



CYBERSEC  
EDUCHECK

## LEKCJA 1 - Phishing

# Phishing: jak cyberprzestępcy oszukują i jak się bronić





## LEKCJA 1 - Phishing

### LEKCJA 1 - Phishing

#### Scenariusz lekcji dla szkół ponadpodstawowych

Scenariusz opracowany w ramach projektu „CyberSec EduCheck” – projekt nr. 2023-2-PL01-KA210-VET-000176822

**Autorzy scenariusza:** Weronika Kędzierska, Mateusz Pękala - Coventry University Wrocław

**Redakcja merytoryczna:** Pavla Vybíhalová - European Centre for Career Education

**Projekt graficzny:** Karolina Kornecka-Kupiec, Jadwiga Maj – Stowarzyszenie KREA

Wrocław 2024

*Publikacja jest rozpowszechniana na zasadach licencji Creative Commons Uznanie autorstwa – Użycie niekomercyjne (CC BY-NC) 4.0 Międzynarodowe*

## LEKCJA 1 - Phishing

### **Szanowni Państwo,**

*Przekazujemy Państwu scenariusz zajęć na temat phishingu, istotnego zagrożenia w zakresie bezpieczeństwa cyfrowego. Phishing jest jednym z najczęstszych sposobów, w jaki cyberprzestępcy próbują wyłudzić informacje, w naszej lekcji skupiliśmy się na kluczowych aspektach związanych z tym socjotechnikami.*

*Nasze 45-minutowe zajęcia mają na celu zrozumienie phishingu, rozpoznawanie podejrzanych e-maili, wiadomości tekstowych i stron internetowych, a także naukę, jak reagować na phishingowe próby i gdzie zgłaszać takie incydenty.*

*Zajęcia są zaplanowane na krótki czas, dlatego skoncentrujemy się na kluczowych działaniach, takich jak analiza przykładowych wiadomości phishingowych oraz omówienie procedur zgłaszania incydentów. Jeśli mają Państwo więcej czasu, sugerujemy rozbicie tego tematu na mniejsze segmenty, aby umożliwić głębszą analizę i lepsze zrozumienie zagrożenia.*

*Scenariusz oraz materiały dydaktyczne, w tym prezentacja, mogą być dostosowane do potrzeb Państwa grupy.*

*Pozdrawiamy serdecznie,*

*Zespół Projektu CyberSec*



## LEKCJA 1 - Phishing

### Spis treści

Cele lekcji.....	5
Kontekst - słowa kluczowe.....	5
Przygotowanie do lekcji .....	6
Struktura lekcji.....	7
Materiały i wiedza dla nauczycieli .....	8
Autorzy i eksperci.....	12

## LEKCJA 1 - Phishing

---

### Cele lekcji

- **Cele jawne:**
  - Zrozumienie definicji phishingu i technik wykorzystywanych przez cyberprzestępców
  - Rozpoznawanie podejrzanych e-maili, wiadomości tekstowych oraz stron internetowych
  - Umiejętność reagowania na phishingowe próby i znajomość procedur zgłaszania incydentów.
- **Cele ukryte:**
  - Rozwijanie umiejętności analitycznych i krytycznego myślenia przy ocenie wiadomości i stron internetowych
  - Wzmacnianie umiejętności komunikacyjnych poprzez dzielenie się doświadczeniami i wiedzą na temat phishingu
  - Zwiększenie świadomości osobistego bezpieczeństwa w internecie i odpowiedzialności za ochronę danych osobowych

---

### Kontekst - słowa kluczowe

phishing, bezpieczeństwo cyfrowe, techniki socjotechniczne, odpowiedzialność

- **Uzasadnienie wyboru tematu:**
  - Phishing jest jednym z najpowszechniejszych zagrożeń w internecie, które może prowadzić do kradzieży tożsamości, utraty danych oraz strat finansowych.
  - Zrozumienie technik phishingowych i umiejętność ich rozpoznawania są kluczowe dla ochrony osobistych informacji oraz bezpieczeństwa cyfrowego.
  - Edukacja na temat phishingu pozwala nie tylko na zwiększenie świadomości dotyczącej zagrożeń, ale również na rozwijanie umiejętności krytycznego myślenia i odpowiedzialności w sieci.
  - Kształtowanie postaw takich jak czujność oraz umiejętność reagowania na próby phishingowe przyczynia się do większego bezpieczeństwa w internecie oraz wspiera budowę bezpieczniejszej przestrzeni cyfrowej..

## LEKCJA 1 - Phishing

---

### Przygotowanie do lekcji

- **Materiały:**
    - Prezentacja multimedialna [Phishing – jak cyberprzestępcy oszukują i jak się bronić].
    - Arkusze pracy z ćwiczeniami.
    - Tablica (tradycyjna lub interaktywna).
  - **Doświadczenie:**
    - Wykorzystaj aktywność tuż przed lekcją, aby wprowadzić uczniów w temat phishingu, wykorzystując element zaskoczenia i angażując ich w doświadczenie. Przykłady:
      - „Ważna wiadomość od nauczyciela”. Przebieg: Wyślij uczniom e-mail (lub pokaż na tablicy/projektorze) wiadomość od „nauczyciela” z prośbą o kliknięcie linku, np. w celu wypełnienia „ankiety dotyczącej szkoły”. Link prowadzi do fałszywej strony (np. formularz wypełniony zabawnymi pytaniami).
      - „Zgubiony pendrive”. Przebieg: Połóż w widocznym miejscu pendrive z etykietą np. „Oceny uczniów – ściśle tajne” i obserwuj, kto go podniesie. Po chwili poinformuj, że to „phishing sprzętowy”.
      - „Fake SMS od Dyrektora”. Przebieg: Wyświetl na ekranie wiadomość SMS: „Od Dyrektora: Uczniowie klasy X proszeni są o potwierdzenie obecności klikając w link: [link]”.
      - „Logowanie do fikcyjnej sieci Wi-Fi”. Przebieg: Przed lekcją rozłóż tabliczkę „Nowa sieć Wi-Fi: Free\_School\_WiFi” z hasłem i poinformuj uczniów, że to darmowy internet. Po kilku minutach wyjaśnij, że to „przykład phishingu przez fałszywe Wi-Fi”.
  - **Przestrzeń:**
    - Ustawienie ławek w sposób umożliwiający pracę w grupach lub indywidualnie.
-

## LEKCJA 1 - Phishing

### Struktura lekcji

Cel	Aktywność	Czas	Materiały
<b>Wprowadzenie</b>	<p>Prezentowanie tematu lekcji: phishing oraz socjotechniki.</p> <p>Wyjaśnienie celów zajęć: poznanie rodzajów zagrożeń, umiejętność rozpoznawania prób phishingu oraz poznanie metod obrony.</p>	5 min	Prezentacja, tablica
<b>Przekazanie wiedzy</b>	<p>Rodzaje zagrożeń:</p> <p>Phishing: wyłudzenie danych za pomocą fałszywych wiadomości e-mail, SMS-ów (smishing) itp.</p> <p>Socjotechniki: techniki manipulacji wykorzystywane do oszukania użytkownika.</p>	10 min	Prezentacja, przykłady multimedialne
<b>Ćwiczenia praktyczne</b>	<p>Rozpoznawanie phishingu - Arkusz 1: Praca w grupach nad zadaniem rozpoznawania prób phishingu.</p> <p>Phishing Simulator – wykorzystany do wygenerowania arkusza 1</p> <p><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></p> <p>Omówienie wyników: Prezentowanie wyników pracy grup. Dyskusja na temat użytych kryteriów oraz wyjaśnienie trudniejszych zagadnień.</p> <p>Dyskusja grupowa:</p> <p>Pytania wspierające dyskusję: Jakie elementy w analizowanych próbach phishingu były najbardziej przekonujące? Jakie techniki socjotechniczne były użyte i dlaczego?</p>	15 min	Arkusze pracy, komputery/tablety

## LEKCJA 1 - Phishing

	Co sprawiło, że rozpoznałeś próbę phishingu?		
<b>Omówienie wyników i dyskusja</b>	Rozpoznawanie phishingu: Kryteria: przynęta naturalna, ciekawość, opóźnienie dostawy, wiadomość o wygranej, szybkie działanie, błędy językowe, obawa przed opłatami, nietypowa nazwa nadawcy, nieoficjalne link.	10 min	Tablica, notatki
<b>Podsumowanie i refleksja</b>	Zaproszenie do testu przy użyciu narzędzia: <a href="https://phishingquiz.withgoogle.com/">https://phishingquiz.withgoogle.com/</a>  Podsumowanie kluczowych zagadnień: Powtórzenie najważniejszych informacji na temat rozpoznawania i obrony przed phishingiem. Podkreślenie roli świadomego korzystania z komunikacji elektronicznej.  Refleksja nad tematem: Zachęta do refleksji nad tym, jak chronić się przed phishingiem w codziennym życiu. Informacja o zgłaszaniu prób phishingu pod numerem 8080.  Bezpieczeństwo telefonów: Podkreślenie, że telefon to również komputer, i omówienie zasad zabezpieczania urządzeń mobilnych.	5 min	Prezentacja

## Materiały i wiedza dla nauczycieli

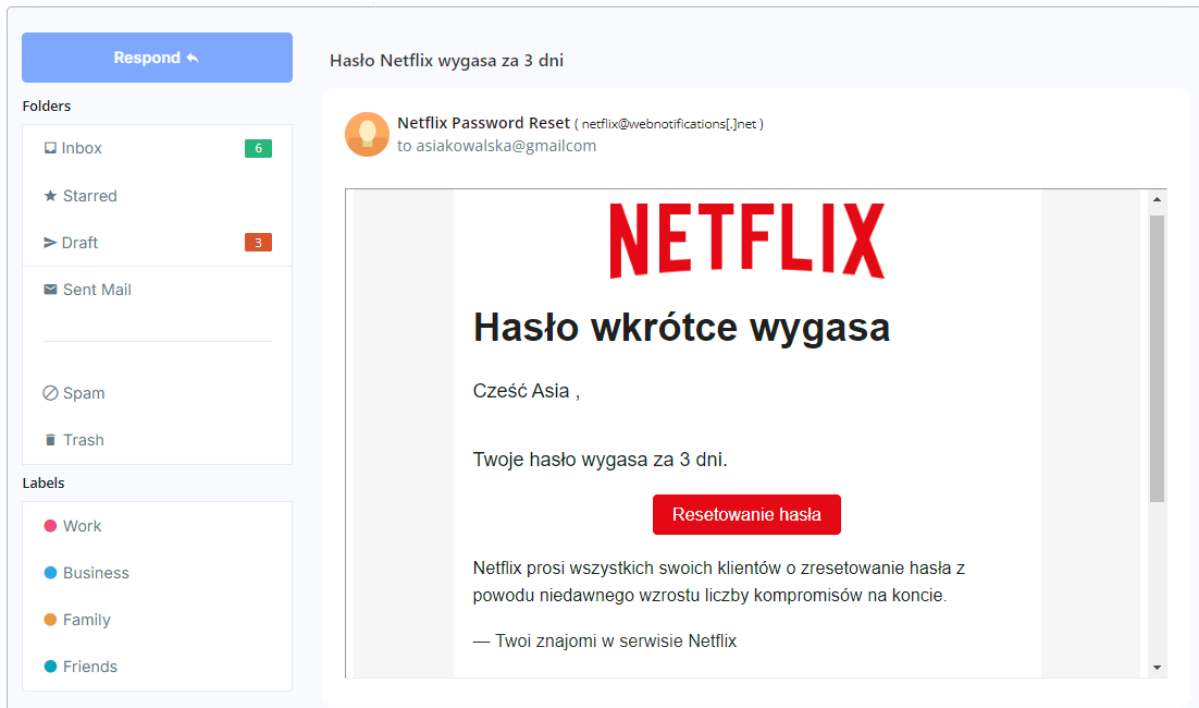
### Strony internetowe i portale edukacyjne

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



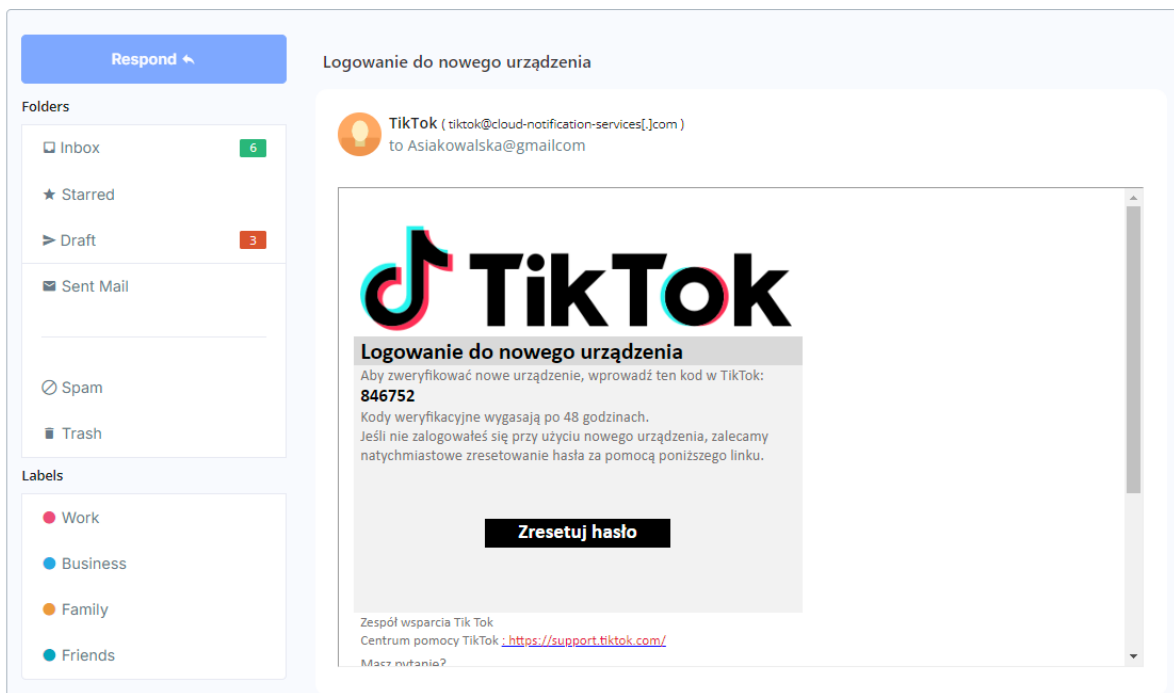
## LEKCJA 1 - Phishing

### Arkusz 1



The screenshot shows a simulated phishing email in a Gmail interface. The email is titled "Hasło Netflix wygasa za 3 dni" (Netflix password expires in 3 days). The sender is "Netflix Password Reset (netflix@webnotifications[.]net)" to "asiakowalska@gmail.com". The email content features the Netflix logo and a message in Polish: "Hasło wkrótce wygasa" (Password expires soon), "Cześć Asia," (Hello Asia), and "Twoje hasło wygasa za 3 dni." (Your password expires in 3 days). A prominent red button labeled "Resetowanie hasła" (Reset password) is visible. Below the button, the text reads: "Netflix prosi wszystkich swoich klientów o zresetowanie hasła z powodu niedawnego wzrostu liczby kompromisów na koncie." (Netflix asks all its customers to reset their password due to a recent increase in account compromises). At the bottom, it says "— Twój znajomy w serwisie Netflix" (— Your friend on Netflix).

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



The screenshot shows a simulated phishing email in a Gmail interface. The email is titled "Logowanie do nowego urządzenia" (Login to new device). The sender is "TikTok (tiktok@cloud-notification-services[.]com)" to "Asiakowalska@gmail.com". The email content features the TikTok logo and a message in Polish: "Logowanie do nowego urządzenia" (Login to new device), "Aby zweryfikować nowe urządzenie, wprowadź ten kod w TikTok: 846752" (To verify the new device, enter this code in TikTok: 846752), "Kody weryfikacyjne wygasają po 48 godzinach." (Verification codes expire after 48 hours), and "Jeśli nie zalogowałeś się przy użyciu nowego urządzenia, zalecamy natychmiastowe zresetowanie hasła za pomocą poniższego linku." (If you did not log in using the new device, we recommend immediately resetting your password using the link below). A prominent black button labeled "Zresetuj hasło" (Reset password) is visible. At the bottom, it says "Zespół wsparcia Tik Tok" (Tik Tok support team), "Centrum pomocy TikTok : <https://support.tiktok.com/>", and "Masz pytania?" (Have questions?).

## LEKCJA 1 - Phishing

Respond ↩

ronika Kedzierska (ae3267@coventry.ac.uk)

**Folders**


- Inbox 6
- Starred
- Draft 3
- Sent Mail
- Spam
- Trash

**Labels**

- Work
- Business
- Family
- Friends

**Hasło do Twojego konta 1Password zostało zmienione**

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



Cześć Asia Kowalska,


Hasło do Twojego konta 1Password zostało zmienione. Jeśli nie zmienisz hasła, [kliknij tutaj, aby cofnąć tę zmianę](#) w ciągu najbliższych 24 godzin.

**1Password**  
wykonane przez 1Password • wysłane do: [asiakowalska@gmail.com](mailto:asiakowalska@gmail.com)  
4711 Yonge St. 10th Floor • Toronto • Ontario • M2N 6K8 • Kanada


Respond ↩

**Nowe logowanie do Instagrama z Chrome w systemie Windows**

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

 **Instagram**

Asia, zauważyliśmy nowy login.  
Zauważyliśmy login z urządzenia, którego zwykle nie używasz.



Windows - Chrome - Bangkok, Tajlandia  
Tue Sep 17 2024 12:17:11 GMT+0200 (czas środkowoeuropejski letni) (PDT)

Jeśli to byłeś ty, możesz bezpiecznie zignorować ten e-mail. Jeśli to nie ty, możesz [zabezpieczyć swoje konto tutaj](#).

Dowiedz się więcej o zabezpieczaniu konta.


from

## LEKCJA 1 - Phishing

Respond ↩

Żądanie resetowania hasła

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



**Resetowanie hasła do obszaru roboczego Slack**

Poprosiłeś nas o przesłanie linku do resetowania hasła dla [auth.slack.com](https://auth.slack.com). To żądanie resetowania hasła **dotyczy asiakowalska@gmailcom**.

Jeśli nie autoryzowałeś tej prośby o zresetowanie hasła, **powiadomić** zespół w slack.

Ten link do resetowania hasła będzie ważny przez następne 24 godziny i jest powiązany z adresem e-mail: **asiakowalska@gmailcom**. Jeśli masz jakiegokolwiek problemy, skontaktuj się z administratorem w celu uzyskania pomocy technicznej.

**Folders**

- Inbox 6
- Starred
- Draft 3
- Sent Mail
- Spam
- Trash

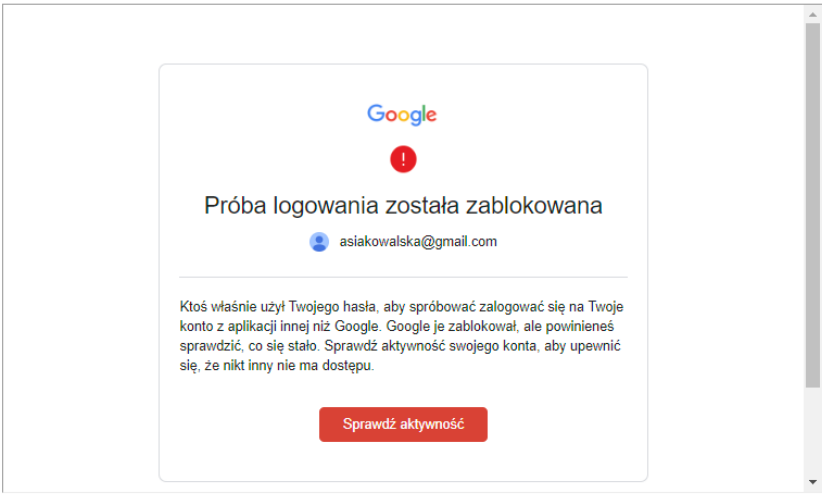
**Labels**

- Work
- Business
- Family
- Friends

Respond ↩

Alert bezpieczeństwa: Próba logowania zablokowana.

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



**Próba logowania została zablokowana**

asiakowalska@gmail.com

Ktoś właśnie użył Twojego hasła, aby spróbować zalogować się na Twoje konto z aplikacji innej niż Google. Google je zablokował, ale powinieneś sprawdzić, co się stało. Sprawdź aktywność swojego konta, aby upewnić się, że nikt inny nie ma dostępu.

**Sprawdź aktywność**

**Folders**

- Inbox 6
- Starred
- Draft 3
- Sent Mail
- Spam
- Trash

**Labels**

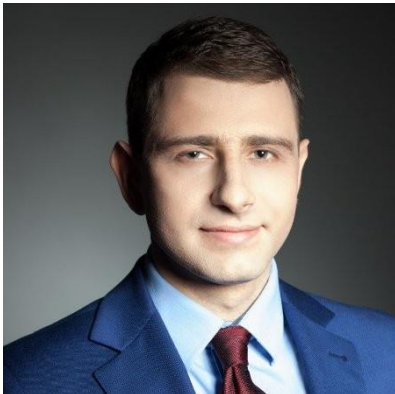
- Work
- Business
- Family
- Friends

## LEKCJA 1 - Phishing

### Autorzy i eksperci



**Weronika Kędzierska** - ekspertka w zakresie miękkich aspektów cyberbezpieczeństwa, skupiająca się na tworzeniu bezpiecznej bazy cyberochrony dla młodych organizacji. Specjalizuje się w rozwijaniu efektywnych zespołów, zmianach organizacyjnych oraz wdrażaniu strategii innowacji. Jako niezależny konsultant i trener, pomaga liderom i zespołom w budowaniu zaangażowania i współpracy. Ceniona za kreatywne i wartościowe sesje, które skutecznie inspirują zespoły do osiągnięcia ich celów.



**Mateusz Pękala** - specjalista w podnoszeniu świadomości bezpieczeństwa informacji, zgodności zabezpieczeń, audytu bezpieczeństwa informacji oraz zarządzaniu ryzykiem. Ma wieloletnie doświadczenie jako audytor, trener i konsultant w obszarze bezpieczeństwa informacji. Jest członkiem organizacji zawodowych, takich jak ISSA Polska i ISACA. Posiada certyfikaty Certified in Risk and Information Systems Control™ (CRISC), Certified Information Security Professional (CISSP), Certified Data Privacy Solutions Engineer™ (CDPSE®) oraz Certified Information Systems Auditor® (CISA), a także certyfikację audytora w zakresie ISO 27001.



## LEKCJA 1 - Phishing

### Więcej informacji o projekcie

Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Unia Europejska ani EACEA nie ponoszą za nie odpowiedzialności.

Wszystkie rezultaty wypracowane w ramach niniejszego projektu udostępniane są na zasadzie otwartych licencji (CC BY-NC 4.0). Można z nich korzystać bezpłatnie i bez ograniczeń. Kopiowanie lub przetwarzanie tych materiałów w całości lub w części bez zgody autora jest zabronione. W przypadku wykorzystania rezultatów niezbędne jest podanie źródła finansowania oraz jego autorów.

#### PROJEKT NR. 2023-2-PL01-KA210-VET-000176822

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

