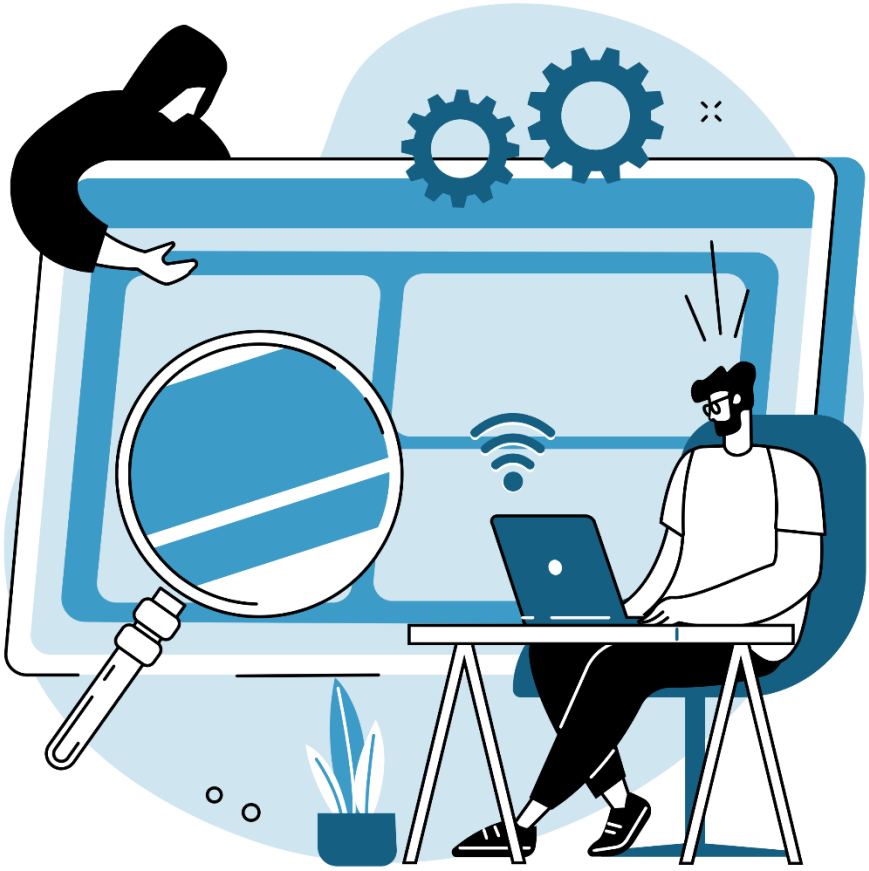
Incydenty Bezpieczeństwa Cyfrowego



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

LEKCJA 3 - Incydenty

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

Szanowni Państwo,

Oddajemy w Państwa ręce scenariusz zajęć na temat incydentów bezpieczeństwa cyfrowego, kluczowego elementu w zarządzaniu ryzykiem związanym z ochroną danych osobowych i systemów informatycznych. Nasze 45-minutowe zajęcia mają na celu uświadomienie uczniom, jak skutecznie reagować na incydenty bezpieczeństwa, w tym zmieniać hasła, przeglądać zabezpieczenia oraz zgłaszać naruszenia. Skoncentrujemy się również na znaczeniu regularnych kopii zapasowych (backupów) oraz najlepszych praktykach ich tworzenia. Uczniowie poznają narzędzia takie jak Have I Been Pwned do monitorowania bezpieczeństwa danych i będą rozwijać umiejętności analityczne oraz krytyczne myślenie, aby lepiej oceniać zagrożenia i skutecznie reagować na nie w przyszłości.

W trakcie zajęć przewidujemy ćwiczenia praktyczne oraz dyskusje, które mają na celu wzmocnienie zdobytej wiedzy. Zdajemy sobie sprawę, że 45 minut to ograniczony czas, dlatego sugerujemy, by w razie potrzeby rozłożyć temat na kilka sesji, co pozwoli uczniom na głębszą analizę i lepsze zrozumienie zagadnień.

Scenariusz oraz materiały dydaktyczne, w tym prezentacja, mogą być dostosowane i modyfikowane według Państwa potrzeb i możliwości 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

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

Cele lekcji

- **Cele jawne**:
    - Reagowanie na Incydent: Uczniowie będą wiedzieli, jakie kroki należy podjąć po wykryciu naruszenia bezpieczeństwa, takie jak zmiana haseł i przegląd zabezpieczeń.
    - Znaczenie Backupów: Uczniowie zrozumieją, jak ważne są regularne kopie zapasowe (backupy) i jak je wykonywać.
    - Narzędzia i Serwisy: Uczniowie nauczą się korzystać z narzędzi takich jak https://haveibeenpwned.com/ do sprawdzania, czy ich dane zostały naruszone
    - Rozwijanie umiejętności analizy i krytycznego myślenia.
- **Cele ukryte**:
    - Wzmacnianie współpracy w grupie.
    - Zachęcanie do samodzielnego myślenia i rozwiązywania problemów.

Kontekst - słowa kluczowe

incydenty bezpieczeństwa, reagowanie na incydent, backupy, zabezpieczenia danych, narzędzia monitorujące, cyberbezpieczeństwo

- **Uzasadnienie wyboru tematu**:

W dobie powszechnego dostępu do technologii i internetu, ryzyko incydentów bezpieczeństwa rośnie, zwłaszcza gdy użytkownicy nie są świadomi, jak odpowiednio reagować na naruszenia. Młodzież często korzysta z różnych serwisów online, co zwiększa szanse na utratę prywatnych danych lub włamania na konta.

Wiedza na temat skutecznego reagowania na takie incydenty, w tym zmiany haseł i przeglądu zabezpieczeń, jest kluczowa dla ochrony danych osobowych.

Zrozumienie znaczenia regularnych backupów oraz umiejętność korzystania z narzędzi monitorujących, jak Have I Been Pwned, pomaga w minimalizowaniu skutków naruszeń bezpieczeństwa.

Edukacja w zakresie zarządzania incydentami oraz rozwijanie umiejętności analizy i krytycznego myślenia w kontekście cyberbezpieczeństwa są istotne dla budowania świadomości zagrożeń i odpowiedzialnego podejścia do ochrony danych w cyfrowym świecie.

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 [Incydenty Bezpieczeństwa Cyfrowego].
  - Arkusze pracy z ćwiczeniami.
  - Tablica (tradycyjna lub interaktywna).
  - Komputery/tablety z dostępem do internetu (jeśli potrzebne).
- **Przestrzeń**:
  - Sala wyposażona w rzutnik/projektor.
  - Ustawienie ławek w sposób umożliwiający pracę w grupach lub indywidualnie.

Struktura lekcji

Cel	Aktywność	Czas	Materiały
Wprowadzenie	Przedstawienie tematu. Nauczyciel pyta się uczniów Co rozumiecie przez słowo Incydent? Jakie znacie przykłady incydentów bezpieczeństwa? Coś z Waszego doświadczenia? Nauczyciel przedstawia kilka przykładów incydentów bezpieczeństwa.	5 min	Prezentacja, tablica
Mini Quiz – Sprawdzenie podatności	Nauczyciel zadaje uczniom 7 pytań „Sprawdź swoją podatność na ataki hackerów” 1. Czy ktoś może chcieć Cię zaatakować?	10 min	Prezentacja

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

	a) Nie, bo nie mam żadnych ważnych danych, które można sprzedać b) Tak, bo ktoś może użyć mojego konta na mediach społecznościowych do oszukiwania innych c) Tak, bo ktoś może zaszyfrować moje dane i zażądać okupu 2. Czy używasz tego samego hasła do kilku różnych kont? a) Tak, bo łatwiej je zapamiętać b) Nie, mam unikalne hasło do każdego konta c) Używam jednego głównego hasła, a na innych kontach drobnych modyfikacji 3. Czy weryfikujesz źródła linków, które otrzymujesz w e-mailach lub wiadomościach? a) Nie zawsze, zazwyczaj klikam, jeśli nadawca wygląda znajomo b) Zawsze sprawdzam, czy link jest bezpieczny przed kliknięciem c) Tylko wtedy, gdy wiadomość wydaje się podejrzana 4. Co robisz, gdy otrzymasz podejrzany e-mail z prośbą o podanie danych? a) Ignoruję go lub usuwam b) Sprawdzam szczegóły nadawcy i linki, zanim podejmę decyzję c) Otwieram, ale nie podaję żadnych danych 5. Jakie kroki podejmujesz, aby chronić swoje urządzenia? a) Nie używam żadnych dodatkowych zabezpieczeń b) Mam zainstalowany program antywirusowy i regularnie go aktualizuję c) Korzystam z antywirusa, aktualizuję oprogramowanie i używam menedżera haseł 6. Czy uważasz, że Twoje dane osobowe są cenne dla innych? a) Nie, nikt nie będzie chciał moich danych b) Tak, mogą być użyte do kradzieży tożsamości lub oszustw c) Tylko moje dane bankowe lub hasła są ważne 7. Co robisz, gdy zobaczysz podejrzane działania na swoim koncie?		

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

	a) Nic, może to błąd b) Natychmiast zmieniam hasło i sprawdzam swoje inne konta c) Czekam i obserwuję, czy sytuacja się powtórzy Przewaga odpowiedzi "a": Masz wiele do poprawy, hakerzy mogą wykorzystać Twoje słabe zabezpieczenia. Zwiększ świadomość zagrożeń i wprowadź lepsze nawyki. Przewaga odpowiedzi "b": Jesteś dobrze przygotowany i świadomy zagrożeń, ale zawsze warto pogłębiać wiedzę na temat bezpieczeństwa online. Przewaga odpowiedzi "c": Masz podstawową wiedzę, ale wciąż jest miejsce na poprawę. Pracuj nad wzmocnieniem zabezpieczeń swoich kont i urządzeń. Nauczyciel zadaje jedno lub więcej pytań, aby pobudzić dyskusję: - Co sprawia, że nasze konta w internecie mogą być narażone na atak? - Jakie są najczęstsze problemy z bezpieczeństwem w internecie, które mogą nas spotkać? - Jakie mogą być skutki, jeśli nasze konto zostanie zaatakowane lub ukradzione? - Co możemy zrobić, żeby uniknąć problemów z bezpieczeństwem w internecie? - Czy znasz jakieś znane przypadki, kiedy ktoś miał problem z bezpieczeństwem w internecie? - Jak często słyszymy o problemach z bezpieczeństwem w internecie? Czy to rzadkie, czy codzienne?		

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

	- Co zrobić, jeśli ktoś ukradnie nasze konto lub dostęp do niego? - Jakie są różnice między różnymi problemami bezpieczeństwa w internecie, jak na przykład kradzież konta i wirusy? - Jakie aplikacje lub programy mogą nam pomóc chronić nasze konta w internecie? - Jakie instytucje lub organizacje zajmują się ochroną naszych danych w internecie?		
Przekazanie wiedzy - ransoware	Kim jest hacker? Oczekiwania vs Rzeczywistość Oczekiwania: Filmowy obraz: Często wyobrażamy sobie hackerów jako osoby w kapturach, które potrafią złamać każdy system komputerowy. Superbohaterowie: Wyglądają na bardzo inteligentnych i działają w ciemnościach, aby zdobyć tajne informacje. Rzeczywistość: Różne rodzaje hackerów: Są różne typy hackerów, w tym tacy, którzy pomagają w poprawie bezpieczeństwa (tzw. "białe kapelusze") i tacy, którzy robią coś nielegalnego (tzw. "czarne kapelusze"). Umiejętności i narzędzia: Hackerzy używają specjalnych narzędzi i technik, ale ich działania są często bardziej techniczne niż w filmach. Nie zawsze działają w tajemnicy. Często wykorzystują socjotechniki. Monitorowanie wycieków Nauczyciel prezentuje stronę Have I Been Pwned https://haveibeenpwned.com/ Popularne narzędzie do sprawdzania, czy Twój e-mail lub hasło znalazło się w wyciekach danych.	10 min	Prezentacja, przykłady multimedialne

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

	Nauczyciel zachęca uczniów do sprawdzenia czy ich maile też tam się znajdują Opcjonalnie do wykorzystania – **Arkusz pracy nr 1. Co zrobić w przypadku wycieku hasła?** Co zrobić w przypadku wycieku hasła? 1. Jak najszybciej zmień hasło Im szybciej zmienisz hasło, tym mniejsza szansa, że ktoś niepowołany zdąży wykorzystać dostęp do Twojego konta. Jak: Wejdź na stronę lub do aplikacji, zaloguj się, przejdź do ustawień i zmień hasło na nowe, mocne hasło. 2. Zweryfikuj aktywne zalogowania Sprawdzenie, gdzie jesteś zalogowany, pozwala wylogować potencjalnie niebezpieczne sesje. Jak: W ustawieniach konta znajdź sekcję „Aktywne sesje" lub „Urządzenia" i zobacz, z jakich miejsc i urządzeń jesteś zalogowany. Wyloguj się z podejrzanych sesji. 3. Zmień wszystkie podobne hasła Jeśli używasz podobnych haseł na innych kontach, zmień je, aby uniknąć przejęcia innych kont przez osoby, które zdobyły jedno z Twoich haseł. Jak: Upewnij się, że każde konto ma unikalne hasło, które nie jest podobne do żadnego innego. 4. Wprowadź logowanie wieloskładnikowe (2FA) Logowanie wieloskładnikowe zapewnia dodatkową warstwę bezpieczeństwa, nawet jeśli ktoś zna Twoje hasło. Jak: Włącz 2FA w ustawieniach konta, wybierając opcję dodania drugiego czynnika, np. kodu SMS, aplikacji autoryzującej (np. Google Authenticator), lub klucza sprzętowego. 5. Zacznij korzystać z menedżera haseł		

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

	Menedżer haseł pomoże Ci generować i przechowywać silne, unikalne hasła dla każdego konta. Jak: Zainstaluj menedżer haseł (np. KeePassXC, LastPass) i przenieś do niego wszystkie swoje hasła. Używaj go do automatycznego wypełniania haseł podczas logowania. Prezentacja kluczowych informacji na temat Ransoware. Ochrona przed ransoware – narzędzie w Windows,		
Ćwiczenia praktyczne – backup danych	Praca indywidualna lub w grupach nad sprawdzenie czy jest włączony antywirus. Ransomware – wyjaśnienie czym jest i jak się chronić To rodzaj złośliwego oprogramowania, które blokuje dostęp do twoich plików na komputerze i żąda okupu za ich odblokowanie. Wygląda to tak, jakby ktoś zamknął cię w pokoju i zażądał pieniędzy, aby cię wypuścić. - Regularne kopie zapasowe: Przechowuj ważne pliki na zewnętrznym dysku lub w chmurze. Jeśli komputer zostanie zainfekowany, możesz przywrócić pliki z kopii zapasowej. - Aktualizacje oprogramowania: Upewnij się, że system operacyjny i wszystkie programy są zawsze aktualne. Nowe aktualizacje często naprawiają luki bezpieczeństwa.	15 min	Komputery

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

	- Antywirus: Zainstaluj i używaj programu antywirusowego, który może wykrywać i blokować zagrożenia. - Bezpieczne surfowanie: Nie klikaj w podejrzane linki ani nie pobieraj plików z nieznanych źródeł. - Edukacja: Naucz się rozpoznawać podejrzane wiadomości e-mail i komunikaty, które mogą zawierać złośliwe oprogramowanie. Sprawdzenie w ustawieniach maszyn czy ochrona przed ransomware jest włączona na ich komputerze. **Zasada 3-2-1** 3 kopie danych: Miej przynajmniej trzy kopie swoich danych. Jedna kopia to oryginał, a pozostałe to kopie zapasowe. 2 różne nośniki: Przechowuj te kopie na dwóch różnych rodzajach nośników. Na przykład, jedna kopia na komputerze, a druga na zewnętrznym dysku twardym. 1 kopia offline: Miej przynajmniej jedną kopię zapasową, która nie jest podłączona do internetu, żeby była bezpieczna, nawet jeśli komputer zostanie zainfekowany wirusem. Przykład dla 13-latka: Wyobraź sobie, że masz ważne zdjęcia i projekty w swoim komputerze. Chcesz się upewnić, że nie stracisz tych danych, nawet jeśli coś pójdzie nie tak. Oto jak możesz zastosować zasadę 3-2-1: 3 kopie danych: Zrób trzy kopie swoich zdjęć. Jedna kopia to ta na komputerze, a druga to na zewnętrznym dysku twardym (np. pendrive).		

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

	Trzecią kopię możesz umieścić w chmurze (np. Google Drive). 2 różne nośniki: Przechowuj te kopie na różnych nośnikach. Na przykład, jedna kopia na komputerze, druga na pendrivie, a trzecia w chmurze. Pendrive i chmura to różne nośniki. 1 kopia offline: Trzymaj pendrive (z drugą kopią) w bezpiecznym miejscu, które nie jest ciągle podłączone do internetu. To zabezpiecza Twoje dane, nawet jeśli komputer ulegnie awarii lub zostanie zaatakowany przez wirus.		
Omówienie wyników i dyskusja	Przedstawienie wyników pracy, dyskusja, wyjaśnienie trudniejszych zagadnień.	10 min	Tablica, notatki
Podsumowanie i refleksja	Podsumowanie kluczowych zagadnień. Zachęta do refleksji nad tematem.	5 min	Prezentacja

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

LEKCJA 3 – INCYDENTY

Arkusz pracy dla uczniów 1 Komentarz dla nauczyciela

Cel: Pomóc uczniom zrozumieć, jak reagować na wyciek hasła i jakie kroki podjąć, aby zminimalizować jego skutki.

Czas trwania: 15-30 minut

Opis aktywności:

1) Wprowadzenie do sytuacji: Uczniowie zostają poinformowani, że doszło do wycieku ich hasła (może to być fikcyjna sytuacja, np. „Otrzymujesz e-mail, że Twoje konto zostało zhakowane").

Pytanie do uczniów: Co myślicie, czujecie i co robicie, kiedy dowiadujecie się o wycieku hasła? (arkusz pracy nr 1)

2) Przygotowanie do opowiedzenia historii: W ramach grupy uczniowie przygotowują historię, zaczynając od „nieszczęsnego wydarzenia" – dowiedzenia się o wycieku hasła. Powinni podzielić się swoimi przemyśleniami, emocjami i działaniami, które podjęli w tej sytuacji. Można zacząć od trzech pytań:

- Co myślisz? – Jakie myśli pojawiają się w Twojej głowie, gdy dowiadujesz się, że Twoje hasło zostało wykradzione? Zastanawiasz się, co może stać się z Twoimi danymi?
- Co czujesz? – Jakie emocje towarzyszą Ci w tej chwili? Czy czujesz panikę, niepokój, złość, może wstyd? Jak reagujesz na tę sytuację?
- Co robisz? – Jakie kroki podejmujesz, aby naprawić sytuację? Czy zmieniasz hasło, kontaktujesz się z administratorem, sprawdzasz swoje konto? Co dokładnie robisz, aby zapewnić bezpieczeństwo swoich danych?
- Wydarzenia – Jakie mogą być konsekwencje tego wydarzenia? Co się może zadziać? (np. włamanie na skrzynkę pocztową/popularny serwis gdzie było takie samo hasło).

3) Praca nad historią: Uczniowie traktują arkusz pracy jako bazę do stworzenia swojej historii. Powinni wskazać kluczowe wydarzenia (np. dowiedzenie się o wycieku hasła) i zastanowić się, jak doprowadzić historię do pozytywnego zakończenia (tzw. happy end).
4) Prezentacja grup: Każda grupa prezentuje swoją historię, opisując emocje i działania podejmowane po wycieku hasła.
5) Wspólne omówienie działań: Na podstawie przedstawionych historii nauczyciel omawia właściwe kroki postępowania po wycieku hasła np:

- Zmiana hasła na wszystkich serwisach, gdzie używane było to samo hasło
- Sprawdzenie historii logowań (jeśli dostępne)
- Skontaktowanie się z administratorem serwisu lub pomocą techniczną
- Korzystanie z menedżera haseł i włączenie dwuetapowego uwierzytelniania
- Monitorowanie konta w celu wykrycia nietypowej aktywności

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

LEKCJA 3 – INCYDENTY

Arkusz pracy dla uczniów 1

Co robię?	Co czuję?	Co myślę?	Wydarzenia	Co zrobić w przypadku wycieku hasła?
			OH NO	

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

Opcjonalne zadanie domowe

- **Sprawdź swoje adresy e-mail:**

Skorzystaj z serwisu Have I Been Pwned i sprawdź, czy Twoje adresy e-mail brały udział w wyciekach danych.

Zrób listę adresów e-mail, które zostały ujawnione w wyciekach.

- **Dowiaduj się o nowych wyciekach:**

Skorzystaj z opcji powiadamiania o nowych wyciekach w serwisie Have I Been Pwned. Wprowadź swoje adresy e-mail, aby otrzymywać powiadomienia o przyszłych wyciekach związanych z tymi adresami.

- **Zmień hasła:**

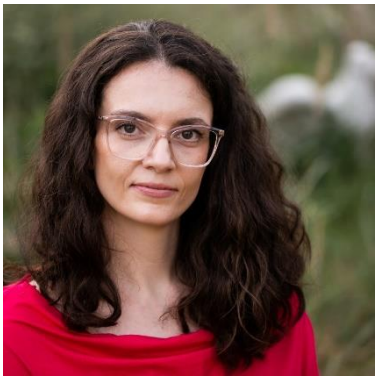
Zmień hasła do kont, które były zaangażowane w wycieki. Użyj silnych, losowych haseł. Możesz wykorzystać menedżer haseł, taki jak KeePassXC, aby wygenerować i przechować nowe hasła.

- **Stwórz kopie zapasowe:**

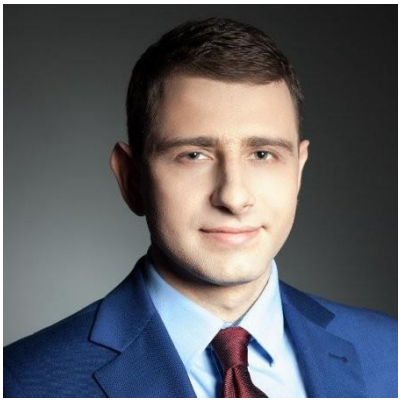
Wybierz ważne pliki, takie jak dokumenty, zdjęcia i inne dane, które chcesz zabezpieczyć przed utratą. Wykorzystaj zewnętrzne nośniki (np. dysk zewnętrzny) lub chmurę (np. Google Drive, OneDrive), aby stworzyć kopie zapasowe tych plików. Upewnij się, że dostęp do kopii jest chroniony silnym hasłem oraz że regularnie aktualizujesz kopie zapasowe.

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: Coventry University Research Institute Europe
PARTNERZY: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

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/

CYBERSEC
EDUCHECK

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