Eenentwintigste jaargang nummer 12: DEC 2020

De COMPUTERCLUB

Nissewaard

Computerclub Nissewaard is voortgekomen uit een samenwerking van CcUpdate en Stichting wijkgroep de Akkers

Colofon

Dagelijks bestuur

Voorzitter:	**H.Kubbinga**	**Tel. 0181-640669**
Penningmeester:	**B.W.Tijl**	**Tel. 06-54692942**
Secretariaat:	**A v Bronckhorst**	**Tel. 06-36147051**

Vrijwillige medewerkers Computerclub Nissewaard

Boekje:	**Arie van Bronckhorst**
Magazijn en lesgevende:	**Arie van Bronckhorst**
Lesgevende:	**Bart Tijl**
Lesgevende:	**Hans Kubbinga**
Lesgevende:	**Karel Kleijn**
Netwerkbeheerder:	**Peter Mout**

Betalingen via de bank is mogelijk.
Rekening nummer IBAN: NL44ABNA0506627470
tnv B.W.Tijl.
Onder vermelding van: Penningmeester **CCUPDATE.**

Correspondentieadres is:
computerclubnissewaard@gmail.com
tel 06-54692942
of Voorzitter@computerclubnissewaard.nl
secretaris@computerclubnissewaard.nl
penningmeester@computerclubnissewaard.nl
Internet: http://www.computerclubnissewaard.nl

Computerclub Nissewaard is voortgekomen uit een samenwerking van CcUpdate en de Stichting Wijkgroep de Akkers.

Bestuursmededeling
December 2020
Beste leden,

Het jaar 2020 vliegt voorbij zonder dat we de normale clubavonden hadden door de gedeeltelijke lockdown waar we allemaal tegen aan hikken. De start van 2021 zal pas eind februari/begin maart zijn door de verbouwing in het wijkgebouw. We hopen dat hierna de lesstart voorspoediger verloopt. We moeten er zelf maar wat van maken met Sinterklaas en Kerst volgens de RIVM-regels.
In dit clubblad zijn we begonnen met het aanbrengen van een inhoudsopgave. Zie pagina 5. Hiermee zijn onderwerpen later makkelijker terug te zoeken. Je moet natuurlijk wel de boekjes bewaren.
Het bestuur en lesgevenden wensen u en uw dierbaren een leuke Sinterklaas en goede Kerstdagen.

2020

Groet van uw voorzitter: Hans Kubbinga

Bezoek ook onze nieuwe website eens
www.computerclubnissewaard.nl

Servicepagina

Deze pagina is een vast onderwerp in het boekje en geeft u informatie over het doen en laten van Computerclub Nissewaard.

Lidmaatschap kost u maandelijks	**€ 10,00**
Betaalt u in eens voor een heel jaar, betaalt U	**€ 90,00**
U kunt bij ons een cursus volgen vanaf	**€ 25.00 incl. Lesmateriaal.**
Wilt U zomaar een avondje doorbrengen bij ons dan kan dat voor	**€5,00**
Hulp bij Computerstoringen of Software problemen kan ook bij ons. U betaald dan een bijdrage van:	**€ 10.00 per keer, excl. materiaalkosten.**

Vraag aan de penningmeester naar de diverse mogelijkheden, of kijk op onze website: **http://www.computerclubnissewaard.nl**
Bij het beëindigen van het Lidmaatschap, dient u een opzeggingstermijn **van één maand** in acht te nemen **en dit schriftelijk** te melden aan de secretaris: **A v Bronckhorst**
Of Wijkgroep de Akkers Tel: 0181-643249 op Dinsdag en Donderdag.
Hebt u vragen en of opmerkingen, mail ons uw probleem en dan kunnen wij er samen wel uitkomen.
computerclubnissewaard@gmail.com

Voorzitter: Hans Kubbinga	**voorzitter@computerclubnissewaard.nl**
Secretariaat: Arie v Bronckhorst	**secretaris@computerclubnissewaard.nl**
Penningmeester: Bart Tijl	**penningmeester@computerclubnissewaard.nl**
De Computerclub Nissewaard:	**http://www.computerclubnissewaard.nl**

Computerclub Nissewaard de gezelligste club in de regio.
Bij ons krijgt u meer voor minder, vertel dit verder.

Inhoudsopgave

Leuk of niet leuk?

Erasmusbrug gehackt: iedereen kon kleur Rotterdamse brug aanpassen.

Daniel

Het is voor iedereen mogelijk geweest de kleuren van de Erasmusbrug aan te passen. Eén van de digitale toegangspoorten van de bekende Rotterdamse brug heeft, tot 10 nov 2020, ruim een jaar wagenwijd opengestaan.

Dat blijkt uit onderzoek van RTL Nieuws. Het online systeem om de verlichting van de brug te beheren was niet beveiligd met een wachtwoord, waardoor iedereen de kleuren kon aanpassen.

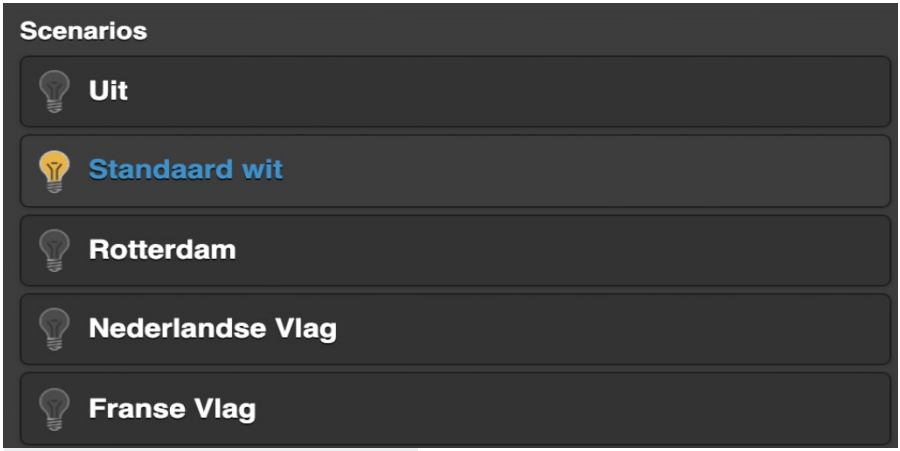
RTL Nieuws heeft de brug 9nov tijdelijk roze laten kleuren en hem daarna de kleuren van de regenboog gegeven.

Op knopjes drukken

Het online systeem voor de verlichting was te bereiken via een ip-adres en een specifieke poort. Als je alleen het ip-adres bezocht, kreeg je een inlogpagina te zien, maar met de juiste poort erachter had je direct toegang.

Het systeem oogt als een mobiele website met knopjes, met aan de bovenkant een foto van de Erasmusbrug. Met de knopjes verander je de kleuren van de brug, volgens het systeem ook wel scenario's genoemd.

Je kunt het standaard witte licht veranderen in onder andere de kleuren rood, groen, oranje, blauw, geel en roze, samen met de kleuren van de Nederlandse vlag, Feyenoord of de regenboog.



Een screenshot van het systeem.

Zodra je op één van de de kleurenscenario's drukt, wordt de verlichting van de Erasmusbrug binnen een seconde aangepast. Dat kan onwenselijke scenario's opleveren, zoals van de brug één grote disco maken door veelvuldig van kleuren te wisselen, of het tonen van de kleuren van de Duitse vlag op Bevrijdingsdag.

Het was via het systeem niet mogelijk de brug open te zetten of de verkeerslichten te bedienen. RTL Nieuws heeft gewacht met publiceren tot de gemeente Rotterdam het lek in het systeem had gedicht.

Topje van ijsberg

"Dit is een duidelijk voorbeeld van een digitaal systeem dat impact heeft op onze fysieke wereld", stelt Dave Maasland, directeur bij cybersecuritybedrijf ESET. "Iemand heeft vanaf zijn computer een directe invloed op de fysieke wereld. En die wereld wordt steeds vaker aangestuurd via digitale systemen waarvan we weten dat ze niet veilig genoeg zijn."

Volgens Maasland is dit nog maar het topje van de ijsberg: "Bijna alle steden zijn bezig met hun zogeheten smart city, maar we moeten begrijpen dat je met al die digitale apparatuur ook nieuwe gevaren creëert. Het lek bij de Erasmusbrug is letterlijk zichtbaar, maar het probleem is veel groter dan we denken. En dit signaal moeten we serieus nemen."

Reactie gemeente Rotterdam

De Erasmusbrug is een icoon van de stad. De sierverlichting van de Erasmusbrug heeft de mogelijkheid (maximaal 30x per jaar) om bij speciale gelegenheden in kleur gezet te worden. Denk aan Koningsdag of de herdenking van het bombardement op 14 mei. Het is daarom mogelijk voor organisaties, bedrijven en bewoners om een aanvraag in te dienen. Aan de hand van een afwegingskader wordt de aanvraag toegekend of afgewezen.

Halverwege 2019 is het bedieningssysteem voor de verlichting aangepast. Het nieuwe systeem biedt de mogelijkheid om de sierverlichting van de Erasmusbrug en Hofpleinfontein aan te passen

en aan en uit te zetten. Helaas is het RTL Nieuws gisteravond gelukt om in te breken in het bedieningssysteem en de verlichting aan te passen.

Uiteraard is het niet de bedoeling dat de sierverlichting door derden kan worden aangepast. We hebben contact met de leverancier van het systeem om te kijken welke aanpassing benodigd is om dit in het vervolg te voorkomen. Tot die tijd is het nieuwe bedieningssysteem buiten gebruik gesteld.

Hofpleinfontein

RTL Nieuws is het online systeem van de Erasmusbrug op het spoor gekomen na een anonieme tip. De persoon had het onbeveiligde systeem gevonden via de website Shodan.io, een zoekmachine voor slimme apparaten. Na het intypen van de zoekterm 'rotterdam' was het verlichtingssysteem één van de eerste resultaten.

Naast de Erasmusbrug is het ook mogelijk de kleuren van de verlichting van de Hofpleinfontein aan te passen (zie screenshot boven). De tipgever heeft dit een keer geprobeerd om te kijken of het mogelijk was, en het lek in het systeem daarna bij RTL Nieuws gemeld.

Hoe zie je of een Tikkie-betaalverzoek veilig is?

Seniorweb

Een betaalverzoek via de app Tikkie is snel en eenvoudig. En veilig. Maar pas wel op voor nep-betaalverzoeken en leer ze herkennen.

Wat is een Tikkie?

Met de app Tikkie vragen gebruikers gemakkelijk geld terug bij anderen. Door in de app een betaalverzoek aan te maken en dit via WhatsApp te delen. Bijvoorbeeld na een etentje met een groep of een uitstapje waarbij iemand (alle) kosten vooruit heeft betaald. 'Stuur maar even een Tikkie', zeggen mensen dan. Een Tikkie is bijzonder handig. Iedereen maakt geld over via iDEAL.

Hoe betrouwbaar is Tikkie?

Tikkie is ontwikkeld door ABN Amro. Betaling verloopt altijd via iDEAL. Dat betekent dat u de betaling altijd afrondt via uw eigen bank. Dat maakt de app Tikkie tot een heel veilige betaalmethode.

Een echt Tikkie herkennen

Helaas is Tikkie ook ontdekt door oplichters. Het is dus opletten geblazen. Gelukkig is het gemakkelijk om een echt betaalverzoek te herkennen. Tikkie gebruikt altijd een link die er zo uitziet:

https://tikkie.me/pay/[code]

Zie het voorbeeld hieronder. Krijgt u een Tikkie let dan op de link. Deze bevat altijd:
- 'https' aan het begin.
- 'tikkie.me/pay/' in de rest van de link.

Oplichters spelen graag met de link. U ziet dan bijvoorbeeld 'tlkkie.nl' in plaats van 'tikkie.me'. Let dus heel goed op de link.

Verwijderde mail terughalen

Seniorweb

Oeps, per ongeluk de verkeerde mail verwijderd? Haal deze met een paar stappen terug in Outlook of Gmail.

Verwijderde mails terughalen

Het is u vast weleens overkomen: u verwijdert een mail die eigenlijk bewaard moet blijven. Gelukkig is dit gemakkelijk recht te zetten. De mail is meestal namelijk nog niet definitief verwijderd. Hij belandt in de map ‘Prullenbak’. Hier blijven verwijderde mails nog een bepaalde periode staan voordat ze écht verdwijnen.

Mail terughalen in Outlook.com

Per ongeluk een mail verwijderd in Outlook.com? Er zijn meerdere manieren om 'm terug te halen. Het snelst is de toetsencombinatie Ctrl+Z. Die werkt als volgt als u in de mailomgeving zit:

-Druk op uw toetsenbord de Ctrl-toets in en houdt vast. Druk op de Z-toets en laat los.

De laatst verwijderde mail wordt teruggezet. Wilt u in één keer meerdere mails terughalen? Volg daarvoor deze stappen in Outlook.com:

-Open de map ‘Verwijderde items’.
-Klik op het bolletje voor iedere mail die moet worden teruggezet.
-Klik op **Herstellen**.

De verwijderde mails staan weer in het Postvak In.

Mail terughalen in Outlook

Ook in het mailprogramma (de app) Outlook is het mogelijk verwijderde mails terug te zetten. Haal één mail terug met de toetsencombinatie Ctrl+Z:

-Druk op uw toetsenbord de Ctrl-toets in en houdt vast. Druk vervolgens op de Z-toets en laat los.

De verwijderde mail wordt teruggezet.

Meerdere mails tegelijk terughalen kan ook:

-Open de map 'Verwijderde items'.
-Houdt de Ctrl-toets ingedrukt en klik tegelijkertijd meerdere mails aan met de muis. Deze mails worden lichtblauw gemarkeerd.
-Klik met de rechtermuisknop op één van de mails.
-Klik op Verplaatsen > Postvak IN.

De verwijderde mails staan weer in het Postvak In.

Mail terugzetten in Gmail

In Gmail is er een snelle manier om verwijderde mails terug te halen:

-Klik op de knop **Ongedaan maken** die in beeld verschijnt nadat u een mail hebt verwijderd.

De mail staat weer in de Inbox.

Oudere mails terugzetten of meerdere mails tegelijk terughalen kan ook. Doe dit als volgt:

-Open de map 'Prullenbak'.
- Klik op het vierkantje voor de mail om deze aan te vinken.
-Klik op de vierkantjes voor meerdere mails, als u in één keer meer verwijderde mails terug wilt zetten.
-Klik op het icoon van het mapje met een pijl erop  .
-Klik op **Inbox**. Eventueel kunt u de mail ook naar een andere map verplaatsen.

Extra beeldscherm toevoegen aan je laptop

Jeroen

Een laptop heeft natuurlijk al een ingebouwd scherm, als je nog een extern beeldscherm hebt staan, zou je die kunnen aansluiten. Met een tweede scherm kun je een stuk beter thuiswerken of gamen. Zo ga je te werk.

Aansluitmogelijkheden

Vrijwel iedere laptop die tegenwoordig van de band rolt, heeft een aansluiting om er een beamer of een beeldscherm aan te hangen. Voor oudere Macbooks heb je standaard een verloopkabeltje nodig, net als voor oudere laptops die bijna altijd beschikken over een vga-, dvi, displayPort of hdmi-aansluiting. Omdat veel laptops minder ruimte hebben voor aansluitingen, beschikken de laptops over een minidisplayport- of mini-hdmi-aansluiting. Deze werken verder hetzelfde.

Er zijn dus een hoop aansluitingen om een tweede scherm aan je laptop (of pc natuurlijk) te koppelen. Er ontbreekt er echter nog een: usb-c.

Het is ironisch, nóg een extra aansluiting met als doel de poortenchaos te versimpelen. De universele aansluiting is echter ook geschikt om je laptop op te laden, data-overdracht, het koppelen van je smartphone

en meer. Bovendien beschikken alle moderne laptops, inclusief Macbooks, over usb-c.

De verschillen tussen beide kabels en aansluitingen zie je in bovenstaande en onderstaande afbeeldingen.

Moderne laptops beschikken meestal over een usb-c-aansluiting.

De DisplayPort aansluiting, welke ook in mini-variant voorkomt.

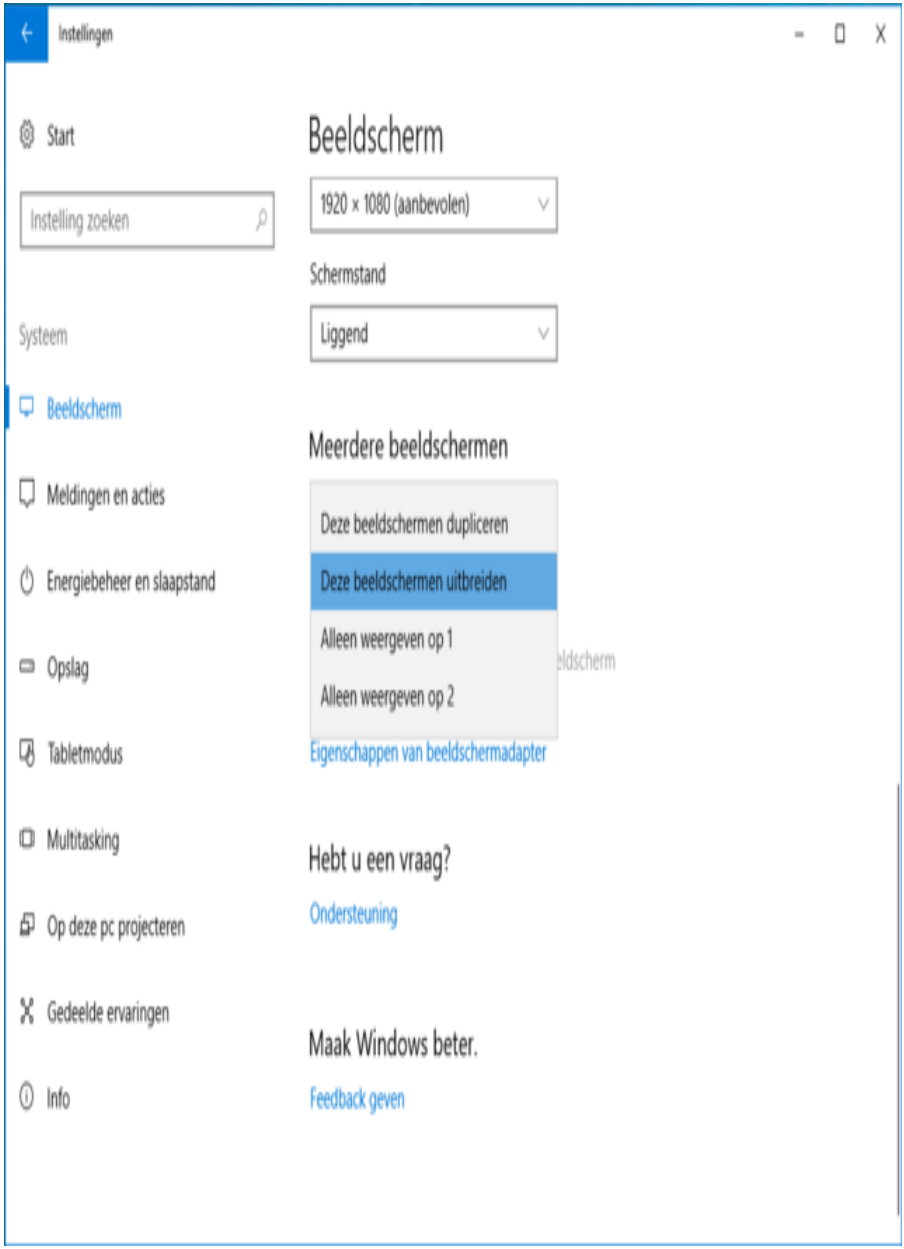
Het beeldscherm aansluiten

Wat je dus nodig hebt om een extern scherm op je laptop aan te sluiten: een vga-kabel of een hdmi-kabel, je laptop en natuurlijk het externe beeldscherm met een hdmi- of vga-poort.

Via hdmi, displayport of usb-c: Het fijne van het aansluiten van een moderne laptop via hdmi is dat de apparaten direct met elkaar gaan 'praten', zonder dat je daar nou echt veel voor hoeft te doen. Sluit je je laptop via hdmi aan op je externe monitor, dan dupliceert Windows standaard je laptop-beeldscherm op de externe monitor. Die instelling kun je nog aanpassen, daarover later meer.

Via vga of dvi: Sluit je de laptop aan via een vga-kabel, dan loopt dat meestal ook wel soepel. Het hangt er wel van af hoe oud je laptop is en welk besturingssysteem er op draait.

Heb je Windows XP of Vista dan moet je via de instellingen nog wat aanpassen, als je Windows 7, Windows 8 of Windows 10 hebt draaien dan dupliceert je scherm vrijwel direct automatisch na het aansluiten.


Instellingen
Start
Instelling zoeken
Systeem
Beeldscherm
Meldingen en acties
Energiebeheer en slaapstand
Opslag
Tabletmodus
Multitasking
Op deze pc projecteren
Gedeelde ervaringen
Info
Beeldscherm
1920 × 1080 (aanbevolen)
Schermstand
Liggend
Meerdere beeldschermen
Deze beeldschermen dupliceren
Deze beeldschermen uitbreiden
Alleen weergeven op 1
Alleen weergeven op 2
Eigenschappen van beeldschermadapter
Hebt u een vraag?
Ondersteuning
Maak Windows beter.
Feedback geven

Via het configuratiescherm kan je instellen hoe je het tweede scherm wilt gebruiken.

Instellingen en toepassingen

Als je een beeldscherm aansluit op je laptop, wordt elk nieuw scherm automatisch door Windows herkend. Er zijn meerdere opties die je kunt kiezen, en het is zeker aan te raden om te kijken wat je zelf het prettigst vindt werken!

Beeldschermen uitbreiden

Hiermee wordt het bureaublad verspreid over beide schermen en kun je items tussen beide schermen heen en weer slepen.

Beeldschermen dupliceren

Hiermee wordt op beide beeldschermen hetzelfde bureaublad weergegeven. Voor een laptop is dit de standaardinstelling. De optie is handig als je een presentatie geeft met je laptop aangesloten op een projector of groot beeldscherm.

Bureaublad op één beeldscherm weergeven

Deze optie wordt meestal gebruikt op een laptop als je het scherm van de laptop leeg wilt houden nadat je een groot beeldscherm hebt aangesloten.

Zo configureer je de firewall van Windows 10

Ronald

Windows 10 beschikt over een ingebouwde firewall, die de grootste ellende buiten de deur moet houden. Waarmee we doelen op hackers die stiekem jouw systeem gekoppeld aan een slecht beveiligde router of openbare hotspot hangt.

Windows 10 beschikt niet alleen direct na de installatie over een ingebouwde virusscanner, maar ook over een al even ingebouwde firewall. Voor gemiddeld gebruik volstaan beide onderdelen, wil je meer controle en (of) een betere bescherming tegen virussen en andere vormen van malware, dan is het verstandig om een commercieel AV-pakket te installeren.

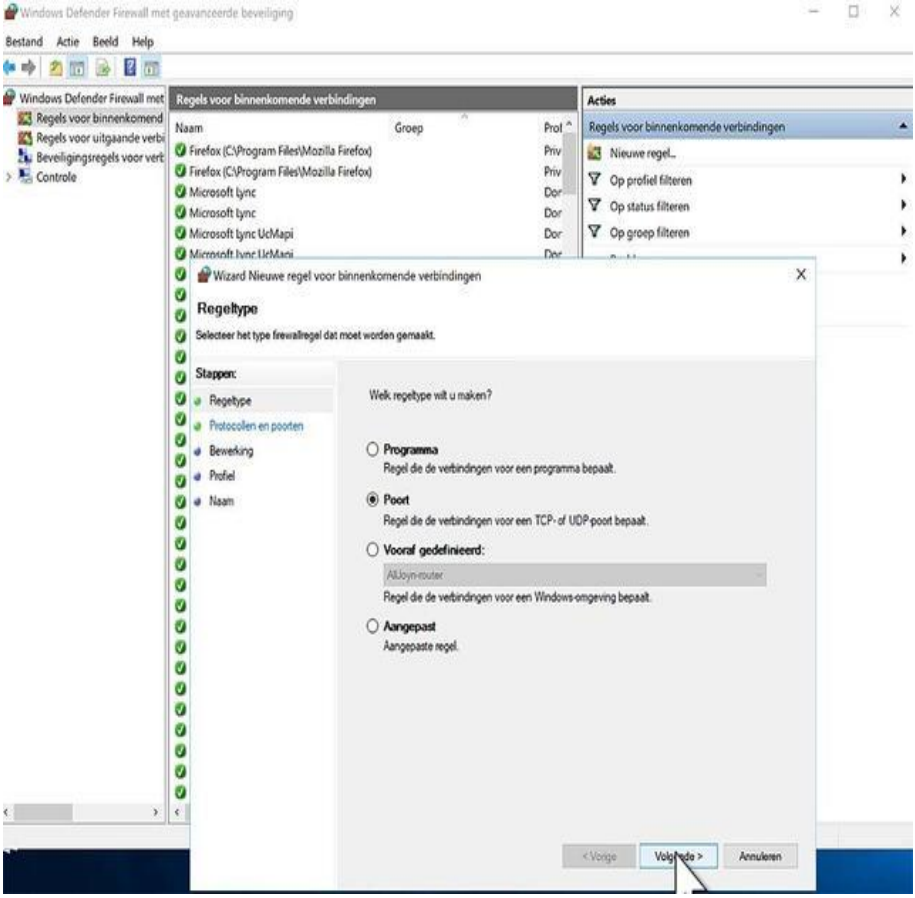
Maar gebruik je de Windows-eigen variant dan ben je inmiddels ook redelijk veilig. De firewall is bovendien behoorlijk configureerbaar! In principe staan de standaardinstellingen goed en heb je er verder geen omkijken naar.

Wel is het zaak om bij koppeling aan een nieuw netwerk dat niet het jouwe is, dit vooral niet als vertrouwd aan te merken als daarom gevraagd wordt. Alleen dan houdt je gespuis echt buiten de deur.

Om eens een kijkje te nemen bij de instellingsmogelijkheden van de Windows firewall, klik je op het Defender-schildje rechtsonder in de systeemwerkbalk. Klik in het geopende venster op Firewall- en netwerkbeveiliging.

Afhankelijk van hoe je netwerk is opgebouwd zie je diverse opties. Een daarvan is actief. Door daarop te klikken kun je tenminste één optie aanzetten: **Alle binnenkomende verbindingen blokkeren, inclusief verbindingen in de lijst met toegestane apps**.

Doe dat alleen in geval van nood, als je het gevoel hebt dat er iemand jouw systeem probeert binnen te dringen. Sommige programma's hebben voor een correcte werking namelijk binnenkomende verbindingen nodig. Maar in geval van nood kan dit een prima blokkeeroptie zijn.



Bepaal app-toestemmingen

Je kunt software in principe blokkeren door eerst (via het pijltje linksboven) weer terug te gaan naar het vorige venster. Klik dan op **Een app toestaan door de firewall**. Klik op de knop **Instellingen wijzigen** en schakel de ongewenste app uit.

Het is niet helemaal helder wat er nu gebeurt, in ons geval bleef bijvoorbeeld het als test uitgeschakelde Firefox gewoon internettoegang houden. In dit geval zou Hitman Pro een oorzaak kunnen zijn, mogelijk 'overruled' dit de Windows firewall.

Overigens geldt dat in geval van een geïnstalleerde internet security suite de Windows firewall sowieso niet meer gebruikt wordt, dus dan heeft het geen enkele zin om de settings daarvan aan te passen! Hoe dan ook, klik na het uitschakelen van een programma op **OK** en in principe zou je er vervolgens niet meer het internet mee op moeten kunnen.

Veel meer mogelijkheden vind je onder **Geavanceerde instellingen**. Hier kun je door links op **Regels voor binnenkomend verkeer** te klikken en dan rechts op **Nieuwe regel**. Selecteer in de eerste stap van de wizard de optie **Poort** en doorloop de rest van de vragen. Op die manier kun je je Windowssysteem bijvoorbeeld opzetten als een webserver die over je hele thuisnetwerk bereikbaar is.

Wil je dat je systeem ook via internet bereikbaar is, dan zul je in je router port forwarding-instellingen moeten activeren. Let echter extreem goed op met het openen van poorten op je systeem: vaak leidt dit tot grote veiligheidsrisico's. Alleen doen dus als je heel precies weet waar je mee bezig bent!

Veilig verstopt browsen met TOR in iOS

Ronald

Lang niet altijd hoeft iedereen te weten waar je vandaan komt tijdens het browsen, of welke sites je bezocht hebt. Daarnaast is er ook nog zoiets als het 'dark web', alleen toegankelijk via een speciale TOR-browser. De iOS-app Onion Browser realiseert alles voor je op het vlak van privacy en dark web.

Onion Browser voor iOS is een browser bedoeld voor een ieder die begaan is met zijn of haar privacy. En veiligheid. De gratis app maakt gebruik van het TOR-netwerk dat het nagenoeg onmogelijk maakt surfende gebruikers te achterhalen.

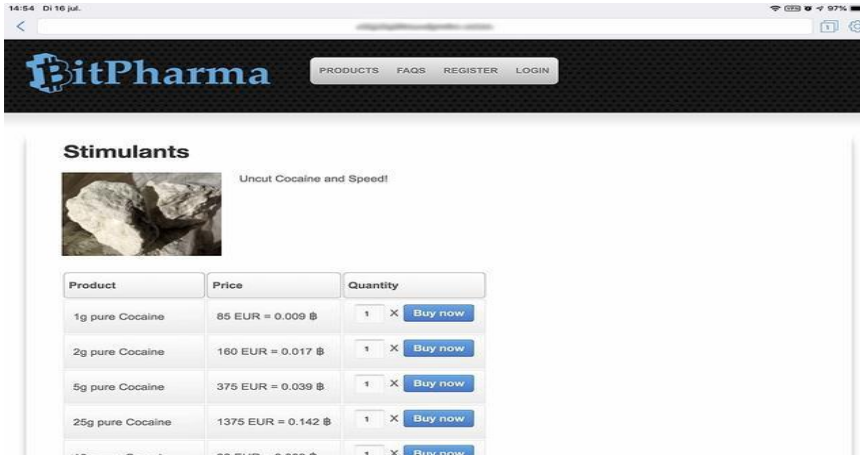
Bovendien is het geheel zo ingesteld dat allerlei riskante extraatjes van het web niet werken. Je zult dus zien dat behoorlijk wat sites ietwat uitgekleder ogen. Dat is de prijs die je betaalt voor privacy. Javascripts en dergelijke zorgen voor risico's op dat vlak en werken dus niet of niet goed.

Daarnaast is het browsen via deze browser duidelijk wat trager dan gewoon. Dat ligt niet aan de app zelf, maar aan het achterliggende netwerk. Daarmee is het voor de gemiddelde mens geen browser die je dagelijks voor al je avonturen op het web gebruikt.

Maar wel eentje die bijvoorbeeld ook op vakantie goed van pas kan komen. Bijvoorbeeld als je - tegen alle wijze raad in - toch ergens aanhaakt bij een openbare hotspot en je wilt voorkomen dat een kwaadwillende meeleest.

Het gebruik van Onion Browser is een eitje; het werkt net zoals elke andere browser. Tik het adres in de adresbalk en gaan. Ook kun je hier een zoekterm invoeren. Er wordt gebruik gemaakt van DuckDuckGo, een zoekmachine die veel gebruik maakt van ándere zoekmachines en de resultaten daarvan bundelt.

Ook heeft het een eigen search bot, wat samen een prima bruikbaar geheel oplevert. Belangrijkste feature echter is, dat zoeken hier volledig anoniem gebeurt. Google & co kunnen je zoekgedrag dus niet volgen en koppelen aan bijvoorbeeld je IP-adres. Altijd een prettige gedachte.



Je kunt de Onion Browser gebruiken voor het 'darkweb'.

Dark web

Dan is er nog dat mysterieuze **dark web**. Via een normale browser is dat niet toegankelijk, maar via het TOR-netwerk weer wel. Een deel van de sites op het dark web is gewoon bedoeld voor een ieder die net wat meer om privacy geeft dan de rest.

Helaas tref je er ook veel 'ellende' aan. Zo bestel je er moeiteloos harddrugs, een nieuwe Kalasjnikov of een donororgaan. We adviseren je om vooral niet in zee te gaan met dergelijke criminele websites en je ook verre te houden van fora met meer duistere onderwerpen.

Al was het maar omdat ook politie en dergelijke geïnfiltreerd is op het netwerk. Even voor de lol een pilletje bestellen kan dan onder de streep vervelende gevolgen krijgen.

Hoe dan ook, om het dark web te betreden kun je het best gebruik maken van een van de standaard bookmarks in Onion Browser. Kwestie van even op de adresbalk klikken en daar een van de bladwijzers gebruiken.

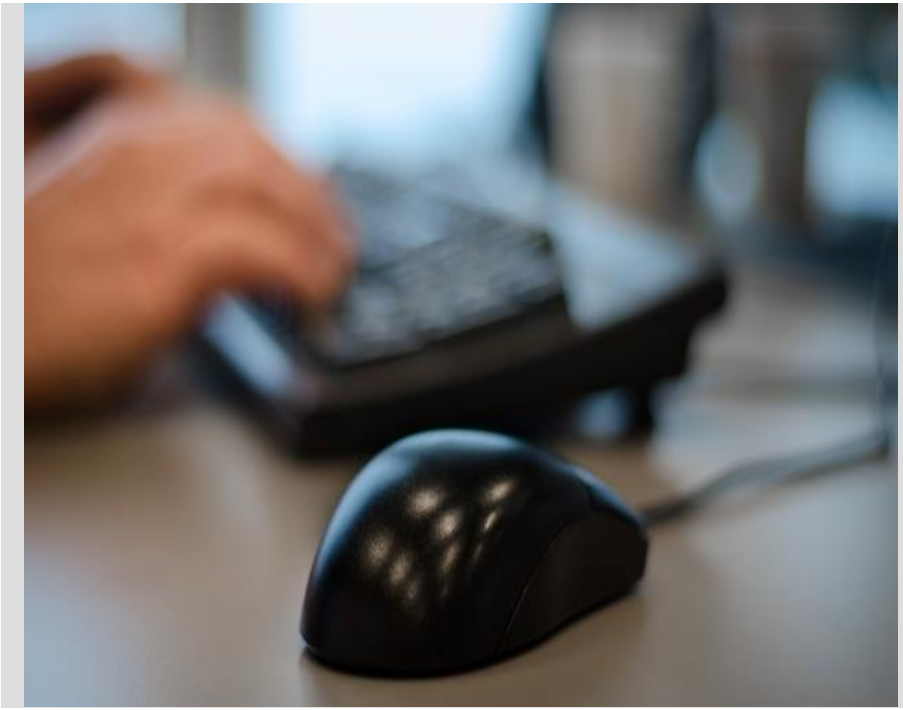
Ook kun je zoeken naar darkweb-sites via DuckDuckGo. Een complete handleiding voor dat soort meer illegale activiteiten gaan we hier vanzelfsprekend niet geven.

Onion Browser is wat ons betreft vooral interessant vanwege de extra privacy die het biedt. Dat komt prima van pas op vakantie, maar ook gewoon thuis of op het werk als je sites bezoekt die je niet helemaal vertrouwt bijvoorbeeld.

Wil je extreem voorzichtig zijn, gebruik dan naast deze browser ook een **VPN-server.**

Wat is VPN en waarom heb je het nodig?

Jeroen



Wellicht heb je weleens van VPN gehoord en als dat niet het geval is dan moet je zeker doorlezen. Want ook als je niet geregeld films of muziek downloadt, kan een VPN belangrijk voor je zijn. Wij beantwoorden de tien belangrijkste vragen over VPN.

Wat is VPN?

VPN staat voor Virtual Private Network en kun je zien als een privénetwerk binnen een groter netwerk. Meestal gaat het om een versleutelde verbinding tussen twee andere netwerken via openbare netwerken (internet).

Denk aan je thuisnetwerk en het bedrijfsnetwerk van je werkgever. VPN helpt je om een soort privétunnel of -pijplijn tussen die twee netwerken te maken.

Waarom moet je VPN gebruiken?

Groot voordeel van VPN: geen pottenkijkers. Doordat de verbinding is versleuteld, kan iemand die ook toegang heeft tot datzelfde netwerk jouw VPN-verbinding toch niet afluisteren. Denk aan een hotel, trein, restaurant of een andere plek met open wifi. Dankzij VPN zien sniffers (afluisteraars) geen zinnige informatie voorbijkomen. Wel zo prettig als je je bankzaken of andere privédingen regelt.

Wanneer moet je VPN gebruiken?

Van oudsher wordt VPN gebruikt in zakelijke omgevingen om werknemers overal ter wereld toch toegang tot het bedrijfsnetwerk te geven. De laatste maanden/jaren wordt VPN ook interessant voor particulieren. Zeker waar de overheid en andere diensten steeds meer meegluren met wat je op internet aan het doen bent.

Daarnaast kunnen bepaalde diensten je niet zo makkelijk blokkeren als je uit een bepaald (voor hen ongewenst) land komt, omdat je met een VPN-dienst het kan laten lijken dat je uit een ander (wel gewenst) land komt.

ik echt anoniem met VPN?

Nee, echt anoniem op internet ben je nooit. Je internetprovider weet met wie je contact maakt, bijvoorbeeld je VPN-dienst. Je VPN-dienst weet wel wat je doet, maar houdt daar normaal gesproken geen

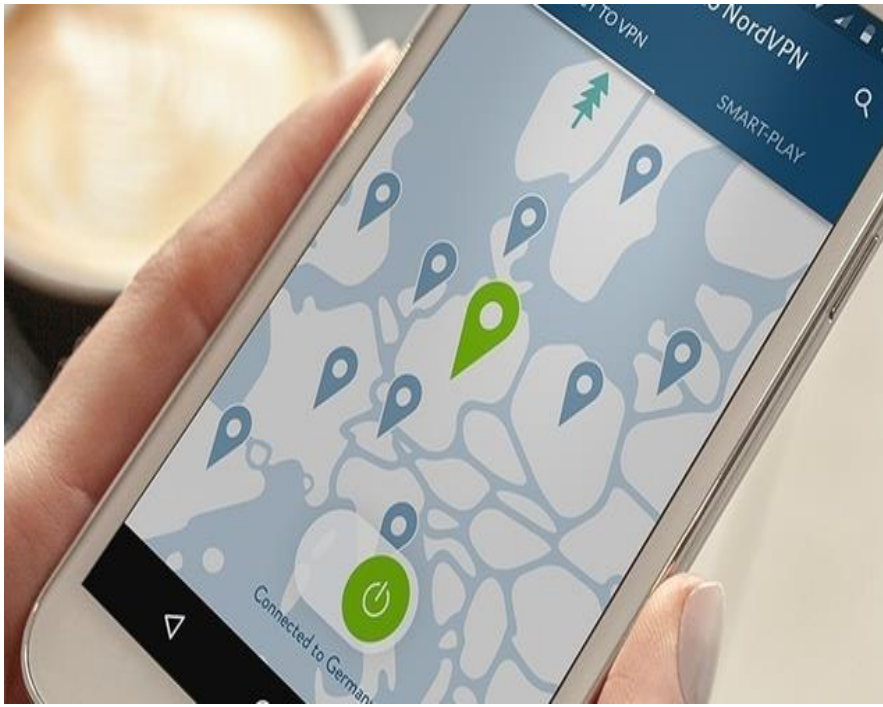
logs van bij. Toch hoeft er maar iemand een tap te plaatsen en je bent gezien.

Gelukkig kan dat niet zomaar, dat is zelfs voor een overheid, geheime dienst of andere kwaadwillige geen koud kunstje.

Welke VPN-protocol kan ik het beste gebruiken?

De meest gebruikte protocollen zijn PPTP, L2TP/IPsec en OpenVPN. De meeste VPN-diensten en VPN-software ondersteunen deze drie protocollen. PPTP is de minst veilige en is relatief eenvoudig te kraken.

Niet gebruiken dus! Het beste en snelste is OpenVPN, maar niet elk apparaat ondersteunt dat. Mocht je OpenVPN niet aan de praat krijgen, kies dan voor L2TP/IPsec.



Er zijn verschillende gratis en betaalde VPN-diensten beschikbaar.

Thuis of extern?

Wil je vooral voorkomen dat niemand je internet gebruik kan zien als je onderweg bent? Dan kun je prima een VPN-verbinding met je thuisnetwerk opzetten. Dit kan via je **router** of **NAS**, of via een computer thuis die je altijd aan laat staan.

Hiermee loopt al het internetverkeer op je smartphone via je internetverbinding thuis en kun je veilig op openbare wifi-netwerken je gang gaan. Zorg wel dat je een snelle internetverbinding thuis hebt, liefst via de kabel of glasvezel. Wil je ook thuis voorkomen dat men weet wat je online doet, maak dan gebruik van een VPN-dienst.

Een betaalde of gratis VPN?

Gratis VPN-diensten hebben beperkingen op snelheid, hoeveelheid data, aantal verbindingen of een combinatie hiervan. Wil je alleen veilig je mail op je smartphone of tablet checken als je niet thuis bent, dan biedt bijvoorbeeld **TunnelBear** een gratis abonnement aan waarmee je 500 megabyte per maand kunt verbruiken. Wil je meer, dan moet je gaan betalen.

Wat zijn de beste VPN-diensten?

De prestaties van en verschillen tussen VPN-diensten zijn echter erg wisselend. Ook is dat erg afhankelijk van de locatie, de snelheid van de internetverbinding die wordt gebruikt en de rekenkracht van de gebruikte apparatuur.

Daarnaast is het lastig te achterhalen of de VPN-diensten geen privégegevens doorspelen. Zelf hebben we tevens goede ervaringen met **VyprVPN**, **Private Internet Access (PIA)** en **NordVPN**.

Hoe zit het met mijn snelheid?

Gebruik je VPN, dan gaat dat altijd ten koste van je snelheid. Je aanvraag voor een bepaalde webpagina of andere internetinfo gaat niet meer direct naar die webserver, maar eerst naar de server van je VPN-dienst, dan naar die webserver, weer terug naar je VPN-dienst en dan weer naar jou. En dat gaat continu zo door.

Heb je een snelle kabel- of glasvezelverbinding, dan hoef je er amper wat van te merken. Daarnaast heb je de extra rekenkracht die de versleuteling vraagt. Voor een dikke pc geen probleem, maar op sommige mobiele apparaten merk je er wel wat van.

Ben je gamer, dan is een lage ping heel belangrijk en daar zijn de extra tussenstappen van een VPN-dienst niet bevorderlijk voor. In alle gevallen: test eerst of de VPN-dienst snel genoeg voor je is. Veel diensten bieden proefpakketten.

Zijn er alternatieven voor VPN?

Veelgenoemde alternatieven voor VPN zijn **TOR** en **een anonieme proxy**. Die laatste wordt gebruikt om regiogebonden content van bijvoorbeeld Netflix, Hulu, BBC iPlayer en Uitzending Gemist toch op een andere plek te kunnen bekijken.

Veel anonieme proxy's doen alleen niets voor jouw privacy, sterker nog, ze delen deze gegevens met anderen.

Bij **TOR,** een netwerk waarop je anoniem kunt surfen, is je privacy in principe wel goed geregeld, maar ook hier zijn er weleens 'infiltranten' en is de snelheid vaak een zwak punt.

Makkelijk overstappen in het ov met Google Maps-app

Seniorweb

Wie een route met het **OV** plant via Google Maps, krijgt straks via Live View te zien waar de overstap zich bevindt.

De app van Google Maps helpt gebruikers de weg te vinden. Via Live View krijg je precies te zien welke kant je op moet lopen. Er verschijnen pijlen in beeld die aangeven welke straat iemand in moet en hoe die straat heet.

Overstap in Maps

Live view wordt binnenkort ook beschikbaar voor mensen die routes plannen met het openbaar vervoer. Zo kunnen reizigers bijvoorbeeld zien waar hun bushalte zich precies bevindt of welke halte ze moeten hebben. De gebruiker tikt bij een overstap direct op 'Live View' en wandelt zo moeiteloos naar de juiste halte.

Makkelijk de weg vinden met Google Maps Live View

Handig dat Google Maps, maar welke kant moet ik nou op? Google Maps Live View helpt met virtuele richtingaanwijzers bij het vinden van de juiste looproute.

De goede kant op

We hebben het allemaal weleens gehad: de routekaart staat op de telefoon. Maar na enkele meters lopen, blijkt u toch precies de verkeerde kant te zijn opgelopen. Zou het niet handiger zijn als er herkenningspunten in beeld verschenen tijdens het volgen van een routebeschrijving?

Dat is precies wat Live View doet. De nieuwe functie projecteert virtuele witte pijlen in Street View, zodat u geen afslag mist of de verkeerde kant opgaat.
Mocht de functie niet beschikbaar zijn, download dan de laatste versie van Google Maps. Zorg dat de Google-locatieservice van het apparaat aanstaat.

Wandelen met Live View
- Open Google Maps op de telefoon of tablet.
- Typ een bestemming in de zoekbalk of tik op de kaart.
- Tik op **Route**.
- Tik boven de kaart op het pictogram 'Lopen'. Dat is het wandelende poppetje.
- Tik onderaan op **Live weergave**.
- Google Maps vraagt eventueel om wat toestemmingen. De app wil bijvoorbeeld de camera gebruiken om de buurt te herkennen.
- Richt de telefooncamera op gebouwen en borden zodat Maps weet waar u bent.

Er verschijnen witte pijlen op het scherm. Dat is de route die u kunt volgen. De telefoon trilt bij elke volgende navigatiestap of op de eindbestemming. Het is trouwens veiliger om niet steeds op het scherm te kijken. Berg de telefoon op zodra u weet welke kant u op moet en haal 'm weer tevoorschijn als u bij een volgende afslag komt. Zo houdt u aandacht voor het verkeer.

Hier kan ook Uw advertentie komen als U donateur van ons wordt.

Inlichtingen: tel: 0181-641381

Of: 06-54692942

computerclubnissewaard@gmail.com

secretaris@computerclubnissewaard.nl

http://www.computerclubnissewaard.nl