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

Oszustwa online i inżynieria społeczna Przewodnik po ochronie

Phishing e-mailowy, sfałszowane domeny, vishing, oszustwa związane z pomocą techniczną, weryfikacja poza kanałem (out-of-band), BEC

PRZEGLĄD NAUKI: OSZUSTWA ONLINE

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 obronę przed oszustwami internetowymi. Poznasz fałszywe strony phishingowe, taktyki inżynierii społecznej, oszustwa związane z pomocą techniczną, wektory oszustw przelewowych i metody weryfikacji płatności.

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/oszustwa-internetowe/

Twoja ścieżka nauki: ochrona przed oszustwami internetowymi

- Rozpoznaj typowe oznaki oszustw związanych z fałszywym wsparciem technicznym i domen typosquattingowych.
- Wdróż protokoły weryfikacji poczty e-mail (SPF, DKIM, DMARC) przeciw spoofingowi.
- Ustanów weryfikację transakcji poza kanałem (out-of-band), aby zapobiegać firmowym oszustwom przelewowym.

INSTRUKCJE DO PRZEWODNIKA O OSZUSTWACH ONLINE

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 przed oszustwami internetowymi. Zakończ zadaniem dodatkowym Myśl szybko.

OCHRONA PRZED OSZUSTWAMI ONLINE I INŻYNIERIĄ SPOŁECZNĄ (WPROWADZENIE)

Oszustwa online wykorzystują ludzkie zachowania przez phishing, wyskakujące okienka pomocy technicznej, vishing i oszustwa związane z przelewami. Wymuszanie weryfikacji transakcji innym kanałem oraz reguły domen SPF/DKIM/DMARC pomaga blokować wektory inżynierii społecznej na bramie.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Jaki jest główny wskaźnik oszustwa na pomoc techniczną?

- A. Wyskakujące okienko twierdzące, że system jest zainfekowany, i żądające zadzwonienia pod numer telefonu
- B. Automatyczna aktualizacja zabezpieczeń pobrana z oficjalnego rejestru
- C. Menedżer haseł odmawiający wypełnienia danych logowania w domenie firmowej
- D. Kopia zapasowa plików działająca w tle na konfiguracji dysku zewnętrznego

2. Jaka technika wykorzystuje sfałszowane domeny nadawcy, aby wykraść dane bankowe?

- A. Phishing e-mailowy
- B. Skanowanie portów
- C. Wstrzykiwanie do pamięci
- D. Kryptograficzne niszczenie

3. Co reprezentuje oszustwo z użyciem przelewu bankowego?

- A. Nakłanianie ofiar socjotechniką do wysyłania pieniędzy na fałszywe konta firmowe
- B. Szyfrowanie systemowych baz danych za pomocą ładunków ransomware
- C. Odpytywanie baz danych za pomocą poleceń wstrzykiwania SQL
- D. Tworzenie kopii zapasowych plików systemowych na dyskach offline

4. Dlaczego oszuści tworzą fałszywe strony sklepów internetowych?

- A. Aby ukraść dane kart kredytowych i dane płatnicze kupujących
- B. Aby hostować tabele bazy danych do analizy złośliwego oprogramowania w piaskownicy
- C. Aby przyspieszyć dostawę zamówień online
- D. Aby bezpłatnie testować nowe projekty stron internetowych

5. Co oznacza vishing?

- A. Oszustwa phishingu głosowego przez sieci telefoniczne w celu kradzieży danych uwierzytelniających
- B. Skanowanie sieci lokalnych w poszukiwaniu niezabezpieczonych urządzeń systemowych
- C. Przywracanie systemowych baz danych po nieautoryzowanym naruszeniu
- D. Uruchamianie niezaufanego kodu w bezpiecznych kontenerach wirtualnych

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Oszustwa phishingowe są skierowane wyłącznie przeciw użytkownikom końcowym, nigdy przeciw celom typu whaling na szczeblu zarządu.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. Sfałszowane domeny często używają drobnych literówek (jak amaz0n.com), aby naśladować zaufane marki.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. Oszustwa na pomoc techniczną można rozwiązać, przyznając dzwoniącemu zdalny dostęp.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. Socjotechnika wykorzystuje ludzką psychologię, taką jak strach i pośpiech, aby ominąć reguły bezpieczeństwa.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. Prośby o przelew bankowy należy zawsze weryfikować przy użyciu kanałów komunikacji spoza pasma (out-of-band).

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Oszukańcze e-maile wprowadzające użytkowników w błąd nazywa się _____ .
2. Adres internetowy naśladujący zaufaną markę jest _____ .
3. Oszustwa głosowe wymierzone w dane bankowe nazywa się _____ .
4. Wyskakujące okienko żądające pieniędzy za usunięcie wirusa to _____ na wsparcie techniczne.
5. Aby potwierdzić prośbę o płatność, potrzebna jest pozakanałowa _____ .
6. Kierowanie transakcji firmowych na konta złodziei to oszukańcze _____ .

BANK SŁÓW

KEYLOGGER OSZUSTWO PHISHING PRZEKIEROWANIE SFAŁSZOWANY
VISHING WERYFIKACJA WHALING

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

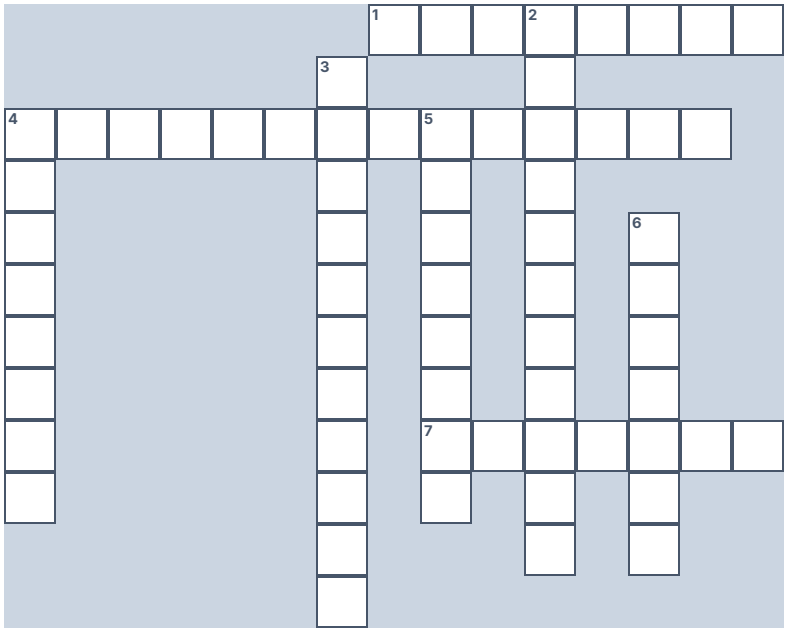
DOPASOWYWANIE DEFINICJI

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

☐	1. PHISHING	A	Oszukańcze przekierowanie przelewów bankowych na konta przestępców.
☐	2. SFAŁSZOWANY	B	Oszukańczy schemat mający na celu wyłudzenie pieniędzy lub danych dostępowych od ofiar.
☐	3. VISHING	C	Wysyłanie oszukańczych wiadomości SMS w celu kradzieży danych logowania do kont mobilnych.
☐	4. OSZUSTWO	D	Oszukańcze połączenia głosowe mające na celu kradzież danych logowania i danych konta.
☐	5. WERYFIKACJA	E	Ukierunkowane ataki phishingowe mające na celu kradzież danych logowania dyrektorów wysokiego szczebla (C-level).
☐	6. PRZELEW	F	Podszywający się adres nadawcy e-maila lub witryny, wyglądający na prawdziwy.
☐	7. WHALING	G	Oszukańcze kampanie e-mailowe mające na celu kradzież danych logowania i haseł.
☐	8. SMISHING	H	Potwierdzanie danych płatności za pomocą zaufanej dodatkowej metody kontaktu.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

1. Wysyłanie oszukańczych SMS-ów w celu wykradzenia danych logowania do kont mobilnych. (8)

4. Oszukańcze przekierowanie transakcji bankowych na konta przestępców. (14)

7. Ukierunkowane ataki phishingowe mające wykraść dane uwierzytelniające kadrze zarządzającej szczebla C. (7)

PIONOWO

2. Podrobiony adres nadawcy e-maila lub witryny, który ma wyglądać na wiarygodny. (11)

3. Potwierdzanie danych płatności zaufaną dodatkową metodą kontaktu. (11)

4. Oszukańcze kampanie e-mailowe mające wykraść dane logowania i hasła. (8)

5. Oszukańczy schemat mający wyłudzić pieniądze lub dostęp do danych uwierzytelniających od ofiar. (8)

6. Oszukańcze rozmowy głosowe mające wykraść dane uwierzytelniające i dane kont. (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

1 poziomo: Wysyłanie oszukańczych SMS-ów w celu wykradzenia danych logowania do kont mobilnych. (8 liter):

4 poziomo: Oszukańcze przekierowanie transakcji bankowych na konta przestępców. (14 liter):

7 poziomo: Ukierunkowane ataki phishingowe mające wykraść dane uwierzytelniające kadrze zarządzającej szczebla C. (7 liter):

PIONOWO

2 pionowo: Podrobiony adres nadawcy e-maila lub witryny, który ma wyglądać na wiarygodny. (11 liter):

3 pionowo: Potwierdzanie danych płatności zaufaną dodatkową metodą kontaktu. (11 liter):

4 pionowo: Oszukańcze kampanie e-mailowe mające wykraść dane logowania i hasła. (8 liter):

5 pionowo: Oszukańczy schemat mający wyłudzić pieniądze lub dostęp do danych uwierzytelniających od ofiar. (8 liter):

6 pionowo: Oszukańcze rozmowy głosowe mające wykraść dane uwierzytelniające i dane kont. (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.

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

LISTA SŁÓW

PHISHING SFAŁSZOWANY VISHING OSZUSTWO WERYFIKACJA PRZEKIEROWANIE WHALING SMISHING

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

- **A. PHISHING**
- **B. SFAŁSZOWANY**
- **C. VISHING**
- **D. OSZUSTWO**
- **E. WERYFIKACJA**
- **F. PRZEKIEROWANIE**
- **G. WHALING**
- **H. SMISHING**

DEFINICJE I POLA DOPASOWANIA

1. Podrobiony adres nadawcy e-maila lub witryny, który ma wyglądać na wiarygodny.
2. Potwierdzanie danych płatności zaufaną dodatkową metodą kontaktu.
3. Oszukańcze przekierowanie transakcji bankowych na konta przestępców.
4. Wysyłanie oszukańczych SMS-ów w celu wykradzenia danych logowania do kont mobilnych.
5. Ukierunkowane ataki phishingowe mające wykraść dane uwierzytelniające kadrze zarządzającej szczebla C.
6. Oszukańcze rozmowy głosowe mające wykraść dane uwierzytelniające i dane kont.
7. Oszukańcze kampanie e-mailowe mające wykraść dane logowania i hasła.
8. Oszukańczy schemat mający wyłudzić pieniądze lub dostęp do danych uwierzytelniających od ofiar.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

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

1. NSHPIHGI
2. VSGNIHI
3. WKIAREJAFCY
4. GHILNWA
5. AFWOAYSZSNŁ
6. WOUTOSSZ
7. AIWPORZEINREEK
8. SMHGSNII

Zadanie dodatkowe: Myśl szybko

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

1	Urządzenia, które można zhakować			
2	Zwroty, których często używają oszuści			
3	Metody płatności, o które proszą oszuści			
4	Rodzaje oszustw internetowych			
5	Oferty zbyt dobre, by były prawdziwe			
6	Miejsca, w których można zgłosić oszustwo			
7	Słowa związane z cyberbezpieczeństwem			
8	Osoby, które możesz ostrzec przed oszustwami			
9	Rzeczy, z których robisz kopie zapasowe			
10	Sygnały ostrzegawcze w e-mailu			
11	Oznaki, że komputer jest zainfekowany			
12	Sposoby na sprawdzenie sklepu internetowego			
13	Sposoby na ochronę twoich kont			
14	Rzeczy do zrobienia, jeśli zostaniesz oszukany			
15	Rzeczy do zrobienia po wycieku danych			

Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

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

STUDIUM PRZYPADKU 1: ZAPOBIEGANIE OSZUSTWOM PRZY FIRMOWYCH PRZELEWACH BANKOWYCH



Scenariusz: Dział finansowy otrzymuje pilny e-mail z sfałszowanego adresu dostawcy z prośbą o kierowanie przyszłych przelewów za faktury na nowy numer rozliczeniowy.

Pytanie do dyskusji: Opisz politykę weryfikacji oszustw z przelewami i wskaż mechanizmy uwierzytelniania poczty e-mail.

STUDIUM PRZYPADKU 2: INCYDENT PHISHINGOWY TYPU WHALING WOBEC KADRY KIEROWNICZEJ



Scenariusz: Członek zarządu kliknął link phishingowy twierdzący, że zawiera bezpieczny dokument na posiedzenie zarządu, wprowadzając swoje główne firmowe dane uwierzytelniające na sfałszowanym portalu.

Pytanie do dyskusji: Opisz szczegółowo kroki reagowania na incydent i wyjaśnij, jak przeprowadzić audyt logowań członków zarządu.

Punkt kontrolny 9: Odszyfruj szyf

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

30	32	14	24	32	30	1	13		22	11	12	25	11	12	18	10

25	14	1	18	7	24	7	17		12

30	7	24	32	9	12	14	1	4	13	2

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 oszustwo online?

Oszustwo wykorzystujące kanały cyfrowe, aby nakłonić ofiary do wysłania pieniędzy lub ujawnienia danych uwierzytelniających.

Q2: Jaki jest główny wskaźnik e-mailowego phishingu?

Wiadomość sugerująca pilność (np. zawieszenie konta) i kierująca do linku, który nie pasuje do oficjalnej domeny.

Q3: Czym jest typosquatting?

Rejestrowanie domen z częstymi literówkami popularnych marek (np. amaz0n.com) w celu hostowania fałszywych witryn phishingowych.

Q4: Czym jest oszustwo na wsparcie techniczne?

Wyskakujące okienko twierdzące, że Twój komputer jest zainfekowany, i nakłaniające do zadzwonienia pod numer oraz zapłaty za fałszywe oprogramowanie czyszczące lub usługi zdalnego dostępu. [1]

Q5: Czym jest vishing?

Ataki phishingowe z użyciem rozmów telefonicznych, by nakłonić ofiary do podania danych konta bankowego lub logowania.

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

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q6: Co oznacza oszustwo przy użyciu przelewu (wire fraud)?

Przekierowywanie transakcji płatniczych na konta oszustów przez podszywanie się pod dostawców lub członków zarządu.

Q7: Czym jest whaling?

Bardzo ukierunkowana forma spear phishingu, wymierzona bezpośrednio w cenne cele, takie jak kadra zarządzająca wyższego szczebla w firmach.

Q8: Czym jest smishing?

Oszukańcze wiadomości tekstowe wysyłane na urządzenia mobilne, zawierające linki do fałszywych portali lub aktualizacji śledzenia przesyłek.

Q9: Dlaczego weryfikacja poza pasmem (out-of-band) jest kluczowa?

Potwierdza szczegóły transakcji innym kanałem komunikacji (np. rozmową telefoniczną), unikając przejętych wątków e-mailowych.

Q10: Jak działa oszustwo z fałszywym rachunkiem powierniczym?

Oszuści tworzą sfałszowaną witrynę rachunku powierniczego, twierdząc, że środki są bezpiecznie przechowywane, a następnie kradną przelew kupującego.

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 oszuści używają BEC (Business Email Compromise) do wyłudzeń przelewów?

Przejmują konto e-mail prawowitego pracownika, monitorują wątki dotyczące faktur i wysyłają zaktualizowane dane do rozliczeń z oszukańczymi kontami bankowymi.

Q2: Jakie jest ryzyko ataków homograficznych IDN w oszustwach online?

Używanie znaków spoza ASCII, które wyglądają identycznie jak zwykłe litery (np. cyrylicy 'a'), do rejestrowania sfałszowanych domen naśladujących prawdziwe marki.

Q3: Dlaczego sprawdzanie nagłówków e-mail jest ważne w wykrywaniu oszustw?

Ujawnia rzeczywisty adres IP serwera pochodzenia i status walidacji SPF/DKIM, pokazując, czy domena nadawcy jest sfałszowana.

Q4: Jak oszuści podszywający się pod wsparcie techniczne wykorzystują oprogramowanie do zdalnego pulpitu?

Używają narzędzi takich jak AnyDesk lub TeamViewer, aby połączyć się z urządzeniem ofiary, podłożyć złośliwe oprogramowanie i wykraść zapisane hasła.

Q5: Jaki jest cel oszustw typu advance-fee (zaliczka z góry)?

Nakłanianie ofiar do wpłacenia z góry opłat manipulacyjnych w zamian za dużą nagrodę finansową, która nie istnieje.

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: Jak oszuści wykorzystują profilowanie w mediach społecznościowych do ukierunkowanego phishingu?

Zbierają informacje o strukturach organizacyjnych firm i nazwiskach pracowników, aby tworzyć przekonujące e-maile typu spear phishing.

Q7: Dlaczego fałszywe sklepy internetowe oferują duże zniżki?

Aby zwabić kupujących do wpisania danych karty kredytowej i przechwycić dane uwierzytelniające do ponownego użycia lub odsprzedaży na forach carderów.

Q8: Jak rekordy DMARC blokują oszustwa phishingowe?

DMARC pozwala właścicielom domen poprosić odbiorców o poddanie kwarantannie lub odrzucenie poczty, która nie przechodzi dopasowanych kontroli SPF i DKIM, co blokuje bezpośrednie podszywanie się. [5]

Q9: Jakie zagrożenie stanowią portale wyłudzające dane uwierzytelniające?

Sfałszowane strony docelowe zaprojektowane tak, aby wyglądały dokładnie jak Microsoft 365 lub przestrzenie Google, kradnące dane logowania w trakcie ich wpisywania.

Q10: Jak zespoły bezpieczeństwa zgłaszają i wyłączają domeny oszustów?

Przez przesłanie dowodów oszustwa na adres e-mail do zgłaszania nadużyć rejestratora, dostawcy hostingu oraz do rejestru Google Safe Browsing.

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

Phishing i spoofing były w 2025 roku najczęściej zgłaszanym rodzajem przestępstw do IC3 FBI, z 191 561 skargami. [2]

2. WGLĄD W BEZPIECZEŃSTWO

Business Email Compromise (BEC) spowodował straty przekraczające 3 mld USD zgłoszone do IC3 FBI w 2025 roku. [2]

3. WGLĄD W BEZPIECZEŃSTWO

Domeny typosquattingowe różnią się od prawdziwych nazw marek o jeden lub dwa znaki, więc szybkie spojrzenie może je przeoczyć.

4. WGLĄD W BEZPIECZEŃSTWO

Oszustwa na pomoc techniczną spowodowały w 2025 roku straty przekraczające 2.1 mld USD zgłoszone do IC3 FBI. [2]

5. WGLĄD W BEZPIECZEŃSTWO

Ataki homograficzne wyglądają identycznie na paskach adresu przeglądarki, chyba że przeglądarka wyświetla konfiguracje punycode.

6. WGLĄD W BEZPIECZEŃSTWO

Oszustwa za pomocą wiadomości SMS (smishing) wykorzystują krótkie, pilne wiadomości z linkami, dając ofiarom niewiele kontekstu, by rozpoznać oszustwo.

7. WGLĄD W BEZPIECZEŃSTWO

Ataki typu whaling są wymierzone w służbowe adresy e-mail kadry zarządzającej, ponieważ osoby te kontrolują dostęp do dużych przelewów płatniczych.

8. WGLĄD W BEZPIECZEŃSTWO

Weryfikowanie zmian płatności przez telefon pod znany, zapisany numer to kluczowa obrona przed oszustwami przelewowymi BEC.

9. WGLĄD W BEZPIECZEŃSTWO

Fałszywe strony rachunku powierniczego (escrow) to częste oszustwo na rynkach internetowych: wyglądają jak bezpieczna usługa płatnicza, ale kradną przelew kupującego.

10. WGLĄD W BEZPIECZEŃSTWO

Google Safe Browsing ostrzega użytkowników, zanim otworzą strony oznaczone jako phishingowe lub zawierające złośliwe oprogramowanie.

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.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] 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

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] 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

Jaki jest główny wskaźnik oszustwa na pomoc techniczną? → Wyskakujące okienko twierdzące, że system jest zainfekowany, i żądające zadzwonienia pod numer telefonu

2 Pytanie 2

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Jaka technika wykorzystuje sfałszowane domeny nadawcy, aby wykraść dane bankowe? → Phishing e-mailowy

3 Pytanie 3

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Co reprezentuje oszustwo z użyciem przelewu bankowego? → Nakłanianie ofiar socjotechniką do wysyłania pieniędzy na fałszywe konta firmowe

4 Pytanie 4

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Dlaczego oszuści tworzą fałszywe strony sklepów internetowych? → Aby ukraść dane kart kredytowych i dane płatnicze kupujących

5 Pytanie 5

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Co oznacza vishing? → Oszustwa phishingu głosowego przez sieci telefoniczne w celu kradzieży danych uwierzytelniających

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Pytanie 6** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: phishing dotyczy też kadry kierowniczej; whaling to phishing wymierzony w wyższe kierownictwo.

7 **Pytanie 7** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Sfałszowane domeny często używają drobnych literówek (jak amaz0n.com), aby naśladować zaufane marki.

8 **Pytanie 8** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: przyznanie oszustowi podszywającemu się pod pomoc techniczną zdalnego dostępu pozwala mu podrzucić złośliwe oprogramowanie i wykraść dane.

9 **Pytanie 9** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Socjotechnika wykorzystuje ludzką psychologię, taką jak strach i pośpiech, aby ominąć reguły bezpieczeństwa.

10 **Pytanie 10** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Prośby o przelew bankowy należy zawsze weryfikować przy użyciu kanałów komunikacji spoza pasma (out-of-band).

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

G 1. PHISHING	F 2. SFAŁSZOWANY	D 3. VISHING	B 4. OSZUSTWO
H 5. WERYFIKACJA	A 6. PRZELEW	E 7. WHALING	C 8. SMISHING

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 PHISHING	2 SFAŁSZOWANY	3 VISHING	4 OSZUSTWO
5 WERYFIKACJA	6 PRZEKIEROWANIE		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 B – SFAŁSZOWANY	2 E – WERYFIKACJA	3 F – PRZEKIEROWANIE	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – OSZUSTWO

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia PHISHING, SFAŁSZOWANY i VISHING 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

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

ROZWIĄZANIE KRZYŻÓWKI

						S	M	I	S	H	I	N	G	
					W				F					
P	R	Z	E	K	I	E	R	O	W	A	N	I	E	
H					R		S		Ł					
I					Y		Z		S		V			
S					F		U		Z		I			
H					I		S		O		S			
I					K		T		W		H			
N					A		W	H	A	L	I	N	G	
G					C		O		N		N			
					J				Y		G			
					A									

PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

1 poziomo: SMISHING Wysyłanie oszukańczych SMS-ów w celu wykradzenia danych logowania do kont mobilnych. (8 liter)

4 poziomo: PRZEKIEROWANIE Oszukańcze przekierowanie transakcji bankowych na konta przestępców. (14 liter)

7 poziomo: WHALING Ukierunkowane ataki phishingowe mające wykraść dane uwierzytelniające kadrze zarządzającej szczebla C. (7 liter)

PIONOWO

2 pionowo: SFAŁSZOWANY Podrobiony adres nadawcy e-maila lub witryny, który ma wyglądać na wiarygodny. (11 liter)

3 pionowo: WERYFIKACJA Potwierdzanie danych płatności zaufaną dodatkową metodą kontaktu. (11 liter)

4 pionowo: PHISHING Oszukańcze kampanie e-mailowe mające wykraść dane logowania i hasła. (8 liter)

5 pionowo: OSZUSTWO Oszukańczy schemat mający wyłudzić pieniądze lub dostęp do danych uwierzytelniających od ofiar. (8 liter)

6 pionowo: VISHING Oszukańcze rozmowy głosowe mające wykraść dane uwierzytelniające i dane kont. (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. NSHPIHGI — **PHISHING**
2. VSGNIHI — **VISHING**
3. WKIAREJAFCY — **WERYFIKACJA**
4. GHILNWA — **WHALING**
5. AFWOAYSZSNŁ — **SFAŁSZOWANY**
6. WOUTOSSZ — **OSZUSTWO**
7. AIWPORZEINREEK — **PRZEKIEROWANIE**
8. SMHGSNII — **SMISHING**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"WYKRYWAJ PHISHING SKANEREM I WERYFIKACJĄ"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Zapobieganie oszustwom przy firmowych przelewach bankowych

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Dział finansowy otrzymuje pilny e-mail ze sfałszowanego adresu dostawcy z prośbą o kierowanie przyszłych przelewów za faktury na nowy numer rozliczeniowy.
- Zalecana strategia i rozwiązanie: Wprowadź politykę podwójnej autoryzacji dla wszystkich płatności. Zastosuj weryfikację poza pasmem z użyciem wcześniej zapisanego numeru telefonu i blokuj na bramie e-maile z sfałszowanych domen.

B Studium przypadku 2: Incydent phishingowy typu whaling wobec kadry kierowniczej

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Członek zarządu kliknął link phishingowy rzekomo prowadzący do bezpiecznego dokumentu na posiedzenie zarządu i wpisał główne dane logowania firmowego na sfałszowanym portalu.
- Zalecana strategia i rozwiązanie: Odizoluj urządzenie członka zarządu. Zresetuj wszystkie firmowe tokeny sesji i dane uwierzytelniające. Przejrzyj logi dostępu pod kątem wycieku danych i wdróż sprzętowe MFA przy wszystkich logowaniach.