



Nationaal Coördinator  
Terrorismebestrijding en Veiligheid  
*Ministerie van Justitie en Veiligheid*

# Uw eigen veiligheid

Wat u zelf kunt doen om uw veiligheid te vergroten





**Sommige (publieke) functies kunnen mensen kwetsbaar maken voor veiligheidsincidenten. In deze brochure vindt u concrete tips en adviezen over wat u zélf kunt doen om uw veiligheid te vergroten. Ook leest u waar u op kunt letten om risico's te verkleinen.**

Met bewust gedrag, een bewuste houding en bewuste keuzes werkt u aan uw eigen veiligheid en kunt u mogelijke gevolgen beperken. Vaak is het niet nodig om extra maatregelen te nemen. Soms is dat wel wenselijk, bijvoorbeeld vanwege de gevoeligheid van de informatie waarmee u werkt. Informatie die voor derden interessant kan zijn. Kies de maatregelen die voor uw situatie relevant zijn. Het is daarbij raadzaam om ook na te gaan wat u van uw werkgever kunt verwachten en welke bijdrage hij kan leveren.

Informeer uw gezinsleden goed over de maatregelen die u neemt en het belang ervan. Heeft u kinderen? Leer ze hoe te reageren in noodsituaties, zoals het alarmnummer bellen of naar de burens gaan. Vertel jonge kinderen de deur of post niet te openen. Herhaal dit regelmatig, zodat ze het niet vergeten.

---

Het belangrijkste advies luidt: Let op uw omgeving en signaleer afwijkende situaties en/of personen. Schroom niet om verdachte situaties te melden bij de politie. Vertrouw daarbij op uw eigen intuïtie, u kent uw eigen omgeving immers het beste. Als u kinderen heeft, luister ook naar hen. Zij hebben een scherp observatievermogen en zien snel veranderingen.

De geschetste maatregelen in deze brochure zijn uiteraard niet bedoeld om angst of achterdocht te zaaien. Hier is vooral het bekende spreekwoord van toepassing: een gewaarschuwd mens telt voor twee.

## **Voor wie is deze brochure**

Deze brochure is primair bedoeld voor personen die door een (publieke) functie mogelijk kwetsbaar zijn voor veiligheidsincidenten. Maar door het algemene karakter van de informatie is de brochure geschikt voor iedereen die zijn of haar veiligheidsbewustzijn wil vergroten.

## **Blijf op de hoogte van de algemene dreigings situatie**

Het is van belang om op de hoogte te blijven van de algemene dreigings situatie in Nederland. De NCTV publiceert driemaal per jaar het Dreigingsbeeld Terrorisme Nederland (DTN) en eenmaal per jaar het Cybersecuritybeeld Nederland (CSBN).

De tips, voorbeelden en handvatten in deze brochure zijn tot stand gekomen in samenwerking met publieke en private partners.

# Inhoudsopgave

<b>Woning</b>	<b>6</b>
Sleutels	7
Ramen en deuren	7
Alarm	8
Verlichting	8
Personeel	8
Om het huis	9
<b>Communicatie</b>	<b>10</b>
Algemene tips	11
Smartphones	12
Computer	12
Internet	12
Wifinetwerken	13
Sociale media	13
Kinderen en internet	14
E-mail	14
Postbezorging	14
<b>Onderweg</b>	<b>16</b>
Algemene tips	17
De beveiliging van uw auto	18
Tijdens het autorijden	18
In en uit de auto stappen	18
Gebruik van openbaar vervoer	18
Gebruik van taxi's	18
<b>Werkplek</b>	<b>20</b>
<b>Buitenlandse (dienst)reis</b>	<b>24</b>
Belangrijke documenten en telefoonnummers	25
Reisvoorbereiding	25
Tijdens de reis	26
Hotel	26
Digitaal	27

Woning

**Door kritisch te kijken naar uw woning, kunt u mogelijk inbraken, insluipingen en andere vormen van criminaliteit voorkomen. Internet en de vele online registratiesystemen maken het eenvoudiger om adressen van mensen (met publieke functies) te achterhalen.**

**U maakt uzelf minder kwetsbaar door bijvoorbeeld de herkenbaarheid van uw woning te verminderen of ervoor te zorgen dat u niet meteen de deur van uw woning hoeft te openen om te kijken wie er voor de deur staat. Met de volgende tips maakt u uw huis minder toegankelijk voor ongewenste gasten.**

### **Sleutels**

- Beperk het aantal (reserve)sleutels.
- Zorg dat u weet wie een sleutel heeft van uw woning.
- Vervang slot/cilinder bij diefstal/verlies van sleutels.
- Voorzie sleutels nooit van naam en adres. Vermelding van een o6 nummer kan eventueel wel.
- Hang sleutels binnenshuis op een vaste, bereikbare plaats die niet zichtbaar is van buitenaf.

### **Ramen en deuren**

- Overweeg om geen naambordje aan uw woning te plaatsen. Indien u toch een naambordje wenst, vermeld dan alleen de familienaam en geen namen van gezinsleden.
- Maak gebruik van een deurbel intercom met videobeeld of het kijkvenster van de voordeur (indien aanwezig).
- Controleer of uw voor-en achterdeur zijn voorzien van kierstanden.
- Bevestig deugdelijk hang- en sluitwerk dat voldoet aan het Politiekeurmerk Veilig Wonen en gebruik het op de juiste manier.

- Beveilig ook de bovenverdieping van de woning indien die kwetsbaar is voor inklimming.
- Sluit altijd alle deuren en ramen, ook als u maar kort weg bent. Denk aan een wc-raam of garagedeur.

## Alarm

- Schakel uw alarmsysteem altijd in bij het verlaten van de woning (indien aanwezig).
- Overweeg om cameratoezicht rondom de woning te installeren.
- Zorg voor duidelijke afspraken met de alarmcentrale/bewaking over alarmopvolging.
- Zorg ervoor dat u en uw familieleden – en eventuele andere sleutelhouders – weten hoe te handelen bij alarmsituaties.

## Verlichting

- Zorg voor goede buitenverlichting. Dit kan kwaadwillenden afschrikken en draagt eventueel bij aan duidelijke en heldere camerabeelden (indien aanwezig).
- Geef de woning een bewoonde indruk als u er niet bent. Laat bij afwezigheid geen briefje achter op uw deur en laat licht branden in verschillende vertrekken in huis (met behulp van een tijdschakelaar en/of handige apps).

---

Bij het verlaten van uw woning:

Doe altijd alle ramen dicht, lichten aan en de deuren op slot.

## Personeel

- Selecteer zorgvuldig uw personeel voor in en om het huis, zoals schoonmakers, kinderoppas, tuinman of aannemer.
- Controleer bij het aannemen van nieuwe mensen hun referenties en identiteitsbewijs. Vraag, indien u dat wenst, naar een 'Verklaring omtrent gedrag'.
- Zorg dat uw personeel u altijd kan bereiken: geef hen uw mobiele telefoonnummer.



## Om het huis

- Geef alles rondom het huis een vaste plek. Zo is een afwijking direct zichtbaar. Dit stelt u in staat om ongewone of verdachte objecten snel te identificeren.
- Verwijder alles wat mogelijk gebruikt kan worden om schade aan te richten of binnen te treden. Denk hierbij aan losse stenen of een ladder.
- Plaats buiten geen hoge aanplant of grote objecten. Deze kunnen een hulpmiddel of schuilplaats vormen voor inbrekers.
- Ken uw burens, maak afspraken over wat te doen als iemand iets verdachts ziet.
- Wanneer u vertrouwelijk of gevoelig materiaal weggooit, behandel dit dan als vertrouwelijk afval. Gooi het niet weg bij het gewone afval. Versnipper documenten zoveel mogelijk of bewaar vertrouwelijk materiaal veilig tot het op de juiste manier afgevoerd kan worden.

---

## Handige links

[www.politiekeurmerk.nl](http://www.politiekeurmerk.nl)  
[www.justis.nl/producten/vog/](http://www.justis.nl/producten/vog/)  
[www.maakhetzeniettemakkelijk.nl](http://www.maakhetzeniettemakkelijk.nl)

# Communicatie

**Digitale communicatiemiddelen zijn niet weg te denken uit het dagelijks leven, maar brengen ook risico's met zich mee. Zo kan een valse e-mail of link naar een nepwebsite leiden tot een hackpoging of oplichting. Door het treffen en actueel houden van uw (digitale) beveiligingsmaatregelen kunt u het risico dat derden ongemerkt toegang tot uw informatie krijgen beperken.**

**Weet met wie u communiceert en kies bewust welke informatie u online plaatst. Hoe bewuster u omgaat met uw gegevens op internet, hoe kleiner de kans dat er misbruik wordt gemaakt van deze gegevens. Met onderstaande tips kunt u de risico's inschatten en beperken.**

---

### **Algemene tips**

- Installeer steeds software-updates van besturingssystemen, browsers en andere programma's. Deze worden uitgebracht om beveiligingslekken te verhelpen. Het helpt om hiervoor automatisch updaten in te stellen.
- Beveilig en vergrendel uw elektronische en mobiele apparaten altijd met een wachtwoord, vingerafdruk of eventueel gezichtsherkenning. Verander wachtwoorden bij (vermoeden van) inbreuk op een account en gebruik waar mogelijk tweestapsverificatie (SMS, pincode, token of biometrie).
- Laat u nooit onder druk zetten in berichten (in welke vorm dan ook) die u vragen snel bepaalde handelingen uit te voeren. Ga voordat u iets doet na of u:
  - de afzender kent;
  - het bericht verwacht;
  - begrijpt wat er gevraagd wordt en waarom;
  - het gevraagde logischerwijs past bij de afzender en het moment.

- Bij twijfel: probeer de afzender via een ander kanaal te bereiken, bijvoorbeeld een algemeen telefoonnummer van een organisatie.
- Er zijn bedrijven zijn die zich specialiseren in vertrouwelijke afvalverwerking. Vernietig via hen CDs, DVD's, USB's, PC's, laptops, tablets, smartphones en andere apparaten die gevoelige of vertrouwelijke data kunnen bevatten.

## Smartphones

- Zet uw nummeridentificatie uit als u belt met onbekenden.
- Bespreek geen vertrouwelijke informatie per telefoon; u kunt ongemerkt afgeluisterd worden.
- Programmeer alarmnummers in uw telefoon zodat ze eenvoudig te bellen zijn.
- Zet uw bluetooth-functie uit. Bluetooth is onveilig en spionage via deze functie is eenvoudig.
- Plaats een privacy screen op uw smartphone, tablet en laptop. Zo wordt meegelezen vanaf uw scherm moeilijker. Plak tevens uw webcam of camera af met een schuifluikje.
- Installeer alleen apps via de officiële applicatiewinkels.
- Zet de locatiefunctie uit om er voor te zorgen dat uw telefoon geen locatiegegevens meezendt ('geotagging') bij het gebruik van sociale media, het maken van foto's of het gebruik van andere apps. Stel een snelkoppeling in om de locatie eventueel in te schakelen als dat nodig is en schakel het weer uit als u klaar bent.
- Laat uw smartphone nooit onbeheerd achter.

## Computer

- Zorg voor goede beveiliging van uw computer en/of laptop; denk aan een virusscanner, firewall, ad-blocker en sterke wachtwoorden.
- Gebruik geen ongeautoriseerde software.

## Internet

- Controleer het webadres (URL) en de aanwezigheid van een certificaat (zichtbaar als hangslotje in de adresbalk) van websites die u bezoekt om vast te stellen dat u geen nagemaakte of onveilige website bezoekt.
- Vul wachtwoorden of persoonlijke informatie alleen in op websites waar u uit eigen beweging (bijvoorbeeld via uw bladwijzers) naartoe bent

gegaan. Wees zeer terughoudend op websites waar u via een link in een bericht op bent gekomen.

- Sluit pop-ups in uw browser af met Alt+F4. Klik nooit op 'akkoord', 'ok', de 'X' of 'nee' om een pop-up af te sluiten; u kunt hiermee per ongeluk malware installeren.
- Installeer een ad-blocker om pop-ups te blokkeren.
- Gebruik een beveiligde USB-stick voor het opslaan van vertrouwelijke informatie. Beveilig deze met een wachtwoord.

## Wifinetwerken

Steeds vaker wordt er openbare wifi aangeboden. Voor kwaadwillenden is dit een eenvoudige manier om (inlog)gegevens buit te maken.

Zodra u inlogt op een openbaar wifinetwerk, is het voor kwaadwillenden mogelijk toegang te krijgen tot uw apparaat en (inlog)gegevens. Het kan ook voorkomen dat kwaadwillenden hun eigen netwerk een bekende naam geven, zoals bijvoorbeeld die van de wifi in de trein. Zo wordt u het idee gegeven dat u inlogt op een bekend netwerk. Met de volgende twee tips kunt u de risico's beperken.

- Vermijd het gebruik van wifinetwerken die worden aangeboden in openbare ruimtes. Gebruik bij voorkeur een goedgekeurde VPN-verbinding of het 4G-netwerk.
- Zet 'automatisch verbinden' uit om te voorkomen dat uw mobiele apparaat buitenshuis onopgemerkt verbinding maakt een (zogenaamd) bekend of vertrouwd netwerk.

## Sociale media

- Scherm uw sociale netwerksites goed af en wees selectief in wie toegang krijgt tot uw profiel en gegevens.
- Wees voorzichtig met het vermelden van persoonlijke gegevens. Geef niet meer informatie dan noodzakelijk.
- Wees terughoudend in het bekend maken van privéplannen, reisbewegingen of gewoontes via sociale media.
- Ieder platform biedt beveiligingsinstellingen aan. Controleer deze regelmatig.
- Kies bewust wat u wel of niet deelt.

## Kinderen en internet

- Praat regelmatig met kinderen over de gevaren van internet, maar praat ze geen angst aan.
- Vermijd dat kinderen apps kunnen installeren of belangrijke instellingen veranderen op uw smartphone.
- Geef kinderen geen beheerrechten op uw laptop of pc. Dit verkleint de kans dat malware uw hele systeem infecteert.

## E-mail

- Wees terughoudend met het openen van berichten, e-mails, bijlages, (ingekorte) hyperlinks of onbekende bestanden die u niet verwacht, niet vertrouwt of waarvan de afzender onbekend is.
- Gebruik meerdere e-mailadressen. Geef uw primaire e-mailadres alleen aan betrouwbare personen.
- Verwijder eventuele dreigmail niet. Neem contact op met uw beveiligingsambtenaar of de lokale politie voor aangifte en volg hun instructies op.
- Verstuur zakelijke informatie enkel met uw zakelijke e-mailadres.

---

Bij alles geldt: wees altijd kritisch. Als iets te mooi is om waar te zijn, is het meestal ook niet waar.

## Postbezorging

De mogelijkheid bestaat dat iemand u post stuurt met een vervelende inhoud. Indien u dit poststuk niet vertrouwt, open het dan niet maar bel de lokale politie. Voorbeelden van een verdacht stuk zijn:

- U verwacht geen post van de persoon en/of instelling die het verstuurd heeft.
- De adressering is onjuist of onvolledig, of met veel dan wel opvallende spelfouten.
- Het retouradres ontbreekt, verschilt van de locatie van waar het stuk is verstuurd of betreft een ongewone of onbekende locatie.

- Het poststuk is (ruim) overgefrankeerd. Mogelijk wil de verzender niet het risico lopen dat het poststuk wegens onderfranking onderzocht of geretourneerd wordt.
- Het poststuk is voorzien van het opschrift “persoonlijk”, “vertrouwelijk”, of “alleen te openen door...” terwijl u geen post verwacht.
- Het poststuk heeft een vreemde geur, olie- of vetvlekken, rare vorm of verkleuring van de omslag. Dit kan worden veroorzaakt door de aanwezigheid van/aanraking met gevaarlijke stoffen.

---

### Handige links

[www.alertonline.nl](http://www.alertonline.nl)

[www.veiliginternetten.nl](http://www.veiliginternetten.nl)

[www.mijnonlineidentiteit.nl](http://www.mijnonlineidentiteit.nl)

[www.mijndigitalewereld.nl](http://www.mijndigitalewereld.nl)

[www.ncsc.nl](http://www.ncsc.nl)

[www.politie.nl/themas/controleer-of-mijn-inloggegevens-zijn-gestolen.html](http://www.politie.nl/themas/controleer-of-mijn-inloggegevens-zijn-gestolen.html)

Onderweg



**Als u onderweg bent - lopend, op de fiets, in de auto of met het openbaar vervoer - kunt u kwetsbaar zijn. Het is daarom van belang om uw reis van te voren goed te plannen. Ook kan het verstandig zijn om er voor te zorgen dat u niet alleen reist, maar in gezelschap. Met onderstaande tips kunt u mogelijke veiligheidsrisico's onderweg beperken.**

---

### **Algemene tips**

- Draag niet al uw waardevolle spullen op dezelfde plek. Bewaar bijvoorbeeld uw portemonnee in een binnenzak.
- Voorkom voorspelbaar gedrag en gewoontegebruiken; varieer in routes en tijdstippen van aankomst en vertrek.
- Overweeg een familielid, vriend of collega op de hoogte te stellen van uw reisbewegingen en vertrek- en aankomsttijden.
- Zorg dat u weet welke buurten u op bepaalde tijdstippen beter kunt mijden.
- Voorkom dat u 's nachts alleen op straat loopt: een groep is minder kwetsbaar.
- Loop tegen het verkeer in, zodat een auto u niet ongezien van achteren kan naderen. Indien u toch in dezelfde richting als het verkeer moet lopen en een voertuig plotseling naast u stopt, draai om en loop of ren weg in tegengestelde richting.
- Als u denkt dat u gevolgd wordt, verander dan meerdere malen onopvallend van richting en kijk of u nog steeds gevolgd wordt.
- Indien u er zeker van bent dat u gevolgd wordt, onthoud het kenteken en/of uiterlijke kenmerken en/of neem indien mogelijk foto's. Neem vervolgens contact op met de lokale politie.

## De beveiliging van uw auto

- Overweeg bij de aanschaf van een auto voorzieningen voor elektronische beveiliging zoals een startonderbreker, benzine-toevoeronderbreking, autoalarm-immobilizer en centrale deurvergrendeling.
- Houd uw autosleutels apart van andere sleutels: daarmee beperkt u verdere schade in geval van diefstal van uw auto.
- Leg geen kostbare voorwerpen in uw auto en laat uw dashboardkastje open staan. Kwaadwillenden zien zo dat er geen kostbaarheden in uw auto liggen.
- Laat nooit gevoelige informatie achter in uw auto.

## Tijdens het autorijden

- Houd tassen en mobiele telefoons uit het zicht.
- Sluit portieren, ramen en uw achterbak tijdens het rijden.

## In en uit de auto stappen

- Let op de omgeving bij het in- en uitstappen.
- Maak er een gewoonte van direct na het instappen de portieren te vergrendelen.
- Stap niet uit wanneer er mogelijk verdachte personen in de omgeving rondhangen. Zoek een andere plek om te parkeren en/of neem contact op met de lokale politie.

## Gebruik van openbaar vervoer

- Plan uw reis van te voren.
- Vermijd verlaten, ondergrondse en slecht verlichte metro- en busstations, vooral 's nachts.
- Vermijd verlaten coupés.
- Houd persoonlijke bezittingen, zoals een ov-chipkaart bij de hand; voorkom dat u uw tas of portemonnee moet doorzoeken.

## Gebruik van taxi's

- Maak alleen gebruik van erkende taxibedrijven en bestel uw taxi mogelijk vooraf.
- Programmeer telefoonnummers van de erkende taxibedrijven in uw mobiele telefoon.



Werkplek

**Ook op uw werkplek kunt u bloot komen te staan aan veiligheidsrisico's. Zorg ervoor dat u op de hoogte bent van de verschillende beveiligingsprocedures op uw werkplek, zoals toegangsprocedures, ontruimingsregels en de regels voor informatiebeveiliging. Hoewel sommige informatie voor u onschuldig lijkt, kan het voor kwaadwillenden toch interessant zijn.**

**Weet ook bij wie u incidenten kunt melden; bij de meeste werkgevers kunt u terecht bij een security manager of beveiligingsambtenaar. Bovendien is het belangrijk dat u zich realiseert dat informatiebeveiliging niet ophoudt bij de deur van het kantoor.**

- Meld incidenten, zoals vermissing, een datalek en diefstal, zo spoedig mogelijk bij uw beveiligingsambtenaar en werkgever.
- Indien u niet op uw kamer bent, sluit deze (indien mogelijk) af.
- Indien u niet achter uw computer zit, maak dan gebruik van de schermbeveiliging van uw computer.
- Zorg ervoor dat niet op uw beeldscherm kan worden meegelezen.
- Ga voorzichtig om met vertrouwelijke informatie en hanteer bij verspreiding altijd het principe van 'need to know' in plaats van 'nice to know'.
- Vermijd het telefonisch bespreken van vertrouwelijke informatie waar mogelijk.
- Wees u ervan bewust dat er meer vertrouwelijke informatie is dan enkel de 'papieren' documenten waarop dat staat vermeld; bespreek bijvoorbeeld ook geen vertrouwelijke informatie op openbare plaatsen.
- Hanteer na werktijd het 'clear desk'-principe: laat geen documenten slingeren op uw bureau. Bewaar documenten bij voorkeur in een afgesloten kast, locker of kluis of versnipper de documenten na gebruik.

- Indien u werkt met staatsgeheime informatie; neem dit nooit mee naar huis.
- Neem geen mobiele apparaten (smartphone, iPad en/of laptop) mee naar een ruimte waar vertrouwelijke gesprekken worden gevoerd.
- Communiceer zoveel mogelijk via beveiligde kanalen.

---

### Handige links

[www.aivd.nl/onderwerpen/spionage/spionage-u-als-doelwit](http://www.aivd.nl/onderwerpen/spionage/spionage-u-als-doelwit)



Buitenlandse  
(dienst)reis



**Als bezoeker in een ander land, kunt u te maken krijgen met verschillende veiligheidsrisico's. Een goede voorbereiding van uw reis beperkt de risico's aanzienlijk. Zorg dat u op de hoogte bent van de actuele situatie in het land dat u gaat bezoeken. Mocht zich een verdachte situatie hebben voorgedaan, maak er altijd een melding van bij uw security manager of beveiligingsambtenaar.**

### **Belangrijke documenten en telefoonnummers**

- Bewaar kopieën van uw paspoort en visum digitaal op een beveiligd netwerk.
- Neem geen of zo min mogelijk vertrouwelijke documenten mee. Neemt u deze toch mee, stel dan een lijst op met de documenten en gegevensdragers en maak foto's van de apparatuur die u meeneemt. Bij diefstal of verlies is direct duidelijk wat er mist. Bewaar de lijst op kantoor, neem deze niet mee.
- Noteer uw creditcardnummers en het telefoonnummer dat u nodig hebt als u ze wilt blokkeren.
- Programmeer belangrijke telefoonnummers in uw mobiele telefoon (telefoonnummer van de Nederlandse diplomatieke post, thuisnummers, alarmnummer van uw reis- en zorgverzekering en lokale noodnummers).
- Programmeer een ICE-nummer in uw telefoon. ICE is de internationale afkorting voor In Case of Emergency. De persoon onder het nummer dat u in uw mobiele telefoon opslaat onder de naam ICE, wordt gebeld in noodgevallen.

### **Reisvoorbereiding**

- Lees het reisadvies van het ministerie van Buitenlandse Zaken.
- Meld een dienstreis altijd aan bij de ambassade en vermeld daarbij ook de bestemming van de reis. De ambassade kan eventueel nog (veiligheids)tips geven.
- Maak voor reserveringen gebruik van diensten van bekende en betrouwbare reisorganisaties en veilige luchtvaartmaatschappijen.

- Kies voor een hotel dat buiten eventuele risicogebieden ligt.
- Schrijf op de bagagelabels alleen uw businessadres of het verblijfadres tijdens de reis en uw mobiele telefoonnummer.
- Zorg voor voldoende geld in verschillende vormen en verberg dit op meerdere plekken.
- Stop vertrouwelijke documenten in uw handbagage. Neem kennis van de regels voor het vervoeren van staatsgeheime informatie. Zorg dat u kunt controleren of iemand de vertrouwelijke gegevens heeft ingezien door middel van sealbags.

### Tijdens de reis

- Houd uw bagage altijd scherp in de gaten en laat deze nooit onbeheerd achter.
- Neem geen pakjes of spullen van anderen aan.
- Loop een andere kant op als er onderweg ergens ongeregelheden zijn.
- Draag informele kleding zonder blijk van persoonlijke status, logo of andere herkenningstekens.
- Neem geen zaken mee die aanstootgevend kunnen zijn voor bewoners van het land dat u bezoekt, bijvoorbeeld alcohol of voor hen contro-versiële tijdschriften of boeken.
- In een land waar de situatie instabiel is; mijd overheidsgebouwen, ambassades of radio en tv-stations.

### Hotel

- Gebruik altijd de hoofdingang van het hotel.
- Zorg dat bij het inchecken zo min mogelijk mensen uw naam en kamernummer horen.
- Laat uw kamersleutel nergens slingeren, haal desnoods het label met het kamernummer ervan af.
- Ga bewust om met het gebruik van een hotelkluis, deze kan kwetsbaar zijn.
- Check uw kamer op de veiligheid van ramen en deuren, op goede verlichting en op vluchtroutes naar buiten.
- Ontvang eventuele (onbekende) bezoekers in de hotelloobby, niet op uw hotelkamer.
- Sluit bij vertrek altijd uw kamerdeur, ramen en balkondeur goed af.

## Digitaal

- Wis de belgeschiedenis van uw telefoon en verwijder ontvangen en verzonden berichten, zoals SMS en WhatsApp.
- Zet alleen noodzakelijke contacten in uw contactenlijst.
- Overweeg een wegwerp mobiele telefoon, simkaart en tijdelijk e-mail-adres te gebruiken. Indien u regelmatig naar het buitenland reist, is het raadzaam apparatuur mee te nemen die u alleen voor dit doel gebruikt.
- Gebruik nooit apparatuur van derden. Sluit uw systeem ook nooit aan op apparatuur van anderen (bijvoorbeeld printers). Neem eigen opladers en kabels mee. Gebruik een usb-condoom als er geen gewone wandcontactdoos beschikbaar is en u moet opladen via een usb-contactdoos.
- Download of installeer geen programma's/applicaties tijdens de reis.
- Schakel de automatische updates uit voor de app- of playstore.
- Pas wachtwoorden voor (en na) uw reis aan.
- Zet uw wifi tijdens uw reis uit. Gebruik bij voorkeur een goedgekeurde VPN-verbinding of het 4G-netwerk.

---

## Handige links

[www.nederlandwereldwijd.nl](http://www.nederlandwereldwijd.nl)

<https://www.aivd.nl/onderwerpen/spionage/spionage-u-als-doelwit>

Download de 24/7 BZ reis app









### **Uitgave**

Nationaal Coördinator  
Terrorismebestrijding  
en Veiligheid (NCTV)  
Postbus 20301, 2500 EH Den Haag  
Turfmarkt 147, 2511 DP Den Haag  
070 751 5050

### **Meer informatie**

[www.nctv.nl](http://www.nctv.nl)  
[info@nctv.minvenj.nl](mailto:info@nctv.minvenj.nl)  
[@nctv\\_nl](https://twitter.com/nctv_nl)

januari 2019 | 117467