**Imię i nazwisko:** _____ **Data:** _____ **Wynik:** _____

# Zapobieganie kradzieży tożsamości i aktywa Przewodnik po bezpieczeństwie

Wycieki poświadczeń, MFA, monitoring dark webu, alerty zastrzeżenia kredytowego, socjotechnika

## OMÓWIENIE NAUKI: ZAPOBIEGANIE KRADZIEŻY TOŻSAMOŚCI

**CHRONIONY**
**SZYFROWANIE DANYCH**
Standard AES 256-bitowy

**ZGODNY**
**STANDARDY GLOBALNE**
Ramy prawne RODO (GDPR) i CCPA

**ZERO TRUST**
**POLITYKA DOSTĘPU**
Uwierzytelnianie wieloskładnikowe

**Witaj!** Ten pakiet ćwiczeń przeprowadzi cię przez zapobieganie kradzieży tożsamości i ograniczanie jej skutków. Poznasz wycieki poświadczeń, uwierzytelnianie wieloskładnikowe, monitorowanie dark webu, alerty o zastrzeżeniu kredytowym i obronę przed inżynierią społeczną.

### PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj cyberbezpieczeństwo i zapobieganie zagrożeniom.**
- [ ] **Część 5–7: Rozwiąż krzyżówkę i wykreślankę.**
- [ ] **Część 8–9: Rozwiąż studia przypadków i wyzwanie z szyfrem.**
- [ ] **Część 10: Przejrzyj strony z podstawowymi i zaawansowanymi najczęściej zadawanymi pytaniami.**
- [ ] **Część 11: Poznaj 10 ciekawych faktów z praktyki.**
- [ ] **Bonus: wyzwanie Myśl szybko.**

**Otwórz przewodnik VPN.com po cyberbezpieczeństwie**

URL: https://www.vpn.com/pl/cyberbezpieczenstwo/kradkiez-tozsamosci/

# Twoja ścieżka nauki: ochrona tożsamości

- Zrozum ryzyko ujawnienia danych logowania na forach dark webu.
- Wdróż uwierzytelnianie wieloskładnikowe (MFA) i alerty o zamrożeniu kredytu.
- Zaprojektuj firmowe zabezpieczenia przed ukierunkowanymi oszustwami opartymi na inżynierii społecznej.

## INSTRUKCJE DO PRZEWODNIKA O KRADZIEŻY TOŻSAMOŚCI

Odpowiedz na pytania testu wielokrotnego wyboru oraz pytania prawda/fałsz, uzupełnij zdania z lukami za pomocą banku wyrazów, dopasuj definicje i rozwiąż krzyżówkę oraz wykreślankę. Zastosuj swoją wiedzę z zakresu ochrony tożsamości. Zakończ zadaniem dodatkowym Myśl szybko.

## ZAPOBIEGANIE KRADZIEŻY TOŻSAMOŚCI I OCHRONA AKTYWÓW (WPROWADZENIE)

Kradzież tożsamości wykorzystuje wyciekłe dane logowania i słabe loginy do przejmowania kont osobistych i firmowych. Wdrożenie MFA, zamrożeń kredytowych, skanerów dark webu oraz ram SPF/DKIM/DMARC stanowi kluczową obronę przed cyfrowym podszywaniem się.

**PRZECZYTAJ UWAŻNIE KAŻDY PUNKT KONTROLNY I WYBIERZ LUB NAPISZ POPRAWNĄ ODPOWIEDŹ.**

## Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

**1** **1. Jaka jest główna metoda, której złodzieje tożsamości używają do kradzieży danych logowania?**

- A. Wysyłanie fałszywych alertów e-mail, które nakłaniają użytkowników do wpisania haseł na sfałszowanych portalach
- B. Słuchanie audycji radiowych w pobliżu firmowego biura użytkownika
- C. Defragmentacja lokalnego dysku pamięci serwera użytkownika
- D. Odłączanie zewnętrznych konfiguracji kopii zapasowych sieci

**2** **2. Które zabezpieczenie zapewnia najsilniejszą obronę przed wyciekami danych uwierzytelniających?**

- A. Uwierzytelnianie wieloskładnikowe z użyciem kluczy sprzętowych
- B. Tworzenie długich haseł w domyślnych formatach przeglądarki
- C. Zmienianie nazw użytkowników poczty e-mail co sześć miesięcy
- D. Usuwanie zapisanych historii przeglądarki śledzonej przez pliki cookie

**3** **3. Co reprezentuje zamrożenie kredytu?**

- A. Blokowanie raportów kredytowych, aby złodzieje nie mogli zaciągać nieautoryzowanych pożyczek
- B. Usuwanie z baz danych historii transakcji na rachunkach bankowych
- C. Wyłączanie magnetycznych czytników kart kredytowych w skanerach
- D. Szyfrowanie lokalnych dysków twardych bazy danych w spoczynku

**4** **4. Dlaczego monitorowanie dark webu jest przydatne?**

- A. Ostrzega użytkowników, jeśli ich wyciekłe dane uwierzytelniające pojawią się w nielegalnych bazach danych
- B. Uniemożliwia działanie aktywnego złośliwego oprogramowania w wirtualnych piaskownicach
- C. Przyspiesza routing przeglądarki w sieciach wirtualnych
- D. Blokuje próby dostępu przez wstrzykiwanie SQL do zaplecza bazy danych

**5** **5. Co oznacza inżynieria społeczna?**

- A. Manipulowanie ludźmi, aby dobrowolnie ujawnili poufne dane uwierzytelniające
- B. Skanowanie portów firmowych serwerów w poszukiwaniu aktywnych exploitów bezpieczeństwa
- C. Tworzenie kopii zapasowych plików baz danych systemu na dyskach twardych offline
- D. Kierowanie pakietów sieciowych przez trzy zaszyfrowane węzły onion

## Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

### 6 Pytanie 6

6. Kradzież tożsamości dotyczy wyłącznie internetowych kont cyfrowych, a nie fizycznej poczty.

- ○ Prawda
- ○ Fałsz

### 7 Pytanie 7

7. Wymuszenie MFA na wszystkich kontach osobistych blokuje większość ataków botów typu credential stuffing.

- ○ Prawda
- ○ Fałsz

### 8 Pytanie 8

8. Zastrzeżenie kredytowe blokuje sprawdzanie zdolności kredytowej, ale uniemożliwia dostęp do własnego konta bankowego.

- ○ Prawda
- ○ Fałsz

### 9 Pytanie 9

9. Menedżery haseł chronią użytkowników przed phishingiem, odmawiając automatycznego wypełniania haseł na sfałszowanych domenach.

- ○ Prawda
- ○ Fałsz

### 10 Pytanie 10

10. E-maile phishingowe często używają ponaglającego języka, aby wywołać emocjonalne, szybkie reakcje.

- ○ Prawda
- ○ Fałsz

# Punkt kontrolny 3: Wstawianie kluczowych terminów

Przeczytaj każde poniższe zdanie i uzupełnij lukę poprawnym terminem z banku słów.

1. Złodzieje tożsamości celują w osobiste hasła i _____ użytkowników.

2. Powiadamianie użytkowników o naruszeniach baz danych pozwala zidentyfikować prywatne _____ danych kont.

3. Wymaganie tymczasowego kodu przy logowaniu nazywa się _____ .

4. Skanowanie forów hakerskich w poszukiwaniu skradzionych danych to _____ dark webu.

5. Aby zablokować nieautoryzowane sprawdzanie kredytu, potrzebne jest _____ kredytowe.

6. Dzięki szkoleniu pracowników z rozpoznawania phishingu powstaje aktywna _____ w zakresie bezpieczeństwa.

**BANK SŁÓW**

MFA MONITORING OBRONA PHISHING POŚWIADCZENIA SPOOFING WYCIEKI ZASTRZEŻENIE

**Wpisz tutaj swoje odpowiedzi:**

1. 
2. 
3. 
4. 
5. 
6. 

# Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

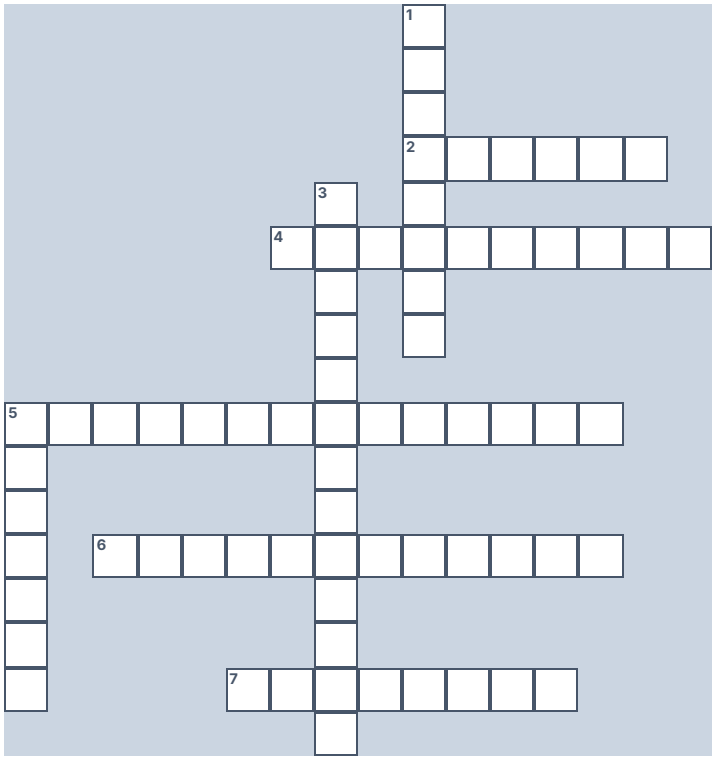
## DOPASOWYWANIE DEFINICJI

Dopasuj każde pojęcie po lewej stronie do jego poprawnej definicji po prawej, wpisując odpowiednią literę (A-H) w edytowalne pole.

| | | | |
|---|---|---|---|
| ☐ | 1. POŚWIADCZENIA | A | Dodatkowy etap weryfikacji (taki jak klucze sprzętowe) chroniący logowanie do konta. |
| ☐ | 2. WYCIEKI | B | Tworzenie fałszywej strony internetowej lub e-maila naśladujących legalną organizację. |
| ☐ | 3. MFA | C | Ograniczanie dostępu do akt kredytowych, aby zapobiec fałszywym wnioskom o pożyczkę. |
| ☐ | 4. MONITOROWANIE | D | Nieautoryzowane ujawnienie prywatnych baz danych zawierających osobiste rekordy użytkowników. |
| ☐ | 5. ZAMROŻENIE | E | Szkolenia i środki techniczne służące ochronie przed kradzieżą tożsamości. |
| ☐ | 6. OBRONA | F | Wysyłanie fałszywych wiadomości, aby nakłonić użytkowników do ujawnienia danych logowania. |
| ☐ | 7. SPOOFING | G | Skanowanie forów internetowych i kanałów hakerskich w poszukiwaniu skradzionych danych firmowych. |
| ☐ | 8. PHISHING | H | Nazwy użytkowników, hasła i prywatne tokeny używane do uwierzytelniania tożsamości cyfrowych. |

# Punkt kontrolny 5: Krzyżówka

Rozwiąż krzyżówkę, wpisując litery w aktywne białe pola. Numery odpowiadają wskazówkom poniżej.




## POZIOMO

**2. Szkolenia i kontrole techniczne stosowane w celu ochrony przed kradzieżą tożsamości. (6)**

**4. Skanowanie forów internetowych i kanałów hakerów w poszukiwaniu skradzionych danych firmowych. (10)**

**5. Dodatkowy etap weryfikacji (na przykład kluczami sprzętowymi) chroniący logowanie do kont. (14)**

**6. Ograniczenie dostępu do akt kredytowych, aby zapobiec oszukańczym wnioskom o pożyczkę. (12)**

**7. Wysyłanie oszukańczych wiadomości, aby nakłonić użytkowników do ujawnienia poświadczeń. (8)**

## PIONOWO

**1. Tworzenie fałszywej strony internetowej lub e-maila naśladujących prawdziwą organizację. (8)**

**3. Nazwy użytkownika, hasła i prywatne tokeny służące do uwierzytelniania tożsamości cyfrowych. (13)**

**5. Nieautoryzowane ujawnienie prywatnych baz danych zawierających osobiste dane użytkowników. (7)**

# Punkt kontrolny 5, wariant alternatywny: Dostępne wskazówki do krzyżówki

Użytkownicy czytników ekranu i klawiatury mogą wpisywać odpowiedzi do krzyżówki bezpośrednio w polach tekstowych poniżej.

## POZIOMO

**2 poziomo: Szkolenia i kontrole techniczne stosowane w celu ochrony przed kradzieżą tożsamości. (6 liter):**

**4 poziomo: Skanowanie forów internetowych i kanałów hakerów w poszukiwaniu skradzionych danych firmowych. (10 liter):**

**5 poziomo: Dodatkowy etap weryfikacji (na przykład kluczami sprzętowymi) chroniący logowanie do kont. (14 liter):**

**6 poziomo: Ograniczenie dostępu do akt kredytowych, aby zapobiec oszukańczym wnioskom o pożyczkę. (12 liter):**

**7 poziomo: Wysyłanie oszukańczych wiadomości, aby nakłonić użytkowników do ujawnienia poświadczeń. (8 liter):**

## PIONOWO

**1 pionowo: Tworzenie fałszywej strony internetowej lub e-maila naśladujących prawdziwą organizację. (8 liter):**

**3 pionowo: Nazwy użytkownika, hasła i prywatne tokeny służące do uwierzytelniania tożsamości cyfrowych. (13 liter):**

**5 pionowo: Nieautoryzowane ujawnienie prywatnych baz danych zawierających osobiste dane użytkowników. (7 liter):**

## Punkt kontrolny 6: Ukryte słowa w wykreślance

Znajdź w poniższej siatce 8 kluczowych terminów słownictwa. Wyrazy mogą biec poziomo, pionowo lub po przekątnej.

A L Ś S W Q Ź E H E S C A Ł P
I C G N I R O T I N O M Ż W P
N M L W O B R O N A S U Y H Ą
E S X K M M G H N H R C I Ę L
Z Ś Ł R X H B U Ę Z I S O Ź X
C S G T Y A Ó V Ń E H Ń Ź O H
D P T H Ó V U O K I U T K A E
A Ó N L Ą Ń V I N F F P Q Y Ź
I J K V K Ź X G Z Ó K I Ż I J
W N A E G N I F O O P S I Ą Ś
Ś W E R Y F I K A C J A M F A
O A K Ę X E K Ż K D L Q N K A
P Ę Z A S T R Z E Ż E N I E O
K Ń Ć N C Ć G I Ą Ą Ó R Ł P W
T I Ź Ę Ź S G Y X H Ę R T Ń U

**LISTA SŁÓW**

POŚWIADCZENIA WYCIEKI WERYFIKACJAMFA MONITORING ZASTRZEŻENIE
OBRONA SPOOFING PHISHING

# Punkt kontrolny 6, wariant alternatywny: Dostępne dopasowywanie słownictwa

Dopasuj każde z 8 pojęć z wykreślanki do jego poprawnej definicji, wpisując literę (A-H) w puste pole.

| TERMINY ZE SŁOWNICZKA | DEFINICJE I POLA DOPASOWANIA |
|---|---|
| A. POŚWIADCZENIA | _____ 1. Wysyłanie oszukańczych wiadomości, aby nakłonić użytkowników do ujawnienia poświadczeń. |
| B. WYCIEKI | _____ 2. Nazwy użytkownika, hasła i prywatne tokeny służące do uwierzytelniania tożsamości cyfrowych. |
| C. WERYFIKACJAMFA | _____ 3. Tworzenie fałszywej strony internetowej lub e-maila naśladujących prawdziwą organizację. |
| D. MONITORING | _____ 4. Szkolenia i kontrole techniczne stosowane w celu ochrony przed kradzieżą tożsamości. |
| E. ZASTRZEŻENIE | _____ 5. Skanowanie forów internetowych i kanałów hakerów w poszukiwaniu skradzionych danych firmowych. |
| F. OBRONA | _____ 6. Ograniczenie dostępu do akt kredytowych, aby zapobiec oszukańczym wnioskom o pożyczkę. |
| G. SPOOFING | _____ 7. Nieautoryzowane ujawnienie prywatnych baz danych zawierających osobiste dane użytkowników. |
| H. PHISHING | _____ 8. Dodatkowy etap weryfikacji (na przykład kluczami sprzętowymi) chroniący logowanie do kont. |

## Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z cyberbezpieczeństwem. Wpisz odpowiedzi w przygotowanych polach.

1. DŚZIAOCEPNA IW
2. FEIRKFWMAA JACY
3. ZAŻEIESZERN T
4. ONGIFSPO
5. EIICWKY
6. NTIRIMOOGN
7. NOOARB
8. SHHGPNII

# Zadanie dodatkowe: Myśl szybko

3 ODPOWIEDZI W KAŻDEJ KATEGORII. WYGRYWA OSOBA, KTÓRA PIERWSZA WYPEŁNI LISTĘ.

| | | | | |
|---|---|---|---|---|
| 1 | Rzeczy do zrobienia, jeśli twoja tożsamość zostanie skradziona | | | |
| 2 | Rzeczy, których nie należy udostępniać w mediach społecznościowych | | | |
| 3 | Rzeczy, z których robisz kopie zapasowe | | | |
| 4 | Karty lub dokumenty tożsamości w twoim portfelu | | | |
| 5 | Dokumenty, które powinieneś chronić | | | |
| 6 | Rzeczy do zrobienia po wycieku danych | | | |
| 7 | Powody, dla których warto aktualizować oprogramowanie | | | |
| 8 | Informacje, których chce złodziej tożsamości | | | |
| 9 | Urządzenia, które można zhakować | | | |
| 10 | Miejsca, z których mogą wyciec twoje dane | | | |
| 11 | Bezpieczne nawyki, które możesz zacząć już dziś | | | |
| 12 | Oznaki, że komputer jest zainfekowany | | | |
| 13 | Sposoby na udowodnienie, kim jesteś | | | |
| 14 | Oznaki kradzieży tożsamości | | | |
| 15 | Sygnały ostrzegawcze w e-mailu | | | |

# Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

Zastosuj poznane pojęcia, aby rozwiązać poniższe scenariusze z życia wzięte.

## STUDIUM PRZYPADKU 1: OCHRONA PRZED PODSZYWANIEM SIĘ POD KADRĘ KIEROWNICZĄ

👨‍💻

**Scenariusz:** Znany członek kadry zarządzającej wyższego szczebla stał się celem domen z literówkami (typosquatting) naśladujących jego prywatny adres e-mail w celu oszukiwania klientów. Zaprojektuj plan ochrony marki.

**Pytanie do dyskusji:** Przeanalizuj ryzyka podszywania się pod markę i opisz szczegółowo SPF/DKIM/DMARC oraz mechanizmy uwierzytelniania.

## STUDIUM PRZYPADKU 2: UJAWNIENIE FIRMOWYCH POŚWIADCZEŃ W DARK WEBIE

👨‍💻

**Scenariusz:** Zrzut bazy danych z dark webu zawiera kilkaset firmowych danych uwierzytelniających należących do administratorów systemów przedsiębiorstwa. Zaprojektuj strategię ograniczania skutków.

**Pytanie do dyskusji:** Opisz proces czyszczenia danych uwierzytelniających i zaplanuj wdrożenie menedżera haseł.

# Punkt kontrolny 9: Odszyfruj szyfr

Specjalista ds. cyberbezpieczeństwa chroni zasoby sieciowe przed cyberprzestępcami. Użyj poniższego klucza liter i liczb, aby odszyfrować wiadomość, wpisując pasujące litery w puste miejsca.

**KLUCZ SZYFROWANIA LITERA-LICZBA**

A=1 Ą=2 B=3 C=4 Ć=5 D=6 E=7 Ę=8 F=9 G=10 H=11 I=12
J=13 K=14 L=15 Ł=16 M=17 N=18 Ń=19 O=20 Ó=21 P=22 Q=23 R=24
S=25 Ś=26 T=27 U=28 V=29 W=30 X=31 Y=32 Z=33 Ź=34 Ż=35

| 4 | 11 | 24 | 20 | 19 | | 27 | 20 | 35 | 25 | 1 | 17 | 20 | 26 | 5 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | |

| 4 | 32 | 9 | 24 | 20 | 30 | 2 | | 33 | 1 | | 22 | 20 | 17 | 20 | 4 | 2 | | 17 | 9 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | |

**Odszyfrowana wiadomość:**

WSKAZÓWKA: KAŻDA LICZBA OZNACZA POZYCJĘ TEJ LITERY W ALFABECIE (NP. 1 = A, 2 = B, 35 = Ż).

# Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część A)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

### Q1: Czym jest kradzież tożsamości?

Przestępstwo, w którym atakujący kradnie dane osobowe (takie jak hasła lub numery SSN), aby podszywać się pod inną osobę w celu osiągnięcia korzyści finansowej.

### Q2: Jaka jest najczęstsza przyczyna kradzieży tożsamości?

Phishing to jeden z głównych sposobów, w jaki złodzieje zdobywają hasła, wabiąc użytkowników na fałszywe, sfałszowane strony internetowe.

### Q3: Jak uwierzytelnianie wieloskładnikowe (MFA) chroni tożsamość?

MFA wymaga dodatkowego potwierdzenia (np. klucza sprzętowego) przy logowaniu, blokując atakujących nawet wtedy, gdy ukradną twoje hasło.

### Q4: Czym jest zamrożenie kredytu (credit freeze)?

Bezpłatna usługa blokująca udostępnianie Twojego pliku kredytowego przez biura informacji kredytowej, co uniemożliwia złodziejom zaciąganie nowych pożyczek na Twoje nazwisko. [2]

### Q5: Czym jest monitorowanie dark webu?

Oprogramowanie sprawdzające fora hakerskie pod kątem wyciekłych adresów e-mail, haseł i danych osobowych, które powiadamia Cię, jeśli Twoje dane zostały ujawnione.

# Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część B)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

### Q6: Co oznacza credential stuffing?

Zautomatyzowane boty testujące wycieknięte listy haseł w setkach witryn, aby przejąć aktywne konta.

### Q7: Dlaczego spoofing e-maili jest niebezpieczny?

Pozwala atakującym podszywać się pod nazwę nadawcy w wiadomościach e-mail, przez co wiadomości phishingowe wyglądają, jakby pochodziły od zaufanych współpracowników.

### Q8: Jak menedżery haseł powstrzymują kradzież tożsamości?

Przechowują złożone, unikalne hasła do każdego konta i odmawiają automatycznego wypełniania danych logowania na fałszywych domenach phishingowych.

### Q9: Czym jest spear phishing?

Bardzo ukierunkowany atak phishingowy dostosowany do imienia i danych ofiary, aby zwiększyć szansę oszustwa.

### Q10: Czym alert kredytowy różni się od zamrożenia?

Alert informuje kredytodawców, aby zweryfikowali Twoją tożsamość przed otwarciem kont, a zastrzeżenie całkowicie blokuje dostęp do Twojego pliku kredytowego. [2]

# Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część C)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

### Q1: Jak SIM swapping prowadzi do kradzieży tożsamości?

Atakujący przekonują pracowników operatora do przeniesienia numeru telefonu ofiary na nową kartę SIM, przejmując w ten sposób kody 2FA wysyłane SMS-em.

### Q2: Jaką rolę odgrywa DMARC w zapobieganiu kradzieży tożsamości?

DMARC pozwala właścicielom domen blokować fałszywe wiadomości e-mail, zanim trafią do skrzynek odbiorczych, co powstrzymuje podszywanie się pod domeny firmowe.

### Q3: Dlaczego kradzież tożsamości syntetycznej jest trudna do wykrycia?

Złodzieje łączą prawdziwe numery SSN z fałszywymi imionami i nazwiskami oraz datami urodzenia, aby budować zupełnie nowe profile kredytowe, omijając podstawowe alerty o oszustwach.

### Q4: Jak brokerzy danych wykorzystują tożsamości osobiste?

Pośrednicy danych gromadzą rejestry publiczne, zachowania w sieci i historie zakupów, aby tworzyć dossier profili, które mogą wyciec lub zostać sprzedane.

### Q5: Dlaczego MFA oparte na SMS-ach uważa się za podatne na ataki?

Ruch SMS jest podatny na przechwycenie, phishing i exploity zamiany karty SIM na poziomie operatora.

# Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część D)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

### Q6: Czym jest blokada pliku kredytowego (credit file lock)?

Usługa komercyjna podobna do zastrzeżenia kredytowego, pozwalająca użytkownikom natychmiast odblokowywać lub blokować swój plik kredytowy za pomocą aplikacji mobilnej.

### Q7: Jak wycieki danych korporacyjnych napędzają kradzież tożsamości?

Wycieki baz danych ujawniają miliony haseł zapisanych jawnym tekstem, dając złodziejom surowe dane potrzebne do przeprowadzenia ukierunkowanych oszustw tożsamościowych.

### Q8: Jakie ryzyko wiąże się z nadmiernym dzieleniem się informacjami w mediach społecznościowych?

Publiczne podawanie imion zwierząt, miejsc urodzenia i nazwisk panieńskich matek daje złodziejom odpowiedzi na typowe pytania służące do odzyskiwania konta.

### Q9: Jak logowanie biometryczne chroni profile tożsamości?

Biometria wiąże logowanie z cechami, takimi jak odciski palców lub twarze; przechowywana na urządzeniu jest trudna do ukradzenia, ale przechowywane dane biometryczne mogą wyciec.

### Q10: Jak reguła Red Flags Rule zwalcza kradzież tożsamości?

Regulacja federalna wymagająca od instytucji finansowych opracowania pisemnych programów wykrywania oznak kradzieży tożsamości i reagowania na nie.

# Część 11: 10 faktów o cyberbezpieczeństwie z praktyki i spostrzeżeń

Przejrzyj prawdziwe fakty dotyczące naruszeń bezpieczeństwa, mechanizmów obronnych i standardów zgodności.

**1. WGLĄD W BEZPIECZEŃSTWO**

IdentityTheft.gov, prowadzony przez FTC, pozwala ofiarom w USA zgłaszać kradzież tożsamości i otrzymać osobisty plan odzyskiwania. [1]

**2. WGLĄD W BEZPIECZEŃSTWO**

Sprzętowe klucze bezpieczeństwa to uwierzytelnianie wieloskładnikowe odporne na phishing, czyli najsilniejszy rodzaj MFA, do którego zachęca CISA. [4]

**3. WGLĄD W BEZPIECZEŃSTWO**

Przejęte hasła są częstym punktem wejścia w naruszeniach danych i napędzają późniejsze oszustwa tożsamościowe.

**4. WGLĄD W BEZPIECZEŃSTWO**

Zastrzeżenie kredytowe jest bezpłatne na mocy prawa federalnego i uniemożliwia kredytodawcom sprawdzanie plików kredytowych do czasu jego odblokowania. [2]

**5. WGLĄD W BEZPIECZEŃSTWO**

DMARC pozwala właścicielom domen poinstruować serwery pocztowe, aby odrzucały lub poddawały kwarantannie sfałszowane wiadomości, które nie przechodzą kontroli. [7]

**6. WGLĄD W BEZPIECZEŃSTWO**

Zamiana karty SIM (SIM swapping) pozwala hakerom ominąć uwierzytelnianie dwuskładnikowe oparte na SMS w portalach bankowych.

**7. WGLĄD W BEZPIECZEŃSTWO**

Oszustwo z użyciem tożsamości syntetycznej miesza prawdziwe i fałszywe dane, przez co pożyczkodawcom trudno je wykryć.

**8. WGLĄD W BEZPIECZEŃSTWO**

Wiele osób używa tego samego hasła do różnych kont online, więc jeden wyciek może ujawnić kilka z nich.

**9. WGLĄD W BEZPIECZEŃSTWO**

Brokerzy danych gromadzą szczegółowe dossier dotyczące dużej liczby konsumentów, co stwarza skoncentrowane ryzyko dla prywatności.

**10. WGLĄD W BEZPIECZEŃSTWO**

Odzyskiwanie po kradzieży tożsamości może zająć miesiące pracy, takiej jak kwestionowanie obciążeń i poprawianie raportów kredytowych.

# Źródła i odnośniki techniczne

Przewodnik do nauki i interaktywne łamigłówki powstały na podstawie globalnych standardów NIST, OWASP i zgodności z przepisami o ochronie prywatności danych.

## PUBLIKACJE NAUKOWE I BRANŻOWE

[1] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

## Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

### 1 Pytanie 1

**Poprawna odpowiedź: A**

#### UWAGA DLA NAUCZYCIELA

Jaka jest główna metoda, której złodzieje tożsamości używają do kradzieży danych logowania? → Wysyłanie fałszywych alertów e-mail, które nakłaniają użytkowników do wpisania haseł na sfałszowanych portalach

### 2 Pytanie 2

**Poprawna odpowiedź: A**

#### UWAGA DLA NAUCZYCIELA

Które zabezpieczenie zapewnia najsilniejszą obronę przed wyciekami danych uwierzytelniających? → Uwierzytelnianie wieloskładnikowe z użyciem kluczy sprzętowych

### 3 Pytanie 3

**Poprawna odpowiedź: A**

#### UWAGA DLA NAUCZYCIELA

Co reprezentuje zamrożenie kredytu? → Blokowanie raportów kredytowych, aby złodzieje nie mogli zaciągać nieautoryzowanych pożyczek

### 4 Pytanie 4

**Poprawna odpowiedź: A**

#### UWAGA DLA NAUCZYCIELA

Dlaczego monitorowanie dark webu jest przydatne? → Ostrzega użytkowników, jeśli ich wyciekłe dane uwierzytelniające pojawią się w nielegalnych bazach danych

### 5 Pytanie 5

**Poprawna odpowiedź: A**

#### UWAGA DLA NAUCZYCIELA

Co oznacza inżynieria społeczna? → Manipulowanie ludźmi, aby dobrowolnie ujawnili poufne dane uwierzytelniające

## Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

### 6 Pytanie 6

**Poprawna odpowiedź: Fałsz**

#### UWAGA DLA NAUCZYCIELA

Kradzież tożsamości może się też zaczynać offline, na przykład od skradzionej poczty lub dokumentów.

### 7 Pytanie 7

**Poprawna odpowiedź: Prawda**

#### UWAGA DLA NAUCZYCIELA

Wymuszenie MFA na wszystkich kontach osobistych blokuje większość ataków botów typu credential stuffing.

### 8 Pytanie 8

**Poprawna odpowiedź: Fałsz**

#### UWAGA DLA NAUCZYCIELA

Zastrzeżenie kredytu (credit freeze) zatrzymuje nowe sprawdzenia kredytowe, ale nie wpływa na twoje istniejące konta.

### 9 Pytanie 9

**Poprawna odpowiedź: Prawda**

#### UWAGA DLA NAUCZYCIELA

Menedżery haseł chronią użytkowników przed phishingiem, odmawiając automatycznego wypełniania haseł na sfałszowanych domenach.

### 10 Pytanie 10

**Poprawna odpowiedź: Prawda**

#### UWAGA DLA NAUCZYCIELA

E-maile phishingowe często używają ponaglającego języka, aby wywołać emocjonalne, szybkie reakcje.

# Klucze słownictwa i kryteria oceny

**Schemat oceniania dla nauczyciela: Przyznaj 1 punkt za każde poprawne dopasowanie (łącznie 8 pkt) i pojęcie w kontekście (łącznie 6 pkt).**

## PUNKT KONTROLNY 4: KLUCZ – DOPASOWYWANIE POJĘĆ

| | | | |
|---|---|---|---|
| H 1. POŚWIADCZENIA | D 2. WYCIEKI | A 3. MFA | G 4. MONITOROWANIE |
| C 5. ZAMROŻENIE | E 6. OBRONA | B 7. SPOOFING | F 8. PHISHING |

## PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

| | | | |
|---|---|---|---|
| 1 POŚWIADCZENIA | 2 WYCIEKI | 3 MFA | 4 MONITORING |
| 5 ZASTRZEŻENIE | 6 OBRONA | | |

## PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

| | | | |
|---|---|---|---|
| 1 H – PHISHING | 2 A – POŚWIADCZENIA | 3 G – SPOOFING | 4 F – OBRONA |
| 5 D – MONITORING | 6 E – ZASTRZEŻENIE | 7 B – WYCIEKI | 8 C – WERYFIKACJAMFA |

## UWAGI DO DYSKUSJI DLA NAUCZYCIELI

**Kluczowe pojęcia:**
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia POŚWIADCZENIA, WYCIEKI i MFA oraz podać przykład każdego z nich.

**Studia przypadków:**
Poproś uczniów, aby uzasadniali swoje zalecenia faktami z karty pracy, a nie przypuszczeniami.

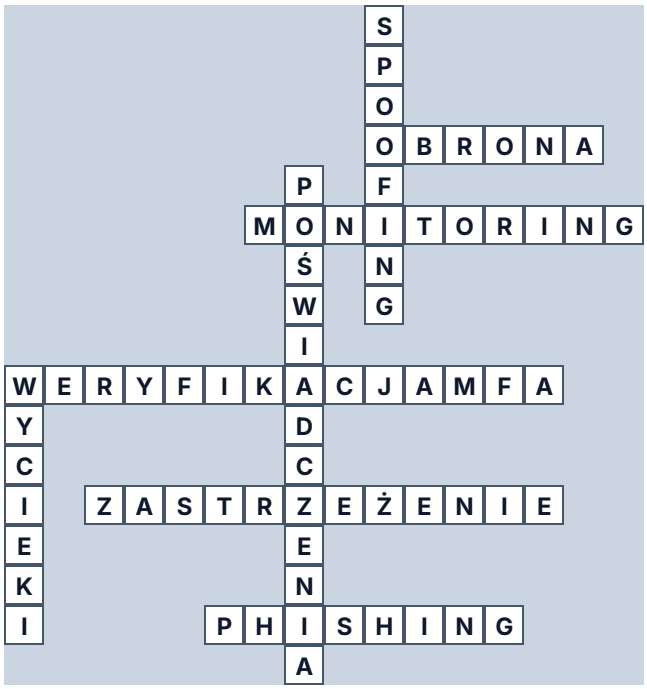
**Ocena źródeł:**
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

# Klucze do łamigłówek i uwagi dla nauczyciela

## ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | L | Ś | S | W | Q | Ź | E | H | E | S | C | A | Ł | P |
| I | C | G | N | I | R | O | T | I | N | O | M | Ż | W | P |
| N | M | L | W | O | B | R | O | N | A | S | U | Y | H | Ą |
| E | S | X | K | M | M | G | H | N | H | R | C | I | Ę | L |
| Z | Ś | Ł | R | X | H | B | U | Ę | Z | I | S | O | Ź | X |
| C | S | G | T | Y | A | Ó | V | Ń | E | H | Ń | Ź | O | H |
| D | P | T | H | Ó | V | U | O | K | I | U | T | K | A | E |
| A | Ó | N | L | Ą | Ń | V | I | N | F | F | P | Q | Y | Ź |
| I | J | K | V | K | Ź | X | G | Z | Ó | K | I | Ż | I | J |
| W | N | A | E | G | N | I | F | O | O | P | S | I | Ą | Ś |
| Ś | W | E | R | Y | F | I | K | A | C | J | A | M | F | A |
| O | A | K | Ę | X | E | K | Ż | K | D | L | Q | N | K | A |
| P | Ę | Z | A | S | T | R | Z | E | Ż | E | N | I | E | O |
| K | Ń | Ć | N | C | Ć | G | I | Ą | Ą | Ó | R | Ł | P | W |
| T | I | Ź | Ę | Ź | S | G | Y | X | H | Ę | R | T | Ń | U |

## ROZWIĄZANIE KRZYŻÓWKI




## PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

### POZIOMO

**2 poziomo: OBRONA** Szkolenia i kontrole techniczne stosowane w celu ochrony przed kradzieżą tożsamości. (6 liter)

**4 poziomo: MONITORING** Skanowanie forów internetowych i kanałów hakerów w poszukiwaniu skradzionych danych firmowych. (10 liter)

**5 poziomo: WERYFIKACJAMFA** Dodatkowy etap weryfikacji (na przykład kluczami sprzętowymi) chroniący logowanie do kont. (14 liter)

**6 poziomo: ZASTRZEŻENIE** Ograniczenie dostępu do akt kredytowych, aby zapobiec oszukańczym wnioskom o pożyczkę. (12 liter)

**7 poziomo: PHISHING** Wysyłanie oszukańczych wiadomości, aby nakłonić użytkowników do ujawnienia poświadczeń. (8 liter)

### PIONOWO

**1 pionowo: SPOOFING** Tworzenie fałszywej strony internetowej lub e-maila naśladujących prawdziwą organizację. (8 liter)

**3 pionowo: POŚWIADCZENIA** Nazwy użytkownika, hasła i prywatne tokeny służące do uwierzytelniania tożsamości cyfrowych. (13 liter)

**5 pionowo: WYCIEKI** Nieautoryzowane ujawnienie prywatnych baz danych zawierających osobiste dane użytkowników. (7 liter)

# Klucz do słów rozsypanych i rozwiązania szyfru

Klucz odpowiedzi do ćwiczenia z rozszyfrowywania słownictwa i Tajemniczego wyzwania szyfrowego.

## KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. DŚZIAOCEPNAIW — **POŚWIADCZENIA**
2. FEIRKFWMAAJACY — **WERYFIKACJAMFA**
3. ZAŻEIESZERNT — **ZASTRZEŻENIE**
4. ONGIFSPO — **SPOOFING**
5. EIICWKY — **WYCIEKI**
6. NTIRIMOOGN — **MONITORING**
7. NOOARB — **OBRONA**
8. SHHGPNII — **PHISHING**

## KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

**"CHROŃ TOŻSAMOŚĆ CYFROWĄ ZA POMOCĄ MFA"**

# Klucz odpowiedzi do studiów przypadków

## A Studium przypadku 1: Ochrona przed podszywaniem się pod kadrę kierowniczą

Rozwiązanie dla nauczyciela

### WYTYCZNE OCENIANIA

**Odpowiedzi uczniów powinny obejmować następujące punkty:**

- Analiza scenariusza: Wysoko postawiony członek kadry kierowniczej najwyższego szczebla stał się celem domen typosquattingowych naśladujących jego osobisty adres e-mail w celu oszukiwania klientów. Zaprojektuj plan ochrony marki.
- Zalecana strategia i rozwiązanie: Zarejestruj wszystkie typowe warianty pisowni imienia i nazwiska członka zarządu. Wdróż protokoły uwierzytelniania poczty (DMARC, DKIM, SPF), aby zapobiec podszywaniu się pod domenę. Wymuś sprzętowe MFA przy wszystkich firmowych logowaniach kadry kierowniczej najwyższego szczebla.

## B Studium przypadku 2: Ujawnienie firmowych poświadczeń w dark webie

Rozwiązanie dla nauczyciela

### WYTYCZNE OCENIANIA

**Odpowiedzi uczniów powinny obejmować następujące punkty:**

- Analiza scenariusza: Zrzut bazy danych z dark webu zawiera kilkaset firmowych danych uwierzytelniających należących do administratorów systemów przedsiębiorstwa. Zaprojektuj strategię ograniczania skutków.
- Zalecana strategia i rozwiązanie: Przeprowadź resetowanie haseł w całej firmie. Nakaż używanie firmowego menedżera haseł. Wymuś MFA we wszystkich portalach systemowych i skonfiguruj ciągłe, zautomatyzowane alerty monitorowania dark webu.