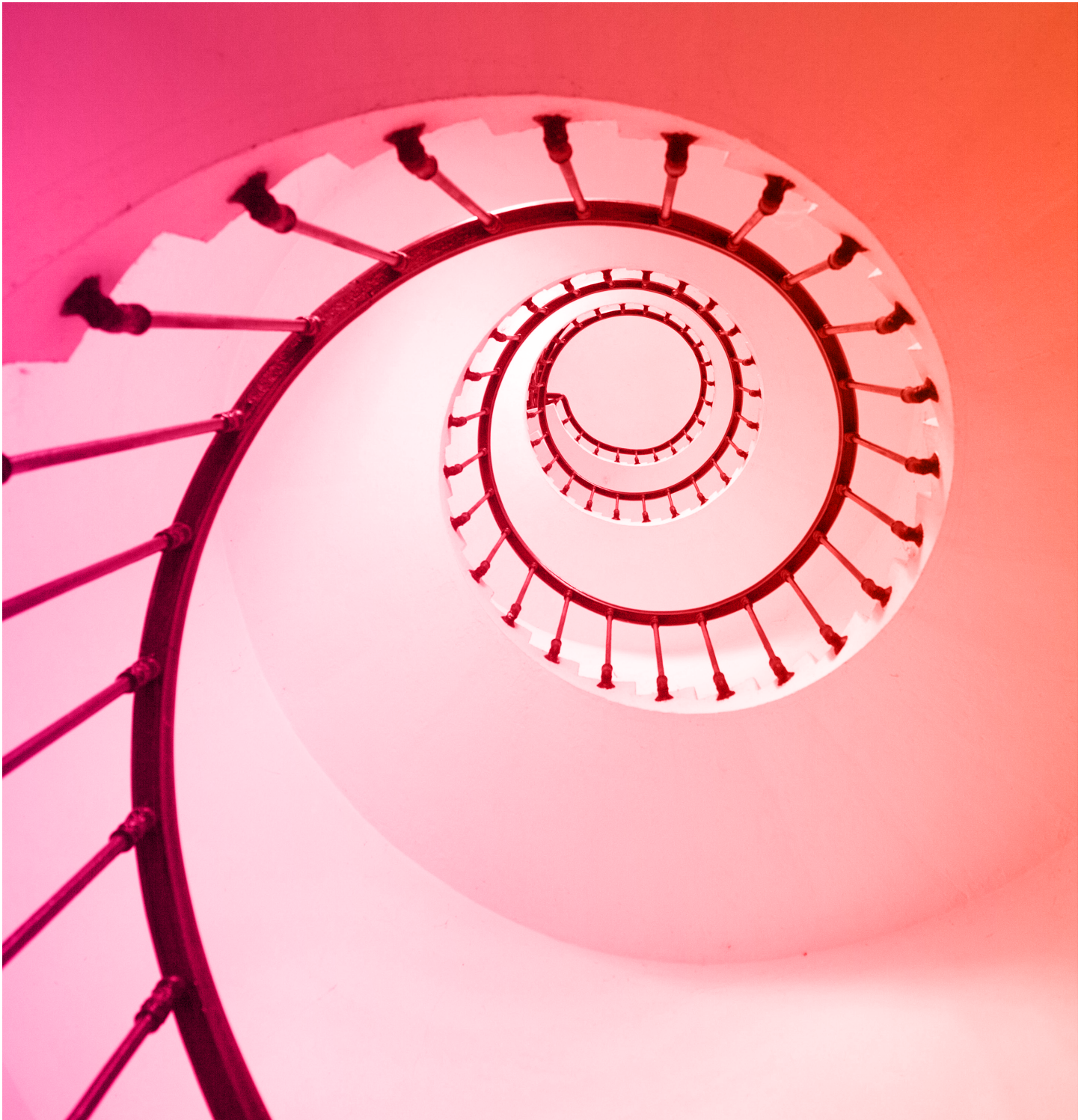




Taloushallintoalan työntekijän tietoturvakoulutus

¹ Järjestömme noudattaa kilpailulakia



Kilpailulaki kieltää sellaiset sopimukset, päätökset sekä yhdenmukaistetut menettelytavat, joiden tarkoituksena on merkittävästi estää, rajoittaa tai vääristää kilpailua tai joista seuraa, että kilpailu merkittävästi estyy, rajoittuu tai vääristyy.

Mikäli keskustelu liittyy kiellettyyn teemaan, kaikkien osallistujien tehtävä on lopettaa keskustelu. Emme keskustele seuraavista teemoista, jotka sisältävät jäsenen luottamuksellista tietoa:

- Yksityiskohtaiset sopimusehdot
- Toimittajat, asiakkaat
- Tarjoukset
- Tuotantomäärät
- Laajentumissuunnitelmat, jotka eivät vielä julkisia
- Muut tulevaisuudensuunnitelmat (esim. T&K-panostukset, tuotantoseisokit)

- Alan yleinen hintataso ja siihen vaikuttaminen
- Hinnoittelukäytännöt ja –mekanismit
- Osto- ja myyntihinnat
- Markkinaosuudet
- Kustannukset
- Kannattavuus
- Yhteiset boikotit

Moduuli 1: Tietoturva ja tietosuoja taloushallintoalalla

23.9.2024 ©Taloushallintoliitto



**talous
hallinto
liitto**



Huoltovarmuuskeskus

Tietoturvan perusteet ja merkitys taloushallintoalalla

Taloushallinnon työntekijöiden tietoturva

Moduuli 1: Tietoturva ja tietosuoja taloushallintoalalla

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Tietoturvan perusteet ja merkitys taloushallintoalalla



- Tämä on työntekijöiden tietoturvakurssin ensimmäinen osio, jossa kerrotaan tietoturvan perusteista ja merkityksestä taloushallintoalalla.
- Osio kertoo lähtökohdat tälle tietoturvakurssille, eli mitä tietoturva on, miksi se on tärkeää ja millaisia vaikutuksia sillä käytännössä voi olla työssä.
- Kurssin käytyäsi osaat toimia oikein ja omalla toiminnallasi autat organisaatiotasi pitämään sekä omat että asiakkaiden tiedot turvassa.

Johdanto: Tietoturvan perusteet ja merkitys taloushallintoalalla



- Taloushallinnon ammattilaisilla ja alan yrityksillä on merkittävä rooli ja vaikutus suomalaisessa yhteiskunnassa.
- Suomessa on 4200 tilitoimistoa, jotka vastaavat päivittäin suomalaisen yhteiskunnan toiminnan kannalta keskeisistä tehtävistä.
- Vuoden jokaisena päivänä taloushallintoala huolehtii palkanmaksusta, yritysten välisestä maksuliikenteestä, verojen maksusta ja monesta muusta taloudellisesta toiminnosta, joita ilman yhteiskuntamme ei toimisi normaalilla tavalla.
- Taloushallinnon tehtävien suorittaminen vaatii tietojen luotettavaa käsittelyä, tietojen oikeellisuutta ja eheyttä sekä ajantasaista saatavuutta – toisin sanoen asioita, jotka vaativat onnistuakseen rautaisen ammattilaisuuden lisäksi hyvin hoidettua tietoturvaa.

Mitä ”tietoturva” tarkoittaa käsitteenä?



Tietoturvalla tarkoitetaan tietojen luottamuksellisuuden, eheyden ja saatavuuden suojaamista. Näitä tavoitteita varmistetaan tietoturvatoimenpiteillä ja -kontrolleilla, esimerkiksi henkilöstön tietoturvaosaamisen kehittämisellä, hallituilla prosesseilla ja tietoturvaa tukevilla teknologiaratkaisuilla.

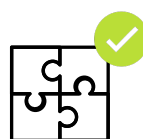
Tietoturvan tavoitteet

Luottamuksellisuus



Tieto on vain luvallisten henkilöiden saatavilla.

Eheys



Tietoa ei voi muokata luvatta eivätkä ne voi muuttua vahingossa.

Saatavuus



Tietojärjestelmät ja niiden sisältämät tiedot ovat saatavilla oikea-aikaisesti.

Tässä koulutuksessa keskitymme sähköisessä muodossa oleviin tietoihin ja IT-järjestelmiin. Tietoturvan perusperiaatteet koskevat silti samoin esimerkiksi paperimuodossa olevia tietoja.

Taloushallinnon työntekijöinä työmme tietoturvalla vaikutamme



Yksilöihin

Työssämme käsittelemme henkilötietoja, ja esimerkiksi huolimattomasta käsittelystä voi aiheutua erilaisia riskejä näille yksilöille.

Organisaatioihin

Työnantaja- ja asiakasorganisaatiomme luottavat siihen, että tiedot pysyvät luottamuksellisina, ovat oikeita ja saatavilla kun tarvitaan.

Koko Suomeen

Alaamme kohdistuva laaja tietoturvaongelma voisi aikaansaada mittavat vaikutukset esimerkiksi palkansaaajille ja veronkantoon.

Taloushallinnon työntekijöinä työmme tietoturvalla vaikutamme



Yksilöihin

Organisaatioihin

Koko Suomeen

Jokainen taloushallintoalan työntekijä vaikuttaa omalla työllään tähän kokonaisuuteen. Sillä, että huomioit työssäsi tietoturvatavoitteita tukevat hyvät toimintamallit, on valtavan suuri merkitys.

Tietoturvan merkitys erityisesti luottamuksellisten ja arkaluonteisten tietojen käsittelyn näkökulmasta



Huoltovarmuuskeskus

- Käytämme työssämme päivittäin sähköisiä järjestelmiä ja laitteita, ja on tärkeää osata käyttää näitä välineitä tietoturvallisesti.
- Taloushallinnon työntekijänä työskentelet työssäsi todennäköisesti sekä luottamuksellisten taloudellisten tietojen että henkilötietojen parissa. Sinulle on tärkeää, että nämä tiedot eivät päädy asiattomien henkilöiden käsiin. Tietoturalla estetään luvattomien henkilöiden pääsy näihin tietoihin, mikä suojaa sekä työntekijöitä että asiakkaita mahdollisilta tietojen väärinkäytöksiltä.
- Vääristä käsittelytavoista voi myös seurata korvausvelvollisuus, ja asiaton tai lainvastainen tietojenkäsittely voi johtaa jopa viranomaisseurauksiin.
- Hyvin hoidettu tietoturva puolestaan tuo suojaa jokaiselle osapuolelle, niin asiakkaille, taloushallintoalan organisaatioille kuin sinulle, joka työskentelet taloushallintoalalla.

Tietoturvariskejä



Huoltovarmuuskeskus

Tietoturva voi vaarantua hyvin erilaisten uhkien toteutuessa. Tällöin seuraus kohdistuu yhteen tai useampaan tietoturvan tavoitteista. Seuraavassa joitakin esimerkkejä tavanomaisista uhkista ja niiden seurauksista.

Uhka	Luottamuksellisuus	Eheys	Saatavuus
Liian laajat käyttövaltuusmääritykset	Luvaton henkilö katselee tietoja		
Työntekijän salasana päätty rikolliselle esim. kalasteluhyökkäyksessä	Rikollinen varastaa tietoja	Rikollinen muuttaa tietoja	
Palvelunestohyökkäys estää järjestelmän käytön		Muuttuneiden tietojen päivittäminen viivästyy	Tietojärjestelmä ja sen tiedot eivät ole saatavilla
Haavoittuvuus taloushallinto-ohjelmistossa	Rikollinen tunkeutuu järjestelmään ja pääsee käsiksi tietoihin	Rikollinen saattaa muuttaa tietoja	Rikollinen tuhoaa tiedot tai kiristää niiden palauttamisella
Valelasku		Perusteeton maksu	
Vika IT-järjestelmässä		Tiedot saatavat korruptoitua	Häiriö estää tietojen käytön

Hyvin hoidetun tietoturvan hyödyt



Huolehtimalla teknisestä tietoturvasta ja hyvistä toimintatavoista hallitsemme tietoturvariskejä tehokkaasti.

Henkilötiedot ovat suojattu

Henkilötietojen käsittelystä ei aiheudu haittoja yksilöille.

Vaatimustenmukaisuus

Toimimme lakien ja asetusten mukaisesti taloustietojen ja henkilötietojen osalta.

Liiketoiminnan jatkuvuus

Yrityksen toiminta ei vaarannu tietoturvaan liittyvien ongelmatilanteiden, kuten järjestelmähäiriöiden tai henkilötietoihin liittyvien tietoturvaloukkauksien takia.

Hyvä luottamus ja maine

Asiakkaiden ja yhteistyökumppaneiden luottamus säilyy, kun heihin liittyviä tietoja suojataan hyvin.

Työnteon sujuvuus

Työnteko yrityksessä on sujuvaa, kun tietoturvaan ja turvalliseen tietojenkäsittelyyn liittyvät asiat ovat selkeitä eivätkä aiheuta hämmennystä.

23.9.2024 ©Taloushallintoliitto

Tässä videossa olet oppinut



- Tässä videossa kävimme läpi, mitä tietoturvalla tarkoitetaan ja kuinka suuri merkitys jokaisen teolla on tietoturvalle. Tietoturva on erityisen merkityksellistä taloushallintoalalla: alaamme kohdistuva laaja tietoturvaongelma voisi aikaansaada mittavat vaikutukset koko Suomen toiminnalle.
- Käsittelimme videossa myös tietoturvan kolme keskeistä periaatetta: luottamuksellisuuden, saatavuuden ja eheyden.



23.9.2024 ©Taloushallintoliitto



Huoltovarmuuskeskus

Henkilötietojen tietosuoja perusteet taloushallintoalalla

Taloushallinnon työntekijöiden tietoturva

Moduuli 1: Tietoturva ja tietosuoja
taloushallintoalalla

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Henkilötietojen tietosuoja perusteet taloushallintoalalla



Huoltovarmuuskeskus

- Tämän osion aiheena on tietosuoja.
- Osiossa kerrotaan, mitä tietosuoja on, millainen merkitys sillä on niin yksilöille kuin organisaatioille ja minkälaisia periaatteita ja riskejä henkilötietojen käsittelyyn liittyy.

Mitä ”tietosuoja” tarkoittaa käsitteenä?



Tietosuojavaltuutetun toimisto määrittelee tietosuojan seuraavasti:

”Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.”

Henkilötieto ja henkilötietojen käsittely

- **Henkilötietoa on mikä tahansa tieto, joka liittyy tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön** (eli ihmiseen). Henkilötieto voi siis olla mikä tahansa tieto, joka liittyy henkilöön.
- **Henkilötietojen käsittely** tarkoittaa esimerkiksi henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista. Kaikki henkilötietoihin kohdistuvat toimenpiteet henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen ovat henkilötietojen käsittelyä.

Henkilötietoa ovat esimerkiksi



Tietosuojan sääntely

- Tietosuojaa säädellään lailla ja asetuksilla, kuten Euroopan yleisellä tietosuojasetuksella (GDPR). Laissa säädettyjä tietosuojaperiaatteita on noudatettava aina, kun käsitellään henkilötietoja.
- Tietosuojasetuksen tarkoituksena on suojella ihmisten oikeutta henkilötietojensa suojaan ja sitä kautta varmistaa kaikille ihmisille kuuluvien perusoikeuksien toteutuminen.
- Käydään seuraavaksi läpi sääntelyn keskeisiä periaatteita, eli rooleja ja vastuita, tietosuojaperiaatteita, ja rekisteröityjen oikeuksia.

Sääntely: Roolit ja vastuut



- **Rekisterinpitäjä** on ihminen tai organisaatio, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjä voi olla esimerkiksi työntekijöistään ja asiakkaistaan rekistereitä ylläpitävä organisaatio.
- Rekisterinpitäjän tulee dokumentoida tietosuojakäytännöt ja -prosessit, sekä pystyä osoittamaan, että se noudattaa tietosuojalainsäädäntöä.
- **Henkilötietojen käsittelijä** on ihminen tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi olla esimerkiksi toisen yrityksen palkanlaskentaa hoitava yritys. Myös henkilötietojen käsittelijän tulee dokumentoida omat tietosuojakäytäntönsä ja -prosessinsa.
- **Työntekijänä** sinun tulee noudattaa omassa organisaatiossasi voimassa olevia tietosuojakäytäntöjä.

Tilitoimiston tulee sopia henkilötietojen käsittelystä asiakkaiden kanssa kirjallisesti EU:n tietosuoja-asetuksen mukaan tilanteissa, joissa asiakkaiden rekisterien henkilötietoja käsitellään. Lisäksi tilitoimiston tulee dokumentoida prosesseissaan henkilötietojen suoja.

– Taloushallintoliitto, Henkilötietojen käsittelijän opas

Sääntely: Tietosuojaperiaatteet



Periaate	Mitä periaatteella tarkoitetaan
Lainmukaisuus, asianmukaisuus ja läpinäkyvyys	Henkilötietoja on käsiteltävä lainmukaisesti, kohtuullisesti suhteessa käsittelyn tarkoitukseen ja läpinäkyvästi suhteessa rekisteröityihin.
Käyttötarkoituksidonnaisuus	Henkilötietoja kerätään ja käytetään vain ennalta määriteltyihin, laillisiin tarkoituksiin, eikä niitä käsitellä alkuperäisen käyttötarkoituksen kanssa yhteensopimattomalla tavalla.
Tietojen minimointi	Henkilötietoja saa kerätä ja käsitellä vain siinä laajuudessa kuin on tarpeellista käsittelyn tarkoituksen kannalta. Henkilötietoja saa käsitellä vain silloin, kun se on tarpeellista käsittelyn tarkoituksen kannalta. Henkilötietojen säilytysaika on pidettävä mahdollisimman lyhyenä.
Tietojen täsmällisyys	Henkilötiedot pidetään täsmällisinä ja ajan tasalla, ja epätarkat tai virheelliset tiedot oikaistaan tai poistetaan viipymättä.
Säilytyksen rajoittaminen	Henkilötietoja säilytetään vain niin kauan kuin on tarpeen niiden käsittelyn tarkoitusten ja lakivelvoitteiden toteuttamiseksi. Esimerkiksi kirjanpitoa- ja arkistolaista tai toimialakohtaisista laeista voi aiheutua vaatimuksia arkistointiajajolle.
Luottamuksellisuus ja turvallisuus	Henkilötietoja käsitellään siten, että niiden asianmukainen turvallisuus varmistetaan, mukaan lukien suojaaminen luvattomalta tai laittomalta käsittelyltä ja vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

Sääntely: Rekisteröidyn oikeudet

Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus

- saada tietoa henkilötietojensa käsittelystä
- saada tutustua tietoihin
- oikaista tietoja
- poistaa tiedot ja tulla unohdetuksi
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- vastustaa tietojen käsittelyä ja
- olla joutumatta automaattisen päätöksenteon kohteeksi.

Rekisteröity ei kuitenkaan voi käyttää kaikkia oikeuksiaan kaikissa tilanteissa. Esimerkiksi silloin, kun henkilötietojen käsittelyn perusteena on palkanmaksu henkilölle ja palkanmaksutietojen välittäminen vero- ja muille viranomaisille, rekisteröity ei voi vastustaa tietojen käsittelyä.

Tilitoimiston tulee sopia rekisteröityjen oikeuksiin sovellettavista käytännöistä asiakasyritystensä kanssa. Tyypillistä on, että kun henkilötietojen käsittelijä on tilitoimisto, pyynnöt ohjataan aina rekisterinpitäjälle eli tilitoimiston asiakasyritykselle.

Tietosuojan tärkeys ja merkitys taloushallintoalan työtehtävissä

Lakisääteisistä velvoitteista huolehtiminen:

Noudattamalla tietosuojalainsäädäntöä organisaatiot välttävät mahdolliset sakot ja oikeudelliset seuraamukset.

Luotettava toiminta: Hyvä tietosuoja lisää asiakkaiden ja työntekijöiden luottamusta organisaatioon. He voivat luottaa siihen, että heidän tietonsa ovat turvassa ja että niitä käsitellään vastuullisesti.

Riskien hallinta: Tietosuojakäytännöt auttavat vähentämään tietovuotojen ja väärinkäytösten riskiä, mikä suojaa organisaation mainetta ja taloudellista vakautta, sekä **ennen kaikkea rekisteröityjä** henkilötietojen väärinkäyttöihin liittyviltä riskeiltä.

Työssä, jossa käsitellään henkilötietoja, on vastuu tietosuojan noudattamisesta. Henkilötietojen käsittelyssä on tärkeää varmistaa, että tiedot ovat aina suojattuja ja että niitä käsitellään lainmukaisesti.

Me taloushallintoalan työntekijät käsittelemme tuhansien henkilöiden henkilötietoja päivittäin. Se, miten me huolehdimme henkilötietojen tietosuojasta näissä tärkeissä tehtävissä, vaikuttaa lukuisten henkilöiden elämään.

Henkilötietojen käsittelyn riskejä



- Monissa työtehtävissä henkilötietojen käsittely on välttämätöntä.
- Henkilötietoja on käsiteltävä sellaisella tavalla, ettei se vaaranna kenenkään oikeutta turvalliseen elämään, kotiin, kunniaan, kotirauhaan, elinkeinon harjoittamiseen ja omaisuuden suojaan, aseta ihmisiä eriarvoiseen asemaan tai heikennä esimerkiksi rikosoikeudellista asemaa tai työoloja.
- Henkilötietojen käsittelyyn liittyviltä riskeiltä suojaudutaan parhaiten noudattamalla tietosuoja-asetuksen periaatteita ja toteuttamalla organisaatiossa riittävät toimenpiteet, joilla henkilötietoja suojataan.
- Käydään seuraavaksi läpi, minkälaisia riskejä voi seurata, mikäli henkilötietoja ei suojata riittävästi tai suojaukset pettävät.

Henkilötietojen käsittelyn riskejä



Tietovuodot ja tietomurrot	Luvaton käyttö	Tietojen katoaminen
Henkilötietojen vuotaminen esimerkiksi tietomurron seurauksena voi johtaa väärinkäytöksiin ja identiteettivarkauksiin. Vuodon seurauksena voi olla yksilöihin kohdistuvia riskejä, esimerkiksi heidän henkilötietojensa väärinkäyttöä tai luvattonta julkaisua.	Puutteelliset pääsynhallintakäytännöt voivat antaa luvattomille henkilöille pääsyn arkaluonteisiin tietoihin, mikä voi johtaa tietojen väärinkäyttöön.	Henkilötietojen vahingossa tapahtuva poistaminen tai tuhoutuminen, esimerkiksi IT-häiriötilanteessa, jonka seurauksena henkilötietoja ei pystytäkään käsittelemään silloin kun pitäisi, esimerkiksi palkanmaksun yhteydessä.
Virheellinen tieto	Oikeudelliset seuraukset	Mainehaitat
Vanhentuneet tai virheelliset henkilötiedot voivat johtaa virheellisiin päätöksiin.	Organisaatioon voi kohdistua seuraamusmaksuja tai korvausvaatimuksia tietosuojalainsäädännön tai sopimusten rikkomisesta. Vuonna 2023 korkein tietosuojavaltuutetun Suomessa määräämä seuraamusmaksu oli 440 000 euroa.	Tietosuojaan liittyvät virheet saavat helposti julkisuutta, mikä vaikuttaa yrityksen maineeseen. Seurauksena voi olla luottamuksen menetys pitkäksi aikaa.

Tässä videossa olet oppinut



Huoltovarmuuskeskus

- Tässä osiossa kävimme läpi tietosuoja-asioita. Keskustelimme tietosuojaperiaatteista ja niiden noudattamisesta taloushallinnossa.
- Lisäksi pohdimme, minkälaisia riskejä henkilötietojen käsittelyyn liittyy.



23.9.2024 ©Taloushallintoliitto



Huoltovarmuuskeskus

Yrityksiin kohdistuvat huijaukset ja tietojenkalastelu

Taloushallinnon työntekijöiden tietoturva

Moduuli 1: Tietoturva ja tietosuoja taloushallintoalalla

2024

23.9.2024 ©Taloushallintoliitto

Yrityksiin kohdistuvat tietoturvahyökkäykset



- Tämän osion aiheena ovat yrityksiin kohdistuvat huijaukset ja tietojenkalastelu.
- Osiossa kerrotaan, minkälaisia tyypilliset tietoturvauhkut ovat ja minkälaisia huijausyrityksiä taloushallintoalaan kohdistuu. Videon tarkoitus ei ole pelotella, vaan antaa sinulle kyvykkyudet tunnistaa huijausyritykset ja riittävä tietotaito, jolla vältät ne.
- Tämä tietotaito on tarpeellista, sillä verkkorikolliset ovat taitavia ja huijaukset kehittyvät koko ajan. Vuonna 2023 suomalaisilta pankkitileiltä huijattiin 44 miljoonaa euroa. Huijaaminen ja hyökkäykset ovat rikollisille bisnestä, joten ne eivät ole vähenemään päin.

Yrityksiin kohdistuvat tietoturvahyökkäykset



Kaikenlaisiin yrityksiin, niiden koosta riippumatta, kohdistuu tietoturvahyökkäyksiä. Karkeasti ottaen hyökkäyksiä on kahdenlaisia: automatisoituja tietoturvahyökkäyksiä, joilla yritetään löytää helppoja kohteita, sekä kohdennettuja hyökkäyksiä.

Kohdennetuissa hyökkäyksissä rikollinen käyttää merkittävästi resursseja juuri tiettyyn kohteeseen, esimerkiksi tietyn yrityksen tietoihin tai varoihin päästäkseen.

Yrityksiin kohdistuvat tietoturvahyökkäykset



Hyökkääjät ovat erityisen kiinnostuneita kohteista, joiden avulla he voivat saada **taloudellista hyötyä** – esimerkiksi huijaamalla rahaa valelaskuilla tai tunkeutumalla talouden järjestelmiin, varastamalla yrityksestä rahanarvoisia henkilötietoja tai liike tietoja, tai kiristämällä yritykseltä rahaa lukitsemalla sen järjestelmät.

Lisäksi on olemassa **poliittisesti motivoituneita** hyökkääjiä, jotka kohdistavat hyökkäyksensä esimerkiksi yhteiskunnalle merkityksellisiin toimijoihin.

Yleisiä organisaatioiden tietoturva uhkia



Uhka	Kuvaus	Suojautumistoimia
Tietojenkalastelu	Hyökkääjät lähettävät viestejä, jotka näyttävät tulevan luotettavalta lähteeltä, mutta niiden tarkoitus on kalastella tunnuksia ja salasanoja.	Käyttäjän huolellisuus ja tietojenkalasteluviestien tunnistaminen, ajantasainen haittaohjelasuojaus päätelaitteissa, ajantasainen roskapostisuodatus sähköpostissa.
Haittaohjelmat	Hyökkääjät voivat kiristyshaittaohjelmalla lukita yrityksen tiedostot ja vaatia lunnaita niiden vapauttamiseksi, mikä voi pysäyttää liiketoiminnan ja aiheuttaa tappioita.	Ajantasainen haittaohjelasuojaus päätelaitteissa ja yleinen käyttäjän huolellisuus internetin käytössä.
Palvelunesto- hyökkäykset	Palvelunestohyökkäykset ylikuormittavat yrityksen verkkopalvelut, mikä voi estää niiden käytön.	Tietojärjestelmien ja tietoliikenneyhteyksien suunnittelu kuormitustilanteita kestäväksi.
Haavoittuvuuk- sien hyödyntäminen	Hyökkääjät voivat hyödyntää yrityksen tietojärjestelmissä olevia tunnettuja haavoittuvuuksia, jos niitä ei ole korjattu.	Tietojärjestelmien säännölliset päivitykset ja turvalliset asetukset.

Kohdennetut hyökkäykset ja räätälöity sisältö



Huoltovarmuuskeskus

- Nykyään monien tietoturvahyökkäysten ja huijausten sisältö on kohdennettu kohdeyritykseen sopivaksi.
- Taloushallintoalan yrityksiinkin – ja erityisesti niiden henkilöstöön – kohdistuu työn kontekstiin sopivia huijausyrityksiä. Tämän vuoksi huijausyritysten tunnistaminen ei aina ole helppoa.
- Kyberhyökkääjät hyödyntävät tehokkaasti uusia teknologioita, esimerkiksi tekoälyn mahdollisuuksia, ja kehittävät niillä tekniikoitaan. Tekoälyn myötä esimerkiksi kalasteluviesteissä käytetty kieli saattaa olla kieliopillisesti hyvää ja sisällöllisesti uskottavaa.
- Käydään seuraavaksi läpi tyypillisiä taloushallintoon liittyviä huijaustapoja.

Taloushallintoalan henkilöstöön kohdistuvat huijaukset ja hyökkäykset



Huoltovarmuuskeskus

Väärät laskut ja maksupyynnöt

Hyökkääjät voivat lähettää laskuja tai maksupyyntöjä, jotka näyttävät tulevan luotettavilta toimittajilta tai asiakkailta. Viestit saattavat sisältää väärennettyjä laskuja tai linkkejä, jotka ohjaavat petollisille maksusivustoille.

Suojautuminen: Huolelliset laskujen tarkastus- ja hyväksyntäprosessit varmistavat, että vääriä laskuja ei päädy maksuun. Erityisesti lomasijaisten tulee olla tarkkana kesäaikaan.

Sisäiset pyynnöt eli ”toimitusjohtajahuijaus”

Hyökkääjät voivat esittää olevansa yrityksen johtajia tai kollegoita ja lähettää sähköpostilla, tekstiviesteillä ja WhatsApp-viesteillä pyyntöjä rahansiirroista tai tilitietojen vahvistamisesta. Näissä viesteissä voidaan käyttää virallisia yrityksen logoja ja muotoilua tai jopa deepfake-tekniikoita, jotta ne näyttäisivät aidoilta.

Suojautuminen: Pyyntöissä tyypillistä on kiire, poikkeaminen normaaleista toimintatavoista ja pyyntö pitää asia luottamuksellisena esimerkiksi vedoten sisäpiiritietoon. Kun tunnistat nämä ”hälytysmerkit”, osaat varmistaa pyynnön aitouden esimerkiksi soittamalla henkilölle.

Taloushallintoalan henkilöstöön kohdistuvat huijaukset ja hyökkäykset



Huoltovarmuuskeskus

Muuttuneet maksutiedot

Hyökkääjät voivat lähettää toisen yrityksen nimissä viestejä, joissa ilmoitetaan yrityksen maksutietojen muuttumisesta, ja pyytää päivittämään maksutiedot uuteen, huijarille kuuluvaan tilinumeroon.

Suojautuminen: Taloushallinnon systemaattiset toimittajarekisteröinnin prosessit auttavat torjumaan tilanteita, jossa yritetään perustaa uusia osapuolia tai vaihtaa tilitietoja perusteetta.

Turvatilihuijaus

Turvatilihuijaus on "kaksoishuijaus", jossa henkilö lankeaa ensin pankkitunnusten kalasteluviestiin. Seuraavaksi rikollinen soittaa uhrille esittäen olevansa pankin työntekijä ja ilmoittaa, että tilillä olevat varat tulee siirtää nopeasti suojaan "turvatilille". Henkilöä pyydetään hyväksymään varojen siirto.

Suojautuminen: Pankista tai viranomaisilta tulevat odottamattomat puhelut, joissa pyydetään pankkitunnuksia, maksukorttitietoja tai hyväksymään transaktio, eivät ole aitoja eikä niitä tule uskoa.

23.9.2024 ©Taloushallintoliitto

Sisäpiiriuhkat



- Uhkat ja väärinkäytökset eivät aina tule organisaation ulkopuolelta, vaan tekijänä voi olla myös organisaation oma työntekijä. Tästä syystä riittävä valvonta kuuluu taloushallintoalan organisaatioiden toimintaan ja on osa huolellisuusvelvoitetta.
- Työntekijöiden tekemiä kavalluksia voidaan torjua varmistamalla, että organisaatiossa ei ole käytössä niin sanottuja vaarallisia työyhdistelmiä. Vaarallinen työyhdistelmä tarkoittaa sellaista työtehtävien yhdistelmää, joka mahdollistaa väärinkäytöksen – esimerkiksi niin että sama henkilö voi ensin hyväksyä laskun ja sitten maksaa sen.
- Jos vaarallisia työyhdistelmiä ei voida täysin välttää (esimerkiksi yrityksen pienen henkilöstömäärän vuoksi), tulee yrityksen käyttää muita sisäisen valvonnan keinoja väärinkäytösten estämiseen ja havaitsemiseen. Näitä keinoja ovat esimerkiksi auditoinnit, tarkastukset ja muu sisäinen valvonta.

Yrityksiin kohdistuvat tietoturvahyökkäykset



Huijausten ja kavallusten seuraukset voivat olla vakavia ja vaikuttaa yrityksen taloudelliseen tilanteeseen, maineeseen ja toimintaan.

Meidän kaikkien on oltava erityisen valppaina ja varmistettava, että kaikki maksupyyntöihin, tilitietoihin ja henkilökohtaisiin tietoihin liittyvät pyynnöt ovat aitoja ennen niiden käsitlemistä.

Tässä videossa olet oppinut

- Tässä videossa kävimme läpi yrityksiin kohdistuvien huijausten ja tietojenkalastelun keinoja.
- Nyt osaat tunnistaa tyypilliset tietoturvauhkat ja taloushallintoalaan kohdistuvat huijausyritykset.



Moduuli 2: Tietoturvallinen käyttö

23.9.2024 ©Taloushallintoliitto



**talous
hallinto
liitto**



Huoltovarmuuskeskus

Päätelaitteiden turvallinen käyttö

Taloushallinnon työntekijöiden tietoturva

Moduuli 2: Tietoturvallinen käyttö

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Päätelaitteiden turvallinen käyttö

- Tämän videon aiheena on päätelaitteiden turvallinen käyttö.
- Käymme läpi päätelaitteiden, kuten kannettavien tietokoneiden ja älypuhelimien, turvallisuutta ylläpitäviä toimintatapoja.
- Päätelaitteiden turvallisuudesta huolehtiminen vähentää riskiä siihen, että haittaohjelmat ja muut tietoturvaohkat pääsevät laitteille ja vaarantavat tietojen eheyttä ja luottamuksellisuutta.

Päätelaitteiden turvallisuus



Päätelaitteiden eli tietokoneiden, tablettien ja älypuhelimien turvallisuus on olennainen osa yrityksen tietoturvaa. Päätelaitteet ovat niitä työkaluja, joilla teemme päivittäiset työtehtävät. Ne sisältävät tärkeitä tietoja ja tarjoavat pääsyn yrityksen sisäisiin järjestelmiin ja resursseihin. Tämä tekee niistä houkuttelevia kohteita rikollisille.

Työasemien turvallinen käyttö

Organisaatiollasi on todennäköisesti olemassa tekniset suojauskeinot, esimerkiksi tietoturvaohjelmistot, joilla työasemaa suojataan. Näiden lisäksi suojaat työasemaasi ja sitä kautta työasemallasi käsiteltäviä tietoja, kun noudatat näitä käytäntöjä.



Käytä työasemaa vain työasioiden hoitoon	Työasema pysyy paremmin turvassa, kun sillä käytetään vain työnteossa tarvittavia ohjelmistoja ja vieraillaan vain työn kannalta välttämättömillä sivustoilla.
Noudata työnantajan antamia ohjeita	Yrityksissä on erilaisia käytäntöjä siihen, miten työasemista huolehditaan. Tutustu oman työnantajasi ohjeisiin ja noudata niitä.
Valitse tiedostosijainnit käyttötarpeen mukaan	Tallenna tiedostot työnantajasi ohjeistuksen mukaisiin sijainteihin, jolloin niitä suojataan riittävästi esim. luvattomalta pääsylvä. Älä jaa pääsyä tarpeettomasti.
Pidä ohjelmistot ajan tasalla	Ohjelmistoissa havaittuja tietoturva-aukkoja korjataan ohjelmistoihin julkaistavilla päivityksillä. Asenna päivitykset aina työasemaasi viipymättä.
Huomioi työaseman hälytykset	Jos työasemasi tai jokin sovellus hälyttää ja ilmoittaa ongelmasta, lue hälytyksen teksti ja pyydä tarvittaessa neuvoa.
Rajoita pääsyä työasemaan	Älä anna muiden käyttää työasemaasi. Lukitse näyttösi, kun jätät työaseman ilman valvontaa. Viikonlopun ja loman ajaksi työasema on hyvä sammuttaa.

Älypuhelinien turvallisuus



Älypuhelimet ovat yhä yleisemmin työvälineitä, joilla voi päästä käsiksi muun muassa yrityksen sähköpostiin ja luottamuksellista tietoa sisältäviin tiedostoihin.

Jos älypuhelimet eivät ole asianmukaisesti suojattuja, ne voivat altistua monenlaisille uhkille, kuten haittaohjelmille, tietomurroille ja fyysisille varkauksille.

Älypuhelinten turvallinen käyttö työtehtävissä 1/2

Suojaa älypuhelimasi noudattamalla seuraavia hyviä käytäntöjä:

- Päivitä älypuhelimien käyttöjärjestelmä ja sovellukset säännöllisesti. Päivitykset sisältävät usein tietoturvaparannuksia ja korjauksia haavoittuvuuksiin, jotka voivat muuten altistaa puhelimen hyökkäyksille.
- Suojaa älypuhelimesi vahvalla koodilla tai biometrisillä tunnistella, kuten sormenjäljellä tai kasvojentunnistuksella. Tämä estää luvattoman pääsyn puhelimeen, jos se katoaa tai varastetaan.
- Tutustu puhelimesi muihin asetuksiin, jotka liittyvät tietosuojaan ja puhelimen suojaamiseen. Puhelimessa voi esimerkiksi olla toimintoja, jotka auttavat hukkuneen laitteen löytämisessä tai nollaamisessa. Käytä näitä toimintoja vahvistaaksesi turvallisuuttasi ja yksityisyyttäsi.

Älypuhelinten turvallinen käyttö työtehtävissä 2/2

- Käytä työtehtävien suorittamiseen vain työnantajasi hyväksymiä sovelluksia ja ilmoita kadonneesta työpuhelimesta heti työnantajalle.
- Jos käytät samaa älypuhelimia töissä ja vapaa-ajalla, erota työ ja vapaa-aika. Käytä työasioiden hoitamiseen erillisiä sovelluksia ja tilejä, kuten erillistä sähköpostisovellusta työviesteille.
- Suosi mobiilidataa ja käytä vain tuntemiasi langattomia verkkoja (Wi-Fi).
- Lataa sovelluksia vain luotettavista lähteistä, kuten virallisista sovelluskaupoista. Tarkista sovellusten luvat puhelimen asetuksista ja varmista, että et salli niille tarpeettomia pääsyoikeuksia tietoihisi (esimerkiksi kameran tai mikrofonin käyttöoikeutta).
- Varo tekstiviesteillä tapahtuvia huijauksia. Älä koskaan klikkaa tekstiviestin kautta tullutta linkkiä, jossa pyydetään siirtymään esimerkiksi verkkopankkiin. Esimerkiksi Verohallinnon, Postin ja pankkien nimissä tapahtuu paljon tekstiviesteillä välitettyjä huijauksia.

Sovellusten ja pilvipalveluiden turvallinen käyttö



Sovellusten ja pilvipalveluiden turvallisen käytön A ja O on käyttää ainoastaan luotettavia palveluntarjoajia. Yleensä ottaen työnantajasi määrittelee, mitä sovelluksia tai pilvipalveluita työn suorittamisessa käytetään, tai tietyissä tapauksissa asiakkaasi voi pyytää sinua käyttämään tiettyä sovellusta, esimerkiksi heidän toiminnanohjausjärjestelmäänsä. Näiden palveluiden käyttäjänä varmista käytön turvallisuus seuraavasti:

- Älä itse asenna työasemalle ohjelmistoja, **jollet** ole saanut siihen lupaa työnantajaltasi.
- Suojaa kaikki tilisi vahvoilla ja monimutkaisilla salasanoilla ja päivitä sovellus aina heti, kun päivityksiä on saatavilla.
- Ota käyttöön monivaiheinen tunnistautuminen. Joissakin sovelluksissa monivaiheinen tunnistautuminen ei ole tarjolla automaattisesti, vaan se otetaan käyttöön sovelluksen asetuksista.
- Käy läpi sovelluksen asetukset, sillä usein niissä on tietoturvaan liittyviä asetuksia. Muista myös pitää sovelluksissa yhteystietosi ajan tasalla, sillä niitä voidaan tarvita, jos unohdat salasanan.

Monivaiheisesta tunnistautumisesta ja vahvoista salasanoista opit lisää myöhemmässä moduulissa.

Tässä videossa olet oppinut



- Tässä videossa kävimme läpi päätelaitteiden, kuten kannettavien tietokoneiden ja älypuhelimien, turvallisuuteen liittyviä parhaita käytäntöjä.
- Tiedät nyt, miten voit parhaiten huolehtia näiden laitteiden turvallisuudesta.





Huoltovarmuuskeskus

Sähköpostin turvallinen käyttö

Taloushallinnon työntekijöiden tietoturva

Moduuli 2: Tietoturvallinen käyttö

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Sähköpostin turvallinen käyttö



Huoltovarmuuskeskus

- Tässä videossa fokuksessa on sähköposti ja sen turvallinen käyttö.
- Videossa kerrotaan sähköpostiin liittyvistä uhkista ja miten niiltä voi välttyä. Käymme läpi myös kalasteluviestien parhaat tunnistamisvinkit.
- Sähköposti on yksi käytetyimmistä viestintävälineistä, mutta se on myös merkittävä tietoturvariskien lähde.
- Sähköposteja on helppo epähuomiossa lähettää väärälle vastaanottajalle ja erityisesti matkapuhelimen pienellä näytöllä virheitä sattuu helposti. Lisäksi tietojenkalasteluviestit, haittaohjelmat ja muut sähköpostin kautta leviävät uhkat ovat merkittäviä tietoturvariskejä.

Sähköpostin turvallinen käyttö



Sähköpostin käyttäjänä sinun tarkkaavaisuutesi ja huolellisuutesi on avaintekijä, jolla voidaan ehkäistä sähköpostiin liittyviä tietoturvauhkia.

Keskeiset sähköpostiin liittyvät uhat

Sähköpostien lähettäminen

Tietojen lähettäminen väärälle vastaanottajalle

Sähköpostilla saattaa epähuomiossa lähettää luottamuksellisia tietoja tai jopa kokonaisia tiedostoja väärälle vastaanottajalle. Sähköpostiohjelmat usein tarjoavat käyttäjälle vastaanottajien nimiä nimen ensimmäisten kirjainten perusteella. Näistä on vahingossa helppo valita vastaanottajaksi väärä henkilö.

Väärän liitteen lähettäminen

Erityisesti liitetiedostoja lähetettäessä voi helposti käydä niin, että valitsee väärän tiedoston.

Sähköpostien vastaanottaminen

Tietojenkalastelu

Huijausviestit, jotka houkuttelevat lähettämään tietoja, kuten tunnuksia ja salasanoja.

Haittaohjelmia sisältävät viestit

Sähköpostiliitteet ja linkit voivat sisältää haittaohjelmia, joiden tavoitteena on varastaa tai vahingoittaa tietoja.

Valelähettäjän käyttö

Sähköpostin lähettäjä voi väärentää sähköpostin lähettäjä tiedot, jolloin viesti näyttää tulevan luotettavalta taholta.

Kalasteluviestin tunnistaminen – parhaat tunnistamisvinkit

Kalasteluviestit ovat yhä kehittyneempiä ja voivat näyttää hyvin aidoilta, joten niiden tunnistaminen vaatii tarkkaavaisuutta. Seuraavien vinkkien avulla voit tunnistaa huijauksen.



Huoltovarmuuskeskus

Jotain outoa

Kalasteluviestit voivat sisältää epätavallisia tai yllättäviä pyyntöjä ja näyttää olevan peräisin tutulta tai tunnetulta taholta. Mieti, onko pyyntö järkevä ja tavanomainen kyseiseltä lähettäjältä. Jos olet epävarma viestin aitoudesta, ota yhteyttä lähettäjään esimerkiksi puhelimitse, äläkä vastaa viestiin suoraan.

Kiireen tuntu

Kalasteluviestit pyrkivät usein luomaan kiireen tuntua ja painostamaan vastaanottajaa toimimaan nopeasti – tämä heikentää harkintakykyämme. Jos viesti vaatii välitöntä toimintaa, kuten tilin vahvistamista salasanalla, ole erityisen varovainen ja varmista viestin aitous ennen kuin reagoit.

Pienet virheet

Tarkista aina, että lähettäjän osoite vastaa lähettäjäorganisaation virallista osoitetta. Pienet kirjoitusvirheet tai ylimääräiset merkit osoitteessa tarkoittavat, että viesti on kalastelua.

Odottamattomat viestit ja liitteet

Älä avaa liitteitä tai klikkaa linkkejä, ellet ole varma lähettäjän luotettavuudesta. Joskus kalasteluviestien liitteet nimetään tavalla, joka vetoaa uteliaisuuteemme ja suorastaan kutsuu lukemaan liitteen sisällön.

Turvalliset käytännöt sähköpostin käyttöön



Huoltovarmuuskeskus

- Käytä työsähköpostitilissä monivaiheista tunnistautumista. Jos sellaista ei ole saatavilla, salasanan tulee olla pitkä ja sellainen, joka ei ole käytössä missään muussa palvelussa.
- Ole huolellinen lähettäessäsi sähköpostia:
 - Tarkista aina huolellisesti, että olet lähettämässä viestiä oikealle henkilölle ja että lähettämäsi liitteet ovat oikeita. Huomioi, että henkilötietojen lähettäminen väärälle vastaanottajalle saattaa aiheuttaa tietoturvaloukkauksen.
 - Sähköpostin asetuksissa voi valita sähköpostin lähtemään vastaanottajalle viiveellä – pienellä viiveellä saattaa huomata tekemänsä virheen, ja sähköpostin lähetyksen voi vielä perua.
 - Älä jaa arkaluontoisia tai luottamuksellisia tietoja sähköpostitse, ellei se ole ehdottoman välttämätöntä. Varmista aina, että vastaanottaja on luotettava ja että tiedot on suojattu salauksella. Liitetiedostojen sijaan on parempi käyttää yrityksen käytössä olevia tiedonjakopalveluita.
- Jos saat epäilyttävän sähköpostin, älä avaa sitä, vaan ilmoita siitä heti organisaatiosi käytäntöjen mukaan esimerkiksi esihenkilölle tai IT-tuelle.

Sähköpostitse saapuvien linkkien ja liitteiden tarkistaminen



Linkkien tarkistaminen

- Ennen kuin klikkaat linkkiä, vie hiiren osoitin sen päälle tarkistaaksesi osoitteen. Tämä näkyy yleensä selaimen alareunassa. Varmista, että osoite vastaa odotettua ja että se näyttää luotettavalta. Lyhennetyissä linkeissä tämä ei kuitenkaan toimi, joten klikkaa niitä vain, jos todella luotat linkin lähettäjään.
- Ole tarkkana, ettei osoitteessa ole pieniä kirjoitusvirheitä tai ylimääräisiä merkkejä, jotka voivat viitata huijaussivustoon (esim. "postii.fi" vs. "posti.fi").

Liitteiden tarkistaminen

- Älä avaa epäilyttäviä liitteitä. Jos et odottanut liitettä tai se vaikuttaa epäilyttävältä, älä avaa sitä.
- Jos saat odottamattoman liitteen tutulta henkilöltä, varmista ennen avaamista viestin aitous lähettäjältä esimerkiksi soittamalla hänelle.
- Tiedoston voi tarkistaa haittaohjelmien varalta maksutta osoitteessa **www.virustotal.com**. Koska kyse on verkkopalvelusta, tarkista, että työnantajasi käytännöt sallivat palvelun käytön.

23.9.2024 ©Taloushallinto Liitto

Tässä videossa olet oppinut



- Tässä videossa kävimme läpi sähköpostiin liittyviä turvallisuusasioita.
- Tutustuimme sähköpostiin liittyviin uhkiin ja opimme keinot välttää näiltä uhkilta noudattamalla turvallisia sähköpostikäytäntöjä.



23.9.2024 ©Taloushallinto Liitto



Huoltovarmuuskeskus

Internetin turvallinen käyttö

Taloushallinnon työntekijöiden tietoturva

Moduuli 2: Tietoturvallinen käyttö

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Internetin turvallinen käyttö



Huoltovarmuuskeskus

- Tämän videon aiheena on internetin turvallinen käyttö. Käymme läpi yleisimpiä verkkouhkia ja turvallisen selailun ja tiedon jakamisen keskeiset käytännöt.
- Internet tarjoaa valtavasti tietoa, mutta se on myös alusta täynnä erilaisia uhkia. Erilaiset huijaussivustot houkuttelevat käyttäjiä luovuttamaan esimerkiksi luottokorttitietonsa tai lataamaan haittaohjelman. Lisäksi internetissä liikkuu paljon valetietoa. Internet on kuitenkin yksi työssämme käytettävistä välineistä, joten on oleellista, että osaamme käyttää sitä turvallisesti ja välttää vaaran paikat.
- Tutustutaan seuraavaksi joihinkin yleisimpiin verkkouhkiin.

Yleisiä verkkouhkia

23.9.2024 ©Taloushallinto

Yleisiä verkkouhkia: Huijaussivustot



- Huijaussivustot voivat näyttää aidoilta verkkosivustoilta, kuten pankkien, verkkokauppojen tai sosiaalisen median sivustoilta.
- Niiden ulkoasu ja verkko-osoite voivat olla lähes identtisiä alkuperäisen sivuston kanssa, mutta ne on luotu keräämään henkilökohtaisia tietoja, kuten käyttäjätunnuksia, salasanoja ja maksutietoja.
- Tyypillisiä esimerkkejä Suomessa ovat pankkien ja viranomaisten sivustoja jäljittelevät huijaussivustot.

Näin tunnistat ja vältät huijaussivustot

Älä siirry esimerkiksi pankin tai viranomaisten sivustolle hakukoneen kautta

Hakukoneiden tulokset sisältävät linkkejä huijaussivustoille. Kirjoita mieluummin osoite suoraan selaimeen.

Huijaussivustojen osoitteet voivat sisältää pieniä kirjoitusvirheitä tai ylimääräisiä merkkejä. Tarkista aina verkko-osoite, ja varmista, että se vastaa tuntemaasi sivustoa.

Usein käytetyt sivustot kannattaa tallentaa selaimen suosikkeihin, jolloin oikeat osoitteet ovat aina helposti saatavilla.

Usko selainta

Selaimet sisältävät toimintoja valesivustojen tunnistamiseen. Jos selaimesi varoittaa haitallisesta osoitteesta tai sivustosta, usko sitä.

Käytä tietoturvasovelluksia

Päätelaitteiden tietoturvaohjelmat voivat tunnistaa ja estää pääsyn tunnetuille huijaussivustoille. Pidä tietoturvaohjelmistosi ajan tasalla ja käytä sen tarjoamia selausturvaominaisuuksia.

Yleisiä verkkouhkia: Haittaohjelmat

- Haittaohjelmat ovat ohjelmistoja, jotka on suunniteltu vahingoittamaan tietokonejärjestelmiä, varastamaan tietoja tai aiheuttamaan häiriöitä.
- Internetin käyttämisen yhteydessä laitteellesi voi tulla haittaohjelma, mikäli lataat tiedoston epäluotettavasta lähteestä.
- Parhaiten vältät haittaohjelmat, kun
 - käytät ajantasaista virustorjuntaohjelmaa ja pidät sen päivitetynä
 - et lataa etkä asenna ohjelmia epäluotettavista lähteistä
 - vieraillet vain luotettavilla verkkosivuilla
 - pidät käyttöjärjestelmän ja muut ohjelmistot ajan tasalla.

Yleisiä verkkouhkia: väärä tieto

Internetissä kuka vain voi julkaista tietoa, mikä johtaa siihen, että kaikki internetissä oleva tieto ei perustu faktoihin tai ole luotettavaa.

Misinformaatio on termi, jota käytetään väärästä tai harhaanjohtavasta tiedosta, joka leviää ilman pahantahtoista aikomusta. Internetissä jaetaan esimerkiksi väärin ymmärrettyjä tietoja tai virheellisiä faktoja "totena". Tällaiset tiedot saattavat erityisesti sosiaalisessa mediassa lähteä leviämään todella nopeasti.

Disinformaatio on termi, joka kuvaa tarkoituksella luotua ja levitettyä väärää tietoa, jolla levittäjä pyrkii edistämään jotakin tavoitettaan. Internetissä jaetaan esimerkiksi politiikkaan tai kriiseihin liittyviä vääriä väitteitä, joilla halutaan vaikuttaa esimerkiksi vaalituloksiin tai aiheuttaa paniikkia.

Jos käytät internetistä peräisin olevia tietoja työtehtävissä, muista aina tarkistaa tietojen lähteet ja varmistaa, että ne ovat luotettavia.

Kun törmäät internetissä tunteita herättäviin väitteisiin tai uutisiin, vedä syvään henkeä ja muista, että kaikki internetissä ei välttämättä ole totta. Tarkista tiedot luotettavista lähteistä ennen niiden uskomista tai jakamista.



Turvallinen selailu ja tiedon jakaminen

Turvallinen selailu

Aiemmin käsitelimme merkkejä, joista voit tunnistaa huijaussivuston. Pääsääntöisesti internetissä liikkeessa kannattaa pysytellä luotettavilla sivustoilla. Käydään kuitenkin vielä läpi muutamia muita vinkkejä turvalliseen selailuun.



- Tarkista internet-selaimesi tietoturvaan ja tietosuojaan liittyvät asetukset, sillä ne tarjoavat yleensä vahvemman suojauksen vaihtoehtoja. Voit esimerkiksi poistaa automaattiset tiedostolataukset käytöstä, jolloin selain pyytää sinulta vahvistuksen ennen lataamista.
- Muita hyödyllisiä asetuksia ovat selaimen automaattiset tietoturvapäivitykset sekä ponnahdusikkunoiden esto. Ponnahdusikkunat voivat sisältää haittaohjelmia tai huijauksia.
- Käytä eri selaimia eri tarkoituksiin: esimerkiksi oman yrityksen intranetiä ja ohjelmistoja yhdellä selaimella ja asiakkaan ohjelmistoja toisella selaimella.
- Varmista, että verkkosivusto käyttää suojattua HTTPS-yhteyttä, mikä näkyy lukkokuva-akkeena osoiterivin alussa. HTTPS tarkoittaa, että yhteys on salattu ja turvallinen, mutta ota huomioon että se ei yksinään takaa sivuston aitoutta.
- Internetissä tarvitaan myös tietynlaista medialukutaitoa, sillä siellä julkaistu tieto sisältää runsaasti mielipiteitä ja muita tietoja, jotka eivät perustu faktoihin.

Tietojen jakaminen internetissä



- Sanotaan, että sitä mitä kerran laittaa internetiin, ei koskaan saa sieltä pois. Tämä on hyvä pitää mielessä, ennen kuin tietoja jakaa internetissä.
- Koska internet on julkinen paikka ja siellä jaetut tiedot saattavat kulkeutua hyvinkin laajalle, tietojen jakamiseen internetissä liittyy riskejä.
- Eri sosiaalisen median kanaviin ja sivustoille jaettuja tietoja voidaan yhdistellä ja eri tietoja voidaan käyttää myös rikollisiin tarkoituksiin: esimerkiksi organisaatorakenteisiin ja työtehtäviin liittyviä tietoja käytetään uskottavien tietojenkalasteluviestien rakentamiseen.
- Pahantahtoiset toimijat voivat myös hyödyntää työpaikalta ja kulkukorteista jaettuja valokuvia tunnistamaan työpaikan turvallisuusjärjestelyjä. Tällaisten kuvien jakamista ei siis voi suositella.

Tässä videossa olet oppinut



Huoltovarmuuskeskus

- Tässä videossa kävimme läpi internetin turvallista käyttöä.
- Videossa kerrottiin yleisimmistä verkkouhkista ja käytiin läpi turvallisen selailun ja tiedon jakamisen keskeisiä käytäntöjä.



23.9.2024 ©Taloushallintoliitto



Huoltovarmuuskeskus

Tietojen turvallinen hallinta ja siirtäminen

Taloushallinnon työntekijöiden tietoturva

Moduuli 2: Tietoturvallinen käyttö

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Tietojen turvallinen hallinta ja siirtäminen



- Tässä videossa kerrotaan tietojen hallinnan ja siirtämisen turvallisista käytännöistä, joiden avulla suojataan yritys- ja henkilötietoja.
- **Tietojen hallinnan** toimenpiteillä varmistetaan, että tiedot ovat suojattuja koko niiden elinkaaren ajan ja että vain valtuutetut henkilöt pääsevät niihin käsiksi.
- **Tietojen siirtäminen** turvallisella tavalla on tärkeää, jotta tiedot eivät joudu siepatuksi tai muutu matkalla.

Tietojen turvallinen hallinta



Työssäsi käsittelet paljon luottamuksellista tietoa ja todennäköisesti myös henkilötietoa. Näiden tietojen turvallisella hallinnalla varmistetaan, että tiedot ovat käytettävissä, kun niitä tarvitaan, niihin pääsevät vain valtuutetut henkilöt ja tiedot eivät katoa tai tuhoudu.

Tietojen turvallinen säilytys

- Käydään ensiksi läpi tietojen turvalliseen säilytykseen liittyviä asioita.
- Muistatko vielä kurssilla aiemmin käsitellyt tietosuojaperiaatteet? Kaksi niistä liittyy olennaisesti tietojen säilytykseen ja on hyvä pitää mielessä, jos käsittelet työssäsi henkilötietoja:
 - **Säilytyksen rajoittaminen** = Henkilötietoja säilytetään vain niin kauan kuin on tarpeen niiden käsittelytarkoitusten toteuttamiseksi.
 - **Luottamuksellisuus ja turvallisuus** = Henkilötietoja käsitellään siten, että niiden asianmukainen turvallisuus varmistetaan, mukaan lukien suojaaminen luvattomalta tai laittomalta käsittelyltä ja vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.
- Säilytä sähköisessä muodossa olevia tietoja organisaatiosi määrittelemissä säilytyspaikoissa: tietojärjestelmissä, ohjelmistoissa ja tiedostojainneissa. Tiedoista ei tule "varmuuden vuoksi" säilyttää ylimääräisiä kopioita esimerkiksi tietokoneen työpöydällä tai omassa sähköpostissa.
- Jos organisaatiossasi säilytetään vielä tietoja paperimuodossa, säilytä myös nämä tiedot niille määritellyissä säilytyspaikoissa, ei esimerkiksi pöytälaatikossa.

Tietojen turvallisen hallinnan käytäntöjä

Tietojen luokittelu

Organisaatiollasi voi olla käytössä tapa luokitella tietoja. Tiedon luokittelulla ohjataan esimerkiksi eri tietotyypeille tarvittavia suojaustoimenpiteitä. Yleensä ottaen arkaluonteiset tiedot, kuten henkilötiedot, taloudelliset tiedot ja yrityssalaisuudet, vaativat erityistä suojausta.

Pääsynhallinta

Pääsynhallinnan avulla hallitaan, kenellä on pääsy organisaation resursseihin, kuten tietojärjestelmiin, tietoihin ja fyysisiin tiloihin. Jokaisella tulee olla pääsy vain niihin tietoihin, joita tarvitsee työssään.

Salaus

Salaus on prosessi, jossa tieto muunnetaan muotoon, jota voivat lukea vain valtuutetut tahot. Salauksen avulla voidaan suojata arkaluonteisia tietoja luvattomalta käytöltä ja väärinkäytöltä.

Säilytysaikojen määrittely

Kaikkia tietoja ei tarvitse säilyttää ikuisesti, vaan organisaation tulee määritellä eri tyyppisille tiedoille säilytysajat, huomioiden niihin kohdistuvat vaatimukset (esim. kirjanpitolaki, tietosuojasetus). Jokaisen organisaation tulee luoda prosessit, joilla huolehditaan siitä, että tiedot poistetaan säilytysajan päätyttyä.

Tietojen turvallinen siirtäminen



Taloushallintoalan töissä siirrämme usein luottamuksellista tietoa palvelusta tai paikasta toiseen. Tietojen turvallisella siirtämisellä tietoja suojataan mahdollisilta väärinkäytöksiltä ja uhkilta, kuten tietomurroilta ja tietojen sieppaukselta.

Tietojen turvallisen siirtämisen käytäntöjä

Hyväksytyt ja luotettavat palvelut

Käytä työtehtäviesi suorittamiseen ainoastaan sellaisia tiedonsiirto- ja tiedonjakopalveluita, joiden käytön työnantajasi ja/tai asiakkaasi on hyväksynyt. Näitä voivat olla esimerkiksi viranomaisten viralliset palvelut ja työnantajasi/asiakkaasi käytössä olevat pilvipalvelut ja ohjelmistot (esim. palkanlaskentaohjelmistot).

Vältä tietojen siirtämistä sellaisten palveluiden kautta, jotka eivät ole työkäyttöön tarkoitettuja (esim. sosiaalisen median palvelut, viestisovellukset) tai internetistä löytyvät ilmaiset tiedostonsiirtopalvelut. Näiden turvallisuudesta ei ole mitään takuuta.

Pääsynhallinta

Kun käytät tiedonsiirto- tai -jakopalvelua, varmista, että vain tarkoittamasi vastaanottaja voi avata tiedot. Esimerkiksi, jos pääsy tiedostojakoon perustuu linkkiin, voiko linkin myöhemmin sulkea?

Salauskäytännöt

Tavallinen sähköposti ei ole turvallinen tapa siirtää luottamuksellisia tietoja ja tiedostoja. Noudata työnantajasi ohjeita sähköpostiviestin salauksesta.

Tässä videossa olet oppinut

- Tässä videossa kävimme läpi tietojen turvallisen hallinnan ja siirtämisen käytäntöjä.
- Tietojen käsittely huolellisesti ja turvallisissa palveluissa on todella tärkeää tietojen luottamuksellisuuden kannalta.
- Muista aina noudattaa työnantajasi ohjeita ja työnantajasi hyväksymiä palveluja, jotta tietojen hallinta ja siirtäminen tapahtuu turvallisesti.



Moduuli 3: Turvalliset tunnistautumismenetelmät



Huoltovarmuuskeskus

Käyttäjätunnusten ja salasanojen turvallinen käyttö

Taloushallinnon työntekijöiden tietoturva

Moduuli 3: Turvalliset tunnistautumismenetelmät

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Käyttäjätunnusten ja salasanojen turvallinen käyttö



Huoltovarmuuskeskus

- Tässä videossa puhutaan käyttäjätunnuksista ja salasanoista.
- Käyttäjätunnuksiin ja salasanoihin kohdistuu paljon tietojenkalasteluyrityksiä, koska ne haltuunsa saamalla voi saada pääsyn erilaisiin tileihin ja tietoihin.
- Sinulta käyttäjänä vaaditaan siis paljon valppautta, että käyttäjätunnuksesi ja salasanasasi eivät valu tietojenkalastelun kautta verkkorikollisille.

Käyttäjätunnusten ja salasanojen turvallinen käyttö



Huoltovarmuuskeskus



Salasanat ja muut todennusmenetelmät suojaavat tilejä ja tietoja luvattomalta käytöltä.

Heikkoihin salasanakäytäntöihin liittyy merkittävä väärinkäytösten riski. Heikkoja salasanakäytäntöjä ovat esimerkiksi saman salasanan käyttäminen monissa eri palveluissa, salasanan tallentaminen tiedostoon ja salasanan säilyttäminen paperilla muiden sivullisten saatavilla.

Vahvat salasanat



Huoltovarmuuskeskus

Vahvalla salasanalla on iso merkitys tietoturvan kannalta. Vahvojen salasanoiden luominen on melko yksinkertaista. Tee se näin.

Luo salasanalause

Vahva salasana on pitkä. Kyberturvallisuuskeskus suosittelee vähintään 15-merkkisiä salasanvoja. Sellaisen luominen ja muistaminen helpottuu, kun salasana on yksittäisen sanan sijaan salasanalause.

Vältä arvattavia tietoja

Vältä helposti arvattavia tietoja salasanassa. Sellaisia ovat vaikkapa salasanan vaihdon kuukausi ja vuosi, tai lemmikin tai läheisen nimi.

Pidä se salassa

Älä kirjoita salasanaa ylös tiedostoon tai paperille. Sen sijaan varmista, että voit salasanan unohtuessa tarvittaessa palauttaa tilin IT-yksikön avustuksella tai muutoin.

Salasanalauseen luominen



**Luo
salasanalause**

Jotain muistettavaa, mutta sellaista, joka ei sisällä henkilökohtaisia tietoja.

Salasanalauseen luominen



**Luo
salasanalause**

Taloushallinto-ON-päivittäinen-TYÖNI

Salasanalauseen luominen

**Luo
salasanalause**

Taloushallinto-ON-päivittäinen-TYÖNI

**Sisällytä numeroita
ja merkkejä**

Voit lisätä lauseeseen esimerkiksi numeroita ja erikoismerkkejä.

Salasanalauseen luominen

**Luo
salasanalause**

Taloushallinto-ON-päivittäinen-TYÖNI

**Sisällytä numeroita
ja merkkejä**

Taloushallinto1ON2päivittäinen3TYÖNI4!

**Molemmat esimerkit ovat pitkiä ja
erinomaisia salasanoja**

Pidä hyvää huolta salasanoista

Käytä jokaisessa palvelussa eri salasanaa

Tällä varmistat, että yhdestä palvelusta vuotanutta salasanaa ei voida käyttää muihin palveluihin kirjautumiseen.

Vaihda salasana, jos epäilet sen vaarantuneen

Jos epäilet syöttäneesi salasanan huijaussivustolle tai salasanan muuten vaarantuneen, vaihda salasana välittömästi.

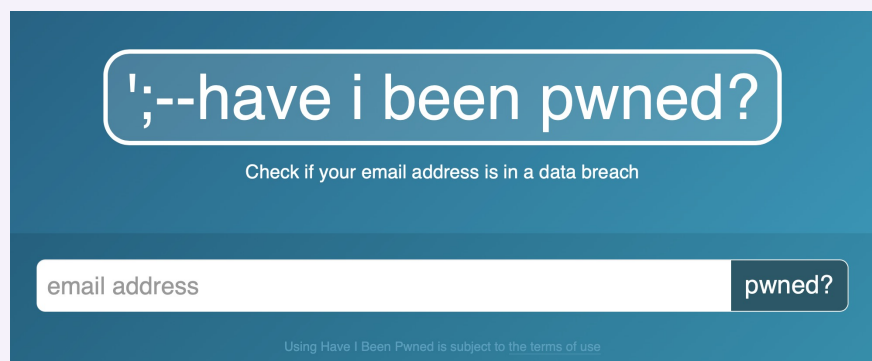
Käytä salasanojen hallintasovellusta

Salasanojen hallintaa ja muistamista voi helpottaa käyttämällä salasanojen hallintasovellusta, jos sellainen on käytössä omassa organisaatiossa. Salasanojen hallintasovelluksessa käyttäjän tarvitsee muistaa vain hallintasovelluksen salasana – muut salasanat ovat tallessa ja muistissa sen takana.

Onko salasanani joutunut väärin käsiin?

Voit tarkistaa osoitteessa <https://haveibeenpwned.com> onko salasanasi joutunut rikollisille. Sivuston tiedot perustuvat internetistä löytyneisiin tietovuotoihin.

Tämä palvelu on tunnetun tietoturva-ammattilaisen ylläpitämä. Muut vastaavat sivustot voivat olla huijauksia.



Käyttäjätunnusten jakamiseen liittyvät riskit

Käyttäjätunnukset ja niihin yhdistettävät salasanat ovat henkilökohtaisia. Käyttäjätunnuksella nimensä mukaisesti tunnistetaan *käyttäjä*, eli kuka tiettyä palvelua on käyttänyt. Kun palvelu on tietoturvaltaan laadukas, voidaan tunnuksesta palvelussa tehdyt toimet yhdistää kyseiseen käyttäjään. Näin esimerkiksi väärinkäyttötilanteissa voidaan selvittää, kuka jonkin toimenpiteen on tehnyt.

Käyttäjätunnusten jakaminen on riski sekä organisaation että yksilön näkökulmasta:

- Kun käyttäjät jakavat tunnusta, on vaikea jäljittää, kuka on suorittanut tietyn toimenpiteen. Tämä vaikeuttaa vastuun määrittämistä väärinkäytöksissä, kuten esimerkiksi kavallustilanteissa.
- Kun useat henkilöt jakavat tunnusta ja salasanaa, sen hallinta ja suojaus heikkenee. Pahimmillaan jaetun tunnuksen salasana on yrityksestä lähteneiden vanhojen työntekijöidenkin tiedossa, mikä lisää riskiä siihen, että järjestelmää käytetään väärin.

86 Tässä videossa olet oppinut

- Tässä videossa kävimme läpi salasanoja ja sitä, miten salasanalauseilla on helppoa tehdä pitkiä ja muistettavia salasanoja.
- Keskustelimme myös siitä, miksi käyttäjätunnusten tulee aina olla henkilökohtaisia.





Huoltovarmuuskeskus

Monivaiheinen tunnistautuminen

Taloushallinnon työntekijöiden tietoturva

Moduuli 3: Turvalliset tunnistautumismenetelmät

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Monivaiheinen tunnistautuminen



- Tässä videossa parannetaan tietoturvaa ottamalla käyttöön monivaiheinen tunnistautuminen.
- Opit jo aikaisemmin, kuinka tärkeää on huolehtia salasanoista ja tehdä niistä vahvoja, jotta käyttäjätunnustasi ei pääsisi käyttämään kukaan muu.
- Paras keino lisätä tunnistautumisen turvallisuutta on lisäksi ottaa käyttöön kaikissa mahdollisissa palveluissa monivaiheinen tunnistautuminen.

Monivaiheinen tunnistautuminen



Monivaiheinen tunnistautuminen tarkoittaa sitä, että kirjautumistilanteessa henkilöllisyytesi varmistetaan kahdella tai useammalla tunnistautumistavalla.

Monivaiheinen tunnistautuminen antaa ylimääräisen suojakerroksen, joka estää luvattoman pääsyn palveluun, vaikka yksi todennusmenetelmä, esimerkiksi salasana, olisi päätyntä jonkun ulkopuolisen haltuun.



**Miten monivaiheinen
tunnistautuminen toimii?**

Monivaiheisessa tunnistautumisessa pääsy palveluun vaatii useamman tavan tunnistaa käyttäjä, esimerkiksi:

Jotain mitä tiedät

Tiedossasi oleva tieto, esimerkiksi salasana

Jotain mitä sinulla on

Kirjautuminen hyväksytään esimerkiksi erillisellä sovelluksella

Jotain mitä olet

Tunnistautuminen tapahtuu esimerkiksi sormenjäljellä



Huoltovarmuuskeskus



23.9.2024 ©Taloushallintoliitto

Monivaiheisessa tunnistautumisessa pääsy palveluun vaatii useamman tavan tunnistaa käyttäjä, esimerkiksi:

Jotain mitä tiedät

Tiedossasi oleva tieto, esimerkiksi salasana

Jotain mitä sinulla on

Kirjautuminen hyväksytään esimerkiksi erillisellä sovelluksella

Jotain mitä olet

Tunnistautuminen tapahtuu esimerkiksi sormenjäljellä



Huoltovarmuuskeskus



23.9.2024 ©Taloushallintoliitto

Kun monivaiheinen tunnistautuminen on käytössä, pelkkä salasana ei avaa pääsyä palveluun

Jotain mitä tiedät

Tiedossasi oleva tieto, esimerkiksi salasana

Jotain mitä sinulla on

Kirjautuminen tapahtuu esimerkiksi erillisellä

Jotain mitä sinulla on

Tunnistautuminen tapahtuu esimerkiksi sormenjäljellä



Jos joku on saanut tietoonsa salasanasasi, sillä **ei pääse** kirjautumaan palveluun.

Monivaiheisen tunnistautumisen käyttöönotto

- Monivaiheisen tunnistautumisen käyttäminen ei ole monimutkaista ja siitä saatava lisäturvallisuus on todella arvokasta.
- Monissa järjestelmissä monivaiheinen tunnistautuminen ei ole automaattisesti päällä, vaan **se pitää itse ottaa käyttöön**. Käyttöönotto on tehtävä jokaisessa palvelussa erikseen. Useimmiten järjestelmän asetuksista löytyy kohta, jossa valitaan monivaiheisen tunnistautumisen käyttöönotto.
- Monivaiheinen tunnistautuminen ei vaadi toisen salasanan muistamista, vaan siinä hyödynnetään yleisesti jotakin tunnistautumismenetelmää, esimerkiksi todennussovellusta, kertakäyttöistä tekstiviesti- tai sähköpostikoodia tai biometristä tunnistetta, kuten sormenjälki- tai kasvojentunnistusta.
- Tämän moduulin linkkilistasta löydät Kyberturvallisuuskeskuksen ohjeen monivaiheisesta tunnistautumisesta, jossa kerrotaan tarkemmin eri tunnistautumismenetelmien käyttöönotosta.

- Tässä videossa kävimme läpi monivaiheista tunnistamista ja sen hyötyjä.
- Monivaiheisen tunnistautumisen käyttö vie vain hetken – ja se tuo todella paljon lisäsuojaa.



Sähköisen tunnistautumisen turvallisuus

Taloushallinnon työntekijöiden tietoturva

Moduuli 3: Turvalliset tunnistautumismenetelmät

Johdanto: Sähköisen tunnistautumisen menetelmät

- Tässä videossa käydään läpi sähköisen tunnistautumisen menetelmiä.
- Vahvalla sähköisellä tunnistautumisella voidaan todentaa henkilöllisyys luotettavasti.
- Vahvoja sähköisiä tunnistuspalveluja ovat
 - pankkien verkkopankkitunnukset
 - teleyritysten mobiilivarmenteet
 - Digi- ja väestötietoviraston kansalaisvarmenne poliisin myöntämällä henkilökortilla.
- Tässä videossa käydään läpi näitä menetelmiä ja keskustellaan niiden käytöstä työtehtävissä.

Sähköisen tunnistautumisen menetelmät



Suomessa on käytössä useita vahvan sähköisen tunnistautumisen menetelmiä, jotka ovat laajalti käytössä eri palveluissa. Vahvasta sähköisestä tunnistautumisesta säädetään *Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)*.

Yleistä

Vahvat tunnistautumismenetelmät tarjoavat pääsyn esimerkiksi viranomais- ja pankkipalveluihin, jonka vuoksi niitä tulee säilyttää huolellisesti, eikä niitä koskaan tule luovuttaa kenellekään toiselle.

Tämä velvollisuus on kirjattu lakiin:

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista

23 § Tunnistusvälineen haltijan velvollisuudet

Tunnistusvälineen haltijan on käytettävä tunnistusvälinettä sopimuksen ehtojen mukaisesti. Haltijan on säilytettävä tunnistusvälinettä huolellisesti.

Haltijan velvollisuus huolehtia tunnistusvälineestä alkaa, kun hän on vastaanottanut sen.

Tunnistusvälineen haltija ei saa luovuttaa välinettä toisen käyttöön.

Pankkien verkkopankkitunnukset



Tarjoajat: Suomalaiset pankit



Käyttö: Käyttäjä kirjautuu palveluun käyttämällä pankilta saamaansa käyttäjätunnusta sekä tunnistautumiseen tarvittavaa tunnistautumisvälinettä (esimerkiksi pankin mobiilisovellusta, erillistä laitetta tai avainlukulistaa).



Huomioita:

- Laajasti käytössä ja luotettava, pankkien vahvasti suojaama järjestelmä.
- Samalla tunnuksella laaja pääsy – niin viranomaisten palveluihin kuin omiin pankkipalveluihinkin.

Teleyritysten mobiilivarmenteet



Tarjoajat: Suuret teleoperaattorit.



Käyttö: Käyttäjä syöttää puhelinnumeronsa palveluun ja hyväksyy tunnistautumisen matkapuhelimellaan syöttämällä siihen PIN-koodin.



Huomioita:

- Helppokäyttöinen, vaatii vain matkapuhelimen, laajasti tuettu eri palveluissa.
- Ratkaisu, joka ei ole yhteydessä käyttäjän pankkisuhteeseen.

Kansalaisvarmenne



Tarjoajat: Poliisit myöntävät henkilökortteja, jotka sisältävät varmenteen.



Käyttö: Käyttäjä syöttää varmennekortin kortinlukijaan ja syöttää PIN-koodin.



Huomioita:

- Varmennekortin käyttö vaatii sirukortinlukijalaitteen ja kortinlukijaohjelmiston.
- Kansalaisvarmennetta ei voi käyttää puhelimella.

Vahva tunnistautuminen työtehtävissä



- Taloushallinnon tehtävissä saatetaan tarvita vahvaa tunnistautumista, esimerkiksi viranomaisten palveluihin. Kirjautumisia voi tulla päivän aikana useita.
- Kaikki edellä läpikäytyt menetelmät ovat varteenotettavia vahvan tunnistautumisen tapoja. Kaikissa on omat hyvät puolensa ja haasteensa.
- Voit oman elämäsi riskien hallinnan kannalta miettiä, olisiko hyvä, että käytössäsi olisi ainakin kaksi vahvan tunnistautumisen menetelmää:
 - Jos yhteen tulee vika, niin käytettävissäsi on varamenetelmä.
 - Lisäksi tällöin esimerkiksi pankkitunnukset voisi pyhittää ainoastaan pankkiasointiin ja muissa asioinneissa voisi käyttää toista käytössä olevaa tunnistautumismenetelmää. Silloin pankkitunnuksia ei tulisi vahingossakaan syötettyä huijaussivustoille työpäivän aikana.

Tässä videossa olet oppinut



- Tässä videossa kävimme läpi vahvan sähköisen tunnistautumisen menetelmiä ja niiden käyttöä työtehtävissä.



Moduuli 4: Tietoturva työpaikalla ja etätöissä

23.9.2024 ©Taloushallintoliitto



**talous
hallinto
liitto**



Huoltovarmuuskeskus

Toimitilaturvallisuuden hyvät käytännöt

Taloushallinnon työntekijöiden tietoturva

Moduuli 4: Tietoturva työpaikalla ja etätöissä

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Miksi tilojen turvallisuus on tärkeää tietoturvan kannalta



- Tilojen turvallisuus on keskeinen osa kokonaisvaltaista tietoturvaa. Vaikka digitaalinen turvallisuus saa usein enemmän huomiota, fyysinen turvallisuus on myös tärkeää tietojen ja järjestelmien suojaamisessa.
- Vaikka puhutaan pilvipalveluista ja etätöistä, on tärkeää huomata, että tietoja sisältävät laitteet ja tietoja käsittelevät ihmiset sijaitsevat aina fyysisesti jossakin. Tietojen suojaamiseksi myös niiden käsittelytilojen on oltava turvallisia.
- Fyysisiä suojauskeinoja ovat esimerkiksi tiloja suojaavat ovet, lukot, kulunvalvontaratkaisut ja niin edelleen. Fyysiset turvatoimet estävät luvattoman pääsyn tiloihin ja suojaavat laitteita ja henkilöstöä.
- Tässä videossa käymme läpi, millä tavoilla voimme ylläpitää työskentelytilojen tietoturvasuhteita.

Toimitilaturvallisuus



Kuvittele tilanne, jossa organisaatiosi tiloihin saapuu odottamatta ulkopuolinen henkilö. Näkisikö hän tiloissa asiakkaiden nimiä sisältäviä papereita tai mappeja, tai muuta luottamuksellista tietoa? Voisiko hän päästä tiloihin, joissa säilytetään tietoteknistä laitteistoa tai esimerkiksi paperiarkistoa?

Toimiston kyberhygienia

Toimiston kyberhygienialla pyritään siihen, että toimistossa fyysisesti sijaitsevista tiedoista (esimerkiksi papereista) ja tietoja sisältävistä laitteista (tietokoneista, palvelimista jne.) huolehditaan tavalla, joka pienentää niiden väärinkäytön tai varastamisen riskiä. Jokainen voi parantaa toimiston kyberhygieniaa huolehtimalla ainakin näistä:



Fyysisen turvallisuuden peruspilarit

Varmista aina, että toimiston ovet ja ikkunat pidetään lukossa eikä ulkopuolisilla ole pääsyä tiloihin.

Mahdollisimman paperiton toimisto

Minimoi työpaikalla olevien papereiden määrä, erityisesti sellaisten, jotka sisältävät luottamuksellista tietoa.

Hävitä luottamuksellista tietoa sisältävät paperit tietosuojaa-astiaan, josta ne tuhotaan.

Siistin työpöydän periaate

Pidä työpöytäsi siistinä ja poista kaikki arkaluontoiset asiakirjat, kun et ole työpisteelläsi.

Lukitse asiakirjat ja tallennusvälineet kaappeihin päivän päätteeksi.

Laitteiden säilytyspaikat

Varmista, että kaikki laitteet, kuten USB-tikut ja ulkoiset kiintolevyt, ovat turvassa ja lukittuna, kun niitä ei käytetä. Laitteiden sisältö tulee myös suojata salaamalla, jotta väärin käsiin joutuessaan tiedot eivät ole luettavissa.

Toimitilojen vierailijakäytännöt



- Toimiston turvalliset vierailijakäytännöt vahvistavat olennaisesti tietoturvaa. Vieraiden hallinta ja valvonta auttavat estämään luvattoman pääsyn arkaluontoisiin tietoihin ja tiloihin, suojaamaan työntekijöitä ja laitteita sekä varmistamaan toiminnan jatkuvuuden.
- Jos toimitila on jaettu julkiseen tilaan ja vain henkilöstölle tarkoitettuun tilaan, älä päästä henkilökuntaan kuulumattomia henkilöitä henkilöstön tiloihin. Näin tuet tietojen luottamuksellisena pysymistä.
- Silloin kun toimistoon tulee vieraita, esimerkiksi asiakas, huolehtikaa, että joku henkilökunnasta huolehtii vieraasta koko tämän vierailun ajan eikä vieras ole tiloissa yksin.

Kutsumattomia vieraita?



- On hyvä tietää, että verkkorikollisten työkalupakkiin kuuluu myös toimitiloihin luvatta ujuttautuminen. Toimitiloissa he voivat pyrkiä pääsemään käsiksi organisaation laitteisiin ja asentaa niihin haittaohjelmia, varastaa ne tai kopioida niillä olevia tietoja.
- Rikollisten usein käyttämä keino päästä toimitiloihin on esittää huoltotyöntekijää, joka kädet täynnä kantaa tikkaita tai maalipurkkeja. Silloin ihmiset avaavat kohteliaasti heille ovia sen enempää kyselemättä.
- Ole tietoinen tästä riskistä – kun avaat oven vain henkilöstölle tarkoitettuun tilaan, varmista, että samalla ovenavauksella ei tule sisään sellaisia henkilöitä, joilla ei ole pääsyoikeutta.
- Jos tiloihin pyrkii huoltohenkilöitä, varmista työnantajaltasi, että heidän tulostaan on sovittu.

Tässä videossa olet oppinut



- Tässä videossa kävimme läpi fyysisten tilojen turvallisuutta.
- Käsittelimme toimistotilan tietoturvallisuuden ylläpitämistä kyberhygienian keinoin ja kävimme läpi, miten hyvillä vierailijakäytännöillä varmistetaan toimiston tietoturvaa.





Huoltovarmuuskeskus

Etätyöskentelyn tietoturvallisuus

Taloushallinnon työntekijöiden tietoturva

Moduuli 4: Tietoturva työpaikalla ja etätöissä

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Etätyöskentelyn tietoturvallisuus



- Jos organisaatiosi sallii etätyöskentelyn, on tärkeää varmistaa, että voit työskennellä turvallisesti myös toimiston ulkopuolella.
- Tässä videossa käydään läpi käytäntöjä, joilla parannat tietoturvaa etätöissä.

Etätyöskentelyn tietoturvallisuus



Vaikka tekisit töitä kotona, käytä työntekoon vain työnantajan tarjoamia päätelaitteita. Älä käytä henkilökohtaisia laitteita (esimerkiksi kotitietokonetta tai omaa henkilökohtaista puhelintasi) työtehtävissä, ellei organisaatio ole erikseen sallinut sitä ja tarjonnut tarvittavaa tukea ja tietoturvatöimä.

Etätyöskentelyn turvallisuuden parhaat käytännöt

Laitteiden ja tietöjen suojaaminen

Lukitse tietokoneesi, kun et käytä sitä. Aseta tietokone lukittumaan automaattisesti. Pidä työskentelyalueesi siistinä ja poista luottamuksellista tietoa sisältävät asiakirjat, kun et käytä niitä. Säilytä laitteet turvallisessa paikassa.

Suojattu Wi-Fi

Muuta kotonasi olevan reitittimen oletuskäyttäjätunnus ja -salasana vahvemmiksi. Oletustunnukset ovat usein julkisesti tiedossa ja voivat johtaa luvattomaan käyttöön. Muista myös asentaa reitittimeen päivitykset.

Keskustelujen yksityisyydestä huolehtiminen

Ylläpidä tietöjen luottamuksellisuutta siten, että et käy luottamuksellisia keskusteluja sivullisten ollessa kuuloetäisyydellä.

Tuen saaminen

Varmista, että sinulla on käytettävissäsi organisaation IT-tuen yhteystiedot, jotta voit tarvittaessa saada apua teknisiin ongelmiin ja tietoturvakysymyksiin.

Turvallisuus työskennellessä julkisella paikalla

Julkisilla paikoilla, kuten kahviloissa ja kirjastoissa työskenteleminen tuo mukanaan myös tiettyjä tietoturvariskejä. Käydään läpi käytäntöjä, jotka auttavat parantamaan julkisella paikalla työskentelyn turvallisuutta:

- **Vältä julkisia ja suojaamattomia Wi-Fi-verkkoja** (esimerkiksi kahviloiden tai hotellien verkkoja). Jos mahdollista, käytä henkilökohtaista hotspot-yhteyttä puhelimestasi. Jos työnantajasi tarjoaa VPN-yhteyden, käytä sitä. VPN salaa verkkoliikenteen ja suojaa tietosi julkisissa ja epäluotettavissa verkoissa.
- **Huolehdi laitteistasi hyvin** äläkä jätä niitä hetkeksikään valvomatta julkisella paikalla.
- **Käsittele julkisilla paikoilla vain sellaisia tietoja, jotka eivät ole arkaluonteisia.** Älä käsittele luottamuksellisia tietoja tai tiedostoja, jos olet julkisessa tilassa ja joku voi nähdä näyttösi sisällön.
- **Älä käy sivullisten ollessa läsnä** (esimerkiksi lounasravintolassa tai junassa) **työhön liittyviä, luottamuksellista tietoa sisältäviä keskusteluja** tai puheluita.

Matkustamisen tietoturvallisuus



Työhön liittyvä matkustaminen, olipa kyseessä matkustaminen ulkomaille tai kotimaan sisällä, tuo mukanaan erilaisia tietoturvariskejä.

Matkoilla välineet katoavat helposti ja myös altistuvat varkauksille.

Tietoturvanäkökulmasta kaikkein tärkeintä on, että otat matkalle mukaan vain ne tiedot ja laitteet, joita todella tarvitset. Arkaluontoiset tiedot ja ylimääräiset laitteet kannattaa jättää kotiin tai toimistolle.

Parhaat käytännöt matkustamisen tietoturvallisuuteen

Varmista, että kaikki laitteet ovat päivitettyjä ja että niissä on ajantasaiset virustorjunta- ja haittaohjelmien torjuntaohjelmistot.

Pidä laitteesi aina hallinnassasi. Älä jätä niitä valvomatta edes hetkeksi, esimerkiksi lentokentällä tai junassa. Käytä hotellihuoneessa laitteiden säilyttämiseen tallelokeroa, jos mahdollista, ja pidä lentokoneessa laitteet mukana käsimatkatavaroissa.

Älä käsittele luottamuksellisia tietoja, jos olet tilassa, jossa joku voi nähdä näyttösi sisällön. Jos teet töitä kulkuvälineessä, esimerkiksi junassa tai lentokoneessa, huomioi, että takanasi istuvat henkilöt pystyvät näkemään näyttösi sisällön.

Jos matkustat ulkomaille, varmista työnantajasi kanta siihen, saako työhön liittyviä laitteita viedä ulkomaille.

Huomioi, että henkilötietojen käsittelyyn eri sijainneista voi liittyä rajoitteita: et esimerkiksi voi matkustaa EU- ja ETA-maiden ulkopuolelle etätöihin ja käsitellä sieltä käsin henkilötietoja samoilla säännöillä kuin Suomessa.

Tässä videossa olet oppinut

- Tässä videossa kävimme läpi etätyöskentelyn ja matkustamisen turvallisuutta.
- Kävimme läpi, että tietoturvallisuus tulee huomioida, työskentelit sitten kotona etätöissä, jossakin julkisessa tilassa tai matkustaessa.



Moduuli 5: Toiminta poikkeustilanteessa

23.9.2024 ©Taloushallinto



**talous
hallinto
liitto**



Huoltovarmuuskeskus

Henkilötietojen tietoturvaloukkaukset

Taloushallinnon työntekijöiden tietoturva

Moduuli 5: Toiminta poikkeustilanteessa

2024

23.9.2024 ©Taloushallinto

Henkilötietojen tietoturvaloukkaukset

- Tämän videon aiheena ovat henkilötietojen tietoturvaloukkaukset.
- Käymme läpi, mitä henkilötietojen tietoturvaloukkaukset ovat, minkälaisia vaikutuksia niillä voi olla ja miten henkilötietojen tietoturvaloukkaustilanteessa tulisi työntekijänä toimia.

Henkilötietojen tietoturvaloukkaukset



Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, joka johtaa **henkilötietojen** luvattomaan käyttöön, paljastumiseen, muuttumiseen, häviämiseen tai tuhoamiseen. Tällainen loukkaus voi aiheuttaa merkittävää haittaa henkilölle, jonka tiedot ovat vaarantuneet, sekä organisaatiolle, joka on vastuussa tietojen suojaamisesta.

Esimerkkejä henkilötietojen tietoturvaloukkauksista



- Tietosuoja-asetuksen tarkoittama henkilötietojen tietoturvaloukkaus syntyy, kun henkilötietoja tuhoutuu, häviää tai muuttuu tai niitä käytetään luvatta.
- Kaikki työssä tapahtuvat tietoturvaloukkaustilanteet on aina käsiteltävä organisaatiossa. Loukkauksen jälkeen on tärkeä arvioida, millaisen riskin tapahtuma aiheuttaa rekisteröidylle.
- Käydään seuraavaksi läpi tyypillisiä esimerkkejä tietoturvaloukkauksista.

126 Esimerkkejä henkilötietojen tietoturvaloukkauksista



Tapahtuma	Kuvaus	Esimerkki	Merkit ja varoitusmerkit
Tietojen vuotaminen	Henkilötiedot paljastuvat luvattomille osapuolille tietomurron, inhimillisen virheen tai muun tietoturvapoikkeaman seurauksena.	Hakkeriija pääsee käsiksi yrityksen asiakasrekisteriin, joka sisältää asiakkaiden nimet, osoitteet ja henkilötunnukset, ja levittää nämä tiedot verkossa.	Erikoisia tapahtumia yrityksen verkossa tai järjestelmässä, poikkeavia kirjautumisia järjestelmään
Väärälle lähettäjälle lähetetyt viestit	Henkilötietoja sisältävä sähköposti tai muu viesti lähetetään vahingossa väärälle vastaanottajalle.	Palkanlaskija lähettää vahingossa työntekijän henkilötietoja sisältävän sähköpostin toiselle asiakkaalle.	Viestin vastaanottajalta saatu palaute, virheen huomaaminen
Kadonneet tai varastetut laitteet	Laitte, joka sisältää henkilötietoja, katoaa tai varastetaan, ja tiedot joutuvat luvattomien henkilöiden käsiin.	Työntekijän kannettava tietokone, joka sisältää henkilötietoja, varastetaan matkalla.	Laitteen katoamisen huomaaminen
Sisäpiiriläisen väärinkäytös	Organisaation työntekijä käyttää asemaansa väärin ja pääsee käsiksi henkilötietoihin luvattomasti tai levittää niitä.	Suivaantunut työntekijä kopioi asiakasrekisterin ja käyttää tietoja omiin tarkoituksiinsa.	Poikkeava käytös, uhkaukset
Inhimilliset virheet	Henkilötietojen käsittelyssä tapahtuu virhe, joka johtaa tietojen paljastumiseen tai muuttamiseen.	Työntekijä tallentaa henkilötiedot väärään kansioon, joka on kaikkien työntekijöiden nähtävissä.	Virheen huomaaminen, puutteellinen ohjeistus/koulutus

Henkilötietojen tietoturvaloukkausten seuraukset



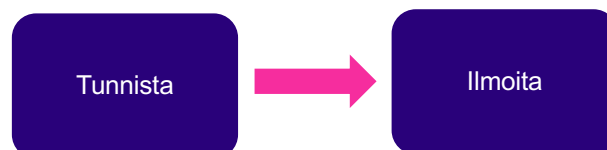
Huomasitko edellä käydyistä esimerkeistä, että usein henkilötietojen tietoturvaloukkausten syyt ovat helposti estettävissä? Estämiseen kannattaa panostaa, sillä henkilötietojen tietoturvaloukkaukset voivat aiheuttaa merkittäviä seurauksia sekä yksilöille että organisaatioille:

- Tietoturvaloukkauksen kohteeksi joutuneet henkilöt voivat kärsiä identiteettivarkauksista ja muista henkilökohtaisista haitoista.
- Organisaation maine voi kärsiä, mikä voi johtaa asiakkaiden ja yhteistyökumppaneiden luottamuksen menettämiseen. Organisaatio voi myös joutua oikeudelliseen vastuuseen ja saada sakkoja tietosuojasäädösten rikkomisesta.

Mitä tehdä tietoturvaloukkauksen sattuessa



- Organisaatioilla on velvollisuus dokumentoida kaikki tietoturvaloukkaukset.
- **Tunnista:** ilmoita siis aina, jos havaitset henkilötietojen luvaton käyttöä, niiden paljastumista, häviämistä tai tuhoamista. Tee ilmoitus, vaikka et olisi varma, onko kyseessä henkilötietojen tietoturvaloukkaus.
- **Ilmoita:** tee ilmoitus organisaatiosi toimintaohjeen mukaisesti. Ilmoita aina heti, sillä nopeasti tehty ilmoitus voi auttaa estämään lisävahinkoja.



Tässä videossa olet oppinut



Huoltovarmuuskeskus

- Tässä videossa kävimme läpi henkilötietojen tietoturvaloukkauksia.
- Jokaisessa organisaatiossa on oma ohjeensa siitä, miten havaitusta tietoturvaloukkausesta tulee ilmoittaa organisaation sisällä. Noudata tätä ohjetta, ja ilmoita aina havainnoistasi.



23.9.2024 ©Taloushallintoliitto



Huoltovarmuuskeskus

Tietoturvahäiriöt

Taloushallinnon työntekijöiden tietoturva

Moduuli 5: Toiminta poikkeustilanteessa

2024

23.9.2024 ©Taloushallintoliitto

Johdanto: Tietoturvahäiriöt

- Tässä videossa käsitellään tietoturvahäiriöitä.
- Tietoturvahäiriöt ovat tapahtumia, joissa tietojen luottamuksellisuus, eheys tai saatavuus vaarantuu. Tietoturvahäiriöt voivat johtua esimerkiksi tietoturvahyökkäyksistä, inhimillisistä virheistä tai teknisistä vioista.
- On tärkeää, että tunnistat ja reagoit tietoturvahäiriöihin havaitessasi sellaisen, sillä nopealla reagoinnilla tilanteen aiheuttamia vahinkoja voidaan rajata.

Esimerkkejä tietoturvahäiriöistä



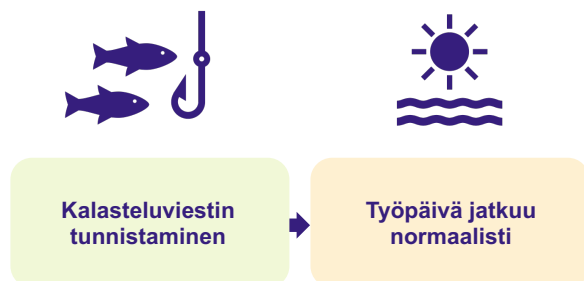
- Klikkaat sähköpostiviestissä ollutta linkkiä ja syötät epähuomiossa käyttäjätietosi huijaussivustolle.
- Työpuhelin katoaa, mikä saattaa johtaa tietojen päätymiseen väärin käsiin.
- Tietokoneessasi on häiriö, joka vaikuttaa haittaohjelmalta.
- Organisaatioon kohdistuu tietomurto, jossa luottamuksellisia tietoja paljastuu hyökkääjälle.
- Palvelunestohyökkäys lamauttaa yrityksen verkkosivut tai -palvelut.

Esimerkki tietoturvahäiriötilanteen etenemisestä



©Taloushallintoliitto

Miten tilanteessa voisi toimia?



©Taloushallintoliitto

Miten tilanteessa voisi toimia?



©Taloushallinto-liitto

Tietoturvahäiriöiden seuraukset

Tietoturvahäiriöitä on monenlaisia ja niiden seuraukset voivat vaihdella hetkellisestä työn keskeytymisestä kuukausia kestäväan kriisitilaan. Tietoturvahäiriöt voivat vaikuttaa organisaatioihin monilla tavoilla.

Liiketoiminnan häiriö

Organisaation liiketoiminnan prosessit, kuten valmistus, toimitukset tai myynti, voivat vaikeutua tai keskeytyä tietoturvahäiriön johdosta.

Taloudelliset menetykset

Organisaatiot voivat kärsiä suoria taloudellisia menetyksiä tietojen varastamisen, vakoilun tai palvelunestohyökkäysten seurauksena.

Tietojen menetys

Organisaatiot voivat menettää liiketoiminnalleen välttämättömiä tietoja tai sellaisia tietoja, jotka laki velvoittaa organisaation säilyttämään.

Luottamuksen menetys

Asiakkaat, yhteistyökumppanit ja sijoittajat saattavat menettää luottamuksen organisaatioon. Tilanne voi johtaa jopa organisaation toiminnan päättymiseen tai yrityksen osakekurssin laskuun.

Tietoturvahäiriöiden vaikutukset yksilöihin



Vakavat häiriötilanteet ovat aina kriisejä, jotka vaikuttavat syvästi yrityksen henkilöstöön ja johtoon.

Häiriöillä voi myös olla vaikutusta organisaation ulkopuolisten henkilöiden elämään, jos heidän tietojaan on vuotanut, tai jos häiriö estää esimerkiksi palkkojen maksamisen ajallaan.

Toimi näin tietoturvahäiriötilanteessa

Tietojenkalasteluviestit:

- Jos saat epäilyttävän sähköpostin, älä klikkaa siinä olevia linkkejä tai avaa liitteitä. Ilmoita mahdollisesta kalastelusähköpostista organisaatiosi ohjeistuksen mukaan, eli esimerkiksi IT-tuelle tai tietoturvatiimille.
- Jos olet klikannut tietojenkalasteluviestissä olevia linkkejä tai avannut liitteen, ilmoita asiasta eteenpäin **välittömästi**. Pysy rauhallisena ja odota lisäohjeita.

Muut häiriötilanteet:

- Jos huomaat toisenlaisen tietoturvahäiriön tai tietoturvaan liittyvän läheltä piti -tilanteen, ilmoita myös siitä heti organisaatiosi käytäntöjen mukaisesti. Ilmoita, vaikka et ole varma, onko kyseessä niin sanottu ”väärä hälytys” vai ihan oikea tilanne. Mitä nopeammin asia saadaan selvitettyä, sitä pienemmillä vahingoilla usein selvittää. Tilanteen selvittämisessä on yleensä apua todisteista, kuten kuvakaappauksista. Ota siis talteen mahdolliset todisteet.

Kaikissa tietoturvahäiriötilanteissa tärkeintä on aina ilmoittaa asiasta, eikä jäädä pohtimaan pitäisikö ilmoittaa vai eikö.

Tässä videossa olet oppinut

- Tässä videossa kävimme läpi tietoturvahäiriöitä ja niiden vaikutuksia.
- Videon tärkein oppi meistä jokaiselle on, että tietoturvahäiriöhavainnoista pitää aina ilmoittaa eteenpäin.
- Tämä oli kurssin viimeinen video. Kurssilla on videoiden lisäksi paljon muutakin materiaalia, kuten tehtäviä ja hyödyllisiä linkkejä, joten tutustu niihinkin.
- Kiitos kurssin suorittamisesta!

