Nimi: _____ Päivämäärä: _____ Pisteet: _____

Tietojenkalasteluhyökkäykset ja sosiaalinen manipulointi

Spear phishing, whaling-huijaukset, SPF/DKIM/DMARC-protokollat, lähettäjän väärentäminen ja työntekijöiden tietoturvakoulutus.

TIETOJENKALASTELUHYÖKKÄYKSET, OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: tietojenkalasteluhyökkäykset ja sosiaalinen manipulointi. Tutustut kohdennettuun tietojenkalasteluun (spear phishing), johtajiin kohdistuvaan kalasteluun (whaling), verkkotunnuksen väärentämiseen, SPF-, DKIM- ja DMARC-protokolliin, linkkien turvallisuuteen ja työntekijöiden tietoisuuskoulutukseen.

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/tietojenkalasteluhyokkaukset/

Oppimispolkusi: tietojenkalastelun torjunta

- Tunnista yleiset tietojenkalastelu-, vishing- ja tukiponnahdushuijaukset.
- Toteuta kanavan ulkopuoliset maksutapahtumien vahvistusmenettelyt.
- Määritä SPF-, DKIM- ja DMARC-säännöt väärennettyjen verkkotunnusten estämiseksi.

TIETOJENKALASTELUOPAS, OHJEET

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

TIETOJENKALASTELUHYÖKKÄYKSET JA SOSIAALINEN MANIPULOINTI (JOHDANTO)

Tietojenkalasteluhyökkäykset hyödyntävät kohdennettuja viestejä, huippujohtajiin kohdistuvia huijauksia (whaling) ja verkkotunnusten väärentämistä käyttäjien kirjautumistietojen keräämiseen. Yritysjärjestelmien suojaaminen edellyttää SPF-, DKIM- ja DMARC-sääntöjen käyttöönottoa yhdyskäytävässä sekä kanavan ulkopuolisia hyväksyntävaiheita.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1 **1. Mitä on kohdennettu tietojenkalastelu (spear phishing)?**

- A. Tietylle henkilölle tai organisaatiolle räätälöity kohdennettu tietojenkalasteluviesti
- B. Laaja massasähköposti, joka lähetetään miljoonille satunnaisille osoitteille
- C. Verkkohyökkäys, joka tulvittaa verkkopalvelimet liikenteellä
- D. Tietokannan poimintatekniikka, joka kohdistuu käyttäjätietueisiin

2 **2. Mikä protokolla antaa verkkotunnuksen luetteloida sallitut lähettävät IP-osoitteensa DNS:ssä huijauksen torjumiseksi?**

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

3 **3. Mikä on whaling-hyökkäys?**

- A. Tietojenkalastelukampanja, joka on kohdistettu erityisesti korkean profiilin yritysjohtajiin
- B. SQL-injektiohyökkäys, joka kohdistuu tietokantojen varmuuskopioihin
- C. Paikallisverkon reitityslaitteiden fyysinen varkaus
- D. Automaattinen credential stuffing -raakavoimaskannaus

4 **4. Mitä DKIM tekee?**

- A. Lisää sähköposteihin kryptografisen allekirjoituksen lähettäjän aitouden varmistamiseksi
- B. Estää saapuvat verkkopaketit palomuurissa
- C. Salaa tietokantojen tallennusvolyymit lepotilassa
- D. Skannaa sähköpostiliitteet allekirjoituspohjaisten haittaohjelmien varalta

5 **5. Mikä on DMARCin tehtävä?**

- A. Vastaanottavien sähköpostipalvelimien ohjeistaminen epäonnistuneiden SPF/DKIM-tarkistusten käsittelyssä
- B. Järjestelmäsalasanojen purkaminen ennalta lasketuilla sateenkaaritaulukoilla
- C. Sähköpostiliitteiden pakkaaminen ennen toimitusta
- D. Verkon reititysoikeuksien määrittäminen

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Spear phishing perustuu yleisiin massasähköposteihin, jotka lähetetään miljoonille satunnaisille osoitteille.

○ Tosi ○ Epätosi

7 Kysymys 7

7. DMARC-käytännöt voivat ohjeistaa postipalvelimia hylkäämään luvattomat väärennetyt viestit.

○ Tosi ○ Epätosi

8 Kysymys 8

8. SPF-varmennus toimii validoimalla sähköpostin sisällön kryptografisen allekirjoituksen.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Whaling-hyökkäykset kohdistuvat alemman tason yrityksen ylläpitäjiin tietokantatiedostojen saamiseksi.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Maksupyyntöjen kaistan ulkopuolinen vahvistus auttaa pysäyttämään rahansiirtohuijaukset.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Tiettyyn työntekijään henkilökohtaisin tiedoin kohdistuva tietojenkalastelu on nimeltään _____ .

2. Sähköpostin otsikon jäljittely viestien uskottavuuden luomiseksi on lähettäjän _____ .

3. Valtuutettujen postipalvelinten IP-osoitteiden DNS-tietueluettelo on _____ .

4. Lähettäjän todennuksen tarjoava sähköpostiallekirjoitusstandardi on _____ .

5. SPF- ja DKIM-tarkistuksissa epäonnistuneiden viestien hylkäämiskäytäntöjen määrittämiseen käytetään standardia nimeltä _____ .

6. Ylimmän johdon edustajiin kohdistuva tietojenkalastelukampanja on nimeltään _____ .

SANASTON SANAPANKKI

DKIM DMARC KOHDISTETTU LUNNASOHJELMA SPF-TIETUE VISHING VÄÄRENTÄMINEN WHALING

Kirjoita vastauksesi tähän:

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

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

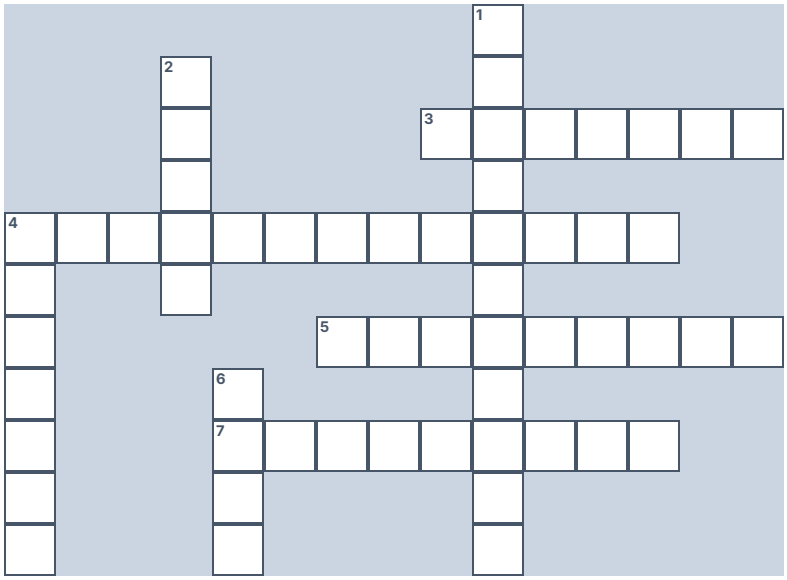
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. KOHDISTETTU	A	Puhelinhuijaukset.
☐	2. VÄÄRENNYS	B	Kohdistuu C-tason johtajiin.
☐	3. SPF	C	Käytäntöä hylkäävät ohjeet.
☐	4. DKIM	D	DNS:ssä valtuutetut lähettäjien IP-osoitteet.
☐	5. DMARC	E	Sosiaalisen manipuloinnin sähköposti.
☐	6. WHALING-HYÖKKÄYS	F	Kohdennettu henkilökohtainen sähköposti.
☐	7. TIETOJENKALASTELU	G	Lähettäjän sähköpostiosoitteen väärentäminen.
☐	8. VISHING	H	Sähköpostin kryptografinen allekirjoitus.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

3. Ylimmän johdon kohdistaminen. (7)

4. Lähettäjän sähköpostiosoitteen väärentäminen. (13)

5. DNS-tietue valtuutetuista lähettäjien IP-osoitteista. (9)

7. Sosiaaliseen manipulointiin perustuva sähköposti. (9)

PYSTYSUORAAN

1. Henkilökohtaistettu kohdennettu sähköposti. (11)

2. Käytäntö, joka ohjeistaa hylkäämään viestit. (5)

4. Puheluihin perustuvat huijaukset. (7)

6. Kryptografinen allekirjoitus sähköpostissa. (4)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

3 vaakasuoraan: Ylimmän johdon kohdistaminen. (7 kirjainta):

4 vaakasuoraan: Lähettäjän sähköpostiosoitteen väärentäminen. (13 kirjainta):

5 vaakasuoraan: DNS-tietue valtuutetuista lähettäjien IP-osoitteista. (9 kirjainta):

7 vaakasuoraan: Sosiaaliseen manipulointiin perustuva sähköposti. (9 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Henkilökohtaistettu kohdennettu sähköposti. (11 kirjainta):

2 pystysuoraan: Käytäntö, joka ohjeistaa hylkäämään viestit. (5 kirjainta):

4 pystysuoraan: Puheluihin perustuvat huijaukset. (7 kirjainta):

6 pystysuoraan: Kryptografinen allekirjoitus sähköpostissa. (4 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

U Y E V Ä X C P C Ö K Y G L I

T G Ö D O R E F S Z A R C W B

T N A Ö A P E T M A L E Q E F

E I H M J D T I S N A F J U Ö

T L D U G S Y E F A S A S Q O

S A R W Å S L T T W T U D O Ä

I H B G U Z Z U K A E T Ö Ä Ä

D W M H J O T E L N L N V Q I

H S S H Ö A Q X G X U C Ä T Ä

O V Ä Ä R E N T Ä M I N E N B

K I N D Ö H K P R P Z C N Ö Ä

G Å K Q Y X M X R B P Y V N H

X I D Ä X L T B Z Ö Å N T S Å

M J Q E A D L S Y Z Z M K I W

SANASTOLISTA

KOHDISTETTU VÄÄRENTÄMINEN SPFTIETUE DKIM DMARC WHALING KALASTELU VISHING

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. KOHDISTETTU**
- **B. VÄÄRENTÄMINEN**
- **C. SPFTIETUE**
- **D. DKIM**
- **E. DMARC**
- **F. WHALING**
- **G. KALASTELU**
- **H. VISHING**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Lähettäjän sähköpostiosoitteen väärentäminen.
2. Henkilökohtaistettu kohdennettu sähköposti.
3. Puheluihin perustuvat huijaukset.
4. DNS-tietue valtuutetuista lähettäjien IP-osoitteista.
5. Sosiaaliseen manipulointiin perustuva sähköposti.
6. Käytäntö, joka ohjeistaa hylkäämään viestit.
7. Kryptografinen allekirjoitus sähköpostissa.
8. Ylimmän johdon kohdistaminen.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. ITTOSEKTHUD
2. ESUTPETIF
3. ADCRM
4. SULAETKAL
5. MNÄÄÄENNITVER
6. IMDK
7. WNIGHLA
8. IHGVNIS

Bonustehtävä: Nopeat vastaukset

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

1	Laitteita, jotka voidaan hakkeroida			
2	Merkkejä tietojenkalastelusähköpostista			
3	Merkkejä siitä, että tietokone on saanut tartunnan			
4	Sanoja, jotka luovat valekiireen			
5	Tapoja tarkistaa lähettäjä			
6	Ihmisiä, joilta voit pyytää IT-apua			
7	Asioita, joista otat varmuuskopion			
8	Kaloja tai merieläimiä, jotka tunnet			
9	Yrityksiä, joiksi huijarit esittäytyvät			
10	Turvallisia tapoja, joita voit aloittaa tänään			
11	Asioita, joita teet väärennettyä linkkiä napsautettuasi			
12	Asioita, joita teet tietovuodon jälkeen			
13	Kanavia, joissa tietojenkalastelua tapahtuu			
14	Asioita, joita et koskaan lähetä sähköpostitse			
15	Tapoja suojata tilisi			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: YLIMMÄN JOHDON WHALING-HYÖKKÄYKSEN KORJAAMINEN



Tilanne: Talousjohtaja saa erittäin henkilökohtaisen sähköpostin, jonka väitetään tulevan toimitusjohtajalta ja jossa pyydetään nopeaa 50 000 dollarin pankkisiirtoa luottamuksellisen verkkotunnuskaupan sulkemiseksi.

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

TAPAUSTUTKIMUS 2: SPF/DKIM/DMARC-YHDYSKÄYTÄVÄKÄYTÄNTÖJEN KÄYTTÖÖNOTTO



Tilanne: Yritys epäonnistuu tietoturvatarkastuksissa, koska lähtevät markkinointisähköpostit merkitään usein roskapostiksi ja hakkerit väärentävät aktiivisesti yrityksen brändiverkkotunnusta.

Keskustelukysymys: Laadi tekniset ja hallinnolliset kontrollit sähköpostin aitouden varmistamiseksi.

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

13	1	14	9	16	21	12	15	9	14	20	9

19	28	8	11	29	16	15	19	20	9	14	1	22	21	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 tietojenkalastelu?

Tietojenkalastelu on sosiaalisen manipuloinnin hyökkäys, jossa rikolliset lähettävät vilpillisiä viestejä huijatakseen käyttäjiä jakamaan arkaluonteisia tietoja.

Q2: Mikä ero on tietojenkalastelulla ja kohdennetulla tietojenkalastelulla?

Tietojenkalastelu kohdistuu laajoihin ryhmiin yleisellä sisällöllä, kun taas kohdennettu tietojenkalastelu kohdistuu tiettyihin uhreihin räätälöityjen tietojen avulla.

Q3: Mitä whaling on?

Whaling on erittäin kohdennettu tietojenkalasteluhyökkäys, joka kohdistuu korkean profiilin johtajiin, joilla on hallinnolliset valtuudet.

Q4: Mitä sähköpostin väärentäminen on?

Sähköpostin väärentäminen tarkoittaa sähköpostiviestien luomista väärennetyllä lähettäjäosoitteella, jotta vastaanottaja luottaa lähteeseen.

Q5: Miten SPF estää väärentämisen?

Se julkaisee DNS:ssä luettelon valtuutetuista lähettävistä IP-osoitteista, jolloin vastaanottavat palvelimet voivat varmistaa postin lähteen. [1]

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

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Mikä on DKIM?

DomainKeys Identified Mail lisää sähköpostin otsikoihin kryptografisen allekirjoituksen, joka osoittaa, että verkkotunnus on ottanut vastuun ja että viestiä ei ole muutettu.

Q7: Mitä DMARC tarkoittaa?

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

Q8: Mikä on DMARC-käytäntö?

Käytäntö, joka kertoo postipalvelimille, miten SPF/DKIM-tarkistuksessa epäonnistuvia viestejä käsitellään (ei mitään, karanteeni tai hylkäys). [2]

Q9: Mitä vishing on?

Vishing eli puhelinhuijaus, jossa hyökkääjät käyttävät vilpillisiä puheluita hallinnollisten tai taloudellisten tietojen urkintaan.

Q10: Miten linkkiskannerit auttavat?

Ne skannaavat ja kirjoittavat uudelleen saapuvien sähköpostien linkit tarkistaakseen kohdesivujen turvallisuuden klikkaushetkellä.

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

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

Q1: Miten homografihyökkäys toimii?

Hyökkääjät rekisteröivät verkkotunnuksia käyttämällä ulkonäöltään samankaltaisia ei-ASCII-Unicode-merkkejä, jotta verkkotunnus muistuttaisi visuaalisesti oikeaa verkkotunnusta.

Q2: Mikä on punycode-esitys?

Koodaus, joka muuntaa Unicode-verkkotunnukset ASCII-yhteensopiviksi merkkijonoiksi, jotka alkavat ”xn--”, jotta DNS voi käsitellä niitä.

Q3: Miksi 'p=reject' on turvallisin DMARC-tila?

Se pyytää vastaanottavia palvelimia hylkäämään postin, joka ei läpäise DMARC-tarkistusta (kohdistettu SPF/DKIM), SMTP-istunnon aikana ja estää suoran väärennöksen. [2]

Q4: Miten hyökkääjät ohittavat SPF-sääntöjä?

Hyödyntämällä samannäköisiä verkkotunnuksia (typosquatting) tai käyttämällä kaapattuja tilejä lailliseen kolmannen osapuolen sähköpostipalveluun.

Q5: Mitä yrityssähköpostin kompromissi (BEC) on?

Yrityksiin kohdistuva huijaus, jossa hyökkääjät kaappaavat yrityksen sähköpostitilejä tai esiintyvät niiden haltijoina vilpillisten maksujen hyväksymiseksi.

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

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

Q6: Miten monivaiheinen todennus pysäyttää tietojenkalastelun?

Se vaatii toissijaisia tunnisteita (kuten laiteavaimia), joita ei voi varastaa pelkästään samannäköisten laskeutumissivujen avulla.

Q7: Mikä on tunnistetietoja urkkiva laskeutumissivu?

Samannäköinen kirjautumisportaali, joka on suunniteltu sieppaamaan syötetyt käyttäjätunnukset, salasanat ja MFA-tunnukset reaaliajassa.

Q8: Mitä aliverkkotunnuksen kaappaus on?

Hyökkääjä ottaa haltuunsa käyttämättömän DNS-aliverkkotunnuksen osoittimen isännöidäkseen haitallisia tietojenkalastelun laskeutumissivuja luotetun ylätason verkkotunnuksen alla.

Q9: Miten DKIM-kohdistuksen tarkistus toimii?

Se varmistaa, että 'From'-otsakkeen verkkotunnus vastaa verkkotunnusta, joka allekirjoitti viestin kryptografisesti DKIM-otsakkeessa.

Q10: Mikä on sähköpostiyhdyskäytävän tehtävä?

Saapuvan sähköpostin suodatus, linkkien tarkastus, liitteiden hiekkalaatikkoeristys ja SPF/DKIM/DMARC-vaatimustenmukaisuuden todennus.

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. [4]

2. TURVALLISUUSOIVALLUS

Yritysviestipetokset (BEC) aiheuttivat FBI:n IC3:lle ilmoitettuja yli 3 miljardin dollarin tappioita vuonna 2025. [4]

3. TURVALLISUUSOIVALLUS

Homografihyökkäykset käyttävät kyrillisiä samannäköisiä kirjaimia jäljitelläkseen visuaalisesti tarkan vastaavuuden brändiverkkotunnuksia selaimissa.

4. TURVALLISUUSOIVALLUS

'p=reject'-asetuksella verkkotunnus pyytää vastaanottajia hylkäämään epäonnistuvan sähköpostin toimituksen aikana eikä ohjaamaan sitä roskapostiin. [2]

5. TURVALLISUUSOIVALLUS

Toimitusjohtajiin kohdistuvat whaling-hyökkäykset vaativat usein kiireellisiä maksuja luottamuksellisia yritysostoja tai verkkotunnusostoja varten.

6. TURVALLISUUSOIVALLUS

Tunnusten kalastelun portaalit kopioivat oikeita kirjautumissivuja, jotta uhrit kirjoittavat salasanansa suoraan hyökkääjän lomakkeeseen.

7. TIETOTURVATIETOA

CISAn yhteinen tietojenkalasteluopas suosittelee käyttäjäkoulutusta DMARC:n, SPF:n, DKIM:n ja kalastelun kestävän MFA:n rinnalla. [3]

8. TIETOTURVATIETOA

SPF-arviointi rajoittuu 10 DNS-kyselyjä tekevään termiin; rajan ylittäminen palauttaa 'permerror'-tuloksen. [1]

9. TIETOTURVATIETOA

FIDO2-laiteturva-avaimet tarjoavat kryptografisesti tuettua suojaa etäyhteyden kautta tapahtuvaa tunnistetietojen keruuta vastaan.

10. TURVALLISUUSOIVALLUS

Tietojenkalastelu on yksi yleisimmistä tavoista, joilla hyökkääjät pääsevät ensimmäisen kerran organisaatioon, minkä vuoksi säännöllinen tietoisuuskoulutus on tehokas puolustus.

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[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

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1

Oikea vastaus: A

OPETTAJALLE

Mitä on kohdennettu tietojenkalastelu (spear phishing)? → Tietylle henkilölle tai organisaatiolle räätälöity kohdennettu tietojenkalasteluviesti

2 Kysymys 2

Oikea vastaus: A

OPETTAJALLE

SPF julkaisee verkkotunnuksen sallitut lähettävät isännät DNS:ssä, jotta vastaanottajat voivat tarkistaa kirjekuoren lähettäjän.

3 Kysymys 3

Oikea vastaus: A

OPETTAJALLE

Mikä on whaling-hyökkäys? → Tietojenkalastelukampanja, joka on kohdistettu erityisesti korkean profiilin yritysjohtajiin

4 Kysymys 4

Oikea vastaus: A

OPETTAJALLE

Mitä DKIM tekee? → Lisää sähköposteihin kryptografisen allekirjoituksen lähettäjän aitouden varmistamiseksi

5 Kysymys 5

Oikea vastaus: A

OPETTAJALLE

Mikä on DMARCin tehtävä? → Vastaanottavien sähköpostipalvelimien ohjeistaminen epäonnistuneiden SPF/DKIM-tarkistusten käsittelyssä

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 Kysymys 6

Oikea vastaus: Epätosi

OPETTAJALLE

Epätosi: kohdennettu tietojenkalastelu (spear phishing) räätälöidään tietyille ihmisille, toisin kuin yleinen massatietojenkalastelu.

7 Kysymys 7

Oikea vastaus: Tosi

OPETTAJALLE

DMARC-käytännöt voivat ohjeistaa postipalvelimia hylkäämään luvattomat väärennetyt viestit.

8 Kysymys 8

Oikea vastaus: Epätosi

OPETTAJALLE

Epätosi: SPF tarkistaa lähettävän IP-osoitteen DNS:stä; DKIM on se, joka varmistaa kryptografisen allekirjoituksen.

9 Kysymys 9

Oikea vastaus: Epätosi

OPETTAJALLE

Epätosi: whaling kohdistuu ylimpään johtoon, joka voi hyväksyä maksuja ja päästä käsiksi arkaluonteisiin tietoihin.

10 Kysymys 10

Oikea vastaus: Tosi

OPETTAJALLE

Tosi: maksupyyntöjen vahvistaminen erillisen, tunnetun kanavan kautta auttaa pysäyttämään pankkisiirtopetokset.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

F 1. KOHDISTETTU	G 2. VÄÄRENNYS	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING-HYÖKKÄYS	E 7. TIETOJENKALASTELU	A 8. VISHING

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 KOHDISTETTU	2 VÄÄRENTÄMINEN	3 SPF-TIETUE	4 DKIM
5 DMARC	6 WHALING		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 B – VÄÄRENTÄMINEN	2 A – KOHDISTETTU	3 H – VISHING	4 C – SPFTIETUE
5 G – KALASTELU	6 E – DMARC	7 D – DKIM	8 F – WHALING

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit KOHDISTETTU, VÄÄRENNYS ja SPF omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

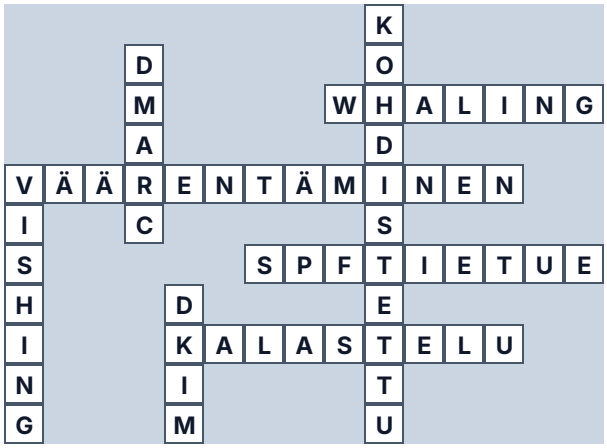
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

3 vaakasuoraan: WHALING Ylimmän johdon kohdistaminen. (7 kirjainta)

4 vaakasuoraan: VÄÄRENTÄMINEN Lähettäjän sähköpostiosoitteen väärentäminen. (13 kirjainta)

5 vaakasuoraan: SPFTIETUE DNS-tietue valtuutetuista lähettäjien IP-osoitteista. (9 kirjainta)

7 vaakasuoraan: KALASTELU Sosiaaliseen manipulointiin perustuva sähköposti. (9 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: KOHDISTETTU Henkilökohtaistettu kohdennettu sähköposti. (11 kirjainta)

2 pystysuoraan: DMARC Käytäntö, joka ohjeistaa hylkäämään viestit. (5 kirjainta)

4 pystysuoraan: VISHING Puheluihin perustuvat huijaukset. (7 kirjainta)

6 pystysuoraan: DKIM Kryptografinen allekirjoitus sähköpostissa. (4 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. ITTOSEKTHUD — **KOHDISTETTU**
2. ESUTPETIF — **SPFTIETUE**
3. ADCRM — **DMARC**
4. SULAETKAL — **KALASTELU**
5. MNÄÄÄENNITVER — **VÄÄRENTÄMINEN**
6. IMDK — **DKIM**
7. WNIGHLA — **WHALING**
8. IHGVNIS — **VISHING**

SALAKIRJOITUSHAASTEEN AVAIN

"TUNNISTA MANIPULOINTI SÄHKÖPOSTIN AVULLA"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Ylimmän johdon whaling-hyökkäyksen korjaaminen

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Talousjohtaja saa erittäin henkilökohtaisen sähköpostin, jonka väitetään tulevan toimitusjohtajalta ja jossa pyydetään nopeaa 50 000 dollarin tilisiirtoa luottamuksellisen verkkotunnuskaupan päättämiseksi.
- Suositeltu strategia ja ratkaisu: Määritä DMARC 'p=reject' -käytännöllä väärennettyjen lähettäjäverkkotunnusten estämiseksi. Lisää ulkoisen lähettäjän varoitusbannerit yhdyskäytävään ja vaadi suullinen, erillisen kanavan vahvistus kaikille rahansiirroille.

B Tapaustutkimus 2: SPF/DKIM/DMARC-yhdyskäytäväkäytäntöjen käyttöönotto

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yritys epäonnistuu tietoturvatarkastuksissa, koska lähtevät markkinointisähköpostit merkitään usein roskapostiksi ja hakkerit väärentävät aktiivisesti yrityksen brändin verkkotunnusta.
- Suositeltu strategia ja ratkaisu: Julkaise SPF:n TXT-tietue, jossa luetellaan valtuutetut lähettäjien IP-osoitteet. Määritä DKIM-allekirjoitusavaimet lähtevän postin palvelimille ja analysoi saapuvia DMARC XML -palauteraportteja väärinkäytösten tunnistamiseksi.