NEW METHODS AND FORMS OF CYBERNETIC SECURITY FOR SENIORS

PROJECT

New methods and forms of cybernetic security for seniors

Methodological suggestion for teaching activities

2019

Programme: ERASMUS + Key Action:

Cooperation for innovation and exchange of good practices

Strategic Partnership Field:

Strategic Partnership for adult education

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held respons ible for any use which may be made of the information contained therein.

Erasmus+

NEW METHODS AND FORMS OF CYBERNETIC SECURITY FOR SENIORS

Authors:

- CPM - Centrum prevencie mládeže, Slovakia
- Foundation Pro Scientia Publica, Poland
- Alvit, Czech Republic
- Inercia Digital, Spain
- Sinergia Società Cooperativa Sociale, Italia

Cover Design:

Reklama Radolský s.r.o., Slovakia

Language adaptation:

GLOBE LANGUAGE SCHOOL s.r.o. .Slovakia

Project number:

2018-1-SK01-KA204-046377

Project title:

New methods and forms of cybernetic security for seniors

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held respons ible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

ISBN 978-80-570-1421-8

TABLE OF CONTENT

INTRODUCTION.....3

Project intention 3

Importance of the project.....3

Aim of this methodological material.....3

Target group.....4

Information about the participating organizations.....4

OUR RESEARCH OUTCOMES.....9

HOW OUR PROJECT METHODOLOGY WORKS.....16

NEW METHODS AND FORMS.....17

1. Secure pasword.....17
2. Identity thefts.....21
3. Security financial management over the internet 25
4. Configuration of their Facebook account 32
5. Fake websites.....38
6. Security software: Anti-virus and Anti-Malware.....42
7. Phishing.....49
8. Malware.....58
9. Cyber Communities.....66
10. General Data Protection Regulation 75
11. Instagram.....81
12. Games.....83
13. Ineternet frauds.....86
14. Secure Gmail.....88
15. Ways how to manipulate pictures.....91
16. Fake News.....97

CONCLUSION.....110

ATTACHMENT.....111

INTRODUCTION

Project intent

The intention of the "Cybersecurity for seniors" project was to prepare such an educational programme for seniors incorporating the subject of basic cybersecurity. We have tested new learning methods aimed at enhancing the digital safety of seniors in each partner country, looking together for the most appropriate topics based on international research. Also part of this publication is our research in three countries where we compared the safety skills of seniors and young people. In total, the publication contains 16 methods that are suitable for inclusion in different courses or individual lessons of lecturers, trainers, or teachers.

Importance of the project

People over the age of 55 often use the Internet for shopping, banking or communicating with their loved ones. However, they often forget to protect themselves and their most valuable things from the tricks of cyber criminals. Despite the fact that this age group considers it important to have security programs installed on their computers, they are lagging behind in the protection of mobile devices or safe behaviour on the Internet. For example, they have shown less attention to the privacy settings on social networks or in their browsers compared to other age groups. That is why it is important for them to pay attention to preventive measures. As Internet usage increases, so does their vulnerability, and they can easily become the victims of fraud or other cyber threat. The lack of awareness of safe behaviour on the Internet together with not knowing how to protect against cyber threats makes this group the least prepared for the dangers of the online world.

Senior citizens rank among the group, which is particularly threatened by social marginalization, or even exclusion. After their retirement from work, there comes the natural reduction of social contacts due to limited (or even discontinued) relationships with former work colleagues, as well as the loosening of family ties. After the death of a partner the feeling of insecurity occurs frequently, accompanied by loneliness and helplessness, especially when tackling new technologies. With the progressing retirement age, there comes the general slowing down of the pace of life as well as the deterioration of cognitive abilities. Hand in hand with physical ageing, the overcoming of barriers and the undertaking of new challenges is hindered. On the other hand, these difficulties naturally accompany the development of civilization and in the increased use of ICT (Information and Communication Technologies) in daily life of an average person, not only seniors.

The aim of this methodological material is:

- to innovate and develop new teaching methods and forms in senior education that focus on cyber security on the Internet as well as on social networks and the reflect the need to prevent the ever-increasing cyber-attacks on seniors.
- to improve and develop competences in media literacy of lecturers in individual partner organizations involved in senior education.
- to support the socio-educational and personal development of seniors as well as the promotion of lifelong learning.

The target group is:

lecturers, trainers, teachers providing adult education with a focus on seniors.

Information about participating organizations:

Five NGOs from Slovakia, the Czech Republic, Italy, Spain and Poland worked on the elaboration of this material.

Sinergia Società Cooperativa Sociale

Sinergia Società Cooperativa Sociale was founded in 2009 with the aim of pursuing the general interest of the community in promoting human and social integration of citizens, through the management of social, health and educational services. The mission of the cooperative takes the form of completed and ongoing projects. As part of its intervention areas, Sinergia realises projects for training, learning and mobility, workshops, information campaigns and promotion of the cooperative principles. The activities carried out in our area are:

- Monitoring and informing local stakeholders about the opportunities offered by the European Union;
- Promoting and supporting the participation of local actors in European, national and local activities, presenting projects in line with EU methodology;
- Spreading European culture in the local context and raising awareness about the concept of European citizenship;
- Starting a constant and constructive dialogue with the EU institutions;
- Valuing initiatives, ideas and local projects through Communitarian opportunities;
- Facilitating the participation of local actors in the political and Communitarian institutional process;
- Promoting the mobility of young people as an opportunity to contribute to the creation of a European identity through different experiences;
- Promote the personal and social development of young people through European opportunities
- Fostering international networks, European partnerships and exchange of good practices;
- Improving the competitiveness of local enterprises and supporting innovation;
- Providing training and guidance on programmes and opportunities for young people promoted by the European Union and the Council of Europe in the fields of education, training, mobility and citizenship;
- Providing training on facilitated finance opportunities for recruitment and self-employment of disadvantaged people.

In addition, Sinergia is a member of the Consortium Social Lab, an organisation coordinating 8 social cooperatives committed to the employment of youth, women, immigrants, disabled, ex-drug addicts and ex-prisoners.

- www.sinergiasociale.it
- info@sinergiasociale.it

CPM-Centrum prevencie mládeže - Youth Prevention Centre

The main goal of our preventive centre consists in preventing the risky behaviour of children and youth, women in danger, adults and the elderly, especially in the area of information literacy, Internet hazards, hate speech, internet addiction, drug addiction, prevention of various forms of violence, racism, bullying, xenophobia, protection of human rights and freedoms, and the like. Throughout the year, we organize educational, training and educational activities that provide a meaningful protection from the risk of various addictions. The target group of our activities is the youth in action, young people general and young people coming from socially disadvantaged backgrounds, young people at risk, women at risk, both adults and the elderly.

The CPM prepares various educational activities aimed at the target groups to provide meaningful compensation against risk behaviours. Our activities are also focused on international exchanges, communication with international partners, searching for new leisure activities in the field of youth prevention.

CPM Čadca has been active in the field of youth work since 2008, when we founded the youth club against crime in general. In this club, we focus on youth work. Our main focus consist in the following: informal education of children and young people coming from disadvantaged communities or environment; education of children and youth in the area of risky behaviour prevention; education of women in danger, adults and seniors; the development of volunteering activities; the promotion of active citizenship of children and youth; the participation of children and youth in local projects with the aim of mobilizing young people in public life; the preparation of preventive projects; information and education campaigns aimed at preventing the negative phenomena of using the Internet of children and youth in our city, which must engage in children's activities in communities to develop their creative potential.

- cpmcadca-sk.webnode.sk
- cpmcadca@gmail.com

Alvit

The company was founded in November 1994. Today, it is presented by a group of young, enthusiastic project managers and lectors, former students and teachers from the local universities in the Moravian-Silesian region. The basic impulse for their work is the location and the historical background of the region, with over 1,3 million residents. This area has been for a long time oriented mainly in the mining and heavy industry with all the effects on its on its population. ALVIT offers and provides opportunities to improve these people's lives through training, transfer of innovation and lifelong learning education. ALVIT is a company committed to quality, innovation and European cooperation. We firmly believe that European cooperation including mobility, exchanges and mutual learning has strong benefits to individuals and European Community, contributing to building of a common European identity. That is why we are concentrating our efforts to serve in practice European cooperation: we participate in European projects; we cooperate with colleagues to develop training courses and materials with a real European dimension; we organize transnational training courses and we love to cooperate with real professionals.

- www.alvit.cz
- info@alvit.cz

Inercia Digital

Inercia Digital is a young Andalusian social enterprise founded in 2012 focused on training, innovation and traineeship in digital skills in a European level.

Our mission is to contribute with employment by promoting training and innovation in digital competences all over Europe, developing the digital skills needed in education for ICT professionals, labour force and all citizens.

Inercia Digital has experience in international and European projects, both in and out the Erasmus+ programme with several projects where we participate. Based on its expertise area, during the last years we have created and lead websites and e-learning platforms for education institutions/providers (such as schools, adult education centres, VET, etc.), in order to integrate ICT in their daily activities while developing extensive trainings on digital competences, web tools, e-learning, virtual opportunities and collaborative learning.

Inercia Digital has received the certificate by AENOR as Young Innovative Company and we are implementing the ISO 29990:2010 – Learning services for non-formal education and training – to offer better learning services.

- www.inerciadigital.com
- contacta@inerciadigital.com

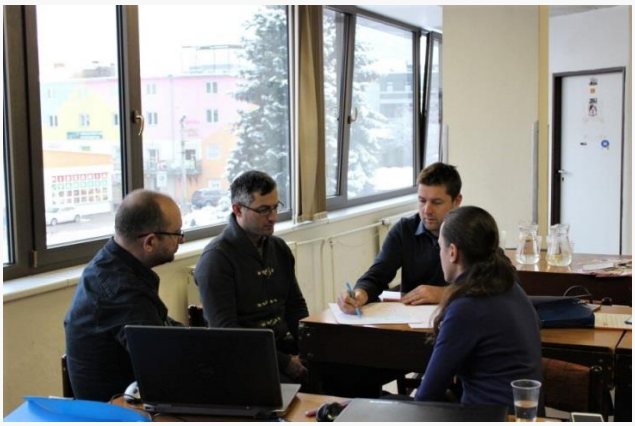
Foundation Pro Scientia Publica

Foundation Pro Scientia Publica (Poland) has been operating since 2010 in the field of adult education, promoting several initiatives with a focus on elderly citizens and their social inclusion.

Our team is experienced in teaching adult and elderly people and we are providing workshops and seminars regarding, among others, the techniques and methods of teaching senior students, autobiography methods in elderly people learning, digital storytelling, development of key competencies of seniors.

Our beneficiaries are people aged 65+ and trainers from other organizations in the region of Lower Silesia. The Foundation also stimulates and supports the activity of young scientific talents, allowing them a good start in the world of science and fostering their professional activities. Also makes its own scientific and educational projects that build bridges of understanding between generations involved in the creation and dissemination of science. The symbol of this agreement is shown as a bridge which is inscribed in the logo of the Foundation.

- www.proscientiapublica.pl
- proscientiapublica@gmail.com

Our team of experts

RESULTS OF OUR RESEARCH

The project includes a research conducted in the form of a questionnaire in order to check how seniors take care of their own cybersecurity and in order to compare their behaviour with the behaviour of other generations and nations. The research involved organizations from Poland, Slovakia and Italy, and included a total of 478 respondents (118 from Poland, 114 from Slovakia and 246 from Italy). 216 of the total number were 60 years-old or over. The questionaire is in attachment No. 1.

The following issues were diagnosed:

1. How do seniors react to security threats?
2. How do seniors take care of passwords and logins?
3. How far are seniors prepared to avoid deception and resist phishing?
4. How do seniors take care of their general security on the Internet?
5. What kinds of attacks and other problems are experienced by seniors when using computers or the Internet?

The data obtained was compared to that obtained from younger generations respondents.

1. How do seniors react to security threats?

In this case, the two factors assessed were mainly designed to find out whether seniors attempt to solve any problems themselves (perhaps with help from the family) or whether they seek specialist help.

Question	Seniors (average answer)	Non-seniors (average answer)
1. When I come across a dangerous situation on the Internet: I immediately ask for help from specialists	2,72	2,79
2.When I come across a dangerous situation on the Internet: I ask for help from family or friends	3,2	3,39
3.When I come across a dangerous situation on the Internet: I try to resolve it myself	3,48	2,73
4.When I come across a dangerous situation on the Internet: I am cautious and try not to fall into a trap	4,2	3,5

5.When I come across a dangerous situation on the Internet: **I look for help on specialist internet forums and in the Internet community**	2,9	2,3

Scale: 1. Never 2. Very rarely 3. Rarely 4. Often 5. Very often

Average analysis shows that seniors assess their own caution quite highly, stating that they generally do not let themselves be drawn into suspicious interactions, and that when problems do arise, they ask friends or family to help solve them. Younger generations are more confident and try to solve any problems or emergencies themselves. In my opinion this is simply a consequence of the fact that younger generations use ICT every day and are familiar with it. In comparison, seniors more often declare themselves to be novices or beginners in the use of the Internet. It could be said that for the younger generation the computer is a daily tool and channel for expressing themselves, whereas for seniors it is still an untamed technology which they have to learn using.

2 How do seniors take care of passwords and logins?

Compared to younger generations, seniors take much less care when it comes to using suitable programs. However, the situation is the worst when it comes to the use of original programs and their regular scanning with antivirus tools. This could be caused by lower income after retirement and by limited financial resources. Neglecting of the regular scanning of the computer with antivirus programs is caused by the lack of awareness of such necessity or by the unfamiliarity with the existence of free programs. In both cases, raising awareness in this area through suitable training is essential.

Question	**Seniors (average answer)**	**Non-seniors (average answer)**
In order to protect myself, I only use authenticated programs	3,83	4,13
In order to protect myself, I use anti-virus programs	4,2	4,31
In order to protect myself, I scan my computer regularly with anti-virus programs	3,6	3,93

Scale: 1. Never 2. very rarely 3. Rarely 4. Often 5. very often

When it comes to password security, in many areas, seniors are unaware of the dangers connected with inappropriate behaviour. In almost all seven types of behaviour researched, they did much worse than younger generations. Seniors:

- do not regularly change their account passwords

- repeatedly use their own passwords on other peoples' computers

- use the same password for multiple accounts

- rarely change allotted passwords

- reveal their passwords and logins to others

Question	Seniors (average answer)	Non-seniors (average answer)
I regularly change my access passwords	2,6	3,2
I avoid using simple passwords by making sure they consist of a combination of at least 12 letters, numbers and special characters	3,3	3,7
I don't log in to other computers	2,8	3,5
I don't use my passwords on other computers	2,8	3,75
I don't use the same password for all my Internet accounts	2,7	3,5
I always change passwords allocated to me by websites	3,1	3,9
I never share my codes or passwords with	3,1	4,0

Scale: 1. Never 2. Very rarely 3. Rarely 4. Often 5. very often

From the above analysis, it is obvious that the use and protection of passwords should be crucial when educating seniors.

3 How far are seniors prepared to avoid deception and resist phishing?

The outcomes of the questionnaire analysis leave no doubt that seniors are relatively easy victims for fraudsters attempting to obtain data via e-mail. This is evidenced by the fact that most of them are not resistant to such dangerous behaviours as:

- opening e-mail from unknown persons

- opening e-mail attachments from unknown persons

- logging in to links sent via e-mail

- replying to e-mails from an unknown source and making contacts by Internet

Question	Seniors (average answer)	Non-seniors (average answer)
I never open messages from unknown people	2,86	3,7
I never open mail attachments from unknown people	2,9	3,85
I never click on links sent to me by email	2,8	3,66
I never react to advertising nor spam sent to me by unknown people	2,8	3,67

Scale: 1. I Strongly disagree 2. I disagree 3. I don't agree nor disagree 4. I agree 5. I Strongly agree

Such behaviour is decidedly different from the behaviour of younger generations who generally restrict such activities.

4 How do seniors take care of their general security on the Internet?

In the case of general security on the Internet, no significant difference between the generations was found. The following behaviours were revealed:

- analysis of shopping terms and conditions before making a final decision

- logging in only on the trusted and certified websites

- regularly updates of programs

- avoidance of unverified websites

- avoidance of unverified smartphone apps

Question	Seniors (average answer)	Non-seniors (average answer)
I check the website's terms and conditions before I decide to purchase	3,96	3,82
I only log into https: websites (with a lock or green belt)	3,47	3,82
I regularly update the programs I use	3,68	3,9
I use two-tier verification for emails (password + SMS code)	3,04	3,5
I don't want to be open to danger, so I use the Internet as little as possible	2,64	2,0
I only use trusted websites	3,9	3,7
I avoid installing unverified apps on my smart phone	3,8	4,0

Scale: 1. Never 2. Very rarely 3. Rarely 4. Often 5. very often

At the same time, respondents declared that they willingly used the internet which, in the case of seniors (in the light of the behaviours described above) may be dangerous itself.

5 What kinds of attacks and other problems are experienced by seniors when using computers or the Internet?

Question: Please indicate (according to the scale) which of the following problems you have personal experience of:	Seniors (average answer)	Non-seniors (average answer)
Defective program which doesn't work	2,3	2,8
Defective Internet browser which doesn't work	2,2	2,5
Computer speed slowing down	3,0	3,4
Data loss	2,1	2,1
Attempt to obtain passwords by a false bank website	1,7	2,0
Attempt to obtain money (requesting a transfer to" people in a difficult situation")	1,8	2,1

Regular redirection by the browser to unwanted and irrelevant websites	1,9	2,7
Theft of money from bank account	1,1	1,2
Theft of money from bank cards or credit cards	1,1	1,2
Computer blocked (hard disk encrypted) and ransom demand	1,1	1,2
Internet bank account broken into	1,0	1,2
Password theft	1,0	1,3
Blackmail attempt (threat to publish compromising material)	1,4	1,4
Identity theft (e.g. on social media)	1,1	1,3
Attempts to contact me by unknown people in my own country	2,3	2,5
Attempts to contact me by unknown people in other countries	2,1	2,5
Immoral propositions via email	1,5	1,7
Harassment via email or text messages	1,4	1,6
Regular receipt of unwanted emails (spam)	2,7	3,2
Automatic forwarding of emails in my name without my knowledge	1,5	1,6
Hate speech	1,3	1,7
Appearance of pornographic content	1,6	2,0
Sharing false information in the conviction that it is true	1,4	1,8

Scale: 1. Never 2. Very rarely 3. Rarely 4. Often 5. very often

Generally, when it comes to the frequency cyber-attacks, no significant difference between the generations was observed. The only noticeable anomaly was the tendency that, in comparison to seniors, younger generations were a little more willing to admit they had been a victim of cyber-attacks. This could be explained by the fact that seniors have less digital experience and (one may suppose) reduced Internet activity, which naturally generates fewer possibilities for attacks by potential cyber criminals. In the questionnaire, seniors clearly described themselves as less experienced, whereas the younger generations declared that they were more experienced, or even “experts”.

Conclusions

Seniors are a group who definitely need digital education. The typical behaviour of seniors using the Internet shows that one of the fundamental subjects which should be taught in computer courses are

the issues related to creating, using and protecting passwords and log-ins. Particular care should also be taken in case of the issues related to forming relationships and friendships via the Internet. Security issues to combat fraud, phishing and identity theft should also make a part of educational content. Seniors have less experience with using new technologies, so they can become the victims of fraudsters more easily. Education in the form of organised and condensed experience can help seniors to gain more confidence, so that they begin to treat the virtual world as a natural environment, just as younger generations do.

HOW OUR PROJECT METODOLOGY WORKS

PROBLEM AND GOAL

What sort of a problem does the activity solve?
What do we reach, what is the aim?

TIME ALLOWANCE

Provides the time allowance for the realisation of the whole activity.
Demanding time for the preparation of the activity shall be stated.

AID

Aid, technics, tools and subjects needed for the activity.
Further equipment needed shall be stated (internet, space, room adjustments etc.).

NUMBER OF PARTICIPANTS

Recommended number, age, further specification of members. Requirements for group divisions, restrictions of members.

ACTIVITY DESCRIPTION

Brief activity description, methodology.
Methodology can be described from the position of the lecturer as well as members of the group.

EXPERIENCE AND PRACTICE

Practical remarks from implementation in practice.
Possible difficulties, variability, adaptation towards environment, age, etc.

PHOTODOCUMENTATION

Activities captured in the Pictures.

NEW METHODS AND FORMS

Youth Prevention Centre

SLOVAK PART

ACTIVITIES

1. **Secure password**
2. **Identity thefts**
3. **Security financial management over the internet**

Activity 1

SECURE PASWORD

PROBLEM AND GOAL

Passwords play an irreplaceable role in the computer security. Unfortunately, many seniors choose either easy passwords or passwords which are challenging and difficult to remember. Computer passwords are met at every corner of the electronic world. This starts with the passwords for logging in to your computer and continues via email, Wi-Fi, e-commerce, various forums, or Facebook. Using one password to sign in to all the services you use is not safe. If someone gets it, they can "steal your identity" at the very moment - talk to your colleagues or friends, browse e-mails, download personal data, shop in e-shops. And all on your behalf. Passwords are a common method of authentication for online accounts, but it is not always easy to invent a password that is safe and easy to remember. On the contrary, it is getting harder because people have more and more online accounts. If you choose a simple password that is easier to remember, the risk of breaking it is higher. On the contrary, if you choose a more complex password, you are more likely to forget it, so you will probably choose to use it on multiple accounts.

So how to create a password which is secure and easy-to-remember?

Objectives of learning activities

The aim of the learning activities consists in remembering the principles of computer security - especially the principles of secure passwords creation, recognition and handling of viruses, etc.

TIME ALLOWANCE

45 minutes in total

- 15 minutes - interactive work in groups

- 30 minutes of discussion and clarification of safety rules

AID

Writing tools

NUMBER OF PARTICIPANTS

Divide seniors into groups, min. for 4 people.

ACTIVITY DESCRIPTION

Activity Start - Foreword

There are several security standards to keep in mind when creating a password

1 The ideal password should have at least 8 characters.

2 When creating a password, use numbers, uppercase and lowercase letters, and special characters.

3 Never use a password that can be found in a dictionary! Also, do not use first names or surnames.

4 Do not use the same password to access various online services (email, social networks).

5 When you are finished working on the Internet, be sure to sign out of the account you are currently using. If you close the browser it doesn´t mean that your account will be automatically signed out.

6 Keep the password secret, do not disclose it to anyone, or your best friend.

7 Ensure important accounts with two-stage authentication that combines the password and code on your mobile phone.

Remark

According to the latest security analysis and mathematical calculations, a long password with fewer types of characters is safer (e.g. only uppercase and lowercase alphabets) than a short password with multiple character variations (letters, numbers, special symbols). However, the difference is essentially insignificant; both ways of creating a password are highly secure.

Task for seniors

Try to create the most secure but memorable password for accessing your account e.g. to the internet banking. - 15 minutes - interactive creation in groups

Questions after presenting passwords to seniors - 30 minutes of discussion and clarification of safety rules

EXPERIENCE AND PRACTICE

1 How did you create your password?

Solution: E.g. combination of a name and a number etc.

2 Assess whether your password meets security standards.

Solution: Let's compare whether the senior password he invented corresponds to points 1-3 of the above standards.

3 Estimate how long it would take an average performance computer to break the 6-character password by default attack (i.e. a combination of characters) that:

A. If it is composed of only numbers, it will take 3 hours to break your password

B. If lowercase letters of the alphabet are used, it will take 8 months to break your password

C. If digits uppercase and lowercase letters are used, it will take 18 years to break your password

If digits, uppercase and lowercase letters, and special characters are used It will take 120 years to break your password

In addition, for most online services, when you re-enter your password, the computer automatically disconnects us and blocks access for several hours. The account penetration time is multiplied.

4 Try to estimate the ranking of the three most common passwords

Solution: 12345, 123456, password, password123, 123password321, aaaaa and qwertz on other rungs

5 Design a way to create a memorable yet secure password.

Solution:

Step 1: Create a core password (part of a password that does not change)

E.g. we choose a familiar sentence from the favourite song and put the letters between the opening words, which will alternate between big and small, letters will be put among the digits.

For example: Anicka soul where were you (known Slovak folk song)

The core of the password will be**: A1S2W3W4Y5**

Since we need more passwords in the online world, it's only good to change the ending, for example:

Bank password - A1S2W3Y4W5Ba

Facebook password: A1S2W3Y4W5Fb

Mail Password: A1S2W3Y4W5Ml

At first glance, such a password does not make any sense, but since it is personal for you and you know the way you used it to generate it, you will easily remember it.

If you are a forgetful person and you are afraid that you will forget your password, you can use one of the encrypted password saving applications, or create passwords just for certain rules, and note them somewhere on paper which you can save at home. But don't write everything on the paper, keep the main sentence in your memory. Of course, you can also use other "bugs", for example, to draw your main sentence through pictures, place it in your favourite book, and so on.

Helpers for creating passwords

If you really need to use more sophisticated passwords that are very difficult to remember, use a password management program. For example, KeePass Password Safe is one of many password managers that keeps your passwords in one place. This software is free and can be installed on your

computer with any operating system (Windows, Linux, Mac OS X). For this password manager, however, be sure to think of a sufficiently complicated password.

PHOTODOCUMENTATION

Activity 2

THEFT OF IDENTITY

PROBLEM AND GOAL

Identity theft involves the theft of personal information such as passwords, identity card numbers, credit card numbers or social security numbers, and their misuse for fraud on behalf of the victim. The sensitive data obtained is misused for various illegal purposes, including loan applications, online purchases or access to the victim's medical and financial data. Identity theft is closely linked to phishing and other social engineering techniques that are often used to trick sensitive data from a victim. Public profiles on social networks or other popular online services can also serve as a valuable source of information about victims. Once thieves have access to the necessary information, they can use it to order goods, take control of the victim's online accounts, or take some legal action on their behalf. In the short term, a victim of identity theft may suffer a financial loss caused by unauthorized withdrawals and purchases made on his/her behalf. However, in the medium term, victims of identity theft may be held accountable for the offender's actions and investigated by law enforcement

authorities. They may also face various consequences, such as legal fees, worse credit standing (creditworthiness), as well as reputational damage.

According to the 2017 identity fraud study, identity theft caused the losses of $ 16 billion in 2016 to 15.4 million consumers in the United States only. In the same year, the British fraud prevention organization Cifas documented almost 173,000 identity fraud cases in the United Kingdom, the highest number since their records began 13 years ago.

TIME ALLOWANCE

45 minutes in total

- 10 minutes - introduction + story reading

- 10 minutes - interactive work in groups

- 25 minutes of discussion and clarification of safety rules + video

AID

Writing tools

NUMBER OF PARTICIPANTS

Divide seniors into groups, min. for 4 people.

ACTIVITY DESCRIPTION

At the very beginning, seniors are read a short story:

Mrs. Alena reported the theft of her Facebook profile to the Police. Using the profile, the offender offered sex to various men on her behalf, which unfortunately was badly explained at home. Investigations revealed that a virtual identity theft was caused by a sixth-grade pupil John who had had a conflict with Mrs. Alena in her residence.

How did he do it? Jan was no hacker. He knew Mrs. Alena's email, so he tried to log in. After several unsuccessful attempts, he took advantage of the possibility of recovering the forgotten password in the form of a tricky control question, which Mrs. Alena set up years ago. The question was: Your favourite movie? Jan cleverly opened the Facebook profile of Mrs. Alena, where 3 films were shown in the "Like" section. One of them was the correct answer to the control question, so Jan took control of Mrs. Alena's mailbox. Then he used the option to restart the password in case he was forgotten by the

Facebook social network, and after sending this link to a verified mailbox (which he already had under his authority) gained power over Mrs. Alena's user account on the Facebook social network. Then, on behalf of Mrs. Alena, he was sending offers to various men, which Mrs. Alena had difficulty explaining.

Task for seniors

- **describe the characteristics of the perfectly negligent person, whose identity can easily be stolen**
- **10 minutes - interactive creation in groups**

EXPERIENCE AND PRACTICE

Questions after activity- 30 minutes of discussion and clarification of safety rules

- How much information do I share on the internet?
- Who can have access to my personal data?
- How secure are my passwords?
- Do I use a proper firewall and virus protection?
- Do I use secure credit payments?
- Am I careful with my personal chat?
- How often do I check my financial accounts?
- Do I use trusted sites?
- What ID cards do I carry in my wallet?
- Do I shred old documents?
- What other precautions can I take?
- Finally, we recommend that seniors to watch a video of 7.45 minutes - ***Secret ways of a hacker to steal your identity*** to consolidate knowledge.

https://www.youtube.com/watch?v=9SVwPZ5scEU&fbclid=IwAR1hGBN7ZADdJKCcxRyiSGcPfsmPCd_hQ7xBuugu_gU8EqcPbO4yhMe67QU

PHOTODOCUMENTATION

Activity 3

SECURE FINANCIAL MANAGEMENT VIA THE INTERNET

PROBLEM AND GOAL

We are used to guarding our wallets carefully. However, not everyone is aware of the fact, that the same caution is needed when it comes to the bank account and a credit card. They are a frequent target of Internet fraudsters.

Thieves are very creative in inventing ways of improving themselves. What are their most common methods - and how to detect them?

TIME ALLOWANCE

- 45 minutes in total
- 15 minutes - introduction + story reading
- 15 minutes - interactive work with test in groups
- 15 minutes of discussion and clarification of safety rules

AID

PC or mobile, WIFI, Internet connection

NUMBER OF PARTICIPANTS

Divide seniors into groups, min. for 4 people.

ACTIVITY DESCRIPTION

At the beginning, we introduce the most common online fraud.

1. A buddy needs to send a change quickly

Typically, it happens this way: you receive a message from your friend via email or a social network such as Facebook. It is written there that he urgently needs to borrow money and there is a question whether you would be so kind and help him. It is not a big sum, just a few euros usually. But then a trick appears. There comes a different bank on the scene. The money needs to be transferred immediately, but the transfer between different banks takes some time. However, your friend cannot wait and will recommend a website where the payment can be made immediately. He assures you that you have nothing to worry about as he himself has done it several times. In time pressure and feeling

that you must help a friend, fill in your credit card information or internet banking login details. It ends sadly - your account does not deduct the amount entered but all the money.

What really happened?

It was not your friend who asked you for money, but a fraudster who accessed your friend´s login details. He took over his identity on the Internet, gave you a false sense of trust, and you gave him access to your card or account by entering your information in a false payment gateway.

How can you discover that someone is trying to deceive you?

Never enter your login information on the page other than your bank's page. Pay by card on the Internet only through well-known and reputable payment gateways. Such gateways are managed by well-known banks or trusted companies that you know and that accept payments via the Internet, such as PayPal. If a friend asks you to borrow money via e-mail or Facebook, be sure to confirm it by phone. The chances of someone stealing his access data and his phone are very small. For example, you can use VIAMO for an instant interbank transfer.

2. Winning a lottery or yielding a forgotten brilliant investment

This scam also begins with an email. It says that you have won the lottery or that they want to pay you a huge pack of money acquired from an investment you do not remember. But who would ask about such details when you have such a chance to gain a huge amount of money?

For the transfer to take place, they need to verify your identity, which usually requires copies of personal documents. They then request additional information from you, including the account number to which you want to be sent the money. On the pretext of verifying that you are the account holder, they can even ask for your online banking login and password. They may also want you to pay the fees associated with the transfer of winnings or investments. You will be willing to provide them with your credit card details etc.

The bad news is that you have just encountered a conman. It is unrealistic to win a lottery that you did not participate in. The same is true of an investment from remote past that you do not remember. The reality is that the fraudster wanted to infatuate you with the vision of big money in order to gain access to your credit card or account.

3. Your bank asks you to increase security or otherwise change settings

A lot of e-mails are sent to your mailbox - statements, offers ...you do not even read them. Suddenly you get a warning from your bank that because of the increasing number of cases of fraud, you should get more security and you are requested to change your online banking settings. You click on it, the page looks as usual - graphics, texts and offer, all fits well. There is no reason not to log in and do what is needed. Your login is usually unsuccessful, but a bank employee will call you in a moment that you

need to insert the SMS code that has just arrived on your phone to increase security. Everything seems to be all right, but the next day your account is empty.

What really happened?

The email that looked like the original bank mail was sent by a conman. The link in the email was not directed to your bank, but to a fake website that faithfully mimics the original. And you thus passed your login to a thief. He logged in to your real account at the bottom, entered a payment order, and sent a confirmation SMS code you during the pretended phone call from the bank.

How to detect fraud?

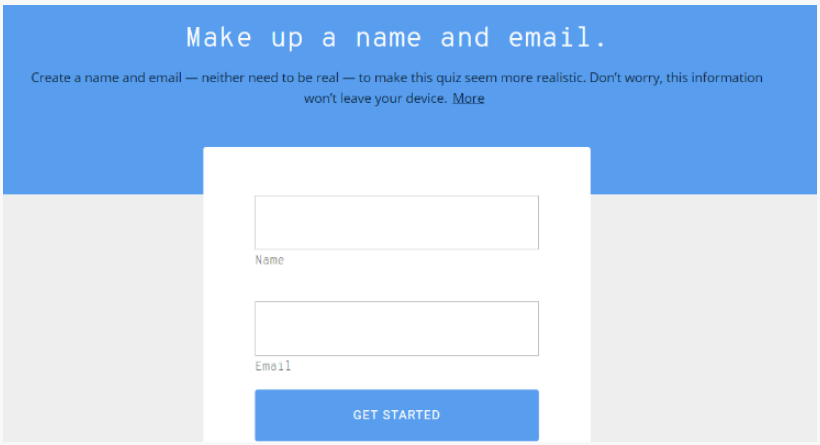
Task for seniors

In January 2019, Google's Incubator introduced an interactive quiz that will test you to detect malicious phishing emails. You will find the most common phishing email scenarios in your test, and you must decide for each message whether it is a legitimate or malicious email for each message.

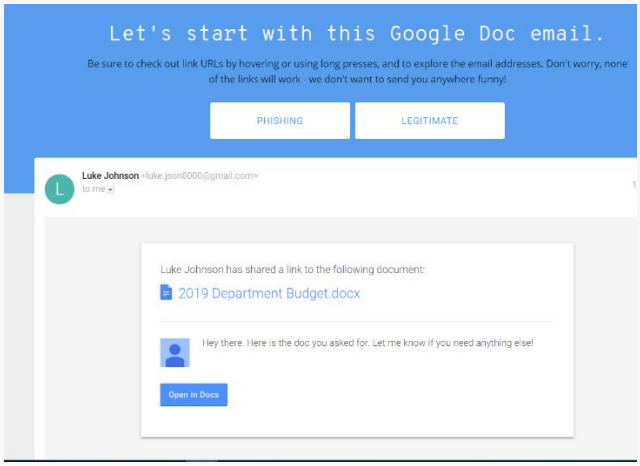
There are 8 scenarios in the test that will guide you through the techniques which cyber attackers use in everyday life. The different scenarios vary, the messages contain different files in the attachment and require your immediate attention.

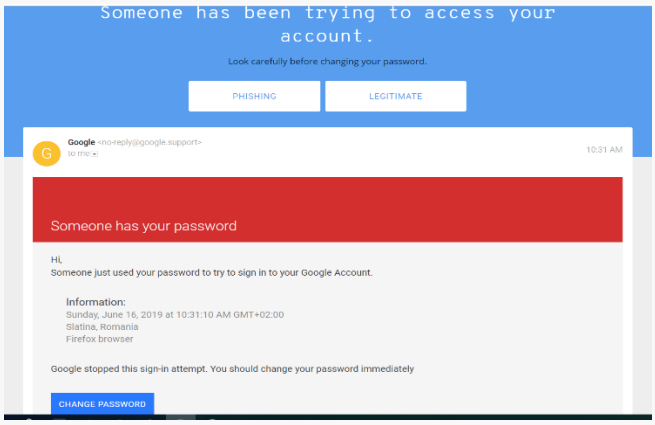
Many security incidents begin by clicking on a malicious link or by opening a malicious file from an attachment. You should not open messages from an unknown recipient or click on the links or files in the attachment.

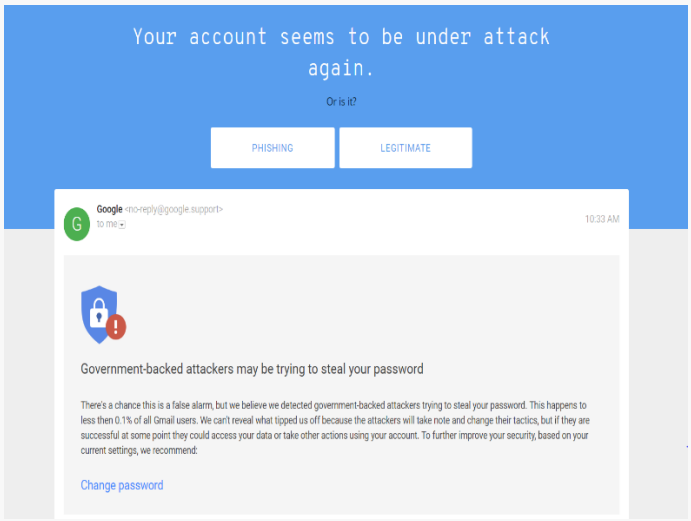
Open this website and start the test. Discuss the right answers together. After 10 minutes we will evaluate the test results and analyse the individual situations. https://phishingquiz.withgoogle.com/



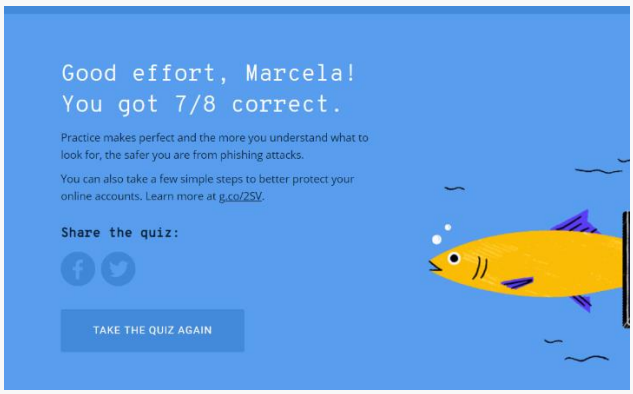
quiz samples







end of quiz with evaluation



EXPERIENCE AND PRACTICE

Questions after presenting passwords to seniors - 30 minutes of discussion and clarification of safety rules:

- What are your achievements?
- It is important to realize how easy it is to trust.
- Let's discuss the individual situations.
- **A closer look, however, reveals that there are several things that do not fit:**

- 1. E-mail uses only general address, although the service where you have a real account must know your name.
- 2. The same applies to the mail recipient. This was apparently sent to multiple addresses listed in the blind copy. The attacker waited to "catch".
- 3. Several minor grammar errors appear if the attackers are not from English speaking countries.
- 4. Nonsense sender address services@paypal.cc . Of course, the domain www.paypal.cc does not exist, the correct address is paypal.com.
- The site address that would appear in the browser after clicking the appropriate button would also be likely to be non-sense. Entering your name and password into this service would certainly send the data straight into the wrong hands.
- However, you do not need to receive similar messages just by email. Quietly, they can lurk in the delivered SMSs (you may not be so careful about the small screen of your mobile), on different websites, or pop up as a new window in your browser.
- The good news is that modern browsers, e-mail clients like Gmail or Hotmail and the most used antivirus programs already provide phishing protection. Often, suspicious mail will end up straight in the spam, and a strong warning will appear when you try to open fraudulent links in Chrome.

  However, you should help them not to click unnecessarily on suspicious emails, open unsolicited attachments, and always check the address on the search bar when entering their login information. **Almost all serious sites already have to offer a secure SSL certificate that will be marked with a green or lock icon in the browser.**

PHOTODOCUMENTATION

Bibliography

Netografia

https://ekonomika.sme.sk/c/20294323/seniori-pri-pouzivani-internetu-zanedbavaju-bezpecnost.html

https://www.jaknainternet.cz/page/1178/pocitacova-hesla/

https://www.omediach.com/tlacove-spravy/8295-online-podvody-ake-su-najcastejsie-triky

https://phishingquiz.withgoogle.com/

https://www.youtube.com/watch?v=9SVwPZ5scEU&fbclid=IwAR1hGBN7ZADdJKCcxRyiSGcPfsmPCd_hQ7xBuugu_gU8EqcPbO4yhMe67QU

INERCIA DIGITAL

SPANISH PART

ACTIVITIES

4. **SOCIAL NETWORKS: Configuration of their Facebook account**

5. **HOW TO RECOGNIZE SECURITY WEBSITE: Fake websites**

6. **SECURITY SOFTWARE: Anti-virus and Anti-Malware**

Activity 4

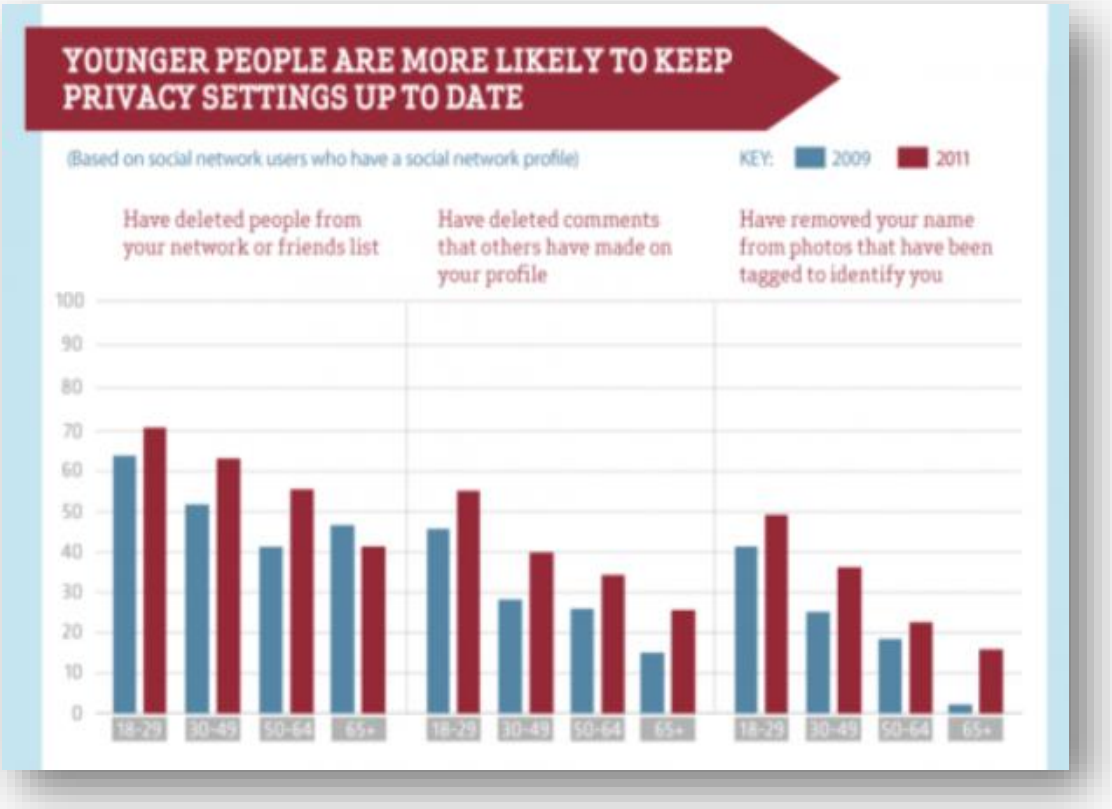
SOCIAL NETWORKS

PROBLEM AND GOAL

According to information sources such as We are social and HootSuite, which make a digital report each year, they affirm in the digital report of 2018 that there are 4 billion people using the internet (Social, W. A.: 2018). Social networks are more and more present in our daily lives regardless the age. First, we should define what social networks are. As we are users of social networks, we can define them as online places where you can interact with other users. Most “popular” or frequent social networks are those known as Facebook, Twitter and Instagram. We tend to get up and usually take our mobile phone to check news in Twitter or to check latest photos of our friends in Facebook or Instagram. The main problem of these social networks is that they are completely public, and anyone can enter your profile and learn much about you. That is why it is so important to learn and take care of your privacy configuration.

In this activity, we are going to consider Facebook as it is the most used social network on the Internet and elderly people tend to have an account there. This data is extracted from The Guardian which claims that the population group using Facebook the most is elderly people (+55 years old people).

Social networks are completely public so privacy must be taken care of. The population is increasingly aware that it is necessary to configure privacy. Most networks have different privacy policies so you can set up certain aspects of your profile. The graph below shows that young people are the most aware of this issue while seniors are the least aware.



Therefore, our main objective is to improve the statistics presented by making elderly people aware of the importance of this context. We attempt to help them making their environment safe on the Internet, protecting themselves, their family and their data. Our specific objectives, which are easy to manage, and which will improve their safety, are presented below:

- Teach them that it is important to read the terms and conditions of the social network you want to access, so we will read the ones of Facebook.
- Configure their privacy to make them safe in social networks, specifically in Facebook.
- Teach them that it is not good in terms of safety to share your personal life, neither publish photos everyday nor reveal your personal data to the unknows. Explain elderly people that anyone is unknown in social networks.
- Explain elderly people that anyone is unknown in social networks, since it depends on what information about you the unknows have at their disposal.

TIME ALLOWANCE

We estimated 45 minutes for the activity.

AID

Requirements:

- Room with Internet.
- One computer per participant.
- Projector.
- Blackboard.

NUMBER OF PARTICIPANTS

Requirements:

- Beneficiaries: seniors.
- Number of participants: 20.
- Age: among 65 and 74.
- Group divisions for one part of the activity.
- Restrictions: people with Facebook account.

ACTIVITY DESCRIPTION

Start - Foreword (15 minutes)

In the first part of the activity, seniors will be presented with the current situation regarding the internet:

Brief introduction:

According to the information sources such as We are social and HootSuite, which make a digital report each year, they affirm in the digital report of 2018 that there are 4 billion people using the internet (Social, W. A.: 2018). Social networks are more and more present in our daily lives no matter our age. First, we should define what social networks are. As we are users of social networks, we are capable of defining them as online places where you can interact with other users. Most "famous" or frequent social networks are those known as Facebook, Twitter and Instagram. We tend to get up and usually take our mobile phone to check news in Twitter or to check latest photos of our friends in Facebook or Instagram. The main problem of these social networks is that they are completely public, and anyone can enter into your profile and learn more about you. This is why it is so important to learn and take care of your privacy configuration. The graph below shows that young people are the most aware of this issue while seniors are the least aware (use graphic).

Provide elderly people with some tips for protecting their privacy on social networks:

- NO! → Communicate your personal information.
- YES! → Accept only petition from people you certainly know.
- YES! → Protect your password combining numbers, letters, signs, and capital letters.
- YES! → Personalize your profile privacy.

Some questions for discussion before the development of the activity:

- When you created your Facebook account, did you accept terms and conditions without reading them?
- Do you provide personal information in social networks?
- Have you ever configurated the privacy of any social network?

Development of the activity (20 min)

In this part of the activity, the main objective is to improve the configuration of an account of elderly people.

- Access to Facebook webpage: https://www.facebook.com/
- Privacy check-up: at first, we will revise how they are sharing information with people on Facebook. Explain them that you can control your posts (public, Friends, Friends except someone). Moreover, you can control the visualization of your profile details such as emails address, birthday, hometown, etc. Finally, you can connect or disconnect apps with your Facebook account → photo documentation 1.
- Check privacy shortcuts and privacy settings tools: in this case, elderly people will check the following items: locations, activity, revision of the posts I am tagged, how people can find you and contact you → photo documentation 2.
- Review of account security: as this issue is already reviewed in other activity we only mention and refer to the other activity in order to learn more. We will explain them they have the opportunity to change password, two-factor authentication, setting up extra security → photo documentation 3.
- Read about data policy: https://www.facebook.com/privacy/explanation/

Discussion (10 min)

The third part of the activity will be dedicated to questions and doubts of seniors. Task or more information: learn about the privacy on Facebook.

https://www.facebook.com/about/basics

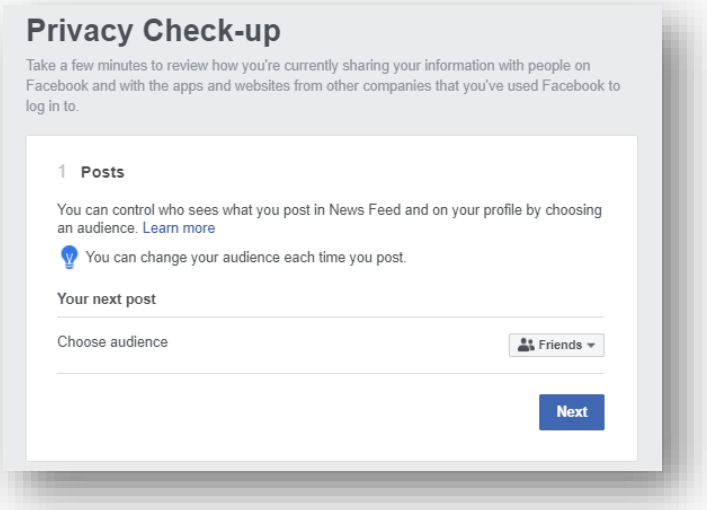
EXPERIENCE AND PRACTICE

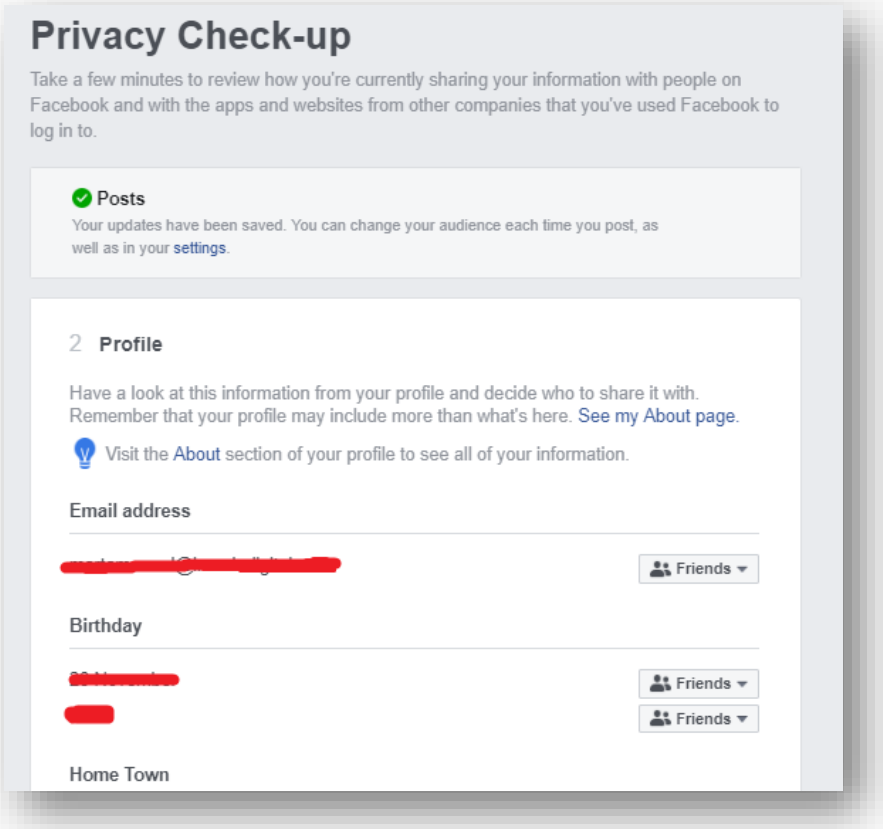
Some tips for the staff:

- YES! → Explain the activity slowly and methodically.
- YES! → A first quick explanation with examples.
- YES! → When elderly people start the activity, follow the process with the help of the projector, people can do it without getting lost.
- YES! → Do not use Facebook jargon.
- YES! → Keep in mind that many common words in the jargon are in English, so they should be translated into the mother tongue of seniors.

PHOTODOCUMENTATION

Photo documentation 1:





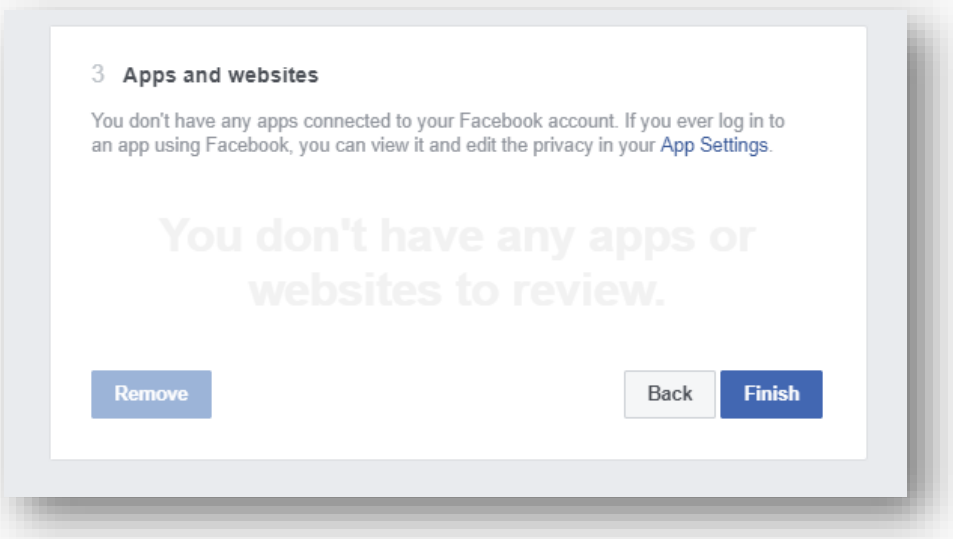
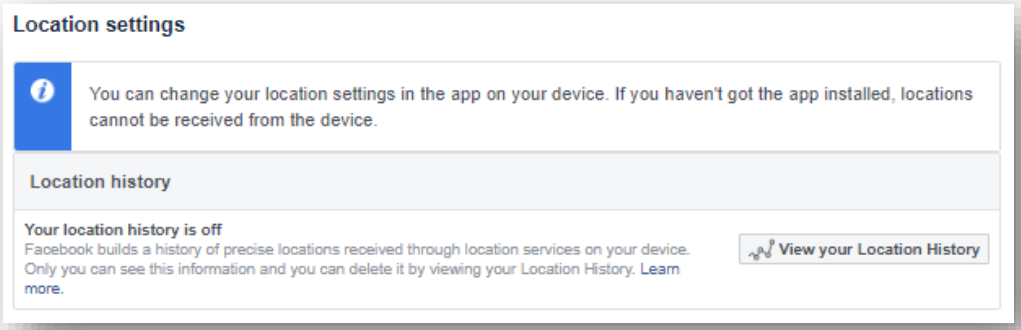
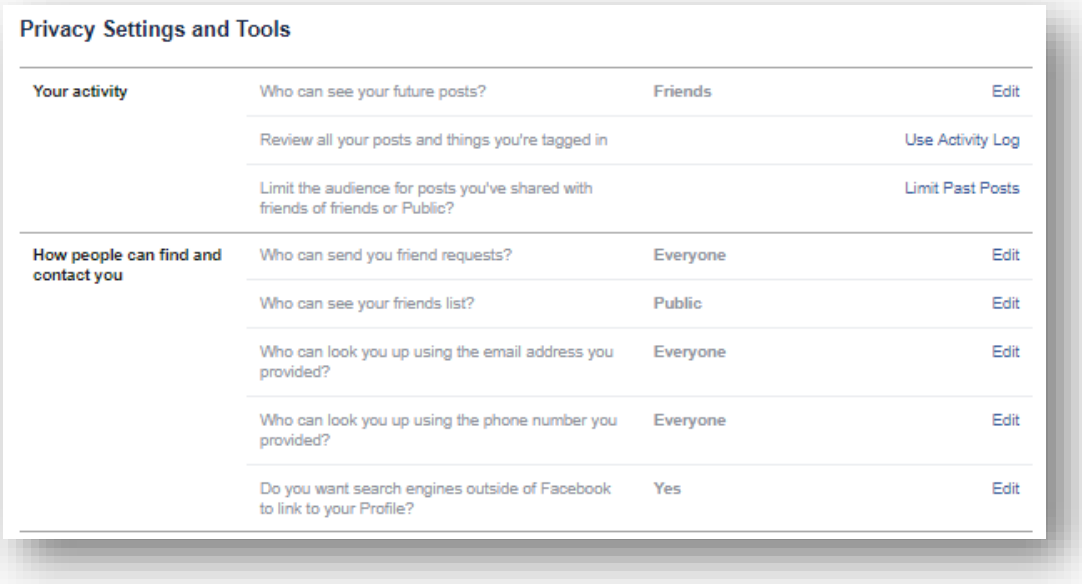


Photo documentation 2:

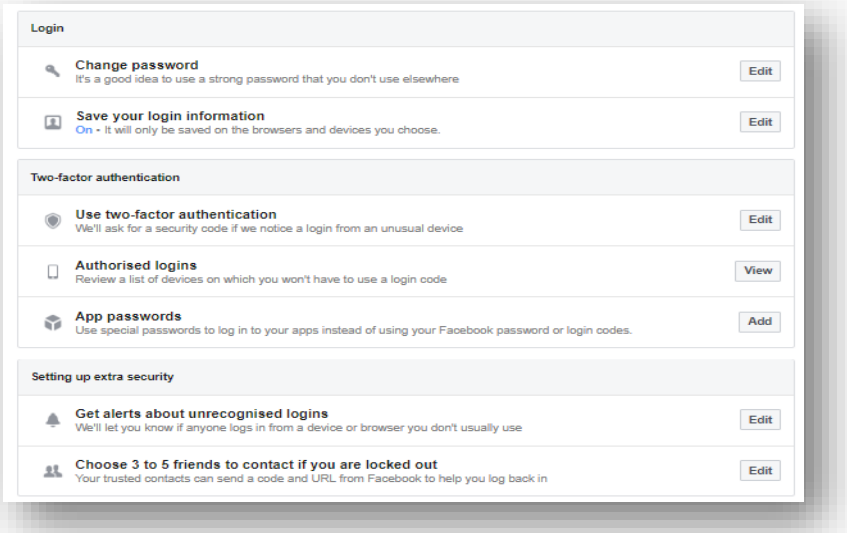




Privacy Settings and Tools

Your activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
How people can find and contact you	Who can send you friend requests?	Everyone	Edit
	Who can see your friends list?	Public	Edit
	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?	Everyone	Edit
	Do you want search engines outside of Facebook to link to your Profile?	Yes	Edit

Photo documentation 3:



Login

Change password
It's a good idea to use a strong password that you don't use elsewhere — Edit

Save your login information
On - It will only be saved on the browsers and devices you choose. — Edit

Two-factor authentication

Use two-factor authentication
We'll ask for a security code if we notice a login from an unusual device — Edit

Authorised logins
Review a list of devices on which you won't have to use a login code — View

App passwords
Use special passwords to log in to your apps instead of using your Facebook password or login codes. — Add

Setting up extra security

Get alerts about unrecognised logins
We'll let you know if anyone logs in from a device or browser you don't usually use — Edit

Choose 3 to 5 friends to contact if you are locked out
Your trusted contacts can send a code and URL from Facebook to help you log back in — Edit

Activity 5

FAKE WEBSITES

PROBLEM AND GOAL

Computer users are always at risk of getting a virus in their devices. Today, a virus in the computer usually means that someone is attempting to enter in your computer system in order to obtain

personal data and specifically your bank account data. There are many subclasses of this type of virus; the problem that we are going to analyse is known as Web Spoofing. This phenomenon consists in the impersonation of a real web site by a fake one in order to commit a crime. The fake website adopts the overall content and format copying every single aspect of the real one, even their URL, not to be recognized as a fake website.

In other words, Website Spoofing consists of the deviation of a victim and his data through a false page created with the same quality, same content, same URL of the real one. The objectives of Web Spoofing are the following ones:

- Phishing: obtaining other users' credentials
- Claims
- Mockery
- Scam
- Fraud
- Blackmailing

The goal of this activity consists in educating elderly people on this phenomenon and providing them with some tips in order to face it.

TIME ALLOWANCE

We estimated 45 minutes for the activity.

AID

Requirements:

- Room with Internet.
- One computer per participant.
- Projector.
- Blackboard.

-

NUMBER OF PARTICIPANTS

Requirements:

- Beneficiaries: seniors.
- Number of participants: 20.
- Age: among 65 and 74.
- Group divisions for one part of the activity.
- No restrictions.

ACTIVITY DESCRIPTION

Start - Foreword (15 minutes)

In the first part of the activity, seniors will be presented with the current situation regarding the web spoofing:

Brief introduction:

- What is web spoofing? This phenomenon consists in the impersonation of a real web site by a fake one in order to commit a crime. The fake website adopts the overall content and format copying every single aspect of the real one, even their URL, not to be recognized as a fake website.

Some questions for discussion before the development of the activity:

- Did you usually provide your personal account?
- Did you provide personal information in websites?
- Have you ever suffered fraud on Internet? Recount your story.

Development of the activity (20 min)

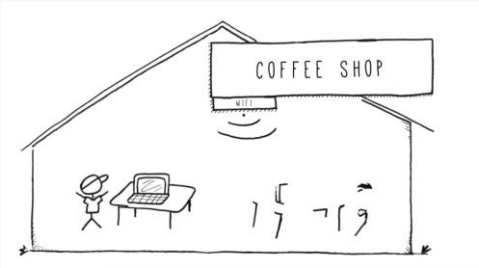
In this part of the activity, there will be a lecture about prevention techniques:

- Avoid using hyperlinks.
- When visiting shopping sites like Amazon or other ones, you will have to take extra care since these websites tend to be stolen.
- Take care of where you click in social networks as they can leave you in a fake website.
- Configure your privacy policy on your social networks.
- Whenever you provide personal data in a website, check first the SSL.

Activities:

- Send an email to our seniors with hyperlinks and observe if they use the hyperlink directly or if they copy it into the browser. Think and discuss about it.
- Visit several webpages where they tend to do shopping and find out whether they are fake webpages or not.

- Check social networks configuration.
- Explain what SSL is. You can help yourself with this video:



What is SSL and how does it work?

- Bookmark important sites they use frequently.
- Install security software or antivirus in your laptops.
- We have created the following Quizizz quiz for the seniors. It is a fun way to learn!

Discussion (10 min)

The third part of the activity will be dedicated to questions and doubts of seniors. Tasks or more information: visit and learn more about the tools provided.

EXPERIENCE AND PRACTICE

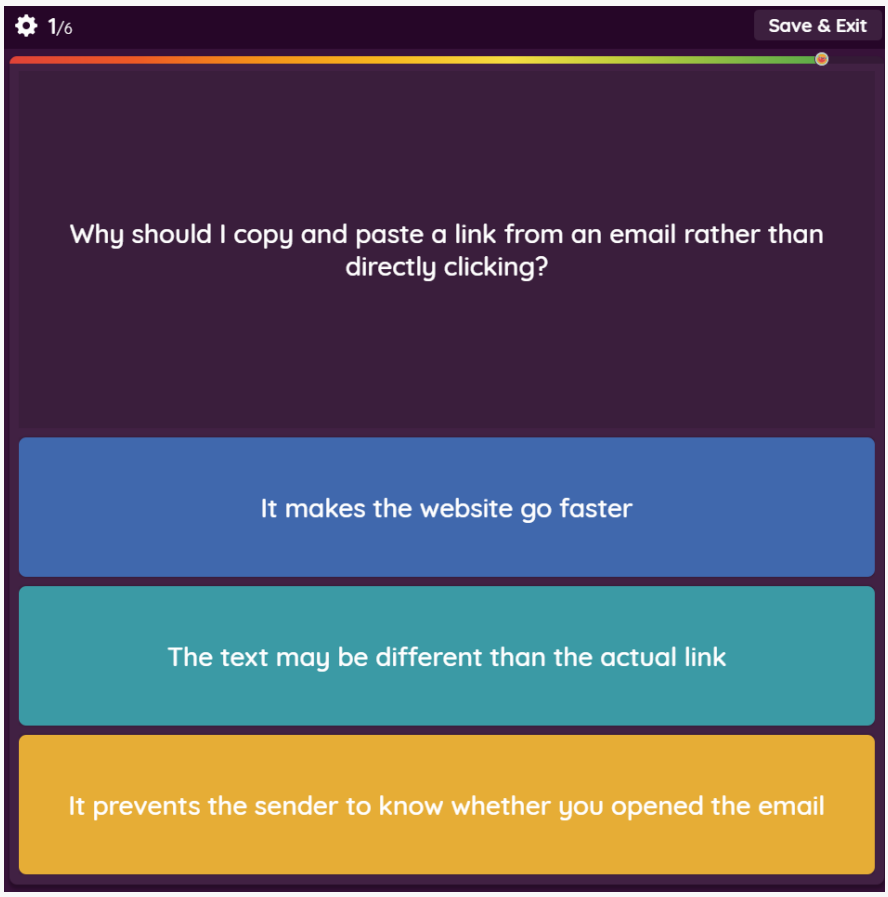
Tips:

- Explain the activity slowly and methodically.
- When they start the activity, follow the process with the help of the projector so that the participants can do it without getting lost.
- Keep in mind that many words referring to the Internet are in English, so they should be translated into the mother tongue of seniors.

PHOTODOCUMENTATION

Photo documentation 1:

Photo documentation 2:



Activity 6

Security Software

PROBLEM AND GOAL

We do mainly all our daily activities on the Internet: shop online, work online, play online. Basically, we live online. We receive a number of attacks in real life: threats, robberies, etc; on the Internet it is similar. Based on the BIS Cyber Security Breaches Survey 2014, Britain is being targeted by up to a thousand cyber-attacks every hour. For SMEs, this could leave traces on their incomes and their financial losses.

However, this is not a problem which only affects enterprises, the attacks occur everywhere, and the impacts fall on anyone. We have the responsibility to protect our services and we can do in by means of security measures and reporting events. Therefore, our main objective is to know the basics of cyber security so that seniors can use the computer and the Internet in a safe way. We attempt to make older users more aware of dangers and threats of the Internet and of the need to protect themselves. Our specific objectives are easy to improve and will improve the quality of life of users.

Specific objectives are presented below:

- To analyse several cases of cyber-attacks and realize how they affect us.
- To reflect on our online reputation and digital identity.
- To know the most common threats to computer and internet security and become familiarised with the terminology.
- To configure basic techniques for protecting our computers and our online information.

We estimated 45 minutes for the activity.

AID

Requirements:

- Room with Internet.
- One computer per participant.
- Projector.
- Blackboard.

Theory explanation regarding malware (for the trainer):

The most common threats to computer and internet security are:

1. Virus
2. Worm
3. Trojan Horse

4. Spyware
5. Adware
6. Phishing
7. Ransomware

Malware Name	Malware Definition
Adware	This software allows to automatically download, play or display advertisements. In some cases, computer users allow this malware to run on their computer in exchange for using the free-of-charge software. By itself, it is usually not dangerous but, in some cases, it behaves like a Spyware and represents a privacy threat.
Virus	It can infect other files, with the intent of spreading to another computer through network, internet or through removable media such as CDs or memory sticks. It can cause some serious damage to your computer, such as deleting or corrupting your data.
Spyware	Its aim is to steal sensitive data from your computer, like bank account information, health-related data, personal information, etc.
Worm	This malicious software program spreads through the network and can replicate itself with a great speed. The main difference between this and a virus is that a worm spreads through the Internet, whereas a virus spreads through the files of a computer.
Trojan	It is a program that looks safe, but once you have run it into your computer it will download another piece of malicious software, such as spyware or adware.
Phishing	It represents attempts of cybercriminals to gain access to private information. E-mail messages or web pages are designed to look like legitimate sources. By pretending to be your bank, e-mail service provider or different legitimate source, cybercriminals try to lure you to their fake web pages and get your personal information, such as passwords, usernames or credit card details.
Adware	This software allows to automatically download, play or display advertisements. In some cases, computer users allow this malware to run on their computer in exchange for using the free-of-charge software. By itself, it is usually not dangerous but, in some cases, it behaves like a Spyware and represents a privacy threat.
Ransomware	This software will hide your files and ask you for money to unlock the files.

NUMBER OF PARTICIPANTS

Requirements:

- Beneficiaries: seniors.
- Number of participants: 20.
- Age: among 65 and 74.
- Group divisions for one part of the activity.
- Restrictions: people with Facebook account.

ACTIVITY DESCRIPTION

Start - Foreword (10 minutes)

In the first part of the activity, trainer will make a brief introduction to cybersecurity and relevant cases of cyberattacks.

The following video is very illustrative and short, and can be used to explain the differences between the different malicious software you can find on the Internet:

Malware: Difference Between Computer Viruses, Worms and Trojans

Brief introduction:

Cybersecurity is the practice of making all our devices safe from cyberattacks. With the intention of the early detection of these threats, the National Institute of Standards and Technology (NIST) recommends continuous monitoring of our devices. There are three threats to cybersecurity: cybercrime, which includes individual actors or groups targeting systems for financial gain; cyberwar, which often involves gathering politically motivated information; and cyberterrorism, which is intended to compromise electronic systems and cause panic or fear.

Common methods of attacking us consist in using and controlling computers or networks including viruses, worms, spyware, and Trojans. In general, the average user comes in contact with malicious codes via an unsolicited email attachment or when downloading programs that appear legitimate, but actually contain a malware.

Development of the activity (30 min)

This activity will be divided in two parts. During the first part of the activity, the participants are to identify the different kinds of threats and malwares. In the second part, the participants will take the necessary measures to protect their software from a cyber-attack.

PART 1: Identifying threats.

There are terms related to software attempting to harm computers in different ways, known as 'malware' (a contraction of malicious software). Depending on what they do, different terms are used. In this part of activity, the trainer will activate this Kahoot! activity we have prepared for the session, and the seniors will compete a quiz to see who knows the most about malware.

PART 2: Protecting our computer from threats: Anti-virus and Anti-malware.

There are two major types of protection: anti-virus and anti-malware. The difference between them is explained as follows.

- Malware is a broader term and includes all sorts of unwanted content. However, the term virus became more popular in the media news because of the attacks in the past. As a result, most companies decided to name their product "anti-virus". The truth is, that contemporary viruses are not very popular among cybercriminals and anti-virus companies focus more on different threats than viruses.
- Anti-virus usually focuses on older, more established threats, such as viruses, worms and Trojan horses. This type of malware is already more predictable, but still very dangerous. Anti-virus is the best at fighting the virus from traditional sources, such as USB or email attachments.
- On the other hand, Anti-malware focuses on newer security threats. It protects computer users from the latest, usually more dangerous threats. Another advantage of anti-malware consists in its ability to update its rules much faster and therefore provides the best protection for internet users.

The best security is to install both of them, anti-virus for the more established threats and anti-malware for the newer and more dangerous threats.

- ❖ Do not use open Wi-Fi (Airport, coffee shop...)
- ❖ Do not open email attachments from somebody you do not know
- ❖ Do not click on the links in email from somebody you do not know
- ❖ Avoid websites with pirated material
- ❖ Manage your personal information, especially on social media
- ❖ Use strong passwords
- ❖ Use different passwords, especially for your bank accounts

- Back up your files, especially the most important ones

Some questions for discussion before the development of the activity:

- How were you infected?
- How did it affect your computer?
- Do you know if it got your personal data?
- What did you do to fix it?
- What security measures do you have in your computer?
- Have you ever installed an anti-virus/anti-malware?
- What should we do if our computer detects a virus?

Discussion (10 min)

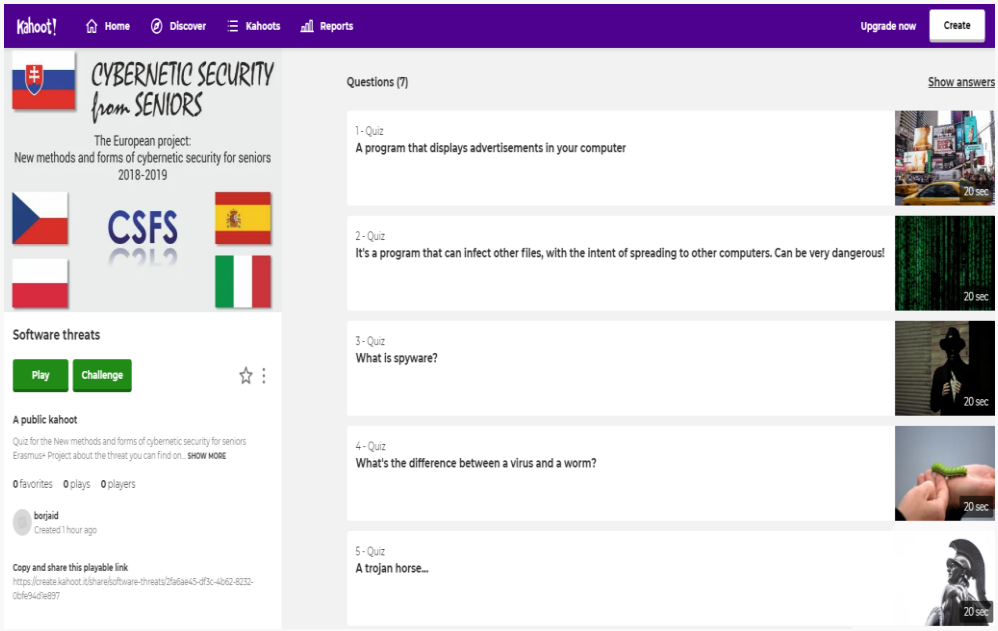
The third part of the activity will be dedicated to questions and doubts of seniors.

EXPERIENCE AND PRACTICE

Tips:

- It is important to discuss the need to protect seniors when using the computer.
- Explain the activity slowly and methodically.
- A first quick explanation with examples.
- When they start the activity, follow the process with the help of the projector in order that the participants can do it without getting lost.
- Keep in mind that many common words in the jargon are in English, so they should be translated into the mother tongue of seniors.

PHOTODOCUMENTATION



Bibliography

"Log in To Facebook | Facebook". *Facebook*, 2019, https://www.facebook.com/settings.

"Malware Definition – What Is It and How to Remove It". *Malwarebytes*, 2019, https://www.malwarebytes.com/malware/.

"News, Sport and Opinion from The Guardian's UK Edition | *The Guardian". The Guardian*, 2019, https://www.theguardian.com/uk.

Social, W. A. (2018). Global digital report 2018. *Erişim*

"SSL Checker - SSL Certificate Verify". *Sslshopper.Com*, 2019, https://www.sslshopper.com/ssl-checker.html.

"Suplantación Web - Ecured". *Ecured.Cu*, 2019, https://www.ecured.cu/Suplantaci%C3%B3n_Web.

"The Difference Between A Virus, Worm and Trojan Horse - *Webopedia*". Webopedia.Com, 2019, https://www.webopedia.com/DidYouKnow/Internet/virus.asp.

"Web Spoofing: Suplantación De Una Web Con La Finalidad De Recoger Los Datos Introducidos Por El Usuario". *Redeszone*, 2019, https://www.redeszone.net/2010/10/30/web-spoofing-suplantacion-de-una-web-con-la-finalidad-de-recoger-los-datos-introducidos-por-el-usuario/.

"What Is Distributed Denial of Service (Ddos) Attack? - Definition from Whatis.Com". *Searchsecurity*, 2019, https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

Fundacia Pro Scienta Publica

POLISH PART

ACTIVITIES

7. Phishing

8. Malware

9. Cyber Communities

Activity 7

Phishing

Phishing:

- Spanish prisoner/Nigerian Scam
- Mailing
- Social Networks (fake profiles)
- Stealing the Identity of a person or an institution

PROBLEM AND GOAL

The Internet today has a huge impact on how society and the life of every individual appears. Being such a powerful medium, on the one hand, is very helpful, but on the other hand- it brings many problems and to some extent has a negative impact on our lives. The Internet plays an important role in everyone's life as a communication tool but also as a source for obtaining information. Some people involved in criminal activities find many possibilities in this. The Internet creates a chance for them to download personal data without actually meeting the owner and at the cost of minimal risk. This is a very popular scam method today, called Phishing, which is a huge threat to the Internet users.

Objectives of the educational activities:

Main goal - to present a given problem to a selected target group, i.e. seniors, who may be the most sensitive group of users on the Internet, relating to a given method of scam.

Specific objectives:

- Increasing awareness about current processes as well as possible threats while navigating the virtual network.
- To explain phishing schemes to the participants, i.e. to show how they work.
- Presentation of selected types of phishing.
- Presentation of techniques for preventing phishing

TIME ALLOWANCE

The whole duration of classes **-** 90 minutes:

- Organizational and preparation activities - 5 min.
- Integration - 5 min.
- Introduction to the workshop content - 10 min.
- Introduction to the topic of the class and problem definition - 10 min.
- Work in groups - 15 min.
- Presentation of selected types of phishing - 10 min.
- Work in groups - 10 min.
- Presentation of techniques protecting against phishing - 15 min.
- Summary - 10 min.

AID

- access to a computer with internet connection, projector
- flipchart, highlighters
- posters, notebooks, writing tools

NUMBER OF PARTICIPANTS

up to 15 people to facilitate communication during the class and divide the group during the performance of tasks into 3-person groups.

ACTIVITY DESCRIPTION

I. Organizational and preparation activities

•Description: Welcoming participants, assigning computer stations, introducing themselves to the group

• Duration: 5 minutes

• Method of implementation: Discussion

II. Integration – Activity 1

• Task description: Each participant gives his/her name and tells the others about the nice things that happened to him/her that morning. It is also worth saying that the integration task is voluntary and if you do not like it, you can only give your name.

• Duration: 5 minutes

• Method of implementation: Discussion

III. Introduction to the content of the workshop

• Description: Explain the objective, schedule and expected length of activity to the participants. Opening questions to the group that can help educators find out the level of participant's knowledge about a given topic: Have you ever heard about Phishing on the Internet? What associations do you have with it? Is this phenomenon common today? Writing on the flipchart answers for summary.

• Duration: 10 minutes

• Method of implementation: lecture, brainstorming

• Materials: flipchart, markers, notebooks, writing tools for participants

IV. Introduction of the topic of the class and problem definition

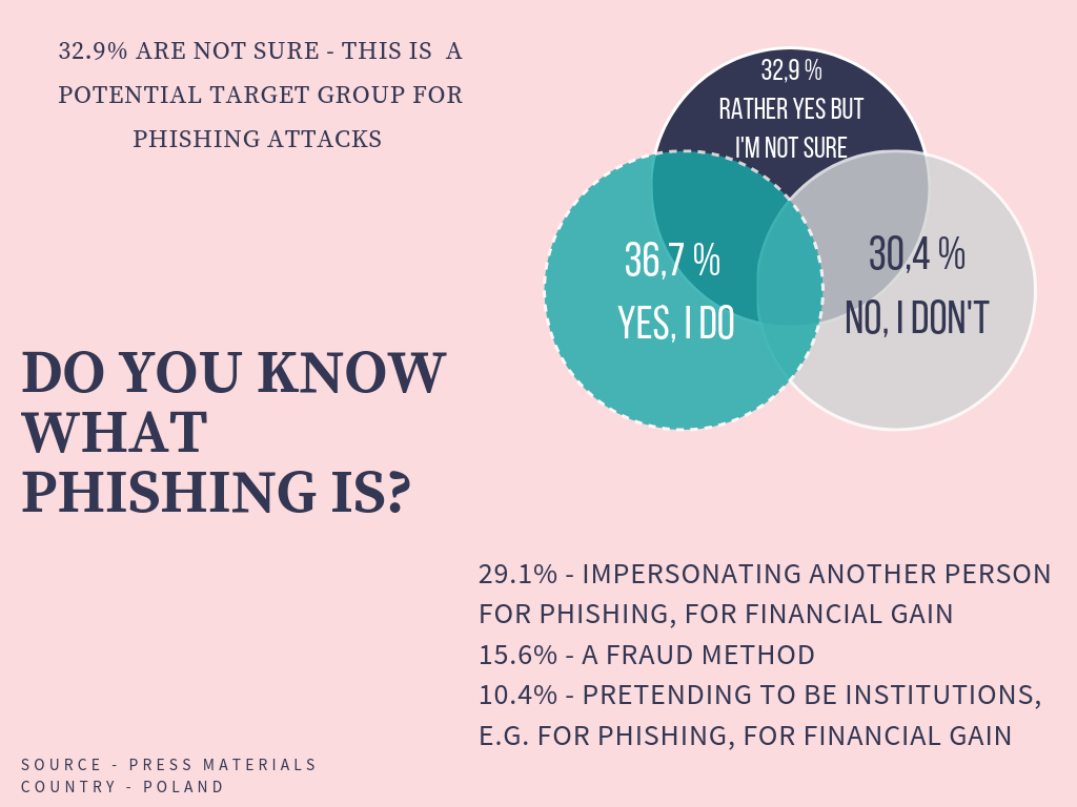
• Description: an approximation of a given problem called Phishing, i.e. a description of a given phenomenon.

• Duration: 10 minutes

• Method of implementation: lecture, discussion

• Materials: printed infograms for class participants, cards, writing tools for participants

As a starting point, it is worth presenting statistics that show the level of awareness of Poles about Phishing on the Internet from Spring, 2019 (source - https://antyweb.pl/co-trzeci-polak-nie-wie-czym-jest-phishing/)



Pic. 1.1 *Do you know what phishing is?*

Source: own study

After explaining the infographics, there may be a brief discussion about these statistics. The next step is to explain to the group what Phishing is about:

Phishing is a method, a source of obtaining information such as usernames, passwords, credit card data, necessary for payment, i.e. confidential data, by the use of electronic correspondence (Dakpa, 2017). Therefore, the term is often translated as *password harvesting fishing*. Phishing is carried out via email, less often via text messages. It often redirects users by means of links to popular but fake websites of shops, banks, etc., which are similar to the official websites of the registered institutions on which the user should enter their data, which will then be stolen. In other words, Phishing happens when someone uses fake emails or text messages to get confidential information (bank account number, login ID, password). This data can be used by phishers to steal money or identity. They can also access the network or a computer using e-mails and text messages. The user, just by clicking on the link provided in the message becomes involved in a network stealing his data.

After briefly introducing to the topic of phishing, we move on to the task which should check how the group keeps up with the topic.

V. Workshop in groups – Activity 2

• Description of the task: The educator divides the participants into 3-member groups, they should create a scheme or structure, which presents the flow of information in phishing. It is worth saying that a given scheme is very complex, so the task is to include in their scheme as many relationships and dependencies as possible.

• Duration: 15 minutes

• Method of implementation: workshop, work in groups

• Materials: posters, writing tools for participants

• Key:

The data flow pattern in Phishing looks like this and is a broad version.

1. Phisher + user = phisher sends an email to the user
2. User + link = the user gets a link in the email
3. Link + website = the user clicks on the link and goes to the fake website
4. User + website = the user logs in to the website i.e. enters the key
5. Website + phisher = at this moment the phisher gets the user's key (confidential data)
6. Phisher + key = users' data is stolen and blocked, and phisher can use it for various purposes.

VI. Presentation of selected types of phishing

• Description: presentation of phishing types, their characteristics and distribution

• Duration: 10 minutes

• Method of implementation: lecture

• Materials: cards, writing tools for participants

There are several types of phishing attacks that always have a similar purpose, i.e. phishing personal data, and have a similar feature - a false excuse.

1. **Spanish prisoner/Nigerian Scam** - Nigerian fraud, a Nigerian scam, a type of phishing that was initially known as a Spanish prisoner. The "Spanish prisoner" is about begging money for a wealthy aristocrat who was imprisoned in Spain. He addresses selected people by an e-mail with a request to buy him out of prison. For the loan, he offers a rich return, and after paying the money - he disappears. Over time, the "Spanish prisoner" evolved into a Nigerian scam - an e-mail message from a Nigerian prince in which we are informed that we can be paid for help in transferring money. After providing the data necessary for the transfer and making a

payment to the cheaters' account, it turns out that nothing like this exists. This is one of the most popular methods of fraud on the Internet.

2. **Mailing - Clone Phishing** – a type of attack that happens with the use of e-mail, where Phisher uses previously delivered mail that include an attachment or link. Then it makes copies or a clone and changes the link or attachment to a similar but fake one. As it often happens, the user does not notice the difference and opens this attachment, thereby providing the phisher with his data or access to the computer. The scammer may use this data or user account to communicate with other users and send fake emails.
3. **Phishing in Social Networks** – Phishing often involves stealing information, personal data that allows access to, for example, bank accounts. Another form of phishing is identity theft. Social networks are becoming a popular and easy source of obtaining information about a selected person. They can do this in a variety of ways: use a link to fake websites to steal login details and password (or other personal data) and collect seemingly insignificant personal data that we unintentionally share with friends. In this way, phishers create fake accounts on Facebook and other social platforms that can be used to extort money from friends, cheat (having the user's personal data), collect information that can be used to carry out cruel attacks.
4. **Stealing the Identity of a person or an institution – spear phishing.** This is the most common form of fraud in Phishing. It differs because the attack here is directed to a specific person or organization. This type of phishing has a selected purpose, needs careful and detailed preparation, i.e. searching for information about a selected person (their name, surname, e-mail address, position at work), and finding a connection with other employees and their responsibilities. The main object is to create a reliable e-mail that will meet the needs of a person or organization. At this point, an employee of an organization, for example, should send a certain amount of money, because it falls under his responsibility through a link that is fake, and the amount goes to the cheat.

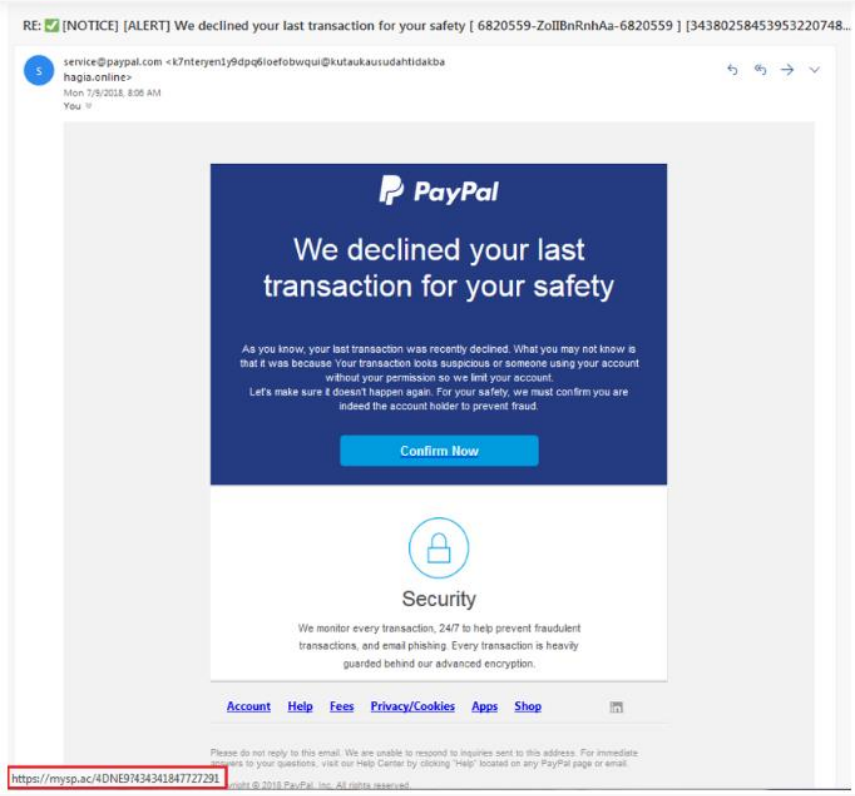
VII. Workshop in groups - How to recognize Phishing – Activity 3

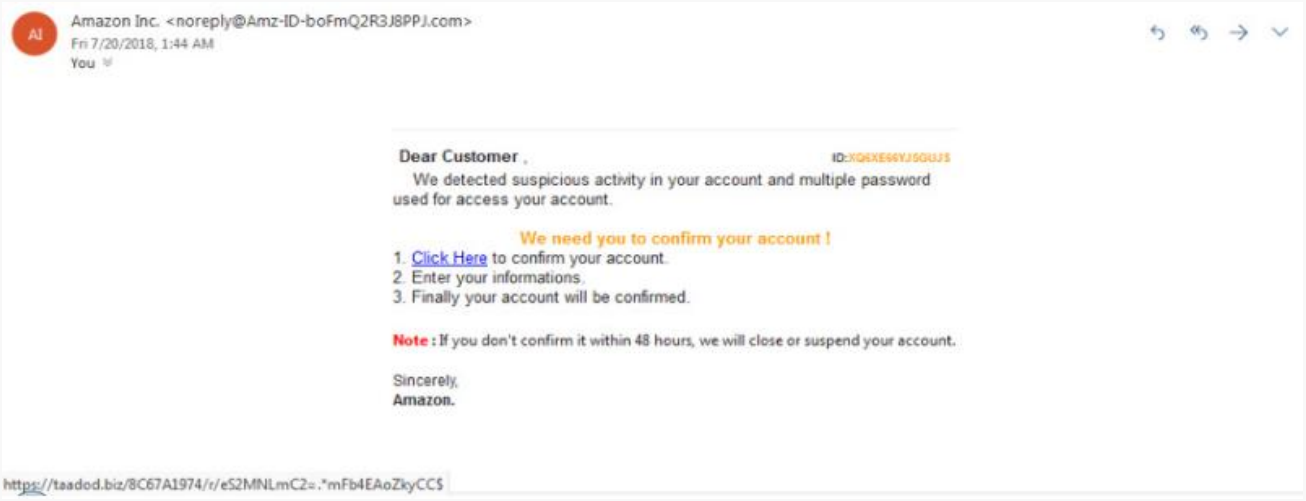
• Task description: the group is divided into 3-memeber subgroups, each of them gets a card with an example of phishing. The task of each group is to recognize what type of phishing is in the picture and to share the result with others.

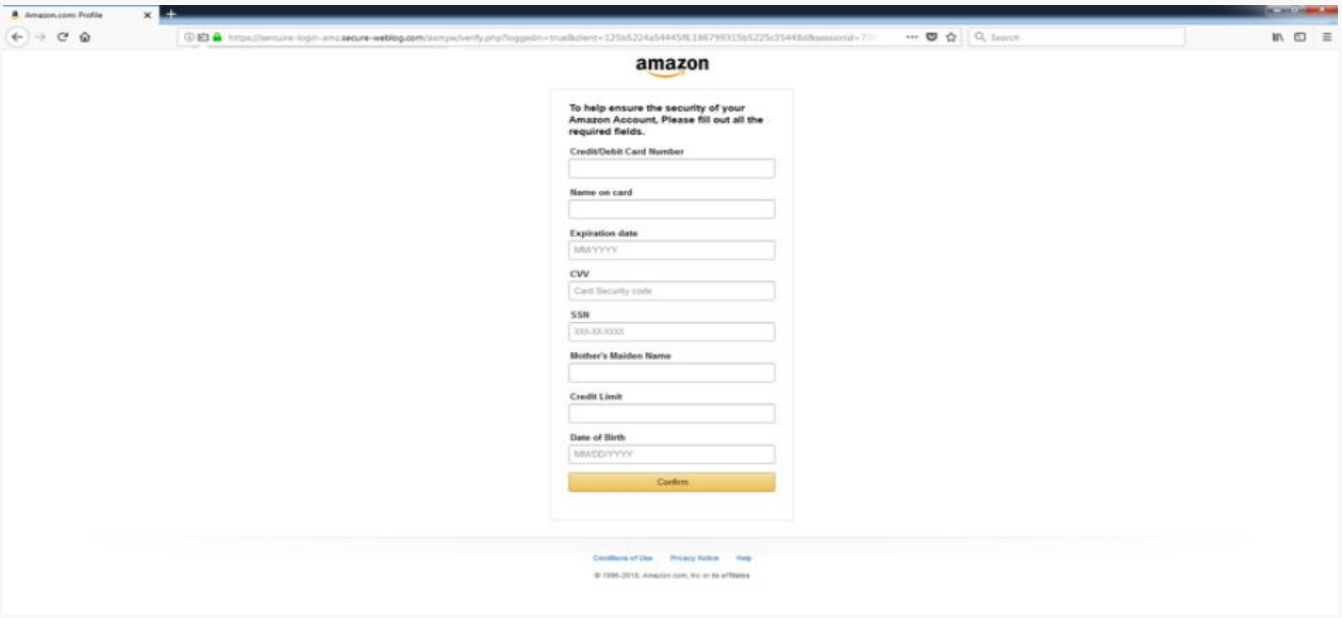
• Duration: 10 minutes

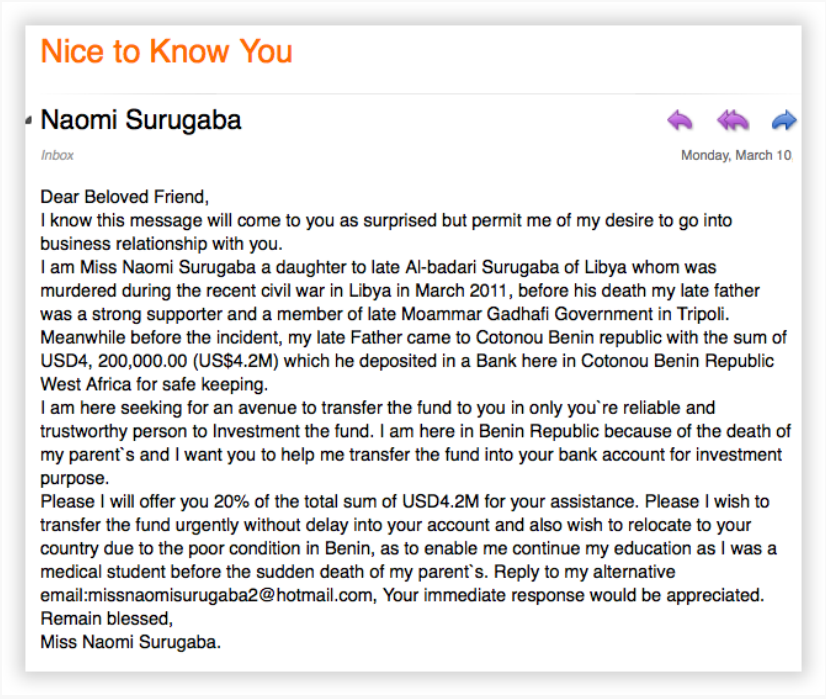
• Implementation method: workshop, discussion

• Materials: printed cards with the pictures, notebooks, writing tools for participants


RE: ✅ [NOTICE] [ALERT] We declined your last transaction for your safety [6820559-ZoIIBnRnhAa-6820559] [34380258453953220748...
service@paypal.com <k7nteryen1y9dpq6loefobwqui@kutaukausudahtidakba hagia.online>
Mon 7/9/2018, 8:06 AM
You
PayPal
We declined your last transaction for your safety
As you know, your last transaction was recently declined. What you may not know is that it was because Your transaction looks suspicious or someone using your account without your permission so we limit your account.
Let's make sure it doesn't happen again. For your safety, we must confirm you are indeed the account holder to prevent fraud.
Confirm Now
Security
We monitor every transaction, 24/7 to help prevent fraudulent transactions, and email phishing. Every transaction is heavily guarded behind our advanced encryption.
Account Help Fees Privacy/Cookies Apps Shop
https://mysp.ac/4DNE9743431847727291


AI
Amazon Inc. <noreply@Amz-ID-boFmQ2R3J8PPJ.com>
Fri 7/20/2018, 1:44 AM
You
Dear Customer ,
ID:XQEXE66YJ5GUJ1
We detected suspicious activity in your account and multiple password used for access your account.
We need you to confirm your account !
1. Click Here to confirm your account.
2. Enter your informations.
3. Finally your account will be confirmed.
Note : If you don't confirm it within 48 hours, we will close or suspend your account.
Sincerely,
Amazon.
https://taadod.biz/8C67A1974/r/eS2MNLmC2=.*mFb4EAoZkyCC$





Key:

Pic. 1 - By clicking the "Confirm now" button, you are redirected to the false address. The real URL is shown on the left side of picture after moving the mouse cursor over the link.

Pic. 2 - the content of the e-mail specifies that you have to go through the link to confirm the data, which is often a phishing scam

Pic. 3 - after going through the link we can see a form where confidential data must be provided

Pic. 4 - an example of a phishing attack called "Nigerian Scam"

VIII. Workshop in groups - Presentation of techniques protecting against phishing – Activity 4

• Description of the task: The task is based on the group working - collecting ideas on how to recognize Phishing. Participants exchange their ideas; the educator writes the ideas on a Flipchart so that, at the end of the task, the participants together create a guide on how to avoid phishing on the Internet.

• Duration: 15 minutes

• Method of implementation: Brainstorming

• Materials: flipchart, markers, notebooks, writing tools for participants

• Key: The guide created at the end of the activity may contain the points as follows:

Pic. 1.2 *How to avoid Phishing?*

Source: own study

IX. Summary

• Description: a summary of the classes, sharing conclusions and own experience in the field of Phishing, asking questions and answering them, getting feedback and comments from participants.

• Duration: 10 minutes

• Method: discussion

QUIZ:

https://create.kahoot.it/share/phishing-or-fishing/1a580a26-9432-4032-8d0e-df369144d410?fbclid=IwAR2DRSgoaFTuarBSUXUbJPun06Wf-k6N20J3geFT7_2uLqBa9Uxyiot1Sgc

PHOTODOCUMENTATION

Activity 8

Malware

PROBLEM AND GOAL

The Internet is not only a wide spectrum of opportunities and possibilities flowing from the virtual world. It is also a constant check-in of our vigilance and security of the operating system we use.

Malware is a variety of programs that are designed to hinder or completely allow your personal computer or other devices to be vulnerable to this type of threat. Malware (a combination of words, malicious "sinister, malicious" and software "software") refers to software that is intended to do harm and to destroy our devices. The more we are sensitive to the whole pool of possible symptoms resulting from infecting the operating system, (better when it is guarded by programs that prevent such activities), the pleasure of using the Internet will be greater. Despite the fact that there are actions aimed to harming us on a virtual level, their effects can be felt in a real way in the real world.

Objectives of educational activities:

Increasing awareness during navigating the virtual network, as well as possible prevention. The aim of the course consists in learning about the possible dangers that you may meet using online goods, which may not be immediately apparent. We will also deepen our knowledge about the features emphasizing the security of the operating system on the website we visit, as well as anti-virus programs and types of security measures to protect against unwanted effects.

TIME ALLOWANCE

The whole duration of classes, 90 minutes:

Organizational activities: 5 minutes.

Integration: 5 minutes.

Introduction to the content of the workshop: 5 minutes.

Introduction to the topic of the course and definition of the problem (presentation of selected types of malware and symptoms that are worth paying attention to): 45 minutes.

Sharing your own experience: 5 minutes.

Workshop in groups: 10 minutes.

Discussion and systematization of acquired information: 15 minutes.

AIDS

Computer, projector, writing tools, cards, poster, flipchart

NUMBER OF PARTICIPANTS

A maximum of 20 people to be able to divide the group into 5 small groups of 4 members during group work classes.

ACTIVITY DESCRIPTION

Beginning of activity - introduction.

1. Welcoming the participants, presenting them with individual points according to which the classes will be conducted.

2. Integration:

A task that stimulates thinking towards abstraction. The exercise consists in creating ideas suggesting the given category defining a feature or function (in this case, it would be good if the topic concerns new technologies), e.g.

a) is electric,

b) is small,

c) has keys,

d) connects with the world,

e) works without internet access, e.g. it is rectangular: laptop, smartphone, pen drive but it will not be a mistake if someone writes, for example, a book. However, we try to hold a certain thematic area to make it easier to implement the course.

1. Introduction to the thematic area, brief description of individual issues.

2. Issues:

a) A **spy program** can be called a **spy**. It is software that **collects all information about us and about our activities** on the web. Beginning from the type of websites visited, ending with credit card numbers, logins and passwords.

b) We associate the **Trojan Horse** with a kind of **"trap"**, which is still used in the IT area today. **It does not duplicate like a virus, but it hides in a file or parts of it**. We are in contact with it in activities that cause harmful changes to the system, under the guise of attractive, useful files that at the same time spread hidden, troublesome functions contrary to those expected by the user.

c) The most important feature of a **computer virus** is its **ability to split itself**. In order to exist, **it needs a host**, i.e. a file which it attaches and at the same time gives it the ability to infect and spread over the network.

d) **The Internet worm** is a **brother of a virus**, but the main difference is that **it does not need any file to spread. It only exploits security vulnerabilities**. Its functions depend on the code assigned to it, from destructive to spy activities.

e) **Backdoors,** like a Trojan horse, impersonate files, but their range is so serious that they **are able to take control of the infected computer**, enabling administrative actions such as deleting or saving files.

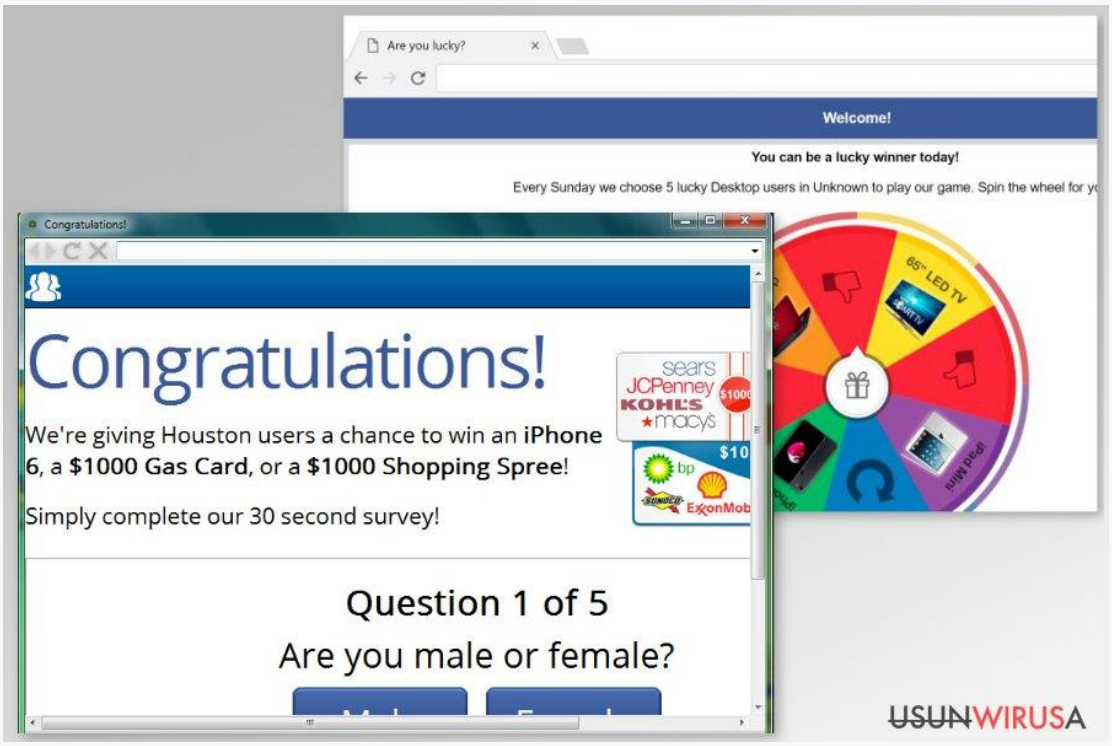
f) **Ransomware** are blackmail programs operating under the cover of special services, such as **the uniformed services - the police**. It is a group of programs whose common feature is a ransom demand. The word is a combination of the word's "**ransom**" and "soft**ware**". The computer gets into total blockade of the device and displays a message that does not arouse suspicion, which appears to be generated by the police. At the same time, **it calls for a high amount to be paid for the alleged internet crime**.

g) **Locker** is a malware from **the ransomware family** that has been more developed and refined in its operation. Its activity consists **in completely blocking access to the computer** and preventing logging in to it.

h**) Exploits** are **software gaps** that are the result of a programming error that hackers use to their own needs by taking control of a computer. It can be compared to **an open door**, which is not locked, even invites uninvited guests inside without any barrier and security.

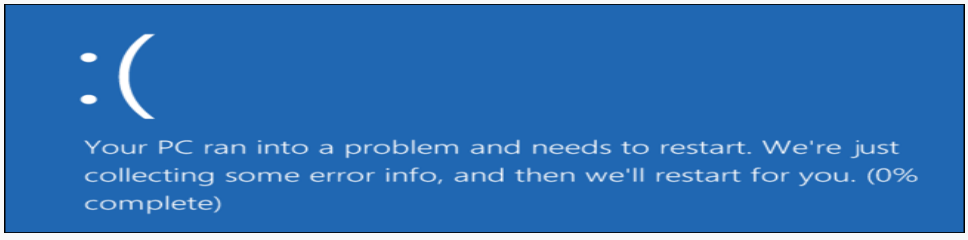
1. Warning signs, which are examples of things that we should pay attention to, at the same time give alarming signals that malware has found its place on your device.

a) The anti-virus program on your computer stops working while blocking the possibility of updating the threat database and depriving the user of any firewall from uninvited guests.
b) For example, there are plugins not installed by us in the browser.
c) The browser's home page has changed to a different one, without any user interaction, any attempt to restore the browser to its original state that results in automatic, persistent messages, "reward windows" that redirect user to a completely different place on the network.



Pic 1.3 *Congratulations!*
Source: https://usunwirusa.pl/oszustwo-gratulacje-wygrales/, (access: 06.07.2019)

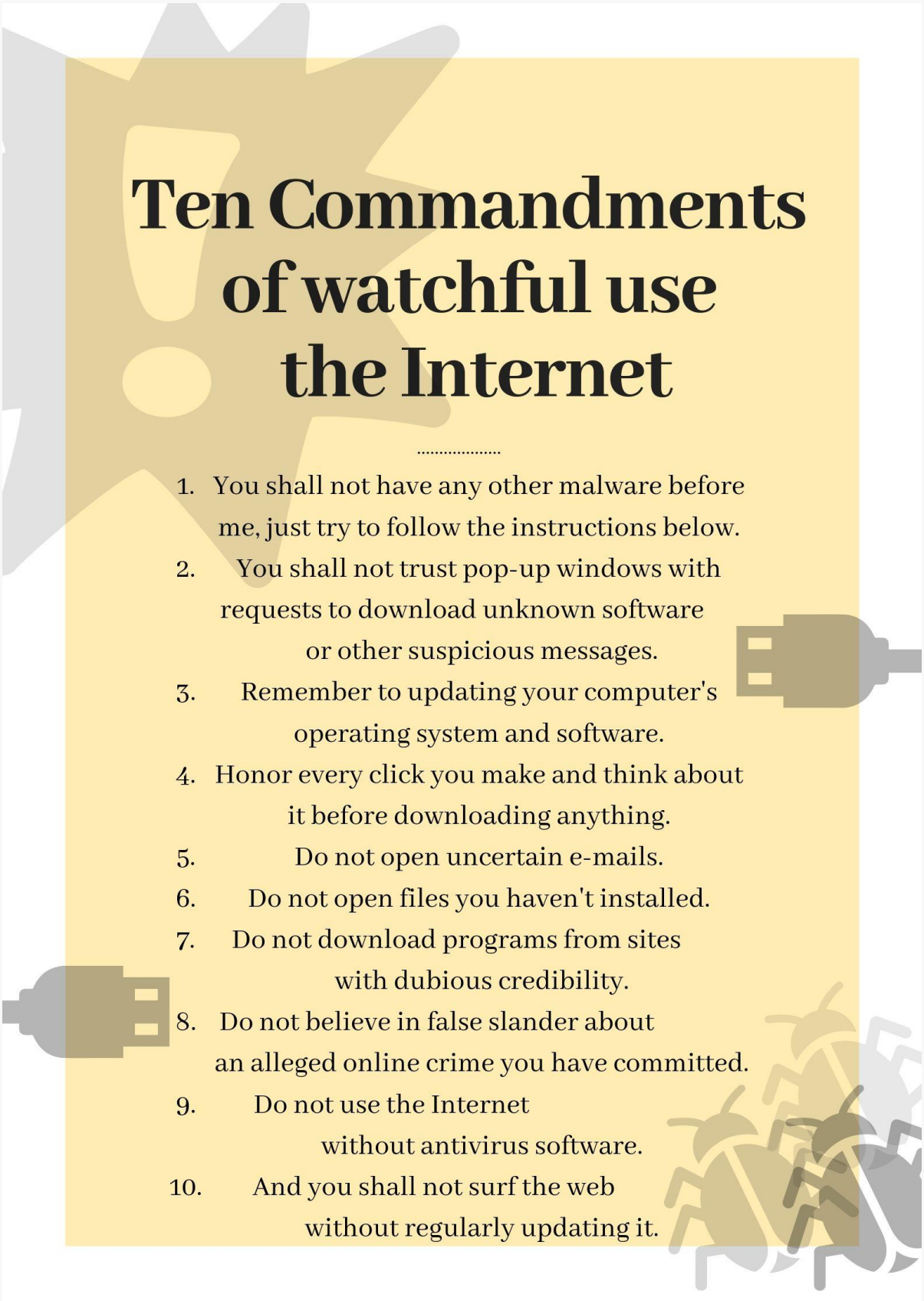
d) The computer is running slower and its work is extremely intense, the fan is constantly active and working loudly is another of the symptoms of work in the background of unwanted software,
e) You may notice an inexplicable loss of disk space,
f) The system often "spills out" displaying a blue screen - *blue screen of death*,



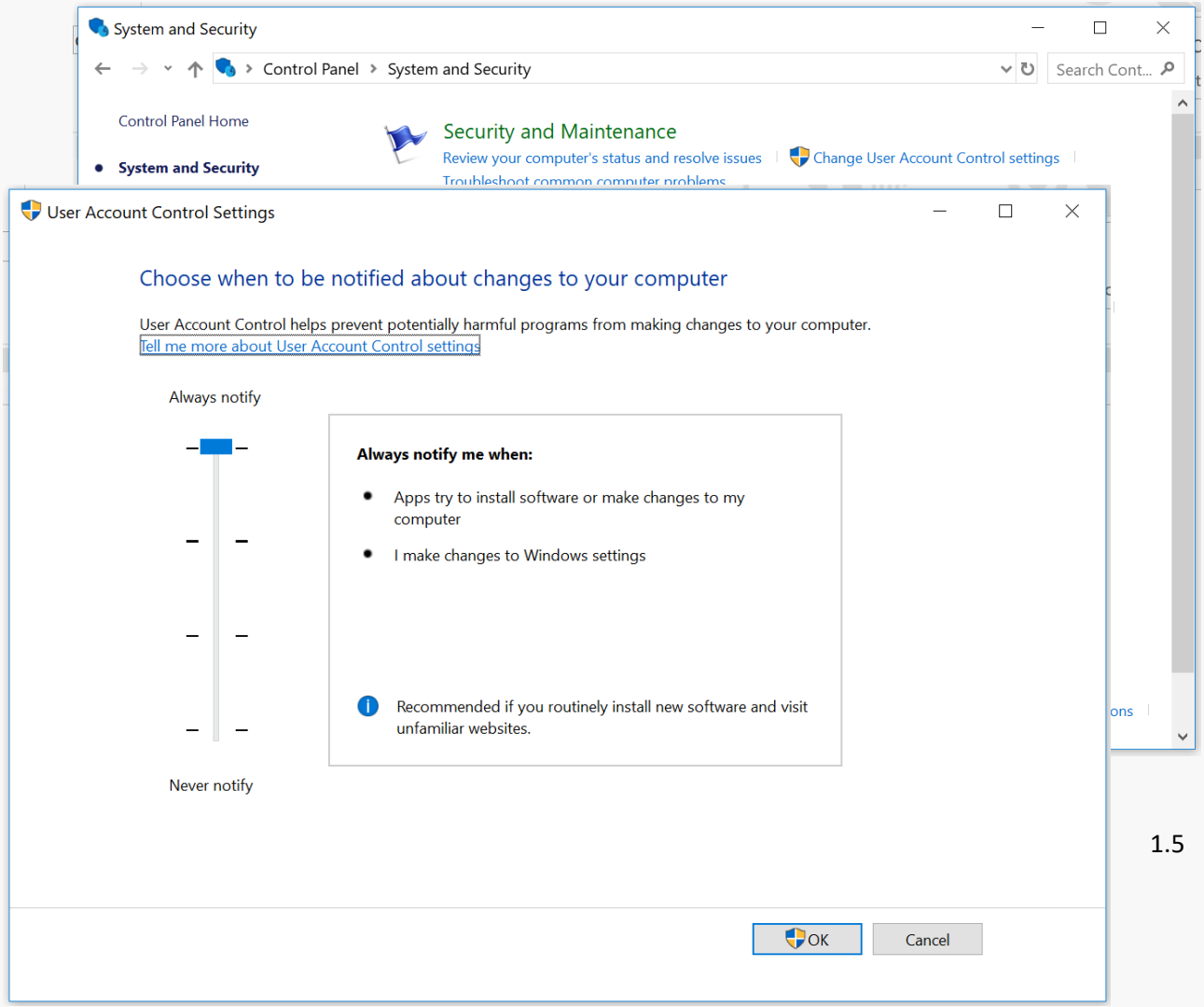
Pic 1.4 *Blue screen*

Source: https://www.howtogeek.com/163452/everything-you-need-to-know-about-the-blue-screen-of-death/, (access: 06.07.2019)

1. **Poster presentation.**



2. Windows Security Checklist.



1.5

Checklist

Source: own source

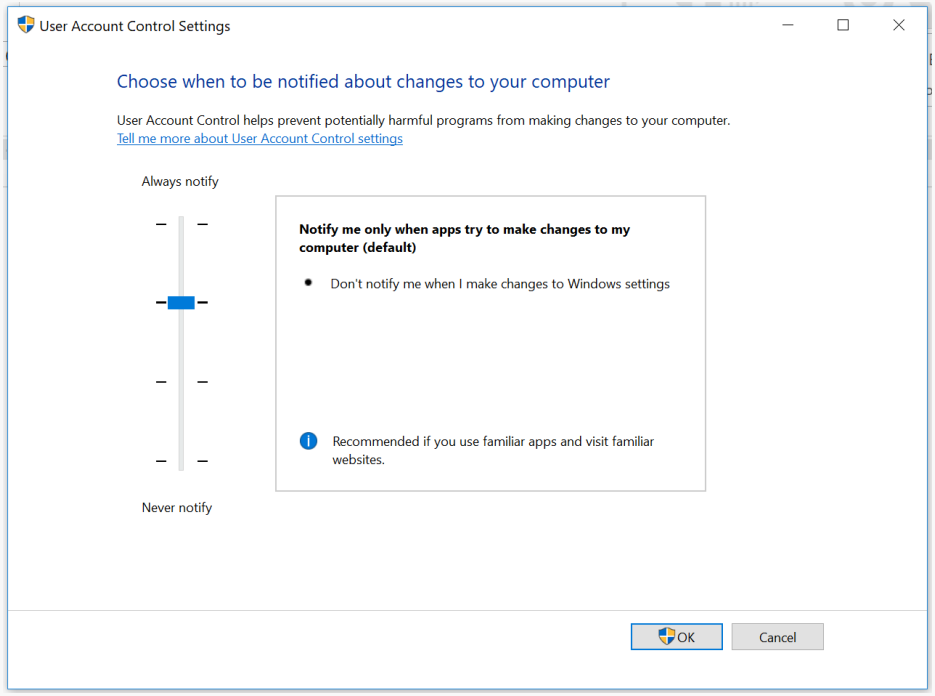
In front of us there is a tab "security system" in Windows 7 software, where we have for example:

a) Action Centre, which informs if the firewall is enabled, malware protection is updated and necessary updates are automatically installed on your computer.

b) Windows Firewall enabled firewall protects against uninvited visitors, e.g. viruses accessing a computer via a network.

c) Windows Update, which automatically downloads and installs the latest updates.

d) Backup/restore, enables regular automatic backup of files, e.g. photos, documents, which can be restored in case of loss or hardware failure thanks to this option,It is also worth noting the user account control settings, where we will get support for potential malware and block the possibility of making changes on your computer. The slider allows you to decide when you want to be notified of changes that malware wants to make on your device.



1.6 *Control settings*

Source: own study

These are just a few suggestions that are offered to the user by the system with regard to taking care of his or her protection.

3. Workshops in groups

Use a mixed deck of 20 cards, including four aces, four ladies, four kings and four jokers, to divide the group. After you have folded the cards, ask each participant to draw one of the available pots to form working groups.

a) First task:

Give out 4 passwords to each group. On one card: Trojan horse, backdoor, virus, ransomware, on the other card: spyware, worm, exploit, lockers. So, among the 4 groups, two groups will work on the same definitions, which will additionally introduce an element of competition. The task is to present in the most creative and accurate way, graphically, the threats described above, which will be in the centre of the page, and around them on a brainstorming principle, write the key words they remember during the classes. Then each group will present their proposals and they will be discussed.

b) Second task:

It consists in arranging a crossword to the password, SECURITY, the most desirable will be passwords and questions matching thematically to the class area or concerning new technologies, threats that have been presented and possible security measures.

c) Third task:

Refers to the creation of chains of associations between two given words, one of which forms the beginning and the other the end of the chain. There must be a minimum of 3 words between them that will "link" the initial word and the final word.

Example: DESKTOP - VIRUS

DESKTOP, CURSOR, APPLICATION, INSTALLATION, UNKNOWN SOURCE, VIRUS

Other words:

1. MEADOW - TROJAN HORSE

2. THE WORM - LAPTOP

3. SPY - CURRENT

4. GAP - DOOR

5. TRAP - POLICE

QUIZ:

https://create.kahoot.it/share/malware/99898ed4-c329-44c8-96ab-73ff1d974c19?fbclid=IwAR1_2pzvPHbsxC_EyC_gV9eaXojuioq9ZsJUS0TUfWhXWXQ0FVBLSitGw5M

PHOTODOCUMENTATION

Activity 9

Cyber Communities

Cyber Communities:

- Forums
- Facebook Groups
- Websites

PROBLEM AND GOAL

As you know, the Internet is powerful force these days. When we talk about the Internet and other mass media, we can see their advantages. we can, among other things, both look for answers to questions and help solve them. It is also useful in our everyday life, making it much easier. It is worth remembering that the Internet and modern technologies, on the one hand, are helpful, provided that they have the skills and proper use of the flowing goods. On the other hand, irrational use may create various types of difficulties and have a negative impact on an individual's life.

Objectives of educational activities:
Main objective - to familiarise seniors with the topic of cyber-communities, i.e. virtual communities where they are or can be participants.
Specific objectives:

- To bring the topic of cyber communities closer together and to identify the benefits and dangers that can arise.
- To familiarise participants with the principles according to which cyber communities work.
- Identify and distinguish types of cyber communities.
- To present simple steps to find and join a cyber community.
- To find ways to prevent carelessness, such as manipulation and advertising in the use of social networks.

TIME ALLOWANCE

The whole duration of classes - 90 minutes:

- Organizational and preparation activities - 5 min.
- Introduction to the content of the workshop - 10 min.
- Work in groups - 10 min.
- Presentation of selected types of cyber communities - 10 min.
- Work in groups - 10 min.
- Individual work - 15 min.
- Work in groups - 10 min.
- Helpful rules of using cyber communities - 10 min.

- Summary - 10 min.

AID

- access to a computer with internet connection, projector
- flipchart, highlighters
- posters, notebooks, writing tools

NUMBER OF PARTICIPANTS

up to 15 people to facilitate communication during the class and divide the group during the performance of tasks into 3-member groups

ACTIVITY DESCRIPTION

I. Organizational and preparation activities

- Description: Welcoming participants, assigning computer stations, introducing
- themselves to the group
- Duration: 5 minutes
- Method of implementation: Discussion

II. Introduction to the content of the workshop

- Description: Explain the objective, the timetable and the expected length of the course to the participants. Preliminary definition of the subject of the activity, i.e. a general presentation of what cyber communities are and their selected types.
- Duration: 10 minutes
- Method of implementation: lecture

Cyber communities, that is, Internet communities - generally speaking, that are groups of people who create a virtual community that communicates through the Internet. They share common interests that take place on the Internet, and technological progress has allowed them to constantly develop their activities and explore new opportunities related to these interests.

Categorisation of Internet communities:

• Internet forums

• Chats

• Internet portals

• Social networking sites

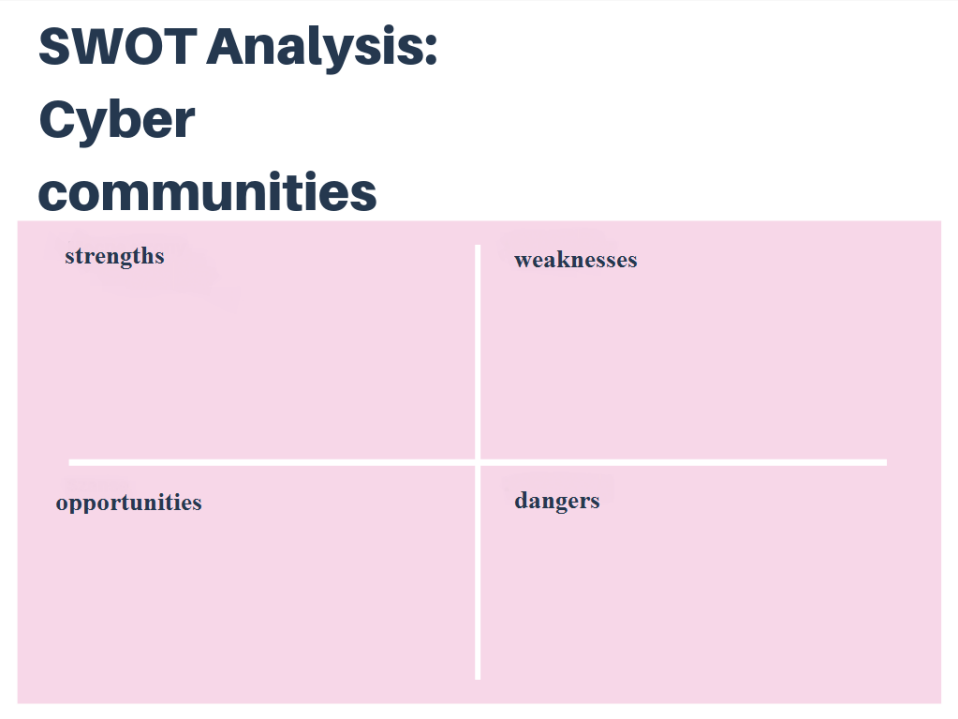
It is also worth remembering that nowadays almost everyone has access to the Internet, including the unlimited possibility of publishing. That is why it is always worth paying attention to what we learn from here, namely, to be rational with regard to the information coming to us from the Internet.

III. Workshop in groups – Activity 1

Description of the task: These days, the Internet has replaced the reality in which we live, almost everyone is a member of portals or social groups and discussion forums. This is an easy way to get the information we need. The task is to find out what advantages and disadvantages the participants see in the presence of cyber communities and in being a member of such a community, and what advantages and disadvantages this may have in the future. The educator asks questions that can help to guide the participants:

- Why are virtual communities so popular today?
- Why do you use them?
- What impact does this have on everyday life?
- Does the environment affect this and how?

The group is divided into 3-member subgroups, each group receives a printed sheet of paper to complete the task.



Once the task is completed, each group shares the results with the others.

• Duration: 10 minutes
• Method: SWOT analysis, discussion
• Materials: printed task sheets, notebooks, writing tools for the participants

IV. Presentation of selected types of cyber communities

- Description: A theoretical introduction to the types of online communities, their presentation and differentiation.
- Duration: 10 minutes
- Method: lecture

Internet forums - are a place for discussion on a selected topic for a specific group of people, they are used to exchange information, opinions, give advice or conduct conversations. A particular interest or topic forms the basis for participation in this type of online community. Therefore, the subject matter of the forums can be very specific or, conversely, very broad. Such Internet forums are created by Internet users, so anyone can create a similar social networking site. It should not be forgotten that each forum has its own specific rules, which you should stick to, because breaking the rules can lead to various types of warnings, for example, account blocking or other available options. In such forums, there is also a visible hierarchy, and its founders have assigned and specified responsibilities: the administrator of the forum is responsible for technical issues related to the Internet network, and the Moderator tracks if the topics discussed correspond to the topics of the forum, and if the users comply with the rules of procedure. We can distinguish various types of Internet forums depending on their structure:

- Anonymous forums - type of forums that do not require registration from users.
- Semi-anonymous forums - the type of forums in which the registration process is simplified, i.e. does not require confirmation of personal data, also allow for anonymous users.
- Restrictive forums - the type of forums that require registration by confirming identity, for example by sending a return e-mail.
- Private forums - a type of forum that has been created for a specific group of people and is available to people who receive invitations to join this type of forum.

1. **Groups on Facebook** - groups that provide a space for communication of people with similar interests in a social network, which is Facebook. Everyone who has an account in this network has the opportunity to create such a group with a selected theme. At this point, you become a group administrator and the Facebook helpdesk can help you to develop and modernize your group. The privacy settings available on Facebook also allow you to regulate who can see the group you created and who can join it.
2. **Social networking sites/websites** - another type of Internet information services, which is distinguished by its multi-functionality. Social networking sites include chats, discussion forums, news, weather forecast, links to other websites, search engines, e-mail services. Due to the fact that they have many functions at the same time, they are so popular among people with different interests, needs and goals. No wonder they are increasingly replacing real communication, storing and sharing memories, and sometimes even being a workplace. The most popular function of social networks is to search for and obtain information, which on the

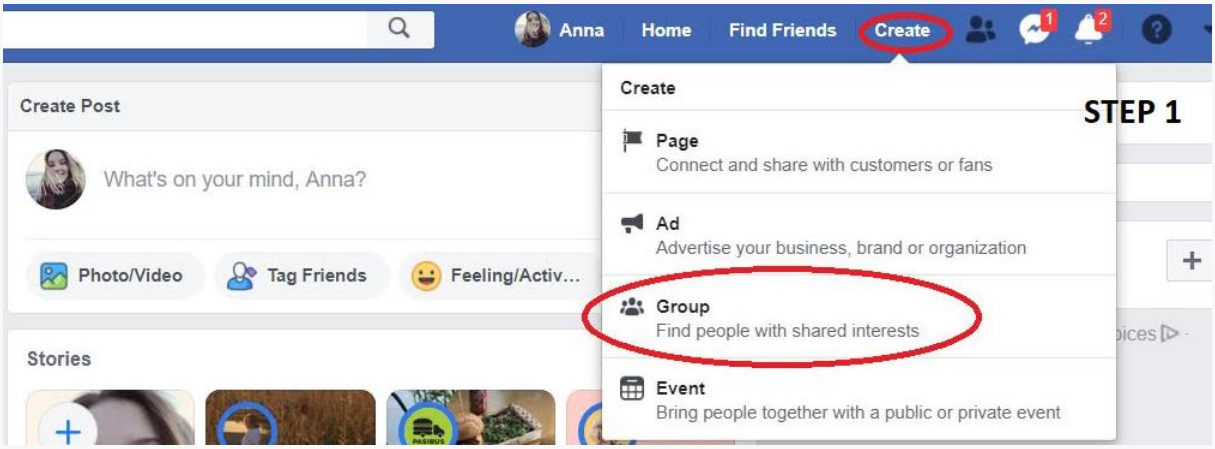
one hand can be helpful in everyday life. On the other hand, in case of irrational use, they can create various types of difficulties and have a negative impact on an individual's life.

V. Workshops with group – Activity 2

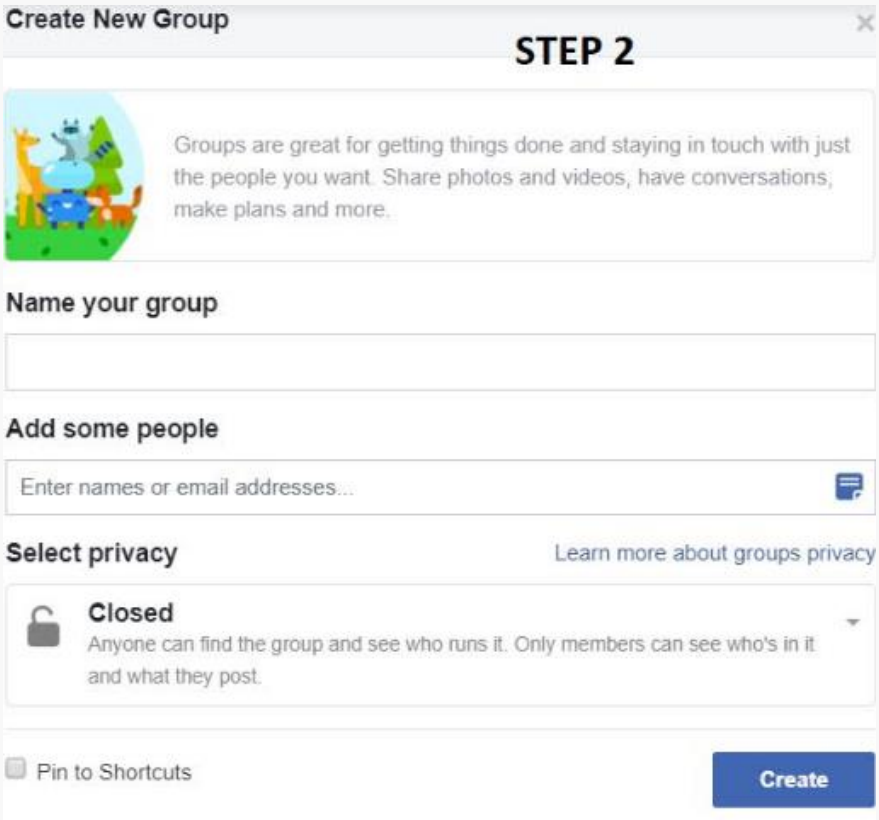
- Description of the task: The group is divided into 3-member groups, the task of the participants is to choose one Internet forum, which they think is useful and trustworthy, which may be of interest to other participants of the classes, each group should justify its choice. If there is access to the Internet, you can also show the public what the forum looks like, how it works, etc. The group should justify its choice. Each group shares its results.
- Duration: 10 minutes
- Method: working in groups, sharing good practices
- Materials: posters, writing tools

VI. Individual work – Activity 3

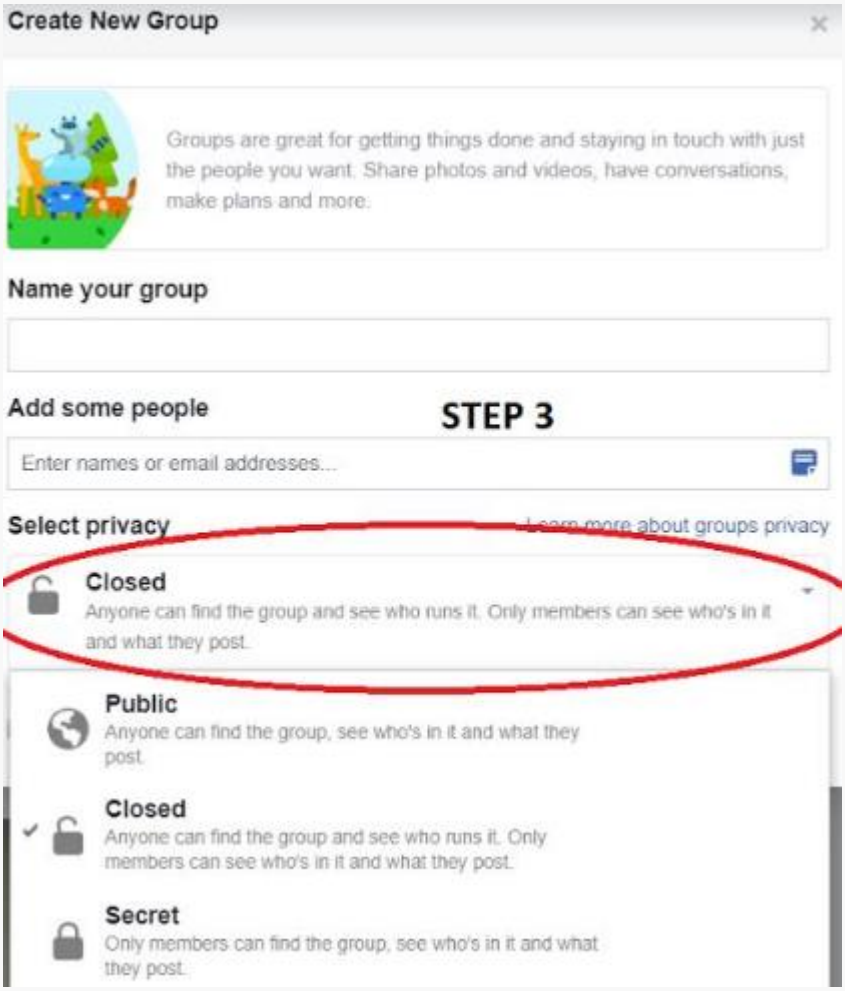
- Description: The task consists in creating a group according to your own interest on Facebook on the basis of a short tutorial that will be given to the participants. The aim of this task is to show how easy it is to create your own group and set it up. During the work, the educator should help the participants if any difficulties arise.
- Duration: 15 minutes
- Method: Workshop, individual work
- Materials: computer, Internet access, printed / displayed tutorials
- Tutorials:

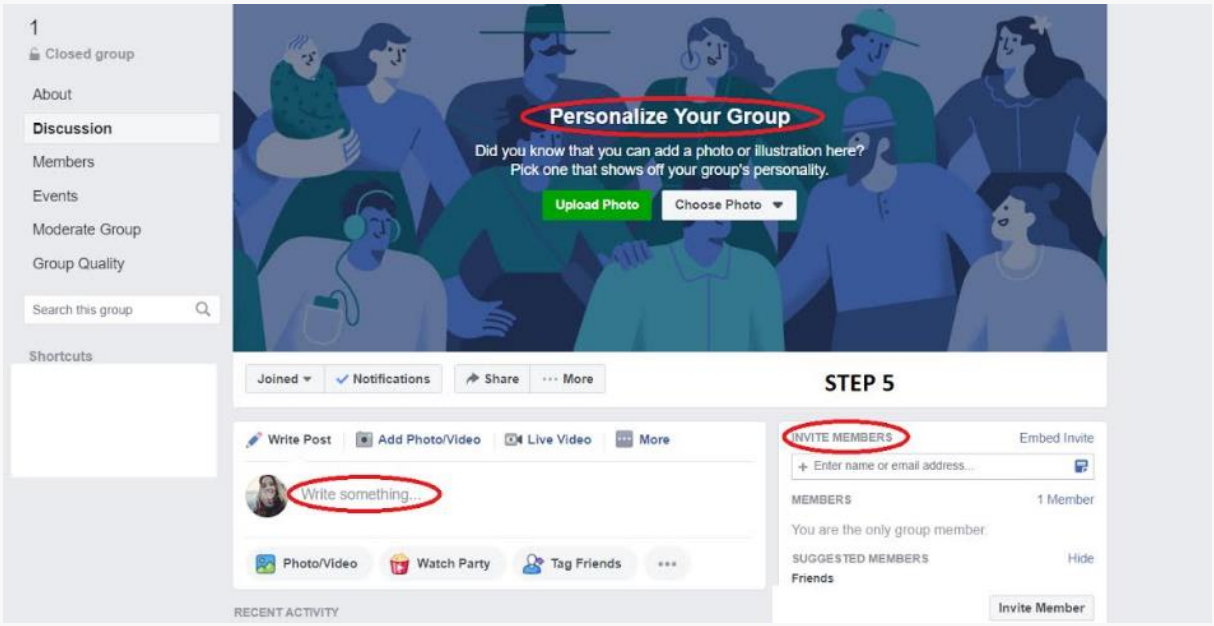
1. 

2.


Create New Group
STEP 2
Groups are great for getting things done and staying in touch with just the people you want. Share photos and videos, have conversations, make plans and more.
Name your group
Add some people
Enter names or email addresses...
Select privacy
Learn more about groups privacy
Closed
Anyone can find the group and see who runs it. Only members can see who's in it and what they post.
Pin to Shortcuts
Create

3.


Create New Group
Groups are great for getting things done and staying in touch with just the people you want. Share photos and videos, have conversations, make plans and more.
Name your group
Add some people
STEP 3
Enter names or email addresses...
Select privacy
Learn more about groups privacy
Closed
Anyone can find the group and see who runs it. Only members can see who's in it and what they post.
Public
Anyone can find the group, see who's in it and what they post.
Closed
Anyone can find the group and see who runs it. Only members can see who's in it and what they post.
Secret
Only members can find the group, see who's in it and what they post.

4. 

VII. Workshops in group - Activity 4.

- Task description: The task aims at increasing participants' awareness of the manipulation of the Internet, especially the manipulation with information. The educator should ask questions for the topic: Did any of the participants encounter manipulation on the Internet or an attempt to convince to any action by means of manipulation? Have they had contact with the dissemination of false information? What may be the consequences of this? When asking questions, it is also worthwhile to encourage the sharing of one's own experiences in this field. The next step should be to work together on tips that can help in the situation of encountering manipulation on the Internet, during a brainstorming session the educator writes down the ideas of the participants on Flipchart.
- Duration: 10 minutes
- Method: discussion, brainstorming
- Materials: Flipchart, markers
- The key:

- Be reasonable, sceptical, rational with regard to the information obtained on the Internet.

- Try to verify the information.

- Check more than one source.

- Do not disseminate false information.

- Do not forget about possible attempts to defraud information.

- Do not accept invitations to groups you don't know.

- Send a report about an attempt to falsify information.

VIII. Helpful rules of using cyber communities – Activity 5.

- Task description: introducing participants to the topic of netiquette, i.e. short rules on how to behave in the Internet community. The task is to get acquainted with a set of these rules together. The educator displays/distributes a printed set of rules. Once you have familiarized yourself with it, you will have a joint discussion about it. The educator can also ask the participants which principles they think are most important and why.
- Duration: 10 minutes
- Method: discussion
- Materials: computer, projector/printed materials

Pic. 1.7 *Netiquette*
Source: own study

IX. Summary of the lesson

- Description: Summary of the activities, sharing conclusions and own experience with Cyber communities, asking questions and answering questions. Feedback from participants.
- Duration: 10 minutes
- Method: discussion

QUIZ:

https://quizizz.com/admin/quiz/5d67c5645951f1001aae9e75

PHOTODOCUMENTATION

Bibliography

1. Dakpa, T., Augustine, P. (2017). *Study of Phishing Attacks and Preventions. International Journal of Computer Applications 163* (2)., Bangalore: Christ University, Department of Computer Science.
2. Wrzos W. (2014), *Bezpieczny Internet Krok Po Kroku*, CafeSenior.pl

Netografia:

1. https://www.avast.com/pl-pl/c-malware
2. https://www.avast.com/pl-pl/c-exploits
3. https://blog.avast.com/pl/przewodnik-ransomware-typy-z%C5%82osliwego-oprogramowania-i-atakow

Sinergia

ITALY PART

ACTIVITIES

10. GDPR

11. Instagram

12. Games

13. Internet frauds

14. E: mail

Activity 10

GDPR

The General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). The GDPR aims primarily at giving control to individuals over their personal data and at simplifying the regulatory environment for international business by unifying the regulation within the EU. Controllers of personal data must put in place appropriate technical and organisational measures in order to implement the data protection principles. Business processes that handle personal data must be designed and built with consideration of the principles and must provide safeguards to protect data (for example, using pseudonymization or full anonymization where appropriate), and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit, informed consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the regulation, or unless the data controller or processor has received an unambiguous and individualized affirmation of consent from the data subject.

This activity aims at providing a broad knowledge on the subject to understand the main notions and updates on privacy and personal data protection. The actual acquisition of knowledge passes through the verification of the explained concepts using a theoretical test. A kahoot questionnaire will be used to test the knowledge of the participants regarding privacy and personal data processing and thus to understand the established rules, so the learning process becomes simple and interactive.

PROBLEM AND GOAL

The participants will test their knowledge dealing with new privacy and personal data processing. Through a kahoot questionnaire the learning process becomes simple and interactive.

TIME ALLOWANCE

2 hours: 30 minutes for explanations about GDPR- 20 minutes for the Kahoot Quiz – 20 minutes for the discussion in the group.

AID

Internet, video projector
Video tutorial on kahoot https://youtu.be/7XzfWHdDS9Q
GDPR: What Is It and How Might It Affect You?
https://www.youtube.com/watch?v=j6wwBqfSk-o

NUMBER OF PARTICIPANTS

Between 10 and 15 participants.

ACTIVITY DESCRIPTION

Activity Start

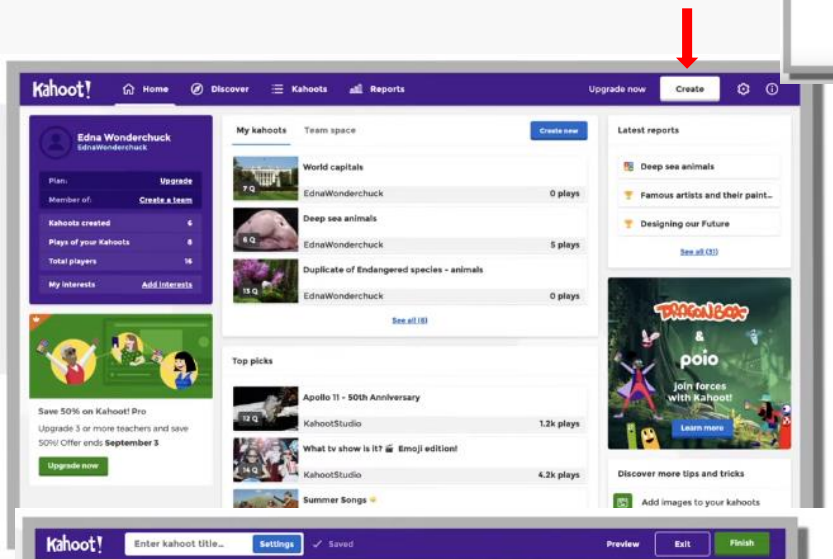
The activity consists of two complementary parts: a test and a theoretical focus. Both analysing on a theoretical level the main notions about the GDPR and filling in a kahoot questionnaire the participant will improve their knowledge on the European regulation on the processing of personal data.

1st STEP - 30 minutes

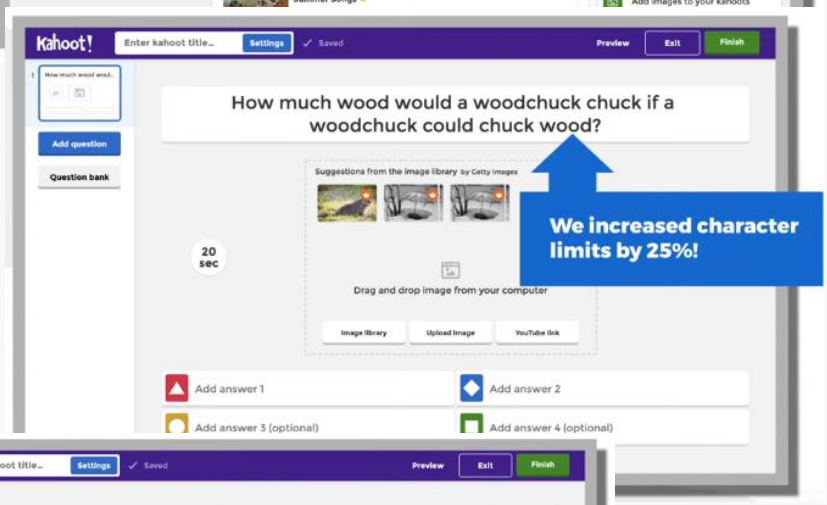
In the first part the trainer will explain the main changes regarding the protection of personal data, with reference to the GDPR. This part of the activity includes a video: GDPR: What Is It and How Might It Affect You? https://www.youtube.com/watch?v=j6wwBqfSk-o

The main points of the investigation will be:
- the implementation of the GDPR
- news on the deadlines and duties of companies
- user´s rights
- fines and penalties for violations

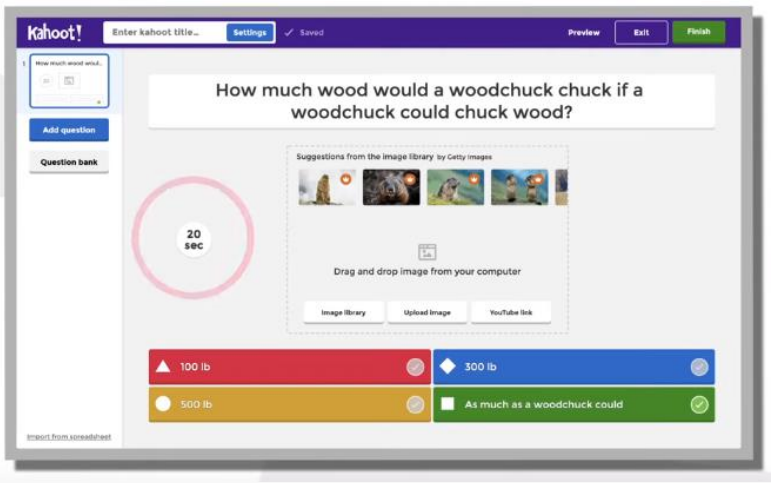
How to create a Kahoot



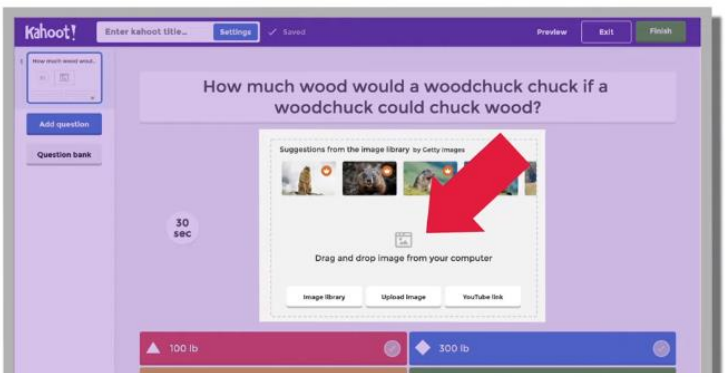
Click the CREATE button.



Input your first question.
Add answer alternatives and mark the correct answer (s).

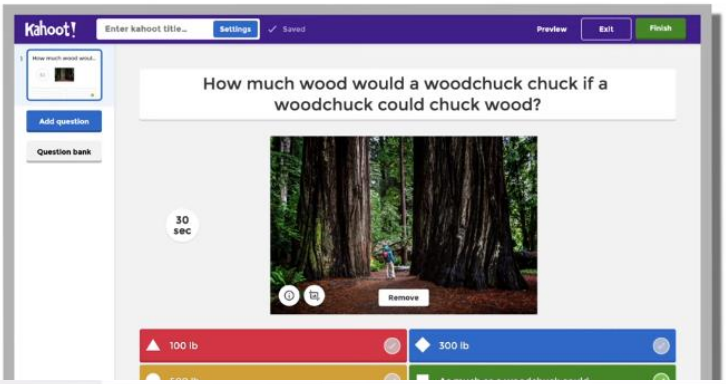


Tune the timer, depending on the question's complexity.

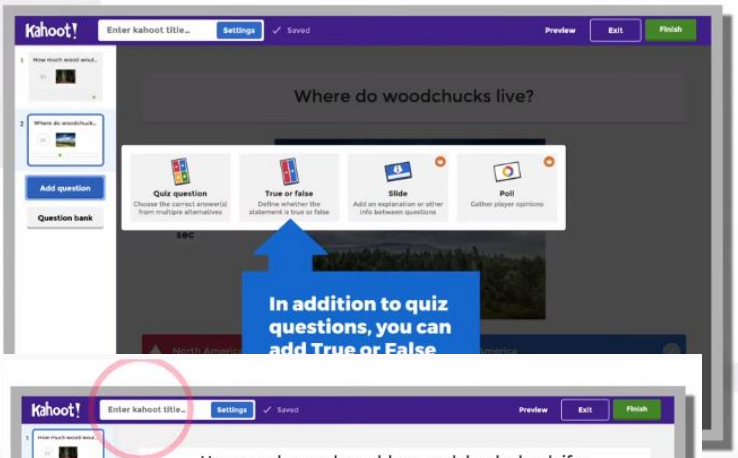


Do not forget to add an image or video!

You can drag and drop from your computer or choose one from our image library.



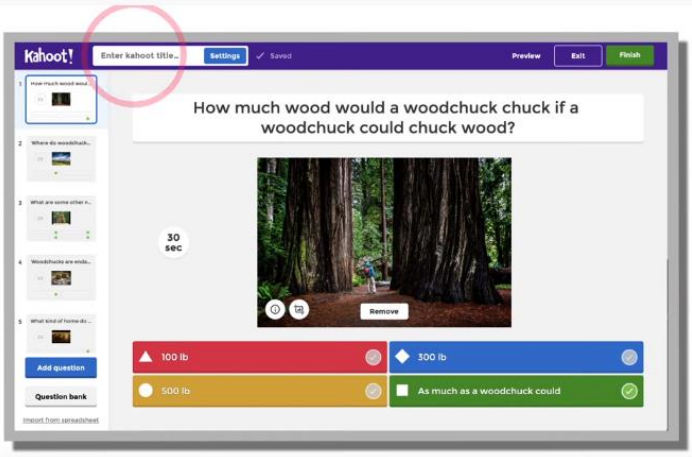
Add the next question from the left-hand side



In addition to quiz questions, you can add True or False question ...

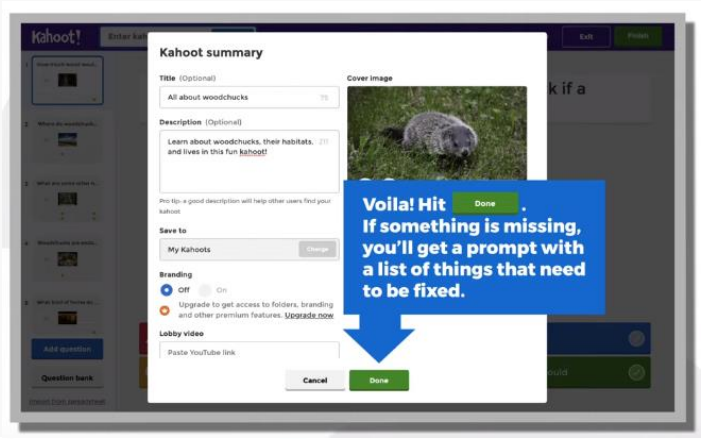
... Slides to introduce a topic or give more context ...

... and Polls to gather feedback.

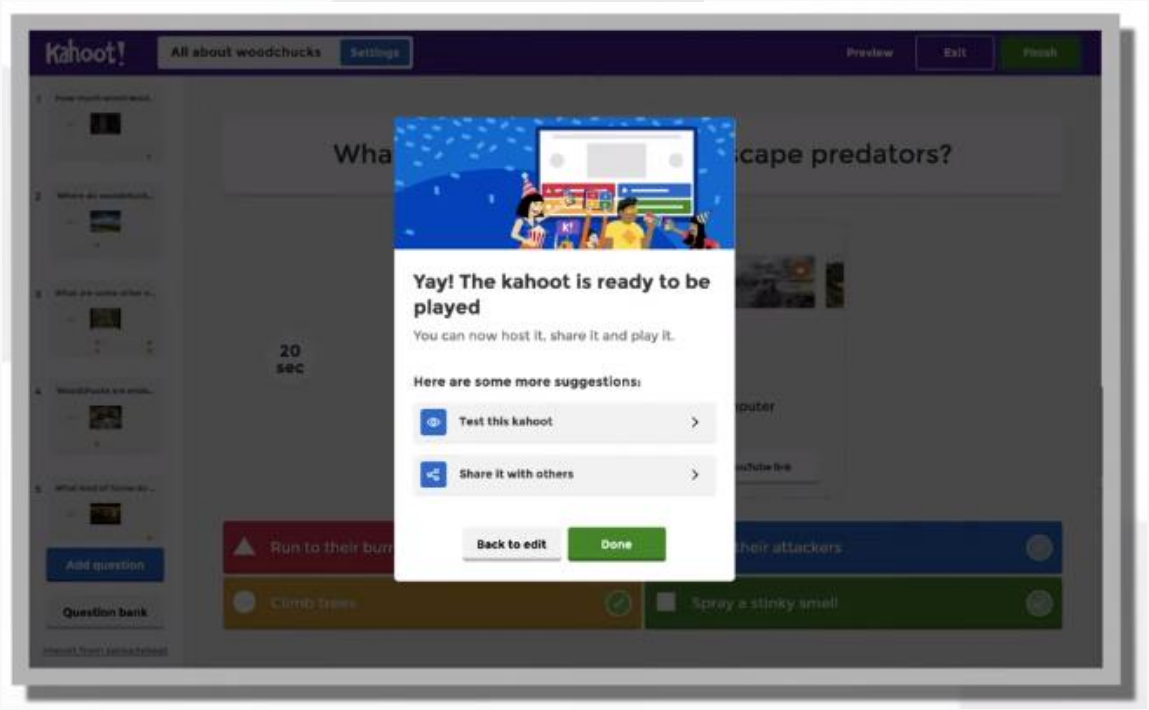


Type a nice catchy title for your kahoot.

Add a description so others can find and play your kahoot. Choose a folder for saving you kahoot and select who you'd like the kahoot to be visible to.



Hit DONE. If something is missing, you will get a prompt with a list of things that need to be fixed.



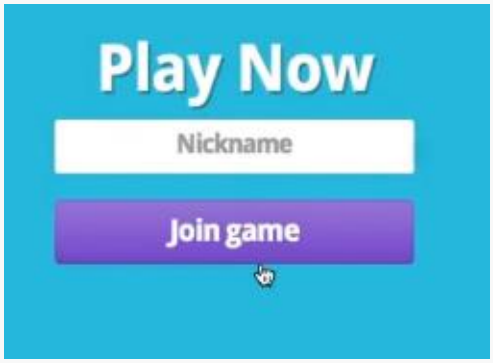
2- STEP

SENIOR TASK- the participants compile a kahoot questionnaire on the notions just learned, to directly verify the understanding of the lesson- 20 minutes

The Kahoot quiz is: GDPR HOW MUCH DO YOU KNOW ABOUT IT? On https://kahoot.com/

How to play in Kahoot

When the teacher launches the quiz, the application generates a code that communicates to the learners and will allow them to access through the following site: https://kahoot.it. Once the code and name have been entered, the student will have to wait until all the participants have carried out the same operations.



Once the participants have been inserted, the teacher starts the quiz by clicking on the "Start" button.

3- STEP

Questions for discussion in group – 20 minutes

1) What was the difficulty level of the quiz?
2) Which were your mistakes?
3) Did you understand the main notions about GDPR? Can you remember them after the lesson?
4) Was the quiz useful to fix the information?

EXPERIENCE AND PRACTICE

Participants are required to have basic computer skills:
computer use and internet browsing.
Participants will have to install the Kahoot app on their devices to participate in the activity.

PHOTODOCUMENTATION

Activity 11

INSTAGRAM

PROBLEM AND GOAL

Instagram is a photo and video-sharing social networking service, the app allows its users to upload photos and videos to the service, which can be edited with various filters and organized with hashtags. Searching for hashtag will yield each message that has been tagged with it. A hashtag archive is collected in a single stream under the same hashtag, it allows users to find the posts that have been tagged using that hashtag. An account's posts can be shared publicly, or Users can set their account as "private", thereby requiring that they approve any new follower requests. Users can browse other users' content by tags and locations, and view trending content. Users can "like" photos and follow other users to add their content to a feed. Recently Instagram has launched Instagram Stories, a feature that allows users to take photos, add effects and layers, and add them to their Instagram story, they expire after 24 hours. The service also provides messaging and shopping services. Introduced in August 2016, the Instagram Stories are certainly the characteristics that most of all have changed the fortunes of the social media, opening even more the way to videos and making users grow rapidly. In June 2017 there were 250 million, while 12 months after 400 million.

The activity conceived for the use of the social network Instagram regards the creation of a story, that is the new function added in the app, and also one of the most popular social media tools. The IG story is a content added by the user to his/her account during only 24 hours, then it is automatically deleted and remains in a private archive. During the 24 hours the story is visible to all contacts connected to the user who created it; it can be a photo, a video, a song or a text. Participants will be involved in the

creation of Instagram stories to understand their sharing and functioning, in order to use the social network in a complete and updated way.

The activity involves the creation of Instagram stories and the sharing of content through this new function of the app. It allows the user to understand how to manage reactions to the added content and user views.

TIME ALLOWANCE

1 hour: 30 minutes for activity start and tutorial – 25 minutes for the task

AID

Internet, video projector
Video tutorial: https://www.youtube.com/watch?v=y_u3riCirmo

NUMBER OF PARTICIPANTS

Between 10 and 15 participants.

ACTIVITY DESCRIPTION

Activity Start
To make the best use of the social network, users will explore one of the most popular features: IG STORIES.
During the activity participants will first watch a video tutorial explaining how to add an Instagram story https://www.youtube.com/watch?v=y_u3riCirmo and then they will try to make it individually. Then they also will learn to interact with the contents of other users, such as adding reactions, managing views and responding to stories.

Task for senior- Create an Instagram Story – 20/25 minutes

Instagram Stories appear in top bars of your feed - and all accounts Instagram will be able to share stories from everyone. When there is something new to see, their profile photo will be trimmed by a colour ring.
How to make Instagram Stories
To create a story on Instagram, you have to tap a new "+" icon at the top left-hand corner of the screen, or you can reveal the story camera by simply swiping left. Now you can take a photo or record a video, just as you would normally on Instagram. After you've recorded your video or taken a photo, you can use a range of filters and also add text and drawings to your content.
Views
Once your story is posted you can also view some basic analytics, to show you how many times each post in your story has been viewed and who has viewed it. When watching your own story, swipe up to check out this data and who's seen each photo and video.

Privacy

Your story follows the privacy settings of your account. If you set your account to private, your story is visible only to your followers. However, you can also easily hide your entire story from anyone you don't want to see it, even if they follow you.

EXPERIENCE AND PRACTICE

The participants are required to have basic competency in the use of smartphones, in particular to take a picture and save it in the private archive.

PHOTODOCUMENTATION

Activity 12

GAMES

PROBLEM AND GOAL

On the Internet, you can find the most popular games provided for free. The users can thus create an account and meet other passionate users playing from all over the world. The web offers a wide range of games: creative games, quizzes, games for children, card games, interactive games, group games. A user can register and participate in challenges and worldwide tournaments, and some sites offer a common chat service where chatting during the match.

This activity aims to introduce users to the entertainment opportunities available on the net, and in particular the possibility of participating in online games in a safe and shared way with their contacts So the participants will learn to register through an online account which requires a username and a password. Users will learn to recognize sites for legal and certified web games. Moreover, they will discover how to meet users interested in participating in a challenge and tournaments, all of this without any risk.

Participants will understand how to recognize a certified online game and how to participate in a safe gamers' community.

TIME ALLOWANCE

1 hour- 20 minutes for activity start and lesson- 30 minutes for the discussion in group – 15 minutes for the task.

AID

Internet, Video projector
Video Tutorial for Solitaire game https://www.youtube.com/watch?v=j38BhamLdNI

NUMBER OF PARTICIPANTS

Among 10 participants.

ACTIVITY DESCRIPTION

Lots of people play games online. Games can be played on consoles and computers, mobile apps, websites. There are many types of online games. Some of them are simple and you can play them on your own like the games, other games are multiplayer games with 2 or more people you might not know.

You can also talk to people through the game itself, a console network, chat site or gaming forum. You can talk through an instant messenger, a headset or video chat. Some people like to watch other gamers playing on live-streaming sites.
Games are a great way to relax and have fun. But it is important to be careful about what you share online and keep yourself safe. People may bully you in games by saying nasty things; stealing or destroying your online items; stealing your identity or sharing your personal information and hacking your account. Some people may use games to build relationships with young people and trick them into sexual activities. Groomers can behave differently. They may talk to a person in the game or ask him/her to talk privately on chat sites such as Skype. They could ask to send sexual pictures or contents. It is crucially important to avoid and report these episodes.

Questions for discussion in group - 30 minutes

1) Do you usually play with online games? Which one do you know?

2) Have ever experienced online grooming or bullying?
3) How would you behave in these cases?
4) Do you feel safe in chatting within online community gamers?

Task for Seniors- Register and play on an online game community – 20 minutes

How to register on a safe online game and how to interact with gamers.

Video Tutorial for Solitaire game https://www.youtube.com/watch?v=j38BhamLdNI

EXPERIENCE AND PRACTICE

The participants are required to have basic computer skills: surfing the net and searching on a search engine.

PHOTODOCUMENTATION

Activity 13

INTERNET FRAUDS

PROBLEM AND GOAL

Internet fraud is a type of fraud or deception which makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace. The most popular types of frauds involve: Online automotive fraud, charity fraud, Internet ticket fraud, gambling fraud and online gift card fraud. Email scams are often called "phishing". This term, which is derived from fishing, means "fishing" and refers to the technique with which the scammer sends mass e-mails to all the addresses he was able to obtain, in a more or less legitimate way, with the hope that at least some recipients are credulous enough to respond - and send money or personal details.

This activity aims to create awareness among the users about the topic of internet frauds, they can take on various appearances, so they are often difficult to be recognized. By creating fraud prototypes, participants will learn how to recognize the illegal message and so how to avoid falling into traps. The identification of a fraud is the main step that users must take to ensure a safe navigation on the Internet.

TIME ALLOWANCE

2 hours: 45 minutes for introduction and explanations- 20 minutes for the task – 30 minutes for the discussion in group

AID

Internet, computers

NUMBER OF PARTICIPANTS

Max 15 participants.

ACTIVITY DESCRIPTION

The participants will test their skills in recognizing and avoiding dangerous messages and situations, by trying to find the fraud among various emails and then they will make an analysis of the problem they faced, sharing the information with the group.

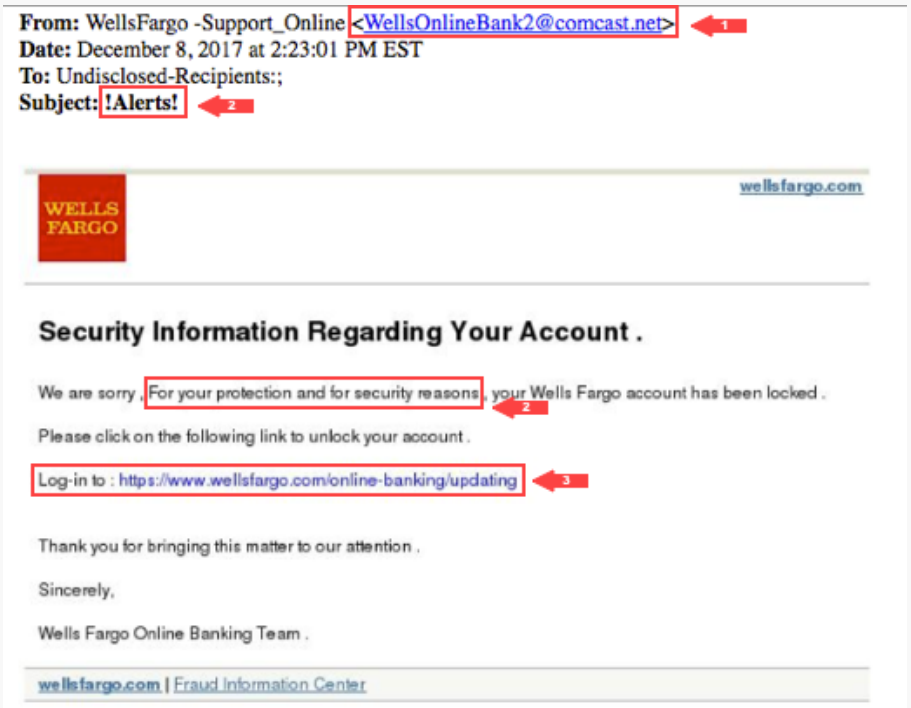
Activity Start

E-mail frauds can take different forms that are difficult to recognize. The objectives may vary as follows:

1) to obtain access to information through deception, convincing someone to enter their personal data on a particular site, such as that of their bank or e-mail account
2) to deceive the victim to convince him/her to send money to the scammer
Many of these scams try to direct you to a fraudulent website. Browsers that support Safe Browsing like Google Chrome, Apple Safari or Mozilla Firefox can usually alert the user if they are going to be directed to a known fraud site. Safe Browsing, however, concerns only the activity carried out on the web and is not able to protect the security of a particular e-mail received.
Task for seniors: to recognize the nature of the fraud among the emails received by a user- 20/25 minutes

ANALYSIS OF A FRAUDULENT E-MAIL

- Unknown sender
- Suspicious subject
- typos or grammar errors
- requests for money or personal information
- unsafe links for access



Questions for discussion and clarification – 30 minutes in group

1) Do you know the sender of the e-mail? Can you find safe information about him/her?
2) Did you find typos or grammar errors?
3) Did you find any requests for money or personal information?
4) Are you able to recognize a fraud?

EXPERIENCE AND PRACTICE

The participants are required to be familiar with the electronic mailbox: to receive and send emails from a personal account.

PHOTODOCUMENTATION

Activity 14

SECURE GMAIL

PROBLEM AND GOAL

Gmail is a free email service developed by Google. Google's mail servers automatically scan emails for multiple purposes, including to filter spam and malware, and to add context-sensitive advertisements next to emails. Through a Gmail account you can access to a wide range of Google products and tools. After a Google Account is created, the owner can selectively enable or disable various Google applications for computers, tablets or smartphones.

Not long ago, Google reported that the platform had passed a billion active users. Now the email service, still steady on its path to world domination, has announced on Twitter that it has accumulated another 500 million users, totalling 1.5 billion. The activity aims at providing greater knowledge and skills in the use of Google services. It deals with the main features of the Gmail account, to make the participants know some of the most important services linked to Gmail, such as downloading applications from the store and using google drive as free file storage. Through a practical exercise the participants will be able to put into practice the acquired knowledge.

TIME ALLOWANCE

1 hour

AID

Internet

NUMBER OF PARTICIPANTS

Between 10 and 15 participants, divided in 3-4 groups.

ACTIVITY DESCRIPTION

In the activity, the participants try to create a google account through an email to access Google Drive and Store services.

Start of the Activity

A Google account lest you use Google Drive: a file storage and synchronization service developed by Google. It offers apps with offline capabilities for computers, smartphones and tablets, like an office suite that permits collaborative editing of documents, presentations, drawings and more. Files created and edited through the office suite are saved in Google Drive.

Task for Seniors: Create a Google Mail Account – 30 minutes

To create your Google Account Identity

1- you can choose “Use my current email address instead” option if you want to use your own mail or “create a Gmail account” option if you want to create a new google account.

2 – Complete all the details requested.

3 – You will receive an email with a verification code on your entered email account, you will need to use this code on the following screen, once entered click on “Verify”.

4– On the following step you will be requested to enter a mobile phone number (optional), your birth date details and your gender. These details will help you recover access to your account in case you forget your password.

Note: If you enter your mobile phone number on the following step you will be asked if you want to verify it, we recommend you do this, an SMS will be sent to your mobile with a code which then you have to enter it on the screen to continue the setup of your Google Account.

5 – Then you will be asked to accept the privacy and terms. Once you are ready click on the two checkboxes at the bottom of the screen (you need to scroll down) and click on the “Create Account” button.

6 – Re-confirm your account creation by clicking “Confirm”.

Once your account has been created, you can let your colleagues or friends share Google Drive documents with the email account they already know. To access files shared with you over Google Drive, go to https://drive.google.com to access them. You will also be able to create Google Drive Docs, Sheets, Slides and more with your new Google Account.

To change any details or if you need to login to your Google Account you can do so by entering to the following link: https://myaccount.google.com

Task for Seniors: what you can do with a Google Mail Account – 40 minutes

- Create and send emails
- Organize your inbox
- Find emails
- Create signatures
- Access to your calendar, notes and tasks

You don't know how to do it?

No problem, check the guide at https://support.google.com/a/users/answer/9297685?hl=en

EXPERIENCE AND PRACTICE

The participants are required to have basic computer skills.
They should be able to use a smartphone with Internet access.

ALVIT

CZECH PART

ACTIVITIES

15. Ways how to manipulate pictures

16. Fake News

Activity 15

WAYS HOW TO MANIPULATE PICTURES

PROBLEM AND GOAL

People 50+ are often afraid of computers, Internet and the digital world. They are not aware of the fact that using a computer and the Internet may facilitate solving problems or dealing with matters in their everyday life. It is important to educate the elderly people that the use of modern technology can improve the quality of their lives, although It is also essential to make them aware that the Internet is a good tool, but they should also be aware of its dangers.

Nowadays, a photo is the first thing which people notice while looking at articles or websites. It is not complicated to take a picture or transform it the way it is needed. Photo manipulation is a popular method made by transforming a picture to achieve desired or needed results (like drawing attention) by using various methods. There are two popular ways of photo manipulation:

1. When a photographer takes a picture, he/she chooses the most sensational or shocking moment.
2. After a photographer takes a picture, he/she edits it using a graphic design tool to make the captured matter to be considered in a different way.

Photo manipulation is a method to show the participants how pictures can be manipulated and how to not be fooled by them.

Participants will learn:

- how easy the picture can be manipulated?
- how changing the perspective of taking picture can change the meaning

- how to be more careful and not to be fooled while looking at the pictures
- how to verify and check where the picture they look for appears on the web

TIME ALLOWANCE

4 x 45 minutes

AID

Equipment and materials needed:

- projector
- Internet
- selected pictures and video
- sheets of paper

NUMBER OF PARTICIPANTS

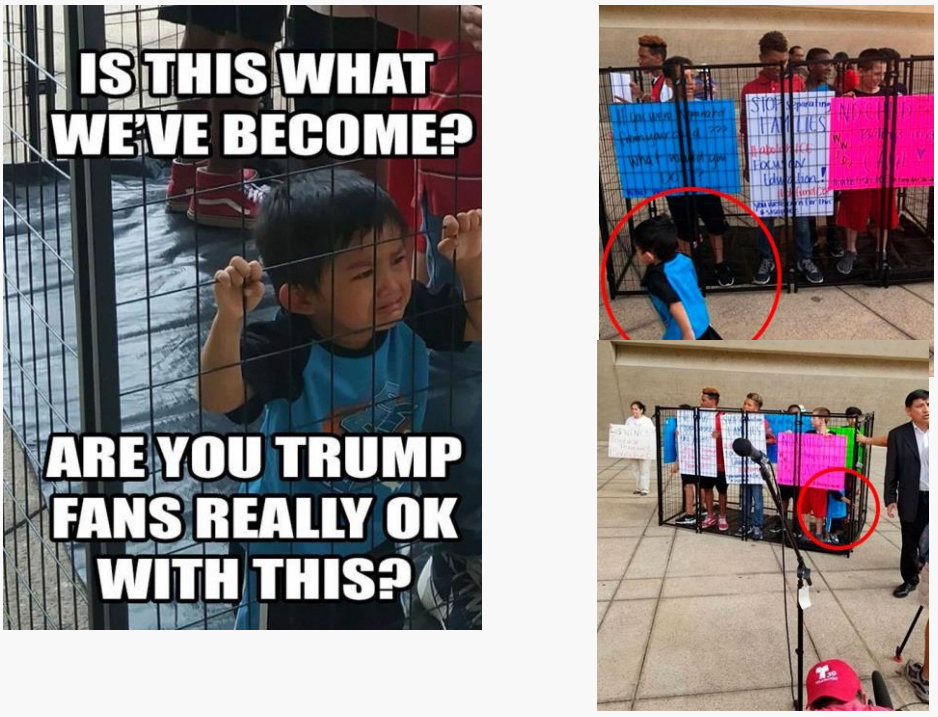
4 - 20 participants

FIRST EXERCISE: FOR THE BEGINNERS

1. Before the lesson the teacher should prepare some pictures which can be considered as manipulated.

Examples:

[Example 1. These images show Theresa May's campaign in Northumberland and Hillary Clinton's event in Omaha. Images downloaded from https://www.boredpanda.com/examples-media-truth-manipulation/?utm_source=google&utm_medium=organic&utm_campaign=organic in June 2019.]



[Example 2. These images show a pro-immigration protest. Images downloaded from https://www.boredpanda.com/examples-media-truth-manipulation/?utm_source=google&utm_medium=organic&utm_campaign=organic in June 2019.]

2. He/she shows the selected pictures. If the matter was captured from two perspectives, he/she shows the first perspective at first. Then he/she asks the following questions:

1. **What can you see in the picture?**
2. **What is the situation like?**
3. **What do you feel about this situation?**

3. He/she shows the pictures of the same thing, but from another perspective and asks the following questions:

4. **What can you see in the picture?**
5. **What is the situation like?**
6. **Have your feelings changed after seeing the second picture/another perspective?**

4. At the end, the teacher should sum up the answers and feelings of participants. If it is needed, it is useful to add a comment or an explanation to the pictures.

SECOND EXERCISE: FOR MORE EXPERIENCED PARTICIPANTS

1. The teacher divides the participants into four groups of approximately the same number of participants. Two groups get the first set of images, the other two groups - the second set. Both sets show the same issues taken from different perspectives. The groups should not see images of others.

Examples:

[Example 3. These images show Hillary Clinton's event in Omaha. Images downloaded from https://www.boredpanda.com/examples-media-truth-manipulation/?utm_source=google&utm_medium=organic&utm_campaign=organic in June 2019.]

[Example 4. These images show photographers covered the conflict between Israeli soldiers and Palestinian youths. The picture was staged in cooperation with a young Palestinian. Images downloaded from https://www.boredpanda.com/examples-media-truth-manipulation/?utm_source=google&utm_medium=organic&utm_campaign=organic in June 2019.]

Hypocrisy from the Royal Court. This is insolent. Ugh.

[Example 5. These images show Prince William after the birth of his third child. Images downloaded from

https://www.boredpanda.com/examples-media-truth-manipulation/?utm_source=google&utm_medium=organic&utm_campaign=organic in June 2019.]

2. The teacher asks the participants to look at the pictures and answer the following questions:

1. **Describe the reality in the pictures as accurately as possible.**
2. **How does it make you feel?**
3. **How many people are there in the picture?**
4. **Is the captured situation dangerous?**

3. After the discussion, each group shows the pictures and compares them with the others. The teacher asks what they learned about the manipulation. It is important to mention that the opinion of the situation is also appropriately and intentionally manipulated by the text of the report.

4. The answers given by the participants can be written as rules on a large sheet of paper. This way they prepare a poster with the most essentials of photo verification.

THIRD EXERCISE: FOR MORE EXPERIENCED PARTICIPANTS

1. If the participants are more experienced, the teacher can do more complicated exercises with them.

2. He/she asks the participants to open the website with the news they like and find some pictures to save them and the information/news they were published with.

3. The participants can start with answering the following questions:

1. **Are you looking at the original version?**
2. **Do you know who captured the content?**
3. **Do you know where, when and why they captured the content?**

4. After answering and downloading, the teacher asks the participants to open one of two websites, *Google Images* (https://images.google.com/) or *TinEye* (https://www.tineye.com/), and to check the picture(s) they selected by using the image search engine. Results will show all articles and posts on the Internet where the picture was used in the past.

5. The participants can find out where the picture was published before and what other resources mention it. This is the way how they can verify the reliability of the selected pictures.

6. They write down all the information they have found and present the way the selected picture(s) appear on the websites.

FOURTH EXERCISE: FOR MORE EXPERIENCED PARTICIPANTS

1. The teacher plays the selected video (ex. https://www.youtube.com/watch?v=07XqF3HKl_o&t=2s; preferably without sound if the participants are Czech).

2. After watching the video, the teacher asks everyone the following questions:

1. **What do you think happened in the video? Describe the reality as accurately as possible. I will also give you two possible explanations:**

a. Filming of the documentary film The Land of the Suffering Virgin which deals with the situation of Greek refugees from Asia Minor in 1922.

b. Staged filming of drowning refugees directed by a non-profit organization to get more funding for its activities.

2. Which one do you think will evoke more emotions? Which one is true, what and why people will rather believe?

3. The answers given by the participants can be written as rules on a large sheet of paper. This way they prepare a poster with the most essentials of video verification.

EXPERIENCE AND PRACTICE

The pictures selected by the teacher should not be obvious to recognized as a manipulation. The best way is to find the pictures which show the matter from at least two perspectives. The examples of the pictures are attached.

Activity 16

FAKE NEWS

PROBLEM AND GOAL

In daily use of the Internet, users meet much information. Especially the elderly people can be confused by all the information they find because the enormous amount of contents found on the Internet can be overwhelming. Very often they can feel lost and not sure which information is true or untrue. Surfing on the Internet they can find fake news which is a kind of false information, disinformation or hoax. It is necessary to explain the participants how they can recognize such information and protect themselves if it is needed. It is good to teach the seniors how to be skilled to find the answers on their own and not to be fooled by unverified information, hoaxes or fake news. They should always wonder if the information is true or manipulated.

Media literacy among seniors is the same as among the rest of the population, but it can lag behind a bit because of the use of technical terms and technologies: *applications, mobile phones, social networks.* The understanding of media, especially the media literacy is higher in case of younger generations than elderly people who are lagging behind in evaluating, judging communication intentions and imagining why someone sends a message to them. The elderly people used to be more familiar with the more traditional media environment. They experience the public service media, like television, radio or commercial media. It is more difficult for them to judge, because they enter the world of the Internet and they are not prepared to the fact that there are a lot of “actors” or ways of spreading false information. It is therefore important for seniors to show them a simple way and instructions of verifying the information, and this is exactly what this lesson offers.

Participants will learn:

- what the unverified information, hoaxes, fake news and resources are
- what is the scope of fake news, disinformation and jokes dissemination?
- how fast a joke or hoax can be considered as true information
- how the unverified or untrue information and jokes can hurt people's feelings
- how useful the resources can be for the participants?
- how to check if the information they found is true
- how not to be fooled by the false information, hoaxes, fake news

TIME ALLOWANCE

3 x 45 minutes

AID

Equipment and materials needed:

- laptops or tablets for groups
- access to the Internet
- projector

NUMBER OF PARTICIPANTS

3 - 10 participants

ACTIVITY DESCRIPTION

FIRST EXERCISE: FOR THE BEGINNERS

1. The teacher asks the participants about typical characteristics of hoaxes, for example: How can we identify a hoax or a false information? Answers should be written down on a blackboard. The first part of the exercise is the introduction of hoax recognition, the second exercise is focused on its verification.

2. After hearing all the answers, the following characteristics are essential and should appear on the board:

Hoaxes try to convince readers by using:

- **the importance of the information**: shocking information, new danger, urgent help, etc.
- **trusted sources which warn**: "FBI warns ...", "Microsoft warns...", "Health organization detected...", etc.

- **a leak of secret information** (the information that official media are silent about and it cannot be spoken about, but the author of the report invites readers to share)
- **a call for resending** (hoaxes always contain this attribute - it is a kind of driver for further distribution; many inexperienced users get the message and become fooled by it, then they trust the call without thinking and share it with others)

SECOND EXERCISE: FOR MORE EXPERIENCED PARTICIPANTS

1. The teacher asks how the information found by the participants can be verified. Again he/she writes down the answers on the blackboard. Then he/she presents the following theory:

a. Who published the report? From whom did I receive it?

1. Decide if the author is reliable. Do not trust the websites which contain misinformation, conspiracy theories, hoaxes, etc. Do not consider them as a credible source. Especially be careful with the information which appear on disinformation websites (check the list of disinformation websites). This information or articles may not be fully fake, they may contain the true basis, but the additional information is false, put in the wrong context, or linked to unreliable source. Finally, always verify if the message does not come from a strictly humorous website.
2. I have received a message from a friend: I have to think over if this person sends this type of messages frequently or exceptionally.

b. Anonymous source and unreal authorities

1. You should not pay attention to articles or information without a source given - this may contain false or misleading information. At the same time, we can experience situations where the message is signed by a non-existing author or by a non-existent authority – e.g. scientists, celebrities, etc. On the Internet, messages referring to the opinion of a recognized (often non-living) authority or to a public service medium (ex. Czech Radio) can be found very often. In this case, it is also necessary to be cautious and try to verify whether the information found is not misinformation.

c. Data verification (Hoaxes databases)

1. It is very important to verify whether the message is not just a hoax which could have been already fully analysed. We have many specialized databases to check this information:

   SNOPES.COM - Urban Legends Reference Pages

   URBANLEGENDS.ABOUT.COM - Urban Legends and Folklore

   TU-Berlin - Hoax Info Service

   HOAXBUSTER.COM

* The teacher should know the list of the websites of his/her own country (the Czech ones include www.hoax.cz, www.manipulatori.cz).

d. Photo and video verification

1. The photo can be verified by using a reverse search, such as the one provided by Google (https://www.google.com/imghp?hl=en) or TinEye (https://www.tineye.com/). The additional tool to detect a photo manipulation can be FotoForensics (http://fotoforensics.com/)
2. In order to verify videos, you must search for the original video by using the keywords that match to the video content, or by the video content file name. The Citizen Evidence (https://citizenevidence.amnestyusa.org/) tool from Amnesty International can check the authenticity of a video on YouTube.
   * The lecturer always presents the search method using both ways.

2. After presenting the theory the teacher presents a sample report analysis to the participants, so they learn the way how to analyse the content they have found. Firstly, the teacher shows the picture of Facebook post using the projector.

Report: Refugees in the Prague subway

Situation: Facebook post: "Look what Bob has sent me. Photos from the metro in Prague, 9th October 2017. Long live multiculturalism! "

[Example 6. This image shows a Facebook post. Image downloaded from http://www.e-bezpeci.cz/index.php/ukazky-analyz/uprchlici-v-prazskem-metru in August 2019.]

3. Secondly, the teacher reads the first part of report to familiarize the participants with the situation.

This report contains the text including the information that the photos were taken in October 2017 in the Prague metro, followed by a collage of 3 photos. The first photo shows a Muslim praying in public transport, the second shows a dark-skinned man urinating in the subway, and the third is a sleeping black man surrounded by mess. The combination of these photographs and a suggestive text evoke strong negative emotions in readers. Now let's make a simple analysis and try to find out if it is a true report or fake news. The source of information is Bob who is not a press office or an agency himself to verify the information and confirm its reliability - it is simply Bob. The manipulated reports use this method of referencing quite often - besides first names, they usually use: my friend told me, my friend experienced it, today I experienced this situation myself, the shop assistant told me, it happened to my friend, etc. In the next step we verify if the text matches to the photos. At first glance it seems we can see the Czech public transport - bus, metro and train. The text therefore does not correspond to the content of the photos after a more detailed examination.

4. The teacher asks if the participants understand the information from the report and if they have any questions. After he continues reading:

The next step is the reverse image analysis - in other words - via some of the web services we try to find out the source of the photo, and on which websites the photo has appeared until now. We use a simple service which allows you to search by photos – it is Google Images. The problem may appear if we tried to analyse a collage which contains multiple photos - the reverse search service will probably only reveal the sources for 1 image, even though there are more than one. In the case of collages, I recommend that you “cut” the picture into separate photographs and then search for them separately. Let's try how to do it.

5. The teacher shows the participant the way of verifying the pictures from this collage. He/she should have the laptop and projector to show the exercise step by step.

1. In order to get more accurate results, we first cut the collage. You can use any graphic editor for cutting.
2. After entering the first cut (the Muslim prayer) to search Google Images instantly reveal the original source image. There are several websites, some of which are located in Turkey, some of them in Azerbaijan.
3. When we look at the content of the articles on the website (using Google Translator), we find that they describe a story from Istanbul in which the bus driver stopped to pray.
4. And in the text from Azerbaijan, which refers to the original report from Turkey, we find that the best place to pray is the mosque, not the bus, so the first photo was not taken in the Czech Republic, it was not taken in the Prague metro. It comes from Turkey, Istanbul.
5. After typing a second slice of a urinating black man in Google Images, we find a variety of resources, especially the social network Twitter.
6. We reveal the original image which we can analyse in more detail (it is of better quality, details can be recognized).
7. At first glance, we can see that the photo was taken in 2015 and was shared by “joeypops”. Upon closer analysis of the photo we reveal two important pieces of information: on the door of the car there is a sign in English “Do not lean on the door” (behind the black man) we find a map of the subway in New York, USA. So, it is clear that this is a photo from the New York

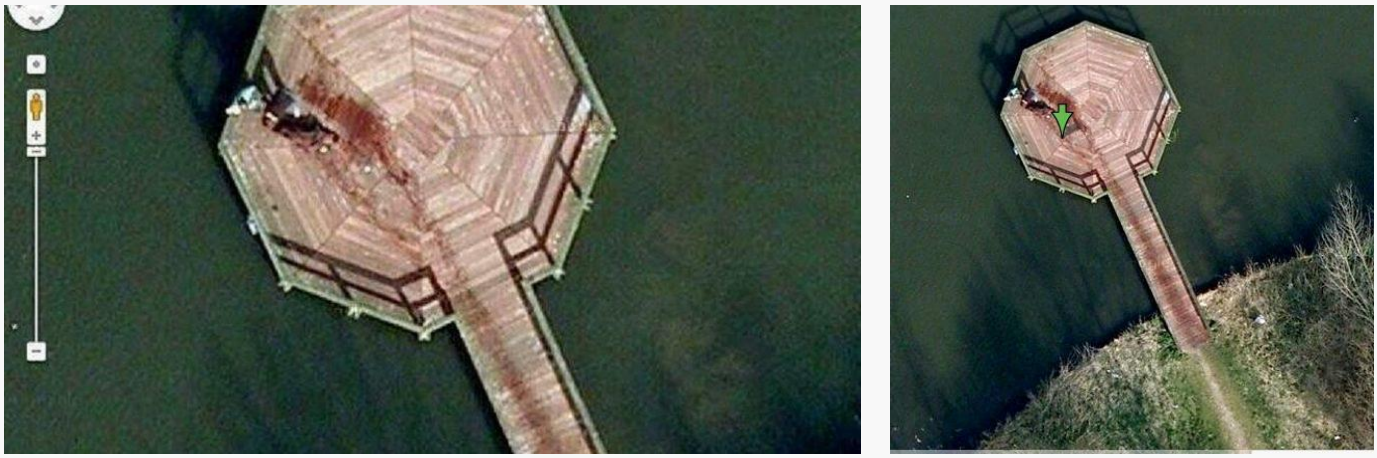
subway. The second photo was not taken in the Czech Republic, it was not taken in the Prague metro. It comes from the USA, New York.

8. We repeat the same procedure with the third photograph of a sleeping black man.
9. Google reveals a large number of German resources, including Pinterest, Imagala, Facebook and other websites. The photo also appears in the German counter-racial group Kontra Kontra Asyl, in which it is also parodied. It can also be found on the Czech site Right Space where it is supplemented by a source: Radio Yerevan. A photograph of a black and sleeping black man also appeared on the website supporting Marie Le Pen's Echo des Montagnes candidacy.
10. Photography was by no means taken in the Czech Republic. So, the third photo was not taken in the Czech Republic, it was not taken in the Prague metro.
11. It spreads mainly through German and French websites. The analysed message is false and can be classified as fake news or hoax. It contains no serious source, contains false information, contains photographs that do not originate from the Czech Republic and have been taken out of context. We can speculate on the purpose of the report and its impact on users who spread it.

6. After presenting the theory and sample report, the teacher forwards three different messages with the picture informing the participants that not all of messages are hoaxes. The task of the participants is to follow the way the teacher presented and find out whether the message is true or not. They write down what kind of signs hoax the message has and what convinced them.

Examples:

[Example 7. This image shows a Facebook post about US President Donald Trump and First Lady Melania Trump with a child who was alone in a mass shooting in August 2019 in El Paso, Texas. Image downloaded fromhttps://twitter.com/joshtpm/status/1159672304542126082/photo/1?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1159672304542126082&ref_url=https%3A%2F%2Fwww.snopes.com%2Ffact-check%2Forphan-thumbs-up%2F in August 2019.]



[Example 8. These images show a Google Maps image which supposedly captured a furtive corpse disposal. Images downloaded from https://www.google.com/maps/place/52%C2%B022'35.6%22N+5%C2%B011'53.9%22E/@52.3765553,5.1961143,17z/data=!3m1!4b1!4m5!3m4!1s0x0:0x0!8m2!3d52.376552!4d5.198303 in August 2019.]

[Example 9. These images show the creations of artist Juan Cabana. Images downloaded from https://www.snopes.com/fact-check/mermaid-in-florida/ in August 2019.]

7. At the end of the activity, the teacher should sum up the answers and feelings of participants. If it is needed, it is useful to add a comment or an explanation to the pictures.

THIRD EXERCISE: FOR MORE EXPERIENCED PARTICIPANTS

1. Based on the theory, which was presented in the previous exercise, the teacher makes the last exercise with the participants.

2. He/she shows the pictures to the participants and asks if they can see anything disturbing or shocking. After looking at the pictures he/she reads them the texts added to the pictures.

Examples:

Text 01:

“PLEASE HELP LITTLE BABY! AND SEND THIS MAIL TO THE PEOPLE!!

Please read it!! It's not annoying chain! And send it to a lot but really

a lot of people!! Little girl in the picture has a brain cancer. AOL

donates her surgery by 5 cents for every email that was sent. Please help.”

[Example 10. This image shows a little baby. Image downloaded from https://www.snopes.com/fact-check/natalie/ in August 2019.]

Text 02:

Milk scandal! Is that even possible??? And the authorities cannot see it...

Did you know? Milk in TetraPak that is not consumed by the end of its shelf life is returned to the processor. The processor opens the package, re-boils and repacks the milk. They can do this up to 5 times! The bottom of the box is under the sealed fold number 12345, where one of the numbers is missing. This missing figure indicates, how many times has milk been "recycled". I.e. 12 45 means it has been re-boiled 3 times. So, enjoy!! On the milk boxes, which were "in action" for 11.90 CZK, 4 in a row were missing! I hope that at least the milk sold as fresh does not carry any missing number in the line. The expiry date is about 1 year, so there is also 5 years old milk in the boxes!!! And because boxed milk is made from dried fabrics with a shelf life of 5 years, you people drink milk even 10 years old!!! So, buy the shit for 9,90 CZK! Enjoy.

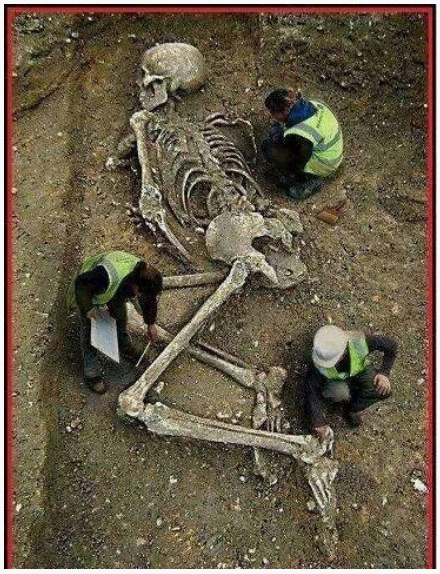
[Example 11. This image shows TetraPak package of milk. Image downloaded fromhttp://www.hoax.cz/hoax/recyklovane-mleko/ in August 2019.]

Text 03:

UNBELIEVABLE!!!
They run at speed 16 km/h and jump up to 92 cm. They are night spiders, so they only come out at night or when they are in the shade. When you get bitten, you get a dose of Novocain, so you get stiff immediately. You don't even know when they bite you in your sleep, then you just wake up without the missing leg or hand, because they gnawed you all night. When you encounter something in the shade while walking and the sun suddenly shows you, what you met it is better to run. They immediately set out for your shadow and scream all the time, whilst following and haunting you.
PS: These are spiders found daily by soldiers in Iraq. Imagine the awakening when you could see one of these crumbs in your tent.

[Example 12. This image shows the camel spiders in Iraq. Image downloaded from http://hoaxes.org/photo_database/image/camel_spiders_in_iraq in August 2019.]

Text 04:



What is it? A skeleton, the Nephilim, so offspring of the fallen angels and daughters of men, or giants hiding in plain sight?

[Example 13. This image shows a giant skeleton. Image downloaded from https://www.pinterest.com/pin/354377064413788348/ in August 2019.]

Text 05:

Alert. They have been found infected with AIDS banana in Mexico.

This afternoon Dr. Carissa F. Etienne, Director of the Regional Office for the Americas of the World Health Organization, complained to the media that there were found about 1 million of bananas infected with the HIV virus (AIDS).

After carrying out the necessary inspections in the fields from Guatemala, it was discovered that fruit was injected with infected blood.

[Example 14. This image shows the hoax with information about infected bananas. Image downloaded from

https://africacheck.org/fbcheck/hoax-alert-hiv-injected-into-bloody-bananas-again/ in August 2019.]

3. After reading the teacher asks the participants the following questions:

1. **Describe the reality as accurately as possible.**
2. **Do you think this is true information?**
3. **How can you find out the sources and the truth?**
4. **How can you tell that this is a hoax?**

4. At the end of the activity, the teacher should sum up the answers and feelings of the participants. If it is needed, it is useful to add a comment or an explanation to the pictures.

EXPERIENCE AND PRACTICE

The teacher should patiently explain all the information, step by step, as many times as it is needed. This game is a good tool to learn about the opinions and fears of the participants. Together with the teacher, the participants should become more skilled in recognizing false information or fake news, but it is still necessary to remind the students that they should be always careful, because even the experienced users can be fooled and consider the false information as the true.

The following rules should be useful for the participants:

1. I always try to use critical thinking about the content I find.
2. I don't just read the headlines - I don't make any judgments.
   The headlines aim to capture the attention of readers, evoke their strong emotions and force them to click on the headline or forward the message.

3. Anyone can write on the Internet with various intentions.
4. Hoaxes are spread in order to harm or affront someone, to relativize the truth, to cause panic, but also to make the author entertained by the stupidity of those who trust and spread these hoaxes.

PHOTODOCUMENTATION

Bibliography

1. Camel Spiders in Iraq. Retrieved from http://hoaxes.org/photo_database/image/camel_spiders_in_iraq in August 2019.
2. Caunt, J. (2018). People Are Posting Examples of How Media Can Manipulate The Truth (12 Pics). Retrieved from https://www.boredpanda.com/examples-media-truth-manipulation/?utm_source=google&utm_medium=organic&utm_campaign=organic in June 2019.
3. E-bezpečí. Retrieved from https://www.e-bezpeci.cz/ in August 2019.
4. Giant Skeletons found in India: Checkmate Atheists. Retrieved from https://www.secrant.com/rant/off-topic/giant-skeletons-found-in-india-checkmate-atheists/57370153/ in August 2019.
5. Google Images. Retrieved from https://images.google.com/ in August 2019.
6. HOAX ALERT: HIV injected into 'bloody' bananas, again. Retrieved from https://africacheck.org/fbcheck/hoax-alert-hiv-injected-into-bloody-bananas-again/ in August 2019.
7. HOAX: Český turista natočil na Krétě inscenované topení uprchlíků pro média. Retrieved from http://www.romea.cz/cz/zpravodajstvi/domaci/hoax-cesky-turista-natocil-na-krete-inscenovane-topeni-uprchliku-pro-media in August 2019
8. Hoax / Co to je hoax. Retrieved from http://www.hoax.cz/hoax/co-je-to-hoax in August 2019.
9. HOAX. Retrieved from http://www.hoax.cz/cze/ in August 2019.
10. HOAX: Video českého turisty z Kréty zachycující inscenované topení uprchlíků pro média. Retrieved from https://www.hatefree.cz/blo/hoaxy/2884-cesky-turista-kreta in August 2019.
11. HOAXBUSTER.COM. Retrieved from https://hoaxbuster.com in August 2019.
12. Image Verification Corpus Released. Retrieved from https://revealproject.eu/image-verification-corpus-released/ in August 2019.
13. Jak si ověřit informace na internetu?. Retrieved from https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/104-jak-overit-informace-na-internetu-2018-letak-skladacka/file in August 2019.
14. Kopecký, K. Zpráva: Uprchlíci v pražském metru. Retrieved from http://www.e-bezpeci.cz/index.php/ukazky-analyz/uprchlici-v-prazskem-metru in August 2019.
15. Manipulátoři - Hoaxy, manipulace a propaganda pod lupou. Retrieved from https://manipulatori.cz/ in August 2019.
16. Natalie. Retrieved from https://www.snopes.com/fact-check/natalie/ in August 2019.
17. Reid, A. (2015). Are you a journalist? Download this free guide for verifying photos and videos. Retrieved from https://firstdraftnews.org/are-you-a-journalist-download-this-free-guide-for-verifying-photos-and-videos/ in August 2019.
18. Recyklovane mleko. Retrieved from http://www.hoax.cz/hoax/recyklovane-mleko/ in August 2019.
19. Snopes.com. Retrieved from https://www.snopes.com/ in August 2019.
20. TinEye. Retrieved from https://www.tineye.com/ in August 2019.

21. TU-Berlin - Hoax Info Service. Retrieved from https://hoax-info.tubit.tu-berlin.de/hoax/ in August 2019.
22. Urban Legends. Retrieved from https://www.liveabout.com/urban-legends-4687955 in August 2019.
23. Video zachytené na Kréte, zaver si urobte kazdy sam :). Retrieved from https://www.youtube.com/watch?v=07XqF3HKl_o&t=2s in August 2019.

CONCLUSION

The Internet and the related technologies can make life easier for today's seniors. However, technological advances and the subsequent leap in civilization first appeared when today's seniors were already well established in the job market and did not necessarily have to face new demands. When they retired, working with computers did not pose such a challenge for today's 70 and 80 year-olds as it does now. In this regard, 'younger' seniors find themselves in a much better position, because they have already had an opportunity of learning basic computer skills which they can then develop in retirement.

Universities of the Third Age provide an excellent opportunity for improving this situation. However, they are generally urban-based and have limited resources, so not everyone can take advantage of their educational programmes.

When inter-generational ties are weakened or broken, seniors no longer have the opportunity of learning from their children and grand-children naturally. Thus, such an educational postulate as presented by Margaret Mead in her concept of pre-figurative culture loses all sense. There are no ties with children and grand-children, so there is no possibility of transmitting models and values from the younger generation to their elders. This makes the situation even worse. Seniors may feel excluded, neglected and redundant, which triggers a whole series of negative feelings which can cause total withdrawal from social life. They may also attempt to teach themselves and try to tackle the challenge of new technologies by trial and error, which of course is not the best educational strategy. Random material, irrelevant content and inadequate methods may all mean that their effort is wasted, and the senior student is discouraged from further investigation.

Non-governmental organizations can help in such a situation, by organizing computer courses for seniors. One of the most important issues of this type of training, which at the same time is under appreciated, is cybersecurity.

The project also includes the creation of an international website through which we present new ideas and innovations for the practice and education of seniors in the field of digital security using modern technologies.

Website: http://www.cybernetsecurityforseniors.eu

ATTACHMENT

Attachment No.1 - Questionnaire: Cyber Attack for seniors

Questionnaire: Cyber Attack

Thank you for agreeing to taking part in our research.
We guarantee your anonymity, and in return ask for honest answers.

1 Please tick the appropriate answer

Sex	F	M				
Age	50-60	61-70	71-80	81-90		
Education			primary	secondary	higher	Technical
Place of residence			village	town	city	Metropolis

2 From the following statements, please choose the one which is closest to your experience of computer use:

a. I rarely use a computer, and very often need the help of others

b. I often use a computer, and regularly help others

c. I have used a computer regularly for many years, and cannot imagine life without the Internet

3 When completing the questionnaire, please give your answers according to the following scale:

1 – never
2 – very rarely
3 – rarely
4 – often
5 – very often

1.A	When I come across a dangerous situation in the Internet: I immediately ask for help from specialists	1 2 3 4 5
2.A.	When I come across a dangerous situation in the Internet: I ask for help from family or friends	1 2 3 4 5
3.A	When I come across a dangerous situation in the Internet: I try to resolve it myself	1 2 3 4 5
4.A.	When I come across a dangerous situation in the Internet: I'm cautious and try not to fall into a trap	1 2 3 4 5
5.A.	When I come across a dangerous situation in the Internet: I look for help on specialist internet forums and the Internet community	1 2 3 4 5
6.B.	In order to protect myself, I only use authenticated programs	1 2 3 4 5
7.B.	In order to protect myself, I use anti-virus programs	1 2 3 4 5
8.B.	In order to protect myself, I scan my computer regularly with anti-virus programs	1 2 3 4 5
9.C.	I regularly change my access passwords	1 2 3 4 5
10.C.	I avoid using simple passwords by making sure they consist of a combination of at least 12 letters, numbers and special characters	1 2 3 4 5
11.C.	I don't log in to other computers	1 2 3 4 5
12.C.	I don't use my passwords on other computers	1 2 3 4 5
13.C.	I don't use the same password for all my Internet accounts	1 2 3 4 5
14.C.	I always change passwords allocated to me by websites	1 2 3 4 5
15.C.	I never share my codes or passwords with	1 2 3 4 5
16.D.	I never open messages from unknown people	1 2 3 4 5
17.D.	I never open mail attatchments from unknown people	1 2 3 4 5
18.D.	I never click on links sent to me by email	1 2 3 4 5
19.D.	I never react to advertising or spam sent to me by unknown people	1 2 3 4 5
20.E.	I check the the website's terms and conditions before I decide to buy	1 2 3 4 5
21.E.	I only log into https: websites (with a lock or green belt)	1 2 3 4 5
22.E.	I regularly update the programs I use	1 2 3 4 5

23.E.	I use two-tier verification for emails (password + SMS code)	1 2 3 4 5
24.E.	I don't want to be open to danger so I use the Internet as little as possible	1 2 3 4 5
25.E	I only use trusted websites	1 2 3 4 5
26.E.	I avoid installing unverified apps on my smart phone	1 2 3 4 5

Please indicate (according to the scale) which of the following problems you have personal experience of:

27.F.	Defective program which doesn't work	1 2 3 4 5
28.F	Defective Internet browser which doesn't work	1 2 3 4 5
29.F.	Computer speed slowing down	1 2 3 4 5
30.F.	Data loss	1 2 3 4 5
31.G.	Attempt to obtain passwords by a false bank website	1 2 3 4 5
32.G.	Attempt to obtain money (requesting a transfer to "people in a difficult situation")	1 2 3 4 5
33.G.	Regular redirection by the browser to unwanted and irrelevant websites	1 2 3 4 5
34.G.	Theft of money from bank account	1 2 3 4 5
35.G.	Theft of money from bank cards or credit cards	1 2 3 4 5
36.G.	Computer blocked (hard disk encrypted) and ransom demand	1 2 3 4 5
37.G.	Internet bank account broken into	1 2 3 4 5
38.G.	Password theft	1 2 3 4 5
39.H.	Blackmail attempt (threat to publish compromising material)	1 2 3 4 5
40.H.	Identity theft (e.g. on social media)	1 2 3 4 5
41.H.	Attempts to contact me by unknown people in my own country	1 2 3 4 5
42.H.	Attempts to contact me by unknown people in other countries	1 2 3 4 5
43.H.	Immoral propositions via email	1 2 3 4 5
44.H	Harassment via email or text messages	1 2 3 4 5
45.I	Regular receipt of unwanted emails (spam)	1 2 3 4 5

46.I.	Automatic forwarding of emails in my name without my knowledge	1	2	3	4	5
47.I	Hate speech	1	2	3	4	5
48.I.	Appearance of pornographic content	1	2	3	4	5
49.I.	Sharing false information in the conviction that it is true	1	2	3	4	5

Here are a number of personality traits that may or may not apply to you. Please write a number next to each statement to indicate the extent to which you agree or disagree with that statement. You should rate the extent to which the pair of traits applies to you, even if one characteristic applies more strongly than the other.

Disagree strongly	Disagree moderately	Disagree a little	Neither agree nor disagree	Agree a little	Agree moderately	Agree strongly
1	**2**	**3**	**4**	**5**	**6**	**7**

I see myself as:

50_____ Extraverted, enthusiastic.

51_____ Critical, quarrelsome.

52_____ Dependable, self-disciplined.

53 _____ Anxious, easily upset.

54 _____ Open to new experiences, complex.

55 _____ Reserved, quiet.

56 _____ Sympathetic, warm.

57 _____ Disorganized, careless.

58_____ Calm, emotionally stable.

59 _____ Conventional, uncreative.