Phishing: jak cyberprzestępcy oszukują i jak się bronić

Dofinansowane przez Unię Europejską

LIDER:
Coventry University Research Institute Europe

PARTNERZY:
STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

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

Dofinansowane przez Unię Europejską

LIDER: Coventry University Research Institute Europe

PARTNERZY: Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

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 zagadnienia.

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

Pozdrawiamy serdecznie,

Zespół Projektu CyberSec

Dofinansowane przez Unię Europejską
LIDER:
Coventry University Research Institute Europe
PARTNERZY:
KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

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

Dofinansowane przez Unię Europejską

LIDER:
Coventry University Research Institute Europe

PARTNERZY:
STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

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..

Dofinansowane przez Unię Europejską
LIDER: Coventry University Research Institute Europe
PARTNERZY: KREA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

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.

Dofinansowane przez Unię Europejską
LIDER: Coventry University Research Institute Europe
PARTNERZY: KREA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

LEKCJA 1 - Phishing

Struktura lekcji

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

Dofinansowane przez Unię Europejską
LIDER:
Coventry University Research Institute Europe
PARTNERZY:
STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

	Co sprawiło, że rozpoznałeś próbę phishingu?		
Omówienie wyników i dyskusja	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
Podsumowanie i refleksja	Zaproszenie do testu przy użyciu narzędzia: https://phishingquiz.withgoogle.com/ 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

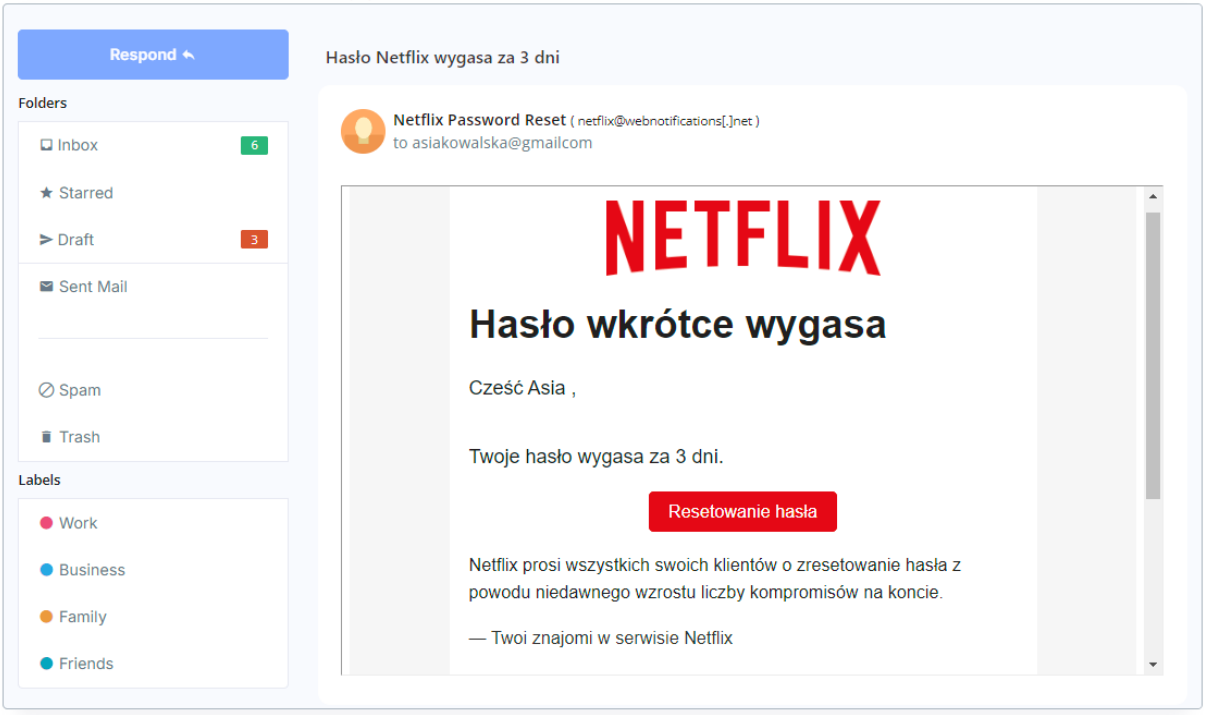
Strony internetowe i portale edukacyjne

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

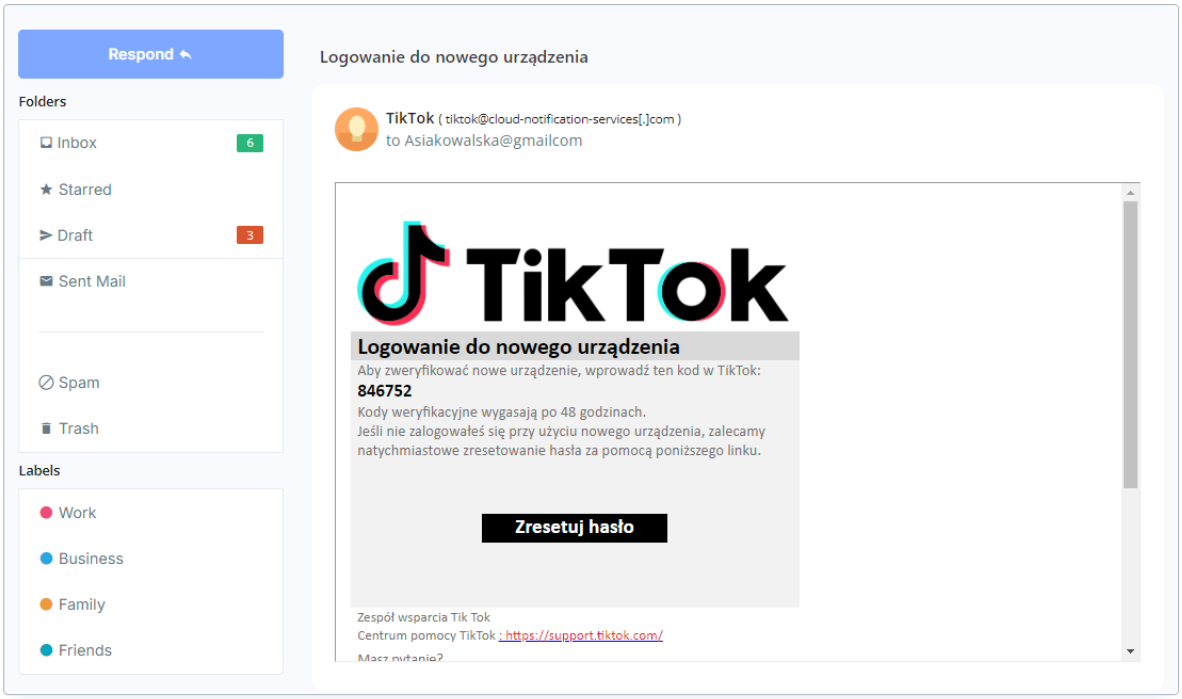
Dofinansowane przez Unię Europejską
LIDER: Coventry University Research Institute Europe
PARTNERZY: STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

LEKCJA 1 - Phishing

Arkusz 1

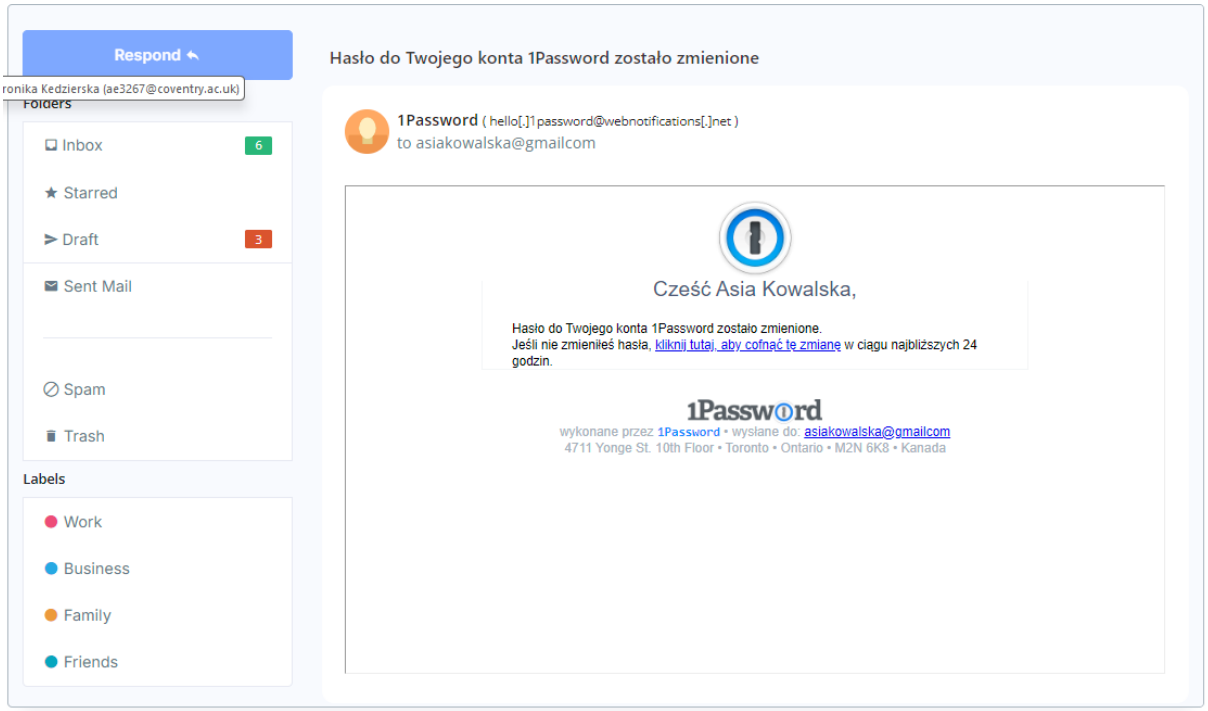


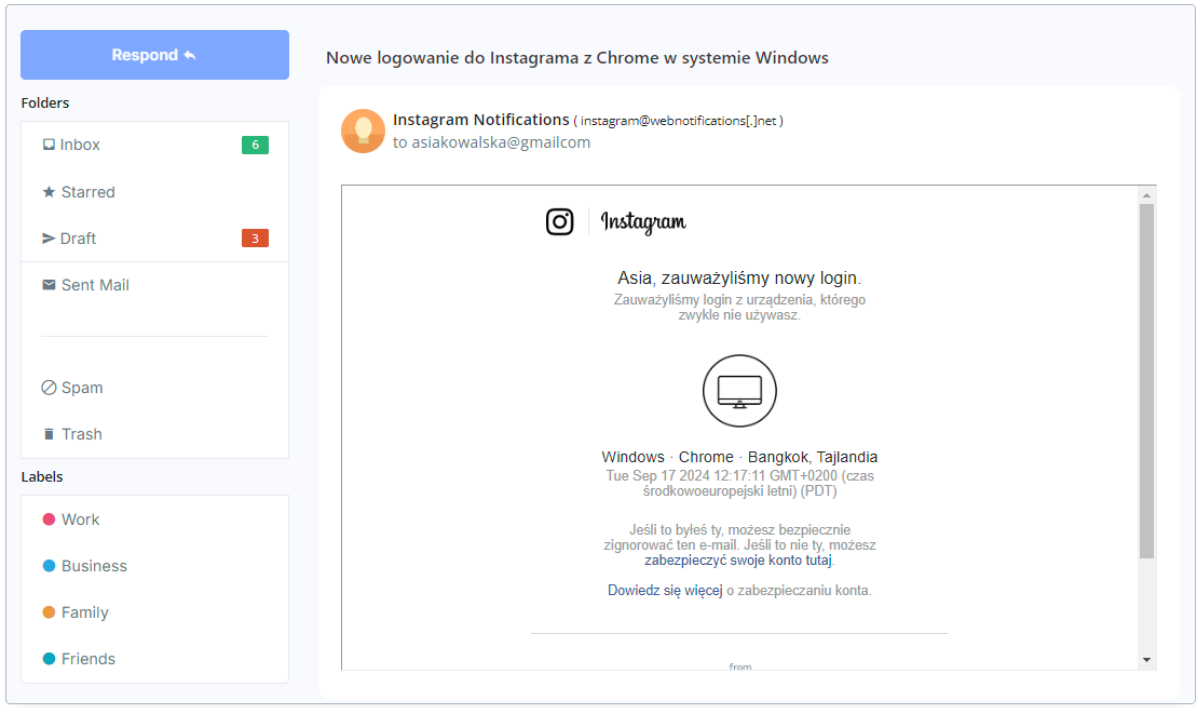
Źródło: https://caniphish.com/email-phishing-simulator?email=Gmail-Blocked-Login#emailTitle



Dofinansowane przez Unię Europejską
LIDER:
Coventry University Research Institute Europe
PARTNERZY:
KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

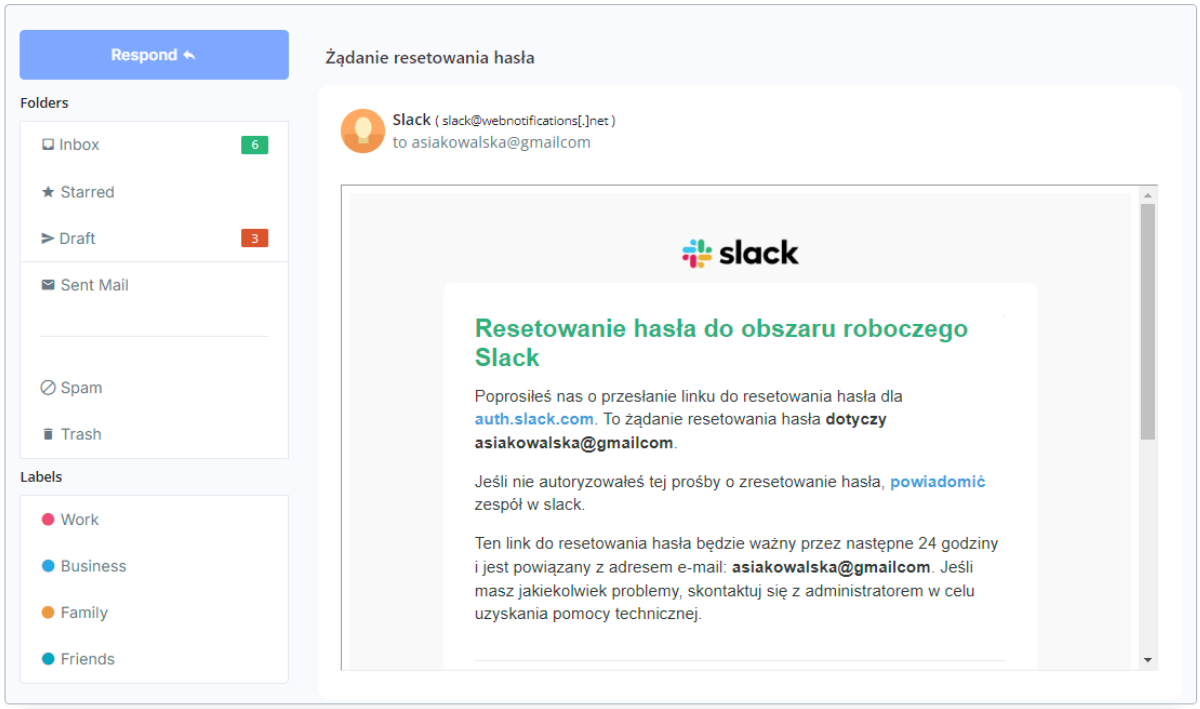
LEKCJA 1 - Phishing

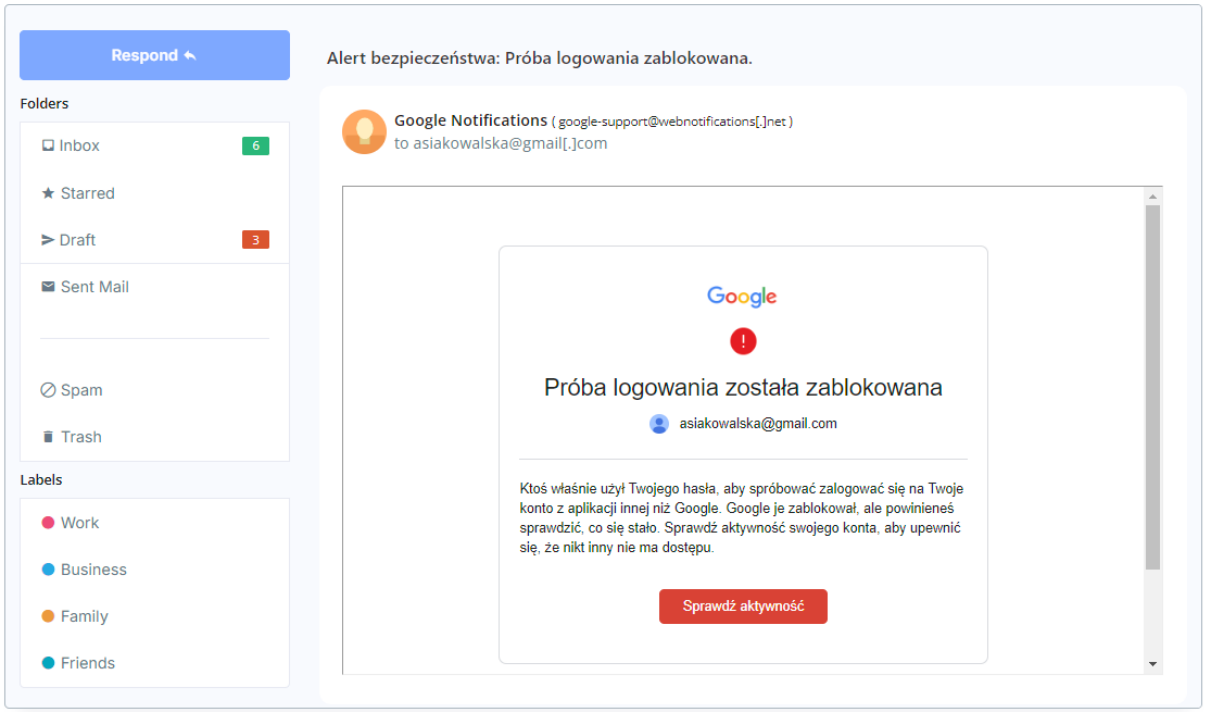




Dofinansowane przez Unię Europejską
LIDER:
Coventry University Research Institute Europe
PARTNERZY:
KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

LEKCJA 1 - Phishing





Dofinansowane przez Unię Europejską
LIDER:
Coventry University Research Institute Europe
PARTNERZY:
KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

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 osiągania 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.

Dofinansowane przez Unię Europejską
LIDER:
PARTNERZY:

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.

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

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

Dofinansowane przez Unię Europejską

LIDER: Coventry University Research Institute Europe

PARTNERZY: Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education