Hasła i ich bezpieczeństwo

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

LEKCJA 2 - Hasła

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

Szanowni Państwo,

Oddajemy w Państwa ręce scenariusz zajęć na temat bezpieczeństwa haseł, kluczowego elementu ochrony prywatnych informacji w internecie. Zdajemy sobie sprawę, że temat bezpieczeństwa cyfrowego jest bardzo szeroki, dlatego ze względu na ograniczenia czasowe skupiliśmy się na podstawowych, ale niezwykle istotnych zagadnieniach związanych z tworzeniem i zarządzaniem hasłami.

Nasze 45-minutowe zajęcia skupiają się na trzech głównych celach: uczniowie nauczą się tworzyć silne i unikalne hasła, zrozumieją, dlaczego dwuetapowe uwierzytelnianie (2FA) zwiększa bezpieczeństwo kont, oraz poznają metody bezpiecznego zarządzania hasłami, w tym korzyści z menedżerów haseł.

Jest to minimalny czas, aby przeprowadzić kluczowe aktywności, takie jak ćwiczenia grupowe i dyskusje, które mają na celu ugruntowanie wiedzy (założyliśmy, że w tych 45minutach nie starczy czasu na konfigurację menadżera haseł na własnych urządzeniach, a szkoda). Jeśli jednak mają Państwo więcej przestrzeni czasowej, sugerujemy rozbicie tego tematu na mniejsze części i wykorzystanie ich podczas kolejnych lekcji, 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:
KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

Cele lekcji

- **Cele jawne**:
    - Uczniowie będą potrafili tworzyć silne i unikalne hasła, które zapewnią lepszą ochronę ich kont online. Zrozumieją konieczność korzystania z innego hasła dla każdego serwisu z jakiego korzystają.
    - Uczniowie zrozumieją, dlaczego dwuetapowe uwierzytelnianie jest ważne i jak je włączyć na swoich kontach.
    - Uczniowie nauczą się zarządzać swoimi hasłami, w tym korzystania z menedżerów haseł.
    - Rozwijanie umiejętności analizy i krytycznego myślenia.
- **Cele ukryte**:
    - Wzmacnianie współpracy w grupie.
    - Zachęcanie do samodzielnego myślenia i rozwiązywania problemów.

Kontekst - słowa kluczowe

hasła, bezpieczeństwo online, dwuetapowe uwierzytelnianie, menedżery haseł, ochrona danych osobowych, cyberbezpieczeństwo

Uzasadnienie wyboru tematu:

- W dzisiejszych czasach dostęp do technologii i internetu jest powszechny i niemal ciągły, młodzież regularnie korzysta z różnorodnych serwisów online. W związku z tym istnieje zwiększone ryzyko utraty prywatnych danych oraz włamań na konta z powodu słabych haseł.
- Wiele osób używa tych samych haseł w różnych serwisach, co naraża ich na poważne konsekwencje w przypadku jednego wycieku danych. Zrozumienie konieczności tworzenia silnych, unikalnych haseł oraz korzyści płynących z dwuetapowego uwierzytelniania ma kluczowe znaczenie dla bezpieczeństwa online.
- Edukacja na temat zarządzania hasłami, w tym korzystania z menedżerów haseł, uczy młodzież odpowiedzialności za własne dane i konta oraz rozwija świadomość zagrożeń w cyberprzestrzeni.

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 [Hasła i ich bezpieczeństwo].
    - Arkusze pracy z ćwiczeniami.
    - Tablica
    - Komputery z dostępem do internetu (jeśli potrzebne).
    - Test online – Opcja skorzystania z platformy pozwalającej tworzyć quizy o hasłach i bezpieczeństwie online (np. kaboot.it - przykładowy gotowy quiz https://play.kahoot.it/v2/?quizId=cd611872-3056-4990-803f-765179e75c0e)
- **Doświadczenie**: Opcjonalnie zaproszenie uczniów do aktywności przed zajęciami np. Gra edukacyjna od Google w formie interaktywnej przygody, która uczy m.in. tworzenia silnych haseł https://beinternetawesome.withgoogle.com/en_us/interland/landing/tower-of-treasure
- **Przestrzeń**:
    - Sala wyposażona w ekran/projektor.
    - 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 2 – HASŁA

Struktura lekcji

Cel	Aktywność	Czas	Materiały
Wprowadzenie	Przedstawienie tematu i celów lekcji. Na początek kilka historii – nauczyciel dzieli się jedną lub więcej historiami innych uczniów. Nauczyciel pyta się: Czy te historie są prawdziwe? Nie. Zostały wymyślone na potrzeby lekcji. Co nie znaczy, że nie mogły się wydarzyć	5 min	Prezentacja
Mini Quiz czy to jest bezpieczne hasło	Nauczyciel zadaje uczniom pytania w formie quizu, prosząco o zapisanie odpowiedzi (1 jest prawdziwa). Przykładowe pytania: 1. Które hasło jest najbardziej bezpieczne? JPL93#q anna1234! Bazylia456 **Idzspachackerzeniezlamiesztego.** 2. Które hasło jest najłatwiejsze do odgadnięcia? **MojeHasło123** Letni2024 Super!2023 Qwerty!123 3. Które hasło jest najmniej bezpieczne? **Qwerty123** P@ssw0rd 1234abc! Secure*Pass123 4. Które z poniższych haseł może być najłatwiejsze do odgadnięcia, jeśli haker zna imię twojego zwierzęcia i jego datę urodzenia? K!ngC0bra L0veCats! Adventure987 **Fluffy2021** 5. Czym jest 2FA? Funkcja w telefonach, która przyspiesza ładowanie baterii	10 min	

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

	Skrót oznaczający dwa filtry antywirusowe działające jednocześnie **To dodatkowe zabezpieczenie, które pomaga upewnić się, że tylko Ty możesz się zalogować, nawet jeśli ktoś zna Twoje hasło** System szyfrowania danych w chmurze, który zwiększa bezpieczeństwo plików Nauczyciel prezentuje odpowiedzi i prosi uczniów o podzielenie się liczbą poprawnych odpowiedzi. 1d) Im hasło dłuższe, tym trudniejsze do złamania. Idealnie, aby hasło miało 15 znaków lub więcej. Hasłem może być 4 lub więcej nieoczywistych słów sklejonych ze sobą 2 a) MojeHasło123 jest najłatwiejsze do odgadnięcia, ponieważ używa prostych słów i sekwencji liczb, które są często stosowane w hasłach przez wiele osób. Pozostałe hasła też są przewidywalne. 3 a) Najsłabsze hasło to Qwerty123. Jest to popularne hasło oparte na prostym wzorze klawiatury i łatwe do odgadnięcia w atakach słownikowych. Pozostałe hasła zawierają różne typy znaków i są mniej przewidywalne, choć nadal mogą wymagać dodatkowych ulepszeń. 4 d) Najłatwiejsze do odgadnięcia hasło to Fluffy2021, ponieważ zawiera imię zwierzęcia i datę, co ułatwia hakerowi odgadnięcie hasła przy znajomości tych informacji. 5c) 2FA (Two-factor authentication) to sposób na dodatkowe zabezpieczenie Twojego konta, oprócz samego hasła. Działa tak, że po wpisaniu hasła musisz jeszcze potwierdzić swoją tożsamość w inny sposób, np. wpisując kod z SMSa, używając specjalnej aplikacji (jak Google Authenticator) albo mając specjalny klucz. Dzięki temu Twoje konto jest dużo bardziej bezpieczne Omówienie wyników – dlaczego takie są niebezpieczne. **Alternatywnie** (zamiast tego quizu) można wykorzystać **Grę „Password Game” (arkusz**		

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

	pracy nr 2). To szybka aktywność, w której uczniowie w grupach odgadują hasła na podstawie jedno- lub dwuwyrazowych wskazówek. Każda grupa wybiera „dawcę wskazówek", który ma 30 sekund na pomoc zespołowi w odgadnięciu hasła, a grupa ma 3 próby. Za każdą poprawną odpowiedź grupa zdobywa 2 punkty, a jeśli nie uda się odgadnąć hasła, tracą kolejkę, ale nie tracą punktów.		
Przekazanie wiedzy: Często popełniane błędy	**1 Pytania otwarte do uczniów (można zadać wszystkie lub wybrane)**: Ile różnych haseł używasz do swoich kont? Jak często używasz tego samego hasła do kilku różnych kont? Jak często zmieniasz swoje hasła? Jak często zdarza Ci się zapomnieć hasło? **2. Prezentacja kluczowych informacji na temat często popełnianych błędów:** • Często używamy jednego hasła w kilku serwisach • Często używamy podobnych haseł • Wykorzystujemy informacje osobiste • Dzielimy się hasłami • Zbyt krótkie hasła • Korzystamy ze wzorców na klawiaturze (np. QWERT) • Podstawienie cyfr/znaków specjalnych (np. Password → P@$$w0rd) • Przechowujemy hasła w plikach tekstowych	10 min	Prezentacja, przykłady multimedialne
Ćwiczenia praktyczne	Praca w grupach Jak Być Bezpiecznym? Nauczyciel dzieli klasę na 4 grupy. Każda grupa ma 5-10 minut na uzupełnienie arkusza pracy nr1. Celem jest odpowiedź na pytania: - Co jest przyczyną problemu w danym przypadku? Może jest ich kilka?	15 min	Arkusz pracy nr 1. Tablica, notatki

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

	- Co Waszym zdaniem mogłoby pomóc w przeciwdziałaniu takiej sytuacji? Przykładowe konteksty dla grup (można wybrać 1 dla wszystkich lub dla każdej grupy inny): • Kliknięcie podejrzanego linku i przejęcie konta: Kliknąłem w link, który wyglądał jak od znajomego, i wpisałem tam swoje dane logowania. Wtedy ktoś przejął moje konto i teraz nie mam dostępu do ważnych rzeczy. • Dostęp do konta po zostawieniu otwartego laptopa: Zostawiłam otwarty laptop w szkole, a ktoś wszedł na moje konto społecznościowe i opublikował niemiłe rzeczy, udając mnie. Teraz muszę tłumaczyć się nauczycielom i znajomym, bo wszyscy myślą, że to ja. • Kradzież pieniędzy przez słabe hasło: Ustawiłam bardzo proste hasło do mojego konta bankowego i ktoś je złamał, kradnąc wszystkie pieniądze. Teraz muszę walczyć o to, żeby je odzyskać. • Utrata konta w grze po podzieleniu się hasłem: Dałem koledze moje hasło do gry, a on zmienił je i zaczął używać mojego konta. Straciłem wszystkie moje osiągnięcia, nad którymi pracowałem przez długi czas.		
Omówienie wyników i dyskusja	Przedstawienie narzędzia menadżera haseł jako rozwiązania. Wyjaśnienie trudniejszych zagadnień.	10 min	
Podsumowanie i refleksja	Podsumowanie kluczowych zagadnień. Zachęta do działania aby wzmocnić swoje bezpieczeństwo	5 min	Prezentacja

Opcjonalne zadanie domowe

Zweryfikuj swoje hasła:

- Sprawdź, czy Twoje hasła są długie, losowe, i unikalne.

Dofinansowane przez Unię Europejską
LIDER: Coventry University Research Institute Europe
PARTNERZY: KREA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

- Zainstaluj KeePassXC (lub inny menedżer haseł) na swoim komputerze.
- Przenieś wszystkie swoje hasła do menedżera haseł. Przestań zapisywać hasła na karteczkach lub w plikach tekstowych.

Zmień hasła słabe i słownikowe:

- Jeśli używasz prostych haseł, takich jak "123456" lub "password", natychmiast je zmień.
- Przejrzyj systemy, z których korzystasz:
- Zrób listę wszystkich kont, aplikacji i systemów, z których korzystasz, i upewnij się, że wszystkie są odpowiednio zabezpieczone.

Włącz uwierzytelnianie dwuskładnikowe (2FA):

- Przynajmniej na najważniejszych kontach, takich jak e-mail, media społecznościowe, bankowość.
- Skorzystaj z aplikacji takich jak Google Authenticator lub innych dostępnych opcji.

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

Materiały i wiedza dla nauczycieli

Opis metody 5 Whys (5xDlaczego)

Metoda 5 Whys (5 x Dlaczego) pomaga uczniom zrozumieć, dlaczego doszło do problemu, poprzez zadawanie pięciu kolejnych pytań „dlaczego?". Polega na zadawaniu pytania „dlaczego?" pięć razy, aby dojść do prawdziwego źródła problemu, a nie zatrzymywać się na pierwszej, oczywistej odpowiedzi. Dzięki temu narzędziu uczniowie mogą lepiej zrozumieć, co stoi za danym problemem, i jak można go rozwiązać.

Alternatywne pytania:

Zamiast zadawać „dlaczego" pięć razy, warto zastosować bardziej otwarte pytania, które nie wywołają w uczniach poczucia bycia osądzanym. W naszym przykładzie używamy „Co jest przyczyną?". Specyficzne pytania mogą wyglądać następująco:

- Jak to się stało, że ktoś dostał Twoje hasło?
- Ciekawi mnie, jak wybrałeś swoje hasło?
- Co myślałeś, kiedy tworzyłeś to hasło?
- Czy możesz mi pomóc zrozumieć, dlaczego to hasło wydawało się wystarczające?

Przykłady zastosowania (Kradzież danych z konta bankowego/ Utrata konta w grze po podzieleniu się hasłem):

Problem: Ktoś włamał się na moje konto bankowe i ukradł wszystkie pieniądze.	Problem: Straciłem dostęp do mojego konta w grze, bo podałem hasło koledze.
• Dlaczego ktoś włamał się na konto? Ponieważ miał dostęp do mojego hasła. • Dlaczego miał dostęp do mojego hasła? Ponieważ użyłem bardzo prostego hasła, które łatwo było złamać. • Dlaczego użyłem prostego hasła? Ponieważ myślałem, że łatwe do zapamiętania hasło będzie wygodniejsze. • Dlaczego zależało mi bardziej na wygodzie niż na bezpieczeństwie? Ponieważ nie rozumiałem, jak ważne jest silne hasło. • Dlaczego nie rozumiałem, jak ważne jest silne hasło? Ponieważ nie miałem wystarczającej wiedzy o zagrożeniach związanych z cyberbezpieczeństwem.	• Dlaczego straciłeś dostęp do konta? Bo mój kolega zmienił hasło. • Dlaczego podałeś koledze swoje hasło? Bo potrzebował dostępu do gry. • Dlaczego myślałeś, że podzielenie się hasłem jest w porządku? Bo ufałem, że kolega nie nadużyje tego zaufania. • Dlaczego nie pomyślałeś o konsekwencjach? Bo nie znałem ryzyka związanego z udostępnianiem haseł. • Dlaczego nie znałeś ryzyka? Bo wcześniej nie zwracałem uwagi na zasady bezpieczeństwa kont online.

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

Rozwiązania

Po zidentyfikowaniu przyczyn, uczniowie mogą wymyślić rozwiązania, które zapobiegną podobnym sytuacjom w przyszłości, np.:

- Używanie silnych i unikalnych haseł.
- Włączanie uwierzytelniania dwuskładnikowego (2FA).
- Nieudostępnianie haseł innym osobom, nawet znajomym.

Wskazówki dla nauczycieli:

- Zwróćcie uwagę, by uczniowie nie szukali winnych, ale starali się zrozumieć, dlaczego doszło do problemu.
- Używajcie alternatywnych pytań, by zbudować atmosferę zaufania i skłonić do szczerych refleksji.
- Na końcu sesji zachęćcie uczniów do wspólnego tworzenia rozwiązań, które mogą zapobiegać takim problemom w przyszłości.
- Skupcie się na pomysłach na rozwiązania, które dotyczą problemów u dołu kartki.

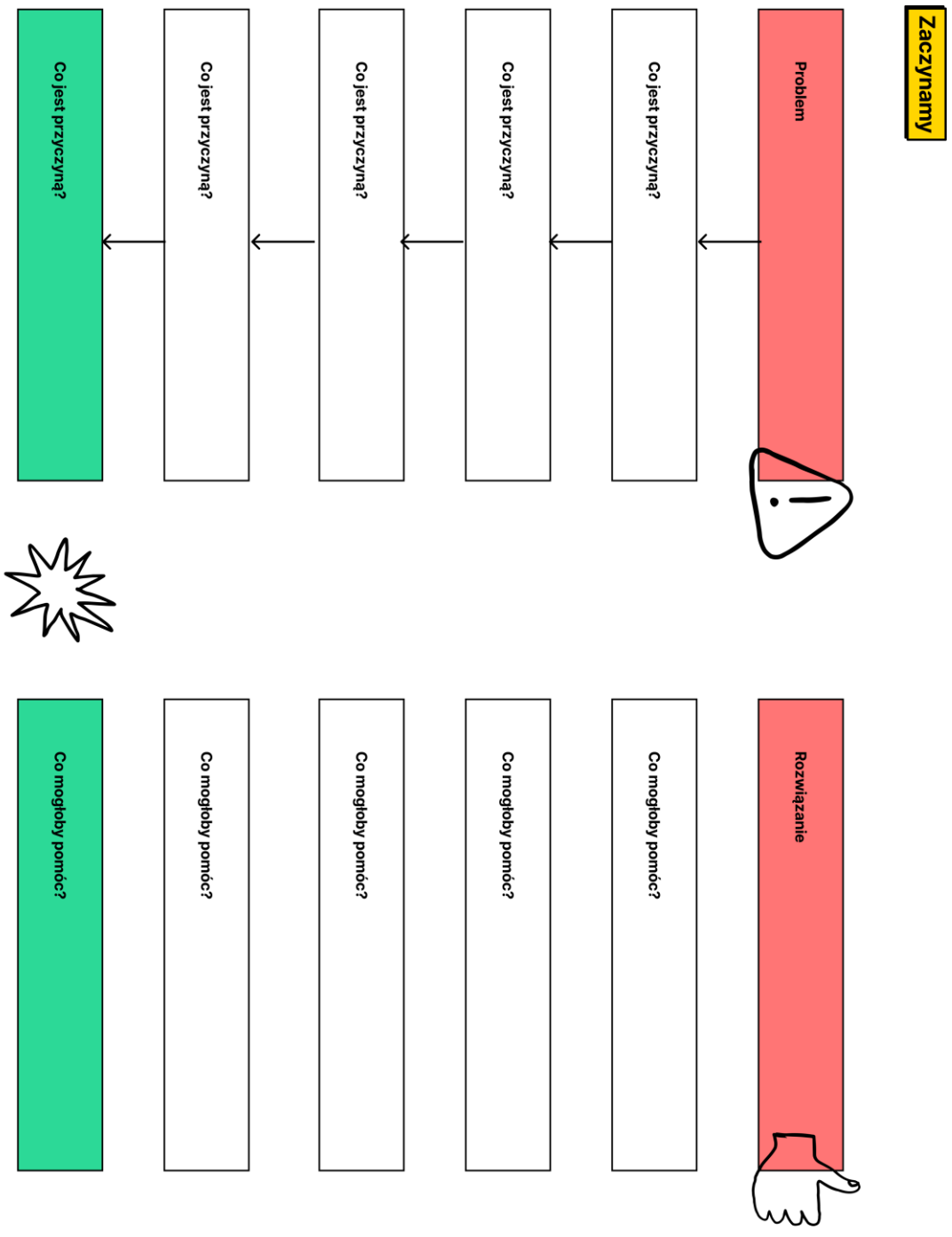
Dofinansowane przez Unię Europejską
LIDER: Coventry University Research Institute Europe
PARTNERZY: KREA Stowarzyszenie Kreatywni dla Biznesu, European Centre for Career Education

LEKCJA 2 – HASŁA

Arkusz pracy nr 1

Zadanie polega na zidentyfikowaniu problemu, zrozumieniu jego przyczyn i wymyśleniu rozwiązań, które pomogą zapobiec podobnym sytuacjom w przyszłości. Na początku zapiszcie jaki jest główny problem w przypadku, który analizujecie (np. "Konto zostało przejęte przez hakera", "Utrata dostępu do konta", "Kradzież danych"). Zastanówcie się co jest przyczyną tej sytuacji (Dlaczego ten problem wystąpił? Co jest jego przyczyną?). Pogłębcie analizę.

W kolejnym kroku zastanówcie się Co mogłoby pomóc? Zapiszcie pomysły w odniesieniu do różnych przyczyn problemów (zaczynając od tych które znajdują się na dole kartki).



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

LEKCJA 2 – HASŁA

Arkusz pracy nr 2 Password Game

Czas trwania: ok. 15 minut dla klasy 25 osób

Przygotowanie:

- Przygotuj 10-15 karteczek z hasłami (lista poniżej).
- Podziel klasę na 5 grup po 5 osób.

Zasady gry:

Podział ról w grupach:

- Każda grupa wybiera 1 osobę jako "dawcę wskazówek", a reszta to "zgadujący".
- Role zmieniają się w każdej rundzie.

Przebieg gry:

- "Dawca wskazówek" losuje karteczkę z hasłem.
- W ciągu 30 sekund daje grupie wskazówki (tylko jedno- lub dwuwyrazowe).
- Grupa ma 3 próby na odgadnięcie hasła.
- Jeśli nie odgadną w czasie, hasło przechodzi do kolejnej grupy (opcjonalnie).

Punktacja:

- Grupa otrzymuje 2 punkty za odgadnięcie hasła.
- Jeśli nie zgadną, tracą kolejkę (ale nie tracą punktów).

Rotacja:

- Po każdej rundzie zmienia się "dawca wskazówek" w grupie.
- Gra trwa do wyczerpania kartek lub upływu czasu (15 minut).

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

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