

The background of the entire page is a photograph of an office interior. In the foreground, there are horizontal window blinds that are partially open, allowing warm, golden light to filter through in horizontal bands. Behind the blinds, a person is visible sitting at a desk, looking at a computer monitor. The person's face is partially obscured by the blinds. On the desk, there are some papers and a computer mouse. The overall atmosphere is quiet and professional.

CCV centrum voor
criminaliteitspreventie en
veiligheid

Advies zelfscan persoonlijke veiligheid

Inleiding

Burgemeesters, wethouders raadsleden en andere politieke ambtsdragers vervullen een belangrijke rol in de Nederlandse samenleving. Zij zijn bepalend voor democratische en integere besluitvormingsprocessen. Vanuit die rol moeten zij open in de samenleving kunnen staan, het politieke debat vrij kunnen voeren en publieke taken vrij van dwang en drang kunnen uitoefenen.

Helaas blijkt uit de 'Monitor Integriteit en Veiligheid Openbaar Bestuur 2016' dat ruim een kwart van de politieke ambtsdragers en 1 op de 5 ambtenaren slachtoffer is van agressie en geweld. Als politieke ambtsdragers zich bij het nemen van besluiten hierdoor laten beïnvloeden, is dat een belangrijk risico voor de integriteit, kwaliteit en continuïteit van het openbaar bestuur en kan het democratisch proces in gevaar komen.

De overheid neemt daarom allerlei maatregelen om de veiligheid van politieke ambtsdragers te vergroten. Politieke ambtsdragers kunnen echter zelf ook maatregelen nemen om de kans om slachtoffer te worden van agressie en geweld te verkleinen. U heeft de zelfscan persoonlijke veiligheid ingevuld om erachter te komen welke maatregelen dit zijn.

In dit document vindt u uw persoonlijke veiligheidsmaatregelen. De tips en adviezen zijn samengesteld op basis van de door u gegeven antwoorden in de zelfscan persoonlijke veiligheid. De tips en adviezen staan per onderwerp gerangschikt en maken u bewust van wat u zelf kunt doen om bepaalde risico's te voorkomen. Ze zijn relatief makkelijk toe te passen en kunnen een veilig gevoel bewerkstelligen.

Het belangrijkste advies:

Vertrouw op uw eigen intuïtie, u kent uw eigen omgeving immers het beste. Als u bijvoorbeeld een onbekende auto of onbekend persoon een aantal keer op verschillende tijden en op verschillende plaatsen heeft gezien, is dit mogelijk verdacht. Ook iemand in winterkleden midden in de zomer is mogelijk verdacht. Neem het zekere voor het onzekere, wees niet bang loos alarm te slaan en meld bijzonderheden die u vreemd vindt bij de politie. Het gaat tenslotte om uw veiligheid!

Bel bij spoed: 112

Geen spoed? Bel: 0900 8844



Veiligheid in en om de woning

Jouw woning, de plek waar jij je terugtrekt uit alle hectiek en je veilig voelt. Maar ben je ook veilig? Je hebt in de zelfscan binnen de categorie 'Veiligheid in en om de woning' antwoord gegeven op een aantal vragen. Op basis van jouw antwoorden vind je hier een persoonlijk advies met een aantal maatregelen die je kunt nemen om de veiligheid in en om je woning te verbeteren.

Alle tips en adviezen over 'Veiligheid in en om de woning' vind je op de [CCV-website](#).

Algemeen

Ken je het **Politiekeurmerk Veilig Wonen** al? Dit is een keurmerk voor woningen die voldoen aan een aantal eisen op het gebied van inbraakpreventie en sociale veiligheid. De eisen die het keurmerk stelt, zorgen ervoor dat een inbreker langer de tijd nodig heeft om een woning binnen te komen.

Het inbreken in een slecht beveiligde woning duurt vaak maar **30 seconden**. Een inbreker bedenkt zich dus wel 2 keer voor hij een woning probeert te betreden die is voorzien van het Politiekeurmerk Veilig Wonen. Onderzoek wijst uit dat de PKVW-maatregelen significant bijdragen aan jouw veiligheid en veiligheidsgevoel. De extra maatregelen, als goed hang-en-sluitwerk, goede verlichting, rolluiken en overzicht in straat en wijk, zorgen ervoor dat inbrekers de woning graag overslaan.

Zorg dat jouw woning ook het Politiekeurmerk Veilig Wonen krijgt. Schakel hiervoor 1 van de [erkende PKVW-bedrijven](#) in. Het bedrijf inspecteert samen met jou je woning. Na het uitvoeren van eventuele verbeterpunten keurt het PKVW-bedrijf jouw woning en ontvang je het certificaat.

Beheer en gebruik van sleutels

U vindt hieronder een paar simpele regels voor het beheer en gebruik van uw sleutels:

- Beperk het aantal (reserve)sleutels. □
- Noteer wie een sleutel van uw woning heeft. □
- Vervang de cilinder van uw slot bij diefstal/verlies van uw sleutels. □
- Gebruik sleutels met certificaat, zodat deze alleen met dit certificaat na te maken zijn. □
- Voorzie sleutels nooit van naam en adres. □
- Fotografeer sleutels niet en plaats deze nooit op sociale media. Van een afbeelding van een sleutel is relatief makkelijk een kopie te maken. □
- Laat sleutels nooit in het slot van de deur zitten. □
- Hang sleutels binnenshuis op een vaste, bereikbare plaats, die niet zichtbaar is van buitenaf. □
- Wellicht overbodig: een mat of bloempot is geen geheime plek om sleutels onder te bewaren. Bij steekproeven



Veiligheid in en om de woning

door de politie in woonwijken of door buurtpreventie-teams worden regelmatig zogenaamd 'verborgen sleutels' gevonden.

Extra tip

Een slot dat voldoet aan het [Politiekeurmerk](#), getest is en volgens de regels is gemonteerd, verkleint sterk de kans op inbraak. Zo'n slot herkent u aan het SKG®-logo, met sterren.

Inbraakwerende ramen en deuren

Je kunt de kans op een inbraak of insluiping verkleinen met een paar simpele regels en gewoonten:

- Controleer de vergrendeling van ramen en deuren voor je vertrek of voor het slapengaan. □
- Ruim ladders en klike's altijd op of leg ze vast, zodat ze niet te gebruiken zijn om via een raam of deur op de bovenverdieping naar binnen te gaan. □
- Bekijk mogelijke vluchtwegen, houd hierbij rekening met afgesloten deuren. □
- Controleer of je voor- en achterdeur zijn voorzien van kierstandhouders (een klem die de deur slechts op een klein kiertje kan zetten, zonder dat je de deur voor onbekenden helemaal open hoeft te doen) of een (digitale) deurspion (een camera die vastlegt wie er voor de deur staat) en gebruik deze ook. □
- Laat deugdelijk hang- en sluitwerk bevestigen, bij voorkeur door een [PKVW-erkend bedrijf](#).

Extra tips

- Mocht je overgaan tot de aanschaf van een nieuw raam of nieuwe ramen, overweeg dan uw raam/ramen te vervangen door dubbelglas met een specifieke inbraakwerende waarde* in plaats van standaard (dubbel)glas. □*P1A= letselbeperkend, P2A= doorgooibeperkend, P4A= goed inbraakwerend. □
- Denk goed na voordat je een naambordje bij je voordeur plaatst. Vermeld alleen de familienaam en geen namen van gezinsleden. Want, als bijvoorbeeld 1 van je kinderen de deur opendoet en je bent niet thuis, kan een kwaadwillend persoon vertrouwen wekken door je voornamen te gebruiken. Voor je kinderen lijkt hij/zij daardoor een vertrouwenwekkend persoon die binnengelaten kan worden.

Verlichting ter beveiliging van uw huis

Hieronder vind je een aantal tips voor het gebruik van licht:

- Sluit 's avonds de gordijnen, zo ben je niet zichtbaar vanaf buiten.
- Laat bij afwezigheid licht branden in verschillende vertrekken in huis. Want, een donker huis is voor een



Veiligheid in en om de woning

inbreker doorslaggevend om een kans te wagen. Verlichting met een tijdschakelaar maakt daarbij een enorm verschil. Gebruik geen klein lampje om te doen alsof je thuis bent. Daar prikken inbrekers wel doorheen. Maar laat bijvoorbeeld ook een lamp aan op de bovenverdieping. Kortom: zorg ervoor dat het huis een bewoonde indruk maakt.

- Gebruik buitenverlichting, bijvoorbeeld op schemerschakelaar of bewegingssensor. Zo kan je een betere afweging maken om wel of niet de deur te openen. Zorg ook voor goede buitenverlichting bij alle deuren die vanaf de openbare weg zichtbaar en bereikbaar zijn. De buitenlamp bij de voordeur dient het gezicht van de bezoekers te verlichten.
- Zorg ervoor dat de verlichting wit licht is. Dit draagt ertoe bij dat mensen beter herkend kunnen worden. Goede verlichting is ook nodig bij eventuele inzet van cameratoezicht.
- Tuinverlichting is bij voorkeur (geheel of gedeeltelijk) gericht op de straatkant of zijkanten van het huis, zodat goed zichtbaar is als iemand om je huis of door de tuin loopt.

Extra tip

Aarzel niet om de gemeente erop te attenderen dat een boom het licht van een lantarenpaal wegneemt. Anders blijft het zicht op de buitendeur beperkt.

Elektronisch alarmsysteem

Een alarmsysteem houdt insluipers niet buiten de deur. Goede sloten wel. **Een alarmsysteem is daarom een aanvulling** op een maatregel als goede sloten.

In combinatie met een garantie van opvolging van het beveiligingsbedrijf bij een urgente situatie -early warning - betekent een alarmsysteem niet dat jij zelf niet meer alert hoeft te zijn op verdachte situaties. Wel kan de 'vervangende alertheid' je een gevoel van veiligheid geven. Je hebt immers de garantie van ondersteuning door surveillanten bij een reële dreiging. Daarnaast helpt het systeem je in het toezicht op verdachte situaties.

Wil je een alarm aanschaffen? Dan volgen hieronder een aantal tips:

- Zorg voor duidelijke afspraken met de alarmcentrale/bewaking over alarmopvolging (wanneer is er sprake van inschakeling van de politie? Wat is de wijze van beoordeling door de centralist over de mate van urgentie?).
- Schakel je (mobiele) alarmsysteem altijd in bij het verlaten van de woning.
- Zorg ervoor dat u en uw familieleden - en eventuele andere sleutelhouders, zoals burens - weten hoe te handelen bij alarmsituaties.

Garage



Veiligheid in en om de woning

Enkele tips:

- Parkeer je auto in de garage. Dit vermindert de kans op diefstal of vandalisme.
- Installeer een automatische opener voor de garagedeur. Zo kan je op afstand de deur openen en hoef je niet uit te stappen.
- Stap in de garage in en uit je auto.
- Zorg dat de deur zo kort mogelijk geopend is of plaats een sensor om deze automatisch te sluiten.

Extra tip

Kijk voor meer informatie over een veilige toegang tot de garage, zoals het verwijderen van obstakels en de juiste verlichting, op de CCV-website bij '[Aanpak autokraak](#)'.

Onbeheerd huis tijdens vakanties

Enkele tips die je kunt gebruiken wanneer je op vakantie gaat:

- Doe alle deuren, ramen, garage(s) en schuren op slot. □
- Berg waardevolle documenten en bezittingen op in een verankerde kluis. □
- Verwijder waardevolle apparatuur of andere waardevolle zaken uit het zicht. □
- Doe niet alle gordijnen dicht. □
- Gebruik tijdklokken voor lampen, radio en tv. □
- Vraag burens, familie, vrienden of een collega's op je huis te letten. Geef hen je contactgegevens. □
- Zorg dat iemand je brievenbus dagelijks leegt of laat je post op een ander adres bezorgen.

Extra tip

Meer informatie over maatregelen die je kunt nemen voorafgaand aan een vakantie kun je lezen op [Politiekeurmerk.nl](#).

(Betaalde) dienstverleners over de vloer

Hieronder volgen tips die betrekking hebben op dienstverleners die bij jou over de vloer komen:

- Selecteer dienstverlenend personeel voor in en om het huis, zoals schoonmakers, kinderoppas, tuinman of aannemer, zorgvuldig. Maak gebruik van erkende bedrijven als je personeel inhuurt.
- Controleer het identiteitsbewijs van de ingehuurd arbeidskracht en bewaar een kopie.



Veiligheid in en om de woning

- Controleer bij het inhuren van een arbeidskracht de referenties. Ga na of die betrouwbaar zijn. Vraag, indien je dat wenst, naar een 'Verklaring Omtrent het Gedrag'. Raadpleeg voor meer informatie over de Verklaring Omtrent het Gedrag de website www.justis.nl.
- Vraag hem/haar niet met anderen te praten over de woning, het gezin en de gewoonten.
- Instrueer de door jou ingehuurde arbeidskracht geen onaangekondigde gasten en onderhoudspersoneel binnen te laten.
- Zorg dat de door jou ingehuurde arbeidskracht jouw personeel of jou altijd kan bereiken: geef hen je mobiele telefoonnummer.
- Instrueer de ingehuurde arbeidskracht de afgesproken veiligheidsmaatregelen altijd in acht te nemen.
- Leg de door jou ingehuurde kracht uit hoe te reageren in noodsituaties (bijvoorbeeld bij een 'early warning' van een aanwezig alarmsysteem).

Gevaarlijke of 'vervelende' post

Het is mogelijk dat iemand jou een brief of poststuk stuurt met een vervelende inhoud. Dit kan een dreigbrief zijn, een poederbrief of zelfs - in zeldzame gevallen - een explosief.

Bekijk je post daarom kritisch. Heb je post ontvangen met een bedreiging of andere vervelende inhoud? Stop het poststuk dan in een plastic zak om te voorkomen dat sporen verloren gaan en raadpleeg de politie. De politie kan het verder onderzoeken. Vertrouw je een poststuk niet? Open het dan niet, maar bel de politie.

Wees oplettend in de volgende situaties:

- De herkomst van het poststuk is jou onbekend. Je verwacht geen post van de persoon en/of instelling die het verstuurd heeft.
- De adressering is onjuist of onvolledig, of bevat veel/opvallende spelfouten.
- De titulatuur is onjuist; de verzender kent vaak wel de naam, maar titels en dergelijke zijn vaak minder bekend.
- Het poststuk is (ruim) overgefrankeerd. Mogelijk wil de verzender niet het risico lopen dat het poststuk wegens onderfranking wordt onderzocht of geretourneerd. Het poststuk is voorzien van het opschrift 'persoonlijk' terwijl je geen post verwacht.
- Het poststuk heeft olie- of vetvlekken of de omslag is verkleurd. Dit kan wijzen op de aanwezigheid van/aanraking met gevaarlijke stoffen.
- De envelop van het poststuk is erg stug. Dit kan te maken hebben met gevaarlijke stoffen; er is vaak een harde ondergrond nodig om verschillende componenten op te kunnen bevestigen.



Veiligheid in en om de woning

- Het poststuk is op een ongebruikelijke wijze verpakt en het is niet duidelijk wat het poststuk bevat.

Extra tip

Open het poststuk niet als het poststuk voldoet aan meerdere van bovengenoemde kenmerken. Raadpleeg in plaats daarvan de politie. De politie heeft de expertise om te bepalen of er echt sprake is van verdachte post. Doe aangifte bij de politie als er sprake is van een bedreiging.

Brandstichting

De zorg voor goede brandveiligheid begint bij de aanschaf van adequate (gecertificeerde) **brandblusmiddelen**. Ook **rook- en koolmonoxidemelders** in de gehele woning en het hebben van een **vluchtplan** bij een brand zijn belangrijk. Verdergaande preventie - eerder bestemd voor gebouwen - is het aanbrengen van **brandvertragende deuren** (om rook en brand buiten de deur houden) of een **sprinklerinstallatie**.

Wanneer je een expert inschakelt om je woning te beveiligen volgens het [Politiekeurmerk Veilig Wonen](#), wordt ook de brandveiligheid van je huis nagelopen. Met een Politiekeurmerkexpert of met PKVW gecertificeerde producten weet je dat je kwaliteitsproducten aanschaft en overbodige maatregelen vermijdt.



Veiligheid en gezin

Jouw positie als politiek ambtsdrager kan ook invloed hebben op je gezinsleden. Zij kunnen onbewust gevaar lopen. Je hebt in de zelfscan binnen de categorie 'Veiligheid en gezin' antwoord gegeven op een aantal vragen. Op basis van jouw antwoorden vind je hier een persoonlijk advies met een aantal tips die jij kunt nemen om de veiligheid te vergroten en risico's te verkleinen.

Alle tips en adviezen over 'Veiligheid en gezin' vind je op de [CCV-website](#).

Uw gezinsleden

Wij begrijpen dat het voor jou wellicht een keuze is om je gezin niet bewust te maken van risico's die jij en je gezin eventueel lopen. Wij willen je er echter op wijzen dat bewustmaken van risico's de **alertheid verhoogt** en **preventief handelen** mogelijk maakt. Daarom enkele tips:

- Informeer je gezinsleden goed over de maatregelen die je neemt (zoals het aanbrengen van een inbraakalarm en de werking ervan).
- Zorg dat je gezinsleden traceerbaar en bereikbaar zijn. In noodsituaties is het handig dat er al afspraken over bereikbaarheid zijn gemaakt, zodat je elkaar snel kunt vinden als dat nodig is. Hiervoor kunt u gebruik maken van de afspraak dat de telefoon (en belsignaal) altijd aanstaat tot en met het gebruik van slimme apps die de locatie van je gezin (en jouzelf) aangeven.
- Hoe herkent mijn gezin een verdachte situatie? Net zoals jijzelf: vertrouw op je intuïtie. Elk gezinslid moet zich bewust zijn van wat er om zich heen afspeelt. Hij of zij kent zijn of haar omgeving het best en herkent al snel een afwijkende situatie. Als een onbekende auto of onbekend persoon een aantal keer op verschillende tijden en op verschillende plaatsen is gezien, dan is dit mogelijk verdacht. Ook iemand die midden in de zomer in winterkleden loopt, is mogelijk verdacht. Neem het zekere voor het onzekere, wees niet bang loos alarm te slaan en meld bijzonderheden die 'vreemd' gevonden worden. Ga na of er risico's zijn bij buitenspelen (straat, openbare speeltuin).
- Als u kleine kinderen heeft: leg de maatregelen spelenderwijs uit, zodat zij eventueel zelfstandig weten te reageren op verdachte situaties. Vertel jonge kinderen de deur niet open te doen, geen onaangekondigde gasten binnen te laten, de post niet te openen en de telefoon niet op te nemen. Herhaal dit regelmatig, zodat ze het niet vergeten.
- Maak indien nodig afspraken met degene die je kinderen van en naar school begeleidt.
- Informeer leerkrachten over wie de kinderen ophaalt, vooral als iemand anders dan jijzelf dit doet.



Veiligheid en gezin

- Leer kinderen geen lift aan te nemen van vreemden, ook niet als die zich voordoen als bekenden van jou of als familie.
- Denk goed na voordat je een naambordje bij je voordeur plaatst. Vermeld alleen de familienaam en geen namen van gezinsleden. Want, als bijvoorbeeld 1 van je kinderen de deur opendoet en jij bent niet thuis, kan een kwaadwillend persoon vertrouwen wekken door uw voornaam te gebruiken. Voor je kinderen lijkt hij/zij een vertrouwenwekkend persoon die binnengelaten kan worden.

Extra tips

- Leer je kinderen hoe ze moeten reageren in noodsituaties, zoals het bellen naar het alarmnummer of naar de burens gaan.
- Luister naar wat je kinderen vertellen. Ze hebben een scherp observatievermogen en signaleren snel ongebruikelijke situaties.

Gebruik van internet door uw gezin

Het komt in Nederland helaas steeds vaker voor dat publieke personen en familieleden op een negatieve manier worden benaderd, ook op het internet. In enkele gevallen worden daadwerkelijk bedreigingen geuit die aanleiding kunnen zijn om beveiligingsmaatregelen te treffen. Hoe bewuster jij en je gezin omgaan met jouw gegevens op internet, hoe kleiner de kans dat jij vanwege internetbedreigingen persoonlijk beveiligd moet worden.

- Bespreek internet- en e-mailgebruik met je kinderen. Wijs hen op de risico's van chatten en het gebruik van een webcam. Zorg dat je betrokken blijft bij hun internetgebruik (zowel binnenshuis als buiten de deur) en weet welke gegevens je gezinsleden op internet plaatsen. Vooral Facebook(messenger), Instagram, SnapChat, Chaton, Twitter, YouTube, WhatsApp, Google Hangouts, Houseparty, Facetime, Pinterest, Skype en Google+ zijn applicaties die onder jongeren populair zijn.
- Beperk het downloaden en uploaden via zogenaamde peer-to-peer-netwerken (zoals BitTorrent, Kodi, en uTorrent). Hierdoor kan allerlei data die aan je eigen thuisnetwerk zijn verbonden ongemerkt op straat komen te liggen.
- Laat ieder gezinslid sterke en verschillende wachtwoorden aanmaken, beperk het aantal accounts op internet, sla gevoelige data alleen lokaal op en niet in de cloud en beveilig je netwerk met een virusscanner en firewall.

Extra tip

Kijk ook eens op de website veiliginternetten.nl.



Veiligheid en digitale communicatie

Computers, laptops, iPads en smartphones zijn niet meer weg te denken uit onze huidige digitale samenleving. Maar hoe ga je ermee om? Wat kun je zelf doen om veilig digitaal te communiceren?

Je hebt in de zelfscan binnen de categorie 'Veiligheid en digitale communicatie' antwoord gegeven op een aantal vragen. Op basis van jouw antwoorden vind je hier een persoonlijk advies met concrete tips om veilig digitaal te communiceren en risico's te verkleinen.

Zie je hieronder geen tips staan, dan doe je er al alles aan om veilig te communiceren en eventuele risico's te verkleinen. Wil je toch deze tips en adviezen lezen? Dan vind je ze op de [CCV-website](#).

Jouw computer/digitale gegevens

Om je desktop, laptop en/of tablet te beveiligen tegen hacken, virussen en dergelijke, kun je de volgende maatregelen treffen:

- Gebruik wachtwoorden voor inloggen.
- Pas ook het door de provider geleverde wifi-wachtwoord aan.
- Zorg voor een goed werkende virusscanner.
- Gebruik een firewall.
- Zorg voor anti-spyware software.
- Probeer werk- en privégebruik van het internet zoveel mogelijk gescheiden te houden.
- Gebruik geen ongeautoriseerde software.
- Gebruik een beveiligde USB-stick of flash-card voor het opslaan van vertrouwelijke informatie. Beveilig deze met een wachtwoord of vingerafdruk.
- Open geen bijlagen van onbekende afzenders.
- Gebruik meerdere e-mailadressen, eventueel onder een andere dan je eigen naam. Deze kan je gebruiken voor aanmeldingen op websites waar een e-mailadres nodig is.
- Geef je belangrijkste e-mailadres alleen aan betrouwbare personen.

Extra tip

Mocht je dreigmail ontvangen, verwijder deze dan niet. Neem contact op met je beveiligingsambtenaar of de politie voor aangifte en volg hun instructies op.



Jouw internetgebruik

Mocht je op het internet gegevens over jou of je naasten tegenkomen die mogelijk een risico vormen, dan kan je zelf al een aantal stappen zetten om deze informatie te verwijderen:

- Stap 1: Zoek uit welke data vindbaar en zichtbaar zijn □
- Stap 2: Verwijder gegevens □
- Stap 3: Maak gegevens onzichtbaar en onvindbaar

Stap 1: Zoek uit welke data vindbaar en zichtbaar zijn

Als je wil weten of er gegevens over jou op het internet staan die je er liever niet op wilt hebben, trek dan eens een uurtje uit om je eigen naam in een aantal zoekmachines in te typen. Wellicht kom ook jij tot de ontdekking dat op het eerste gezicht onschuldige gegevens in combinatie met gegevens op andere websites méér over jou vertellen dan je lief is. Om een volledig beeld te krijgen, doe je er goed aan ook te controleren welke gegevens uw gezinsleden op internet hebben geplaatst. Vooral Facebook, Google+, Tumblr, Twitter en LinkedIn zijn populair. Maar ook kleinere netwerksites, waarvan je allang weer was vergeten dat je er ooit vrijwillig je gegevens op had gezet, leveren soms verrassende resultaten op. Denk bijvoorbeeld aan schoolbank.nl.

Stap 2: Verwijder gegevens

Gegevens die eenmaal op internet staan, zijn er lastig af te halen. Mocht je gegevens over jou of je naasten tegenkomen die mogelijk een risico vormen, dan kan je zelf al een aantal stappen ondernemen om deze informatie te verwijderen: □

- Verwijder zelf je gegevens of verander je privacy-instellingen via een door jouzelf gecreëerd account op een website. □
- Grote interactieve websites hebben vaak moderators in dienst. Moderators zijn verantwoordelijk voor het 'schoonhouden' van de website en het afhandelen van klachten over content op de website. De manier waarop je de moderator kunt bereiken, verschilt per website. Vaak kan je via een klachtenknop (de 'niet ok-knop') je klacht aan de moderator zenden. □
- Mocht er geen moderator zijn die actie onderneemt, dan kan je contact opnemen met de beheerder van de website. Dit is degene die de website heeft gemaakt. Hij of zij schrijft de teksten en houdt de website bij. De websitebeheerder kan teksten aanpassen of eventueel pagina's verwijderen. Als jij zelf of een websitebeheerder op uw verzoek gegevens verwijderd hebt, kan het zijn dat die gegevens nog in de archieven ('cache') van de zoekfunctie voorkomen. Laat daarom ook altijd ongewenste gegevens verwijderen bij zoekmachines van websites. □
- Mocht de beheerder niet te vinden zijn, dan kunt u contact opnemen met de hostingprovider van de



Veiligheid en digitale communicatie

desbetreffende website. De hostingprovider is de organisatie die ervoor zorgt dat de website op het internet is geplaatst. Deze verhuurt 'ruimte' op internet aan de websitebeheerder en zorgt ervoor dat de website te allen tijde vindbaar is. De hostingprovider kan enkele pagina's of een hele website blokkeren. De beheerder en de provider vind je als volgt: Ga naar <http://centralops.net/co/>. Klik op 'Domain Dossier' en vink 'domain whoisrecord' aan. Vul het internetadres in en klik op 'Go'. Noteer de adresgegevens van de websitebeheerder en hostingprovider ('administrative address' en 'technical address').

- Verwijder ook de gegevens uit de archieven van zoekmachines (zoals Google en Bing) en het [Internet Archive](#). Google heeft online aangegeven welke zaken zij als belastend/schadelijk beoordelen en op welke verzoeken wordt ingegaan. Via een formulier op de [website van Google](#) kan je een verzoek tot verwijdering van gegevens indienen. Het verzoek wordt vervolgens beoordeeld door Google. Wil je dit niet zelf regelen? De [Autoriteit Persoonsgegevens](#) biedt aan te bemiddelen met Google om 'ongewenste zoekresultaten' te verwijderen.

Stap 3: Maak gegevens onzichtbaar en onvindbaar

Het internet blijft een aansprekend medium om te communiceren en om te werken aan je carrière en je netwerk. Je hebt mogelijkheden te over om je breed te profileren in schrift, beeld en geluid. Wat anderen over jou op internet zetten, kan je maar ten dele beïnvloeden. Het scheelt al heel veel als je zorgvuldig omgaat met de gegevens die jij zelf publiek toegankelijk maakt.

Enkele tips voor je onzichtbaarheid en onvindbaarheid

- Plaats alleen informatie op websites, waarbij je rechtstreeks of via korte lijnen invloed hebt op de gegevens die over je worden gepubliceerd, zoals je eigen website, de website van je politieke partij en websites van de overheid.
- Sociale netwerksites zijn in beginsel zichtbaar voor iedereen. Zet geen kwetsbare informatie op je sociale netwerksites en scherm je profiel af voor onbekenden.
- Krijg je een verzoek om je aan te sluiten bij het sociale netwerk van een ander? Bedenk dan of je jouw volledige profiel zichtbaar wilt maken binnen dat netwerk.
- Kijk welke persoonsgegevens je kinderen of anderen in je directe omgeving op internet zetten. Deze gegevens kunnen indirect naar jou leiden. Maak mensen in jouw directe omgeving bewust van de risico's van persoonlijke informatie op het internet.
- Een medium als Twitter kent een grote gebruikersgroep. Wees alert met het geven van informatie op Twitter. Als je bijvoorbeeld aangeeft wat je op dat moment doet of die dag gaat doen, dan is voor kwaadwillende personen makkelijk te achterhalen waar jij je bevindt.
- Beoordeel eerst of het strikt noodzakelijk is veel persoonlijke informatie te geven voor je iets aanschaft via internet.
- Neem geen deel aan onderzoeken, polls, enquêtes en quizen via internet. Zij dwingen je er vaak toe om persoonlijke informatie te geven. Bovendien is het in dit soort gevallen vaak moeilijk om in de periode daarna van alle mogelijke vormen van spam in je e-mailbox af te komen.



Veiligheid en digitale communicatie

- Maak, voordat je iets post op een website, voor jezelf een belangenafweging. Als je berichten achterlaat op een forum, verleen je toestemming om jouw mening te publiceren. Je kunt deze toestemming op een later moment wel intrekken. Het verwijderen van je 'post' kan echter tijd kosten. Onbedoeld kunnen anderen uit je persoonlijke leefomgeving details over je privéleven bekendmaken, die je liever niet op internet terugvindt.

Extra tips

- De publicatie van foto's met ondertekening op internet kan direct verbonden worden aan bijvoorbeeld uw hobby of favoriete (vakantie)bestemming. Dit maakt je eerder traceerbaar. Het loont dus ook de moeite om eens via Google op uw naam te zoeken en vervolgens het tabblad 'afbeeldingen' te bekijken. □
- Kijk ook eens op de website veiliginternetten.nl.

Telefoneren

Een aantal tips voor telefoneren met zowel je vaste telefoon als je smartphone:

Algemeen

- Wees terughoudend met het geven van je telefoonnummer(s). □
- Noem niet direct je naam bij het opnemen van de telefoon. □
- Twijfel je over de identiteit van de beller? Vraag naar naam en telefoonnummer van de betreffende persoon/organisatie. Controleer deze en bel zelf terug. □
- Zet je nummeridentificatie uit als je met onbekenden belt. □
- Bespreek geen gevoelige zaken per telefoon. Je kunt ongemerkt afgeluisterd worden. □
- Programmeer alarmnummers in je telefoon, zodat ze eenvoudig te bellen zijn.

Jouw vaste telefoon

□

- Neem een geheim telefoonnummer.

Jouw smartphone

□



Veiligheid en digitale communicatie

- Beveilig je smartphone met een pincode en een zogenaamde smartlock. □
- Maak je smartphone 'Boefproof'. Lees er meer over op de website maakhetzenietmakkelijk.nl. □
- Zorg ervoor dat je telefoon geen locatiegegevens meestuurt ('geotagging') bij het gebruik van sociale media of apps. Het zou vervelend zijn als inbrekers je huis leeghalen, omdat ze op sociale media gelezen of gezien hebben dat je op vakantie bent. Het automatisch koppelen van locatiegegevens (GPS) aan foto's en berichten en het ontkoppelen is via de instellingen van je smartphone of app in te stellen. □
- Kies er, indien mogelijk, voor om géén gebruik te maken van het GSM-netwerk, maar alleen van een 4G-verbinding. Uit onderzoek is gebleken dat andere verbindingen (2G of 3G) relatief makkelijk af te luisteren zijn. Stel je toestel zo in dat deze alleen van 4G-netwerken gebruik maakt. De introductie van een 5G-netwerk is aanstaande (vanaf 2020). Informeer tegen die tijd over de veiligheid van 5G-verbindingen. □
- Zet je bluetooth-verbinding na gebruik uit. Via deze verbinding kunnen kwaadwillenden gegevens uit je telefoon afvangen of apps installeren. □
- Maak voor bellen of verzenden van berichten via je smartphone gebruik van apps waarmee 'encrypted' informatie verzonden kan worden (zoals WhatsApp, Wickr me, Signal, Telegram, Viber). Vereiste is wel dat de ontvanger ook dezelfde app op zijn/haar smartphone heeft geïnstalleerd.

Extra tip

Aan het gebruik van (openbare) wifi-hotspots is een aantal veiligheidsrisico's verbonden. Het is voor jou vaak onbekend wie achter dergelijke hotspots zit of wat er gebeurt met de gegevens die jij met je smartphone verstuurt. Bankier daarom niet online, deel geen bestanden of andere gevoelige informatie, gebruik geen apps en bezoek bij voorkeur sites met een versleuteling ('https://' in plaats van alleen 'http://') De letter 's' staat voor secure. De data die je op deze secured website verstuurt, zijn versleuteld) als je gebruik maakt van een wifi-hotspot.



Veiligheid onderweg

Hoe reis jij naar je werk? Verblijf je voor je werk vaak in een hotel? Gaat je weleens op zakenreis? Als je onderweg bent, kun je kwetsbaar zijn. Je hebt in de zelfscan binnen de categorie 'Veiligheid onderweg' antwoord gegeven op een aantal vragen. Op basis van jouw antwoorden vind je hier een persoonlijk advies met concrete tips en adviezen om veilig onderweg te zijn.

Zie je hieronder geen tips staan, dan doe je al voldoende om veilig onderweg te zijn. Wil je toch deze tips en adviezen lezen? Dan vind je ze op de [CCV-website](#).

Onderweg

Weet jij hoe je de risico's op gevaarlijke situaties onderweg kunt vermijden? Hieronder enkele veiligheidstips:

- Voorkom voorspelbaar gedrag en gewoontegebruiken. Varieer bijvoorbeeld in routes en tijdstippen van aankomst en vertrek.
- Zorg ervoor dat je niet alleen reist, maar in gezelschap.
- Zorg dat je weet welke buurten je op bepaalde tijdstippen beter kunt vermijden.
- Voorkom dat je 's nachts alleen op straat loopt. Een groep is minder kwetsbaar.
- Blijf uit de buurt van samenscholingen, opstootjes, demonstraties en dergelijke.
- Kies voor drukke straten.
- Ga op een verlaten straat zoveel mogelijk in het licht lopen.
- Loop tegen het verkeer in, zodat een auto je niet ongezien van achteren kan naderen.
- Kijk, voordat je een locatie verlaat, uit het raam om eventueel opvallende en verdachte auto's of personen te kunnen ontdekken.
- Als je denkt dat je gevolgd wordt, verander dan meerdere malen onopvallend van richting en kijk of je nog steeds gevolgd wordt.
- Neem, als je er zeker van bent dat je gevolgd wordt, contact op met de politie of zoek een politiebureau op.
- Overweeg, wanneer het tot je mogelijkheden behoort, een chauffeur in dienst te nemen.

Auto

Maak je voor woon-werkverkeer gebruik van een auto? Hieronder enkele tips:



Veiligheid onderweg

- Houd je autosleutels apart van andere sleutels (zoals de sleutel van je woning): daarmee beperkt je verdere schade als je autosleutel is gestolen.
- Leg geen kostbare voorwerpen in je auto en laat je dashboardkastje open staan. Laat kwaadwillenden zo zien dat er geen kostbaarheden in je auto liggen. Laat ook geen gevoelige informatie achter in je auto zoals USB-sticks, laptops en papierwerk (of schaf een gecertificeerde autokluis aan). Een autokraker heeft maximaal 20 seconden nodig om de buit te vergaren.
- Installeer, indien gewenst, een GPS-systeem ('track and trace'), zodat je bij diefstal weet waar je auto zich bevindt.
- Zorg dat je jouw brandstoftank kunt afsluiten.
- Laat het chassisnummer in de ramen graveren of maak gebruik van 'microdots' waarop het chassisnummer vermeld staat.
- Overweeg voorzieningen voor elektronische beveiliging van je auto, zoals een startonderbreker, benzinetoevoeronderbreking, autoalarm-immobiliser en centrale deurvergrendeling.

Parkeren

- Wanneer je jouw auto voor de woning parkeert: zet je auto in het zicht vanaf de woning. Zichtlijnen mogen niet onderbroken zijn (door bijvoorbeeld hoge beplanting) en zorg voor voldoende licht op de auto.
- Parkeren algemeen: maak gebruik van parkeerplaatsen die voldoende verlicht zijn, waar de auto duidelijk zichtbaar is voor de omgeving en parkeer op een plek waar een beperkt aantal toegangswegen naar de parkeerplek leiden.
- Bevestig je kentekenplaten zodanig dat deze lastig te ontvreemden zijn (bevestiging met popnagels).

Extra tip

Voor verdere toelichting op bovenstaande maatregelen kan je terecht bij het onderwerp [Autokraak op de CCV-website](#).

Tijdens het autorijden

- Houd handtassen/laptoptassen en mobiele telefoons uit het zicht.
- Sluit portieren, ramen en dak tijdens het autorijden.
- Houd voldoende afstand tot je voorganger, zodat je tijdig en adequaat kunt inspelen op wijzigende verkeerssituaties.
- Stop alleen voor signalen van daartoe bevoegde personen.
- Let op verdachte verkeersomstandigheden (ongebruikelijke objecten, onnodig stoppen van auto's).
- Neem geen lifters mee.



Veiligheid onderweg

In en uit de auto stappen

- Let op de omgeving als je in en uit je auto stapt.
- Stap niet uit wanneer er mogelijk verdachte personen in de omgeving rondhangen.
- Maak er een gewoonte van direct na het instappen de portieren te vergrendelen, zodat onbevoegden niet zomaar bij je in kunnen stappen als je bijvoorbeeld bij een rood stoplicht staat.

Openbaar vervoer

Maak je voor woon-werkverkeer gebruik van een taxi of het openbaar vervoer? Hieronder vind je enkele tips daarvoor:

- Mijd verlaten, ondergrondse en slecht verlichte metro- en busstations, vooral 's nachts.
- Mijd verlaten coupés.
- Ga in de buurt van de chauffeur/conducteur zitten. Ga met je rug naar het raam van het voertuig zitten, zodat je een goed zicht hebt op de medepassagiers.
- Houd persoonlijke bezittingen dicht bij je en in het zicht.

Gebruik van taxi's

- Maak alleen gebruik van erkende taxibedrijven.
- Bestel een taxi vooraf.
- Programmeer telefoonnummers van de erkende taxibedrijven in je mobiele telefoon.
- Stap niet in een taxi als er al een passagier in zit.
- Instrueer de chauffeur vooraf over de te nemen route, zodat hij geen onbekende routes rijdt.

Reizen met verblijf

Boek je weleens een reis met overnachting of bezoek je weleens een ander land voor je werk? Hieronder enkele tips:

Hotel

- Zorg ervoor dat er bij het inchecken in een hotel zo min mogelijk mensen je naam en kamernummer horen. □
- Laat je kamersleutel nergens slingeren, haal er desnoods het label met het kamernummer vanaf. □
- Berg waardevolle spullen (sieraden, laptop, belangrijke papieren) op in de hotelkluis. □
- Gebruik altijd de hoofdingang van het hotel. □



Veiligheid onderweg

- Check je kamer op de veiligheid van ramen en deuren, op goede verlichting en op eventuele vluchtroutes naar buiten. □
- Ontvang eventuele onbekende bezoekers in de hotellobby, niet op je hotelkamer. □
- Sluit bij vertrek je kamerdeur, ramen en balkondeur af.

Documenten

- Zorg voor kopieën van je identiteitsbewijs. De originele documenten kun je dan opbergen in de kluis van het hotel of op een andere veilige plek. □
- Maak een scan van je belangrijkste documenten en e-mail deze naar jezelf. Een foto van deze documenten kun je ook opslaan op uw smartphone of in de cloud. Dit is handig bij verlies of diefstal. □
- Schrijf je creditcardnummer(s) op en noteer het telefoonnummer dat je nodig hebt als je jouw creditcard(s) wilt blokkeren. □
- Programmeer een ICE-nummer in je telefoon. ICE is de internationale afkorting voor In Case of Emergency. De persoon onder het nummer dat je in je mobiele telefoon opslaat onder de naam ICE, wordt gebeld in noodgevallen.

Buitenlandse reizen

Tips voor de voorbereiding

- Zorg dat je op de hoogte bent van de actuele situatie in het land dat je gaat bezoeken. Voor actuele reisadviezen en landeninformatie kun je terecht op www.wijsopreis.nl. □
- Informeer altijd een vaste contactpersoon over je reisplan en eventuele wijzigingen hierin, zodat er altijd iemand is die weet waar jij je bevindt. □
- Zorg dat je in het bezit bent van een geldig paspoort en visum. □
- Neem uw vaccinatiedocument mee als dit is vereist. □
- Schrijf je creditcardnummer(s) op en noteer het telefoonnummer dat je nodig hebt als jij je creditcard(s) wilt blokkeren. □
- Programmeer belangrijke telefoonnummers in je mobiele telefoon (telefoonnummer van de Nederlandse diplomatieke post, thuisnummers, alarmnummer van je reis- en zorgverzekering, en lokale noodnummers). □
- Maak voor reserveringen gebruik van diensten van bekende betrouwbare reisorganisaties en veilige luchtvaartmaatschappijen. □
- Kies voor een hotel dat buiten eventuele risicogebieden ligt. □
- Schrijf op de bagagelabels alleen je zakelijke adres of het verblijfadres tijdens de reis en je mobiele telefoonnummer. □



Veiligheid onderweg

- Maak gebruik van kofferlabels die je adres binnenin verbergen. □
- Neem geen waardevolle spullen mee als deze niet nodig zijn. □
- Zorg voor voldoende geld in verschillende vormen en verberg dit op meerdere plekken. □
- Stop vertrouwelijke documenten in je handbagage.

Tips voor tijdens de buitenlandse reis

- Houd je bagage altijd scherp in de gaten en laat deze nooit onbeheerd achter. □
- Neem onder geen beding pakjes of boodschappen 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 je bezoekt, bijvoorbeeld alcohol of voor hen controversiële tijdschriften of boeken. □
- Maak gebruik van een transferservice van en naar je hotel in plaats van een taxibedrijf (indien mogelijk). □
- Mijd overheidsgebouwen, ambassades of radio en tv-stations in een land waar de situatie instabiel is.

Colofon

Het CCV ontwikkelde de zelfscan in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en in samenwerking met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Projectcoördinatie

Axel Weggelaar, adviseur CCV

Fotografie

Inge van Mill

© het CCV, 2017

CCV centrum voor
criminaliteitspreventie en
veiligheid

Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een onafhankelijke stichting die partijen en veiligheidsprofessionals helpt om Nederland veiliger en leefbaarder te maken.

Centrum voor Criminaliteitspreventie en Veiligheid
Churchillaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht

T (030) 751 67 00
E info@hetccv.nl
I www.hetccv.nl

