Nimi: _____ Päivämäärä: _____ Pisteet: _____

Identiteettivarkauden ehkäisy ja omaisuuden turva Tietoturvaopas

Käyttötunnusvuodot, MFA, dark web -valvonta, luottotietojen jäädytyshälytykset, sosiaalinen manipulointi

IDENTITEETTIVARKAUDEN ESTÄMINEN: OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: identiteettivarkauksien ehkäisy ja lieventäminen. Tutustut tunnistetietovuotoihin, monivaiheiseen todennukseen, pimeän verkon valvontaan, luottotietojen jäädytyshälytyksiin ja sosiaalisen manipuloinnin torjuntaan.

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/identiteettivarkaus/

Oppimispolkusi: identiteetinsuoja

- Ymmärrä tunnistetietojen paljastumisen riskit pimeän verkon foorumeilla.
- Toteuta monivaiheinen tunnistautuminen (MFA) ja luottotietojen jäädytyshälytykset.
- Suunnittele yrityksen tietoturvapuolustuksia kohdennettuja sosiaalisen manipuloinnin huijauksia vastaan.

IDENTITEETTIVARKAUDEN OPAS: OHJEET

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

IDENTITEETTIVARKAUDEN ESTÄMINEN JA OMAISUUDEN TURVAAMINEN (JOHDANTO)

Identiteettivarkaus hyödyntää vuotaneita tunnistetietoja ja heikkoja kirjautumisia kaapatakseen henkilökohtaisia ja yrityksen tilejä. MFA:n, luottotietojen jäädytysten, pimeän verkon skannerien sekä SPF/DKIM/DMARC-viitekehysten käyttöönotto muodostaa tärkeän puolustuksen digitaalista henkilöllisyyden väärentämistä vastaan.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1 **1. Mikä on ensisijainen tapa, jolla identiteettivarkaat varastavat kirjautumistunnuksia?**

- A. Väärennettyjen sähköpostihälytysten lähettäminen, jotta käyttäjät syöttävät salasanansa väärennetyissä portaaleissa
- B. Radiolähetysten kuuntelu käyttäjän yrityksen toimiston lähellä
- C. Käyttäjän paikallisen palvelimen tallennusaseman eheytys
- D. Ulkoisten verkkovarmuuskopiomääritysten irrottaminen

2 **2. Mikä tietoturvakontrolli tarjoaa vahvimman suojan tunnusvuodoilta?**

- A. Monitekijätodennus laitteistoavaimilla
- B. Pitkien salasanojen luominen selaimen oletusmuodoilla
- C. Sähköpostikäyttäjänimien vaihtaminen kuuden kuukauden välein
- D. Tallennettujen evästeseurantaselainhistorioiden poistaminen

3 **3. Mikä edustaa luottotietojen jäädytystä?**

- A. Luottotietojen lukitseminen, jotta varkaat eivät voi avata luvattomia lainoja
- B. Pankkitilien tapahtumahistorioiden poistaminen tietokannoista
- C. Luottokorttien magneettijuovanlukijoiden poistaminen käytöstä skannereissa
- D. Paikallisten tietokantalevyjen salaus levossa

4 **4. Miksi darkwebin seuranta on hyödyllistä?**

- A. Se hälyttää käyttäjiä, jos heidän vuotaneet tunnistetietonsa näkyvät laittomissa tietokannoissa
- B. Se estää aktiivisia haittaohjelmia toimimasta virtuaalisissa hiekkalaatikoissa
- C. Se nopeuttaa selaimen reititystä virtuaaliverkoissa
- D. Se estää taustajärjestelmän tietokannan SQL-injektioyritykset

5 **5. Mitä sosiaalinen manipulointi tarkoittaa?**

- A. Ihmisten manipulointi paljastamaan luottamuksellisia tunnistetietoja vapaaehtoisesti
- B. Yrityspalvelimien porttien skannaus aktiivisten tietoturva-aukkojen löytämiseksi
- C. Järjestelmätietokantatiedostojen varmuuskopiointi offline-kiintolevyille
- D. Verkkopakettien reititys kolmen salatun onion-solmun kautta

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Identiteettivarkaus vaikuttaa vain verkossa oleviin digitaalisiin tileihin, ei fyysiseen postiin.

- ○ Tosi
- ○ Epätosi

7 Kysymys 7

7. Monivaiheisen tunnistautumisen pakottaminen kaikille henkilökohtaisille tileille estää suurimman osan tunnistetietojen täyttöhyökkäyksistä.

- ○ Tosi
- ○ Epätosi

8 Kysymys 8

8. Luottotietojen jäädytys estää luottotarkistukset, mutta estää sinua käyttämästä omaa pankkitiliäsi.

- ○ Tosi
- ○ Epätosi

9 Kysymys 9

9. Salasananhallinnat suojaavat tietojenkalastelulta kieltäytymällä täyttämästä salasanoja automaattisesti väärennetyille verkkotunnuksille.

- ○ Tosi
- ○ Epätosi

10 Kysymys 10

10. Tietojenkalastelusähköpostit käyttävät usein kiireellistä kieltä herättääkseen tunteita ja nopeita reaktioita.

- ○ Tosi
- ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Identiteettivarkaat tavoittelevat henkilökohtaisia salasanoja ja muita käyttäjän tunnistautumistietoja eli _____ .

2. Yksityisten tilitietojen paljastumisia tietokantamurroissa ovat esimerkiksi _____ .

3. Väliaikaisen koodin vaatiminen kirjautumiseen on _____ .

4. Hakkerifoorumien skannaus varastettujen tietojen löytämiseksi on pimeän verkon _____ .

5. Luvattomien luottotietokyselyjen estämiseksi tarvitaan _____ .

6. Aktiivinen tietoturvan _____ rakentuu muun muassa työntekijöiden koulutuksesta tietojenkalastelun tunnistamiseen.

SANASTON SANAPANKKI

KALASTELU LUOTTOLUKITUS MFA-TUNNISTUS PUOLUSTUS TIETOVUODOT
TUNNISTETIEDOT VALVONTA VÄÄRENNYS

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

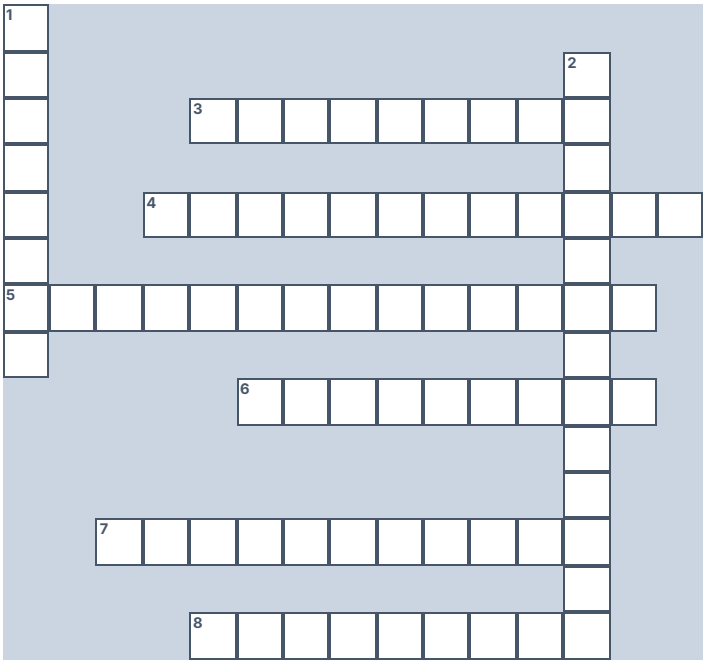
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. KÄYTTÖTUNNUKSET	A	Toissijainen todennusvaihe (esimerkiksi laiteavaimet), joka suojaa tilien kirjautumisia.
☐	2. VUODOT	B	Väärennetyn verkkosivuston tai sähköpostin luominen, joka jäljittelee oikeaa organisaatiota.
☐	3. MFA	C	Luottotietotiedostojen käytön rajoittaminen vilpillisten lainahakemusten estämiseksi.
☐	4. SEURANTA	D	Henkilötietoja sisältävien yksityisten tietokantojen luvaton paljastuminen.
☐	5. JÄÄDYTYS	E	Koulutus ja tekniset kontrollit, joilla suojaudutaan identiteettivarkaudelta.
☐	6. PUOLUSTUS	F	Vilpillisten viestien lähettäminen käyttäjien huijaamiseksi luovuttamaan tunnuksensa.
☐	7. VÄÄRENNYS	G	Verkkofoorumien ja hakkerikanavien skannaus varastettujen yritystietojen löytämiseksi.
☐	8. TIETOJENKALASTELU	H	Käyttäjätunnukset, salasanat ja yksityiset tokenit, joilla digitaaliset identiteetit todennetaan.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

3. Vilpillisten viestien lähettäminen, joilla käyttäjät huijataan luovuttamaan tunnistetietonsa. (9)

4. Toissijainen varmennusvaihe (esimerkiksi laitteistoavaimet), joka suojaa tilien kirjautumisia. (12)

5. Käyttäjätunnukset, salasanat ja yksityiset tunnisteet, joilla todennetaan digitaaliset identiteetit. (14)

6. Koulutus ja tekniset kontrollit, joilla suojaudutaan identiteettivarkauksilta. (9)

7. Henkilötietoja sisältävien yksityisten tietokantojen luvaton paljastuminen. (11)

8. Väärennetyn verkkosivuston tai sähköpostin luominen oikean organisaation jäljittelemiseksi. (9)

PYSTYSUORAAN

1. Verkkofoorumien ja hakkerikanavien skannaus varastettujen yritystietojen löytämiseksi. (8)

2. Luottotietojen käytön rajoittaminen petollisten lainahakemusten estämiseksi. (13)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

3 vaakasuoraan: Vilpillisten viestien lähettäminen, joilla käyttäjät huijataan luovuttamaan tunnistetietonsa. (9 kirjainta):

4 vaakasuoraan: Toissijainen varmennusvaihe (esimerkiksi laitteistoavaimet), joka suojaa tilien kirjautumisia. (12 kirjainta):

5 vaakasuoraan: Käyttäjätunnukset, salasanat ja yksityiset tunnisteet, joilla todennetaan digitaaliset identiteetit. (14 kirjainta):

6 vaakasuoraan: Koulutus ja tekniset kontrollit, joilla suojaudutaan identiteettivarkauksilta. (9 kirjainta):

7 vaakasuoraan: Henkilötietoja sisältävien yksityisten tietokantojen luvaton paljastuminen. (11 kirjainta):

8 vaakasuoraan: Väärennetyn verkkosivuston tai sähköpostin luominen oikean organisaation jäljittelemiseksi. (9 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Verkkofoorumien ja hakkerikanavien skannaus varastettujen yritystietojen löytämiseksi. (8 kirjainta):

2 pystysuoraan: Luottotietojen käytön rajoittaminen petollisten lainahakemusten estämiseksi. (13 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

TUNNISTETIEDOT, TIETOVUODOT, MFATUNNISTUS, VALVONTA, LUOTTOLUKITUS, PUOLUSTUS, VÄÄRENNYS, KALASTELU

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. TUNNISTETIEDOT**
- **B. TIETOVUODOT**
- **C. MFATUNNISTUS**
- **D. VALVONTA**
- **E. LUOTTOLUKITUS**
- **F. PUOLUSTUS**
- **G. VÄÄRENNYS**
- **H. KALASTELU**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Vilpillisten viestien lähettäminen, joilla käyttäjät huijataan luovuttamaan tunnistetietonsa.
2. Käyttäjätunnukset, salasanat ja yksityiset tunnisteet, joilla todennetaan digitaaliset identiteetit.
3. Väärennetyn verkkosivuston tai sähköpostin luominen oikean organisaation jäljittelemiseksi.
4. Koulutus ja tekniset kontrollit, joilla suojaudutaan identiteettivarkauksilta.
5. Verkkofoorumien ja hakkerikanavien skannaus varastettujen yritystietojen löytämiseksi.
6. Luottotietojen käytön rajoittaminen petollisten lainahakemusten estämiseksi.
7. Henkilötietoja sisältävien yksityisten tietokantojen luvaton paljastuminen.
8. Toissijainen varmennusvaihe (esimerkiksi laitteistoavaimet), joka suojaa tilien kirjautumisia.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. ESEITNUTDTOTIN
2. SFUNMTUAISNT
3. ULUIKUSOLTOTT
4. ESYRNNVÄÄ
5. DIOUETOVTOT
6. TAVNVOAL
7. SPUSTLUUO
8. USLKAATEL

Bonustehtävä: Nopeat vastaukset

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

1	Asioita, joita teet, jos identiteettisi varastetaan			
2	Asioita, joita ei kannata jakaa sosiaalisessa mediassa			
3	Asioita, joista otat varmuuskopion			
4	Kortteja tai henkilöllisyystodistuksia lompakossasi			
5	Asiakirjoja, jotka sinun pitäisi suojata			
6	Asioita, joita teet tietovuodon jälkeen			
7	Syitä päivittää ohjelmistot			
8	Tietoja, joita identiteettivaras haluaa			
9	Laitteita, jotka voidaan hakkeroida			
10	Paikkoja, joista tietosi voivat vuotaa			
11	Turvallisia tapoja, joita voit aloittaa tänään			
12	Merkkejä siitä, että tietokone on saanut tartunnan			
13	Tapoja todistaa, kuka olet			
14	Identiteettivarkauden merkkejä			
15	Varoitusmerkkejä sähköpostissa			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: JOHTAJAN IDENTITEETIN VÄÄRENTÄMISEN TORJUNTA

👨‍💼

Tilanne: Korkean profiilin C-tason johtajaa vastaan on kohdistettu kirjoitusvirheisiin perustuvia verkkotunnuksia, jotka jäljittelevät hänen henkilökohtaista sähköpostiaan asiakkaiden huijaamiseksi. Suunnittele brändinsuojasuunnitelma.

Keskustelukysymys: Analysoi brändin väärentämisen riskit ja kuvaa SPF/DKIM/DMARC- ja todennuskontrollit.

TAPAUSTUTKIMUS 2: YRITYKSEN KÄYTTÖTUNNUSTEN PALJASTUMINEN DARK WEBISSÄ

👨‍💼

Tilanne: Pimeän verkon tietokantavedos sisältää useita satoja yrityksen järjestelmänvalvojien yritystunnuksia. Suunnittele lieventämisstrategia.

Keskustelukysymys: Kuvaa tunnusten siivousprosessi ja suunnittele salasanahallinnan käyttöönotto.

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

19	21	15	10	1	1

9	4	5	14	20	9	20	5	5	20	20	9	19	9		13	6	1

20	21	14	14	9	19	20	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: Mitä on identiteettivarkaus?

Rikos, jossa hyökkääjä varastaa henkilötietoja (kuten salasanoja tai henkilötunnuksia) esiintyäkseen toisena taloudellisen hyödyn saamiseksi.

Q2: Mikä on identiteettivarkauden yleisin syy?

Tietojenkalastelu on johtava tapa, jolla varkaat saavat salasanoja, houkuttelemalla käyttäjiä väärennetyille sivustoille.

Q3: Miten monivaiheinen todennus (MFA) suojaa henkilöllisyyksiä?

MFA vaatii kirjautumiseen toisen todisteen (kuten laitteistoavaimen), mikä estää hyökkääjät, vaikka he varastaisivat salasanasi.

Q4: Mikä on luottojen jäädytys?

Ilmainen palvelu, joka estää luottotietoyrityksiä jakamasta luottotietojasi ja estää varkaita avaamasta uusia lainoja nimissäsi. [2]

Q5: Mitä pimeän verkon seuranta on?

Ohjelmisto, joka tarkistaa hakkerifoorumeilta vuotaneita sähköposteja, salasanoja ja henkilötietoja ja hälyttää sinua, jos tietosi ovat paljastuneet.

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

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Mitä credential stuffing tarkoittaa?

Automaattiset botit, jotka testaavat vuodettuja salasanalistoja satoihin verkkosivustoihin ja kaappaavat aktiivisia tilejä.

Q7: Miksi sähköpostin väärentäminen on vaarallista?

Se antaa hyökkääjille mahdollisuuden väärentää lähettäjän nimen sähköposteissa, jolloin tietojenkalasteluviestit näyttävät tulevan luotetuilta kollegoilta.

Q8: Miten salasanojen hallintaohjelmat estävät identiteettivarkauksia?

Ne tallentavat monimutkaiset, yksilölliset salasanat jokaiselle tilille eivätkä täytä tunnistetietoja automaattisesti väärennetyille tietojenkalastelun verkkotunnuksille.

Q9: Mitä kohdennettu tietojenkalastelu (spear phishing) on?

Erittäin kohdennettu tietojenkalasteluhyökkäys, joka on räätälöity uhrin nimellä ja tiedoilla huijauksen onnistumisen todennäköisyyden lisäämiseksi.

Q10: Miten luottohälytys eroaa luottojäädytyksestä?

Hälytys kehottaa luotonantajia varmistamaan henkilöllisyytesi ennen tilien avaamista, kun taas jäädytys estää pääsyn luottotietoihisi kokonaan. [2]

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

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

Q1: Miten SIM-kortin kaappaus johtaa identiteettivarkauteen?

Hyökkääjät saavat operaattorin henkilökunnan siirtämään uhrin puhelinnumeron uudelle SIM-kortille ja kaappaavat tekstiviestipohjaiset kaksivaiheisen tunnistautumisen (2FA) koodit.

Q2: Mikä rooli DMARCilla on identiteettivarkauksien ehkäisyssä?

DMARC antaa verkkotunnusten omistajien estää väärennettyjen sähköpostien pääsyn postilaatikoihin ja estää näin yrityksen verkkotunnuksia jäljittelevät valeviestit.

Q3: Miksi synteettistä identiteettivarkautta on vaikea havaita?

Varkaat yhdistävät oikeita henkilötunnuksia (SSN) keksittyihin nimiin ja syntymäaikoihin rakentaakseen uusia luottoprofiileja ohittaen perustason petoshälytykset.

Q4: Miten tietovälittäjät hyödyntävät henkilöllisyyksiä?

Välittäjät keräävät julkisia tietoja, verkkokäyttäytymistä ja ostohistorioita koostaakseen profiiliasiakirjoja, jotka voivat vuotaa tai päätyä myyntiin.

Q5: Miksi tekstiviestipohjaista MFA:ta pidetään haavoittuvana?

Tekstiviestiliikenne on altista sieppaukselle, tietojenkalastelulle ja operaattoritason SIM-kaappaushyökkäyksille.

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

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

Q6: Mikä on luottotietojen lukitus?

Kaupallinen palvelu, joka muistuttaa jäädytystä ja jonka avulla käyttäjät voivat avata tai lukita luottotietonsa välittömästi mobiilisovelluksella.

Q7: Miten yritysten tietomurrot ruokkivat identiteettivarkauksia?

Vuotaneet tietokannat paljastavat miljoonia selkokielisiä tunnuksia, jotka antavat varkaille raaka-aineen kohdennettuun identiteettipetokseen.

Q8: Mikä on sosiaalisessa mediassa liikaa jakamisen riski?

Lemmikkien nimien, syntymäpaikkojen ja äidin tyttönimen julkinen jakaminen antaa varkaille vastaukset tavallisiin tilin palautuskysymyksiin.

Q9: Miten biometriset kirjautumiset suojaavat identiteettiprofiileja?

Biometriset tiedot sitovat kirjautumisen ominaisuuksiin, kuten sormenjälkiin tai kasvoihin; laitteella säilytettyinä ne on vaikea varastaa, mutta tallennetut biometriset tiedot voivat vuotaa.

Q10: Miten Red Flags Rule torjuu identiteettivarkauksia?

Liittovaltion säädös, joka velvoittaa rahoituslaitokset laatimaan kirjalliset ohjelmat identiteettivarkauden varoitusmerkkien havaitsemiseksi ja niihin reagoimiseksi.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

FTC:n ylläpitämä IdentityTheft.gov antaa yhdysvaltalaisille uhreille mahdollisuuden ilmoittaa identiteettivarkaudesta ja saada henkilökohtaisen toipumissuunnitelman. [1]

2. TURVALLISUUSOIVALLUS

Laitteistoturva-avaimet ovat tietojenkalastelua kestävää monivaiheista tunnistautumista (MFA), vahvinta MFA:n lajia, jota CISA kehottaa käyttämään. [4]

3. TURVALLISUUSOIVALLUS

Vaarantuneet salasanat ovat yleinen sisääntulopiste tietomurroissa ja ruokkivat myöhempää identiteettipetosta.

4. TURVALLISUUSOIVALLUS

Luottotietojen jäädytys on liittovaltion lain mukaan ilmainen, ja se estää luotonantajia tarkistamasta luottotietoja ennen kuin jäädytys puretaan. [2]

5. TURVALLISUUSOIVALLUS

DMARC antaa verkkotunnuksen omistajan kehottaa postipalvelimia hylkäämään tai asettamaan karanteeniin väärennetyn sähköpostin, joka ei läpäise tarkistuksia. [7]

6. TURVALLISUUSOIVALLUS

SIM-kortin kaappaus (SIM swapping) antaa hakkereille mahdollisuuden ohittaa tekstiviestipohjaisen kaksivaiheisen tunnistautumisen pankkiportaaleissa.

7. TIETOTURVATIETOA

Synteettinen identiteettipetos sekoittaa todellisia ja väärennettyjä tietoja, minkä vuoksi luotonantajien on vaikea havaita sitä.

8. TIETOTURVATIETOA

Monet ihmiset käyttävät samaa salasanaa useilla verkkotileillä, joten yksi tietomurto voi paljastaa useita tilejä.

9. TIETOTURVATIETOA

Tietovälittäjät kokoavat suurista kuluttajamääristä yksityiskohtaisia profiileja, mikä keskittää yksityisyysriskin.

10. TURVALLISUUSOIVALLUS

Identiteettivarkaudesta toipuminen voi viedä kuukausia työtä, kuten veloitusten kiistämistä ja luottotietojen korjaamista.

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.). 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

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1

Oikea vastaus: A

OPETTAJALLE

Mikä on ensisijainen tapa, jolla identiteettivarkaat varastavat kirjautumistunnuksia? → Väärennettyjen sähköpostihälytysten lähettäminen, jotta käyttäjät syöttävät salasanansa väärennetyissä portaaleissa

2 Kysymys 2

Oikea vastaus: A

OPETTAJALLE

Mikä tietoturvakontrolli tarjoaa vahvimman suojan tunnusvuodoilta? → Monitekijätodennus laitteistoavaimilla

3 Kysymys 3

Oikea vastaus: A

OPETTAJALLE

Mikä edustaa luottotietojen jäädytystä? → Luottotietojen lukitseminen, jotta varkaat eivät voi avata luvattomia lainoja

4 Kysymys 4

Oikea vastaus: A

OPETTAJALLE

Miksi darkwebin seuranta on hyödyllistä? → Se hälyttää käyttäjiä, jos heidän vuotaneet tunnistetietonsa näkyvät laittomissa tietokannoissa

5 Kysymys 5

Oikea vastaus: A

OPETTAJALLE

Mitä sosiaalinen manipulointi tarkoittaa? → Ihmisten manipulointi paljastamaan luottamuksellisia tunnistetietoja vapaaehtoisesti

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 Kysymys 6

Oikea vastaus: Epätosi

OPETTAJALLE

Identiteettivarkaus voi alkaa myös verkon ulkopuolella, esimerkiksi varastetusta postista tai asiakirjoista.

7 Kysymys 7

Oikea vastaus: Tosi

OPETTAJALLE

Monivaiheisen tunnistautumisen pakottaminen kaikille henkilökohtaisille tileille estää suurimman osan tunnistetietojen täyttöhyökkäyksistä.

8 Kysymys 8

Oikea vastaus: Epätosi

OPETTAJALLE

Luottojäädytys estää uudet luottotarkistukset mutta ei vaikuta nykyisiin tileihisi.

9 Kysymys 9

Oikea vastaus: Tosi

OPETTAJALLE

Salasananhallinnat suojaavat tietojenkalastelulta kieltäytymällä täyttämästä salasanoja automaattisesti väärennetyille verkkotunnuksille.

10 Kysymys 10

Oikea vastaus: Tosi

OPETTAJALLE

Tietojenkalastelusähköpostit käyttävät usein kiireellistä kieltä herättääkseen tunteita ja nopeita reaktioita.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

H 1. KÄYTTÖTUNNUKSET	D 2. VUODOT	A 3. MFA	G 4. SEURANTA
C 5. JÄÄDYTYS	E 6. PUOLUSTUS	B 7. VÄÄRENNYS	F 8. TIETOJENKALASTELU

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 TUNNISTETIEDOT	2 TIETOVUODOT	3 MFA-TUNNISTUS	4 VALVONTA
5 LUOTTOLUKITUS	6 PUOLUSTUS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 H – KALASTELU	2 A – TUNNISTETIEDOT	3 G – VÄÄRENNYS	4 F – PUOLUSTUS
5 D – VALVONTA	6 E – LUOTTOLUKITUS	7 B – TIETOVUODOT	8 C – MFATUNNISTUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit KÄYTTÖTUNNUKSET, VUODOT ja MFA omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

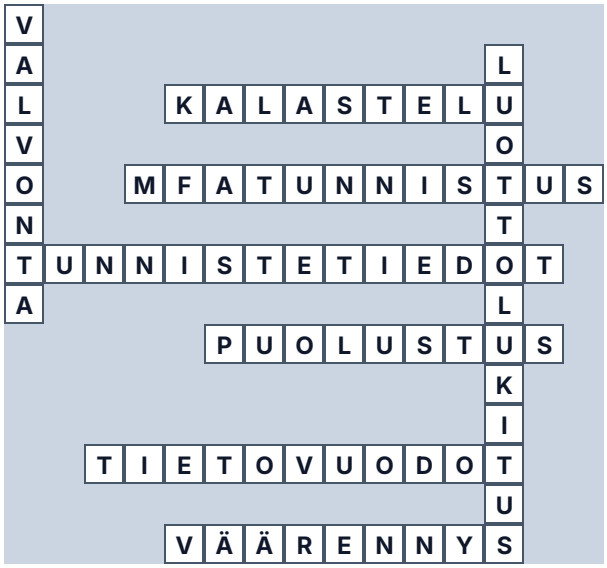
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

3 vaakasuoraan: KALASTELU Vilpillisten viestien lähettäminen, joilla käyttäjät huijataan luovuttamaan tunnistetietonsa. (9 kirjainta)

4 vaakasuoraan: MFATUNNISTUS Toissijainen varmennusvaihe (esimerkiksi laitteistoavaimet), joka suojaa tilien kirjautumisia. (12 kirjainta)

5 vaakasuoraan: TUNNISTETIEDOT Käyttäjätunnukset, salasanat ja yksityiset tunnisteet, joilla todennetaan digitaaliset identiteetit. (14 kirjainta)

6 vaakasuoraan: PUOLUSTUS Koulutus ja tekniset kontrollit, joilla suojaudutaan identiteettivarkauksilta. (9 kirjainta)

7 vaakasuoraan: TIETOVUODOT Henkilötietoja sisältävien yksityisten tietokantojen luvaton paljastuminen. (11 kirjainta)

8 vaakasuoraan: VÄÄRENNYS Väärennetyn verkkosivuston tai sähköpostin luominen oikean organisaation jäljittelemiseksi. (9 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: VALVONTA Verkkofoorumien ja hakkerikanavien skannaus varastettujen yritystietojen löytämiseksi. (8 kirjainta)

2 pystysuoraan: LUOTTOLUKITUS Luottotietojen käytön rajoittaminen petollisten lainahakemusten estämiseksi. (13 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. ESEITNUTDTOTIN — **TUNNISTETIEDOT**
2. SFUNMTUAISNT — **MFATUNNISTUS**
3. ULUIKUSOLTOTT — **LUOTTOLUKITUS**
4. ESYRNNVÄÄ — **VÄÄRENNYS**
5. DIOUETOVTOT — **TIETOVUODOT**
6. TAVNVOAL — **VALVONTA**
7. SPUSTLUUO — **PUOLUSTUS**
8. USLKAATEL — **KALASTELU**

SALAKIRJOITUSHAASTEEN AVAIN

"SUOJAA IDENTITEETTISI MFA TUNNISTUKSELLA"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Johtajan identiteetin väärentämisen torjunta

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Näkyvän ylimmän johdon edustajan kohteena on ollut kirjoitusvirheisiin perustuvia verkkotunnuksia, jotka jäljittelevät hänen henkilökohtaista sähköpostiaan asiakkaiden huijaamiseksi. Laadi brändinsuojasuunnitelma.
- Suositeltu strategia ja ratkaisu: Rekisteröi kaikki johtajan nimen yleiset kirjoitusasuvariantit. Ota käyttöön sähköpostin todennusprotokollat (DMARC, DKIM, SPF) verkkotunnuksen väärentämisen estämiseksi. Pakota laitteistopohjainen MFA kaikkiin ylimmän johdon yrityskirjautumisiin.

B Tapaustutkimus 2: Yrityksen käyttötunnusten paljastuminen Dark Webissä

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Pimeän verkon tietokantavuoto sisältää useita satoja yrityksen järjestelmänvalvojien yritystunnuksia. Suunnittele lieventämisstrategia.
- Suositeltu strategia ja ratkaisu: Suorita koko yrityksen laajuinen salasanojen nollaus. Vaadi yrityksen salasanojen hallintaohjelman käyttö. Ota MFA käyttöön kaikissa järjestelmäportaaleissa ja määritä jatkuvat automaattiset pimeän verkon seurantahälytykset.