Namn: _____ Datum: _____ Poäng: _____

Nätbedrägerier och social manipulation Skyddsguide

E-postnätfiske, förfalskade domäner, vishing, supportbedrägerier, verifiering via en separat kanal, BEC

LÄRANDEÖVERSIKT: NÄTBEDRÄGERIER

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom skydd mot bedrägerier på nätet. Du utforskar falska nätfiskewebbplatser, taktik för social manipulation, supportbedrägerier, vektorer för bankbedrägerier och metoder för betalningsverifiering.

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/bedrerier-natet/

Din inlärningsplan för skydd mot nätbedrägerier

- Identifiera vanliga tecken på supportbedrägerier och typosquatting-domäner.
- Inför protokoll för e-postverifiering (SPF, DKIM, DMARC) mot förfalskning.
- Upprätta verifiering av transaktioner via en separat kanal för att förhindra bedrägerier med företagsbanköverföringar.

INSTRUKTIONER FÖR GUIDEN OM NÄTBEDRÄGERIER

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 mot bedrägerier på nätet. Avsluta med bonusaktiviteten Tänk snabbt.

NÄTBEDRÄGERIER OCH SKYDD MOT SOCIAL MANIPULATION (INTRODUKTION)

Nätbedrägerier utnyttjar mänskligt beteende genom nätfiske, popup-fönster om support, vishing och bedrägerier med banköverföringar. Att kräva verifiering av transaktioner via en separat kanal (out-of-band) och domänregler för SPF/DKIM/DMARC hjälper till att blockera angrepp med social manipulation vid gatewayen.

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

Kontrollpunkt 1: Utmaning med flerval

1. Vad är det främsta tecknet på ett supportbedrägeri?

- A. Ett popup-fönster som påstår att ditt system är infekterat och kräver att du ringer ett telefonnummer
- B. En automatisk säkerhetsuppdatering som laddas ned från ett officiellt register
- C. En lösenordshanterare som vägrar fylla i inloggningsuppgifter på en företagsdomän
- D. En säkerhetskopiering av filer i bakgrunden på en extern enhet

2. Vilken teknik använder förfalskade avsändardomäner för att stjäla bankuppgifter?

- A. Nätfiske via e-post
- B. Portskanning
- C. Minnesinjektion
- D. Kryptografisk strimling

3. Vad representerar bedrägeri med banköverföringar?

- A. Att lura offer att skicka pengar till falska företagskonton med hjälp av social manipulation
- B. Att kryptera systemdatabaser med ransomware-nyttolaster
- C. Att fråga databaser via SQL-injektionskommandon
- D. Att säkerhetskopiera systemfiler till offline-lagringsdiskar

4. Varför skapar bedragare falska webbutiker?

- A. För att stjäla kreditkortsuppgifter och betalningsuppgifter från köpare
- B. För att vara värd för databastabeller för sandlådeanalys av skadlig kod
- C. Att snabba upp leveransen av onlinebeställningar
- D. För att testa nya webbplatsdesigner gratis

5. Vad betyder vishing?

- A. Röstbaserade nätfiskebedrägerier över telefonnät för att stjäla inloggningsuppgifter
- B. Att skanna lokala nätverk efter osäkrade systemenheter
- C. Att återställa systemdatabaser efter ett obehörigt intrång
- D. Att köra opålitlig kod i säkra virtuella containrar

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Nätfiskebedrägerier riktas bara mot slutanvändare, aldrig mot whaling-mål bland chefer.

- ○ Sant
- ○ Falskt

7 Fråga 7

7. Förfalskade domäner använder ofta små stavfel (som amaz0n.com) för att imitera betrodda varumärken.

- ○ Sant
- ○ Falskt

8 Fråga 8

8. Supportbedrägerier kan lösas genom att ge den som ringer fjärråtkomst.

- ○ Sant
- ○ Falskt

9 Fråga 9

9. Social manipulation utnyttjar mänsklig psykologi, som rädsla och brådska, för att kringgå säkerhetsregler.

- ○ Sant
- ○ Falskt

10 Fråga 10

10. Förfrågningar om banköverföring bör alltid verifieras via kommunikationskanaler utanför det ursprungliga flödet.

- ○ Sant
- ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. Bedrägliga e-postmeddelanden som lurar användare kallas _____ .
2. Webbadresser som härmar betrodda varumärken är _____ .
3. Röstbedrägerier som riktar in sig på bankuppgifter kallas _____ .
4. Ett popup-fönster som kräver pengar för att ta bort virus är ett falskt supporterbjudande, alltså ett _____ .
5. Att bekräfta en betalningsbegäran kräver _____ via en annan kanal.
6. Att omdirigera företagstransaktioner till tjuvars konton kallas _____ .

ORDBANK

BEDRÄGERI NÄTFISKE OMDIRIGERING SMISHING SPOOFADE VERIFIERING VISHING WHALING

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

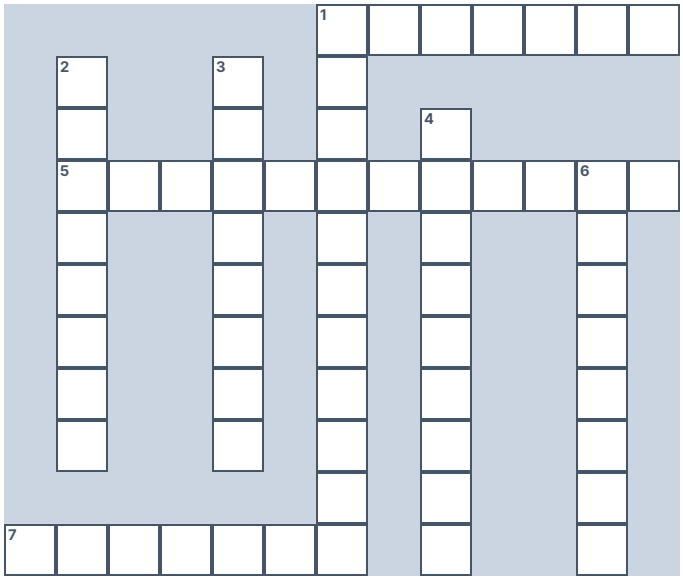
MATCHNING AV DEFINITIONER

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

☐	1. NÄTFISKE	A	Bedräglig omdirigering av banktransaktioner till kriminella konton.
☐	2. FÖRFALSKAD	B	Bedrägeri som syftar till att stjäla pengar eller inloggningsuppgifter från offer.
☐	3. VISHING	C	Skicka bedrägliga sms för att stjäla inloggningsuppgifter till mobilkonton.
☐	4. BEDRÄGERI	D	Bedrägliga röstsamtal utformade för att stjäla inloggningsuppgifter och kontouppgifter.
☐	5. VERIFIERING	E	Riktade nätfiskeattacker som syftar till att stjäla inloggningsuppgifter från chefer på C-nivå.
☐	6. ÖVERFÖRING	F	Förfalskad e-postavsändare eller webbadress som är utformad för att se legitim ut.
☐	7. WHALING	G	Bedrägliga e-postkampanjer utformade för att stjäla inloggningsuppgifter och lösenord.
☐	8. SMISHING	H	Att bekräfta betalningsuppgifter med en betrodd sekundär kontaktmetod.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

1. Bedrägliga röstsamtal som syftar till att stjäla inloggnings- och kontouppgifter. (7)

5. Bedräglig omdirigering av banktransaktioner till brottslingars konton. (12)

7. Riktade nätfiskeattacker som syftar till att stjäla inloggningsuppgifter från högsta chefer. (7)

LODRÄTT

1. Bekräftelse av betalningsuppgifter via en betrodd sekundär kontaktmetod. (11)

2. Imiterad e-postavsändare eller webbadress som är utformad för att se legitim ut. (8)

3. Utskick av bedrägliga sms för att stjäla inloggningsuppgifter till mobilkonton. (8)

4. Bedrägligt upplägg som syftar till att stjäla pengar eller inloggningsuppgifter från offer. (9)

6. Bedrägliga e-postkampanjer som syftar till att stjäla inloggningsuppgifter och lösenord. (8)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

1 vågrätt: Bedrägliga röstsamtal som syftar till att stjäla inloggnings- och kontouppgifter. (7 bokstäver):

5 vågrätt: Bedräglig omdirigering av banktransaktioner till brottslingars konton. (12 bokstäver):

7 vågrätt: Riktade nätfiskeattacker som syftar till att stjäla inloggningsuppgifter från högsta chefer. (7 bokstäver):

LODRÄTT

1 lodrätt: Bekräftelse av betalningsuppgifter via en betrodd sekundär kontaktmetod. (11 bokstäver):

2 lodrätt: Imiterad e-postavsändare eller webbadress som är utformad för att se legitim ut. (8 bokstäver):

3 lodrätt: Utskick av bedrägliga sms för att stjäla inloggningsuppgifter till mobilkonton. (8 bokstäver):

4 lodrätt: Bedrägligt upplägg som syftar till att stjäla pengar eller inloggningsuppgifter från offer. (9 bokstäver):

6 lodrätt: Bedrägliga e-postkampanjer som syftar till att stjäla inloggningsuppgifter och lösenord. (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 N V Ä X C Ö Y G
G G L I Ö D O Ä E S S Z R C W
N N B A Ö P E T M A P E Q E F
I I H J D T S F N F O J U Ö U
R H G S Y F A I A S O Q O B R
E S W Å S L T S W U F D O E Ä
I I B G U Z Z K K A A T Ö D Ä
F M Ä M H J O E T L D N N R V
I S Q I S S H Ö A Q E X G Ä X
R C Ä T Ä B I N Ö H K P R G P
E O M D I R I G E R I N G E Z
V C N Ö Ä G Å Q Y X M X R R B
P Y W H A L I N G V N H X I D
Ä X L T B Z Ö Å N T S Å J Q E
A D L S Y Z Z M K I W I G B F

ORDLISTA

NÄTFISKE SPOOFADE VISHING BEDRÄGERI VERIFIERING OMDIRIGERING WHALING SMISHING

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. NÄTFISKE**
- **B. SPOOFADE**
- **C. VISHING**
- **D. BEDRÄGERI**
- **E. VERIFIERING**
- **F. OMDIRIGERING**
- **G. WHALING**
- **H. SMISHING**

DEFINITIONER OCH MATCHNINGSFÄLT

_____ 1. Imiterad e-postavsändare eller webbadress som är utformad för att se legitim ut.

_____ 2. Bekräftelse av betalningsuppgifter via en betrodd sekundär kontaktmetod.

_____ 3. Bedräglig omdirigering av banktransaktioner till brottslingars konton.

_____ 4. Utskick av bedrägliga sms för att stjäla inloggningsuppgifter till mobilkonton.

_____ 5. Riktade nätfiskeattacker som syftar till att stjäla inloggningsuppgifter från högsta chefer.

_____ 6. Bedrägliga röstsamtal som syftar till att stjäla inloggnings- och kontouppgifter.

_____ 7. Bedrägliga e-postkampanjer som syftar till att stjäla inloggningsuppgifter och lösenord.

_____ 8. Bedrägligt upplägg som syftar till att stjäla pengar eller inloggningsuppgifter från offer.

Kontrollpunkt 7: Utmaning med blandade ord

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

1. **KFINSÄET** _____

2. **VSGNIHI** _____

3. **VEIRRENGFII** _____

4. **GHILNWA** _____

5. **FAPEOSDO** _____

6. **RREEGBÄID** _____

7. **ERROMGGINDI I** _____

8. **SMHGSNII** _____

Bonusaktivitet: Tänk snabbt

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

1	Enheter som kan hackas			
2	Fraser som bedragare ofta använder			
3	Betalningssätt som bedragare ber om			
4	Typer av bedrägerier på nätet			
5	Erbjudanden som är för bra för att vara sanna			
6	Platser där du kan anmäla ett bedrägeri			
7	Ord som hör ihop med cybersäkerhet			
8	Personer du kan varna för bedrägerier			
9	Saker du säkerhetskopierar			
10	Varningstecken i ett e-postmeddelande			
11	Tecken på att en dator är infekterad			
12	Sätt att kontrollera en nätbutik			
13	Sätt att skydda dina konton			
14	Saker att göra om du blir lurad			
15	Saker att göra efter en dataläcka			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

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

FALLSTUDIE 1: FÖREBYGGA BEDRÄGERI MED FÖRETAGSÖVERFÖRINGAR

👷

Scenario: En ekonomiavdelning får ett brådskande e-postmeddelande från en förfalskad leverantörsadress med en begäran om att framtida fakturabetalningar ska skickas till ett nytt routingnummer.

Diskussionsfråga: Beskriv policyn för verifiering av bedrägerier med banköverföringar och ange vilka mekanismer för e-postautentisering som ska användas.

FALLSTUDIE 2: NÄTFISKEINCIDENT MED WHALING MOT LEDNINGEN

👷

Scenario: En chef klickade på en nätfiskelänk som påstod sig innehålla ett säkert dokument för ett styrelsemöte och angav sina primära företagsuppgifter på en förfalskad portal.

Diskussionsfråga: Beskriv i detalj stegen i incidenthanteringen och förklara hur chefens inloggningar granskas.

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		14	28	20	6	9	19	11	5		13	5	4
22	5	18	9	6	9	5	18	9	14	7		1	22						
1	22	19	28	14	4	1	18	5											

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 ett nätbedrägeri?

Ett bedrägeri som använder digitala kanaler för att lura offer att skicka pengar eller lämna ut personliga inloggningsuppgifter.

Q2: Vad är den främsta indikatorn på nätfiske via e-post?

Ett meddelande som hävdar brådska (som kontoavstängning) och leder dig till en länk som inte matchar den officiella domänen.

Q3: Vad är typosquatting?

Att registrera domäner med vanliga stavfel av populära varumärken (som amaz0n.com) för att vara värd för falska nätfiskewebbplatser.

Q4: Vad är en supportbluff?

Ett popup-fönster som påstår att din dator är infekterad och uppmanar dig att ringa ett nummer och betala för falsk rensningsprogramvara eller fjärråtkomsttjänster. [1]

Q5: Vad är vishing?

Nätfiskeattacker via telefonsamtal som lurar offer att lämna ut bankkonto- eller inloggningsuppgifter.

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

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

Q6: Vad betyder telegrafbedrägeri (wire fraud)?

Omdirigering av betalningstransaktioner till bedrägerikonton genom att utge sig för att vara leverantörer eller chefer.

Q7: Vad är whaling?

En mycket riktad form av spear phishing som siktar direkt på mål med högt värde, till exempel företagsledare på högsta nivå.

Q8: Vad är smishing?

Bedrägliga textmeddelanden som skickas till mobila enheter och innehåller länkar till falska portaler eller spårningsuppdateringar.

Q9: Varför är verifiering utanför bandet avgörande?

Den bekräftar transaktionsdetaljer via en separat kommunikationskanal (som ett telefonsamtal) och undviker komprometterade e-posttrådar.

Q10: Hur fungerar ett falskt escrow-bedrägeri (spärrkonto)?

Bedragare skapar en falsk escrow-webbplats (spärrkonto), hävdar att pengarna hålls säkert och stjäl sedan köparens banköverföring.

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

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

Q1: Hur använder bedragare BEC (Business Email Compromise) för att genomföra bedrägerier med banköverföringar?

De kapar en legitim anställds e-postkonto, övervakar fakturatrådar och skickar uppdaterade betalningsuppgifter med bedrägliga bankkonton.

Q2: Vilken risk innebär IDN-homografattacker vid nätbedrägerier?

Att använda icke-ASCII-tecken som ser identiska ut med vanliga bokstäver (t.ex. kyrilliskt 'a') för att registrera förfalskade domäner som imiterar riktiga varumärken.

Q3: Varför är granskning av e-postrubriker viktig för att upptäcka bedrägerier?

Den avslöjar den faktiska ursprungsserverns IP-adress och status för SPF/DKIM-validering och visar om avsändardomänen är förfalskad.

Q4: Hur utnyttjar supportbedragare fjärrskrivbordsprogram?

De använder verktyg som AnyDesk eller TeamViewer för att ansluta till offrets enhet, plantera skadlig kod och stjäla sparade lösenord.

Q5: Vad är målet med förskottsbedrägerier?

Att lura offer att betala avgifter i förskott i utbyte mot en stor ekonomisk belöning som inte finns.

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

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

Q6: Hur använder bedragare profilering i sociala medier för riktat nätfiske?

De sammanställer företags organisationsstrukturer och anställdas namn för att skriva övertygande spear phishing-mejl.

Q7: Varför erbjuder falska webbutiker kraftiga rabatter?

För att locka köpare att ange sina kreditkortsuppgifter och fånga inloggningsuppgifter för återanvändning eller återförsäljning på carding-forum.

Q8: Hur blockerar DMARC-poster nätfiskebedrägerier?

DMARC låter domänägare be mottagare att sätta i karantän eller avvisa e-post som misslyckas med justerade SPF- och DKIM-kontroller, vilket blockerar direkt förfalskning. [5]

Q9: Vad är hotet med portaler för insamling av inloggningsuppgifter?

Förfalskade landningssidor utformade för att se exakt ut som Microsoft 365 eller Google Workspace och som stjäl inloggningsuppgifter när de skrivs in.

Q10: Hur rapporterar och inaktiverar säkerhetsteam bedrägliga domäner?

Genom att skicka bevis på bedrägeri till registratorns missbruks-e-post, webbhotellet och registret Google Safe Browsing.

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. [2]

2. SÄKERHETSINSIKT

Business Email Compromise (BEC) orsakade förluster på över 3 miljarder USD som rapporterades till FBI:s IC3 under 2025. [2]

3. SÄKERHETSINSIKT

Domäner med stavfel (typo-squatting) skiljer sig från riktiga varumärkesnamn med ett eller två tecken, så en hastig blick kan missa dem.

4. SÄKERHETSINSIKT

Bedrägerier med teknisk support orsakade förluster på över 2,1 miljarder USD som rapporterades till FBI:s IC3 under 2025. [2]

5. SÄKERHETSINSIKT

Homografattacker ser identiska ut i webbläsarens adressfält om inte webbläsaren visar punycode-konfigurationer.

6. SÄKERHETSINSIKT

SMS-bedrägerier (smishing) använder korta, brådskande meddelanden med länkar, vilket ger offren lite sammanhang för att upptäcka bedrägeriet.

7. SÄKERHETSINSIKT

Whaling-attacker riktar sig mot chefers e-post eftersom de kontrollerar åtkomsten till stora banköverföringar.

8. SÄKERHETSINSIKT

Att verifiera betalningsändringar genom att ringa ett känt, sparat telefonnummer är ett viktigt försvar mot BEC-bedrägerier med överföringar.

9. SÄKERHETSINSIKT

Falska escrow-webbplatser (spärrkontowebbplatser) är ett vanligt bedrägeri på nätmarknadsplatser: de ser ut som en säker betaltjänst men stjäl köparens banköverföring.

10. SÄKERHETSINSIKT

Google Safe Browsing varnar användare innan de öppnar webbplatser som den har flaggat för nätfiske eller skadlig kod.

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.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

Facit: Kontrollpunkt 1 – Flerval

1 Fråga 1

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad är det främsta tecknet på ett supportbedrägeri? → Ett popup-fönster som påstår att ditt system är infekterat och kräver att du ringer ett telefonnummer

2 Fråga 2

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vilken teknik använder förfalskade avsändardomäner för att stjäla bankuppgifter? → Nätfiske via e-post

3 Fråga 3

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad representerar bedrägeri med banköverföringar? → Att lura offer att skicka pengar till falska företagskonton med hjälp av social manipulation

4 Fråga 4

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Varför skapar bedragare falska webbutiker? → För att stjäla kreditkortsuppgifter och betalningsuppgifter från köpare

5 Fråga 5

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad betyder vishing? → Röstbaserade nätfiskebedrägerier över telefonnät för att stjäla inloggningsuppgifter

Facit: Kontrollpunkt 2 – Sant eller falskt

6 Fråga 6

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: nätfiske riktas också mot chefer; whaling är nätfiske riktat mot högre ledare.

7 Fråga 7

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Förfalskade domäner använder ofta små stavfel (som amaz0n.com) för att imitera betrodda varumärken.

8 Fråga 8

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: att ge en supportbedragare fjärråtkomst låter dem plantera skadlig kod och stjäla data.

9 Fråga 9

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Social manipulation utnyttjar mänsklig psykologi, som rädsla och brådska, för att kringgå säkerhetsregler.

10 Fråga 10

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Förfrågningar om banköverföring bör alltid verifieras via kommunikationskanaler utanför det ursprungliga flödet.

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

G 1. NÄTFISKE	F 2. FÖRFALSKAD	D 3. VISHING	B 4. BEDRÄGERI
H 5. VERIFIERING	A 6. ÖVERFÖRING	E 7. WHALING	C 8. SMISHING

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 NÄTFISKE	2 SPOOFADE	3 VISHING	4 BEDRÄGERI
5 VERIFIERING	6 OMDIRIGERING		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 B – SPOOFADE	2 E – VERIFIERING	3 F – OMDIRIGERING	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – NÄTFISKE	8 D – BEDRÄGERI

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

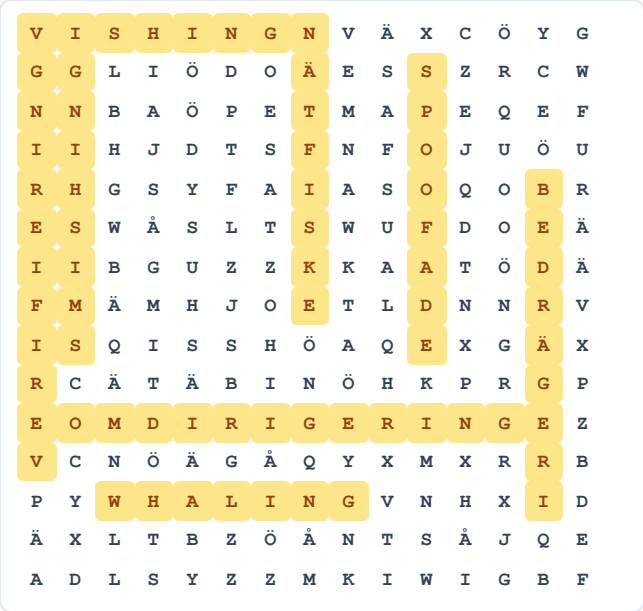
Nyckelbegrepp:
Kontrollera att eleverna kan förklara NÄTFISKE, FÖRFALSKAD och VISHING med egna ord och ge ett exempel på varje.

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

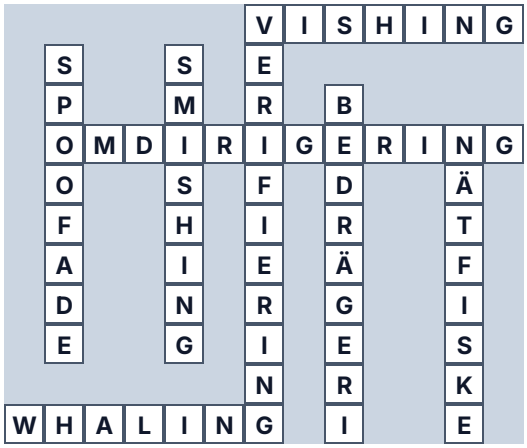
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET



LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

1 vågrätt: VISHING Bedrägliga röstsamtal som syftar till att stjäla inloggnings- och kontouppgifter. (7 bokstäver)

5 vågrätt: OMDIRIGERING Bedräglig omdirigering av banktransaktioner till brottslingars konton. (12 bokstäver)

7 vågrätt: WHALING Riktade nätfiskeattacker som syftar till att stjäla inloggningsuppgifter från högsta chefer. (7 bokstäver)

LODRÄTT

1 lodrätt: VERIFIERING Bekräftelse av betalningsuppgifter via en betrodd sekundär kontaktmetod. (11 bokstäver)

2 lodrätt: SPOOFADE Imiterad e-postavsändare eller webbadress som är utformad för att se legitim ut. (8 bokstäver)

3 lodrätt: SMISHING Utskick av bedrägliga sms för att stjäla inloggningsuppgifter till mobilkonton. (8 bokstäver)

4 lodrätt: BEDRÄGERI Bedrägligt upplägg som syftar till att stjäla pengar eller inloggningsuppgifter från offer. (9 bokstäver)

6 lodrätt: NÄTFISKE Bedrägliga e-postkampanjer som syftar till att stjäla inloggningsuppgifter och lösenord. (8 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. KFINSÄET — NÄTFISKE
2. VSGNIHI — VISHING
3. VEIRRENGFII — VERIFIERING
4. GHILNWA — WHALING
5. FAPEOSDO — SPOOFADE
6. RREEGBÄID — BEDRÄGERI
7. ERROMGGINDII — OMDIRIGERING
8. SMHGSNII — SMISHING

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"UPPTÄCK NÄTFISKE MED VERIFIERING AV AVSÄNDARE"

Facit till fallstudierna

A Fallstudie 1: Förebygga bedrägeri med företagsöverföringar

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En ekonomiavdelning får ett brådskande e-postmeddelande från en förfalskad leverantörsadress med begäran att framtida fakturabetalningar ska skickas till ett nytt clearingnummer.
- Rekommenderad strategi och lösning: Inför en policy med dubbelt godkännande för alla betalningar. Använd verifiering via en separat kanal med ett förhandssparat telefonnummer och blockera e-post från förfalskade domäner i gatewayen.

B Fallstudie 2: Nätfiskeincident med whaling mot ledningen

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En chef klickade på en nätfiskelänk som påstod sig innehålla ett säkert dokument till ett styrelsemöte och angav sina primära företagsuppgifter på en förfalskad portal.
- Rekommenderad strategi och lösning: Isolera chefens enhet. Återställ alla sessionstoken och inloggningsuppgifter i företaget. Granska åtkomstloggar efter dataläckage och inför hårdvarubaserad MFA för alla inloggningar.