



## LESSON 1 - Phishing

# Phishing: Understanding CyberCriminal Tactics and How to Stay Safe





## LESSON 1 - Phishing

### LESSON 1 - Phishing

#### 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

*The publication is distributed under the terms of the Creative Commons Attribution-NonCommercial (CC BY-NC) 4.0 International license*



## LESSON 1 - Phishing

**Dear,**

*We provide you with a lesson plan on phishing, a significant threat in the field of digital security. Phishing is one of the most common ways cybercriminals try to phish information, in our lesson we focused on the key aspects related to this social engineering.*

*Our 45-minute classes are designed to understand phishing, recognize suspicious emails, text messages, and websites, and learn how to respond to phishing attempts and where to report such incidents.*

*The classes are planned for a short time, so we will focus on key activities, such as analyzing sample phishing emails and discussing incident reporting procedures. If you have more time, we suggest breaking this topic down into smaller segments to allow for deeper analysis and a better understanding of the issue.*

*The scenario and teaching materials, including the presentation, can be adapted to the needs of your group.*

*Best regards,*

*CyberSec Project Team*



## LESSON 1 - Phishing

### Table of contents

Lesson objectives .....	5
Context - keywords .....	5
Lesson Preparation .....	6
Lesson structure .....	7
Resources and knowledge for teachers .....	8
Authors and experts .....	12



## LESSON 1 - Phishing

---

### Lesson objectives

- **Explicit purposes:**
  - Understanding the definition of phishing and the techniques used by cybercriminals
  - Recognize suspicious emails, text messages, and websites
  - Ability to respond to phishing attempts and knowledge of incident reporting procedures.
- **Hidden Goals:**
  - Developing analytical and critical thinking skills when evaluating news and websites
  - Strengthening communication skills by sharing experiences and knowledge about phishing
  - Increase awareness of personal security on the Internet and responsibility for the protection of personal data

---

### Context - keywords

phishing, digital security, social engineering techniques, liability

- **Justification for the choice of topic:**
  - Phishing is one of the most common threats on the Internet, which can lead to identity theft, data loss, and financial loss.
  - Understanding phishing techniques and being able to recognize them is crucial for protecting personal information and digital security.
  - Education about phishing allows you not only to increase awareness of threats, but also to develop critical thinking skills and responsibility online.
  - Shaping attitudes such as vigilance and the ability to respond to phishing attempts contributes to greater security on the Internet and supports the construction of a safer digital space.



## LESSON 1 - Phishing

### Lesson Preparation

- **Materials:**

- Multimedia presentation [Phishing – how cybercriminals cheat and how to defend yourself].
- Worksheets with exercises.
- Whiteboard (traditional or interactive).

- **Experience:**

o Use an activity just before the lesson to introduce students to the topic of phishing, using the element of surprise and engaging them in the experience. Examples:

“Important message from the teacher”. Process: Send students an email (or show on the board/projector) a message from the “teacher” asking them to click on a link, e.g. to fill out a “survey about the school”. The link leads to a fake website (e.g. a form filled with funny questions).

“Lost USB stick”. Process: Put a USB stick in a visible place with a label e.g. “Student grades – top secret” and see who picks it up. After a while, inform them that it is “hardware phishing”.

“Fake SMS from the Principal”. Process: Display an SMS message on the screen: “From the Principal: Students of class X are asked to confirm their attendance by clicking on the link: [link]”.

“Logging in to a fake Wi-Fi network”. Procedure: Before the lesson, put out a sign saying “New Wi-Fi network: Free\_School\_WiFi” with the password and tell students that it is free internet. After a few minutes, explain that this is “an example of phishing through fake Wi-Fi.”

- **Space:**

- Arrangement of desks in a way that allows work in groups or individually.

## LESSON 1 - Phishing

### Lesson structure

Purpose	Activity	Time	Materials
<b>Introduction</b>	Presentation of the topic of the lesson: phishing and social engineering. Explanation of the objectives of the class: learning about the types of threats, the ability to recognize phishing attempts and learning about defense methods.	5 min	Presentation, whiteboard
<b>Knowledge transfer</b>	Types of threats: Phishing: phishing through fake emails, SMS (smishing), etc. Social engineering: manipulation techniques used to deceive the user.	10 min	Presentation, multimedia examples
<b>Practical exercises</b>	Recognizing Phishing - Sheet 1: Work in groups on the task of recognizing phishing attempts.  Phishing Simulator – Used to generate sheet 1 <a href="https://caniphish.com/email-phishing-simulator?email=Gmail-Blocked-Login#emailTitle">https://caniphish.com/email-phishing-simulator?email=Gmail-Blocked-Login#emailTitle</a>  <b>Overview of the results:</b> Presentation of the results of the work of the groups. Discussion on the criteria used and explanation of more difficult issues.  <b>Group discussion:</b> Questions to support the discussion: <ul style="list-style-type: none"> <li><input type="checkbox"/> What elements were the most convincing in the analyzed phishing attempts?</li> <li><input type="checkbox"/> What social engineering techniques were used and why?</li> <li><input type="checkbox"/> What made you recognize a phishing attempt?</li> </ul>	15 min	Worksheets, Computers/Tablets
<b>Discussion of the results and discussion</b>	Phishing Recognition: Criteria: Natural bait, curiosity, delivery delay, win message, quick action, language errors, fear of charges, unusual sender name, unofficial link.	10 min	Whiteboard, notes

## LESSON 1 - Phishing

<p><b>Summary and reflection</b></p>	<p>Invitation to test using the tool:  <a href="https://phishingquiz.withgoogle.com/">https://phishingquiz.withgoogle.com/</a></p> <p>Summary of key issues:            Reiterate the most important information about recognizing and defending against phishing.            Emphasizing the role of conscious use of electronic communication.</p> <p>Reflection on the topic:            An encouragement to reflect on how to protect yourself from phishing in everyday life.            Information about reporting phishing attempts at 8080.</p> <p>Phone Security:            Emphasize that a phone is also a computer, and discuss the principles of securing mobile devices.</p>	<p>5 min</p>	<p>Presentation</p>

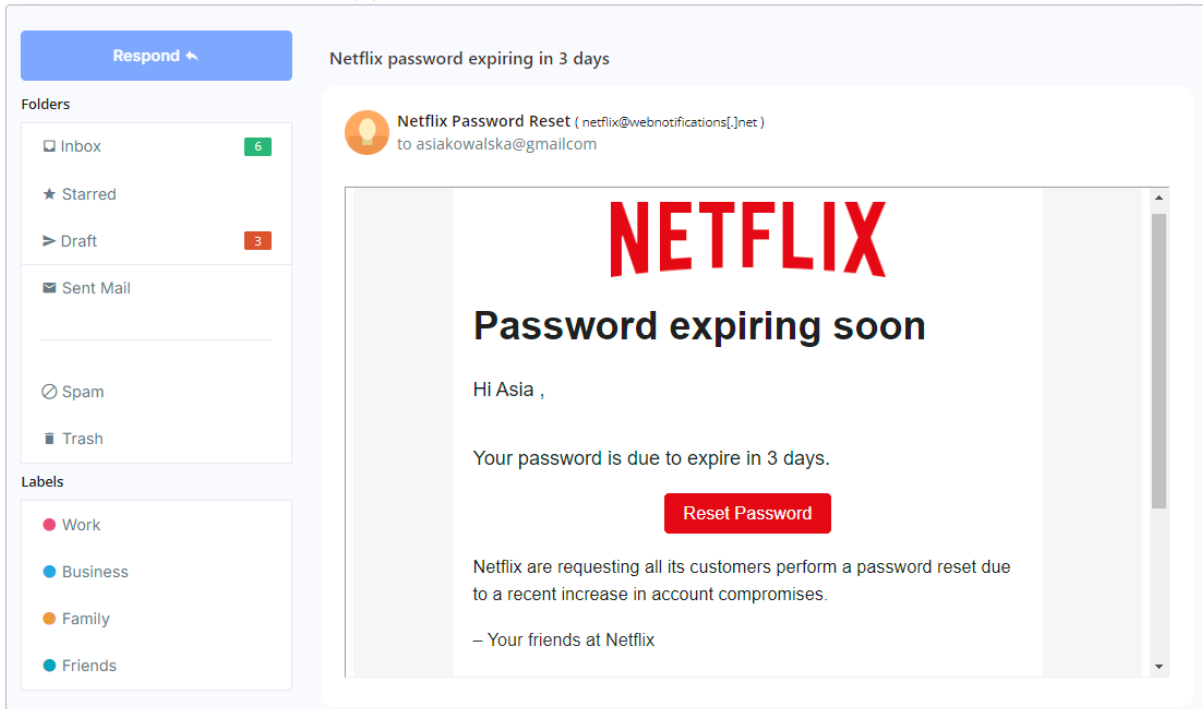
## Resources and knowledge for teachers

### Educational websites and portals

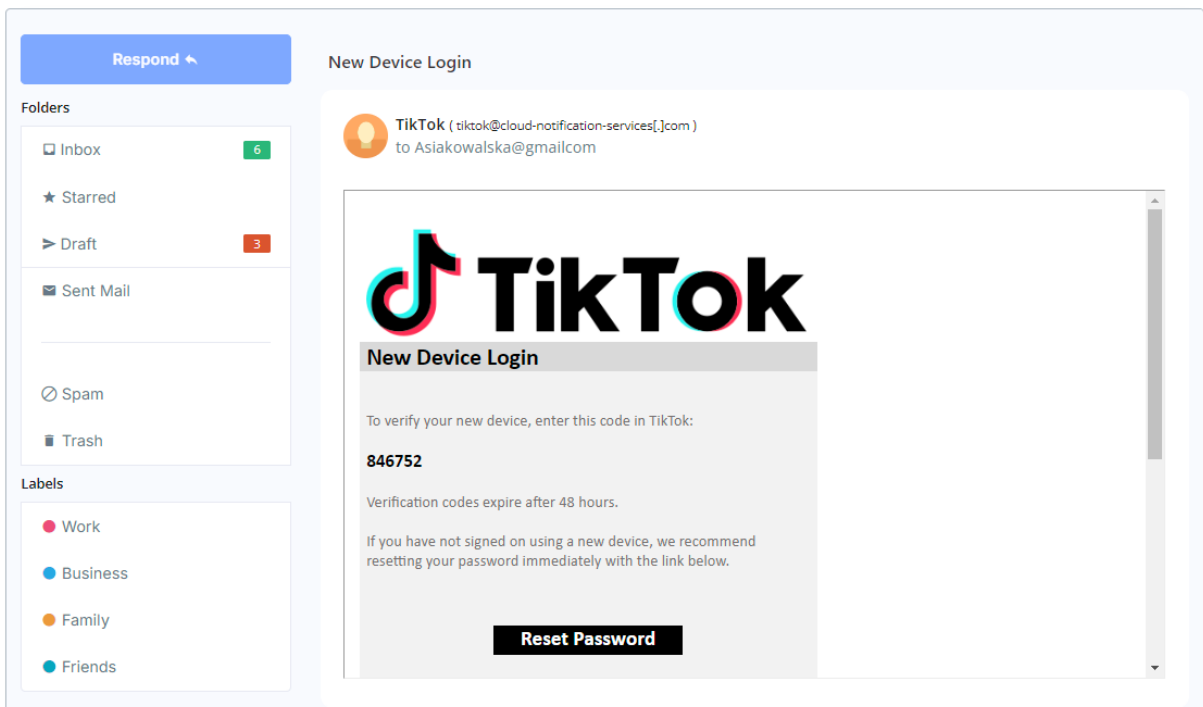
<https://cdn.sekurak.pl/ebook/ebook-sekurak-bezpieczenstwo-2022.pdf>



## LESSON 1 - Phishing



Source: <https://caniphish.com/email-phishing-simulator?email=Gmail-Blocked-Login#emailTitle>



## LESSON 1 - Phishing

Respond ↩

The password for your 1Password account has been changed

**Folders**

- Inbox 6
- ★ Starred
- Draft 3
- ✉ Sent Mail
- 🗑 Spam
- 🗑 Trash

**Labels**

- Work
- Business
- Family
- Friends

**1Password** ( hello[,]1password@webnotifications[.]net )  
to asiakowalska@gmail.com

Hi Asia Kowalska,

The password for your 1Password account has been changed.  
If you didn't change your password, [click here to reverse this change](#) in the next 24 hours.

**1PasswOrd**  
made by 1Password • sent to: [asiakowalska@gmail.com](mailto:asiakowalska@gmail.com)  
4711 Yonge St. 10th Floor • Toronto • Ontario • M2N 6K6 • Canada

Respond ↩

New login to Instagram from Chrome on Windows

**Folders**

- Inbox 6
- ★ Starred
- Draft 3
- ✉ Sent Mail
- 🗑 Spam
- 🗑 Trash

**Labels**

- Work
- Business
- Family
- Friends

**Instagram Notifications** ( instagram@webnotifications[.]net )  
to asiakowalska@gmail.com

**Instagram**

**Asia, we noticed a new login.**

We noticed a login from a device you don't usually use.

Windows · Chrome · Bangkok, Thailand  
Tue Sep 17 2024 12:16:21 GMT+0200 (czas srodkowoeuropejski letni) (PDT)

If this was you, you can safely disregard this email. If this wasn't you, you can [secure your account here](#).

[Learn more about keeping your account secure.](#)

---

from  
 Meta

## LESSON 1 - Phishing


Respond ↩
Password Reset Request


**Folders**

- 📁 Inbox 6
- ★ Starred
- 📄 Draft 3
- ✉ Sent Mail
- 🗑 Spam
- 🗑 Trash

**Labels**

- Work
- Business
- Family
- Friends


**Slack** ( slack@webnotifications[.]net )  
to asiakowalska@gmail[.]com



Reset your Slack workspace password

You asked us to send you a password reset link for [auth.slack.com](https://auth.slack.com). This password reset request is for [asiakowalska@gmail.com](mailto:asiakowalska@gmail.com).

If you didn't authorise this password reset request, please [notify](#) the team at slack.

This password reset link will be valid for the next 24 hours and is tied to the email address: [asiakowalska@gmail.com](mailto:asiakowalska@gmail.com). If you have any issues, please contact your administrator for support.

Reset Password


Respond ↩
Security alert: Sign-in attempt blocked.


**Folders**

- 📁 Inbox 6
- ★ Starred
- 📄 Draft 3
- ✉ Sent Mail
- 🗑 Spam
- 🗑 Trash

**Labels**

- Work
- Business
- Family
- Friends


**Google Notifications** ( google-support@webnotifications[.]net )  
to asiakowalska@gmail[.]com



!

Sign-in attempt was blocked

asiakowalska@gmail.com

Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one else has access.

Check activity

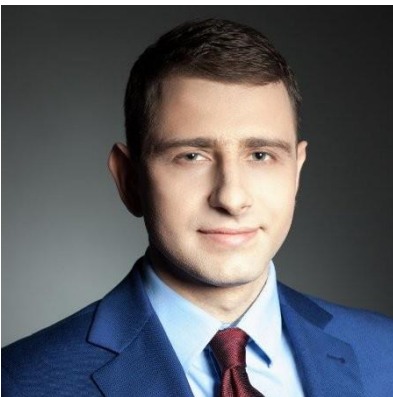


## LESSON 1 - Phishing

### Authors and 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.



## LESSON 1 - Phishing

### 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.

All outcomes generated within this project are accessible under open licenses (CC BY-NC 4.0). They may be utilized at no cost and without limitations. Reproduction or modification of these materials, in whole or in part, without the author's permission is strictly forbidden. When utilizing the results, it is essential to acknowledge the source of funding and the authors.

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

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

