

# A Day in the Life of an Employee



Domain	Vulnerabilities, Attack, Techniques, and Threats
Topic Covered	Threat scenarios and threat prevention
Objectives	<ul style="list-style-type: none"><li>• To raise awareness about potential security risks in the workplace.</li><li>• To identify and discuss behaviours that could put an organisation's security at risk.</li><li>• To educate participants on best practices for staying secure in the workplace.</li><li>• To encourage participants to take personal responsibility for maintaining a secure workplace environment.</li><li>• To promote critical thinking and problem-solving skills through note-taking and group discussion.</li></ul>
Duration	60 minutes
Kind of Method	<ul style="list-style-type: none"><li>• Interactive</li><li>• Presentation and Group Work</li></ul>
Required Materials	<ul style="list-style-type: none"><li>• Note-taking materials for participants</li></ul>



Co-funded by  
the European Union

[www.cyberyouthproject.com](http://www.cyberyouthproject.com)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them  
2021-1-IT03-KA220-YOU-000028668

## Learning Setting and Activity Description

### Overview

This activity raises awareness about workplace security risks through a story-based approach. Participants take note of potentially risky behaviours in the story and discuss them in groups. The activity promotes personal responsibility for maintaining a secure workplace and encourages critical thinking and problem-solving skills.

### Instructions

- Topics introduction (presentation).
- The educator gathers the participants, divide them in groups and gives each group a pen and paper to take notes.
- The educator explains that he/she will be telling a story about a typical day in the life of an employee.
- The educator instructs the participants to listen carefully to the story and to take notes on any “strange” behaviours or actions.



<p>Learning Setting and Activity Description</p>	<ul style="list-style-type: none"> <li>• The educator tells the story (see <i>Supporting Material</i>) and allow the participants a few minutes to take notes.</li> <li>• After telling the story, the educator asks the participants to share what they noticed and compile a list of behaviours that could put an organisation's security at risk.</li> <li>• The educator leads a discussion about the potential consequences of these behaviours and discuss best practices for staying secure in the workplace.</li> </ul>
<p>Activity Evaluation/ Reflection</p>	<p>After telling the story, the educator engages the participants in a discussion about the potential security risks that were present in the story. Participants can discuss the behaviors that Alice displayed and the potential consequences of these behaviors on the organization's security. Finally, the group can discuss best practices for staying secure in the workplace, such as encrypting data, locking computers when away from the desk, and being cautious with email attachments and unknown USB drives.</p>



Supporting Materials	Presentation	
	Story	



Co-funded by  
the European Union

[www.cyberyouthproject.com](http://www.cyberyouthproject.com)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

# Spot the Security Threats



<b>Domain</b>	<b>Vulnerabilities, Attack, Techniques, and Threats</b>
<b>Topic Covered</b>	Security Awareness
<b>Objectives</b>	<ul style="list-style-type: none"><li>• To increase participants' awareness of common security threats in the workplace</li><li>• To encourage participants to develop good security practices</li><li>• To provide an engaging and interactive way to learn about cybersecurity</li></ul>
<b>Duration</b>	60 minutes
<b>Kind of Method</b>	<ul style="list-style-type: none"><li>• interactive</li><li>• Presentation and Group Work</li></ul>
<b>Required Materials</b>	<ul style="list-style-type: none"><li>• Note-taking materials for participants</li><li>• A device with a projector or screen to display the pictures</li><li>• A timer to keep track of the allotted viewing time</li></ul>



Co-funded by  
the European Union

[www.cyberyouthproject.com](http://www.cyberyouthproject.com)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them  
2021-1-IT03-KA220-YOU-000028668

## Learning Setting and Activity Description

### Overview

This activity raises awareness about workplace security risks through a "spot the threat" approach. Participants will view a series of pictures depicting common security threats in a workplace environment, take note of potentially risky behaviours they identify and discuss them in groups. The activity promotes personal responsibility for maintaining a secure workplace and encourages critical thinking and problem-solving skills.



### Instructions

- Topics introduction (presentation).
- The educator gathers the participants, divides them in groups and gives each group a pen and paper to take notes.
- The educator will display the first picture and give participants a set amount of time (e.g. 30 seconds) to view the picture and identify any security threats they can spot. After the time is up, move on to the next picture, repeating the process until all pictures have been shown.



<p>Learning Setting and Activity Description</p>	<ul style="list-style-type: none"> <li>• After all pictures have been shown, the educator facilitates a discussion among participants about what they observed in the pictures. Participants can share their notes and discuss their thought processes for identifying the security threats. The educator can also provide additional information and context about each security threat to deepen participants' understanding.</li> <li>• At the end, the educator summarises the key takeaways from the activity and encourages participants to apply what they learned in their own workplaces.</li> </ul>
<p>Activity Evaluation/ Reflection</p>	<p>After identifying the security threats in the pictures, it's important to discuss ways to mitigate those threats in a workplace environment. Some possible solutions include implementing password policies, securing hardware (such as laptops, USB drives, and network cables) when not in use, using encryption for sensitive data, and regularly training employees on cybersecurity best practices.</p>



<p style="text-align: center;"><b>Activity Evaluation/ Reflection</b></p>	<p>It's also important to create a culture of security awareness in the workplace, where all employees feel responsible for maintaining a secure environment. By working together to identify and address security threats, we can help protect our workplaces from cyber attacks and data breaches.</p>
<p style="text-align: center;"><b>Supporting Materials</b></p>	<p>Presentation </p> <p>Pictures </p>





# Spot the Phish



Domain	Vulnerabilities, Attack, Techniques, and Threats
Topic Covered	Phishing
Objectives	<ul style="list-style-type: none"><li>• To educate participants about the risks of phishing attacks.</li><li>• To teach participants how to identify phishing attempts.</li><li>• To raise awareness about the importance of online security.</li><li>• To promote critical thinking and problem-solving skills through a game-based approach.</li></ul>
Duration	60 minutes
Kind of Method	<ul style="list-style-type: none"><li>• Interactive</li><li>• Presentation and Group Work</li></ul>
Required Materials	<ul style="list-style-type: none"><li>• A device with internet access for each group of participants</li><li>• Access to this website</li></ul>



Co-funded by  
the European Union

[www.cyberyouthproject.com](http://www.cyberyouthproject.com)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

## Learning Setting and Activity Description

### Overview

This activity is designed to educate participants about phishing and raise awareness of the risks associated with this type of cyber attack.

Through a game-based approach, participants will learn how to identify phishing attempts and understand the importance of being vigilant when it comes to online security.

### Instructions

- Topics introduction (presentation).
- The educator gathers the participants, divides them in groups and makes sure that each group has a device with internet access.
- The educator explains that the game involves identifying real and fake emails, and that the participants will need to use their critical thinking skills to spot the phishing attempts.
- The educator provides access to this website.
- The educator instructs the participants to play the game and record their scores.



Learning Setting  
and Activity  
Description

- After everyone has completed the quiz, the educator leads a discussion about the types of phishing attempts that were presented, and the strategies that participants used to identify them.
- At the end the educator discusses the importance of being vigilant when it comes to online security and encourages participants to take steps to protect themselves from phishing attacks.

Activity  
Evaluation/  
Reflection

After playing the game, the educator can engage the participants in a discussion about phishing and the importance of online security. Participants can discuss the types of phishing attempts that were presented and the strategies they used to identify them. The group can also discuss best practices for avoiding phishing attacks, such as never clicking on suspicious links, verifying the sender's email address, and keeping anti-virus software up-to-date.



Supporting  
Materials

Presentation



Quiz Link



Co-funded by  
the European Union

[www.cyberyouthproject.com](http://www.cyberyouthproject.com)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668