Incidents: Responding Effectively to Cyber Incidents

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

LESSON 3 - Incidents

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 3 – INCIDENTS

Dear,

We present to you a lesson plan on digital security incidents, a key element in managing the risk related to the protection of personal data and IT systems. Our 45-minute class is designed to educate students on how to respond effectively to security incidents, including changing passwords, reviewing security measures, and reporting breaches. We will also focus on the importance of regular backups and best practices for creating them. Students will learn about tools such as Have I Been Pwned for monitoring data security and will develop analytical skills and critical thinking to better assess threats and respond to them effectively in the future.

During the classes, we provide practical exercises and discussions to strengthen the acquired knowledge. We understand that 45 minutes is a limited amount of time, so we suggest spreading the topic over several sessions if necessary, allowing students to dig deeper and better understand the issues.

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

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 objectives

- **Explicit purposes**:
  - Incident Response: Students will know what steps to take when a security breach is detected, such as changing passwords and reviewing security.
  - The Importance of Backups: Students will understand the importance of regular backups and how to perform them.
  - Tools and Services: Students will learn how to use tools such as https://haveibeenpwned.com/ to check if their data has been compromised
  - Developing analysis and critical thinking skills.
- **Hidden Goals**:
  - Strengthening cooperation in the group.
  - Encouraging independent thinking and problem-solving.

Context - keywords

security incidents, incident response, backups, data security, monitoring tools, cybersecurity

- **Justification for the choice of topic**:

In the era of widespread access to technology and the Internet, the risk of security incidents increases, especially when users are not aware of how to respond appropriately to breaches. Young people often use various online services, which increases the chances of losing private data or having their accounts hacked.

Knowing how to respond effectively to such incidents, including password changes and security reviews, is crucial to protecting your personal data.

Understanding the importance of regular backups and knowing how to use monitoring tools like Have I Been Pwned helps you minimize the impact of security breaches.

Education in incident management and developing analytical and critical thinking skills in the context of cybersecurity are important for building awareness of threats and a responsible approach to data protection in the digital world.

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

LESSON 3 – INCIDENTS

Lesson Preparation

- **Materials**:
  - Multimedia presentation [Digital Security Incidents].
  - Worksheets with exercises.
  - Whiteboard (traditional or interactive).
  - Computers/tablets with internet access (if needed).
- **Space**:
  - The room is equipped with a projector.
  - Arrangement of desks in a way that allows work in groups or individually.

Lesson structure

Purpose	Activity	Time	Materials
Introduction	Presentation of the topic. The teacher asks the students What do you mean by the word Incident? What examples of security incidents do you know? Anything from your experience? The teacher presents some examples of security incidents.	5 min	Presentation, whiteboard
Mini Quiz – Vulnerability Check	The teacher asks the students 7 questions "Check your vulnerability to hacker attacks" 1. Can someone want to attack you? a) No, because I don't have any important data that can be sold b) Yes, because someone can use my social media account to deceive others c) Yes, because someone can encrypt my data and demand a ransom 2. Do you use the same password for several different accounts? a) Yes, because they are easier to remember b) No, I have a unique password for each account c) I use one master password and minor modifications on other accounts	10 min	Presentation

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

	3. Do you verify the sources of the links you receive in emails or messages? a) Not always, I usually click if the sender looks familiar b) I always check if the link is safe before clicking c) Only if the message seems suspicious 4. What do you do when you receive a suspicious email asking for your data? a) I ignore it or delete it b) I check the sender's details and links before I make a decision c) I open but do not enter any data 5. What steps do you take to protect your devices? a) I don't use any additional security features b) I have an antivirus installed and I update it regularly c) I use an antivirus, update my software, and use a password manager 6. Do you think your personal information is valuable to others? a) No, no one will want my data b) Yes, they can be used for identity theft or fraud c) Only my bank details or passwords are valid 7. What do you do when you see suspicious activity on your account? a) Nothing, maybe it's a mistake b) I change my password immediately and check my other accounts c) I wait and see if the situation repeats itself The advantage of the "a" answer: You have a lot to improve, hackers can take advantage of your weak security. Increase awareness of threats and introduce better habits. Advantage of "b" answer: You are well prepared and aware of the risks, but it is always worth deepening your knowledge of online security. Advantage of "c" answer: You have basic knowledge, but there is still room for improvement. Work to strengthen the security of your accounts and devices. The teacher asks one or more questions to stimulate discussion:		

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

	- What makes our online accounts vulnerable to attack? - What are the most common online security problems that we may encounter? - What can be the consequences if our account is attacked or stolen? - What can we do to avoid problems with security on the Internet? - Do you know of any known cases where someone has had an online security issue? - How often do we hear about online security issues? Is it rare or everyday? - What to do if someone steals our account or access to it? - What are the differences between different online security issues, such as account theft and viruses? - What apps or programs can help us protect our accounts on the Internet? - Which institutions or organizations are responsible for protecting our data on the Internet?		
Knowledge Transfer - Ransoware	Who is a hacker? Expectations vs reality Wait: Cinematic image: We often imagine hackers as hooded people who can crack any computer system. Superheroes: They look very intelligent and work in the dark to get secret information. Reality: Different types of hackers: There are different types of hackers, including those who help improve security (called "white hats") and those who do something illegal (called "black hats"). Skills and tools: Hackers use special tools and techniques, but their actions are often more technical than in the movies. They don't always work in secret. They often use social engineering. Leak monitoring Teacher presents the Have I Been Pwned https://haveibeenpwned.com/ website A popular tool to check if your email or password has been in data leaks.	10 min	Presentation, multimedia examples

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

	The teacher encourages students to check if their e-mails are also there Optionally to use – **Worksheet No. 1. What to do in case of a password leak?** What to do in case of a password leak? 1. Change your password as soon as possible The sooner you change your password, the less chance that someone will take advantage of your account. How: Go to the website or app, log in, go to settings and change your password to a new, strong password. 2. Verify active logins Checking where you are logged in allows you to log out potentially dangerous sessions. How To: In your account settings, find the "Active Sessions" or "Devices" section and see what places and devices you're logged in from. Log out of suspicious sessions. 3. Change all similar passwords If you use similar passwords on other accounts, change them to avoid other accounts being compromised by people who have obtained one of your passwords. How To: Make sure each account has a unique password that is not like any other. 4. Enter multi-factor authentication (2FA) Multi-factor sign-in provides an extra layer of security, even if someone knows your password. How: Enable 2FA in your account settings by selecting the option to add a second factor, e.g. an SMS code, an authentication app (e.g. Google Authenticator), or a dongle. 5. Get started with a password manager A password manager will help you generate and store strong, unique passwords for each account. How: Install a password manager (e.g., KeePassXC, LastPass) and transfer all your passwords to it. Use it to autofill passwords when you log in.		

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

	Presentation of key information about Ransoware. Ransomware protection – a tool in Windows,		
Practical exercises – data backup	Work individually or in groups to check if the antivirus is enabled. Ransomware – Explanation of what it is and how to protect yourself It's a type of malware that blocks access to your files on your computer and demands a ransom to unlock them. It looks like someone locked you in a room and demanded money to let you go. - Regular backups: Store important files on an external drive or in the cloud. If your computer gets infected, you can restore your files from a backup. - Software updates: Make sure your operating system and all programs are always up to date. New updates often fix security vulnerabilities. - Antivirus: Install and use an antivirus program that can detect and block threats. - Safe Surfing: Don't click on suspicious links or download files from unknown sources. - Education: Learn to recognize suspicious emails and messages that may contain malware. Check in the settings of the machines whether ransomware protection is enabled on their computer.	15 min	Computers

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

	The 3-2-1 Rule 3 copies of your data: Have at least three copies of your data. One copy is the original and the others are backups. 2 different media: Store these copies on two different types of media. For example, one copy on your computer and another on an external hard drive. 1 offline backup: Have at least one backup that isn't connected to the internet to keep it safe even if your computer gets infected with a virus. Example for a 13-year-old: Imagine that you have important photos and projects on your computer. You want to make sure you don't lose this data even if something goes wrong. Here's how you can apply the 3-2-1 rule: 3 copies of your data: Make three copies of your photos. One copy is the one on your computer, and the other is on an external hard drive (e.g. a flash drive). You can put a third copy in the cloud (e.g. Google Drive). 2 different media: Store these copies on different media. For example, one copy on your computer, another on a USB stick, and a third in the cloud. A flash drive and a cloud drive are different carriers. 1 Offline Copy: Keep the flash drive (with the second copy) in a safe place that is not constantly connected to the Internet. This secures your data even if your computer crashes or is attacked by a virus.		
Discussion of the results and discussion	Presentation of the results of work, discussion, explanation of more difficult issues.	10 min	Whiteboard, notes
Summary and reflection	Summary of key issues. An encouragement to reflect on the topic.	5 min	Presentation

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

LESSON 3 – INCIDENTS

Worksheet for Students 1 Comment for Teacher

Objective: To help students understand how to respond to a password leak and what steps to take to minimize its impact.

Duration: 15-30 minutes

Activity description:

1. Introduction to the situation: Students are informed that their password has been leaked (this could be a fictitious situation, e.g. "You receive an email that your account has been hacked").

   Question for students: What do you think, feel, and do when you learn about a password leak? (Worksheet No. 1)

2. Preparing to tell a story: As part of a group, students prepare a story, starting with an "unfortunate event" – learning about a password leak. They should share their thoughts, emotions, and actions they took in this situation. There are three questions to start with:
   What do you think? – What thoughts come to your mind when you find out that your password has been stolen? Wondering what could happen to your data?
   What do you feel? – What emotions are you experiencing at the moment? Do you feel panic, anxiety, anger, maybe shame? How do you react to this situation?
   What are you doing? – What steps are you taking to fix the situation? Do you change your password, contact your administrator, check your account? What exactly are you doing to keep your data safe?
   Events – What can be the consequences of this event? What can happen? (e.g. hacking into a mailbox/popular website where there was the same password).
3. Story Work: Students use the worksheet as a base for creating their story. They should point out key events (e.g., learning about a password leak) and think about how to bring the story to a positive ending (the so-called happy ending).
4. Groups Spotlight: Each group presents their story, describing the emotions and actions taken after a password has been leaked.
5. Joint discussion of activities: Based on the stories presented, the teacher discusses the appropriate steps to take after a password leak, e.g.:
   - Password change on all websites where the same password was used
   - Check your login history (if available)
   - Contact your site administrator or technical support
   - Using a password manager and enabling two-factor authentication
   - Monitor your account for unusual activity

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

LESSON 3 – INCIDENTS

Worksheet for Students 1

What to do in case of password leak?

Event	What do I think?	What do I feel?	What do I do?
OH NO			

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

Optional homework

- **Check your email addresses:**

Use the Have I Been Pwned service and check if your email addresses have been involved in data leaks.

Make a list of email addresses that have been leaked.

- **Stay informed about new leaks:**

Use the Have I Been Pwned notification for new leaks. Enter your email addresses to be notified of future leaks related to these addresses.

- **Change passwords:**

Change the passwords of the accounts that were involved in the leaks. Use strong, random passwords. You can use a password manager like KeePassXC to generate and store new passwords.

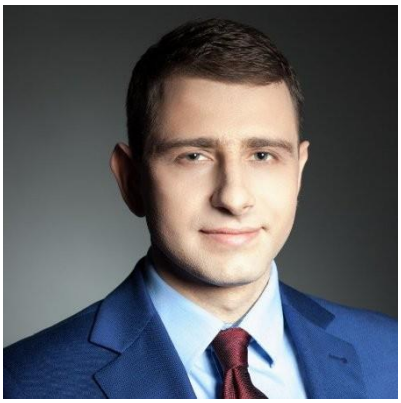
- **Create backups:**

Select important files such as documents, photos, and other data that you want to protect from loss. Use external storage (e.g. external drive) or the cloud (e.g. Google Drive, OneDrive) to back up these files. Make sure that access to your backups is protected by a strong password and that you update your backups regularly.

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: KREA 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/

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