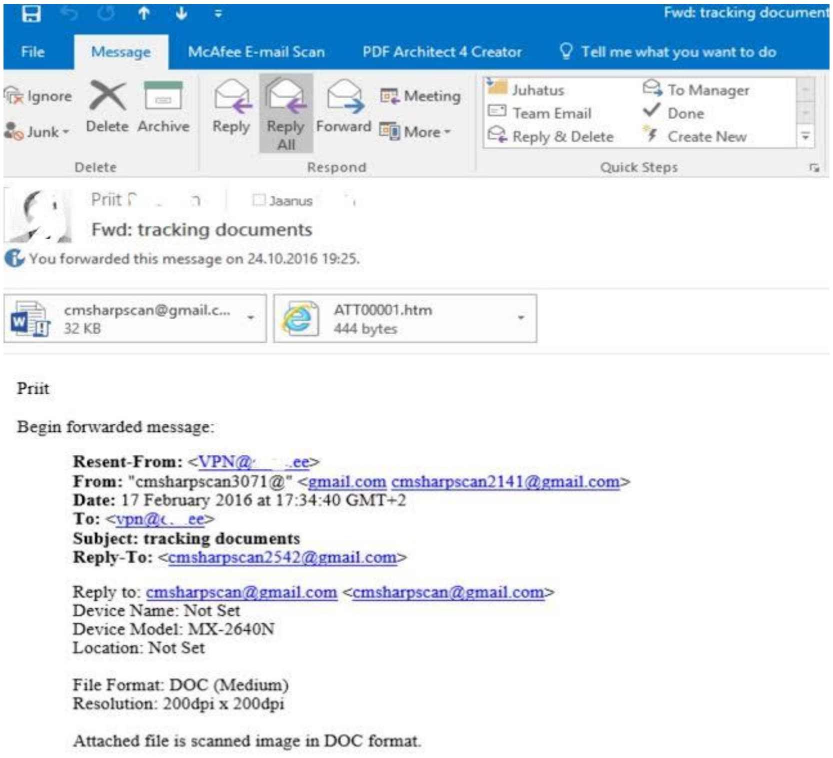


Figure 2. Company "B" employees involved in incident

4.1.3 Malicious e-mail in retail company "C"

The IT department of the company "C" make a report for each cyber security incident that have ever been in the company. After the reports analysis for the incidents in year 2014 - 2016 it is clear how is important cyber security awareness course and what could happen if the employee has a lack of knowledge. During the first half of the year 2014 the company was hacked 2 times. First incident was in January 2014 and was presented by e-mail with attached virus that have encrypted the files. The second one was in March. It was an attempt of social engineering, when in the office was found and used memory stick with virus. According the company report the financial damage from these 2 incidents was 48,000 euro.

In the year 2015 there were organized a cyber security awareness training. The last cyber incident was in February 2016. There were again send a malicious e-mail with attached virus shown on Figure 3.



Fwd: tracking documents

You forwarded this message on 24.10.2016 19:25.

Priit

Begin forwarded message:

Resent-From: <VPN@ .ee>
From: "cmsharpscan3071@" <gmail.com cmsharpscan2141@gmail.com>
Date: 17 February 2016 at 17:34:40 GMT+2
To: <vpn@c. ee>
Subject: tracking documents
Reply-To: <cmsharpscan2542@gmail.com>

Reply to: cmsharpscan@gmail.com <cmsharpscan@gmail.com>
Device Name: Not Set
Device Model: MX-2640N
Location: Not Set

File Format: DOC (Medium)
Resolution: 200dpi x 200dpi

Attached file is scanned image in DOC format.

Figure.3 Malicious e-mail of the company “C”

On the Figure 4 we can see that in the year 2014 the number of involved employees is 63. In the year 2016 the total number of employees involved in incident is 24. Among this 24, only 6 employees who received an awareness training were involved again.

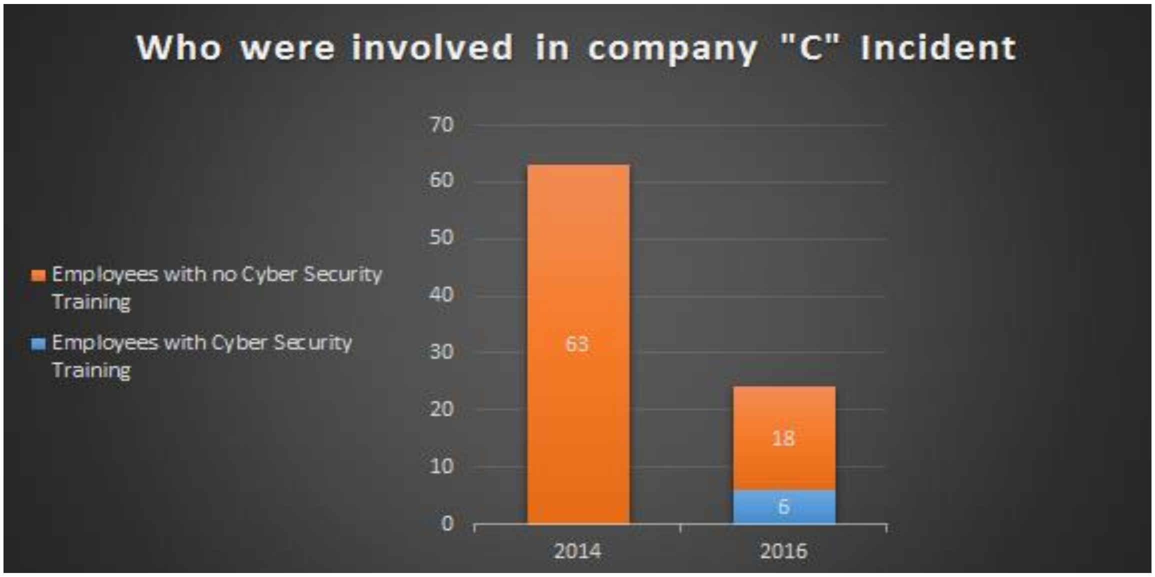


Figure 4. Company “C” employees involved in incident before and after cyber training

According the company records these 18 employees are the new hired one and they never received a cyber security awareness training. 6 out of this 18 are the students to whom was offered a trainee place. On the Figure 5 we can see that 1 student is from HR department, 2 students are from accounting department, 1 from development department and 1 from category management department.

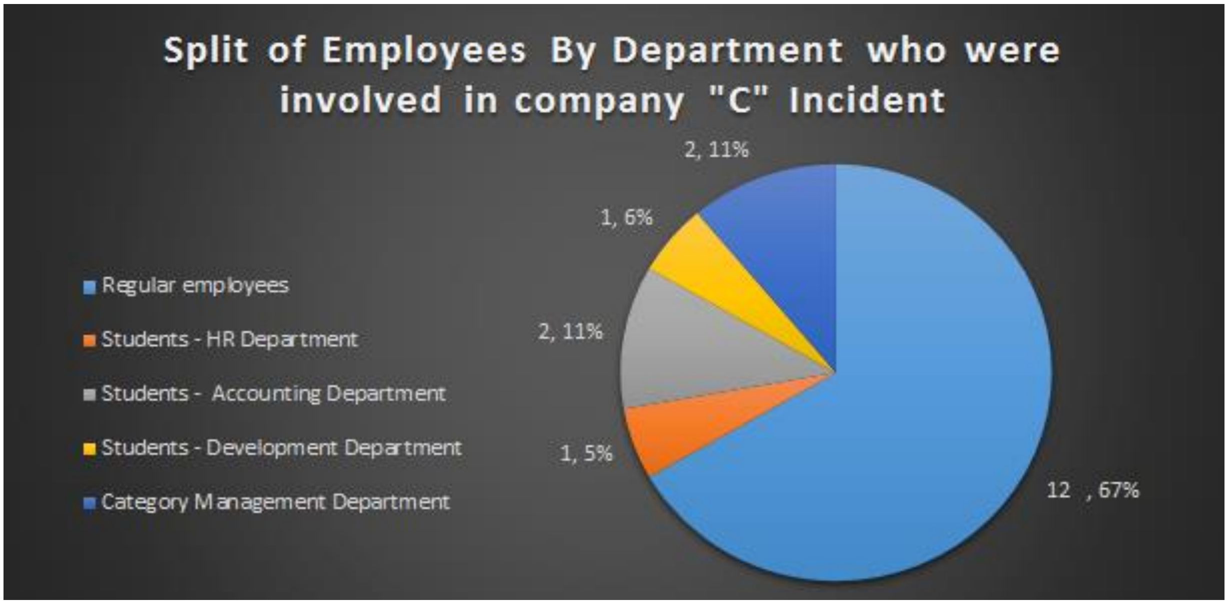


Figure 5. Company “C” employees involved in incident in year 2016

4.2 Survey analysis

After first results based on the example of case study, in general author can say, that there is a lack of knowledge about cyber security and students do not understand the risk that technology using can bring and stay vulnerable to different types of attack. The next step is to look at the general picture of student's knowledge about cyber risks and online threats and to analyze the course expectations.

After analyzing the results of first three questions, author have got the clear picture which audience we are dealing with. Figure 6 indicates that among 250 students who took a part in survey 40% study in the Tallinn University, 37% in the University of Tartu and 23% in the Tallinn University of Technology. On the Figure 7 we can see that that majority of students 30% study economy, business management and sociology study 23% of students, 16% of students are from law faculty and only 8% study IT. Among 250 survey participants 12% work as shown on Figure 8.

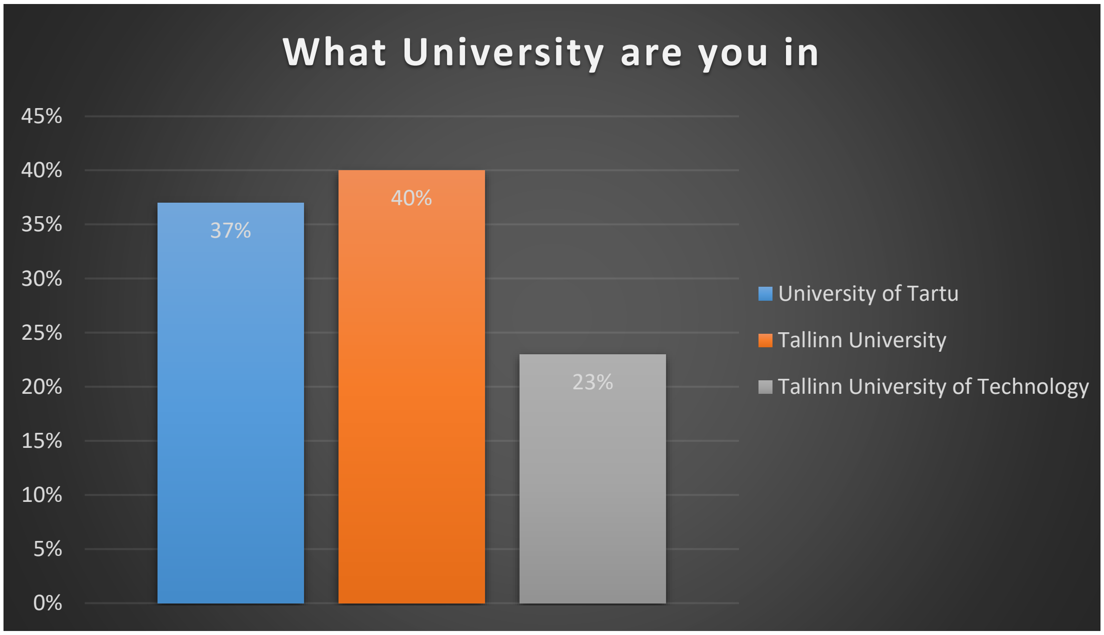


Figure 6. The university of respondent

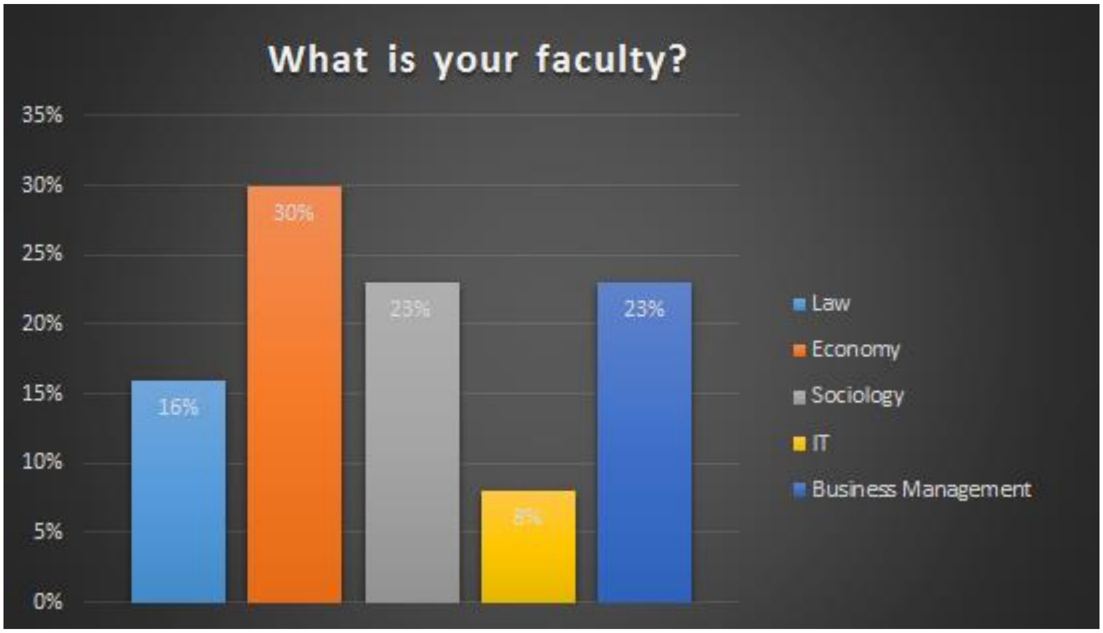


Figure 7. Faculty of respondent

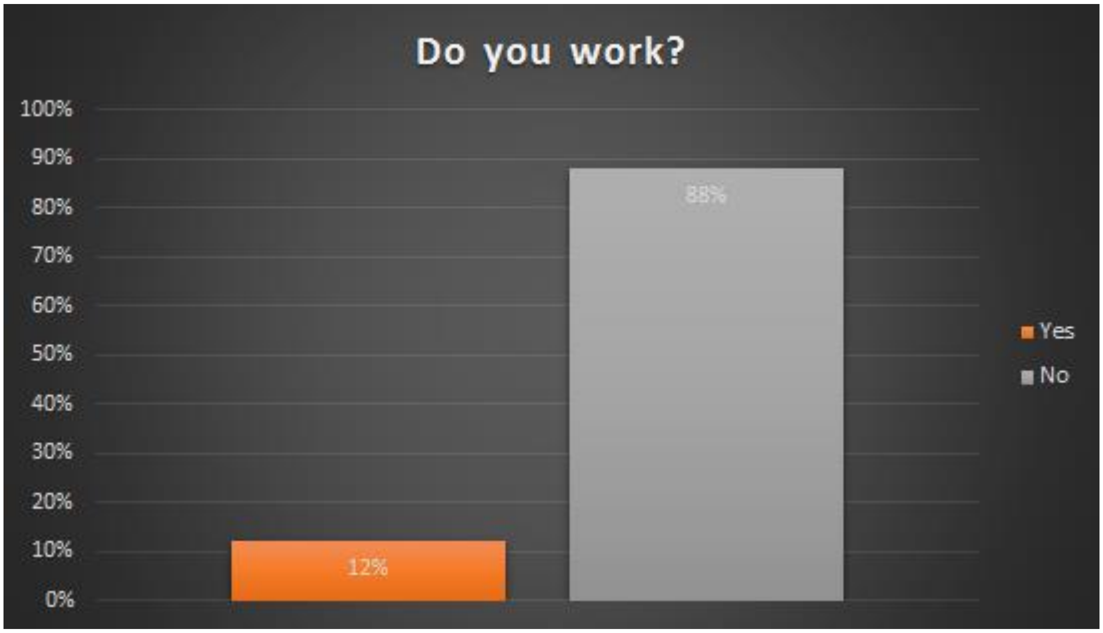


Figure 8. Students work experience

The result on Figure 9 show, that the student’s every day life very closely connected with computer and Internet. 96% respondents said that they always use PC and only 4% use it sometimes.

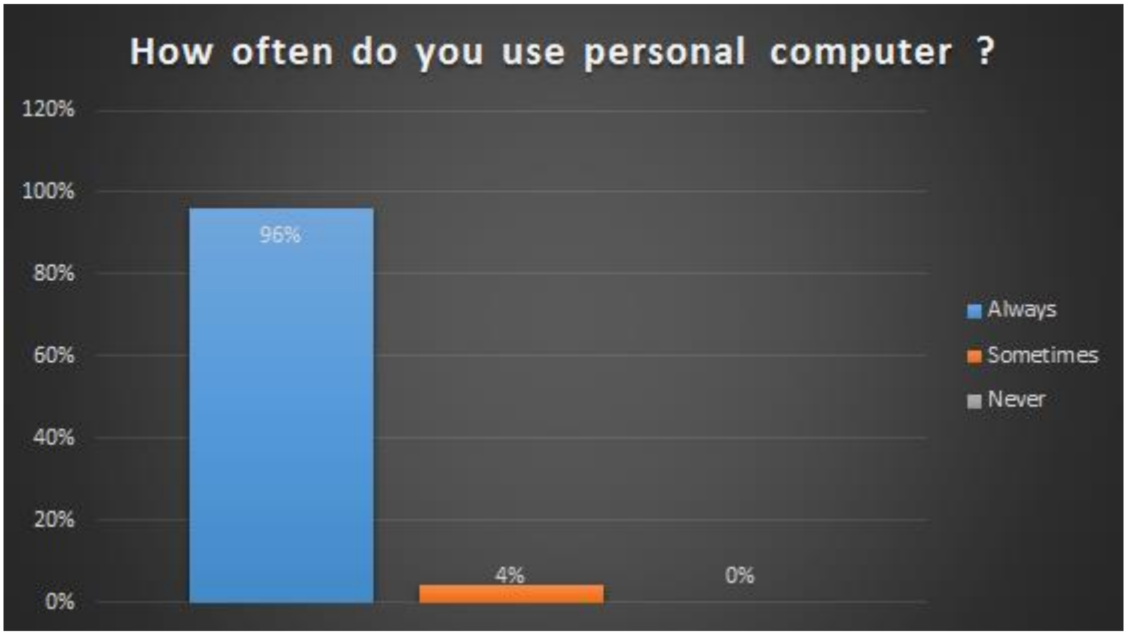


Figure 9. Student dependence on Internet

Shutting down the electronic devices is necessary to reduce the hidden and malicious activities by attackers. Questions about leaving computers working, when students don’t work with them on Figure 10 indicate that 46% sometimes leave their computers running. 38% of students always leave their PC working and only 16% always close their computers after they finish to work with them.

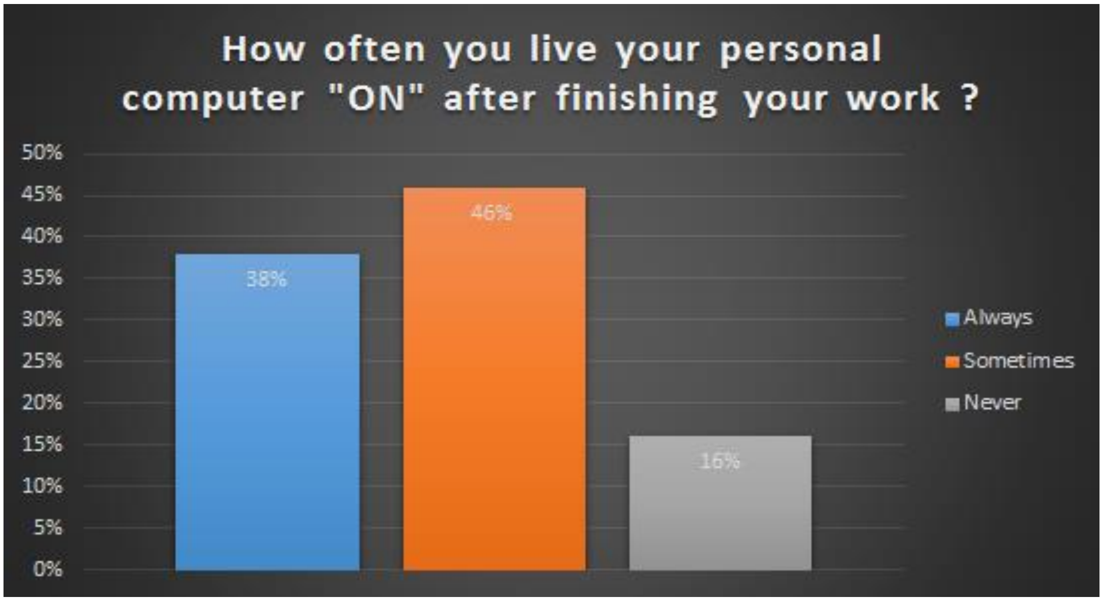


Figure 10. Leaving computer ON when not in use

Virus and spyware. These programs are more than annoying. There is an increasing problem of adware and spyware. Such software is installed on an end-user system when visiting a website. It may collect private and web behavioural information of the user. Side effects are involuntary web redirections and pop-up advertisements as well as the risk of loss of privacy. [7]

The result of this question on Figure 11 shows that 80% are at least aware about antivirus and the protection it is provides. At the same time the 58% of the students do not know what is spyware that in turn put them into situations where they are vulnerable to attackers. Also in the significant risk the 43% of the students who are aware what are antivirus and antispyware but unaware of how to tell whether or not it is running. On the other hand, in spite of the fact that students install antivirus or antispyware programs 67% don't customize security settings, 27% of students even don't know how to do it and only 5% answered that they can and do, as shown on Figure 12.

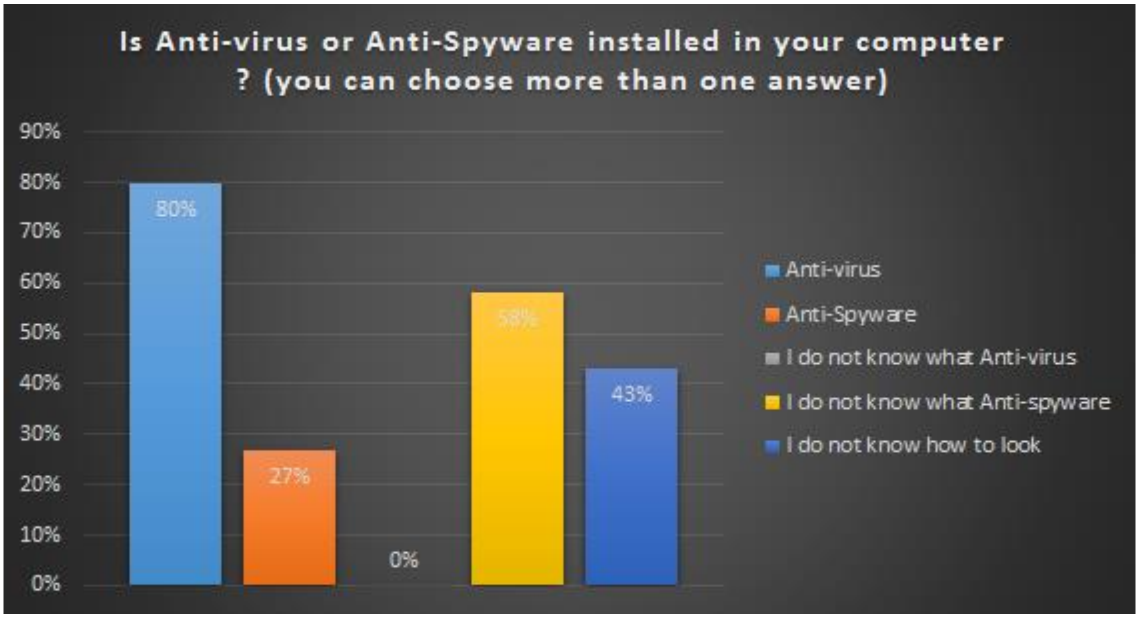


Figure 11. Using of antivirus or antispyware

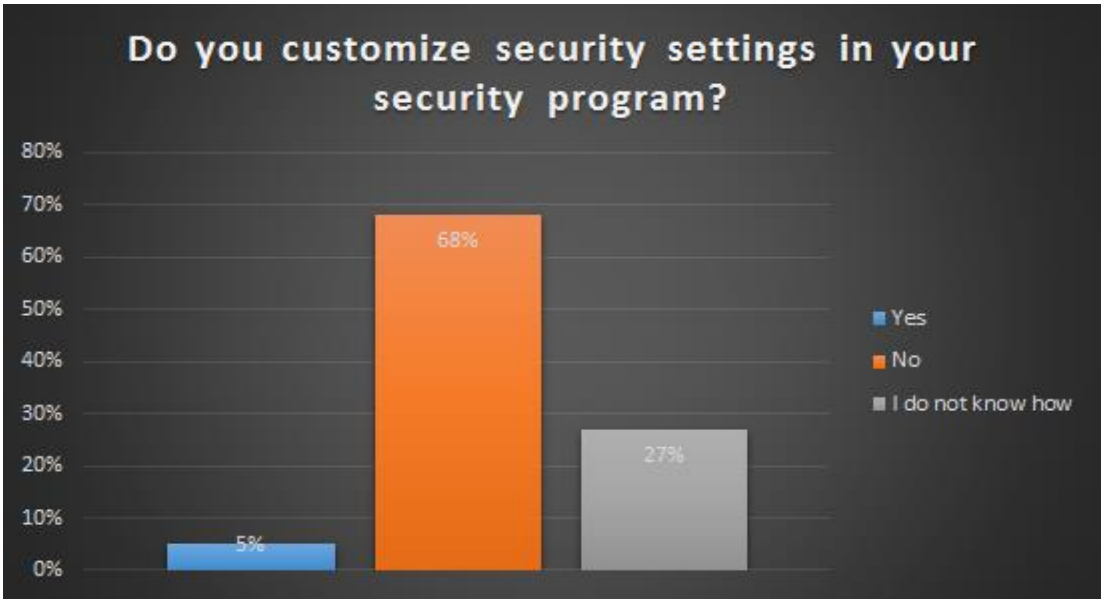


Figure 12. Customizing security settings

Updates of computer are very important, because most of them include security updates. And security issues are the worst possible errors that can be exploited and used by malware or attackers. The Figure 13 indicates that 20% of students don’t know how to look this information and should be just informed. The main risk present the 58% students who know how to see it, but did not configured it automatically. That may indicate that students do not know or do not understand how important it is for their online security.

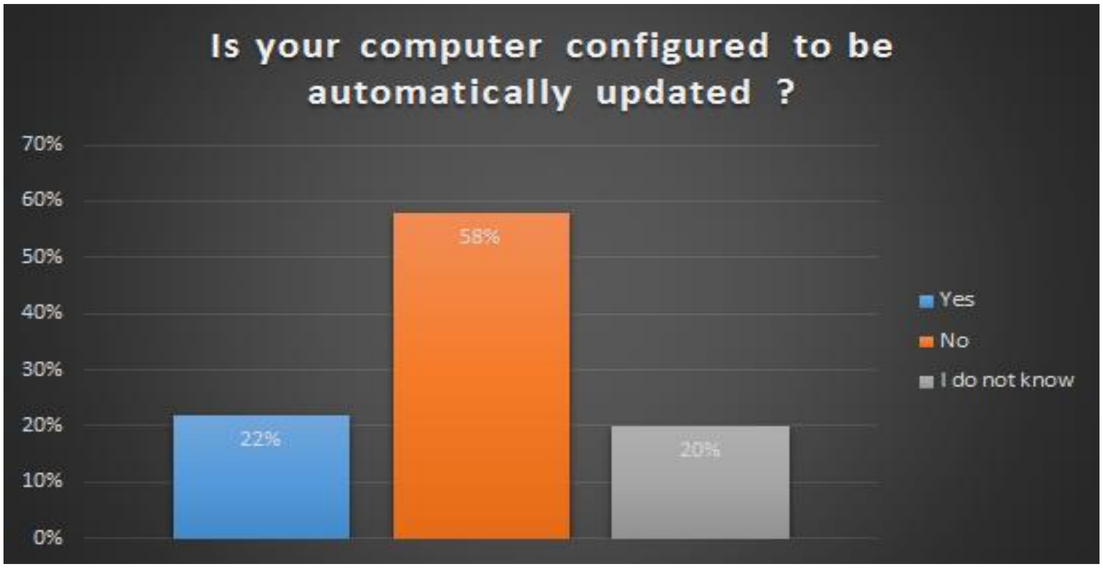


Figure 13. Automatic updates

Today, to have a firewall in computer is necessary the same as to have an anti-virus software. A firewall is like a real wall keeps destructive forces away from your computer. A personal firewall is an application installed on your computer that controls network traffic to and from your computer. Essentially, in order for information to cross the firewall, it must be approved by the firewall's set of rules. A personal firewall together with anti-virus software and system updates, are three important things that help to secure your computer. That is why it is important to understand how it works. Figure 14 indicates that only 4% of students have an idea what is personal firewall. The rest 96% not.

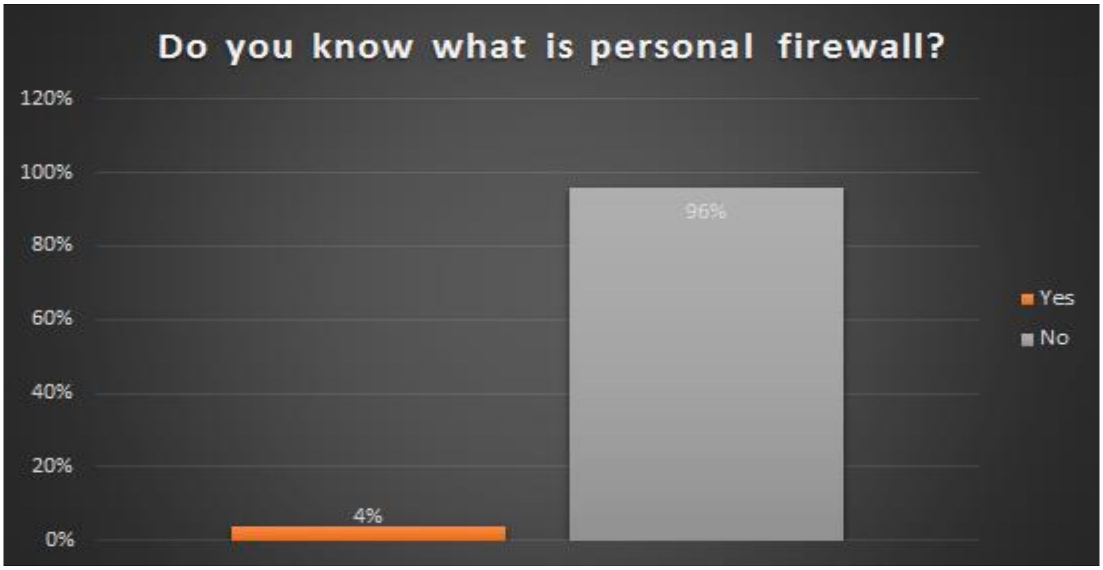


Figure 14. Knowledge about personal firewall

Phishing is also one of the online threat. Using this way attackers usually create a clone of website and ask user to put or update their personal information such as usernames, passwords, credit cards and so on. Then all this information will be directed to attackers. Figure 15 shows that majority of students 74% are do not aware how to identify it.

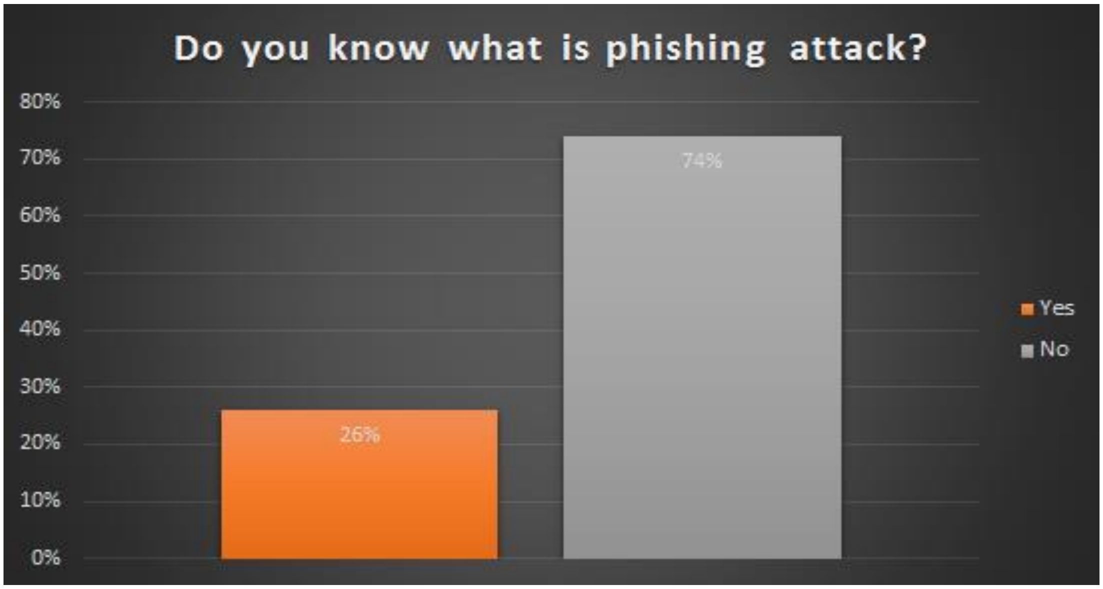


Figure 15. Knowledge about phishing attack

Emails and especially attachments can be really dangerous and harmful. The majority of the students 68% shown on Figure 16 have answered that do not inspect an attachment as long as they trust the source of this e-mail. 27% do not know how to inspect and only 5% have answered that they always inspect links and attachments. The students in first 2 groups are in significant risk, because they first have lack of knowledge how to inspect and second they don’t understand that an attachment can be malicious even if you know the sender.

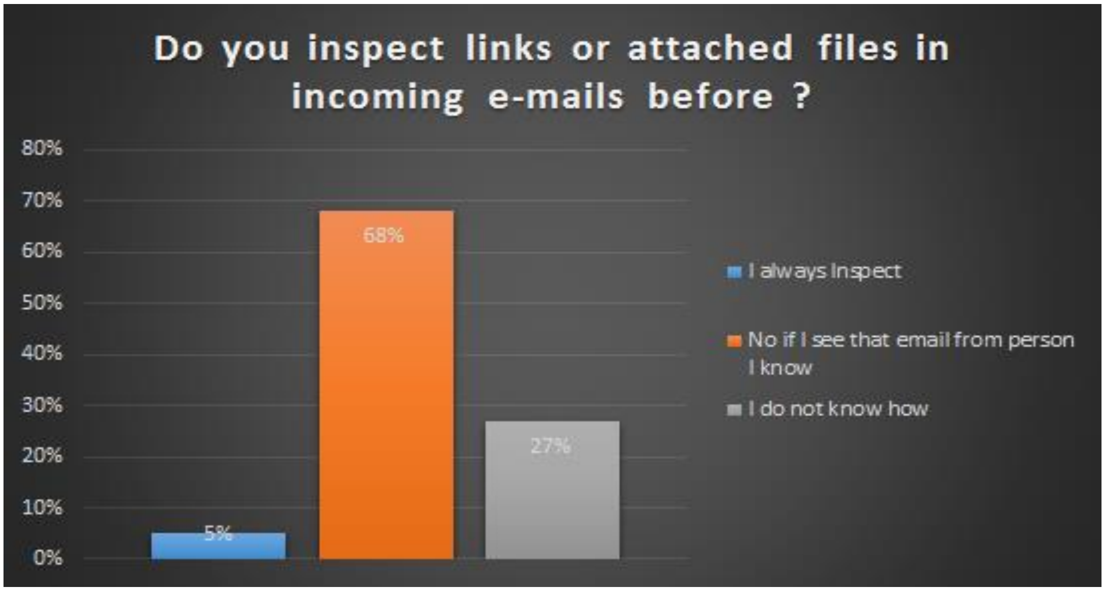


Figure 16. Inspecting e-mail links and attachments

Social engineer is an attacker who exploit an organization weakness like human. Using different techniques they trick employees into offering them access to sensitive information. Unfortunately, on the Figure 17 we can see that only 22% of students aware about it. The rest 78% are potential security gap in organization where they work or will go to work.

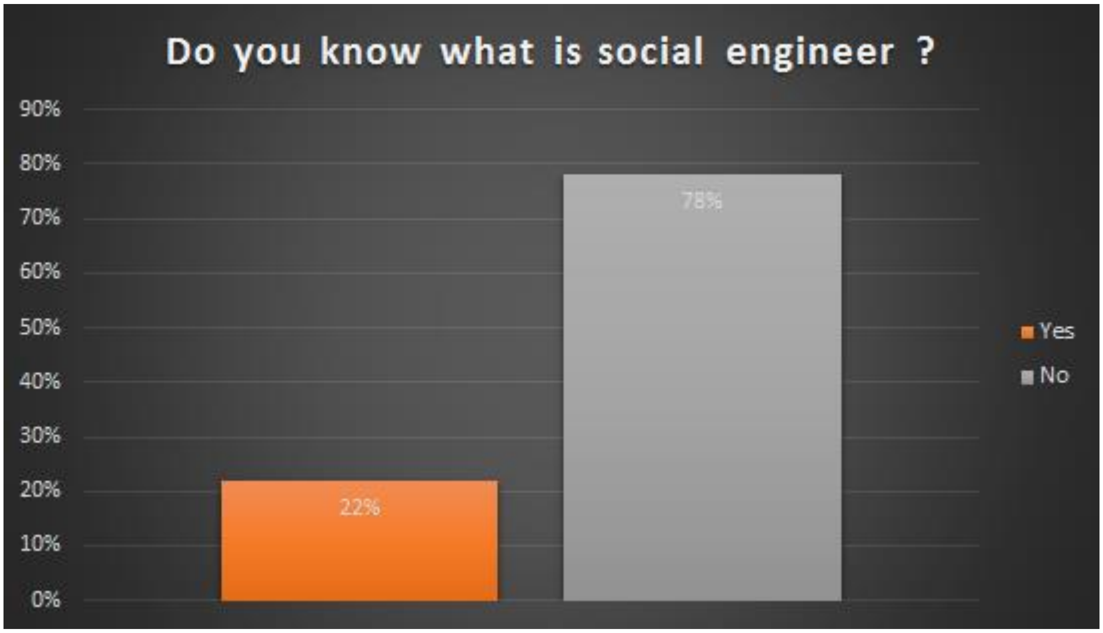


Figure 17. Knowledge about social engineer

Passwords using and remembering is also one indicator of becoming an attacker's victim. The Figure 18 indicates that 37% have one strong password but unfortunately they use it for different accounts. 57% allow computer to save their passwords, 4% of students write it down on paper and only 2% have chosen the other option and answered that they use a password manager. Question about knowing what is password manager indicates some of the result shown on Figure 19 and proves, that only 2% of students who take part in survey answered that they know it. As shown on Figure 19 unfortunately the majority like 98% don't know what is password manager.

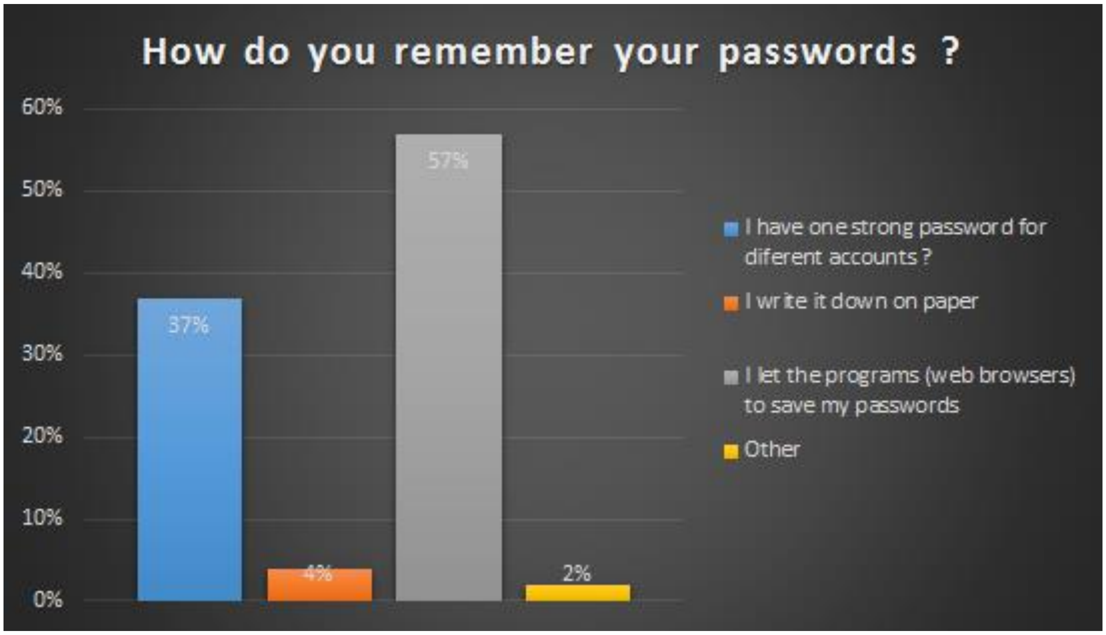


Figure 18. Passwords memorizing

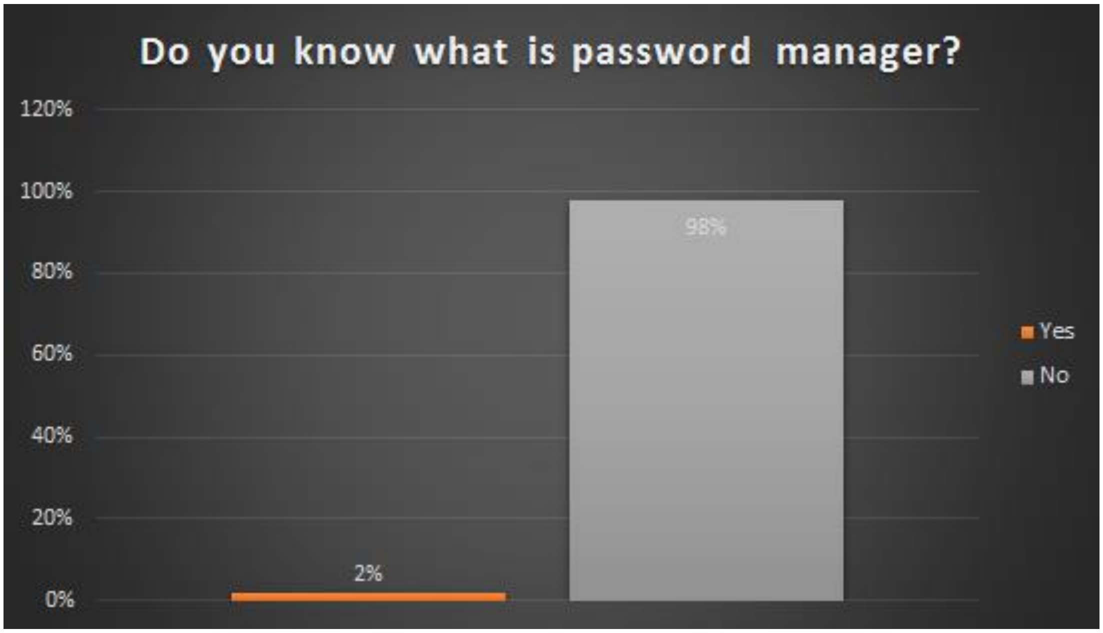


Figure 19. Knowledge about password manager

On the Figure 20 it can be seen that the most preferable teaching method is a group work. Over half prefer to study during seminars. The third method is practicals with 40%. Unfortunately, but not unsurprisingly, the most unpopular are lectures 22% and distance learning 18%.

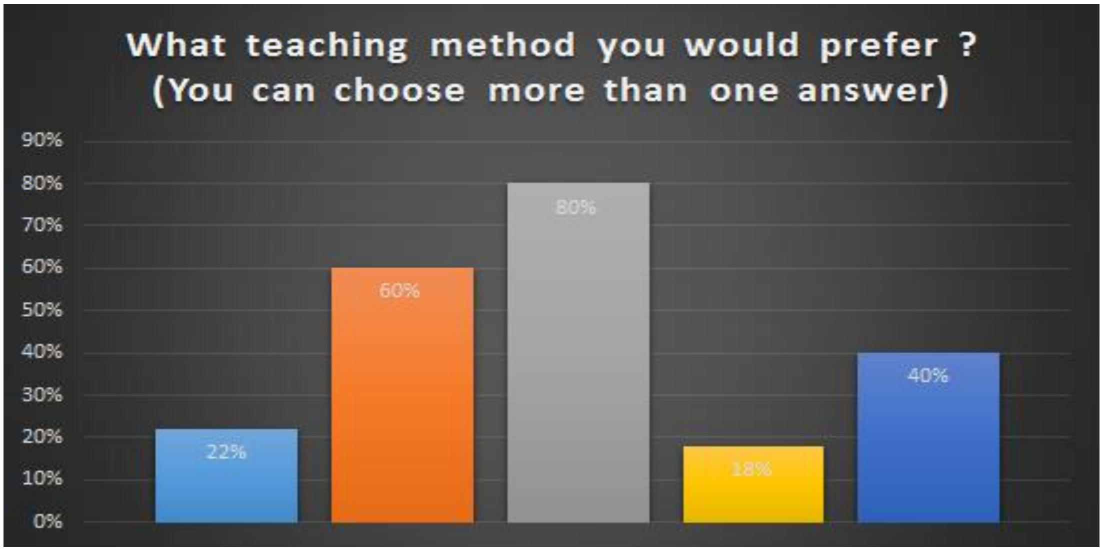


Figure 20. Teaching methods

The next question was asked to understand better how students see the course they can be interested in. As the question of survey was not mandatory author have received only 60 answers. It was very surprisingly to read that all 60 respondents concurred that the most important thing what makes a course interesting is understanding and knowing its usefulness. It is very logical. As long as you understand that you have a lack of knowledge which you really need in life, especially not only for work but for your daily life you are motivated to study.

Second popular answer is connected with the course structure and actually it is somehow describes the results of the first question that is shown on Figure 20. Students have mentioned that the general university course is a lecture. Unfortunately, lectures were described as a boring way of teaching, when students have just to seat and listen. Most lecture even not listen but do other things in their personal devices like smartphones or PC. Especially they are disappointed with the lecture structured course where attendance is mandatory. Majority of respondents described an interesting course as a mix of group work and seminars. Students have mentioned that they would prefer a course where the main person is not a teacher who just read from slides but the whole course together “teacher + students”. Group work makes a course interesting because of collaboration. Students who study together, they learn more better and more quickly. You don't need to spend a lot of time if you have difficulties, you can always ask to help. Also group work helps to understand material better.

An interesting course can not exist without a teacher. It is logically that a teacher makes a course and from teacher depends what kind it will be. That is why it was important to know what student expect from teacher. Unfortunately, only 15 respondents described the “ideal” teacher, but the mentioned is enough that could help to make a right conclusion. Answers analysis shows that students would like to see as teacher a person who creates a welcoming learning environment in class. So they expect that teacher will be positive and with the sense of humor. Second, students understand that for every teacher his course is very important, but they mentioned that a good teacher also understands that his subject is not the only one in curriculum and pays more attention for participation but not for grades. On the one hand also is very important for teacher his communication skills. Teacher should be a very good communicator. But on the other hand he should be a very good listener. There is a proverb “If speaking is silver, then listening is gold”. Students need a teacher who respect and value the opinion of each student.

Successful study begins with acceptance that you have a lack of knowledge and motivation to receive this knowledge, it was important to ask two last question. The results of this question on Figure 21, unfortunately shows us that although our education systems requires students to use a personal computer, we are not in hurry to teach them how to use this computer safely.

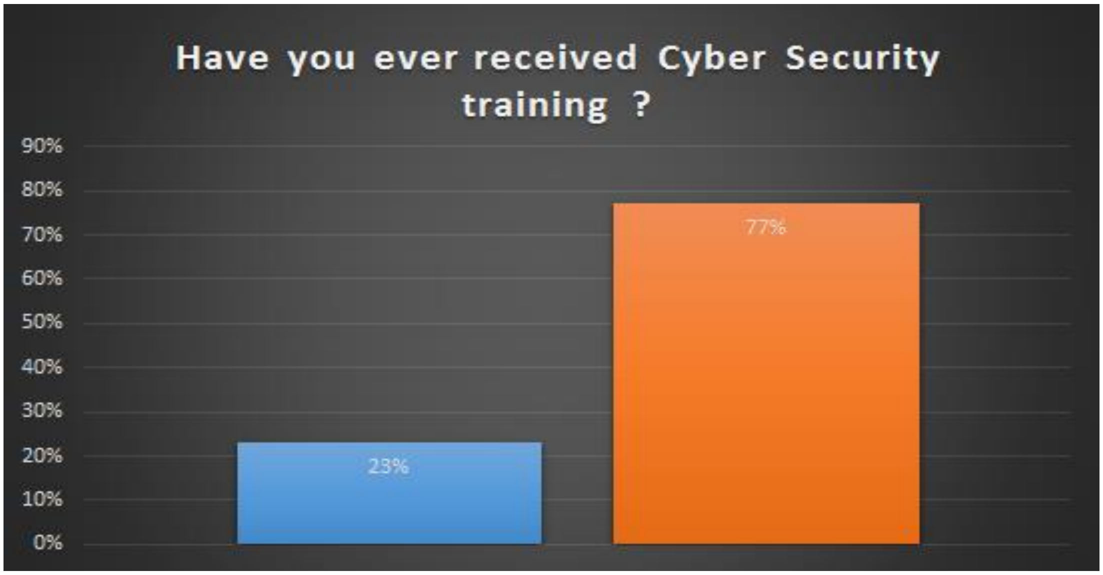


Figure 21. Receiving of cyber security training

On the Figure 21 we can see that only 23% of respondents have received a cyber security awareness course. It is hard to say where from where they received such course. Were they the students who work or they used any online course. It is not so important now. More important to see that 77% of respondents have not. Actually it is a frightening result. It means that majority of respondents are not ready to protect themselves and as the reason they become one of the most significant security risks that organization where they work can face today.

Despite the fact that majority of respondents have never been trained about cyber security, the results shown on Figure 22 give us an optimistic hope that nothing is lost. It is a very good indicator that all this 84% of respondents feel and can honestly accept that their knowledge in this topic are weak and they are interested and ready to take cyber security awareness course.

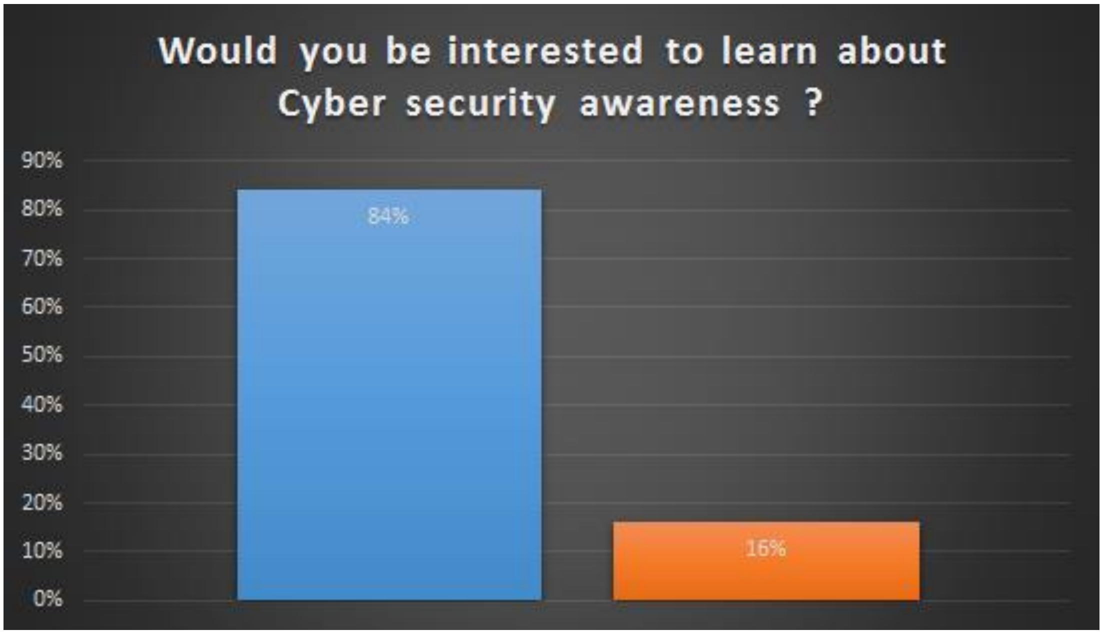


Figure 22. Interest in cyber security training

There is also 16% of respondents who are not interested in such course.

4.3 Conclusions

The analysis of the case study based on the examples of three different companies have showed, that cyber attacks on the companies exist and bring a financial damage. Unfortunately, the success of these attacks was possible due to the lack of knowledge about them and the simple understanding how to act to protect. The analysis of the survey answers has proved the case study results and showed that the majority of students do not understand what is social engineering, how dangerous the e-mail attachments can be and so on. They stay vulnerable. At the same time the result has showed that students understand that they have the lack of knowledge and ready to fill that gap and take a cyber security course. Based on the both result the case study and survey author is sure that there is a significant need to be educated about cyber security awareness and to design a cyber security course for first year non-it students which will be described in the next chapter.

5 Proposed Awareness Program

In the previous chapter author with the help of basic security questions provided in the survey have analysed and concluded that there is a significant need to educate first year non-it students about cyber security. The questionarie is general and gives us only the half of picture what topics cyber security awareness course should consist of.

As we need and effective course, to create it author will firstly use the pedagogical model of teaching and secondly Benjamin Franklin said: “Tell me and I forget. Teach me and I remember. Involve me and I learn. As long as you study something you will remember it. And as long as you remember it is already effective. Any knowledge received during any course make this course effective.

5.1 Course description

Today the data is the most attractive thing for attackers. No matter is it your personal information stored in your computer or the company business information, the ability to secure data is a growing challenge. Threats to information are global and increasingly sophisticated. And our role as a user is to protect our part of cyberspace, including the devices and networks we use. Our actions have a collective impact and when we use the Internet safely, we make it more secure for everyone. To achieve this, we need to be educated about threats and vulnerabilities. It is important to know how to implement different security practices to make cyberspace more safer.

The name of the course is “Promoting Cyber Security Awareness”. This course is designed to teach first year non-it students to understand the risk, threats and vulnerabilities they can face and the methods to protect yourself. To this end, the course addresses a range of topics, each of which is vital to securing your data. These topics introduce the field of cyber security, technologies, analyse of the the risks and threats.

5.2 Target audience and outcomes

This course is intended for the first year non-it students. It is mandatory for the students from different departments and faculties.

After successful completion of this course, students will be expected to be able to:

- Understand what is cybersecurity and main cybersecurity principles
- Understand the basics of computer networking and communications.
- Understand how data is transmitted across the networks, including wireless networks.
- Understand the threats, vulnerabilities and risks that relate to national, commercial or personal information environments
- Understand the different tools and technologies that can help to mitigate those risks
- Understand the basic of cryptology (private and public keys)
- Understand and explain some of the particular risks associated with email
- Understand what is social engineering and recognise the threat is can pose.
- Understand the mobile devices threats and vulnerabilities
- Understand cloud computing threats and vulnerabilities

5.3 Delivery method

The course will consist of lectures, group works and presentations, quizzes. The course duration is 8 weeks. Teaching delivery include lectures and demonstrations. Also students should be prepared that for some course topics teaching delivery will include small-group work. Students have to prepare materials in groups and to present this material in class. There will be a small assessment after each topic. At the end of the course assessment will cover the whole teached material

5.4 Grading

The grading of the course will consist of:

Class participation (20%): The typical week lesson will be presented by combination of lectures provided by instructor and presentation of the topic prepared by students during the group work.

Group work + presentation (30%): The students will be asked to divide into groups and to prepare presentation for some topics. Two days before the next lecture students have to send the slides of presentation to the review. It will give an opportunity to instructor to make the quizz for other students based on the presented topic.

Quizzes (20%): To motivate students to listen the instructor and take an active participation in the classmates presentations, each lecture will be ended with the short quizz. Depends on the topic quizz will consist of 7 till 10 questions that will cover the lecture material.

Final exam (30%): The final exam will cover the whole course topics.

5.5 Course outline

Lecture 1: Introduction to Cyber Security

- Introduction to the course
- General overview and definitions
- Basic cyber security principles

This lecture will introduce students the course aim, delivery method and grading system. Also there will be covered topics that will introduce the basic cyber security definition like threat, vulnerability. Students will also know what is information security and basic security principles such as confidentiality, integrity and availability. The lecture will be delivered by teacher.

Lecture 2: Overview of Networking

- TCP/IP
- Wireless
- Internet

The lecture will provide a general information about network. The history of network. Students will know what is protocol, how data is transmitted across the networks, including wireless networks. Also will be introduced information about Internet and how it works. The lecture will be delivered by teacher.

Lecture 3: Introduction to authentication

- Passwords
- Salt
- Password manager

The lecture will introduce basic knowledge about the role of the passwords and how the authentication works. Also it will be introduced how to use password managers and what is two-factor authentication. The lecture will be delivered by teacher.

Lecture 4: Cryptography/Encryption

- Introduction to Cryptography / Encryption
- Digital Signatures
- Public Key infrastructure

Lecture will provide the basic knowledge about what is cryptography and encryption and why it is important. Also the lecture will introduce the world of digital signatures. Explains what is public and private keys. How the ID cards work.

Lecture 5: Social engineering attacks

- Social Engineering
- Techniques

- Examples
- Countermeasures

The material for this lecture will be prepared and presented by the group of students. Students have to explain what is social engineering, give as much examples as possible about the techniques of this attack and provide possible countermeasures.

Lecture 6: Malware

- Virus
- Worm
- Trojan horse
- Spyware/Adware/ Scareware
- Rootkit / Backdoor

Lecture will be prepared and presented by groups of students. The topics will be divided between 3-4 groups. Each group should explain what kind of malware they talk about. To make a short introduction to the history, provide an examples. Introduce the countermeasures.

Lecture 7: Network security

- Firewalls
- VPN (should be presented by group of students)
- IDS

The lecture will give the general information about the firewall, different types of it. Also it will be explained how to use them for protection. Also it will be introduced the basic information about IDS. The group of students should prepare and introduce material about what is VPN.

Lecture 8: Mobile Devices and Cloud Computing

- Introduction to Mobile devices operation systems
- Mobile devices threats and vulnerabilities

- Introduction to cloud computing
- Cloud computing threats and vulnerabilities

The last lecture will provide an information about mobile devices and cloud computing threats and vulnerabilities. The lecture will be provided by teacher.

5.6 Course evaluation and future development

As this is the first time we will offer this course, the students opinion and feedback is valuable to improve the course for future students. The evaluation will be mandatory after the final exam.

There is also a significant need to improve the questionary and after a year passed after the successful introduction of this course to make a research again. This will give the ability to measure the course effectiveness by statistical data and find the knowledge gap that get unnoticed due to the questionary presented in this research.

6 Summary

The internet has slowly taken over every aspect of our lives. All governmental, industrial, and economic systems depend on computer network. Huge amount of sensitive information stored and transmitted across the network which forced the companies to pay more attention to the security of IT infrastructure. Some companies invest a lot of money for the new designed technologies to protect their data and hire the best cyber security specialist but still face with the cyber attacks due to the lack of employee knowledge about cyber risks.

In the universities we teach students to be a good specialists and to perform their jobs in accounting, sales, law, medicine, engineering and so on, but lack to teach them the basic knowledge about the risks to the systems. Although they are the most important group who need to be aware about cyber security. Firstly all their high education depend on internet, secondly they are potential employee or trainee. And if they are not aware about cyber security they can become a perfect target to attackers. Also they belong to the age group that can teach younger ones like brothers and sisters and also to be a good teachers for the older people, like parents, grandmothers or grandfathers.

In order to prove that there is a significant need for first year non-it students to be educated about cyber security the author used convenience sampling and case study research methods. There was designed a “Cyber security awareness” survey that conditionally consist of two parts. The first part of survey asked students to answer basic questions related to cyber security. The second part asked question that could help to understand student’s needs and expectations from the course. After analysis of the answers from the first part the results showed that there is a significant need to educate students about cyber security. The majority of them do not understand the risk that computer can bring and stay vulnerable to different `types of attack. The second part gave an overview about general students preferences like type of course, type of teacher and showed that there is a interest to be educated about cyber security. The case studies based on the examples on three different companies have proved the results of survey in real life situations.

Based on this results author offered to provide an effective education to first year non-technical students and as a result after designed the course “Promoting Cyber Security Awareness”. This course consist of 8 lectures that introduce the field of cyber security. After successful completion the students will be expected to understand what is cybersecurity and main cybersecurity principles, the basics of computer networking and communications, understand the threats, vulnerabilities and risks, different tools and technologies that can help to mitigate those risks and to protect both yourself and the employer.

References

[1] "Symantec," 2016. [Online]. Available: https://www.symantec.com/security_response/publications/monthlythreatreport.jsp. [Accessed 5 November 2016].

[2] "Stay Safe Online," 2016. [Online]. Available: https://staysafeonline.org. [Accessed 14 October 2016].

[3] "Riigi Teataja," [Online]. Available: https://www.riigiteataja.ee/en/eli/530102013003/consolide/current. [Accessed 20 December 2016].

[4] D. J. David, "The importance of sharing knowledge," [Online]. Available: http://www.greateducationdebate.org.uk/articles.the-importance-of-sharing-knowledge.html?author=dr-david-james.

[5] R. M. Thomas, "Blending Qualitative and Quantitative Research Methods in Theses and Dissertations," Corwin Press, 2003, p. 240.

[6] "Native Intelligence Inc," 2016. [Online]. Available: http://www.nativeintelligence.com/. [Accessed 22 November 2016].

[7] E. A. Luiijf, "The Current State of Threats," 2004.

[8] E. Cole, Network Security Bible, Wiley, 2009.

[9] E. Chien, "Techniques of Adware and Spyware," Symantec Corporation, 2005.

[10] P. Sommer, "Reducing Systemic Cybersecurity Risk," University of Oxford - Oxford Internet Institute, Oxford, 2014.

[11] S. Hawkins, "Awareness and challenges of Internet security," MCB UP Ltd, Minnesota, 1993.

[12] L. Phifer, "Dealing With Adware and Spyware," *BUSINESS COMMUNICATIONS REVIEW*, pp. 44-51, 2006.

[13] J. Aycock, Spyware and Adware, Springer, 2011.

[14] C. Hadnagy, Social Engineering: The Art of Human Hacking, Wiley, 2012.

[15] D. Gragg, "A Multi-Level Defense Against Social Engineering," SANS Institute, 2002.

[16] H. Venter, New Approaches for Security, Privacy and Trust in Complex Environments, Springer, 2003.

[17] M. Jakobsson, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identiti Theft, Wiley, 2007.

[18] E. Cohen, Where Parallels Intersect, Informing Science Press, 2005.

[19] J. Feldman, The Science of Learning and art teaching, NY: Thomposon Delmar Learning, 2008.

[20] M. .. J. Howe, A teacher Quide to psychology of learning, Oxford: Blackwell Publishers, 1999.

[21] L. MacKenny, Improving human learning in the classroom, Landam: Rowman and Littlefield Publishers, Inc, 2008.

[22] P. Rose, "Pedagogy, Curriculum, Teaching Practices and," UK Aid, London, December 2013.

[23] S. Vieluf, "Teaching Practices and Pedagogical Innovation," OECD Publishing, Paris, 2012.

[24] G. Wiggins, "Understanding," Columbia University, Columbia, 1998.

[25] J. S. a. M. Kaplan, "Creating Your Syllabus," *GSI Guidebook, University of Michigan* , pp. 18-22, 1992.

[26] T. M. Brinthaupt, "How Should I Offer This Course ?," *MERLOT Journal of Online Learning and Teaching*, pp. 326-336, 2014.

[27] S. S. A. T. Chris Gutzman, "Differences and Similarities of Spyware and Adware," University of Minnesota Morris , Minnesota.

[28] J. Misko, "Different modes of dilivery," National Centre for Vocational Education Research, 1999.

[29] J. M. Stewart, "Network Security, Firewalls and VPNs," Burlington, Jones and Bartlett Learning, 2014, p. 500.

[30] C. M. Kozierok, "The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference," No Starch Press, 2005, p. 1616.

[31] C. G. Kerry J. Cox, "Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools," O'Reilly Media, 2004, p. 292.

[32] T. U. o. N. C. a. Charlotte, "Effective Ways to Present New Information Orally to Fit Differences in Learning Styles," [Online]. Available: http://teaching.uncc.edu/learning-resources/articles-books/best-practice/large-classes/effective-instruction. [Accessed 12 September 2016].

[33] K. Cochran, "Pedagogical Content Knowledge: A Tentative Model for teacher preperation," 1991. [Online]. Available: http://files.eric.ed.gov/fulltext/ED340683.pdf. [Accessed 11 June 2016].

[34] S. Murphy, "Professional Teaching Portfolio," [Online]. Available: http://teachingportfoliosm.weebly.com/1a-current-learning-theories-and-pedagogical-models.html. [Accessed 17 May 2016].

[35] M. E. T. a. R. v. Solms, "Information security awareness," *Information Management & Computer & Security*, pp. 167-173, 1998.

[36] H. K. a. P. Katerattanakul, "Information security in higher education," *Journal of Information Privacy and Security,* pp. 28-43, 2014.

[37] A. J. a. D. K. S. M. Furnell, "The challenges of understanding and using security: A survey of end-users," *Computer & Security,* pp. 27-35, 2006.

Appendix A – Cyber Security Awareness Questionary

1. What University are you in?

Tallinn University of Technology

University of Tartu

Tallinn University

Other (please specify)

2. What is your faculty

3. Do you work?

Yes

No

4. How often do you use a personal computer?

Always

Sometimes

Never

5. How often you live your personal computer "ON" after finishing your work?

Always

Sometimes

Never

6. Is antivirus or anti-spyware are installed in your computer? (you can choose more than one answer)

Anti-virus

Anti-spyware

I don't know what is antivirus

I don't know what is antispyware

I don't know how to look

7. Do you customize security settings in your security program?

Yes

No

I don’t know how

8. Is your computer configured to be automatically updated?

Yes

No

I don't know

9. Do you know what is personal firewall?

Yes

No

10. Do you know what a phishing attack is?

Yes

No

11. Do you inspect links or attached files in incoming e-mails before to open them?

I always inspect

I do not inspect if I see that e-mail from a person I know

I never inspect, because I do not know how

12. Do you know what is social engineer?

Yes

No

13. How do you remember your passwords?

I have one strong password for different accounts

I write it down on paper

I let the programs (web browsers) to save my passwords

Other (please specify)

14. Do you know what is password manager?

Yes

No

15. What teaching method do you prefer? (you can choose more than one answer)

Lectures

Seminars

Groupwork

Distance learning

Practicals

16. What for you means an "Interesting course"?

17. What do you expect from teacher?

18. Have you ever received a cyber security awareness training?

Yes

No

19. Would you be interested to learn about cyber security awareness?

Yes

No