Turvallisesti matkalla

SUPO
SUOJELUPOLIISI
SKYDDSPOLISEN

TURVALLISESTI MATKALLA

Tässä esitteessä kuvataan hyviä käytäntöjä turvallisuutesi, yksityisyyden suojasi ja tietoturvallisuuden varmistamiseksi, kun matkustat ulkomaille.

Voit olla tehtäväsi ja verkostojesi vuoksi kiinnostava tiedustelun kohde kotimaassa ja matkustaessasi ulkomaille. Mielenkiinto voi kohdistua mukanasi oleviin asiakirjoihin, laitteisiin tai käymiisi keskusteluihin – käytpä niitä puhelimessa tai kasvotusten.

Matkustaessasi voit omalla huolellisella toiminnallasi auttaa suojaamaan Suomen ja oman organisaatiosi turvallisuutta. Huolellisuus on erityisen tärkeää, jos matkustat epädemokraattisiin maihin. Kun huomioit nämä ohjeet, voit pienentää sinuun kohdistuvia riskejä ja estää tiedon joutumista vääriin käsiin.

Noudata lisäksi aina organisaatiosi antamia ohjeita matkustusturvallisuudesta ja tietoturvallisuudesta.

Ennen matkaa

Kun suunnittelet matkaa, harkitse tarkkaan, mitkä asiakirjat ja elektroniset laitteet tarvitset mukaasi. Jos mahdollista, älä ota mukaan sellaista materiaalia, joka vääriin käsiin joutuessaan voi aiheuttaa vahinkoa organisaatiollesi. Ota mukaan vain sellaisia tietoja ja laitteita, joita tarvitset välttämättä matkalla.

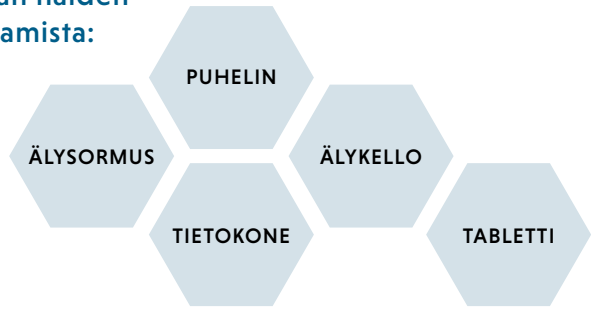
Turvallisinta on, jos organisaatiossasi on käytössä erilliset, vain matkustuskäyttöön tarkoitetut laitteet. Matkalaitteet voit tyhjentää ja alustaa tai tuhota matkan jälkeen. Väliaikaisissakin laitteissa pitää noudattaa oman organisaation määräyksiä tietojen käsittelystä.

Kun otat laitteita mukaan, hoida nämä asiat kuntoon jo ennalta:

- Päivitä laitteet ja sovellukset aina uusimpiin versioihin.
- Aseta laitteisiin pääsykoodi ja säädä viive mahdollisimman lyhyeksi.

Ota huomioon, että joissakin maissa rajaviranomaisilla on oikeus tarkistaa tietokoneiden ja muiden laitteiden sisältö ja ottaa se tarvittaessa talteen.

Mieti erityisen tarkkaan näiden laitteiden mukaan ottamista:



SUUNNITTELE JA ENNAKOI

Ennen matkaa on hyvä ajatella turvallisuuteen liittyviä asioita laajasti. Pohdi, mitä konkreettista matkalla voi sattua ja mistä voit tarvittaessa hakea apua. Pohdi myös, mitä voit tehdä jo ennen turvallisuutta uhkaavaa tilannetta tai kuinka voisit estää sen kokonaan.

- Tutustu ulkoministeriön matkustusohjeisiin ja maakohtaisiin matkustustiedotteisiin. Tee matkustusilmoitus ulkoministeriön verkkosivuilla.
- Suunnittele mahdolliset turvallisuusjärjestelyt tarvittaessa yhdessä turvallisuusasiantuntijoiden kanssa ja mieti, kuinka toimit ongelmatilanteissa. Valmistaudu myös henkisesti mahdollisiin vaaratilanteisiin.
- Tallenna matkakohteen paikallinen hätänumero ja muut tärkeät puhelinnumerot puhelimeesi.
- Pidä työnantajasi tietoisena ja ajan tasalla siitä, missä matkustat, mitä ohjelmaa ja tapaamisia matkaan sisältyy ja miten sinut tavoittaa.

Muista, että kohdemaassa olet paikallisten viranomaisten toimivallan piirissä.

NOUDATA OMAN ORGANISAATIOSI TIETOTURVAOHJEITA.

Matkalla

Pidä työhön liittyvät asiakirjat hallussasi niin, etteivät ulkopuoliset pääse lukemaan niitä.

Kuljeta tietokone, matkapuhelin ja muut mobiililaitteet käsimatkatavaroina. Älä jätä laitteita valvomatta edes hotellihuoneen tallelokeroon, vaan kanna ne aina mukanasi. Hotellin henkilökunnalla ja viranomaisilla on pääsy tallelokeroon.

Jos joudut jättämään laitteet valvomatta, säilytä ne sinetöitävässä turvapussissa. Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa esimerkiksi kahvilan pöydälle tai autoon näkyvälle paikalle.

Tietokoneissa, tableteissa ja matkapuhelimissa on hyvä pitää näkösuojakalvoa, joka estää näytön lukemisen esimerkiksi viereisiltä penkeiltä. Varmista myös, ettei suoraan takanasi istuva henkilö näe laitteesi ruutua.

TIETOTURVA

Kun tarvitset verkkoyhteyttä, käytä ensisijaisesti omaa mobiilidata-yhteyttä. Käytä matkalla organisaatiosi hyväksymää luotettavaa VPN-palvelua. Erityisen tärkeää se on silloin, jos joudut käyttämään langattomia WiFi-yhteyksiä. Jos mahdollista, älä liitä laitteitasi julkisiin WiFi-verkkoihin esimerkiksi hotelleissa tai ravintoloissa. Säädä matkapuhelimesi ja muiden mobiililaitteiden asetuksia suojataksesi yksityisyyttäsi. Kun lataat uuden sovelluksen, tarkasta aina sen asetukset, jottet tahtomattasi ja tietämättäsi luovuta liikaa tietojasi. Vältä uusien, tuntemattomien sovellusten lataamista matkalla. Huomioi tietoturva myös silloin, kun käytät henkilökohtaisia laitteitasi.

Poista ainakin seuraavat toiminnot aina silloin, kun et itse niitä käytä:

- BLUETOOTH
- ÄÄNIOHJAUS TAI PUHEEN-TUNNISTUS
- WLAN- TAI WIFI-YHTEYS
- YHTEYDEN JAKAMINEN TAI YHTEYSPISTE (HOTSPOT)
- PAIKANNUS-PALVELUT

PUHELIMEN KUUNTELU

Tietoliikenneyhteyden omistajalla (esimerkiksi WLAN-tukiaseman ylläpitäjä) tai isäntävaltiolla voi olla pääsy kuuntelemaan liikennettä. Tämä koskee sekä tavallisia puheluita että kaikkea internet-liikennettä, kuten sovellusten kautta soitettuja puheluita. Käytä yhteytesi suojaamiseksi luotettavaa VPN-palvelua tai muuta salausta.

SOSIAALINEN MEDIA

Yksityisyyden suojaamisessa kannattaa ottaa huomioon oma ja läheisten käyttäytyminen sosiaalisessa mediassa. Kerran internetissä julkaistua tietoa tai kuvaa ei saa enää yksityiseksi.

Harkitse, onko työmatkalta tarpeen jakaa tietoja tai kuvia sosiaalisessa mediassa. Jos päätät jakaa tietoja tai kuvia,

- kerro mieluummin, mitä olet tehnyt kuin mitä tulet tekemään.
- harkitse, onko tarkkoja paikkatietoja tarpeen jakaa.
- kysy muilta lupa heitä koskevien tietojen tai kuvien jakamiseen.

Yleiset tietoturvaohjeet pätevät matkallakin. Palveluiden ja käyttäjätilien tai -profiilien turvallisuudessa kannattaa kiinnittää erityistä huomiota salasanojen ja käyttäjätunnusten hallintaan. Älä käytä samaa salasanaa eri palveluissa. Myös saman käyttäjätunnuksen käyttämistä eri palveluissa kannattaa harkita kriittisesti. Älä käytä samoilla tunnuksilla (esimerkiksi Facebook) kirjautumista eri palveluihin. Käytä kriittisimmissä palveluissa kaksiosaista tunnistautumista. Kiinnitä huomiota epätyypillisiin yhteydenottoihin sosiaalisessa mediassa sekä matkalla että sen jälkeen.

IHMISET

Jos työskentelet esimerkiksi politiikassa, virkamiehenä tai elinkeinoelämässä, saatat olla tehtäväsi vuoksi kiinnostava tiedustelun kohde. Ulkomaiset tiedustelupalvelut ovat kiinnostuneita esimerkiksi Suomen politiikan eri osa-alueista sekä suomalaisesta teknologiasta ja sen kehityksestä.

Jos tuntematon henkilö lähestyy sinua ja haluaa keskustella työstäsi, ota huomioon, että taustalla voi olla muukin kuin vilpitön halu ystävystyä. Harkitse, mitä tuntemattomalle kannattaa kertoa.

Jos työkontaktisi hakeutuu kanssasi luottamuksellisiin keskusteluihin ja kyselee paljon, taustalla voi olla halu kerätä tiettyjä tietoja sinusta tai organisaatiostasi.

Runsas alkoholin käyttö altistaa tapaturmille, sairastumisille sekä rikoksille. Se voi myös tehdä sinusta alttiimman erilaisille vaikutuspyrkimyksille.

Pidä mielessäsi, että puheitasi voidaan nauhoittaa tai toimintaasi kuvata niin, että materiaaleja voidaan käyttää myöhemmin sinua vastaan.

Myös lahjoilla voidaan pyrkiä vaikuttamaan sinuun. Jos saat lahjaksi elektronisia välineitä, älä käytä niitä. Tällaisia ovat esimerkiksi muistitikut, laturit, johdot tai vaikkapa USB-ladattavat taskulamput. On mahdollista, että laitteissa on esimerkiksi haittaohjelma, jota voidaan käyttää tiedonhankintaan sinusta ja organisaatiostasi. Jos joudut ottamaan lahjoja vastaan kohteliaisuussyistä, toimi organisaatiosi antamien ohjeiden mukaan.

KADULLA

Voit joutua matkallasi odottamattomiin tilanteisiin. Pohdi, mitä voit tehdä välttääksesi uhkaavia tilanteita jo etukäteen.

Vältä mahdollisuuksien mukaan paikkoja, joissa on paljon ihmisiä tai jotka tiedät etukäteen rauhattomiksi.

HENGENVAARALLISESSA TAI TERRORI-ISKUTILANTEESSA:

- Reagoi aktiivisesti, älä jää seuraamaan tilannetta.
- Jos pystyt, pakene.
- Jos et pääse pakenemaan, piiloudu ja suojaudu.
- Laita puhelin äänettömälle.
- Jos olet turvallisessa paikassa, hälytä apua.
- Älä palaa tarkistamaan tilannetta.
- Odota viranomaisen toimintaohjeita.

Matkan jälkeen

Jos jokin matkalla tapahtunut jää mietityttämään sinua, kannattaa siitä mieluummin kertoa kuin jättää kertomatta. Raportoi havaitsemistasi turvallisuuspoikkeamista organisaatiosi turvallisuusvastaaville ja tarvittaessa turvallisuusviranomaisille.

Harkitse tarkkaan erilaisiin kyselyihin ja palautetiedusteluihin vastaamista. Ole erityisen tarkkana matkan jälkeen saamiesi linkkien ja liitteiden avaamisessa. Uutta sovellusta ladatessasi tarkasta aina sen asetukset, jottet tahtomattasi ja tietämättäsi luovuta liikaa tietojasi.

SUOJELUPOLIISIN YHTEYSTIEDOT LÖYDÄT VERKOSTA

WWW.SUPO.FI/YHTEYSTIEDOT

SUPO