Namn: _____ Datum: _____ Poäng: _____

Skydd mot identitetsstöld och tillgångar Säkerhetsguide

Läckta inloggningsuppgifter, MFA, övervakning av dark web, varningar om kreditspärr, social manipulation

INLÄRNINGSÖVERSIKT: SKYDD MOT IDENTITETSSTÖLD

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom att förebygga och begränsa identitetsstöld. Du utforskar läckta inloggningsuppgifter, flerfaktorsautentisering, övervakning av den mörka webben, varningar om kreditspärr och försvar mot social manipulation.

KONTROLLPUNKTER I ARBETSBLADET

- [ ] **Del 1-4: Behärska cybersäkerhet och hothantering.**
- [ ] **Del 5-7: Lös korsord och ordsökare.**
- [ ] **Del 8-9: Lös fallstudier och chifferutmaning.**
- [ ] **Del 10: Gå igenom sidorna med grundläggande och avancerade vanliga frågor.**
- [ ] **Del 11: Utforska 10 intressanta fakta från verkligheten.**
- [ ] **Bonus: utmaningen Tänk snabbt.**

Öppna VPN.com:s guide om cybersäkerhet

URL: https://www.vpn.com/sv/cybersakerhet/identitetsstold/

Din inlärningsplan för identitetsskydd

- Förstå riskerna med exponerade inloggningsuppgifter på forum på darkwebben.
- Inför multifaktorautentisering (MFA) och aviseringar om kreditspärr.
- Utforma säkerhetsförsvar för företag mot riktade bedrägerier med social manipulation.

INSTRUKTIONER FÖR GUIDE OM IDENTITETSSTÖLD

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om skydd av identitet. Avsluta med bonusaktiviteten Tänk snabbt.

SKYDD MOT IDENTITETSSTÖLD OCH TILLGÅNGSSÄKERHET (INTRODUKTION)

Identitetsstöld utnyttjar läckta inloggningsuppgifter och svaga inloggningar för att kapa personliga konton och företagskonton. Att använda MFA, kreditspärrar, skannrar för darkweb och ramverken SPF/DKIM/DMARC utgör ett avgörande försvar mot digital förklädnad.

LÄS VARJE KONTROLLPUNKT NOGGRANT OCH VÄLJ ELLER SKRIV DET RÄTTA SVARET.

Kontrollpunkt 1: Utmaning med flerval

1. Vilken är den främsta metoden som identitetstjuvar använder för att stjäla inloggningsuppgifter?

- A. Att skicka falska e-postvarningar som lurar användare att ange lösenord på förfalskade portaler
- B. Att lyssna på radiosändningar nära användarens företagskontor
- C. Att defragmentera användarens lokala serverlagringsenhet
- D. Att koppla bort externa konfigurationer för nätverksbackup

2. Vilken säkerhetskontroll ger det starkaste försvaret mot läckta inloggningsuppgifter?

- A. Flerfaktorsautentisering med hårdvarunycklar
- B. Att skapa långa lösenord med webbläsarens standardformat
- C. Att byta e-postanvändarnamn var sjätte månad
- D. Att radera lagrade cookiebaserade spårningshistoriker i webbläsare

3. Vad representerar kreditspärr?

- A. Att låsa kreditupplysningar för att hindra tjuvar från att ta obehöriga lån
- B. Att radera kontotransaktionshistorik från databaser
- C. Att inaktivera magnetkortläsare för kreditkort på skannrar
- D. Att kryptera lokala databashårddiskar i vila

4. Varför är övervakning av darkweb användbar?

- A. Den varnar användare om deras läckta inloggningsuppgifter dyker upp i olagliga databaser
- B. Den hindrar aktiv skadlig kod från att köras i virtuella sandlådor
- C. Den snabbar upp webbläsarens routinghastighet i virtuella nätverk
- D. Den blockerar försök till SQL-injektion mot backend-databasen

5. Vad innebär social ingenjörskonst?

- A. Att manipulera människor så att de frivilligt avslöjar konfidentiella inloggningsuppgifter
- B. Att skanna företagets serverportar efter aktiva säkerhetsluckor
- C. Att säkerhetskopiera systemets databasfiler till hårddiskar offline
- D. Att dirigera nätverkspaket genom tre krypterade onion-noder

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Identitetsstöld drabbar bara digitala onlinekonton, inte fysisk postgång.

- ○ Sant
- ○ Falskt

7 Fråga 7

7. Att kräva MFA på alla personliga konton blockerar de flesta botattacker med credential stuffing.

- ○ Sant
- ○ Falskt

8 Fråga 8

8. En kreditspärr blockerar kreditkontroller men hindrar dig från att komma åt ditt eget bankkonto.

- ○ Sant
- ○ Falskt

9 Fråga 9

9. Lösenordshanterare skyddar användare mot nätfiske genom att vägra fylla i lösenord automatiskt på förfalskade domäner.

- ○ Sant
- ○ Falskt

10 Fråga 10

10. Nätfiskemejl använder ofta brådskande språk för att framkalla känslomässiga, snabba reaktioner.

- ○ Sant
- ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

Läs varje mening nedan och fyll i luckan med rätt term från ordbanken.

1. Identitetstjuvar riktar in sig på personliga lösenord och användarnas _____ .

2. Varningar till användare om dataintrång avslöjar privata kontons _____ .

3. Att kräva en tillfällig kod för inloggning är en form av autentisering med flera faktorer, förkortat _____ .

4. Att söka igenom hackerforum efter stulna data är _____ av darkweb.

5. Att blockera obehöriga kreditupplysningar kräver ett _____ .

6. Utbildning av anställda i medvetenhet om nätfiske bygger upp ett aktivt _____ i säkerhetsarbetet.

ORDBANK

DATALÄCKOR FÖRSVAR KONTOUPPGIFTER KREDITSPÄRR MFA NÄTFISKE SPOOFING ÖVERVAKNING

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

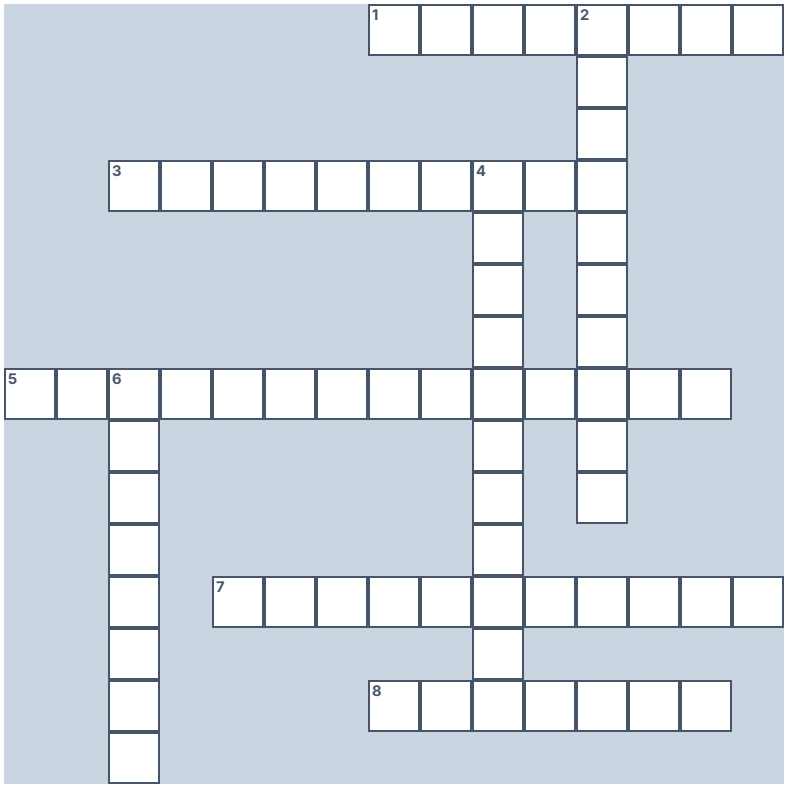
MATCHNING AV DEFINITIONER

Para ihop varje begrepp till vänster med rätt definition till höger genom att skriva motsvarande bokstav (A–H) i det ifyllbara fältet.

☐	1. INLOGGNINGSUPPGIFTER	A	Ett extra verifieringssteg (till exempel hårdvarunycklar) som skyddar kontoinloggningar.
☐	2. LÄCKOR	B	Att skapa en falsk webbplats eller e-post för att efterlikna en legitim organisation.
☐	3. MFA	C	Att begränsa åtkomsten till kreditfiler för att förhindra bedrägliga låneansökningar.
☐	4. ÖVERVAKNING	D	Obehörig exponering av privata databaser som innehåller personliga användarposter.
☐	5. FRYS	E	Utbildning och tekniska kontroller som används för att skydda mot identitetsstöld.
☐	6. FÖRSVAR	F	Skicka bedrägliga meddelanden för att lura användare att lämna ut inloggningsuppgifter.
☐	7. FÖRFALSKNING	G	Att söka igenom onlineforum och hackarkanaler efter stulna företagsdata.
☐	8. NÄTFISKE	H	Användarnamn, lösenord och privata tokens som används för att autentisera digitala identiteter.

Kontrollpunkt 5: Korsord

Lös korsordet genom att skriva bokstäver i de aktiva vita rutorna. Siffrorna motsvarar ledtrådarna nedan.



VÅGRÄTT

1. Att skapa en falsk webbplats eller e-postadress som efterliknar en legitim organisation. (8)

3. Obehörig exponering av privata databaser med användarnas personuppgifter. (10)

5. Användarnamn, lösenord och privata token som används för att autentisera digitala identiteter. (14)

7. Genomsökning av onlineforum och hackerkanaler efter stulna företagsdata. (11)

8. Utbildning och tekniska kontroller som skyddar mot identitetsstöld. (7)

LODRÄTT

2. Extra verifieringssteg (till exempel hårdvarunycklar) som skyddar kontoinloggningar. (10)

4. Begränsning av åtkomsten till kreditfiler för att förhindra bedrägliga låneansökningar. (11)

6. Att skicka bedrägliga meddelanden för att lura användare att lämna ut inloggningsuppgifter. (8)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

Användare av skärmläsare och tangentbord kan skriva korsordssvaren direkt i textfälten nedan.

VÅGRÄTT

1 vågrätt: Att skapa en falsk webbplats eller e-postadress som efterliknar en legitim organisation. (8 bokstäver):

3 vågrätt: Obehörig exponering av privata databaser med användarnas personuppgifter. (10 bokstäver):

5 vågrätt: Användarnamn, lösenord och privata token som används för att autentisera digitala identiteter. (14 bokstäver):

7 vågrätt: Genomsökning av onlineforum och hackerkanaler efter stulna företagsdata. (11 bokstäver):

8 vågrätt: Utbildning och tekniska kontroller som skyddar mot identitetsstöld. (7 bokstäver):

LODRÄTT

2 lodrätt: Extra verifieringssteg (till exempel hårdvarunycklar) som skyddar kontoinloggningar. (10 bokstäver):

4 lodrätt: Begränsning av åtkomsten till kreditfiler för att förhindra bedrägliga låneansökningar. (11 bokstäver):

6 lodrätt: Att skicka bedrägliga meddelanden för att lura användare att lämna ut inloggningsuppgifter. (8 bokstäver):

Kontrollpunkt 6: Dolt ordsök

Hitta de 8 viktiga ordförrådstermerna som är gömda i rutnätet nedan. Orden kan vara vågräta, lodräta eller diagonala.

K R E D I T S P A R R T Ä B I

G N Ö H G N I F O O P S K P F

N R P Z C N Ö Ä G Å Q Y X Ö M

I X R B P Y V N H X D Ä R X L

N R O K C Ä L A T A D S T B Z

K Ö Å N T S Å J Q E V A D L S

A Y Z Z M K I W I A G B F J L

V V U Y T Ö F I R F U C A M R

R C Ö N L Y T W A U Z K N N H

E I O I E K S I F T Ä N T G M

V K O N T O U P P G I F T E R

Ö V M T Z I B W G Ä P Ä Z U I

V Å F L E R F A K T O R A R X

P P Ö Q J R V I R X W Q W W L

A F Q O M B P X G H R S Z Ä K

ORDLISTA

KONTOUPPGIFTER DATALÄCKOR FLERFAKTOR ÖVERVAKNING KREDITSPARR FÖRSVAR SPOOFING NÄTFISKE

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

Para ihop var och en av de 8 begreppen från ordsökningen med rätt definition genom att skriva bokstaven (A–H) på den tomma raden.

ORDLISTA

- **A. KONTOUPPGIFTER**
- **B. DATALÄCKOR**
- **C. FLERFAKTOR**
- **D. ÖVERVAKNING**
- **E. KREDITSPARR**
- **F. FÖRSVAR**
- **G. SPOOFING**
- **H. NÄTFISKE**

DEFINITIONER OCH MATCHNINGSFÄLT

_____ 1. Att skicka bedrägliga meddelanden för att lura användare att lämna ut inloggningsuppgifter.

_____ 2. Användarnamn, lösenord och privata token som används för att autentisera digitala identiteter.

_____ 3. Att skapa en falsk webbplats eller e-postadress som efterliknar en legitim organisation.

_____ 4. Utbildning och tekniska kontroller som skyddar mot identitetsstöld.

_____ 5. Genomsökning av onlineforum och hackerkanaler efter stulna företagsdata.

_____ 6. Begränsning av åtkomsten till kreditfiler för att förhindra bedrägliga låneansökningar.

_____ 7. Obehörig exponering av privata databaser med användarnas personuppgifter.

_____ 8. Extra verifieringssteg (till exempel hårdvarunycklar) som skyddar kontoinloggningar.

Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga begrepp och termer inom cybersäkerhet. Skriv dina svar i rutorna.

1. FUPIPNOGTKE ROT
2. ORFLFRKTAE
3. KSTPERRRIAD
4. ONGIFSPO
5. KÄRAACLDOT
6. VGANNIÖVKE R
7. FAVRÖSR
8. FÄIENKST

Bonusaktivitet: Tänk snabbt

3 SVAR PER KATEGORI. DEN SOM FÖRST FYLLER I LISTAN VINNER.

1	Saker att göra om din identitet har stulits			
2	Saker du inte ska dela på sociala medier			
3	Saker du säkerhetskopierar			
4	Kort eller leg i din plånbok			
5	Dokument du bör skydda			
6	Saker att göra efter en dataläcka			
7	Skäl till att uppdatera programvara			
8	Information som en identitetstjuv vill komma åt			
9	Enheter som kan hackas			
10	Platser som dina uppgifter kan läcka från			
11	Säkra vanor du kan börja med i dag			
12	Tecken på att en dator är infekterad			
13	Sätt att styrka vem du är			
14	Tecken på identitetsstöld			
15	Varningstecken i ett e-postmeddelande			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

Tillämpa de begrepp du har lärt dig för att lösa de verkliga scenarierna nedan.

FALLSTUDIE 1: SKYDD MOT IDENTITETSFÖRFALSKNING AV LEDNING



Scenario: En högt uppsatt företagsledare har utsatts för typosquattade domännamn som efterliknar hens privata e-postadress för att lura kunder. Utforma en plan för varumärkesskydd.

Diskussionsfråga: Analysera riskerna med varumärkesförfalskning och beskriv i detalj SPF/DKIM/DMARC och autentiseringskontroller.

FALLSTUDIE 2: FÖRETAGSUPPGIFTER EXPONERADE PÅ DARK WEB



Scenario: En dump från en databas på darkweb innehåller flera hundra inloggningsuppgifter från företag som tillhör ett företags systemadministratörer. Utforma en strategi för att minska risken.

Diskussionsfråga: Beskriv processen för att rensa upp inloggningsuppgifterna och planera införandet av en lösenordshanterare.

Kontrollpunkt 9: Knäck chiffret

En cybersäkerhetsexpert skyddar nätverkstillgångar mot hotaktörer online. Använd bokstav-till-siffra-nyckeln nedan för att avkoda meddelandet genom att skriva de matchande bokstäverna på de tomma raderna.

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

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 Å=27 Ä=28 Ö=29

19	11	25	4	4	1		4	9	14		9	4	5	14	20	9	20	5	20
										13	5	4							
6	12	5	18	6	1	11	20	15	18	19	9	14	12	15	7	7	14	9	14	7

Avkodat meddelande:

TIPS: VARJE SIFFRA MOTSVARAR BOKSTAVENS PLATS I ALFABETET (T.EX. 1 = A, 2 = B, 29 = Ö).

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del A)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q1: Vad är identitetsstöld?

Ett brott där en angripare stjäl personuppgifter (som lösenord eller personnummer) för att utge sig för att vara någon annan i ekonomiskt syfte.

Q2: Vad är den vanligaste orsaken till identitetsstöld?

Nätfiske är ett av de vanligaste sätten för tjuvar att få tag på lösenord, genom att locka användare till falska, förfalskade webbplatser.

Q3: Hur skyddar flerfaktorsautentisering (MFA) identiteter?

MFA kräver ett andra bevis (som en säkerhetsnyckel) för att logga in och blockerar angripare även om de stjäl ditt lösenord.

Q4: Vad är en kreditspärr?

En gratis tjänst som hindrar kreditupplysningsföretag från att dela din kreditakt och stoppar tjuvar från att ta nya lån i ditt namn. [2]

Q5: Vad är bevakning av darkweb?

Programvara som kontrollerar hackarforum efter läckta e-postadresser, lösenord och personuppgifter och varnar dig om dina data exponeras.

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del B)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q6: Vad betyder credential stuffing?

Automatiserade botar som testar läckta lösenordslistor på hundratals webbplatser för att ta över aktiva konton.

Q7: Varför är e-postförfalskning farligt?

Den låter angripare förfalska avsändarens namn i e-post, så att nätfiskemeddelanden ser ut att komma från betrodda kollegor.

Q8: Hur förhindrar lösenordshanterare identitetsstöld?

De lagrar komplexa, unika lösenord för varje konto och vägrar att automatiskt fylla i inloggningsuppgifter på falska nätfiskedomäner.

Q9: Vad är spjutfiske (spear phishing)?

En mycket riktad nätfiskeattack som anpassas med offrets namn och uppgifter för att öka chansen att lura det.

Q10: Hur skiljer sig en kreditavisering från en kreditspärr?

En varning ber långivare att verifiera din identitet innan konton öppnas, medan en spärr blockerar åtkomsten till din kreditakt helt. [2]

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del C)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q1: Hur leder SIM-byte (SIM swapping) till identitetsstöld?

Angripare övertalar operatörens personal att flytta offrets telefonnummer till ett nytt SIM-kort och kapar på så sätt SMS-baserade 2FA-koder.

Q2: Vilken roll har DMARC för att förhindra identitetsstöld?

DMARC gör det möjligt för domänägare att blockera förfalskade e-postmeddelanden från att nå inkorgar, vilket stoppar falska e-postmeddelanden som imiterar företagsdomäner.

Q3: Varför är syntetisk identitetsstöld svår att upptäcka?

Tjuvar kombinerar riktiga personnummer (SSN) med falska namn och födelsedatum för att bygga helt nya kreditprofiler och kringgå grundläggande bedrägerilarm.

Q4: Hur utnyttjar datamäklare personliga identiteter?

Mäklare (databrokers) samlar in offentliga register, webbbeteende och köphistorik för att sammanställa profildossierer, som kan läcka eller säljas.

Q5: Varför anses SMS-baserad MFA vara sårbar?

SMS-trafik är sårbar för avlyssning, nätfiske och SIM-kortsbyten på operatörsnivå.

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del D)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q6: Vad är en kreditupplysningsspärr?

En kommersiell tjänst som liknar en kreditspärr och låter användare omedelbart låsa eller låsa upp sin kreditakt via en mobilapp.

Q7: Hur göder dataintrång hos företag identitetsstöld?

Läckta databaser exponerar miljontals okrypterade inloggningsuppgifter och ger tjuvar råmaterialet för riktade identitetsbedrägerier.

Q8: Vilken risk innebär att dela för mycket i sociala medier?

Att offentligt dela husdjurs namn, födelseorter och mammans flicknamn ger tjuvar svaren på vanliga kontoåterställningsfrågor.

Q9: Hur skyddar biometriska inloggningar identitetsprofiler?

Biometri kopplar inloggningar till egenskaper som fingeravtryck eller ansikten; när de lagras på enheten är de svåra att stjäla, men lagrade biometriska data kan läcka.

Q10: Hur bekämpar Red Flags Rule identitetsstöld?

En federal förordning som kräver att finansiella institut utarbetar skriftliga program för att upptäcka och agera på varningssignaler för identitetsstöld.

Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

1. SÄKERHETSINSIKT

IdentityTheft.gov, som drivs av FTC, låter offer i USA anmäla identitetsstöld och få en personlig återhämtningsplan. [1]

2. SÄKERHETSINSIKT

Hårdvarusäkerhetsnycklar är nätfiskeresistent MFA, den starkaste sortens MFA som CISA förespråkar. [4]

3. SÄKERHETSINSIKT

Kompromitterade lösenord är en vanlig ingång vid dataintrång och driver senare identitetsbedrägerier.

4. SÄKERHETSINSIKT

En kreditspärr är gratis enligt federal lag och hindrar långivare från att kontrollera kreditakter tills den hävs. [2]

5. SÄKERHETSINSIKT

DMARC låter domänägare tala om för e-postservrar att avvisa eller sätta i karantän förfalskad e-post som misslyckas med kontrollerna. [7]

6. SÄKERHETSINSIKT

SIM-kortsbyte (SIM swapping) gör det möjligt för hackare att kringgå SMS-baserad tvåfaktorsautentisering på bankportaler.

7. SÄKERHETSINSIKT

Bedrägeri med syntetisk identitet blandar verkliga och falska uppgifter, vilket gör det svårt för långivare att upptäcka.

8. SÄKERHETSINSIKT

Många återanvänder samma lösenord på flera onlinekonton, så ett enda dataintrång kan exponera flera av dem.

9. SÄKERHETSINSIKT

Datamäklare sammanställer detaljerade profiler över ett stort antal konsumenter, vilket skapar en koncentrerad risk för den personliga integriteten.

10. SÄKERHETSINSIKT

Att återhämta sig från identitetsstöld kan ta månader av arbete, till exempel att bestrida debiteringar och rätta kreditupplysningar.

Tekniska referenser och källor

Studieguiden och de interaktiva pusslen är sammanställda utifrån globala standarder från NIST och OWASP samt standarder för efterlevnad av dataskydd.

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[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

Facit: Kontrollpunkt 1 – Flerval

1 Fråga 1

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vilken är den främsta metoden som identitetstjuvar använder för att stjäla inloggningsuppgifter? → Att skicka falska e-postvarningar som lurar användare att ange lösenord på förfalskade portaler

2 Fråga 2

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vilken säkerhetskontroll ger det starkaste försvaret mot läckta inloggningsuppgifter? → Flerfaktorsautentisering med hårdvarunycklar

3 Fråga 3

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad representerar kreditspärr? → Att låsa kreditupplysningar för att hindra tjuvar från att ta obehöriga lån

4 Fråga 4

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Varför är övervakning av darkweb användbar? → Den varnar användare om deras läckta inloggningsuppgifter dyker upp i olagliga databaser

5 Fråga 5

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad innebär social ingenjörskonst? → Att manipulera människor så att de frivilligt avslöjar konfidentiella inloggningsuppgifter

Facit: Kontrollpunkt 2 – Sant eller falskt

6 Fråga 6

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Identitetsstöld kan också börja offline, till exempel med stulen post eller stulna dokument.

7 Fråga 7

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Att kräva MFA på alla personliga konton blockerar de flesta botattacker med credential stuffing.

8 Fråga 8

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

En kreditspärr stoppar nya kreditkontroller men påverkar inte dina befintliga konton.

9 Fråga 9

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Lösenordshanterare skyddar användare mot nätfiske genom att vägra fylla i lösenord automatiskt på förfalskade domäner.

10 Fråga 10

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Nätfiskemejl använder ofta brådskande språk för att framkalla känslomässiga, snabba reaktioner.

Facit för ordförråd och bedömningsmall

Bedömningsmatris för läraren: Ge 1 poäng för varje korrekt matchning (totalt 8 poäng) och kontextbegrepp (totalt 6 poäng).

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

H 1. INLOGGNINGSUPPGIFTER	D 2. LÄCKOR	A 3. MFA	G 4. ÖVERVAKNING
C 5. FRYS	E 6. FÖRSVAR	B 7. FÖRFALSKNING	F 8. NÄTFISKE

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 KONTOUPPGIFTER	2 DATALÄCKOR	3 MFA	4 ÖVERVAKNING
5 KREDITSPÄRR	6 FÖRSVAR		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 H – NÄTFISKE	2 A – KONTOUPPGIFTER	3 G – SPOOFING	4 F – FÖRSVAR
5 D – ÖVERVAKNING	6 E – KREDITSPARR	7 B – DATALÄCKOR	8 C – FLERFAKTOR

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara INLOGGNINGSUPPGIFTER, LÄCKOR och MFA med egna ord och ge ett exempel på varje.

Fallstudier:
Be eleverna att stödja sina rekommendationer med fakta från arbetsbladet, inte med antaganden.

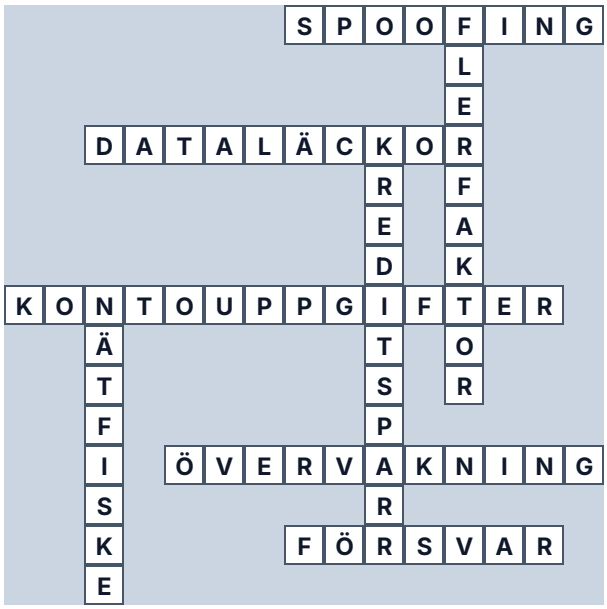
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

1 vågrätt: SPOOFING Att skapa en falsk webbplats eller e-postadress som efterliknar en legitim organisation. (8 bokstäver)

3 vågrätt: DATALÄCKOR Obehörig exponering av privata databaser med användarnas personuppgifter. (10 bokstäver)

5 vågrätt: KONTOUPPGIFTER Användarnamn, lösenord och privata token som används för att autentisera digitala identiteter. (14 bokstäver)

7 vågrätt: ÖVERVAKNING Genomsökning av onlineforum och hackerkanaler efter stulna företagsdata. (11 bokstäver)

8 vågrätt: FÖRSVAR Utbildning och tekniska kontroller som skyddar mot identitetsstöld. (7 bokstäver)

LODRÄTT

2 lodrätt: FLERFAKTOR Extra verifieringssteg (till exempel hårdvarunycklar) som skyddar kontoinloggningar. (10 bokstäver)

4 lodrätt: KREDITSPARR Begränsning av åtkomsten till kreditfiler för att förhindra bedrägliga låneansökningar. (11 bokstäver)

6 lodrätt: NÄTFISKE Att skicka bedrägliga meddelanden för att lura användare att lämna ut inloggningsuppgifter. (8 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1.	FUPIPNOGTKEROT	KONTOUPPGIFTER	5.	KÄRAACLDOT	DATALÄCKOR
2.	ORFLFRKTAE	FLERFAKTOR	6.	VGANNIÖVKER	ÖVERVAKNING
3.	KSTPERRRIAD	KREDITSPARR	7.	FAVRÖSR	FÖRSVAR
4.	ONGIFSPO	SPOOFING	8.	FÄIENKST	NÄTFISKE

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"SKYDDA DIN IDENTITET MED FLERFAKTORSINLOGGNING"

Facit till fallstudierna

A Fallstudie 1: Skydd mot identitetsförfalskning av ledning

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En högprofilerad chef i företagsledningen har utsatts för domännamn med stavfel som imiterar hens privata e-post för att lura kunder. Utforma en plan för varumärkesskydd.
- Rekommenderad strategi och lösning: Registrera alla vanliga stavningsvarianter av chefens namn. Inför e-postautentisering (DMARC, DKIM, SPF) för att förhindra domänförfalskning. Tillämpa hårdvarubaserad MFA för alla inloggningar i företagsledningen.

B Fallstudie 2: Företagsuppgifter exponerade på dark web

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En datadump från den mörka webben innehåller flera hundra inloggningsuppgifter till företag som tillhör systemadministratörer i ett storföretag. Utforma en strategi för att begränsa skadan.
- Rekommenderad strategi och lösning: Genomför en lösenordsåterställning i hela företaget. Kräv att en lösenordshanterare för företag används. Tillämpa MFA i alla systemportaler och ställ in kontinuerliga automatiska varningar från bevakning av darkweb.