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.

Buitenlandse inlichtingendiensten hebben waarschijnlijk meer interesse in u, dan u zelf verwacht. Deze diensten zijn vooral geïnteresseerd in de kennis die u heeft, bij u draagt of digitale toegang tot heeft. Denk hierbij ook aan persoons-, authenticatie-, bedrijfsgevoelige of locatiegegevens.

De informatie in deze folder 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. Vraag aan uw beveiligingsfunctionaris of uw reis een verhoogd risico hierop heeft.

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 een andere manier)?
- Hoe erg zou het zijn als de informatie in verkeerde handen valt?
- Welke apparaten neem ik mee?
- Als een ander de digitale of fysieke beschikking krijgt over dit apparaat, tot welke gegevens heeft die persoon dan toegang?

Neemt u toch vertrouwelijke gegevens en/of apparatuur mee die mogelijk toegang heeft tot vertrouwelijke gegevens, 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 deze lijst op kantoor, neem die 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 gevoelige en/of staatsgeheime informatie.

Stem bezoeken aan overheidsorganisaties of internationale organisaties af met het Nederlandse consulaat, de ambassade of de permanente vertegenwoordiging, voor zover aanwezig.

Digitaal

Gebruik voor werkgerelateerde zaken alleen de communicatiemiddelen van uw organisatie. Deze zijn zodanig ingesteld dat u met minder risico's hiervan gebruik kunt maken.

Zorg dat uw apparatuur voorzien is van de laatste updates.

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

Gebruik hierbij lange wachtwoorden in de vorm van wachtwoordzinnen en/of gebruik een passwordmanager.

Pas wachtwoorden voor (en na) uw reis aan.

Als u een bezoek brengt aan een land met een verhoogd risico op (digitale) spionage en u bereikbaar moet zijn, kies dan voor tijdelijke mobiele apparatuur die u alleen op deze bestemming gebruikt. De beveiligingsfunctionaris van uw organisatie kan u daarbij helpen.

Schakel de locatieservices op uw telefoon alleen in als u deze nodig heeft.

Installeer alleen applicaties die u echt nodig heeft. Voor vragen over apps die u tijdens of voor uw reis nodig heeft, kunt u contact opnemen met de beveiligingsfunctionaris van uw organisatie.

Schakel waar mogelijk Multifactor Authenticatie (MFA) in. Gebruik geen MFA via sms. Kies liever voor een authenticatie-app.

Maak gebruik van schermvergrendeling om uw mobiele apparaten te beveiligen. Ontgrendel uw apparaat met een biometrisch kenmerk (vingerafdruk of gezichtsherkenning).

Wees terughoudend in het gebruik van uw apparatuur in de openbare ruimte: anderen kunnen ongemerkt met u meekijken. Maak gebruik van een privacyscherm om het meekijken te bemoeilijken.

Met speciale anti-tamperstickers kunt u voorkomen dat anderen ongemerkt aan uw apparatuur kunnen rommelen. Vraag na wat binnen uw organisatie beschikbaar is.

Maak bijvoorbeeld gebruik van sealbags. Een sealbag kunt u gebruiken om uw apparatuur of gevoelige documenten in op te bergen.
Als u deze volgens de instructie sluit, is deze alleen te openen door de sealbag zichtbaar te beschadigen.

Wis de belgeschiedenis van uw telefoon en verwijder ontvangen en verzonden sms- berichten. Zet alleen noodzakelijke contacten in uw contactenlijst.

Privé

Wees terughoudend met het meenemen van privéapparatuur. Ook uw privéapparatuur kan doelwit zijn. Bovendien is (mobiele) privéapparatuur doorgaans kwetsbaarder voor digitale aanvallen.

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

Zet niet op sociale media dat u op reis gaat, zoals bijvoorbeeld X (voorheen Twitter), Facebook, Instagram of LinkedIn.

Tijdens de reis

Algemeen

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

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 bijvoorbeeld sealbags voor.

Maak geen gebruik van de hotelkluis voor vertrouwelijke informatie of gegevensdragers. Houd deze bij u.

Digitaal

Schakel al uw apparaten uit als u een vertrouwelijk gesprek voert. Verwijder de batterij als dat mogelijk is, of leg uw apparaat tussen uw kleding of in uw tas zodat het geluid gedempt wordt.

Neem aanvullende maatregelen als u staatsgeheime en/of zeer gevoelige gesprekken moet voeren. Voer deze niet in de aanwezigheid van mobiele apparaten. Apparaten uitschakelen geeft geen garantie, deze kunnen heimelijk nog aan staan.

Herstart regelmatig uw telefoon.

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

Maak altijd gebruik van uw mobiele (data-)abonnement. Gebruik ook een door uw organisatie aanbevolen VPN-verbinding. Zet de wifi-functie uit.

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.

Wees bedacht op het risico van social engineering, geef nooit authenticatie- gegevens of wachtwoordherstel-links af.

Als u wilt bellen, maak dan gebruik van een chat-app die standaard end-to-end-versleuteling toepast en activeer de optie (her) registratie via PIN of MFA.

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

Maak gebruik van beveiligde en goedgekeurde USB-sticks. Ga bij uw beveiligingsfunctionaris na wat goedgekeurd is.

Als u uw USB-stick plaatst in apparatuur van derden, kan deze besmet raken met malware. Gebruik deze USB-stick dan niet meer tijdens uw reis. Laat deze USB-stick achter of neem deze mee terug om deze te laten vernietigen of te schonen.

Plaats geen USB-sticks (of andere gegevensdragers) van derden in uw apparatuur. USB-sticks kunnen besmet zijn met malware. Mocht u USB-sticks met informatie meekrijgen, bespreek met uw beveiligingsfunctionaris hoe u deze informatie veilig op uw bedrijfsnetwerk kunt (laten) overzetten.

Geef uw apparatuur nooit af. Moet dat wel vanwege veiligheidsmaatregelen, geef deze dan aan een collega die niet met u mee naar binnengaat. Is dat niet mogelijk, schakel de apparatuur dan uit, stop deze in een sealbag en bij voorkeur ook in een kluisje waarvan u de sleutel heeft.

Sta niet toe dat anderen gebruikmaken van uw apparatuur.

Waarschuw bij een mogelijk incident altijd direct de beveiligingsfunctionaris van uw organisatie. Hiermee geeft u uw organisatie de mogelijkheid om tijdig maatregelen te treffen.

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 bij uw eigen organisatie 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:

- Pas op voor spearphishing. Ga altijd na of ontvangen berichten voor u bestemd zijn. Bij twijfel controleert u eerst de herkomst van het bericht bij de afzender voordat u bijlagen opent of op links klikt.
- 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 tweefactorauthenticatie.

Lees op www.aivd.nl meer over veilig digitaal werken, zoals in de AIVD-publicatie '*Cyberaanvallen door statelijke actoren: 7 momenten om een aanval te stoppen?*'.

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

Goede reis!

Algemene Inlichtingen- en Veiligheidsdienst
Postbus 20010 | 2500 EA Den Haag
T (079) 320 50 50

www.aivd.nl
April 2024