TRAVEL SECURITY

HOE UZELF EN UW GEGEVENS BESCHERMEN IN HET BUITENLAND

SECURITY PASSPORT

VOOR WIE IS DIT DOCUMENT BESTEMD ?

Deze brochure omvat een reeks nuttige adviezen voor elke persoon of organisatie die de veiligheid van zijn/haar gegevens wil verbeteren tijdens verplaatsingen naar het buitenland.

De adviezen bieden echter geen absolute garantie. Iedereen moet er zelf over waken dat zijn/haar gegevens of die van zijn/haar organisatie zo goed mogelijk beveiligd zijn.

VERHOOGD RISICO IN HET BUITENLAND

We zijn zo gewend geraakt aan reizen naar het buitenland dat we **vaak vergeten aan welke risico's we worden blootgesteld**. Een ongeval, gegevensverlies, diefstal of spionage: niemand blijft ervan gespaard.

Een reiziger is kwetsbaar. Hij verplaatst zich en neemt hierbij gegevens of materiaal mee van zijn organisatie of zijn land. Criminelen, maar zeker ook buitenlandse inlichtingendiensten en andere personen of organisaties zien dit als opportuniteit. Buitenlandse inlichtingendiensten hebben waarschijnlijk meer interesse in u dan u zelf verwacht. Ze zijn vooral uit op de kennis die

u hebt, die u bij zich draagt of waar u digitaal toegang toe hebt.

Onderschat de risico's niet: reputatie- of financieel verlies, vervolging of sancties, diplomatieke of politieke incidenten enzovoort. De gevolgen voor u en uw organisatie kunnen (zeer) groot zijn.

In dit document vindt u adviezen terug voor **elk van de drie fases van een reis**: vóór het vertrek, tijdens de reis en bij de terugkeer.

Het risico is niet in elk land hetzelfde. De adviezen zijn dus niet noodzakelijk van toepassing voor elk van uw reizen of verplaatsingen. U dient finaal de mogelijke risico's zelf goed in te schatten.

HOE KAN U UZELF BESCHERMEN?

Kies adviezen die overeenstemmen met uw noden en met het risiconiveau van uw verplaatsing.

3 NIVEAUS VAN AANBEVELING

BASIC

De minimaal vereiste bescherming voor elke verplaatsing.

MEDIUM

Bijkomende maatregelen voor een betere bescherming van uw persoonlijke gegevens en die van uw organisatie.

HIGH

De strengste maatregelen nodig voor reizen buiten de Europese Unie of wanneer u gevoelige informatie meeneemt.

Bovenstaande aanbevelingsniveaus zijn cumulatief.

3 FASES

VOOR HET VERTREK

Een gedegen voorbereiding is essentieel om het risico te beperken. Wat is het doel? Het aantal documenten en opslagmedia (laptops, smartphones, usb-sticks, etc.) beperken en deze goed te beveiligen.

Stel u daarom altijd de volgende vragen voor u vertrekt:

- Heb ik dit echt nodig?
- Wat is de waarde van de informatie die ik meeneem?
- Wat is de impact van oneigenlijk gebruik van deze informatie?
- Welke apparaten neem ik mee en tot welke informatie hebben deze toegang?

TIJDENS DE REIS

Voorzichtigheid en discretie zijn de sleutelwoorden van een gewaarschuwd reiziger. Wees geen open boek voor anderen en hou permanent de controle over uw informatie.

BIJ DE TERUGKEER

Bepaalde dreigingen blijven bestaan, ook bij uw terugkeer. Laat bij de minste twijfel uw opslagmedia controleren door en rapporteer elk incident aan uw veiligheidsverantwoordelijke.

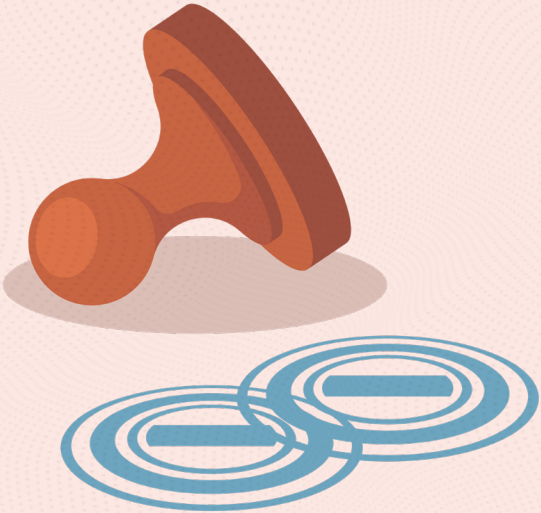
VOOR HET VERTREK

1. Informeer u over uw bestemming

Zorg dat u op de hoogte bent van de **politieke, economische en sociale situatie van uw bestemming**. U vindt nuttige informatie op de pagina “Reisadviezen” van de website van de FOD Buitenlandse Zaken **www.diplomatie.belgium.be**. Meld u ook aan via de website travellersonline.diplomatie.be. Zo kan de FOD Buitenlandse Zaken u eenvoudiger informeren en ondersteunen. BASIC

Vergeet de **gegevens van de dichtstbijzijnde Belgische ambassade of consulaat** niet op te slaan of op papier te noteren. MEDIUM

Informeer naar de lokale wetgeving en eventuele reisvergunningen. Als u voor buitenlandse overheidsdiensten reisdocumenten dient in te vullen, geef dan enkel de **strikt noodzakelijke informatie en geef pas meer details bij aandringen.** HIGH



2. Bereid uw documenten en opslagmedia voor

Ga na welke **veiligheidsvoorschriften gelden binnen uw organisatie**. Aarzel vooral niet om contact op te nemen met de veiligheidsverantwoordelijke(n) om uw reis goed voor te bereiden. BASIC

Neem enkel die documenten en opslagmedia mee die strikt noodzakelijk zijn. Wees u bewust van de context en de doelstellingen van de reis. In sommige landen zijn de veiligheidsdiensten gemachtigd om toegang te vragen tot uw opslagmedia en/of ze in beslag te nemen. Door niet-noodzakelijke documenten of opslagmedia mee te nemen, loopt u dus nodeloos risico's. BASIC

Maak een **back-up** van uw gegevens en laat deze thuis. BASIC

Vervoer uw vertrouwelijke documenten en gegevensdragers altijd in **uw handbagage, nooit in uw koffer**. BASIC

Neem uw gevoelige documenten mee in **verzegelde en beveiligde enveloppes** (zogenaamde sealbags) en voorzie deze ook voor de andere fases van de reis. MEDIUM

Neem – indien mogelijk – enkel mobiele toestellen mee die speciaal voorzien zijn voor de reis en door uw organisatie geleverd werden. Deze toestellen mogen **enkel de strikt noodzakelijke gegevens** bevatten die nodig zijn voor de reis. Bij uw terugkeer moeten deze toestellen opnieuw worden geformatteerd voor ze terug kunnen worden gebruikt. HIGH

3. Bescherm uw mobiele toestellen

Volg de aanbevelingen die beschikbaar zijn via **www.safeonweb.be/tips**

We vestigen graag uw aandacht op de volgende aanbevelingen:

- Installeer de laatste updates van het besturingssysteem (OS) en de programma's en installeer enkel programma's of apps via officiële appstores; BASIC
- Installeer een antivirus op al uw mobiele toestellen; BASIC
- Controleer de veiligheids- en privacy-instellingen op uw toestellen en de accounts die eraan gekoppeld zijn. Scherm daarbij uw persoonsgegevens zoveel mogelijk af; BASIC
- Gebruik veilige vergrendelingsmethodes en schakel de inhoud van meldingen uit, zo kan niemand ongewenst meelezen; BASIC
- Bescherm uw paswoorden! Schrijf deze niet op, wijzig ze regelmatig en gebruik waar mogelijk Two-Factor Authentication (2FA); BASIC
- Installeer end-to-end encrypted berichtenapplicaties; BASIC
- Wis uw bel- en internetgeschiedenis voor uw vertrek. MEDIUM

Hanteer altijd een **onderscheid tussen werk en privé**, zowel voor toestellen, accounts, telefoonnummers als e-mailadressen. MEDIUM

Om geen spoor van de netwerken en toestellen van uw thuis na te laten, selecteer 'vergeet' voor alle eerder **verbonden netwerken en Bluetoothtoestellen**. MEDIUM

Voorzie een door **VPN** beveiligde verbinding, voornamelijk voor de toegang tot uw berichten of tot het netwerk van uw organisatie. MEDIUM

Encrypteer gevoelige gegevens op uw opslagmedia volgens de regels van uw organisatie. MEDIUM

Opgelet: sommige landen verbieden het gebruik van VPN of encryptiesoftware! Ga dit dus zeker na voor u afreist naar uw bestemming.

Zet zo weinig mogelijk applicaties op uw toestel en hanteer zo veel als mogelijk een **webbrowser als alternatief**. Zo heeft de applicatie geen toegang tot de informatie op het toestel. HIGH

4. Sociale netwerken

Controleer uw **privacy-instellingen** op sociale media. Uw persoonsgegevens schermt u best zoveel mogelijk af. BASIC

Kijk de **toegangen per applicatie** (tot microfoon, camera, contacten, locatie, etc.) na. Vaak zijn deze niet strikt nodig voor het gebruik van de applicatie. BASIC

Vermijd - indien mogelijk - over uw reis te communiceren via sociale media. Zet bij voorkeur ook geen details online over het programma, de personen die u begeleiden en/of uw locatie. MEDIUM

Ga niet zomaar in op berichten, netwerkverzoeken of uitnodigingen van derden. Beperk u tot de **voor de reis noodzakelijke communicatie.** MEDIUM

TIJDENS DE REIS

1. Blijf discreet en voorzichtig

Draag geen zichtbare logo's of identiteitsgegevens buiten de werkplek. MEDIUM

Geef uw locatie niet prijs via uw smartphone of tablet. Schakel **de toegang tot uw locatiegegevens uit.** MEDIUM

Vermijd nieuwsgierige blikken. Plaats daarom **een filter op uw scherm** wanneer u op een openbare of drukke plek moet werken. MEDIUM

Praat niet over gevoelige of polariserende onderwerpen op openbare plekken waar anderen kunnen meeluisteren. MEDIUM

Schakel de **niet-noodzakelijke verbindingen** (Bluetooth, Wifi, Near Field Communication) van uw mobiele toestellen uit. **'Vliegtuigstand' is niet voldoende:** in deze stand zijn deze verbindingen niet altijd volledig uitgeschakeld. MEDIUM

Gebruik **geen voice-assistants** zoals Siri, Alexa of Bixby. Vermijd ook andere AI-apps. HIGH

Als u uw smartphone ergens moet afgeven of achterlaat, verwijder dan – indien mogelijk – **de**

simkaart, de geheugenkaart en de batterij. HIGH

2. **Bescherm voortdurend uw gegevens en opslagmedia**

Laat uw documenten, opslagmedia of toestellen **nooit onbeheerd achter** en geef zeker nooit toegang aan derden. BASIC

Laad uw toestellen niet op via aangeboden oplaadapparatuur en/of openbare USB-laadpunten om malware of gegevensdiefstal te vermijden. Indien dit niet anders kan, gebruik dan een datablockerkabel om uw toestel te beschermen. BASIC

Voorzie **aangepaste antidiefstalsystemen** en breng unieke wachtwoorden aan op uw toestellen opdat ze niet met andere kunnen worden verwisseld. MEDIUM

Laat geen gevoelige documenten achter in uw hotelkamer, ook niet in de kluis. Deze kan gemakkelijk door hotelpersoneel worden geopend op vraag van mensen met slechte bedoelingen. MEDIUM

Maak **geen verbinding** met openbare wifi-netwerken, maak geen openbare bluetoothconnecties (bijvoorbeeld met een huurauto) en vermijd het gebruik van QR-codes die u niet vertrouwt. MEDIUM

Schakel uw toestellen 's nachts volledig uit – doe

elke dag een **power cycle** (toestel volledig aan- en uitzetten). HIGH

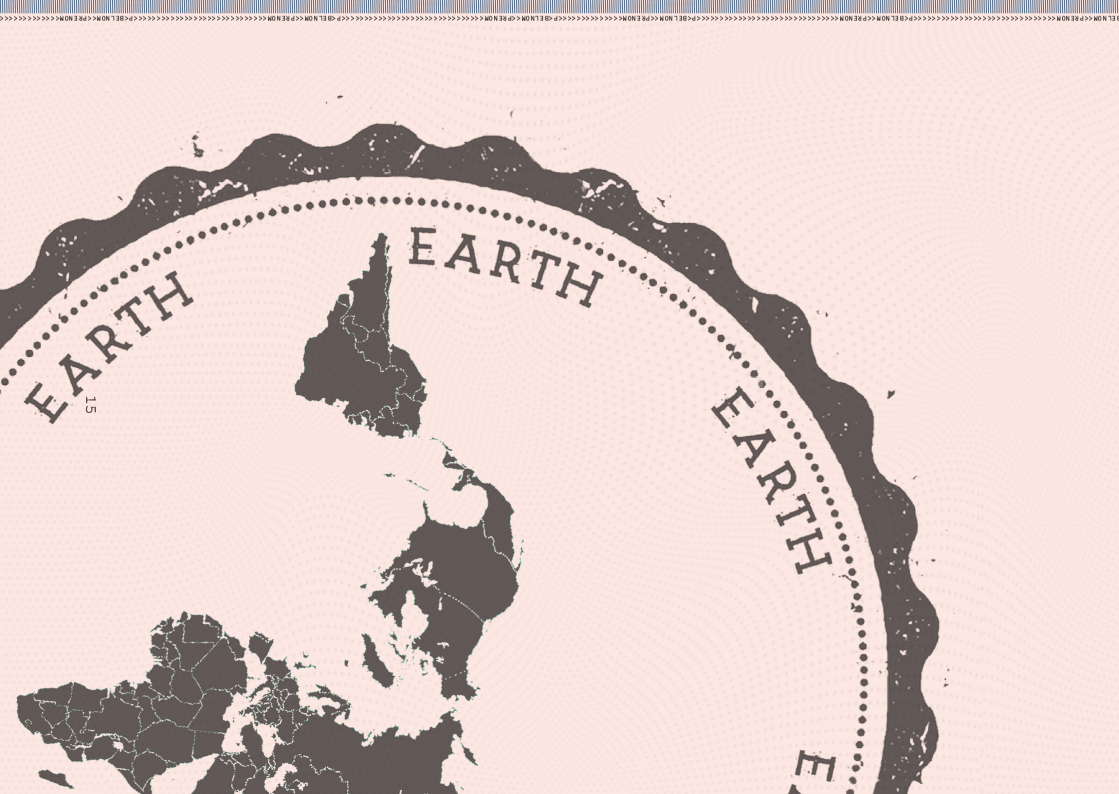
3. Blijf kritisch

Blijf kritisch wanneer u opvallend veel aandacht krijgt of wanneer uw gesprekspartner verwijst naar gedeelde ideologische, culturele of religieuze referenties. MEDIUM

Wees voorzichtig met vleierijen, ontboezemingen en geschenken (zelden is dat belangeloos). MEDIUM

Laat u niet van de wijs brengen door een blijk van verbondenheid of vriendschap. Deze elementen kunnen wijzen op **een poging tot manipulatie**. MEDIUM

Wees even voorzichtig tijdens (sociale) evenementen die worden georganiseerd in de marge van een officiële bijeenkomst. MEDIUM


EARTH
EARTH
EARTH
EARTH

BIJ DE TERUGKEER

Voer bij terugkomst een **power cycle** uit op uw toestellen. BASIC

Meld elk incident of verdacht voorval schriftelijk aan de veiligheidsverantwoordelijke van uw organisatie. BASIC

Als u een **USB-stick of ander elektronisch opslagmedium hebt ontvangen, sluit die nooit aan** op uw computer zonder voorafgaande veiligheidscontrole door een expert. BASIC

Laat bij de minste twijfel **uw computer of smartphone onderzoeken** en **verander uw wachtwoorden**. BASIC

Scan uw toestellen **regelmatig** voor virussen en malware. BASIC

Stel het nut van de tijdens de reis aangeknoopte relaties in vraag. **Blijf kritisch** wanneer na de reis opnieuw contact met u wordt opgenomen: zijn de verzoeken, vragen of aanbiedingen gerechtvaardigd en relevant? MEDIUM

WAT TE DOEN BIJ EEN INCIDENT?

Bij verlies of diefstal van het document of opslagmedium stelt u een lijst op van de betrokken gegevens. Verwittig meteen uw werkgever of veiligheidsverantwoordelijke volgens de voorschriften van uw organisatie. Indien nodig, richt u zich tot de lokale politie.

Neem bij verlies van identiteitsdocumenten contact op met de Belgische ambassade of het consulaat.

Bel naar Cardstop bij verlies van uw bankkaart op het nummer **078 170 170**. U kan uw kaart ook blokkeren via de applicatie van uw bank.

Werd u geconfronteerd met andere verdachte situaties (lange ondervraging tijdens grenscontroles, ongevraagd foto's genomen, verplicht afgeven opslagmedia, …), neem dan contact op via **vsse.be/contact**.

MEER WETEN?

- www.vsse.be
- www.diplomatie.belgium.be
- www.safeonweb.be

DE VSSE

De VSSE is bevoegd voor de opvolging van inmenging of spionage die een bedreiging vormen voor de fundamentele waarden van de staat, met inbegrip van de bescherming van het wetenschappelijk en economisch potentieel. Tijdens buitenlandse reizen is er een verhoogd risico op deze dreigingen.

Als u denkt dat u of uw organisatie het slachtoffer is geworden van inmengings- of spionageactiviteiten, of als u over informatie beschikt die mogelijk gelinkt is aan deze dreigingen, neem dan contact op via **www.vsse.be/contact**.

VSSE

VSSE

.be

Verantwoordelijke uitgever: FRANCISCA BOSTYN
Koning Albert II-laan, 6 - 1000 BRUSSEL