CYBERSEC

EDUCHECK

Lekcja 3

INCYDENTY

BEZPIECZEŃSTWA CYFROWEGO

Dofinansowane przez Unię Europejską

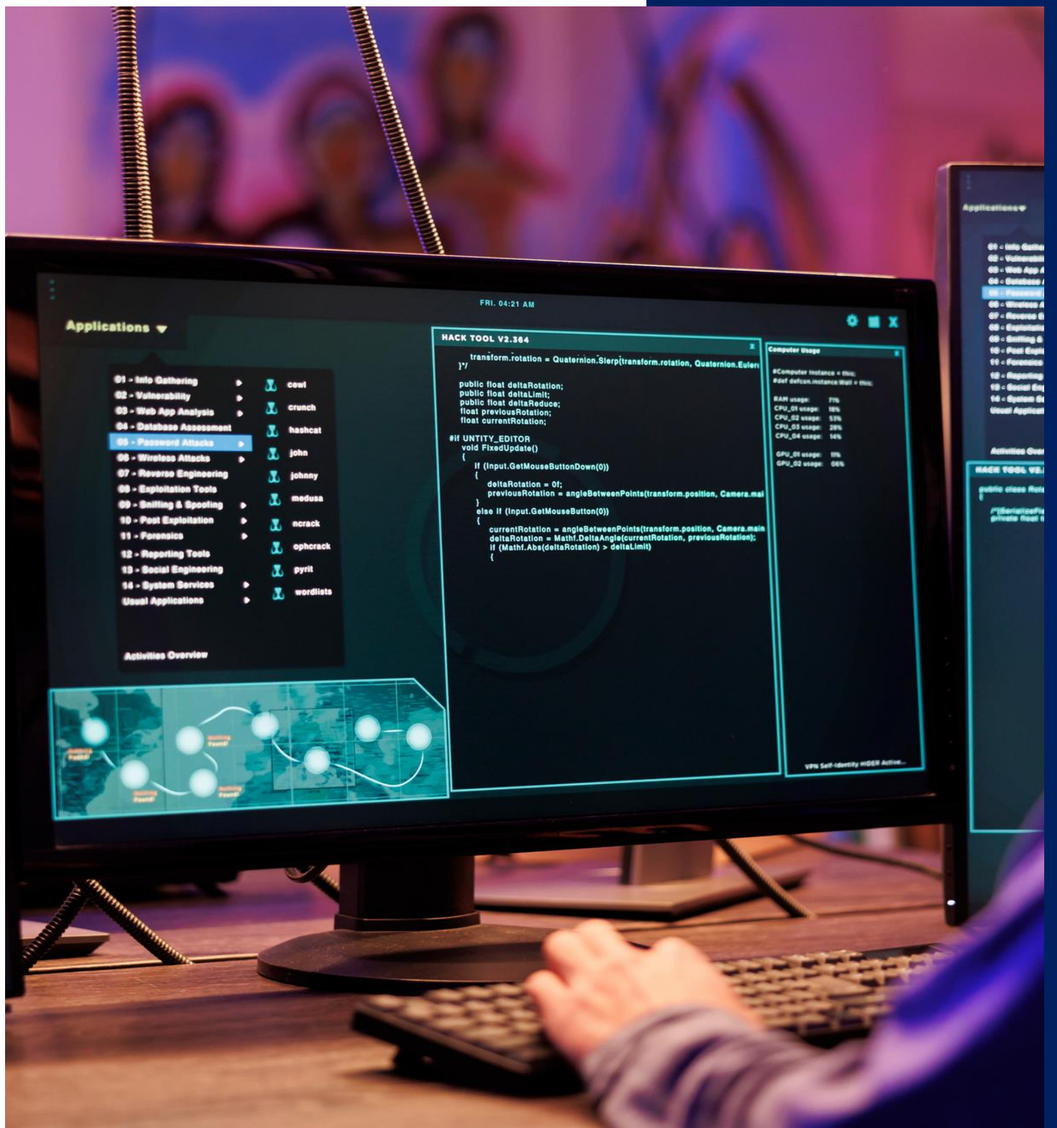
LIDER: Research Institute Europe | Coventry University

PARTNERZY: STOWARZYSZENIE KREATYWNI DLA BIZNESU

EUROPEAN CENTRE FOR CAREER EDUCATION

CYBERSEC
EDUCHECK

Incydenty Bezpieczeństwa Cyfrowego



Incydenty Bezpieczeństwa Cyfrowego

CYBERSEC
EDUCHECK

Włamanie do konta: Ktoś zdobył dostęp do twojego konta bez twojej zgody.

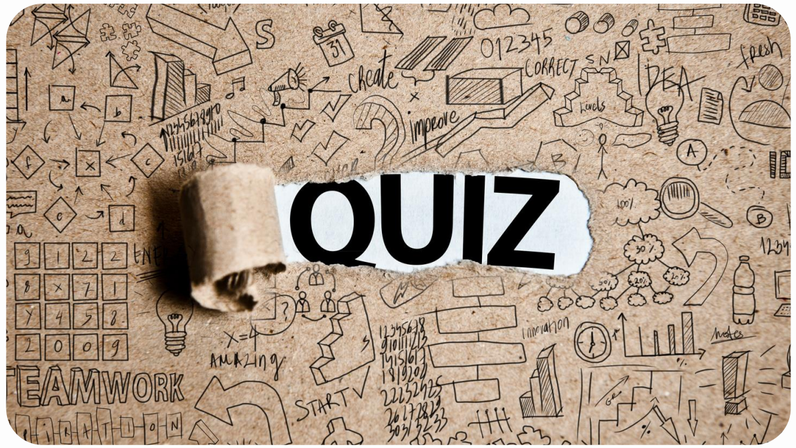
Włamanie do konta bankowego: Ktoś zdobył dostęp do twojego konta bez twojej zgody i przelał pieniądze.

Złośliwe oprogramowanie: Programy, które szkodzą twojemu komputerowi, jak wirusy czy ransomware.

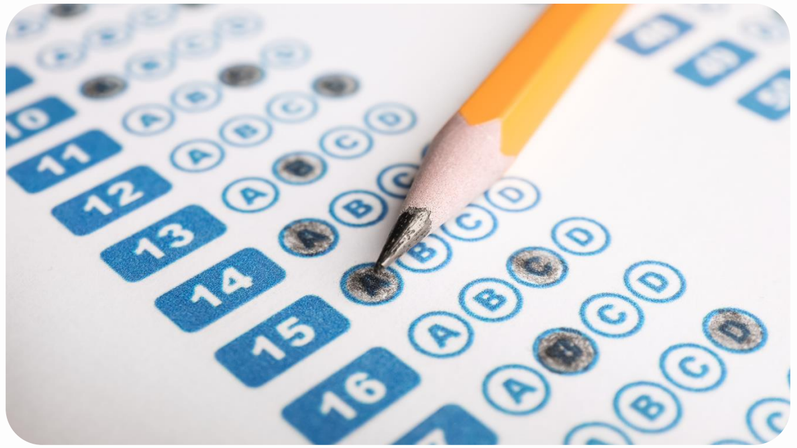
Utrata konta w grze po podzieleniu się hasłem: Ktoś przejął Twoje konto i straciłeś postępy w grze, masz problemy z odzyskaniem konta

Mini Quiz

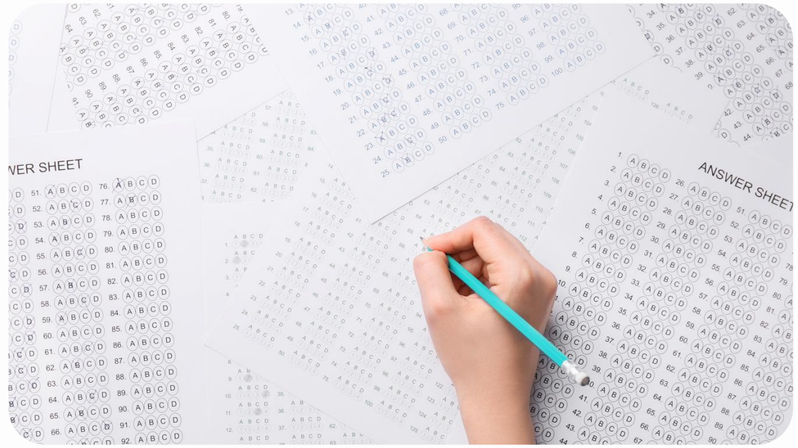
Sprawdź swoją podatność na ataki hackerów



Quiz składa się z siedmiu pytań



Wskaż najbardziej pasującą według Ciebie odpowiedź.



Zapisz swoje odpowiedzi.

CYBERSEC
EDUCHECK

1. Czy ktoś może chcieć Cię zaatakować?

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

CYBERSEC
EDUCHECK

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

CYBERSEC
EDUCHECK

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

CYBERSEC
EDUCHECK

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

CYBERSEC
EDUCHECK

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

CYBERSEC
EDUCHECK

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

CYBERSEC
EDUCHECK

7. Co robisz, gdy zobaczysz podejrzane działania na swoim koncie?

a Nic, może to błąd

b Natychmiast zmieniam hasło i sprawdzam swoje inne konta

c Czekam i obserwuję, czy sytuacja się powtórzy

WYNIK QUIZU

CYBERSEC
EDUCHECK

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.

CYBERSEC
EDUCHECK

Kim jest hacker?

Oczekiwania vs Rzeczywistość

Łamanie haseł

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090
Password hash: bcrypt

HIVE SYSTEMS

› Learn more about this at hivesystems.com/password

Link: https://www.hivesystems.com/password-table

CYBERSEC
EDUCHECK

Monitorowanie wycieków

Have I BeenPwned
https://haveibeenpwned.com/

Popularne narzędzie do sprawdzania, czy Twój e-mail lub hasło znalazło się w wyciekach danych.

DeHashed
https://www.dehashed.com/

Wyszukiwarka wycieków danych, która pozwala sprawdzić, czy Twoje dane zostały ujawnione. Oferuje także bardziej zaawansowane funkcje w płatnej wersji.

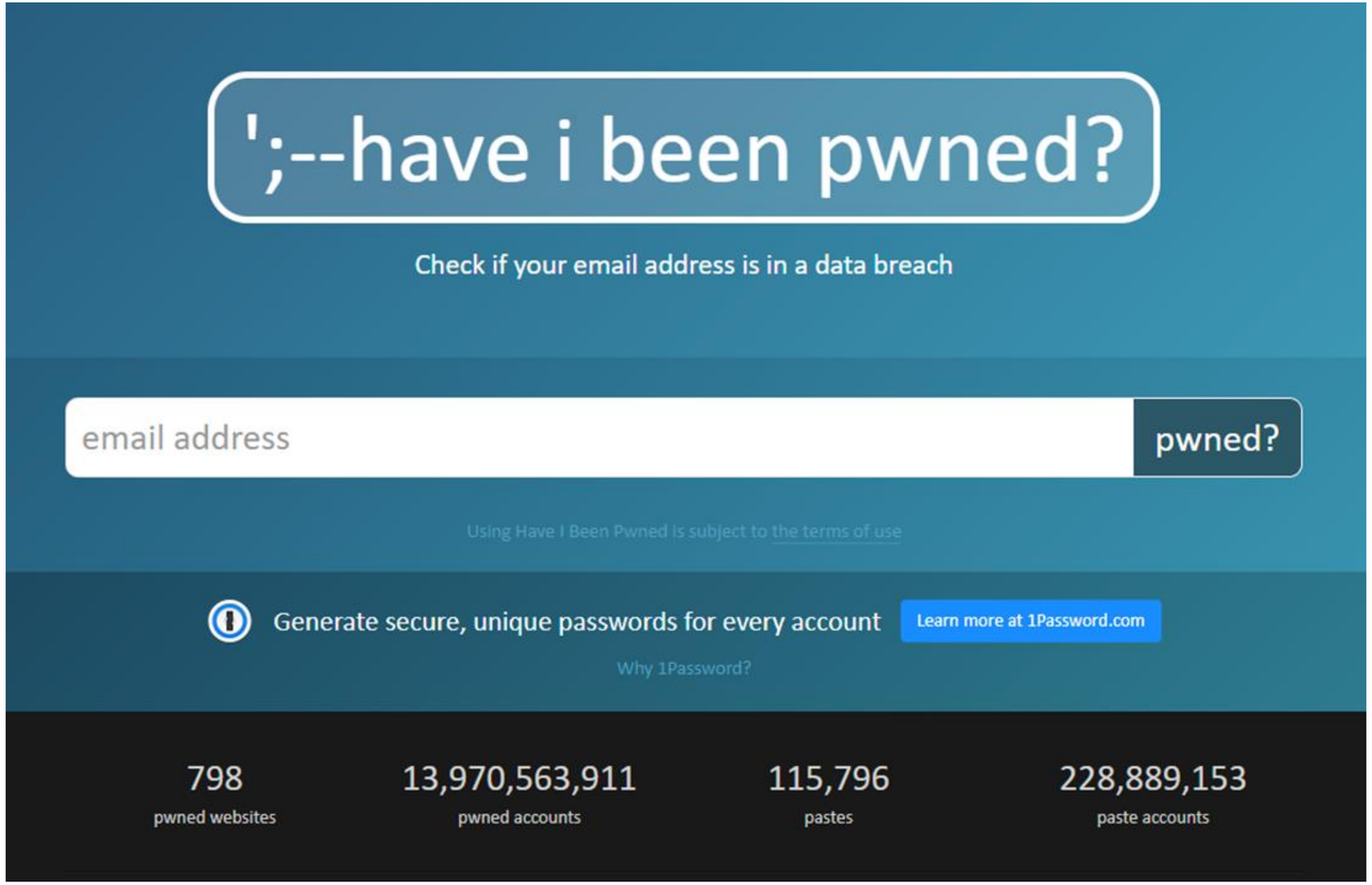
BreachAlarm

https://breachalarm.com/

Narzędzie do sprawdzania wycieków haseł i monitorowania, czy Twoje dane zostały naruszone.

Czy zostałem zhakowany?

CYBERSEC
EDUCHECK



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

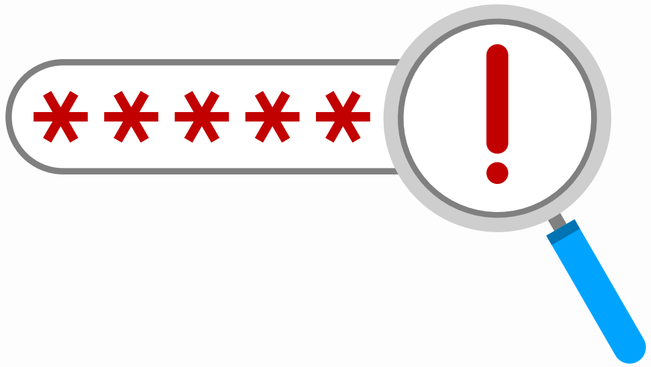
Sprawdzenie, gdzie jesteś zalogowany, pozwala wylogować potencjalnie niebezpieczne sesje.

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.



Otrzymujesz e-mail

Wyobraź sobie, że właśnie dowiadujesz się, że Twoje hasło zostało ujawnione, a Twoje konto zostało naruszone. Może to być przez atak hakerski, wyciek danych z jednego z serwisów, czy nawet przez przypadkowe ujawnienie hasła.

Co się dzieje, gdy dowiadujesz się o takim incydencie? Jak reagujesz? Co myślisz, co czujesz i co robisz?

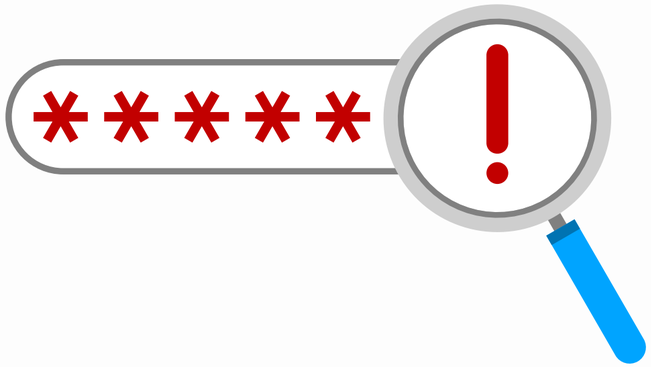
Praca w grupach

Podzielenie się historią

Co zrobić w przypadku wycieku hasła?

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
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.



Ransomware

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.

Ochrona przed Ransoware

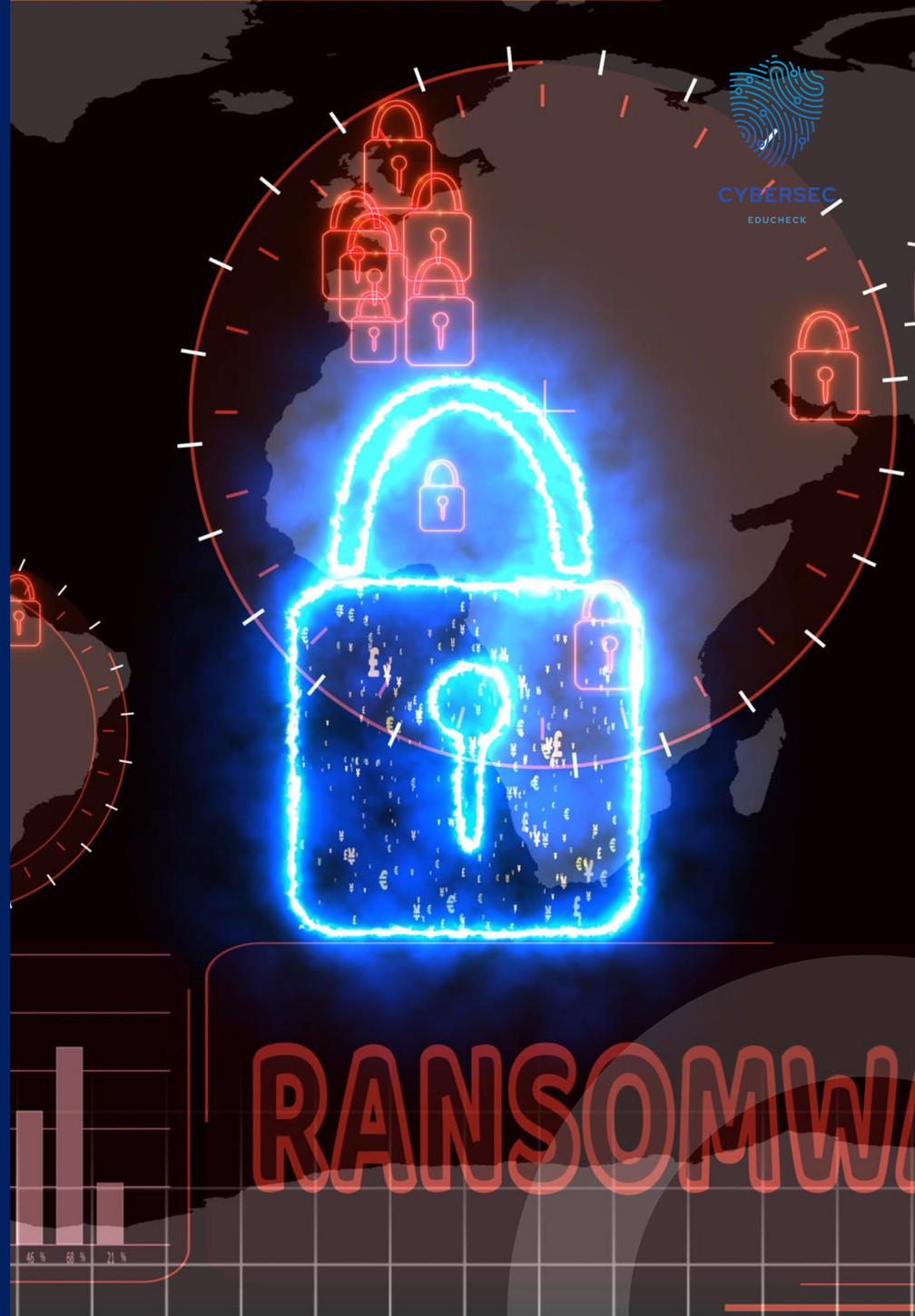
R**egularne kopie zapasowe:** Przechowuj ważne pliki na zewnętrznym dysku lub w chmurze. Jeśli komputer zostanie zainfekowany, możesz przywrócić pliki z kopii zapasowej.

Aktualizacje oprogramowania: Upewnij się, że system operacyjny i wszystkie programy są zawsze aktualne. Nowe aktualizacje często naprawiają luki bezpieczeństwa.

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.

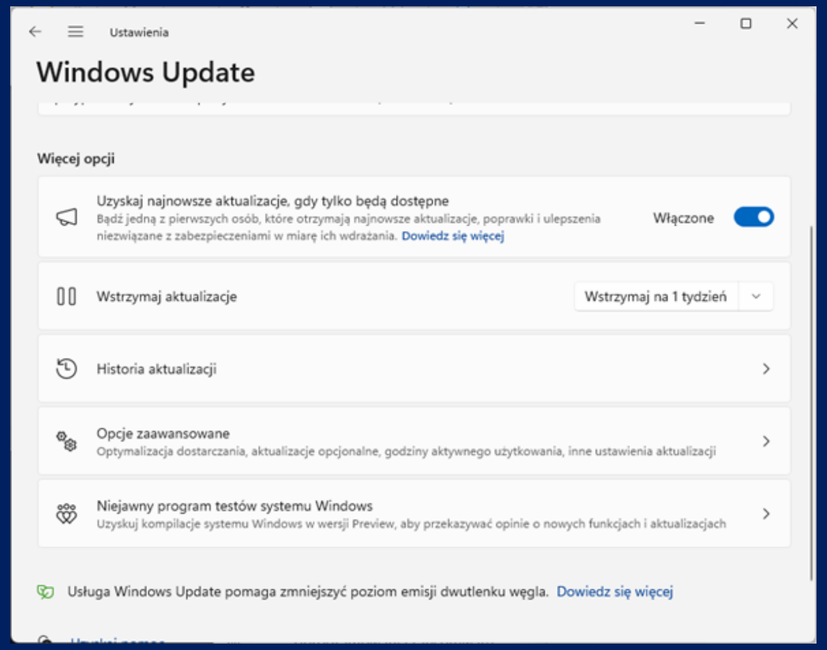
Edukacja: Naucz się rozpoznawać podejrzane wiadomości e-mail i komunikaty, które mogą zawierać złośliwe oprogramowanie.

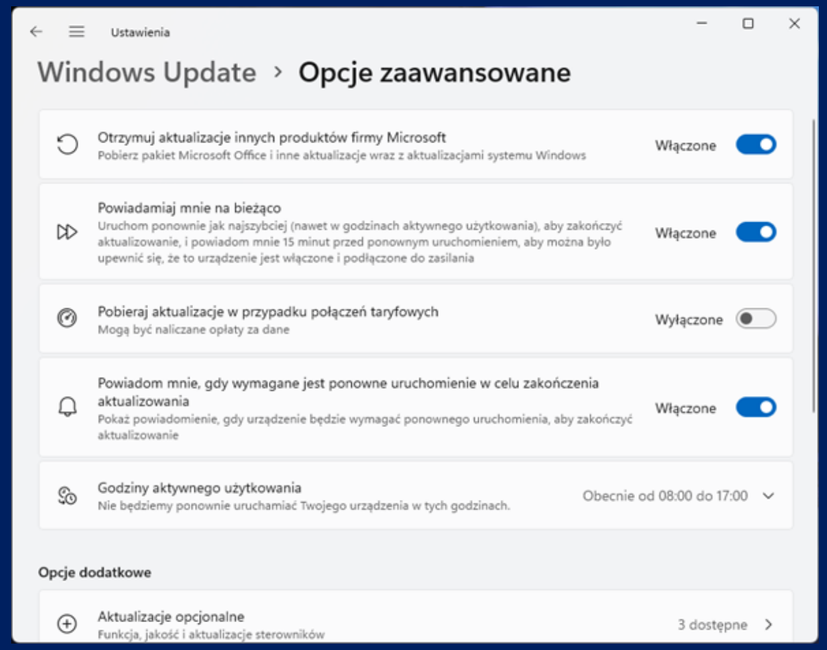


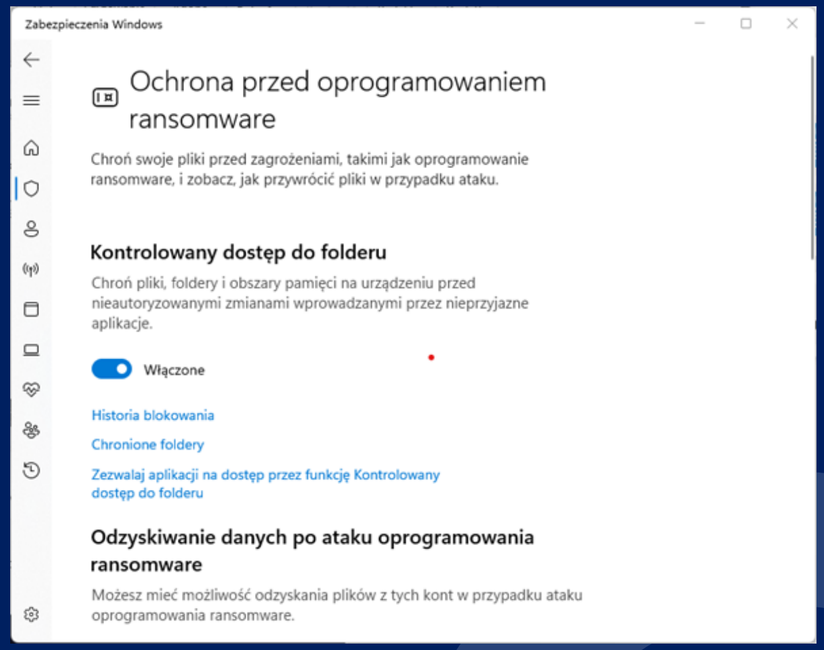
Ochrona przed Ransoware

CYBERSEC
EDUCHECK

Windows Update







Backup Danych

Robisz kopię ważnych plików i przechowujesz ją w bezpiecznym miejscu.

Jeśli coś pójdzie nie tak z komputerem lub telefonem, możesz użyć tej kopii, aby odzyskać swoje dane.

CYBERSEC
EDUCHECK

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.

ZADANIE DOMOWE: ZARZĄDZANIE INCYDENTAMI?

- **Sprawdź swoje adresy e-mail:**

Skorzystaj z serwisu Have I BeenPwned 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.
Obserwuj np. : CERT Polska (@CERT_Polska) / X oraz niebezpiecznik.pl

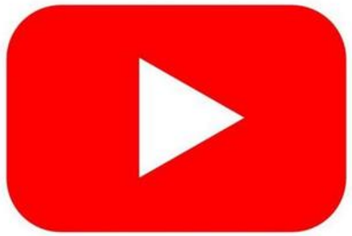
- **Zmień hasła:**

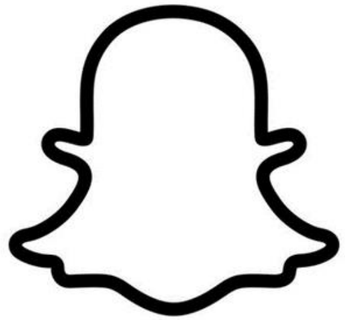
Zmień hasła do kont, które były zaangażowane w wycieki. Użyj silnych, losowych haseł. Możesz wykorzystać menedżer haseł, taki jak KeePassXC, aby wygenerować i przechować nowe hasła.

- Stwórz kopie zapasowe:

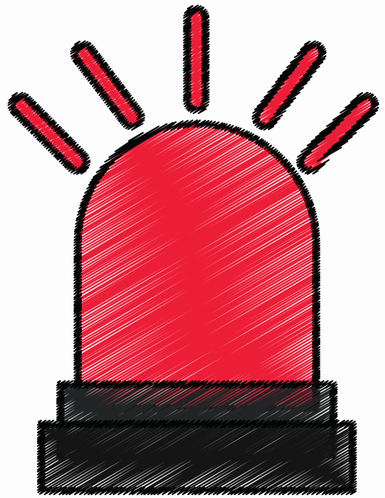
Wystarczy skopiowanie cennych plików na przenośny dysk USB i trzymanie go w bezpiecznym miejscu.

MEDIA SPOŁECZNOŚCIOWE





Zagrożenia



Ataki socjotechniczne i phishing:
Nie klikaj w podejrzane linki ani załączniki w wiadomościach. Uważaj na osoby, które próbują zdobyć Twoje dane osobowe pod pretekstem pomocy.

Nadmierne udostępnianie danych: Nie udostępniaj prywatnych informacji, takich jak adres zamieszkania, numer telefonu czy dane logowania. Zastanów się, zanim podzielisz się zdjęciami lub lokalizacją.

Zbieranie danych: Aplikacje mogą zbierać Twoje dane osobowe, nawet jeśli się tego nie spodziewasz. Sprawdzaj ustawienia prywatności.

Niemonitorowane konta: Regularnie sprawdzaj i aktualizuj swoje ustawienia prywatności. Zabezpiecz swoje konta silnymi hasłami i włącz autoryzację dwuetapową.

Fałszywe strony: Upewnij się, że odwiedzasz tylko zaufane strony internetowe i aplikacje. Sprawdzaj adres URL przed podaniem jakichkolwiek danych.

CYBERSEC
EDUCHECK

Świadome korzystanie, czasem zapominamy...

Przemyślane udostępnianie wiadomości: Zanim wyślesz wiadomość, zastanów się, czy jest bezpieczna i czy nie zawiera prywatnych danych. Unikaj udostępniania informacji, które mogą być wykorzystane do oszustw lub nękania.

Dbanie o bezpieczeństwo urządzeń: Zainstaluj oprogramowanie antywirusowe i regularnie je aktualizuj. Używaj silnych haseł i unikaj używania tych samych haseł na różnych kontach. Zabezpiecz swoje urządzenia hasłem, PIN-em lub odciskiem palca.
Weryfikowanie grona znajomych: Przyjmuj zaproszenia do znajomych tylko od osób, które naprawdę znasz. Regularnie przeglądaj swoją listę znajomych i usuwaj osoby, które nie są Ci znane.

Weryfikacja ustawień prywatności: Regularnie sprawdzaj i aktualizuj ustawienia prywatności na swoich profilach. Ustaw, kto może zobaczyć Twoje posty, zdjęcia i inne informacje. Włącz funkcje bezpieczeństwa, takie jak autoryzacja dwuetapowa, aby dodatkowo chronić swoje konta.

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