Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Op reis naar het buitenland

Veiligheidsrisico's onderweg

Binnenkort gaat u voor uw werk naar het buitenland. Zakelijke reizen naar het buitenland brengen spionagerisico's met zich mee. Ditzelfde geldt voor langdurig werkzaam zijn in het buitenland.

Buitenlandse inlichtingendiensten hebben interesse in u en met name in de kennis die u heeft of bij u draagt.

Deze informatie helpt u bij het nemen van voorzorgsmaatregelen om het risico op (digitale) spionage te verkleinen.

Het risico op spionage is niet in ieder land hetzelfde. Afhankelijk van het land waar u naartoe reist kunt u aanvullend gebriefd worden over eventuele bijzonderheden.

Voor de reis

Algemeen

Neem geen of zo min mogelijk vertrouwelijke gegevens mee. U bent verantwoordelijk voor een zorgvuldige omgang met deze informatie. Stel uzelf voor vertrek daarom altijd de volgende vragen:

- Heb ik dit écht nodig?
- Wat is de waarde van de informatie die ik meeneem (op papier, een gegevensdrager of anderszins)?
- Hoe erg zou het zijn als de informatie in verkeerde handen valt?
- Welke apparaten neem ik mee?

Neemt u toch vertrouwelijke gegevens mee, stel dan een lijst op met de documenten, gegevensdragers en apparatuur die u meeneemt. Bij verlies is dan meteen duidelijk wat er weg is. Bewaar de lijst op kantoor, neem deze niet mee.

Vervoer uw vertrouwelijke documenten en gegevensdragers altijd in uw handbagage, nooit in uw koffer. Neem kennis van de regels voor het vervoeren van staatsgeheime informatie.

Stem bezoeken aan overheidsorganisaties af met het Nederlandse consulaat of de ambassade, indien aanwezig.

Digitaal

Wis de belgeschiedenis van uw telefoon en verwijder ontvangen en verzonden sms-berichten. Zet alleen noodzakelijke contacten in uw contactenlijst. Overweeg een wegwerp mobiele telefoon, simkaart en tijdelijk e-mailadres te gebruiken.

Als u regelmatig naar het buitenland reist, is het raadzaam apparatuur aan te schaffen die u alleen voor dit doel gebruikt. Neem eigen opladers, adapters, kabels en carkit mee.

Installeer alleen applicaties die u daadwerkelijk nodig heeft. Neem voor advies hierover contact op met de beveiligingsfunctionaris binnen uw organisatie.

Pas wachtwoorden voor (en na) uw reis aan.

Gebruik verschillende wachtwoorden voor al uw apparaten en zorg ervoor dat die niet hetzelfde zijn als de inloggegevens van uw werkplek.

Voorkom dat iemand meekijkt of ongemerkt aan uw apparatuur rommelt. U kunt uw webcam afdekken, gebruikmaken van een privacyscherm of speciale anti-tamper stickers. Vraag na wat binnen uw organisatie beschikbaar is.

Privé

Wees terughoudend met het meenemen van privéapparatuur. Ook die is interessant voor inlichtingendiensten.

Zorg dat u verschillende toestellen gebruikt voor uw privégesprekken en uw professionele gesprekken en houd deze zoveel mogelijk gescheiden.

Neem op een privéreis zo min mogelijk zakelijke informatie en gegevensdragers mee.

Zet niet op sociale media, zoals Twitter en Facebook, dat u op reis gaat.

Tijdens de reis

Algemeen

Profileer u bij voorkeur niet als overheids-functionaris.

Voer geen vertrouwelijke gesprekken aan de telefoon of in vervoersmiddelen zoals een huurauto, trein of vliegtuig. Houd informatie en gegevensdragers zoveel mogelijk bij u.

Vertel uw gesprekspartner niet meer dan nodig is.

Wees alert op ‘toevallige’ ontmoetingen met personen die veel belangstelling hebben voor uw werk of uw privéleven. Ook via sociale media kan geprobeerd worden met u in contact te komen.

Uw gedrag kan u direct of op een later moment in een kwetsbare positie brengen. Niet alleen alcohol of drugs, ook geschenken of avances kunnen worden ingezet om u te beïnvloeden.

Wees u ervan bewust dat mensen u kunnen filmen of geluidsopnames kunnen maken om u later onder druk te zetten. Dat geldt zeker ook bij gebruik van sociale media of datingapps!

Zorg dat u kunt controleren of iemand vertrouwelijke gegevens heeft ingezien. Gebruik daar sealbags voor.

Maak geen gebruik van de hotelkluis voor vertrouwelijke informatie of gegevensdragers.

Digitaal

Schakel uw apparaten uit als u een vertrouwelijk gesprek voert. Verwijder de batterij, of leg uw apparaat tussen uw kleding of in uw tas zodat het geluid gedempt wordt. U bent extra kwetsbaar voor spionage als uw apparatuur ingeschakeld is.

Schakel de Bluetooth-functie van al uw apparaten uit. Bluetooth is onveilig en spionage via deze functie is uiterst eenvoudig.

Download of installeer geen applicaties tijdens de reis. Mocht u lokale software moeten gebruiken, gebruik daar dan een apart apparaat voor. Schakel de automatische updates uit voor de app- of playstore.

Let op onverwachte of vreemde (beveiligings-) waarschuwingen op uw telefoon, laptop of tablet. De meldingen kunnen wijzen op een aanval. Houd meldingen en andere opvallende zaken bij en geef deze bij terugkomst door aan de beveiligingsfunctionaris van uw organisatie.

Geef nooit uw wachtwoord en sta niet toe dat anderen gebruik maken van uw apparatuur.

Gebruik voor zakelijke doeleinden geen wifi die wordt aangeboden in openbare ruimtes.

Wilt u mobiel werken? Gebruik dan nooit apparatuur van derden. Sluit uw systeem ook nooit aan op appatuur van anderen (denk aan printers en opladers).

Gebruik bij voorkeur een goedgekeurde VPN-verbinding. Maak gebruik van beveiligde en goedgekeurde usb-sticks. Ga bij uw beveiligingsfunctionaris na wat goedgekeurd is.

Wees terughoudend met het openen van e-mails, sms-berichten of andere elektronische berichten van onbekenden.

Pas op voor spear phishing. Ga altijd na of ontvangen berichten voor u bestemd zijn. Bij twijfel verifieert u eerst de herkomst van het bericht bij de afzender.

Geef uw apparatuur nooit af. Moet dat wel vanwege veiligheidsmaatregelen, stop ze dan in een sealbag of geef ze aan een collega die niet met u mee naar binnen gaat.

Waarschuw bij een incident altijd direct de beveiligingsfunctionaris van uw organisatie. Doe dit ook bij twijfel!

Na de reis

Algemeen

Verander het wachtwoord van de meegenomen apparatuur en van accounts, zoals e-mail en sociale media.

Het kan zijn dat uw apparatuur ingeleverd moet worden voor analyse of opschoning. Soms kan het zelfs nodig zijn om apparatuur te vernietigen bij terugkomst, omdat veilig gebruik niet meer mogelijk is. Per reisbestemming en organisatie kunnen hier specifieke afspraken over bestaan.

Een veilige digitale omgeving

Of u nu op reis bent of niet, zorg altijd voor een veilige digitale omgeving. Een aantal tips:

Zorg altijd voor bijgewerkte detectie- en beveiligingssoftware.

Versleutel gevoelige informatie die u op uw laptop of uw beveiligde usb-stick opslaat.

Maak gebruik van beveiligingssoftware die alleen bepaalde apparaten toegang geeft tot uw computer.

Maak gebruik van versleuteling als u gevoelige informatie op openbare netwerken uitwisselt. Maak daarbij gebruik van toegang die op twee manieren uw identiteit bevestigt, zogenaamde twee-factor authenticatie.

Lees meer over veilig digitaal werken in de AIVD-publicatie ‘Bent u zich bewust van de risico’s van cyberspionage?’ op aivd.nl.

Heeft u vragen? Stel deze dan aan de beveiligingsfunctionaris van uw organisatie.

Goede reis!

Algemene Inlichtingen- en Veiligheidsdienst
www.aivd.nl

december 2017