migrant literacies

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

The contents of this publication are the sole responsibility of the author and can in no way be taken to reflect the views of the European Commission.

What does Internet know about me?

by Polis

Workshop is focused on what kind of information about us is accessible on the internet. During workshop participants will have a possibility to think about, if giving these data is sensible and cosnscious. Do they want it all to be accessible online? As a summary of the workshop participants will prepare code of conduct online.

GENERAL DESCRIPTION

TARGET GROUP	12-20 people; B1 language level; basic media competences that enable the use of smartphone and internet.
TIME	6 hrs (5hrs 30 min + breaks)
FORM	External Workshop or workshops included in regular language classes.
SPACE	Room with Wi-fi network, chairs in circle, 4-5 tables with chairs for group work/tables for work in pairs.
TOPICS COVERED	Safety on the Internet, profiling, data theft, privacy in the internet, data protection.
TOOLS	• Screen device with the access to the internet, flipcharts, markers, spun yarn, prepared by trainers. • Cards with different types of data/information. • Examples of phishing. • Printed language quizzes.
OBJECTIVES	The topic of this workshop is privacy on the web. The main aim of the course is to familiarize participants with: • The risks resulting from sharing their data online, • The issue of building their online-image. • Ways of protecting their data in the Internet.
LINGUISTIC SKILLS	Learning new vocabulary.

DIGITAL/ MEDIA LITERACY REFERENCE	• Participants realize that their being monitored and profiled by companies in the internet. They know about targeted ads. • Students became aware that their personal data can become an actual “currency” in a lot of free services and websites. • Participants will learn about the possible consequences of leakage of personal and sensitive data. • Participants learn how to protect their personal data from phishing attacks and how to recognize phishing. • Participants learn the opportunities and threats resulting from building their own image on the web. They are aware that other people can look for information about them. • Participants learn how to create and modify their image on the Internet depending on their needs - for example, share only some of their data on social networking sites. • Participants learn about the usage and protection of personal data in the internet, • Students will learn to use an important programs in field of cyber security. • Student will learn how to improve their safety on the internet. • Participants will learn how to create strong passwords.

STEP BY STEP DESCRIPTION

STEP 1

Time

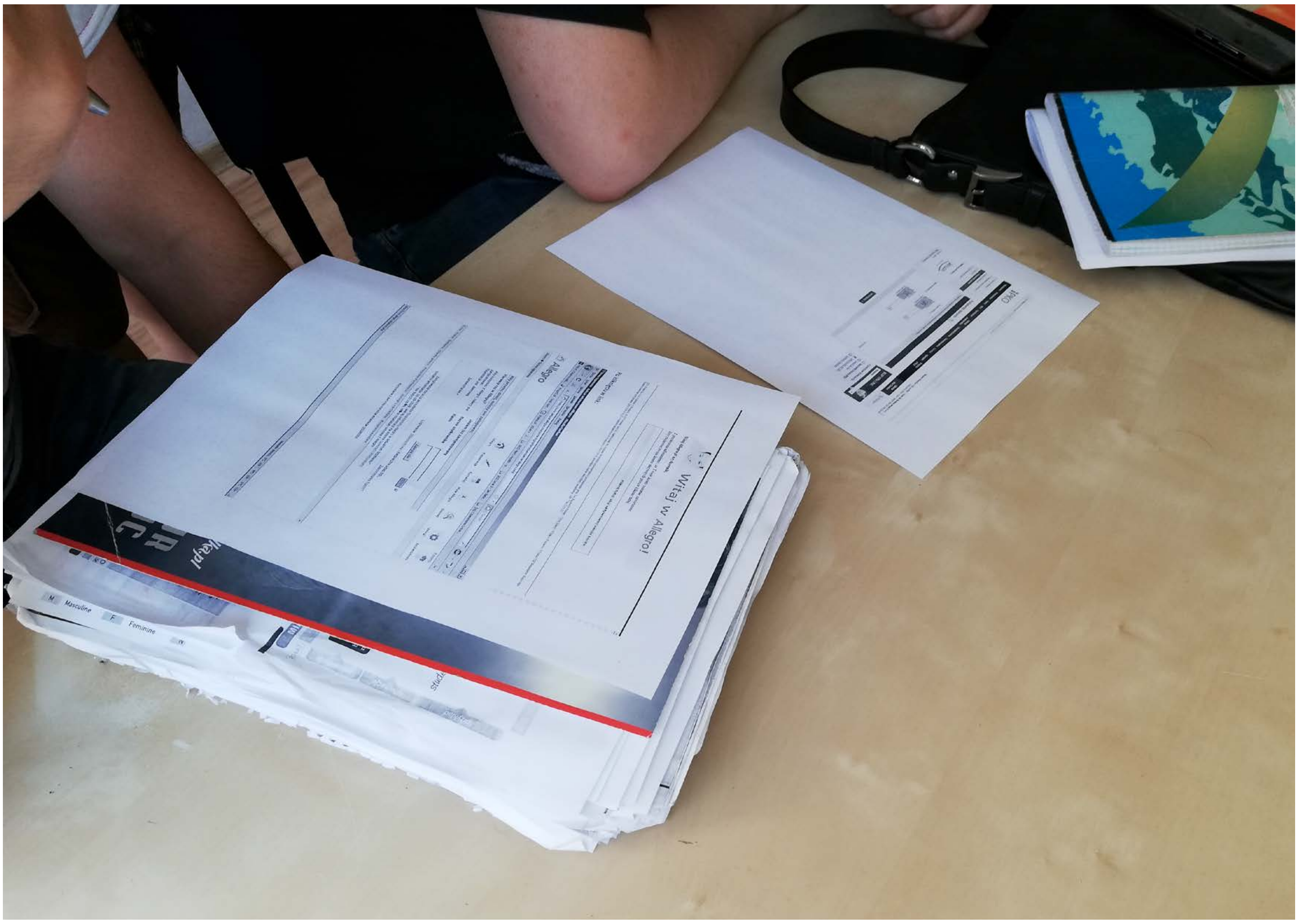
2o min.

Objective

- Integration

Activity description

Participants are standing in the circle. The task is to say your name and show some gesture (raise a hand, do a push up, participants individually choose a gesture). Next person has to repeat a name and a gesture. Third person has to repeat names and gestures of two previous people. And so on. When all finished the circle we change the order of the circle and repeat a task. This exercise will help participants remember their names.



STEP 2

Time

30 min.

Objective

- Contract - setting the rules based on which participants will work,
- Integration of participants,
- Introduction to the topic and explanation of the workshop method.

Material

- Flipchart
- Marker
- Spun yarn

Activity description

Inter-Net

In this exersise trainers use a yarn. Frist trainer wraps the yarn around his finger and throws it to participant whose name he remembers. He says the name loud. The yarn should unwind as he throws it. A person that caught the yard is now wraping the yarn around his finger and throwing it to anoter person along saying name of that person. Each participant does that until all participants are conected by unwinded yarn.

When everyone is connected with a yarn, the trainers asks what has emerged from the unwined yarn. Trainers are looking for answers like “network”, and then explain the subject of the workshop - What does the internet knows about me.

At this point, the trainers can also use the symbolism of the yarn to:

- talk about the workshop plan and the workshop method (involving the participants in activities).
- set common rules for the workshop.

All the participants and the trainer set up rules, which everybody agree to obede during the workshop. Flipchart with the rules should be placed so can everybody can see it.

Comments:
The trainer should use the symbolic bond created between the participants to tell more about the methods of workshop work (which are related to the participants’ activity) and to set rules (you can vote by raising your hand with a wraped yarn).

STEP 3

Time

50 min.

Objective

1. Participants will realize what kind of information are accessible online for strangers.
2. They will have a moment to answer themself a questions, how conscious they put information about themself on the internet.

Material

- Screen devices with an access to the internet.

Literacy skills

- Learning new vocabulary (trainers should circle new / difficult words appearing in discussion and be ready to explain them),.
- Participants learn how to create and modify their image on the Internet depending on their needs - for example, share only some of their data on social networking sites.
- Participants learn the opportunities and threats resulting from building their own image on the web. They are aware that other people can look for information about them.
- Students understand the importance of privacy settings in social networks.

Activity description

Participants are watching part of the youtube video of social experiment made by polish youtuber: https://www.youtube.com/watch?v=CLRBYhd7e4Q

After watching part of the film trainers ask participants:

- what kind of information did we get to know about persons in film?
- how would you feel listening all those things from the person, whom you just met?
- what other kinds of information people share online?
- do you want all these information to be accessible online?
- Trainers write down all the types of information (data) that we share online, given by the participants.

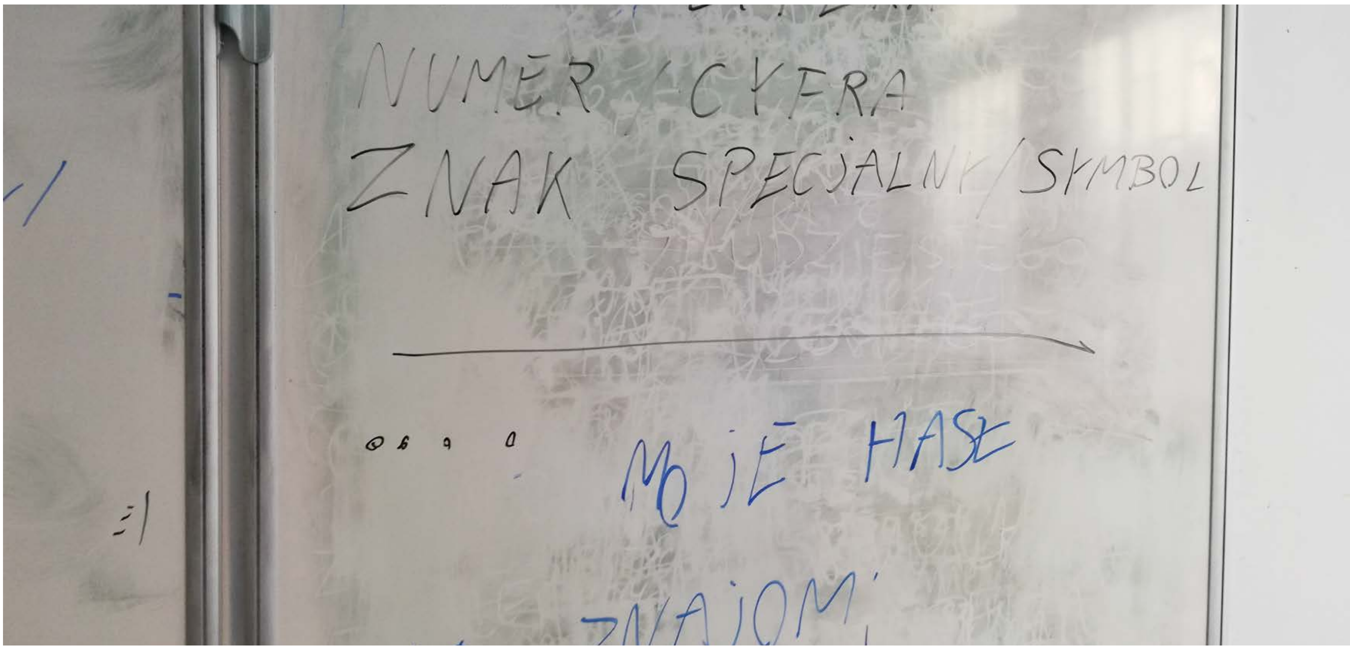
Alternatively:
Participants are divided in pairs. Each pair is choosing one person from their friends who is very active in social media (it could be also one of the trainers). Next, each pair is trying to find out as much as they can about the choosen person on the Internet. Everybody has a 10 minutes for googling. They are writing down, what kind of information they have learned about this person. After this, everyone are coming back to the whole group and discuss with trainers these questions:

- what kind of information did we get to know about this persons?

- how would you feel listening all those things from the person, whom you just met?
- do you want all these information to be accessible online?

Trainers write down all the types of information (data) that we share online, given by the participants.

Comments:
Trainers can choose whether they want to use parts of the film or an alternative exercise.
During alternative exercise, trainers should think about the persons, whose profiles participants will check in social media.
If the group is not well integrated, participants should check the profile of one of the trainers (or some famous person). Checking profiles of their friends (especially in pairs) can be stressful and unpleasant for participants who are not yet well integrated in group and don’t trust each other with private informations. This exercise should be prepared with knowledge about the group and special concern about the privacy of the participants.



STEP 4

Time

30 min.

Objective

1. Participants will learn which data are sensitive ones.
2. Participants will learn which data are personal data.

Material

- Flipchart or whiteboard, marker,
- Cards with different types of data/information (for example: fingerprint scan, sexual orientation, IP address, phone number, pictures)

Literacy skills

- Learning new vocabulary (trainers should circle new / difficult words appearing in discussion and be ready to explain them).
- Participants learn about the usage and protection of personal data in the internet.
- Students became aware that their personal data can become an actual "currency" in a lot of free services and websites.

Activity description

After all examples of data shared in the internet (given by participants) were wrote down by trainers, trainers ask:

- which of those informations are personal data?
- which of those informations are sensitive data?
- why?

After brief discussion, trainers give cards to participants with various examples of information/ data (for example: fingerprint scan, sexual orientation, IP address). Participants are working in groups or in pairs. They have to decide whether given inromation is personal or sensitive data (or both).

The resultes are checked and discussed with other groups.

STEP 5

Time

40 min.

Objective

1. Participants will realize that somebody or something is taking advantage of their data.
2. Students will learn about phishing.
3. Participants will learn to recognize phishing.

Material

- Examples of phishing prepared by trainer (can be screen with projector or printed and handed to participants).

Literacy skills

- Participants learn about usage and protection of personal data in the internet.
- Students became aware that their personal data can become an actual “currency” in a lot of free services and website.
- Participants learn how to protect their personal data from phishing attacks and how to recognize phishing.

Comments:
Trainers should prepare phishing examples for exercise (along with examples of real messages),

Activity description

Data stealers part 1.

In pairs, participants will try to think about who or what can use this sensitive data online. In what purpose? After talking in pairs all participants discuss on issue on the forum.
Trainers are supervising the discussion looking for examples like: criminals, hackers, commpanies, bots.
After that, trainers tell participants during next excersise we will focus on data theft and so called “phishing”.
Trainers explain the definition of phishing and ask if participants have received that kind of messages before?
After that, trainers give participants different examples of on-line messages. Participants should analize those examples in pairs/groups and decide if the’re true or are they phishing messages. After that, the groups are comparing their work with other groups and trainers.
Trainers should support groups in process and prepare a list of question that will help to recognize phishing (for example: Is the website address appropriate? Does it have an HTTPS protocol? Who is the sender of the message? Am I being urged to act? Can I verify the truth of the message in a different way - for example by calling the sender?).

STEP 6

Time

20 min.

Objective

1. Participants will learn about new vocabulary related to cybersecurity.
2. Participants will learn about the principles of safe Internet use and the recognition of false messages.
3. Participants will create a list of online security tips, that they will take home.

Material

- Prepared, printed language quizzes - texts with empty spaces/blanks in selected sentences.

Literacy skills

- Reading comprehension exercise.
- Learning new vocabulary (trainers should circle new / difficult words appearing in the text and be ready to explain them).
- Learning online-safety rules.

Activity description

Safety checklist

Trainers give participants prepared language quizzes - texts with empty spaces/blanks in selected sentences. Participants should read the text and put in those blanks appropriate words. Trainers should however construct this exercise in appropriate way. The text with empty spaces/ blanks should be an online-safety checklist created by trainers. All text should be constructed as a set of rules for recognizing phishing and improving online-security of participants (for example: Always look if the site has a _____ . [HTTPS protocol]). In this way, created language exercise is also an online security exercise that end with a material (checklist) that can be taken home with participants.

Comments:
Trainers should prepare a list of things to pay attention to, in order to recognize phishing – Checklist.

STEP 7

Time

30 min.

Objective

1. Participants will learn about the issue of profiling Internet users for marketing purposes,
2. Students will learn about the ways and mechanisms of collecting data about their activity in the network,
3. Participants will learn how to consciously influence this process in order to protect their data.

Material

- Devices (smartphones/computers) with internet connection.

Literacy skills

- Students became aware that their personal data can become an actual "currency" in a lot of free services and website,
- Participants realize that their being monitored and profiled by companies in the internet. They know about targeted ads,
- Participants learn about cookies – what they use for and how to delete them,
- Participants know where they can find the information about their media activity collected by different apps and can modify it or delete it.

Activity description

Data stealers part 2.

Trainers tell participants that during the next excersise we will focus on another example od data usage (but not theft) – profiled/targeted advertising. Trainers show participants how users are being targeted with ads by different companies. Facebook – participants open their facebook news feed on their phones/laptops and are searching for ad in their facebook feed. They click on the right corner of the ad and check "why do I see this as?". In groups they compare how different companies are profiling their ads. After that, participants should choose "Manage your advertising preferences" and check what facebook knows about them. Google – Participants individually go to https://adssettings.google.com/authenticated?hl=pl and check how their being profiled by Google. Trainers should give participants time to get to know the applications. They should end this exercise with brief discussion (for example: what does the internet knows about me? Did google or facebook algorithms were always right? Is it better to turn of profile ads or to delete unnecessary/unwanted options?

Comments:
Trainers should give participants time to use and play with applications. Participants should individually learn about these applications in order to be able to change their settings after the workshops.

STEP 8

Time

30 min.

Objective

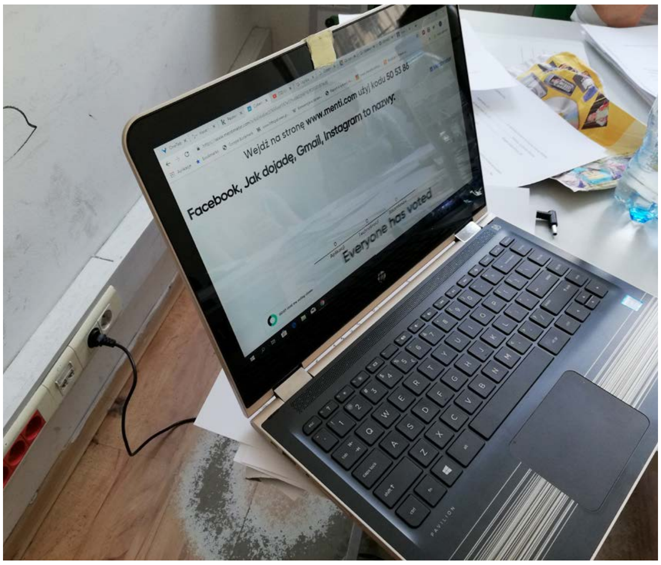
1. Diagnosis of a problem - participants will find out if they have been a victim of a data leak in internet.
2. Student will learn about useful program in field of cyber security.

Material

- Devices (smartphones/computers) with internet connection.

Literacy skills

- Participants will learn about different kind of data collected by the companies,
- Participants will learn about the possible consequences of leakage of personal and sensitive data,
- Students will learn to use an important program in field of cyber security.


Wejdź na stronę www.menti.com użyj kodu 50 53 86
Facebook, Jak dojadę, Gmail, Instagram to nazwy:
Everyone has voted

Activity description

Toolbox

Trainers ask participants whether any of them had been a victim o data theft or data leak?

Trainers collect the answers and show a website where everyone can check if their data has leaked to the internet: https://haveibeenpwned.com/

Trainers ask all participants to check if their mail accounts have been registered in the website database.

Trainers explain how this website works and how to use it:

If someone e-mail is in the website database, then he/she should check from which his data have been leaked and what kinds of personal data got to the internet.

Trainers are writing both name of the websites that had a security breach and type of leaked data.

Comments:

Trainers should give participants time to use and play with applications. participants should individually learn about these applications in order to be able to change their settings after the workshops.

STEP 9

Time

30 min.

Objective

1. Diagnosis of a problem - participants will find out if they have been a victim of a data leak or account hacking.
2. Student will learn about useful programs/sites in field of cyber security.

Material

- Devices (smartphones/computers) with internet connection.

Literacy skills

- Participants will learn about different kind of data collected by the companies,
- Participants will learn about the possible consequences of leakage of personal and sensitive data,
- Students will learn to use an important programs / sites in field of cyber security.

Comments:
Trainers should give participants time to use and play with applications. participants should individually learn about these applications in order to be able to change their settings after the workshops.

Activity description

Toolbox pt. 2

After verifying who has become the victim of the information leak, the workshop leaders should note that the haveibeenpwned site collects information about only the largest data leaks. The fact that our data is not in its database, does not mean that we are safe. Next, the trainers show the participants other pages to check the level of their online-security and types of data collected by various services: https://www.google.com/maps/timeline?pb - Location history. Participants should pay attention to whether there are locations in the map where they have never been. https://myaccount.google.com/device-activity - connected devices.

Participants should pay attention to whether they have disconnected their old devices/smartphones from their accounts. They should also pay attention to devices that they do not recognize.

https://myaccount.google.com/permissions - connected apps.

Participants check which applications have access to their accounts and if they trust these aplications. Trainers should give participants time to get to know the applications. They should finish the exercise with a short discussion summarizing the effects of the activities in the applications: Do you have confidence that your data is safe on the web? Have you seen any suspicious activity on your accounts? Have you changed anything in the settings of your accounts?

STEP 10

Time

30 min.

Objective

1. Summary of knowledge,
2. Participants will learn about new vocabulary related to cybersecurity,
3. Participants will learn about the principles of safe Internet use,
4. Students will learn to create strong passwords for different websites.

Material

- Devices (smartphones/computers) with internet connection.

Literacy skills

- Reading comprehension exercise,
- Learning new vocabulary (trainers should circle new / difficult words appearing in the text and be ready to explain them),
- Students will learn to use an important programs / sites in field of cyber security,
- Student will learn how to improve their safety on the internet,
- Participants will learn how to create strong passwords.

Activity description

Toolbox part 3.
The trainers briefly summarize the discussed threats related to sharing information on the web and ways to protect our data on the Internet (eg disabling the option of profiling ads, disconnecting unused devices from our accounts, checking data leaks).

At the same time, they point to the last, most important way to protect our data from theft - a safe password.

The trainers show the participants the Howsecureismypassword.net website. Participants are asked to check the strength of their passwords (Note: the trainer should explain to the participants that the site is safe, but participants should never enter their real password, but the password changed - with swapped letters / numbers).

Participants check the strength of their passwords. Any password that is not displayed in green should be corrected.

Then the trainers ask the participants what makes the password strong? After a short discussion, the trainers give away prepared grammar exercises:

Trainers give participants prepared language quizzes - texts with empty spaces/blanks in selected sentences. Participants should read the text and put in those blanks appropriate words.

Trainers should however construct this exercise in appropriate way. The text with empty spaces/blanks should be an list of guidelines to for creating a strong password. All text should be constructed as a set of rules for creating strong passwords and improving online-security of participants (for example: Always use at least one _____ letter. [capital]).

In this way, created language exercise is also an online security exercise that end with a material (checklist) that can be taken home with participants.

Comments:
Trainers should prepare a list of guidelines for creating a strong password,
From this list, trainers should prepare a language exercise by removing key words from the text.

STEP 11

Time
20 min.

Objective
1. Summary, evaluation

Activity description
Every participant can now say something about the workshop. What was most important for him/her? How is he/she feeling now? Everybody can take the floor once. Participants do not comment on word of other participants.