Erasmus+ KA2 - KA220-HED - Cooperation partnerships in higher education
2021-1-TR01-KA220-HED-000031993

R1/A2

CONDUCTING FOCUS GROUP ANALYSIS

Cyber IN Practice R1/A2 Combined Report

INDEX

ANALYSIS OF THE RESULTS FROM THE FOCUS GROUP'S INTERVIEWS HELD IN TURKEY - SESSION 1

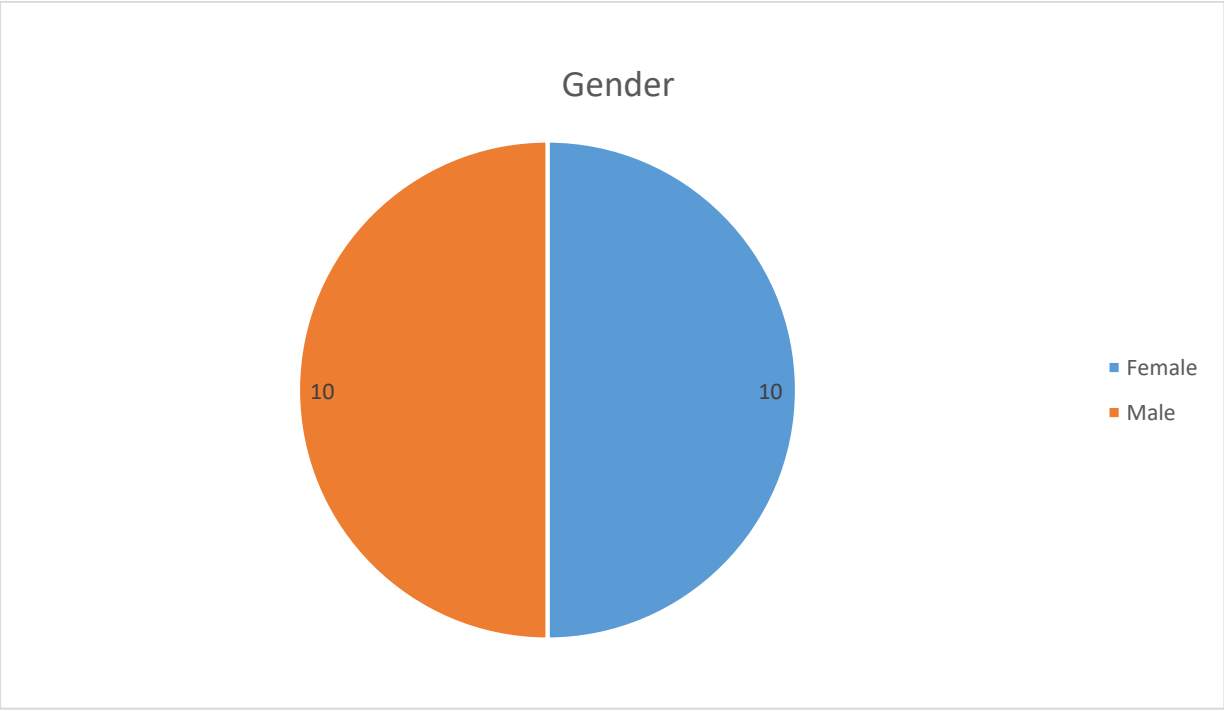
Introduction

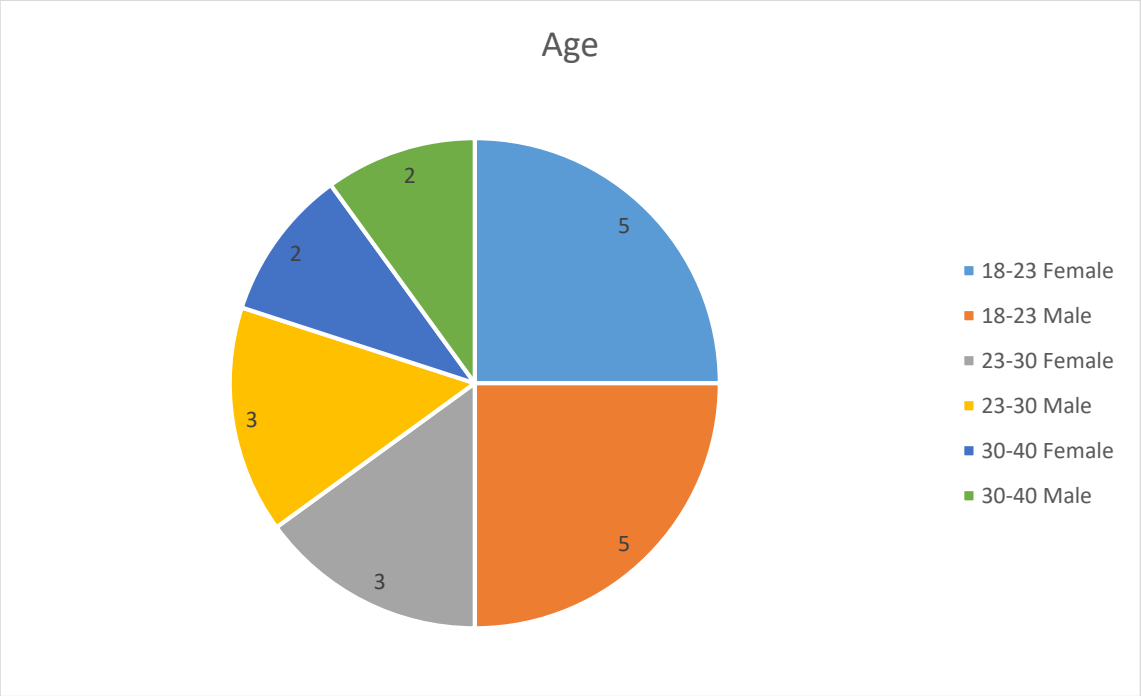
This report was created on a focus group study carried out within the scope of R1 of the project titled "Cybersecurity in practice for non IT oriented HE courses". The first part of the report includes demographic information, followed by the findings regarding the questions asked in the sessions. An overview of the findings is provided in the conclusion section.

The study was conducted in two separate sessions with a total of 20 participants consist of 10 female and 10 male. The sessions included participants from business administration, economics, departments, and sessions lasted approximately 70 minutes each. Focus group studies were conducted at Marmara University, Building of Busines School and reported in accordance with the Project Guideline for the Focus Group Analysis.

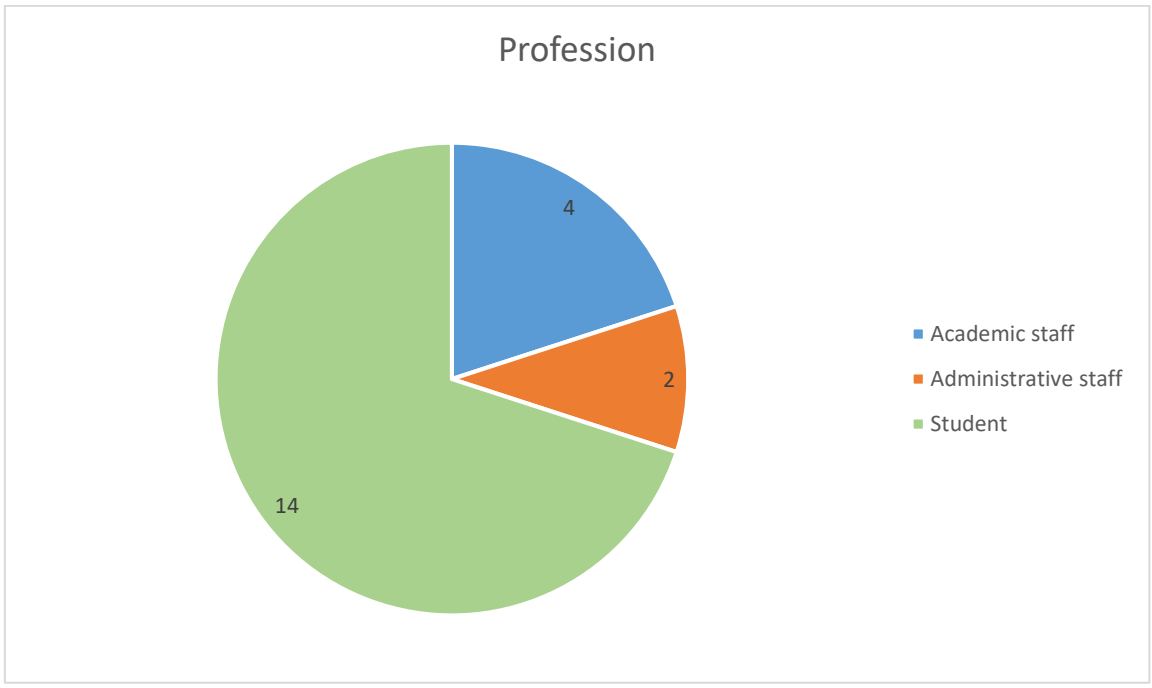
Demographic Information

Graphs showing some demographic information about the participants are shown as follows:

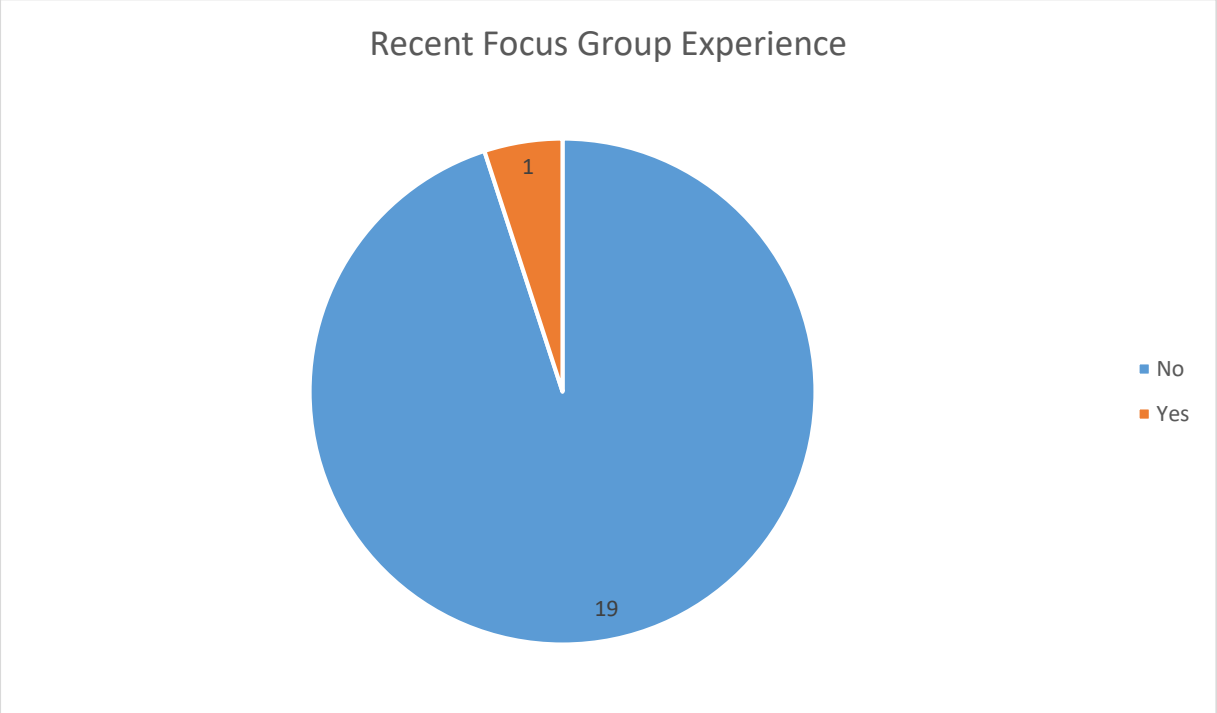




A total of 14 students, 4 academicians and 2 administrative staff took part in the study. There are seven participants studying or working in the field of business administration, two in the field of biology, four in the field of economics, three in the field of political science, and four in the field of psychology. This distribution is also seen in the chart below.



It was stated that only one of the participants had enrolled in a focus group study before, which is about the examination of consumer behaviors in the world of the future.



Study Findings

The relevant section includes the answers provided by the participants to the moderator's questions. “Yes or No” questions were included in the research form given to each participant and everyone was asked to answer these questions. The open-ended questions, on the other hand, were addressed by the participants in an ordered manner, as stated in the focus group working rules at the time, within a free speech environment.

How would you describe cyber security?

Some of the responses to the related question are listed as follows:

- *We can define it as a security system related to the Internet and all kinds of activities. (P1)*

- *All kinds of data security in the social environment*

- *I can say that I am not too much of a judge. (P7)*

- *Taking precautions against situations such as hacking (P11)*

- *Electronic data protection framework (P12)*

It was observed that the participants were able to make some definitions with their own words. However, it is evident that there is no near-perfect definition, and three individuals refrain from defining the term. It is also a remarkable observation that the participants were nervous in the face of the question.

Can you list at least 3 cyber threats?

It was observed that the participants did not have comprehensive knowledge about the types of cyber threats. It should also be noted that awareness and general knowledge level are inversely proportional to age.

- *No, unfortunately I do not know the types of attacks.*
- *I can say phishing specifically.*
- *Hacking in general*
- *I have no idea about their special names, but I definitely do have a general awareness on the topic*

What do you think should be considered when choosing a password?

It was observed that the participants did not act very carefully when setting the password. Although they are generally aware of the ideal situation, it seems possible to say that they act without complying with it too much.

- *I always prefer to use different combinations of the same password. But this is not any specific thing, it's just a combination I made up.*
- *Actually, there are several softwares on the internet that let you know how secure your password is and how long it can be hacked, but how secure these are, is debatable.*

- It should not be anything too obvious and should contain different combinations of numbers, letters and punctuation marks.

- Honestly, I can't say that I put too much thought into it, I think even the most complex passwords can be revealed thanks to artificial intelligence.

- I know it's not true, but I usually always use the same password, otherwise I'm afraid to forget it.

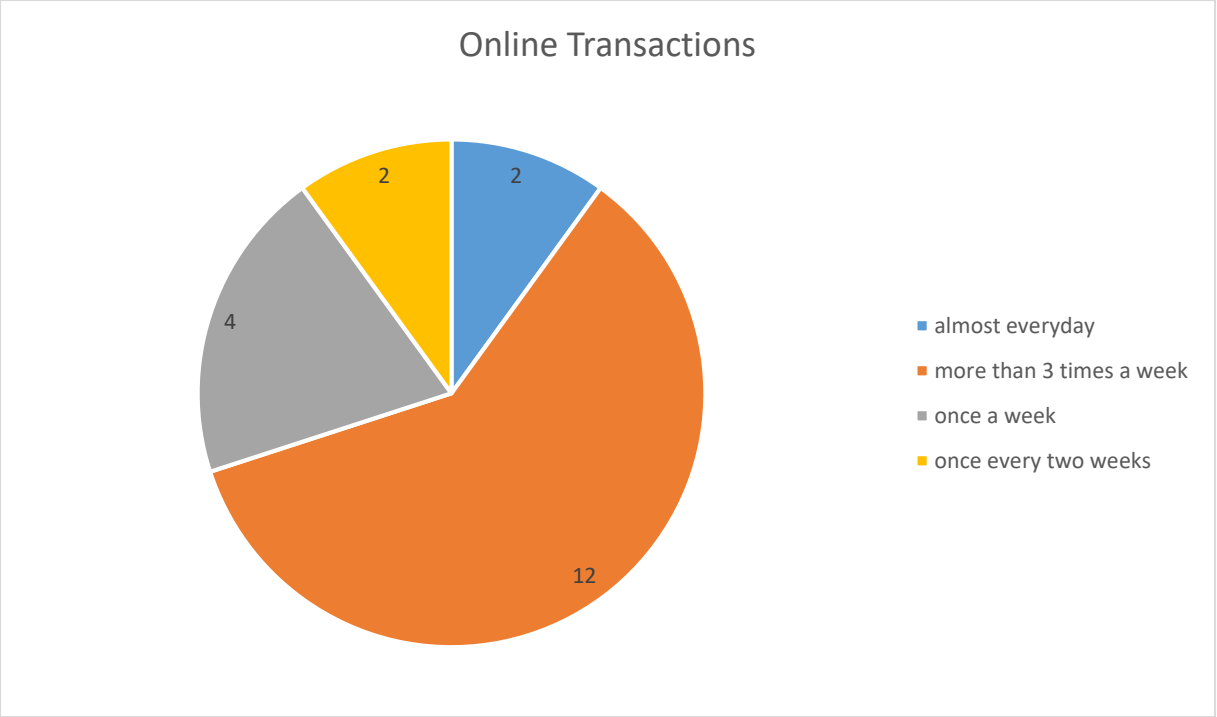
Do you follow the links from the e-mails for “lottery win” or “changes in bank account”?

The participants do not fall into the obvious phishing traps, but they can be targeted in places like social media, where people communicate with each other.

- *I don't trust them at all.*
- *The majority of them spam anyway, so I never see them.*
- *Not of this type, but I made these type of clicks on social media. Sometimes it can be very believable, I think.*
- *Similar things have happened to me, but unfortunately it can happen to everyone. Sometimes we hear in the news that even very famous people fall into such traps.*
- *Not me, but someone I know very well and with a very high level of education, was deceived in this way.*

How often do you make online transactions or orders?

While most of the participants stated that they actively use online transactions, only 2 people emphasized that they found face-to-face transactions more reliable. The graph of online transaction frequencies is given below.



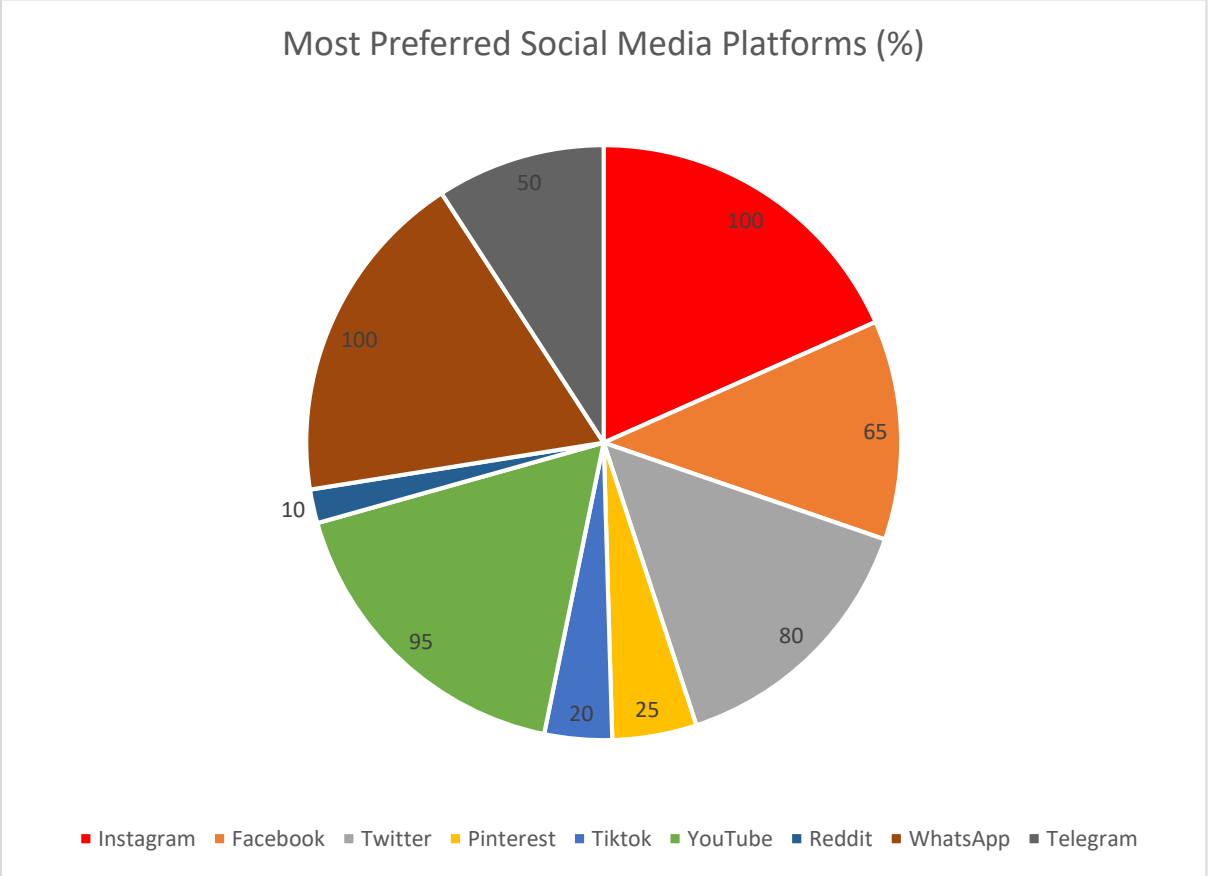
Do you feel safe when you make transactions or share private information?

Observations indicate that most participants make online transactions. Over 95% of the participants said that they used online shopping actively and that they did not have much anxiety or fear when shopping online.

- *It doesn't matter to me, I am completely comfortable*
- *We are living in a digital era, so I see that, online transaction is not a luxury need, but the truth of our world.*
- *In my opinion, online payment systems have improved greatly, so I feel comfortable using them.*
- *My preference is for sites that offer 3D security.*
- *The use of virtual cards is what I prefer.*
- *I don't even feel close to a credit card, so I generally prefer cash payments. I don't use online shopping much.*

On which platforms are you active in social media? How often do you use them? What kind of information do you share on social media?

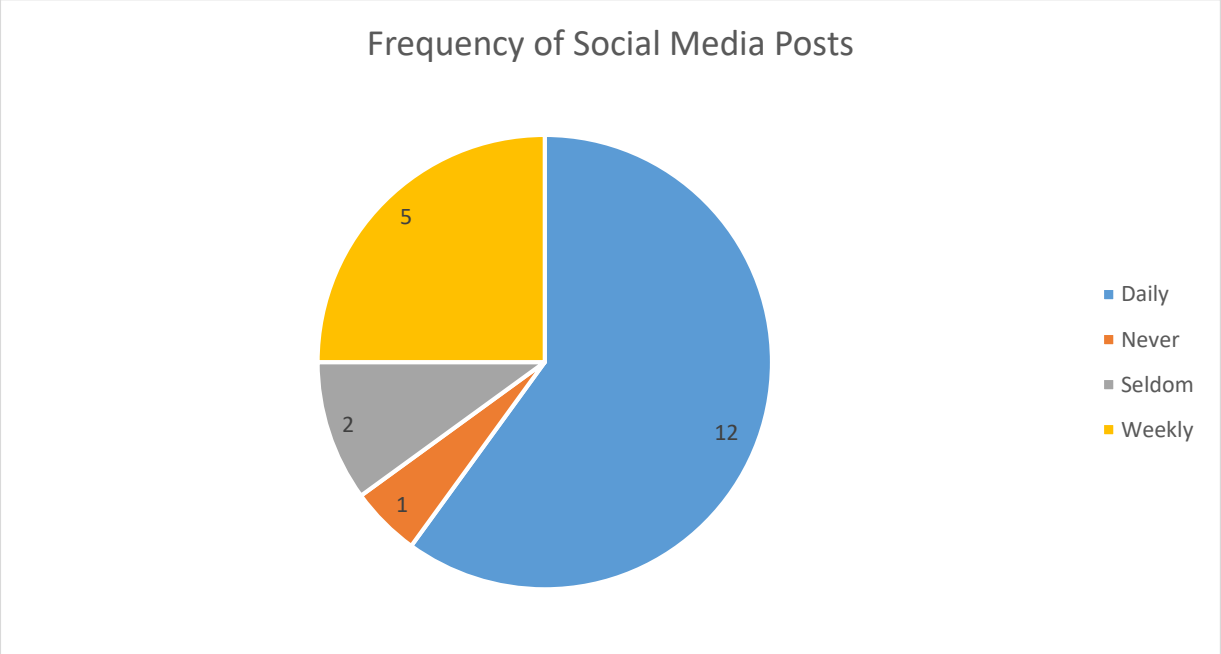
All of the participants, except one, stated that they use social media actively. It was seen that the most used platforms were Instagram and WhatsApp, followed by YouTube and Twitter.



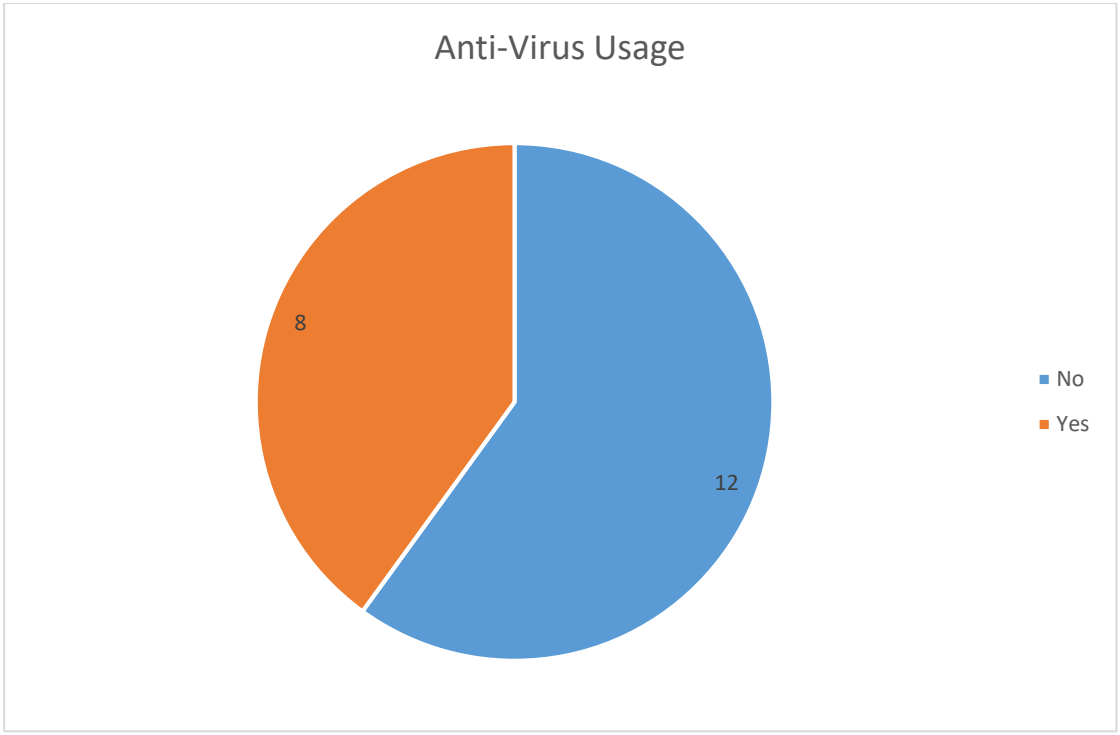
- *I usually share my memories, feelings, and information that I find interesting. Apart from that, I prefer to read posts rather than share them. (P1)*
- *The most recent photo I shared was two years ago, and I rarely share anything else. (P2)*
- *In the past, I attempted to be a phenomenon by sharing almost everything. Basically, it is a youthful enthusiasm. All the places I visit, the cafes I eat at, my house, my room... I have shared everything...*
- *Not photos, but I like to share my comments and opinions on twitter more. I mostly prefer critical posts.*

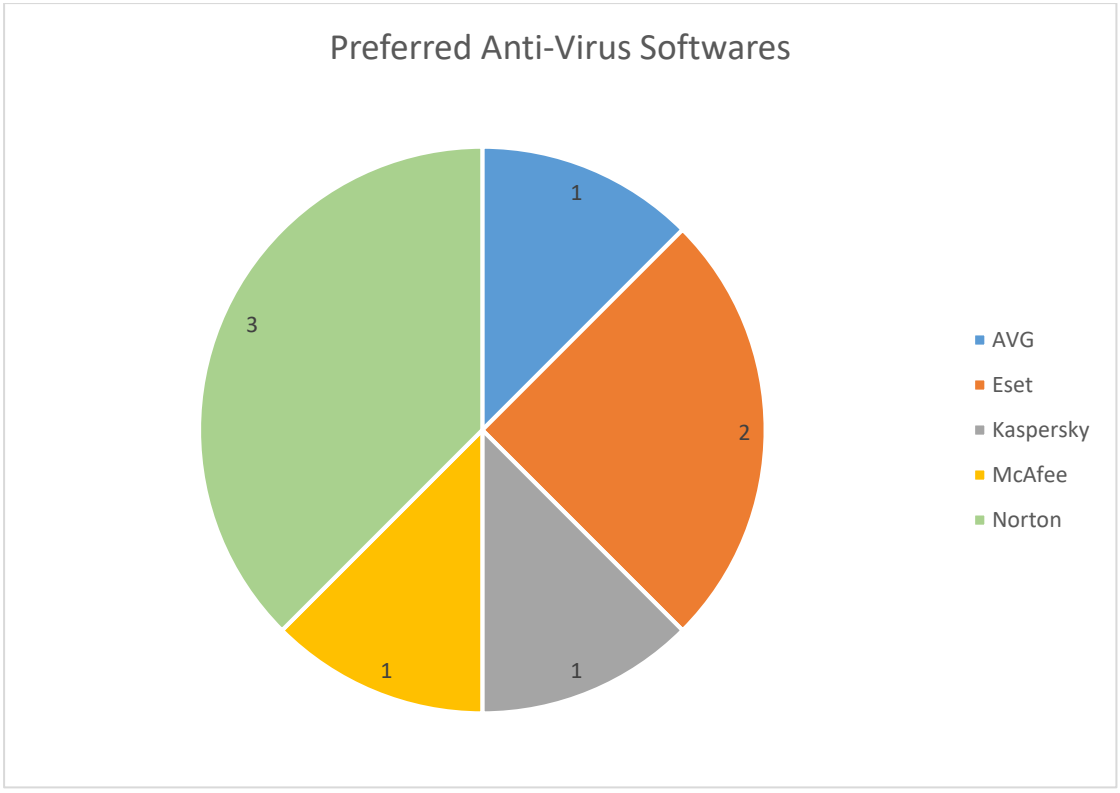
- *- I have two different accounts, professional and personal. My professional account is open to everyone, I usually prefer to make up-to-date posts about my profession there. My personal account is only open to my relatives, I'm a little conservative about it.*
- *- I can say that I share almost everything, because today's world is lived on social media platforms.*

It is also stated that most of the participants regularly share/post on social media. The explanatory chart is presented below.



Do you use antivirus application on your devices?
if yes, Would you define which? Do you have other security measures on your devices? How often do you update them?
if no, What kind of security measures do you have on your devices?


Anti-Virus Usage
8
12
No
Yes


Preferred Anti-Virus Softwares
1
2
1
1
3
AVG
Eset
Kaspersky
McAfee
Norton

- I use Apple products, I know that malicious software cannot easily enter these devices.

- I stopped using antivirus software long ago, many of them take up too much space on the computer and slow down the working speed.

- Frankly, I don't use antivirus software because I don't trust it.

- I've never used it until now and I don't plan to use it either.

- I think the best anti-virus system is the user himself. It doesn't matter which anti-virus program you use, as long as you are careless, somehow the virus can infiltrate your system.

- Yes I'm using.

- When I buy a new device, the first thing I do is to install software such as anti-virus and anti-spy.

How important do you consider staying informed about cyber security? How do you keep yourself up-dated on cyber security related issues from professional and individual point of view?

While the participants emphasized that it is important to reach up-to-date information on cyber security and refresh their own knowledge, they stated that they did not make enough effort for this.

Some of the statements on the subject are as follows:

- Of course, no one can say that it is unimportant, but I do nothing about it.

- I usually try to stay informed via the internet and social media.

- I usually follow the explanations of role models whose opinions I value.

- I have a lot of shortcomings in this regard, unfortunately, I do almost nothing.

- Actually, this session was also stimulating for me, I feel that I am missing a lot.

- I have a lot of shortcomings both professionally and personally. I think that institutions also leave their employees alone in this sense. Cyber security is a very popular concept, but studies can only create a general awareness in people.

What do you think is the role of the HEI top management in minimizing the cyber threats in the learning environment of HEI?

- *I don't think it's on the agenda of universities; the people themselves need to take action.*
- *It should be on the agenda of the state before university administrations. In this way, maybe YÖK (Higher Education Council) can determine general rules.*
- *University administrations are positive in this regard, but I do not think that they are adequately equipped. After all, it is academics who run universities, not professional managers. There is not much of a professional management mentality.*
- *Actually, cyber security is the hot trend right now and I see many training and seminar emails coming in. But I am not sure how much participation is achieved.*

Are you aware if your HEI developed a measurement tool about cyber security awareness both for academic staff and students?

- *As for students, I don't think so, they are hardly aware of their own programs. The vast majority of academics would have known.*
- *This also concerns the communication units of universities. Here, their ability to use social media comes to the fore.*
- *Especially private universities highlight their activities very well, but I do not think that this is the case in all state universities.*
- *I honestly believe that the issue of cyber security is neglected in universities.*

Do you feel your private data is secure when you use the learning environment at your HEI? What is the reason behind your answer?

Although the participants thought that their personal information is not safe when using the learning environment, it was observed that they did not position this situation very high under the "cyber security" topic. On the other hand, it was observed that they could not provide a

broad perspective on the subject. The dominant word regarding the learning environment was “distance education

- *Honestly, I couldn't reconcile personal information security with the learning environment. Of course, we shared some of our information during the distance education process, but other than that, I don't think this is the case in face-to-face education.*
- *We use many systems in this process, of course, but I don't think we can have a big problem.*
- *In my opinion, this issue does not come to the fore in learning processes, because even when downloading an application to the phone, we invite dozens of risks. This is a bigger problem, I think.*
- *It wasn't something I thought much about. All of our personal information is registered in university databases and this information should be well protected and there should be an assurance by the university.*
- *Absolutely not, both the data of schools and the websites of large companies can be hacked frequently, this is not a priority in my opinion at universities.*
- *I don't think that our information is well protected in universities, but the priority is mostly in financial institutions, like banks. After all, there are all kinds of personal information and investments of people there. I think that universities are not in the foreground as it is said. But this can create reverse psychology, making cyber attacks much easier.*

Is there any programme/short informative course which has been created to further educate the academic staff and students, in order to reduce their chance of falling victim to cyber attacks in the learning environment in the HEI? What actions does your university take to raise awareness of cyber security in courses or extracurriculars?

- *I think it's being done, but we usually don't know about it.*

- *I think it can be a striking education, by conducting a study on a certain group of subjects. Thus, the importance of the cyber security issue can be discussed with the animation method through the "case study".*
- *In addition, the subject should be covered in the lessons, especially in terms of ethics.*
- *As I mentioned before, I see training announcements about this in corporate mails, but how efficient it is should be measured well.*
- *First of all, it is necessary to raise awareness about this issue. In other words, before taking action, people need to have pre-awareness about cyber security.*

Conclusions

The related study was carried out in two different sessions in the second week of October, 2022. Focus groups consist of 10 people, 14 students, 4 academics and 2 administrative staffs from departments of business administration, economics, biology, political sciences and psychology. The sessions were moderated by an independent moderator, and the project researchers participated in the sessions as "audience".

In the focus group study sessions, it was observed that although the participants had a general awareness, they do not have a high level of knowledge about cyber security related issues. Even though cyber security is not fully on the agenda of higher education institutes, some fundamental changes and regulations need to be made in order to bring this area up to speed.

The study stimulated and raised awareness among the participants, according to their final thoughts. This situation can be viewed as a promising outcome for the project's future.

Appendix

Number	*Gender*	*Age*	*Profession*	*Focus Group Experience*	*Social Media Activity*	*Anti-Virus Usage*	*Online Transactions*	*Social Media Posts*
1	Female	18-23	Student	No	Yes	No	more than 3 times a week	Daily
2	Female	23-30	Student	No	No	No	once a week	Never
3	Male	23-30	Student	No	Yes	No	more than 3 times a week	Weekly
4	Female	23-30	Academic staff	No	Yes	No	once every two weeks	Seldom
5	Male	23-30	Student	No	Yes	No	almost everyday	Daily
6	Male	18-23	Student	No	Yes	No	more than 3 times a week	Weekly
7	Male	18-23	Student	No	Yes	No	once a week	Daily
8	Female	30-40	Academic staff	Yes	Yes	No	once a week	Daily
9	Male	30-40	Administrative staff	No	Yes	No	once every two weeks	Seldom
10	Female	18-23	Student	No	Yes	No	more than 3 times a week	Daily
11	Female	23-30	Student	No	Yes	No	more than 3 times a week	Weekly
12	Male	23-30	Academic staff	No	Yes	No	more than 3 times a week	Daily
13	Male	18-23	Student	No	Yes	Yes	more than 3 times a week	Daily
14	Male	18-23	Student	No	Yes	Yes	more than 3 times a week	Daily
15	Female	30-40	Administrative staff	No	Yes	Yes	more than 3 times a week	Daily
16	Female	18-23	Student	No	Yes	Yes	more than 3 times a week	Daily
17	Male	30-40	Academic staff	No	Yes	Yes	once a week	Weekly
18	Female	18-23	Student	No	Yes	Yes	more than 3 times a week	Weekly
19	Female	18-23	Student	No	Yes	Yes	almost everyday	Daily
20	Male	18-23	Student	No	Yes	Yes	more than 3 times a week	Daily

ANALYSIS OF THE RESULTS FROM THE FOCUS GROUP'S INTERVIEWS HELD IN TURKEY - SESSION 2

Introduction

The main objective of the study is to get an overview of the level of understanding of cyber threats and the availability of security skills among all categories of participants in the higher education system who are not IT specialists.

The focus group work was conducted in accordance with the Guideline for Focus Group Analysis developed by the MU and MSKU teams. A total of 20 participants were included in the Turkish focus group conducted by MSKU. They were the representatives of secondary school graduates (5%), students (45%), academic staff (35%) and administrative staff (15%) (see Figure 1). All participants are specialists in non-IT sectors or studying non-IT disciplines.

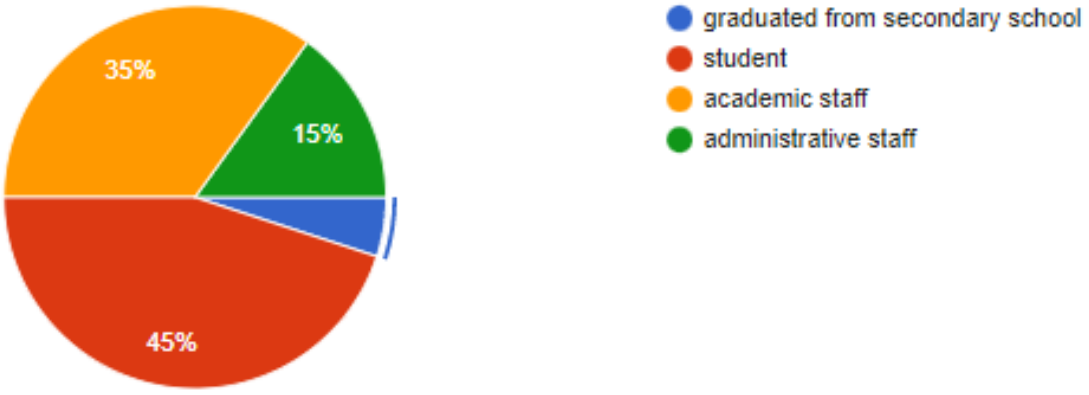


Figure 1: Participants Origin

The age characteristics of the participants can be grouped as follows (see Figure 2).

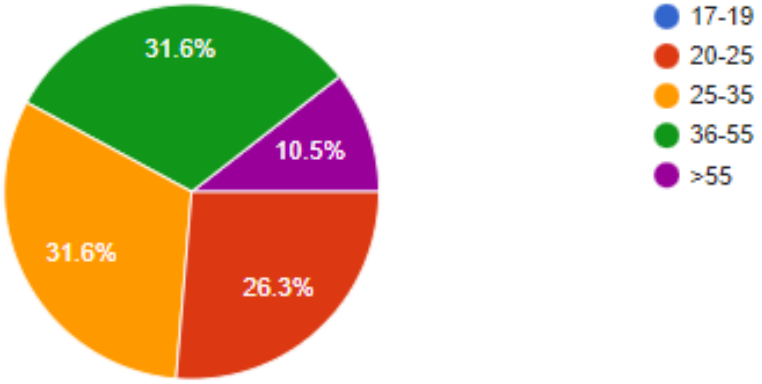


Figure 2: Age of Particapants

Study Findings

Q 03 About cyber-security

The answers to the below two questions indicate that participants have a clear idea of what cyber-security is and a good level of understanding of cyber-threads.

How would you describe cyber security?

The analysis of the answers reveals that most of the participants have a quite clear idea of what cyber-security is. Here are some of the most frequent answers in English:

- Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks.
- Cyber security is information technology security or electronic information security
- Blocking malware and virtual environment security
- To be able to take precautions against digital threats caused by security vulnerabilities.
- cyber security is to protect electronic systems from malicious attacks.
- Electronic information systems security.
- Data security in the social environment
- Preventing online attack
- It's a protect system about cyber attacks.
- Cyber security; It is the application of protecting computers, mobile devices, electronic systems from attacks.
- Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats.
- Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
-

Can you list at least 3 cyber threats?

Concerning the cyber-threats, almost all the participants are able to list some examples; among the most common answers we can mention:

Phishing, Data leakage, Hacking, Malware, sql injection, Password attack, Computer viruses, Identity Theft, Steal data, Spyware, Trojans

Q 04 About password

A collection of below 6 questions is useful to clarify how much participants are familiar with the password security requirements. In summary, participants have a good knowledge of how to create a secure password the most common answers are below:

What do you think should be considered when choosing a password?

Participants declare that they take into consideration several requirements when choosing a password; among the most frequently mentioned, there are:

- It should not be forgotten and contain numbers, letters and punctuation marks.
- It should be a complex password including every kind of character.
- It should not be easy to find and should contain letters, numbers and punctuation marks.
- Choosing a password that is not rest to guess. Use upper- and lower-case letters, choose meaningless numbers, etc

How often do you update your passwords spontaneously?

The answers to this question demonstrate that participants update their passwords in acceptable frequency. 28,6% of participants state that they update in 6 months, while 23,8% update in 3 months. Avery small minority changes their passwords every year or 9 months (See Figure 3).

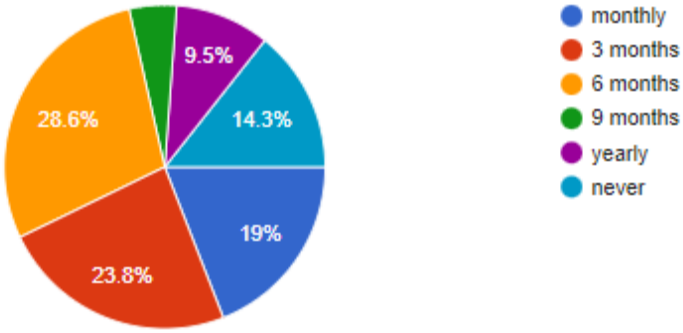


Figure 3:Password Update Frequency

Do you reuse a password you used before?

To the question "Do you reuse a password you used before?" (see Figure 4), the majority of respondents (47,6%) answer "sometimes", while 28,6 % declares to reuse a password often. And 23,8% never reuse it. This indicates a general low awareness that password reuse can facilitate cyber-attacks.

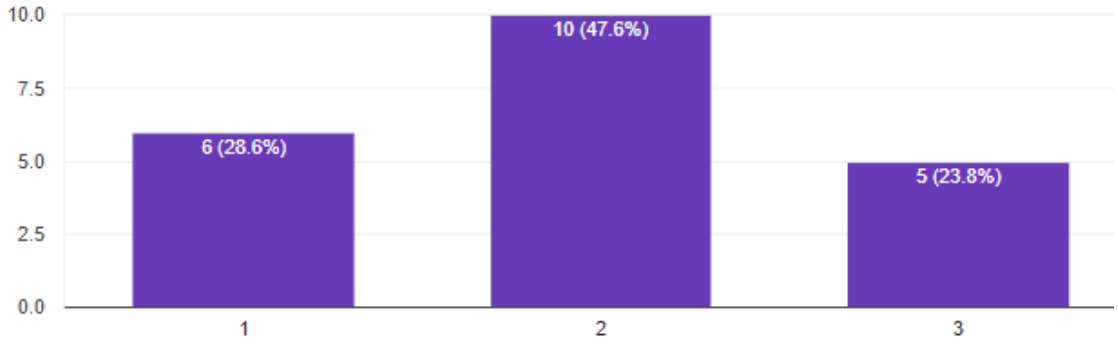


Figure 4:Password Reuse

Does anyone else know your password?

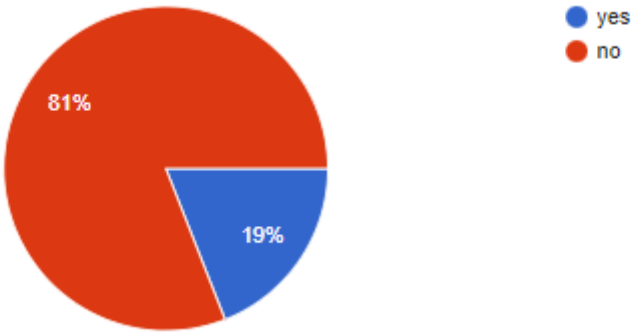


Figure 5:Password Sharing

The large part of interviewees, 81%, does not share information about their passwords with other people, demonstrating a good awareness of the need to protect their access passwords.

Do your passwords consist of meaningful words or specific dates?

Figure 6 shows the distribution of the answers to this question on a scale from 1 to 5, where 1 indicates "meaningful words or specific dates" and 5 "random letter, numbers, symbols".

The most part of the answers is between 2 and 3.

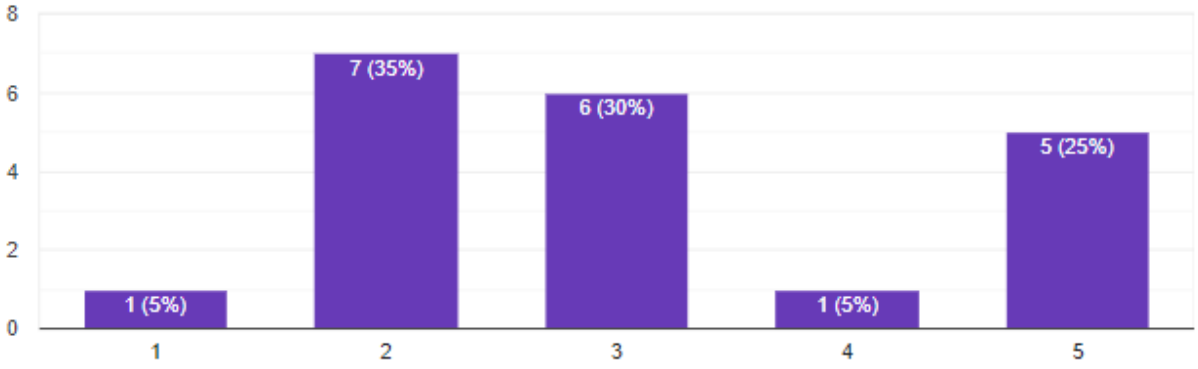


Figure 6: Password Composition

Is there a place where you write down your passwords?

The 93 % of the respondents saves their passwords somewhere. A small part of them write password on paper; the others store them in digital form on their PC or phones. Some respondents use dedicated apps (e.g., google password, bit warden).

Q 05 Reaction to e-mail requests, online transactions, personal info sharing

The following questions aim to understand the participants' behaviour when they receive requests or make transactions.

When you receive a letter that you won the lottery you…?

The large part of the respondents either delete (66,7 5) or not paying attention to the letter (23.8 %). This is showing a good degree of awareness towards potential phishing. However, 9,5 % of the people declares to follow the suggested steps (see figure 7).

Figure 7: Letter About Lottery Win

When you receive a letter that you need to change your bank account settings

The majority of participants (59,1%) affirms that they delete the letter immediately; however, a consistent part (31.8%) goes to the bank to ask. Also 9,1% declares that they follow the suggested steps (see figure 8).

Figure 8: Request to Change Bank Account Setting

How often do you make online transactions or orders?

The answers to this question indicate that participants are quite familiar with online transactions. More than half of them makes 2-5 transactions per month (52,2%), while 17,4% makes more than 10 transactions per month (see figure 9).

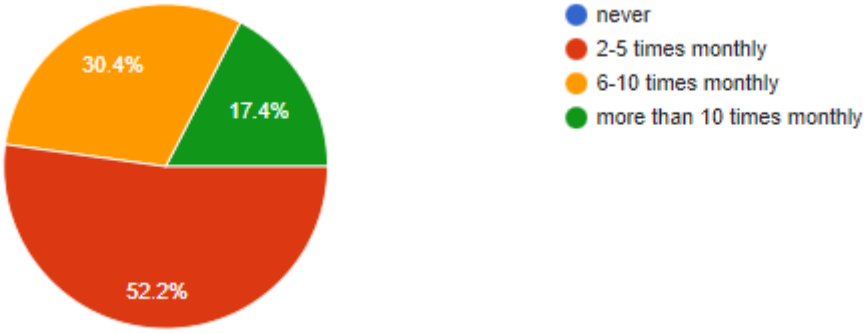


Figure 9: Frequency of Online Transactions

Do you feel safe when you make transactions?

The answers shown in Figure 10 indicate that participants do not feel to much safe when making transactions online. While 30% answers 1 or 2; 55 % answered 4. There is no one answered that they

feel completely safe during the online transactions. Therefore the participants recognise an average level of security associated with online transactions and orders.

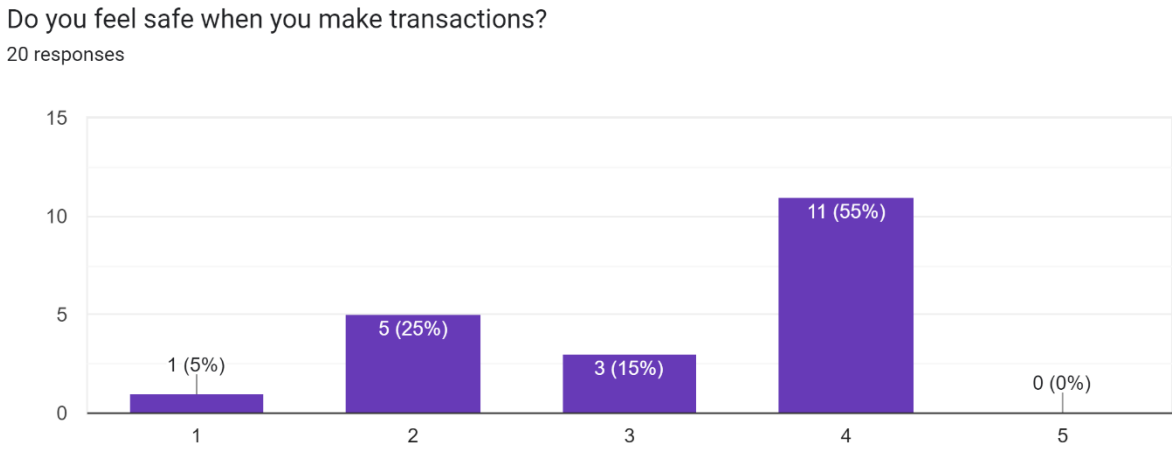


Figure 10: Security Feeling With Transactions

Do you feel safe when you share private information?

It is not same for security feeling in distributing private data. Figure 11 shows that participants do not feel really safe when sharing private information. The majority of the answers; almost 95% of the participants answered between 1 and 3.

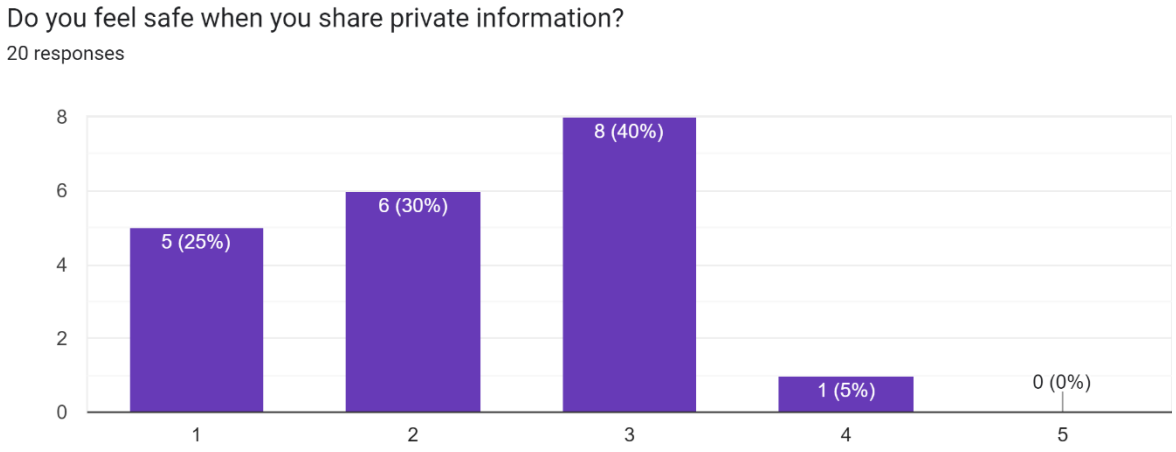


Figure 11: Security Feeling With Sharing Personal Information

Q 06 Social media

A number of different questions are useful to clarify how social media are used by participants; they help us to know which platform is mostly used, how frequently, which information is shared, which devices are used.

On which platforms are you active in social media?

Figure 12 shows the distribution of the answers about social media platforms. The most used platform is *instagram*, selected by more than 95% of the respondents, followed by *YouTube* (65 %) and *whats app* (65 %).

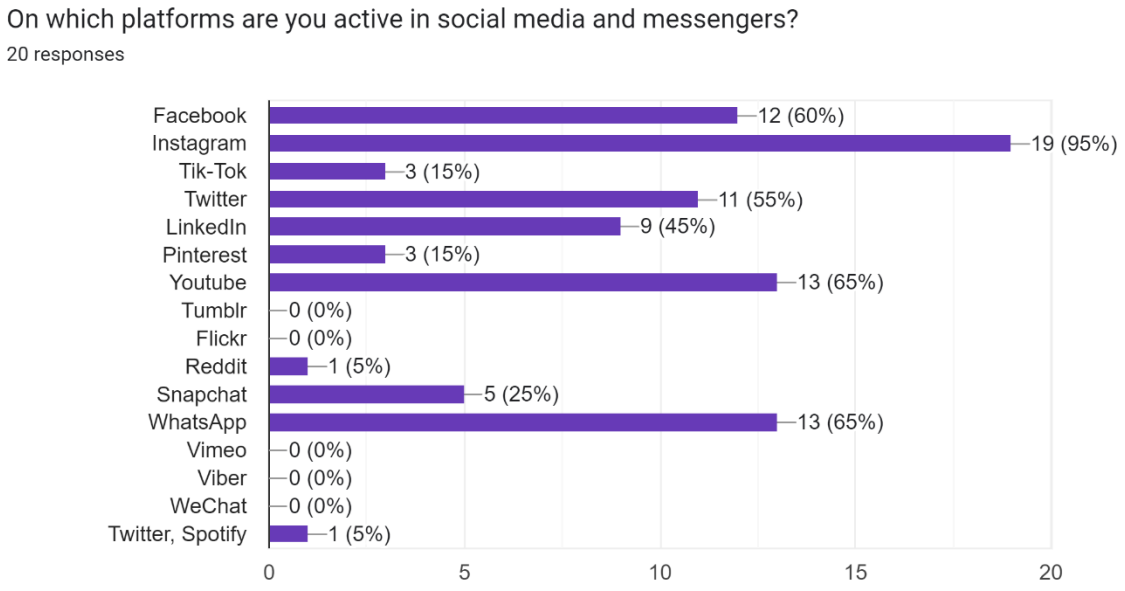


Figure 12: Social Media Platform

How often do you use them?

Figure 13 shows the frequency of use of social media by participants; the answers selected by most respondents are between 4 and 5, indicating that social media are used quite often; while there is no one using social media only 15% of people declare to use them rarely.

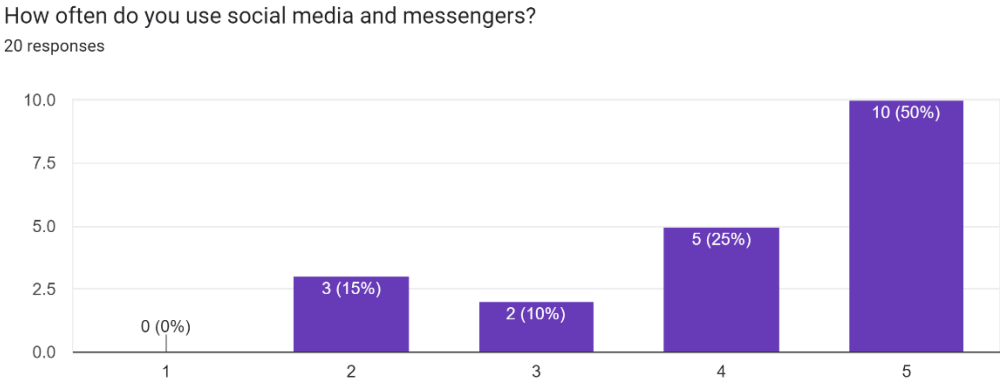


Figure 13: Social Media Use Frequency

What kind of information do you share on social media?

A very large part of participants states that they do not share personal information on social media or as little as possible; most of them just use social media to exchange information on daily news and actions. Few people share information such as images, photos, videos, news, school information.

Do you share your personal life on social media with photos or text?

Although in previous question the participants indicate that they do not share personel information on social media; as indicated by figure 14 a large part of participants (70 %) declares that they share their personal life on social media.

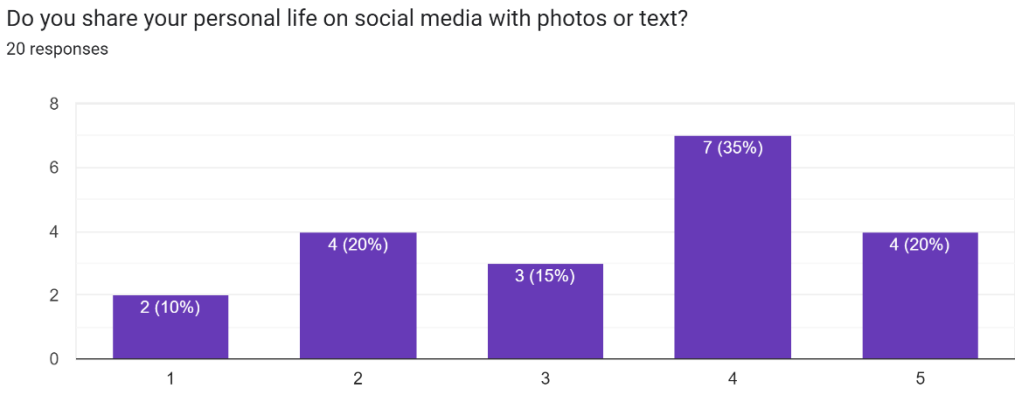


Figure 14: Personal Information Sharin

Do you pay attention to background details in the photos you share?

In line with the previous answers, 70% of the participants pays attention to the background details of their photos (see figure 15).

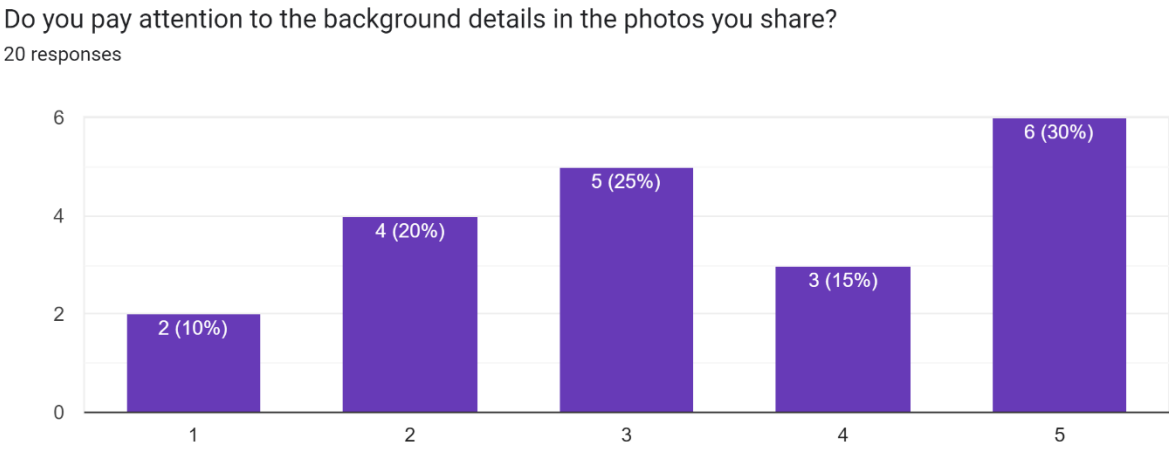


Figure 15: Attention to Background Details

You use social media from…

The most of the participants (85%) use their personal device. However, 10% of the participants use from personal and outside devices and 5 % use mainly from various outside devices (see Figure 16).

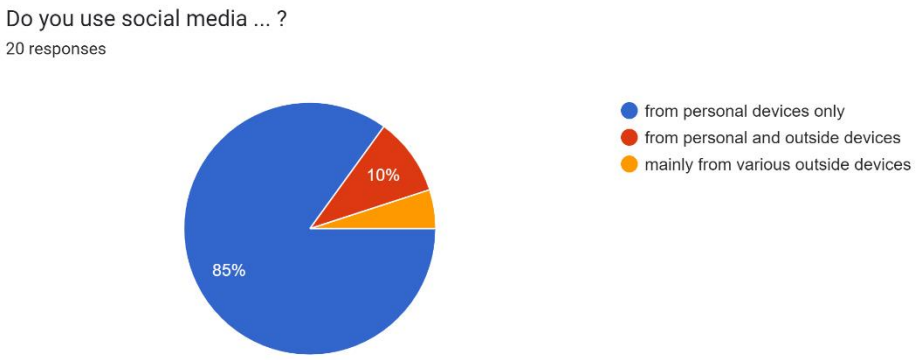


Figure 16:Used Devices

Q 07 Antivirus

A collection of 4 questions aims to get information about the use of anti-virus applications and other security measures.

Do you use antivirus application on your devices?

The use of anti-virus applications is quite common among the participants. 65 % of the respondents uses anti-virus applications on their devices; 35% of the respondents do not use anti-virus applications on their devices.

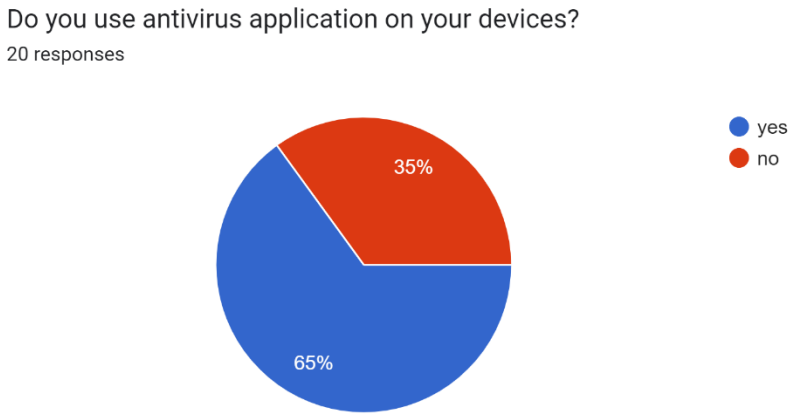


Figure 17: Anti-virus Usage

If yes, would you define which?

The most popular anti-virus applications are McAfee, Kaspersky, and Northon; other applications mentioned by participants include: Windows Security, malware, Sophos, Microsoft Defender.

Do you have other security measures on your devices?

Most of the participants declare to use antivirus and anti-malware applications for periodical scan.

How often do you update anti-virus applications?

The answers to this question show that the most of the interviewees are aware of the importance of updating the anti-virus software installed on their devices. 60% updates anti-virus applications when they receive notifications of updates, while a slight smaller percentage (25%) checks periodically for updates. The others (15%) affirm that they never update anti-virus applications

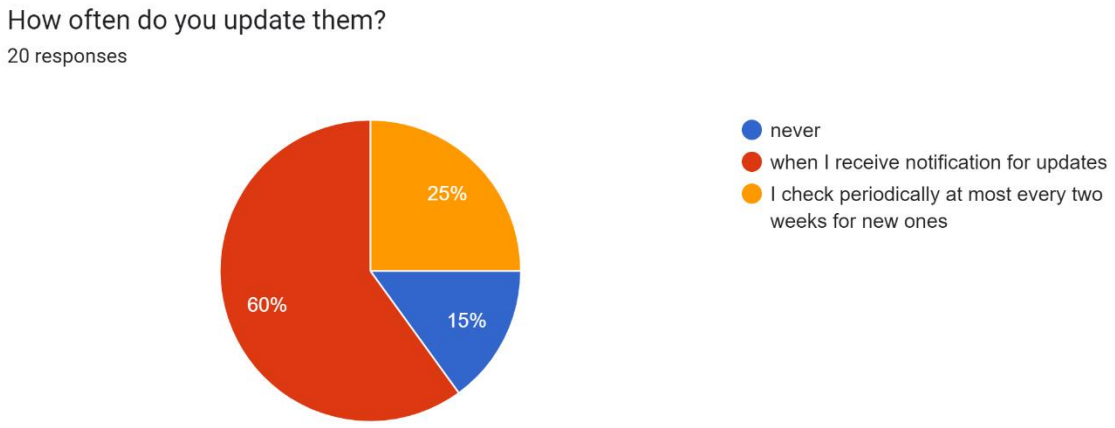


Figure 18: Update Frequency of Anti-Virus Applications

Q 08 Updates on Cyber-security

Concerning this topic, 2 questions are formulated: the first one is about which means are used to keep up-to-date with the cyber-security issue, the second is about the university measures to minimize cyber threats.

How do you keep yourself up-dated on cyber security related issues from professional and individual point of view?

The most part of respondents keeps up-to-date about cyber security related issues and mention a number of different means and tools they commonly use, including: technology channels on youtube, news, forums, web site and articles on the Internet. Few participants (30%) declare that they don't keep up-to-date.

Are conditions created in your university to minimize cyber threats in the learning environment? and if so, do you know which ones?

A majority of the interviewees affirms that they do not know or are not sure about the university's applications. However very minority of the respondents (15 %) answer "yes" and mention some measures taken by the university to reduce cyber-risks, such as, encryption of passwords, use of a wired network with local wireless connection and with static IP access, VPN, university wi-fi, specific training programme.

Q 09 University measures against cyber-threads

A collection of 3 questions is useful to know the participants degree of awareness about university measures against cyber-threads.

Do you know if your university conducts awareness campaigns about cyber security issues? What are they?

All participants answered this question "No".

Are you informed about the security of your confidential information by your institution?

Only 80% participants reply to this question as "NO". The collected answers are positive.

What are the security gaps or threats that you observe in the institution?

Most of the participants think they there are not security gaps or threads in the institution or declare that are not aware of any.

Q 10 Private data

Do you feel your private data is secure when you use the learning environment at your HEI? What is the reason behind your answer?

The general perception of the respondents is that they have no idea and that they do not share personal information.

Q 11 University cyber-security course

Is there any programme/short informative course which has been created to further educate the academic staff and students, in order to reduce their chance of falling victim to cyber-attacks in the learning environment in the HEI?

A large part of the respondents declares that there are not or they are not aware about courses organized by the university about cyber-security.

Q 12 Additional comments

Are there any other points that you would like to add regarding the topic?

Almost the totality of the respondents does not provide additional comments.

Conclusions

This study, run between 2nd and 26th of October 2022, has involved 20 participants among students, academic and administrative staff from Muğla Sıtkı Koçman University, Turkey. The analysis of data collected by means of an online survey demonstrates that participants have a clear idea of what cyber-security is and a good level of understanding of cyber-threads. They know the password security requirements and they are quite careful in not sharing their passwords with others. However, in some cases, we notice a sort of ignorance, for instance, in updating the passwords or not using a password already used before. The most part of respondents keeps updated about cyber-security related issues and mention a number of different tools and channels they commonly use, such as news, forums, specialized.

With respect to their reaction when they receive phishing letters, they usually recognise the deceit and delete the letter immediately.

They are quite familiar with online transactions - most of them make 2-5 transactions per month - and feel not much safe when making them.

They feel less safe when they share personal information. Indeed, a large part of them declare that they do not share personal information on social media. The most used platform is, *Instagram* followed by *WhatsApp* and *Youtube*. Almost the whole group of participants use social media from their personal device very frequently. The use of anti-virus applications is quite common among the participants, who also use other security measures on their devices such as password protection.

About the measures taken by the university and the campaigns against cyber-threads, participants affirm that the university doesn't create the conditions to minimize cyber threads and promote awareness campaigns on cyber-security OR they do not aware of this. No major security gaps or threads are reported. The general perception of the respondents is that their private data are protected. Only a few participants are aware of specific training programs about cyber-security. This is probably because the course is for collaborators.

ANALYSIS OF THE RESULTS FROM THE FOCUS GROUP'S INTERVIEWS HELD IN ITALY

Introduction

The main objective of the interviews conducted with the participants in the focus group was to get an overview of the level of understanding of cyber threats and of cyber security skills among all categories of participants in the higher education system who are not IT specialists.

The focus group work was conducted in accordance with the Guideline for Focus Group Analysis developed by the MU and MSKU teams.

A total of 24 participants were included in the Italian focus group. They were representatives from two different categories, namely: students – 21 participants; researchers and academic staff – 3 participants.

All participants are specialists in non IT sectors or studying non IT disciplines.

The age characteristics of the participants can be grouped as follows:

- 17-19 years – 2 participants
- 20-25 Years – 17 participants
- 25-35 Years – 3 participants
- 36-55 Years – 1 participants
- >55 Years – 1 participants

The focus groups were held in October 2022 and were developed in two phases, the first one face to face at Urbino University with the students from the Faculty of Economics and Law and the second one online with researchers and teachers from the Faculty of Economics and the Faculty of Law both from the Urbino University. During both focus groups, trainers shared a PPT presentation of the project among the students and academic staff, followed by an open discussion related to the main issues of cyber security.

The introductory part of the focus group was conducted to better explain the aim of the project and of the activity, after which the participant was invited to answer the main questions of the cyber in practice focus group guideline.

During this meeting, the objectives of this study were explained. The importance of the participants' opinions and suggestions was also briefly explained, the rules were specified (e.g. expressing one's own opinion, giving honest answers, not using auxiliary materials and devices, privacy policy, etc.). The nature and the scope of the questions to which the participant would have to answer, were disclosed to the participant in general terms. Next, the participant was invited to answer the questions in rotation.

Since almost all questions are open-ended and involved freely formulated answers, the data obtained were not processed with sophisticated statistical methods. In the sections following below, a summary analysis of the obtained data is presented.

Study Findings

Q 01

Could you please introduce yourselves briefly?

According to the results collected, a total of 24 people participated in the focus group. The majority of the participants were students of the Faculty of Economics and Faculty of Law from Urbino University between 17-25 years (including researchers and research assistants) and 3 people over 25 years took part in the survey as academic staff (research fellow and university lecturer).

Q 02

Have you taken part in a study on a similar topic before? What are your expectations about the session we will hold?

Expectations were to share points of view and situations on cybersecurity issues.

Q 03

How would you describe cyber security? Can you list at least 3 cyber threats?

The analysis of the received answers creates the understanding that, in general, the interviewees have a general idea about the nature of cyber security. Most of the given definitions are basically correct, but they do not cover the entire essence of the cyber security phenomenon. Some of the answers are rather confused and not correct. The majority of the respondents correctly described the concept of cyber security in terms of data protection and privacy defining “cyber security” as a range of tools, approaches, methodologies and software required to protect data and information on the network. However no one provided a comprehensive and detailed definition of cyber security.

Only one of the participants admitted that he was not really interested in cyber security issues until the focus group.

It can be summarized that, in general, working and studying in non-IT fields have the most general, and at the same time fragmentary, idea about the essence of cyber security however they did not know the topic in a detailed and sufficient way.

Interesting are the answers given to the following question “Can you list at least 3 cyber threats”.

A long list of possible cyber threats has been identified by the respondents and the most common ones are the following: Personal data breach, Virus Attack, Hacker attack, Phishing, spam, Unidentified URL addresses, identity theft, data theft, Hacking, trolls, Malware, Data appropriation & person substitution, email and message scams, Malware, Trojans, password breach. All the respondents identify at least the 3 possible cyber threats they considered as more dangerous.

Q 04

What do you think should be considered when choosing a password?

In addition to the basic question, five specific questions were asked for receiving more detailed information.

All the answers collected among the participants showed a sufficient knowledge and awareness concerning the importance of choosing a secure password. All participants are very familiar with password security requirements. Combination of letters and numbers, use of special characters, use of lowercase and uppercase letters are among the most frequently mentioned requirements. It is also mentioned that the rules not to use personal data, such as year of birth, personal/surnames, not to be easily guessed by other people. The participants outlined the importance of changing the password often and of not using the same password for all the accesses and accounts. Do not use trivial passwords is a priority according to the participants.

Only one respondent stated that he/she did not care about the importance of a secure password since -according to him/her- the only requisite to be taken into consideration when choosing a password is the easiness to remember it.

To the question "How often do you update your passwords?", a large part of the interviewees do not particularly care about the frequent renewal of their passwords; the majority of the respondents, 13 out of 24 stated that they never update their passwords, while the rest of the respondents state that they change passwords regularly (Yearly, Monthly); 4 interviewees update their passwords yearly, 5 every 6 months and 2 monthly.

The answers to the question "Do you reuse a password you used before?", can be arranged in 3 groups. Only 3 (12,5%) of the participants never reuse old passwords, 8 respondents interviewed reuse a password used before (33,3 %) and the majority of those interviewed state they never reuse passwords previously used to access sites or to register to platforms

The interviewees are almost unanimous on the question **"Does anyone else know your password?".** 75% of them do not share information about their passwords and only six interviewees (25%) admit to share his/her passwords with someone else. This shows that a significant part of those surveyed do not have a clear understanding of the need for personal efforts to ensure protection against potential cyber attacks: not to share personal data is the first condition to avoid cyber attacks.

It can be summarised that, in general, professionals and students from the non IT sector are quite aware of the need to protect themselves from cyberattacks, including protecting their access passwords.

The following question "Do your passwords consist of meaningful words or specific dates?" ask the participants how often do they use meaningful words/specific dates or random numbers or letters in their passwords.

The results show that the majority of the respondents often use meaningful words or specific dates in their passwords: 12 participants state that they very often or always use important words and dates in their passwords, 10 say that they rarely use it and 2 state that they never use personal words or dates in their password. The situation is almost the same, if we consider the answers concerning the use of random letters, numbers and symbols as part of a password; the majority of the interviewees (16 of 24) state that they often or always use random numbers and letters as part of their passwords, 5 say that they rarely use it and 3 state that they never use random values in their password.

The following question was: "Is there a place where you write down your passwords?" If so, where?". Only 8 respondents do not record their passwords anywhere. The other 16 interviewees do, but through several tools: in the Smartphone, in the notes of the mobile phone, in the i-phone memory, in the cloud, in a excel database and on paper.

Q 05

Do you follow the links from the e-mails for “lottery win” or “changes in bank account”? How often do you make online transactions or orders? Do you feel safe when you make transactions or share private information?

The interviewees are quite unanimous on the question "**Do you follow the links from the e-mails for "lottery win"**. Most of them delete such emails immediately (16 out of 24). The other 8 respondents state that do not pay attention to these kind of e-mails. There are slight deviations in the answers to the question "**When you receive a letter that you need to change your bank account settings**" – 70,8% (17) of the interviewees immediately delete such messages, 20,8%; 5 of them go to their bank to make a reference and unfortunately 8,3% (2) follow the proposed steps. This outlines how important it is to increase awareness and knowledge about possible cyber threats among the beneficiaries.

To the question "**How often do you make online transactions or orders**?", 16 persons answered from 2 to 5 times/monthly, 6 make transactions 6 to 10 times a month, two people indicate that they make more than 10 transactions per month, and 1 do not make any transactions. It can be summarised that the majority of the interviewees pay attention and refrain from conducting electronic transactions. It would be interesting to know the reasons for such abstinence, but the study did not plan to ask such questions.

In the following two questions: "**Do you feel safe when making transactions**" and "**Do you feel safe sharing personal information online**?", interviewees are invited to reflect on a 5-point scale the level of security they feel when making transactions or sharing personal information online.

A total of 14 people of those interviewed, feel “safe” or “completely secure” while at the same time, 9 people feel “almost safe”; only one respondent feels “unsafe” when he/she has to carry out electronic transactions.

The security-insecurity level changes when it comes to sharing personal information in cyberspace. The share of those who are „certain“ decreases dramatically from a total of 14 in the previous question to only 4 interviewees stating that they feel safe sharing personal information and data online. At the same time, the people feeling “quite uncertain” and “uncertain” sharing personal data online has risen to a total of 12 people and 8 people instead of 9 who still feel “almost safe” using personal information online.

It must be taken into consideration the fact that if types of transactions were distinguished, the data would be completely different. Due to strong security systems, banking transactions engender a relatively high level of trust and security, while in e-commerce transactions, the degree of uncertainty is much higher.

It can be summarised that the degree of uncertainty when sharing personal data is significantly higher than when making electronic transactions.

Q 06

On which platforms are you active in social media? How often do you use them? What kind of information do you share on social media?

„**On which platforms are you active in social media**?“. The following are the main answers collected: Facebook (12), Instagram (22), YouTube (16) , Tik tok (12), Tweeter (6), Pinterest (7), WhatsApp (24), LinkedIn (4), Snapchat (2), Reddit (1) etc.

To the following question "**How often do you use social networks and messengers?"**, the majority of the respondents state that they use social media "often" (9) and "always" (10), only 3 of them say that they use "not often" social media and only 1 states that he/she do not use social networks ever.

To the question "**What kind of information do you share on social media?**", the following are the most relevant answers collected: Photos, videos, instagram stories, Location, Travel and social life, University life, global news, Professional information about work and study.

In this question **"Do you pay attention to background details in the photos you share**?", the respondents are invited to reflect on a 5-point scale the level of attention they have when sharing photos online. The majority of the respondents state that they pay enough attention to the photos they share (a total of 18 people) while only 6 people state they do not pay attention or very little attention to the photos they share online. These results show that the level of awareness concerning possible risks in sharing personal data and images among the participants is not so high.

When asked **"if they access social networks only from personal devices",** the majority answer "yes" (23 people) while one person recognizes that he/she use not personal devices to access social networks**.** This means that almost all the respondents are aware of the possible risks you can meet when sharing information and account through no personal devices.

Q 07

Do you use antivirus application on your devices? if yes, would you define which? Do you have other security measures on your devices? How often do you update them? if no, What kind of security measures do you have on your devices?

With regard to the question "**Do you usually use antivirus application on your devices**", unfortunately the majority of the respondents answer "not" for a total of 14 people, while 10 of them answer "yes".

Among the most used antivirus applications mentioned by the respondents, we can find: Avast, Adobe, Malwarebytes, Automatic antivirus programme of Windows, Norton, Bitdefender, Ccleaner.

As to **"What kind of security measures do you have on your devices**", the following are the most relevant options provided by the respondents: Screen lock and password, Face ID password and fingerprint, Block of suspicious sites, Antivirus, Input code. Cleaning the phone remove viruses, not to save passwords or not to allow geolocalization, not to accept non-essential cookies, not to open sites or download content from sites flagged as dangerous, use of unlock codes.

To the question "**How often do you update your antivirus applications**?", the majority (12) state that they use to update the antivirus applications only when they receive the notification of a new version available, unfortunately 10 of them state that they never update the antivirus applications and only 2 people answer that they often check the antivirus time limit.

Q 08

How important do you consider staying informed about cyber security? How do you keep yourself up-dated on cyber security related issues from professional and individual point of view?

After question 10, it is of great importance for the continuation of the study to determine what kind of studies are carried out at universities and the level of awareness of university administrators and academicians in this regard.

The most relevant answers to the question **"How do you keep yourself up-dated on cyber security related issues from professional and individual point of view"** are the following**:** Reading materials and articles on the topic, Internet space and internet searches, From specialised web sites, through Colleagues and friends, through word of mouth and attending specific classes focus on this topic.

Q 09

What do you think is the role of the HEI top management in minimizing the cyber threats in the learning environment of HEI? Are you aware if your HEI developed a measurement tool about cyber security awareness both for academic staff and students?

The majority of the respondents do not know the available procedure by the University to minimize the cyber threats in the learning environment; only 2 people state that there are some procedures applied by the University such as the mandatory request for profile credentials to connect to the institute's public network and the need of authentication with university account to access the internal network.

To the first question **"Do you know if your university conducts awareness campaigns about cyber security issues? What are they?",** the respondents list the following examples: seminars, conferences, Cyber security courses, online classes and Discussions with specialists reading materials on the topic and meeting concerning this topic Some of these classes were organized within the University and the Centre for Integrated Instructional Services and E-Learning (CISDEL), a centralized structure serving faculty and students to promote project and research activities aimed at educational innovation. At the university, there are technical and information-system departments that provide technical support (ex Help my desk).

With regard to the question **"Are you informed about the security of your confidential information by your institution**?", many respondents answer "yes" and many others "no": this mean that a more efficient awareness campaign concerning the data protection within the University is required.

As to "**What are the security gaps or threats that you observe in the institution**?", most of the respondents do not know the possible or existing gaps or threats; meanwhile some of them state that the access to the public university's network can be a threat to cybersecurity as well as the need to connect to the public network in order to use a network connection within the university. The same problem for Access to passwords through devices within the university: students usually have the same account and password to access all the platforms and the university services (Library, e-learning etc). This can cause Personal data breach and theft sensitive information if the network is not secure. Finally, some of the respondents state that there are not effective security gaps.

Q 10

Do you feel your private data is secure when you use the learning environment at your HEI? What is the reason behind your answer?

Most of the respondents feel safe when using the learning environment at their HEI. For example to access the university network it is required to enter password and username otherwise you are not able to access the network. There is a whole department that works to solve technical problems and helps and support the users in case of technical issues.

At the same time some of them feel not so safe when working online at the university because there is not a complete protection; all the data can be registered and reused once connected to the public network by external interventions, if it is not safe and secure.

Q 11

Is there any programme/short informative course which has been created to further educate the academic staff and students, in order to reduce their chance of falling victim to cyber attacks in the learning environment in the HEI? What actions does your university take to raise awareness of cyber security in courses or extracurriculars?

All the respondents agree with the fact that at this stage there is no course within their university focused on cyber security.

Q 12

Are there any other points that you would like to add regarding the topic?

Only one respondent recommends to talk more about this topic within the university as well as more widespread control over the use of the university network.

Conclusions

The answers collected during the focus group session will be analyzed by the team and the staff to as the basis of the future training content of the Cyber in Practice Nuggets.

The results show a low level of awareness among students and academic staff of non-IT HEIs; even though the interviewees are able to understand the basic concepts of cyber security, the most common risks of cyber attack and the easier procedure to react in case of cyber attacks, the level of knowledge and awareness is not sufficient yet. Most of the knowledge concerning cyber security is related to the common risks such as malware, Ransomware, Phishing, spam, Data appropriation & person substitution, email and message scams, however the majority of the respondents do not know how to avoid these threats successfully neither which are the most adequate behaviours to adopt in order to not encounter cybersecurity problems.

ANALYSIS OF THE RESULTS FROM THE FOCUS GROUP'S INTERVIEWS HELD IN BULGARIA

Introduction

The main objective of the interviews conducted with the participants in the focus group was to get an overview of the level of understanding of cyber threats and the availability of security skills among all categories of participants in the higher education system who are not IT specialists.

The focus group work was conducted in accordance with the Guideline for Focus Group Analysis developed by the MU and MSKU teams.

A total of 26 participants were included in the Bulgarian focus group. They were representatives from three different categories, namely: students – 12 participants; academic staff – 10 participants; university administration – 4 participants.

All participants are specialists in nonIT sectors or studying nonIT disciplines.

The age characteristics of the participants can be grouped as follows:

- 20-25 Years – 3 participants
- 25-35 Years – 7 participants
- 36-55 Years – 13 participants
- >55 Years – 3 participants

The interviews were held in the period 12-20 July 2022.

The 10 steps of carrying out the interviews, defined in the mentioned Guidelines, were observed. However, one specific should be mentioned - the interviews were held in a mixed way. This peculiarity in the approach was imposed by the summer period in which the interviews took place. On the one hand, this is a period in which the examination sessions for almost all specialties are held, and on the other, this is a time when the academic and administrative staff summer vacations begin.

It was very difficult, if not - impossible - to gather all the participants in one place on a certain day and time. Therefore, the introductory part of the interviews was conducted individually with each participant, after which the participant was invited to answer the questions set in a purpose-built electronic version of the survey published on the ULSIT e-portal.

During the individual meetings, the objectives of this study were explained. The importance of the participants' opinions and suggestions was also briefly explained, the rules were specified (e.g. expressing one's own opinion, giving honest answers, not using auxiliary materials and devices, privacy policy, etc.). The nature and the scope of the questions to which the participant would have to answer, were disclosed to the participant in general terms. Next, the participant was invited to answer the electronic questionnaire.

Although different from working in a group, this approach has a positive side – all participants' responses are properly documented. This allows a better analysis of the obtained results.

Since almost all questions are open-ended and involve freely formulated answers, the data obtained are difficult to process with sophisticated statistical methods. In the sections following below, a summary analysis of the obtained data is presented. The answers of each of the 26 participants have also been translated and published in this report.

Study Findings

Q 03

How would you describe cyber security? Can you list at least 3 cyber threats?

The analysis of the received answers creates the understanding that, in general, the interviewees have a general idea about the nature of cyber security. Most of the given definitions are basically correct, but they do not cover the entire essence of the cyber security phenomenon. Only one of the participants (No25) admitted that he had not thought about this question, and two of them (No18 and 20) did not offer a correct answer.

It can be summarized that, in general, working and studying in non-IT fields have the most general, and at the same time fragmentary, idea about the essence of cyber security.

Interesting are the answers given to the question "to list at least 3 cyber threats". The variations in the answers are diverse - from malware for all kinds of devices, through identity theft, to disinformation, propaganda, espionage. Only three of the answers (15, 20-partially and 25) have nothing to do with the question asked.

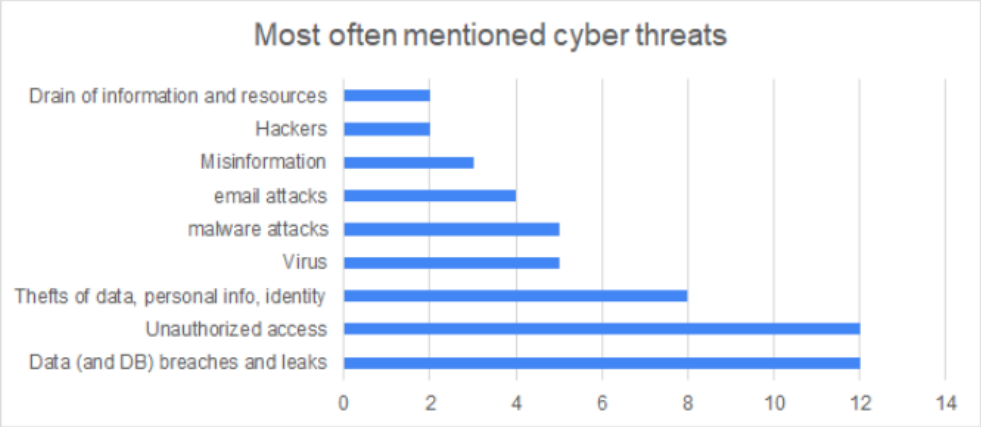


Figure 1

Table with a translation of all the answers given by the interviewees to the questions asked in this section

	How would you describe cyber security?	Can you list at least 3 cyber threats?
1.	Preventive methods used to protect information from theft, compromise or attack	Malware attacks, email attacks, data breaches and leaks
2.	Protection of information and data from theft	Malware SW, database leaks, misinformation
3.	Guaranteed access to information systems and prevention of threats to the security of information and communication channels	Email attacks, data encryption for ransom, data leakage
4.	Protection of the virtual environment	Hackers, information leakage, virus infection
5.	Protection of personal data	Data theft, theft of personal information

6. Security in the online space	Theft of personal data; unauthorized representation by a foreign person; viruses
7. The security in the Internet space and of technical devices	Ddos, social engineering and brute force
8. Ability of information systems to resist impacts negatively affecting the availability, truth and confidentiality of data.	Data breaches or leaks, email attacks, misinformation
9. Network and information security	They are most common in social networks.
10. At a high level, but not completely protected	Access to personal data; disclosure of a company secret; makes it difficult for him to work; identity theft
11. Protection of software, computer programs, websites from fraud	I do not know
12. Anti-malware software and firewalls	email attacks, leakage of personal data, misinformation
13. A state in which a balance is achieved between availability, integrity and confidentiality of data.	Social engineering, SQL injections, DDOS attacks...
14. Network and information security, measures to counter cyber threats and cybercrime, cyber defence	Malware, men-in-the-middle, phishing, Password attacks, DOS, DDoS, Social Engineering
15. Protection in the Internet space	porn - the sites that should be banned and completely removed as an existing factor of being; stolen identity; tracking via drones and satellites...
16. The ability of networks and information systems to withstand a certain level of impact negatively affecting the availability, truth, integrity or confidentiality of stored, processed data or related services.	malicious attack, malware, unauthorized use of computers, smartphones and other devices.
17. Marketing title of Information Security	Virus, Hacker, User
18. Good	propaganda, espionage, cryptohacking, mobile malware
19. Protection of AIS and networks and devices	unauthorized access to networks and devices, viruses and attacks
20. Cyber Security	stealing the phone, forgetting the password, hacking the card - in line at the store
21. The protection of data and processes in a digital environment.	Unauthorized access to data, unauthorized modification of data, data with incorrect content.
22. Protection from hackers	Identity theft, bandwidth theft, ransomware
23. Digital protection	Computer viruses, hacking, information war
24. This is the protection of personal information from the device	Access to photos, passwords, accounts
25. I have not thought about this concept	threats are more than three, no one is alone in the network and can not hide
26. Protection of sensitive information related to state management (part of national security)	Hackers, draining information, draining resources from the state

Q 04

What do you think should be considered when choosing a password?

In addition to the basic question, five specific questions were asked for receiving more detailed information. All these questions are reflected in the table below, marking the columns with the answers given.

All participants are very familiar with password security requirements. Complexity of selected symbols, combination of letters and numbers, lowercase and uppercase letters are among the most frequently mentioned requirements. It is also mentioned that the rules not to use personal data, such as year of birth, personal/surnames, not to be easily guessed by other people.

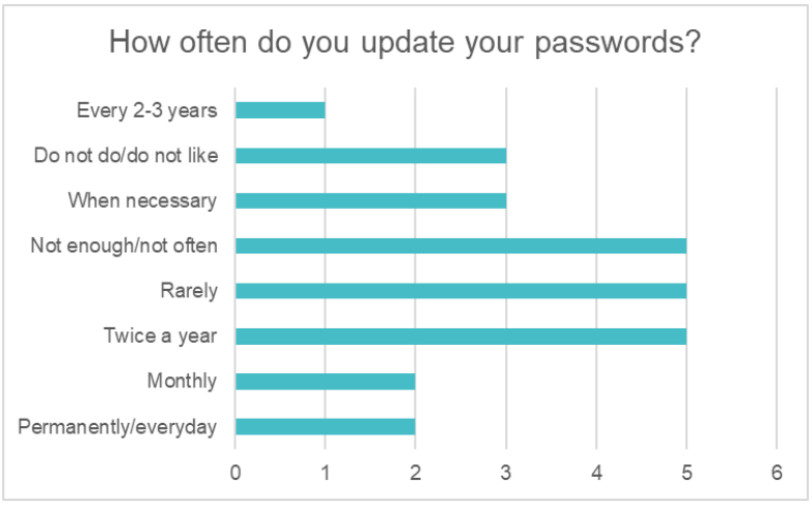


Figure 2

To the question "How often do you update your passwords?", four of the interviewees stated that they update their passwords regularly (Permanently, Monthly – Fig. 2). Relatively large part of the interviewees do not particularly care about the frequent renewal of their passwords (Not often – 5; Rarely -5). It is remarkable that some of them have an awareness of this necessity. Three people admit that they do not like to do this (Fig. 2).

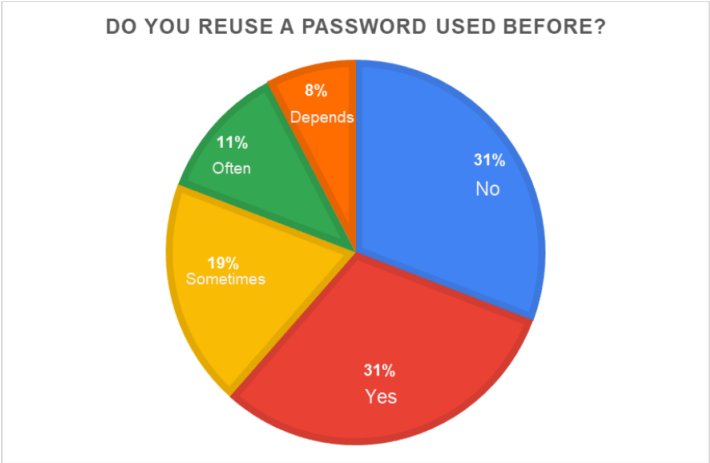


Figure 3

The answers to the question "Do you reuse a password you used before?" (Fig. 3), can be arranged in 5 groups. Only 1/3 (31%) of those interviewed never use old passwords. However, there are also answers that specify that they use passwords previously used only to access sites that do not require personal information or involve payments. It can be summarised that a large part of those surveyed (about 60%) do not have a clear understanding of the need for personal efforts to ensure protection against potential cyber attacks.

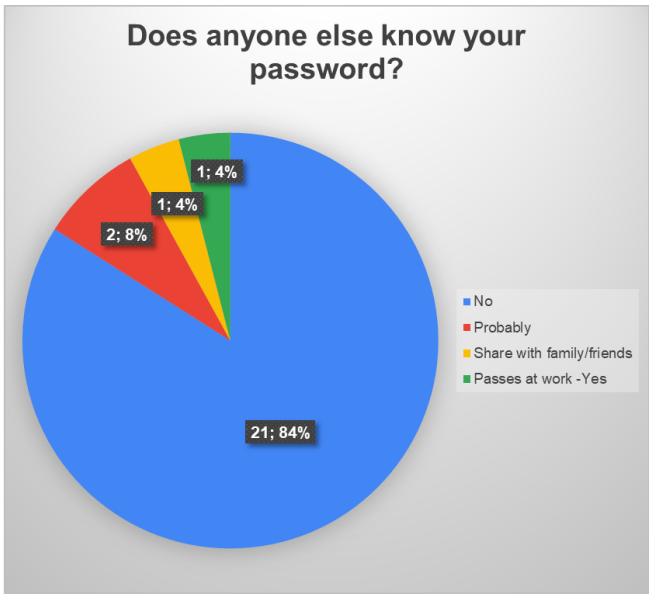


Figure 4

The interviewees are almost unanimous on the question "Does anyone else know your password?". 84% of them do not share information about their passwords and only one interviewee admits to sharing his/her passwords with close family and friends. There is also one answer that specifies that he/she shares only the work passwords with colleagues.

It can be summarised that, in general, professionals and students from the nonIT sector are aware of the need to protect themselves from cyberattacks, including protecting their access passwords.

The question "Do your passwords consist of meaningful words or specific dates?" overlaps to some extent with the main question. Therefore, the deviations in the given answers are not significant.

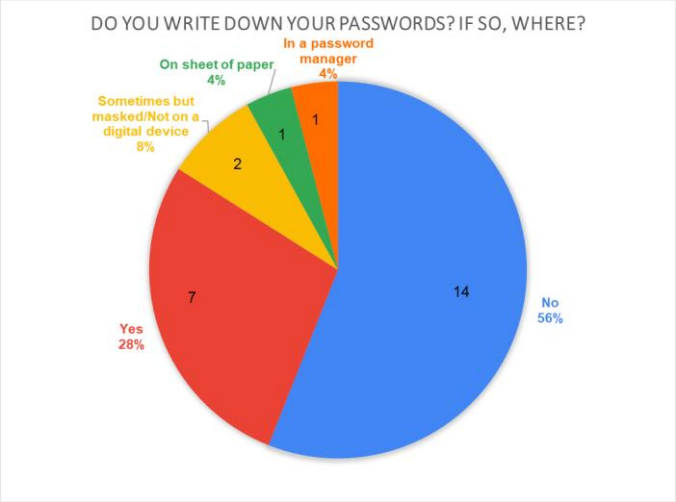


Figure 5

Figure 5 above shows the distribution of responses to the question "Is there a place where you write down your passwords?" If so, where?" More than half of the interviewees (56%) do not record their passwords anywhere. The other 44% do, but there are certain nuances that indicate that when saving their passwords, they follow certain requirements to protect their passwords from cyber theft.

Table with a translation of all the answers given by the interviewees to the questions asked in this section

What do you think should be considered when choosing a password?	How often do you update your passwords?	Do you reuse a password used before?	Does anyone else know your password?	Do your passwords consist of meaningful words or specific dates?	Is there a place where you write down your passwords? If so where?
1. Never use personal data.	Rarely	Sometimes Yes	Probably	Words and figures	Yes
2. Variety of symbols	Rarely	No	No	Both	No
3. Not to include personal data known to a wide range of people, to include letters, numbers, permitted characters, to be changed periodically	6-12 months	Always modified	No	Combination of words without meaning for the others	Sometimes in my phone and masked
4. It should be as complex as possible, containing in addition to numbers, symbols and letters	Not sufficient	No	No	Yes	No
5. The level of security it provides	Twice a year	Sometimes	No	Words and dates	On a sheet of paper
6. The use of different types of symbols	Every 6 months	Yes	No	Not exactly	No
7. Its complexity	Not enough :(	Unfortunately, yes	No	Words	More like a place where I store them
8. The degree of security, the symbols used	Rarely	Yes	No	Both solutions	No
9. As technology advances, I believe that behind every action there is a counteraction.	C do not do this!	Yes	Nobody	I will tell you exactly ;)	Yes, but not on a digital device
10. Use of letters, numbers and special characters	I do not update them	Yes, which is wrong	Work passes – Yes; The personal – are known only by me	Both	Yes
11. Be harder to recognize	Not very often	Yes	No	Word and figures	Yes
12. protection	Monthly	No	No	No	No
13. Number of characters and special characters.	Each month	Only for websites that do not contain my personal data or payment information.	Not and if the person does not need to use the account .	No	B password manager.
14. A set of non-repeating randomly selected signs and symbols that are in no way related to personal information/data about/the user and/or his relatives. Use of Upper and Lowercase	Depending on the account from once a year to once every 3 months	No	No	No	No

15. Password or access code should be understood as a way to protect personal data	When necessary, at least for the moment	Yes	No, only from institutions (banks, workplace)	Both...	No
16. It is necessary to choose such a combination of letters, numbers and symbols that are difficult to detect when accessing e-mail and other sensitive information.	Each month	No	No	Combination of letters and figures	No
17. How to easily change when you forget	Most of them every 3-4 years	Yes, but not more than 3 years	I share the passwords only with my family and several friends	Combination of both	Yes
18. include numbers and characters, upper and lower case letters - at least 8 characters for the password	Rarely	Yes	No	Meaningful words	No
19. Combination of letters, numbers and symbols		Yes	No	No	No
20. To be very complicated and to forget it	Everyday I update more than 30 passwords	Do not remember	May be sold on the hacker market - see Zamunda hacked passwords	Neither - I use a password generator	On the wall in the office
21. Be as secure as possible, containing alphanumeric characters, lowercase and uppercase letters, and other complex combinations..	Permanently	No	No	Yes	No
22. Whether it can be easily guessed	Rarely	Often	Nobody	No	Yes
23. Frequent change and use of different combinations of letters, numbers and symbols	Appr. each 6 months	Yes, with slight changes	No	No	No
24. Password complexity and length. The longer and more special characters it is, the more reliable it is	Not very often. In case of forgetting or threat	Yes, although I know it's wrong	Nobody	Yes	Yes
25. To be unusual for more of the people	I do not like to do this	Depends	I don't think there is one, but maybe someone can crack it	a combination of both with an ornament	No
26. Its complexity	Every 6 months	No	No	Combination	No, I remember them

Q 05

Do you follow the links from the e-mails for “lottery win” or “changes in bank account”? How often do you make online transactions or orders? Do you feel safe when you make transactions or share private information?

The interviewees are unanimous on the question "Do you follow the links from the e-mails for "lottery win". Everyone deletes such emails immediately. There are slight deviations in the answers to the question "When you receive a letter that you need to change your bank account settings" - 62% (16) of the interviewees immediately delete such messages, and 38% (10) of them, go to their bank to make a reference.

To the question "How often do you make online transactions or orders?", 58% (15 persons) answered from 2 to 5 times/monthly, 15% (4) make transactions 6 to 10 times a month, and 19% (5), two people (8%) indicate that they make more than 10 transactions per month, and 19% (5) do not make any transactions (Fig. 6 below). It can be summarised that almost 1/5 of the interviewees refrain from conducting electronic transactions. It would be interesting to know the reasons for such abstinence, but the study did not plan to ask such questions.

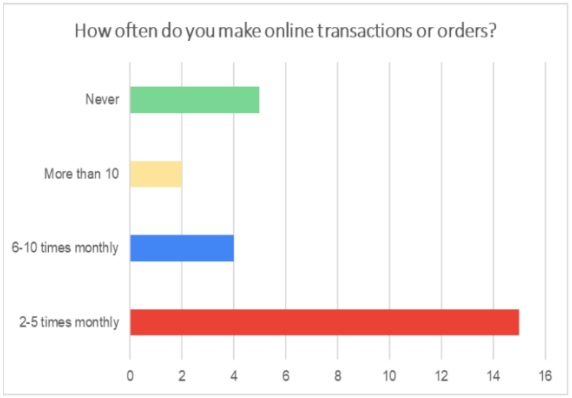


Figure 6

In the following two questions: "Do you feel safe when making transactions" and "Do you feel safe sharing personal information online?", interviewees are invited to reflect on a 5-point scale the level of security they feel when making transactions or sharing personal information online (Fig. 7 and Fig. 8 below).

A total of 46% of those interviewed, feel “safe” (23%) or “completely secure” (23%), while at the same time, a total of 35% feel “unsafe” (19%) or “very unsafe” (16%) when they have to carry out electronic transactions (Fig. 7 below).

The security-insecurity ratio changes when it comes to sharing personal information in cyberspace. The share of those who are „certain“ (0%) and „completely certain“ (12%) decreases dramatically – from a total of 46% in the previous question, here the percentages become only 12%. At the same time, the share of “uncertainty” and “absolute uncertainty” has risen to a total of 61% (15% + 46%).

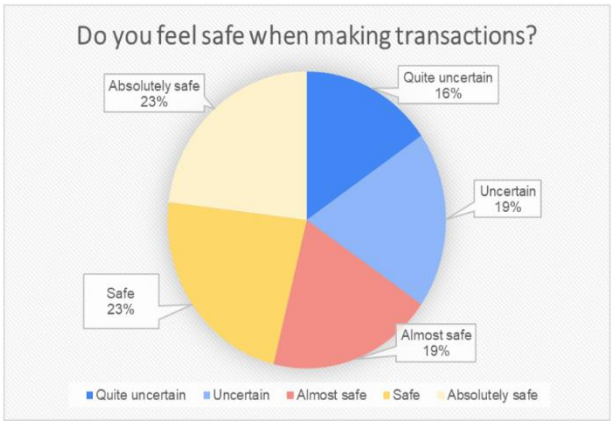


Figure 7

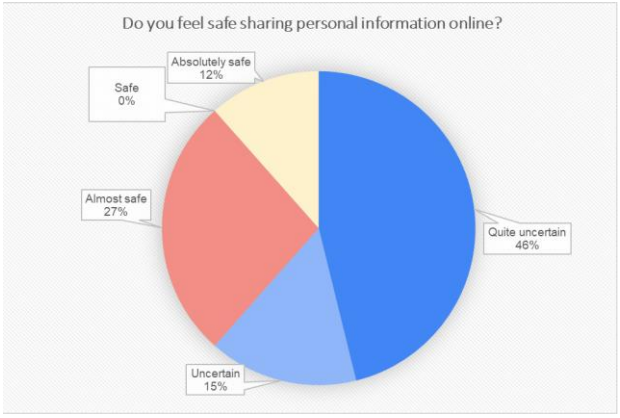


Figure 8

It should be noted that when planning the interview questions, the difference between electronic banking transactions and electronic commerce transactions was not taken into account. The hypothesis is that if these two types of transactions were distinguished, the data would be completely different. Due to strong security systems, banking transactions engender a relatively high level of trust and security, while in e-commerce transactions, the degree of uncertainty is much higher.

It can be summarised that the degree of uncertainty when sharing personal data is significantly higher than when making electronic transactions.

Table with a translation of all the answers given by the interviewees to the questions asked in this section

When you receive a letter that you won the lottery you…	When you receive a letter that you need to change your bank account settings?	How often do you make online transactions or orders?	Do you feel safe when making transactions?	Do you feel safe sharing personal information online?
1. Immediately delete the letter	Immediately delete the letter	2-5 times monthly	1	1
2. Immediately delete the letter	Immediately delete the letter	2-5 times monthly	4	1
3. Immediately delete the letter	Immediately delete the letter	2-5 times monthly	3	3
4. Immediately delete the letter	Immediately delete the letter	Never	2	1
5. Immediately delete the letter	you go to the bank to specify what is required	Never	3	3
6. Immediately delete the letter	you go to the bank to specify what is required	6-10 times monthly	4	3
7. Immediately delete the letter	Immediately delete the letter	6-10 times monthly	4	3
8. I do not pay attention to the letter	you go to the bank to specify what is required	2-5 times monthly	2	2
9. Immediately delete the letter	Immediately delete the letter	Never	3	3
10. Immediately delete the letter	you go to the bank to specify what is required	2-5 times monthly	4	3
11. I do not pay attention to the letter	Immediately delete the letter	6-10 times monthly	5	5

12. Immediately delete the letter	Immediately delete the letter	More than 10 times monthly	5	3
13. I do not pay attention to the letter	Immediately delete the letter	2-5 times monthly	5	5
14. Immediately delete the letter	you go to the bank to specify what is required	2-5 times monthly	3	1
15. I do not pay attention to the letter	you go to the bank to specify what is required	2-5 times monthly	5	5
16. Immediately delete the letter	you go to the bank to specify what is required	Never	2	1
17. I do not pay attention to the letter	you go to the bank to specify what is required	6-10 times monthly	1	1
18. I do not pay attention to the letter	you go to the bank to specify what is required	2-5 times monthly	4	2
19. Immediately delete the letter	Immediately delete the letter	2-5 times monthly	5	2
20. I do not pay attention to the letter	Immediately delete the letter	More than 10 times monthly	1	1
21. Immediately delete the letter	Immediately delete the letter	2-5 times monthly	4	1
22. Immediately delete the letter	Immediately delete the letter	2-5 times monthly	2	1
23. Immediately delete the letter	you go to the bank to specify what is required	2-5 times monthly	3	1
24. Immediately delete the letter	Immediately delete the letter	2-5 times monthly	2	2
25. Immediately delete the letter	Immediately delete the letter	Never	1	1
26. Immediately delete the letter	you go to the bank to specify what is required	2-5 times monthly	5	1

Q 06

On which platforms are you active in social media? How often do you use them? What kind of information do you share on social media?

Всички интервюирани са доста активни в социалните медии. Те дават по 3 и повече отговора на въпроса „On which platforms are you active in social media?“. Сред най-често споменатите са Facebook (22), YouTube (21), Viber (20), Instagram (13), LinkedIn (11), etc.

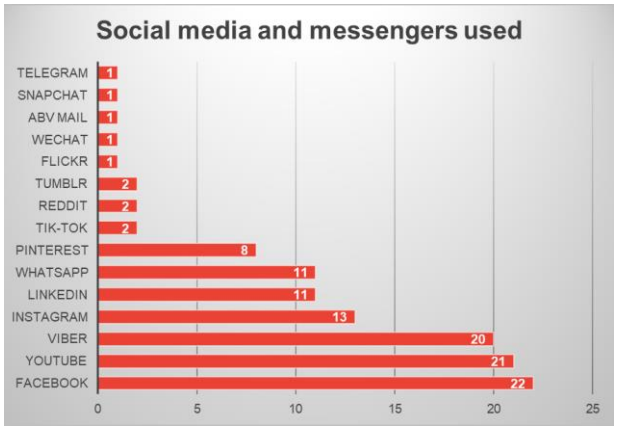


Figure 9

За отговора на въпроса „How often do you use social networks and messengers?“ е използвана 5 степенна скала. Нагласите на интервюираните са както следва: 42% ползват социалните медии много рядко, 31% - само понякога. Само 4% ползват социални медии ежедневно.

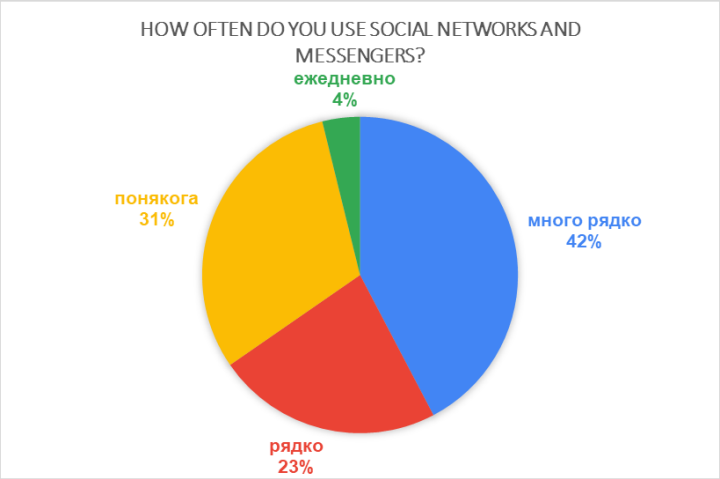


Figure 10

Отговорите на въпроса „What kind of information do you share on social media?“ са най-разнообразни, но като цяло, може да се обобщи, че мнозинството споделя неща от общ характер e.g. photos and chats, news and commentary, general info, cheerful and necessary, gossip and business info. Много от интервюираните съобщават, че избягват да споделят лична информация.

Table with a translation of all the answers given by the interviewees to the questions asked in this section

Which social media and messengers do you use?	How often do you use social networks and messengers?	What kind of information do you share on social media?	Do you share your personal life on social media with photos or text?	Do you pay attention to background details in the photos you share?	You use social media from... ?
1. Facebook, Twitter, LinkedIn, Pinterest, Youtube, Viber	1	I have logged out of most social networks	3	3	from personal and foreign devices
2. Youtube, WhatsApp, Viber	5	General	1	1	from personal devices
3. WhatsApp, Viber	3	I only share personal information with those closest to me or with colleagues - business information	1	5	from personal devices
4. Facebook, Instagram, Pinterest, Youtube, Viber	4	Almost none	1	5	from personal devices
5. Facebook, Instagram, Pinterest, Youtube	4	I do not share info	2	4	from personal devices
6. Facebook, Instagram, LinkedIn, Pinterest, Youtube, Tumblr, Reddit, Snapchat, Viber	4	Personal	3	2	from personal devices

7. Facebook, Instagram, LinkedIn, Pinterest, Youtube, Viber	4	Memes	1	5	from personal devices
8. Facebook, Instagram, Youtube, Viber	3	heterogeneous	3	4	from personal and foreign devices
9. Instagram, Youtube, WhatsApp, Viber	1	Natural landscapes and national holiday events	1	2	from personal devices only
10. Facebook, Youtube, Viber	4	Very scarce on some occasions	3	5	from personal devices only
11. Facebook, Instagram, LinkedIn, Youtube, WhatsApp, Viber	5	Any other than personal	2	5	from personal devices only
12. Facebook, Instagram, LinkedIn, Youtube, Viber	5	photos and chat	3	5	from personal devices only
13. Facebook, Instagram, Tik-Tok, LinkedIn, Pinterest, Youtube, WhatsApp, Viber	5	Mostly news and commentary.	3	4	from personal devices only
14. Facebook, Instagram, LinkedIn	3	non-personal information only.	2	5	from personal devices only
15. Pinterest, Youtube, ABV MAIL	3	Cheerful and necessary	1	1	от лични и чужди устройства
16. Facebook	1	without personal data	3	5	from personal devices only
17. Facebook, LinkedIn, Youtube, Reddit, WhatsApp, Viber	4	Important	3	3	from personal devices only
18. Facebook, Instagram, Youtube	4	a little private, rarely share much	2	4	from personal devices only
19. Facebook, Youtube, Viber	4	None	1	1	from personal devices only
20. Facebook, Instagram, Tik-Tok, Twitter, LinkedIn, Pinterest, Youtube, Tumblr, Flickr, WhatsApp, Vimeo, Viber, WeChat, Telegram, Line, Messenger, Twitch, Signal	5	gossip and business	5	1	from personal devices only
21. Facebook, Youtube, WhatsApp, Viber	5	Working info	2	5	from personal devices only
22. Facebook, LinkedIn, Youtube, WhatsApp, Viber	3	I don't share	1	3	from personal devices only
23. Facebook, Instagram, Youtube, WhatsApp, Viber	5	None	1	5	from personal devices only
24. Facebook, Viber	5	Less and less. If I used to share a lot besides photos and location, lately I've been avoiding doing it	2	3	from personal devices only

25. Facebook	5	Nothing, they know what my interests are though based on what I visit	1	1	from personal devices only
26. Facebook, LinkedIn, Youtube, WhatsApp, Viber	5	General	1	5	from personal devices only

Q 07

Do you use antivirus application on your devices?
if yes, would you define which? Do you have other security measures on your devices? How often do you update them?
if no, What kind of security measures do you have on your devices?

Table with a translation of all the answers given by the interviewees to the questions asked in this section

Do you use antivirus application on your devices?	if yes, would you define which?	Do you have other security measures on your devices?	How often do you update them?
1. Yes	My service company takes care of them	Yes	When there is a new version announcement
2. Yes	Avira	I do not share personal information; I don't open emails with information that is suggestive, I use different passwords	I check periodically at most every two weeks for new ones
3. Yes	built in by default	Update information, delete unnecessary regularly, clear search history regularly	When there is a new version announcement
4. No	No	No	When there is a new version announcement
5. Yes	Automatic antivirus programme of Samsung	Password, fingerprint	When there is a new version announcement
6. Yes	The system, offered to the device	Passwords, caution when entering certain sites, scrubbing suspicious emails	When there is a new version announcement
7. No	No	Digital hygiene	When there is a new version announcement
8. No	No	No	Never
9. Yes	Sim security, Mchield	No	When there is a new version announcement
10. Yes	AVG protection, This to the computer I do not know	Yes	I check periodically at most every two weeks for new ones
11. Yes	McAfee	I do not give personal information, I do not record passwords	When there is a new version announcement
12. Yes	Antivirus programme	Yes	I check periodically at most every two weeks for new ones
13. Yes	Malwarebytes	Two- and three-factor authentication.	When there is a new version announcement

14. Yes	I don't want to share	Yes	I check periodically at most every two weeks for new ones
15. Yes	ESET NOD 32; AVAST; AVG	I follow the security measures	When there is a new version announcement
16. Yes	Bitdefender	I change the password often, update the security, lock the screens of the devices I use	When there is a new version announcement
17. Yes	Microsoft	Yes	When there is a new version announcement
18. No	HHH	I don't open spam, I don't give personal information from an ID card, bank details - only on the spot in a bank, if a phone number is requested - only if they are couriers or registration for participation in some event.	When there is a new version announcement
19. Yes	Avast, NOD32	Yes. Secure sites and antivirus programs	When there is a new version announcement
20. Yes	All on the market, watched by the American, Russian and Israeli services	I lock them in a safe at night	Never
21. Yes	ESET	All recommended and foreign ai pi as needed.	I check periodically at most every two weeks for new ones
22. Yes	AVG AntiVirus	No	When there is a new version announcement
23. Yes	No	No	Never
24. Yes	Nod-32	Nothing special	When there is a new version announcement
25. Yes	Not important for me	I'm trying, but I'm no expert	When there is a new version announcement
26. Yes	Avast	Yes	I check periodically at most every two weeks for new ones

Q 08

How important do you consider staying informed about cyber security?
How do you keep yourself up-dated on cyber security related issues from professional and individual point of view?

After question 10, it is of great importance for the continuation of the study to determine what kind of studies are carried out at universities and the level of awareness of university administrators and academicians in this regard.

Table with a translation of all the answers given by the interviewees to the questions asked in this section

How do you keep yourself up-dated on cyber security related issues from professional and individual point of view?	Are conditions created in your university to minimize cyber threats in the learning environment? and if so, do you know which ones?
1. I'm reading	Do not know
2. Through reading	Yes

3. In Internet and with specialists	Yes
4. From colleagues and acquaintances who are also familiar with IT threats	No
5. Internet space	Do not know
6. I ask acquaintances	Do not know
7. I'm following the specialists in the field	Limitation of the rights
8. Reading materials and articles on the topic	Yes
9. From both.	Yes, there are conditions. I am not familiar with the details.
10. I'm not informed	Yes, I suppose there are conditions. I am not familiar with the details
11. I'm not informed very well	Do not know
12. Internet	Yes
13. Discussions with specialists, reading materials on the topic	No
14. Through new specialised literature and newsletters	Yes, but they can be improved
15. I am informed via the Internet	Yes, conditions have been created to minimize cyber threats as much as possible
16. I ask experts, I look for information from verified sources	I'm not familiar
17. specialized publications	YES, firewall.
18. If there is someone to ask, then - I'm not a specialist - I don't want to load my computer unnecessarily	Do not know
19. From specialised web sites	Yes. Authorised access
20. I'm following the news on BNT	Security has been instructed not to let cyber threats into the building
21. Through specialised websites and discussions with experts	Yes. Do not know.
22. I do nothing to inform myself	Do not know
23. Colleagues and friends	Do not know
24. Only if I come across an article or something	I know there are, but I'm not sure what they are
25. Ex officio	Do not know
26. I read	Yes

Q 09

What do you think is the role of the HEI top management in minimizing the cyber threats in the learning environment of HEI? Are you aware if your HEI developed a measurement tool about cyber security awareness both for academic staff and students?

- Do you consider your institution sufficient in terms of taking cyber security measures?
- Are you informed about the security of your confidential information by your institution?
- What are the security gaps or threats that you observe in the institution?

Table with a translation of all the answers given by the interviewees to the questions asked in this section

Do you know if your university conducts awareness campaigns about cyber security issues? What are they?	Are you informed about the security of your confidential information by your institution?	What are the security gaps or threats that you observe in the institution?

1.	Do not know	No	Do not know
2.	Seminars, conferences	Yes	At this stage - there are no gaps
3.	No	No	Do not know
4.	I've no idea	Yes	Do not know
5.	Do not know	Yes	Do not know
6.	Yes, meetings with different specialists in the field	Yes	Do not know
7.	There are often guest speakers specializing in national security	No	Ignorance
8.	Yes	Yes	None were observed
9.	I'm not familiar	Do not remember	I'm not that competent.
10.	Do not know	No	I am not familiar with their security system
11.	Do not know	Yes	I have no observations of such
12.	Yes	Yes	...
13.	No	No	The university server is physically located at the university, including being accessible from the network.
14.	No	No	Mainly in the financing for the purchase of specialized software, as in most VUs.
15.	Yes	I am somewhat informed	No security gaps or threats!!!
16.	I've not participated in such	Upon request, I receive information	Access to passwords
17.	Yes	Yes	I haven't seen such
18.	for campaigns - I don't think they are frequent, but more often there are colleagues who defend a dissertation or present a book, as well as symposia, on this topic	No, only if it is personal or departmental information that is not good to share with everyone. If there is something confidential, the interested parties are told personally.	Do not know
19.	No	Yes	I haven't found out
20.	I know, there are no such campaigns	In the institution, confidential information is stored on paper.	ask the institution's security auditors
21.	Do not know	No.	I don't see any
22.	No	No	Lack of info
23.	I'm not familiar	No	Can not answer
24.	No	Yes	Do not know
25.	Do not know	Can not answer	Can not answer
26.	Yes	Yes	Not such for the moment

Q 10

Do you feel your private data is secure when you use the learning environment at your HEI? What is the reason behind your answer?

Table with a translation of all the answers given by the interviewees to the questions asked in this section

Do you feel your private data is secure when you use the learning environment at your HEI? What is the reason behind your answer?
1. Do not know
2. Yes. There is protection
3. I believe Yes
4. Not quite. I have no idea who can have and access specific data
5. Yes
6. Do not know
7. No, there is never 100% protection
8. Yes
9. .
10. I hope they are well protected, at least that's what I'm informed
11. Yes, I feel they are protected because I feel safe at my University
12. Yes
13. Yes, I simply do not use the university network for personal purposes
14. No
15. Yes
16. Can not precise
17. Yes at the level at which I'm using it
18. Yes, because if a problem arises, I can ask for help from the "computer lab". And 98% of the mail is used only for work at our university
19. Yes.
20. Yes, more of them are on a paper or prevented with password
21. Yes. The reputation of the HE institution
22. I doubt it. Lack of concrete information.
23. Sooner Yes
24. Yes, I feel safe because I know there is a whole department that works in this direction
25. I believe
26. Yes

Q 11

Is there any programme/short informative course which has been created to further educate the academic staff and students, in order to reduce their chance of falling victim to cyber attacks in the learning environment in the HEI? What actions does your university take to raise awareness of cyber security in courses or extracurriculars?

Table with a translation of all the answers given by the interviewees to the questions asked in this section

Is there any programme/short informative course which has been created to further educate the academic staff and students, in order to reduce their chance of falling victim to cyber attacks in the learning environment in the HEI? What actions does your university take to raise awareness of cyber security in courses or extracurriculars?
1. Do not know
2. No. But it's good to introduce
3. I have no info
4. Do not know

5.	Do not know
6.	No
7.	Lectures are held
8.	Yes
9.	I'm not familiar
10.	I'm not informed whether there is such a programme
11.	Do not know
12.	...
13.	No
14.	Yes
15.	There is
16.	Do not know
17.	Do not know
18.	I'm not familiar with it, there may be, and I don't know
19.	I'm not familiar
20.	And if there is, they will become a victim again. for more see the phone mafia - constant media reports and constant grandma/grandpa throwing a wad of money ... same with cyber security ... naivety and trusting is a human quality and scammers are good psychologists.
21.	Do not know
22.	No
23.	I think No.
24.	I'm not sure
25.	Do not know
26.	Yes

Q 12

Are there any other points that you would like to add regarding the topic?

Table with a translation of all the answers given by the interviewees to the questions asked in this section

Are there any other points that you would like to add regarding the topic?	
1.	No
2.	No
3.	No
4.	It would be good if the non-learning and non-IT communities are informed more regularly when changes are made to cybersecurity.
5.	No
6.	No
7.	No
8.	No
9.	.
10.	It's good to talk more and be informed about how to keep our data fully secure. It will always have gaps, there is no way but to have greater reliability and security
11.	No
12.	...
13.	No
14.	No

15.	In my opinion, cyber specialists should commit to protecting both children and adults on the Internet, arpanet and intranet in relation to virtual levels and porn, completely erasing this page from the life of humanity!!!
16.	knowledge must be constantly updated
17.	The questions in the survey are not based on reality
18.	It would be nice, in addition to protecting personal data, to not be asked for phone numbers to access our mails if we happen to be on the same device. (pretend - you get a new computer/laptop and it won't let you access your mail because it wants a phone number.) Sometimes email addresses are created for conferences and other events that are not personal, but data is requested. And if these conferences for annual, but the people who work on it change (not 100%) and have to work with this mail... etc. (this year X is in charge, and next year P... .and they work on different computers.....) It turns out that the same people who push all kinds of software and platforms on us are the ones who want more personal data from us (only they don't call it "cyberattacks" but "to ensure your security".) ....yeah well...
19.	No
20.	Antivirus programs are now automatically updated - your question is irrelevant. Questions about the lottery and bank accounts are not answered - I mark as spam/phishing. Question omitted: Do you use an application to store passwords. Password questions are old - no one has one or two passwords anymore. No question about two-step authentication!
21.	No
22.	No
23.	No
24.	No
25.	No
26.	No

ANALYSIS OF THE RESULTS FROM THE FOCUS GROUP'S INTERVIEWS HELD IN POLAND

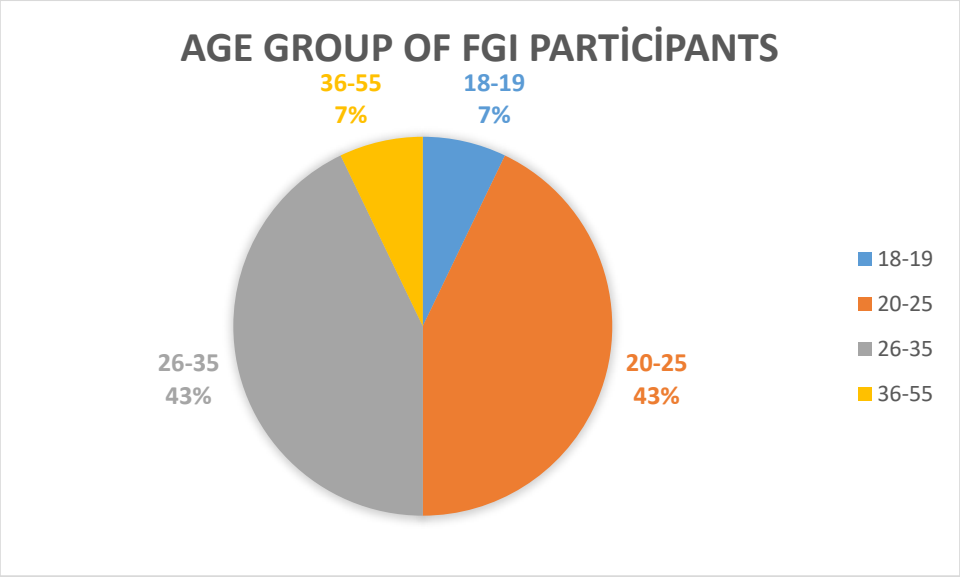
Introduction

Following report was prepared as a part of Erasmus Strategic Partnership in Higher Education named "Cybersecurity in practice for non IT oriented HE courses". The report is divided into demographic information, description/analysis of the answers received during the focus study group and final conclusion section.

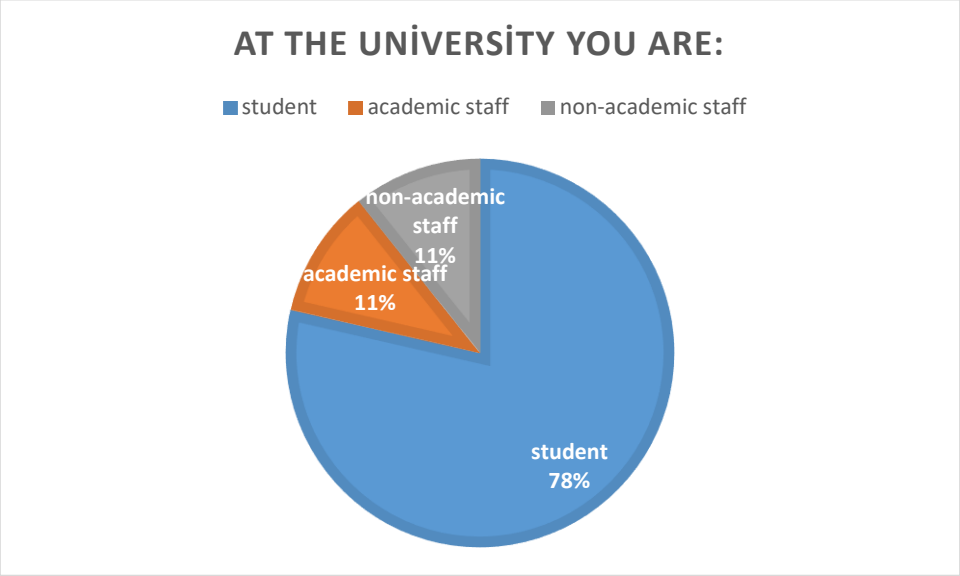
The actual study took place on 27th October 2022 in the University of Opole, building of the Faculty of Economics. In the focus group in total took place 28 people divided into two groups and the sessions included participants from the economics and business departments. The sessions lasted on average 75 minutes and were reported in the accordance with the Project Guideline for the Focus Group Analysis.

Demographic Information

The age of the participants is duly presented by the graph below. The majority of the participants are of age between 20 to 25 (43%) and 26 to 35 (43%).



A total of 22 students, 3 academicians and 3 administrative staff took part in the study. All the participants who took in the study are studying business and economics (including academicians). The administrative staff is related to the administrative functioning of the university and lecturers work in business and economics field.



Amongst the participants who took part in the study no student had experience of participating in the focus group interview before. Academicians and administrative had all experiences of taking part of similar research, mostly through European Union Projects.

Study Findings

In this part of the report Eduvibes Foundation which moderated the focus group interviews collected the findings. “Yes or No” questions were included in the research form given to each participant and everyone was asked to answer these questions. As for the open-ended questions, we followed the guidelines and the participants were allowed to freely express their opinions related to the topic.

The open-ended questions, on the other hand, were addressed by the participants in an ordered manner, as stated in the focus group working rules at the time, within a free speech

environment. The moderator facilitated the discussion with the support of the guidelines for the activity.

How would you describe cyber security?

Participants came with the own definitions of the cyber security. Some of the noted definitions are as follows:

- *Cybersecurity has to do with the safety and security of online transaction and private information, protection of sensitive information (P5)*

- *Cybersecurity is the practice of defending computer and mobile devices and its electronic systems (P8)*

- *The protection of a private data and sensitive information systems for individuals and corporations over the internet (P4)*

- *Cybersecurity is the application of technology processes and controls to protects systems, networks, software, devices and data from cyber attacks. (P16)*

- *It entails all the processes and security put in place to make online and offline data transfer or activities safe from criminal manipulation of theft (P17)*

Participants were coming with own definitions or cyber security and they mostly agreed on the most common features of such definition. Some of the participants understood it only in the more narrow form (such as protecting their personal data), while others understand it more broadly and mentioned that cyber security is as important for individuals as for the corporations. Participants understood is as a form of defence against malicious attacks and cyber crime which can harm them as users. All participants were active duing the question and everyone came with the defintion of their own (which often was similar to other participants).

Can you list at least 3 cyber threats?

Most participants had understanding of most important types of cyber threats and did provide their selections. They had provided as with variety of threats, some of them of high advancement. Amongst the most popular answers we noted down:

- *Viruses*
- *Phishing*
- *Spam*
- *Hacking*
- *Evil usage of AI (they mentioned the threat which was described by Elon Musk);*
- *Blackmailing*
- *Data breakage*
- *Identity theft*
- *Scamming*
- *Financial online crime*
- *Spyware*
- *Ransomware*
- *Malware*
- *Distributed Denial of Service (DDOS)*

What do you think should be considered when choosing a password?

The participants have various approaches for choosing of the password. Some of them had clearly negligent attitudes (like sharing the password to roommates or writing them down on the wall), while others never shared a password with anyone else. Amongst their ideas what is considered important while choosing the password, amongst popular answers we could find:

- It should be at least 10 characters and have both uppercase and lowercase letters and as well numerals (P21);

- Complex characters which have nothing to do with your name and birthdate. It should contain numbers and special characters (P9);

- You can use a randomizer to create a password. The password protects not only your private data but as well your environment (P20);

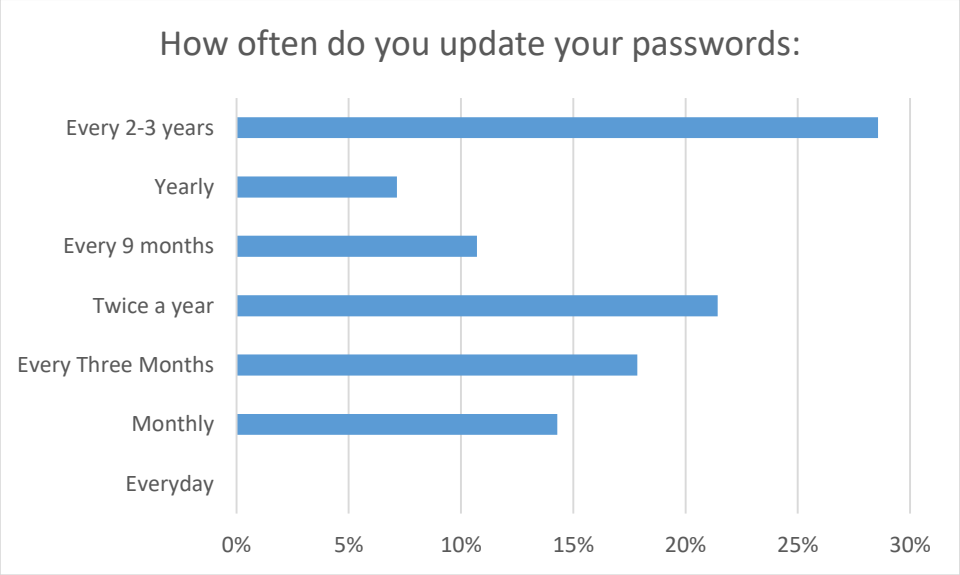
- You should also take into account your ability to memorize password (P17);

- Don't ever use your personal information for the passwords. Try to use different passwords for different accounts and set up two-step verification (P18)

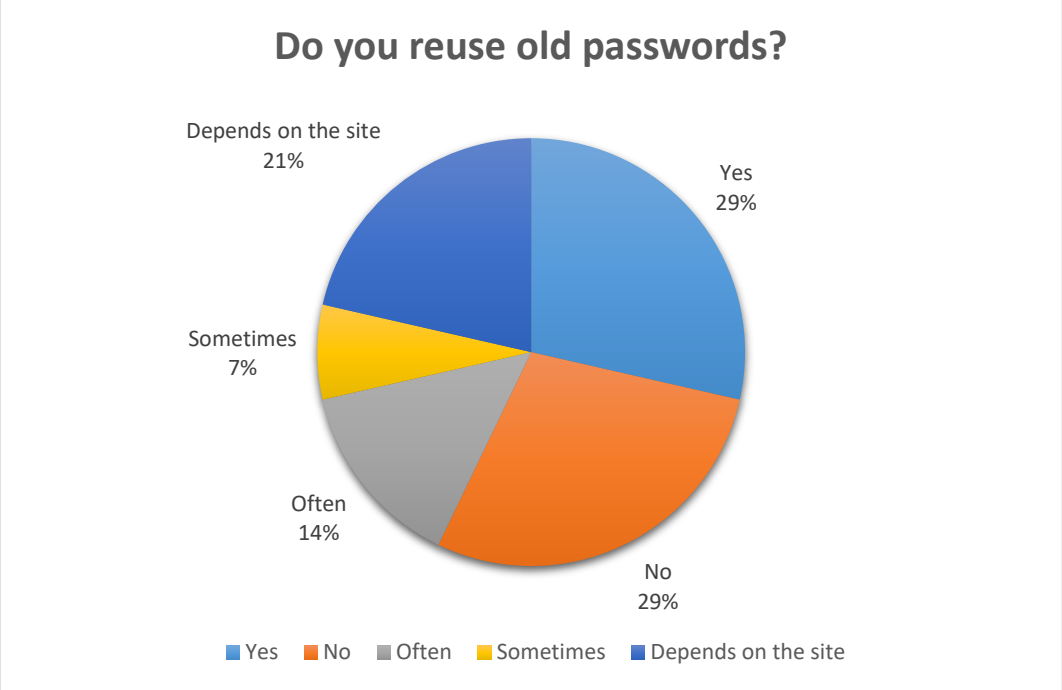
- It has to be something which we can remember and at the same time it must be unpredictable to others (P13)

- It has to be something personal/private and be complex/hard (P6)

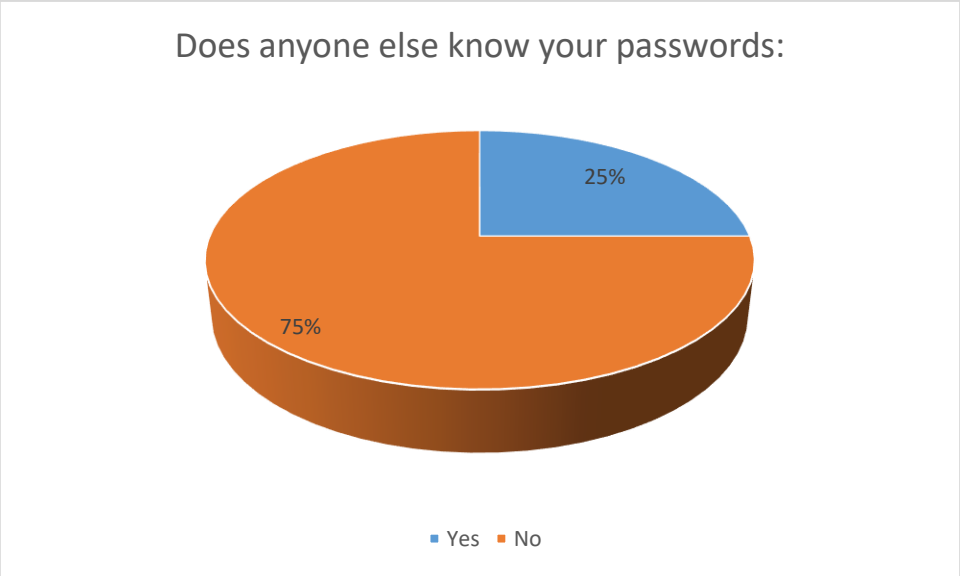
We have asked the participants about the frequency on how often they change their passwords. The most popular answer amongst surveyed participants was that they change password relatively rarely, every two to three years (29% percent of the participants).



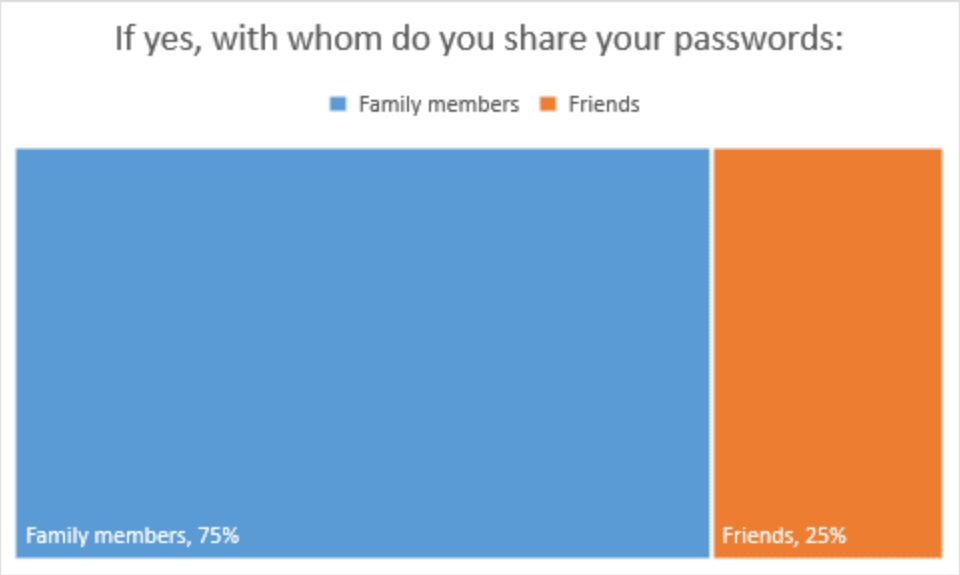
We have also discussed with he participants whether they reuse the passwords which they have used in the past. Only 29% of the participants never use the older passwords in their devices. Remaining people re-use them with various frequency. It clearly states that there is a need for higher consciousness amongst the group regarding the threats of using old passwords.



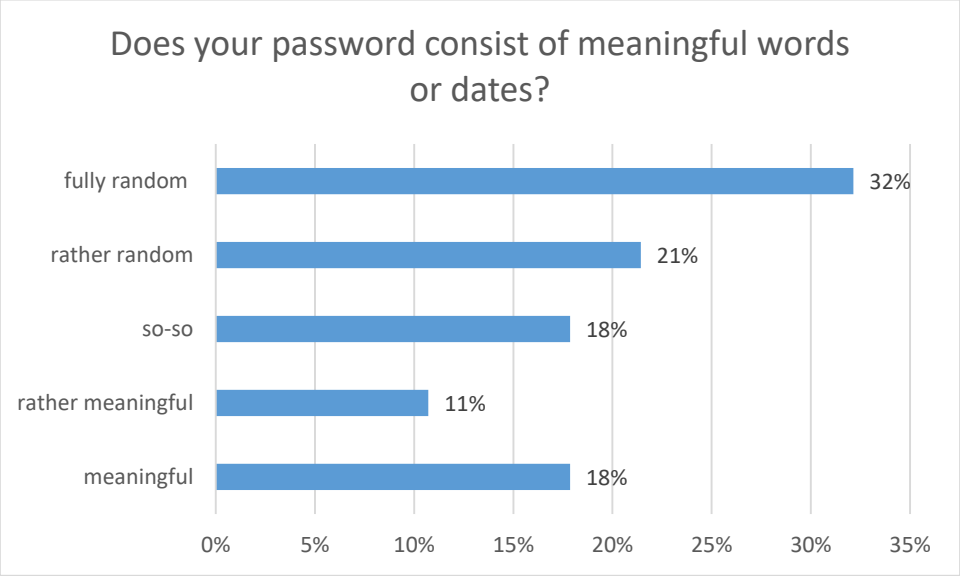
The last part of focus group discussion regarding the password usage concerned if and to whom the participants share such sensitive data as passwords. It appeared that 75% of the participants do not share the passwords with anyone, while one fourth of the studied group indeed shares their passwords with others.



If we look in more detailed way with whom the participants share the passwords, three fourth of participants shared the data with family members and 25% of them gave the passwords to friends. Noone gave passwords to the co-workers.



We also asked the participants if they choose passwords with the meaningful personal dates or names (for example name of mother or own's birthday) or random passwords. We used Likert scale from 1 to 5 to obtain data for this question. The vast majority of participants use random or rather random passwords (summed up to 53%). Around 18% of participants used fully personal dates or meaningful names for their passwords.

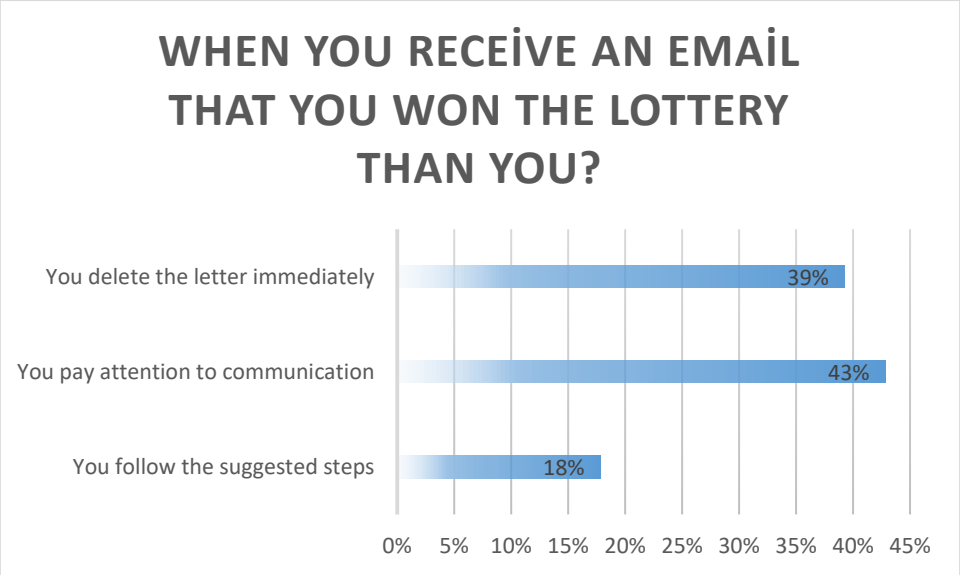


Do you follow the links from the e-mails for "lottery win" or "changes in bank account"?

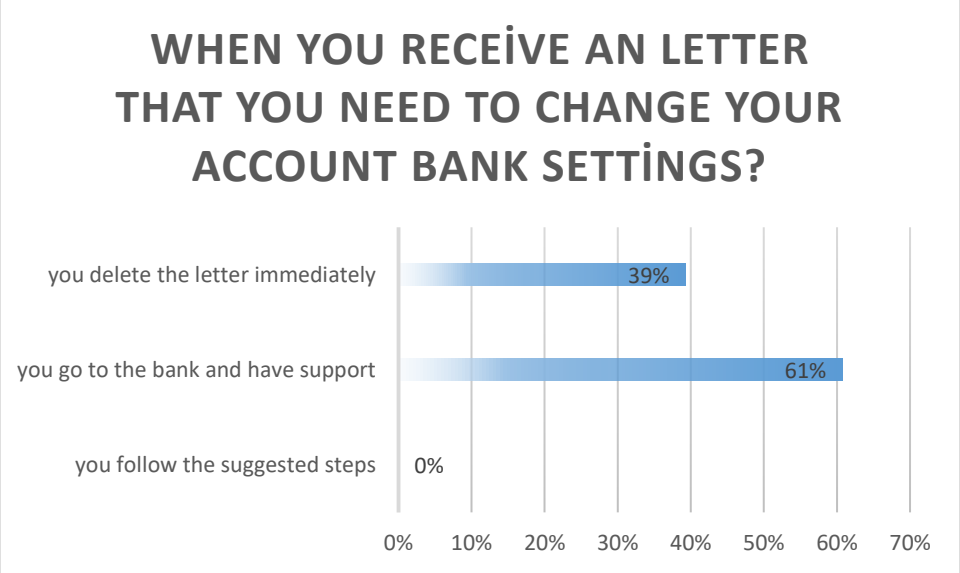
This next section of the focus group interview related to the approaches to unexpected emails from the third parties which might be a phishing attempts. We have discussed with the

participants two possible options of “lottery win” message and request from the bank by email about “changes in bank account”.

Surprisingly the participants had different attitudes to both type of dangers. In case of winning lottery email, participants where much careless than in the situation of dealing with bank and their money. It appeared that 18% of them would follow the suggested steps, while 43% of them would communicate cautiously. 39% of the FGI parttakers would immediately delete such dangerous emails.

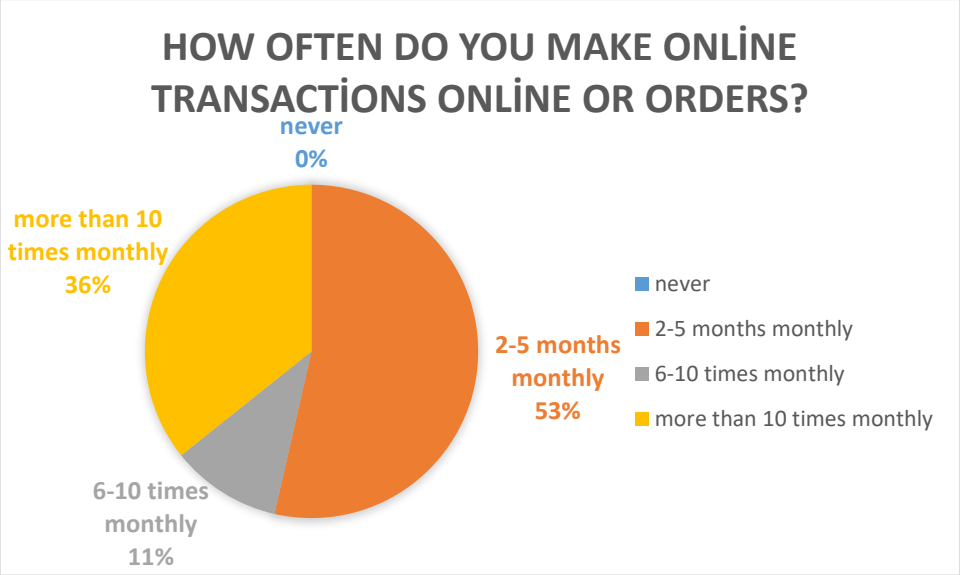


But if the communication by email would come from the bank, the participants would pay much more attention to it and their security.



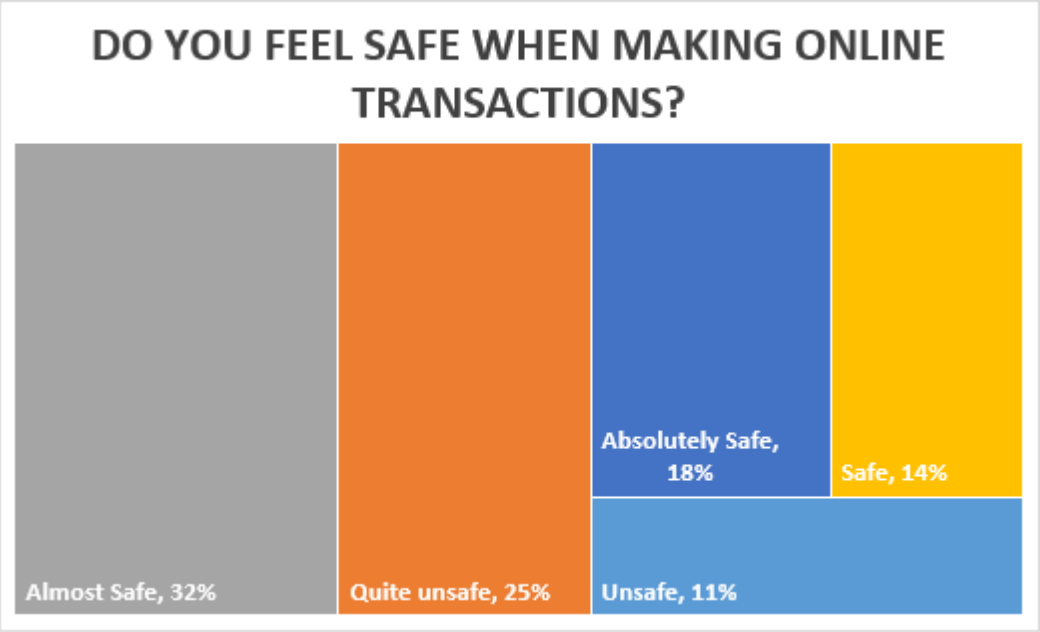
How often do you make online transactions or orders?

The participants are active in the online transactions and there was no person in the FGI that would state that never uses online transactions. The large chunk of the interviewed participants (36%) makes more than 10 online transactions monthly.

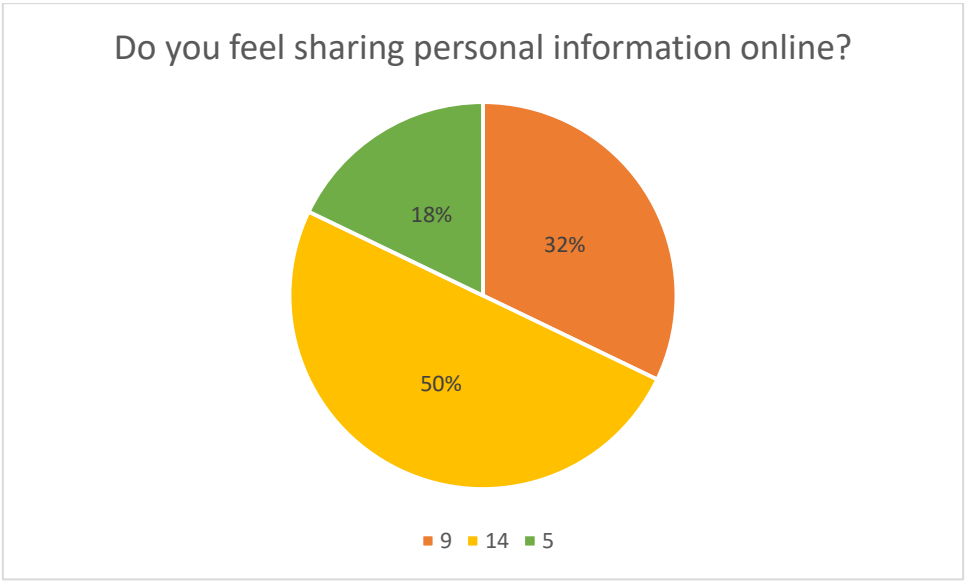


Do you feel safe when you make transactions or share private information?

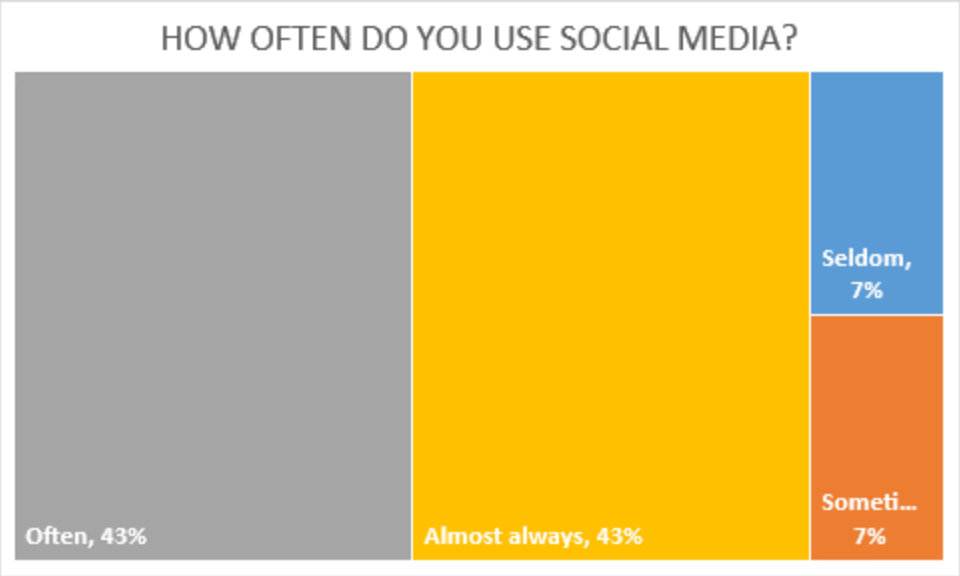
As we see that all participants make online transactions, we asked them what is their feeling regarding their safety while doing transactions online. We obtained the following data in the Likert Scale (1 to 5) and the most popular answer was so-so (3 in Likert Scale).



We asked the participants also the same question about sharing the private information online. It appeared that FGI partakers are more afraid of sharing their private data online, while 82% of them felt safe or absolutely unsafe, while astonishing 0%! felt safe or absolutely safe. It shows that they are aware of the potential dangers of sharing private information online.

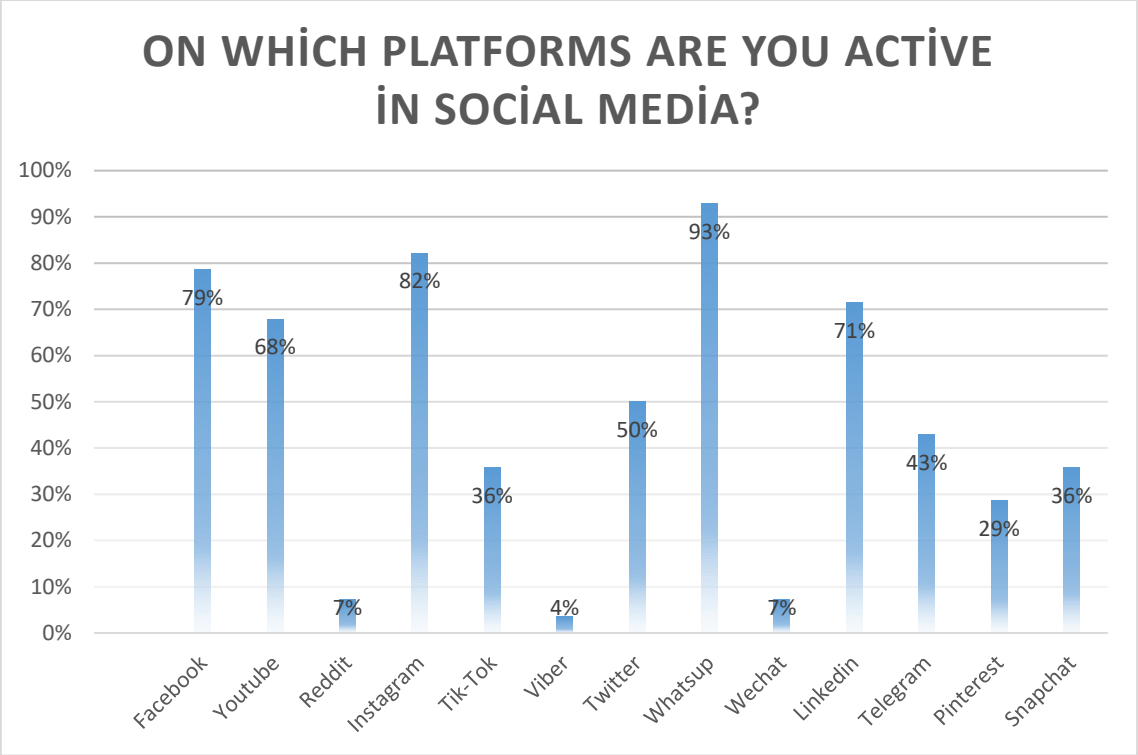


On which platforms are you active in social media? How often do you use them? What kind of information do you share on social media?



In the next section of the FGI we discussed usage of the social media. It appeared that all the participants use social media very actively (86%) and there was no single participant which would not use social media at all.

If we look at the statistics which social media are the most used by the participants, we have received following picture (multiple answers where possible). The most popular platform was Whatsup (92%) followed by Instagram (82%) and Facebook (79%). It comes at no surprise that three most popular platforms are owned by the same company Meta Corporation.



When asked in the discussion, how they use social media and what they shared we received following answers amongst others:

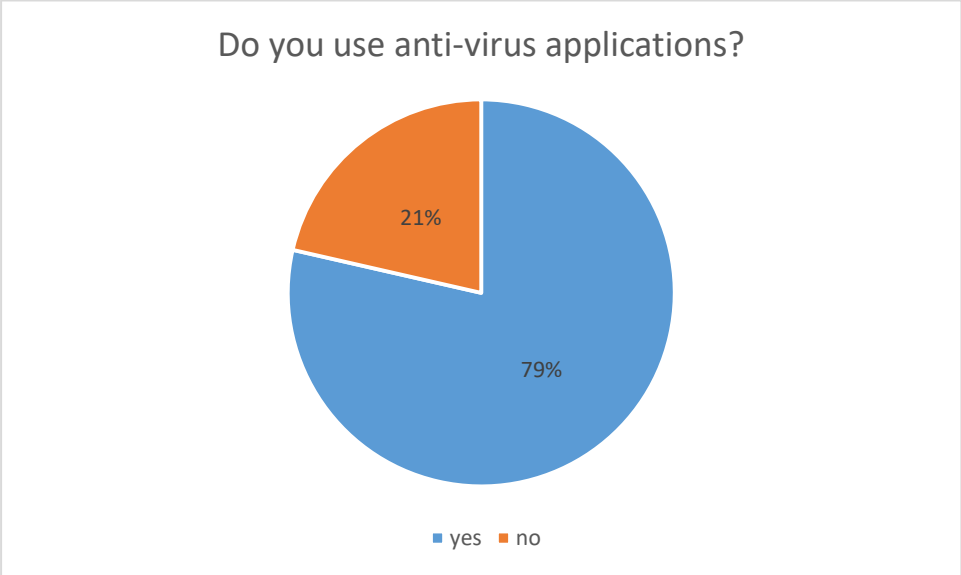
- *I share photos, videos, basic bio data (P17)*
- *Just photos sometimes (P6)*
- *Contents that inspire other people. Yes, mostly inspirational content (P1)*
- *Information about my professional life and some basic information about my personal identification (P19)*
- *Most of the times I share my picture and some ideas which I find interestig (P13).*
- *Photos of places that I visit and meetings with friends (P23)*
- *Mostly funny videos depending on the social media type. I am using especially Tik-Tok. I also share school stuff (P18)*

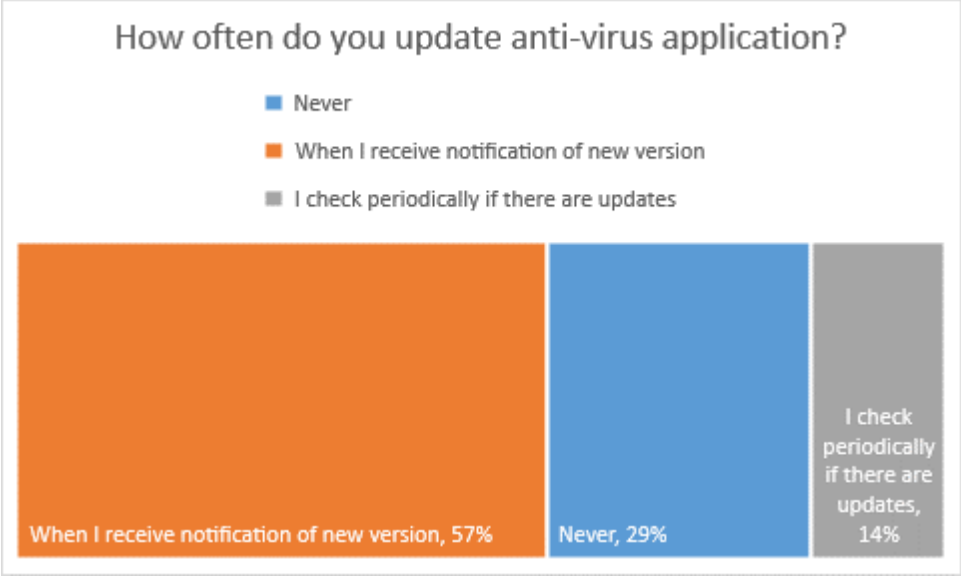
Do you use antivirus application on your devices?
if yes, Would you define which? Do you have other security measures on your devices? How

often do you update them?

if no, What kind of security measures do you have on your devices?

In the next section we discussed anti-virus applications. Surprisingly 25% of the participants do not use anti-virus software or at least is not aware of this. Amongst those who use anti-virus applications 29% claims that never updates their virus software.





Participants mentioned various anti-virus applications including:

- *AVG Antivirus*
- *Microsoft Windows Defender*

- *Avast*

-*MfAfee (the most common answer chosen by participants)*

How important do you consider staying informed about cyber security? How do you keep yourself up-dated on cyber security related issues from professional and individual point of view?

Participants generally agreed that it is important to stay informed about cyber security, while stressed out that in current situation of information overload it is only one of the important issues which have to be tackled (others included amongst others: climate change, economic situation etc).

Some of the statements on the subject are as follows:

- *I don't keep myself updated. I just follow the trend and what is going on about cybersecurity (P5)*
- *I don't keep myself updated on cybersecurity topic (P6)*
- *I just get some general information from the news (P4)*
- *I really don't do it, sometimes just click on some news (P10)*

While most of participants did not update themselves about cybersecurity issues, some of them tackled the topic:

- *I read relevant contents online. And I sometimes watch videos regarding cybersecurity online (P1).*

- *I read articles and attend conferences (P16)*

What do you think is the role of the HEI top management in minimizing the cyber threats in the learning environment of HEI?

This section was harder for the participants as they could not envisage the role of HEI top management in minimizing the cyber threats in the learning environment of HEI. They could not come up with any meaningful ideas in that part of FGI, maybe because of their limited understanding of the role of administration and management in the role of the university.

Are you aware if your HEI developed a measurement tool about cyber security awareness both for academic staff and students?

In this section participants agreed that their HEI did not develop any measurement tool about cyber security awareness both for academic staff and students. They were not aware of existing of such tool and never heard of its existence.

Do you feel your private data is secure when you use the learning environment at your HEI? What is the reason behind your answer?

Participants generally did not feel that they data is safe with the university systems and also could not come up with many cybersecurity initiatives which could improve the situation at their HEI. Their reasons behind the answers were as follows:

- *No, I don't think it is safe as it is stored in the outside databases. I don't think uses private databases is safe at all.*
- *I think university is trying to do something about the security of the students, for example blocking the access to pornographic or betting websites from the campus;*
- *I don't evaluate them good with regards to cybersecurity;*
- *There is not so much about security. I remember when the main system of the university USOS was down due to some cybersecurity problem.*
- *I am afraid to use wi-fi of the university and prefer to use my private instead in order not to share information with others.*
- *I don't think so they do anything about it.*

Is there any programme/short informative course which has been created to further educate the academic staff and students, in order to reduce their chance of falling victim to cyber attacks in the learning environment in the HEI? What actions does your university take to raise awareness of cyber security in courses or extracurriculars?

- *I am pretty sure nothing is done about it.*
- *I don't really know if there are such programmes.*
- *Not sure about it.*

- *Sometimes they request for the change of the password.*

Generally, students were not able to pinpoint initiatives of their HEI in this regard, however generally they stressed that such initiatives could be important and helpful

Conclusions

The actual study took place on 27th October 2022 in the University of Opole, building of the Faculty of Economics. In the focus group in total took place 28 people divided into two groups and the sessions included participants from the economics and business departments. The sessions lasted on average 90 minutes and were reported in the accordance with the Project Guideline for the Focus Group Analysis.

The focus groups showed that students have some basic understanding what the cybersecurity is and its importance for their personal and professional life. They differed in the behaviours in the Internet, as some of them were very cautious, other followed the negligent behaviour regarding to passwords and activities online. None of them have any formal or informal courses in the cybersecurity ever and they stressed out that it is first time they discuss the issue of the cybersecurity in the higher education institutional environment. They would be eager to learn more and get some more courses on the topic from their HEI, although they agree that cybersecurity is not the priority issue for the universities and it is their own atttitudes and self-learning which is important for the issue. However, only few of partakers in FGI update themselves on the issues of cybersecurity and current trends.

ANALYSIS OF THE RESULTS FROM THE FOCUS GROUP'S INTERVIEWS HELD IN SWITZERLAND

Introduction

The main objective of the study is to get an overview of the level of understanding of cyber threats and the availability of security skills among all categories of participants in the higher education system who are not IT specialists.

A total of 21 participants took part in the study, including students, academic staff and administrative staff.

The answers were collected in the period 2-17 October 2022. Considering the number of people required for the test, and the nature and number of questions (more than 30 organized in 10 categories as specified in the guidelines), it was very difficult to organize a real focus group, gathering all the participants in one place at the same time. Therefore, data collection was held in a mixed mode. A group of about 20 students was initially involved in presence to explain the objective of the study; after this introduction, the students were invited to answer a survey individually; the questionnaire was made available in digital form on the web in Italian. Other participants (academic and administrative staff) were involved through e-mail messages, where, after a short introduction to the study objective, a link to the digital survey was provided.

This approach allows us to collect a consistent amount of data, most of them coming from open-ended questions. In the following sections the participant profile is outlined, then the questions to each question are examined and a summary of the analysis is presented. The answers to each question of the 21 participants have also been translated and published in the appendix section.

Demographic Information

A total of 21 participants took part in the survey, including 15 students (71,4%), 2 people of academic staff (9,5%), 4 of the administrative staff (19%).

Q 01 Participant category

Are you student, academic staff, or administrative staff ?

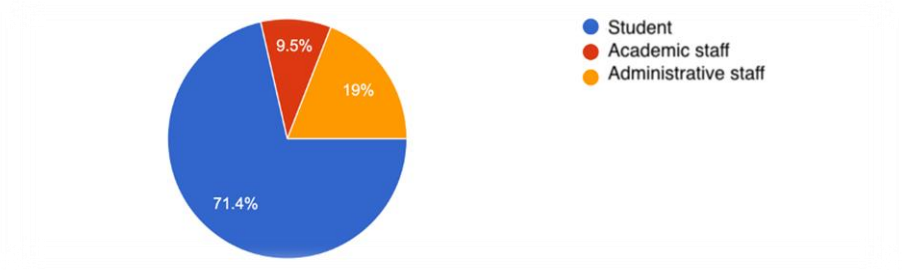


Figure 1: participant categories

Q 02 Participant age

How old are you?

The age of the participants is distributed as follows:

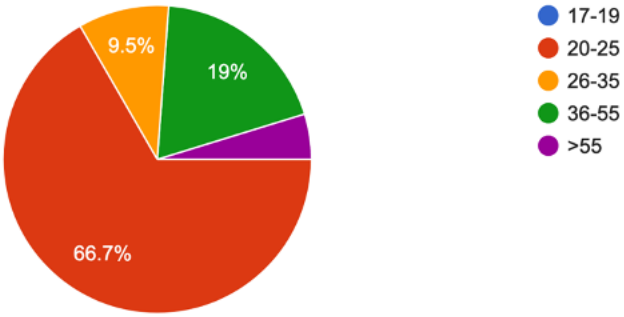


Figure 2: participant age

- 20-25 Years – 66,7% of participants (14)
- 26-35 Years – 9,5% of participants (2)
- 36-55 Years – 19% of participants (4)
- >55 Years – 4,8% of participants (1)

Study Findings

Q 03 About cyber-security

The answers to these two questions indicate that participants have a clear idea of what cyber-security is and a good level of understanding of cyber-threads.

How would you describe cyber security?

The analysis of the answers reveals that most of the participants have a quite clear idea of what cyber-security is. Here are some of the most frequent answers translated in English:

- IT security are technologies that prevent data theft or attacks on large or small electronic devices, but it is also data and information security and protection from computer crimes;

- protection from cyber-attacks;
- the set of means by which a user can keep their personal data safe;
- In my opinion, IT security is to have your data on IT infrastructures safe;
- Antivirus, block fraud, emails with trojan horses, etc.
- The level of protection of your personal information on an electronic device.

Can you list at least 3 cyber threats?

Concerning the cyber-threats, almost all the participants are able to list some examples; among the most common answers we can mention:

- viruses
- phishing
- trojans
- false emails
- malware
- spyware
- data theft

Q 04 About password

A collection of 6 questions is useful to clarify how much participants are familiar with the password security requirements.

In summary, participants have a good knowledge of how to create a secure password (use of complex strings with combination of letters, symbols, numbers, not connected to personal data), although they do not update their passwords very frequently and often reuse a password used before. The majority of them does not share their passwords with other people. The large part of the interviewees saves their passwords somewhere in paper or digital form.

What do you think should be considered when choosing a password?

Participants declare that they take into consideration several requirements when choosing a password; among the most frequently mentioned, there are:

- Use passwords that are not meaningful, not linked to dates or data traceable on the net
- Do not use the same for different accounts
- Insert a combination of numbers, letters, uppercase and lowercase characters, special characters

How often do you update your passwords spontaneously?

The answers to this question demonstrate that participants do not update their passwords frequently. 47,6% of participants (10) state that they update them yearly, while 42,9% (9) never change them. Avery small minority changes their passwords every 6 or 9 months (2 participants).

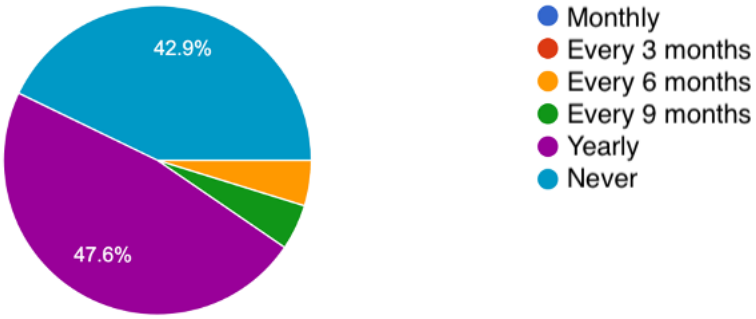


Figure 3: password update frequency

Do you reuse a password you used before?

To the question "Do you reuse a password you used before?" (Fig. 4), the majority of respondents (52,4%) answer "Often", while one third declares to reuse a password sometimes. Only a small percentage never reuse it.

This indicates a general low awareness that password reuse can facilitate cyber-attacks.

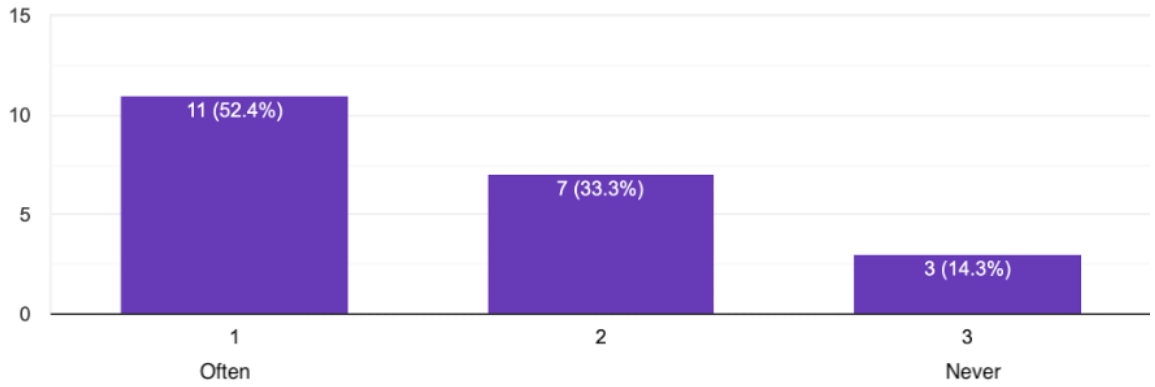


Figure 4: password reuse

Does anyone else know your password?

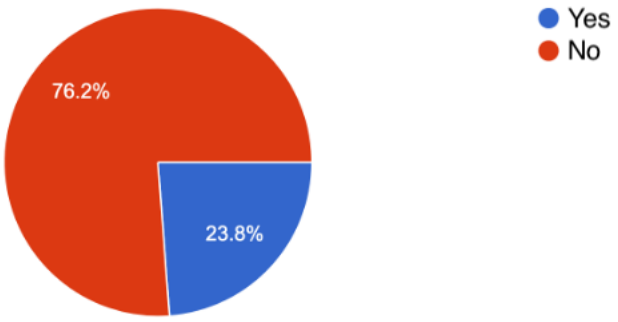


Figure 5: password sharing

The large part of interviewees, more than 75%, does not share information about their passwords with other people, demonstrating a good awareness of the need to protect their access passwords.

Do your passwords consist of meaningful words or specific dates?

Figure 6 shows the distribution of the answers to this question on a scale from 1 to 5, where 1 indicates "meaningful words or specific dates" and 5 "random letter, numbers, symbols".

The most part of the answers is between 3 and 4. This means that participants do not express a remarkable tendency towards the extremes, although there is a slight tendency towards the use of random characters for their passwords.

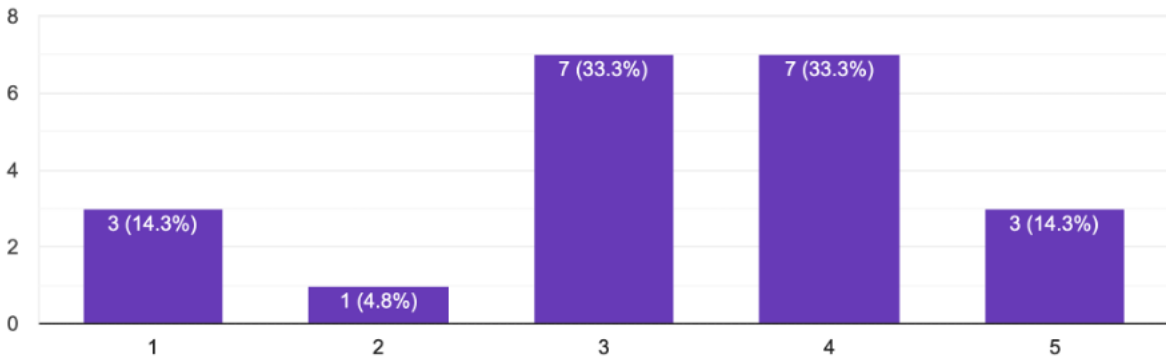


Figure 6: password composition

Is there a place where you write down your passwords?

The large part of the respondents (more than 80%) saves their passwords somewhere. A small part of them write password on paper; the others store them in digital form on their PC or phones. Some respondents use dedicated apps (e.g., google password, bit warden).

Q 05 Reaction to e-mail requests, online transactions, personal info sharing

The following questions aim to understand the participants' behaviour when they receive requests or make transactions.

When you receive a letter that you won the lottery you…?

The large part of the respondents (more than 80%) affirms that they delete the letter immediately, showing a good degree of awareness towards potential phishing. Nobody declares to follow the suggested steps (see figure 7).

Figure 7: letter about lottery win

When you receive a letter that you need to change your bank account settings

The majority of participants (57,1%%) affirms that they delete the letter immediately; however, a consistent part goes to the bank to ask. One participant declares that he/she follows the suggested steps (see figure 8).

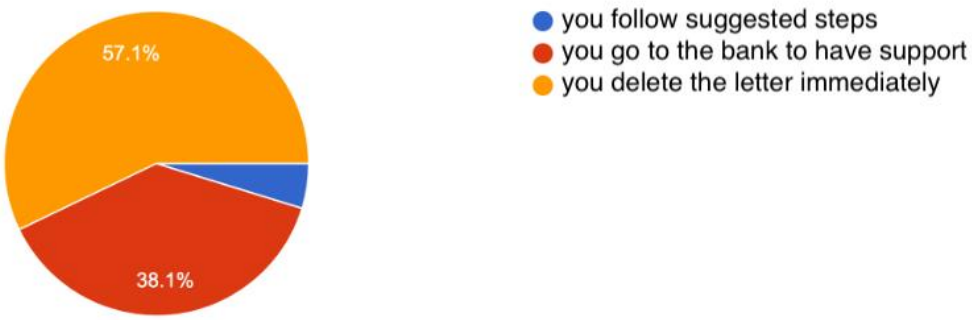


Figure 8: request to change bank account setting

How often do you make online transactions or orders?

The answers to this question indicate that participants are quite familiar with online transactions. More than half of them makes 2 or 5 transactions per month, while 23,8% makes more than 10 transactions per month (see figure 9).

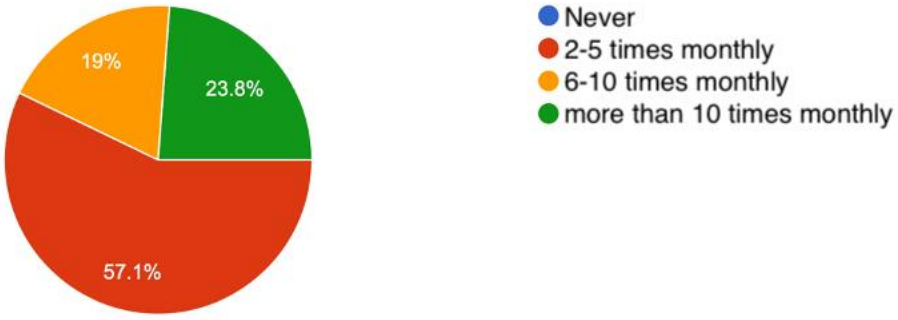


Figure 9: frequency of online transactions

Do you feel safe when you make transactions?

The answers shown in figure 10 indicate that participants feel safe when making transactions online. More than 65% answers 4 or 5. Therefore they recognise a good level of security associated with online transactions and orders.

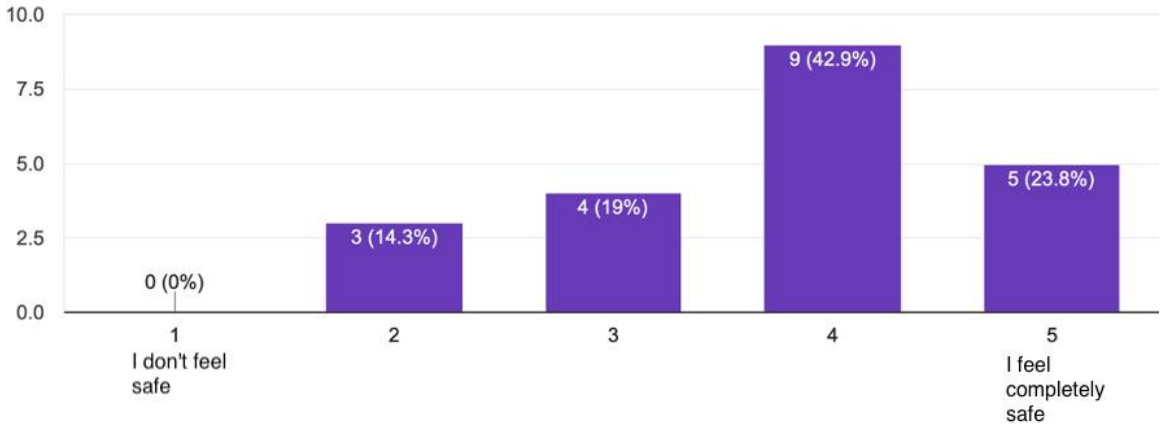


Figure 10: security feeling with transactions

Do you feel safe when you share private information?

It is not same for security feeling in distributing private data. Figure 10 shows that participants do not feel really safe when sharing private information. The majority of the answers is between 1 and 3.

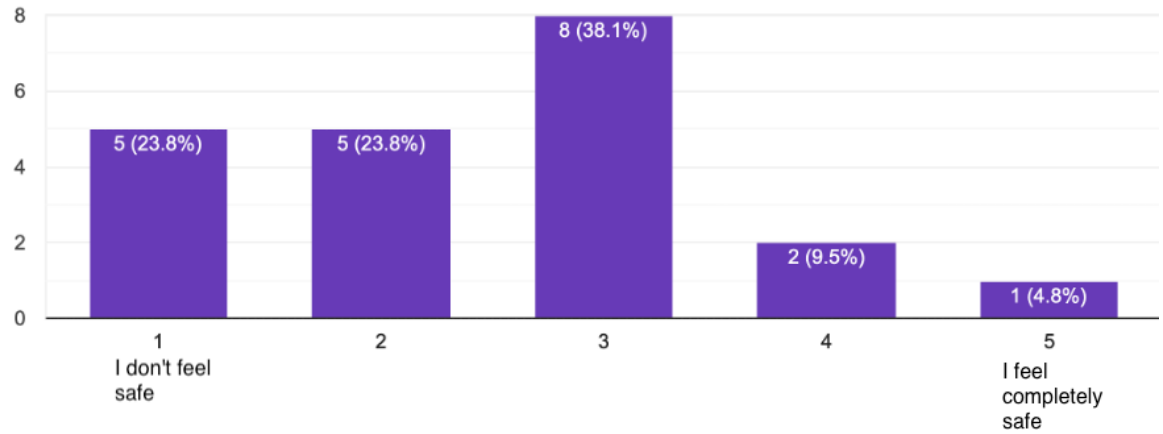


Figure 11: security feeling with sharing personal information

Q 06 Social media

A number of different questions are useful to clarify how social media are used by participants; they help us to know which platform is mostly used, how frequently, which information is shared, which devices are used.

On which platforms are you active in social media?

Figure 12 shows the distribution of the answers about social media platforms. The most used platform is *WhatsApp*, selected by more than 90% of the respondents, followed by *YouTube* (81%) and *Instagram* (71,4%).

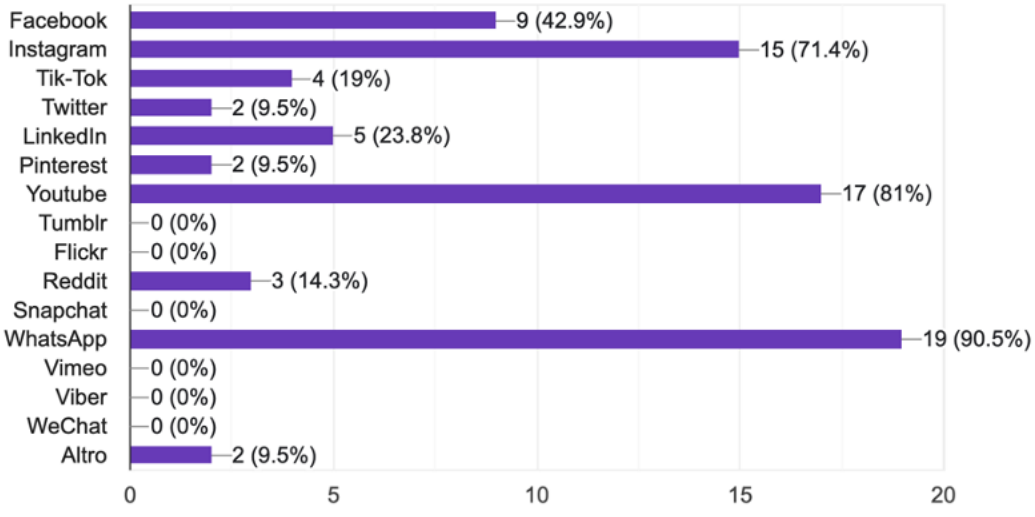


Figure 12: social media platform

How often do you use them?

Figure 13 shows the frequency of use of social media by participants; the answers selected by most respondents are between 3 and 5, indicating that social media are used quite often; 28,6% of interviewees declare to use them continuously.

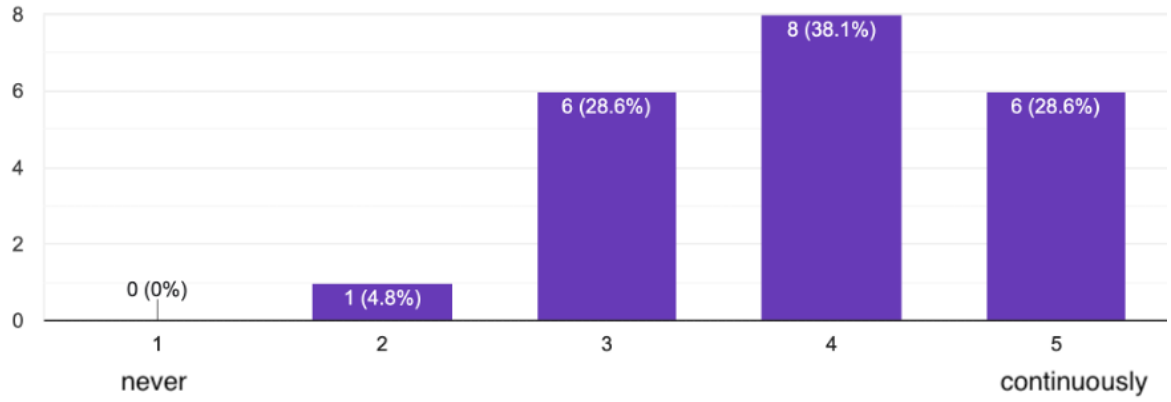


Figure 13: frequency of use

What kind of information do you share on social media?

A very large part of participants states that they do not share personal information on social media or as little as possible; most of them just use WhatsApp to exchange information. Few people share information such as images, photos, videos, news, school information.

Do you share your personal life on social media with photos or text?

As a confirmation of what indicated in the answers to the previous question, figure 14 shows that a large part of participants declares that they do not share their personal life on social media or limitedly.

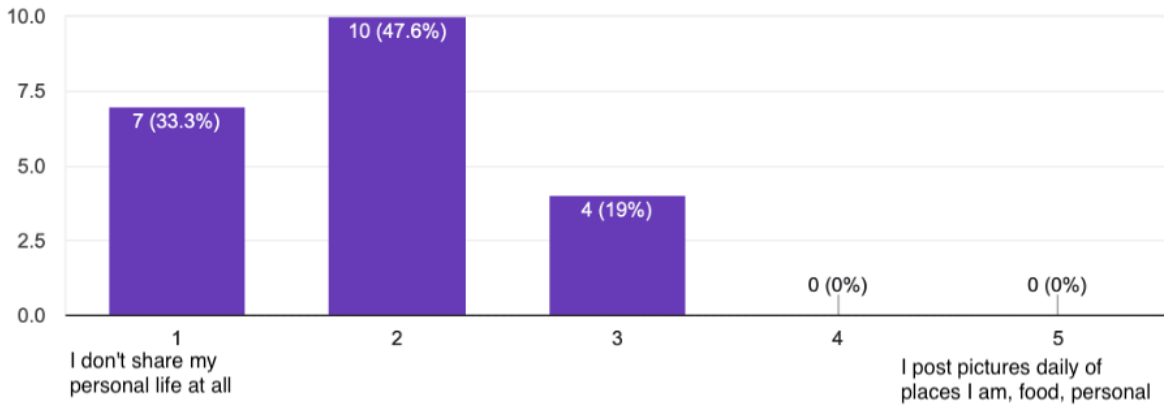


Figure 14: personal information sharing

Do you pay attention to background details in the photos you share?

In line with the previous answers, more than half of the participants pays attention to the background details of their photos (see figure 15)

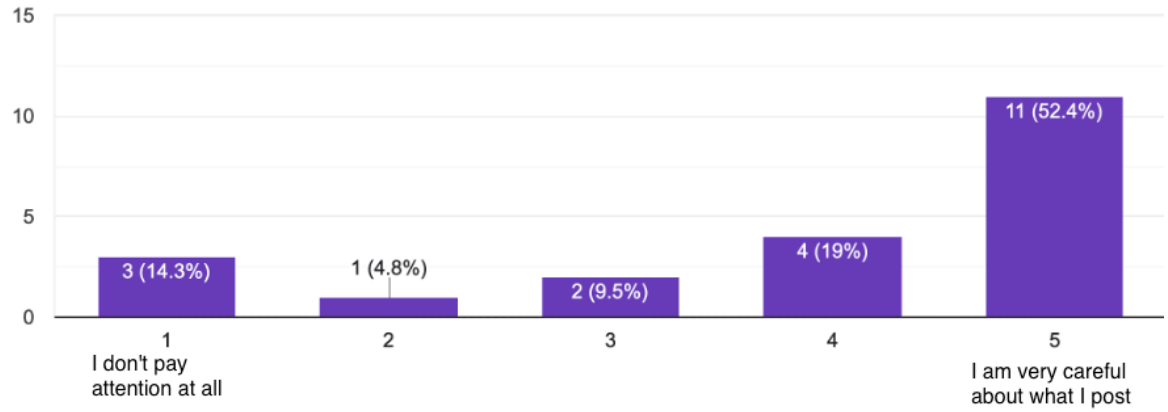


Figure 15: attention to background details

You use social media from… ?

Almost the whole group of participants use their personal device (see figure 16).

Figure 16 used devices

Q 07 Antivirus

A collection of 4 questions aims to get information about the use of anti-virus applications and other security measures.

Do you use antivirus application on your devices?

The use of anti-virus applications is quite common among the participants. 66,7 % of the respondents uses anti-virus applications on their devices.

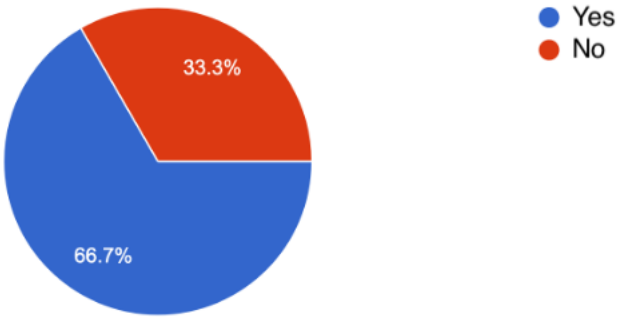


Figure 17 anti-virus usage

if yes, would you define which?

The most popular anti-virus applications are avast, Window Defender, and Northon; other applications mentioned by participants include: Kaspersky, McAfee, Windows Security, Vodafone protection malware, Sophos, Microsoft Defender.

Do you have other security measures on your devices?

Most of the participants declare to use antivirus and anti-malware applications for periodical scan, device protection with password, regular backup, attention to what is dowloaded, regular updates, use of virtual machines and VPN, change of passwords, no permissions to applications if not indispensable, 3 login steps for payment transactions, no personal data sharing, no answer to unknown phone numbers and suspicious emails, device tracking.

Only 2 participants declare that they do not use security measures.

How often do you update anti-virus applications?

The answers to this question show that the most of the interviewees are aware of the importance of updating the anti-virus software installed on their devices.

42,9% updates anti-virus applications when they receive notifications of updates, while a slight smaller percentage (38,1%) checks periodically for updates.

The others (19%) affirm that they never update anti-virus applications

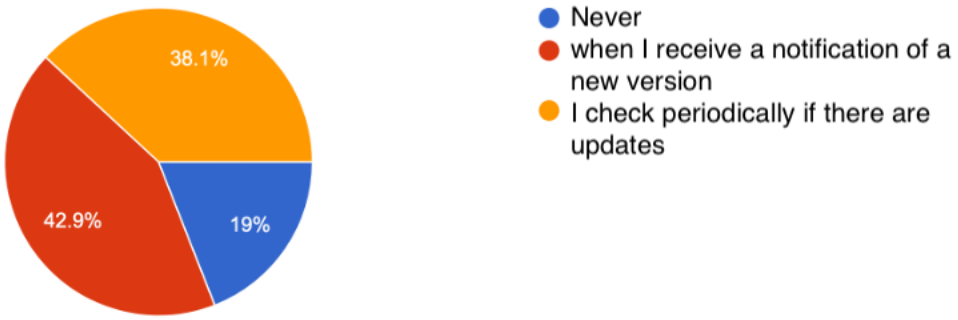


Figure 18 update frequency of anti-virus applications

Q 08 Updates on Cyber-security

Concerning this topic, 2 questions are formulated: the first one is about which means are used to keep up-to-date with the cyber-security issue, the second is about the university measures to minimize cyber threats.

> How do you keep yourself up-dated on cyber security related issues from professional and individual point of view?

The most part of respondents keeps up-to-date about cyber security related issues and mention a number of different means and tools they commonly use, including: technology channels on youtube, news, forums, web site and articles on the Internet. Few participants (25%) declare that they don't keep up-to-date.

> Are conditions created in your university to minimize cyber threats in the learning environment? and if so, do you know which ones?

Almost all the respondents answer “yes” and mention some measures taken by the university to reduce cyber-risks, such as, encryption of passwords, use of a wired network with local wireless connection and with static IP access, VPN, university wi-fi, specific training programme. A minority of the interviewees affirms that they do not know or are not sure.

Q 09 University measures against cyber-threads

A collection of 3 questions is useful to know the participants degree of awareness about university measures against cyber-threads.

> Do you know if your university conducts awareness campaigns about cyber security issues? What are they?

The majority of respondents answers “yes” and mentions some training organized by the university with a quiz-type activity and phishing email to induce users “in a trap”. The rest of the interviewees declare that they are not aware of awareness campaigns conducted by the university.

Are you informed about the security of your confidential information by your institution?

Only 11 participants reply to this question in a meaningful way (some of them just write a character to skip it). The collected answers are positive ("yes" or "approximately")

What are the security gaps or threats that you observe in the institution?

Most of the participants think they there are not security gaps or threads in the institution or declare that are not aware of any. Only few of them report potential security gaps, for instance: spam mail, use of external PCs with access, laziness passwords.

Q 10 Private data

Do you feel your private data is secure when you use the learning environment at your HEI? What is the reason behind your answer?

The general perception of the respondents is that their private data are protected. The reported reasons are different: credentials are required to access the system and any access is controlled; the university is a reliable and secure environment; the university is obliged to treat personal data in a confidential way.

Only few participants declare that they have no idea and that they do not share personal information.

Q 11 University cyber-security course

Is there any programme/short informative course which has been created to further educate the academic staff and students, in order to reduce their chance of falling victim to cyber-attacks in the learning environment in the HEI?

A large part of the respondents declares that there are not or they are not aware about courses organized by the university about cyber-security. Some students state that one of their courses covers topics connected to networking and security. A minority of respondents affirms that there are courses and events within the university to increase awareness about cyber-security.

We suppose they are collaborators (administrative and academic staff), since teh university has specific training programs with interactive material and videos for academic and administrative staff on this subject.

Q 12 Additional comments

Are there any other points that you would like to add regarding the topic?

Almost the totality of the respondents does not provide additional comments. One person states that often certain aspects are underestimated: “Maybe you have secure passwords but you enter them in plain sight ... Even phone unlocks”. Another person highlights the need

to help all citizens to protect themselves from cyber-attacks. “For me there is a serious problem of over-usage and inability to manage.”

Conclusions

This study, run between 2nd and 17th of October 2022, has involved 21 participants among students (15), academic (2) and administrative staff (4) from a Swiss university. The analysis of data collected by means of an online survey demonstrates that participants have a clear idea of what cyber-security is and a good level of understanding of cyber-threads. They know the password security requirements and they are quite careful in not sharing their passwords with others. However, in some cases, we notice a sort of laziness, for instance, in updating the passwords or not using a password already used before. The most part of respondents keeps updated about cyber-security related issues and mention a number of different tools and channels they commonly use, such as youtube, news, forums, specialized.

With respect to their reaction when they receive phishing letters, they usually recognise the deceit and delete the letter immediately.

They are quite familiar with online transactions - most of them make 2-5 transactions per month - and feel quite safe when making them.

They feel less safe when they share personal information. Indeed, a large part of them declare that they do not share personal information on social media. The most used platform is *WhatsApp*, followed by *YouTube* and *Instagram*. Almost the whole group of participants use social media from their personal device very frequently.

The use of anti-virus applications is quite common among the participants, who also use other security measures on their devices such as password protection.

About the measures taken by the university and the campaigns against cyber-threads, participants affirm that the university creates the conditions to minimize cyber threads and promote awareness campaigns on cyber-security. No major security gaps or threads are reported. The general perception of the respondents is that their private data are protected.

Few participants are aware of specific training programs about cyber-security. This is probably because the course is for collaborators.

Appendix 1: translated answers to the open questions

Q 03 About cyber-security

Q 03 a - How would you describe cyber security?

1. It is an important issue to deal with
2. Methods to eliminate privacy violations
3. The set of means by which a user can keep their personal data safe.
4. Fundamental component of network management, to allow anyone to use it without running into problems such as malware or scams.
5. All the measures to be taken to use IT means in a safe and conscious way so as not to run into privacy or fraud problems
6. In my opinion, IT security is to have your data on IT infrastructures safe (e.g. PCs, smartphones, ...)
7. Browse safely
8. I think cybersecurity is an excellent tool for protecting data from external attacks.
9. how their systems are up-to-date and protected. Also be aware that there may be threats.
10. The level of protection of your personal information on an electronic device.
11. cyber security is preventing others from seeing personal data that you don't want to share
12. (I'm not sure how to answer) Computer security?
13. the ability of a computer system to recognize and filter unwanted and harmful actions for the user and for the system itself
14. A way to defend against bad guys who try to steal money or information over the internet.
15. a method to protect personal data
16. Cyber attack protection
17. IT security are technologies that prevent data theft or attacks on large or small electronic devices, but it is also data and information security and protection from computer crimes.
18. That it is very important, but that I personally don't give you the right attention.
19. Very good
20. Antivirus, block fraud, emails with trojan horses, etc.
21. Protect your data, files, etc.

Q 03 b – Can you list at least 3 cyber threats?

1. Data theft. Viruses, malware, phishing, ...

2. Identity theft, stealing of credentials
3. viruses, malware, phishing.
4. generally malware, divided into sub-categories: trojans, spyware, viruses.
5. false emails, computer viruses, data fraud, password and account theft
6. viruses, malware, phishing
7. virus, malware,
8. Malware, Viruses and Hacking
9. phishing, malicious, trojan
10. Viruses, Hackers and scams.
11. viruses, spyware bots
12. virus, Hacker, malware
13. phishing keylogger spyware
14. Virus, Hacker attacks, Phishing
15. phishing, malware, trojans
16. virus, phising,
17. data theft, intrusion into electronic devices, computer crimes
18. Password theft, viruses that block computer operation, access to protected areas (e.g. SUPSI common areas)
19. Emails asking you to pay money, emails asking you to click on a link, USB sticks
20. viruses, trojan horses
21. Viruses, phishing, hacking

Q 04 About password

Q 04 a - What do you think should be considered when choosing a password?

1. Do not use names or numbers or words that can lead back to us. Use special characters
2. Do not link the password to your person, and do not use meaningful words
3. Long (> 8 char), not related to your person, using special characters.
4. the length, the use of special characters, the uppercase and lowercase alters, the writing of a nonsense word. ex. C1à @ f1Li
5. Length, predictability, presence of numbers, uppercase and lowercase letters, special characters
6. It must be long, with alphanumeric characters and symbols
7. use different characters, uppercase, lowercase and must be long
8. it must be composed of both numbers and characters
9. you should include special signs (such as -, _, *, etc) in capital letters and try not to put meaningful words
10. Add numbers, uppercase and special characters. Don't use the same password for multiple different accounts.
11. not meaningful, not linked to dates or data traceable on the net
12. Insert numbers, letters, uppercase and lowercase characters, special characters
13. you have to choose long passwords with numbers, letters and special characters, but above all they must be different
14. Do not enter the year of birth, discounted sequences such as 1234 etc ... It would be better to enter in addition to lowercase letters also special characters, uppercase letters, numbers and choose a long password.

15. use a password manager and choose a random long password mixed with letters, numbers and special characters
16. use uppercase, lowercase, numbers, special characters, avoid personal references (e.g. dates of birth)
17. enter uppercase letters, numbers and special characters
18. Change it regularly, do not choose "classic" pw (eg 123456789), change them and do not always put the same for different sites, use symbols-numbers-letters.
19. It must contain at least special characters, numbers and capital letters. It doesn't have to be the date of birth (for example)
20. difficulty
21. It must be long, contain different characters (numbers, symbols, uppercase and lowercase letters) and must not be linked to something personal (e.g. date of birth, name of partner / children, etc.)

Q 04 f - Is there a place where you write down your passwords? If so where?

1. on my device protected by the device unlock password and my account password
2. Google
3. No
4. google password
5. On paper in a safe place
6. Yes, in a notebook
7. yes, on the pc
8. brain
9. Yes, protected folder on the phone
10. In a private excel file
11. cell phone
12. Google
13. OneDrive Personal Vault
14. Some of the passwords are automatically saved by Google
15. bit warden
16. google and paper
17. no
18. I'm not saying it, it's a secret place, on paper.
19. on a leaflet and dedicated apps.
20. It depends on what types of passwords; you buy websites yes, on word, others (pc access, net-id etc.) no
21. No, I memorize them, so I don't use a different password every time but I reuse the usual 3/4 passwords

---

Q 06 Social media

Q 06 c - What kind of information do you share on social media?

1. none
2. information related to my hobbies and that I want to share, I do not share sensitive information about my person
3. None
4. As little as possible, necessary for login.
5. practically nothing, except for rare events.
6. Minimal, we remain vague.
7. Nothing on YouTube, while on WhatsApp the name and sometimes the images I put on the status.
8. photos, videos
9. name and date of birth
10. Nothing
11. photos, videos
12. None, I only use Whatsapp, the other social networks I used only in the past to view but not share
13. I don't use social media, but I exchange information on Whatsapp, mainly of a school or organizational nature.
14. almost none
15. few and never personal (never addresses, never places where I am)
16. a lot on whattsapp, less on Facebook
17. I only use whatsapp for messages and rarely sharing images
18. Nothing private and confidential
19. not personal
20. Virtually nothing, I only have Facebook and I publish very little (above all I share events or news, I haven't published photos for years)

Q 07 Antivirus

Q 07 a - Do you use antivirus application on your devices?

Yes – 66,7%

No – 33,3 %

Q 07 b - if yes, would you define which?

- Avast (4)
- Window Defender (3)
- Northon (2)
- Kaspersky
- McAfee
- Windows Security
- Vodafone protection malware
- Sophos
- Microsoft defender

Q 07 c - Do you have other security measures on your devices?

1. all my devices have a code to unlock them and in case of loss I can block them from other devices by initializing them. I regularly make backups.
2. Lenovo antivirus
3. Yes, I avoid giving permissions to applications if they are not necessary for the functioning of the same.
4. complete weekly scan, with correction of system files and control of software via virtual machine before installing them. Every year I format the device, as well as change the most important passwords.
5. The most used sites, where my credit card is saved, I associate them with both the phone and the email to log in. (3 login steps)
6. Virus scan, enabling security settings.
7. Yes, the password is required to access, I keep the device updated, I do not leave it unattended and I pay close attention to what I download or connect to the device scans
8. Antimalware and Antivirus
9. every now and then I do a complete check of the devices
10. password and antivirus
11. no
12. I use virtual machines and VPN (for computer), no security on android phone
13. Periodic scans
14. Antivirus scan
15. I check the devices connected to the main accounts and verify that they are my devices / I protect them with a password / I attach a number to call in case of loss / I keep GPS active for device tracking and I keep connected to control it remotely for data reset in case of loss (if lost I unlink main accounts from another device)
16. McAfee
17. I don't call back or answer unknown numbers and suspicious emails
18. antivirus, I avoid sites in which to watch streaming movies, I do not download movies, if a site does not have a lock in principle I avoid it.
19. I have removed Google maps tracking, I don't want to share information to improve apps.
20. antivirus
21. Nothing in particular

Q 08 Updates on Cyber-security

Q 08 a - How do you keep yourself up-dated on cyber security related issues from professional and individual point of view?

1. I follow technology channels on youtube
2. News and information
3. forums or websites of the operating system in use.
4. notifications or when it cost a sudden slowdown computer problem.
5. Through web news, TV programs
6. Honestly, I'm not very up to date on security issues.
7. I don't
8. I read information from the internet
9. Reading articles on the internet
10. Via online news.
11. internet
12. I do not update in any way, they are not things of my interest
13. I don't keep up to date
14. I don't follow this field very much.
15. youtube
16. –

Q 08 b - Are conditions created in your university to minimize cyber threats in the learning environment? and if so, do you know which ones?

1. I do not know
2. For example, encryption of passwords
3. yes, a good degree of security regarding the WLAN connection.
4. use of a wired network, with local wireless connection and with static IP access (whitelist).
5. I can't answer
6. I think yes
7. I think so
8. yes, telematics
9. I'm not sure
10. Yes, create a separate and isolated network from the rest of the networks
11. I don't know
12. No such notions have been introduced, what I know is self-taught
13. not just in the know
14. VPN
15. supsi wifi with filters
16. I hope so
17. yes, but I don't know exactly which ones

18. They offer trainings, I have participated in an interesting (practical) course and every now and then they send a trap email to see who falls into the trap
19. yes, through communications from the IT service
20. Ask the systems engineers
21. From time to time we receive communications or the like. Software like Teams is made available which I imagine is safe.

Q 09 University measurements against cyber-threads

Q 09 a - Does your HEI provide awareness campaigns about cyber security issues? What are they?

1. no
2. yes
3. I do not know
4. I know they exist, but I've never been a part of them.
5. Yes, during the lessons related to computer science and telematics.
6. I think yes
7. I am not aware of it
8. I do not know
9. No it does not lead (that I know of)
10. I am not aware of it
11. With the lessons of telematics, cryptography and security, the teacher explains various problems relating to security, which can make us reflect on the various IT risks.
12. I do not remember
13. -
14. Mini training by the IT service
15. yes, courses and information
16. yes, test mails often arrive to understand if you are falling for it or not.
17. yes, see mail systems engineers
18. Yes, we receive communications in this sense from time to time. I remember that once a quiz-type activity was created to be done on the collaborator portal

Q 09 b - Are you informed about the security of your confidential information by your institution?

1. yes
2. no
3. Yes
4. Somewhere it says they are being used confidentially
5. YES
6. yes, there are sheets to sign about it. When you enroll in university
7. Yes
8. approximately

9. -
10. yes, but in my opinion the user should be made more aware
11. A bit'
12. Enough

Q 09 c - What are the security gaps or threats that you observe in the institution?

1. -
2. I do not know
3. none
4. I don't observe any
5. none, so far.
6. Currently none
7. I observed that during the course of the day in the classroom many passwords are entered in different accounts (school platforms, emails, social networks, etc.) with many people around without paying too much attention to any indiscretions of classmates etc ... Even the fact of relying on laziness password managers in my opinion is a possible threat ...
8. Honestly, I've never thought about it
9. None
10. I have no idea, I don't even use SUPSI wifi, I use the 4G on the phone
11. I don't observe any
12. I don't see any
13. users connected to the same network potentially (?)
14. I do not know
15. Use of external PCs with access, no control of external PCs, too much dependence on shared networks
16. I don't see any personally
17. spam mail
18. They don't come to mind right now

Q 10 Private data

Q 10 a - Do you feel your private data is secure when you use the learning environment at your HEI? What is the reason behind your answer?

1. -
2. Yes
3. yes
4. each access is controlled, and no external person can access, except in the event of a physical attack on the system via LAN. (I believe)
5. Yes, I think the environment is simply trustworthy.
6. I think so, because I believe it is important for a university to have reliable and secure systems.
7. I hope so
8. yes, because there are researchers dedicated to protecting sensitive data
9. Yes, I think my data is protected as SUPSI should be obliged to treat it correctly
10. it is already difficult to access the WI-FI even if you have the correct credentials
11. I have no idea, and frankly it is unimportant, no personal information is shared about the learning environment.
12. I think so, the connection to the university networks requires you to log in with your email and password
13. Yes, because studying in a department of innovative technologies I think that the means to guarantee cyber security are there.
14. Approximately, being semi-public wifi
15. yes, but in my opinion the user should be made more aware
16. I do not know. I think so, but I trust and am quite unaware of the real dangers. I have no social media, I don't share my life, I avoid spending too much extra-work time in front of screens.
17. Yes, because to access it you must have a suspi account with the relative accesses.
18. no idea
19. I guess so, even when I work from home I have to connect via vpn otherwise I can't access files on the work server. I don't have the skills to judge if this is enough but I guess so

---

Q 11 University cyber-security course

Q 11 a - Is there any programme/short informative course which has been created to further educate the academic staff and students, in order to reduce their chance of falling victim to cyber-attacks in the learning environment in the HEI

1. no
2. -
3. I do not know
4. I do not know
5. As a student with the Telematics lesson we deal with issues related to computer science with hints of techniques to protect or make our connections less vulnerable.
6. I think yes
7. Telematics
8. not that I know
9. I do not know
10. No, there is none of this (that I know or have told us)
11. I am not aware of it

12. I don't know about it, but through the telematics, cryptography and security lessons, we are learning how networking works, so we can automatically understand the various risks of the network, in this way we are made aware of what not to do on the internet.
13. I don't know
14. Yes
15. Yup
16. I am not aware of a short program or course.
17. yes
18. As I said before I remember that a kind of quiz was done, other things do not come to mind at the moment

---

Q 12 Additional comments

Q 12 a - Are there any other points that you would like to add regarding the topic?

1. no
2. -
3. Laziness does not help and often certain aspects are underestimated. Maybe you have secure passwords but you enter them in plain sight ... Even phone unlocks.
4. Nothing, because unfortunately computer science is not my field so I have no interest in it.
5. It is necessary to help all citizens to manage information technology and to protect themselves. For me there is a serious problem of overuse and inability to manage. The risks are high, mainly due to the aggressiveness of the producers.