CYBERSEC

EDUCHECK

Lekcja 2

HASŁA

I ICH BEZPIECZEŃSTWO

Dofinansowane przez Unię Europejską

LIDER: Research Institute Europe | Coventry University

PARTNERZY: KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU

EUROPEAN CENTRE FOR CAREER EDUCATION

Na początek kilka historii

Kliknąłem w podejrzany link, który wyglądał jak od znajomego. Zamiast sprawdzić, co to za strona, wpisałem swoje dane logowania. Zostałem natychmiast wylogowany z wszystkich urządzeń, a moje konto zostało przejęte. Teraz jestem bez dostępu do ważnych danych i nie wiem, co robić.

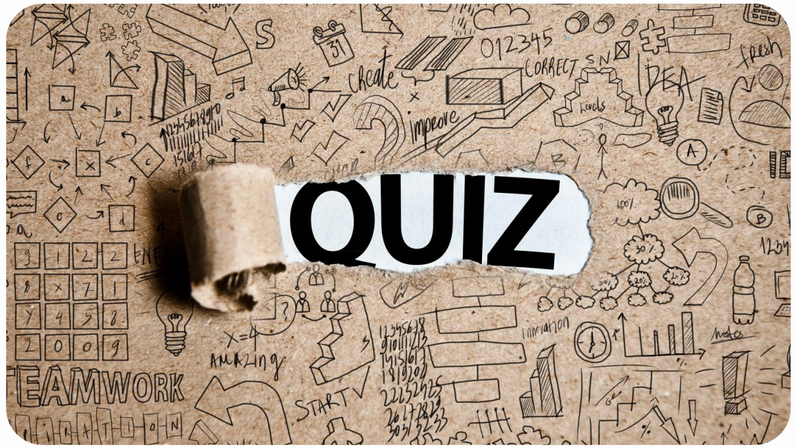
Zignorowałam ostrzeżenia o silnych hasłach i ustawiłam bardzo proste hasło do mojego konta bankowego. Ktoś je złamał i wyczyścił moje konto do zera. Teraz muszę walczyć o zwrot pieniędzy i bardzo się boję, że nie odzyskam wszystkiego.

Podzieliłem się hasłem z kolegą, bo potrzebował dostępu do mojego konta w grze. Po kilku dniach odkryłem, że zmienił mi hasło i używał mojego konta, żeby zdobyć przewagę. Straciłem wszystkie osiągnięcia, nad którymi pracowałem miesiącami.

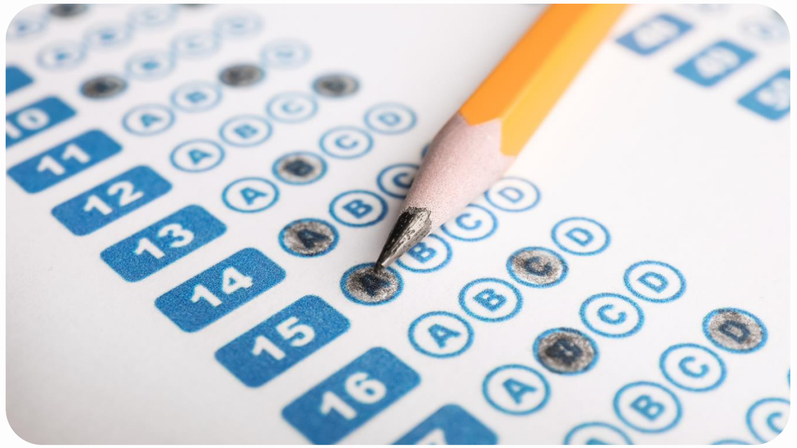
Przez przypadek zostawiłam swój laptop otwarty w szkole. Ktoś dostał się do mojego konta na platformie społecznościowej i opublikował obraźliwe treści, podszywając się pode mnie. Teraz mam poważne problemy i muszę tłumaczyć się przed nauczycielami i znajomymi

CYBERSEC
EDUCHECK

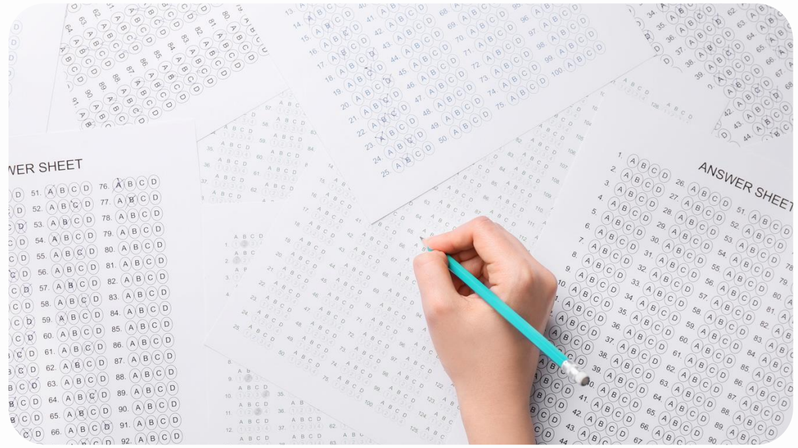
Mini Quiz



Quiz składa się z pięciu pytań



Jedna odpowiedź jest prawidłowa.



Zapisz swoje odpowiedzi.

CYBERSEC
EDUCHECK

1. Które hasło jest najbardziej bezpieczne?

a JPL93#q

b anna1234!

c Bazylia456

d Idzspachackerzeniezlamiesztego

2. Które hasło jest najłatwiejsze do odgadnięcia

a MojeHasło123

b Letni2024

c Super!2023

d Qwerty!123

CYBERSEC
EDUCHECK

3. Które hasło jest najmniej bezpieczne?

a Qwerty123

b P@ssw0rd

c 1234abc!

d Secure*Pass123

CYBERSEC
EDUCHECK

4. Które z poniższych haseł może być najłatwiejsze do odgadnięcia, jeśli haker zna imię twojego zwierzęcia i jego datę urodzenia?

a. K!ngC0bra

b. L0veCats!

c. Adventure987

d. Fluffy2021

CYBERSEC
EDUCHECK

5. Czym jest 2FA?

a Funkcja w telefonach, która przyspiesza ładowanie baterii

b Skrót oznaczający dwa filtry antywirusowe działające jednocześnie

c To dodatkowe zabezpieczenie, które pomaga upewnić się, że tylko Ty możesz się zalogować, nawet jeśli ktoś zna Twoje hasło

d System szyfrowania danych w chmurze, który zwiększa bezpieczeństwo plików

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

Jakie błędy popełniamy?

- **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?**

Jakie błędy popełniamy?

Często używamy jednego hasła w kilku serwisach

TikTok
goosiaczek2245@gmail.com
MegaTrudneHaslo123!

Poczta
goosiaczek2245@gmail.com
MegaTrudneHaslo123!

Szkoła
1989817
MegaTrudneHaslo123!

Jakie błędy popełniamy?

Często używamy podobnych haseł

TikTok

goosiaczek2245@gmail.com

MegaTrudneHaslo1!

Poczta

goosiaczek2245@gmail.com

MegaTrudneHaslo2!

Szkoła

1989817

MegaTrudneHaslo3!

Jakie błędy popełniamy?

Wykorzystujemy informacje osobiste

TikTok

goosiaczek2245@gmail.com

Spooky!Dog

Poczta

goosiaczek2245@gmail.com

SpookyMoj@Piesio

Szkoła

1989817

XXXXXXXXXXX (numer PESEL)

Jakie błędy popełniamy?

Dzielimy się hasłami

Cześć, podaj mi hasło do swojego ... potrzebuję dostępu na chwilę, żeby...

CYBERSEC
EDUCHECK

Jakie błędy popełniamy?

Zbyt krótkie hasła

Najpopularniejsze PIN-y

1234 0000 2580 1111 5555
5683 0852 2222 1212 1998

Jakie błędy popełniamy?

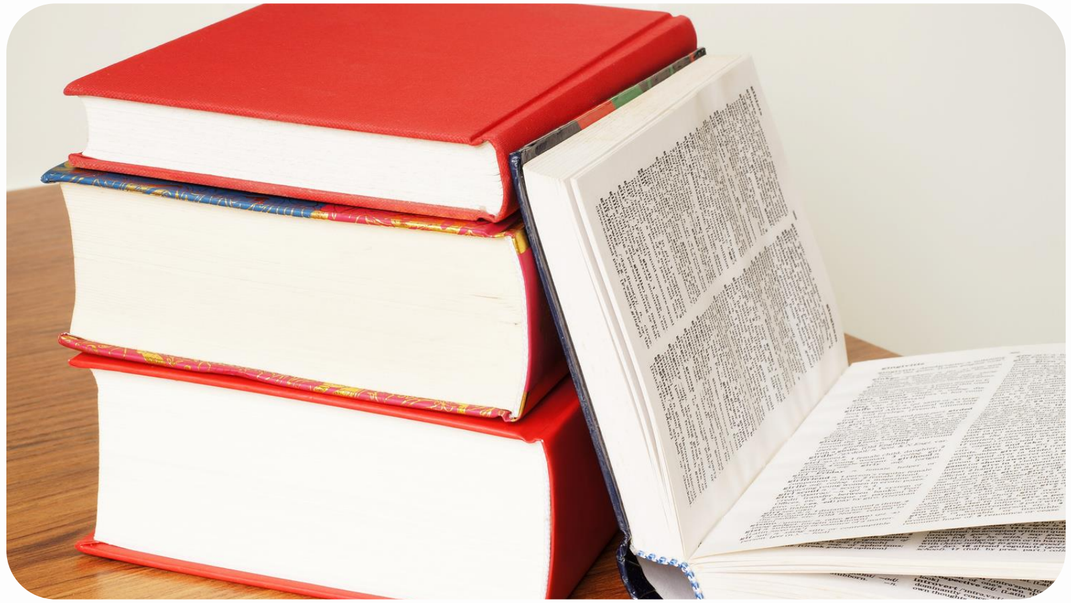
Korzystamy ze wzorców na klawiaturze

(np. QWERT)

Jakie błędy popełniamy?

Korzystamy z haseł słownikowych

- Password
- Qwerty
- Sunshine
- Football
- Monkey
- Iloveyou
- Welcome
- Dragon
- Princess
- Chocolate



Jakie błędy popełniamy?

Podstawienie cyfr/znaków specjalnych

- Password → P@$$w0rd
- Qwerty → Qw3r7y
- Sunshine → unh1n3
- Football → F00tb@ll
- Monkey → M0nk3y
- Iloveyou → 1L0v3Y0u!
- Welcome → W3lc0m3!
- Dragon → Dr@g0n
- Princess → Pr1nc3$$
- Chocolate → Ch0c0l@t3!

Jakie błędy popełniamy?

Przechowujemy hasła w plikach tekstowych

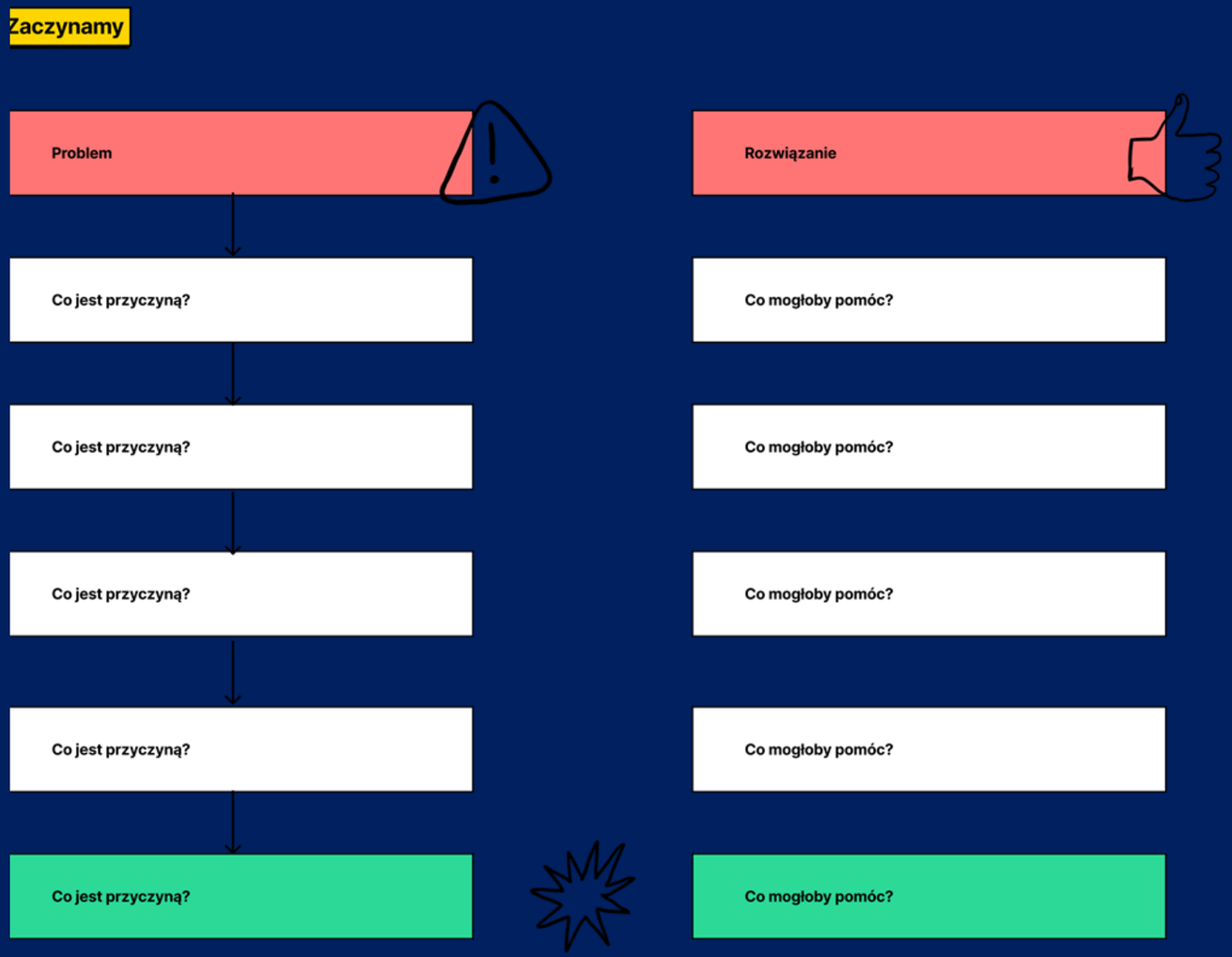
Jak być bezpiecznym?

Karta pracy nr 1

W ramach grupy zastanówcie się:

-Co jest przyczyną problemu w danym przypadku? Może jest ich kilka?

-Co Waszym zdaniem mogłoby pomóc w przeciwdziałaniu takiej sytuacji?



Kilka historii

Kliknięcie podejrzanego linku i przejęcie konta

Dostęp do konta po zostawieniu otwartego laptopa

Kradzież pieniędzy przez słabe hasło

Utrata konta w grze po podzieleniu się hasłem

CYBERSEC
EDUCHECK

Cztery kroki: Jak być bezpiecznym?

CYBERSEC
EDUCHECK

Cztery kroki: Jak być bezpiecznym?

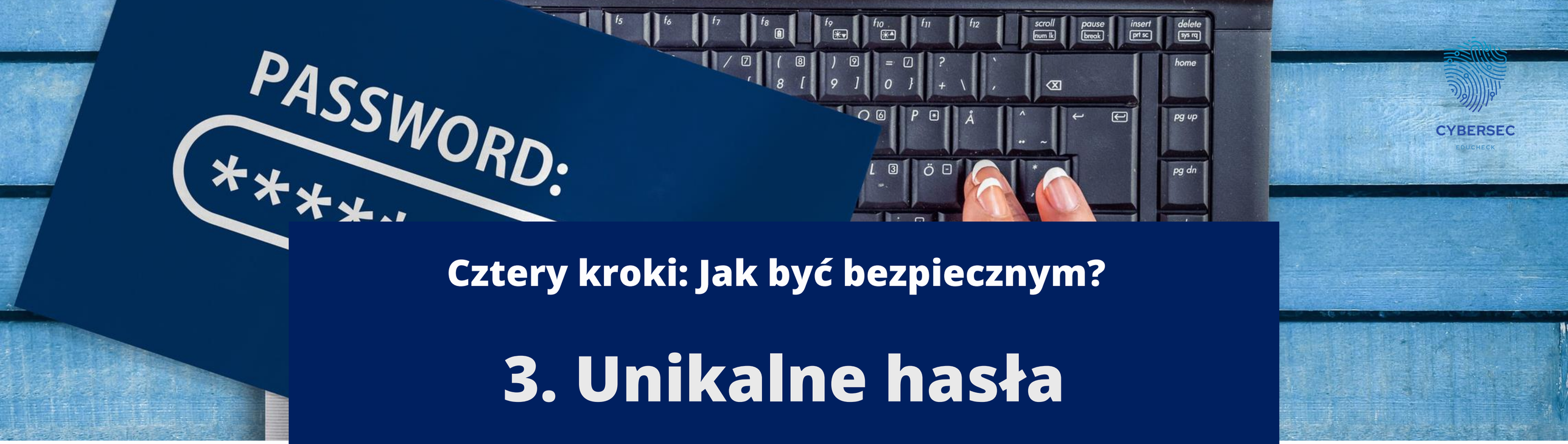
1.Długie hasła

Minimum 12 znaków. Im dłuższe, tym lepsze!
Przykład: T0t@llyS3cur3!2024

Cztery kroki: Jak być bezpiecznym?

2. Losowe hasła

Używaj losowych, niesłownikowych ciągów znaków i wyrażeń.
Przykład: G$8w!XpK23z lub tepskttuwizoMa



CYBERSEC
EDUCHECK

Cztery kroki: Jak być bezpiecznym?

3. Unikalne hasła

Bądź kreatywny! Nie używaj tego samego hasła w różnych miejscach.
Przykład: Bjuti-Polisz&Inglisz

CYBERSEC
EDUCHECK

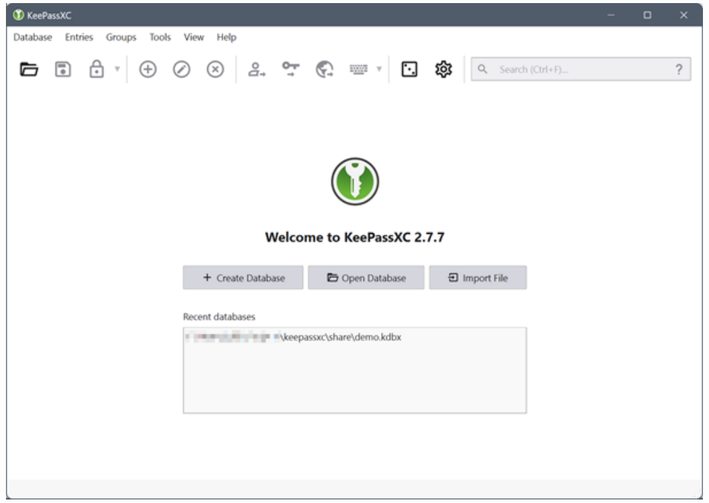
Cztery kroki: Jak być bezpiecznym?

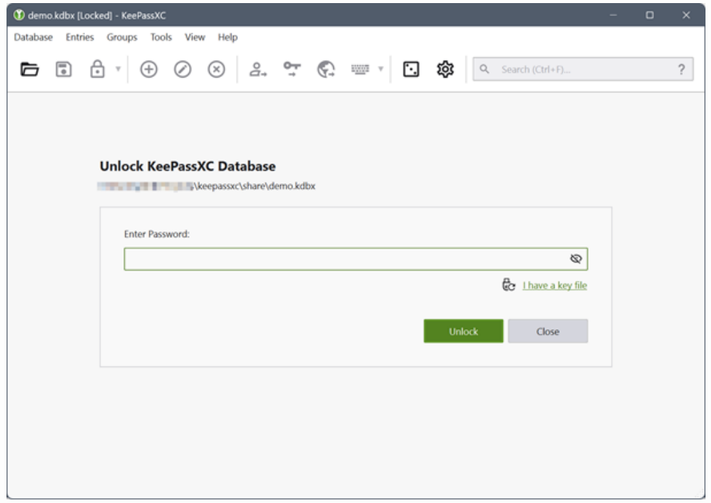
4. Menadżer haseł

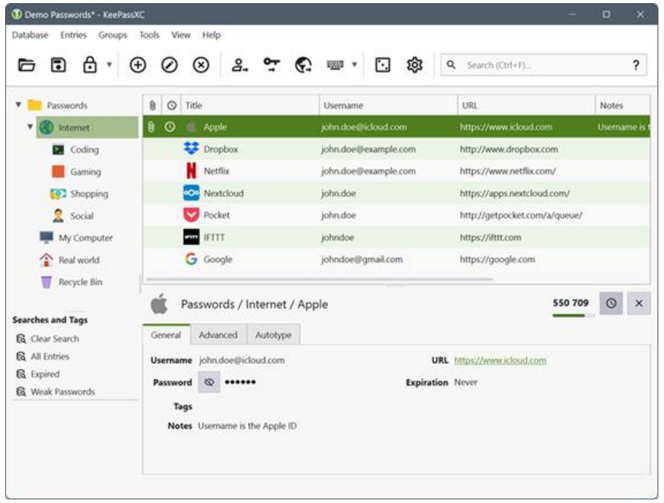
Używaj narzędzi do zarządzania hasłami, by nie musieć ich pamiętać.
Przykład: LastPass, 1Password, Bitwarden, KeePass XC

CYBERSEC
EDUCHECK

KeePassXC







Zainstaluj

Stwórz swoją bazę

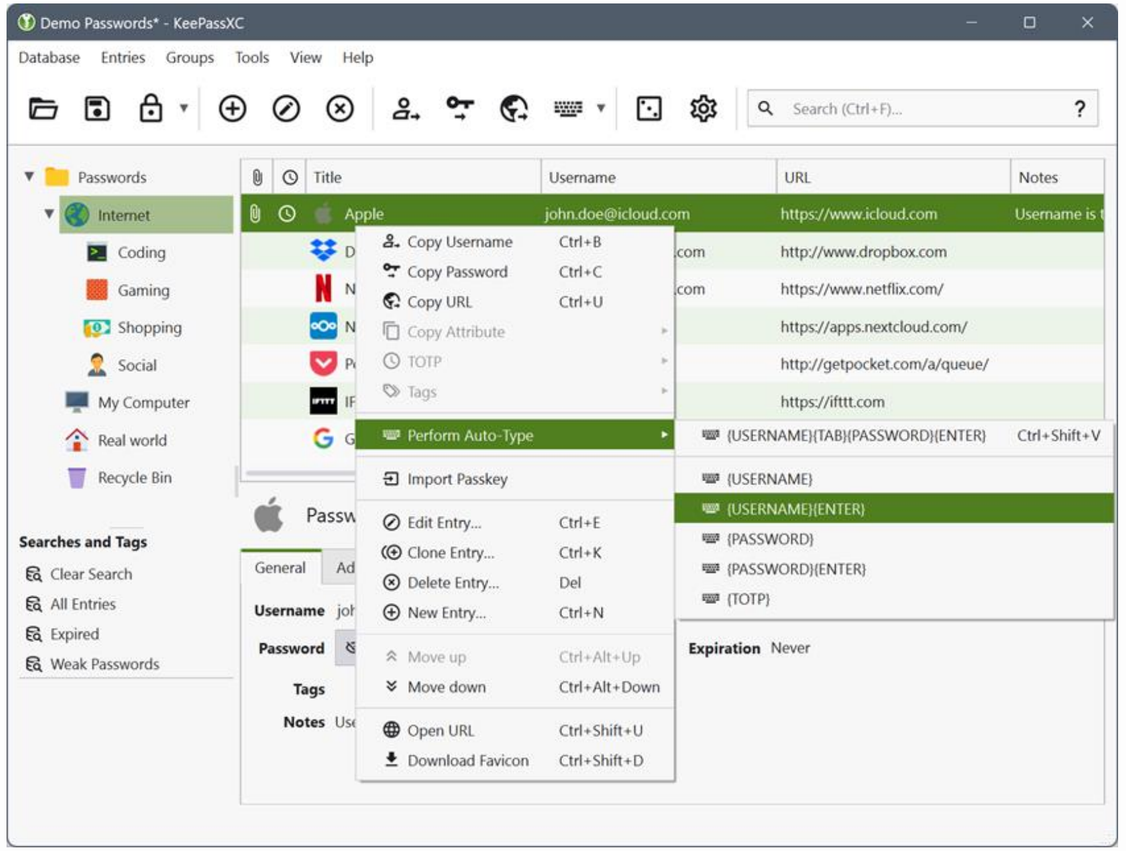
Dodaj hasła i loginy

Link do strony: https://keepassxc.org/download/#windows

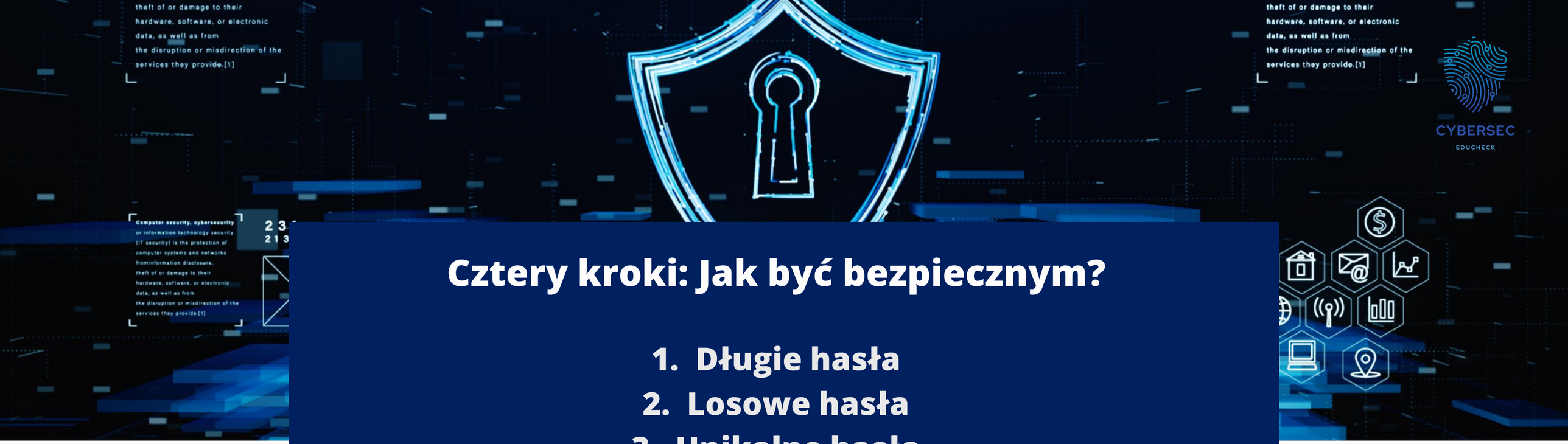
KeePassXC

Korzystając z menadżera haseł dobrze jest pamiętać:

1)Hasło do komputera
2)Hasło do jednej skrzynki pocztowej
3)Hasło do menadżera



Link do strony: https://keepassxc.org/download/#windows



Cztery kroki: Jak być bezpiecznym?

1. Długie hasła
2. Losowe hasła
3. Unikalne hasła
4. Menadżer haseł

Klucz do bezpieczeństwa Twoich kont!

D-L-U-M

DLACZEGO WARTO KORZYSTAĆ Z 2FA/MFA?

- **2FA/MFA to dodatkowa warstwa zabezpieczeń:**

Oprócz hasła, potrzebujesz jeszcze jednej formy potwierdzenia, że to Ty.

- **Jakie są dodatkowe formy potwierdzenia?**

Kod SMS: Dostajesz jednorazowy kod na telefon.
Aplikacja uwierzytelniająca: Generuje kody (np. Google Authenticator).
Klucz sprzętowy: Małe urządzenie, które podłączasz do komputera.
Odcisk palca lub rozpoznawanie twarzy: Biometryczne zabezpieczenia.

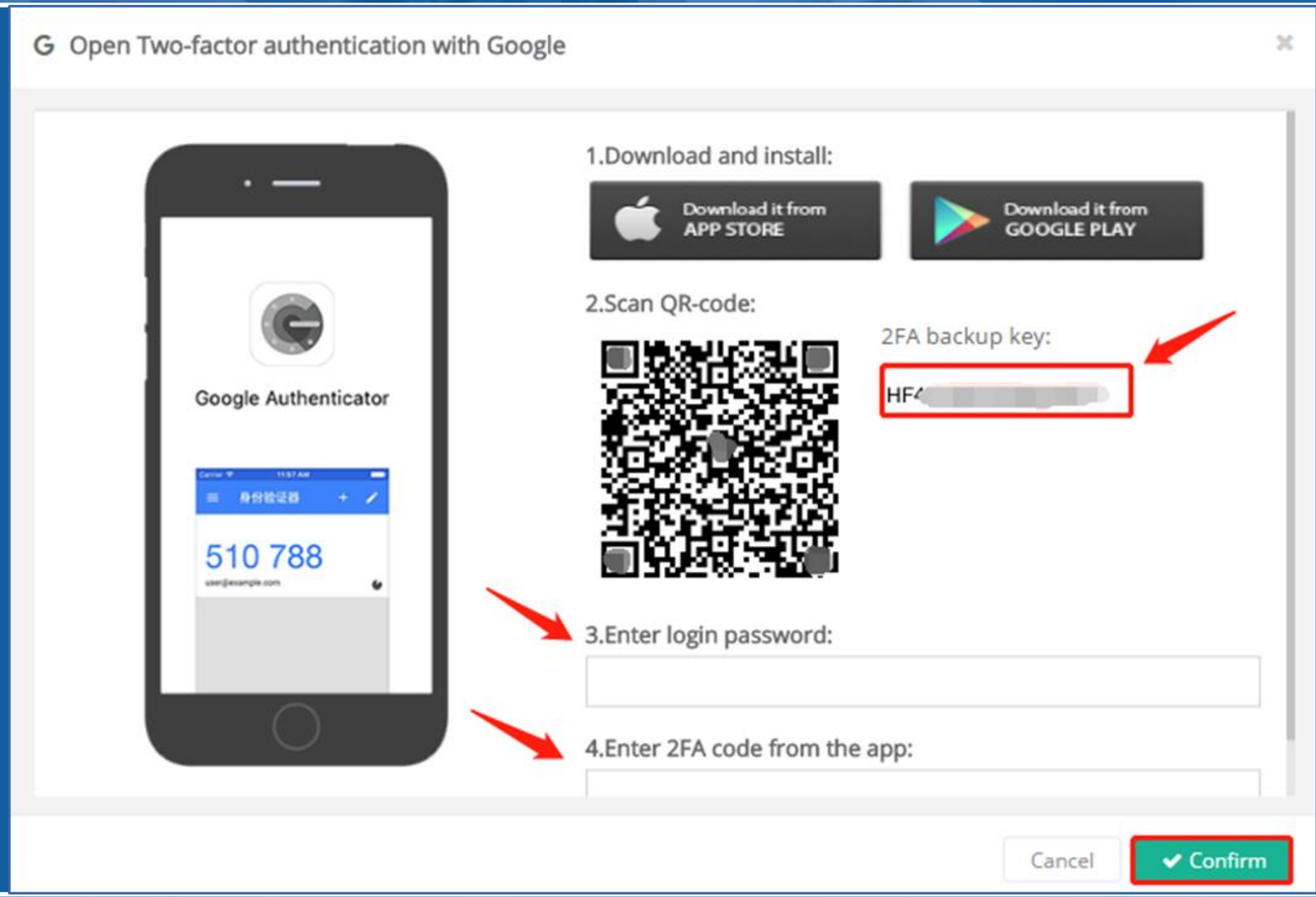
- **Dlaczego warto używać 2FA/MFA?**

Większe bezpieczeństwo: Nawet jeśli ktoś pozna Twoje hasło, nie dostanie się do Twojego konta.
Ochrona przed atakami hakerów: Utrudnia przejęcie konta przez nieuprawnione osoby.

- **Gdzie włączyć 2FA/MFA?**

Większość serwisów, jak Facebook, Instagram, Gmail, oferuje tę opcję w ustawieniach bezpieczeństwa.

GOOGLE / MICROSOFT AUTENITCATOR



Zadanie domowe: Zabezpiecz swoje konta

Zweryfikuj swoje hasła:

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

Dalsze informacje na temat projektu

https://www.coventry.ac.uk/wroclaw/

https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/

https://eccedu.net/

Finansowane przez Unię Europejską. Wyrażone poglądy i opinie są jednak poglądami i opiniami wyłącznie autora(-ów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Ani Unia Europejska, ani EACEA nie mogą być za nie pociągnięte do odpowiedzialności.

CYBERSEC

EDUCHECK

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

Dofinansowane przez Unię Europejską

LIDER: Research Institute Europe | Coventry University

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