Nimi: _____ Päivämäärä: _____ Pisteet: _____

Verkkohuijaukset ja sosiaalinen manipulointi Suojausopas

Sähköpostitietojenkalastelu, väärennetyt verkkotunnukset, vishing, tukihuijaukset, kanavan ulkopuolinen vahvistus, BEC

VERKKOHUIJAUKSET, OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: verkkopetosten torjunta. Tutustut väärennettyihin kalastelusivustoihin, sosiaalisen manipuloinnin taktiikoihin, tukipetoksiin, tilisiirtopetosten reitteihin ja maksujen varmennusmenetelmiin.

TEHTÄVÄMONISTEEN TARKISTUSPISTEET

- [ ] **Osat 1–4: Hallitse kyberturvallisuus ja uhkien ehkäisy.**
- [ ] **Osat 5–7: Ratkaise ristisanatehtäviä ja sanahakuja.**
- [ ] **Osat 8–9: Ratkaise tapaustutkimuksia ja salakirjoitushaaste.**
- [ ] **Osa 10: Tarkista perus- ja jatkotason UKK-sivut.**
- [ ] **Osa 11: Tutustu 10 mielenkiintoiseen tosielämän faktaan.**
- [ ] **Bonus: Nopeat vastaukset -haaste.**

Avaa VPN.comin kyberturvallisuusopas

URL: https://www.vpn.com/fi/kyberturvallisuus/verkkohuijaukset/

Oppimispolkusi: verkkopetosten torjunta

- Tunnista tukihuijausten ja kirjoitusvirheisiin perustuvien (typosquatting) verkkotunnusten yleiset tunnusmerkit.
- Toteuta sähköpostin todennusprotokollat (SPF, DKIM, DMARC) väärennystä vastaan.
- Ota käyttöön kanavan ulkopuolinen tapahtumavahvistus yritysten pankkisiirtopetosten estämiseksi.

VERKKOHUIJAUSOPAS, OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: verkkohuijauksilta suojautuminen. Lopuksi bonustehtävä Nopeat vastaukset.

VERKKOHUIJAUKSET JA SOSIAALISEN MANIPULOINNIN TORJUNTA (JOHDANTO)

Verkkohuijaukset hyödyntävät ihmisten käyttäytymistä tietojenkalastelun, tukitoiminnon ponnahdusikkunoiden, puhelinhuijausten (vishing) ja tilisiirtopetosten kautta. Kanavan ulkopuolinen tapahtumien vahvistus ja SPF/DKIM/DMARC-verkkotunnussäännöt auttavat estämään sosiaalisen manipuloinnin hyökkäysreitit yhdyskäytävässä.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1 **1. Mikä on tukihuijauksen ensisijainen tunnusmerkki?**

- A. Ponnahdusikkuna, joka väittää järjestelmäsi olevan saastunut ja vaatii soittamaan puhelinnumeroon
- B. Automaattinen tietoturvapäivitys, joka ladataan viralliselta rekisteriltä
- C. Salasanojen hallinta kieltäytyy täyttämästä tunnistetietoja yrityksen verkkotunnuksella
- D. Ulkoisella asemalla ajettava taustatiedostojen varmuuskopiointi

2 **2. Mikä tekniikka käyttää väärennettyjä lähettäjän verkkotunnuksia pankkitietojen varastamiseen?**

- A. Sähköpostitse tehtävä tietojenkalastelu
- B. Porttiskannaus
- C. Muistiin injektointi
- D. Kryptografinen tuhoaminen

3 **3. Mikä edustaa tilisiirtopetosta?**

- A. Uhrien huijaaminen lähettämään rahaa väärennetyille yritystileille sosiaalisen manipuloinnin avulla
- B. Järjestelmätietokantojen salaaminen kiristysohjelman hyötykuormilla
- C. Tietokantojen kysely SQL-injektiokomennoilla
- D. Järjestelmätiedostojen varmuuskopiointi offline-tallennuslevyille

4 **4. Miksi huijarit luovat valeverkkokauppoja?**

- A. Varastaa ostajien luottokorttitiedot ja maksutunnistetiedot
- B. Isännöidä hiekkalaatikoituja haittaohjelma-analyysin tietokantatauluja
- C. Verkkotilausten toimituksen nopeuttaminen
- D. Uusien verkkosivustojen suunnitelmien testaamiseksi ilmaiseksi

5 **5. Mitä vishing tarkoittaa?**

- A. Puhelinverkoissa tehtävät äänipohjaiset tietojenkalastelu-huijaukset tunnistetietojen varastamiseksi
- B. Paikallisverkkojen skannaus suojaamattomien järjestelmälaitteiden löytämiseksi
- C. Järjestelmätietokantojen palauttaminen luvattoman tietomurron jälkeen
- D. Epäluotettavan koodin ajaminen suojatuissa virtuaalisissa konteissa

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Tietojenkalastelu kohdistuu vain loppukäyttäjiin, ei koskaan johtajiin kohdistuviin whaling-kohteisiin.

- ○ Tosi
- ○ Epätosi

7 Kysymys 7

7. Väärennetyt verkkotunnukset käyttävät usein pieniä kirjoitusvirheitä (kuten amaz0n.com) jäljitelläkseen luotettuja brändejä.

- ○ Tosi
- ○ Epätosi

8 Kysymys 8

8. Tukihuijaukset voidaan ratkaista antamalla soittajalle etäkäyttö.

- ○ Tosi
- ○ Epätosi

9 Kysymys 9

9. Sosiaalinen manipulointi hyödyntää ihmisen psykologiaa, kuten pelkoa ja kiireellisyyttä, ohittaakseen tietoturvasäännöt.

- ○ Tosi
- ○ Epätosi

10 Kysymys 10

10. Tilisiirtopyynnöt tulisi aina varmentaa erillisen viestintäkanavan kautta.

- ○ Tosi
- ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

Lue jokainen alla oleva lause ja täytä aukko oikealla termillä sanapankista.

1. Käyttäjiä harhaanjohtavien sähköpostien käyttö on nimeltään _____ .
2. Luotettuja brändejä jäljittelevä verkko-osoite on _____ .
3. Pankkitietoihin kohdistuvan puhelinpetoksen nimi on _____ .
4. Virusten poistoa rahaa vastaan vaativa ponnahdusikkuna on tukipalvelun _____ .
5. Maksupyynnön vahvistamiseen tarvitaan toista kanavaa käyttävä _____ .
6. Yritysten maksujen uudelleenohjaaminen varkaiden tileille on _____ .

SANASTON SANAPANKKI

HUIJAUS | KALASTELU | SIIRTOPETOS | SMISHING | VARMENNUS | VISHING | VÄÄRENNETTY | WHALING

Kirjoita vastauksesi tähän:

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

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

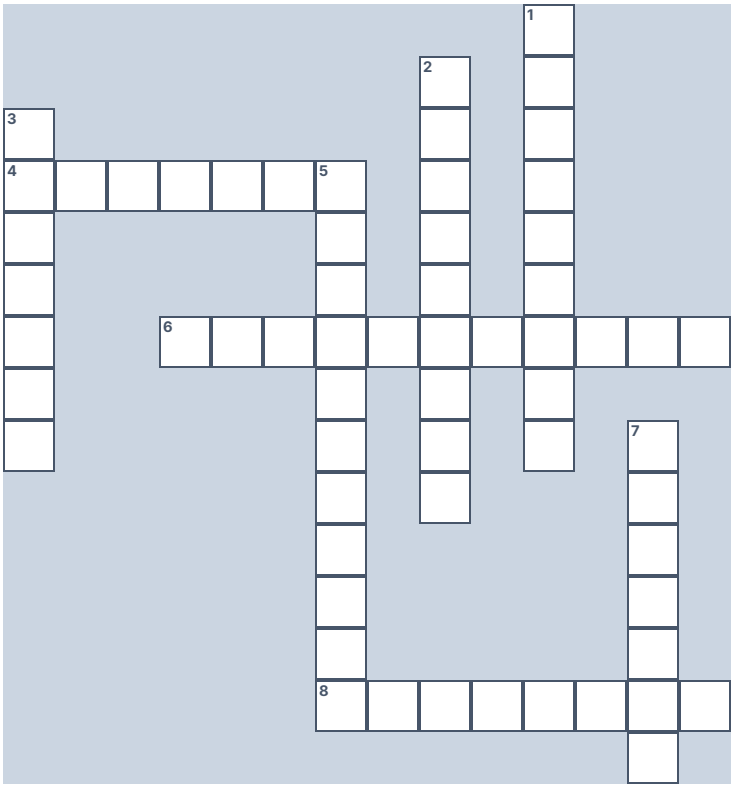
MÄÄRITELMIEN YHDISTÄMINEN

Yhdistä kukin vasemman puolen sanastotermi oikean puolen oikeaan määritelmään kirjoittamalla vastaava kirjain (A–H) täytettävään kenttään.

☐	1. TIETOJENKALASTELU	A	Pankkitapahtumien petollinen ohjaaminen rikollisten tileille.
☐	2. VÄÄRENNETTY	B	Petollinen järjestely, jonka tarkoituksena on varastaa uhreilta rahaa tai tunnistetietoja.
☐	3. VISHING	C	Huijaustekstiviestien lähettäminen mobiilitilin tunnusten varastamiseksi.
☐	4. HUIJAUS	D	Petolliset puhelut, joiden tarkoituksena on varastaa tunnistetietoja ja tilitietoja.
☐	5. TARKISTUS	E	Kohdennetut tietojenkalasteluhyökkäykset, joiden tarkoituksena on varastaa tunnuksia C-tason johtajilta.
☐	6. JOHTO	F	Jäljitelty sähköpostin lähettäjä tai verkkosivuston osoite, joka on tehty näyttämään aidolta.
☐	7. WHALING-HYÖKKÄYS	G	Sähköpostihuijauskampanjat, joiden tarkoituksena on varastaa kirjautumistietoja ja salasanoja.
☐	8. SMISHING	H	Maksutietojen vahvistaminen luotettavalla toissijaisella yhteydenottotavalla.

Tarkistuspiste 5: Ristikko

Ratkaise ristikko kirjoittamalla kirjaimia aktiivisiin valkoisiin ruutuihin. Numerot vastaavat alla olevia vihjeitä.



VAAKASUORAAN

4. Vilpillinen juoni, jolla pyritään varastamaan uhrien rahaa tai tunnistetietoja. (7)

6. Sähköpostin lähettäjän tai verkkosivun osoite, joka on jäljitelty näyttämään aidolta. (11)

8. Huijaustekstiviestien lähettäminen mobiilitilien tunnistetietojen varastamiseksi. (8)

PYSTYSUORAAN

1. Vilpilliset sähköpostikampanjat, joilla pyritään varastamaan kirjautumistunnuksia ja salasanoja. (9)

2. Maksutietojen vahvistaminen luotettavan toissijaisen yhteydenottotavan kautta. (9)

3. Kohdennetut tietojenkalasteluhyökkäykset, joilla pyritään varastamaan ylimmän johdon tunnistetietoja. (7)

5. Pankkisiirtojen vilpillinen ohjaaminen rikollisten tileille. (11)

7. Vilpilliset puhelut, joilla pyritään varastamaan tunnistetietoja ja tilitietoja. (7)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

Näytönlukijan ja näppäimistön käyttäjät voivat kirjoittaa ristikon vastaukset suoraan alla oleviin tekstikenttiin.

VAAKASUORAAN

4 vaakasuoraan: Vilpillinen juoni, jolla pyritään varastamaan uhrien rahaa tai tunnistetietoja. (7 kirjainta):

6 vaakasuoraan: Sähköpostin lähettäjän tai verkkosivun osoite, joka on jäljitelty näyttämään aidolta. (11 kirjainta):

8 vaakasuoraan: Huijaustekstiviestien lähettäminen mobiilitilien tunnistetietojen varastamiseksi. (8 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Vilpilliset sähköpostikampanjat, joilla pyritään varastamaan kirjautumistunnuksia ja salasanoja. (9 kirjainta):

2 pystysuoraan: Maksutietojen vahvistaminen luotettavan toissijaisen yhteydenottotavan kautta. (9 kirjainta):

3 pystysuoraan: Kohdennetut tietojenkalasteluhyökkäykset, joilla pyritään varastamaan ylimmän johdon tunnistetietoja. (7 kirjainta):

5 pystysuoraan: Pankkisiirtojen vilpillinen ohjaaminen rikollisten tileille. (11 kirjainta):

7 pystysuoraan: Vilpilliset puhelut, joilla pyritään varastamaan tunnistetietoja ja tilitietoja. (7 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

Etsi ruudukosta 8 piilotettua keskeistä sanastotermiä. Sanat voivat olla vaaka-, pysty- tai vinosuunnassa.

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

SANASTOLISTA

KALASTELU
VÄÄRENNETTY
VISHING
WHALING
HUIJAUS
SMISHING
VARMENNUS
SIIRTOPETOS

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

Yhdistä kukin sanahaun 8 sanastotermistä sen oikeaan määritelmään kirjoittamalla kirjain (A–H) tyhjään kohtaan.

SANASTOTERMIT

- **A. KALASTELU**
- **B. VÄÄRENNETTY**
- **C. VISHING**
- **D. HUIJAUS**
- **E. VARMENNUS**
- **F. SIIRTOPETOS**
- **G. WHALING**
- **H. SMISHING**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Sähköpostin lähettäjän tai verkkosivun osoite, joka on jäljitelty näyttämään aidolta.
2. Maksutietojen vahvistaminen luotettavan toissijaisen yhteydenottotavan kautta.
3. Pankkisiirtojen vilpillinen ohjaaminen rikollisten tileille.
4. Huijaustekstiviestien lähettäminen mobiilitilien tunnistetietojen varastamiseksi.
5. Kohdennetut tietojenkalasteluhyökkäykset, joilla pyritään varastamaan ylimmän johdon tunnistetietoja.
6. Vilpilliset puhelut, joilla pyritään varastamaan tunnistetietoja ja tilitietoja.
7. Vilpilliset sähköpostikampanjat, joilla pyritään varastamaan kirjautumistunnuksia ja salasanoja.
8. Vilpillinen juoni, jolla pyritään varastamaan uhrien rahaa tai tunnistetietoja.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi keskeisiä kyberturvallisuuden käsitteitä ja termejä. Kirjoita vastauksesi annettuihin syöttökenttiin.

1. **TSAAKELUL** _____
2. **VSGNIHI** _____
3. **VNEANSMUR** _____
4. **GHILNWA** _____
5. **TÄENÄYENVTR** _____
6. **UIAHJSU** _____
7. **ETSIPSTOIOR** _____
8. **SMHGSNII** _____

Bonustehtävä: Nopeat vastaukset

3 VASTAUSTA JOKAISEEN LUOKKAAN. VOITTAJA ON SE, JOKA TÄYTTÄÄ LISTAN ENSIMMÄISENÄ.

1	Laitteita, jotka voidaan hakkeroida			
2	Fraaseja, joita huijarit usein käyttävät			
3	Maksutapoja, joita huijarit pyytävät			
4	Verkkohuijausten tyyppejä			
5	Tarjouksia, jotka ovat liian hyviä ollakseen totta			
6	Paikkoja, joihin huijauksesta voi ilmoittaa			
7	Kyberturvallisuuteen liittyviä sanoja			
8	Ihmisiä, joita voit varoittaa huijauksista			
9	Asioita, joista otat varmuuskopion			
10	Varoitusmerkkejä sähköpostissa			
11	Merkkejä siitä, että tietokone on saanut tartunnan			
12	Tapoja tarkistaa verkkokauppa			
13	Tapoja suojata tilisi			
14	Asioita, joita teet, jos joudut huijatuksi			
15	Asioita, joita teet tietovuodon jälkeen			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: YRITYKSEN PANKKISIIRTOHUIJAUKSEN EHKÄISY

👷

Tilanne: Talousosasto saa kiireellisen sähköpostin väärennetystä toimittajan osoitteesta, jossa pyydetään ohjaamaan tulevat laskusiirrot uuteen reititysnumeroon.

Keskustelukysymys: Kuvaa rahansiirtopetosten varmennuskäytäntö ja määritä sähköpostin todennuksen estot.

TAPAUSTUTKIMUS 2: JOHTAJIIN KOHDISTUNUT WHALING-TIETOJENKALASTELUTAPAUS

👷

Tilanne: Johtaja napsautti tietojenkalastelulinkkiä, joka väitti sisältävänsä suojatun hallituksen kokouksen asiakirjan, ja syötti ensisijaiset yritystunnuksensa väärennetyllä portaalilla.

Keskustelukysymys: Kuvaa tietoturvapoikkeamaan reagoinnin vaiheet ja selitä, miten johtajan kirjautumiset tarkastetaan.

Tarkistuspiste 9: Salakirjoituksen purkaminen

Kyberturvallisuuden ammattilainen suojaa verkon resursseja verkkohyökkääjiltä. Käytä alla olevaa kirjain–numero-avainta purkaaksesi viestin kirjoittamalla vastaavat kirjaimet tyhjiin kohtiin.

KIRJAIN-NUMERO-SALAUSAVAIN

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

20	21	14	14	9	19	20	1

11	1	12	1	19	20	5	12	21	25	18	9	20	25	11	19	5	20

22	1	18	13	5	14	14	21	11	19	5	12	12	1

Purettu viesti:

VIHJE: JOKAINEN NUMERO VASTAA KIRJAIMEN PAIKKAA AAKKOSISSA (ESIM. 1 = A, 2 = B, 29 = Ö).

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa A)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q1: Mikä on verkkohuijaus?

Vilpillinen juoni, jossa digitaalisia kanavia käytetään huijaamaan uhreja lähettämään rahaa tai luovuttamaan henkilökohtaisia tunnistetietoja.

Q2: Mikä on sähköpostitietojenkalastelun tärkein tunnusmerkki?

Viesti, joka väittää olevansa kiireellinen (kuten tilin jäädyttäminen) ja ohjaa sinut linkkiin, joka ei vastaa virallista verkkotunnusta.

Q3: Mitä typosquatting on?

Suosittujen brändien yleisiä kirjoitusvirheitä sisältävien verkkotunnusten (kuten amaz0n.com) rekisteröinti väärennettyjen tietojenkalastelusivustojen ylläpitämiseksi.

Q4: Mikä on tukihuijaus?

Ponnahdusikkuna, joka väittää tietokoneesi olevan saastunut ja ohjaa sinut soittamaan numeroon ja maksamaan väärennetystä siivousohjelmistosta tai etäkäyttöpalveluista. [1]

Q5: Mitä vishing on?

Puhelinsoittoja hyödyntävät tietojenkalasteluhyökkäykset, joilla uhrit huijataan antamaan pankkitilin tai kirjautumistietonsa.

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa B)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Mitä wire fraud tarkoittaa?

Maksutapahtumien ohjaaminen huijaustileille esiintymällä toimittajina tai johtajina.

Q7: Mitä whaling on?

Erittäin kohdennettu keihäskalastelun muoto, joka kohdistuu suoraan arvokkaisiin kohteisiin, kuten yritysten ylimpään johtoon.

Q8: Mitä smishing on?

Huijaustekstiviestit, jotka lähetetään mobiililaitteisiin ja sisältävät linkkikehotteita väärennettyihin portaaleihin tai seurantapäivityksiin.

Q9: Miksi erillisen kanavan varmennus on kriittistä?

Se vahvistaa maksutapahtuman tiedot erillisellä viestintäkanavalla (kuten puhelulla) ja välttää vaarantuneet sähköpostiketjut.

Q10: Miten väärennetty sulkutilihuijaus (escrow scam) toimii?

Huijarit luovat väärennetyn sulkutilisivuston, väittävät varojen olevan turvallisesti säilössä ja varastavat sitten ostajan pankkisiirtotalletuksen.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa C)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q1: Miten huijarit käyttävät BEC-huijausta (Business Email Compromise) tilisiirtopetoksiin?

Ne kaappaavat oikean työntekijän sähköpostitilin, seuraavat laskuketjuja ja lähettävät päivitetyt laskutustiedot huijaustilinumeroineen.

Q2: Mikä on IDN-homografihyökkäysten riski verkkohuijauksissa?

Sellaisten ei-ASCII-merkkien käyttö, jotka näyttävät samalta kuin tavalliset kirjaimet (esim. kyrillinen 'a'), väärennettyjen, oikeita brändejä jäljittelevien verkkotunnusten rekisteröimiseksi.

Q3: Miksi sähköpostin otsikkotietojen tarkastus on tärkeää huijausten tunnistamisessa?

Se paljastaa todellisen alkuperäpalvelimen IP-osoitteen ja SPF/DKIM-validoinnin tilan, mikä näyttää, onko lähettäjän verkkotunnus väärennetty.

Q4: Miten tukihuijarit hyödyntävät etätyöpöytäohjelmistoja?

Ne käyttävät AnyDeskin tai TeamViewerin kaltaisia työkaluja yhdistääkseen uhrin laitteeseen, asentaakseen haittaohjelmia ja varastaakseen tallennettuja salasanoja.

Q5: Mikä on ennakkomaksuhuijausten tavoite?

Uhrien huijaaminen maksamaan etukäteen käsittelymaksuja vastineeksi suuresta taloudellisesta palkkiosta, jota ei ole olemassa.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa D)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q6: Miten huijarit hyödyntävät sosiaalisen median profilointia kohdennetussa tietojenkalastelussa?

Ne keräävät yrityksen organisaatiorakenteita ja työntekijöiden nimiä laatiakseen uskottavia kohdennettuja tietojenkalasteluviestejä.

Q7: Miksi väärennetyt verkkokaupat tarjoavat jyrkkiä alennuksia?

Houkutellakseen ostajia syöttämään luottokorttitietonsa ja kaapatakseen tunnistetietoja uudelleenkäyttöä tai jälleenmyyntiä varten carding-foorumeilla.

Q8: Miten DMARC-tietueet estävät tietojenkalasteluhuijauksia?

DMARC antaa verkkotunnuksen omistajan pyytää vastaanottajia asettamaan karanteeniin tai hylkäämään viestit, jotka eivät läpäise SPF- ja DKIM-tarkistuksia, ja estää näin suoran väärentämisen. [5]

Q9: Mikä on tunnistetietoja urkkivien portaalien uhka?

Väärennetyt kohdesivut, jotka on suunniteltu näyttämään täsmälleen Microsoft 365:ltä tai Googlen työtiloilta ja jotka varastavat kirjautumistunnukset niitä syötettäessä.

Q10: Miten tietoturvatiimit ilmoittavat huijausverkkotunnuksista ja poistavat ne käytöstä?

Toimittamalla näyttöä petoksesta rekisterinpitäjän väärinkäyttösähköpostiin, isännöintipalveluntarjoajalle ja Google Safe Browsing -rekisteriin.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

Tietojenkalastelu ja väärentäminen olivat FBI:n IC3:lle vuonna 2025 ilmoitetuin rikostyyppi 191 561 valituksella. [2]

2. TURVALLISUUSOIVALLUS

Yritysviestipetokset (BEC) aiheuttivat FBI:n IC3:lle ilmoitettuja yli 3 miljardin dollarin tappioita vuonna 2025. [2]

3. TURVALLISUUSOIVALLUS

Kirjoitusvirheitä hyödyntävät verkkotunnukset eroavat oikeista brändinimistä yhden tai kahden merkin verran, joten ne voi ohittaa nopealla vilkaisulla.

4. TURVALLISUUSOIVALLUS

Teknisen tuen huijaukset aiheuttivat vuonna 2025 yli 2,1 miljardin dollarin tappiot, jotka ilmoitettiin FBI:n IC3:lle. [2]

5. TURVALLISUUSOIVALLUS

Homografihyökkäykset näyttävät selaimen osoiterivillä identtisiltä, ellei selain näytä punycode-muotoja.

6. TURVALLISUUSOIVALLUS

Tekstiviestihuijaukset (smishing) käyttävät lyhyitä, kiireellisiä viestejä ja linkkejä, jolloin uhreilla on vain vähän asiayhteyttä petoksen tunnistamiseen.

7. TIETOTURVATIETOA

Whaling-hyökkäykset kohdistuvat johtajien sähköposteihin, koska heillä on valtuudet suuriin tilisiirtoihin.

8. TIETOTURVATIETOA

Maksumuutosten varmistaminen soittamalla tunnettuun, tallennettuun puhelinnumeroon on keskeinen puolustus BEC-maksupetoksia vastaan.

9. TIETOTURVATIETOA

Väärennetyt sulkutilisivustot (escrow) ovat yleinen huijaus verkkomarkkinapaikoilla: ne näyttävät turvalliselta maksupalvelulta mutta varastavat ostajan pankkisiirron.

10. TURVALLISUUSOIVALLUS

Google Safe Browsing varoittaa käyttäjiä ennen kuin he avaavat sivustoja, jotka se on merkinnyt tietojenkalasteluun tai haittaohjelmiin liittyviksi.

Tekniset viitteet ja lähteet

Opiskeluopas ja interaktiiviset pulmat on koottu maailmanlaajuisista NIST-, OWASP- ja tietosuojavaatimustenmukaisuusstandardeista.

TIETEELLISET JA ALAN VIITTEET

[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

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1

Oikea vastaus: A

OPETTAJALLE

Mikä on tukihuijauksen ensisijainen tunnusmerkki? → Ponnahdusikkuna, joka väittää järjestelmäsi olevan saastunut ja vaatii soittamaan puhelinnumeroon

2 Kysymys 2

Oikea vastaus: A

OPETTAJALLE

Mikä tekniikka käyttää väärennettyjä lähettäjän verkkotunnuksia pankkitietojen varastamiseen? → Sähköpostitse tehtävä tietojenkalastelu

3 Kysymys 3

Oikea vastaus: A

OPETTAJALLE

Mikä edustaa tilisiirtopetosta? → Uhrien huijaaminen lähettämään rahaa väärennetyille yritystileille sosiaalisen manipuloinnin avulla

4 Kysymys 4

Oikea vastaus: A

OPETTAJALLE

Miksi huijarit luovat valeverkkokauppoja? → Varastaa ostajien luottokorttitiedot ja maksutunnistetiedot

5 Kysymys 5

Oikea vastaus: A

OPETTAJALLE

Mitä vishing tarkoittaa? → Puhelinverkoissa tehtävät äänipohjaiset tietojenkalastelu-huijaukset tunnistetietojen varastamiseksi

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kysymys 6** — **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: tietojenkalastelu kohdistuu myös johtajiin; whaling on ylimpään johtoon kohdistuvaa tietojenkalastelua.

7 **Kysymys 7** — **Oikea vastaus: Tosi**

OPETTAJALLE

Väärennetyt verkkotunnukset käyttävät usein pieniä kirjoitusvirheitä (kuten amaz0n.com) jäljitelläkseen luotettuja brändejä.

8 **Kysymys 8** — **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: etäyhteyden antaminen tukihuijarille antaa tämän asentaa haittaohjelmia ja varastaa tietoja.

9 **Kysymys 9** — **Oikea vastaus: Tosi**

OPETTAJALLE

Sosiaalinen manipulointi hyödyntää ihmisen psykologiaa, kuten pelkoa ja kiireellisyyttä, ohittaakseen tietoturvasäännöt.

10 **Kysymys 10** — **Oikea vastaus: Tosi**

OPETTAJALLE

Tilisiirtopyynnöt tulisi aina varmentaa erillisen viestintäkanavan kautta.

Sanastoavaimet ja arviointikriteerit

Opettajan arviointikriteeri: Anna 1 piste jokaisesta oikeasta yhdistämisestä (yhteensä 8 pistettä) ja asiayhteystermistä (yhteensä 6 pistettä).

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

G 1. TIETOJENKALASTELU	F 2. VÄÄRENNETTY	D 3. VISHING	B 4. HUIJAUS
H 5. TARKISTUS	A 6. JOHTO	E 7. WHALING-HYÖKKÄYS	C 8. SMISHING

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 KALASTELU	2 VÄÄRENNETTY	3 VISHING	4 HUIJAUS
5 VARMENNUS	6 SIIRTOPETOS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 B – VÄÄRENNETTY	2 E – VARMENNUS	3 F – SIIRTOPETOS	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – KALASTELU	8 D – HUIJAUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit TIETOJENKALASTELU, VÄÄRENNETTY ja VISHING omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

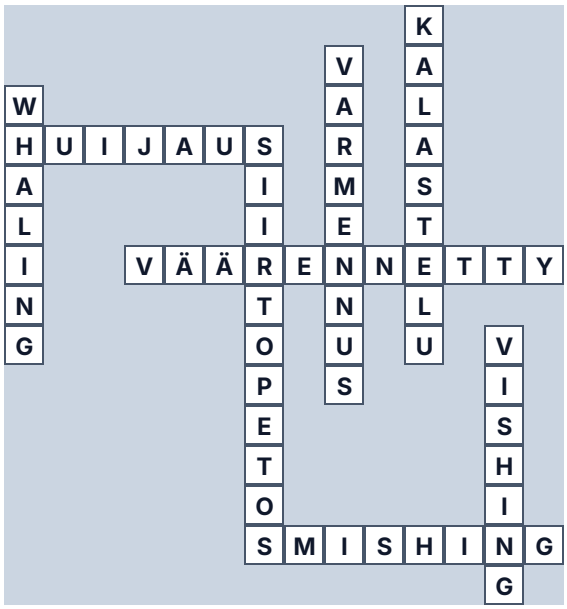
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

4 vaakasuoraan: HUIJAUS Vilpillinen juoni, jolla pyritään varastamaan uhrien rahaa tai tunnistetietoja. (7 kirjainta)

6 vaakasuoraan: VÄÄRENNETTY Sähköpostin lähettäjän tai verkkosivun osoite, joka on jäljitelty näyttämään aidolta. (11 kirjainta)

8 vaakasuoraan: SMISHING Huijaustekstiviestien lähettäminen mobiilitilien tunnistetietojen varastamiseksi. (8 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: KALASTELU Vilpilliset sähköpostikampanjat, joilla pyritään varastamaan kirjautumistunnuksia ja salasanoja. (9 kirjainta)

2 pystysuoraan: VARMENNUS Maksutietojen vahvistaminen luotettavan toissijaisen yhteydenottotavan kautta. (9 kirjainta)

3 pystysuoraan: WHALING Kohdennetut tietojenkalasteluhyökkäykset, joilla pyritään varastamaan ylimmän johdon tunnistetietoja. (7 kirjainta)

5 pystysuoraan: SIIRTOPETOS Pankkisiirtojen vilpillinen ohjaaminen rikollisten tileille. (11 kirjainta)

7 pystysuoraan: VISHING Vilpilliset puhelut, joilla pyritään varastamaan tunnistetietoja ja tilitietoja. (7 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. TSAAKELUL — **KALASTELU**
2. VSGNIHI — **VISHING**
3. VNEANSMUR — **VARMENNUS**
4. GHILNWA — **WHALING**
5. TÄENÄYENVTR — **VÄÄRENNETTY**
6. UIAHJSU — **HUIJAUS**
7. ETSIPSTOIOR — **SIIRTOPETOS**
8. SMHGSNII — **SMISHING**

SALAKIRJOITUSHAASTEEN AVAIN

"TUNNISTA KALASTELUYRITYKSET VARMENNUKSELLA"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Yrityksen pankkisiirtohuijauksen ehkäisy

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Talousosasto saa kiireellisen sähköpostin väärennetystä toimittajan osoitteesta, jossa pyydetään ohjaamaan tulevat laskumaksut uuteen reititysnumeroon.
- Suositeltu strategia ja ratkaisu: Ota käyttöön kahden hyväksyjän käytäntö kaikille maksuille. Toteuta erillisen kanavan kautta tehtävä varmennus etukäteen tallennetulla puhelinnumerolla ja estä väärennetyiltä verkkotunnuksilta tulevat sähköpostit yhdyskäytävässä.

B Tapaustutkimus 2: Johtajiin kohdistunut whaling-tietojenkalastelutapaus

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Johtaja klikkasi tietojenkalasteluviestin linkkiä, jonka väitettiin sisältävän suojatun hallituksen kokousasiakirjan, ja syötti yrityksen pääkäyttäjätunnuksensa väärennetylle portaalille.
- Suositeltu strategia ja ratkaisu: Eristä johtajan laite. Nollaa kaikki yrityksen istuntotunnisteet ja tunnukset. Tarkista käyttölokeista tietojen ulosvienti ja ota käyttöön laitteistopohjainen MFA kaikissa kirjautumisissa.