Phishing: Porozumění taktikám kyberzločinců a jak zůstat v bezpečí

Spolufinancováno Evropskou unií

VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe

PARTNEŘI: KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

LEKCE 1 – Phishing

Plán výuky pro střední školy

Scénář vytvořený v rámci projektu „CyberSec EduCheck“ – projekt č. 2023-2-PL01-KA210-VET-000176822

Autoři scénáře: Weronika Kędzierska, Mateusz Pękala - Coventry University Wrocław

Věcná redaktorka: Pavla Vybíhalová - European Centre for Career Education

Grafická úprava: Karolína Kornecka-Kupiec, Jadwiga Maj - KREA Association

Wroclaw 2024

Spolufinancováno Evropskou unií

VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe

PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

LEKCE 1 - Phishing

Vážení,

poskytujeme vám plán lekce na téma phishing, což je významná hrozba v oblasti digitální bezpečnosti. Phishing patří mezi nejčastější způsoby, jak se kyberzločinci snaží získat informace. V naší lekci jsme se zaměřili na klíčové aspekty související s touto formou sociálního inženýrství.

Naše 45minutové hodiny jsou navrženy tak, aby pomohly porozumět phishingu, rozpoznat podezřelé e-maily, textové zprávy a webové stránky, a naučit se, jak na phishingové pokusy reagovat a kam takové incidenty hlásit.

Lekce jsou plánovány na krátký čas, proto se zaměříme na klíčové aktivity, jako je analýza ukázkových phishingových e-mailů a diskuse o postupech hlášení incidentů. Pokud máte více času, doporučujeme toto téma rozdělit do menších segmentů, aby bylo možné provést hlubší analýzu a lepší pochopení problematiky.

Scénář a výukové materiály, včetně prezentace, lze přizpůsobit potřebám vaší skupiny.

S pozdravem,
Tým projektu CyberSec

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

Obsah

Spolufinancováno Evropskou unií

VEDOUCÍ PROJEKTU:
Coventry University
Research Institute Europe

PARTNEŘI:
KREA
STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

Cíle lekce

- **Explicitní účely:**
    - Porozumět definici phishingu a technikám používaným kyberzločinci.
    - Rozpoznat podezřelé e-maily, textové zprávy a webové stránky.
    - Schopnost reagovat na phishingové pokusy a znalost postupů pro hlášení incidentů.
- **Skryté cíle:**
    - Rozvoj analytického a kritického myšlení při hodnocení zpráv a webových stránek.
    - Posílení komunikačních dovedností sdílením zkušeností a znalostí o phishingu.
    - Zvýšení povědomí o osobní bezpečnosti na internetu a odpovědnosti za ochranu osobních údajů.

Kontext - klíčová slova

phishing, digitální bezpečnost, techniky sociálního inženýrství, odpovědnost

- **Odůvodnění výběru tématu:**
    - Phishing je jednou z nejčastějších hrozeb na internetu, která může vést ke krádeži identity, ztrátě dat a finančním ztrátám.
    - Porozumění phishingovým technikám a schopnost je rozpoznat jsou klíčové pro ochranu osobních údajů a digitální bezpečnosti.
    - Vzdělávání o phishingu umožňuje nejen zvýšit povědomí o hrozbách, ale také rozvíjet kritické myšlení a odpovědnost v online prostředí.
    - Formování postojů, jako je ostražitost a schopnost reagovat na phishingové pokusy, přispívá k větší bezpečnosti na internetu a podporuje budování bezpečnějšího digitálního prostoru.

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

Příprava na lekci

- **Materiály:**
    - Multimediální prezentace [Phishing – jak kyberzločinci podvádějí a jak se bránit].
    - Pracovní listy s cvičeními.
    - Tabule (tradiční nebo interaktivní).

- **Zkušenosti:**

  o Aktivita před lekcí: Použijte úvodní činnost k uvedení studentů do tématu phishingu, využijte prvek překvapení a zapojte je do zážitkové aktivity. Příklady:

  „Důležitá zpráva od učitele“. Postup: Pošlete studentům e-mail (nebo zobrazte na tabuli/projektoru) zprávu od „učitele“, která je žádá o kliknutí na odkaz, např. k vyplnění „průzkumu o škole“. Odkaz povede na falešnou webovou stránku (např. formulář s vtipnými otázkami).

  „Ztracený USB disk“. Postup: Položte USB disk na viditelné místo s popiskem, např. „Známky studentů – přísně tajné“, a sledujte, kdo ho zvedne. Po chvíli vysvětlete, že jde o příklad „hardwarového phishingu“.

  „Falešná SMS od ředitele“. Postup: Zobrazte na obrazovce SMS zprávu: „Od ředitele: Žáci třídy X jsou požádáni, aby potvrdili svou účast kliknutím na odkaz: [odkaz]“.

  „Přihlášení k falešné Wi-Fi síti“. Postup: Před lekcí vyvěste ceduli s nápisem „Nová Wi-Fi síť: Free_School_WiFi“ s heslem a sdělte studentům, že jde o bezplatný internet. Po několika minutách vysvětlete, že jde o „příklad phishingu pomocí falešné Wi-Fi sítě“.

- **Prostor**:
    - Uspořádání lavic tak, aby umožňovalo práci ve skupinách nebo individuálně.

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

Struktura lekce

Účel	Aktivita	Čas	Materiály
Úvod	Představení tématu lekce: phishing a sociální inženýrství. Vysvětlení cílů lekce: Seznámení se s typy hrozeb. Schopnost rozpoznat phishingové pokusy. Naučit se metody obrany proti phishingu.	5 min	Prezentace, tabule
Předání znalostí	Typy hrozeb: Phishing: Phishing prostřednictvím falešných e-mailů, SMS (smishing) atd. Sociální inženýrství: Manipulační techniky používané k oklamání uživatele.	10 min	Prezentace, multimediální ukázky
Praktická cvičení	Rozpoznání phishingu – Pracovní list 1: Pracujte ve skupinách na úkolu rozpoznávání phishingových pokusů. Phishingový simulátor – použit k vytvoření pracovního listu 1. https://caniphish.com/email-phishing-simulator?email=Gmail-Blocked-Login#emailTitle Přehled výsledků: Prezentace výsledků práce skupin. Diskuze o použitých kritériích a vysvětlení obtížnějších problémů. Skupinová diskuze: Otázky pro podporu diskuze: Které prvky byly nejpřesvědčivější v analyzovaných phishingových pokusech?	15 min	Pracovní listy, počítače/tablety

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREATYWNI DLA BIZNESU, EUROPEAN CENTRE FOR CAREER EDUCATION

	Jaké techniky sociálního inženýrství byly použity a proč? Co vám pomohlo rozpoznat phishingový pokus?		
Diskuze k výsledkům **Rozpoznání phishingu**	Kritéria: Přirozená návnada, zvědavost, zpoždění doručení, zpráva o výhře, rychlá akce, jazykové chyby, strach z poplatků, neobvyklé jméno odesílatele, neoficiální odkaz.	10 min	Tabule, poznámky
Shrnutí a zamyšlení	Pozvánka k testování pomocí nástroje: https://phishingquiz.withgoogle.com/ Shrnutí klíčových problémů: Zopakování nejdůležitějších informací o rozpoznání a obraně proti phishingu. Zdůraznění role vědomého používání elektronické komunikace. Zamyšlení nad tématem: Podnět k přemýšlení, jak se chránit před phishingem v každodenním životě. Bezpečnost telefonu: Zdůraznění, že telefon je také počítač, a diskuse o zásadách zabezpečení mobilních zařízení.	5 min	Prezentace

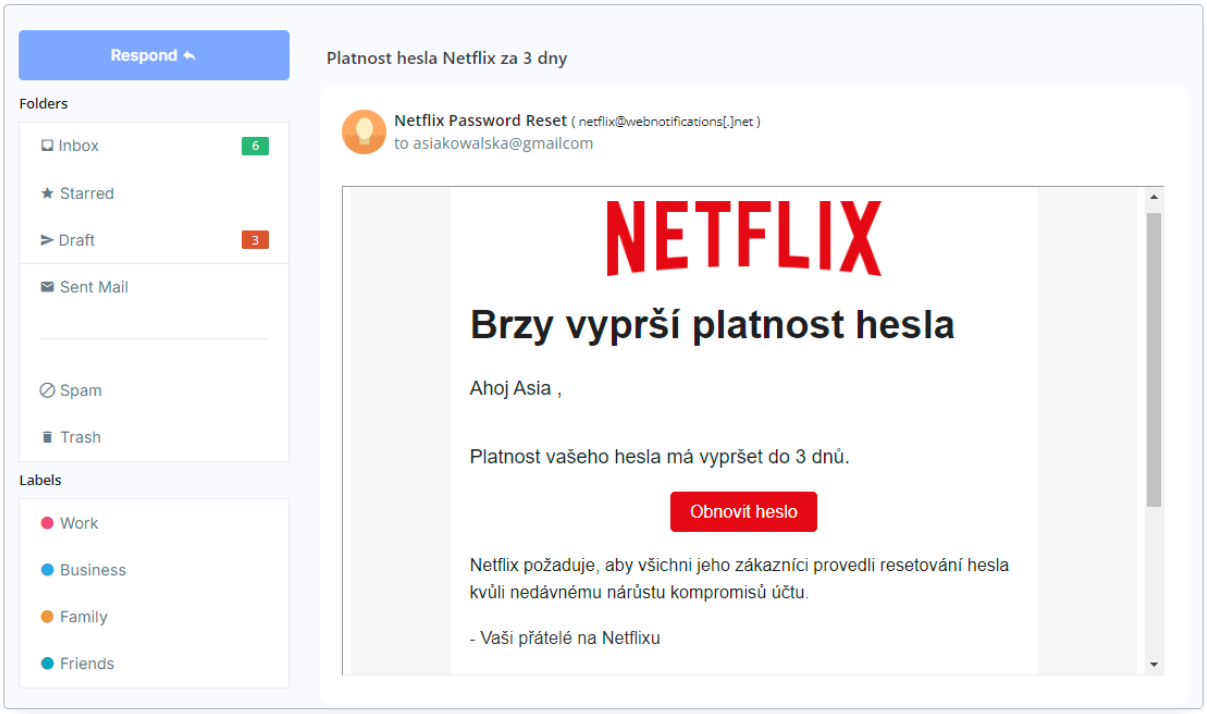
Zdroje a informace pro učitele

Vzdělávací weby a portály

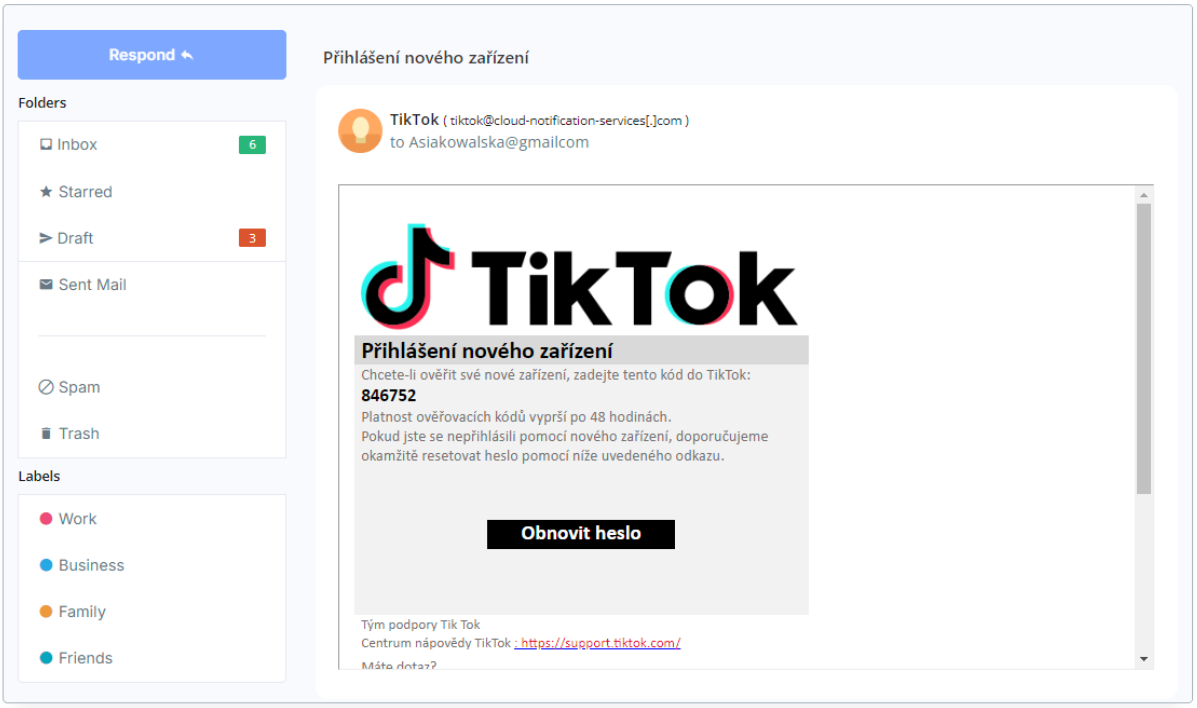
https://nukib.gov.cz/download/publikace/doporuceni/Doporuceni_spear_phishing_2.0.pdf

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

LEKCE 1 - Phishing

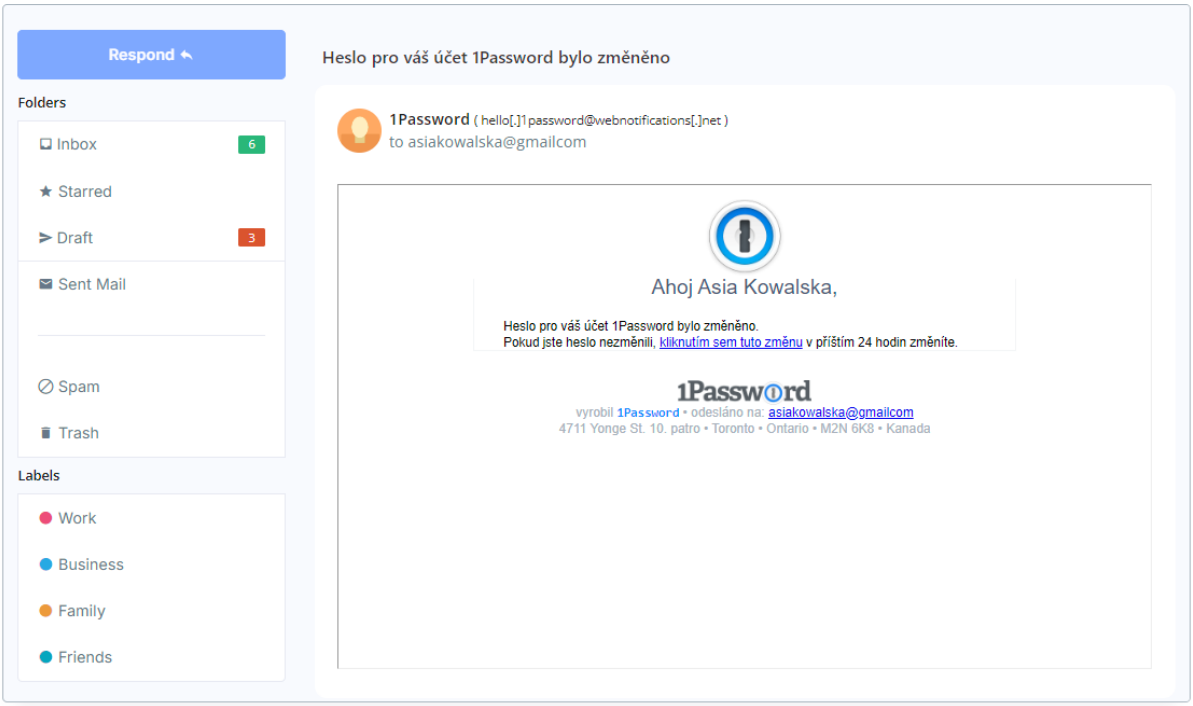


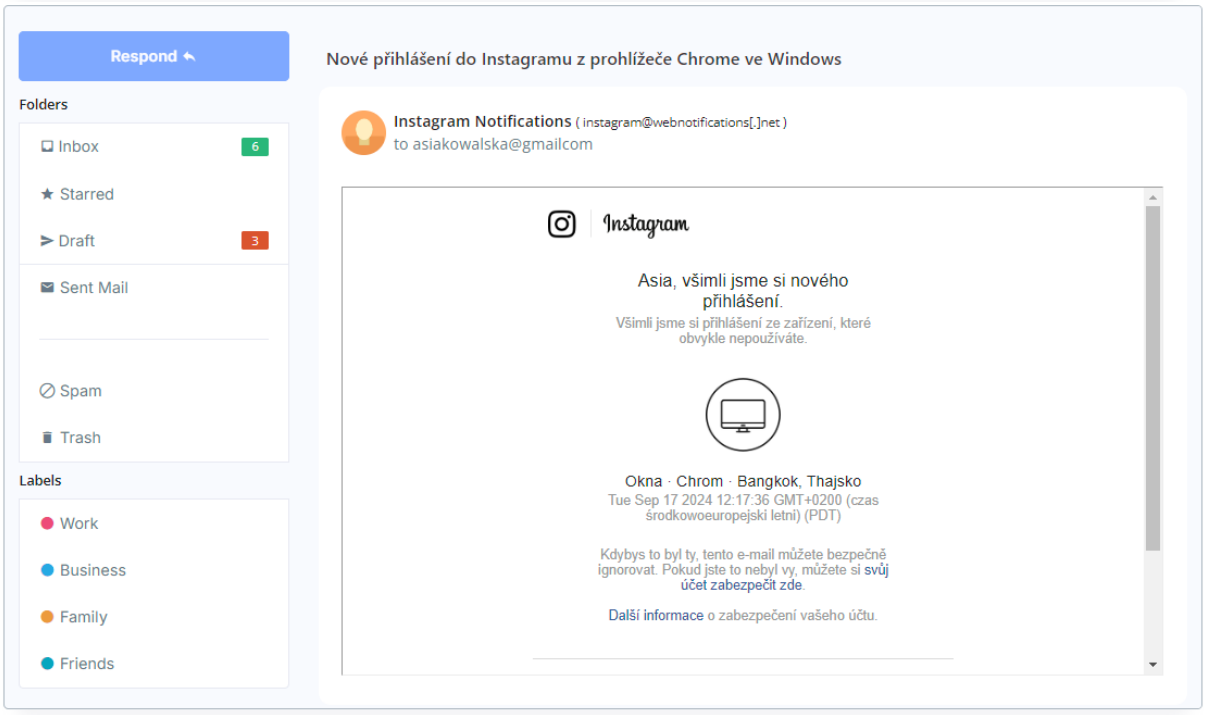
Zdroj: https://caniphish.com/email-phishing-simulator?email=Gmail-Blocked-Login#emailTitle



Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

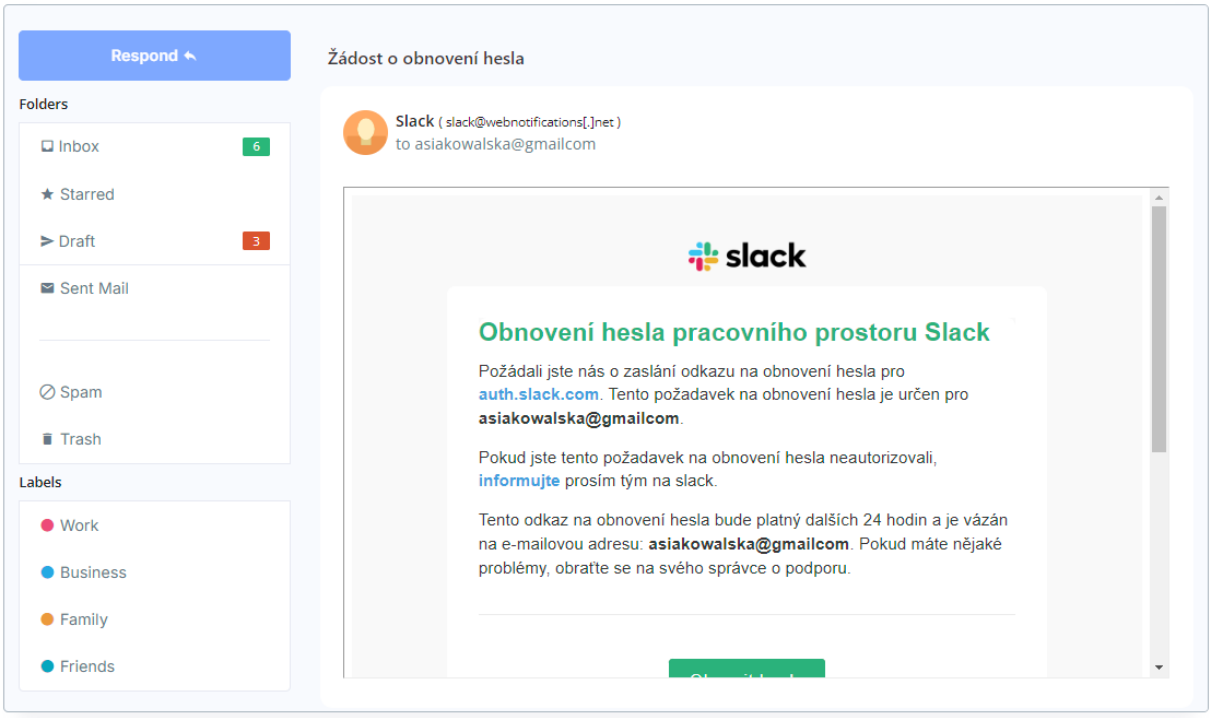
LEKCE 1 - Phishing

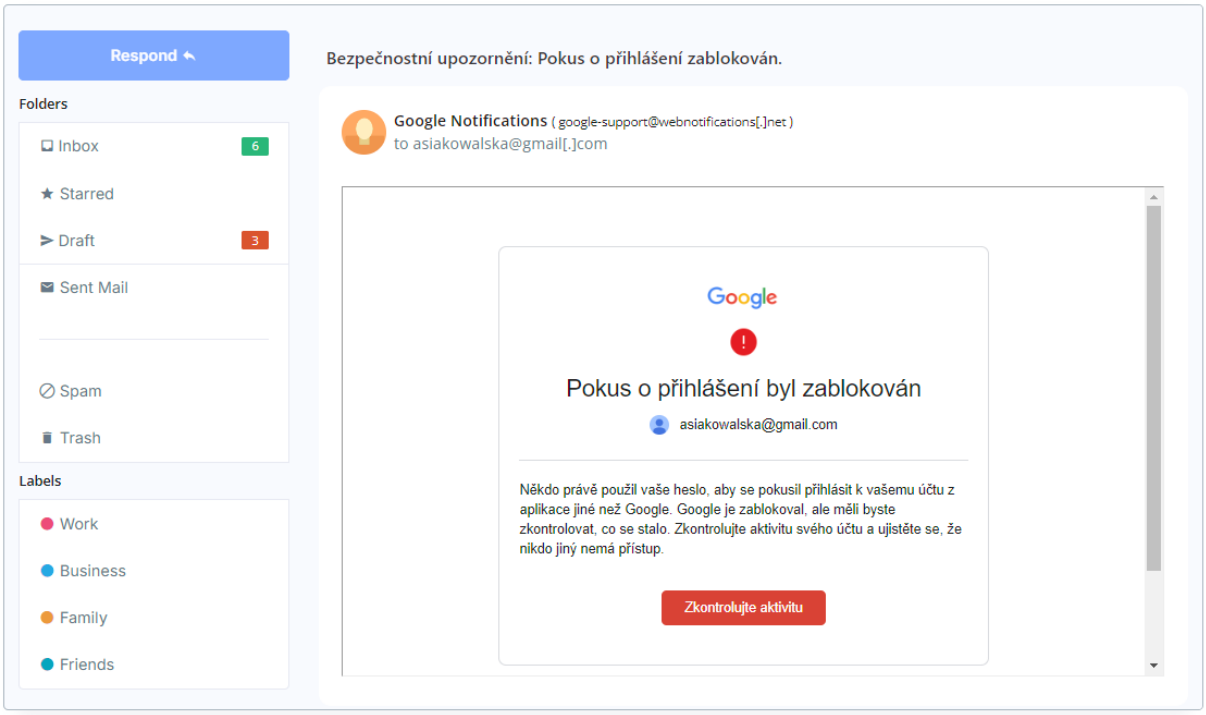




Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU:
Coventry University Research Institute Europe
PARTNEŘI:
KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

LEKCE 1 - Phishing

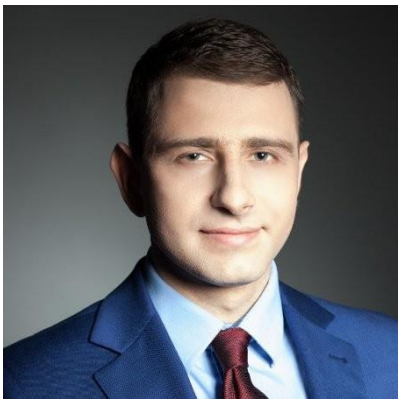




Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU:
Coventry University Research Institute Europe
PARTNEŘI:
KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

Autoři a odborníci

Weronika Kędzierska – expertka v oblasti měkkých aspektů kyberbezpečnosti, zaměřující se na vytváření bezpečné základny kyberbezpečnosti pro mladé organizace. Specializuje se na rozvoj efektivních týmů, organizační změny a implementaci inovačních strategií. Jako nezávislá konzultantka a koučka pomáhá lídrům a týmům budovat zapojení a spolupráci. Je oceňována za kreativní a hodnotné workshopy, které efektivně inspirují týmy k dosahování jejich cílů.



Mateusz Pękala – specialista na zvyšování povědomí o bezpečnosti informací, security compliance, audity informační bezpečnosti a řízení rizik. Má dlouholeté zkušenosti jako auditor, školitel a konzultant v oblasti informační bezpečnosti. Je členem profesionálních organizací, jako jsou ISSA Poland a ISACA. Vlastní certifikace Certified in Risk and Information Systems Control™ (CRISC), Certified Information Security Professional (CISSP), Certified Data Privacy Solutions Engineer™ (CDPSE)® a Certified Information Systems Auditor® (CISA), a je také certifikovaným auditorem v oblasti ISO 27001.

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREATYWNI DLA BIZNESU, EUROPEAN CENTRE FOR CAREER EDUCATION

Více informací o projektu

Financováno Evropskou unií. Vyjádřené názory a názory jsou však výhradně názory autora (autorů) a nemusí nutně odrážet názory Evropské unie nebo Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za ně nemohou nést odpovědnost.

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

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

CYBERSEC
EDUCHECK

Spolufinancováno Evropskou unií

VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe

PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education