Naam: _____ Datum: _____ Score: _____

Preventie van identiteitsdiefstal en beveiliging van bezittingen Beveiligingsgids

Gelekte inloggegevens, MFA, monitoring van het dark web, waarschuwingen voor creditfreeze, social engineering

LEEROVERZICHT PREVENTIE VAN IDENTITEITSDIEFSTAL

BEVEILIGD
GEGEVENSVERSLEUTELING
256-bits AES-standaard

COMPLIANT
WERELDWIJDE NORMEN
AVG- en CCPA-kaders

ZERO-TRUST
TOEGANGSBELEID
Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door het voorkomen en beperken van identiteitsdiefstal. Je verkent gelekte inloggegevens, multifactorauthenticatie, monitoring van het dark web, waarschuwingen voor kredietblokkades en verdediging tegen social engineering.

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/identiteitsdiefstal/

Jouw leertraject: identiteitsbescherming

- Begrijp de risico's van blootgestelde inloggegevens op darkwebforums.
- Voer multifactorauthenticatie (MFA) en waarschuwingen voor kredietblokkades in.
- Ontwerp bedrijfsbeveiligingsmaatregelen tegen gerichte social-engineeringoplichting.

INSTRUCTIES GIDS IDENTITEITSDIEFSTAL

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 identiteitsbescherming. Sluit af met de bonusopdracht Snel denken.

PREVENTIE VAN IDENTITEITSDIEFSTAL EN BEVEILIGING VAN BEZITTINGEN (INLEIDING)

Identiteitsdiefstal maakt misbruik van gelekte inloggegevens en zwakke logins om persoonlijke en zakelijke accounts over te nemen. MFA, kredietblokkades, darkwebscanners en SPF/DKIM/DMARC-kaders vormen samen een belangrijke verdediging tegen digitale imitatie.

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

Controlepunt 1: Meerkeuzeopdracht

1. Welke methode gebruiken identiteitsdieven vooral om inloggegevens te stelen?

- A. Nep-e-mailmeldingen versturen waarmee gebruikers worden misleid om wachtwoorden in te voeren op nagemaakte portalen
- B. Luisteren naar radio-uitzendingen in de buurt van het bedrijfskantoor van een gebruiker
- C. De lokale serveropslagschijf van een gebruiker defragmenteren
- D. Externe configuraties voor netwerkback-ups loskoppelen

2. Welke beveiligingsmaatregel biedt de sterkste verdediging tegen lekken van inloggegevens?

- A. Multifactorauthenticatie met hardwaresleutels
- B. Lange wachtwoorden maken met de standaardformaten van de browser
- C. Elk halfjaar de gebruikersnamen van e-mailadressen wijzigen
- D. Opgeslagen cookietracking in browsergeschiedenissen verwijderen

3. Wat staat voor kredietbevriezing?

- A. Kredietrapporten vergrendelen om te voorkomen dat dieven ongeautoriseerde leningen afsluiten
- B. Transactiegeschiedenissen van bankrekeningen uit databases verwijderen
- C. Magneetstriplezers voor creditcards op scanners uitschakelen
- D. Lokale databaseschijven in ruststaat versleutelen

4. Waarom is dark webmonitoring nuttig?

- A. Het waarschuwt gebruikers als hun gelekte inloggegevens in illegale databases opduiken
- B. Het voorkomt dat actieve malware in virtuele sandboxes draait
- C. Het versnelt de routeringssnelheid van de browser op virtuele netwerken
- D. Het blokkeert pogingen tot toegang via SQL-injectie op de database in de backend

5. Wat betekent social engineering?

- A. Mensen manipuleren zodat ze vrijwillig vertrouwelijke inloggegevens prijsgeven
- B. Poorten van bedrijfsservers scannen op actieve beveiligingsexploits
- C. Systeemdatabasebestanden back-uppen op offline harde schijven
- D. Netwerkpakketten routeren via drie versleutelde onion-nodes

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Identiteitsdiefstal treft alleen digitale online accounts, niet fysieke post.

- ○ Waar
- ○ Onwaar

7 Vraag 7

7. Het afdwingen van MFA op alle persoonlijke accounts blokkeert de meeste credential-stuffing-aanvallen door bots.

- ○ Waar
- ○ Onwaar

8 Vraag 8

8. Een kredietblokkade blokkeert kredietcontroles, maar verhindert dat je toegang hebt tot je eigen bankrekening.

- ○ Waar
- ○ Onwaar

9 Vraag 9

9. Wachtwoordmanagers beschermen gebruikers tegen phishing door wachtwoorden niet automatisch in te vullen op nagemaakte domeinen.

- ○ Waar
- ○ Onwaar

10 Vraag 10

10. Phishing-e-mails gebruiken vaak dringende taal om emotionele, snelle reacties uit te lokken.

- ○ Waar
- ○ Onwaar

Controlepunt 3: Kernbegrippen invullen

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

1. Identiteitsdieven richten zich op persoonlijke wachtwoorden en _____ van gebruikers.

2. Het waarschuwen van gebruikers over databasebreuken brengt _____ van privéaccounts aan het licht.

3. Het vereisen van een tijdelijke code om in te loggen heet _____ .

4. Het scannen van hackerforums op gestolen gegevens is _____ van het dark web.

5. Het blokkeren van ongeautoriseerde kredietcontroles vereist een _____ .

6. Het trainen van werknemers in phishingbewustzijn bouwt een actieve _____ op voor de beveiliging.

WOORDENBANK

DATALEKKEN INLOGGEGEVENS KREDIETBLOKKADE MFA-VERIFICATIE MONITORING PHISHING SPOOFING VERDEDIGING

Schrijf hier je antwoorden:

1. **2.**

3. **4.**

5. **6.**

Controlepunt 4: Beveiligingsbegrippen koppelen

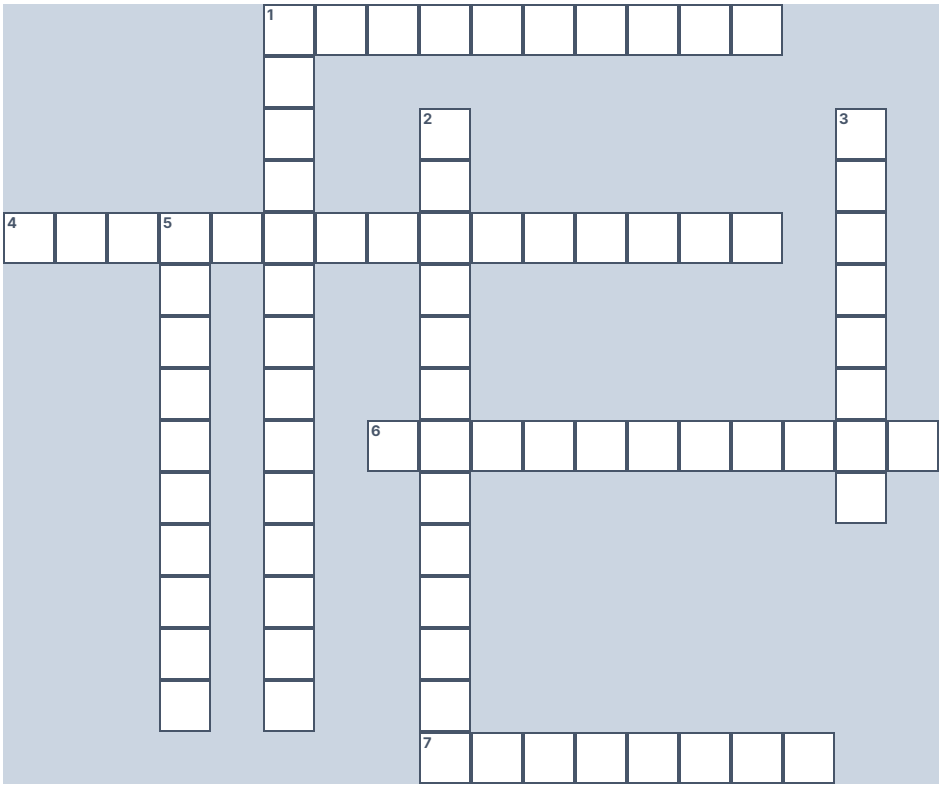
DEFINITIES KOPPELEN

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. INLOGGEGEVENS	A	Extra verificatiestap (zoals hardwaresleutels) die accountlogins beschermt.
☐	2. LEKKEN	B	Een nepwebsite of nep-e-mail maken om een legitieme organisatie na te bootsen.
☐	3. MFA	C	De toegang tot kredietdossiers beperken om frauduleuze leningaanvragen te voorkomen.
☐	4. MONITORING	D	Ongeautoriseerde blootstelling van privédatabases met persoonlijke gebruikersgegevens.
☐	5. BEVRIEZEN	E	Training en technische maatregelen om te beschermen tegen identiteitsdiefstal.
☐	6. VERDEDIGING	F	Frauduleuze berichten versturen om gebruikers te verleiden inloggegevens prijs te geven.
☐	7. SPOOFING	G	Online forums en hackerkanalen scannen op gestolen bedrijfsgegevens.
☐	8. PHISHING	H	Gebruikersnamen, wachtwoorden en privétokens waarmee digitale identiteiten worden geauthenticeerd.

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 scannen van online forums en hackerkanalen op gestolen bedrijfsgegevens. (10)

4. Het beperken van de toegang tot kredietdossiers om frauduleuze leningaanvragen te voorkomen. (15)

6. Training en technische maatregelen ter bescherming tegen identiteitsdiefstal. (11)

7. Het maken van een nepwebsite of nep-e-mail om een legitieme organisatie na te bootsen. (8)

VERTICAAL

1. Aanvullende verificatiestap (zoals hardwaresleutels) die accountaanmeldingen beschermt. (14)

2. Gebruikersnamen, wachtwoorden en privétokens waarmee digitale identiteiten worden geauthenticeerd. (13)

3. Het versturen van frauduleuze berichten om gebruikers inloggegevens te laten afgeven. (8)

5. Ongeautoriseerde blootstelling van privédatabases met persoonlijke gebruikersgegevens. (10)

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 scannen van online forums en hackerkanalen op gestolen bedrijfsgegevens. (10 letters):

4 horizontaal: Het beperken van de toegang tot kredietdossiers om frauduleuze leningaanvragen te voorkomen. (15 letters):

6 horizontaal: Training en technische maatregelen ter bescherming tegen identiteitsdiefstal. (11 letters):

7 horizontaal: Het maken van een nepwebsite of nep-e-mail om een legitieme organisatie na te bootsen. (8 letters):

VERTICAAL

1 verticaal: Aanvullende verificatiestap (zoals hardwaresleutels) die accountaanmeldingen beschermt. (14 letters):

2 verticaal: Gebruikersnamen, wachtwoorden en privétokens waarmee digitale identiteiten worden geauthenticeerd. (13 letters):

3 verticaal: Het versturen van frauduleuze berichten om gebruikers inloggegevens te laten afgeven. (8 letters):

5 verticaal: Ongeautoriseerde blootstelling van privédatabases met persoonlijke gebruikersgegevens. (10 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.

S A F O K G N K D N C D H I B

N A P R L N P R W T M I Y F Y

E S G X W I H E F R F T N U K

V R D T D H S D L P A L M S H

E K M P A S H I Y P V L G W U

G N O Y T I Q E Q B E A N L S

E P N M A H B T L I R F I I P

G N I Y L P B B Z Z I Y G B O

G N T V E X M L C F F P I W O

O Q O Q K X H O E Y I C D W F

L L R F K G H K Z W C C E O I

N R I J E X X K R K A Z D A N

I N N R N Z R A M G T S R W G

G L G W J B Y D C C I Y E O U

Z O Z U T B H E V P E X V C N

WOORDENLIJST

INLOGGEGEVENS DATALEKKEN MFAVERIFICATIE MONITORING KREDIETBLOKKADE VERDEDIGING SPOOFING PHISHING

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. INLOGGEGEVENS**
- **B. DATALEKKEN**
- **C. MFAVERIFICATIE**
- **D. MONITORING**
- **E. KREDIETBLOKKADE**
- **F. VERDEDIGING**
- **G. SPOOFING**
- **H. PHISHING**

DEFINITIES EN KOPPELVELDEN

1. Het versturen van frauduleuze berichten om gebruikers inloggegevens te laten afgeven.
2. Gebruikersnamen, wachtwoorden en privétokens waarmee digitale identiteiten worden geauthenticeerd.
3. Het maken van een nepwebsite of nep-e-mail om een legitieme organisatie na te bootsen.
4. Training en technische maatregelen ter bescherming tegen identiteitsdiefstal.
5. Het scannen van online forums en hackerkanalen op gestolen bedrijfsgegevens.
6. Het beperken van de toegang tot kredietdossiers om frauduleuze leningaanvragen te voorkomen.
7. Ongeautoriseerde blootstelling van privédatabases met persoonlijke gebruikersgegevens.
8. Aanvullende verificatiestap (zoals hardwaresleutels) die accountaanmeldingen beschermt.

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. ELENGNGVIESGO
2. EFRAIIMTFECAIV
3. KEORDELKKDBETAI
4. ONGIFSPO
5. KENAAKLDET
6. NTIRIMOOGN
7. GEVEIGINRDD
8. SHHGPNII

Bonusopdracht: Snel denken

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

1	Dingen die je doet als je identiteit is gestolen			
2	Dingen die je niet op sociale media deelt			
3	Dingen waarvan je een back-up maakt			
4	Kaarten of identiteitsbewijzen in je portemonnee			
5	Documenten die je moet beschermen			
6	Dingen die je doet na een datalek			
7	Redenen om software bij te werken			
8	Informatie die een identiteitsdief wil hebben			
9	Apparaten die gehackt kunnen worden			
10	Plekken waar je gegevens kunnen lekken			
11	Veilige gewoonten die je vandaag kunt beginnen			
12	Tekenen dat een computer is geïnfecteerd			
13	Manieren om te bewijzen wie je bent			
14	Tekenen van identiteitsdiefstal			
15	Waarschuwingssignalen in een e-mail			

Controlepunt 8: Casestudy's cyberbeveiliging

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

CASESTUDY 1: BESCHERMING TEGEN IDENTITEITSIMITATIE VAN DIRECTIELEDEN



Scenario: Een prominente C-suitebestuurder is het doelwit geworden van typosquatting-domeinnamen die zijn persoonlijke e-mailadres nabootsen om klanten op te lichten. Ontwerp een plan voor merkbescherming.

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

CASESTUDY 2: BLOOTSTELLING VAN ZAKELIJKE INLOGGEGEVENS OP HET DARK WEB



Scenario: Een dump van een database op het dark web bevat enkele honderden zakelijke inloggegevens van systeembeheerders van een onderneming. Ontwerp een mitigatiestrategie.

Discussievraag: Schets het proces voor het opschonen van inloggegevens en plan de uitrol van een wachtwoordmanager.

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

2	5	19	3	8	5	18	13		10	5		4	9	7	9	20	1	12	5
	9	4	5	14	20	9	20	5	9	20		13	5	20		13	6	1	

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 identiteitsdiefstal?

Een misdrijf waarbij een aanvaller persoonlijke gegevens (zoals wachtwoorden of burgerservicenummers) steelt om zich voor te doen als iemand anders en daar financieel voordeel uit te halen.

Q2: Wat is de meest voorkomende oorzaak van identiteitsdiefstal?

Phishing is een van de belangrijkste manieren waarop dieven aan wachtwoorden komen, door gebruikers naar nagemaakte, gespoofde websites te lokken.

Q3: Hoe beschermt multifactorauthenticatie (MFA) identiteiten?

MFA vereist een tweede bewijs (zoals een hardwaresleutel) om in te loggen, en houdt aanvallers buiten, zelfs als ze je wachtwoord stelen.

Q4: Wat is een kredietblokkade?

Een gratis dienst die voorkomt dat kredietbureaus je kredietdossier delen, zodat dieven geen nieuwe leningen op jouw naam kunnen afsluiten. [2]

Q5: Wat is dark webmonitoring?

Software die hackerforums controleert op gelekte e-mailadressen, wachtwoorden en persoonlijke gegevens en je waarschuwt als je gegevens zijn blootgesteld.

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

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

Q6: Wat betekent credential stuffing?

Geautomatiseerde bots die lijsten met gelekte wachtwoorden op honderden websites uitproberen om actieve accounts over te nemen.

Q7: Waarom is e-mailspoofing gevaarlijk?

Het stelt aanvallers in staat de naam van de afzender in e-mails te vervalsen, waardoor phishingberichten lijken te komen van vertrouwde collega's.

Q8: Hoe voorkomen wachtwoordmanagers identiteitsdiefstal?

Ze bewaren voor elk account complexe, unieke wachtwoorden en weigeren inloggegevens automatisch in te vullen op valse phishingdomeinen.

Q9: Wat is spearphishing?

Een zeer gerichte phishingaanval die op maat is gemaakt met de naam en gegevens van het slachtoffer om de kans op misleiding te vergroten.

Q10: Waarin verschilt een kredietmelding van een kredietblokkade?

Een waarschuwing vraagt kredietverstrekkers je identiteit te verifiëren voordat ze accounts openen, terwijl een blokkade de toegang tot je kredietdossier volledig blokkeert. [2]

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe leidt SIM-swapping tot identiteitsdiefstal?

Aanvallers overtuigen medewerkers van een provider om het telefoonnummer van het slachtoffer over te zetten naar een nieuwe simkaart, waarmee ze sms-gebaseerde 2FA-codes kapen.

Q2: Wat is de rol van DMARC bij het voorkomen van identiteitsdiefstal?

Met DMARC kunnen domeineigenaren voorkomen dat vervalste e-mails in inboxen terechtkomen, zodat nepmails bedrijfsdomeinen niet kunnen nabootsen.

Q3: Waarom is synthetische identiteitsfraude moeilijk te detecteren?

Dieven combineren echte burgerservicenummers (SSN's) met valse namen en geboortedata om gloednieuwe kredietprofielen op te bouwen en zo eenvoudige fraudemeldingen te omzeilen.

Q4: Hoe misbruiken datahandelaren persoonlijke identiteiten?

Gegevensmakelaars verzamelen openbare registers, webgedrag en aankoopgeschiedenis om profieldossiers samen te stellen, die kunnen worden gelekt of verkocht.

Q5: Waarom wordt sms-gebaseerde MFA als kwetsbaar beschouwd?

Sms-verkeer is kwetsbaar voor onderschepping, phishing en SIM-swapping-exploits op providerniveau.

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Wat is een vergrendeling van het kredietdossier?

Een commerciële dienst die lijkt op een kredietblokkade, waarmee gebruikers hun kredietdossier via een mobiele app direct kunnen ontgrendelen of vergrendelen.

Q7: Hoe voeden datalekken bij bedrijven identiteitsdiefstal?

Gelekte databases leggen miljoenen wachtwoorden en gebruikersnamen in platte tekst bloot, waardoor dieven de ruwe gegevens krijgen die ze nodig hebben voor gerichte identiteitsfraude.

Q8: Wat is het risico van te veel delen op sociale media?

Het openbaar delen van namen van huisdieren, geboorteplaatsen en meisjesnamen van moeders geeft dieven de antwoorden op veelgebruikte vragen voor accountherstel.

Q9: Hoe beschermen biometrische logins identiteitsprofielen?

Biometrie koppelt inloggen aan kenmerken zoals vingerafdrukken of gezichten; als ze op het apparaat blijven, zijn ze moeilijk te stelen, maar opgeslagen biometrische gegevens kunnen wel lekken.

Q10: Hoe bestrijdt de Red Flags Rule identiteitsdiefstal?

Een federale regelgeving die financiële instellingen verplicht schriftelijke programma's te ontwikkelen om waarschuwingssignalen van identiteitsdiefstal te herkennen en erop te reageren.

Deel 11: 10 cyberbeveiligingsfeiten en inzichten uit de praktijk

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

1. BEVEILIGINGSINZICHT

IdentityTheft.gov, beheerd door de FTC, laat Amerikaanse slachtoffers identiteitsdiefstal melden en een persoonlijk herstelplan krijgen. [1]

2. BEVEILIGINGSINZICHT

Hardwarebeveiligingssleutels zijn phishingbestendige MFA, de sterkste vorm van MFA waar CISA op aandringt. [4]

3. BEVEILIGINGSINZICHT

Gelekte wachtwoorden zijn een veelvoorkomend toegangspunt bij datalekken en voeden later identiteitsfraude.

4. BEVEILIGINGSINZICHT

Een kredietblokkade is volgens de federale wet gratis en voorkomt dat kredietverstrekkers kredietdossiers controleren totdat de blokkade wordt opgeheven. [2]

5. BEVEILIGINGSINZICHT

Met DMARC kunnen domeineigenaren mailservers opdragen vervalste e-mail die de controles niet doorstaat te weigeren of in quarantaine te plaatsen. [7]

6. BEVEILIGINGSINZICHT

Met SIM-swapping kunnen hackers sms-gebaseerde tweefactorauthenticatie op bankportalen omzeilen.

7. BEVEILIGINGSINZICHT

Synthetische identiteitsfraude combineert echte en valse gegevens, waardoor kredietverstrekkers het moeilijk kunnen detecteren.

8. BEVEILIGINGSINZICHT

Veel mensen gebruiken hetzelfde wachtwoord voor meerdere online accounts, dus één datalek kan er meerdere blootleggen.

9. BEVEILIGINGSINZICHT

Databrokers stellen gedetailleerde dossiers samen over grote aantallen consumenten, wat een geconcentreerd privacyrisico vormt.

10. BEVEILIGINGSINZICHT

Herstel na identiteitsdiefstal kan maanden werk kosten, zoals het betwisten van afschrijvingen en het corrigeren van kredietrapporten.

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.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[5] 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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[7] 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

Welke methode gebruiken identiteitsdieven vooral om inloggegevens te stelen? → Nep-e-mailmeldingen versturen waarmee gebruikers worden misleid om wachtwoorden in te voeren op nagemaakte portalen

2 Vraag 2

Juist antwoord: A

DOCENTENNOTITIE

Welke beveiligingsmaatregel biedt de sterkste verdediging tegen lekken van inloggegevens? → Multifactorauthenticatie met hardwaresleutels

3 Vraag 3

Juist antwoord: A

DOCENTENNOTITIE

Wat staat voor kredietbevriezing? → Kredietrapporten vergrendelen om te voorkomen dat dieven ongeautoriseerde leningen afsluiten

4 Vraag 4

Juist antwoord: A

DOCENTENNOTITIE

Waarom is dark webmonitoring nuttig? → Het waarschuwt gebruikers als hun gelekte inloggegevens in illegale databases opduiken

5 Vraag 5

Juist antwoord: A

DOCENTENNOTITIE

Wat betekent social engineering? → Mensen manipuleren zodat ze vrijwillig vertrouwelijke inloggegevens prijsgeven

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Vraag 6** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Identiteitsdiefstal kan ook offline beginnen, bijvoorbeeld met gestolen post of documenten.

7 **Vraag 7** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Het afdwingen van MFA op alle persoonlijke accounts blokkeert de meeste credential-stuffing-aanvallen door bots.

8 **Vraag 8** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Een kredietblokkade stopt nieuwe kredietcontroles maar heeft geen invloed op je bestaande rekeningen.

9 **Vraag 9** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Wachtwoordmanagers beschermen gebruikers tegen phishing door wachtwoorden niet automatisch in te vullen op nagemaakte domeinen.

10 **Vraag 10** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Phishing-e-mails gebruiken vaak dringende taal om emotionele, snelle reacties uit te lokken.

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

H 1. INLOGGEGEVENS	D 2. LEKKEN	A 3. MFA	G 4. MONITORING
C 5. BEVRIEZEN	E 6. VERDEDIGING	B 7. SPOOFING	F 8. PHISHING

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 INLOGGEGEVENS	2 DATALEKKEN	3 MFA-VERIFICATIE	4 MONITORING
5 KREDIETBLOKKADE	6 VERDEDIGING		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 H – PHISHING	2 A – INLOGGEGEVENS	3 G – SPOOFING	4 F – VERDEDIGING
5 D – MONITORING	6 E – KREDIETBLOKKADE	7 B – DATALEKKEN	8 C – MFAVERIFICATIE

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen INLOGGEGEVENS, LEKKEN en MFA 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.

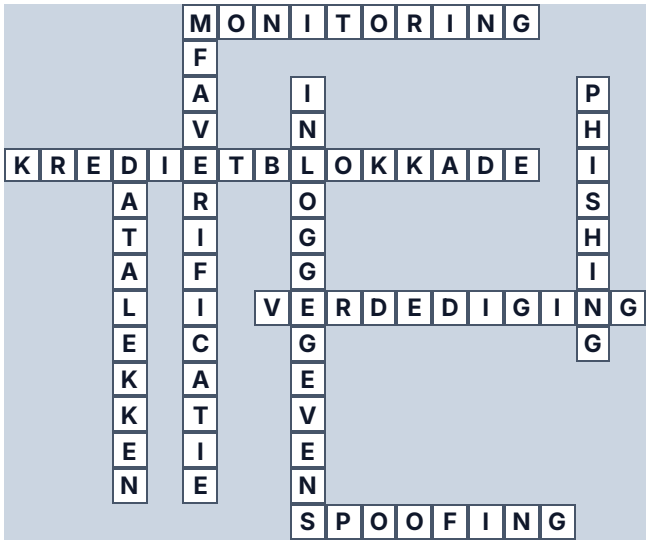
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

1 horizontaal: MONITORING Het scannen van online forums en hackerkanalen op gestolen bedrijfsgegevens. (10 letters)

4 horizontaal: KREDIETBLOKKADE Het beperken van de toegang tot kredietdossiers om frauduleuze leningaanvragen te voorkomen. (15 letters)

6 horizontaal: VERDEDIGING Training en technische maatregelen ter bescherming tegen identiteitsdiefstal. (11 letters)

7 horizontaal: SPOOFING Het maken van een nepwebsite of nep-e-mail om een legitieme organisatie na te bootsen. (8 letters)

VERTICAAL

1 verticaal: MFAVERIFICATIE Aanvullende verificatiestap (zoals hardwaresleutels) die accountaanmeldingen beschermt. (14 letters)

2 verticaal: INLOGGEGEVENS Gebruikersnamen, wachtwoorden en privétokens waarmee digitale identiteiten worden geauthenticeerd. (13 letters)

3 verticaal: PHISHING Het versturen van frauduleuze berichten om gebruikers inloggegevens te laten afgeven. (8 letters)

5 verticaal: DATALEKKEN Ongeautoriseerde blootstelling van privédatabases met persoonlijke gebruikersgegevens. (10 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. ELENGNGVIESGO — **INLOGGEGEVENS**
2. EFRAIIMTFECAIV — **MFAVERIFICATIE**
3. KEORDELKKDBETAI — **KREDIETBLOKKADE**
4. ONGIFSPO — **SPOOFING**
5. KENAAKLDET — **DATALEKKEN**
6. NTIRIMOOGN — **MONITORING**
7. GEVEIGINRDD — **VERDEDIGING**
8. SHHGPNII — **PHISHING**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"BESCHERM JE DIGITALE IDENTITEIT MET MFA"

Antwoordsleutel casestudy's

A Casestudy 1: Bescherming tegen identiteitsimitatie van directieleden

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een hooggeplaatste C-suite-directeur is het doelwit van typosquatting-domeinnamen die zijn persoonlijke e-mail nabootsen om klanten op te lichten. Ontwerp een merkbeschermingsplan.
- Aanbevolen strategie en oplossing: Registreer alle gangbare spellingsvarianten van de naam van de directeur. Zet e-mailauthenticatieprotocollen (DMARC, DKIM, SPF) in om domeinvervalsing te voorkomen. Dwing hardware-MFA af bij alle bedrijfsaanmeldingen van de C-suite.

B Casestudy 2: Blootstelling van zakelijke inloggegevens op het dark web

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een dumpbestand van het dark web bevat enkele honderden bedrijfsinloggegevens van systeembeheerders van een onderneming. Ontwerp een strategie om de gevolgen te beperken.
- Aanbevolen strategie en oplossing: Voer een bedrijfsbrede reset van wachtwoorden uit. Maak het gebruik van een zakelijke wachtwoordmanager verplicht. Dwing MFA af op alle systeemportalen en stel continue, geautomatiseerde waarschuwingen voor dark webmonitoring in.