Naam: _____ Datum: _____ Score: _____

Phishingaanvallen en social engineering

Spearphishing, whaling-oplichting, SPF/DKIM/DMARC-protocollen, afzenderspoofing en beveiligingstraining voor medewerkers.

LEEROVERZICHT PHISHINGAANVALLEN

BEVEILIGD

GEGEVENSVERSLEUTELING

256-bits AES-standaard

COMPLIANT

WERELDWIJDE NORMEN

AVG- en CCPA-kaders

ZERO-TRUST

TOEGANGSBELEID

Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door phishing aanvallen en social engineering. Je verkent spearphishing, whaling, domeinvervalsing, SPF/DKIM/DMARC-protocollen, linkveiligheid en bewustwordingstraining voor medewerkers.

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/phishing-aanvallen/

Jouw leertraject: phishing beperken

- Veelvoorkomende phishing-, vishing- en nepsupport-pop-upoplichting herkennen.
- Voer procedures in voor verificatie van transacties buiten de gewone kanalen om.
- Configureer SPF-, DKIM- en DMARC-regels om vervalste domeinen te blokkeren.

INSTRUCTIES VOOR DE GIDS OVER PHISHINGAANVALLEN

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 e-mailauthenticatie. Sluit af met de bonusopdracht Snel denken.

PHISHINGAANVALLEN EN SOCIAL ENGINEERING (INLEIDING)

Phishingaanvallen maken gebruik van gerichte berichten, whaling-oplichting en domeinspoofing om inloggegevens van gebruikers te verzamelen. Het beveiligen van bedrijfssystemen vereist het inzetten van SPF-, DKIM- en DMARC-regels bij de gateway, naast goedkeuringsstappen via een apart kanaal (out-of-band).

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

Controlepunt 1: Meerkeuzeopdracht

1. Wat is spear phishing?

- A. Een gerichte phishingmail die is afgestemd op een specifiek persoon of een specifieke organisatie
- B. Een brede bulkmail die naar miljoenen willekeurige adressen wordt gestuurd
- C. Een netwerkaanval die webservers overspoelt met verkeer
- D. Een techniek om databasegegevens te onttrekken die gericht is op gebruikersrecords

2. Welk protocol laat een domein in DNS de IP-adressen vermelden die mogen verzenden, om spoofing te bestrijden?

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

3. Wat is een whaling-aanval?

- A. Een phishingcampagne die specifiek is gericht op bekende bedrijfsleiders
- B. Een SQL-injectieaanval gericht op databaseback-ups
- C. Fysieke diefstal van routerapparatuur van een lokaal netwerk
- D. Een geautomatiseerde brute-forcescan voor credential stuffing

4. Wat doet DKIM?

- A. Voegt een cryptografische handtekening toe aan e-mails om de authenticiteit van de afzender te verifiëren
- B. Blokkeert inkomend netwerkverkeer op de firewall
- C. Versleutelt databaseopslagvolumes in rust
- D. Scant e-mailbijlagen op malware op basis van handtekeningen

5. Wat is de rol van DMARC?

- A. Ontvangende mailservers instrueren hoe ze moeten omgaan met mislukte SPF/DKIM-controles
- B. Systeemwachtwoorden ontsleutelen met vooraf berekende rainbow tables
- C. E-mailbijlagen comprimeren vóór verzending
- D. Toegangsrechten voor netwerkroutering configureren

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Spearphishing vertrouwt op generieke massamails die naar miljoenen willekeurige adressen worden verzonden.

- ○ Waar
- ○ Onwaar

7 Vraag 7

7. DMARC-beleid kan mailservers opdracht geven onbevoegde, vervalste berichten te weigeren.

- ○ Waar
- ○ Onwaar

8 Vraag 8

8. SPF-verificatie werkt door de cryptografische handtekening van de e-mailtekst te valideren.

- ○ Waar
- ○ Onwaar

9 Vraag 9

9. Whaling-aanvallen richten zich op bedrijfsbeheerders op laag niveau om toegang te krijgen tot databasebestanden.

- ○ Waar
- ○ Onwaar

10 Vraag 10

10. Verificatie van betaalverzoeken via een ander kanaal (out-of-band) helpt oplichting met bankoverschrijvingen te stoppen.

- ○ Waar
- ○ Onwaar

Controlepunt 3: Kernbegrippen invullen

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

1. Een specifieke werknemer aanvallen met persoonlijke informatie heet _____ .
2. Het vervalsen van een e-mailheader zodat berichten legitiem lijken, is _____ van de afzender.
3. De DNS-recordlijst van geautoriseerde IP's van mailservers is het _____ .
4. De e-mailstandaard voor ondertekening die afzenderverificatie biedt, is _____ .
5. Het instellen van beleid om mislukte SPF/DKIM-controles te weigeren gebeurt met _____ .
6. Een phishingcampagne gericht op C-level-leidinggevenden heet _____ .

WOORDENBANK

DKIM DMARC FIREWALL RANSOMWARE SPEARPHISHING SPF-RECORD SPOOFING WHALING

Schrijf hier je antwoorden:

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

Controlepunt 4: Beveiligingsbegrippen koppelen

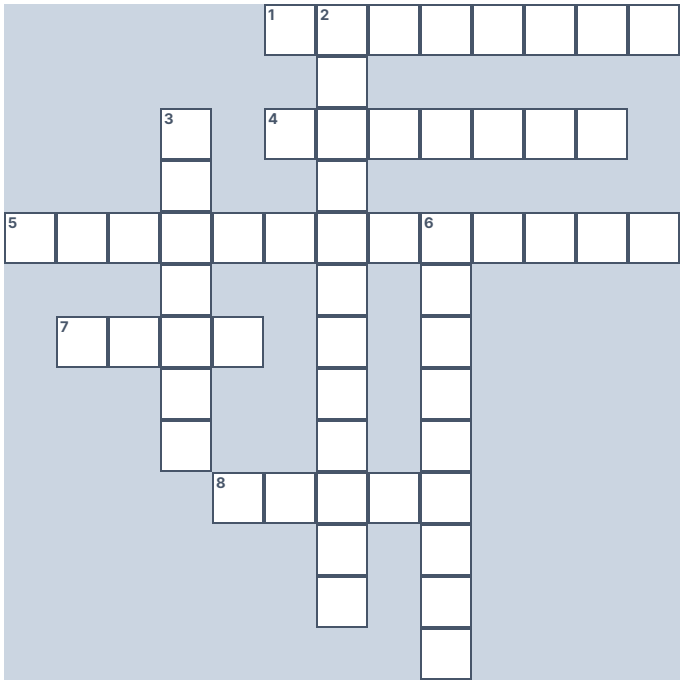
DEFINITIES KOPPELEN

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. SPEAR	A	Oplichtingsgesprekken via de telefoon.
☐	2. SPOOFING	B	Richt zich op C-level-leidinggevenden.
☐	3. SPF	C	Instructies voor het weigeren van beleid.
☐	4. DKIM	D	IP-adressen van DNS-geautoriseerde afzenders.
☐	5. DMARC	E	E-mail met social engineering.
☐	6. WHALING	F	Gepersonaliseerde gerichte e-mail.
☐	7. PHISHING	G	Het e-mailadres van de afzender vervalsen.
☐	8. VISHING	H	Cryptografische handtekening in e-mail.

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

1. Het vervalsen van het e-mailadres van de afzender. (8)

4. Oplichtingstelefoontjes via spraak. (7)

5. Gepersonaliseerde, gerichte e-mail. (13)

7. Cryptografische handtekening in e-mail. (4)

8. Beleid met instructies om berichten te weigeren. (5)

VERTICAAL

2. E-mail die op social engineering berust. (12)

3. Gericht op C-level-leidinggevenden. (7)

6. Via DNS geautoriseerde IP-adressen van afzenders. (9)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

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

HORIZONTAAL

1 horizontaal: Het vervalsen van het e-mailadres van de afzender. (8 letters):

4 horizontaal: Oplichtingstelefoontjes via spraak. (7 letters):

5 horizontaal: Gepersonaliseerde, gerichte e-mail. (13 letters):

7 horizontaal: Cryptografische handtekening in e-mail. (4 letters):

8 horizontaal: Beleid met instructies om berichten te weigeren. (5 letters):

VERTICAAL

2 verticaal: E-mail die op social engineering berust. (12 letters):

3 verticaal: Gericht op C-level-leidinggevenden. (7 letters):

6 verticaal: Via DNS geautoriseerde IP-adressen van afzenders. (9 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.

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

WOORDENLIJST

SPEARPHISHING SPOOFING SPFRECORD DKIM DMARC WHALING PHISHINGMAIL VISHING

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. SPEARPHISHING
B. SPOOFING
C. SPFRECORD
D. DKIM
E. DMARC
F. WHALING
G. PHISHINGMAIL
H. VISHING

DEFINITIES EN KOPPELVELDEN
1. Het vervalsen van het e-mailadres van de afzender.
2. Gepersonaliseerde, gerichte e-mail.
3. Oplichtingstelefoontjes via spraak.
4. Via DNS geautoriseerde IP-adressen van afzenders.
5. E-mail die op social engineering berust.
6. Beleid met instructies om berichten te weigeren.
7. Cryptografische handtekening in e-mail.
8. Gericht op C-level-leidinggevenden.

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. **HESNPPIHSIG RA** _____
2. **DSRRPCOEF** _____
3. **ADCRM** _____
4. **IGHINLIAMPH S** _____
5. **FIPGOSNO** _____
6. **IMDK** _____
7. **WNIGHLA** _____
8. **IHGVNIS** _____

Bonusopdracht: Snel denken

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

1	Apparaten die gehackt kunnen worden			
2	Tekenen van een phishingmail			
3	Tekenen dat een computer is geïnfecteerd			
4	Woorden die nepurgentie creëren			
5	Manieren om een afzender te controleren			
6	Mensen die je om IT-hulp kunt vragen			
7	Dingen waarvan je een back-up maakt			
8	Vissen of zeedieren die je kent			
9	Bedrijven waarvan oplichters zich voordoen als			
10	Veilige gewoonten die je vandaag kunt beginnen			
11	Dingen die je doet nadat je op een valse link hebt geklikt			
12	Dingen die je doet na een datalek			
13	Kanalen waar phishing plaatsvindt			
14	Dingen die je nooit per e-mail verstuurt			
15	Manieren om je accounts te beschermen			

Controlepunt 8: Casestudy's cyberbeveiliging

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

CASESTUDY 1: HERSTEL NA EEN WHALING-AANVAL OP DE C-SUITE



Scenario: Een financieel directeur (CFO) ontvangt een zeer gepersonaliseerde e-mail die beweert van de CEO te zijn, met het verzoek om snel $50.000 over te maken om een vertrouwelijke domeinaankoop af te ronden.

Discussievraag: Analyseer de risico's van merkvervalsing en beschrijf in detail SPF/DKIM/DMARC en authenticatiecontroles.

CASESTUDY 2: GATEWAYBELEID VOOR SPF/DKIM/DMARC IMPLEMENTEREN



Scenario: Een onderneming faalt bij beveiligingsaudits omdat uitgaande marketingmails vaak als spam worden gemarkeerd en hackers actief het merkdomein van het bedrijf vervalsen.

Discussievraag: Stel technische en administratieve controles vast om de echtheid van e-mail te verifiëren.

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

8	5	18	11	5	14		19	15	3	9	1	12		
5	14	7	9	14	5	5	18	9	14	7		13	5	20
		5	13	1	9	12	1	21	4	9	20	19		

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 phishing?

Phishing is een social-engineeringaanval waarbij criminelen frauduleuze berichten sturen om gebruikers gevoelige gegevens te laten delen.

Q2: Wat is het verschil tussen phishing en spearphishing?

Phishing richt zich op brede groepen met generieke inhoud, terwijl spearphishing zich richt op specifieke slachtoffers met behulp van aangepaste details.

Q3: Wat is whaling?

Whaling is een zeer gerichte phishingaanval op prominente leidinggevenden met beheerbevoegdheden.

Q4: Wat is e-mailspoofing?

E-mailspoofing is het maken van e-mailberichten met een vervalst afzenderadres om de ontvanger te laten vertrouwen op de bron.

Q5: Hoe voorkomt SPF spoofing?

Het publiceert in DNS een lijst met geautoriseerde verzendende IP-adressen, zodat ontvangende servers de bron van de e-mail kunnen verifiëren. [1]

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

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

Q6: Wat is DKIM?

DomainKeys Identified Mail voegt een cryptografische handtekening toe aan e-mailheaders, waarmee wordt bewezen dat een domein verantwoordelijkheid heeft genomen en het bericht niet is gewijzigd.

Q7: Waar staat DMARC voor?

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

Q8: Wat is een DMARC-beleid?

Een beleid dat mailservers vertelt hoe ze berichten moeten behandelen die SPF/DKIM niet doorstaan (none, quarantine of reject). [2]

Q9: Wat is vishing?

Voice phishing, waarbij aanvallers frauduleuze telefoongesprekken gebruiken om beheer- of financiële gegevens los te krijgen.

Q10: Hoe helpen linkscanners?

Ze scannen en herschrijven links in binnenkomende e-mail om op het moment van klikken de veiligheid van de bestemmingswebpagina's te controleren.

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe werkt een homograafaanval?

Aanvallers registreren domeinnamen met op elkaar lijkende niet-ASCII-Unicode-tekens om visueel een echte domeinnaam na te bootsen.

Q2: Wat is een punycoderepresentatie?

Een codering die Unicode-domeinnamen omzet in ASCII-compatibele tekenreeksen die beginnen met 'xn--', zodat DNS ze kan verwerken.

Q3: Waarom is 'p=reject' de veiligste DMARC-status?

Het vraagt ontvangende servers om e-mail te weigeren die DMARC (uitgelijnde SPF/DKIM) niet doorstaat tijdens de SMTP-sessie, zodat directe spoofing wordt geblokkeerd. [2]

Q4: Hoe omzeilen aanvallers SPF-regels?

Door misbruik te maken van lookalike-domeinen (typosquatting) of gehackte accounts bij legitieme e-maildiensten van derden.

Q5: Wat is business email compromise (BEC)?

Een bedrijfsfraude waarbij aanvallers zakelijke e-mailaccounts kapen of nabootsen om frauduleuze betalingen goed te keuren.

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Hoe stopt multifactorauthenticatie phishing?

Het vereist tweede tokens (zoals hardwaresleutels) die niet alleen via lookalike-landingspagina's kunnen worden gestolen.

Q7: Wat is een landingspagina voor het verzamelen van inloggegevens?

Een nagemaakt inlogportaal dat is ontworpen om ingevoerde gebruikersnamen, wachtwoorden en MFA-tokens in realtime te onderscheppen.

Q8: Wat is subdomeinkaping?

Een aanvaller die de controle overneemt over een ongebruikte DNS-subdomeinverwijzing om schadelijke phishinglandingspagina's te hosten onder een vertrouwd bovenliggend domein.

Q9: Hoe werkt de DKIM-alignmentcontrole?

Het controleert of het domein in de 'From'-header overeenkomt met het domein dat het bericht cryptografisch heeft ondertekend in de DKIM-header.

Q10: Wat is de rol van een e-mailgateway?

Inkomende e-mail filteren, links controleren, bijlagen in een sandbox uitvoeren en naleving van SPF/DKIM/DMARC valideren.

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. [4]

2. BEVEILIGINGSINZICHT

Business email compromise (BEC) veroorzaakte in 2025 meer dan $3 miljard aan verliezen die bij de IC3 van de FBI zijn gemeld. [4]

3. BEVEILIGINGSINZICHT

Homografische aanvallen gebruiken Cyrillische lookalike-letters om domeinen met een exacte merknaam in browsers visueel te dupliceren.

4. BEVEILIGINGSINZICHT

Met 'p=reject' vraagt een domein ontvangers om mislukte e-mail tijdens de aflevering te weigeren, en niet als spam op te bergen. [2]

5. BEVEILIGINGSINZICHT

Whaling-aanvallen op CEO's vragen vaak om dringende betalingen voor vertrouwelijke fusies of domeinaankopen.

6. BEVEILIGINGSINZICHT

Portalen voor het oogsten van inloggegevens kopiëren echte inlogpagina's, zodat slachtoffers hun wachtwoorden rechtstreeks in het formulier van de aanvaller typen.

7. BEVEILIGINGSINZICHT

De gezamenlijke phishingrichtlijnen van CISA bevelen gebruikerstraining aan naast DMARC, SPF, DKIM en phishingbestendige MFA. [3]

8. BEVEILIGINGSINZICHT

De SPF-evaluatie is beperkt tot 10 termen die een DNS-query uitvoeren; bij overschrijding van de limiet volgt het resultaat 'permerror'. [1]

9. BEVEILIGINGSINZICHT

FIDO2-hardwarebeveiligingssleutels bieden cryptografisch onderbouwde bescherming tegen het op afstand verzamelen van inloggegevens.

10. BEVEILIGINGSINZICHT

Phishing is een van de meest voorkomende manieren waarop aanvallers voor het eerst binnenkomen bij een organisatie, en daarom is regelmatige bewustwordingstraining een effectieve verdediging.

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] 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

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 Vraag 1

Juist antwoord: A

DOCENTENNOTITIE

Wat is spear phishing? → Een gerichte phishingmail die is afgestemd op een specifiek persoon of een specifieke organisatie

2 Vraag 2

Juist antwoord: A

DOCENTENNOTITIE

SPF publiceert de toegestane verzendende hosts van een domein in DNS, zodat ontvangers de envelop-afzender kunnen controleren.

3 Vraag 3

Juist antwoord: A

DOCENTENNOTITIE

Wat is een whaling-aanval? → Een phishingcampagne die specifiek is gericht op bekende bedrijfsleiders

4 Vraag 4

Juist antwoord: A

DOCENTENNOTITIE

Wat doet DKIM? → Voegt een cryptografische handtekening toe aan e-mails om de authenticiteit van de afzender te verifiëren

5 Vraag 5

Juist antwoord: A

DOCENTENNOTITIE

Wat is de rol van DMARC? → Ontvangende mailservers instrueren hoe ze moeten omgaan met mislukte SPF/DKIM-controles

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 Vraag 6

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: spear phishing is op specifieke personen toegesneden, anders dan algemene bulkphishing.

7 Vraag 7

Juist antwoord: Waar

DOCENTENNOTITIE

DMARC-beleid kan mailservers opdracht geven onbevoegde, vervalste berichten te weigeren.

8 Vraag 8

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: SPF controleert het verzendende IP-adres met DNS; DKIM is degene die een cryptografische handtekening verifieert.

9 Vraag 9

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: whaling richt zich op hoge bestuurders, die betalingen kunnen goedkeuren en toegang hebben tot gevoelige gegevens.

10 Vraag 10

Juist antwoord: Waar

DOCENTENNOTITIE

Waar: betaalverzoeken bevestigen via een apart, bekend kanaal helpt overschrijvingsfraude te stoppen.

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

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

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 SPEARPHISHING	2 SPOOFING	3 SPF-RECORD	4 DKIM
5 DMARC	6 WHALING		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 B – SPOOFING	2 A – SPEARPHISHING	3 H – VISHING	4 C – SPFRECORD
5 G – PHISHINGMAIL	6 E – DMARC	7 D – DKIM	8 F – WHALING

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen SPEAR, SPOOFING en SPF 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.

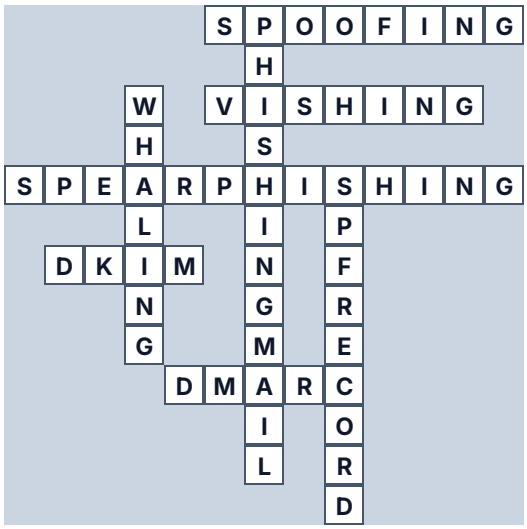
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

1 horizontaal: SPOOFING Het vervalsen van het e-mailadres van de afzender. (8 letters)

4 horizontaal: VISHING Oplichtingstelefoontjes via spraak. (7 letters)

5 horizontaal: SPEARPHISHING Gepersonaliseerde, gerichte e-mail. (13 letters)

7 horizontaal: DKIM Cryptografische handtekening in e-mail. (4 letters)

8 horizontaal: DMARC Beleid met instructies om berichten te weigeren. (5 letters)

VERTICAAL

2 verticaal: PHISHINGMAIL E-mail die op social engineering berust. (12 letters)

3 verticaal: WHALING Gericht op C-level-leidinggevenden. (7 letters)

6 verticaal: SPFRECORD Via DNS geautoriseerde IP-adressen van afzenders. (9 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. HESNPPIHSIGRA — **SPEARPHISHING**
2. DSRRPCOEF — **SPFRECORD**
3. ADCRM — **DMARC**
4. IGHINLIAMPHS — **PHISHINGMAIL**
5. FIPGOSNO — **SPOOFING**
6. IMDK — **DKIM**
7. WNIGHLA — **WHALING**
8. IHGVNIS — **VISHING**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"HERKEN SOCIAL ENGINEERING MET EMAILAUDITS"

Antwoordsleutel casestudy's

A Casestudy 1: Herstel na een whaling-aanval op de C-suite

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een Chief Financial Officer ontvangt een zeer gepersonaliseerde e-mail die beweert van de CEO te komen en waarin om een snelle overboeking van $50.000 wordt gevraagd om een vertrouwelijke domeinaankoop af te ronden.
- Aanbevolen strategie en oplossing: Configureer DMARC met het beleid 'p=reject' om vervalste afzenderdomeinen te blokkeren. Voeg waarschuwingsbanners voor externe afzenders toe op de gateway en eis mondelinge bevestiging buiten de e-mail om (out-of-band) voor alle financiële transacties.

B Casestudy 2: Gatewaybeleid voor SPF/DKIM/DMARC implementeren

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een groot bedrijf valt door beveiligingsaudits omdat uitgaande marketingmails regelmatig als spam worden gemarkeerd en hackers actief de domeinnaam van het bedrijfsmerk vervalsen (spoofing).
- Aanbevolen strategie en oplossing: Publiceer een TXT-record voor SPF met de IP-adressen van geautoriseerde afzenders. Configureer DKIM-ondertekeningssleutels op uitgaande mailservers en analyseer inkomende DMARC-XML-feedbackrapporten om misbruik op te sporen.