Passwords: Creating and Managing Secure Access

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 2 - PASSWORDS

Lesson plan for secondary schools

Scenario developed as part of the “CyberSec EduCheck” project – project no. 2023-2-PL01-KA210-VET-000176822

Script authors: Weronika Kędzierska, Mateusz Pękala - Coventry University Wrocław

Substantive editor: Pavla Vybíhalová - European Centre for Career Education

Graphic design: Karolina Kornecka-Kupiec, Jadwiga Maj - KREA Association

Wrocław 2024

Co-funded by the European Union

LEADER: Research Institute Europe | Coventry University

PARTNERS: KREA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

LESSON 2 – PASSWORDS

Dear,

We present to you a lesson plan on password security, a key element of protecting private information on the Internet. We are aware that the topic of digital security is very broad, so due to time constraints, we focused on the basic, but extremely important issues related to creating and managing passwords.

Our 45-minute class focuses on three main objectives: students will learn how to create strong and unique passwords, understand why two-factor authentication (2FA) increases account security, and learn how to manage passwords securely, including the benefits of password managers.

This is the minimum time to do key activities like group exercises and discussions to solidify your knowledge (we assumed that in those 45 minutes you wouldn't have enough time to set up the password manager on your own devices, which is a shame). However, if you have more time space, we suggest breaking this topic down into smaller parts and using them in future lessons, which will allow students to analyze and understand the issues better.

The scenario and teaching materials, including the presentation, can be adapted and modified according to your needs and the group's capabilities.

Best regards,

CyberSec Project Team

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 2 – PASSWORDS

Table of contents

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 2 – PASSWORDS

Lesson objectives

- **Explicit purposes**:
    - Students will be able to create strong and unique passwords that will provide better protection for their online accounts. They will understand the need to use a different password for each service they use.
    - Students will understand why two-step authentication is important and how to enable it on their accounts.
    - Students will learn how to manage their passwords, including how to use password managers.
    - Developing analysis and critical thinking skills.
- **Hidden Goals**:
    - Strengthening cooperation in the group.
    - Encouraging independent thinking and problem-solving.

Context - keywords

passwords, online security, two-factor authentication, password managers, personal data protection, cybersecurity

Justification for the choice of topic:

- Nowadays, access to technology and the Internet is widespread and almost continuous, young people regularly use various online services. Therefore, there is an increased risk of losing private data and hacking into accounts due to weak passwords.
- Many people use the same passwords on different services, which exposes them to serious consequences in the event of a single data breach. Understanding the need to create strong, unique passwords and the benefits of two-factor authentication is critical to online security.
- Education about password management, including the use of password managers, teaches youth to be responsible for their own data and accounts and develops awareness of cyber threats.

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KEA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

LESSON 2 – PASSWORDS

Lesson Preparation

- **Materials**:
    - Multimedia presentation [Passwords and their security]
    - Worksheets with exercises
    - Blackboard
    - Computers with internet access (if needed)
    - Online test – An option to use a platform that allows you to create quizzes about passwords and online security (e.g. kaboot.it - a sample ready-made quiz https://play.kahoot.it/v2/?quizId=cd611872-3056-4990-803f-765179e75c0e)

- **Experience**: Optionally, inviting students to an activity before class, e.g. an educational game from Google in the form of an interactive adventure that teaches, m.in, how to create strong passwords https://beinternetawesome.withgoogle.com/en_us/interland/landing/tower-of-treasure

- **Space**:
    - The room is equipped with a screen/projector.
    - Arrangement of desks in a way that allows work in groups or individually.

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 2 – PASSWORDS

Lesson structure

Purpose	Activity	Time	Materials
Introduction	Presentation of the topic and objectives of the lesson. First, a few stories – the teacher shares one or more stories of other students. The teacher asks: Are these stories true? No. They were invented for the needs of lessons. Which does not mean that they could not have happened	5 min	Presentation
Mini Quiz if this is a secure password	The teacher asks the students questions in the form of a quiz, asking them to write down the answer (1 is true). Sample questions: 1. Which password is the most secure? JPL93#q anna1234! Basil456 **Gospachackeryou won't break.** 2. Which password is the easiest to guess? **MyPassword123** Summer2024 Great!2023 Qwerty!123 3. Which password is the least secure? **Qwerty123** P@ssw0rd 1234abc! Secure*Pass123 4. Which of the following passwords might be the easiest to guess if a	10 min	

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

	hacker knows your pet's name and date of birth? K!ngC0bra L0veCats! Adventure987 **Fluffy2021** 5. What is 2FA? Feature on phones that speeds up battery charging An abbreviation for two antivirus filters running simultaneously **It's an extra security feature that helps make sure only you can log in, even if someone knows your password** Cloud encryption system that enhances file security The teacher presents the answers and asks the students to share the number of correct answers. 1d) The longer the password, the harder it is to crack. Ideally, the password should be 15 characters or more. A password can be 4 or more non-obvious words glued together 2 a) MyPassword123 is the easiest to guess because it uses simple words and number sequences that are often used in passwords by many people. Other passwords are also predictable. 3 a) The weakest password is Qwerty123. This is a popular password based on a simple keyboard pattern and easy to guess in dictionary attacks. Other passwords contain different character types and are less predictable, although they may still require additional improvements. 4 d) The easiest password to guess is Fluffy2021 because it contains the		

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

	name of the animal and the date, which makes it easier for a hacker to guess the password with the knowledge of this information. 5c) 2FA (Two-factor authentication) is a way to add extra security to your account, in addition to just your password. It works in such a way that after entering the password, you still have to confirm your identity in another way, e.g. by entering a code from a text message, using a special application (such as Google Authenticator) or having a special key. This makes your account much more secure Discussion of the results – why they are dangerous. **Alternatively** (instead of this quiz), you can use **the "Password Game" (worksheet 2).** It is a quick activity in which students in groups guess passwords based on one- or two-word clues. Each group chooses a "clue giver" who has 30 seconds to help the team guess the password, and the group has 3 attempts. For each correct answer, the group earns 2 points, and if they fail to guess the password, they lose their turn, but they do not lose points.		
Knowledge transfer: Common mistakes	**1 Open-ended questions to students (all or selected questions can be asked):** How many different passwords do you use for your accounts? How often do you use the same password for several different accounts? How often do you change your passwords?	10 min	Presentation, multimedia examples

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KEA STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

	How often do you forget your password? **2. Presentation of key information on common mistakes:** • We often use the same password on several websites • We often use similar passwords • We use personal information • We share passwords • Passwords that are too short • We use patterns on the keyboard (e.g. QWERT) • Substitution of digits/special characters (e.g. Password → P@$$w 0rd) • We store passwords in text files		
Practical exercises	How to Be Safe Group Work? The teacher divides the class into 4 groups. Each group has 5-10 minutes to complete worksheet No. 1. The aim is to answer the following questions: - What is causing the problem in this case? Maybe there are several of them? - What do you think could help to counteract such a situation? Example contexts for groups (you can choose 1 for all or for each group different): • Clicking on a suspicious link and taking over my account: I clicked on a link that looked like it was from a friend and entered my login credentials	15 min	Worksheet No. 1. Whiteboard, notes

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KEA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

	there. Then someone took over my account and now I can't access important things. • Accessing my account after leaving my laptop unlocked: I left my laptop unlocked at school, and someone went to my social account and posted nasty things pretending to be me. Now I have to explain myself to my teachers and friends, because everyone thinks it's me. • Stealing money through a weak password: I set a very simple password for my bank account and someone cracked it, stealing all the money. Now I have to fight to get them back. • Losing your game account after sharing your password: I gave my game password to a friend and he changed it and started using my account. I lost all my achievements that I had been working on for a long time.		
Discussion of the results and discussion	Introducing the password manager tool as a solution. Explanation of more difficult issues.	10 min	
Summary and reflection	Summary of key issues. An incentive to act to strengthen your security	5 min	Presentation

Optional homework

Verify your passwords:

- Check that your passwords are long, random, and unique.
- Install KeePassXC (or another password manager) on your computer.

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

- Transfer all your passwords to a password manager. Stop writing passwords on sticky notes or text files.

Change weak and dictionary passwords:

- If you use simple passwords like "123456" or "password," change them immediately.
- Review the systems you use:
- Make a list of all the accounts, apps, and systems you use, and make sure they're all secured.

Enable two-factor authentication (2FA):

- At least on the most important accounts such as email, social media, banking.
- Use apps like Google Authenticator or other available options.

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

Resources and knowledge for teachers

Description of the 5 Whys Method (5xWhy)

The 5 Whys method helps students understand why the problem occurred by asking five consecutive "why?" questions. It involves asking the question "why?" five times to get to the real root of the problem, rather than stopping at the first, obvious answer. With this tool, students can better understand what is behind a given problem and how it can be solved.

Alternative questions:

Instead of asking the "why" five times, it is worth using more open-ended questions that do not make students feel judged. In our example, we use "What is the cause?". Specific questions might look like this:

- How did it happen that someone got your password?
- I'm curious how you chose your password?
- What were you thinking when you created this slogan?
- Can you help me understand why this slogan seemed sufficient?

Examples of use (Theft of bank account data/ Loss of game account after password sharing):

Problem: Someone hacked into my bank account and stole all my money.	Problem: I lost access to my game account because I gave my password to a friend.
• Why did someone hack an account? Because he had access to my password. • Why did he have access to my password? Because I used a very simple password that was easy to crack. • Why did I use a simple password? Because I thought an easy-to-remember password would be more convenient. • Why did I care more about comfort than safety? Because I didn't understand the importance of a strong password. • Why didn't I understand the importance of a strong password? Because I didn't have enough knowledge about cybersecurity threats.	• Why did you lose access to your account? Because my friend changed his password. • Why did you give your friend your password? Because he needed access to the game. • Why did you think it was okay to share your password? Because I trusted that my colleague would not abuse this trust. • Why haven't you thought about the consequences? Because I didn't know the risks of sharing passwords. • Why didn't you know the risks? Because before that, I didn't pay attention to the security rules of online accounts.

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KEA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

Solutions

Once the causes have been identified, students can come up with solutions to prevent similar situations from happening in the future, such as:

- Use strong and unique passwords.
- Enable two-factor authentication (2FA).
- Not sharing passwords with other people, even friends.

Tips for teachers:

- Ask students not to look for someone to blame but to try to understand why the problem occurred.
- Use alternative questions to build trust and encourage honest reflection.
- At the end of the session, encourage students to come up with solutions that can prevent such problems in the future.
- Focus on ideas for solutions that address the problems at the bottom of the page.

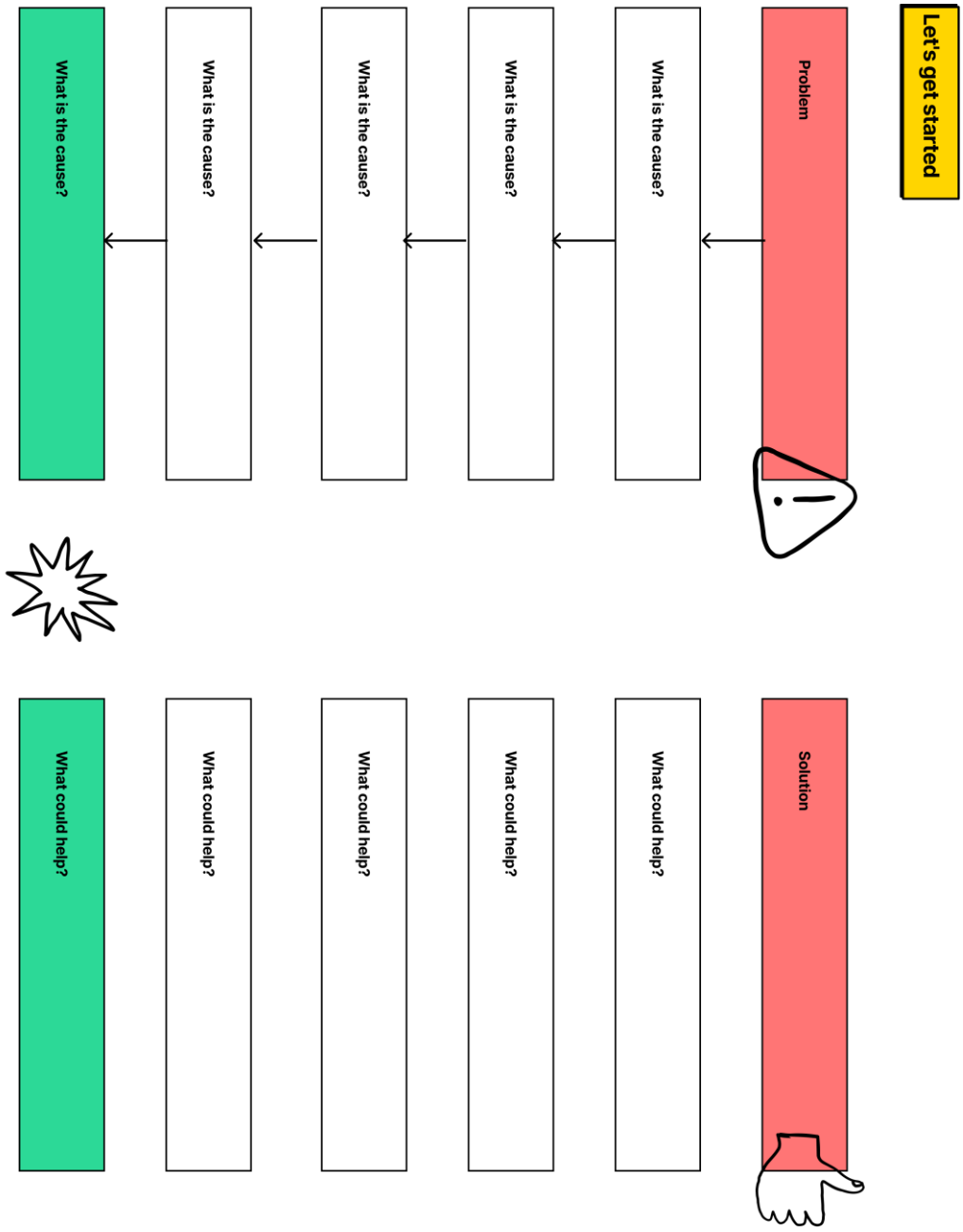
Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 2 – PASSWORDS

Worksheet No. 1

The task is to identify the problem, understand its causes, and come up with solutions to help prevent similar situations from happening in the future. At the beginning, write down what the main problem is in the case you are analyzing (e.g. "The account has been taken over by a hacker", "Loss of access to the account", "Data theft"). Think about what is the cause of this situation (Why did this problem occur? What is its cause?). Dig deeper.

In the next step, think about What could help? Write down ideas in relation to the different causes of problems (starting with those at the bottom of the paper).



Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 2 – PASSWORDS

Worksheet No. 2 Password Game

Duration: approx. 15 minutes for a class of 25 people
Preparation:

1. Prepare 10-15 sticky notes with passwords (list below).
2. Divide the class into 5 groups of 5 people.

Rules of the game:
Division of roles in groups:

1. Each group chooses 1 person as the "clue giver" and the rest are the "guessers".
2. The roles change each round.

Gameplay:

1. The "clue giver" draws a piece of paper with a password.
2. Within 30 seconds, he gives the group cues (only one or two words).
3. The group has 3 attempts to guess the password.
4. If they don't guess in time, the password moves to the next group (optional).

Scoring:

1. The group receives 2 points for guessing the password.
2. If they don't guess, they lose their turn (but don't lose points).

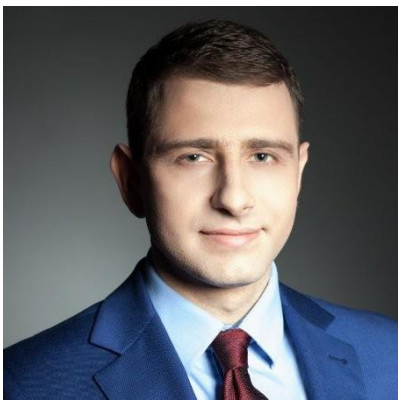
Rotation:
After each round, the "clue giver" in the group changes.
The game lasts until the cards are exhausted or the time runs out (15 minutes).

qwerty	password	letmein
iloveyou	admin	welcome
dragon	master	hello
whatever	freedom	token
sunshine	starwars	trustno1

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

Authors & Experts

Weronika Kędzierska - an expert in the field of soft aspects of cybersecurity, focusing on creating a secure cybersecurity base for young organizations. He specializes in developing effective teams, organizational changes and implementing innovation strategies. As an independent consultant and coach, she helps leaders and teams build engagement and collaboration. Valued for creative and valuable sessions that effectively inspire teams to achieve their goals.



Mateusz Pękala - specialist in raising awareness of information security, security compliance, information security auditing and risk management. He has many years of experience as an auditor, trainer and consultant in the field of information security. He is a member of professional organizations such as ISSA Poland and ISACA. He is certified as Certified in Risk and Information Systems Control™ (CRISC), Certified Information Security Professional (CISSP), Certified Data Privacy Solutions Engineer™ (CDPSE)® and Certified Information Systems Auditor® (CISA), as well as certified as an auditor in the field of ISO 27001.

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

More information about project

Funded by the European Union, the views and opinions expressed herein are solely those of the author(s) and do not necessarily represent the views of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the EACEA can be held accountable for these perspectives.

PROJECT NO. 2023-2-PL01-KA210-VET-000176822

- https://www.coventry.ac.uk/wroclaw/
- https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/
- https://eccedu.net/

CYBERSEC
EDUCHECK

Co-funded by the European Union
LEADER: Research Institute Europe | Coventry University
PARTNERS: STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION