# VUB Informatieveiligheid en Privacy

## How To – Reizen naar landen met een hoog risico

**Verantwoordelijke:**
**CISO**

**Contact:**
ciso@vub.be

**Huidige versie:**
6 december 2019

# I. Inleiding

Een «How To»-document verschaft informatie en/of tips over onderwerpen die specifiek verband houden met Informatieveiligheid en Privacy. Het bevat geen verplichte richtlijnen, enkel informatie over hoe een standaard/richtlijn toegepast kan worden.

Het is een document dat voortdurend evolueert en de kwaliteit ervan hangt deels af van de feedback van de lezers/gebruikers. Op pagina 1 staat het e-mailadres waar u uw feedback naar toe kunt sturen.

Een «How To»-document vereist geen formeel advies of goedkeuringsproces.

Dit «How To»-document handelt over reizen naar landen met een hoog risico, dit zijn landen met een specifiek hoog risico inzake Informatieveiligheid en Privacy.

# II. Reizen naar landen met een hoog risico

## II.1. Landen met een hoog risico

Wie op reis gaat moet altijd het reisadvies nalezen dat verstrekt wordt door de Belgische dienst Buitenlandse Zaken[1]. Men kan ook de Amerikaanse reisadviezen[2] raadplegen, maar vergeet daarbij niet dat deze zich specifiek richten tot Amerikaanse burgers, die misschien een ander risicoprofiel hebben als Europese burgers. Reizigers met een andere nationaliteit kunnen ook het reisadvies van hun thuisland nalezen op zoek naar specifieke vereisten/waarschuwingen die met hun nationaliteit verband houden.

Een land kan een hoog-risicoland zijn vanwege fysieke risico's. Zo is Colombia een hoog-risicoland vanwege de hoge criminaliteit en terrorisme. Andere landen zijn landen met een hoog risico vanwege de risico's inzake informatieveiligheid en privacy. China is bijvoorbeeld een hoog-risicoland vanwege zijn door de staat gesponsorde cybercapaciteit en de bereidheid om deze voor economische, militaire en politieke doeleinden in te zetten.

⚠Dit document zal enkel handelen over reizen naar landen die een hoog risico vormen voor de informatieveiligheid en privacy van de VUB en de VUB-reizigers.

Landen als China en Rusland zijn voorbeelden van hoog-risicolanden met een hoog informatieveiligheid en privacy risico. Het is belangrijk niet uit het oog te verliezen dat dit geen open democratieën zijn en dat de privacy er niet beschermd wordt zoals in de EU. Zowel het gaan en staan als alle communicatie van individuen kan in de gaten gehouden worden. Het is mogelijk dat er binnengedrongen wordt in elektronische apparatuur, dit om informatie te stelen en/of om deze met malware te besmetten met de bedoeling bij de terugkeer van de reiziger binnen te dringen in het VUB-netwerk. Het is mogelijk dat de toegang tot bepaalde websites, waaronder veel gebruikte Westerse sociale media, geblokkeerd wordt. En de websites die niet geblokkeerd zijn worden mogelijk in de gaten gehouden. Ook is het mogelijk dat beveiligde websites ("https") en/of het VUB "virtual private network (VPN)" netwerk geblokkeerd wordt, dit omdat het voor de overheden van die landen moeilijker is om dit versleutelde verkeer te controleren.

[1] https://diplomatie.belgium.be/nl/Diensten/Op_reis_in_het_buitenland/reisadviezen (informatie beschikbaar in het Nederlands en het Frans).
[2] https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

## II.2. Risico's

VUB-reizigers zijn zeker een potentieel doelwit als zij rechtstreeks betrokken zijn bij vertrouwelijk of gepatenteerd onderzoek in een STEM-discipline (Science, Technology, Engineering & Mathematics). Ook VUB-reizigers die niet rechtstreeks bij een STEM-discipline betrokken zijn kunnen een doelwit zijn omdat zij kunnen gebruikt worden om het VUB-netwerk binnen te dringen.

Alle elektronische apparatuur (laptops, tablets, e-book readers, smart phones, gsm's) kunnen door middel van malware of geautomatiseerde hackingtools met succes aangevallen en gecompromitteerd worden. Beveiligingssoftware, waaronder antivirussystemen, kunnen zelfs wanneer zij up-to-date worden gehouden niet altijd voorkomen dat elektronisch apparatuur gecompromitteerd wordt.
Het is mogelijk dat elektronische apparatuur bij de grens door de douane gecontroleerd of zelfs volledig gekopieerd wordt. In bepaalde landen is het mogelijk dat de douanebeambten uw apparaat, bij aankomst in of vertrek uit het land, tijdelijk in beslag nemen en daarbij een kopie nemen van uw volledige systeem.

Versleutelingstools kunnen gebruikt worden voor illegale doeleinden, inclusief terroristische activiteiten. Daarom dat meerdere landen de invoer, uitvoer en het gebruik van versleutelingstools reguleren. Reizigers moeten bij twijfel informatie over het standpunt van het land van bestemming inzake versleutelingstools inwinnen. China en Rusland zijn allebei hoog-risicolanden die negatief staan tegenover versleuteling op elektronische apparatuur.

Het "Akkoord van Wassenaar[3]" laat krachtens een "vrijstelling voor persoonlijk gebruik" toe dat een reiziger een deelnemend land zonder problemen met een versleuteld apparaat bezoekt, dit op voorwaarde dat de reiziger de versleutelingstechnologie tijdens zijn bezoek niet aanmaakt, uitbreidt, deelt, verkoopt of op een andere wijze verspreidt. Ga naar de website om te zien welke landen het akkoord ondertekend hebben.

## II.3. Aanbevelingen

Hoop op het beste, verwacht u aan het ergste.

- Het is onmogelijk om een apparaat tegen alle mogelijke aanvallen te beschermen, zeker niet als die aanvallen uitgaan van een nationale overheid. Het is daarom best om ervan uit te gaan dat elk apparaat dat u meeneemt naar een hoog-risicoland op de een of andere allicht niet op te sporen manier gecompromitteerd werd.
- Ga ervan uit dat alles wat u doet, zeker via het internet, onderschept zal worden. Blijf waakzaam met betrekking tot de inhoud die u deelt (via e-mail, datatransmissie, spraak).

### II.3.1. Voordat u naar een hoog-risicoland afreist

- Zoek informatie op over mogelijke bijzondere plaatselijke wetten die in het land van bestemming gelden. Deze kunnen totaal verschillend zijn van wat wij gewoon zijn.

- Hou het aantal elektronische apparaten (data/communicatie) die u meeneemt, beperkt.

- Als u apparaten moet meenemen, neem dan zeker geen apparaten mee die u voor uw dagelijkse activiteiten gebruikt.
    - Gebruik een tijdelijke (goedkope/afgeschreven) laptop.
    - Gebruik een prepaid wegwerp-gsm, die speciaal voor uw reis aangekocht wordt.

  Departementen waar vaak medewerkers naar hoog-risicolanden reizen, dienen te overwegen om een reiskit die alle vereiste elektronische apparaten bevat ter beschikking te houden.

[3] https://www.wassenaar.org/

- Gebruik een (tijdelijke) laptop voorzien van:
  - Een webcam cover.
  - Een dummy audio-kabel (de ingebouwde microfoon van de laptop wordt uitgeschakeld door een connector in de audio-aansluiting van de laptop te plaatsen, zelfs wanneer geen koptelefoon of gelijkaardig op die connector aangesloten is).
  - Werk niet met Office 365-authenticatie, maar wel met een plaatselijke account.
    Ideaal is één admin-gebruiker, enkel indien nodig te gebruiken, en één standaardgebruiker, voor dagelijks gebruik tijdens de reis. Maak gebruik van veilige, lange wachtwoorden.
  - Zorg ervoor dat de Office 365 OneDrive-functie niet geïnstalleerd is. Vergeet immers niet dat OneDrive al uw gegevens zou synchroniseren met een kopie op de laptop.

- Schakel alle onnodige netwerkprotocollen (zoals WiFi, Bluetooth of infrarood) en locatiedeling uit. En dit op al uw apparaten.

- Wis de gespreks- en navigatiegeschiedenis op uw apparaten.

- Zorg ervoor dat de systemen die u gebruikt, volledig gepatcht zijn (d.w.z. met de meest recente beveiligingsupdates geïnstalleerd).

- Zorg ervoor dat op al uw apparaten antivirus- en antimalwaresoftware geïnstalleerd is.

- Overweeg om een tijdelijk e-mailadres aan te maken (bijvoorbeeld via Gmail), dat u enkel tijdens deze reis gebruikt.
  Indien het noodzakelijk is dat u over bepaalde gegevens zou kunnen beschikken, overweeg dan om een tijdelijke opslagaccount in de cloud aan te maken (b.v. via Dropbox), die enkel dient voor gebruik tijdens uw reis. U kan de gegevens die u mogelijk nodig hebt, op die locatie opslaan, maar ga er opnieuw van uit dat de opgeslagen gegevens onderschept kunnen worden van zodra u inlogt. Voor bijkomende veiligheid kunt u de in de cloud opgeslagen gegevens versleutelen met een tool zoals Boxcryptor[4] .

- Laat alle onnodige deursloten, smartkaarten, eenmalige wachtwoord hard tokens en andere gelijkaardige vergrendelingsystemen thuis.

- Zorg ervoor dat u, in geval van nood, de contactgegevens van de ambassade/vertegenwoordiging in het land van bestemming binnen handbereik hebt.

### II.3.2. Tijdens uw reis

- Wees waakzaam voor schoudersurfen (persoon met slechte bedoelingen die over uw schouder meekijkt wanneer u gegevens intikt zoals uw gebruikersnaam en wachtwoord). Kijk altijd om u heen wanneer u in uw apparaat inlogt of er gegevens invoert.

- Hou uw elektronisch apparatuur altijd binnen handbereik. Het kluisje in uw hotel is niet veilig.

- Zet uw systeem niet in slaap- of sluimerstand wanneer u er niet op aan het werken bent. Beter is om uw apparaat volledig uit te schakelen.

[4] Opgepast: deze tools worden door VUB DICT niet centraal ondersteund. Zij mogen enkel gebruikt worden indien de gebruiker ze voldoende beheerst.

- Maak beter geen gebruik van Office 365 online.

- Indien u niet wilt dat u geografisch traceerbaar bent, of u probeert om een vertrouwelijk gesprek te voeren, dan moet u de batterijen uit uw gsm verwijderen. Uw gsm uitschakelen volstaat niet.

- Probeer niet om de nationale censuur te omzeilen (b.v. met Tor of een gelijkaardige tool). Deze producten/processen kunnen in sommige hoog-risicolanden geblokkeerd worden en/of aanleiding geven tot gerechtelijke vervolging.

- Zorg ervoor dat u afgedankt (bv., kapot) elektronisch/niet-elektronisch materiaal waarop ooit vertrouwelijke gegevens hebben gestaan veilig vernietigd. Fysiek vernietigen is de beste oplossing.

- Maak geen gebruik van laadstations die werken met een USB-aansluiting, aangezien het laadstation via de USB-interface meer kan doen dan alleen stroom verstrekken (b.v. uw apparaat uitlezen).

- Maak geen gebruik van openbare werkstations, tenzij u geen andere keuze hebt. Vergeet niet dat alles wat u invoert, ook uw inloggegevens, gevaar loopt.

- Koop tijdens uw reis geen nieuwe hardware.

- Koop of download tijdens uw reis nooit nieuwe software.

- Laat een defect elektronisch apparaat tijdens uw reis niet ter plaatse herstellen of nakijken.

- Sluit nooit een onbekende USB-stick, CD/DVD/Blue Ray of andere randapparatuur aan op uw apparaat.

- Verwittig in geval van een incident, waaronder een verloren/gestolen apparaat, zo snel mogelijk de VUB Helpdesk (helpdesk@vub.be). Deze zal dan de nodige maatregelen treffen (zo nodig uw account blokkeren tot u terug bent).

- Pas op voor pogingen om u in verlegenheid te brengen. U kunt immers het doelwit worden van afpersing.

- Indien u gearresteerd, in hechtenis genomen of verhoord wordt, leg dan geen verklaringen af of onderteken geen documenten, in het bijzonder niet als deze opgesteld zijn in een taal die u niet begrijpt. Vraag dat de Belgische ambassade of het Belgische consulaat (of indien u een andere nationaliteit hebt, de ambassade van uw land) van uw hechtenis ingelicht wordt.

### II.3.3. Bij uw terugkeer van reis

- Laat alle elektronische apparatuur indien mogelijk volledig wissen en van nul af aan opnieuw installeren. Alle gegevens die bewaard moeten blijven, worden op een USB-stick gezet. Het elektronisch apparaat zelf wordt nooit op het VUB-netwerk aangesloten. (gebruik maken van een reiskit maakt dit eenvoudiger, aangezien niet geraakt wordt aan de apparatuur waarmee u dag in dag uit werkt).

- Verander alle wachtwoorden die u tijdens uw reis gebruikt hebt. Het is aan te raden dat u altijd uw Office 365-wachtwoord verandert, zelfs wanneer u dit tijdens uw reis niet gebruikt zou hebben.

## II.4. Landen met lager risico

Bemerk dat voor lager-risicolanden zoals de Verenigde Staten ook bepaalde veiligheidsoverwegingen gelden. De douane kan het recht hebben om uw laptop te doorzoeken en u kunt wettelijk verplicht worden om uw gebruikersnaam en wachtwoord nodig om uw laptop op te starten, te verstrekken. Op die manier kan gevoelige informatie op een laptop gevaar lopen.

U moet een risicobeoordeling maken van het land van bestemming en in het licht daarvan bepalen welke gegevens u zult meenemen. Het kan verstandig zijn sommige van de hierboven verstrekte aanbevelingen om uw gegevens te beschermen ook toe te passen bij een bezoek lager-risicolanden.

## A. Bijlage: Bronnen

Stanford University: https://uit.stanford.edu/security/travel/high-risk-countries-recommendations

University of Rhode Island: https://security.uri.edu/travel/travel-to-china-or-russia/

Princeton University: https://informationsecurity.princeton.edu/intltravel

China Business Review: https://www.chinabusinessreview.com/cybersecurity-best-practices-for-the-traveling-executive-a-qa-with-crumpton-groups-rick-doten/

Harris/Bricken: https://www.chinalawblog.com/2016/01/when-going-to-china-be-paranoid-about-your-data-and-your-privacy.html

België Buitenlandse Zaken: https://diplomatie.belgium.be/nl/Diensten/Op_reis_in_het_buitenland/reisadviezen

US Department of State: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

Het Akkoord van Wassenaar: https://www.wassenaar.org/

Freshfields Bruckhaus Deringer: https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/data/china-rules-on-encryption/

 