Jméno: _____ Datum: _____ Body: _____

Phishingové útoky a sociální inženýrství

Spear phishing, whaling podvody, protokoly SPF/DKIM/DMARC, spoofing odesílatele a bezpečnostní školení zaměstnanců.

PŘEHLED VÝUKY: PHISHINGOVÉ ÚTOKY

ZABEZPEČENO
ŠIFROVÁNÍ DAT
Standard 256bitového AES

VYHOVUJÍCÍ
GLOBÁLNÍ STANDARDY
Rámce GDPR a CCPA

ZERO-TRUST
ZÁSADY PŘÍSTUPU
Vícefaktorové ověřování

Vítejte! Tento balíček aktivit vás provede phishingovými útoky a sociálním inženýrstvím. Prozkoumáte spear phishing, whaling, spoofing domén, protokoly SPF/DKIM/DMARC, bezpečnost odkazů a školení povědomí zaměstnanců.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte kyberbezpečnost a prevenci hrozeb.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce kyberbezpečností od VPN.com

URL: https://www.vpn.com/cs/kyberneticka-bezpecnost/phishingove-utoky/

Váš studijní plán: obrana proti phishingu

- Určete běžné podvody typu phishing, vishing a falešná vyskakovací okna podpory.
- Zavést postupy ověřování transakcí mimo hlavní komunikační kanál.
- Nakonfigurujte pravidla SPF, DKIM a DMARC k blokování podvržených domén.

POKYNY K PRŮVODCI PHISHINGOVÝMI ÚTOKY

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na ověřování e-mailů. Zakončete bonusovou aktivitou Mysli rychle.

PHISHINGOVÉ ÚTOKY A SOCIÁLNÍ INŽENÝRSTVÍ (ÚVOD)

Phishingové útoky využívají cílené zprávy, whalingové podvody a spoofing domén ke sběru přihlašovacích údajů uživatelů. Zabezpečení firemních systémů vyžaduje nasazení pravidel SPF, DKIM a DMARC na bráně spolu se schvalovacími kroky mimo hlavní kanál.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1 **1. Co je spear phishing?**

- A. Cílený phishingový e-mail šitý na míru konkrétní osobě nebo organizaci
- B. Široký hromadný e-mail rozeslaný na miliony náhodných adres
- C. Síťový útok, který zahlcuje webové servery provozem
- D. Technika extrakce databáze cílící na záznamy uživatelů

2 **2. Který protokol umožňuje doméně uvést v DNS autorizované odesílací IP adresy v boji proti spoofingu?**

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

3 **3. Co je whalingový útok?**

- A. Phishingová kampaň cílená konkrétně na vysoce postavené firemní manažery
- B. Útok SQL injection cílící na zálohy databáze
- C. Fyzická krádež routeru místní sítě
- D. Automatizovaný brute-force sken typu credential stuffing

4 **4. Co dělá DKIM?**

- A. Přidává k e-mailům kryptografický podpis k ověření pravosti odesílatele
- B. Blokuje příchozí provoz síťových paketů na firewallu
- C. Šifruje databázové úložné svazky v klidu
- D. Skenuje e-mailové přílohy na malware podle signatur

5 **5. Jaká je role DMARC?**

- A. Určuje přijímajícím poštovním serverům, jak nakládat s neúspěšnými kontrolami SPF/DKIM
- B. Dešifrování systémových hesel pomocí předpočítaných duhových tabulek
- C. Komprese e-mailových příloh před doručením
- D. Konfigurace oprávnění síťového směrování

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Spear phishing se spoléhá na generické hromadné e-maily rozesílané milionům náhodných adres.

○ Pravda ○ Nepravda

7 Otázka 7

7. Zásady DMARC mohou poštovním serverům nařídit odmítnutí neautorizovaných podvržených zpráv.

○ Pravda ○ Nepravda

8 Otázka 8

8. Ověření SPF funguje validací kryptografického podpisu těla e-mailu.

○ Pravda ○ Nepravda

9 Otázka 9

9. Whalingové útoky cílí na nižší firemní administrátory, aby získaly přístup k databázovým souborům.

○ Pravda ○ Nepravda

10 Otázka 10

10. Ověřování platebních žádostí mimo hlavní kanál pomáhá zastavit podvody s bankovními převody.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Cílení na konkrétního zaměstnance pomocí personalizovaných informací se nazývá _____ phishing.
2. Padělání hlavičky e-mailu, aby zpráva vypadala legitimně, se nazývá _____ .
3. Seznam autorizovaných IP adres poštovních serverů v DNS definuje záznam _____ .
4. Standard e-mailového podpisu poskytující ověření odesílatele se označuje zkratkou _____ .
5. Politiku odmítání zpráv, které neprojdou kontrolami SPF/DKIM, stanovuje záznam _____ .
6. Phishingová kampaň cílící na vrcholové manažery se nazývá _____ .

ZÁSOBNÍK SLOV

DKIM DMARC PHISHING SPEAR SPF SPOOFING VISHING WHALING

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

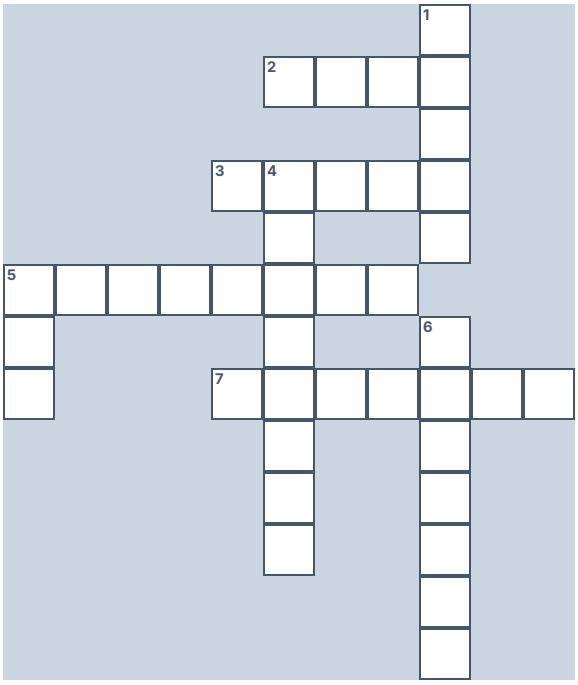
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. SPEAR	A	Hlasové podvodné telefonáty.
☐	2. SPOOFING	B	Cílit na vedoucí pracovníky C-úrovně.
☐	3. SPF	C	Instrukce odmítnutí dle pravidel.
☐	4. DKIM	D	IP adresy autorizovaných odesílatelů v DNS.
☐	5. DMARC	E	E-mail sociálního inženýrství.
☐	6. WHALING	F	Personalizovaný cílený e-mail.
☐	7. PHISHING	G	Falšování adresy odesílatele e-mailu.
☐	8. VISHING	H	Kryptografický podpis v e-mailu.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

2. Kryptografický podpis v e-mailu. (4)

3. Personalizovaný cílený e-mail. (5)

5. Falšování adresy odesílatele e-mailu. (8)

7. Cílení na vrcholové manažery. (7)

SVISLÉ NÁPOVĚDY

1. Politika s pokyny k odmítnutí. (5)

4. E-mail sociálního inženýrství. (8)

5. Autorizované IP odesílatelů v DNS. (3)

6. Podvodné hlasové hovory. (7)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

2 vodorovně: Kryptografický podpis v e-mailu. (4 písmen):

3 vodorovně: Personalizovaný cílený e-mail. (5 písmen):

5 vodorovně: Falšování adresy odesílatele e-mailu. (8 písmen):

7 vodorovně: Cílení na vrcholové manažery. (7 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Politika s pokyny k odmítnutí. (5 písmen):

4 svisle: E-mail sociálního inženýrství. (8 písmen):

5 svisle: Autorizované IP odesílatelů v DNS. (3 písmen):

6 svisle: Podvodné hlasové hovory. (7 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

Z	R	Y	Ě	Q	M	Č	S	Š	I	Ě	O	S	N	R
Y	R	Ó	Č	U	T	Ť	P	V	E	L	Í	B	A	B
C	P	M	Y	L	J	Y	E	L	I	Y	U	K	Ď	Ř
N	J	I	D	I	O	Ň	A	K	R	S	Q	F	Ň	Ň
Ř	S	K	T	U	S	Ť	R	F	C	D	H	T	R	Ó
G	H	D	Š	B	P	V	P	D	T	Z	M	I	Ů	C
N	Ž	V	Ě	K	O	G	Ž	H	D	Ň	Ď	A	N	Ř
I	X	Q	C	Ú	O	B	A	Ž	I	O	D	L	R	G
L	A	Ď	Ó	Ď	F	É	G	I	D	S	S	Ř	N	C
A	E	I	Š	Ž	I	T	É	Ř	Ů	E	H	A	Á	Ř
H	P	O	Q	U	N	Y	R	J	S	U	Š	I	Č	Ň
W	Ý	B	Ě	Š	G	X	W	Í	F	A	S	Ž	N	Ý
Ý	L	F	I	N	S	J	N	P	M	Ť	P	G	R	G
Ř	G	Ž	Á	Ó	Ů	Ě	S	Ú	C	Ý	Š	Ý	B	G
M	Ž	F	J	Ó	Q	O	X	C	N	Ž	Z	Ě	Ý	P

SEZNAM SLOV

SPEAR SPOOFING SPF DKIM DMARC WHALING PHISHING VISHING

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY	DEFINICE A POLE K PŘIŘAZENÍ
A. SPEAR	1. Falšování adresy odesílatele e-mailu.
B. SPOOFING	2. Personalizovaný cílený e-mail.
C. SPF	3. Podvodné hlasové hovory.
D. DKIM	4. Autorizované IP odesílatelů v DNS.
E. DMARC	5. E-mail sociálního inženýrství.
F. WHALING	6. Politika s pokyny k odmítnutí.
G. PHISHING	7. Kryptografický podpis v e-mailu.
H. VISHING	8. Cílení na vrcholové manažery.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny kybernetické bezpečnosti. Odpovědi pište do připravených polí.

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

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Zařízení, která lze hacknout			
2	Známky phishingového e-mailu			
3	Známky toho, že je počítač nakažený			
4	Slova, která vytvářejí falešnou naléhavost			
5	Způsoby, jak ověřit odesílatele			
6	Lidé, které můžete požádat o pomoc s IT			
7	Věci, které si zálohujete			
8	Ryby nebo mořští živočichové, které znáte			
9	Firmy, za které se podvodníci vydávají			
10	Bezpečné návyky, se kterými můžete začít už dnes			
11	Věci, které je třeba udělat po kliknutí na falešný odkaz			
12	Co udělat po úniku dat			
13	Kanály, kde dochází k phishingu			
14	Věci, které nikdy neposíláte e-mailem			
15	Způsoby, jak chránit své účty			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: NÁPRAVA WHALINGOVÉHO ÚTOKU NA VEDENÍ FIRMY



Scénář: Finanční ředitel obdrží vysoce personalizovaný e-mail, který se vydává za zprávu od generálního ředitele a žádá o rychlý převod 50 000 USD k uzavření důvěrného nákupu domény.

Otázka k diskusi: Analyzujte rizika podvržení značky a popište SPF/DKIM/DMARC a kontroly ověřování.

PŘÍPADOVÁ STUDIE 2: NASAZENÍ POLITIK BRÁNY SPF/DKIM/DMARC



Scénář: Podnik neprochází bezpečnostními audity, protože odchozí marketingové e-maily jsou často označovány jako spam a hackeři aktivně spoofují doménu značky společnosti.

Otázka k diskusi: Zaveďte technické a administrativní kontroly k ověření pravosti e-mailů.

Kontrolní bod 9: Dešifrování šifry

Profesionál v kyberbezpečnosti chrání síťová aktiva před online útočníky. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

28 22 4 14 2 18 20 15 14 20 41 8 20 39 26 28 30 35 15

22 6 13 1 18 15 1 32 6 14 30 8 19 1 14 18 22 35 9

3 26 2 20 38

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část A)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q1: Co je phishing?

Phishing je útok sociálního inženýrství, při němž zločinci posílají podvodné zprávy, aby vylákali od uživatelů citlivá data.

Q2: Jaký je rozdíl mezi phishingem a spear phishingem?

Phishing cílí na široké skupiny obecným obsahem, zatímco spear phishing cílí na konkrétní oběti pomocí údajů na míru.

Q3: Co je whaling?

Whaling je vysoce cílený phishingový útok zaměřený na vysoce postavené vedoucí pracovníky s administrativními pravomocemi.

Q4: Co je e-mailový spoofing?

E-mailový spoofing je vytváření e-mailových zpráv s padělanou adresou odesílatele s cílem přimět příjemce důvěřovat zdroji.

Q5: Jak SPF brání spoofingu?

Zveřejňuje v DNS seznam autorizovaných odesílajících IP adres, což přijímajícím serverům umožňuje ověřit zdroj pošty. [1]

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část B)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Co je DKIM?

DomainKeys Identified Mail přidává do hlaviček e-mailu kryptografický podpis, který dokazuje, že doména převzala odpovědnost a zpráva nebyla pozměněna.

Q7: Co znamená zkratka DMARC?

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

Q8: Co je politika DMARC?

Zásada říkající poštovním serverům, jak nakládat se zprávami, které neprojdou SPF/DKIM (none, quarantine nebo reject). [2]

Q9: Co je vishing?

Hlasový phishing (vishing), kdy útočníci pomocí podvodných telefonátů získávají administrativní nebo finanční data.

Q10: Jak pomáhají skenery odkazů?

Skenují a přepisují odkazy v příchozích e-mailech, aby v okamžiku kliknutí ověřily bezpečnost cílových stránek.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část C)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q1: Jak funguje homografický útok?

Útočníci registrují doménová jména s použitím vizuálně podobných non-ASCII znaků Unicode, aby napodobili legitimní doménové jméno.

Q2: Co je reprezentace punycode?

Kódování, které převádí doménová jména v Unicode na řetězce kompatibilní s ASCII začínající 'xn--', aby je DNS dokázal zpracovat.

Q3: Proč je 'p=reject' nejbezpečnější stav DMARC?

Žádá přijímající servery, aby odmítaly poštu, která neprojde kontrolou DMARC (zarovnané SPF/DKIM), během SMTP relace, čímž blokuje přímý spoofing. [2]

Q4: Jak útočníci obcházejí pravidla SPF?

Zneužíváním podobně vypadajících domén (typosquatting) nebo používáním kompromitovaných účtů u legitimních poštovních služeb třetích stran.

Q5: Co je kompromitace firemního e-mailu (BEC)?

Firemní podvod, při kterém útočníci ovládnou nebo napodobí firemní e-mailové účty k autorizaci podvodných plateb.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část D)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q6: Jak vícefaktorové ověřování zastavuje phishing?

Vyžaduje sekundární tokeny (například hardwarové klíče), které nelze ukrást pouze pomocí napodobených přihlašovacích stránek.

Q7: Co je stránka pro sběr přihlašovacích údajů?

Napodobený přihlašovací portál navržený k zachycování zadaných uživatelských jmen, hesel a tokenů MFA v reálném čase.

Q8: Co je únos subdomény?

Útočník ovládne nepoužívaný ukazatel subdomény DNS, aby pod důvěryhodnou nadřazenou doménou hostoval škodlivé phishingové stránky.

Q9: Jak funguje kontrola zarovnání DKIM?

Ověřuje, že doména v hlavičce 'From' odpovídá doméně, která zprávu kryptograficky podepsala v hlavičce DKIM.

Q10: Jaká je role e-mailové brány?

Filtrování příchozí pošty, kontrola odkazů, sandboxování příloh a ověřování souladu se SPF/DKIM/DMARC.

Část 11: 10 faktů a poznatků o kyberbezpečnosti z praxe

Projděte si fakta z praxe o bezpečnostních incidentech, obranných mechanismech a standardech souladu.

1. BEZPEČNOSTNÍ POSTŘEH

Phishing a spoofing byly v roce 2025 nejčastěji hlášeným typem trestné činnosti u FBI IC3 se 191 561 stížnostmi. [4]

2. BEZPEČNOSTNÍ POSTŘEH

Kompromitace firemních e-mailů (BEC) způsobila v roce 2025 ztráty přes $3 miliardy nahlášené IC3 při FBI. [4]

3. BEZPEČNOSTNÍ POSTŘEH

Homografické útoky využívají azbukou psaná podobná písmena k vizuálnímu napodobení exact-match domén značek v prohlížečích.

4. BEZPEČNOSTNÍ POSTŘEH

S 'p=reject' doména žádá příjemce, aby nevyhovující poštu odmítli už při doručení, nikoli ji zařadili jako spam. [2]

5. BEZPEČNOSTNÍ POSTŘEH

Whalingové útoky cílené na ředitele běžně požadují urgentní platby za důvěrné fúze nebo nákupy domén.

6. BEZPEČNOSTNÍ POSTŘEH

Portály pro sběr přihlašovacích údajů kopírují skutečné přihlašovací stránky, takže oběti zadávají hesla přímo do útočníkova formuláře.

7. POSTŘEH K BEZPEČNOSTI

Společné pokyny CISA k phishingu doporučují školení uživatelů spolu s DMARC, SPF, DKIM a MFA odolnou proti phishingu. [3]

8. POSTŘEH K BEZPEČNOSTI

Vyhodnocení SPF je omezeno na 10 členů vyžadujících DNS dotaz; překročení limitu vrací výsledek 'permerror'. [1]

9. POSTŘEH K BEZPEČNOSTI

Hardwarové bezpečnostní klíče FIDO2 poskytují kryptograficky podloženou ochranu před vzdáleným vylákáním přihlašovacích údajů.

10. BEZPEČNOSTNÍ POSTŘEH

Phishing je jedním z nejběžnějších způsobů, jak se útočníci poprvé dostanou do organizace, a proto je pravidelné školení povědomí účinnou obranou.

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních standardů NIST, OWASP a předpisů o ochraně osobních údajů.

AKADEMICKÉ A OBOROVÉ REFERENCE

[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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co je spear phishing? → Cílený phishingový e-mail šitý na míru konkrétní osobě nebo organizaci

2 Otázka 2 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

SPF zveřejňuje autorizované odesílací servery domény v DNS, takže příjemci mohou zkontrolovat odesílatele obálky.

3 Otázka 3 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co je whalingový útok? → Phishingová kampaň cílená konkrétně na vysoce postavené firemní manažery

4 Otázka 4 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co dělá DKIM? → Přidává k e-mailům kryptografický podpis k ověření pravosti odesílatele

5 Otázka 5 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaká je role DMARC? → Určuje přijímajícím poštovním serverům, jak nakládat s neúspěšnými kontrolami SPF/DKIM

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: spear phishing je šitý na míru konkrétním lidem, na rozdíl od generického hromadného phishingu.

7 **Otázka 7** **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Zásady DMARC mohou poštovním serverům nařídit odmítnutí neautorizovaných podvržených zpráv.

8 **Otázka 8** **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: SPF kontroluje odesílací IP proti DNS; kryptografický podpis ověřuje DKIM.

9 **Otázka 9** **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: whaling cílí na vrcholové manažery, kteří mohou schvalovat platby a mají přístup k citlivým datům.

10 **Otázka 10** **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Pravda: potvrzování platebních žádostí přes samostatný, známý kanál pomáhá zastavit podvody s převody.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

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

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

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

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

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

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy SPEAR, SPOOFING a SPF a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

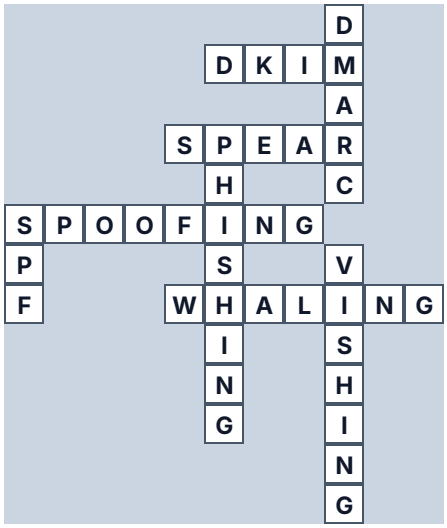
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

Z	R	Y	Ě	Q	M	Č	S	Š	I	Ě	O	S	N	R
Y	R	Ó	Č	U	T	Ť	P	V	E	L	Í	B	A	B
C	P	M	Y	L	J	Y	E	L	I	Y	U	K	Ď	Ř
N	J	I	D	I	O	Ň	A	K	R	S	Q	F	Ň	Ň
Ř	S	K	T	U	S	Ť	R	F	C	D	H	T	R	Ó
G	H	D	Š	B	P	V	P	D	T	Z	M	I	Ů	C
N	Ž	V	Ě	K	O	G	Ž	H	D	Ň	Ď	A	N	Ř
I	X	Q	C	Ú	O	B	A	Ž	I	O	D	L	R	G
L	A	Ď	Ó	Ď	F	É	G	I	D	S	S	Ř	N	C
A	E	I	Š	Ž	I	T	É	Ř	Ů	E	H	A	Á	Ř
H	P	O	Q	U	N	Y	R	J	S	U	Š	I	Č	Ň
W	Ý	B	Ě	Š	G	X	W	Í	F	A	S	Ž	N	Ý
Ý	L	F	I	N	S	J	N	P	M	Ť	P	G	R	G
Ř	G	Ž	Á	Ó	Ů	Ě	S	Ú	C	Ý	Š	Ý	B	G
M	Ž	F	J	Ó	Q	O	X	C	N	Ž	Z	Ě	Ý	P

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: DKIM Kryptografický podpis v e-mailu. (4 písmen)

3 vodorovně: SPEAR Personalizovaný cílený e-mail. (5 písmen)

5 vodorovně: SPOOFING Falšování adresy odesílatele e-mailu. (8 písmen)

7 vodorovně: WHALING Cílení na vrcholové manažery. (7 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: DMARC Politika s pokyny k odmítnutí. (5 písmen)

4 svisle: PHISHING E-mail sociálního inženýrství. (8 písmen)

5 svisle: SPF Autorizované IP odesílatelů v DNS. (3 písmen)

6 svisle: VISHING Podvodné hlasové hovory. (7 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1. AESRP — SPEAR
2. FPS — SPF
3. ADCRM — DMARC
4. SNGIHPHI — PHISHING
5. FIPGOSNO — SPOOFING
6. IMDK — DKIM
7. WNIGHLA — WHALING
8. IHGVNIS — VISHING

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"SOCIÁLNÍ INŽENÝRSTVÍ ODHALÍ AUDIT EMAILOVÉ BRÁNY"

Klíč k případovým studiím

A Případová studie 1: Náprava whalingového útoku na vedení firmy

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Finanční ředitel obdrží vysoce personalizovaný e-mail, který se vydává za zprávu od CEO a žádá rychlé odeslání $50,000 bankovním převodem k uzavření důvěrného nákupu domény.
- Doporučená strategie a řešení: Nakonfigurujte DMARC s politikou 'p=reject', která blokuje podvržené domény odesílatelů. Přidejte na bráně varovné bannery pro externí odesílatele a vyžadujte ústní out-of-band potvrzení všech finančních transakcí.

B Případová studie 2: Nasazení politik brány SPF/DKIM/DMARC

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Podnik neprochází bezpečnostními audity, protože odchozí marketingové e-maily jsou často označovány jako spam a hackeři aktivně spoofují doménu firemní značky.
- Doporučená strategie a řešení: Publikujte TXT záznam pro SPF s výčtem autorizovaných odesílacích IP. Nastavte podpisové klíče DKIM na odchozích poštovních serverech a analyzujte příchozí XML zpětné reporty DMARC k odhalení zneužití.