Naam: _____ Datum: _____ Score: _____

Online oplichting en social engineering Beschermingsgids

E-mailphishing, vervalste domeinen, vishing, supportoplichting, verificatie via een apart kanaal, BEC

LEEROVERZICHT ONLINE OPLICHTING

BEVEILIGD
GEGEVENSVERSLEUTELING
256-bits AES-standaard

COMPLIANT
WERELDWIJDE NORMEN
AVG- en CCPA-kaders

ZERO-TRUST
TOEGANGSBELEID
Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door online oplichtingsverdediging. Je verkent nepphishingwebsites, social-engineeringtactieken, supportoplichting, vectoren voor betalingsfraude en methoden voor betalingsverificatie.

CONTROLEPUNTEN VAN HET WERKBLAD

- [ ] **Deel 1-4: Beheers cyberbeveiliging en dreigingspreventie.**
- [ ] **Deel 5-7: Los kruiswoord- en woordzoekpuzzels op.**
- [ ] **Deel 8-9: Los casestudy's en de codeopdracht op.**
- [ ] **Deel 10: Bekijk de pagina's met veelgestelde vragen (basis en gevorderd).**
- [ ] **Deel 11: Ontdek 10 interessante feiten uit de praktijk.**
- [ ] **Bonus: Snel denken-uitdaging.**

Open de VPN.com-gids over cyberbeveiliging

URL: https://www.vpn.com/nl/cyberbeveiliging/online-oplichting/

Jouw leertraject: bescherming tegen online oplichting

- Veelvoorkomende kenmerken van oplichting via nepsupport en typosquatting-domeinen herkennen.
- Voer e-mailverificatieprotocollen (SPF, DKIM, DMARC) in tegen spoofing.
- Zet transactieverificatie via een apart kanaal op om zakelijke bankfraude te voorkomen.

INSTRUCTIES VOOR DE GIDS OVER ONLINE OPLICHTING

Beantwoord de meerkeuzevragen en de vragen waar/onwaar, vul de zinnen aan met behulp van de woordenbank, koppel de definities en los de kruiswoordpuzzel en de woordzoeker op. Pas je kennis toe op bescherming tegen oplichting op internet. Sluit af met de bonusopdracht Snel denken.

BESCHERMING TEGEN ONLINE OPLICHTING EN SOCIAL ENGINEERING (INLEIDING)

Online oplichting maakt misbruik van menselijk gedrag via phishing, pop-ups van nepsupport, vishing en oplichting met overschrijvingen. Het afdwingen van verificatie van transacties via een apart kanaal (out-of-band) en domeinregels voor SPF/DKIM/DMARC helpen social-engineeringvectoren bij de gateway te blokkeren.

LEES ELK CONTROLEPUNT ZORGVULDIG EN KIES OF SCHRIJF HET JUISTE ANTWOORD.

Controlepunt 1: Meerkeuzeopdracht

1. Wat is de belangrijkste aanwijzing voor een supportscam?

- A. Een pop-up die beweert dat je systeem is geïnfecteerd en eist dat je een telefoonnummer belt
- B. Een automatische beveiligingsupdate die van een officieel register is gedownload
- C. Een wachtwoordmanager die weigert inloggegevens in te vullen op een bedrijfsdomein
- D. Een back-up van bestanden op de achtergrond naar een externe schijf

2. Welke techniek gebruikt vervalste afzenderdomeinen om bankgegevens te stelen?

- A. E-mailphishing
- B. Poortscanning
- C. Geheugeninjectie
- D. Cryptografisch vernietigen

3. Wat staat voor overschrijvingsfraude?

- A. Slachtoffers met social engineering misleiden om geld over te maken naar nepbedrijfsrekeningen
- B. Systeemdatabases versleutelen met ransomwarepayloads
- C. Databases bevragen met SQL-injectieopdrachten
- D. Systeembestanden back-uppen naar offline opslagschijven

4. Waarom maken oplichters nepwebwinkels?

- A. Om creditcardgegevens en betalingsgegevens van kopers te stelen
- B. Om databasetabellen voor malware-analyse in een sandbox te hosten
- C. Om de levering van online bestellingen te versnellen
- D. Om nieuwe websiteontwerpen gratis te testen

5. Wat betekent vishing?

- A. Voice-phishingoplichting via telefoonnetwerken om inloggegevens te stelen
- B. Lokale netwerken scannen op onbeveiligde systeemapparaten
- C. Systeemdatabases herstellen na een ongeautoriseerde inbreuk
- D. Onbetrouwbare code uitvoeren in beveiligde virtuele containers

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Phishingoplichting richt zich alleen op eindgebruikers, nooit op whaling-doelwitten onder het topmanagement.

- ◯ Waar
- ◯ Onwaar

7 Vraag 7

7. Vervalste domeinen gebruiken vaak kleine typefouten (zoals amaz0n.com) om vertrouwde merken na te bootsen.

- ◯ Waar
- ◯ Onwaar

8 Vraag 8

8. Support-oplichting kan worden opgelost door de beller toegang op afstand te geven.

- ◯ Waar
- ◯ Onwaar

9 Vraag 9

9. Social engineering maakt misbruik van menselijke psychologie, zoals angst en urgentie, om beveiligingsregels te omzeilen.

- ◯ Waar
- ◯ Onwaar

10 Vraag 10

10. Verzoeken om overschrijvingen moeten altijd worden geverifieerd via een ander communicatiekanaal (out-of-band).

- ◯ Waar
- ◯ Onwaar

Controlepunt 3: Kernbegrippen invullen

Lees elke zin hieronder en vul de open plek in met de juiste term uit de woordenbank.

1. Frauduleuze e-mails die gebruikers misleiden, heten _____ .

2. Webadressen die vertrouwde merken nabootsen, zijn _____ .

3. Telefoonoplichting gericht op bankgegevens heet _____ .

4. Een pop-up die geld eist voor het verwijderen van virussen, is een vorm van _____ via nepsupport.

5. Het bevestigen van een betalingsverzoek vereist _____ via een ander kanaal.

6. Het omleiden van zakelijke transacties naar rekeningen van dieven is _____ .

WOORDENBANK

BETAALFRAUDE DEEPFAKE GESPOOFD OPLICHTING PHISHING
ROMANCEFRAUDE VERIFICATIE VISHING

Schrijf hier je antwoorden:

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

Controlepunt 4: Beveiligingsbegrippen koppelen

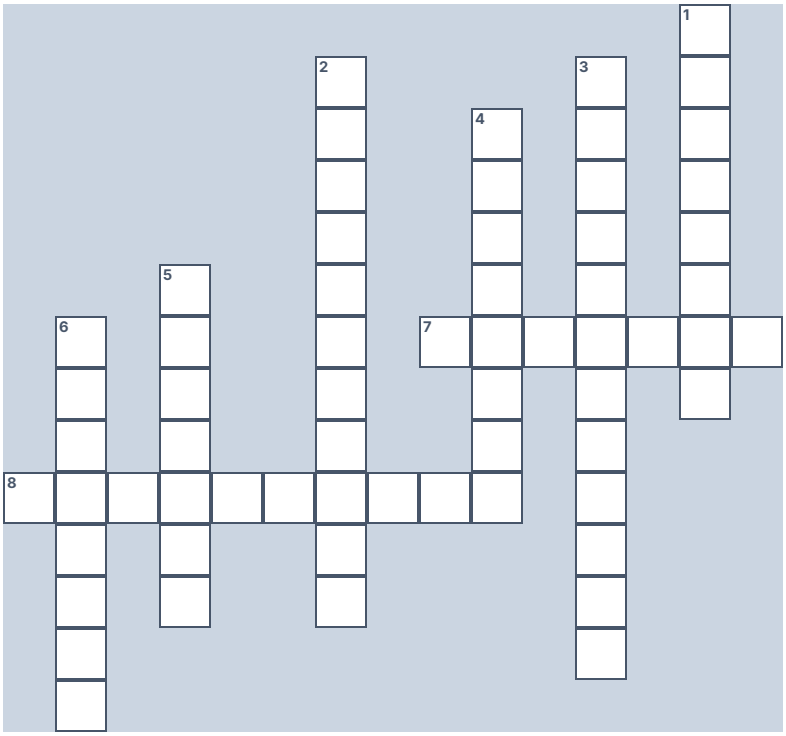
DEFINITIES KOPPELEN

Koppel elke term aan de linkerkant aan de juiste definitie aan de rechterkant door de bijbehorende letter (A-H) in het invulvak te schrijven.

☐	1. PHISHING	A	Frauduleuze omleiding van banktransacties naar criminele rekeningen.
☐	2. VERVALST	B	Frauduleus plan bedoeld om geld of inloggegevens van slachtoffers te stelen.
☐	3. VISHING	C	Oplichtende sms-berichten versturen om inloggegevens van mobiele accounts te stelen.
☐	4. OPLICHTING	D	Frauduleuze telefoongesprekken bedoeld om inloggegevens en accountgegevens te stelen.
☐	5. VERIFICATIE	E	Gerichte phishingaanvallen die erop gericht zijn inloggegevens van C-level-leidinggevenden te stelen.
☐	6. OVERSCHRIJVING	F	Nagebootst e-mailadres van de afzender of websiteadres dat er legitiem uit moet zien.
☐	7. WHALING	G	Frauduleuze e-mailcampagnes bedoeld om inloggegevens en wachtwoorden te stelen.
☐	8. SMISHING	H	Betalingsgegevens bevestigen via een vertrouwde tweede contactmethode.

Controlepunt 5: Kruiswoordpuzzel

Los de kruiswoordpuzzel op door letters in de actieve witte vakjes te typen. De nummers komen overeen met de aanwijzingen hieronder.



HORIZONTAAL

7. Gerichte phishingaanvallen om inloggegevens van C-level-leidinggevenden te stelen. (7)

8. Frauduleuze constructie om geld of toegangsgegevens van slachtoffers te stelen. (10)

VERTICAAL

1. Oplichtings-sms'jes versturen om mobiele accountgegevens te stelen. (8)

2. Betalingsgegevens bevestigen via een vertrouwde tweede contactmethode. (11)

3. Frauduleuze omleiding van banktransacties naar rekeningen van criminelen. (12)

4. Frauduleuze e-mailcampagnes om inloggegevens en wachtwoorden te stelen. (8)

5. Frauduleuze telefoongesprekken om inloggegevens en accountgegevens te stelen. (7)

6. Nagebootst e-mailadres van de afzender of websiteadres dat er legitiem uit moet zien. (8)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

Gebruikers van schermlezers en toetsenborden kunnen de antwoorden van de kruiswoordpuzzel rechtstreeks typen in de tekstvelden hieronder.

HORIZONTAAL

7 horizontaal: Gerichte phishingaanvallen om inloggegevens van C-level-leidinggevenden te stelen. (7 letters):

8 horizontaal: Frauduleuze constructie om geld of toegangsgegevens van slachtoffers te stelen. (10 letters):

VERTICAAL

1 verticaal: Oplichtings-sms'jes versturen om mobiele accountgegevens te stelen. (8 letters):

2 verticaal: Betalingsgegevens bevestigen via een vertrouwde tweede contactmethode. (11 letters):

3 verticaal: Frauduleuze omleiding van banktransacties naar rekeningen van criminelen. (12 letters):

4 verticaal: Frauduleuze e-mailcampagnes om inloggegevens en wachtwoorden te stelen. (8 letters):

5 verticaal: Frauduleuze telefoongesprekken om inloggegevens en accountgegevens te stelen. (7 letters):

6 verticaal: Nagebootst e-mailadres van de afzender of websiteadres dat er legitiem uit moet zien. (8 letters):

Controlepunt 6: Verborgen woorden zoeken

Zoek de 8 belangrijkste vakwoorden die in het onderstaande rooster verborgen zijn. Woorden kunnen horizontaal, verticaal of diagonaal staan.

V I S H I N G P S Z V C Z W F

E G K H Z D N H D Q G X P C U

I N B A Z N D I K A E D O D F

T I H I D R Q S M E S I R Z S

A H F Q V F A H A Q P O N O P

C S T X Q K R I U S O D N P Y

I I B F S X W N J A O R Z L Y

F M Y L G I M G R J F M L I T

I S O H Q Q H Z A O D V G C U

R B Y R Y B H L Z G J O P H N

E B E T A A L F R A U D E T W

V C M Z Y G Y O W U K V P I B

N V W H A L I N G T M G V N D

Y U K R B X Z Y M R Q X I G P

D A D J Q V W W L J H T H G B

WOORDENLIJST

PHISHING GESPOOFD VISHING OPLICHTING VERIFICATIE BETAALFRAUDE WHALING SMISHING

Controlepunt 6, alternatief: Toegankelijk woordenschat koppelen

Koppel elk van de 8 vaktermen uit de woordzoeker aan de juiste definitie door de letter (A-H) in de lege ruimte te schrijven.

BEGRIPPEN
A. PHISHING
B. GESPOOFD
C. VISHING
D. OPLICHTING
E. VERIFICATIE
F. BETAALFRAUDE
G. WHALING
H. SMISHING

DEFINITIES EN KOPPELVELDEN

_____ 1. Nagebootst e-mailadres van de afzender of websiteadres dat er legitiem uit moet zien.

_____ 2. Betalingsgegevens bevestigen via een vertrouwde tweede contactmethode.

_____ 3. Frauduleuze omleiding van banktransacties naar rekeningen van criminelen.

_____ 4. Oplichtings-sms'jes versturen om mobiele accountgegevens te stelen.

_____ 5. Gerichte phishingaanvallen om inloggegevens van C-level-leidinggevenden te stelen.

_____ 6. Frauduleuze telefoongesprekken om inloggegevens en accountgegevens te stelen.

_____ 7. Frauduleuze e-mailcampagnes om inloggegevens en wachtwoorden te stelen.

_____ 8. Frauduleuze constructie om geld of toegangsgegevens van slachtoffers te stelen.

Controlepunt 7: Opdracht met door elkaar gehaalde woorden

Ontcijfer de letters hieronder om kernbegrippen van cyberbeveiliging te onthullen. Schrijf je antwoorden in de invulvelden.

1. NSHPIHGI
2. VSGNIHI
3. VCIAREIEFTI
4. GHILNWA
5. OOEDPGFS
6. NCITIOPHGL
7. RAABEFEUDTLA
8. SMHGSNII

Bonusopdracht: Snel denken

3 ANTWOORDEN PER CATEGORIE. WIE DE LIJST ALS EERSTE INVULT, WINT.

1	Apparaten die gehackt kunnen worden			
2	Zinnen die oplichters vaak gebruiken			
3	Betaalmethoden waar oplichters om vragen			
4	Soorten online oplichting			
5	Aanbiedingen die te mooi zijn om waar te zijn			
6	Plekken om oplichting te melden			
7	Woorden die met cyberbeveiliging te maken hebben			
8	Mensen die je kunt waarschuwen voor oplichting			
9	Dingen waarvan je een back-up maakt			
10	Waarschuwingssignalen in een e-mail			
11	Tekenen dat een computer is geïnfecteerd			
12	Manieren om een webwinkel te controleren			
13	Manieren om je accounts te beschermen			
14	Dingen die je doet als je bent opgelicht			
15	Dingen die je doet na een datalek			

Controlepunt 8: Casestudy's cyberbeveiliging

Pas de concepten die je hebt geleerd toe om de onderstaande praktijkscenario's op te lossen.

CASESTUDY 1: PREVENTIE VAN OPLICHTING MET ZAKELIJKE OVERSCHRIJVINGEN

👨‍💻

Scenario: Een financiële afdeling ontvangt een dringende e-mail van een vervalst leveranciersadres met het verzoek om toekomstige factuurbetalingen naar een nieuw rekeningnummer te laten gaan.

Discussievraag: Schets het beleid voor verificatie van betalingsfraude en geef de blokkades voor e-mailauthenticatie aan.

CASESTUDY 2: WHALING-PHISHINGINCIDENT BIJ EEN DIRECTIELID

👨‍💻

Scenario: Een bestuurder klikte op een phishinglink die beweerde een beveiligd document voor een bestuursvergadering te bevatten en voerde zijn primaire zakelijke inloggegevens in op een vervalst portaal.

Discussievraag: Beschrijf in detail de stappen voor incidentrespons en leg uit hoe je de logins van bestuurders controleert.

Controlepunt 9: De code ontcijferen

Een cyberbeveiligingsprofessional beschermt netwerkmiddelen tegen online bedreigers. Gebruik de onderstaande letter-naar-cijfersleutel om het bericht te ontcijferen door de bijbehorende letters in de lege vakjes te schrijven.

LETTER-NAAR-CIJFER-VERSLEUTELINGSSLEUTEL

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

4	5	20	5	3	20	5	5	18		16	8	9	19	8	9	14	7

13	5	20

19	3	1	14	14	5	18	22	5	18	9	6	9	3	1	20	9	5

Ontcijferd bericht:

TIP: ELK GETAL STAAT VOOR DE POSITIE VAN DIE LETTER IN HET ALFABET (BIJV. 1 = A, 2 = B, 26 = Z).

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel A)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q1: Wat is online oplichting?

Een frauduleuze opzet die digitale kanalen gebruikt om slachtoffers te misleiden geld over te maken of persoonlijke inloggegevens prijs te geven.

Q2: Wat is de belangrijkste aanwijzing voor phishing via e-mail?

Een bericht dat urgentie claimt (zoals opschorting van je account) en je naar een link stuurt die niet overeenkomt met het officiële domein.

Q3: Wat is typosquatting?

Domeinen registreren met veelgemaakte typefouten van populaire merken (zoals amaz0n.com) om nepphishingsites te hosten.

Q4: Wat is een supportscam?

Een pop-up die beweert dat je pc besmet is en je aanzet een nummer te bellen en te betalen voor nep-opruimsoftware of diensten voor toegang op afstand. [1]

Q5: Wat is vishing?

Phishingaanvallen via telefoongesprekken om slachtoffers te laten doorgeven wat hun bankrekening- of inloggegevens zijn.

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel B)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q6: Wat betekent telefraude (wire fraud)?

Het omleiden van betalingstransacties naar oplichtersrekeningen door zich voor te doen als leveranciers of directieleden.

Q7: Wat is whaling?

Een zeer gerichte vorm van spearphishing die zich direct richt op doelwitten met hoge waarde, zoals C-level-managers van bedrijven.

Q8: Wat is smishing?

Oplichterssms'jes die naar mobiele apparaten worden gestuurd en links bevatten naar nepportalen of trackingupdates.

Q9: Waarom is out-of-band-verificatie cruciaal?

Het bevestigt transactiegegevens via een apart communicatiekanaal (zoals een telefoongesprek), zodat gecompromitteerde e-mailconversaties worden vermeden.

Q10: Hoe werkt oplichting met een nep-escrow?

Oplichters maken een vervalste escrowsite (derdenrekening) en beweren dat het geld veilig wordt vastgehouden, om vervolgens de overgemaakte storting van de koper te stelen.

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel C)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe gebruiken oplichters BEC (Business Email Compromise) om overschrijvingsfraude te plegen?

Ze kapen het e-mailaccount van een legitieme werknemer, volgen factuurgesprekken en sturen bijgewerkte factuurgegevens met oplichtersbankrekeningen.

Q2: Wat is het risico van IDN-homograafaanvallen bij online oplichting?

Niet-ASCII-tekens gebruiken die er hetzelfde uitzien als gewone letters (bijvoorbeeld het Cyrillische 'a') om vervalste domeinen te registreren die echte merken nabootsen.

Q3: Waarom is het controleren van e-mailheaders belangrijk bij het herkennen van oplichting?

Het toont het werkelijke IP-adres van de oorspronkelijke server en de SPF-/DKIM-validatiestatus, waaruit blijkt of het domein van de afzender vervalst is.

Q4: Hoe misbruiken oplichters van nepsupport software voor extern bureaublad?

Ze gebruiken hulpprogramma's zoals AnyDesk of TeamViewer om verbinding te maken met het apparaat van het slachtoffer, malware te plaatsen en opgeslagen wachtwoorden te stelen.

Q5: Wat is het doel van voorschotfraude?

Slachtoffers ertoe verleiden vooraf verwerkingskosten te betalen in ruil voor een grote financiële beloning die niet bestaat.

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel D)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Hoe gebruiken oplichters profilering via sociale media voor gerichte phishing?

Ze stellen organisatiestructuren en werknemersnamen van bedrijven samen om overtuigende spearphishing-e-mails op te stellen.

Q7: Waarom bieden nepwebwinkels forse kortingen aan?

Om kopers te verleiden hun creditcardgegevens in te voeren, zodat inloggegevens worden buitgemaakt voor hergebruik of verkoop op carding-forums.

Q8: Hoe blokkeren DMARC-records phishingoplichting?

Met DMARC kunnen domeineigenaren ontvangers vragen e-mail die niet door uitgelijnde SPF- en DKIM-controles komt in quarantaine te plaatsen of te weigeren, waardoor directe spoofing wordt geblokkeerd. [5]

Q9: Wat is de dreiging van portalen voor het verzamelen van inloggegevens?

Vervalste landingspagina's die er precies uitzien als Microsoft 365- of Google-werkruimtes en inloggegevens stelen terwijl ze worden ingevoerd.

Q10: Hoe melden beveiligingsteams oplichtingsdomeinen en schakelen ze die uit?

Door bewijs van fraude in te dienen bij het misbruik-e-mailadres van de registrar, de hostingprovider en het Google Safe Browsing-register.

Deel 11: 10 cyberbeveiligingsfeiten en inzichten uit de praktijk

Bekijk feiten uit de praktijk over beveiligingsincidenten, verdedigingsmechanismen en compliancenormen.

1. BEVEILIGINGSINZICHT

Phishing en spoofing waren in 2025 het vaakst gemelde misdrijftype bij de IC3 van de FBI, met 191,561 klachten. [2]

2. BEVEILIGINGSINZICHT

Business Email Compromise (BEC) veroorzaakte in 2025 meer dan $3 miljard aan verliezen die bij de IC3 van de FBI zijn gemeld. [2]

3. BEVEILIGINGSINZICHT

Typosquatting-domeinen verschillen een of twee tekens van echte merknamen, dus je kunt ze bij een vluchtige blik missen.

4. BEVEILIGINGSINZICHT

Oplichting via technische support veroorzaakte in 2025 meer dan $2.1 miljard aan verliezen die bij de IC3 van de FBI zijn gemeld. [2]

5. BEVEILIGINGSINZICHT

Homografische aanvallen zien er in de adresbalk van de browser identiek uit, tenzij de browser punycode-weergaven toont.

6. BEVEILIGINGSINZICHT

Sms-oplichting (smishing) maakt gebruik van korte, dringende berichten met links, waardoor slachtoffers weinig context hebben om fraude te herkennen.

7. BEVEILIGINGSINZICHT

Whaling-aanvallen richten zich op e-mailadressen van leidinggevenden, omdat zij toegang hebben tot grote bankoverschrijvingen.

8. BEVEILIGINGSINZICHT

Betalingswijzigingen verifiëren door een bekend, opgeslagen telefoonnummer te bellen is een belangrijke verdediging tegen BEC-betalingsfraude.

9. BEVEILIGINGSINZICHT

Nep-escrowwebsites (derdenrekening) zijn een veelvoorkomende vorm van oplichting op online marktplaatsen: ze lijken op een veilige betaaldienst maar stelen de overschrijving van de koper.

10. BEVEILIGINGSINZICHT

Google Safe Browsing waarschuwt gebruikers voordat ze sites openen die als phishing- of malwaresite zijn gemarkeerd.

Technische referenties en bronnen

De studiegids en de interactieve puzzels zijn samengesteld uit wereldwijde NIST- en OWASP-standaarden en standaarden voor naleving van gegevensprivacy.

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[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

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 Vraag 1

Juist antwoord: A

DOCENTENNOTITIE

Wat is de belangrijkste aanwijzing voor een supportscam? → Een pop-up die beweert dat je systeem is geïnfecteerd en eist dat je een telefoonnummer belt

2 Vraag 2

Juist antwoord: A

DOCENTENNOTITIE

Welke techniek gebruikt vervalste afzenderdomeinen om bankgegevens te stelen? → E-mailphishing

3 Vraag 3

Juist antwoord: A

DOCENTENNOTITIE

Wat staat voor overschrijvingsfraude? → Slachtoffers met social engineering misleiden om geld over te maken naar nepbedrijfsrekeningen

4 Vraag 4

Juist antwoord: A

DOCENTENNOTITIE

Waarom maken oplichters nepwebwinkels? → Om creditcardgegevens en betalingsgegevens van kopers te stelen

5 Vraag 5

Juist antwoord: A

DOCENTENNOTITIE

Wat betekent vishing? → Voice-phishingoplichting via telefoonnetwerken om inloggegevens te stelen

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 Vraag 6

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: phishing richt zich ook op bestuurders; whaling is phishing gericht op hoge leidinggevenden.

7 Vraag 7

Juist antwoord: Waar

DOCENTENNOTITIE

Vervalste domeinen gebruiken vaak kleine typefouten (zoals amaz0n.com) om vertrouwde merken na te bootsen.

8 Vraag 8

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: als je een oplichter van een helpdesk toegang op afstand geeft, kan die malware plaatsen en gegevens stelen.

9 Vraag 9

Juist antwoord: Waar

DOCENTENNOTITIE

Social engineering maakt misbruik van menselijke psychologie, zoals angst en urgentie, om beveiligingsregels te omzeilen.

10 Vraag 10

Juist antwoord: Waar

DOCENTENNOTITIE

Verzoeken om overschrijvingen moeten altijd worden geverifieerd via een ander communicatiekanaal (out-of-band).

Woordenlijstsleutels en beoordelingsrubriek

Beoordelingsrubriek voor docenten: Geef 1 punt voor elke juiste koppeling (totaal 8 punten) en elk juist contextbegrip (totaal 6 punten).

CONTROLEPUNT 4: ANTWOORDEN BEGRIPPEN KOPPELEN

G 1. PHISHING	F 2. VERVALST	D 3. VISHING	B 4. OPLICHTING
H 5. VERIFICATIE	A 6. OVERSCHRIJVING	E 7. WHALING	C 8. SMISHING

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 PHISHING	2 GESPOOFD	3 VISHING	4 OPLICHTING
5 VERIFICATIE	6 BETAALFRAUDE		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 B – GESPOOFD	2 E – VERIFICATIE	3 F – BETAALFRAUDE	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – OPLICHTING

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen PHISHING, VERVALST en VISHING in eigen woorden kunnen uitleggen en van elk een voorbeeld kunnen geven.

Casestudy's:
Laat leerlingen hun aanbevelingen onderbouwen met feiten uit het werkblad in plaats van met aannames.

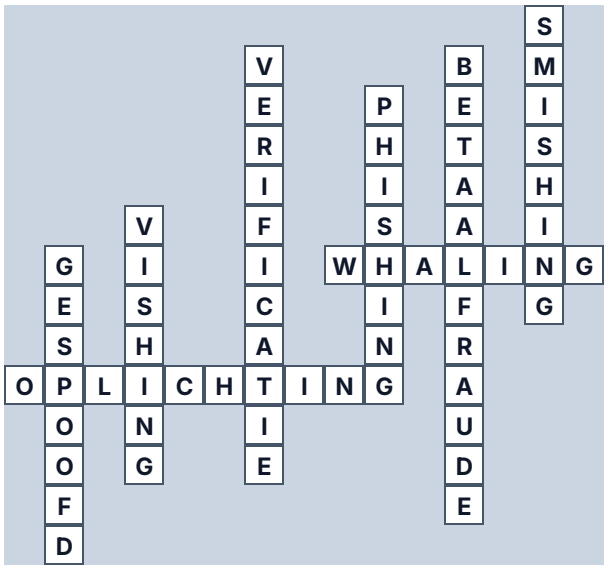
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

7 horizontaal: WHALING Gerichte phishingaanvallen om inloggegevens van C-level-leidinggevenden te stelen. (7 letters)

8 horizontaal: OPLICHTING Frauduleuze constructie om geld of toegangsgegevens van slachtoffers te stelen. (10 letters)

VERTICAAL

1 verticaal: SMISHING Oplichtings-sms'jes versturen om mobiele accountgegevens te stelen. (8 letters)

2 verticaal: VERIFICATIE Betalingsgegevens bevestigen via een vertrouwde tweede contactmethode. (11 letters)

3 verticaal: BETAALFRAUDE Frauduleuze omleiding van banktransacties naar rekeningen van criminelen. (12 letters)

4 verticaal: PHISHING Frauduleuze e-mailcampagnes om inloggegevens en wachtwoorden te stelen. (8 letters)

5 verticaal: VISHING Frauduleuze telefoongesprekken om inloggegevens en accountgegevens te stelen. (7 letters)

6 verticaal: GESPOOFD Nagebootst e-mailadres van de afzender of websiteadres dat er legitiem uit moet zien. (8 letters)

Sleutel voor husselwoorden en coderaadsel

Beoordelingssleutel voor de woordenschatopdracht met door elkaar gehusselde woorden en de Geheime codeopdracht.

SLEUTEL WOORDEN ORDENEN

1. NSHPIHGI — **PHISHING**
2. VSGNIHI — **VISHING**
3. VCIAREIEFTI — **VERIFICATIE**
4. GHILNWA — **WHALING**
5. OOEDPGFS — **GESPOOFD**
6. NCITIOPHGL — **OPLICHTING**
7. RAABEFEUDTLA — **BETAALFRAUDE**
8. SMHGSNII — **SMISHING**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"DETECTEER PHISHING MET SCANNERVERIFICATIE"

Antwoordsleutel casestudy's

A Casestudy 1: Preventie van oplichting met zakelijke overschrijvingen

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een financiële afdeling ontvangt een dringende e-mail van een vervalst leveranciersadres met het verzoek toekomstige factuuroverschrijvingen naar een nieuw routeringsnummer te sturen.
- Aanbevolen strategie en oplossing: Hanteer een beleid met dubbele autorisatie voor alle betalingen. Voer out-of-band-verificatie uit met een vooraf opgeslagen telefoonnummer en blokkeer e-mails van vervalste domeinen bij de gateway.

B Casestudy 2: Whaling-phishingincident bij een directielid

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een leidinggevende klikte op een phishinglink die beweerde een beveiligd document voor een bestuursvergadering te bevatten en voerde de primaire bedrijfsgegevens in op een vervalst portaal.
- Aanbevolen strategie en oplossing: Isoleer het apparaat van de directeur. Reset alle sessietokens en inloggegevens van het bedrijf. Bekijk de toegangslogs op gegevensuitstroom en voer hardware-MFA in bij alle aanmeldingen.