# Draadloos internetten thuis en onderweg

## Inleiding.

Met de moderne apparaten zoals Laptops, netbooks, tablets en smartphones wilt u natuurlijk overal met internet kunnen werken. Thuis zult u dit bij voorkeur met uw draadloze netwerk doen; buitenshuis zult u een keus moeten maken uit de beschikbare communicatie mogelijkheden. In alle gevallen zult u aandacht moeten besteden aan veiligheid: u zult uw gegevens, inlogcodes en wachtwoorden moeten beschermen tegen ongewenste "meekijkers", fysieke personen of figuren die uw communicatie "aftappen".

Draadloze data communicatie technieken kunnen we onderscheiden in:
1. Wifi, gebaseerd op het internet protocol, met een reikwijdte van enkele honderden meters vanaf het basis station
2. GSM, met uw mobiele telefoon contact zoeken met uw telefoon provider; uw telefoon moet geschikt zijn voor data verkeer en uw abonnement moet het toelaten. Zo nodig moet uw mobiele telefoon met uw laptop verbonden worden.
3. Bluetooth, communicatie op korte afstand tussen 2 apparaten
4. Infrarood, waarbij beide apparaten elkaar moeten "zien"

De laatste 2 technieken kunt u bijvoorbeeld gebruiken om verbinding te maken tussen uw mobiele telefoon en uw laptop of uw autoradio systeem.

## Wat biedt een router?

Aan de ene kant wordt de router via de WAN-poort aangesloten op het apparaat waarmee met het wereldwijde Internet wordt gecommuniceerd, in ons geval het breedbandmodem van Onsbrabantnet. Dat modem communiceert met een centrale computer-server van Onsbrabantnet, van waaruit de informatie die u verstuurt wordt gerouteerd naar andere computers in het wereldwijde netwerk of omgekeerd.
De router bevat ook 4 LAN poorten met aansluitmogelijkheden via UTP kabels voor PC's, printer servers, storage servers, etc.
Sommige routers hebben ook een USB poort om direct een harde schijf op aan te sluiten, welke dan toegankelijk is voor alle PC's die op de router zijn aangesloten.

Voor ons is van belang: de draadloze communicatie door middel van 1, 2 of 3 antennes.
Een standaard aanwezige FIREWALL beschermt de computers achter de router tegen ongewenste toegang (inbraak) vanuit het internet.U dient echter zelf maatregelen te nemen om de draadloze communicatie tussen de router en uw PC te beschermen.

## Draadloos internetten thuis.

U hebt dus een ROUTER nodig welke (naast de meestal ook aanwezige 4 LAN-aansluitpunten) een of meer antennes heeft voor de zender voor draadloze communicatie. Soms is in het glasvezel- of kabelmodem de zender voor draadloze communicatie al aanwezig, anders zult u een extra router via een UTP kabel met het modem moeten verbinden.

Maar nu moet er meer gebeuren om de internet-aansluiting van uw laptop of tablet tot stand te brengen. Allereerst moet u ook in uw computer een voorziening hebben voor draadloze communicatie;

- een ingebouwde adapter (vaak in laptops), of
- een USB-insteek module, of
- een PCMCIA insteekmodule, of
- een inbouw module voor desktop PC's.

Deze communicatie voorziening ondersteunt een of meer communicatie protocollen en snelheden. Voor de router bepaalt het ondersteunde protocol zowel het bereik als ook de snelheid van communicatie:

| Standaard | Introductie | Frequentie | Bandbreedte | Maximale afstand | |
|---|---|---|---|---|---|
| | | | | binnenshuis | buitenshuis |
| 802.11a | 1999 | 5 GHz 5 | 4 Mbit/sec | 35 | 120 |
| 802.11b | 1999 | 2,4 GHz | 11 Mbit/sec | 40 | 140 |
| 802.11g | 2003 | 2,4 GHz | 54 MBit/sec | 40 | 140 |
| 802.11n | 2009 | 2,4 / 5 GHz | 150 MBit/sec | 70 | 250 |

Let wel op:
- als er meerdere apparaten met de router communiceren, bepaalt het apparaat met de traagste verbinding (= het laagste protocol) de snelheid. Vervang zonodig de adapter in uw traagste apparaat!
- Omdat de b/g protocollen van de 2,4GHz band gebruik maken, is het advies om routers met 802.11n protocollen in te stellen om gebruik te maken van de 5 GHz frequentie.

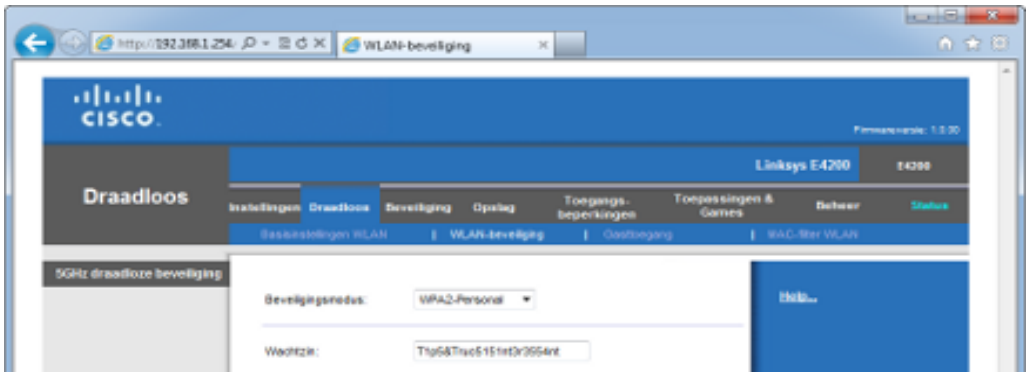
De 802.11-standaarden gebruiken een bepaalde frequentie om hun signaal uit te zenden. Dat is de 2,4GHz- of de 5GHz-frequentie of beide, in het geval van 802.11n. De zenders en ontvangers gebruiken niet de hele frequentie, maar een zogeheten 'kanaal' dat er slechts een deel van beslaat. Iedere frequentie kent meerdere van dit soort kanalen. Binnen de 2,4GHz-band zijn dat er elf, binnen de 5GHz-band acht. De kanalen zijn niet helemaal van elkaar gescheiden. Ze overlappen elkaar, maar toch heeft het zin als netwerken zoveel mogelijk een eigen kanaal gebruiken en niet allemaal hetzelfde, bijvoorbeeld kanaal 5.

> Met het programma inSSIDer kunt u zien welke kanalen de andere netwerken in de buurt gebruiken. Daarvoor kijkt u in de kolom **Channel**. Gebruikt uw draadloos netwerk een kanaal dat ook al door veel andere netwerken wordt gebruikt, dan kunt u in uw router bij **Kanaal WLAN-verbinding** een ander kanaal kiezen. Bepaal in inSSIDer welk kanaal het minste wordt gebruikt en selecteer het vervolgens in uw router. Omdat kanalen elkaar overlappen en het voordeel het grootst is wanneer de afstand ertussen maximaal is, kunt u het meeste voordeel verwachten wanneer binnen de elf kanalen van de 2,4GHz-band de kanalen 1, 6 en 11 worden gebruikt. Die liggen immers het verst van elkaar af.

## Beveiliging van de draadloze verbinding.

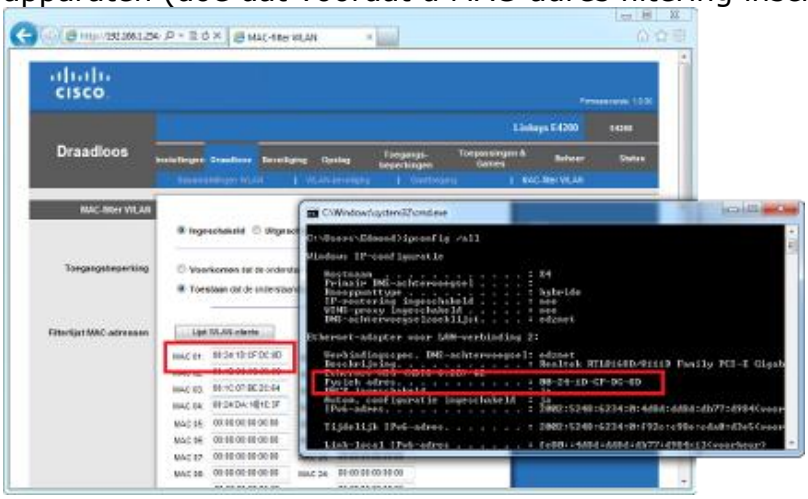
Draadloze netwerken zijn onveiliger dan bedrade netwerken, omdat iedereen met de meest elementaire netwerk apparatuur kan inbreken in vrijwel ieder draadloos netwerk in zijn bereik. Maar zelfs met weinig technische kennis kun je je draadloos netwerk goed beveiligen met de volgende eenvoudige tips voor de instelling van je router:

- **Beveilig de beheer inlogcodes van de router:** de meeste apparatuur wordt geleverd met standaard inlogcodes (admin  wachtwoord admin) en deze zijn natuurlijk bekend bij de hackers. Dus als je je router configureert, wijzig dan als eerste het wachtwoord (en schrijf dat ergens op!).
- **Stop met het uitzenden van de SSID:** je draadloze router zendt voortdurend de SSID (Service Set Identifier, de naam van je router) uit. Dat is in een thuis situatie niet nodig. Schakel het uitzenden van je SSID uit. Wireless LAN "sniffers" zullen je network nog wel kunnen ontdekken, maar verder is je network onzichtbaar voor anderen. Overigens is het ook verstandig een SSID te kiezen die niet direct op jou terug te voeren is. Komt er zo nu en dan een "gast", dan zul je hem of haar de SSID van het netwerk en het wachtwoord moeten vertellen om verbinding te maken.
- **Kies de best mogelijke encryptie standaard:** In oplopende mate van geavanceerdheid (en dus moeilijker te kraken) zijn de volgende protocollen: WEP, WPA, WPA2. Het advies is om WPA2 te kiezen als beschikbaar in uw router.
- **Kies een sterk wachtwoord of wachtzin:** Bedenk een goed wachtwoord of een sterke wachtzin. Dat is de sleutel die voortaan in ieder apparaat moet worden ingevoerd om verbinding met het draadloos netwerk te kunnen maken. Dat hoeft u overigens maar één keer te doen, daarna onthoudt elk apparaat de sleutel. Bedenk een zo sterk mogelijke sleutel, waarin hoofdletters, kleine letters, leestekens en enkele cijfers voorkomen.
  Goed documenteren!




- **Gebruik MAC- adress filtering:** Stel MAC-adres filtering in. Daardoor kun (en moet!) je het MAC- adres van al je apparaten die draadloos willen communiceren met hun MAC-adres aanmelden bij de router. Zo kan

niemand anders toegang krijgen tot je router en je netwerk..
Het MAC-adres van een apparaat staat vaak op een sticker op de onder- of achterkant, en anders kunt u het altijd nog achterhalen door naar **Start** / **Uitvoeren** te gaan, het commando **cmd** uit te voeren en via **ipconfig /all** het fysiek adres op te vragen van alle op dat moment aangesloten apparaten (doe dat voordat u MAC-adres filtering inschakelt…).




- **Beperk het vermogen van de zender:** Verminder het vermogen van de draadloze zender zodanig dat het signaal niet buiten je huis reikt. Daardoor is je netwerk onbereikbaar voor buitenstaanders..
- **Schakel de beheer mogelijkheid op afstand uit:** Die mogelijkheid wordt zelden gebruikt, dus als je hem aan zou laten creëer je een onnodig risico.

MAC-adressen zijn te lastig om te onthouden en bovendien hebt u ze maar zelden nodig. De MAC-filterlijst van een router raakt in de loop der tijd echter wel vervuild met adressen waarvan u niet meer weet bij welke apparaten ze horen. Een trucje om dat alsnog te achterhalen, is door even bij de DHCP-reserveringen te kijken. Dat is geen onderdeel van het draadloos accesspoint maar van de router zelf. Bij veel routers kan via deze functie een lijst worden opgevraagd met netwerkapparaten die via DHCP een IP-adres hebben opgevraagd, en daar worden dan ook de MAC-adressen bij getoond.

## Voorbereiding voor op reis.

**U ziet er tegenop het om uw computer mee te nemen op vakantie, maar wilt graag gebruik maken van de mogelijkheden van internet. Dan biedt een internetcafé een oplossing. Op voorwaarde dat u enkele veiligheidsregels in acht neemt!**

Eerst en vooral nog een raadgeving voor het vertrek.
Een aantal documenten moet u steeds zorgvuldig bewaren en bij u hebben wanneer u reist. Welke dat zijn hangt een beetje af van de manier waarop u reist en van uw bestemming: bijvoorbeeld uw reis pas, visum, vliegtickets, reisverzekering, autopapieren, uw hotelreservering of

reservering van een huurwagen ter plaatse, enz. We wensen het natuurlijk niemand toe, maar als u één van deze papieren verliest of ze worden gestolen, kan dat knap lastig zijn.
Daarom is het altijd nuttig om al deze belangrijke documenten ook in digitale vorm mee te hebben. Deze hebben weliswaar niet altijd dezelfde waarde als het origineel, maar ze kunnen u toch vaak een kostbare hulp zijn in geval van nood.

Hoe uw reisdocumenten digitaal meenemen?
Er zijn twee manieren:
U plaatst alle documenten op **een USB-stick**, Deze bestaan tegenwoordig in zeer handige, kleine en lichte formaten. Van heel wat documenten heeft u ongetwijfeld al een digitale vorm. Veel vliegtickets en reserveringen worden tegenwoordig per mail doorgestuurd in pdf-vorm. Die hoeft u nog enkel te copiëren op uw USB-stick. Van verzekeringsdocumenten kunt u meestal ook heel eenvoudig een pdf opvragen bij uw verzekeringsagent. En de overige documenten? Veel zullen dat er nooit zijn, maar die moeten wel ingescand worden. Beschikt u thuis niet over een scanner, informeer dan even bij vrienden en kennissen. Er is allicht wel een goede ziel die dat klusje even voor u wil doen. Veel werk vergt dat echt niet. Vraag om uw documenten als pdf op te slaan.

Een andere mogelijkheid: deze documenten **online opslaan**. Want ook een usb-stick kan natuurlijk zoek raken. Online opslaan kan gerust op één van de vele gratis online opslagdiensten zoals Dropbox of Windows Live SkyDrive (http://skydrive.live.com). Deze dienst geeft u 5 GB online opslagruimte. Daar kunnen heel veel documenten op. Het volstaat dat u een Windows Live- of een Hotmail-account hebt om vanuit om het even welke plek ter wereld waar u over een computer (of zelfs uw mobiele telefoon of iPad) en internet kunt beschikken in te loggen op uw persoonlijke opslagruimte. Ga naar de website van skydrive.Live.com en kies 'Start met delen'. Kies vervolgens 'Een persoonlijke map maken'. Geef de map een naam en kies voor 'Alleen ikzelf'. Klik vervolgens op 'Map maken'. Vervolgens kunt u alle gewenste bestanden toevoegen aan deze map door te klikken op 'Bladeren', het gewenste document te selecteren, en te klikken op 'Uploaden'.

## Technische voorbereidingen thuis

Als u binnenkort op vakantie gaat en uw **laptop, smartphone of tablet meeneemt**, kunt u het thuisfront de laatste foto's mailen en met een drankje in de hand Skypen met uw vrienden. Dat klinkt goed, maar zonder goede voorbereiding loopt u het risico te worden geconfronteerd met diefstal of torenhoge rekeningen. We zetten de beste tips op een rij, zodat u onbezorgd van uw vakantie kunt genieten.

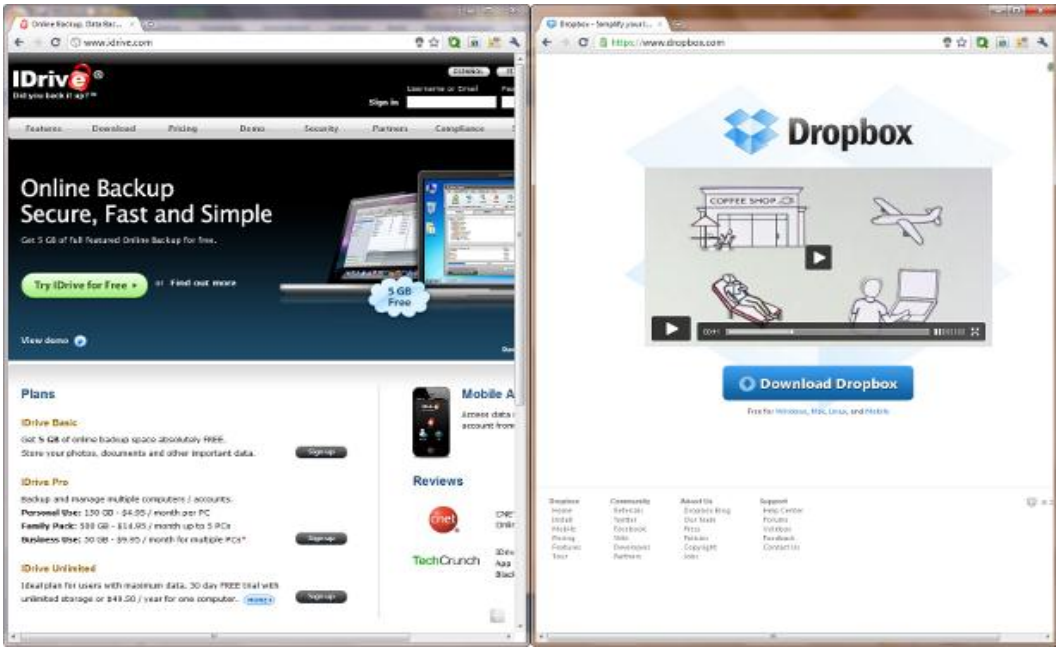
### 1. Back-up

Het zal u maar overkomen. Neemt u uw laptop veilig mee op vakantie, valt het apparaat in een ravijn of wordt het gestolen. Het gevolg: uw dure apparaat is weg en u bent al uw dierbare bestanden kwijt. Het is daarom verstandig om een gedegen back-up van uw laptop te maken. U kunt hiervoor een speciaal back-up programma aanschaffen, maar Windows 7 is voorzien van eigen software.
Om het back-upproces te starten, klikt u op **Start** en typt u **back-up maken**.

Klik nu op **Een back-up van uw computer maken**. U hebt de keuze om een systeemkopie of een 'normale' back-up te maken. Een systeemkopie is een exacte kopie van de harde schijf, terwijl u met de normale back-up zelf bestanden kunt selecteren.

## 2. Gegevens opbergen

Nu de externe harde schijf vol staat met persoonlijke gegevens, is het noodzaak deze veilig op te bergen. Mocht u over een kluis beschikken, dan is het geen gek idee om de schijf hierin te bewaren. Een alternatieve optie voor een externe schijf, is om een online kluis aan te maken. U betaalt hiervoor een vast bedrag per maand, mocht het om een groot aantal GB's gaan. Via diensten als iDrive (5 GB gratis opslag) of Dropbox (2 GB gratis opslag) kunt u wellicht de volledige map 'Mijn Documenten' gratis bewaren. Als u meer ruimte nodig hebt, kunt u die tegen betaling krijgen.




## 3. Stel toegang op afstand in

Wanneer je gebruikmaakt van een smartphone, een tablet of een laptop, dan kun je deze zo instellen dat je deze kunt gebruiken om je belangrijke mails te blijven lezen en beantwoorden **(Onsbrabantnet staat niet toe e-mails te verzenden als u niet direct op hun net bent aangesloten, stel daarom eventueel de SMTP server van een andere provider bij uw Onsbrabantnet account in om uw mail te verzenden!)**. Eventueel kun je ook een configuratie maken waarin je jouw eigen werkcomputer geheel op afstand kunt benaderen, mocht je denken daar eventueel gebruik van te maken. Al deze dingen moeten van tevoren natuurlijk wel ingesteld worden.

## 4.Wat niet weet, wat niet deert

De verleiding is groot om via Hyves, Facebook en Twitter het thuisfront mee te laten genieten van uw welverdiende vakantie. Helaas kunnen onbekenden gewoon meelezen op een slecht beveiligde pagina. Terwijl u een foto post waarop u een cocktail drinkt, weten insluipers rustig uw huis binnen te dringen. Wees dus verdacht op dergelijke zaken en zet foto's pas op Picasa of Flickr bij thuiskomst. Zo maakt u het uzelf gemakkelijker en dieven moeilijker! Natuurlijk meldt u op uw sociale netwerk ook niet dat u op vakantie bent…. Ook het vermelden van uw woonadres is onverstandig.

## 5. Beveiligingsupdates

Wees hackers en ander gespuis voor! Installeer de laatste beveiligingsupdates van Windows en van software die verbinding met internet moet maken om te kunnen worden gebruikt. Windows werkt u bij door op **Start** te klikken en vervolgens **Windows Update** in te typen. Laat het systeem naar updates zoeken en kies **Belangrijke updates zijn beschikbaar**. Download en installeer de beveiligingsupdates. Andere updates waaraan u moet denken zijn die van HP, Google, Apple en Adobe. Vooral Adobe is roemrucht vanwege lekken in programma's als Adobe Reader en Adobe Flash. Als u in het buitenland gebruikmaakt van een openbare internetverbinding, kunt maar beter alles hebben dichtgespijkerd.

## 6. Beveiligingspakket

Mocht u nog geen antivirus of firewall op uw computer hebben geïnstalleerd, dan is dit een perfect moment om deze software aan te schaffen of gratis te downloaden. Enkele gratis scanners zijn volgens diverse tests net zo goed als dure pakketten. Installeer bijvoorbeeld Security Essentials, een antiviruspakket van Microsoft, Avira AntiVir Personal of Avast! Free Antivirus. De keuze is aan u; het verschil zit voornamelijk in de lay-out van de software. Sommige pakketten leggen de nadruk op specifieke functies. Zo brengt Microsoft de optie 'Netwerkinspectiesysteem' naar voren, ter beveiliging van het netwerk waarmee u verbonden bent. Dit is een handige functie als u onbekende wifi-verbindingen gebruikt.

## 7. Thuismodem veilig achterlaten

Als u enkele dagen of weken van huis gaat, moet het niet zo zijn dat de buren even flink profiteren van uw snelle thuisnetwerk. Trek daarom de stekker uit het stopcontact

## 8. Tijdelijk e-mailadres

U weet nooit op wat voor locaties u terechtkomt in de wereld en met wat voor internetverbindingen u te maken krijgt. Om spam en andere narigheid te voorkomen, en om tegen te gaan dat een keylogger (software die uw toetsaanslagen registreert in bijvoorbeeld een internetcafé) het wachtwoord van uw e-mailaccount achterhaalt, is het aanmaken van een tijdelijk extra e-mailadres een goed idee. Dit kan bijvoorbeeld bij Hotmail, Gmail, Yahoo of een

soortgelijke dienst. Laat uw familie en vrienden even weten dat dit adres slechts voor de vakantieduur van kracht is. U kunt ook van uw eigen e-mail adres de e-mails automatisch laten doorsturen.

> Surf bijvoorbeeld naar Hotmail en klik op **Registreren** of volg de registratiestappen achter de knop **Een account maken** op Gmail. Op Ikbenspamvrij.nl kunt u een tijdelijk mailadres aanmaken voor de registratieprocedure op een website. Zo blijft uw eigen mailadres veilig achter schot. Op de website vult u bij **Je eigen emailadres** het adres in dat u dagelijks gebruikt en vervolgens bepaalt u de **Geldigheid**, ofwel de periode waarin het adres moet werken. Sluit af met **Maak tijdelijk emailadres**.

## 9. Kaarten voor onderweg

Het gps-signaal van uw navigatiesysteem of mobiele telefoon is natuurlijk uiterst handig, maar in het geval van een smartphone hebt u een internetverbinding nodig om de locatie op een kaart te laten zien. U kunt daarom beter vooraf al enkele kaarten uitprinten, zodat u alsnog de weg gewezen wordt. We zetten enkele websites op een rij die u hierbij van dienst kunnen zijn. Uiteraard zijn deze pagina's ook handig in de favorietenlijst van uw browser, voor het geval u onderweg alsnog een wifi-signaal oppikt.

**Zoekmachine:**

De gemakkelijkste manier om een toeristenkaart te verkrijgen zonder een VVV-kantoor te bezoeken, is door de zoekterm *** map filetype:pdf** in te voeren in bijvoorbeeld Google, waarbij u op de plek van het sterretje een plaatsnaam invult. Zoekt u naar een kaart van het lokale openbaar vervoer, vul dan in: *** transport map filetype:pdf**. Gebruik *** hotels map filetype:pdf** om alle hotels in de betreffende plaats te vinden.

**Fietsroutes:**

Op Bikemap.net vindt u alle populaire fietsroutes in de regio. Of u nu in Nederland of in Bolivia op de tweewieler stapt: er is voor iedereen een perfecte route te vinden. Het mooie aan deze pagina is dat u gewoon op het land van keuze klikt, inzoomt op de locatie waar u bent en direct een aantal suggesties aantreft. De route is zichtbaar op een duidelijke satellietkaart en kan direct worden geëxporteerd. Klik op **Afdrukken** voor een fysieke print, of op **Gps export** om de coördinaten in een Google Earth-bestand (.kml) of universeel gps-formaat (.gpx) te verkrijgen. Gedetailleerde informatie over de route is af te lezen door de muis op de route te plaatsen, of door onder het kopje **Details** aan de rechterzijde van het scherm te kijken.

**Vliegroutes:**

Als u met de rugzak naar het buitenland trekt, is het fijn om te weten of u ook een vliegtuig naar een andere locatie kunt nemen. Op Skyscanner vindt u een uitgebreide prijsvergelijking tussen maatschappijen, maar ook een kaart met luchthavens en belangrijke informatie hierover. Op de homepage klikt u op **Luchthavens**. Kies nu onder **Vliegvelden ter wereld** voor **Alle** en zoek naar uw gewenste locatie. U kunt ook op regio zoeken, onder **Luchthavens - op continent**. Eenmaal een plaats gekozen, ziet u alle details, zoals de lengte- en breedtegraad, vliegvelden in de buurt en welke maatschappijen er vliegen. Verder vindt u hier een routekaart, aankomsttijden en een prijsoverzicht.

**Zeeroutes:**

Een dagje met de boot naar Newcastle, Rostock of Helsinki? Via Openseamap

krijgt u een volledig overzicht van alle ferry-routes ter wereld.

**Kaarten-apps:**

Uiteraard zijn er ook applicaties voor de tablet of smartphone verkrijgbaar. Of u hiermee uit de voeten kunt, ligt aan de locatie die u bezoekt. Zo zijn voor diverse grote steden speciale apps ontwikkeld waarmee u niet alleen een plattegrond op het scherm krijgt, maar ook specifieke route-informatie en de historische achtergrond van bijvoorbeeld standbeelden die u tegenkomt. Kijk in de app-store die bij uw telefoon hoort of ook voor uw vakantieplek een app is ontwikkeld.

## 10. Wachtwoordenkluis

KeyPass is een handig programmaatje om mee te nemen op vakantie, zodat u geen papieren schrift met belangrijke wachtwoorden voor e-mail en internetbankieren hoeft mee te nemen. U kunt KeyPass gewoon op een usb-stick zetten, waarna u alle wachtwoorden opslaat onder één 'Master Password'. In geval van verlies of diefstal kan dus niemand in uw wachtwoordenkluis komen, aangezien alleen u de code ervan kent.

Surf naar keepass.info en klik op Downloads. Kies voor Portable KeePass (ZIP Package). Unzip het bestand op de usb-stick (of op een harde schijf), door te kiezen voor Alle bestanden uitpakken / Bladeren en de locatie te selecteren waar het programma moet worden opgeslagen. Open KeyPass nu. Klik File / New en voer een Master Password in dat als slot voor de kluis geldt. Eventueel kunt u een Key File gebruiken. Dat is een bestandje dat u zelf selecteert en dat altijd aanwezig moet zijn om de databank te kunnen openen. Klik ten slotte op OK. Met de toetscombinatie Ctrl+Y kunt u wachtwoorden genereren en toevoegen. U kunt ook nog informatie toevoegen over de websites of software waarvan u de wachtwoorden bewaart.

## 11. Schijf delen

Als u uw laptop buiten de vakantie om vooral als hoofdcomputer gebruikt, kan het zo zijn dat u ten behoeve van het thuisnetwerk al uw bestanden deelt met aan het netwerk gekoppelde computers. Controleer daarom de instellingen.

Ga in Windows naar **Start** en typ **Netwerkcentrum**. In het Netwerkcentrum gaat u naar **Geavanceerde instellingen voor delen wijzigen**. De instellingen op de eerste rij gelden voor een thuisnetwerk of een verbinding die als zodanig is ingesteld. Scroll naar beneden en ga naar het tabblad **Openbaar** door op het pijltje te klikken. U kunt u nu een aantal opties in- of uitschakelen. De volgende zaken moet u uitschakelen: **Netwerkdetectie**, **bestands- en printerdeling**, en **openbare mappen delen uitschakelen**. Juist ingeschakeld moeten worden:**128-bitsversleuteling gebruiken** en **Met wachtwoord beveiligd delen inschakelen**. Sluit af met **Wijzigingen opslaan**. In het Netwerkcentrum controleert u onder het kopje **De actieve netwerken weergeven** of de connectie is ingesteld als thuisnetwerk of als openbaar netwerk. Klik op het type netwerk om het te wijzigen in een ander type.

## 12. Dataroaming uitzetten

Voordat u de grens overgaat of het vliegtuig instapt, moet u controleren of dataroaming op uw smartphone 'uit' staat. Bij roaming wordt uw mobiele telefoonverbinding overgenomen door het signaal van een andere aanbieder. Dat is handig, want zo kunt u ook in het buitenland via een lokale provider naar Nederland bellen. Bij dataroaming, waarbij u dus via een lokale provider verbinding met internet maakt, kunnen de kosten echter hoog oplopen. U zou

niet de eerste vakantieganger zijn die bij thuiskomst wordt verrast door een rekening van enkele honderden euro's.

> Bij een iPhone staat roaming standaard al uit. Als u een BlackBerry hebt, gaaat u naar **Opties** / **Netwerk** / **Gegegevensservices uit**. Bij een telefoon die is voorzien van een oude Android-versie (bijvoorbeeld. 1.5) moet u een APN-widget installeren die u in de Android Market kunt downloaden. In nieuwere versies van het besturingssysteem is APN al in het optiemenu opgenomen. Ook bij Windows Mobile is er verschil tussen versies, maar meestal staat dataroaming ook hierbij standaard al uit. Controleer hoe dan ook altijd even wat de 'roaming-status' is, in het optiemenu van uw telefoon

# Op reis

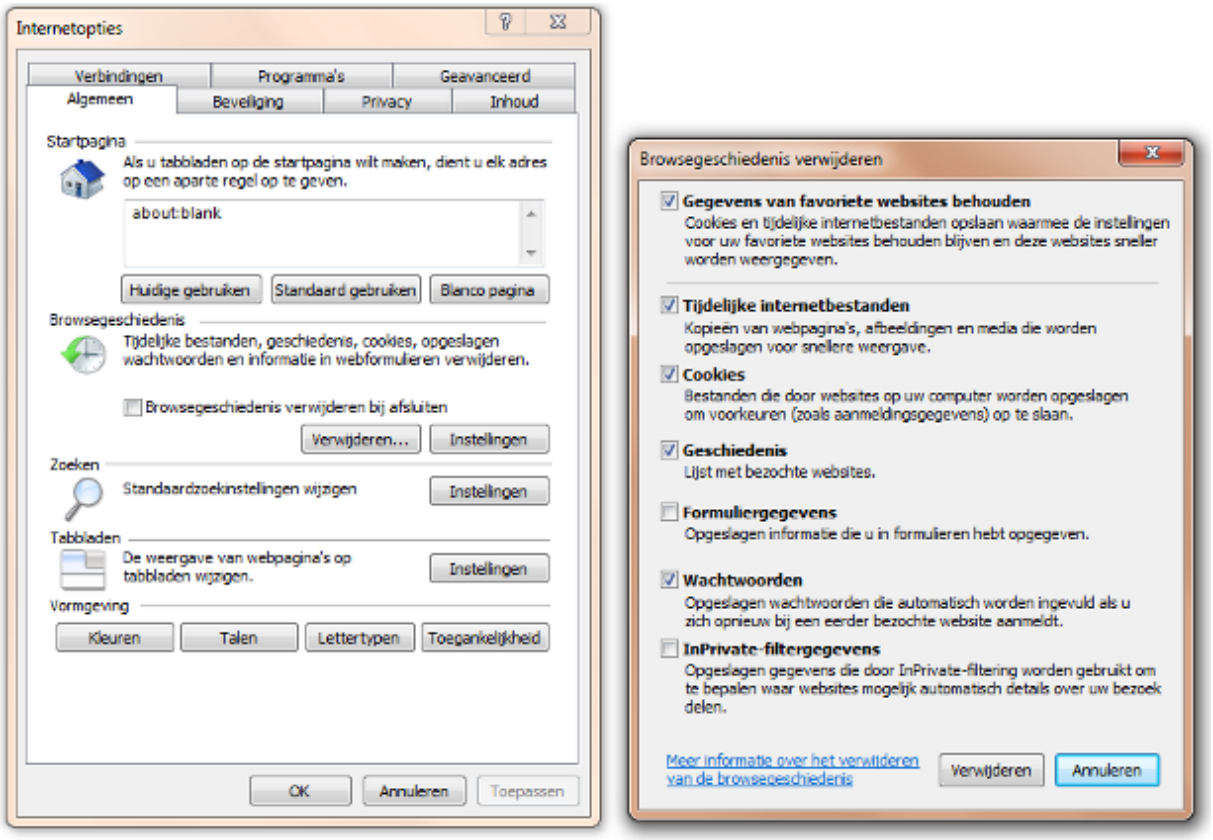
## 13. Veilige hotspots

Als u in het buitenland gebruikmaakt van internet, moet u er eerst zeker van zijn dat de netwerkverbinding die u aanklikt van een betrouwbare partij afkomstig is. Dat kan bijvoorbeeld de lokale bibliotheek of een internetcafé zijn. Gebruikmaken van een gratis toegankelijke verbinding is altijd af te raden. Als u geen wachtwoord hoeft in te voeren, is de kans groot dat criminelen direct toegang hebben tot uw computer. Bent u toch met een open netwerk verbonden? Let er dan in ieder geval goed op dat u alleen persoonlijke gegevens invoert op websites met het https-protocol, die u herkent doordat het webadres begint met https://. De 's' staat voor secure, oftewel 'veilig' en veel mailservers en banken maken gebruik van dit protocol. Let hier goed op! Met een https-verbinding is de overdracht versleuteld en dus niet toegankelijk voor anderen op het netwerk.

## 14. Historie verwijderen

Een rondje langs de geschiedenispagina's van Internet Explorer (IE) levert vaak persoonlijk getinte informatie op: de bezochte Facebookpagina's van vrienden, bij welke bank u hebt ingelogd, en nog veel meer. Klik daarom ook nooit op 'wachtwoord automatisch opslaan' wanneer u in een internetcafé of bibliotheek zit. Als u dit per ongeluk toch hebt gedaan of gewoon uw browsegeschiedenis wilt verwijderen, moet u het volgende doen.

> In IE klikt u op **Extra** / **Internetopties** en hier kiest u het tabblad **Algemeen**. Kies onder **Browsegeschiedenis** de knop **Verwijderen**. Zet een vinkje voor elke optie, dus ook bij **Wachtwoorden** en **Formuliergegevens**. Bevestig de actie met **Verwijderen**. In andere browsers komt u een soortgelijk optie tegen in het optiemenu. Let daarbij op een term als 'Browsegegevens wissen' of 'Wis browsegeschiedenis'.




## 15. Slecht taalbarrières

Verschillende apps voor uw smartphone en programma's voor uw notebook maken het leven in het buitenland een stuk gemakkelijker. Allereerst is er Google Vertalen. Bij deze software kiest u de gewenste vertaaltaal en vervolgens typt u uw tekst in. U kunt ook een url invoeren, zodat Google een hele webpagina omzet naar het Nederlands. Sinds kort kan Google Vertalen ook woorden uitspreken; dat kan erg handig zijn als u bijvoorbeeld in een restaurant iets wilt bestellen. Verder is er voor bijna ieder model smartphone een vertaal-app beschikbaar. In de App Store van Apple en in de Android Market vindt u bijvoorbeeld het handige My Words. Deze app is aardig aan de prijs (€ 9,95), maar hij is bijzonder veelzijdig. U kunt er teksten mee laten omzetten naar tientallen talen, waaronder Duits, Frans en Engels, maar ook Chinees en Turks. De app biedt ook taalspelletjes en een tool die u helpt om uw uitspraak te verbeteren.

Bronnen:

Computer!Totaal
Wikipedia

# VEILIG INTERNET ONDERWEG

hcc digizine

## Veilig internet onderweg

*Auteur: Ron Onrust*

**Op vakantie heb je minder contact met het internet. Misschien maakt dat ook wel een belangrijk deel uit van de vakantie; even weg van alles, dus ook van het internet. Maar als eenmaal op de eindbestemming de omgeving is verkend, dan begint het te kriebelen. Zou die ene e-mail zijn binnengekomen? Of is dat ene bedrag wel afgeschreven van de bankrekening? Hoe doe je dat nou veilig? Internetgebruik in het buitenland. Hier een paar valkuilen en tips.**

Je wilt even weg uit de hitte en loopt een lokaal restaurantje binnen voor wat afkoeling en een drankje. Tot je verrassing staat daar binnen een pc aan met erop een bordje; gratis internet. Gratuide, Free, Libre. Wat doe je? Even e-mail checken? Het beste advies is: nee! De reden hiervoor is een zogenoemde 'keylogger'; een apparaatje of programmaatje dat alle toetsaanslagen vastlegt. Iedere pc waar je niet zelf het beheer over hebt, kan zo'n keylogger bevatten. En dat zijn wachtwoordsponzen. Dus die gratis pc is leuk voor toeristische informatie, voor Google Maps, en voor het lezen van het laatste nieuws, maar niet voor e-mail, of (hemeltjelief) bankzaken. Dat geldt in principe voor alle pc's, dus ook die in internetcafés. Keyloggers zijn er in hardware-matige vorm, dan zitten ze tussen de kabel van het toetsenbord en kun je ze dus zien zitten, maar ze zijn er ook in software en dan zie je er niets van.

**Oppassen geblazen**

Je kunt veel veiliger met je eigen pc het internet op, en je gaat dus met de laptop onder de arm op zoek naar een draadloze verbinding, en die is vaak snel gevonden. Overal is wel ergens een draadloos netwerk dat 'open' staat en kan worden gebruikt zonder wachtwoord. Goed idee? Nou, ook hier is het oppassen geblazen, zelfs als er wel sprake is van een wachtwoord , bijvoorbeeld in het hotel. Bij ieder gedeeld draadloze netwerk kan de data door alle 'deelnemers' in het netwerk worden onderschept. Dat werd enige tijd geleden gedemonstreerd door 'Firesheep', een programma dat bij zo'n netwerk de actieve verbindingen in beeld bracht bij de andere deelnemers op het netwerk met websites als Facebook, twitter of Flickr. De bezitter van Firesheep kan vanachter zijn pc 'meedoen' met een sessie van een ander in Facebook. Dus ook bij een draadloos netwerk: geen wachtwoorden intypen!

Er is een methode die zorgt voor een veilige verbinding tussen pc en website, en dat is middels het protocol SSL. Dat kan per website worden gebruikt, door in de browser voor het adres het 'http' weg te halen en te vervangen door 'https'. Let op, de website moet dat wel ondersteunen, maar gelukkig doen de meeste websites waar je op moet inloggen dat tegenwoordig wel. Met een SSL-verbinding kan redelijk veilig de e-mail worden bekeken. Maar sommige websites doen alleen de login via SSL, en de rest van de verbinding onbeveiligd. In de gaten houden of bij het adres 'https' blijft staan of niet is hier het devies.

**Firewall in buitenland**

Dan tenslotte; de meeste mensen hebben thuis een prima router met een ingebouwde firewall, maar of die firewall er in het buitenlandse ook is, is onzeker. Installeer dus nog thuis een desktop- of personal firewall . Dat geldt met name voor de wat oudere versies van Windows; Windows 7 bijvoorbeeld, heeft zelf een prima firewall. Dan is de pc goed beschermd. En natuurlijk is het niet verstandig om te vertrekken met een pc waarop niet alle laatste updates en patches zijn geïnstalleerd. Maar dat spreekt voor zich.