LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Oppilaitoksen tietoturvataso

Helenius, Max & Lääkkö, Tero

Laurea-ammattikorkeakoulu

Oppilaitoksen tietoturvataso

Helenius Max, Lääkkö Tero
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Tammikuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Tero Lääkkö, Max Helenius

Oppilaitoksen tietoturvataso

Vuosi 2017 Sivumäärä 46

Opinnäytetyön tarkoituksena oli päivittää asiakasyrityksen henkilöstön tietoturvadokumentaatio nykyaikaiseksi. Tämä tehtäisiin tutustumalla henkilökunnan tietoturvaosaamiseen ja -arvoihin, nykyiseen käytäntöön sekä aiheeseen liittyvään teoriaan, jonka jälkeen uusi tietoturvadokumentaatio valmistetaan tutkimuksessa havaitsemiemme parhaiden kokonaisratkaisujen pohjalta.

Työn tavoitteena on luoda katsaus nykypäivän tietoturvauhkiin ja -käytänteisiin, joista tuotamme vaaditun tietoturvadokumentaation. Työn tuloksena syntyy asiakasyritykselle hyödyllisiä ja tarkoituksenmukaisia titoturvallisuutta ja tietoturvatietoisuutta parantavia käytänteitä.

Pääviitekehyksenä opinnäytetyön toteutuksessa toimi Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmän (VAHTI) ohjeet, jotka ovat Valtiovarainministeriön ylläpitämät. Etenimme vaiheittain, ensiksi teoriaan ja asiakasyrityksen nykytilanteeseen tutustuen muuan muassa haastatteluilla, jonka jälkeen kokosimme työn ja tietoperustaan perehtymisen jälkeen laadimme oppilaitokselle uuden tietoturvadokumentin

Asiakasyrityksen henkilöstön tietoturvaosaaminen ja tietoisuus tietoturvan tärkeydestä on lisääntynyt työn tuloksena syntyneen tietoturvadokumentin ansiosta. He itse ovat oman työympäristönsä turvallisuuden takaajat viime kädessä ja tekemämme tietoturvadokumentaatio auttaa parantamaan tietoturvallisuuden tasoa oppilaitoksessa.

Asiasanat: tietoturva, työympäristö, koulutus, riskienhallinta, henkilöstö

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Programme in Business Information Technology

Tero Lääkkö, Max Helenius

Information Security Level in an Educational Institution

Year 2017 Pages 46

This thesis was made with the purpose of updating the customer company's information security documentation to modern standards. This would be achieved by familiarizing ourselves with the current level of information security know-how amongst the personnel, current day practices and up-to-date theory on the subject. Based on this work we will form a new information security documentation.

Our main objective is to review the current state and practices of information security at work from whence we'll form the required documentation. Our focus will be on the most useful and purposeful practices concerning the work environment.

As our main frame of reference we will be using the Government Information Security Management Board VAHTI under the supervision of the Ministry of Finance. We advanced in phases throughout, first acquainting ourselves with the appropriate theory and current situation of the customer company by e.g. interviews with the personnel after which we compiled the work, drafted a new information security document and evaluated the results.

We want to bring out the importance of ingrained values towards information security present in the personnel. They themselves are the sole guarantors of safety in their work environment ja we hope our work will only support and strengthen the existing understanding on the subject amongst the staff.

Keywords: information, security, work environment, training, risk management, personnel

Sisällys

1 Johdanto

Toimiva tietoturva on yritysten elinehto ja yksi tärkeimmistä asioista menestyksekkääseen liiketoimintaan. Toimivalla tietoturvalla minimoidaan monia riskejä, kuten tietosuoja-asioiden ja tärkeiden dokumenttien vuotamista sellaisten henkilöiden käsiin, joilla ei niihin pitäisi olla minkäänlaista pääsyoikeutta. Jokaisella ihmisillä on omanlaisensa tapa työskentelyyn, mutta yhteneväinen tietoturvallinen työskentely on todella tärkeää ja tätä asiaa pitäisi teroittaa perehdytyksessä sekä päivittää tietoturvatietoutta pitkin työsuhdetta.

Nykyään lukuisat, ellei peräti kaikki, yritykset tarjoavat työntekijöilleen työsuhdepuhelimen, työsuhdekannettavan tai työsuhdetabletin. Kaikkiin näihin arkisinakin asioina kokemiimme liittyy olennaisena asiana tietoturvan muistaminen. Jokainen laite täytyy suojata hyvällä, toimivalla salasanalla, jota ei voida helposti yrityksen asioihin kuulumattoman henkilön selvittää.

Jokapäiväisessä työssämme painimme monien eri tietoturvaan liittyvien asioiden parissa. Yllä mainituilla salasanoilla pääsemme työkoneellemme ja pystymme avaamaan kännykkämme. Näiden lisäksi vastaamme tulee heti päivän alussa töihin saapuessamme kulunvalvontaa, monella työpaikalla täytyy leimata itsensä sisälle ja eri tiloihin pääsee vain eri kulkuoikeuksilla. Mitkä olisivatkaan seuraamukset, jos kiireessä oma kulkulupa tippuukin taskusta kadulle? Asia ei ole aivan niin yksinkertainen uuden kulkukortin noutaminen, mitä moni voi kuvitella.

Varsinkin koulumaailmassa työhuoneissakin on monia eri seikkoja, joita on hyvä ottaa huomioon työskentelytavoissaan. Kovalla kiireellä asioille syöksyessään voi herkästi jäädä työasema lukitsematta, tai mikä yhtä lailla iso virhe, työhuoneen ovi lukitsematta. Käytävillä saattaa liikkua monia riskitekijöitä.

Työparina pohdimme kaikkia näitä asioita. Mietimme monia eri aihevalintoja, mutta tämä kyseinen vaikutti mielestämme kaikkein ”arkisimmilta”. Maailma digitalisoituu valtavaa vauhtia ja haluamme auttaa omalta osaltamme tätä matkaa muistuttamalla tietoturvallisista työskentelytavoista.

Toivomme työskentelymme johtavan työskentelytapojen parantumiseen ja parantamaan eri oppilaitoksen toimintojen luotettavuutta. Puutteellinen tietoturva saattaa johtaa tarpeettomiin lisäkustannuksiin ja niiden riskiä pyrimme minimoimaan mahdollisimman pieneksi.

Opinnäytetyömme asiakas on Suomen johtava ammatilliseen aikuiskoulutukseen ja työelämän kehittämispalveluihin erikoistunut ja keskittynyt koulutuksen järjestäjä. Yrityksen taustayhteisöjä ovat X-säätiön 40 vuotta sitten perustaneet Helsingin, Espoon, Vantaan ja Kauniaisten

kaupungit. Säätiö perustettiin ammatilliseksi kurssikeskukseksi, joka tuotti alkuvaiheessa palveluja vain työvoimapoliittisin perustein. Tutkintotavoitteinen koulutus nousi hieman myöhemmin säätiön toiseksi tukijalaksi erityisesti näyttötutkintojärjestelmän kehittymisen myötä.

2000-luvun alussa säätiö uudisti strategiansa ja käynnisti laaja-alaisen hankkeen laajentaakseen asemaansa henkilöstökoulutusten markkinoilla. Tulevaisuuden työskentelyssä henkilöstökoulutuksen määrän ja vaikuttavuuden on arvioitu kasvavan roimasti yritysten halutessa kehittää oma henkilökuntaansa. Luonnollisesti taloudelliset resurssit ovat tänäpäivänä hieman rajalliset.

Vuonna 2015 yrityksen liikevaihto oli noin 33,5 M€ ja henkilökunnan lukumäärä vähän yli 300 henkilöä. Nyttemmin taloudelliset tiukennukset ovat iskeneet myös koulutustoimintaan, ja se on havaittavissa myös asiakasyrityksemme toiminnassa.

Koulutusaloja asiakasyrityksessämme on lukuisia. Ne ovat jaettuna eri yksiköihin, joita on yhteensä kymmenen: ICT, Energia ja teollisuus, Kauppa, Yritysturvallisuus, Maahanmuuttajapalvelut, Muutosvalmennus, Eläintenhoito ja välinehuolto, Hoito- ja hoivatyö, Kiinteistöpalvelut ja Rakentamispalvelut. Yhteensä näiden kaikkien kymmenen yksikön sisällä liikkuu vuositasolla runsaat 22 000 opiskelijaa.

Yrityksen arvoja ovat yhteiskunnallinen vastuullisuus, vaikuttavuus, luotettavuus ja luovuus. Tulevaisuuden visiona on toimia johtavana kehittämiskumppanina ammatillisen osaamisen alalla. Ydinosaamisalueekseen asiakasyrityksemme laskee liiketoimintaosaamisen sekä työelämäosaamisen. Näiden lisäksi palveluratkaisuosaaminen ja projektinhallintaosaaminen lasketaan korkealle osaamiskartoituksessa.

Hoito- ja hoivatyön yksikkö on asiakasyrityksemme yksi kärkikohteista ja suurimpia yksiköitä. Se työllistää yli 20 henkilöä, joista valtaosa on kouluttajia. Kouluttajia on palkattu monista eri taustoista monipuolisten osaamisen ja ammattitaidon takaamiseksi. Lisäksi oppilaitos hyödyntää kattavaa konsulttiverkostoa koulutustoiminnassaan.

Suurin yksikön koulutusala on lähihoitajakoulutus. Asiakasyrityksemme kautta valmistuu vuosittain lukuisia uusia lähihoitajia esimerkiksi työvoimapoliittisen koulutuksen kautta. Lähihoitajia valmistuu monille eri osaamisaloille. Mielenterves- ja päihdetyö, sairaanhoito- ja huolenpito, vanhustyö ja vammaistyö ovat eräitä suosituimpia osaamisaloja.

Lähihoitajakoulutuksen lisäksi yrtiyksessä opintojaan käyvät tulevat koulunkäyntiavustajat. Myös ensiapukoulutukset kuuluvat koulutusvalikoimaan ja niitä järjestetään viikoittain useampia. Tarjolla on kaksipäiväisiä ensiavun peruskursseja sekä jatkokursseja, kuin myös työpäivän mittaisia hätäensiaputoteutuksia.

Alan useimmat suuret palveluntuottajat ovat tällä hetkellä asiakasyrityksemme asiakkaita. Monien asiakkaiden kanssa räätälöidään erinäisiä täsmäkoulutuksia kestoltaan päivästä muutamaan päivään, joiden tarkoituksena on lisäkouluttaa jo palkkalistoilla olevaa henkilökuntaa kohtaamaan hoitotyön uusia haasteita.

Hoito- ja hoivatyö itsessään elää murroskautta ja se tuo omat haasteensa myös koulutustoimintaan. Esimerkiksi teknologiaosaamisen kouluttaminen lisääntyy teknologian aina kehittyessä ja sen tuoden mukanaan uusia mahdollisuuksia hoitotapahtumien kirjaamisissa, työajan seurannoissa sekä resurssien suunnittelussa.

2 Työn aiheen esittely

Tietoturvasta vain 20 prosenttia on tekniikkaa ja 80 prosenttia on kaikkea muuta, mitä tietoturvaan sisältyy. Tekniikkapuoleen kuuluvat palomuurit, virustorjunta ja pääsynvalvonta. Loput 80 prosenttia on toimintatapoja, sääntöjä ja ohjeita. (Y-Lehti 2010)

Opinnäytteemme aiheena on tarkastella nykypäivän tietoturvastandardeja, toimintatapoja, sääntöjä sekä ohjeita ja päivittää tehdyn työn pohjalta asiakasyrityksemme Hoito- ja hoivatyön yksikön tietoturvaosaamista tuottamalla asiakkaan ehtojen mukainen tietoturvakoulutuksen ohjeistus. Tulemme kartoittamaan, kuinka hyvien tapojen mukainen tietoturvallinen työnteko käytännössä tapahtuu ja sovellamme oppimaamme teoriaa sekä käytännön havainnointia asiakasyrityksen tilaaman tietoturvavihkosen tuottamisessa.

Tietoturvavihkosen tarkoituksena on ohjeistaa ja opastaa asiakasyrityksen kohdeyksikön toimintaa tavalla, joka on helposti ymmärrettävissä ja omaksuttavissa, mutta myös ehdottomasti tämän päivän tietoturvatietämyksen tasalla.

2.1 Työn taustojen esittely

Asiakasyrityksellä on tietoturvan pohjanaan käytössä VAHTI-dokumentit. Tietoturvaohjeistus on olemassa, mutta sen aihioita ja sisältöä ei ole hetkeen virkistetty työntekijöille tietoon, joten pieni muistinvirkistys tärkeistä tietoturvan osa-aluista on olennaisen tärkeää.

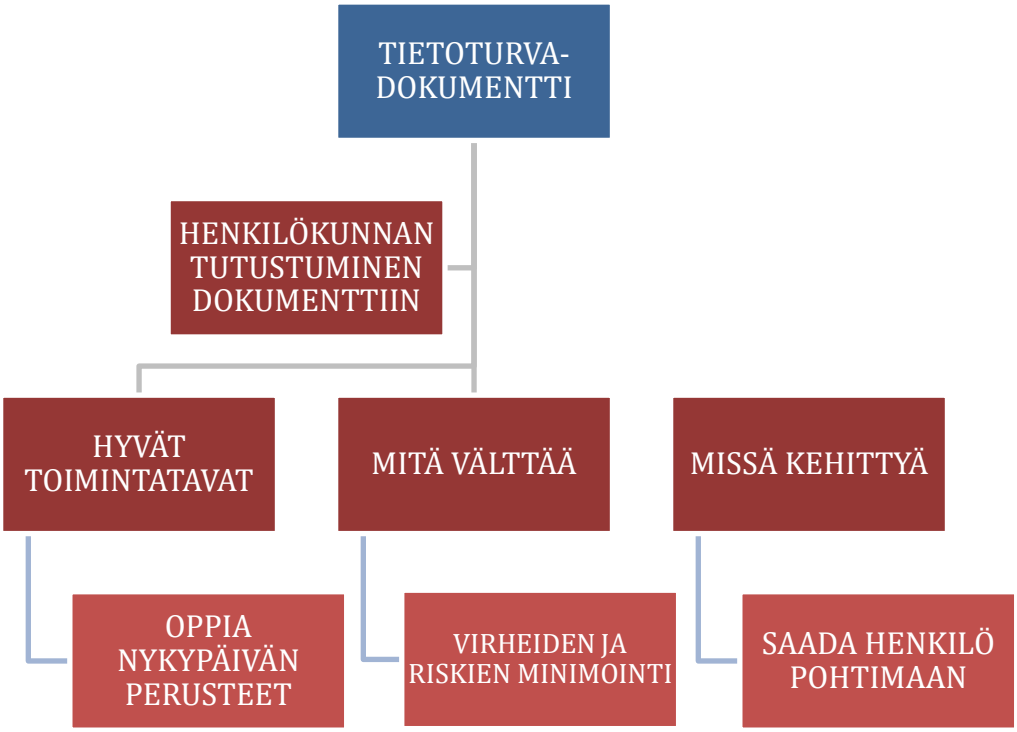
Opinnäytetyön pääviitekehyksenä toimii myös tietoturvavihkosen tuottamisen teoriapohjana käyttämämme Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) julkaisema

ohjeistus. Uskomme VAHTIn olevan työllemme sekä aiheellemme edullinen ja täsmällinen työkalu. Lisäksi tutustumme muuhun teoreettiseen pohjaan sekä käytännön kokemuksiin hyvistä tietoturvaratkaisuista.

Tietotekniikan merkitys modernin työympäristön toimivuuden kannalta on muodostanut tarpeen tutkia ja ylläpitää tietoturvan mekanismeja, toimintatapoja sekä skaalaa. Sen huomioiminen on kasvanut osaksi jokaisen työntekijän vastuuta ja sen kehittäminen on saatettu vastaamaan niitä haasteita, joita VAHTI-ohjeistuksessa on pyritty huomioimaan.

2.2 Työn tavoitteet

Työmme tavoitteena on kehittää Hoito- ja hoivatyön yksikön tietoturvaosaamista vastaamaan tämän päivän minimivaatimuksia. Toivomme voivamme vaikuttaa tietoturvallisen työympäristön luomiseen panostuksemme pohjalta.



Kuvio 1: Työn tavoitteet

Kuten yllä oleva kaavio esittää, tavoitteemme on saada yksikön henkilökunnassa aikaan kolme erilaista ajattelun aihetta; Mitkä ovat hyvät toimintatavat? Mitä välttää omassa työskentelyssäni? Miten voin kehittää omaa tietoturvallista työskentelyäni?

Toivomme tietoturvaoppaamme tuovan sitä myöten nykypäivän perusteet hallintaan, sekä saada oppaan lukijassa aikaan omaa pohdintaa siitä, miten hän työskentelee ja kiinnittämään huomiota, voisiko hän tehdä asioita toisin.

3 Tietoturvan nykytaso oppilaitoksessa

Asiakasyrityksen tietoturva pohjautuu Valtiohallinnon tietoturvallisuuden johtoryhmän VAHTI-ohjeistukseen. Ohjeistus on tarkoitettu yleisesti niin henkilökunnalle kuin ulkopuoliselle toimeksiannosta työskentelevälle henkilöstölle, kuten konsulteille. Tässä luvussa käymme läpi kaikkein keskeisimpiä tietoturva-ohjeistuksia.

Tietoturvallisuus on asiakasyrityksen toimintonen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys, jolla turvataan yksilön ja yrityksen etuja. Suurimmat tietoturvallisuuden ongelmat liittyvät yleensä kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin. Siksi tietoturvallisuudesta huolehtiminen on jokaisen organisaatiossa työskentelevän velvollisuus ja puutteellinen tietoturvallisuus vaarantaa yrityksen, henkilöstön ja asiakkaiden etuja sekä saattaa aiheuttaa lisätyötä ja lisäkustannuksia. (Yrityksen TT)

Asiakasyrityksessämme käsitellään runsaasti sekä julkista että salassa pidettävää tietoa, joten tietoturvallisuus on hoidettava asianmukaisesti.

Asiakasyrityksemme tietoturvaohjeet ovat kaiken kaikkiaan kattavat ja ne löytyvät hakusanoilla yrityksen intranetistä. Ne pitävät sisällään tiivistelmän tärkeimmistä asioista sekä laajemman kokonaisuuden, jossa kohtia tietoturvasäännöistä avataan tarkemmin. Olemme koonneet mielestämme olennaisimpia asioita ohjeistuksesta.

- Vain tietohallinto saa asiakasyrityksessämme asentaa ohjelmia työntekijöiden koneelle. Yrityksessä on käytössä tietohallinnon julkaisukanava, josta voi halutessaan ladata esimerkiksi Google Chromen tai Mozilla Firefoxin selaimekseen. Oletuksena on Internet Explorer.
- Aina koneelta poistuessa, oli se sitten oma kone tai muiden tilojen koneet, täytyy kone lukita CTRL-ALT-DEL –yhdistelmällä. Yksikään ulkopuolinen ei saa käyttää työntekijän tietokonetta.
- Ohjeet kehoittavat tallentamaan tietoa verkkopalvelimen levylle, eikä esimerkiksi jokaisen käytössä olevaan henkilökohtaiseen työtilaan, jotta tieto on saatavilla, mikäli työntekijä on poissa.
- Tietohallinto luo työnkuvan perusteella oikeudet, käyttäjätunnukset ja salasanat. Niitä ei saa luovuttaa kenellekään eteenpäin, ei ole sallittua luovuttaa niitä edes tietohallinnolle.

- Sähköpostin käytössä pitää käyttää yhteneväistä sähköpostipohjaa sekä tietynlaista, määrättyä allekirjoistusta.
- Sähköpostilla ei suositella liitteiden lähettämistä vaan mieluummin linkitys tiedosto-sijaintiin.
- Työsuhteen päättyessä sähköpostilaatikko suljetaan, ja esimiehen täytyy pyytää kirjallinen lupa työntekijältä, mikäli henkilön sähköpostia halutaan lukea työsuhteen päättymisen jälkeen.
- Työpöydällä ei saa säilyttää papereita tai muuta salassa pidettävää materiaalia.
- Työhuoneeseen ei saa päästää valvomatta ulkopuolisia.
- Huoneeseen saapuessa kehoitetaan tarkastamaan, ettei ole sattunut mitään poikkeavaa.
- Tuhottavat paperit on hävitettävä asianmukaisesti, eikä niitä saa heittää vain normaaliin paperikeräykseen.
- Tietokoneen näyttö täytyy olla oikein aseteltu niin, että ulkopuoliset eivät näe näytöllä olevaa tietoa tai käyttäjätunnusta ja salasanaa.

4 Tietoturvahaastattelu oppilaitoksen yksikössä

Päätavoitteemme on keskittyä työssämme yhteen yksikköön, joten painotumme laajemmin sen työntekijöiden tietoturvaosaamiseen. Yksittäiset haastattelut ovat ajankäytöllinen mahdottomuus, joten päätimme toteuttaa kartoituksen suunnittelemalla käyttöömme haastattelulomakkeen.

Haluamme ottaa haastattelun kautta selville niin nykyistä tietoturvan tasoa kohteessa kuin sen henkilöstön asenteita tietoturvallisuutta kohtaan. Hyvät lähtökohdat onnistuneelle tietoturvalle saadaan motivoituneesta ja vastaanottavaisesta henkilökunnasta.

4.1 Haastattelulomakkeen suunnittelu ja aiheet

Haastattelulomakkeen päätimme toteuttaa sähköisessä muodossa ja sen jakelu tapahtui yksikön työntekijöiden sähköpostiosoitteisiin. Vastaaja avaa saamansa linkin ja pääsee täyttämään kyselyä. Täytettyään kyselyn kaikki vastaukset tallentuvat tietokantaan, josta voimme lopuksi tarkastella yhteenvetoja.

Lomake on toteutettu Surveypal-palautejärjestelmää hyödyntäen. Kyselyn pystyi toteuttamaan täysin itse suunnitellen ilman mitään ennaltamääritettyjä muotoja. Halusimme saada vastaajat ajattelemaan laajemmin, joten käytimme monia avoimia kenttiä vastauksia varten. Lisäksi mukaan teimme monivalintakysymyksiä kartoittamaan perusasioita, kuten salasanojen pituutta ja kuinka usein sen vaihtaa.

Kysymykset muodostettiin aikuispedagogiikan suosituksia mukaillen haastateltavien kokemus- ja tietopohjaan keskittyen. Tietoturvallinen toiminta on täysin riippuvainen henkilöstön asenteista sen tähdellisyyttä kohtaan, joten näimme erittäin tärkeäksi ottaa haastatteluissa selvää näistä seikoista.

Painotimme haastateltavien omia kokemuksia tietoturvallisuudesta. Tärkeitä seikkoja hyvän tietoturvaosaamisen ja -asenteen luomisessa henkilöstöön ovat kohdeyleisölle räätälöity koulutus sekä koulutuksen onnistumisen seuranta. Haasteet tietoturvan eheyttä koskien lisääntyvät palvelujen monimutkaistuessa ja koulutuksen on oltava ajan tasalla, joten tämä oli meille myös tärkeä seikka ottaa selville.

Lisäksi koimme tärkeäksi ottaa selvää henkilöstön rutiineista tietoturvaa koskien. Otamme selvää, kuinka edellinen tietoturvaohjeistus on ollut henkilöstön käytössä ja kuinka helppokäyttöinen se on ollut.

4.2 Tietoturvan nykytaso yksikössä

Tekemämme haastattelulomake tavoitti yksikössä 24 työntekijää. Heistä 11 vastasi kyselyyn eli vastausprosentiksi muodostui 45,8%. Tarkempaa erottelua emme vastaajien suhteen tehneet, sillä kaikki yksikön henkilöstöstä toimivat samojen asioiden äärellä.

Vastanneista yli puolet ilmoittaa lukitsevansa tietokoneensa poistuessaan työpisteeltään. Kuitenkin muiden vaihtoehtojenkin kanssa on paljon hajontaa ja onkin huomattavissa, että useammalla kone jää lukitsematta.

Kuvio 2: Tietokoneen lukitseminen

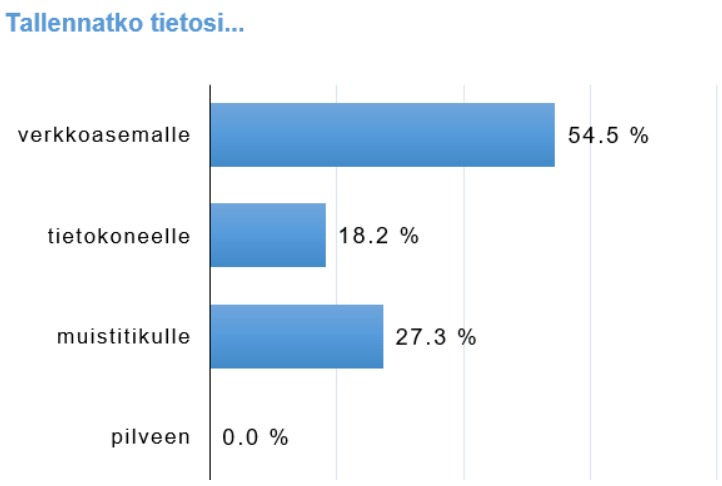
Tietoturvakoulutusta ei ole tarjottu millään toistuvalla kaavalla ja toive haastateltavien keskuudessa olikin sen lisäämisestä. Hyvä tietoturvataso koetaan tärkeäksi yksikössä ja haastateltavat olivat kiinnostuneita sen eri osa-alueista. Edellisestä koulutuksesta oli joko 2-10 vuotta aikaa tai vastaaja ei muistanut milloin viimeeksi tietoturvakoulutusta oli järjestetty.

Kysyttäessä tietoturvakoulutuksen lisäämisestä olivat vastaajat sen kannalla, mutta myös toivoivat tietoturvadokumentaation näyttelevän osaa heidän tietoturvaosaamisensa vahvistamisessa. Pyrimme ottamaan selvää mitä kautta henkilöstö mieluiten oppisi ja tapahtuisiko se ohjatusti vai itsenäisesti.

Tietoturvadokumentaatio koettiin vastanneiden keskuudessa tärkeäksi turvallisen työskentelyn kannalta. Sen sisällön yksityiskohdat vaihtelivat vastaajasta seuraavaan mutta liittyivät kunkin työtehtäviin. Toivoimme löytävämme yhteneviä kohtia henkilöstön tietoturvaosaamisen puutteissa.

Lisäksi verkkokoulutuksen ja -ohjeistuksen mahdollisuutta on kysytty. Tietoturvadokumentaatiota yksinään ei koeta täydelliseksi ratkaisuksi vaan toimivan kommunikaation ja ohjeistuksen sähköpostiliikenteen sekä intranetin välityksellä toivotaan olevan osa sitä.

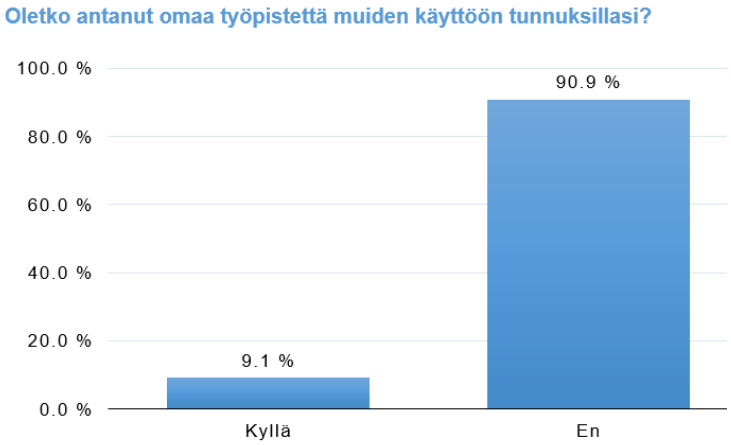
Vastaajista yli puolet kertoo tallentavansa tietonsa pääasiassa verkkoasemalle. Osa kuitenkin ilmoittaa käyttävänsä tallennusmuotona myös oman tietokoneen muistia sekä erillistä muistitikkua.
Nykyisin yhä enemmän suosiotaan kasvattava pilvipalvelu, kuten OneDriveen tallentaminen, ei ole vielä tavoittanut yksikön työntekijöitä, sillä kukaan vastaajista ei kertonut tallentavansa töitään pilveen.



Kuvio 3: Tietojen tallennus

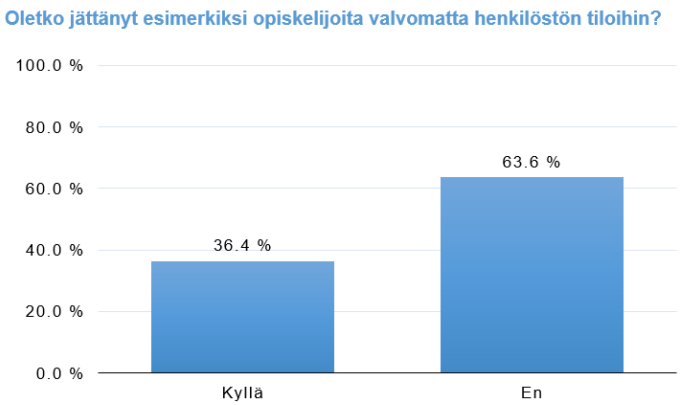
Tiedustelimme lisäksi työntekijöiden tietoturvallisista työskentelytavoista heidän omissa työhuoneissaan.

Kysyttäessä antavatko työntekijät ulkopuolisten käyttää konettaan omilla tunnuksillaan, vastaajista lähes jokainen kielsi antavansa konettaan muiden käyttöön. Vastaajamäärästä löytyi kuitenkin murto-osa sellaisia, jotka niin tekevät.



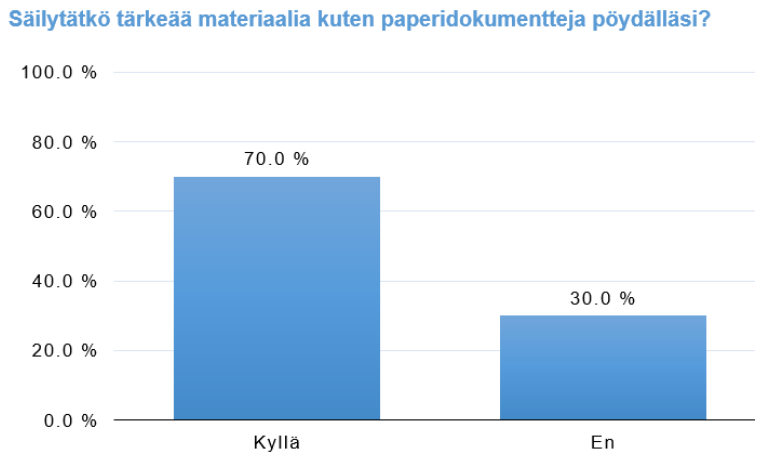
Kuvio 4: Työpisteen käyttö

Oman koneen käytön lisäksi tiedustelimme jättävätkö työntekijät ulkopuolisia henkilöitä valvomatta henkilöstön tiloihin.
Kysymys herätti vastaajissa lähes tasatuloksen molemmin puolin. Reilu kolmannes vastasi kysymykseemme ”Ei”, mutta reilu 36 % vastasi jättävänsä ulkopuolisia valvomatta eri henkilöstön käyttöön suunniteltuihin tiloihin.



Kuvio 5: Ulkopuolisten valvonta

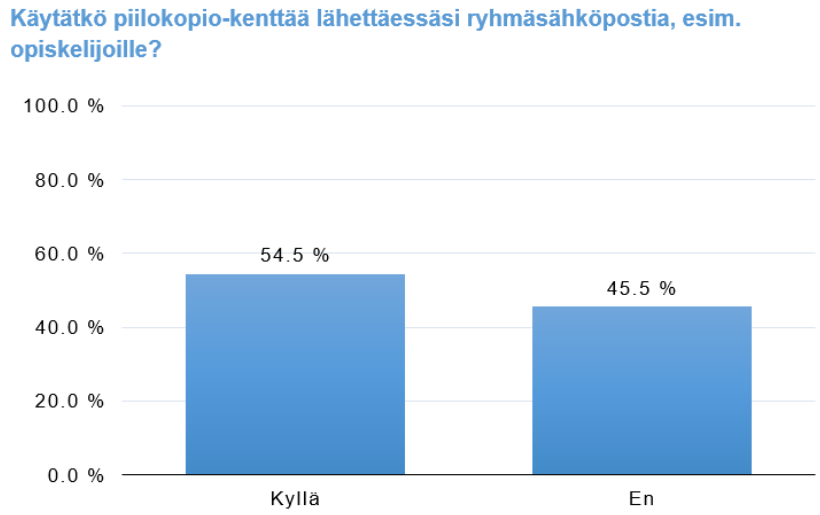
Työhuoneen toiminnasta tiedustelimme vielä työntekijän oman pöydän huolellisuudesta. Vastaajista peräti 70 % tunnusti säilyttävänsä työpöydällään luottamuksellista ja tärkeää materiaalia.



Kuvio 6: Tärkeiden dokumenttien säilytys

Halusimme kyselyssämme paneutua haastateltavien sähköpostikäyttäytymiseen, sillä se on puhelimen lisäksi olennaisin asiakasyrityksemme yhteydenpitokanava asiakkaisiinsa.

Tiedustelimme liitteiden käytöstä sähköpostissa ja jokainen vastaaja ilmoitti käyttävänsä niitä työskentelyssään. Lisäksi halusimme tietää sähköpostin piilokopio-kentän käytöstä ryhmäsähköposteissa. Koska kyseessä on oppilaitos, pitävät kouluttajat ja muu opetushenkilökunta yhteyttä opiskelijoiden usein ryhmäsähköposteilla.

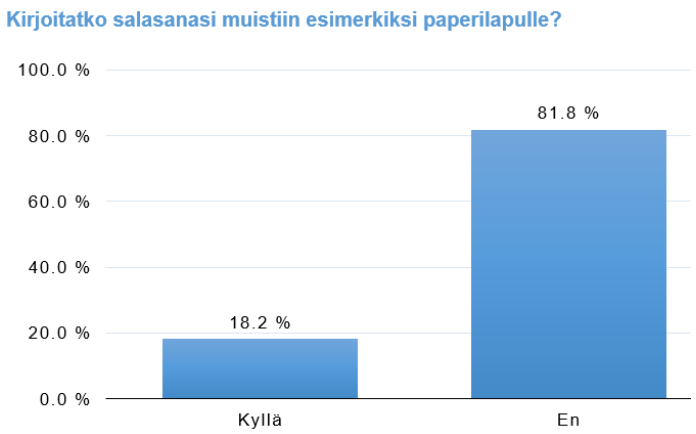


Kuvio 7: Piilokopion käyttö

Tämänkin kyselyn kanssa vastaukset jakaantuivat lähes tasan. Hieman yli puolet kuitenkin ilmoitti käyttävänsä ryhmäsähköposteissa hyödykseen piilokopiokenttää.

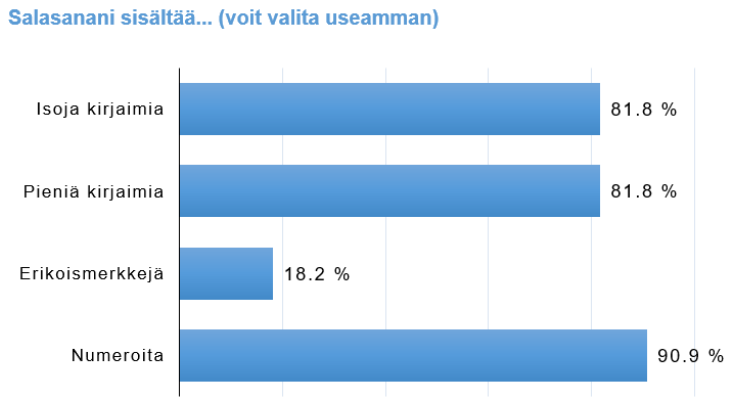
Sähköpostiin saattaa ilmaantua monenlaista roskapostia ja linkkejä eri haittaohjelmiin. Kyselyssämme pyysimme vastaajilta tietoa, onko heidän sähköpostiin ilmaantunut epäilyttäviä viestejä. Vastaajista reilu viidennes oli huomannut erinäköistä roskapostia työsähköpostissaan. Vastaajat yksilöivät viestien olevan erilaisia mainoksia tai epäilyttäviä kyselyjä lähinnä ulkomailta. Yksi oli havainnut roskapostissaan kyselyn pankilta, jonka asiakas hän ei edes ole. Seuraava kyselymme kokonaisuus liittyi salasanoihin. Aluksi kysyimme salasanojen vaihtamisen tiheydestä. Jokainen kertoi vaihtavansa salasanansa vain silloin, kun tietokone niin heiltä vaatii.

Kysyttäessä kirjoittavatko työntekijät salasanansa ylös esimerkiksi paperilapulle, vastasi yli 80% kielteisesti.



Kuvio 8: Salasanan kirjoittaminen ylös

Salasanan vaikeudesta sekä pituudesta kyselyssämme oli kaksi kysymystä. Halusimme kartoittaa hieman, kuinka hyvin työntekijät ovat tietoisia miten tärkeä vahva salasana on.

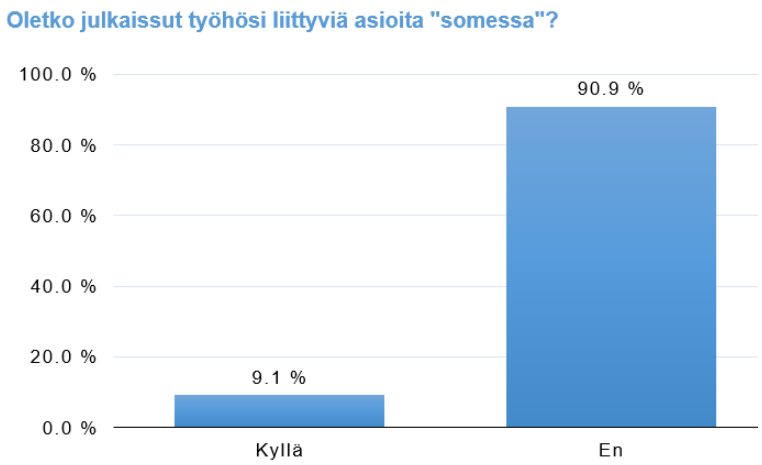


Kuvio 9: Salasanan vaikeus

Salasanoja vastanneet vaihtavat ainoastaan, kun saavat käyttöjärjestelmältä asiasta kehoitteen. Salasanat ovat yli kahdeksan merkkiä pitkiä ja yli 90 % tapauksista sisältävät pieniä sekä isoja kirjaimia numeroiden lisäksi. Erikoismerkkien käyttö on vähäistä mutta viidesosa vastanneista sisällyttävät muita merkkejä osaksi salasanojaan.

Viimeisenä kyselymme kokonaisuutena oli tiedustella työntekijöiden käyttäytymistä sosiaalisessa mediassa, sillä se oli yksi opinnäytetyöhömme valitsemistamme pääkohdista.

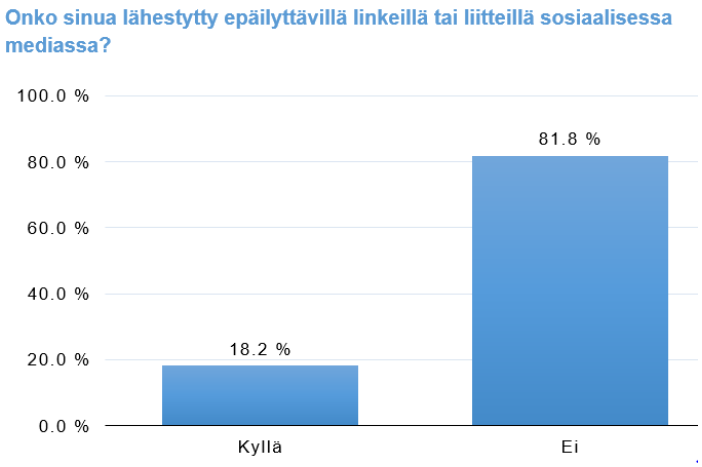
Aluksi kysyimme kertovatko työntekijät työhönsä liittyvistä asioista eri sosiaalisen median kanavissa.



Kuvio 10: Sosiaalinen media

Vajaat 10 % kertoi julkaisevansa työhönsä liittyvistä asioista eri sosiaalisen median kanavilla, mutta valtaosa kertoi jättävänsä työnsä ympärillä pyörivät asiat pois sieltä.

Kysyimme sähköpostiin tulleista epäilyttävistä linkeistä ja viesteistä. Halusimme tietää saman asian sosiaalisen median osalta.



Kuvio 11: Sosiaalisen median uhkakuvat

Reilua 18% vastaajista on lähestytty epäilyttävillä yhteydenotoilla. Tarkempien vastausten perusteella spesifioitiin epäilyttäviä ehdotuksia sekä ventovieraiden kaveripyyntöjä. Kyselymme löytyy kokonaisuudessaan opinnäytetyömme liitteistä.

5 VAHTI ja sen läpileikkaus

Pääviitekehyksenämme toimii Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmän (lyh. VAHTI) tietoturvaohjeet. VAHTI on Suomen valtiovarainministeriön asettama tietoturvallisuuden kaikkien osa-alueiden kehittämiseen tähtäävä elin. VAHTI-ohjeistusten hyödyntäminen on yleisön vapaassa käytössä ja niiden käyttö on tarkoitettu edistämää mm. kunnallishallinnon, elinkeinoelämän ja kansainvälisen yhteistyön tietoturvallisuutta.

Pystymme vertaamaan saatuja tuloksia faktatietoon. Aluksi esittelemme tarkemmin VAHTI-ohjeistuksen keskeisimmät piirteet. Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on Suomen valtiovarainministeriön asettama hallinnon tietoturvallisuuden kehittämiseen tähtäävä elin. Valtionhallinnossa on luotu VAHTI-tietoturvaohjeet, joita hyödynnetään valtionhallinnon lisäksi kunnallishallinnossa, elinkeinoelämässä ja kansainvälisessä tietoturvayhteistyössä. VAHTI:n mukaan tietoturvariskin suuruusluokka määräytyy sen mukaan, kuinka vakava riski on ja miten todennäköisenä sen toteutumista pidetään (VM 2016)

Tietoturvallisuuden kehittämistoimet on jaettu VAHTI:ssa seuraavaan kahdeksaan osa-alueeseen. Neljä ulointa kerrosta ovat hallinnollinen tietoturva, henkilöstöturvallisuus, fyysinen turvallisuus sekä tietoliikenneturvallisuus. Puolestaan neljä sisintä kerrosta ovat ohjelmistoturvallisuus, tietoaineistoturvallisuus, käyttöturvallisuus sekä laitteistoturvallisuus. (VM 2016)

Opinnäytetyömme kannalta kaikki osa-alueet eivät olennaisia, sillä pääpaino työssämme on henkilöstön osaaminen, joten esimiehille ja tietylle sidosryhmälle, kuten ylläpitäjille, ohjatut ohjeistukset jäävät vähemmälle huomiolle.

5.1 Hallinnollinen tietoturvallisuus

VAHTI-ohjeistus tarjoaa monipuolisen tarjonnan hallinnollisen tietoturvallisuuden perusohjeita työelämään ja työpaikalla tapahtuvaan toimintaan.
Oma yksityisyys on hyvä säilyttää työpaikalla. Kaikki henkilökohtainen sähköpostiviestintä kuuluu käydä vain omalla, työsähköpostiin täysin sitoutumattomalla, sähköpostin palvelutarjoajalla, kuten Hotmail tai GMail. Omia henkilökohtaisia tiedostoja ei pidä tarpeettomasti tallentaa työpaikan matkapuhelimeen, työasemaan tai palvelimelle. (VAHTI 2006)

Jos itse sattuu saamaan haltuunsa toisten viestejä, on olemassa vaitiolovelvollisuus niiden sisällöstä, eikä esimerkiksi käytäväpuheita saa lähteä leviämään.

Työpaikalla liikkumisessa kehoitetaan käyttämään kulunvalvontaa, eli mahdollisia kulkukortteja sekä kuvallisia henkilökortteja, jos sellaisia on yrityksessä käytössä. Ketään vierasta ei saa päästää tiloihin valvomatta heidän toimintaansa siellä. Mahdolliset vierailijat on hyvä vastaanottaa neuvottelutiloissa, jotta esimerkiksi omalle työpisteelle sattumalta jääneet arkaluontoiset, salassapidettävät asiakirjat eivät päädy väärien henkilöiden tarkkailtavaksi. (VAHTI 2006)

Omalla koneella tapahtuvaa toimintaa on myös hyvä harkita varoen. Tietohallinnolta saadut käyttäjätunnukset ja itsevalitsema salasana ovat ainoat suositellut kirjautumisvaihtoehdot työkoneelle. Mikäli koneelta poistuu edes hetkeksi, kuuluu kone asianmukaisesti lukita näppäinyhdistelmällä Ctrl+Alt+Del ja valita Lukitse tietokone. Mikäli työhuoneeseen ei jää poistuessa ketään, ovi täytyy muistaa lukita perässä. Kaikki tärkeä tieto pitää tallentaa sellaiselle verkkoasemalle, josta tietohallinto ottaa säännöllisesti varmuuskopiot. (VAHTI 2006) Nykyisin suosiossa on myös erinäiset pilvitallennusalustat, kuten OneDrive.

Työntekijän henkilökohtaista käyttäjätunnusta ja salasanaa ei saa luovuttaa eteenpäin kenellekään. Oma salasana onkin hyvä saada mahdollisimman vaikeaksi laittamalla siihen isoja sekä pieniä kirjaimia sekaisin, lisätä mukaan numeroita ja mahdollisesti erinäisiä erikoismerkkejä. Salasanan kuuluu olla lisäksi tarpeeksi pitkä. Oma salasana täytyy vaihtaa säännöllisin väliajoin, eikä sitä saa kirjoittaa muistiin esimerkiksi post it-lapulle, jota pitää kiinni työpöydällään tai näkyvästi seinällä. (VAHTI 2006)

Sähköpostin ja internetin käyttö on lähes jokaisessa työpaikassa nykyään rutiinia ja tärkeä osa jokaista työpäivää. Niiden käytössä vaaditaankin käyttäjältä erityistä huolellisuutta. Omalle työkoneelleen ei saa ladata mitä ohjelmia haluaa, vaan latausten täytyy tapahtua tietohallinnon hyväksynnästä.

Sähköpostiin saapuvia viestejä ei saa ohjata eteenpäin omalle siviilisähköpostilleen ja kaikki työasialiikenne kuuluu tapahtua organisaation sähköpostijärjestelmässä.
Sähköpostiin tulevat liitetiedostot saattavat sisältää haittaohjelmia, kuten troijalaisia tai viruksia. Siksi niiden avaamisen suhteen kuuluu olla varovainen, eikä epäilyttävästä lähteestä tulleita viestejä kuulu avata, vaan tuhota. Sama koskee saapuvaa roskapostia. Roskapostit saattavat pitää sisällään ”kalasteluviestejä”, joissa pyydetään lähettämään omia henkilökohtaisia tunnuksiaan. (VAHTI 2006)

Omaa työsähköpostia ei saa luovuttaa ulkopuolisille muuten kuin työhön liittyvissä asioissa. Mikäli työntekijän sähköpostiin tulee toiselle henkilölle kuuluva viesti, pitää se ohjata oikealle henkilölle ja ilmoittaa lähettäjälle oikean vastaanottajan osoite. Jos sitä ei ole tiedossa, pitää asiasta myös ilmoittaa lähettäjälle. (VAHTI 2006)

Jos lähettää massaviestiä useammalle vastaanottajalle kerralla, suositellaan käyttämään sähköpostin piilokopiokenttää. Näin estetään vastaanottajia näkemästä ketjukirjeiden saajien osoitteita.

Liikkuvassa työssä tai etätyössä kuuluu myös muistaa tietoturvalliset työskentelytavat. Etätyössä täytyy huolehtia, että käytössä olevat laitteet, ohjelmistot, dokumentit sekä käyttäjätunnus ja salasana pysyvät vain työntekijän hallussa. (VAHTI 2006)

Liikkuvassa työssä ei saa julkisella paikalla keskustella luottamuksellisista työasioista. Esimerkiksi junassa työskennellessä täytyy huolehtia, etteivät kanssamatkustajat pysty katsomaan tietokoneen ruudulla näkyviä tietoja. Julkisten päätteiden, kuten nettikahviloiden tai kirjastojen koneiden käyttöä ei suositella ollenkaan työasioiden hoitamiseen. (VAHTI 2006)

5.2 Ohjelmistoturvallisuus

Toinen hyvin tärkeä VAHTI-osa-alue opinnäytetyömme kannalta on ohjelmistoturvallisuus. Ohjelmistoturvallisuus kattaa sisällään erityisesti sosiaalisen median, jonka suosio on noussut viime vuosina valtavin harppauksin ja moni yritys käyttää sosiaalista mediaa yhteydenpitokanavanaan asiakkaisiin sekä mainosväylänä isoillekin ihmismassoille. Valtiovarainministeriön Sosiaalisen media tietoturvaohje kuvaa keskeisimmät sosiaalisen median palveluihin liittyvät tietoturvallisuusuhat sekä ohjeistaa organisaatioita mahdollisista ratkaisuvaihtoehdoista.(VAHTI 2006)

Sosiaalinen media ei itsessään tuo suurempia tietoturvahaasteita, mutta ihmisten käyttötavat siellä ovat niin erilaisia, että tietoturvauhat ilmenevät eri tavalla, kuin muissa medioissa. Yksityisen käyttäjän toimet saattava riskeerata organisaation tietoturvallisuuden itsessään. Vahingossa voi jokin arkaluotoinen dokumentti olla liitteenä päivityksessä, tai yksityinen työntekijä voi antaa oman mielipiteensä edustaen samalla koko organisaatiota.

Valtiovarainministeriön ”Sosiaalisen median tietoturvaohje” –dokumenteissa mainitaan, että ammattirikolliset yrittävät hyödyntää sosiaalisen median palveluita ja niiden kautta levitettäviä haittaohjelmia, jotka mahdollistavat esimerkiksi tietokoneen etähallinnan ja käyttämisen rikollisten haluamaan käyttötarkoitukseen. (VAHTI 2006)

Suurimpia uhkakuvia ovat eri tietoaineistoon liittyvät riskitekijät. Jo yllä mainitut vahingossa jaetut dokumentit ja tiedot ovat yksi ala-alue. Yleinen uskomus on, että kaikki julkaistu jää ”ikuisesti” verkkoon, vaikka virheen huomattuaan tiedoston poistaisikin. Tämän lisäksi käyttäjä saattaa esimerkiksi julkaisemassaan valokuvasaan palajstaa tahattomasti yrityksen luottamuksellisia tietoja. (VAHTI 2006)

Sosiaalisen median myötä yhdeksi suureksi uhkatekijäksi on noussut tietojen kalastelu. Yrityksen työntekijää saatetaan yrittää saamaan paljastamaan itsestään tai edustamastaan yrityksestä tietoja eri kyselyjen avulla. Henkilöstöä on ohjeisettu olla avaamatta eri epäiltyttäviä linkkejä sähköposteissa tai roskaposteja, mutta sosiaaliseen mediaan suhtaudutaan usein hieman rennommin. (VAHTI 2006)

Toinen suuri osa-alue on eri tekniset uhat. Nämä pitävät sisällään jo mainittujen sovellushaavoittuvuuksien lisäksi muut haittaohjelmat sekä roskapostit. (VAHTI 2006)

Sosiaalisessa mediassa haittaohjelmien levitys on helpompaa. Syitä on esimerkiksi ystävältä tai tutulta tullut viesti, joka voi vaikuttaa epäilyttävälle, mutta tutustua osoitteesta tultuna se koetaan kuitenkin turvallisemmaksi. Toinen tapa on linkittää jokin uutinen käyttäen hyödyksi jotain lyhytosoite-palvelua, kuten TinyURL. Käyttäjä klikkaa linkkiä ja haittaohjelma latautuu koneelle.

Ohjeistus ja koulutus ovat hyvin keskeisessä aasemassa sosiaalisen median käytön kehittyessä. Ohjeistuksessa on tehtävä selväksi se, missä määrin organisaation asioita saa käsitellä sosiaalisessa mediassa. Esimerkiksi organisaation yrityssalaisuuksia ei saa käsitellä millään tavalla. (VAHTI 2006) On eri asia kertoa olevansa työmatkalla ulkomailla, kuin osallistuvansa x-tarjouksella hankkeen toteutukseen.

6 Havaintoja oppilaitoksen yksikön tietoturvan tasosta

Olemme käyneet läpi kohteemme yksikön nykytilanteen tietoturvallisesta näkökulmasta hyödyntäen teettämäämme haastattelulomaketta. Olemme lisäksi syventyneet tarkemmin yrityksen omiin tietoturvaohjeisiin sekä VAHTI-ohjeiston työmme kannalta oleellisimpiin asianhaaroihin.

Seuraavaksi käymme läpi analysoiden huomaamiamme toimivia asioita, puutteelisia asioita sekä kehitysehdotuksia parantamaan tietoturvallista työskentelyä.

6.1 Hyvällä tasolla oleva tietoturvallisuus

Kun vertaamme VAHTI-ohjeistusta ja yrityksen tietoturvaohjeistusta, on huomattavissa monia tärkeitä yhteneväisyyksiä. Pääpaino yrityksen tietoturvaohjeissa on hallinnollisessa tietoturvallisuudessa ja ne onkin pääpiirteissään käsitelty läpi. Yrityksellä on olemassa laajempi kokonaisuus tietoturvaohjeista, joissa paneudutaan asioihin tarkemmin, mutta lisäksi on tarjolla tiivistelmä ohjeistuksesta.

Kaikki olennaisimmat tiedot ovat työntekijöiden saatavilla, kuten ohjeistuksia asiakkaiden kanssa käyttäytymiseen ja koneen kanssa oikeanlaiseen toimimiseen. Tietoturvaohjeistus esimerkiksi muistuttaa lukitsemaan koneen aina sen luota poistuessa. Lisäksi tietoturvaohjeistus kertoo yksityiskohtaiset ohjeet sähköpostin kanssa toimimiseen.

Yritys on tehnyt mielestämme täysin oikean ratkaisun rajaamalla työntekijöiden oikeuksia ladata eri ohjelmistoja omalle työkoneelleen. Yrityksellä on käytössään tietohallinnon julkaisukanava, josta voi halutessaan ladata esimerkiksi Google Chromen tai Mozilla Firefoxin selaimekseen. Lisäksi tarjolla on Officen eri työkaluja sekä muita mahdollisesti työntekoa hyödyntäviä ohjelmia.

Salasanat ovat tietoturvallisuuden eräs pääteemoista ja mielestämme olennaisimmista asioista. Salasanan on oltava vahva. Sen pitää olla yli 8 merkkiä pitkiä. Vahva salasana sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Huonoja salasanoja ovat esimerkiksi salasana, 12345678, 111111, qwerty ja 123123. (Heikkilä 2013)

Haastattelulomakkeen perusteella olikin erittäin hienoa huomata, kuinka kohteemme henkilökunta pääasiassa huolehtii salasanansa vahvuudesta. Noin 82% vastaajista ilmoittaa salasanansa sisältävän sekä pieniä ja isoja kirjaimia. Yli 90% vastaajista kertoo salasanan sisältävän lisäksi numeroita. Jokainen 11 vastaajasta vahvistaa salasanansa olevan yli kahdeksan merkkiä pitkä.

Haastateltavat kokevat tietoturvakoulutuksen tärkeäksi ja näkevät sen olevan hyvin olennainen osa työskentelyä nykypäivän työelämässä. Moni saattaa yhä suhtautua tietoturvallisuuteen hieman ylimalkaisesti, mutta oli hienoa huomata kyselymme perusteella, että näin ei ole kohdeyrityksessämme yksikössä.

Kuten Valtiovarainministeriön ” Sosiaalisen median tietoturvaohjeessa” todetaan, on yrityksen tehtävä työntekijöilleen selväksi se, missä määrin organisaation asioita saa käsitellä sosiaalisessa mediassa ja esimerkiksi yrityksen hallussa olevia salassa pidettäviä tietoja ja yritysalaisuuksia ei saa käsitellä sosiaalisessa mediassa millään tavalla. (VAHTI 2006) Siksi onkin hyvä, että sosiaalinen media ei näyttele sen suurempaa osaa vastanneiden arjessa, vain 9,1 %

ovat käyttäneet sosiaalista mediaa osana työskentelyään. Vastaavasti koetut uhkat somessa ovat jääneet vähäisiksi.

Kun kysyimme sähköpostiin liittyvän epäilyttävän sisällön esiintyvyyttä vastanneiden arjessa, 27,3 % ilmoitti kohdanneensa muun muassa phishing-yrityksiä sekä roskapostia. Vastaajat huomioivat kysyttäessä tämän vähentyneen runsaasti viime vuosina. Kukaan ei kuitenkaan ilmoittanut kokevansa epävarmuutta roskapostin kanssa, vaan ymmärtävät olla kiinnittämättä niihin sen suurempaa huomiota.

6.2 Kehityskohteet tietoturvallisuudessa

Yrityksen tietoturvaohjeistus on ehkä hieman vaikeasti löydettävissä. Yrityksen sisäisen verkon etusivulla olisi hyvä olla suora linkitys tietoturvaohjeistukseen. Tarjolla on kuitenkin linkkikirjasto, josta pääsee yhdellä painalluksella suoraan pohjapiirrustuksiin, parkkihallin koodeihin ja talon yleisiin järjestysääntöihin. Tietoturvaohjeistus on vähintäänkin yhtä olennainen asia olla saatavilla.

Vaikka yrityksen tietoturvaohjeistus on hyvin rakennettu pohjautuen VAHTI-dokumentteihin, on huolestuttavaa, että kovin moni kyselyymme vastaajista ei joko tiedä sen olemassaoloa tai konsultoi sitä työssään lainkaan. Lisäksi moni kyselyymme vastannut kokee, että ei ole saanut tarpeeksi tietoturvakoulutusta työpaikallaan.

Tietoturvaohjeistusta ei ole käytetty henkilöstön keskuudessa kovinkaan paljoa. Vastaajista puolet ovat tietoisia tietoturvaohjeistuksen olemassaolosta ja heistä vain yksi käyttää sitä kuukausittain. Suosittelisimme mahdollisten koulutustilaisuuksien ohessa henkilökunnalle esiteltäväksi ohjeistuksen.

Tietoturvasta tietämätön työntekijä on automaattisesti riskitekijä yrityksen toiminnan sujuvuudelle. Työntekijä saattaa vaarantaa tärkeitä liiketoimintasalaisuuksia lähettämällä liitteitä sähköpostitse, tai vaarantaa salassa pidettäviä asioita yksinkertaisesti suuntaamalla työhuoneensa näyttönsä väärään suuntaan.

Kyselyyn vastanneet kokevat tietoturvakoulutuksen tämän päivän työelämässä hyvin tärkeäksi, mutta eivät koe saavansa koulutusta tarpeeksi. Kohdeyrityksemme olisi hyvä miettiä erinäisten ”tietoturvatietoiskujen” tekemistä esimerksi yrityksen sisäisiin viestintäkanaviin tai järjestää pienimuotoisia tietoturvakoulutuksia, joissa muistutetaan työntekijöitä tietoturvallisuuden ohjenuorista.

Kahdella kolmesta vastanneesta on tapana säilyttää paperidokumentteja turvaamattomana työpisteillään. On valitettavaa, että asiakirjojen tietoturvallisessa säilyttämisessä on epäonnistuttu. Uskomme että kyseessä on koulutuspuute, aiheesta voisi kenties tehdä tulevan tietoturvadokumentaation lisäksi muistion jaettavaksi henkilöstölle.

Tiedostojen, tiedon ja muun datan käsittely sekä tallennus tapahtuvat suurelta osin asiakasyrityksen verkkoasemille. Vastanneista 54,5 % tallentavat tietonsa verkkoasemille talteen, mutta loput 45,5 % käyttää paikallista talletusta joista 27,3 % tapahtuu muistitikuille, loput tietokoneen omalle kiintolevylle. Lisäksi yksikään vastanneista ei ilmoittanut käyttävänsä pilvipalveluita tietojensa tallettamiseen.

Olisikin hyvä muistuttaa OneDriven ja vastaavien pilvipalvelujen hyödyllisyydestä. Pilvipalvelujen käyttäminen onkin hyvin ikäsidonnaista. Tilastokeskuksen vuonna 2014 teettämän tutkimuksen mukaan alle 35-vuotiasta peräti 40 % käyttää pilvipalveluja tallennusalustanaan, kun taas yli 50-vuotiasta pilvitallennusta hyödyntää vain noin kymmenes. (Tilastokeskus 2014) Kohdeyksikömme henkilökunta on lähes 100 % yli 40-vuotiaita, joten tutkimukseenkin perustuen heidän kokemuksensa pilvitallennuksesta on hyvin pientä.

Kysyimme myös henkilöstön sähköpostitottumuksista, jotka havaitsimme koulutusta kaipaaviksi. Ottaen huomioon pilvipalveluiden käytön puuttuvan kokonaan, 100 % vastanneista ilmoittaa käyttävänsä liitteitä sähköpostissaan on myös tietoturvan kannalta ongelma, johon tulisi puuttua. Tietojen eheyttä asiakasyrityksessä ei välttämättä koeta osaksi samaa tietoturvakokonaisuutta, kuten virustorjunta tai palomuurit.

7 Ehdotuksia parantamaan tietoturvallista työskentelyä

Teettämässämme kyselyssä noin neljännes vastaajista myöntää kirjoittavansa salasanansa ylös paperille. Vahva salasana on pakollinen, mutta sen kuuluu olla myös sellainen, joka on muistettavissa ilman, että sen paljastuminen muille vaarantuu. Yksi suositus on, että käyttäjän salasana pitää sisällään jonkin käyttäjälle merkityksellisen tarinan, jotta salasanan myös helposti muistaa. (Jacobson & Idziorek 2013, 77)

Tarinan luomiseen annetaan ohjeeksi aloittaa salasana jollakin itselle merkityksellisellä sanalla, kuten lempipaikka tai suosikkiartisti. Tämän perään on hyvä laittaa numerosarja, kuten esimerkiksi Bon Jovin keikan vuosi. Lisäksi osan sanasta voi korvata erikoismerkeillä. (Jacobson & Idziorek 2013, 77) Esimerkkinä hyvästä ja toimivasta salasanasta voidaan pitää ”B0nJov12012”.

Vaikka moni vastaajista ilmoitti salasanansa olevan monipuolinen, on hyvä muistaa myös sääntöjä siitä, millainen on kehno salasana. Muiden esimerkeissä olevaa salasanaa ei saa ottaa

omaan käyttöönsä. Eli yllä mainittua esimerkkiä ei sen vahvuudesta huolimatta saa käyttää, koska se on ollut julkisessa dokumentissa esillä. Salasana ei saa olla helposti arvattavissa olevaa henkilökohtaista informaatiota, kuten oma nimi + syntymäaika. Salasana ei lisäksi saa olla näppäimistön merkkejä peräjälkeen. Esimerkkinä ”asdfg12345” on kovin helposti aavistettavissa mahdolliselle tunkeutujalle. (Jacobson & Idziorek 2013, 80)

Perinteinen yrityksen tietoturvaopas ei ole enää välttämättä paras tapa viedä tietoturvaosaamista eteenpäin. Työntekijät eivät jaksa tai heillä ei ole aikaa selata läpi useamman kymmenen sivun tietoturvaoppaita. Lisäksi niiden pituudet saattavat vain jatkossa kasvaa tietouden eri uhkista laajentuessa. Mielestämme tietoturvakoulutuksessa voisi hyvin hyödyntää yrityksen sosiaalisia kanavia, kuten intranettiä, Tietotekniikka on uhka, mutta se saattaa olla myös ratkaisu. (Lacey 2009, 26)

Moni kyselyyn vastanneista toivoo lisää tietoturvakoulutusta. Yrityksen olisikin hyvä koulutuksia järjestää, mutta kuunnella työntekijöidensä sisältötoiveita, jotta pysytään arkisen työskentelyn olennaisimmissa asioissa. Kyselyn perusteella toivottuja sisältöjä on juurikin arkipäiväisen työskentelyn nitoutuvia asioita. Esimerkiksi puhelimen kanssa työskentely on kasvanut vuosien mittaan ja sen kanssa toimimiseen toivotaan ohjeita. Lisäksi etäkäyttö, kannettavien kanssa työskentely ja eri opiskelijoihin liittyvät tietosuoja-asiat keräävät kannatusta. Tietosuoja-asioista pohdintaa herätti erityisesti tieto siitä, että mitä saa kertoa ja kenelle saa kertoa.

Pilvipalvelujen nykypäiväisyydestä on tärkeää muistuttaa työntekijöitä, sillä kukaan kyselyymme vastaajista ei ilmoittanut sitä käyttävänsä tallennusvälineenä. Pilvipalveluiden suurena etuna on se, että ”pilveen” tallennetun aineiston käyttö ovat yksittäisestä laitteesta riippumatonta ja työpaikallaan tehtyyn asiakirjaan pääsee käsiksi myöhemmin, vaikka kotikoneeltaan. (Tilastokeskus 2014)

Sähköpostin käyttöä tulee tarkentaa. Vain hieman yli puolet kyselyymme vastaajista ilmoitti käyttävänsä sitä ryhmäsähköpostien kanssa. Oppilaitoksen ja suurien opiskelijamäärien kanssa toimiessa onkin työntekijän hyvä käyttää piilokopiota viestiessään isoille ryhmille, sillä vastaanottajien ei tarvitse saada tietoonsa muiden henkilöiden sähköpostiosoitteita. Ohjeistuksessa onkin hyvä muistuttaa työntekijöille piilokopiokentän olemassaolosta ja kuinka sen saa käyttöönsä, jos ei ole asiasta tietoinen.

Tietoturvallista näkökulmasta katsottuna työntekijöiden ehkä hieman huolettomaan käyttäytymiseen tuohuoneensa kanssa olisi hyvä puuttua. Sekä yrityksen oma tietoturvaohjeistus sekä VAHTI-ohje ohjeistavat, että työhuoneeseen ei saa päästää valvomatta ulkopuolisia henkilöitä. Kyselyymme vastanneista yli 36 prosenttia kertoi jättäneensä ulkopuolisia valvomatta

henkilöstön tiloihin, joka on auttamatta liian suuri määrä. Työntekijät toivoivat kyselyssä tietoturvan perusteiden muistutusta ja mielestämme työhuonetoiminta on yksi tulevan tietoturvadokumenttiimme nostettavista olennaisista asioista.

8 Koulutus

On edullista tietoturvadokumentin sisäistämiselle kohdeyrityksen henkilökunnan keskuudessa, että tutustumme koulutukseen liittyviin seikkoihin, kuten aikuispedagogiikan suosituksiin sekä toimintatapoihin kirjoitetun aineiston oppimisen kannalta ja hyödynnämme näitä oppeja tietoturvadokumentin luomisessa. Käymme läpi koulutuksen suunnittelua, toteutusta, materiaaleja sekä lopputuloksen arviointia. Uskomme aiheen olevan yleishyödyllinen tietoturvadokumentin luomisen kannalta sekä kriittinen sen sisällön esittelyssä kohdeyrityksen henkilöstölle.

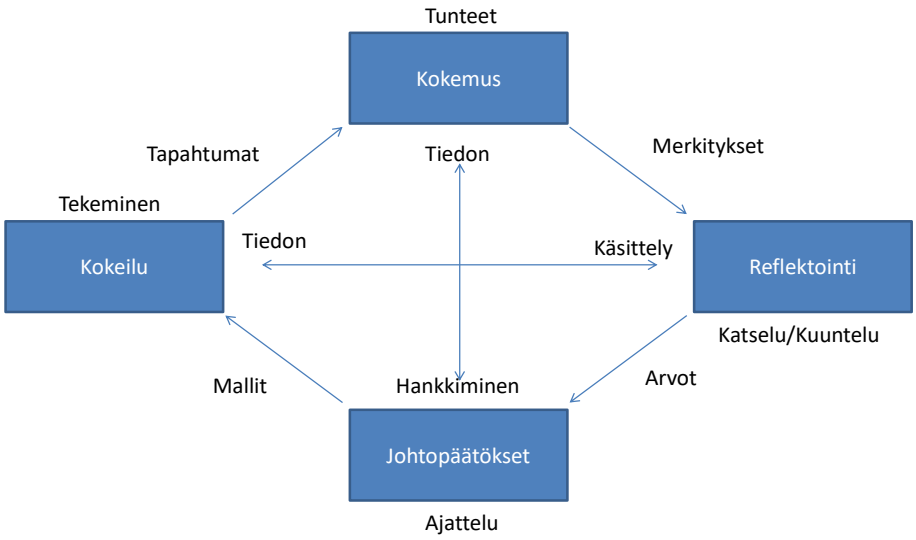
Parhaimpienkin tietoturvakäytäntöjen epäonnistumisessa on kyse ihmistekijästä. Ohjeistusten noudattamatta jättäminen, huolimattomuus uhkien tiedostamisessa, liika luotto teknisiin ratkaisuihin sekä vastuun sysääminen muualle ovat tyypillisiä esimerkkejä tilanteista, joissa koulutuksen puute näkyy. Lisäksi vaarana on koulutuksen kattavuuden pettäminen, kuten kausiapulaisten, vuokratyöläisten, alihankkijoiden ym. sidosryhmien jättäminen tietoturvakoulutuksen ulkopuolelle.

8.1 Oppimisprosessi

Käyttämässämme materiaalissa todetaan aikuisen oppimisen olevan laadultaan kokemusperäistä. Tämä tarkoittaa uuden tiedon kannalta valikoivaa oppimista. Jos uusi tieto on aiemman kokemuksemme perusteella merkityksellistä, sen voi sisäistää. Kun lähdemme tarjoamaan uutta tietoa kohdeyrityksen henkilöstölle, on tämä pidettävä mielessä. Yleisöllämme siis on jo entuudestaan vanhaa tietoa, jonka pohjalta he tekevät niin tietoisesti, kuin tiedostomattomasti arvioita uudesta tiedosta ja tämä vaikuttaa suuresti koulutuksen onnistumiseen.

Uudet tietoturvakäytänteet vaativat henkilöstöltä uuden tiedon omaksumisen lisäksi kykyä oppia uusia asenteita parempaa tietoturvaa ajatellen. Tällainen muutos vaatii oppijalta heidän tunne- ja arvomaailmojensa uudelleenarviointia, sillä parempien tietoturvakäytäteiden oppiminen on suurelta osin oikeiden toimintatapojen ja asenteiden omaksumista.

Käytämme tätä kuvastamaan David Kolbin kehittämää ja laajalti kokemuksellisen oppimisen piirissä käytettyä kehämallia jossa tämän oppimisprosessin vuorovaikutussuhteet käyvät ilmi.



Kuvio 12: Kehämalli

Jo hankitun kokemuksen ja toiminnan aiheuttamien tunteiden myötä oppija antaa merkityksiä uudelle tiedolle. Oppijan arvomaailma vaikuttaa uusien toimintamallien kehittymiseen valikoimalla siihen sopivammat muutokset. Tämä johtaa joko onnistuneeseen tai epäonnistuneeseen oppimisprosessiin, jossa kouluttajan tulee toiminnallaan edesauttaa oikean tiedon sekä asenteiden omaksumista. (Laine & Malinen 2009)

Aikuinen oppija on kokonaisuus oppimiskykyä, vuorovaikutustaitoja ja ennen kaikkea aiempaa elämänkokemusta, johon kaikki uusi pohjautuu. Ihminen säilyttää kyvyn oppia läpi koko elämänsä, mutta iän myötä valikoi tarkemmin uutta tietoa.

8.2 Työssä oppiminen

Jotta voimme toimittaa eheän ja toimivan uuden tietoturvadokumentaation asiakasyrityksen henkilöstölle, on tarpeellista tutustua myös tiedonvälitykseen koulutuksen muodossa. Keskitymme etenkin hyvien koulutusmateriaalien ja -aineistojen vaatimuksiin sekä muihin seikkoihin.

VAHTI-aineisto opastaa omia koulutus- ja ohjeaineistoja luodessa kiinnittämään huomiota viiteen seikkaan: tietosisältöön, helppolukuisuuteen, ymmärrettävyyteen, kirjoitustyyliin sekä ohjeen kykyyn herättää ajatuksia lukijassaan. Koulutusmateriaalin tulee tukea koulutuksen päämääriä.

9 Tietoturvadokumentin tekeminen

Aloitimme koostamaan tietoturvadokumenttia havaintojemme sekä VAHTI-ohjeistuksen pohjalta. Asiakasyrityksen henkilöstöltä saatujen vastausten perusteella saimme hahmotettua hyvän ja vakaan pohjan tietoturvadokumentillemme. Annoimme sille nimeksi Henkilöstön tietoturvadokumentti (HeTi).

Henkilöstön tietoturvadokumentin on tarkoitus muistuttaa kohdeyksikkömme työntekijöitä tietoturvan tärkeydestä sekä antaa pieniä käytännön ohjeita arkipäiväiseen, tietoturvalliseen, työskentelyyn. Päätimme pitää oppaan sisällön hyvin yksinkertaisena, jotta sitä tarkastelevan henkilön on helppo omaksua siinä olevat vinkit omaan työskentelyynsä.

9.1 Aiheiden valinta ja dokumentin suunnittelu

Aiheet valikoituivat HeTi-ohjeistukseen pääasiassa tuotetun kyselyn tulosten perusteella. Saimme siitä hyvää tietoa asioista, jotka ovat hieman epäselviä kohdeyrityksen yksikön työntekijöille. Lisäksi päätimme kerrata tietoturvallisuuden perusasioita dokumentissamme, sillä niiden kanssa työntekijät toimivat päivittäin ja voivat kätevästi konsultoida HeTi-ohjeistusta.

Henkilöstön Tietoturvadokumentti on osoitettu aikuisille, ja aikuisoppijat ovat erilaisia, kuin lapset, joten materiaalin työstö vaatii paneutumistaan kohderyhmäämme. Kuten aiemmin kirjoitimme, yksikön työntekijoillä siis on entuudestaan vanhaa tietoa jonka pohjalta he tekevät niin tietoisesti kuin tiedostomattomasti arvioita uudesta tiedosta ja tämä vaikuttaa suuresti koulutuksen onnistumiseen.

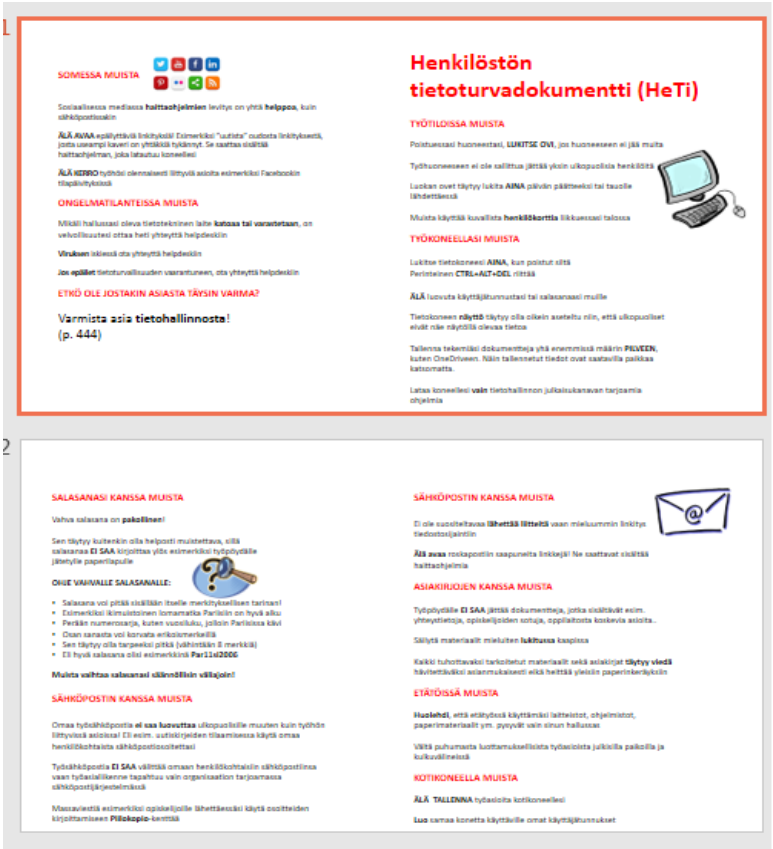
Mo Hamza toteaa kirjassaan Developing Training Material Guide, että aikuisoppija oppii parhaiten, kun uusi oppi heijastuu jo entuudesta tuttuun asiaan sekä opittava asia on merkityksellistä heille. (Swedish Civil Contingencies Agency 2012). Näin ollen voimme palata takaisin kyselyymme ja siitä saatuihin toiveisiin ja tuloksiin. Saatoimme huomata, miten tietoturvallisuudesta kaivataan uutta infoa ja kyselyyn vastaajilla oli entuudestaan pienimuotoinen pohja tietoturvatietoudelle.

Päätimme luoda loogisen ja ytimekkään kokonaisuuden, eräänlaisen tietoiskutyyppisen. Nykyinen koko talon tietoturvaohjeistus on laaja kokonaisuus, mutta omamme kohdalle halusimme panostaa tiiviiseen pakettiin, sillä kiireisessä arjessa sitä ei ole aikaa selata pitkiä aikoja. Aiheet pyrimme lajittelemaan punaiseksi langaksi.

Halusimme heti etusivulle laittaa työhuonetoiminnan ohjeistuksia, kuten muistutus oman työaseman lukitsemista poistuessa ja ulkopuolisten henkilöiden kanssa toimimisesta, jotka molemmat löytyvät sekä yrityksen tietoturvaohjeessa, että yleisissä VAHTI-ohjeissa. Valtaosa yrityksen toiminnasta tapahtuu joku työhuoneessa tai luokkatilassa, joten rajasimme asian yhdeksi pääkohdista.

Toinen asia, joka dokumentin etusivulle päätyi, oli toiminta omalla tietokoneellaan. Yksikön työntekijöiden peruspäivä pyörii paljon luokkatilojen lisäksi tietokoneella työskentelystä tehden esimerkiksi eri opiskelumateriaaleja, joten sen lisääminen mukaan heti aluksi oli luonnollinen jatkumo työhuoneen ohjeiden lisäksi.

Salasanat vaikuttivat kyselymme perusteella olevan hyvällä tasolla, mutta mielestämme vahvan salasanan tärkeyttä ei voi liikaa korostaa, joten nostimme salasanatkin mukaan tietoturvadokumenttiimme. Kirjasimme mukaan yksinkertaisen, mutta hyvin tehokkaan, ohjeen vahvan salasanan luomiseksi.



Kuvio 13: HeTi-dokumentti

Sähköpostitoiminnan suhteen toimme esiin muistutuksia, kuten piilokopio-kentän käyttö ryhmäsähköposteissa, liitteiden kanssa toiminta sekä roskapostin avaamiseen liittyviä varoituksia.

Lisäksi kysyimme asiakirjojen hallinnasta, ja tästäkin asiasta kirjoitimme mukaan ohjeistuksia. Mukaan mahtui pienet kohdat etätyöskentelyn ohjeista ja kotikoneella toimimisesta. Moni asiakasyrityksemme työntekijä tekee töitä paljon myös etänä, joten sekin asia oli hyvä nostaa esiin.

Sosiaalisesta mediasta kysyimme haastatteluvaiheessa ja nostimme sen alun perin yhdeksi pääkohdaksi työhömme, joten some oli mielestämme hyvä lisä dokumenttimme loppuun. Viimeiseksi lisäsimme mukaan vielä ohjeet ongelmatilanteita varten.

Henkilöstön Tietoturvadokumentti löytyy opinnäytetyömme liitteistä.

9.2 Käyttötarkoitus

Henkilöstön Tietoturvadokumentti on luotu ennen kaikkea auttamaan yksikön henkilöstöä arkipäiväisessä toiminnassa, jotta se olisi mahdollisimman tietoturvallista. HeTi:n tarkoitus on olla tiivis infopaketti kaikkein yleisimmistä asioista.

Toiveenamme on, että Henkilöstön Tietoturvadokumentista on yksiköllemme hyötyä työskentelytavojen kehittämisessä aina yhä tietoturvallisempaan suuntaan. Koemme tiiviin tietopaketin olevan erittäin hyvä konsultaation kohde, jos henkilölle tulee edes pieniä pohdintoja oman työskentelynsä turvallisuudesta.

9.3 Vastaanotto yksikössä

Henkiöstön Tietoturvadokumentti jaettiin yksikön työntekijöille. He saivat aikaa tutustua siihen, jonka jälkeen kysyimme mielipiteitä työmme tuloksesta ja mielipiteiden perusteella valmistauduimme sitä vielä muokkaamaan.

Vastaanotto yksikössä oli hyvin positiivinen. Uusi tietoturvadokumentaatio sai kiitoksia kattavuudestaan, eheydestään ja helppokäyttöisyydestään. Tietoturvadokumentaation sisältämä uusi tieto omaksuttiin helposti. Työmme koettiin sopivan tiiviiksi tietopaketiksi, jossa oli mukana kaikki työn kannalta olennainen asia.

Alkuperäinen versiomme Henkilökunnon Tietoturvadokumentista keräsi ulkoasumoitteita. Jokainen ohjeemme päättyi huutomerkkiin, joka koettiin "pomottavana”, joten päädyimme poistamaan ne lähes kokonaan lopulliseen versioon.

Sisältömuutoksia emme enää tehneet ja HeTi otettiin käyttöön pienen ulkoasuun tehdyn muokkauksen jälkeen.

10 Yhteenveto ja pohdintoja

Tietoturvallisuus on minkä tahansa liiketoiminnan jatkuvuuden kannalta keskinäinen elementti. Siihen on panostettu valtava määrä tutkimusta, käytännön työtä, ohjeistusten laatimista sekä muuta tietotaitoa. Tämän työn tuloksena syntyneet standardit ja hyvät käytänteet ovat osaltaan turvaamassa asiakasyrityksen tietoturvallisuutta, mutta tämä tavoite ei voi täyttyä, ellei henkilöstö ole motivoitunutta sitä ylläpitämään. Ongelma tietoturvallisuudessa nykyään ei ole tekniset ratkaisut, kilpavarustelu lain ja rikollisten välillä, vaan jokaisen asenteet sitä kohtaan.

Vaikka suurin osa työyhteisöstä olisi osaltaan motivoitunut, valveutunut sekä koulutettu toimimaan oikein on tämän kettingin murruttava vain yhestä kohtaa, jotta vahinko pääsee tapahtumaan. Uskomme työmme korostaneen hyvälaatuisen koulutuksen merkitystä tietoturvallisuuden takaamisessa. Koulutuksen hyödyt mittaamattoman arvokkaat. Tämä on fakta, joka myönnetään usein vasta liian myöhään.

Työstä on hyötyä asiakasyritykselle. Olemme kartoittaneet yrityksen toimintaa haastattelemalla henkilökuntaa kysymyksillä, jotka vetosivat heidän arvomaailmaansa ja tähän pohjautuen olemme koonneet Henkilöstön Tietoturvadokumentaation selventämään, ohjaamaan sekä neuvomaan tilanteissa, jotka nousivat esille.

Koemme onnistuneemme tavoitteessamme auttaa asiakasyritystä kohtaamaan tietoturvallisen työskentelyn haasteet saamamme palautteen perusteella. Työstämämme Henkilöstön Tietoturvadokumentti koettiin positiivisena asiana ja uskomme sen johtavan työntekijöiden työskentelytapojen parantumiseen.

Yksikön henkilöstöllä on käytössään uusi dokumentti, uudet opit ja he voivat soveltaa HeTi:n avulla tietoturvallisen työskentelyn käytänteitä. Tietoturvallisen työskentelyn käytännöt on hyvä ottaa osaksi jokapäiväistä työskentelyä oppilaitoksen kaikissa yksiköissä. Tämä onnistuu parhaiten järjestämällä koulutustilaisuuksia ja ottamalla tietoturvadokumentaatio osaksi perehdytysmateriaalia.

Lähteet

Jacobson, D. & Idziorek, J. 2013. Computer Security Literacy: Staying Safe in a Digital World. Boca Raton: CRC Press

Lacey, D. 2009. Managing the Human Factor in Information Security: How to win over staff and influence business managers. Chichester: John Wiley & Sons Ltd

Laine, T.& Malinen, A (toim.) 2009. Elävä peilisali : aikuista pedagogiikkaa oppimassa. Helsinki: Kansanvalistusseura.

Asiakasyrityksen kertomus 2016. Viitattu 5.11.2016.

Heikkilä, M. Tekniikka & Talous 26.9.2013. http://www.tekniikkatalous.fi/tekniikka/ict/2013-09-26/10-tietoturvavinkki%C3%A4-pk-yrityksille-3315410.html

Swedish Civil Contingencies Agency 2012. Viitattu 16.11.2016. https://www.msb.se/RibData/Filer/pdf/26433.pdf s19

Tilastokeskus 6.11.2014. Viitattu 13.11.2016. http://www.stat.fi/til/sutivi/2014/sutivi_2014_2014-11-06_kat_002_fi.html

Suomen Valtiovarainministeriö. Viitattu 13.11.2016. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp

VAHTI 2006. Viitattu 5.11.2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c338d07d-ac04-4884-b941-1554d07ae41f&groupId=10229

Y-Lehti 2010. Viitattu 13.11.2016. http://www.y-lehti.fi/arkisto/artikkeli/3192/Tietoturvasta+huolehtiminen+on+elinehto

Kuviot

Liitteet

Liite 1 : Tietoturvallisuuden kysely kokonaisuudessaan

Oletko tietoinen yrityksen tietoturvaohjeista?

- En ole tietoinen (Kaikki)
- Periaatteessa käytännöt on tiedossa yleisellä tasolla ainakin:-) (Kaikki)
- Kyllä olen, sitä ollaan päivitetty viime aikoina. (Kaikki)
- Joksenkin tietoinen. (Kaikki)
- Suurin piirtein (Kaikki)
- Pääpiirteittäin kyllä (Kaikki)
- en (Kaikki)
- En (Kaikki)
- en täysin (Kaikki)
- Osittain. Kertaus ja tarkennus olisi tarpeen. (Kaikki)
- Kyllä olen. (Kaikki)

Kuinka usein konsultoit tietoturvaohjeistusta?

- En ole ollut tietoinen siitä, joten en lainkaan (Kaikki)
- ajoittain, tarvittaessa, vuosittain (Kaikki)
- Harvoin. (Kaikki)
- Näyttöjen yhteydessä; harvoin. (Kaikki)
- En koskaan (Kaikki)
- n. kerran 2:ssa viikossa (Kaikki)
- ? (Kaikki)
- Ei ole kokemusta (Kaikki)
- en konsultoi (Kaikki)
- N. 2-3 kertaa 1/2 vuoden aikana. (Kaikki)
- Harvoin. (Kaikki)

Milloin olet viimeeksi huomannut muutoksia tietoturvaohjeistuksessa?

- - (Kaikki)
- intran ilmoitukset, yhteiset viestit (Kaikki)
- Siitä on kyllä aikaa... (Kaikki)
- En osaa sanoa. (Kaikki)
- En muista (Kaikki)
- Hmmm. viime syksynä (Kaikki)
- Office 365 kouluryksessa (Kaikki)
- En ole tietoinen (Kaikki)
- en ole huomannut (Kaikki)
- En ole huomannu. (Kaikki)
- En muista. (Kaikki)

Oletko saanut tietoturvakoulutusta?

- Sen mitä sisäisessä intrassamme on ollut uutisia (Kaikki)
- perehdytyksen yhteydessä (?) (Kaikki)
- Kyllä. (Kaikki)
- En muistaakseni. Tiedotteita on tullut joskus asiasta. (Kaikki)
- Kyllä, päivän koulutuksen (Kaikki)
- En (Kaikki)
- kyllä (Kaikki)
- En (Kaikki)
- hyvin vähän (Kaikki)
- Kyllä. (Kaikki)
- Olen aikaisemmissa paikoissa. (Kaikki)

Jos olet saanut tietoturvakoulutusta, milloin tämä on tapahtunut?

- Satunnaisia pätkiä vuosien varrella. Varsinaista koulutuspäivää en ole saanut. (Kaikki)
- vuosia sitten...? (Kaikki)
- kaksi vuotta sitten, ehkä (Kaikki)

- En muista/osaa sanoa. (Kaikki)
- Ehkä viisi vuotta sitten? (Kaikki)
- Kts. edellä (Kaikki)
- 2005 (Kaikki)
- N. Pari vuotta sitten. (Kaikki)
- Noin. 10 vuotta sitten. (Kaikki)

Koetko tietoturvakoulutuksen tärkeäksi?

- Kyllä, olemme tekemisissä ison opiskelijamäärän kanssa, joten tietous siitä on tärkeää. (Kaikki)
- toki:-) (Kaikki)
- Kyllä (Kaikki)
- Kyllä, erittäin tärkeäksi. (Kaikki)
- Melko, en kovin (Kaikki)
- Erittäin tärkeä asia tänäpäivänä (Kaikki)
- kyllä (Kaikki)
- Kyllä (Kaikki)
- kyllä (Kaikki)
- Kyllä. (Kaikki)
- Kyllä. (Kaikki)

Toivoisitko lisää tietoturvakoulutusta?

- "Uutiset" ovat kiireisessä työssämme mielestäni riittävä koulutus. Ohjeistus olisi hyvä olla (Kaikki)
- kertaus on opintojen äiti - voisi olla esim verkkokoulutus..? (Kaikki)
- Kyllä ja yleistä turvallisuuskoulutusta on työsuojelutoimikunnassa suunniteltukin (Kaikki)
- Kyllä toivoisin. (Kaikki)
- En oikeastaan (Kaikki)
- Kyllä (Kaikki)

- en (Kaikki)
- Kyllä (Kaikki)
- kyllä (Kaikki)
- Kyllä. (Kaikki)
- Kyllä. (Kaikki)

Koetko tietoturvaohjeistuksen tärkeäksi oman työsi kannalta?

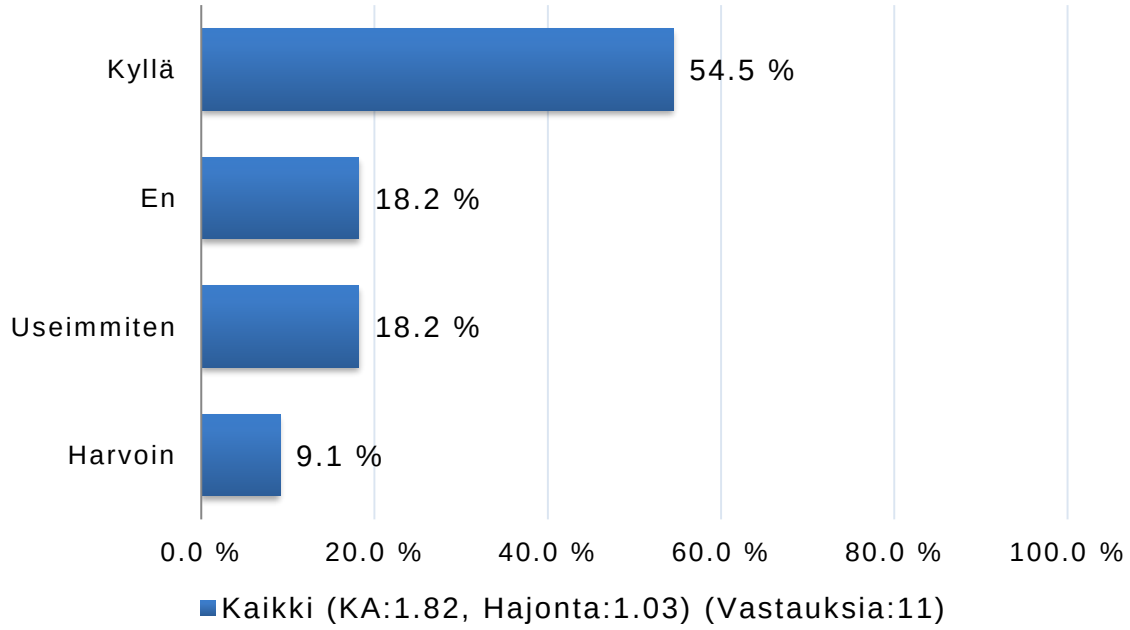
- Kyllä siitä olisi hyötyä. (Kaikki)
- ilman muuta! (Kaikki)
- Kyllä (Kaikki)
- Ehdottomasti koen tärkeäksi. (Kaikki)
- En kovin (Kaikki)
- Kyllä (Kaikki)
- en (Kaikki)
- Kyllä (Kaikki)
- kyllä (Kaikki)
- Kyllä. (Kaikki)
- Kyllä. (Kaikki)

Mihin seikkoihin toivoisit uuden ohjeistuksen kiinnittävän huomiota?

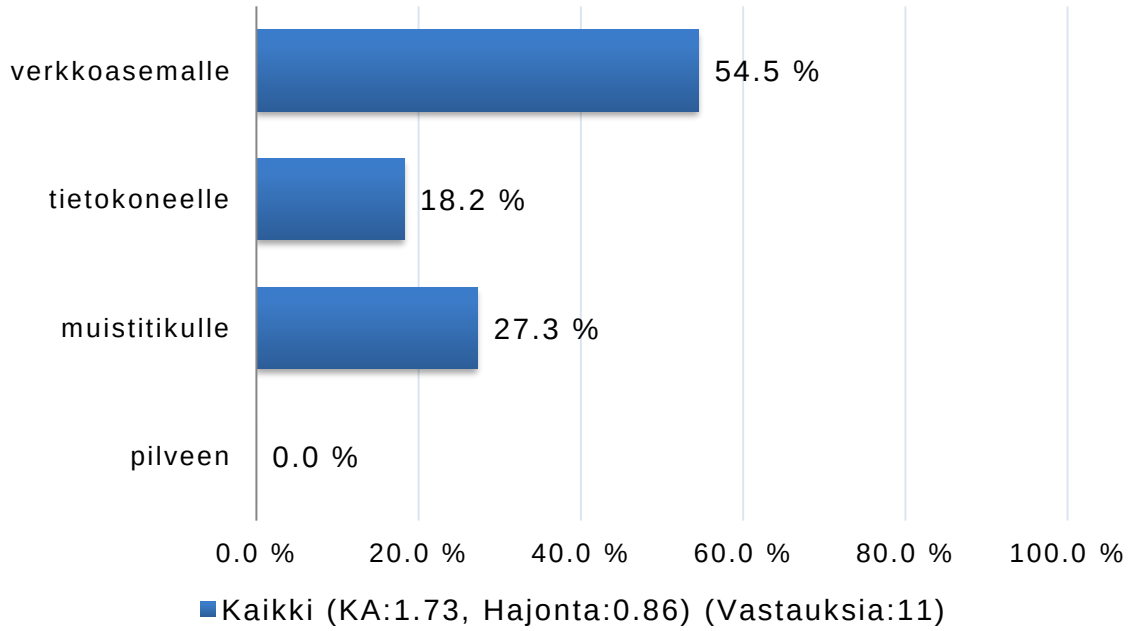
- Perinteisiin asioihin, jokapäiväisen työskentelyn ympärillä keskittyvää (Kaikki)
- päivettyihin tietoihin, uusimpiin asioihin (Kaikki)
- Arkipäivän asioihin, esim. puhelimen kautta toimimme nykyään paljon (Kaikki)
- Kannettavat koneet, etäkäyttö, ylipäätään ohjeiden päivitys ja tiedotus. (Kaikki)
- En osaa sanoa (Kaikki)
- kouluttajan ja opiskelijan henkilötietoihin ja arviointiin liittyvät seikat (Kaikki)
- asiakirjojen säilytykseen (Kaikki)
- opiskelijoiden tietoturva (Kaikki)
- Varsinkin tietosuoja-asioihin. Mitä saa kertoa, mitä saa tietoja laittaa esim. studentaan. (Kaikki)

Monivalintakysymyksiä

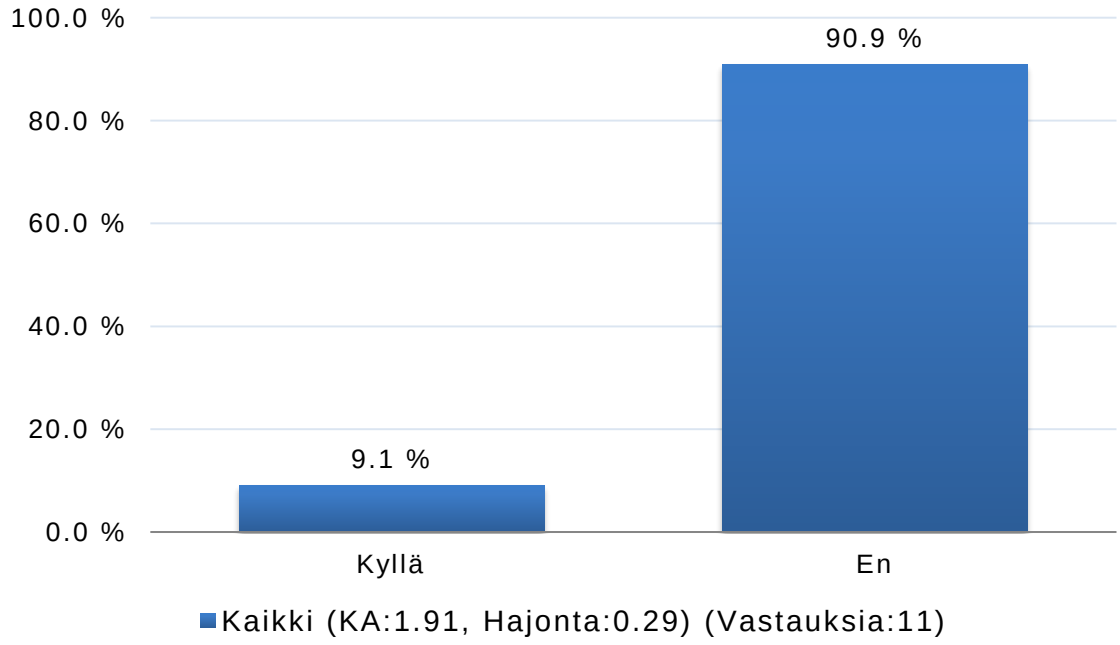
Lukitsetko tietokoneesi kun poistut työpisteeltä?



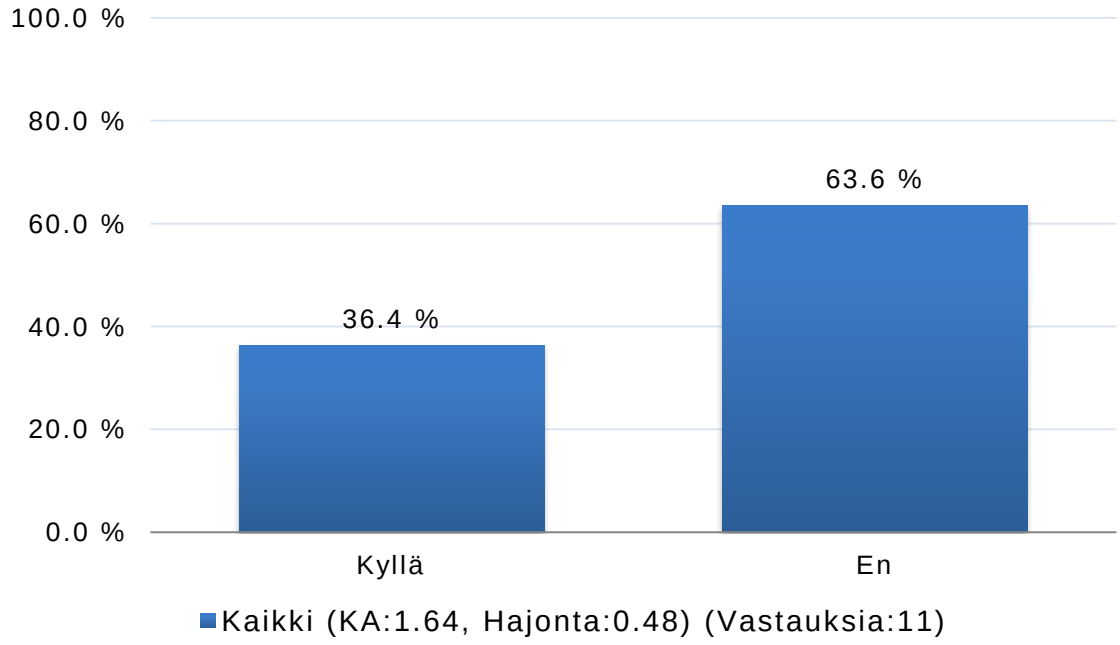
Tallennatko tietosi...



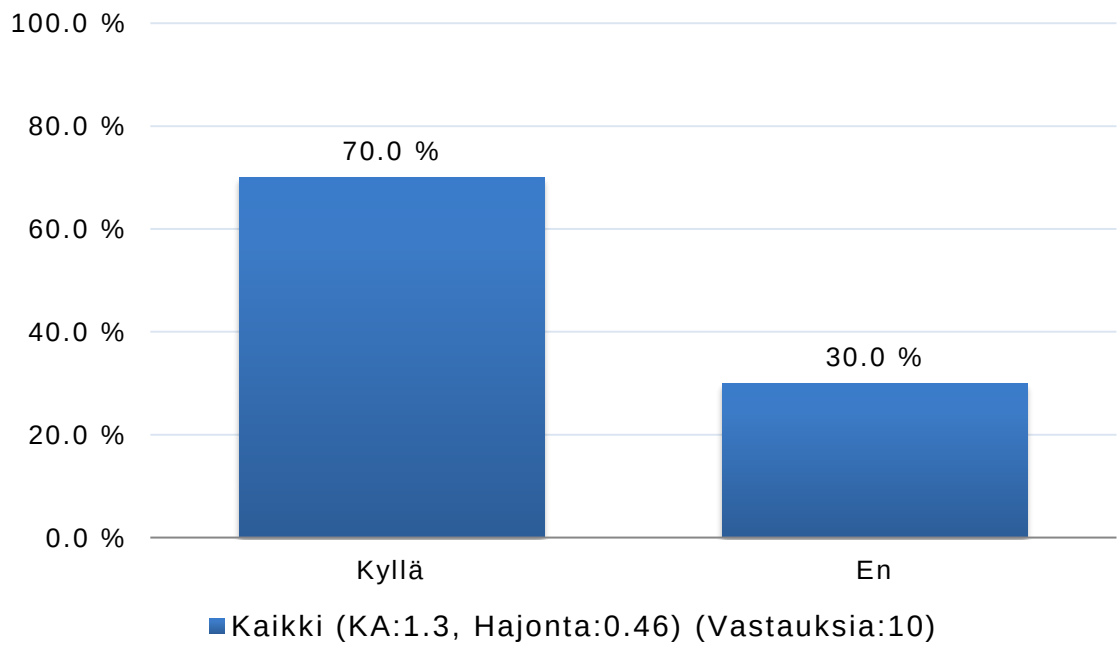
Oletko antanut omaa työpistettä muiden käyttöön tunnuksillasi?



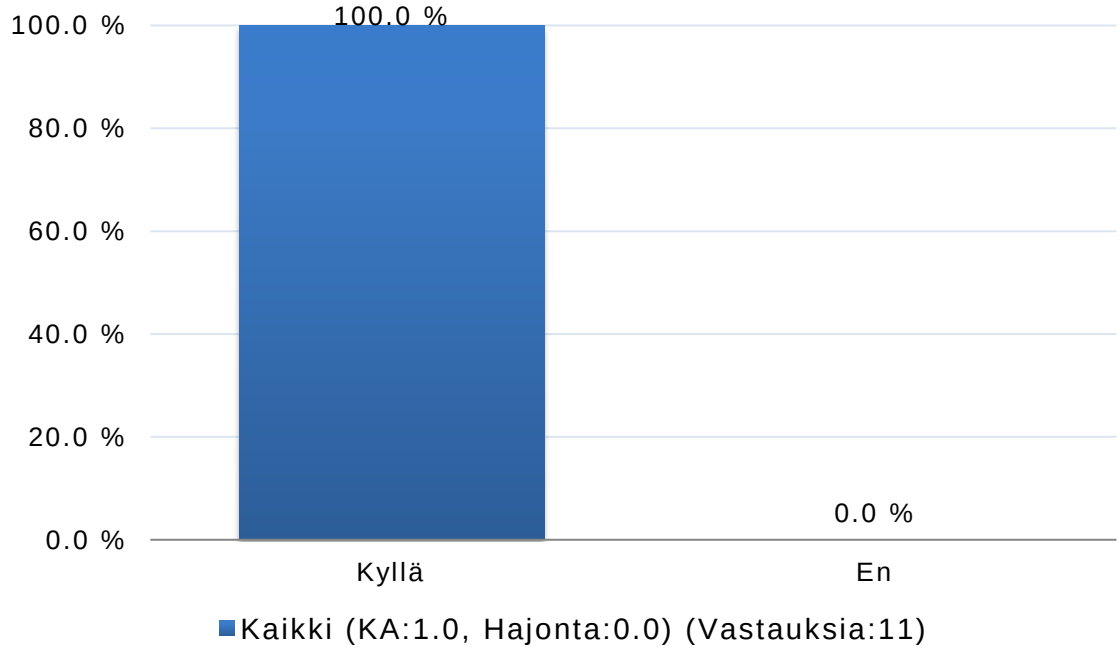
Oletko jättänyt esimerkiksi opiskelijoita valvomatta henkilöstön tiloihin?



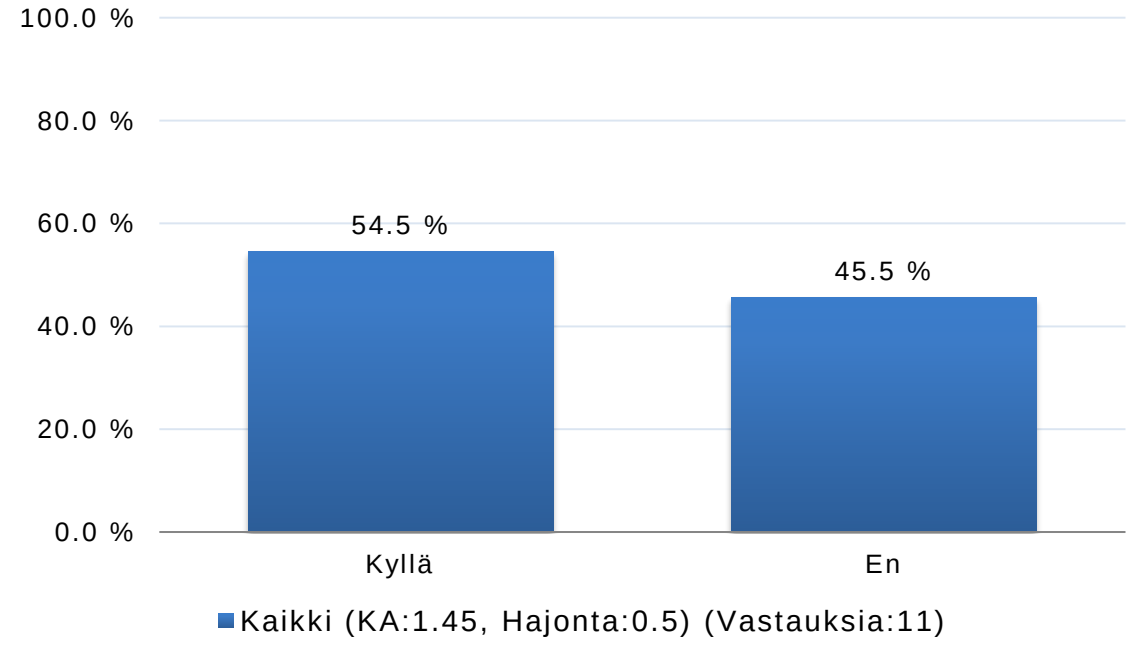
Säilytätkö tärkeää materiaalia kuten paperidokumentteja pöydälläsi?



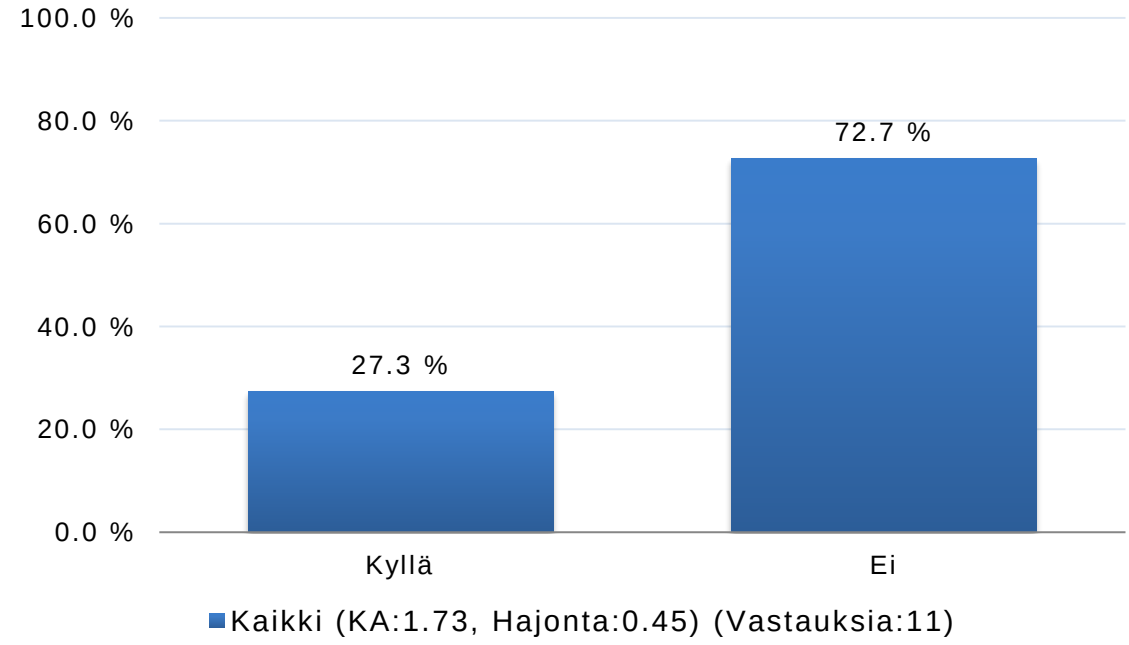
Käytätkö liitteitä työsähköpostissa?



Käytätkö piilokopio-kenttää lähettäessäsi ryhmäsähköpostia, esim. opiskelijoille?



Onko sinua lähestytty epäilyttävillä linkeillä tai liitteillä työsähköpostissa?

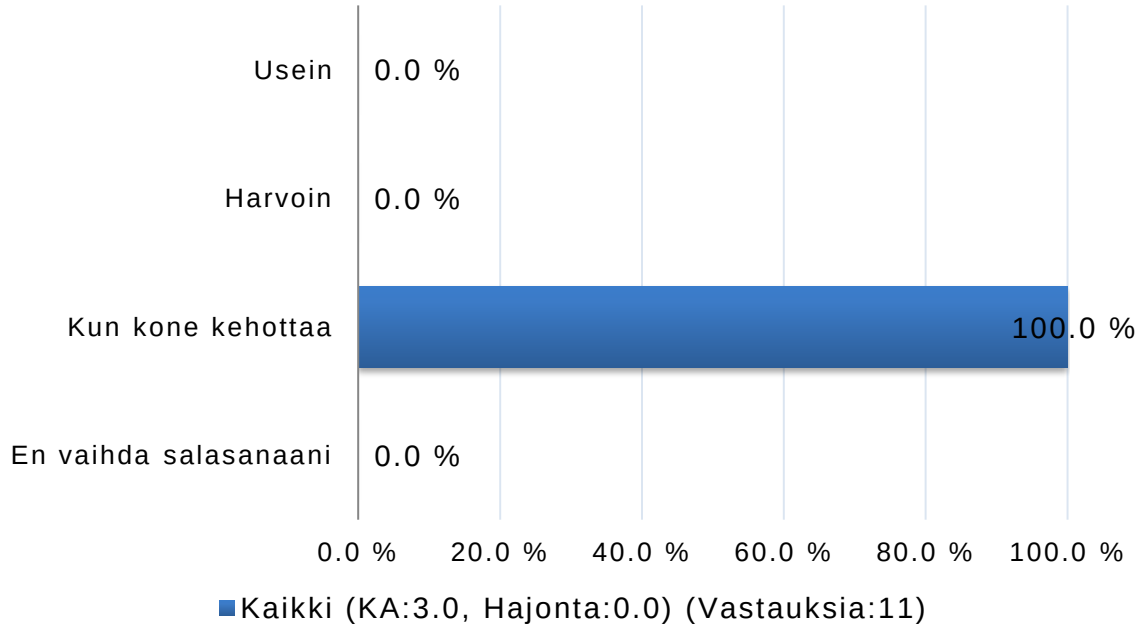


Jos vastasit "Kyllä", millaisia ne ovat olleet?

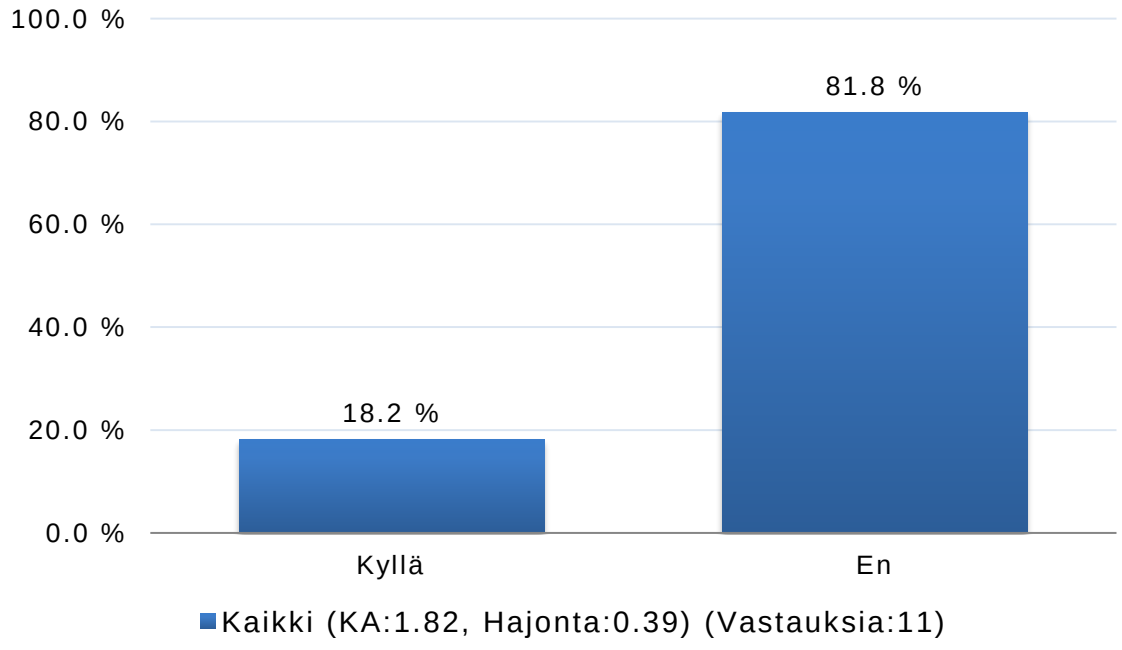
- Roskaposti ohjelmia ja mainolksia ovat pääsääntöisesti (Kaikki)
- Ei enää; epäilyttävät menevät tarpeettomiin tai roskapostiin nykyään suoraan. Aiemmin oli suuri ongelma. (Kaikki)
- Epäilyttäviä kyselyitä eri tahoilta jotka eivät mitenkää liity työhön. Ulkomailta lähinnä. (Kaikki)

- Roskapostista on löytynyt joskus muka pankin kysely, pankilta, jonka asiakas en edes ole. (Kaikki)

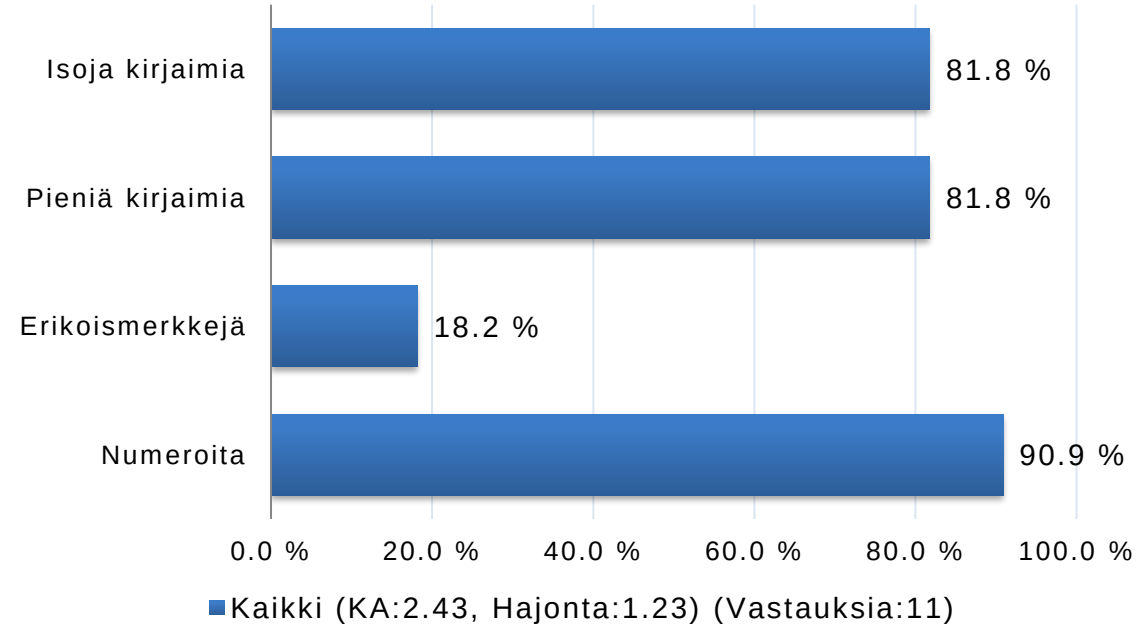
Kuinka usein vaihdat tietokoneesi salasanan?



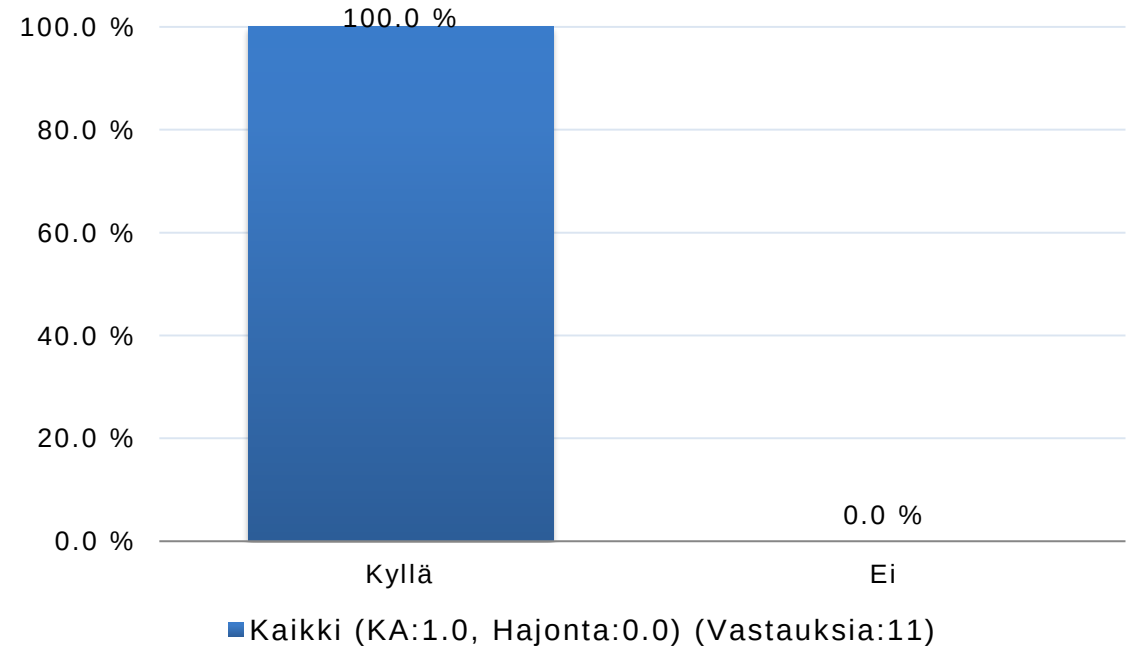
Kirjoitatko salasanasi muistiin esimerkiksi paperilapulle?



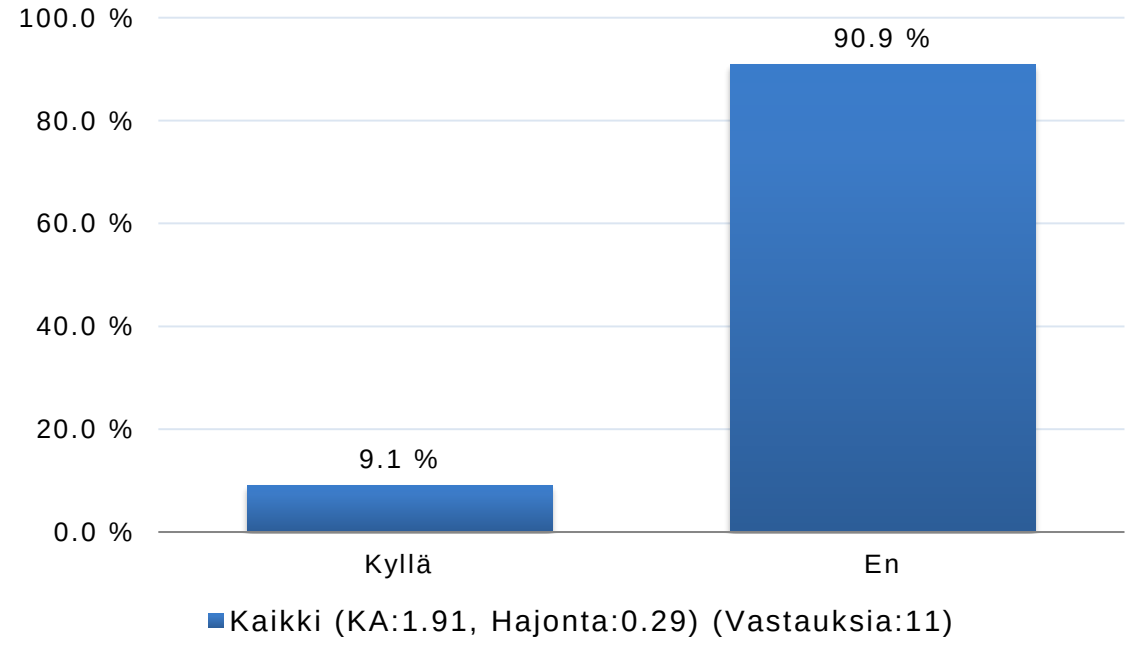
Salasanani sisältää... (voit valita useamman)



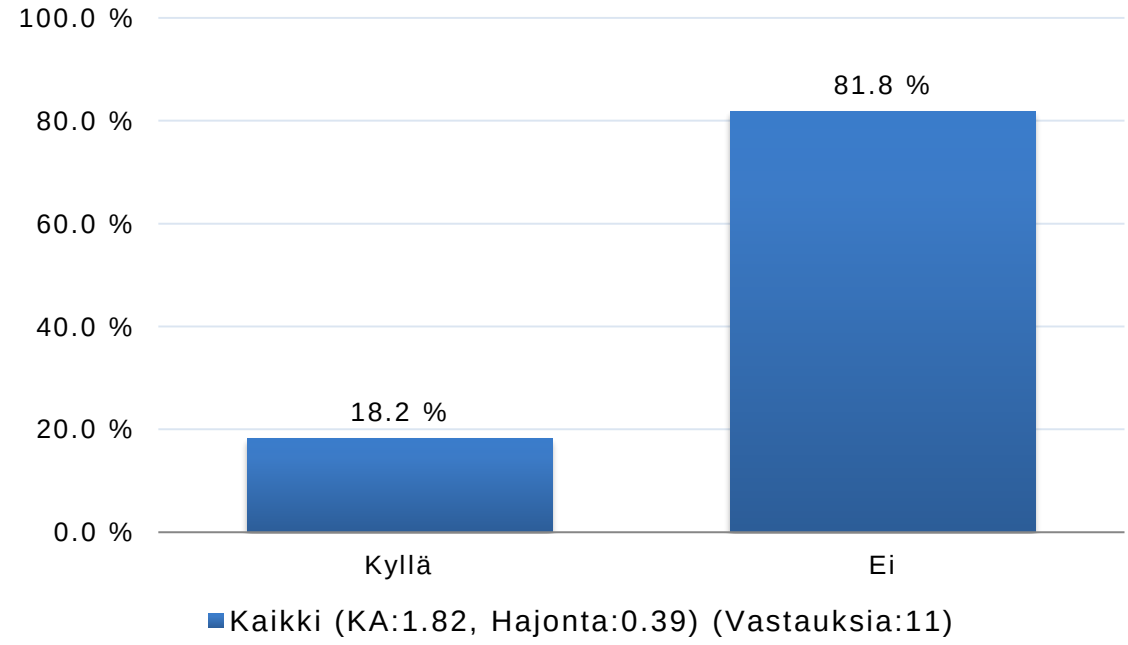
Onko salasanasi yli 8 merkkiä pitkä?



Oletko julkaissut työhösi liittyviä asioita "somessa"?



Onko sinua lähestytty epäilyttävillä linkeillä tai liitteillä sosiaalisessa mediassa?



Jos vastasit "Kyllä", millaisia ne ovat olleet?

- ehdotuksia / kuvia jne (Kaikki)
- Olen "huono" somen käyttäjä (Kaikki)
- ventovieraat haluavat kaveriksi (Kaikki)

Liite 2: Henkilöstön Tietoturvadokumentti (HeTi) -malli

SOMESSA MUISTA!

Sosiaalisessa mediassa **haittaohjelmien** levitys on yhtä **helppoa**, kuin sähköpostissakin!

ÄLÄ AVAA epäilyttäviä linkityksiä! Esimerkiksi ”uutista” oudosta linkityksestä, josta useampi kaveri on yhtäkkiä tykännyt. Se saattaa sisältää haittaohjelman, joka latautuu koneellesi!

ÄLÄ KERRO työhösi olennaisesti liittyviä asioita esimerkiksi Facebookin tilapäivityksissä!

ONGELMATILANTEISSA MUISTA!

Mikäli hallussasi oleva tietotekninen laite **katoaa tai varastetaan**, on velvollisuutesi ottaa heti yhteyttä helpdeskiin!

Viruksen iskiessä ota yhteyttä helpdeskiin!

Jos epäilet tietoturvallisuuden vaarantuneen, ota yhteyttä helpedeskiin!

ETKÖ OLE JOSTAKIN ASIASTA TÄYSIN VARMA?

Varmista asia **tietohallinnosta**!

Henkilöstön tietoturvadokumentti (HeTi)

TYÖTILOISSA MUISTA!

Poistuessasi huoneestasi, **LUKITSE OVI**, jos huoneeseen ei jää muita!

Työhuoneeseen ei ole sallittua jättää ulkopuolisia henkilöitä!

Luokan ovet täytyy lukita **AINA** päivän päätteeksi tai tauolle lähdettäessä!

Muista käyttää kuvallista **henkilökorttia** liikkuessasi talossa!

TYÖKONEELLASI MUISTA!

Lukitse tietokoneesi **AINA**, kun poistut siltä!
Perinteinen **CTRL+ALT+DEL** riittää.

ÄLÄ luovuta käyttäjätunnustasi tai salasanaasi muille!

Tietokoneen **näyttö** täytyy olla oikein aseteltu niin, että ulkopuoliset eivät näe näytöllä olevaa tietoa!

Tallenna tekemiäsi dokumentteja yhä enemmissä määrin **PILVEEN**, kuten OneDriveen. Näin tallennetut tiedot ovat saatavilla paikkaa katsomatta.

Lataa koneellesi **vain** tietohallinnon julkaisukanavan tarjoamia ohjelmia!

SALASANASI KANSSA MUISTA!

Vahva salasana on **pakollinen**!

Sen täytyy kuitenkin olla helposti muistettava, sillä salasanaa **EI SAA** kirjoittaa ylös esimerkiksi työpöydälle jätetylle paperilapulle!

OHJE VAHVALLE SALASANALLE:

- Salasana voi pitää sisällään itselle merkityksellisen tarinan!
- Esimerkiksi ikimuistoinen lomamatka Pariisiin on hyvä alku
- Perään numerosarja, kuten vuosiluku, jolloin Pariisissa kävi
- Osan sanasta voi korvata erikoismerkeillä
- Sen täytyy olla tarpeeksi pitkä (vähintään 8 merkkiä)
- Eli hyvä salasana olisi esimerkkinä **Par11si2006**

Muista vaihtaa salasanasi säännöllisin väliajoin!

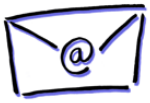
SÄHKÖPOSTIN KANSSA MUISTA!

Omaa työsähköpostia **ei saa luovuttaa** ulkopuolisille muuten kuin työhön liittyvissä asioissa! Eli esim. uutiskirjeiden tilaamisessa käytä omaa henkilökohtaista sähköpostiosoitettasi!

Työsähköpostia **EI SAA** välittää omaan henkilökohtaisiin sähköpostiinsa vaan työasialiikenne tapahtuu vain organisaation tarjoamassa sähköpostijärjestelmässä

Massaviestiä esimerkiksi opiskelijoille lähettäessäsi käytä osoitteiden kirjoittamiseen **Piilokopio**-kenttää!

SÄHKÖPOSTIN KANSSA MUISTA!



Ei ole suositeltavaa **lähettää liitteitä** vaan mieluummin linkitys tiedostosijaintiin!

Älä avaa roskapostiin saapuneita linkkejä! Ne saattavat sisältää haittaohjelmia!

ASIAKIRJOJEN KANSSA MUISTA!

Työpöydälle **EI SAA** jättää dokumentteja, jotka sisältävät esim. yhteystietoja, opiskelijoiden sotuja, oppilaitosta koskevia asioita..

Säilytä materiaalit mieluiten **lukitussa** kaapissa

Kaikki tuhottavaksi tarkoitetut materiaalit sekä asiakirjat **täytyy viedä** hävitettäväksi asianmukaisesti eikä heittää yleisiin paperinkeräyksiin!

ETÄTÖISSÄ MUISTA!

Huolehdi, että etätyössä käyttämäsi laitteistot, ohjelmistot, paperimateriaalit ym. pysyvät vain sinun hallussasi

Vältä puhumasta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä!

KOTIKONEELLA MUISTA!

ÄLÄ TALLENNA työasioita kotikoneellesi!

Luo samaa konetta käyttäville omat käyttäjätunnukset!