



Koventaminen – labra 6

Ryhmä 3

Markku Sutinen

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Harjoitustyö

Huhtikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

Sisältö

1	Johdanto	3
2	Miksi mobiililaitteita pitää koventaa?	3
2.1	Puhelimen koventaminen yleisesti	3
3	Oman puhelimen kovennukset.....	4
3.1	Viisi hyvää kovennusta	4
3.2	Viisi kovennusta mitä ei tekisi	9
4	Yrityksen puhelimen kovennukset.....	10
4.1	Viisi hyvää kovennusta	10
4.2	Viisi kovennusta mitä ei tekisi	12
5	Pohdinta.....	13
	Lähteet	14

Kuviot

Kuvio 1. Yubico BIO -turva-avain USB-C.....	5
Kuvio 2. Force encrypted backups kovennusohjeet. (CIS Apple iOS 17 Benchmark v1.0.0. 2023.)	6
Kuvio 3. Ensure Instant apps is set to disabled kovennusohjeet. (CIS Google Android Benchmark v1.5.0 2023.)	7
Kuvio 4. Ensure VPN is configured kovennusohjeet. (CIS Apple iOS 17 Benchmark v1.0.0. 2023.)	8
Kuvio 5. Tunnuskoodin asettaminen tai vaihtaminen. (Set a passcode on iPhone 2024.).....	9

1 Johdanto

Kevään viimeisessä labrassa on tehtävänä selvittää, miten mobiililaitteita kannattaa koventaa. Lähestymistapamme on valita muutama kovennus sekä Android, että iOS laitteiden puolelta. Lopuksi arviomme minkälaisia kovennuksia yritysten ja organisaatioiden kannattaa tehdä omiin puhelimiinsa.

2 Miksi mobiililaitteita pitää koventaa?

Vuoden 2022 alussa Proofpointin tutkijat havaitsivat 500 %:n hyppäyksen mobiilihaittaohjelmien jakeluyrityksissä Euroopassa. Mobiililaitteiden arvo on kasvanut etenkin etätyöaikana, etenkin tämän uskotaan lisänneen niihin kohdistuvia hyökkäyksiä. Tästä lisääntyvien hyökkäysten tiedosta huolimatta on raportoitu, että yli 80 % Android-laitteista oli alttiita vähintään yhdelle 25 haavoittuvuudesta. Koventamattomille laitteille hyökkäysten seuraukset voivat olla tuhoisia yksittäiselle käyttäjälle tai organisaation laitteille ja tiedoille. (Android hardening guide 2023.)

2.1 Puhelimen koventaminen yleisesti

Mobiililaitte kulkee melkein jokaisen taskussa ja sitä käytetään paljon. Puhelin on matkassa mukana kaikkialla ja sitä käytetään monenlaisiin asioihin. Sillä tehdään ostoksia, käytetään verkkopankkia, viestitään ja käytetään paljon moneen muihin päivittäisiin toimiin. Mobiililaitteeseen tallennetaan paljon tietoa. Valokuvia, muistiinpanoja, salasanoja, maksukorttitietoja ja jne. Nämä kaikki tarvitsevat hyvää suojausta.

Mobiililaitteen tulee pystyä torjumaan uhat. Mobiilihaittaohjelmat, epäilyttävät sovellukset, tietovuodot, suojaamattomat Wi-Fi verkot ja tietojenkalasteluhuijaukset. Mobiililaitteen suojausta voi parantaa käyttämällä sitä varten tehtyä virustentorjuntaohjelmaa. Haittaohjelma voi lukita laitteesi ja vaatia lunnaita. Varastaa henkilötietoja ja pankkitietoja tai tehdä veloituksia luottokortiltasi. Suojausta voit parantaa välttämällä epäilyttäviä sovelluksia. Käytä siis virallisia sovelluskauppoja. Älä anna sovelluksille tarpeettomia käyttöoikeuksia. Voit myös estää puhelimen

hakkeroinnin kytkemällä pois päältä, silloin kun ei ole tarvetta bluetoothin ja Wi-Fi verkon. Voit myös estää sijainnin jakamisen. Hyviä suojautumiskeinoja ovat myös VPN:n käyttö ja varsinkin silloin, jos joudut käyttämään julkisia Wi-Fi yhteyksiä vaikkapa lomapaikan hotellilla. Älä avaa myöskään tuntemattomia tai epäilyttäviä linkkejä. Hyvä keino on myös uudelleen käynnistää mobiililaite viikoittain. (F-Secure 2024.)

3 Oman puhelimen kovennukset

3.1 Viisi hyvää kovennusta

Kaksivaiheinen tunnistautuminen fyysisellä turva-avaimella (a FIDO certified). Apple tarjoaa korkeaa henkilökohtaista turvallisuutta julkkiksille tai tunnetuille henkilöille tuomalla fyysisen turva-avaimen kaksivaiheiseen tunnistautumiseen. Perinteinen kaksivaiheinen tunnistautuminen lähettää yleensä tekstiviestin, sähköpostin tai käyttää sitä varten tehtyä mobiilisovellusta varmistaakseen henkilöllisyytesi kuusinumeroisella varmennuskoodilla. Voit käyttää kuusinumeroisen koodin sijaan fyysistä avainta ja sen todennusprosessia. Tätä varten on tarjolla turva-avain (security key). Turva-avain on pieni ulkoinen laite, joka näyttää muistitikulta (ks. Kuvio 1) tai tunnisteelta ja sitä voidaan käyttää varmennuksessa kirjautumisen yhteydessä esimerkiksi Apple ID:lläsi. Turva-avaimet hyödyntävät FIDO U2F Open -tunnistautumista ja se on yhteensopiva erilaisten liitäntöjen kanssa. Tarjolla on mm. USB-A, USB-C ja NFC-yhteensopivuus. Turva-avain auttaa estämään toisen todennustekijän väärinkäytön. Turva-avaimia tarvitaan kaksi kappaletta. Yhden fyysisen avaimen hinta alkaen Verkkokauppa.com:ssa on 39,99 € ja kalleimmat NFC:llä toimivat ovat 149,99 €. (Apple support 2024.)



Kuvio 1. Yubico BIO -turva-avain USB-C

Force encrypted backups is set to “Enabled”: Tietoihin, jotka ovat tallennettu turvallisesti iOS laitteeseen, voidaan helposti päästä käsiksi paikallisen tietokoneen varmuuskopiosta. Salauksen pakottaminen varmuuskopioille suojaa tietoja, jos isäntäkone on uhattuna. Varmuuskopioiden käyttöä suositellaan vahvasti, koska ne mahdollistavat kopioitujen tietojen palauttamisen laitteisto- tai ohjelmistovian sattuessa, tietojen korruptoitua, ihmisen aiheuttaman tapahtuman tai tietojen tahattoman poistamisen vuoksi. (CIS Apple iOS 17 Benchmark v1.0.0. 2023.)

Kovennuksen voi tehdä kahdella tapaa, käyttäen Apple Configuratoria tai suoraan laitteen kautta (ks. Kuvio 2).

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Force encrypted backups` is checked.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Encrypted backups enforced` is displayed.

Kuvio 2. Force encrypted backups kovenusohjeet. (CIS Apple iOS 17 Benchmark v1.0.0. 2023.)

Ensure 'Instant apps' is set to 'Disabled': Pikasovellukset mahdollistavat käyttäjien käyttää osaa sovelluksesta ilman, että heidän tarvitsee asentaa koko sovellusta. Käyttäjät voivat yksinkertaisesti klikata linkkiä ja tarvittava sovellusmoduuli ladataan ja suoritetaan laitteessa. Altistuminen tämäntyyppiselle sovellukselle on vaarallista koska haitallisia linkkejä voidaan käyttää käyttäjien huijaamiseen. Lisäksi se voi ohittaa tietoturvakäytännöt ja suojatoimenpiteet, jonka vuoksi on suositeltavaa poistaa pikasovellukset käytöstä. (CIS Google Android Benchmark v1.5.0 2023.)

Ensure 'Instant apps' is set to 'Disabled' kovenuksen ohjeet (ks. Kuvio 3).

Follow the below steps to verify that `Instant apps` is Disabled:

1. Open phone's `Settings` app.
2. Tap `Apps & notifications`.
3. Tap `Advanced`.
4. Tap `Default apps`.
5. Tap `Opening links`.
6. Verify that `Instant apps` setting is set to `OFF` position.

Kuvio 3. Ensure Instant apps is set to disabled kovennusohjeet. (CIS Google Android Benchmark v1.5.0 2023.)

Ensure "VPN" is "Configured": Verkko, johon laite yhdistää, tarjoaa tärkeitä palveluita, joita haitallinen toimija voi hyödyntää. VPN-yhteyden käyttö vähentää näihin liittyviä riskejä salaamalla tiedot siirron aikana käyttäen tunnettuja hyviä verkkopalveluita, kuten DNS. Kovennuksessa suositellaan sovelluskohtaista VPN-konfiguraatiota mutta järjestelmän laajuinen VPN on myös hyväksyttävä. (CIS Apple iOS 17 Benchmark v1.0.0. 2023.)

Ensure "VPN" is "Configured" kovennuksen ohjeet voidaan myös toteuttaa kahdella tapaa. (ks. Kuvio 4).

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the **VPN** tab.
4. In the right window pane, enter an appropriate VPN configuration.
5. Deploy the Configuration Profile.

From the device:


1. Tap **Settings**.
2. Tap **General**.
3. Tap **VPN**.
4. Inspect the configuration.

Kuvio 4. Ensure VPN is configured kovennusohjeet. (CIS Apple iOS 17 Benchmark v1.0.0. 2023.)

Passcode (Apple): Tunnuskoodin asettaminen estää satunnaisen luvattoman pääsyn laitteeseen. Tunnuskoodia tarvitaan myös, jos halutaan ottaa Data Protection käyttöön ja hyödyntää kaikkien viimeaikaisten iOS-laitteiden salattua tallennustilaa. Tavallisen neljän numeron tunnuskoodin lisäksi, Apple tukee myös yli neljän numeron pituisia tunnuskoodoja ja tavallisia aakkosnumeerisia salasanoja. On ollut esimerkkejä brute force -hyökkäyksistä tunnuskoodoja vastaan, jotka kiertävät normaalit käyttäjän sisäänkirjautumismekanismit ja hyökkäävät suoraan avaimiin estääkseen tietojen poistumisen kymmenen virheellisen yrityksen jälkeen. Nelinumeroisella tunnuskoodilla on vain enintään 10 000 mahdollista yhdistelmää, joten suositus on valita pidempi tunnuskoodi. (Apple iOS Hardening Checklist.)

Applen omilta sivuilta löytyy ohje tunnuskoodin asettamiseen (ks. Kuvio 5).

Set or change the passcode

1. Go to Settings , then depending on your model, do one of the following:

- *On an iPhone with Face ID:* Tap Face ID & Passcode.
- *On an iPhone with a Home button:* Tap Touch ID & Passcode.

2. Tap Turn Passcode On or Change Passcode.

To view options for creating a password, tap Passcode Options. The most secure options are Custom Alphanumeric Code and Custom Numeric Code.

After you set a passcode, on supported models you can [use Face ID](#) or [Touch ID](#) to unlock iPhone (depending on your model). For additional security, however, you must always enter your passcode to unlock your iPhone under the following conditions:

- You turn on or restart your iPhone.
- You haven't unlocked your iPhone for more than 48 hours.
- You haven't unlocked your iPhone with the passcode in the last 6.5 days, and you haven't unlocked it with Face ID or Touch ID in the last 4 hours.
- Your iPhone receives a remote lock command.
- There are five unsuccessful attempts to unlock your iPhone with Face ID or Touch ID.
- An attempt to use Emergency SOS is initiated (see [Use Emergency SOS](#)).
- An attempt to view your Medical ID is initiated (see [Set up and view your Medical ID](#)).

Kuvio 5. Tunnuskoodin asettaminen tai vaihtaminen. (Set a passcode on iPhone 2024.)

3.2 Viisi kovennusta mitä ei tekisi

Lockdown Mode (iOS): Uusimmissa iOS 16 tai uudemmissa oleva valinnainen suojausominaisuus, joka on suunniteltu erityisesti niille harvoille henkilöille, jotka voivat joutua erittäin kehittyneiden kyberhyökkäysten kohteeksi. Kun Lockdown Mode on käytössä, laitteen toiminnallisuus muuttuu merkittävästi: tietyt sovellukset, verkkosivustot ja ominaisuudet ovat tiukasti rajoitettuja turvallisuuden vuoksi, ja jotkin kokemukset eivät välttämättä ole lainkaan käytettävissä. Lockdown Mode:n ollessa päällä esimerkiksi monet viestiliitteet estetään, tietyt monimutkaiset

verkkoteknologiat kielletään ja FaceTime-puhelut sallitaan vain, jos olet aiemmin soittanut kyseiselle henkilölle. (About Lockdown Mode 2024.)

Erase data after 10 failed passcode: Kyseinen kovennus poistaa kaiken datan puhelimesta 10 väärän puhelimen avaamisen tarvittavan salasanan yrityksen jälkeen. (Set a passcode on iPhone 2024.)

Passcode. Ensure "Minimum passcode length" is set to a value of 6 or greater. Minimi salasanan pituus on asennettu suuremmaksi, kuin kuusi merkkiä. (CIS Apple IOS 17 2023.)

F-securen virustorjuntaohjelma käyttöönotto. Apit ovat suojausarkkitehtuurin kriittisimpiä elementtejä. Apple tarjoaa useita suojausvarmistuksia, että sovelluksissa ole haittaohjelmia, eikä niitä ole peukaloitu. Lisäsuojaukset tuovat turvaa, että sovellusten pääsyä käyttäjien tietoihin rajoitetaan. Nämä suojaustoimet tarjoavat vakaan ja turvallisen alustan sovelluksille. Käyttäjät voivat käyttää sovelluksia Apple-laitteissa ilman, että heidän tarvitsee pelätä viruksia, haittaohjelmia tai luvattomia hyökkäyksiä. (Apple-alustojen tietoturva 2024.)

Pilvipalvelut varmuuskopiot disable tilaan. Nykypäivänä on tarjolla puhelimen varmuuskopioille automaattista pilvipalvelua. Moni ei kuitenkaan halua tätä käyttää, koska pelkää tietonsa joutuvan ulkomailla sijaitseville palvelimille, joihin ei voi luottaa. Apple tarjoaa varmuuskopioille salattua tiedonsiirtoa sekä avain parilla suojattua salausta. Apple ilmoittaa, ettei sillä ole pääsyä käyttäjän tietoihin, koska salausavaimet sijaitsevat käyttäjällä.

4 Yrityksen puhelimen kovennukset

4.1 Viisi hyvää kovennusta

Do not root a user device: roottaaminen rikkoo puhelimen käyttäjätason asetukset ja tarkoittaa hallinnollisen pääsyn saamista laitteen järjestelmätietoihin ja asetuksiin. Ohjelmistojen asentaminen, järjestelmätiedostojen muokkaaminen ja suorittaminen onnistuvat, kun laite on

rootattu. Tämä altistaa laitteen suuremmalle riskille, koska laitetta on mahdollista muokata ilman rajoituksia. Rootatun laitteen palauttaminen takaisin ei rootatuksi, vaatii usein tehdasasetusten palautuksen ja kaikki puhelimelle ladattu tieto voi hävitä. Yritysmailmassa tämä on erittäin tärkeää, jotta laitteelle voi tehdä muutoksia vain laitehallinnasta vastaavat tahot. (CIS Android Benchmark v1.5.0. 2023.)

Ensure 'Voice & Audio Activity' is set to 'Disabled': Estää puheesi ja muun audion tallentamisen Google- tilille. Google tallentaa käyttäjän ääntä ja muuta audiota, kun "audio activations" on käytössä. Ääntä voidaan tallentaa silloinkin, kun laite on off-line tilassa. Kun *Voice & Audio Activity* on pois päältä ääni inputteja ei tallenneta, vaikka käyttäjä olisi kirjautuneena Google-tilille. Ne voidaan tallentaa vain nimettömillä tunnisteilla (anonymous identifier). Äänen tallentaminen google-tilille on asia, joka ei tule herkästi edes mieleen. Kuitenkin työelämässä tämä voidaan pitää joissain yrityksissä turvallisuustekijänä. (CIS Android Benchmark v1.5.0. 2023.)

Ensure 'Allow remote lock and erase' is set to enabled: Mahdollistaa laitteen lukitsemisen passcodella tai kaiken tiedon poistamisen, jos laite on kadonnut tai varastettu. Lisää laiteturvallisuutta ja suojaa dataa luvattomalta käytöltä. Vaatii kuitenkin paikannuspalveluiden jatkuvaa käyttöä, mikä saattaa joillain yrityksillä olla muodostua turvallisuustekijäksi. Joka tapauksessa helpottaa kriittisen tiedon suojaamista tilanteissa, joissa puhelin syystä tai toisesta katoaa tai joutuu väärin käsiin. (CIS Android Benchmark v1.5.0. 2023.)

Apple Mobile Device Management (MDM): MDM voi toimia sekä pilvessä, että paikallisella palvelimella. Se on https- perusteinen protokolla, jonka avulla laitteita pystyy hallitsemaan missä päin maailmaa tahansa. Applella on useita erilaisia MDM- ratkaisuita esim Mac- koneille tai iPhone-laitteille. Joihinkn palveluihin, kuten Apple School Manageriin, Apple Business Manageriin ja Apple Business Essentialsiin on mahdollista luoda useita eri tunnuksia ja ryhmiä. Tämä mahdollistaa mm. erilaiset rekisteröintiasetukset erilaisille laitejoukoille. Jaetuilla laitteilla voi olla erilaiset asetukset, kuin henkilökohtaiseen käyttöön myönnetyllä laitteella. MDM mahdollistaa mm. ohjelmistopäivitysten käynnistämisen ja appian lataamisen sekä laitteiden paikannuksen. Sillä

voidaan kysellä laiteilta erilaisia tietoja kuten laitteiston sarjanumeron, Wi-fin, Mac-osoitteen tai FileVault salauksen tilan. Se voidaan myös integroida Active Directoryn ja LDAPin kanssa. (MDM-ratkaisun valitseminen 2024.) Yritykselle, jolla on käytössä Applen tuotteita, MDM voi olla hyödyllinen työkalu keskitettyyn laitehallintaan ja sitä kautta ympäristön koventamiseen.

Salasanojen hallintasovelluksen käyttö: Helpottaa salasanojen hallintaa, koska kaikki salasanat ovat yhden pääsalasanan takana. Tarvitsee muistaa vain yksi vahva salasana. Salasanamanageri helpottaa vahvojen salasanojen käyttöä eri palveluissa. Monissa sovelluksissa on myös mahdollista verkkoselaimen lisäosaa käyttämällä automatisoida salasanojen täyttäminen. Salasanojen hallintasovellus monipuolistaa erilaisten salasanojen käyttämistä ja suojaa näin ollen paremmin hyökkäyksiltä, jotka kohdistuvat salasanoihin. (Neuvoja salasanan hallintasovelluksen käyttöönottoon 2023.)

4.2 Viisi kovennusta mitä ei tekisi

Lockdown Mode (iOS): Uusimmissa iOS 16 tai uudemmissa oleva valinnainen suojausominaisuus, joka on suunniteltu erityisesti niille harvoille henkilöille, jotka voivat joutua erittäin kehittyneiden kyberhyökkäysten kohteeksi. Kun Lockdown Mode on käytössä, laitteen toiminnallisuus muuttuu merkittävästi: tietyt sovellukset, verkkosivustot ja ominaisuudet ovat tiukasti rajoitettuja turvallisuuden vuoksi, ja jotkin kokemukset eivät välttämättä ole lainkaan käytettävissä. Lockdown Mode:n ollessa päällä esimerkiksi monet viestiliitteet estetään, tietyt monimutkaiset verkkoteknologiat kielletään ja FaceTime-puhelut sallitaan vain, jos olet aiemmin soittanut kyseiselle henkilölle. (About Lockdown Mode 2024)

Erase data after 10 failed passcode: Kyseinen koventaminen poistaa kaiken datan puhelimesta 10 väärän puhelimen avaamisen tarvittavan salasanan yrityksen jälkeen. (Set a passcode on iPhone 2024)

Passcode. Ensure "Minimum passcode length" is set to a value of 6 or greater. Minimi salasanan pituus on asennettu suuremmaksi kuin kuusi merkkiä. (CIS Apple IOS 17 2023.)

F-securen virustorjuntaohjelman käyttöönotto. Apit ovat suojausarkkitehtuurin kriittisimpiä elementtejä. Apple tarjoaa useita suojauksia varmistamaan, että apeissa ole haittaohjelmia, eikä niitä ole peukaloitu. Lisäsuojaukset tuovat turvaa, että appien pääsyä käyttäjien tietoihin rajoitetaan. Nämä suojaustoimet tarjoavat vakaan ja turvallisen alustan apeille. Käyttäjät voivat käyttää appeja Apple-laitteessa ilman, että heidän tarvitsee pelätä viruksia, haittaohjelmia tai luvattomia hyökkäyksiä. (Apple-alustojen tietoturva 2024.)

Pilvipalvelut varmuuskopiot disable tilaan. Nykypäivänä on tarjolla puhelimen varmuuskopioille automaattista pilvipalvelua. Moni ei kuitenkaan halua tätä käyttää, koska pelkää tietonsa joutuvan ulkomailla sijaitseville palvelimille, joihin ei voi luottaa. Apple tarjoaa kuitenkin varmuuskopioille salattua tiedonsiirtoa sekä avain parilla suojattua salausta ja ainakin omien puheidensa mukaan ilmoittaa, ettei sillä ole pääsyä käyttäjän tietoihin, koska salausavaimet sijaitsevat käyttäjällä.

5 Pohdinta

Mukava pikku tehtävä loppuun. Harmaita hiuksia aiheutti lähinnä keksiä kovennuksia, joita emme nähneet järkeviksi tehdä, sekä omalla puhelimella, että yrityspuolella. Yllättävän hankalaa oli keksiä mitä ei tekisi. Oli myös mukava kokea monipuolinen keskustelu näin kurssin päätteeksi, koska tässä labrassa ei tarvinnut tehdä muuta kuin pohtia mitkä kovennukset valitaan ja miten ne toimivat. Tämä oli ihan mukava lopetus tälle kurssille.

Tässä viimeinen pohdinta ryhmältä kolme. Kiitos kurssista, hienosti vedetty, järjestelyt toimivat ja paljon tuli uutta oppia matkaan!

Lähteet

About Lockdown Mode. 2024. Viitattu 21.4.2024. <https://support.apple.com/en-gb/105120>

About Security Keys for Apple ID. 2024. Apple support. Viitattu 22.4.2024. <https://support.apple.com/en-us/102637>

Android hardening guide. 2023. Deep Dive Security. Viitattu 23.4.2024. <https://deepdivesecurity.ca/blog/android-hardening-guide>

Applen suojauksen yleiskatsaus. 2024. Apple support. Viitattu 22.4.2024. <https://support.apple.com/fi-fi/guide/security/sec35dd877d0/web>

Apple iOS Hardening Checklist. Viitattu 22.4.2024. <https://security.utexas.edu/handheld-hardening-checklists/ios>

CIS Apple iOS 17 Benchmark v1.0.0. 2023. Viitattu 22.4.2024. Center for Internet Security

CIS Google Android Benchmark v1.5.0. 2023. Viitattu 22.4.2024. Center for Internet Security

MDM-ratkaisun valitseminen. 2024. Apple-alustojen käyttöönotto. Viitattu 23.4.2024. <https://support.apple.com/fi-fi/guide/deployment/dep1d7afa557/web>

Neuvoja salasanan hallintasovelluksen käyttöönottoon. 2023. Traficom. Viitattu 23.4.2024. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon?toggle=Huomioitavia%20ominaisuuksia>

Näin suojaat puhelimesi hakkeroinnilta. 2024. F-Secure. Viitattu 22.4.2024. <https://www.f-secure.com/fi/articles/how-to-protect-your-phone-from-hackers>

Set a passcode on iPhone. 2024. Viitattu 21.4.2024. <https://support.apple.com/en-il/guide/iphone/iph14a867ae/ios>