Hesla: Vytváření a správa bezpečného přístupu

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

LEKCE 2 – Hesla

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 2 - Hesla

Vážení,

představujeme vám plán lekce na téma bezpečnosti hesel, což je klíčový prvek ochrany soukromých informací na internetu. Jsme si vědomi, že téma digitální bezpečnosti je velmi široké, a proto jsme se vzhledem k časovým omezením zaměřili na základní, ale nesmírně důležité otázky týkající se vytváření a správy hesel.

Naše 45minutová lekce se zaměřuje na tři hlavní cíle: studenti se naučí, jak vytvářet silná a jedinečná hesla, pochopí, proč dvoufaktorová autentifikace (2FA) zvyšuje bezpečnost účtů, a naučí se, jak bezpečně spravovat hesla, včetně výhod používání správce hesel.

To je minimální čas na provedení klíčových aktivit, jako jsou skupinová cvičení a diskuze, které pomohou upevnit získané znalosti (předpokládali jsme, že během těchto 45 minut nebudete mít dost času na nastavení správce hesel na svých zařízeních, což je škoda). Nicméně, pokud máte více času, doporučujeme rozdělit toto téma do menších částí a využít je v budoucích lekcích, což umožní studentům lépe analyzovat a pochopit dané problémy.

Scénář a výukové materiály, včetně prezentace, lze přizpůsobit a modifikovat podle vašich potřeb a schopností 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: STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

Cíle lekce

- **Explicitní cíle**:
    - Studenti budou schopni vytvářet silná a jedinečná hesla, která poskytnou lepší ochranu jejich online účtům. Pochopí potřebu používat jiná hesla pro každou službu, kterou využívají.
    - Studenti pochopí, proč je dvoufázová autentifikace důležitá a jak ji povolit na svých účtech.
    - Studenti se naučí, jak spravovat svá hesla, včetně použití správce hesel.
    - Rozvoj analytických a kritických dovedností.

- **Skryté cíle**:
    - Posílení spolupráce ve skupině.
    - Podpora samostatného myšlení a řešení problémů.

Kontext - klíčová slova

hesla, online bezpečnost, dvoufaktorová autentifikace, správci hesel, ochrana osobních údajů, kyberbezpečnost

Odůvodnění výběru tématu:

- V současnosti je přístup k technologii a internetu široce rozšířený a téměř nepřetržitý, mladí lidé pravidelně využívají různé online služby. To zvyšuje riziko ztráty soukromých údajů a hacknutí účtů kvůli slabým heslům.
- Mnoho lidí používá stejná hesla na různých službách, což je vystavuje vážným následkům v případě úniku dat. Pochopení potřeby vytvářet silná, jedinečná hesla a výhod dvoufaktorové autentifikace je klíčové pro online bezpečnost.
- Vzdělávání o správě hesel, včetně použití správců hesel, učí mladé lidi odpovědnosti za vlastní data a účty a rozvíjí povědomí o kyberhrozbách.

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 [Hesla a jejich bezpečnost]
    - Pracovní listy s cvičeními
    - Tabule
    - Počítače s připojením k internetu (pokud je potřeba)
    - Online test – Možnost využít platformu, která umožňuje vytvářet kvízy o heslech a online bezpečnosti (např. kaboot.it) - ukázkový připravený kvíz: https://play.kahoot.it/v2/?quizId=cd611872-3056-4990-803f-765179e75c0e)
- **Zkušenost**: Volitelně pozvat studenty na aktivitu před lekcí, např. vzdělávací hra od Googlu ve formě interaktivního dobrodružství, které učí, mimo jiné, jak vytvářet silná hesla

  https://beinternetawesome.withgoogle.com/en_us/interland/landing/tower-of-treasure

- **Učebna**:
    - Místnost je vybavena obrazovkou/projektorem.
    - 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 a cílů lekce. Nejprve několik příběhů – učitel sdílí jeden nebo více příběhů jiných studentů. Učitel se ptá: Jsou tyto příběhy pravdivé? Ne. Byly vymýšleny pro potřeby lekce. Což neznamená, že se nemohly stát.	5 min	Prezentace
Mini kvíz, zda je toto bezpečné heslo	Učitel se studenty položí otázky ve formě kvízu, ve kterém je požádá, aby si napsali odpovědi (1 je pravda). Ukázkové otázky: 1. Které heslo je nejbezpečnější? JPL93#q anna1234! Basil456 **Gospachackeryou won't break.** 2. Které heslo je nejsnadněji uhádnutelné? **MyPassword123** Summer2024 Great!2023 Qwerty!123 3. Které heslo je nejméně bezpečné? **Qwerty123** P@ssw0rd 1234abc! Secure*Pass123 4. Které z následujících hesel by mohl hacker snadno uhádnout, pokud zná jméno vašeho domácího mazlíčka a datum narození? K!ngC0bra L0veCats! Adventure987 **Fluffy2021** 5. Co je 2FA?	10 min	

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

	Funkce na telefonech, která urychluje nabíjení baterie Zkratka pro dva antivirové filtry běžící současně **Je to dodatečná bezpečnostní funkce, která pomáhá zajistit, že se přihlásíte pouze vy, i když někdo zná vaše heslo.** Cloudový šifrovací systém, který zvyšuje bezpečnost souborů Učitel prezentuje odpovědi a požádá studenty, aby sdíleli počet správných odpovědí. 1d) Čím delší je heslo, tím těžší je ho prolomit. Ideálně by heslo mělo mít 15 znaků nebo více. Heslo může být 4 nebo více ne zcela běžných slov spojených dohromady. 2a) MyPassword123 je nejsnadněji uhádnutelné, protože používá jednoduchá slova a sekvence čísel, které jsou často používány v heslech mnoha lidmi. Další hesla jsou také předvídatelná. 3a) Nejslabší heslo je Qwerty123. To je populární heslo založené na jednoduchém vzoru klávesnice a snadno se uhodne při útocích slovníkovými metodami. Další hesla obsahují různé typy znaků a jsou méně předvídatelná, i když by si mohla zasloužit další zlepšení. 4d) Nejsnadněji uhodnutelné heslo je Fluffy2021, protože obsahuje jméno zvířete a datum, což hackerovi usnadňuje uhodnutí hesla, pokud zná tyto informace. 5c) 2FA (dvoufaktorová autentifikace) je způsob, jak přidat další bezpečnost k vašemu účtu, kromě pouhého hesla. Funguje to tak, že po zadání hesla musíte ještě jiným způsobem potvrdit svou identitu, například zadáním kódu z textové zprávy, použitím speciální aplikace (např. Google Authenticator) nebo použitím speciálního klíče. To činí váš účet mnohem bezpečnějším.		

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

	Diskuze o výsledcích – proč jsou nebezpečná. **Alternativně** (místo tohoto kvízu) můžete použít **„Herní aktivitu s hesly“** (pracovní list 2). Je to rychlá aktivita, ve které studenti ve skupinách hádají hesla na základě jedno- nebo dvouslovných nápověd. Každá skupina si vybere člověka, který bude dávat nápovědy“, který má 30 sekund na to, aby pomohl týmu uhádnout heslo, a skupina má 3 pokusy. Za každou správnou odpověď skupina získá 2 body, a pokud se jim nepodaří heslo uhodnout, ztrácí svůj tah, ale neztrácí body.		
Předání znalostí: Běžné chyby	**1. Otevřené otázky pro studenty (mohou být položeny všechny nebo některé otázky):** • Kolik různých hesel používáte pro své účty? • Jak často používáte stejné heslo pro několik různých účtů? • Jak často měníte svá hesla? • Jak často zapomenete své heslo? **2. Prezentace klíčových informací o běžných chybách:** • Často používáme stejné heslo na několika webech. • Často používáme podobná hesla. • Používáme osobní informace. • Sdílíme hesla. • Hesla, která jsou příliš krátká. • Používáme vzory na klávesnici (např. QWERT). • Nahrazení číslicemi/speciálními znaky (např. Password → P@$$w 0rd). • Ukládáme hesla do textových souborů.	10 min	Prezentace, multimediální ukázky
Praktická cvičení	**Jak být v bezpečí – Skupinová práce** Učitel rozdělí třídu do 4 skupin. Každá skupina má 5-10 minut na vyplnění pracovního listu č. 1.	15 min	Pracovní list č. 1, tabule, poznámky

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

	- Cílem je odpovědět na následující otázky: - Co v tomto případě způsobuje problém? Možná je jich více? - Co si myslíte, že by pomohlo zabránit takové situaci? Příkladové situace pro skupiny (můžete si vybrat jednu pro všechny nebo různé pro každou skupinu): ● Kliknutí na podezřelý odkaz a převzetí mého účtu: Klikl(a) jsem na odkaz, který vypadal, že je od kamaráda, a zadal(a) jsem tam své přihlašovací údaje. Poté někdo převzal můj účet a nyní nemám přístup k důležitým věcem. ● Přístup k mému účtu po opuštění odemčeného laptopu: Nechal(a) jsem svůj laptop odemčený ve škole a někdo se dostal na můj sociální účet a napsal hnusné věci, předstíral, že jsem to já. Teď se musím obhajovat před učiteli a kamarády, protože všichni si myslí, že to jsem já. ● Krádež peněz díky slabému heslu: Nastavil(a) jsem si velmi jednoduché heslo pro svůj bankovní účet a někdo ho prolomil a ukradl všechny peníze. Teď se musím snažit je dostat zpět. ● Ztráta herního účtu po sdílení hesla: Dal(a) jsem své herní heslo kamarádovi a on je změnil a začal používat můj účet. Přišel(a) jsem o všechna svá dosažená vítězství, na kterých jsem dlouho pracoval(a).		
Diskuze o výsledcích	Představení nástroje pro správu hesel jako řešení. Vysvětlení obtížnějších problémů.	10 min	
Shrnutí a zamyšlení	Shrnutí klíčových problémů. Podnět k akci pro posílení vaší bezpečnosti	5 min	Prezentace

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

Volitelný domácí úkol

Ověřte svá hesla:

- Zkontrolujte, zda jsou vaše hesla dlouhá, náhodná a jedinečná.
- Nainstalujte KeePassXC (nebo jiného správce hesel) na svůj počítač.
- Přeneste všechna svá hesla do správce hesel. Přestaňte psát hesla na samolepicí poznámky nebo do textových souborů.

Změňte slabá a slovníková hesla:

- Pokud používáte jednoduchá hesla jako „123456“ nebo „heslo“, okamžitě je změňte.
- Přehodnoťte systémy, které používáte:
- Vytvořte seznam všech účtů, aplikací a systémů, které používáte, a ujistěte se, že jsou všechny zabezpečeny.

Povolne dvoufázové ověření (two-factor authentication - 2FA):

- At least on the most important accounts such as email, social media, banking.
- Use apps like Google Authenticator or other available options.

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

Zdroje a znalosti pro učitele

Popis metody 5 Proč (5xWhy)

Metoda 5 Proč pomáhá studentům pochopit, proč k problému došlo, kladením pěti po sobě jdoucích otázek „proč?“. Spočívá v tom, že se otázka „proč?“ položí pětkrát, aby se dostalo k opravdovému jádru problému, místo aby se zastavilo u první zřejmé odpovědi. Tento nástroj pomáhá studentům lépe pochopit, co je za daným problémem a jak jej lze vyřešit.

Alternativní otázky:

Místo toho, abyste se ptali „proč?“ pětkrát, stojí za to použít více otevřené otázky, které nevedou k tomu, že se studenti budou cítit souzeni. V našem příkladu používáme otázku „Jaká je příčina?“. Konkrétní otázky mohou vypadat takto:

- Jak se stalo, že někdo získal vaše heslo?
- Zajímalo by mě, jak jste si vybrali své heslo?
- Co vás napadlo, když jste vytvářeli toto heslo?
- Můžete mi pomoci pochopit, proč se vám toto heslo zdálo dostatečné?

Příklady použití (krádež údajů o bankovním účtu / ztráta herního účtu po sdílení hesla):

Problém: Někdo se nabourал do mého bankovního účtu a ukradl všechny mé peníze.	**Problém: Přišel jsem o přístup ke svému hernímu účtu, protože jsem dal své heslo kamarádovi.**
• Proč někdo hacknul účet? Protože měl přístup k mému heslu. • Proč měl přístup k mému heslu? Protože jsem použil velmi jednoduché heslo, které bylo snadné prolomit. • Proč jsem použil jednoduché heslo? Protože jsem si myslel, že heslo, které je snadné si zapamatovat, bude pohodlnější. • Proč jsem dával přednost pohodlí před bezpečností? Protože jsem nechápal důležitost silného hesla. • Proč jsem nechápal důležitost silného hesla? Protože jsem neměl dostatek znalostí o kyberbezpečnostních hrozbách.	• Proč jsi přišel(a) o přístup k účtu? Protože můj kamarád změnil heslo. • Proč jsi dal(a) své heslo kamarádovi? Protože potřeboval(a) přístup ke hře. • Proč sis myslel(a), že je v pořádku sdílet své heslo? Protože jsem věřil(a), že můj kamarád nezneužije mé důvěry. • Proč jsi nepřemýšlel(a) o důsledcích? Protože jsem nevěděl(a) o rizicích sdílení hesel. • Proč jsi neznal(a) rizika? Protože jsem se předtím nezajímal(a) o bezpečnostní pravidla online účtů.

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu, European Centre for Career Education

Řešení
Jakmile jsou příčiny identifikovány, studenti mohou navrhnout řešení, jak předejít podobným situacím v budoucnosti, například:

- Používat silná a jedinečná hesla.
- Povolit dvoufaktorovou autentifikaci (2FA).
- Nesdílet hesla s jinými lidmi, ani s kamarády.

Tipy pro učitele:

- Požádejte studenty, aby nehledali někoho, koho obvinit, ale aby se snažili pochopit, proč k problému došlo.
- Používejte alternativní otázky k vybudování důvěry a podpoře upřímného zamyšlení.
- Na konci lekce povzbuďte studenty, aby přišli s řešeními, která mohou v budoucnu zabránit těmto problémům.
- Zaměřte se na nápady na řešení, která se zaměřují na problémy uvedené na spodní části stránky.

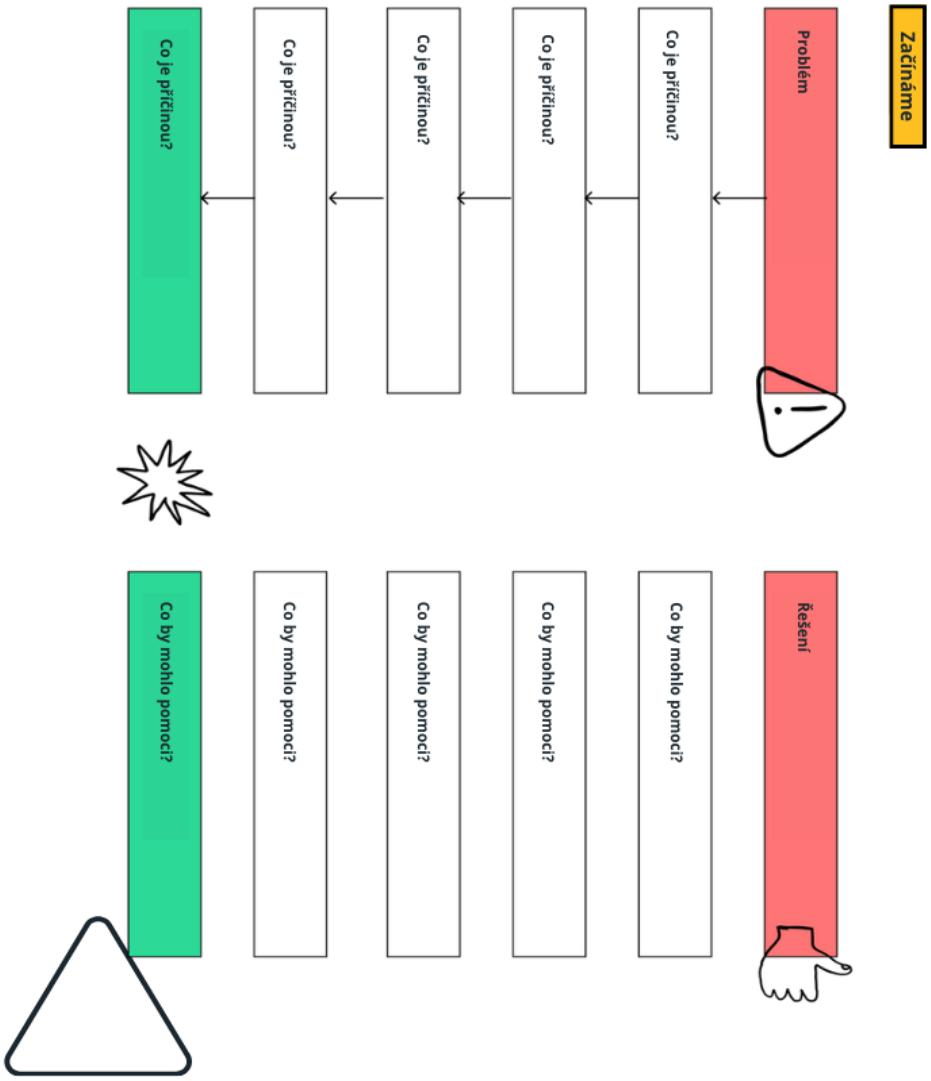
Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

LEKCE 2 - Hesla

Pracovní list č. 1

Úkolem je identifikovat problém, pochopit jeho příčiny a přijít s řešeními, která pomohou předejít podobným situacím v budoucnu. Na začátku si napište, jaký je hlavní problém v případě, který analyzujete (např. „Účet byl převzat hackerem“, „Ztráta přístupu k účtu“, „Krádež dat“). Zamyslete se, co je příčinou této situace (Proč k tomuto problému došlo? Jaká je jeho příčina?). Hledejte hlubší příčiny.

V dalším kroku se zamyslete nad tím, co by mohlo pomoci. Napište nápady v souvislosti s různými příčinami problémů (začněte těmi na spodní části papíru).



Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

Pracovní list č. 2 – Hra s hesly

Doba trvání: přibližně 15 minut pro třídu o 25 žácích

Příprava:

1. Připravte 10-15 samolepicích poznámek s hesly (seznam níže).
2. Rozdělte třídu do 5 skupin po 5 lidech.

Pravidla hry:

Rozdělení rolí ve skupinách:

1. Každá skupina si vybere 1 osobu, která bude dávat nápovědy a ostatní jsou „hádači“.
2. Role se mění po každém kole.

Průběh hry:

1. Osoba, která dává nápovědy, vytáhne papírek s heslem.
2. Během 30 sekund dává skupině nápovědy (pouze jedno nebo dvě slova).
3. Skupina má 3 pokusy na uhodnutí hesla.
4. Pokud heslo neuhodnou včas, heslo přechází na další skupinu (volitelně).

Bodování:

1. Skupina získá 2 body za uhodnutí hesla.
2. Pokud neuhodnou, ztrácejí svůj tah (ale neztrácejí body).

Rotace:

Po každém kole se v skupině mění „dávající nápovědy“.

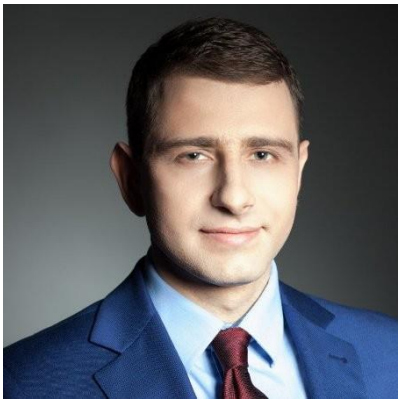
Hra trvá, dokud nejsou vyčerpány všechny karty nebo dokud neuplyne čas (15 minut).

qwerty	password	letmein
iloveyou	admin	welcome
dragon	master	hello
whatever	freedom	token
sunshine	starwars	trustno1

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: KREA Stowarzyszenie 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