Jméno: _____ Datum: _____ Body: _____

Online podvody a sociální inženýrství Průvodce ochranou

E-mailový phishing, podvržené domény, vishing, podvody s podporou, ověřování mimo hlavní kanál, BEC

PŘEHLED VÝUKY: ONLINE PODVODY

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 obranou proti online podvodům. Prozkoumáte falešné phishingové weby, taktiky sociálního inženýrství, podvody s podporou, vektory podvodných převodů a metody ověřování plateb.

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/online-podvody/

Váš studijní plán: ochrana před online podvody

- Určete běžné indikátory podvodů technické podpory a typosquattingových domén.
- Zavést protokoly ověřování e-mailů (SPF, DKIM, DMARC) proti spoofingu.
- Zaveďte ověřování transakcí mimo hlavní kanál k prevenci firemních podvodů s převody.

POKYNY K PRŮVODCI ONLINE PODVODY

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 ochranu před online podvody. Zakončete bonusovou aktivitou Mysli rychle.

OCHRANA PŘED ONLINE PODVODY A SOCIÁLNÍM INŽENÝRSTVÍM (ÚVOD)

Online podvody zneužívají lidské chování prostřednictvím phishingu, podvodných vyskakovacích oken podpory, vishingu a podvodných bankovních převodů. Vynucení ověřování transakcí mimo hlavní kanál a doménových pravidel SPF/DKIM/DMARC pomáhá blokovat vektory sociálního inženýrství už na bráně.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. Jaký je hlavní indikátor podvodu s technickou podporou?

- A. Vyskakovací okno tvrdící, že váš systém je infikován, a požadující, abyste zavolali na telefonní číslo
- B. Automatická bezpečnostní aktualizace stažená z oficiálního registru
- C. Správce hesel odmítající vyplnit přihlašovací údaje na firemní doméně
- D. Záloha souborů běžící na pozadí na externím disku

2. Jaká technika používá podvržené domény odesílatele ke krádeži bankovních údajů?

- A. E-mailový phishing
- B. Skenování portů
- C. Injekce do paměti
- D. Kryptografické skartování

3. Co představuje podvod s bankovním převodem?

- A. Oklamání obětí pomocí sociálního inženýrství, aby poslaly peníze na falešné firemní účty
- B. Šifrování systémových databází pomocí ransomwarových payloadů
- C. Dotazování databází pomocí příkazů SQL injection
- D. Zálohování systémových souborů na offline disky

4. Proč podvodníci vytvářejí falešné nákupní weby?

- A. Ukrást kupujícím údaje o kreditních kartách a platební přihlašovací údaje
- B. Hostovat databázové tabulky sandboxované analýzy malwaru
- C. Zrychlit doručování online objednávek
- D. Zdarma testovat nové designy webu

5. Co znamená vishing?

- A. Hlasové phishingové podvody přes telefonní sítě ke krádeži přihlašovacích údajů
- B. Skenování místních sítí kvůli nezabezpečeným zařízením
- C. Obnovení systémových databází po neoprávněném narušení
- D. Spouštění nedůvěryhodného kódu v zabezpečených virtuálních kontejnerech

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Phishingové podvody cílí pouze na koncové uživatele, nikdy na vedoucí pracovníky (whaling).

- ○ Pravda
- ○ Nepravda

7 Otázka 7

7. Podvržené domény často používají drobné překlepy (jako amaz0n.com), aby napodobily důvěryhodné značky.

- ○ Pravda
- ○ Nepravda

8 Otázka 8

8. Podvody s technickou podporou lze vyřešit udělením vzdáleného přístupu volajícímu.

- ○ Pravda
- ○ Nepravda

9 Otázka 9

9. Sociální inženýrství zneužívá lidskou psychologii, jako je strach a naléhavost, k obcházení bezpečnostních pravidel.

- ○ Pravda
- ○ Nepravda

10 Otázka 10

10. Žádosti o bankovní převod by měly být vždy ověřeny jiným komunikačním kanálem (out-of-band).

- ○ Pravda
- ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Podvodné e-maily klamající uživatele se souhrnně označují jako _____ .
2. Když webová stránka napodobuje důvěryhodnou značku, je její doménové jméno _____ .
3. Hlasové podvody cílící na bankovní údaje se nazývají _____ .
4. Vyskakovací okno požadující platbu za odstranění viru je typický _____ s technickou podporou.
5. Potvrzení platebního požadavku jiným komunikačním kanálem se označuje jako mimopásmové _____ .
6. Zloději přesměrovávají obchodní platby tak, že napadnou _____ .

ZÁSOBNÍK SLOV

BANKOVNÍ PŘEVOD | OVĚŘOVÁNÍ | PHISHING | PODVOD | PODVRŽENO | SMISHING | VISHING | WHALING

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

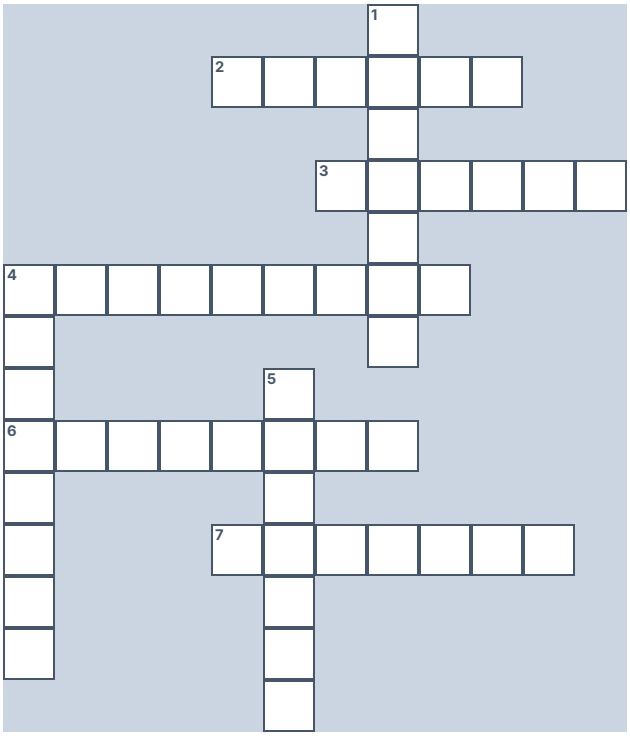
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. PHISHING	A	Podvodné přesměrování bankovních transakcí na účty zločinců.
☐	2. PODVRŽENO	B	Podvodné schéma navržené ke krádeži peněz nebo přístupových údajů obětí.
☐	3. VISHING	C	Rozesílání podvodných textových zpráv s cílem ukrást přihlašovací údaje k mobilním účtům.
☐	4. PODVOD	D	Podvodné telefonáty navržené ke krádeži přihlašovacích údajů a údajů o účtech.
☐	5. OVĚŘOVÁNÍ	E	Cílené phishingové útoky s cílem ukrást přihlašovací údaje vedoucích pracovníků C-úrovně.
☐	6. BANKOVNÍ PŘEVOD	F	Napodobený odesílatel e-mailu nebo adresa webu vytvořené tak, aby vypadaly legitimně.
☐	7. WHALING	G	Podvodné e-mailové kampaně navržené ke krádeži přihlašovacích údajů a hesel.
☐	8. SMISHING	H	Potvrzení platebních údajů důvěryhodným druhotným kontaktním kanálem.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

2. Podvodné schéma navržené ke krádeži peněz nebo přístupových údajů obětí. (6)

3. Podvodné přesměrování bankovních transakcí na účty zločinců. (6)

4. Napodobená adresa odesílatele e-mailu nebo webu, která má působit legitimně. (9)

6. Rozesílání podvodných textových zpráv ke krádeži údajů mobilních účtů. (8)

7. Cílené phishingové útoky zaměřené na krádež údajů vrcholových manažerů. (7)

SVISLÉ NÁPOVĚDY

1. Potvrzení platebních údajů pomocí důvěryhodného druhého kontaktního kanálu. (7)

4. Podvodné e-mailové kampaně navržené ke krádeži přihlašovacích údajů a hesel. (8)

5. Podvodné hlasové hovory navržené ke krádeži přihlašovacích údajů a detailů účtů. (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: Podvodné schéma navržené ke krádeži peněz nebo přístupových údajů obětí. (6 písmen):

3 vodorovně: Podvodné přesměrování bankovních transakcí na účty zločinců. (6 písmen):

4 vodorovně: Napodobená adresa odesílatele e-mailu nebo webu, která má působit legitimně. (9 písmen):

6 vodorovně: Rozesílání podvodných textových zpráv ke krádeži údajů mobilních účtů. (8 písmen):

7 vodorovně: Cílené phishingové útoky zaměřené na krádež údajů vrcholových manažerů. (7 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Potvrzení platebních údajů pomocí důvěryhodného druhého kontaktního kanálu. (7 písmen):

4 svisle: Podvodné e-mailové kampaně navržené ke krádeži přihlašovacích údajů a hesel. (8 písmen):

5 svisle: Podvodné hlasové hovory navržené ke krádeži přihlašovacích údajů a detailů účtů. (7 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

PHISHING, PODVRŽENÝ, VISHING, PODVOD, OVĚŘENÍ, PŘEVOD, WHALING, SMISHING

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

- **A. PHISHING**
- **B. PODVRŽENÝ**
- **C. VISHING**
- **D. PODVOD**
- **E. OVĚŘENÍ**
- **F. PŘEVOD**
- **G. WHALING**
- **H. SMISHING**

DEFINICE A POLE K PŘIŘAZENÍ

1. Napodobená adresa odesílatele e-mailu nebo webu, která má působit legitimně.
2. Potvrzení platebních údajů pomocí důvěryhodného druhého kontaktního kanálu.
3. Podvodné přesměrování bankovních transakcí na účty zločinců.
4. Rozesílání podvodných textových zpráv ke krádeži údajů mobilních účtů.
5. Cílené phishingové útoky zaměřené na krádež údajů vrcholových manažerů.
6. Podvodné hlasové hovory navržené ke krádeži přihlašovacích údajů a detailů účtů.
7. Podvodné e-mailové kampaně navržené ke krádeži přihlašovacích údajů a hesel.
8. Podvodné schéma navržené ke krádeži peněz nebo přístupových údajů obětí.

Kontrolní bod 7: Výzva s přeházenými slovy

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

1. **NSHPIHGI** _____
2. **VSGNIHI** _____
3. **ŘOEÍĚNV** _____
4. **GHILNWA** _____
5. **EROÝŽVPND** _____
6. **OVPDDO** _____
7. **OPVDEŘ** _____
8. **SMHGSNII** _____

Bonusová aktivita: Mysli rychle

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

1	Zařízení, která lze hacknout			
2	Fráze, které podvodníci často používají			
3	Platební metody, které podvodníci požadují			
4	Typy online podvodů			
5	Nabídky, které jsou příliš dobré na to, aby byly pravdivé			
6	Místa, kde nahlásit podvod			
7	Slova související s kyberbezpečností			
8	Lidé, které můžete před podvody varovat			
9	Věci, které si zálohujete			
10	Varovné signály v e-mailu			
11	Známky toho, že je počítač nakažený			
12	Způsoby, jak prověřit e-shop			
13	Způsoby, jak chránit své účty			
14	Věci, které je třeba udělat, když vás někdo podvede			
15	Co udělat po úniku dat			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: PREVENCE PODVODŮ S FIREMNÍMI BANKOVNÍMI PŘEVODY

👷

Scénář: Finanční oddělení obdrží urgentní e-mail z podvržené dodavatelské adresy s požadavkem, aby budoucí fakturační převody směřovaly na nové směrovací číslo.

Otázka k diskusi: Popište politiku ověřování proti podvodným převodům a určete blokace založené na ověřování e-mailů.

PŘÍPADOVÁ STUDIE 2: WHALINGOVÝ PHISHING NA VEDENÍ FIRMY

👷

Scénář: Vedoucí pracovník klikl na phishingový odkaz, který údajně obsahoval zabezpečený dokument ze schůze představenstva, a zadal své primární firemní přihlašovací údaje na podvrženém portálu.

Otázka k diskusi: Popište kroky reakce na incident a vysvětlete, jak auditovat přihlášení vedení.

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

22 6 13 1 18 30 8 24 13 14 28 13 14 20 12

24 22 19 22 4 15 22 35 10 27 22 35 2 20 15 1

17 22 20 30 26 22 18 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 online podvod?

Podvodné schéma využívající digitální kanály k oklamání obětí, aby poslaly peníze nebo vydaly osobní přihlašovací údaje.

Q2: Jaký je hlavní indikátor e-mailového phishingu?

Zpráva tvrdící naléhavost (například pozastavení účtu) a směrující vás na odkaz, který neodpovídá oficiální doméně.

Q3: Co je typosquatting?

Registrace domén s běžnými překlepy populárních značek (jako amaz0n.com) pro hostování falešných phishingových webů.

Q4: Co je podvod s technickou podporou?

Vyskakovací okno tvrdící, že váš počítač je infikován, které vás vyzývá zavolat na číslo a zaplatit za falešný čisticí software nebo služby vzdáleného přístupu. [1]

Q5: Co je vishing?

Phishingové útoky využívající hlasové telefonáty k vylákání údajů o bankovním účtu nebo přihlašovacích údajů od obětí.

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

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Co znamená wire fraud (podvod s bankovním převodem)?

Přesměrování platebních transakcí na podvodné účty vydáváním se za dodavatele nebo vedení firmy.

Q7: Co je whaling?

Vysoce cílená forma spear phishingu mířící přímo na cíle s vysokou hodnotou, jako jsou vrcholoví manažeři.

Q8: Co je smishing?

Podvodné textové zprávy zasílané na mobilní zařízení s odkazy na falešné portály nebo aktualizace sledování zásilek.

Q9: Proč je out-of-band ověření klíčové?

Potvrzuje podrobnosti transakce pomocí odděleného komunikačního kanálu (například telefonátu), čímž se vyhýbá kompromitovaným e-mailovým vláknům.

Q10: Jak funguje podvod s falešnou úschovou (escrow)?

Podvodníci vytvoří falešný web úschovy (escrow), tvrdí, že prostředky jsou bezpečně drženy, a poté ukradnou zálohu kupujícího zaslanou převodem.

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

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

Q1: Jak podvodníci používají BEC (kompromitaci firemního e-mailu) k podvodným bankovním převodům?

Ovládnou e-mailový účet legitimního zaměstnance, sledují vlákna s fakturami a rozešlou aktualizované platební údaje s podvodnými bankovními účty.

Q2: Jaké je riziko homografických útoků IDN u online podvodů?

Použití znaků mimo ASCII, které vypadají stejně jako běžná písmena (např. cyrilské 'a'), k registraci podvržených domén napodobujících skutečné značky.

Q3: Proč je kontrola hlaviček e-mailů důležitá při odhalování podvodů?

Odhaluje skutečnou IP původního serveru a stav validace SPF/DKIM a ukazuje, zda je doména odesílatele padělaná.

Q4: Jak podvodníci s podporou zneužívají software pro vzdálenou plochu?

Používají nástroje jako AnyDesk nebo TeamViewer, aby se připojili k zařízení oběti, nasadili malware a ukradli uložená hesla.

Q5: Jaký je cíl podvodů se zálohovou platbou?

Vylákání záloh na poplatky za zpracování výměnou za velkou finanční odměnu, která neexistuje.

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

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

Q6: Jak podvodníci využívají profilování na sociálních sítích k cílenému phishingu?

Sestavují organizační struktury firem a jména zaměstnanců k tvorbě přesvědčivých spear-phishingových e-mailů.

Q7: Proč falešné e-shopy nabízejí extrémní slevy?

Aby kupující nalákali k zadání údajů o platební kartě a získali údaje k dalšímu použití nebo prodeji na carderských fórech.

Q8: Jak záznamy DMARC blokují phishingové podvody?

DMARC umožňuje vlastníkům domén požádat přijímající servery, aby poštu, která neprojde sladěnými kontrolami SPF a DKIM, daly do karantény nebo odmítly, čímž blokuje přímé podvržení. [5]

Q9: Jaká je hrozba portálů pro sběr přihlašovacích údajů?

Podvržené vstupní stránky navržené tak, aby vypadaly přesně jako Microsoft 365 nebo Google workspace, kradoucí přihlašovací údaje při jejich zadávání.

Q10: Jak bezpečnostní týmy hlásí a vypínají podvodné domény?

Předložením důkazů o podvodu na e-mail registrátora pro hlášení zneužití, hostingovému poskytovateli a do registru Google Safe Browsing.

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. [2]

2. BEZPEČNOSTNÍ POSTŘEH

Kompromitace firemních e-mailů (BEC) způsobila v roce 2025 ztráty přes $3 miliardy nahlášené IC3 při FBI. [2]

3. BEZPEČNOSTNÍ POSTŘEH

Domény s překlepy (typosquatting) se od skutečných názvů značek liší o jeden dva znaky, takže letmý pohled je může přehlédnout.

4. BEZPEČNOSTNÍ POSTŘEH

Podvody s technickou podporou způsobily ztráty přes $2.1 miliardy nahlášené centru IC3 při FBI v roce 2025. [2]

5. BEZPEČNOSTNÍ POSTŘEH

Homografické útoky vypadají v adresním řádku prohlížeče identicky, pokud prohlížeč nezobrazuje punycode.

6. BEZPEČNOSTNÍ POSTŘEH

Textové podvody přes SMS (smishing) používají krátké naléhavé zprávy s odkazy, takže oběti mají málo kontextu k odhalení podvodu.

7. POSTŘEH K BEZPEČNOSTI

Whalingové útoky cílí na e-maily vedoucích pracovníků, protože ti řídí přístup k velkým bankovním převodům plateb.

8. POSTŘEH K BEZPEČNOSTI

Ověřování změn plateb telefonátem na známé uložené číslo je klíčovou obranou proti podvodům BEC s bankovními převody.

9. POSTŘEH K BEZPEČNOSTI

Falešné escrow weby jsou běžným podvodem na online tržištích: vypadají jako bezpečná platební služba, ale ukradnou bankovní převod kupujícího.

10. BEZPEČNOSTNÍ POSTŘEH

Google Safe Browsing varuje uživatele před otevřením stránek, které označil za phishingové nebo šířící malware.

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] 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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jaký je hlavní indikátor podvodu s technickou podporou? → Vyskakovací okno tvrdící, že váš systém je infikován, a požadující, abyste zavolali na telefonní číslo

2 Otázka 2

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jaká technika používá podvržené domény odesílatele ke krádeži bankovních údajů? → E-mailový phishing

3 Otázka 3

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Co představuje podvod s bankovním převodem? → Oklamání obětí pomocí sociálního inženýrství, aby poslaly peníze na falešné firemní účty

4 Otázka 4

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Proč podvodníci vytvářejí falešné nákupní weby? → Ukrást kupujícím údaje o kreditních kartách a platební přihlašovací údaje

5 Otázka 5

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Co znamená vishing? → Hlasové phishingové podvody přes telefonní sítě ke krádeži přihlašovacích údajů

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

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

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: phishing cílí i na manažery; whaling je phishing zaměřený na vrcholové vedení.

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

POZNÁMKA PRO VYUČUJÍCÍ

Podvržené domény často používají drobné překlepy (jako amaz0n.com), aby napodobily důvěryhodné značky.

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

POZNÁMKA PRO VYUČUJÍCÍ

Nepravda: poskytnutí vzdáleného přístupu podvodné podpoře jí umožní nasadit malware a krást data.

9 **Otázka 9** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Sociální inženýrství zneužívá lidskou psychologii, jako je strach a naléhavost, k obcházení bezpečnostních pravidel.

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

POZNÁMKA PRO VYUČUJÍCÍ

Žádosti o bankovní převod by měly být vždy ověřeny jiným komunikačním kanálem (out-of-band).

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

G 1. PHISHING	F 2. PODVRŽENO	D 3. VISHING	B 4. PODVOD
H 5. OVĚŘOVÁNÍ	A 6. BANKOVNÍ PŘEVOD	E 7. WHALING	C 8. SMISHING

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 PHISHING	2 PODVRŽENO	3 VISHING	4 PODVOD
5 OVĚŘOVÁNÍ	6 BANKOVNÍ PŘEVOD		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 B – PODVRŽENÝ	2 E – OVĚŘENÍ	3 F – PŘEVOD	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – PODVOD

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy PHISHING, PODVRŽENO a VISHING a ke každému uvést příklad.

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

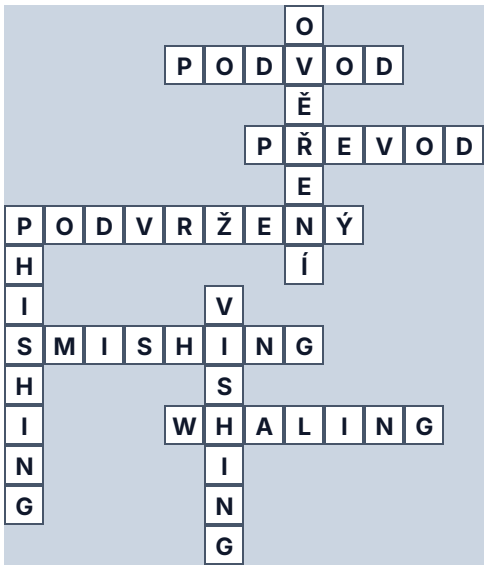
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: PODVOD Podvodné schéma navržené ke krádeži peněz nebo přístupových údajů obětí. (6 písmen)

3 vodorovně: PŘEVOD Podvodné přesměrování bankovních transakcí na účty zločinců. (6 písmen)

4 vodorovně: PODVRŽENÝ Napodobená adresa odesílatele e-mailu nebo webu, která má působit legitimně. (9 písmen)

6 vodorovně: SMISHING Rozesílání podvodných textových zpráv ke krádeži údajů mobilních účtů. (8 písmen)

7 vodorovně: WHALING Cílené phishingové útoky zaměřené na krádež údajů vrcholových manažerů. (7 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: OVĚŘENÍ Potvrzení platebních údajů pomocí důvěryhodného druhého kontaktního kanálu. (7 písmen)

4 svisle: PHISHING Podvodné e-mailové kampaně navržené ke krádeži přihlašovacích údajů a hesel. (8 písmen)

5 svisle: VISHING Podvodné hlasové hovory navržené ke krádeži přihlašovacích údajů a detailů účtů. (7 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1.	N S H P I H G I	PHISHING	5.	E R O Ý Ž V P N D	PODVRŽENÝ
2.	V S G N I H I	VISHING	6.	O V P D D O	PODVOD
3.	Ř O E Í Ě N V	OVĚŘENÍ	7.	O P V D E Ř	PŘEVOD
4.	G H I L N W A	WHALING	8.	S M H G S N I I	SMISHING

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"ODHALTE PHISHING POMOCÍ OVĚŘOVÁNÍ A KONTROLY"

Klíč k případovým studiím

A Případová studie 1: Prevence podvodů s firemními bankovními převody

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Finanční oddělení obdrží urgentní e-mail z podvržené adresy dodavatele s žádostí, aby budoucí fakturační platby směřovaly na nové číslo účtu.
- Doporučená strategie a řešení: Vynuťte politiku dvojí autorizace všech plateb. Zaveďte out-of-band ověření přes předem uložené telefonní číslo a blokujte e-maily z podvržených domén na bráně.

B Případová studie 2: Whalingový phishing na vedení firmy

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Vedoucí pracovník klikl na phishingový odkaz, který tvrdil, že vede k zabezpečenému dokumentu ze zasedání představenstva, a zadal své hlavní firemní přihlašovací údaje na podvrženém portálu.
- Doporučená strategie a řešení: Izolujte zařízení manažera. Resetujte všechny firemní relační tokeny a přihlašovací údaje. Projděte přístupové logy kvůli odlivu dat a zaveďte hardwarové MFA u všech přihlášení.