F-SECURE TOTAL PALVELUKUVAUS

Sisällysluettelo

F-SECURE TOTAL

YLEISKUVAUS

F-Secure TOTAL on lisämaksullinen palvelu, joka koostuu seuraavista F-Securen tuotteista: SAFE, ID Protection ja Freedome VPN. F-Secure SAFE –tuote on myös mahdollista ostaa erikseen, mikäli tilaa suojauksen vain yhdelle laitteelle. Kuukausimaksullinen palvelu tarjoaa kattavan suojan viruksia, haitta- ja vakoiluohjelmia, sekä muita Internetin uhkia vastaan, salasanojen hallintasovelluksen ID Protectionin sekä yksityisyyden suojan tarjoavan VPN-ohjelmiston Freedome VPN. TOTAL –sovellusten hallinta tapahtuu My F-Secure hallintasivustolla. Palvelu myydään kulloinkin voimassaolevan hinnaston mukaisesti.

1. F-Secure SAFE

F-Secure SAFE sisältää useita ominaisuuksia, joista tarkemmat kuvaukset edempänä. SAFE suojaa tietokonetta tai mobiililaitetta ulkopuolisilta uhilta kuten viruksilta ja haittaohjelmilta, mutta myös henkilökohtaisten tietojen karkaamiselta rikollisten käsiin. Ominaisuuksien toiminnassa saattaa olla päätelaitekohtaisia eroja ja ominaisuudet saattavat muuttua käyttöjärjestelmien omien päivitysten myötä. Ajantasaisimmat tiedot löydät osoitteesta www.f-secure.fi.

1.1. Viruksen torjunta

Haittaohjelmilta suojaus toimii kaikissa avoimissa käyttöjärjestelmissä (Win, Mac, Android), jotka ovat haavoittuvaisempia uhille. Haittaohjelmien suojaus suojaa laitetta viruksia, troijalaisia ja haittaohjelmia vastaan, jotka voivat kerätä henkilökohtaisia tietojasi, kuten luottokortin tiedot tai pankkitunnukset. Haittaohjelmien suojaus ehkäisee laitettasi joutumasta osaksi suurempaa rikollisten toteuttamaa verkkohyökkäystä sekä suojaa tiedostojasi lukittumasta lunnastroijalaisen toimesta.

Automaattinen ja reaaliaikainen virusten torjunta tutkii koneelle pyrkiviä ja asennettavia ohjelmia ja tiedostoja jatkuvasti. Se tunnistaa ennalta määriteltyjä malleja tiedostoista ja tarvittaessa eristää saastuneet tiedostot ja pyytää poistamaan ne. Tietokoneen tarkastuksen ja puhdistamisen voi suorittaa manuaalisesti tai asettaa tarkastuksen automaattiseksi. Keskeisintä haittaohjelmien tunnistamisessa on reaaliaikaisuus, jolloin uudet tunnistetut uhat ovat heti kaikkien F-Secure SAFE -tuotetta käyttävien laitteiden tiedossa ja niiden pääsy laitteelle estetään.

1.2. Palomuuri

Palomuuri on keskeinen osa tietoturvaa, jonka avulla suodatetaan laitteeseen saapuvaa ja lähtevää liikennettä ja estetään mahdollisia tunkeutumisyrityksiä. Palomuurin ominaisuudet riippuvat laitteen käyttöjärjestelmästä. PC ja Mac versiossa käytetään käyttöjärjestelmän omaa palomuuria parhaimman yhteensopivuuden takaamiseksi. Mac versiossa palomuuri ei yleensä ole oletuksena päällä, mutta SAFE kytkee sen käyttöön.

PC versiossa normaalin TCP/IP tason lisäksi SAFE osaa ottaa kantaa myös sovellustason käyttäytymiseen. Tällä tarkoitetaan sitä, että sovellusten tekemää kommunikointia ulkomaailmaan seurataan reaaliaikaisesti ja epäilyttäviin viestintäpyyntöihin reagoidaan estämällä sovellus.

1.3. Etsintätoiminto

Etsintätoiminto tarjoaa turvaa tilanteisiin, jossa laite (Android tai iOS) on hävinnyt tai varastettu. Etsintätoiminto on käytettävissä My F-Secure hallintaportaalista, silloin kuin SAFE on asennettuna lapsen laitteeseen tai omaan laitteeseen.

Etsintätoiminto tarjoaa seuraavat toiminnot My F-Secure portaalissa: laitteen paikannus, hälytys, lukitse ja pyyhi tiedot. Laitteen paikannus näyttää kadonneen laitteen kartalla. Hälytys aktivoi laitteeseen kovaäänisen hälytysäänen, joka sammuu vasta kun laitteen näyttö aktivoituu. Lukitse toiminto lukitsee näytön lukituksen (vaatii, että laitteeseen on otettu käyttöön jokin näytön lukitustapa esim. PIN-koodi, sormenjälki, kuvio tai salasana). Pyyhi tiedot –toiminto aktivoi tehdasasetusten palautuksen ja tyhjentää laitteen muistin ja mahdolliset laitteeseen kytketyt muistikortit.

Lukitse ja pyyhi tiedot ovat käytettävissä vain Android –laitteissa. Etsintätoiminto edellyttää, että laite on päällä, internet-yhteydessä ja että SAFE sovellus on aktiivinen.

1.4. Selaus- ja verkkopankkisuojaus

Selauksen suojaus huolehtii taustalla turvallisesta verkkokauppa- ja pankkiasioinnista, estää haitalliset sivustot ja varoittaa epäilyttävästä sisällöstä. Selauksen suojaus estää pääsyn vaarallisille sivustoille ja suojaa näin mm. avaamasta huijaussähköpostista ohjautuvia linkkejä väärennetyille pankkisivustoille.

Pankkitoimintojen suojaus on erittäin tärkeä ja näkyvä osa selauksen suojausta. Sen avulla käyttäjä tietää olevansa oikean pankin sivuilla, sekä nettipankin käytön olevan turvallista.

1.5. Perhesäännöt

Perhesäännöt tarjoavat useita ominaisuuksia koko perheen suojaustarpeisiin. Ominaisuudet ovat esiteltynä alla. Ominaisuuksien hallinta tapahtuu My F-Secure hallintaportaalin kautta. Ominaisuudet aktivoituvat käyttöön, kun SAFE sovellus on asennettu ja määritetty lapsen profiililla käyttöön.

Sisällön suodatus

Sisällönsuodatuksen avulla Internet sivustoista voi luokitella pois haitalliset sisällöt, kuten aikuisviihde, väkivalta, ostaminen, pelaaminen, sosiaalinen media jne. Sivustojen käyttö estetään sisältöluokituksen perusteella, jonka voi valita ikäryhmän mukaan. PC:ssä sisällönsuodatus on käytössä jokaiselle käyttäjälle (Windows –käyttäjätili) erikseen. Android ja iOS –sisällönsuodatus toimii SAFE tuotteen asennuksen yhteydessä asennetussa SAFE Browser –internet selaimessa.

Aikarajoitukset

Aikarajoitukset ominaisuuden avulla voit ottaa lapsesi ajankäytön paremmin hallintaan. Voit määrittää päivittäisen aikarajan laitteen sovellusten käytölle (rajoittamaton tai 15min-8h). Määrityksen voi tehdä erikseen viikonpäiviksi (maanantai-perjantai) ja viikonlopuiksi (lauantai ja sunnuntai). Soittaminen ja tekstiviestien lähettäminen on aina sallittua.

Nukkumaanmenoaika

Nukkumaanmenoaika ominaisuuden avulla voit rajoittaa niiden sovellusten käyttöä öisin, jotka olet määrittänyt aikarajoitteisiksi. Määrityksen (esim. klo 20.00-08.00) voi tehdä erikseen kouluilloille (sunnuntai-torstai) tai viikonloppuiltoihin (perjantai ja lauantai). Soittaminen ja tekstiviestien lähettäminen on aina sallittua.

Sovellusten hallinta

Sovellusten hallinnan avulla vanhemmat voivat sallia ja estää tiettyjen sovellusten toiminnan lapsen laitteessa. Sovelluskohtaisesti voidaan myös määrittää koskevatko aikarajoitukset sovelluksen käyttöä.

1.6. Yksityisyyden suoja

Yksityisyyden suoja on ominaisuuksien yhdistelmä, joka suojaa henkilökohtaisia tietoja digitaalisessa maailmassa. Selauksen suojaus ehkäisee sinua joutumista huijaus- tai tietojenkalastelusivustoille, haittaohjelmien suojaus turvaa laitteesi, ettei toimintaasi seurata salaa tai sinusta kerätä tietoja ja tarvittaessa voit lukita puhelimen etänä tai jopa tyhjentää sen tiedot, jos laite joutuu vääriin käsiin.

SAFE Android laitteille mahdollistaa turvallisen Internet sivujen selauksen lisäksi myös sovellusten, jotka antavat vähän, mutta ottavat paljon, suojaamisen. Monet sovellukset pyytävät luvan moniin henkilökohtaisiin tietoihisi, kuten yhteystietoihin, kameraan ja mikrofoniin, vaikkeivat välttämättä näitä

ominaisuuksia käyttäisikään. Tyypillisin luvan pyyntö on paikkatietoon, mikä ei esim. pelisovellukselle ole välttämättä mitenkään relevantti, mutta sovelluksen tuottaja kerää näin käyttäjistään paljon henkilökohtaista tietoa ehkä johonkin muuhun tarkoitukseen. Kaikkeen tietojen luovuttamiseen kannattaakin suhtautua pienellä varauksella. Androidin SAFE sovelluksesta näet sovellusten käyttämät luvat sekä listauksen sovelluksista, joissa on monia mahdollisia yksityisyys uhkia.

1.7. Kiristysohjelmasuojaus

SAFE:n PC-ohjelmisto sisältää kiritysohjelmasuojauksen, jossa tiettyjä kansioita/hakemistoja valvotaan jatkuvasti ja kaikki hakemistoon tapahtuvat muutokset tai toiminnot pysäytetään, mikäli niissä havaitaan riskialtista käyttäytymistä. Näistä näytetään aina käyttäjälle varoitus. Kiristysohjelmasuojaus tuo lisäsuojauskerroksen normaalin suojaustoiminnan lisäksi.

2. F-Secure ID Protection

ID Protection on helppokäyttöinen ratkaisu, jolla suojaat verkon identiteettisi. ID Protection tarjoaa salasananhallinnan ”Holvin” ja tietovuotojen valvonnan ”Monitorointi”.

Sovellukseen voit tallentaa tietoturvallisesti käyttäjätunnukset, salasanat, PIN-koodit ja esimerkiksi luottokorttitiedot. Vahva salaus suojaa kaikki merkinnät ulkopuolisilta, vaikka menettäisit laitteen. Lisäksi F-Secure ilmoittaa käyttäjälle välittömästi, jos se havaitsee tietovuotoja, joissa on ollut osallisena käyttäjän sähköposti tai muita henkilökohtaisia tietoja. Näin käyttäjä ehtii reagoimaan ennen kuin rikolliset ehtivät käyttää tietoja väärin.

ID Protection sovelluksen käyttöönoton yhteydessä määritetään pääsalasana, jota ei ole mahdollista nollata myöhemmin. Sovelluksen pääsalasana kysytään aina sovellusta avattaessa (Android ja iOS – laitteissa voi avauksen tehdä sormenjälkitunnistimella). Pääsalasanan luonnin jälkeen ID Protection ehdottaa salasanan tallentamista QR-koodi kuvaksi. Kuvan voi tulostaa tai tallentaa itselleen. QR-kuva on ainut tapa kirjautua, mikäli pääsalasanan unohtaa.

ID Protection toimii kaikissa laitteissa: Windows PC, Mac, Android ja iOS. Salasanat ja tiedot, joita tallennat synkronoituvat käyttämiesi laitteiden välillä, joten mukanasi on aina ajantasaiset tunnukset ja salasanat. Monitorointi on saatavana vain Android ja iOS sovelluksissa. ID Protectionin pääominaisuudet: ”Monitorointi” ja ”Holvi” ovat esiteltynä alla.

Monitorointi

F-Securen tietoturva-analyytikot seuraavat tietovuotoja 24/7, jonka vuoksi saat välittömästi tiedon, mikäli henkilötietosi ovat paljastuneet tietovuodossa. Tyypillisesti tällaisia henkilötietoja, ovat ne tiedot, joita käyttäjä on syöttänyt esimerkiksi rekisteröinnin yhteydessä (nimi, sähköpostiosoite, salasana, luottokortin numero jne.). ID Protection käyttää sähköpostiosoitetta yksilöllisenä tunnisteena ID-seurannassa, koska se on ainoa henkilökohtainen tunnistetieto, joka liitetään jokaiseen online-tiliin. Sovellus ilmoittaa käyttäjälle, jos käyttäjän henkilökohtaiset tiedot ovat olleet osana tietovuotoa, niitä on väärinkäytetty tai paljastettu verkossa. Monitoroinnin ominaisuudet ovat esiteltynä alla.

Monitoroinnin käyttöönotto

F-Secure ID Protection otetaan käyttöön mobiililaitteessa (Android tai iOS). Kun käyttäjä on kirjautunut sisään olemassa olevilla tunnistetiedoilla, häntä opastetaan salasananhallinnan asetusten määrittämisessä. Sitten käyttäjää pyydetään lisäämään ensimmäinen sähköpostiosoite valvontaa varten. Tästä sähköpostiosoitteesta tulee ensisijainen sähköposti myös tietovuotoja koskevissa ilmoituksissa. Käyttäjän on vahvistettava annettu sähköpostiosoite napsauttamalla vahvistusviestissä olevaa linkkiä. Vahvistus on välttämätön, jotta vältetään muiden ihmisten henkilökohtaisten tietojen väärinkäyttö. Kun sähköposti on vahvistettu, loppukäyttäjälle näytetään ensimmäiset tulokset. Tämä aloittaa myös jatkuvan seurannan. Monitorointiin on mahdollista lisätä kolme sähköpostiosoitetta.

Tietovuotojen hälytykset

F-Secure ID Protection lähettää välittömästi ilmoituksen sähköpostitse aina, kun käyttäjien henkilökohtaiset, valvotut tiedot ovat paljastuneet. Hälytykset näkyvät myös mobiilisovellusten käyttöliittymässä. Jos käyttäjä on käyttänyt vahvoja salasanoja, käyttäjä tietää, että tapahtuma rajoittuu kyseiseen palveluun. Jos käyttäjä on käyttänyt uudelleen tunnistetietoja, on kaikki palvelut helppo tunnistaa salasananhallintapuolen kautta.

Tietovuotojen tiedot

F-Secure ID Protection näyttää käyttäjälle tietovuodon vakavuuden ja kaikki arvokkaat henkilökohtaiset tiedot (tärkeät henkilökohtaiset tiedot). Tämä auttaa käyttäjää ymmärtämään vuotaneiden henkilökohtaisten tietojen vakavuuden. Käyttäjä voi myös paremmin ryhtyä välittömiin korjaaviin toimenpiteisiin vuotojen henkilökohtaisiin tietoihin liittyvien riskien vähentämiseksi esim. peruuttamalla luottokortin tai vaihtamalla salasanoja. Tietovuodot voivat sisältää tietoja, kuten sähköpostiosoite, salasana, koko nimi, kotiosoite, passin numero, luottokortin numero, sosiaaliturvatunnus, koordinaatit jne.

Suositellut toimenpiteet

Suositellut toimet on lueteltu tietovuodon tietojen lopussa. Suositeltavat toimet voivat sisältää yleisiä ohjeita tai tarkempia ohjeita tähän erityiseen tietovuotoon. Koska F-Secure ID Protection sisältää salasananhallintaominaisuudet, käyttäjä voi helposti esimerkiksi kirjautua sisään tietovuodon palveluun, luoda uuden vahvan ja yksilöllisen salasanan ja tallentaa sen turvallisesti sovellukseen.

Holvi

F-Secure painottaa eniten tietoturvallisuudessa alkuvaiheita. On parempi estää asioita tapahtumasta, kuin yrittää lieventää vahinkoja jälkikäteen. F-Secure ID Protection tarjoaa turvallisen tallennustilan salasanoille ja muille henkilökohtaisille tiedoille. ID Protection auttaa käyttäjiä parantamaan salasanan laatua, vaihtamaan heikot ja uudelleenkäytetyt salasanat vahvoiksi ja ainutlaatuisiksi salasanoiksi, jotta voidaan minimoida useiden palvelujen hakkeroinnin riski samanaikaisesti. Se osoittaa myös, käytetäänkö samoja salasanoja useissa paikoissa vai käyttäjät käyttävätkö heikkoja tai yleisiä salasanoja, jotka on helppo murtaa. Holvin ominaisuudet ovat esiteltynä alla.

Vahvojen salasanojen luonti

ID Protection auttaa sinua luomaan vahvoja ja yksilöllisiä salasanoja palveluihisi. Lisätessäsi uutta salasanaa, voit joko keksiä itse salasanan tai käyttää salasanageneraattoria luodaksesi varmasti vahvan ja yksilöllisen salasanan. Käyttäessäsi salasanageneraattoria, voit itse valita salasanan pituuden ja ehdot salasanan luontiin. Sovellus näyttää salasanan vahvuustason lopuksi.

Salasanojen hallinnointi

ID Protection kertoo tallennettujen salasanojen vahvuuden ja näin voit helposti vaihtaa salasanat, jotka ovat heikkoja ja mahdollisesti käytössä useissa palveluissa. Mikäli olet käyttänyt aiemmin jotain muuta salasanojen hallintaohjelmistoa, on sovellukseen mahdollista tuoda salasanat useista eri ohjelmista. ID Protection tukee ainakin seuraavia tiedostomuotoja: Password Safe XML, KeePass 2.x XML, 1Password 'interchange ja F-Secure ID Protectionin oma tiedostomuoto.

Salasanojen automaattinen täyttö

Automaattinen täyttö mahdollistaa käyttäjätunnuksen ja salasanan helpon täyttämisen www-sivujen kirjautumisnäytöissä. PC ja Mac –laitteissa tuettuina on Chrome ja Firefox selaimet. Käyttöönotto vaatii erillisen selainlaajennuksen asennuksen, jonka voi tehdä ID Protection sovelluksen Asetukset näkymältä. Automaattinen täyttö on käytössä myös Android ja iOS –laitteille.

3. F-Secure Freedome VPN

Älypuhelimet ovat yhtä aikaa korvaamattomia ja haavoittuvaisia. Ne ovat usein täynnä arkaluonteisia tietoja ja esimerkiksi käyttäessä julkista Wi-Fi verkkoa on mahdollista, että lähettämiäsi sähköposteja voidaan seurata. Haitalliset sivustot ja sovellukset voivat vuotaa vielä enemmän tietoja ja aiheuttaa valtavia puhelinlaskuja. F-Secure Freedome VPN varmistaa langattoman verkon turvallisuuden, suojaa yksityisyytesi ja tarjoaa mahdollisuuden muuttaa virtuaalista sijaintiasi, jolloin voit välttää netissä olevan sisällön käyttöön liittyviä rajoituksia.

VPN

Mobiililaitteiden VPN salaa mobiililaitteen ja valitun virtuaalisen sijainnin välisen liikenteen automaattisesti. Tämä mahdollistaa julkisten Wi-Fi- ja mobiiliverkkojen turvallisen käytön.
Se estää sähköpostien, selainistuntojen ja online-palvelujen salakuuntelun, ja lisää tietoturvakerroksen HTTPS-yhteyksille. Sen avulla voit myös vaihtaa virtuaalisen sijaintisi, piilottaa IP-osoitteesi ja käyttää paikallisia palveluja ulkomailla. Android-laitteiden ohjauskanavassa käytetään OpenVPN:ää ja AES-256-salausta, ja tiedoille käytetään AES-128:aa. iOS-laitteissa käytetään IPSECiä ja AES-256:ta. Jos käytössä on nopea verkkoyhteys, voi verkkoyhteyden nopeus hidastua käytettäessä Freedome VPN –sovellusta. Tämä johtuu siitä, että Freedome salaa ja reitittää verkkoliikenteen käyttämäsi virtuaalisen sijainnin kautta. Mitä kauempana virtuaalinen sijainti on, sitä kauemmin tietojen siirtäminen kestää. Myös OpenVPN:n tekniset rajoitukset vaikuttavat enimmäisnopeuteen.

Sovellusten suojaus

VPN-yhteyttä käytettäessä mobiililaitteet suojataan automaattisesti haittaohjelmilta ja haitalliselta sisällöltä. Android-laitteiden tietoturvaa on parannettu esimerkiksi paikallisella reaaliaikaisella mainetarkistuksella tietoturvapilvestä myös silloin, kun VPN-yhteyttä ei ole muodostettu. Kun applikaatio tai tiedosto ladataan, se tarkistetaan ja sille tehdään mainetarkistus. Haitallisten tiedostojen suoritus estetään ja tuntemattomat tiedostot ja sovellukset ladataan tarkempaa tarkistusta varten. Tarkistuksen tuloksista on etua kaikille käyttäjille, sillä niiden avulla voidaan esimerkiksi minimoida väärät hälytykset ja estää hyökkäykset.

Seurannan esto

Seurannan esto estää useimpia verkkopalveluita keräämästä tietoja käyttäjästä. Näitä tietoja ovat esimerkiksi haettu sisältö, avatut sivustot, klikatut bannerit, maantieteellinen sijainti ja niin edelleen. Seurannan esto estää erilaiset seurantamenetelmät, kuten evästeet, komentosarjat ja pikseliseurannan. Verkkoseuranta ja -mainonta on nykyään niin läpitunkevaa ja resursseja kuluttavaa, että niiden estäminen parantaa mobiililaitteen selausnopeutta jopa 30 %.

Virtuaalinen sijainti

Voit valita virtuaalisen sijainnin lähes 30 vaihtoehdosta, neljästä eri maanosasta. Tämän avulla on mahdollista käyttää ulkomaisia palveluita kotimaassa ja kotimaisia palveluita ulkomailla. Virtuaalinen sijainti piilottaa todellisen IP-osoitteesi ja näin ollen sitä ei voida liittää verkkotoimintaasi.

4. PALVELUKOMPONENTIT

4.1. F-Secure TOTAL

Palvelu sisältää pelkän tietoturvapalvelun tai tietoturvapalvelun sekä ID Protection ja Freedome VPN sovellukset jotka asiakas voi asentaa haluamilleen laitteille. F-Secure TOTAL paketteja on viisi erisuuruista:

- SAFE 1 (pelkkä tietoturvapalvelu SAFE yhdelle laitteelle)
- TOTAL 3 (SAFE, ID Protection ja Freedome VPN kolmelle laitteelle)
- TOTAL 5 (SAFE viidelle laitteelle, ID Protection ja Freedome VPN kolmelle laitteelle)
- TOTAL 8 (SAFE kahdeksalle laitteelle, ID Protection ja Freedome VPN kolmelle laitteelle)
- TOTAL 10 (SAFE kymmenelle laitteelle, ID Protection ja Freedome VPN kolmelle laitteelle)

Tietoturvan ominaisuudet riippuvat siitä mihin laitteeseen tai käyttöjärjestelmään ohjelmistoa ollaan asentamassa ja ne muuttuvat jatkuvasti tapahtuvan kehitystyön ansiosta.

4.1.1. Tuetut käyttöjärjestelmät

F-Secure SAFE

Windows 7 (SP1) tai uudempi, macOS 10.14 tai uudempi, Android 5.0 tai uudempi, iOS 12 tai uudempi

F-Secure Freedome VPN

Windows 7 tai uudempi, macOS 10.12 tai uudempi, Android 5.0 tai uudempi, iOS 11 tai uudempi

F-Secure ID Protection

Windows 7 tai uudempi, macOS 10.14 tai uudempi, Android 6.0 tai uudempi, iOS 13 tai uudempi

*Viimeisimmän listauksen tuetuista käyttöjärjestelmistä löydät www.f-secure.com/productlifecycle

Laitteisto- ja käyttöjärjestelmävaatimukset ovat kulloinkin palvelun tuottajan (F-Secure Oy) voimassa olevien määritysten mukaiset ja saattavat muuttua käyttöjärjestelmien päivittyessä.

4.2. Päivitykset

Tietoturvasovellukset päivittyvät automaattisesti, kun laitteessa on toimiva Internetyhteys. F-Secure tuottaa aika-ajoin isompia ohjelmiston versiopäivityksiä, joiden asennukseen vaaditaan asiakkaan hyväksyntä. Nämä päivitykset asiakkaan tulee hyväksyä, muutoin emme pysty takaamaan tietoturvan ajantasaisuutta. Päivitysten yhteydessä asiakkaan tulee hyväksyä myös mahdolliset F-Securen sopimusehdot.

5. TOIMITUS JA KÄYTTÖÖNOTTO

Palvelun voi tilata Lounean palvelupisteestä, asiakaspalvelusta tai asiakkaiden itsehallintaportaalista OmaLouneasta. Sähköpostiosoite on pakollinen tieto tilauksen tekemiseksi, sillä sähköpostiosoite toimii palvelun käyttäjätunnuksena. Kun tilaus on käsitelty Lounealla asiakas saa sähköpostiosoitteeseensa F-Securelta viestin, josta pääsee lataamaan ja asentamaan TOTAL –sovellukset. Viestissä toimitetaan myös tunnukset My F-Secure hallintaportaaliin. **Sovelluksen asennus ja käyttöönotto ovat asiakkaan vastuulla, pelkkä sopimus palvelusta ei riitä suojaamaan laitetta!**

Palveluun voi lisätä käyttäjiksi esimerkiksi perheenjäsenet kirjautumalla My F-Secure sivustolle sähköpostiin toimitetuilla tunnuksilla. Täältä voi myös tarvittaessa asentaa ohjelmiston uudelleen, tarkkailla asennettujen laitteiden tilaa ja hallita perhesääntöjä.

6. TUKI JA YLLÄPITO

6.1. Virheen korjaustoiminta

Häiriöilmoitukset tehdään toimittajan Asiakastukeen 0800 30 304 tai sähköpostilla asiakastuki@lounea.fi. Palvelun tuottaja voi olla suoraan asiakkaaseen yhteydessä pyytämällä tarkempia tietoja asiakkaan laitteistosta.

6.2. Tuki

Tuotteiden käyttötukea annetaan asiakaspalvelusta ja asiakaspalvelupisteistä tarvittaessa. Tuen tarjoaminen tapahtuu tapauskohtaisesti ja ensisijaisesti asiakkaan tulee noudattaa tietoturvaohjelmistojen omia ohjeita käyttöön liittyvissä kysymyksissä.

6.3. Palvelun käyttöönotto

Asiakas ottaa palvelun käyttöön omalla tietokoneellaan tai mobiililaitteellaan itse. Asiakkaan tulee hyväksyä F-Securen tietoturvapalvelua koskevat sopimusehdot asennuksen yhteydessä. Palvelun käyttöönottoon liittyvät asennusohjeet löytyvät Lounean www-sivuilta.

Asennettaessa tietoturvaa tietokoneelle, matkapuhelimelle tai tabletille, laitteen tulee olla kytkettynä Internetiin. Asennuspaketissa on asennuksen käynnistävä ohjelma, ajantasaiset tiedot haetaan Internetistä asennuksen yhteydessä. Ilman Internetyhteyttä asennus ei onnistu tai keskeytyy.

7. PALVELUTASOT

7.1. Toimitusaika

Asiakas saa tarvittavat käyttäjätunnukset palvelun käyttöönottoa varten sähköpostiinsa, kun tilaus on käsitelty Lounealla. Palvelut ovat tämän jälkeen käytettävissä heti.

7.2. Käytettävyys

My F-Secure palvelu on käytettävissä jatkuvasti, pois lukien mahdolliset huoltokatkot.
Tietoturvaohjelmisto on käytössä jatkuvasti ja uusimmat virustunnisteet ja suojaustiedot ladataan aina kun niitä on saatavilla ja yhteys Internettiin on olemassa.

7.3. Virheen korjaus

Palvelun perushintaan sisältyy Palveluntarjoajan kuluttajatuotteille määritelty peruspalvelu-taso, jonka mukaisesti palvelun virheen korjaus aloitetaan palveluaikana 8/16 palveluaika-tunnin sisällä.
Palveluaika on arkisin klo. 08.00-16.00. Peruspalvelutaso ei takaa korjausaikaa.
Palveluun ei ole saatavissa erillistä korotettua palvelutasoa. Palvelutasot on määritelty tarkemmin erillisessä Palvelutaso dokumentissa.

8. PALVELUEHDOT

Tähän palveluun sovelletaan Palveluntarjoajan yleisiä sopimusehtoja kuluttajille sekä F-Securen ehtoja, jotka ovat nähtävillä ennen sovelluksen asentamista ja ovat käyttöjärjestelmäriippuvaisia.

9. PALVELUN PÄÄTTÄMINEN

Asiakas voi irtisanoa palvelun kahden (2) viikon irtisanomisajalla. Toimittaja tai palvelun tuottaja eivät vastaa asiakkaan tietokoneen tai mobiililaitteen saastumisesta palvelun päätyttyä.

10. PALVELUKUVAUKSEN MUUTTAMINEN

Palveluntarjoaja voi muuttaa tätä palvelukuvausta. Asiakas voi tutustua kulloinkin voimassaolevaan palvelukuvaukseen osoitteessa www.lounea.fi. Suuremmista muutoksista palvelussa tiedotetaan sovellusten versiopäivitysten yhteydessä tai muulla asiakasviestinnällä. Ensisijainen yhteydenottotapa on asiakkaan sähköpostiosoite, joka toimii käyttäjätunnuksena myös palvelun hallintaan.