

Lauri Leppijoki

## PIKAVIESTIMIEN TIETOTURVA YRITYSYMPÄRISTÖSSÄ

Tietojenkäsittelyn koulutusohjelma  
2018

# PIKAVIESTIMIEN TIETOTURVA YRITYSYMPÄRISTÖSSÄ

Leppijoki, Lauri  
Satakunnan ammattikorkeakoulu  
Tietojenkäsittelyn koulutusohjelma  
Marraskuu 2018  
Sivumäärä: 37  
Liitteitä: 0

Asiasanat: opastus, pikaviestiohjelmat, tietoturva

---

Tämän opinnäytetyön tarkoituksena oli selvittää mitä pikaviestimet ovat ja mitä vaaroja niiden käytössä piilee sekä luoda yleispätevä ohjeistus yrityksille pikaviestimien käyttöön. Pikaviestintä on nykyään yksi yleisimmistä viestinnän muodoista, jonka vuoksi aihe on tärkeä ja ajankohtainen.

Työssä käsitellään yleisellä tasolla mitä pikaviestimet ovat sekä esitellään kaksi eri tyyppistä pikaviestintä. Työssä käydään läpi yleisimmät pikaviestinnän uhat sekä keinot suojautua niiltä. Työn päätarkoituksena oli tehdä yritysympäristöön soveltuva helppolukuinen ohjeistus pikaviestinten käytöstä.

## SECURITY OF INSTANTMESSENGERS IN ENTERPRISES

Leppijoki, Lauri

Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences

Degree Programme in Business Information Technology

November 2018

Number of pages: 37

Appendices: 0

Keywords: guidance, instant messaging software, information security

---

The purpose of this thesis was to find out what instant messengers are and what dangers lie in use of them and then create general guidelines for companies for using instant messengers. Instant messaging is currently one of the most common forms of communication, which makes the subject important and timely.

The work deals with the general level of instant messaging and introduce two different types of instant messengers. The work is going through the most common threats of instant messaging and ways to protect from them. The main purpose of the thesis was make easy to use guidelines for the use of instant messengers which is suitable for business environments.

# SISÄLLYS

1	JOHDANTO.....	5
2	MITÄ OVAT TIETOTURVA JA TIETOSUOJA.....	6
2.1	Tietoturva lyhyesti .....	6
2.2	Tietosuoja lyhyesti .....	7
3	PIKAVIESTIMET.....	9
3.1	Mikä on pikaviestin.....	9
3.2	Skype.....	9
3.3	Whatsapp.....	10
4	PIKAVIESTIMIEN UHAT.....	11
4.1	Käyttäjä ja haittaohjelmat .....	11
4.2	Salattu sisältö .....	12
4.3	Tietojenkalastelu .....	12
5	SUOJAUTUMINEN .....	13
5.1	Mobiililaitteiden hallintaohjelmisto ja virusturva.....	13
5.2	Käyttäjien koulutus ja tiedottaminen .....	14
6	WHATSAPPIN KÄYTTÖÖNOTTO ANDROID LAITTEELLA.....	15
6.1	Aloitutus.....	15
6.2	Asennus.....	15
6.3	WhatsApp asetusten muuttaminen.....	23
6.4	WhatsApp käyttöönnotto työasemalla .....	29
7	YHTEENVETO JA POHDINTA .....	34
7.1	Yhteenveto .....	34
7.2	Pohdinta .....	34
	LÄHTEET.....	36
	LIITTEET	

# 1 JOHDANTO

Opinnäytetyöni tarkoituksena on selvittää, mitä yritysten tulisi ottaa huomioon pikaviestimien käytössä tietoturvan osalta. Nykypäivänä pikaviestintä on yleisimpiä viestinnän muotoja, niin arkielämässä, kuin yritysmaailmassa. Vain harva pikaviestimen käyttäjä kuitenkaan ymmärtää täysin, mitä pikaviestimet ovat ja mitä riskejä niiden käytössä piilee. Aihe on osa suurempaa kokonaisuutta, mutta sen tärkeyttä ei voi korostaa liikaa. Pikaviestimiin kohdistuvat uhat yleistyvät nopeasti, jonka vuoksi aihe kiinnostaa minua.

Tarkoituksena on tehdä tiivis ja selkeä paketti, joka auttaa hahmottamaan mahdolliset pikaviestimistä johtuvat heikot kohdat oman yrityksen tietoturvassa. Työssä käsitellään tietoturvaa ja tietosuojaa käsitteenä, mutta keskiössä ovat kuitenkin pikaviestimet ja niihin liittyvät uhat. Tarkoituksena ei ole vertailla sovelluksia keskenään, vaan tuoda esiin yleisiä pikaviestimiin kohdistuvia uhkia sekä tapoja suojautua niiltä.

## 2 MITÄ OVAT TIETOTURVA JA TIETOSUOJA

### 2.1 Tietoturva lyhyesti

Tietoturva on kokonaisuus eri toimista, jotka varmistavat sen eri osa-alueiden toteutumisen. Tietoturvan osa-alueita ovat: luottamuksellisuus (confidentiality) ja pääsynvalvonta (access control), käytettävyys (availability), eheys (integrity) sekä kiistämättömyys (non-repudiation). Lähes kaikki tieto on nykypäivänä sähköisessä muodossa, joten tietoturva on yritysten maineen ja toiminnan kannalta keskeisessä osassa. Kuten Andreasson, Koivisto ja Ylipartanen (2013, 20) toteavat, ”luottamuksen jälleenrakentaminen onnistuu usein huonosti tai ainakin se vie aikaa”.

Luottamuksellisuutta ylläpidetään tehokkaalla pääsynvalvonnalla rajaamalla tietojärjestelmiin ja tietoihin pääsyä esimerkiksi käyttäjätunnuksella ja salasanalla. Näin pyritään rajaamaan tieto vain henkilöille, joilla siihen on oikeus. Käytössä voi olla myös erilaisia salausmenetelmiä, joiden avulla estetään tiedon luvaton käsittely (Hakala, Vainio, Vuorinen 2006, 5).

Käytettävyys tarkoittaa, että tiedot ja niiden muodostamat palvelut ovat niille tarkoitettujen tahojen saavutettavissa oikeaan aikaan. Tietojen ja palveluiden käytön tulisi olla mahdollisimman helppoa ja viiveetöntä (Hakala, Vainio, Vuorinen 2006, 4).

Jotta käsiteltävä tieto olisi käyttökelpoista, on tiedon eheys varmistettava niin, että tieto säilyy muuttumattomana käsittelyn, siirron ja tallennuksen aikana. Eheyden ylläpito toteutetaan usein ohjelmistollisin ratkaisuin. Käsiteltävän tiedon syötteitä voidaan rajoittaa sekä tarkkailla käsittelyn aikana. Lisäksi tallennetusta tiedosta voidaan tehdä tarkastussummia ja tiivisteitä, joiden avulla sen muuttumattomuus voidaan varmistaa (Hakala, Vainio, Vuorinen 2006, 4).

Tiedon kiistämättömyyteen pyritään pitämällä järjestelmään kirjautumisista ja tietojen käytöstä lokia. Käyttäjän henkilöllisyyden varmistamiseen voidaan käyttää sähköistä henkilökorttia tai jopa biometrisia tunnisteita, kuten sormenjälki- tai silmänpohjätunnistetta. Tiedon kiistämättömyys on tärkeää etenkin tilanteissa, joissa joudutaan turvautumaan oikeudellisiin toimiin (Hakala, Vainio, Vuorinen 2006, 5).

## 2.2 Tietosuoja lyhyesti

Tietosuoja on yksityishenkilöiden sekä organisaatioiden työntekijöiden henkilötietojen turvaamista niiden käsittelyn, siirron ja arkistoinnin aikana. (Rousku, 2014, 52) Tietosuojaa säädellään perustuslailla, henkilötietolailla sekä Euroopan unionin yleisellä tietosuoja-asetuksella, josta käytetään lyhennettä GDPR. Tietosuojan tarkoitus on varmistaa, että rekisteröidyn eli yksityisen henkilön yksityisyyden suoja sekä oikeusturva on suojattu. Rekisterinpitäjällä eli taholla, joka päättää ”miksi” ja ”miten” henkilötietoja käsitellään, on velvollisuus turvata käsiteltävän tiedon kohteen yksityisyys, edut ja oikeudet (Andreasson, Koivisto, Ylipartanen 2013, 14). Tietoturva voidaan pitää työkaluna tietosuojan toteutumiseen.

Suomen perustuslakiin on kirjattu, että oikeus yksityisyyden suojaan on kansalaisen perusoikeus. Kyseinen säännös määrää, että henkilötietojen suoja tulee säätää tarkemmin lailla. Perustuslain mukaan myös henkilötietojen käsittelyä tulee säätää lain tasoisesti. Perustuslaki ei varsinaisesti suojaa käsiteltävää tietoa tai dataa, vaan ihmisiä, joita tieto koskee (Andreasson, Koivisto, Ylipartanen 2013, 31).

Henkilötietolain tarkoitus tietosuojan näkökulmasta on toteuttaa yksityiselämän suoja sekä muut yksityisyyttä turvaavat perusoikeudet, kun käsitellään henkilötietoja. Henkilötietolaki on voimassa henkilötietoja käsiteltäessä, jollei muualla laissa säädetä toisin (Andreasson, Koivisto, Ylipartanen 2013, 34).

EU:n yleisen tietosuoja-asetuksen tarkoitus on vahvistaa yksilön oikeuksia, lujittaa sisämarkkinaulottuvuutta, huomioida tietosuojan globaalit ulottuvuudet sekä tehostaa tietosuojasääntöjen valvontaa. Se luo Euroopan unionille ajanmukaisen, vahvan ja yhtenäisen tietosuojakehyksen. EU:n yleisen tietosuoja-asetus pitää sisällään säännökset henkilötietojen käsittelyä koskevista periaatteista, käsittelyn lainmukaisuudesta, rekisteröidyn suostumuksen edellytyksistä ja arkaluonteisten tietojen käsittelystä. Asetus koskee kaikkea henkilötietojen käsittelyä EU:n jäsenvaltioissa. Rekisterinpitäjälle, joka laiminlyö tietosuojavelvoitteensa voidaan langettaa seuraamusmaksuja. Asetuksessa lueteltuja rekisteröidyn oikeuksia ovat omia henkilötietoja koskeva tiedonsaantioikeus, oikeus saada tiedot oikaistua, oikeus tulla unohdetuksi sekä oikeus tietojen poistamiseen ja tietojenkäsittelyn vastustamiseen. Rekisterinpitäjällä on myös

velvollisuus antaa rekisteröidylle avoimia ja helposti saatavia tietoja heidän tietojensa käsittelystä. Asetuksen lähtökohtana on riskipohjainen lähestymistapa, jonka tarkoitus on välttää ylisääntelyä sekä turvata rekisteröidyn suoja korkean riskin toiminnassa. Sen vuoksi tietojen laatu, luonne, käsittelytarkoitus ja laajuus on arvioitava (Andreasson, Koivisto, Ylipartanen 2013, 35).



### 3 PIKAVIESTIMET

#### 3.1 Mikä on pikaviestin

Pikaviestimet ovat ohjelmistoja, jotka mahdollistavat reaaliaikaisen tekstipohjaisen viestimisen kahden tai useamman osanottajan välillä. Usein viestin vaihtoon käytetään Internet-yhteyttä tai lähiverkkoa, mutta osa pikaviestimistä osaa kuljettaa sanomat myös puhelinverkon välityksellä. Pikaviestimien perusominaisuus on lähettää ja vastaanottaa tekstipohjaisia viestejä, mutta suurin osa ohjelmistoista kykenee lähettämään myös monipuolista mediaa, kuten kuva-, ääni- ja videotiedostoja. Nykyään vain harvat pikaviestimet rajoittavat lähetettävien tiedostojen tyyppin. Pikaviestinpalveluiden käyttäminen vaatii lähes poikkeuksetta tunnuksen luomisen palveluun. Tunnus voi määrittyä käyttäjän sähköpostiosoitteen, puhelinnumeron tai halutun käyttäjänimen mukaan, riippuen mitä palvelua käytetään. Pikaviestinohjelmalla asiakas yhdistää itsensä pikaviestinpalveluun. Viestit kulkevat asiakasohjelmistosta palveluntarjoajan palvelimeen, joka välittää viestin vastaanottajalle. Viestiliikenne on usein salattua päästä päähän, eli viestejä ei voi periaatteessa lukea kuin lähettäjä ja vastaanottaja. Usein viestit ovat tallennettuna palveluntarjoajan palvelimelle, joka mahdollistaa viestien kulkemisen perille, vaikka vastaanottaja ei olisi kirjautuneena lähetys hetkellä (Paul Gil, 2018).

#### 3.2 Skype

Skype mielletään usein VoIP eli IP-puhelu palveluksi, mutta se pitää sisällään identtisiä ominaisuuksia ja toimintoja pikaviestinsovellusten kanssa.

Skype on ilmainen sovellus, joka mahdollistaa teksti-, ääni- ja videopohjaisen viestinnän kahden tai useamman henkilön välillä. Skypellä voi soittaa myös lanka- ja matkapuhelinverkkoon. Skypen julkaisivat alunperin Niklas Zennström ja Janus Friis vuonna 2003. Sovellus on virallisesti julkaistu Windows-, Linux-, macOS X-, Android- sekä iOS-käyttöjärjestelmille sekä epävirallisesti lukuisille muille järjestelmille, kuten Playstation Portable (Tory Foulk. 2018).

Skype saavutti nopeasti suuren suosion ja jo vuonna 2005 yhdysvaltalainen eBay Inc. osti sen. eBayllä oli vaikeuksia toimia kahden yrityksen yhdistelmänä, joten vuonna 2009 se alkoi valmistella Skypestä itsenäistä yritystä. Vuonna 2011 eBay kuitenkin päätyi myymään Skypen nykyiselle omistajalleen Microsoftille (Anna Bishop. 2012).

Skypestä on omat versiot yksityis- ja yrityskäyttöön. Maksuton Skype on suunnattu yksityishenkilöille, mutta se soveltuu myös yrityksille, joilla on enintään 20 työntekijää. Käyttö on ilmaista, mutta puhelut lanka- ja matkapuhelimiin ovat maksullisia. Puhelut maksetaan etukäteen lataamalla Skypeen puheaikaa (Microsoft. 2018).

Yritykset voivat hankkia Skype for Businessin joko itsenäisenä tuotteena tai osana Office 365 Enterprise-tilausta. Yritys voi tarvittaessa käyttää konesalissaan myös omaa Skype for Business palvelinta (Margaret Rouse. 2017).

Skype for Business mahdollistaa jopa 250 osanottajan verkkotapaamiset, tarjoaa yritystason tietoturvan, mahdollistaa käyttäjätilien hallinnan ja se on integroitu kaikkiin Office-sovelluksiin. Skype for Businessin käytöstä laskutetaan käyttäjämäärän mukaan kuukausimaksulla (Microsoft. 2018).

### 3.3 WhatsApp

WhatsApp on Facebookin omistama puhelimille suunnattu pikaviestinsovellus, jonka ensisijainen päämäärä oli korvata perinteiset tekstiviestit. Tekstipohjaisten viestien lisäksi WhatsAppilla voidaan lähettää kuvia, videoita, ääniviestejä, yhteystietoja sekä sijaintitietoja. Se julkaistiin alun perin Applen iPhoneille, mutta siitä on viralliset käännökset myös Androidille, Windows Phonelle, BlackBerryille sekä Nokian Symbian60-puhelimille. WhatsAppia voi käyttää nykyään myös Internet-selaimella tai Windowsin ja Macin natiivilla sovelluksella, mutta niiden aktivointiin vaaditaan puhelin, jolla on jo WhatsApp-tili (Cella Lao Rousseau. 2018).

Viestien salaamiseen WhatsApp käyttää osaa Open Whisper Systemsin valmistamasta salaustokokollasta nimeltään SignalProtocol. Open Whisper Systemsillä on oma pikaviestinsovellus nimeltään Signal (Henry Burrell. 2017).

## 4 PIKAVIESTIMIEN UHAT

### 4.1 Käyttäjä ja haittaohjelmat

Käyttäjä on tietoturvan kannalta heikoin lenkki myös pikaviestimien käytössä. Vaikka yrityksen tietoturvajärjestelmät olisivat markkinoiden parhaimmista, niin inhimillisiltä virheiltä on mahdotonta suojautua. Koska pikaviestintä on nykyään lähes kaikille ihmisille arkipäivää, niin myös pikaviestimien käyttö on todella huoletonta. Vaarana on, että yrityksen työntekijä lähettää arkaluonteista sisältöä väärälle vastaanottajalle tai jopa väärään ryhmäkeskusteluun. Etenkin GDPR tulisi ottaa huomioon yrityksen pikaviestinten käytössä. Henkilötietojen käsittely pikaviestimillä voi vaarantaa yrityksen tietosuojan ja tietoturvan (Continuity Central. 2017).

Kuten mitä tahansa tietojärjestelmää, niin myös pikaviestin-ohjelmistoja vastaan voidaan hyökätä haittaohjelmilla, jotka on tehty varta vasten niitä varten tai ne osaavat hyödyntää pikaviestimien ominaisuuksia.

KasperSkyLabs ilmoitti vuoden 2018 tammikuussa löytäneensä uuden haittaohjelman, joka on koodattu hyödyntämään pikaviestinsovelluksien ominaisuuksia hyökkäyksessä. Skygofree-niminen haittaohjelma on saanut alkunsa jo vuonna 2014 ja sitä on päivitetty aktiivisesti sen elinkaaren aikana. Kyseisestä haittaohjelmasta erikoisen tekee sen laaja ominaisuuksien skaala. Skygofree-tartuntoja on havaittu vain Android laitteissa, mutta se sisältää useita Windows ympäristöön tarkoitettuja ominaisuuksia. Ohjelma itsessään ei leviä pikaviestimien välityksellä, mutta se osaa hakea tietoja tietyiltä pikaviestin-sovelluksilta (BALAJI.N. 2018). Skygofreen kaltaisia kehittyneitä haittaohjelmia julkaistaan nykypäivänä usein ja ne kehittyvät nopealla vauhdilla.

Pikaviestimien välityksellä leviävät haittaohjelmat eivät usein kuitenkaan aktivoidu ilman, että vastaanottaja avaa vastaanotettua tiedostoa. Etenkin mobiililaitteilla haittaohjelma joutuu pyytämään järjestelmän käyttöluvia, jotta se voi toimia laitteella vaipaasti.

## 4.2 Salattu sisältö

Viestiliikenteen salaus on todella tärkeä ja olennainen ominaisuus yrityksen pikaviestintä valitessa. Vaikka salaus on pääosin positiivinen ominaisuus voi siitä kuitenkin olla myös haittaa yrityksen tietoturvan kannalta. Jos käytössä on pikaviestin, joka salaa liikenteen päästä-päähän, niin haitallisen sisällön suodattaminen voi olla täysin mahdotonta. Automatisoidut tietoturvajärjestelmät eivät pysty käsittelemään salattuja viestejä, koska niiden sisältö selviää vasta valtuutetulle käyttäjälle. Silloin vastuu viestiliikenteen sisällöstä jää käyttäjälle (Christopher Boyd. 2018).

Etenkään pikaviestinnässä salaukseen ei pidä luottaa liikaa. Salaus toimii ainoastaan, jos lähettäjän ja vastaanottajan luottamussuhde on kestävä ja molempien laitteet on suojattu asianmukaisesti. Pikaviestimien salaus suojaa viestejä lähinnä niiden siirron aikana. Viestinnän osapuolet voivat levittää viestien sisältöä ulkopuolisille salauksesta huolimatta. Jotkin pikaviestinsovellukset yrittävät estää viestien leviämistä ulkopuolisille niin, että viestit tuhoutuvat lukemisen jälkeen, mutta se ei ole kovin tehokas ratkaisu etenkään yritysympäristössä (Lily Hay Newman. 2018).

## 4.3 Tietojenkalastelu

Tietojenkalastelu eli verkkourkinta on verkkohyökkäyksen muoto, joka toteutetaan usein sähköpostin, puhelun tai pikaviestimen välityksellä. Tietojenkalastuksen tarkoituksena on saada hyökkäyksen uhri paljastamaan arkaluonteista tietoa, kuten salasanoja, käyttäjätunnuksia tai luottokorttitietoja. Tavallisesti rikollisten motivaationa on raha, mutta yhä useammin rikolliset pyrkivät pääsemään käsiksi organisaation tietojärjestelmiin (Yksityisyydensuoja. 2018.). Tietoturvasivusto phishme.com (nykyään cofence) julkaisi vuonna 2016 tutkimuksen, jonka mukaan 91-prosenttia tietovuotoon johtaneista kyberhyökkäyksistä sai alkunsa tietojen kalastelusta (Phisme. 2016).

Tietojenkalastelun selkeästi nousevana trendinä ovat hyökkäykset, jotka kohdistuvat mobiililaitteisiin. Puhelimet ja tablettitietokoneet ovat huomattavasti helpompi tapa lähestyä uhria, koska tapamme käyttää mobiililaitteita on arkisempi verrattuna tietokoneen käyttöön. Myös työ- ja arkielämän rajan hämärtyminen tekee mobiililaitteista rikollisia kiinnostavan kohteen. Nykyään ihmisillä saattaa olla organisaation laitteistoa

käytössä myös kotona ja työpuhelinta voidaan käyttää ainoana henkilökohtaisena puhelimena (Michelle Drolet. 2018).

Pikaviestimet toimivat kuin majakat, jotka auttavat hyökkääjiä kohdistamaan hyökkäykset suoraan mobiililaitteisiin. Ihmiset myös klikkaavat paljon todennäköisemmin pikaviestimien välityksellä vastaanotettuja linkkejä, kuin esimerkiksi sähköpostin välityksellä saapuneita linkkejä.

## 5 SUOJAUTUMINEN

### 5.1 Mobiililaitteiden hallintaohjelmisto ja virusturva

Mobiililaitteiden hallintaohjelma (eng. Mobile Device Management, MDM) on nimensä mukaan mobiililaitteiden hallintaan ja ylläpitoon tarkoitettu ohjelmisto. Aluperin MDM-ohjelmistot ovat suunniteltu mobiilialustoille, mutta suurin osa niistä tukee myös Windows ympäristöä. MDM:n tärkeimpiä ominaisuuksia ovat nopea käyttöönotto, sovellusten keskitetty jakelu sekä laitteiden valvonta. Mobiililaitteisiin voidaan MDM:n avulla luoda tietoturvaa vahvistavia sääntöjä. Esimerkiksi sähköpostin lähettäminen voidaan estää, jos puhelimen virustunnisteet eivät ole ajan tasalla. Edellä mainittu on vain suppea esimerkki mahdollisista säännöistä, mutta se antaa kuitenkin hyvän kuvan siitä, kuinka tehokas mobiililaitteiden hallintaohjelma voi olla (Continuum. 2018.).

Mobiililaitteiden hallintaohjelmistoilla voidaan myös estää käyttäjää asentamasta sovelluksia laitteeseen. Näin voidaan varmistaa, että käytössä on vain yrityksen sallimia sovelluksia ja samalla estetään käyttäjää asentamasta haittaohjelmia (Continuum. 2018.).

Mobiililaitteiden hallintaohjelmistojen tarjoajat ovat riippuvaisia yhteistyöstä mobiililaitteiden valmistajien kanssa, koska ne vaativat toimiakseen vahvoja järjestelmäoikeuksia. Siksi etenkin Android-laitteille on tarjolla valtava määrä eri tehoisia hallintaohjelmia.

Tehokkaimmat mobiililaitteiden hallintaohjelmistot toimivatkin vain tietyissä merkeissä ja malleissa. (David Kennedy. 2012.)

Virusturva voi olla sisäänrakennettuna mobiililaitteiden hallintaohjelmaan, mutta etenkin pienemmille yrityksille vahva viruksentorjuntaohjelmisto on yksin riittävä. Koska pikaviestimien välityksellä on mahdollista lähettää tiedostoja, voidaan niillä levittää myös haittaohjelmia. Kehittyneet haittaohjelmat voivat levitä laitteesta toiseen USB-yhteyden välityksellä, jonka vuoksi on tärkeää, että virustorjunta on asennettu niin yrityksen tietokoneille kuin mobiililaitteille.

## 5.2 Käyttäjien koulutus ja tiedottaminen

Inhimillisiltä virheiltä ei voida koskaan täysin suojautua, mutta tietoturvan kannalta on tärkeää kouluttaa ja tiedottaa työntekijöitä säännöllisesti. Turha pelon luominen on kuitenkin turhaa eikä tietoturvasta pidä tehdä käyttäjälle päänvaivaa. Koulutus olisikin hyvä hoitaa pienissä ja selkeissä moduuleissa, jotta oppimisen motivaatio säilyisi. Koulutus tulisi perustella työntekijälle, jotta se tuntuisi merkitykselliseltä. Käyttäjän koulutus ja tiedotus ovat tietoturvan vaikeimpia osa-alueita, mutta niihin kannattaa panostaa, koska tietoverkon käyttäjä on sen heikoin lenkki (Kratikal Tech. 2018.).

Nykyaikaisissa virustorjunta ohjelmistoissa on usein suojausominaisuuksia pikaviestimiin kohdistuvaa tietojenkalastelua varten, mutta tämä yksin on toimimaton suoja. Koska pikaviestimien viestit ovat usein salattuja niin myös viestien sisältämät haitalliset linkit tai liitteet on salattu. Salauksen vuoksi virustorjuntaohjelmisto saattaa havaita uhan vasta kun on liian myöhäistä. Kaikkia haittaohjelmia virustorjuntaohjelmistot eivät edes osaa havaita, koska rikollisten hyökkäystekniikat kehittyvät nopeasti. Yrityksellä tulisi olla valmiit käytännöt ja ohjeistukset siitä, kuinka työntekijöiden tulee toimia havaitessaan tietojenkalastelua tai muuta epäilyttävää viestiliikennettä.

## 6 WHATSAPPIN KÄYTTÖÖNOTTO ANDROID LAITTEELLA

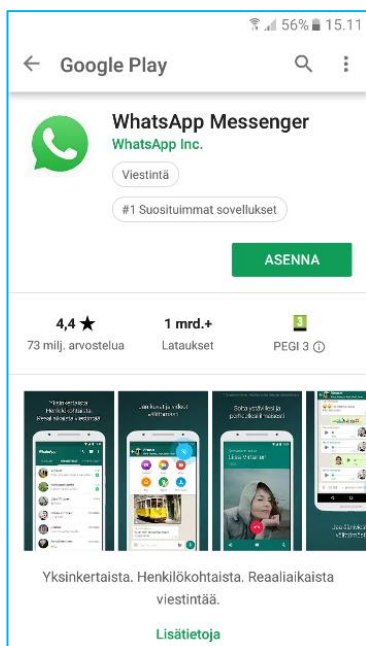
### 6.1 Aloitus

WhatsAppin käyttö työviestimenä ei ole suositeltavaa. On mahdotonta tietää mitä dataa käyttäjästä Facebook kerää WhatsAppin kautta. Ilmaiset palvelut rahoitetaan usein mainostuloilla tai ne myyvät käyttäjätietoa kolmansille osapuolille. Kuitenkin siitä huolimatta WhatsAppin käyttö on todella yleistä yrityksissä, jonka vuoksi tein ohjeen, joka opastaa mahdollisimman turvallisen WhatsAppin käyttöönoton.

Ennen WhatsAppin asennusta käyttäjän tulee selvittää, onko sen käyttö sallittua yrityksen laitteilla ja saako työpuhelimien numeron rekisteröidä käyttäjätiliin. Asiaa voi tiedustella oman yrityksen tietohallinnosta tai järjestelmänvalvojalta. WhatsApp tilin luominen vaatii älypuhelimien sekä matkapuhelinliittymän, joka sisältää datapalvelun.

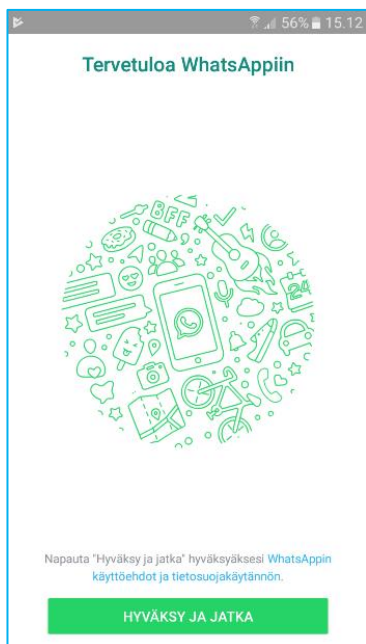
### 6.2 Asennus

Ensimmäiseksi ladataan WhatsApp puhelimelle. Internetistä löytää monia lähteitä, joista WhatsAppin saa ladattua, mutta on suositeltavaa käyttää Google Play-kaupan versiota. Muiden lähteiden asennukset saattavat vaarantaa tietoturvan sekä tietosuojan. Kuvassa 1 on esimerkki Google Play-kaupan WhatsApp näkymästä.



Kuva1. Google Play kauppa.

Sovelluksen asentamisen jälkeen luodaan käyttäjätunnus WhatsAppin käyttöön. Ensimmäisellä käynnistyskerralla aukeaa kuvan 2 näkymä, jossa WhatsApp pyytää lukemaan käyttöehdot ja hyväksymään ne. Jos hyväksyt käyttöehdot ja haluat jatkaa WhatsAppin käyttöä, niin paina vihreää **HYVÄKSY JA JATKA**-painiketta.



Kuva 2. Tervetuloa WhatsAppiin.

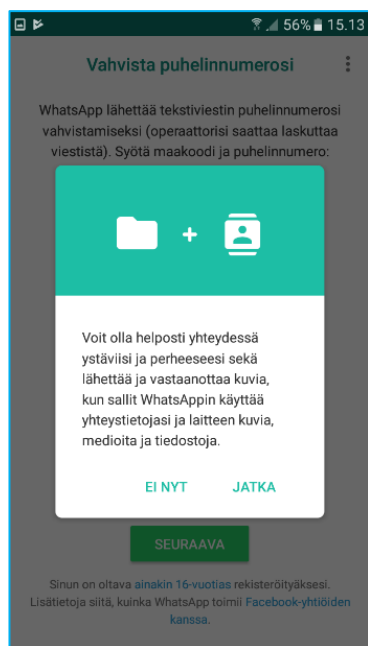


Seuraavaksi WhatsApp pyytää lupaa käyttää puhelimesi yhteystietoja sekä kuvia ja tiedostoja. Käyttöoikeudet on jaettu kahteen ryhmään, joista toinen pitää sisällään yhteystiedot ja toinen taas kuvat sekä tiedostot. Yhteystietojen käytön salliminen mahdollistaa puhelimeen tallennettujen kontaktien helpon löytämisen WhatsAppissa sekä yhteystietojen lisäämisen WhatsAppin kautta.

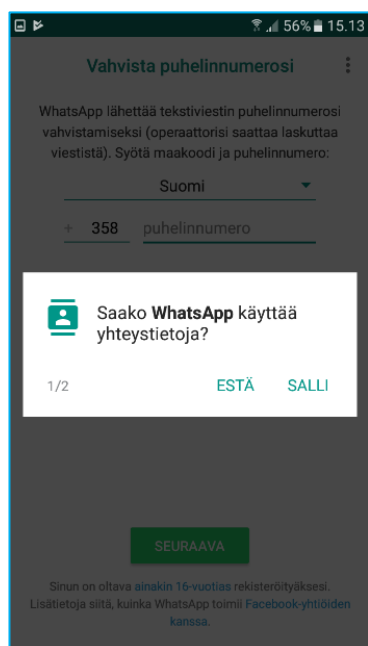
Kuvien ja tiedostojen käyttöoikeus taas mahdollistaa puhelimeen tallennettujen kuvien sekä tiedostojen lähettämisen WhatsAppin välityksellä. Käyttöoikeuksien salliminen on vapaaehtoista ja WhatsApp toimii ilman näitä käyttöoikeuksia, mutta sen käyttö on huomattavasti hankalampaa. Kuitenkin yritysympäristössä on huomioitava mahdolliset arkaluonteiset yhteystiedot ja tiedostot, joita puhelimella on.

Käyttäjä on ensisijaisesti itse vastuussa WhatsAppin käytöstä johtuvista tietoturva ja tietosuoja ongelmista.

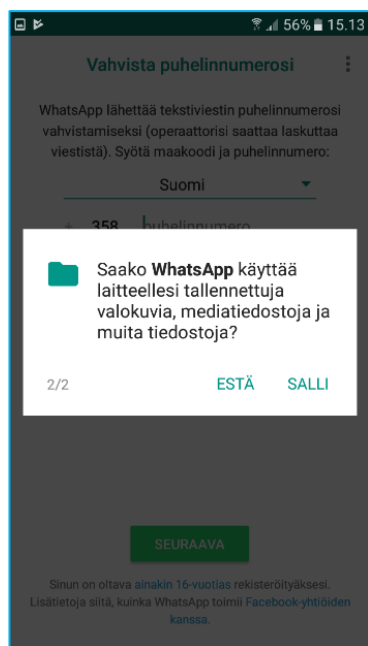
Ensin näyttöön tulee kuvan 3 mukainen ilmoitus yhteystietoihin ja mediatiedostoihin liittyvästä käyttöluva kyselystä. Jos et halua antaa lupia niin paina **EI NYT**, mutta jos haluat antaa käyttöluvan niin paina **JATKA**. Jos painoit **JATKA**, niin ruutuun tulee ensin kuvan 4 mukainen kysely. Paina **SALLI**, jos haluat myöntää yhteystietojen käyttöluvan sovellukselle. Seuraavaksi ruutuun ilmestyy kuvan 5 mukainen mediatiedostojen käyttöluva kysely. Jos haluat antaa sovellukselle luvan lukea mediatiedostojasi, jatka painamalla **SALLI**.



Kuva 3. Selostus yhteystietojen ja medioiden käyttöluvasta.



Kuva 4. Yhteystietojen käyttöluvan kysely.

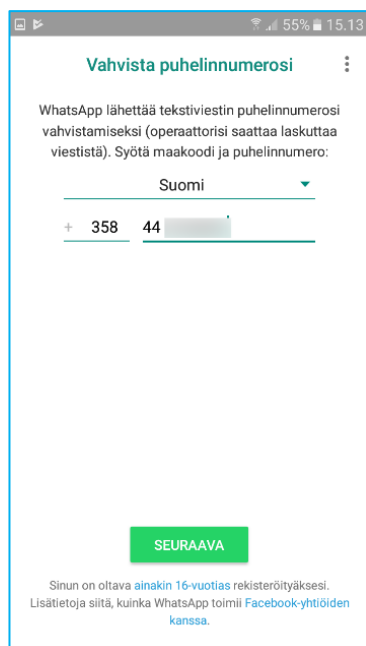


Kuva 5. Medioiden käyttöluvan kysely.

Kun olet sallinut tai vaihtoehtoisesti päättänyt olla sallimatta käyttöoikeudet, niin WhatsApp pyytää puhelinnumeroasi. Normaalisti puhelinnumeroksi asetetaan numero, joka on käytössä puhelimessa, jonka kanssa rekisteröinti tehdään. Voit kuitenkin käyttää esimerkiksi prepaid-liittymää, mutta puhelinnumeron on oltava sinun omassa käytössä.

WhatsApp lähettää rekisteröinnissä käytettävään puhelinnumeroon tarkistuskoodin, joka syötetään sovellukselle. Puhelinnumero toimii WhatsAppin käyttäjätunnuksena, joten käytä ainoastaan puhelinnumeroa, joka on sinun hallinnassasi tai, johon sinulla on käyttöoikeus, kuten työnumero tai henkilökohtainen puhelinnumero.

Ruudussa pitäisi nyt näkyä kuvan 6 mukainen näkymä johon puhelinnumero syötetään. Kun olet valinnut oikean suuntanumeron ja syöttänyt puhelinnumerosi, paina vihreää **SEURAAVA** painiketta. Kuvassa 7 on esimerkki näkymästä, kun WhatsApp varmistaa, että numero on oikein. Jos puhelinnumero on oikea, niin paina **OK** tai muokkaa syöttämäsi puhelinnumeroa **MUOKKAA** painikkeella.



Vahvista puhelinnumerosi

WhatsApp lähettää tekstiviestin puhelinnumerosi vahvistamiseksi (operaattorisi saattaa laskuttaa viestistä). Syötä maakoodi ja puhelinnumero:

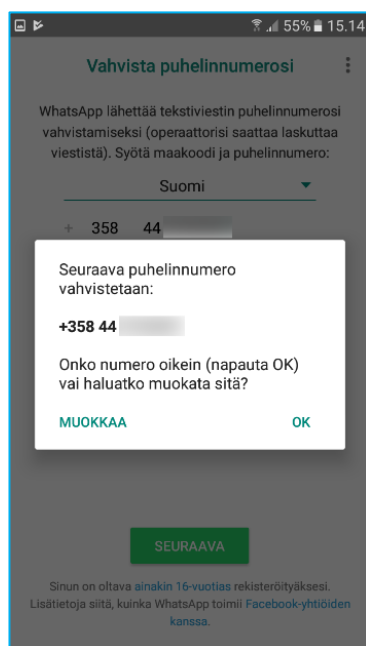
Suomi

+ 358 44

SEURAAVA

Sinun on oltava ainakin 16-vuotias rekisteröityäksesi. Lisätietoja siitä, kuinka WhatsApp toimii Facebook-yhtiöiden kanssa.

Kuva 6. Puhelinnumeron kysely.



Vahvista puhelinnumerosi

WhatsApp lähettää tekstiviestin puhelinnumerosi vahvistamiseksi (operaattorisi saattaa laskuttaa viestistä). Syötä maakoodi ja puhelinnumero:

Suomi

+ 358 44

Seuraava puhelinnumero vahvistetaan:

+358 44

Onko numero oikein (napauta OK) vai haluatko muokata sitä?

MUOKKAA OK

SEURAAVA

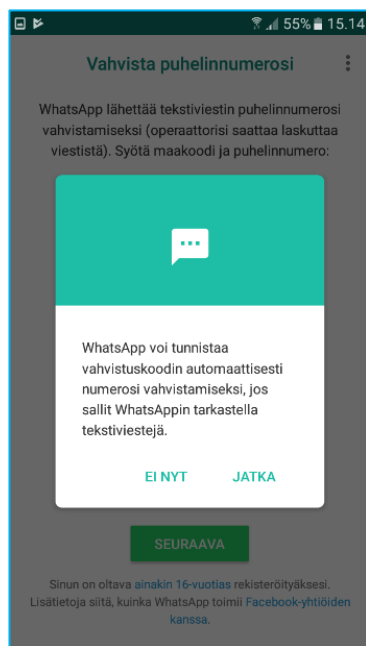
Sinun on oltava ainakin 16-vuotias rekisteröityäksesi. Lisätietoja siitä, kuinka WhatsApp toimii Facebook-yhtiöiden kanssa.

Kuva 7. Puhelinnumeron varmistus.

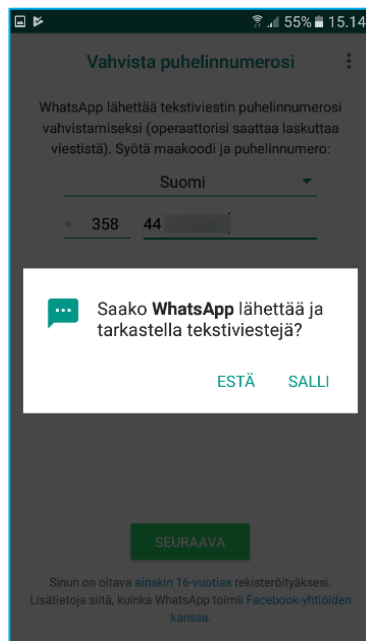
Puhelinnumeron varmistamisen jälkeen ruutuun tulee kuvan 8 mukainen seloste. Selosteessa kerrotaan, että WhatsApp pyytää lupaa lukea tekstiviestejäsi. Luvan antaminen ei ole suositeltavaa. WhatsApp ei tarvitse toimintaansa pääsyä käyttäjän tekstiviesteihin. Kyseinen ominaisuus on vähintäänkin epäilyttävä. WhatsApp pyytää lupaa lukea tekstiviestejä, että se voi automaattisesti lukea rekisteröinnin tarkistuskoodin. Kun puhelinnumero rekisteröidään palveluun, niin WhatsApp lähettää tekstiviestin,

joka sisältää tarkistuskoodin rekisteröityyn puhelinnumeroon. Käyttäjä voi syöttää koodin itse.

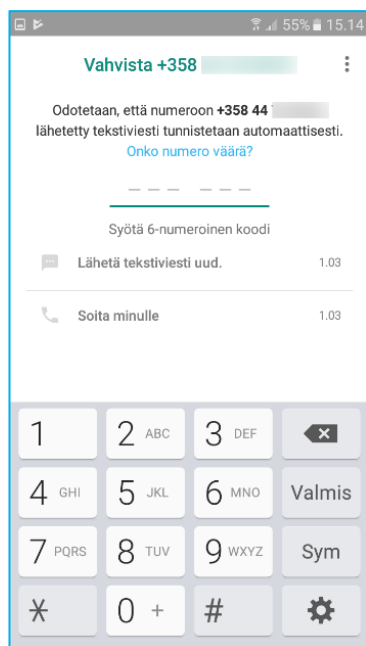
Vastaa kuvassa 9 näkyvään kyselyyn **ESTÄ**. Kun olet saanut rekisteröintikoodin tekstiviestinä, niin syötä kuusi numeroinen koodi kuvan 10 mukaiseen WhatsAppin koodikenttään. Kun olet syöttänyt koodin WhatsApp jatkaa automaattisesti tarkastusta.



Kuva 8. Tekstiviestien käyttöoikeus selostus.

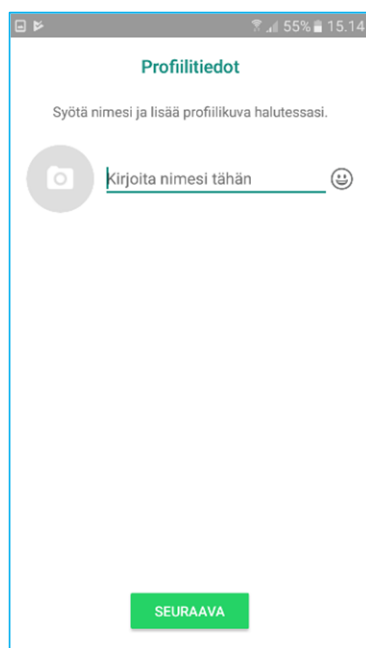


Kuva 9. Tekstiviestien käyttöoikeus kysely.



Kuva 10. Vahvistuskoodin kysely.

Kun tunnus on luotu ja puhelinnumero on rekisteröity, niin WhatsApp pyytää käyttäjää syöttämään nimensä. Tähän ei ole pakko laittaa omaa nimeä, jos sitä ei halua käyttää. Voit vaihtoehtoisesti käyttää valitsemaasi käyttäjänimeä. Painamalla nimikentän vieressä olevaa kameran kuvaa voit halutessasi lisätä WhatsApp-profiilillesi profiilikuvan. Profiilikuvan käyttö ei ole pakollista. Täytä kuvan 11 mukaiseen näkymään haluamasi tiedot. Kun olet syöttänyt nimesi/käyttäjänimen niin paina vihreää **SEURAAVA** painiketta.

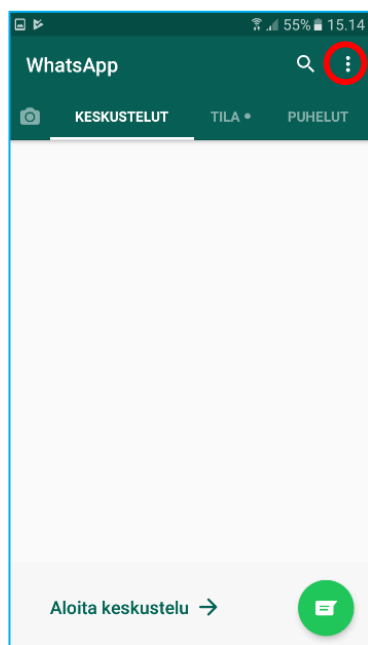


Kuva 11. Nimisyöte.

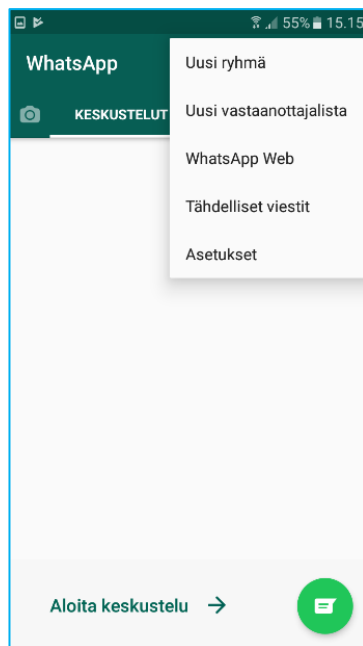
Nyt WhatsApp on asennettu ja käyttäjätilisi on luotu. Ennen kuin aloitat viestinnän WhatsAppilla, niin on suositeltavaa muuttaa sovelluksen asetuksia. Tarvittavat muutokset käydään läpi seuraavassa kappaleessa.

### 6.3 WhatsAppin asetusten muuttaminen

WhatsAppin asetukset löytyvät sovelluksen oikeassa yläkulmassa olevan kolmipiste-valikon alta, joka on ympyröity punaisella kuvassa 12. Kun kuvan 13 mukainen valikko aukeaa, niin valitse listalta **Asetukset**.

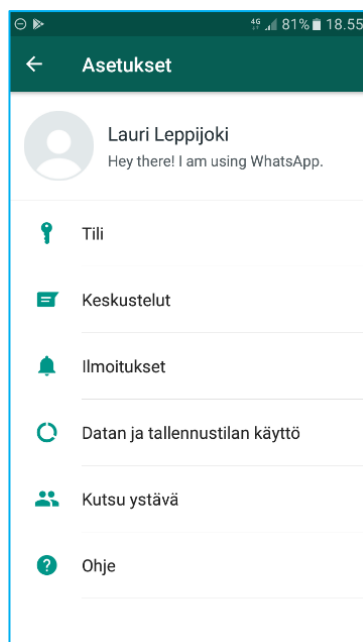


Kuva 12. Kolmipiste-valikko.



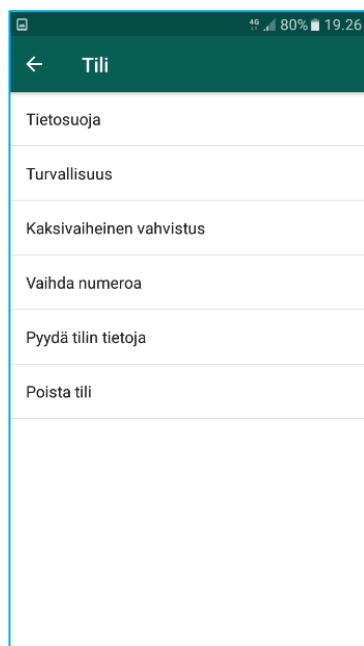
Kuva 13. Asetukset.

Ensimmäiseksi muokataan käyttäjätilin tietosuoja-asetuksia. Valitse kuvan 14 mukaisesta **Asetukset**-valikosta kohta **Tili**. Kun olet kuvan 15 mukaisessa **Tili**-valikossa, niin valitse **Tietosuoja**.



Kuva 14. WhatsApp asetukset.





Kuva 15. WhatsApp tilin-asetukset.

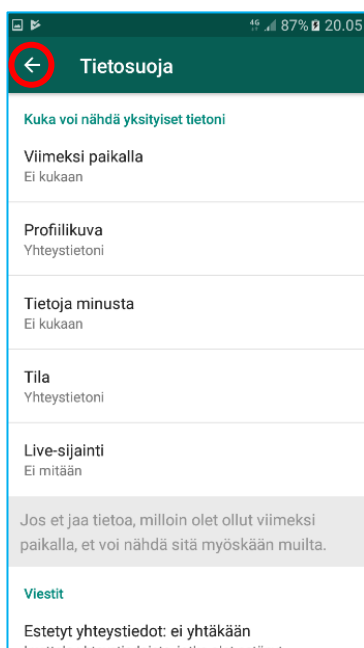
Huomioi, että seuraavat asetukset ovat vain suosituksia. Jokainen voi itse valita haluamansa asetukset.

Kuvassa 16 on esimerkki WhatsAppin tietosuoja-asetusten näkymästä. Muuta kohtaan **Viimeksi paikalla**, joko **Yhteystietoni** tai **Ei kukaan**. Jos valittuna on **Kaikki**, niin WhatsAppin käyttöäsi voidaan seurata lisäämällä puhelinnumerosi WhatsAppin yhteystietoihin. Sillon kuka tahansa näkee koska olet viimeksi lukenut tai lähettänyt viestejä.

Kohtaan **Profiilikuva** suosittelen asettamaan **Yhteystietoni** tai **Ei kukaan**. Tämä asetus on tärkeä etenkin silloin, jos profiilikuvana on kuva, josta sinut voidaan tunnistaa. Jos valittuna on **Kaikki**, niin lisäämällä puhelinnumerosi WhatsAppin yhteystietoihin kuka tahansa voi nähdä profiilikuvasi.

Kohta **Tietoja minusta** koskee **Asetukset**-valikossa käyttäjänimen alla olevaa tekstiä. Tämän asetuksen tärkeys riippuu siitä, mitä olet asettanut **Tietoja minusta**-tekstiksi. Jos et muokkaa esiasetettua ”Hey there! I am using WhatsApp.”-tekstiä, niin tällä ei ole kovin suurta merkitystä tietosuojan kannalta. Kuitenkin suosittelen asettamaan tähän joko **Yhteystietoni** tai **Ei kukaan**.

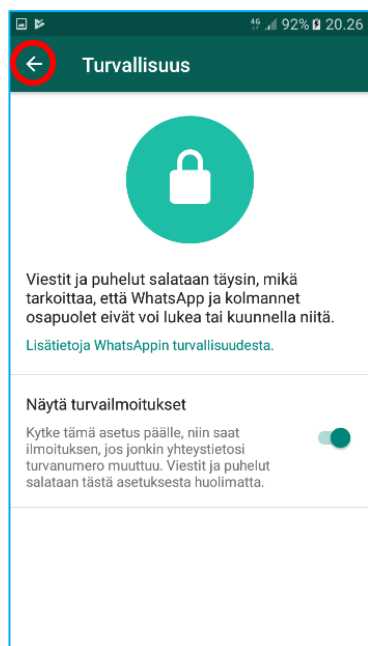
Omaa sijaintia ei tulisi koskaan jakaa WhatsAppin välityksellä! En suosittele antamaan WhatsAppille sijainnin käyttöoikeutta sitä pyydettyäessä. Jos kuitenkin jostain syystä päätät jakaa sijaintisi keskustelussa, niin kohdassa **Live-sijainti** näet aktiiviset sijainnin jakosi ja voit keskeyttää ne.



Kuva 16. WhatsApp tietosuoja-asetukset.

Seuraavaksi voit palata **Tili**-valikkoon painamalla sovelluksen vasemmassa yläkulmassa olevaa nuolta, joka on ympyröity punaisella kuvassa 16. Valitse kuvan 15 mukaisesta valikosta kohta **Turvallisuus**. Ruutuun tulee näkyviin kuvan 17 mukainen näkymä, jossa suosittelen kytkemään päälle **Näytä turvailmoitukset**-asetuksen.

Tällä asetuksella voit varmistaa, että keskusteluissa olevat jäsenet ovat ”aitoja”. Kun tämä asetusta on päällä, niin saat ilmoituksen, jos keskustelujesi jäsenen turvanumero muuttuu. Turvanumero muuttuu yleensä silloin, kun WhatsApp asennetaan uudestaan tai joku vaihtaa puhelimensa uuteen. Turvanumeron muuttuminen voi kuitenkin myös tarkoittaa sitä, että keskustelussa olevan jäsenen tili on kaapattu. Jos saat ilmoituksen keskustelun jäsenen turvanumeron muuttumisesta, niin suosittelen tarkastamaan asianomaiselta, että onko hän tehnyt muutoksia WhatsAppiinsa.



Kuva 17. WhatsApp turvallisuus-asetukset.

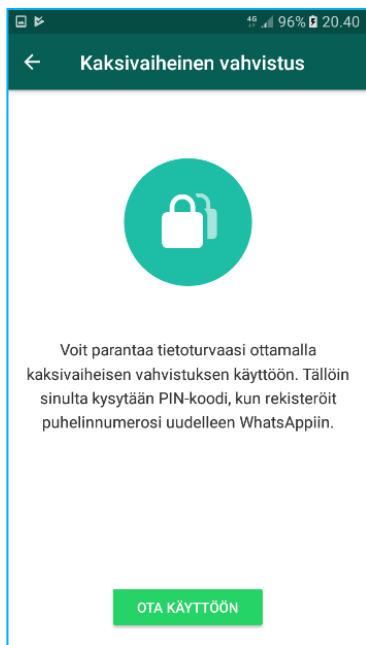
Nyt voit poistua **Turvallisuus**-valikosta painamalla sovelluksen vasemmassa yläkulmassa olevaa nuolta, joka on ympyröity punaisella kuvassa 17. Valitse sen jälkeen kuvan 15 mukaisesta **Tili**-valikosta kohta **Kaksivaiheinen vahvistus**.

Suosittelen ottamaan **Kaksivaiheisen vahvistuksen** käyttöön koska tämä vaikeuttaa tilisi kaappaamista. Kun tämä asetus on päällä, niin WhatsApp pyytää asettamaasi kuusinnumeroista PIN-koodia aina, kun puhelinnumeroasi yritetään rekisteröidä WhatsAppiin uudelleen tai tilillesi kirjaututaan uudelleen. Uudelleen kirjautuminen tapahtuu yleensä puhelimen uudelleen käynnistymisen jälkeen. Suosittelen asettamaan myös tilillesi palautus sähköpostiosoitteen, joka pyydetään **Kaksivaiheista vahvistusta** käyttöönottaessa. Sen avulla voit palauttaa tilisi, vaikka unohtaisit WhatsApp pin-koodin.

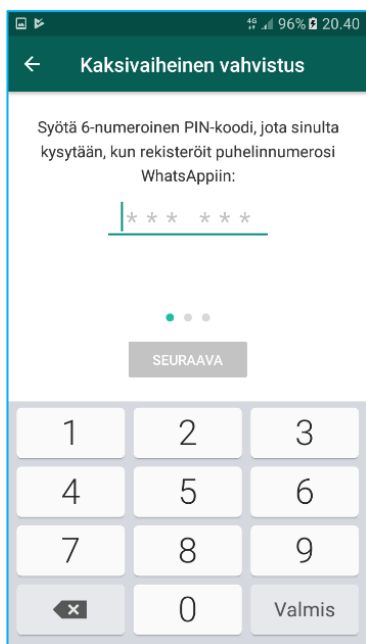
Kuvan 18 mukaisessa **Kaksivaiheinen vahvistus** näkymässä paina vihreää **OTA KÄYTTÖÖN** painiketta. Seuraavaksi aukeaa kuvan 19 mukainen näkymä. Syötä valitsemasi kuusinnumeroinen PIN-koodi ja paina **SEURAAVA**. Syötä PIN-koodisi uudelleen ja paina **SEURAAVA**.

Kuvan 20 mukaisessa näkymässä voit syöttää sähköpostiosoitteen, jota haluat käyttää WhatsAppin PIN-koodin palautus osoitteena. Sähköpostiosoitteen asettaminen ei ole

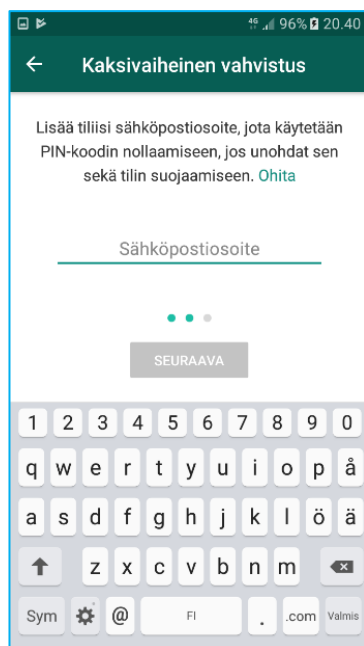
pakollista **Kaksivaiheisen vahvistuksen** käyttöönotossa. Jos et halua asettaa sähköpostiosoitetta paina **Ohita**. Kun olet syöttänyt sähköpostiosoitteesi paina **SEURAAVA**. Syötä sähköpostiosoite uudelleen ja paina **TALLENNA**.



Kuva 18. WhatsApp kaksivaiheisen vahvistuksen käyttöönotto.



Kuva 19. WhatsApp kaksivaiheisen vahvistuksen pin-koodin valinta.



Kuva 20. WhatsApp kaksivaiheisen vahvistuksen varmistus sähköpostin valinta.

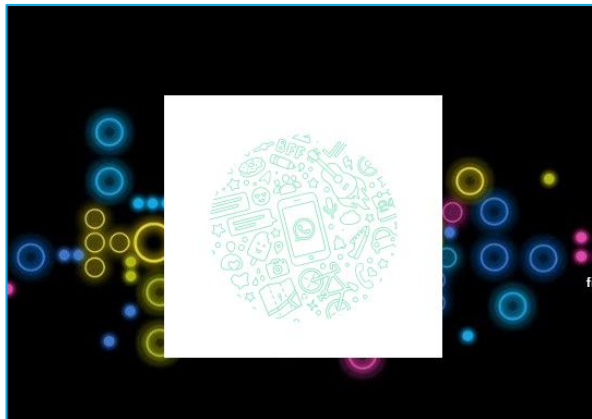
Nyt WhatsApp on käyttöön otettu tietoturvallisesti puhelimellasi ja voit aloittaa viestimisen. En kuitenkaan suosittele lähettämään WhatsAppin välityksellä työhön liittyviä tiedostoja tai tietoja. Yrityksille on tarjolla lukuisia kohtuuhintaisia viestintäalustoja, joiden tietoturva ja tietosuojat on suunniteltu yrityskäyttöön. Vain harva sovellus on oikeasti ilmainen.

#### 6.4 WhatsAppin käyttöönotto työasemalla

Seuraavaksi käydään läpi, miten WhatsApp otetaan käyttöön tietokoneella. Ohjeen aikaisempi osuus on välttämätön, jotta saat WhatsAppin työasemaversioon käyttöösi.

WhatsAppin työasemaversioon saa ladattua osoitteesta: <https://www.whatsapp.com/download/>. WhatsAppia ei koskaan tule ladata työasemalle kolmannen osapuolen lähteistä. Epävirallisten lähteiden sovellukset voivat sisältää haitallista koodia tai muita haitallisia ominaisuuksia, eikä virustorjuntaohjelmistot välttämättä osaa havaita niitä.

Kun olet ladannut asennustiedoston (WhatsAppSetup.exe) työasemalle, niin tupla klikkaa sitä hiiren vasemman puoleisella painikkeella. Näytölle ilmestyy kuvan 21 mukainen vaalea kuvioitu neliö, kun asennusta suoritetaan.



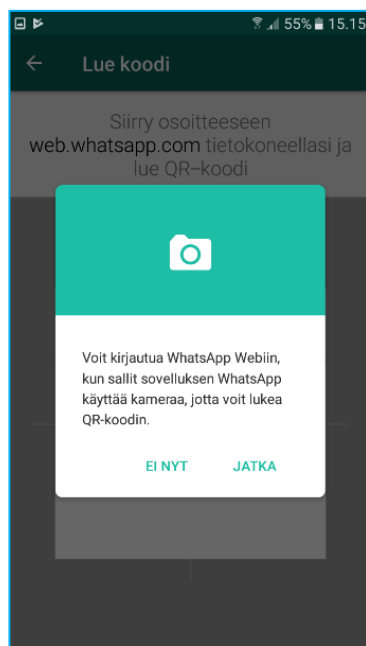
Kuva 21. WhatsApp työpöytä asennus.

Kun asennus on valmis WhatsApp aukeaa automaattisesti. Nyt tarvitset puhelimen, johon WhatsApp on käytöönnotettu. Avaa puhelimesi WhatsApp ja sen jälkeen soveluksen oikeassa yläkulmassa oleva kolmipiste-valikko, joka on ympäröity punaisella kuvassa 12. Sen jälkeen valitse kuvan 13 mukaisesta valikosta **WhatsApp Web**.

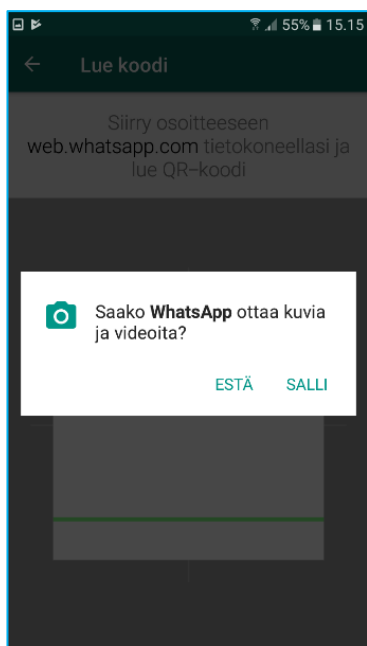
Kuvan 22 mukaisessa näkymässä paina oikeassa alakulmassa olevaa **OK**-painiketta. Nyt WhatsApp pyytää lupaa käyttää puhelimesi kameraa. Jos haluat käyttää WhatsAppin työpöytä sovellusta, niin sinun on annettava kameran käyttöoikeus. Käyttöoikeuden voi myös perua toimenpiteen jälkeen puhelimen asetuksista. Paina kuvan 23 näkymässä **JATKA**, jos haluat antaa käyttöluvan WhatsAppille. Näyttöön tulee kuvan 24 mukainen kysely, jos sallit kameran käyttöoikeuden niin paina **SALLI**.



Kuva 22. WhatsApp QR-ohje.

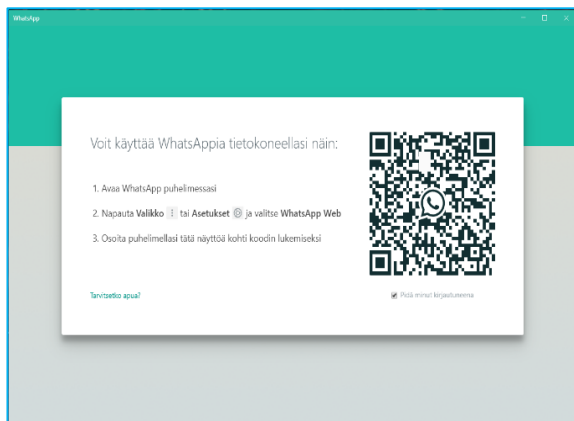


Kuva 23. WhatsApp kamerankäyttöoikeus seloste.



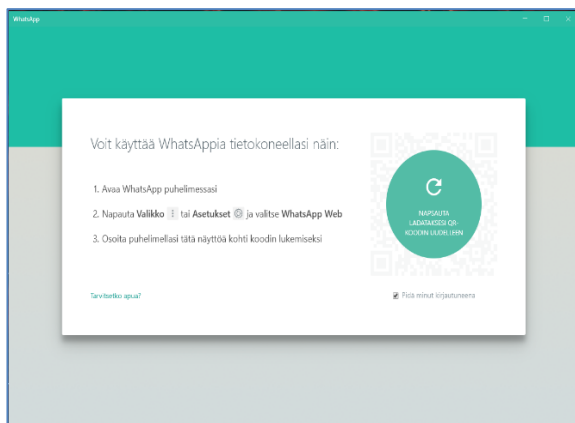
Kuva 24. WhatsApp kamerankäyttöoikeus kysely.

Työasemalla pitäisi olla näkyvissä kuvan 25 mukainen näkymä. Osoita puhelimen kamera kohti WhatsAppin työpöytä sovelluksen QR-koodia niin, että koodi näkyy kokonaan rajatulla alueella. Kun sovellus on lukenut koodin, se etenee automaattisesti. Jos QR-koodia ei näy, niin paina kuvan 26 mukaisessa näkymässä **NAPSAUTA LADATAKSESI QR-KOODIN UUDELLEEN** painiketta.



Kuva 25. WhatsApp QR-koodi työasemalla.





Kuva 26. Lataa WhatsApp QR-koodi uudelleen.

Nyt WhatsApp on otettu onnistuneesti käyttöön myös tietokoneella. WhatsAppin työpöytäversio on todella pelkistetty asiakasohjelma. WhatsAppin asetuksia säädetään puhelimelta, eikä puhelinversion käyttöä voi lopettaa kokonaan, vaikka käyttäisi pääasiallisesti WhatsAppia työasemaltaan käsin. WhatsApp työpöytä version käyttö vaatii, että tiliin rekisteröity puhelin on päällä ja että siinä on Internet-yhteys.

## 7 YHTEENVETO JA POHDINTA

### 7.1 Yhteenveto

Pikaviestimiin kohdistuvat hyökkäykset ja niiden hyödyntäminen hyökkäyksissä yleistyy nopealla vauhdilla. Suurin uhka on yksittäiseen työntekijään kohdistuva tietojenkalastelu. Siksi olisi tärkeää kouluttaa koko organisaatiota tietoturvalliseen työskentelyyn. Omien laitteiden käyttö työelämässä lisää merkittävästi pikaviestimien aiheuttamaa riskiä, jonka vuoksi koko henkilöstön tietoturallinen työskentely on tärkeää.

Jokainen yrityksen verkkoon liitetty laite on riski eivätkä automatisoidut järjestelmät ole koskaan pettämättömiä. Tietotekniset työkalut kehittyvät helpommiksi käyttää, jonka myötä niiden käyttö arkipäiväistyy. Lisäksi työelämässä saatetaan käyttää täysin samoja alustoja viestintään, mitä ihmiset käyttävät arjessa. Nämä lisäävät inhimillisten virheiden riskiä huomattavasti. Yrityksien olisikin hyvä käyttää viestintään alustaa, joka on tarkoitettu yritys käyttöön.

Paras suojaus pikaviestimien välityksellä leviäviä uhkia vastaan on siis vaarojen tiedostaminen. Pikaviestimet ovat usein ihmisten elämässä kellon ympäri ja siksi jokaisen olisi hyvä tutustua niiden käyttöön liittyviin riskeihin.

### 7.2 Pohdinta

Opinnäytetyön tekeminen oli projektina kiinnostava sekä opettavainen. Olin tutustunut aiheeseen jo ennen projektin alkua, mutta huomasin nopeasti, että se on erittäin hankala spesifisen olemuksensa vuoksi. Jouduin muuttamaan työn rakennetta useasti ennen kuin opin hahmottamaan miten avaan aihetta lukijalle pysymällä kuitenkin valitsemani aiheen sisällä.

Aloitin työn lukemalla tietoturvaa ja tietosuojaa käsittelevää kotimaista kirjallisuutta. Omaan työhöni en kuitenkaan löytänyt niistä paljon materiaalia, koska pikaviestimiä

käsitellään harvoin omana asiana, jos ollenkaan. Kuitenkin tietoturvan ja tietosuojan juridinen puoli aukesi minulle paremmin ja opin määrittelemään ne omina kokonaisuuksinaan.

Opin projektin aikana, että pikaviestimien tietoturva ja tietosuoja on käytännössä käyttäjän sekä organisaation harteilla. Sain työtä tehdessäni todella hyvän kuvan siitä, kuinka tärkeää käyttäjien koulutus on tietoturvan kannalta. Yllättävintä oli huomata, miten suuri vaikutus laitevalmistajilla on mobiililaitteiden tietoturvaan ja miten paljon ne voivat vaikuttaa tarjolla oleviin mobiililaitteiden tietoturvaratkaisuihin.

Toiminnallisessa osuudessa päätin tehdä ohjeen WhatsAppin käyttöönottoon android-laitteella, koska se oli minusta luonnikkain tapa tuoda esiin pikaviestimen kyseenalaisia ominaisuuksia. Päätin jo työtä suunnitellessa, että en halua verrata sovelluksia keskenään, sillä en kokenut sitä konseptiini sopivaksi. Perehtyessäni WhatsAppin tietosuoja-asetuksiin opin kyseenalaistamaan entistä paremmin sovellusten esiasetettuja asetuksia.

## LÄHTEET

Andreasson,A., Koivisto,J., Ylipartanen,A. 2013. Tietosuojavastaavan käsikirja. Helsinki: Tietosanoma Oy

BALAJI,N. 2018. Spyware Discovered that Almost Steal Everything in Your Mobile. GBHackers On Security Viitattu 17.8.2018 Saatavilla: <https://gbhackers.com/skygo-free-android-spyware/>

Bishop,A. 2012. Skype Case Study. NetHosting Viitattu 15.7.2018. Saatavissa: <https://nethosting.com/skype-case-study/>

Boyd,C. 2018. Keeping your business and personal instant messages secure. Malwarebytes Labs Viitattu: 16.8.2018 Saatavilla: <https://blog.malwarebytes.com/101/2018/04/keeping-your-business-and-personal-instant-messages-secure/>

Burrell,H.2017. How secure is WhatsApp? WhatsApp security and encryption explained. Tech Advisor Viitattu 21.7.2018 Saatavissa: <https://www.techadvisor.co.uk/feature/internet/how-secure-is-whatsapp-whatsapp-security-encryption-explained-3637780/>

Continuity Central. 2017. The security and compliance issues related to instant messaging use. Viitattu 4.8.2018 Saatavilla: <https://www.continuitycentral.com/index.php/news/technology/2270-the-security-and-compliance-issues-related-to-instant-messaging-use>

Continuum. Everything You Need to Know about Mobile Device Management (MDM). Support Viitattu 14.9.2018 Saatavilla: <https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm>

Drolet,M. 2018. The rise of mobile phishing attacks and how to combat them. CSOnline. Viitattu 22.8.2018 Saatavilla: <https://www.csoonline.com/article/3268109/phishing/the-rise-of-mobile-phishing-attacks-and-how-to-combat-them.html>

Foult,T. 2018. Skype: Everything you need to know!. iMore Viitattu 13.7.2018. Saatavissa: <https://www.imore.com/skype>

Hakala, M., Vainio, M., Vuorinen,O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docento Finland Oy

Kennedy,D. 2012. The Security Pro's Guide To MDM, MAM, MIM, and BYOD. TrustedSec viitattu 24.8.2018 Saatavilla: <https://www.trustedsec.com/2012/09/the-security-pros-guide-to-mdm-mam-mim-and-byod/>

Kratikal Tech Pvt Ltd. 2018. Humans are the weakest link in the information security chain. Medium Viitattu 25.9.2018 Saatavilla: <https://medium.com/@kratikal/humans-are-the-weakest-links-in-cyber-security-of-any-organisation-ac04c6e6e71>

Microsoft. 2018. What's the difference between Skype, Skype Meetings, and Skype for Business?. Support Viitattu 13.7.2018. Saatavissa: <https://support.skype.com/en/faq/FA34551/what-s-the-difference-between-skype-skype-meetings-and-skype-for-business>

Newman,L. 2018. Encrypted Messaging Isn't Magic. Wired Viitattu 25.10.2018 Saatavilla: <https://www.wired.com/story/encrypted-messaging-isnt-magic>

Phisme. 2016. Phishing Susceptibility and Resiliency Report. Viitattu 21.8.2018 Saatavilla: <https://www.bankinfosecurity.com/whitepapers/enterprise-phishing-susceptibility-resiliency-report-w-3055#dynamic-popup>

Rouse,M. 2017. Skype for Business. TechTarget Viitattu 13.7.2018 Saatavissa: <https://searchunifiedcommunications.techtarget.com/definition/Skype-for-Business>

Rousku, K. 2014. Kyberturvaopas: Tietoturvaa kotona ja työpaikalla.Talentum Media Oy

Rousseau,C,L. 2018. WhatsApp: Everything you need to know!. iMore Viitattu 19.7.2018 Saatavissa: <https://www.imore.com/whatsapp>

Yksityisyydensuoja. 2018. Verkkourkinta. Viitattu 17.8.2018 Saatavilla: <https://www.yksityisyydensuoja.fi/verkkourkinta>