Namn: _____ Datum: _____ Poäng: _____

Nätfiskeattacker och social manipulation

Spear phishing, bedrägerier mot toppchefer (whaling), protokollen SPF/DKIM/DMARC, avsändarförfalskning och säkerhetsutbildning för anställda.

LÄRANDEÖVERSIKT: NÄTFISKEATTACKER

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom nätfiskeattacker och social manipulation. Du utforskar spjutfiske, valfiske (whaling), domänförfalskning, protokollen SPF/DKIM/DMARC, länksäkerhet och utbildning för att öka de anställdas medvetenhet.

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/natfiskeattacker/

Din inlärningsplan för att begränsa nätfiske

- Identifiera vanliga bedrägerier med nätfiske, vishing och supportpopupfönster.
- Inför rutiner för transaktionsverifiering utanför bandet.
- Konfigurera regler för SPF, DKIM och DMARC för att blockera förfalskade domäner.

INSTRUKTIONER FÖR GUIDEN OM NÄTFISKEATTACKER

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

NÄTFISKEATTACKER OCH SOCIAL MANIPULATION (INTRODUKTION)

Nätfiskeattacker använder riktade meddelanden, whaling-bedrägerier och domänförfalskning för att samla in användares inloggningsuppgifter. Att säkra företagssystem kräver att SPF-, DKIM- och DMARC-regler införs vid gatewayen tillsammans med godkännandesteg via en separat kanal (out-of-band).

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

Kontrollpunkt 1: Utmaning med flerval

1. Vad är spear phishing?

- A. Ett riktat nätfiskemejl anpassat till en specifik person eller organisation
- B. Ett brett massutskick av e-post till miljontals slumpmässiga adresser
- C. Ett nätverksangrepp som översvämmar webbservrar med trafik
- D. En teknik för att extrahera databasdata riktad mot användarposter

2. Vilket protokoll låter en domän lista sina auktoriserade avsändande IP-adresser i DNS för att bekämpa förfalskning?

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

3. Vad är en whaling-attack?

- A. En nätfiskekampanj riktad specifikt mot högt uppsatta företagsledare
- B. Ett SQL-injektionsangrepp mot databassäkerhetskopior
- C. Fysisk stöld av lokal routerutrustning
- D. En automatiserad brute force-skanning med credential stuffing

4. Vad gör DKIM?

- A. Lägger till en kryptografisk signatur i e-post för att verifiera avsändarens äkthet
- B. Blockerar inkommande nätverkspaket i brandväggen
- C. Krypterar databaslagringsvolymer i vilande tillstånd
- D. Skannar e-postbilagor efter signaturbaserad skadlig kod

5. Vilken roll har DMARC?

- A. Att tala om för mottagande e-postservrar hur misslyckade SPF/DKIM-kontroller ska hanteras
- B. Att dekryptera systemlösenord med förberäknade regnbågstabeller
- C. Att komprimera e-postbilagor före leverans
- D. Att konfigurera behörigheter för nätverksroutning

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Spear phishing bygger på generiska massmejl som skickas till miljontals slumpmässiga adresser.

- ○ Sant
- ○ Falskt

7 Fråga 7

7. DMARC-policyer kan instruera e-postservrar att avvisa obehöriga förfalskade meddelanden.

- ○ Sant
- ○ Falskt

8 Fråga 8

8. SPF-verifiering fungerar genom att validera den kryptografiska signaturen för e-postens brödtext.

- ○ Sant
- ○ Falskt

9 Fråga 9

9. Whaling-attacker riktar sig mot administratörer på låg nivå i företag för att komma åt databasfiler.

- ○ Sant
- ○ Falskt

10 Fråga 10

10. Verifiering utanför bandet av betalningsförfrågningar hjälper till att stoppa bedrägerier med banköverföringar.

- ○ Sant
- ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. Att rikta in sig på en viss anställd med personlig information kallas _____ .

2. Att förfalska ett e-posthuvud så att meddelanden ser legitima ut kallas _____ av avsändare.

3. DNS-postlistan över auktoriserade IP-adresser för e-postservrar är _____ .

4. Standarden för e-postsignatur som ger avsändarverifiering är _____ .

5. Att fastställa policyer som avvisar misslyckade SPF-/DKIM-kontroller sker med _____ .

6. En nätfiskekampanj riktad mot toppchefer kallas _____ .

ORDBANK

DKIM | DMARC | SMISHING | SPEAR PHISHING | SPF | SPOOFING | VISHING | WHALING

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

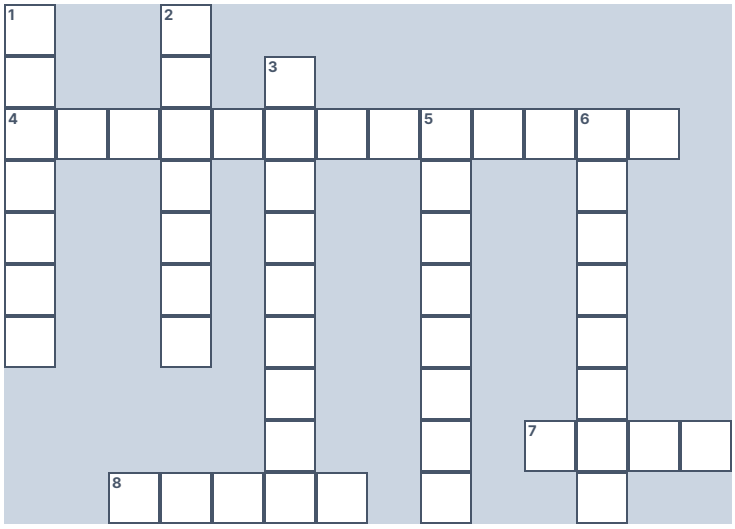
MATCHNING AV DEFINITIONER

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

☐	1. SPEAR	A	Bedrägerisamtal via röst.
☐	2. FÖRFALSKNING	B	Riktar in sig på chefer på C-nivå.
☐	3. SPF	C	Instruktioner för policyavslag.
☐	4. DKIM	D	IP-adresser som är auktoriserade att skicka för DNS.
☐	5. DMARC	E	Mejl med social manipulation.
☐	6. WHALING	F	Personligt riktat e-postmeddelande.
☐	7. NÄTFISKE	G	Förfalskad avsändaradress i e-post.
☐	8. VISHING	H	Kryptografisk signatur i e-post.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

4. Personligt riktat e-postmeddelande. (13)

7. Kryptografisk signatur i e-post. (4)

8. Policy med instruktioner om att avvisa meddelanden. (5)

LODRÄTT

1. Bedrägliga samtal via röst. (7)

2. Riktat mot toppchefer. (7)

3. DNS-poster med behöriga avsändar-IP-adresser. (9)

5. Förfalskning av avsändarens e-postadress. (8)

6. Social manipulation via e-post. (8)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

4 vågrätt: Personligt riktat e-postmeddelande. (13 bokstäver):

7 vågrätt: Kryptografisk signatur i e-post. (4 bokstäver):

8 vågrätt: Policy med instruktioner om att avvisa meddelanden. (5 bokstäver):

LODRÄTT

1 lodrätt: Bedrägliga samtal via röst. (7 bokstäver):

2 lodrätt: Riktat mot toppchefer. (7 bokstäver):

3 lodrätt: DNS-poster med behöriga avsändar-IP-adresser. (9 bokstäver):

5 lodrätt: Förfalskning av avsändarens e-postadress. (8 bokstäver):

6 lodrätt: Social manipulation via e-post. (8 bokstäver):

Kontrollpunkt 6: Dolt ordsök

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

V I S H I N G S C U S Q I U C

Y E V Ä X C C P Ö Y N G L I Ö

D G O E S R Z O R C Ä W B A Ö

R N P E A M A O E Q T E F H J

E I D M T S N F F J F U Ö U G

T L D S Y F A I A S I Q O R W

S A Å S L T W N U D S O Ä B G

O H U Z Z K A G T Ö K Ä Ä M H

P W J O T L N N V Q E I S S H

F Ö A Q X G X C Ä T Ä B I N Ö

P S P E A R P H I S H I N G H

S K P D R P Z C N Ö Ä G Å Q Y

X M K X R B P Y V N H X D Ä X

L I T B Z Ö Å N T S Å J Q E A

M D L S Y Z Z M K I W I G B F

ORDLISTA

SPEARPHISHING SPOOFING SPFPOSTER DKIM DMARC WHALING NÄTFISKE VISHING

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. SPEARPHISHING**
- **B. SPOOFING**
- **C. SPFPOSTER**
- **D. DKIM**
- **E. DMARC**
- **F. WHALING**
- **G. NÄTFISKE**
- **H. VISHING**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Förfalskning av avsändarens e-postadress.
2. Personligt riktat e-postmeddelande.
3. Bedrägliga samtal via röst.
4. DNS-poster med behöriga avsändar-IP-adresser.
5. Social manipulation via e-post.
6. Policy med instruktioner om att avvisa meddelanden.
7. Kryptografisk signatur i e-post.
8. Riktat mot toppchefer.

Kontrollpunkt 7: Utmaning med blandade ord

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

1. **HESNPPIHSIG RA** _____

2. **RSEPPSTOF** _____

3. **ADCRM** _____

4. **FKESINÄT** _____

5. **FIPGOSNO** _____

6. **IMDK** _____

7. **WNIGHLA** _____

8. **IHGVNIS** _____

Bonusaktivitet: Tänk snabbt

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

1	Enheter som kan hackas			
2	Tecken på ett nätfiskemejl			
3	Tecken på att en dator är infekterad			
4	Ord som skapar falsk brådska			
5	Sätt att kontrollera en avsändare			
6	Personer du kan fråga om IT-hjälp			
7	Saker du säkerhetskopierar			
8	Fiskar eller havsdjur du känner till			
9	Företag som bedragare utger sig för att vara			
10	Säkra vanor du kan börja med i dag			
11	Saker att göra efter att ha klickat på en falsk länk			
12	Saker att göra efter en dataläcka			
13	Kanaler där nätfiske förekommer			
14	Saker du aldrig skickar med e-post			
15	Sätt att skydda dina konton			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

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

FALLSTUDIE 1: ÅTGÄRDER MOT WHALING-ATTACK MOT LEDNINGEN



Scenario: En finansdirektör får ett mycket personligt e-postmeddelande som påstås komma från vd:n, med en begäran om en snabb överföring på 50 000 USD för att slutföra ett konfidentiellt domänköp.

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

FALLSTUDIE 2: INFÖRA GATEWAY-POLICYER FÖR SPF/DKIM/DMARC



Scenario: Ett företag misslyckas med säkerhetsrevisioner eftersom utgående marknadsföringsmejl ofta flaggas som skräppost och hackare aktivt förfalskar företagets varumärkesdomän.

Diskussionsfråga: Ta fram tekniska och administrativa kontroller för att verifiera e-postens äkthet.

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

21	16	16	20	28	3	11		19	15	3	9	1	12
13	1	14	9	16	21	12	1	20	9	15	14	9	5	16	15	19	20

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 nätfiske?

Nätfiske är en attack med social manipulation där brottslingar skickar bedrägliga meddelanden för att lura användare att dela känsliga data.

Q2: Vad är skillnaden mellan nätfiske och spear phishing?

Nätfiske riktas mot breda grupper med generiskt innehåll, medan spear phishing riktas mot specifika offer med anpassade uppgifter.

Q3: Vad är whaling?

Whaling är en mycket riktad nätfiskeattack mot högt uppsatta chefer som har administrativ makt.

Q4: Vad är e-postförfalskning (email spoofing)?

E-postförfalskning är skapandet av e-postmeddelanden med förfalskad avsändaradress för att lura mottagaren att lita på källan.

Q5: Hur förhindrar SPF förfalskning?

Den publicerar en lista över behöriga sändande IP-adresser i DNS, så att mottagande servrar kan verifiera e-postens källa. [1]

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

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

Q6: Vad är DKIM?

DomainKeys Identified Mail lägger till en kryptografisk signatur i e-postens huvuden, vilket bevisar att en domän tagit ansvar och att meddelandet inte ändrats.

Q7: Vad står DMARC för?

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

Q8: Vad är en DMARC-policy?

En policy som talar om för e-postservrar hur meddelanden som misslyckas med SPF/DKIM ska hanteras (none, quarantine eller reject). [2]

Q9: Vad är vishing?

Röstnätfiske (vishing), där angripare använder bedrägliga telefonsamtal för att få fram administrativa eller finansiella uppgifter.

Q10: Hur hjälper länkskannrar?

De skannar och skriver om inkommande e-postlänkar för att verifiera säkerheten hos målsidorna i det ögonblick du klickar.

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

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

Q1: Hur fungerar en homografattack?

Angripare registrerar domännamn med liknande icke-ASCII-tecken i Unicode för att visuellt efterlikna ett legitimt domännamn.

Q2: Vad är en punycode-representation?

En kodning som omvandlar Unicode-domännamn till ASCII-kompatibla strängar som börjar med "xn--" så att DNS kan hantera dem.

Q3: Varför är "p=reject" det säkraste DMARC-läget?

Den ber mottagande servrar avvisa e-post som misslyckas med DMARC (justerad SPF/DKIM) under SMTP-sessionen, vilket blockerar direkt förfalskning. [2]

Q4: Hur kringgår angripare SPF-regler?

Genom att utnyttja liknande domäner (typosquatting) eller använda komprometterade konton på legitima e-posttjänster från tredje part.

Q5: Vad är komprometterad företagsmejl (BEC)?

Ett företagsbedrägeri där angripare kapar eller imiterar företags e-postkonton för att godkänna bedrägliga betalningar.

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

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

Q6: Hur stoppar flerfaktorsautentisering nätfiske?

Den kräver sekundära tokens (som hårdvarunycklar) som inte kan stjälas enbart via förfalskade målsidor.

Q7: Vad är en målsida för att samla in inloggningsuppgifter?

En förfalskad inloggningsportal som är utformad för att fånga inmatade användarnamn, lösenord och MFA-koder i realtid.

Q8: Vad är kapning av underdomäner?

En angripare som tar kontroll över en oanvänd DNS-underdomänpekare för att vara värd för skadliga nätfiskesidor under en betrodd överordnad domän.

Q9: Hur fungerar DKIM-justeringskontrollen?

Den verifierar att domänen i huvudet "From" matchar den domän som kryptografiskt signerade meddelandet i DKIM-huvudet.

Q10: Vilken roll har en e-postgateway?

Filtrering av inkommande e-post, granskning av länkar, körning av bilagor i sandlåda och validering av efterlevnad av SPF/DKIM/DMARC.

Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

1. SÄKERHETSINSIKT

Nätfiske och förfalskning (spoofing) var den mest anmälda brottstypen till FBI:s IC3 2025, med 191 561 anmälningar. [4]

2. SÄKERHETSINSIKT

Business email compromise (BEC) orsakade förluster på över 3 miljarder USD som rapporterades till FBI:s IC3 under 2025. [4]

3. SÄKERHETSINSIKT

Homografattacker använder kyrilliska tecken som liknar latinska bokstäver för att visuellt kopiera domäner med exakt matchande varumärken i webbläsare.

4. SÄKERHETSINSIKT

Med ”p=reject” ber en domän mottagarna att avvisa e-post som inte klarar kontrollen under leveransen, inte lägga den i skräppost. [2]

5. SÄKERHETSINSIKT

Whaling-attacker mot vd:ar kräver ofta brådskande betalningar för konfidentiella fusioner eller domänköp.

6. SÄKERHETSINSIKT

Portaler för insamling av inloggningsuppgifter kopierar riktiga inloggningssidor så att offren skriver in lösenord direkt i angriparens formulär.

7. SÄKERHETSINSIKT

CISA:s gemensamma vägledning om nätfiske rekommenderar användarutbildning vid sidan av DMARC, SPF, DKIM och nätfiskesäker MFA. [3]

8. SÄKERHETSINSIKT

SPF-utvärderingen är begränsad till 10 termer som kräver DNS-frågor; om gränsen överskrids returneras resultatet 'permerror'. [1]

9. SÄKERHETSINSIKT

Maskinvarubaserade säkerhetsnycklar med FIDO2 ger kryptografiskt förankrat skydd mot fjärrinsamling av inloggningsuppgifter.

10. SÄKERHETSINSIKT

Nätfiske är ett av de vanligaste sätten för angripare att först ta sig in i en organisation, vilket är anledningen till att regelbunden utbildning i medvetenhet är ett effektivt försvar.

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] 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

Facit: Kontrollpunkt 1 – Flerval

1 Fråga 1 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad är spear phishing? → Ett riktat nätfiskemejl anpassat till en specifik person eller organisation

2 Fråga 2 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

SPF publicerar en domäns auktoriserade avsändande värdar i DNS så att mottagare kan kontrollera kuvertavsändaren.

3 Fråga 3 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad är en whaling-attack? → En nätfiskekampanj riktad specifikt mot högt uppsatta företagsledare

4 Fråga 4 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad gör DKIM? → Lägger till en kryptografisk signatur i e-post för att verifiera avsändarens äkthet

5 Fråga 5 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vilken roll har DMARC? → Att tala om för mottagande e-postservrar hur misslyckade SPF/DKIM-kontroller ska hanteras

Facit: Kontrollpunkt 2 – Sant eller falskt

6 Fråga 6

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: spear phishing är skräddarsytt för specifika personer, till skillnad från generiskt massutskickat nätfiske.

7 Fråga 7

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

DMARC-policyer kan instruera e-postservrar att avvisa obehöriga förfalskade meddelanden.

8 Fråga 8

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: SPF kontrollerar den avsändande IP-adressen mot DNS; det är DKIM som verifierar en kryptografisk signatur.

9 Fråga 9

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: whaling riktar sig mot högre chefer, som kan godkänna betalningar och komma åt känsliga data.

10 Fråga 10

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Sant: att bekräfta betalningsförfrågningar via en separat, känd kanal hjälper till att stoppa bedrägerier med banköverföringar.

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

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

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 SPEAR PHISHING	2 SPOOFING	3 SPF	4 DKIM
5 DMARC	6 WHALING		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

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

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara SPEAR, FÖRFALSKNING och SPF med egna ord och ge ett exempel på varje.

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

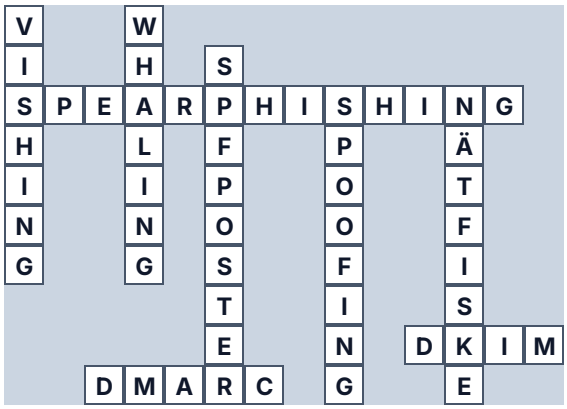
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

4 vågrätt: SPEARPHISHING Personligt riktat e-postmeddelande. (13 bokstäver)

7 vågrätt: DKIM Kryptografisk signatur i e-post. (4 bokstäver)

8 vågrätt: DMARC Policy med instruktioner om att avvisa meddelanden. (5 bokstäver)

LODRÄTT

1 lodrätt: VISHING Bedrägliga samtal via röst. (7 bokstäver)

2 lodrätt: WHALING Riktat mot toppchefer. (7 bokstäver)

3 lodrätt: SPFPOSTER DNS-poster med behöriga avsändar-IP-adresser. (9 bokstäver)

5 lodrätt: SPOOFING Förfalskning av avsändarens e-postadress. (8 bokstäver)

6 lodrätt: NÄTFISKE Social manipulation via e-post. (8 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1.	HESNPPIHSIGRA	SPEARPHISHING	5.	FIPGOSNO	SPOOFING
2.	RSEPPSTOF	SPFPOSTER	6.	IMDK	DKIM
3.	ADCRM	DMARC	7.	WNIGHLA	WHALING
4.	FKESINÄT	NÄTFISKE	8.	IHGVNIS	VISHING

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"UPPTÄCK SOCIAL MANIPULATION I EPOST"

Facit till fallstudierna

A Fallstudie 1: Åtgärder mot whaling-attack mot ledningen

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En ekonomichef får ett mycket personligt utformat e-postmeddelande som utger sig för att komma från vd:n och begär en snabb överföring på 50 000 USD för att slutföra ett konfidentiellt domänköp.
- Rekommenderad strategi och lösning: Konfigurera DMARC med policyn "p=reject" för att blockera förfalskade avsändardomäner. Lägg till varningsbanderoller för externa avsändare i gatewayen och kräv muntlig bekräftelse utanför bandet för alla finansiella transaktioner.

B Fallstudie 2: Införa gateway-policyer för SPF/DKIM/DMARC

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: Ett företag misslyckas med säkerhetsgranskningar eftersom utgående marknadsföringsmejl ofta flaggas som skräppost och hackare aktivt förfalskar företagets varumärkesdomän.
- Rekommenderad strategi och lösning: Publicera en TXT-post för SPF som anger tillåtna avsändar-IP-adresser. Konfigurera DKIM-signeringsnycklar på utgående e-postservrar och analysera inkommande DMARC XML-återkopplingsrapporter för att upptäcka missbruk.