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

Ataki phishingowe i inżynieria społeczna

Spear phishing, oszustwa typu whaling, protokoły SPF/DKIM/DMARC, podszywanie się pod nadawcę i szkolenia pracowników z bezpieczeństwa.

PRZEGLĄD NAUKI: ATAKI PHISHINGOWE

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 ataki phishingowe i inżynierię społeczną. Poznasz spear phishing, whaling, podszywanie się pod domeny, protokoły SPF/DKIM/DMARC, bezpieczeństwo linków i szkolenia uświadamiające dla pracowników.

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/ataki-phishingowe/

Twoja ścieżka nauki: ograniczanie skutków phishingu

- Rozpoznaj typowe oszustwa typu phishing, vishing i fałszywe wyskakujące okna wsparcia.
- Wdróż procedury weryfikacji transakcji poza kanałem głównym (out-of-band).
- Skonfiguruj reguły SPF, DKIM i DMARC, aby blokować sfałszowane domeny.

INSTRUKCJE DO PRZEWODNIKA O ATAKACH PHISHINGOWYCH

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 uwierzytelniania poczty e-mail. Zakończ zadaniem dodatkowym Myśl szybko.

ATAKI PHISHINGOWE I INŻYNIERIA SPOŁECZNA (WPROWADZENIE)

Ataki phishingowe wykorzystują ukierunkowane wiadomości, oszustwa typu whaling i spoofing domen do pozyskiwania danych logowania użytkowników. Zabezpieczenie systemów firmowych wymaga wdrożenia reguł SPF, DKIM i DMARC na bramie oraz dodatkowych kroków zatwierdzania innym kanałem.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Czym jest spear phishing?

- A. Ukierunkowany e-mail phishingowy dostosowany do konkretnej osoby lub organizacji
- B. Szeroka wiadomość masowa wysłana do milionów losowych adresów
- C. Atak sieciowy zalewający serwery WWW ruchem
- D. Technika wydobywania danych z bazy, wymierzona w rekordy użytkowników

2. Który protokół pozwala domenie wypisać w DNS swoje autoryzowane adresy IP nadawców, aby walczyć ze spoofingiem?

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3. Czym jest atak typu whaling?

- A. Kampania phishingowa skierowana specjalnie do znanych dyrektorów firm
- B. Atak typu SQL injection wymierzony w kopie zapasowe baz danych
- C. Fizyczna kradzież sprzętu routerów sieci lokalnej
- D. Zautomatyzowane skanowanie siłowe typu credential stuffing

4. Co robi DKIM?

- A. Dodaje do e-maili podpis kryptograficzny, aby zweryfikować autentyczność nadawcy
- B. Blokuje przychodzący ruch pakietów sieciowych na zaporze sieciowej
- C. Szyfruje woluminy magazynu bazy danych w spoczynku
- D. Skanuje załączniki e-mail w poszukiwaniu złośliwego oprogramowania na podstawie sygnatur

5. Jaką rolę pełni DMARC?

- A. Informowanie odbierających serwerów pocztowych, jak postępować z wiadomościami, które nie przeszły kontroli SPF/DKIM
- B. Odszyfrowywanie haseł systemowych za pomocą wstępnie obliczonych tęczowych tablic
- C. Kompresowanie załączników e-mail przed dostarczeniem
- D. Konfigurowanie uprawnień dostępu do routingu sieciowego

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Spear phishing opiera się na ogólnych masowych e-mailach wysyłanych do milionów losowych adresów.

- ○ Prawda
- ○ Fałsz

7 Pytanie 7

7. Polityki DMARC mogą nakazać serwerom pocztowym odrzucanie nieautoryzowanych, sfałszowanych wiadomości.

- ○ Prawda
- ○ Fałsz

8 Pytanie 8

8. Weryfikacja SPF działa poprzez sprawdzanie podpisu kryptograficznego treści wiadomości e-mail.

- ○ Prawda
- ○ Fałsz

9 Pytanie 9

9. Ataki typu whaling są wymierzone w administratorów niskiego szczebla w firmach, aby uzyskać dostęp do plików baz danych.

- ○ Prawda
- ○ Fałsz

10 Pytanie 10

10. Weryfikacja żądań płatności innym kanałem (out-of-band) pomaga powstrzymywać oszustwa z przelewami finansowymi.

- ○ Prawda
- ○ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Atak na konkretnego pracownika z użyciem spersonalizowanych informacji to _____ phishing.

2. Sfałszowanie nagłówka e-maila, aby wiadomości wyglądały wiarygodnie, to _____ nadawcy.

3. Lista w DNS autoryzowanych adresów IP serwerów pocztowych to _____ .

4. Standard podpisu e-mail zapewniający weryfikację nadawcy to _____ .

5. Ustalanie zasad odrzucania wiadomości, które nie przeszły kontroli SPF/DKIM, wykorzystuje _____ .

6. Kampania phishingowa wymierzona w kadrę zarządzającą szczebla C nazywa się _____ .

BANK SŁÓW

DKIM DMARC RANSOMWARE SPEAR SPF SPOOFING VISHING WHALING

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

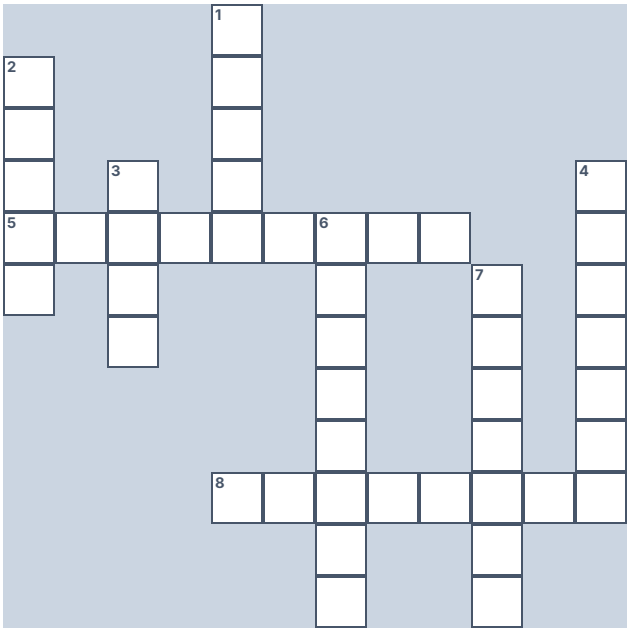
DOPASOWYWANIE DEFINICJI

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

☐	1. CELOWANY	A	Oszukańcze rozmowy telefoniczne.
☐	2. SPOOFING	B	Cel: dyrektorzy wysokiego szczebla (C-level).
☐	3. SPF	C	Instrukcje odrzucania według polityki.
☐	4. DKIM	D	Autoryzowane adresy IP nadawców w DNS.
☐	5. DMARC	E	E-mail socjotechniczny.
☐	6. WHALING	F	Spersonalizowany, ukierunkowany e-mail.
☐	7. PHISHING	G	Podszywanie się pod adres e-mail nadawcy.
☐	8. VISHING	H	Podpis kryptograficzny w e-mailu.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

5. Adresy IP autoryzowanych nadawców w DNS. (9)

8. E-mail oparty na socjotechnice. (8)

PIONOWO

1. Spersonalizowany, ukierunkowany e-mail. (5)

2. Polityka z instrukcjami odrzucania. (5)

3. Podpis kryptograficzny w e-mailu. (4)

4. Oszukańcze rozmowy telefoniczne. (7)

6. Fałszowanie adresu e-mail nadawcy. (8)

7. Ataki na kadrę zarządzającą szczebla C. (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

5 poziomo: Adresy IP autoryzowanych nadawców w DNS. (9 liter):

8 poziomo: E-mail oparty na socjotechnice. (8 liter):

PIONOWO

1 pionowo: Spersonalizowany, ukierunkowany e-mail. (5 liter):

2 pionowo: Polityka z instrukcjami odrzucania. (5 liter):

3 pionowo: Podpis kryptograficzny w e-mailu. (4 liter):

4 pionowo: Oszukańcze rozmowy telefoniczne. (7 liter):

6 pionowo: Fałszowanie adresu e-mail nadawcy. (8 liter):

7 pionowo: Ataki na kadrę zarządzającą szczebla C. (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.

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

LISTA SŁÓW

SPEAR SPOOFING REKORDSPF DKIM DMARC WHALING PHISHING VISHING

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. SPEAR	1. Fałszowanie adresu e-mail nadawcy.
B. SPOOFING	2. Spersonalizowany, ukierunkowany e-mail.
C. REKORDSPF	3. Oszukańcze rozmowy telefoniczne.
D. DKIM	4. Adresy IP autoryzowanych nadawców w DNS.
E. DMARC	5. E-mail oparty na socjotechnice.
F. WHALING	6. Polityka z instrukcjami odrzucania.
G. PHISHING	7. Podpis kryptograficzny w e-mailu.
H. VISHING	8. Ataki na kadrę zarządzającą szczebla C.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

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

1. AESRP
2. FRPOEDSRK
3. ADCRM
4. SNGIHPHI
5. FIPGOSNO
6. IMDK
7. WNIGHLA
8. IHGVNIS

Zadanie dodatkowe: Myśl szybko

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

1	Urządzenia, które można zhakować			
2	Oznaki wiadomości phishingowej			
3	Oznaki, że komputer jest zainfekowany			
4	Słowa wywołujące fałszywą pilność			
5	Sposoby na sprawdzenie nadawcy			
6	Osoby, które możesz poprosić o pomoc IT			
7	Rzeczy, z których robisz kopie zapasowe			
8	Ryby lub stworzenia morskie, które znasz			
9	Firmy, pod które podszywają się oszuści			
10	Bezpieczne nawyki, które możesz zacząć już dziś			
11	Rzeczy do zrobienia po kliknięciu w fałszywy link			
12	Rzeczy do zrobienia po wycieku danych			
13	Kanały, w których występuje phishing			
14	Rzeczy, których nigdy nie wysyłasz e-mailem			
15	Sposoby na ochronę twoich kont			

Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

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

STUDIUM PRZYPADKU 1: ZAPOBIEGANIE SKUTKOM ATAKU WHALINGOWEGO NA KADRĘ ZARZĄDZAJĄCĄ

👨‍💻

Scenariusz: Dyrektor finansowy otrzymuje wysoce spersonalizowany e-mail rzekomo od prezesa z prośbą o szybki przelew 50 000 USD na sfinalizowanie poufnego zakupu domeny.

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

STUDIUM PRZYPADKU 2: WDRAŻANIE ZASAD BRAMY SPF/DKIM/DMARC

👨‍💻

Scenariusz: Przedsiębiorstwo nie przechodzi audytów bezpieczeństwa, ponieważ wychodzące e-maile marketingowe są często oznaczane jako spam, a hakerzy aktywnie podszywają się pod domenę marki firmy.

Pytanie do dyskusji: Ustal techniczne i administracyjne mechanizmy kontroli weryfikujące autentyczność poczty e-mail.

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

30 32 14 24 32 30 1 13

25 20 4 13 20 27 7 4 11 18 12 14 8

1 28 6 32 27 7 17 3 24 1 17 14 12 7 17 1 12 15

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 phishing?

Phishing to atak inżynierii społecznej, w którym przestępcy wysyłają fałszywe wiadomości, aby nakłonić użytkowników do ujawnienia wrażliwych danych.

Q2: Jaka jest różnica między phishingiem a spear phishingiem?

Phishing jest skierowany do szerokich grup z ogólną treścią, natomiast spear phishing jest skierowany do konkretnych ofiar z użyciem dopasowanych szczegółów.

Q3: Czym jest whaling?

Whaling to wysoce ukierunkowany atak phishingowy skierowany przeciwko znanym osobom z kierownictwa, które mają uprawnienia administracyjne.

Q4: Czym jest spoofing e-maili?

Spoofing e-maila to tworzenie wiadomości e-mail ze sfałszowanym adresem nadawcy, aby nakłonić odbiorcę do zaufania źródłu.

Q5: Jak SPF zapobiega spoofingowi?

Publikuje w DNS listę autoryzowanych adresów IP wysyłających pocztę, co pozwala serwerom odbierającym zweryfikować źródło wiadomości. [1]

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

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q6: Czym jest DKIM?

DomainKeys Identified Mail dodaje podpis kryptograficzny do nagłówków wiadomości e-mail, co dowodzi, że domena wzięła za nią odpowiedzialność i że wiadomość nie została zmieniona.

Q7: Co oznacza skrót DMARC?

Domain-based Message Authentication, Reporting, and Conformance. [2]

Q8: Czym jest polityka DMARC?

Polityka informująca serwery pocztowe, jak traktować wiadomości, które nie przechodzą weryfikacji SPF/DKIM (none, quarantine lub reject). [2]

Q9: Czym jest vishing?

Phishing głosowy (vishing), w którym atakujący wykorzystują oszukańcze rozmowy telefoniczne, aby wyłudzić dane administracyjne lub finansowe.

Q10: Jak pomagają skanery linków?

Skanują i przepisują linki w przychodzących e-mailach, aby w chwili kliknięcia zweryfikować bezpieczeństwo stron docelowych.

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 działa atak homograficzny?

Atakujący rejestrują nazwy domen z użyciem podobnie wyglądających znaków Unicode spoza ASCII, aby wizualnie naśladować prawdziwą nazwę domeny.

Q2: Czym jest reprezentacja punycode?

Kodowanie, które zamienia nazwy domen Unicode na ciągi zgodne z ASCII zaczynające się od „xn--”, aby DNS mógł je obsłużyć.

Q3: Dlaczego „p=reject” jest najbezpieczniejszym stanem DMARC?

Prosi serwery odbierające o odrzucanie poczty, która nie przechodzi DMARC (dopasowane SPF/DKIM) podczas sesji SMTP, blokując bezpośrednie podszywanie się. [2]

Q4: Jak atakujący omijają reguły SPF?

Przez wykorzystywanie domen łudząco podobnych (typosquatting) lub używanie przejętych kont w legalnych zewnętrznych usługach poczty.

Q5: Czym jest przejęcie firmowej poczty e-mail (BEC)?

Oszustwo korporacyjne, w którym atakujący przejmują lub podszywają się pod firmowe konta e-mail, aby autoryzować oszukańcze płatności.

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 uwierzytelnianie wieloskładnikowe powstrzymuje phishing?

Wymaga dodatkowych tokenów (takich jak klucze sprzętowe), których nie da się ukraść samymi fałszywymi stronami docelowymi.

Q7: Czym jest strona docelowa służąca do wyłudzania danych uwierzytelniających?

Łudząco podobny portal logowania zaprojektowany do przechwytywania w czasie rzeczywistym wpisywanych nazw użytkowników, haseł i tokenów MFA.

Q8: Czym jest przejęcie subdomeny (subdomain hijacking)?

Atakujący przejmujący kontrolę nad nieużywanym wskaźnikiem subdomeny DNS, aby hostować złośliwe strony docelowe phishingu pod zaufaną domeną nadrzędną.

Q9: Jak działa sprawdzanie zgodności DKIM?

Sprawdza, czy domena w nagłówku „From” zgadza się z domeną, która kryptograficznie podpisała wiadomość w nagłówku DKIM.

Q10: Jaka jest rola bramy poczty e-mail?

Filtrowanie przychodzących e-maili, audytowanie linków, uruchamianie załączników w piaskownicy oraz weryfikacja zgodności z SPF/DKIM/DMARC.

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. [4]

2. WGLĄD W BEZPIECZEŃSTWO

Business email compromise (BEC) spowodował straty przekraczające 3 mld USD zgłoszone do IC3 FBI w 2025 roku. [4]

3. WGLĄD W BEZPIECZEŃSTWO

Ataki homograficzne wykorzystują cyrylicowe litery podobne do łacińskich, aby wizualnie powielić w przeglądarkach domeny marek z dokładnym dopasowaniem.

4. WGLĄD W BEZPIECZEŃSTWO

Przy „p=reject" domena prosi odbiorców, aby odrzucali wiadomości niespełniające weryfikacji już podczas dostarczania, a nie kierowali ich do spamu. [2]

5. WGLĄD W BEZPIECZEŃSTWO

Ataki typu whaling wymierzone w prezesów zwykle zawierają prośby o pilne płatności związane z poufnymi fuzjami lub zakupami domen.

6. WGLĄD W BEZPIECZEŃSTWO

Portale wyłudzające poświadczenia kopiują prawdziwe strony logowania, aby ofiary wpisywały hasła bezpośrednio w formularz atakującego.

7. WGLĄD W BEZPIECZEŃSTWO

Wspólne wytyczne CISA dotyczące phishingu zalecają szkolenie użytkowników obok DMARC, SPF, DKIM i odpornego na phishing MFA. [3]

8. WGLĄD W BEZPIECZEŃSTWO

Ocena SPF jest ograniczona do 10 terminów wykonujących zapytania DNS; przekroczenie limitu zwraca wynik 'permerror'. [1]

9. WGLĄD W BEZPIECZEŃSTWO

Sprzętowe klucze bezpieczeństwa FIDO2 zapewniają kryptograficznie wspartą ochronę przed zdalnym zbieraniem danych uwierzytelniających.

10. WGLĄD W BEZPIECZEŃSTWO

Phishing to jeden z najczęstszych sposobów, w jaki atakujący po raz pierwszy dostają się do organizacji, dlatego regularne szkolenia uświadamiające są skuteczną obroną.

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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

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

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

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

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

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

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

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 Pytanie 1

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest spear phishing? → Ukierunkowany e-mail phishingowy dostosowany do konkretnej osoby lub organizacji

2 Pytanie 2

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

SPF publikuje w DNS autoryzowane hosty nadawcze domeny, aby odbiorcy mogli sprawdzić nadawcę z koperty.

3 Pytanie 3

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest atak typu whaling? → Kampania phishingowa skierowana specjalnie do znanych dyrektorów firm

4 Pytanie 4

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Co robi DKIM? → Dodaje do e-maili podpis kryptograficzny, aby zweryfikować autentyczność nadawcy

5 Pytanie 5

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Jaką rolę pełni DMARC? → Informowanie odbierających serwerów pocztowych, jak postępować z wiadomościami, które nie przeszły kontroli SPF/DKIM

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 Pytanie 6

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Fałsz: spear phishing jest dostosowany do konkretnych osób, w przeciwieństwie do ogólnego masowego phishingu.

7 Pytanie 7

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Polityki DMARC mogą nakazać serwerom pocztowym odrzucanie nieautoryzowanych, sfałszowanych wiadomości.

8 Pytanie 8

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Fałsz: SPF sprawdza adres IP nadawcy względem DNS; to DKIM weryfikuje podpis kryptograficzny.

9 Pytanie 9

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Fałsz: whaling jest wymierzony w wyższe kierownictwo, które może zatwierdzać płatności i mieć dostęp do wrażliwych danych.

10 Pytanie 10

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Prawda: potwierdzanie żądań płatności osobnym, znanym kanałem pomaga powstrzymywać oszustwa z przelewami.

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

F 1. CELOWANY	G 2. SPOOFING	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING	E 7. PHISHING	A 8. VISHING

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 SPEAR	2 SPOOFING	3 SPF	4 DKIM
5 DMARC	6 WHALING		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 B – SPOOFING	2 A – SPEAR	3 H – VISHING	4 C – REKORDSPF
5 G – PHISHING	6 E – DMARC	7 D – DKIM	8 F – WHALING

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia CELOWANY, SPOOFING i SPF oraz podać przykład każdego z nich.

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

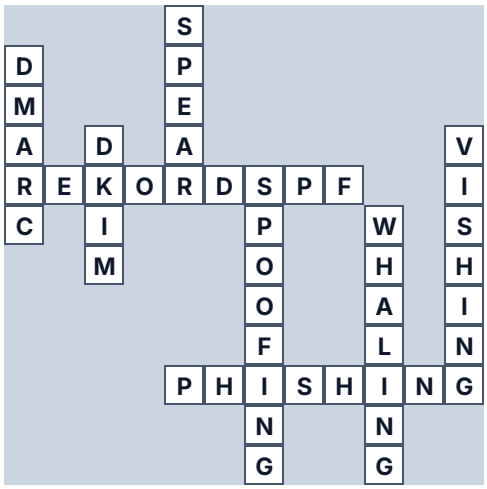
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

5 poziomo: REKORDSPF Adresy IP autoryzowanych nadawców w DNS. (9 liter)

8 poziomo: PHISHING E-mail oparty na socjotechnice. (8 liter)

PIONOWO

1 pionowo: SPEAR Spersonalizowany, ukierunkowany e-mail. (5 liter)

2 pionowo: DMARC Polityka z instrukcjami odrzucania. (5 liter)

3 pionowo: DKIM Podpis kryptograficzny w e-mailu. (4 liter)

4 pionowo: VISHING Oszukańcze rozmowy telefoniczne. (7 liter)

6 pionowo: SPOOFING Fałszowanie adresu e-mail nadawcy. (8 liter)

7 pionowo: WHALING Ataki na kadrę zarządzającą szczebla C. (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. AESRP — **SPEAR**
2. FRPOEDSRK — **REKORDSPF**
3. ADCRM — **DMARC**
4. SNGIHPHI — **PHISHING**
5. FIPGOSNO — **SPOOFING**
6. IMDK — **DKIM**
7. WNIGHLA — **WHALING**
8. IHGVNIS — **VISHING**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"WYKRYWAJ SOCJOTECHNIKĘ AUDYTEM BRAMKI EMAIL"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Zapobieganie skutkom ataku whalingowego na kadrę zarządzającą

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Dyrektor finansowy otrzymuje bardzo spersonalizowany e-mail rzekomo od prezesa z prośbą o pilny przelew 50,000 USD w celu sfinalizowania poufnego zakupu domeny.
- Zalecana strategia i rozwiązanie: Skonfiguruj DMARC z polityką „p=reject”, aby blokować sfałszowane domeny nadawców. Dodaj banery ostrzegawcze o zewnętrznym nadawcy na bramie i wymagaj ustnego potwierdzenia poza pasmem (out-of-band) dla wszystkich transakcji finansowych.

B Studium przypadku 2: Wdrażanie zasad bramy SPF/DKIM/DMARC

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Firma nie przechodzi audytów bezpieczeństwa, ponieważ wychodzące e-maile marketingowe są często oznaczane jako spam, a hakerzy aktywnie podszywają się pod domenę marki firmy.
- Zalecana strategia i rozwiązanie: Opublikuj rekord TXT dla SPF ze wskazaniem autoryzowanych adresów IP nadawców. Skonfiguruj klucze podpisu DKIM na serwerach poczty wychodzącej i analizuj przychodzące raporty zwrotne DMARC w formacie XML, aby wykrywać nadużycia.