FLANDERS COMPUTER CLUB VZW

FLANDERS NIEUWSFLASH BULLETIN

WERKJAAR 37 - EDITIE: JUNI 2022

Flanders Nieuwsflash Bulletin brengt maandelijks een overzicht van de artikels die verschenen zijn op onze website als Flanders Nieuwsflash Express. Bezoek onze website voor de meest recente artikels.
www.flanderscomputerclub.be

WINDOWS 11 – 27/06/2022
22H2 - DE EERSTE GROTE JAARLIJKSE UPDATE

Windows 11 heeft al heel wat veranderingen ondergaan sinds zijn lancering. Zoals de nieuwe updatestrategie het bepaalt, heeft Microsoft reeds doorlopend een stroom van opnieuw ontworpen app-updates, bugfixes en verbeteringen aan de gebruikersinterface uitgebracht.
Desondanks zijn de grote jaarlijkse Windows-updates nog steeds heel belangrijk. Het is hier dat Microsoft de belangrijkste wijzigingen aanbrengt in de look en feel van Windows 11 en de functies onder de motorkap. Microsoft heeft bevestigd dat de build, die momenteel beschikbaar is voor het Windows Insider Beta-kanaal onder het buildnummer 22621.1, zal dienen als basis voor versie 22H2.
We geven hier een overzicht van Windows 11 22H2 zoals het momenteel bestaat. Tegen het moment van lancering voor het grote publiek kunnen er nog extra aanpassingen gebeurd zijn.

Verplichte aanmelding bij Microsoft-account
Je hebt ook een Microsoft-account nodig om toekomstige versies van Windows 11 Pro te installeren. Dit was reeds zo voor de Home-editie.
Dus voor alle versies is een internetverbinding en een aanmelding verplicht.

Deze manier van werken heeft natuurlijk ook voordelen, waaronder een geautomatiseerde lokale schijfversleuteling en back-up van herstelsleutels, inloggen zonder wachtwoord, snelle toegang tot Microsoft Store-apps en tot services zoals Microsoft 365 en PC Game Pass en gegevenssynchronisatie voor apps zoals OneDrive en Edge.
Als je later wil inloggen met een lokaal account, dan is de enige oplossing: een nieuw lokaal account aanmaken als u eenmaal bij het bureaublad bent geraakt.
De enige uitzondering is wanneer u tijdens de installatie de optie "werk of school" kiest in plaats van de optie "persoonlijk gebruik". In dat geval kan je inloggen met het Microsoft-account van uw werk of school.
Dit beleid is alleen van toepassing op nieuwe Windows-installaties en heeft geen invloed bij een upgrade van een bestaande installatie.

Nieuwe beveiligingsfunctie
De basisbeveiligingsvereisten van Microsoft voor Windows 11 veranderen niet: Secure Boot, TPM 2.0 en een ondersteunde processor zijn alles wat u nodig hebt om de compatibiliteitscontroles te doorstaan. Voor systemen die niet aan deze vereisten voldoen, kan je deze controles nog steeds op dezelfde manier omzeilen .
Maar Microsoft voegt ten minste één nieuwe beveiligingsfunctie toe: ***Smart App Control***. Deze plaatst een extra laag bovenop de SmartScreen-functie die u probeert te waarschuwen wanneer je een potentieel schadelijke app wil uitvoeren.
Microsoft gebruikt hiervoor een “AI-model voor applicatievertrouwen". Het gedrag van een nieuw uit te voeren app wordt vergeleken met dit model en als de app gedrag vertoont dat door het model als kwaadaardig wordt geïnterpreteerd, blokkeert Windows de uitvoering.

Een nieuwe Taakbeheer en Efficiency-modus voor apps
Versie 22H2 bevat de grootste update van Taakbeheer sinds deze opnieuw is ontworpen voor Windows 8.
De nieuwe Taakmanager heeft een lay-out die meer in lijn is met de instellingen of de Windows-beveiligingsapps, met verticaal uitgelijnde navigatiepictogrammen aan de linkerkant in plaats van horizontale tabbladen met tekst.
De Taakmanager ondersteunt ook de donkere modus en zal de door u gekozen accentkleuren gebruiken bij het markeren van gebruikte app-bronnen.
Een nieuwe functie-update van Taakbeheer is de mogelijkheid om de efficiëntiemodus voor processen te activeren. Deze modus is bedoeld om energie te besparen door de prioriteit te verlagen en het gebruik van hulpbronnen voor specifieke taken te verminderen.
Apps kunnen ervoor kiezen zichzelf in de efficiëntiemodus te zetten wanneer ze dit ondersteunen (*Microsoft Edge zou reeds aangepast zijn*). Maar de gebruiker kan ook handmatig de efficiëntiemodus activeren voor specifieke processen. Microsoft waarschuwt in dit laatste geval dat het inschakelen van de efficiëntiemodus, instabiliteit voor bepaalde processen kan veroorzaken.

Vernieuwde touchscreen-bewegingen en tweaks voor vensterbeheer
Er zijn een paar nieuwe veegbewegingen, die worden uitgelegd in een zelfstudie wanneer u een laptop voor het eerst in tabletmodus zet:

- veeg omhoog vanaf middenonder op het scherm om het ***menu Start*** te zien
- veeg omhoog vanaf rechtsonder om ***Snelle acties*** te zien
- veeg vanaf de linkerkant naar binnen om het ***Widgets-menu*** te zien
- veeg vanaf de rechterkant naar binnen om het ***Meldingscentrum*** te zien
- veeg met drie vingers naar links of rechts over het scherm om heen en weer te schakelen tussen uw twee meest recent gebruikte apps.

Er zijn ook enkele verbeteringen voor het klikken op vensters voor zowel touchscreen- als muis-en-toetsenbordgebruikers.

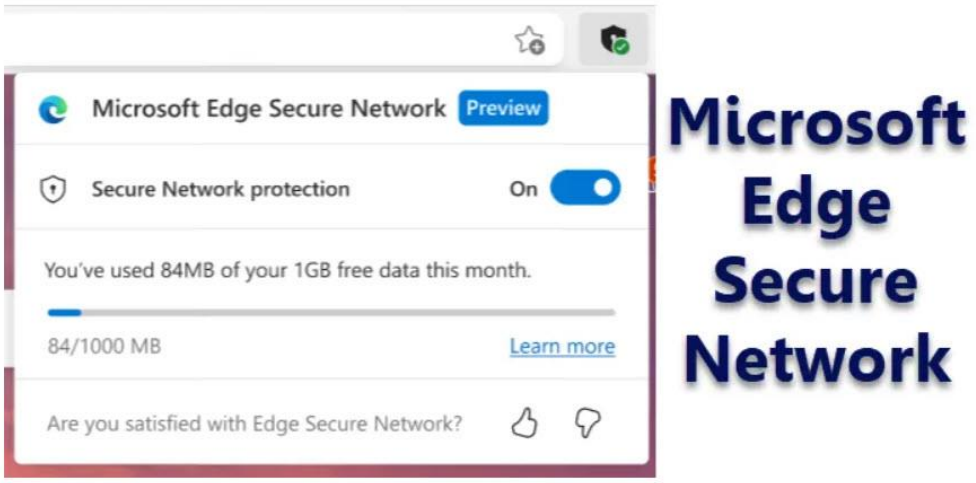
Verbeteringen in het startmenu, maar de taakbalk is vergeten
Het Start-menu kan nu vastgezette apps in mappen plaatsen om ruimte te besparen. Je kan er voortaan via de instellingen ook voor kiezen om een groter aantal apps of een groter aantal aanbevelingen te zien.

De taakbalk, aan de andere kant, heeft heel weinig veranderingen ondergaan. De beloofde aanpassing om zoals in Windows 10 bestanden in een app te openen of te plaatsen door ze naar hun taakbalkpictogram te slepen is nog steeds niet aanwezig!
Wil je de pictogramgrootte of de hoogte van de taakbalk wijzigen buiten de geautomatiseerde wijzigingen die plaatsvinden wanneer u zich in de tabletmodus bevindt? Dat kan nog steeds niet.
Wil je de taakbalk aan de linker- of rechterkant van uw scherm plaatsen? Ook een nee!

(Geraadpleegde bron: ArsTechnica)

BEVEILIGING – 14/06/2022
MICROSOFT INTRODUCEERT VPN-SERVICE VOOR EDGE

Microsoft is van plan om gebruikers van hun Edge-browser in de nabije toekomst te voorzien van een ingebouwde **VPN** (***Virtual Private Network***) om zo op een beveiligde manier gegevens te downloaden of te streamen. Microsoft stelt dit nieuwe project voor als **Secure Network-feature**. Eigenlijk komt het erop neer dat het tracken van gebruikers wordt voorkomen door middel van encryptie.



Mircosoft zou hiervoor gaan samenwerken met het bedrijf **Cloudflare**. Gebruikers zouden de beschikking krijgen over 1GB gratis beveiligd dataverkeer per maand. Hiervoor moet je als gebruiker wel inloggen met je Microsoft-account, aangezien het de browser is die bijhoudt hoeveel data er verbruikt is. Er is nog niet bekend of het mogelijk is extra data aan te schaffen. Vermoedelijk zal dat wel mogelijk worden maar moet hiervoor de prijs nog bepaald worden.
Wanneer dit aan Edge wordt toegevoegd is nog niet bekend, maar aangezien Microsoft hiervoor al een supportpagina heeft opgezet, zal dit vermoedelijk niet lang op zich laten wachten.

(Geraadpleegde bron: HardwareInfo)

SNELCURSUS → BEVEILIGING – 04/06/2022
HET WAT EN HOE VAN VPN

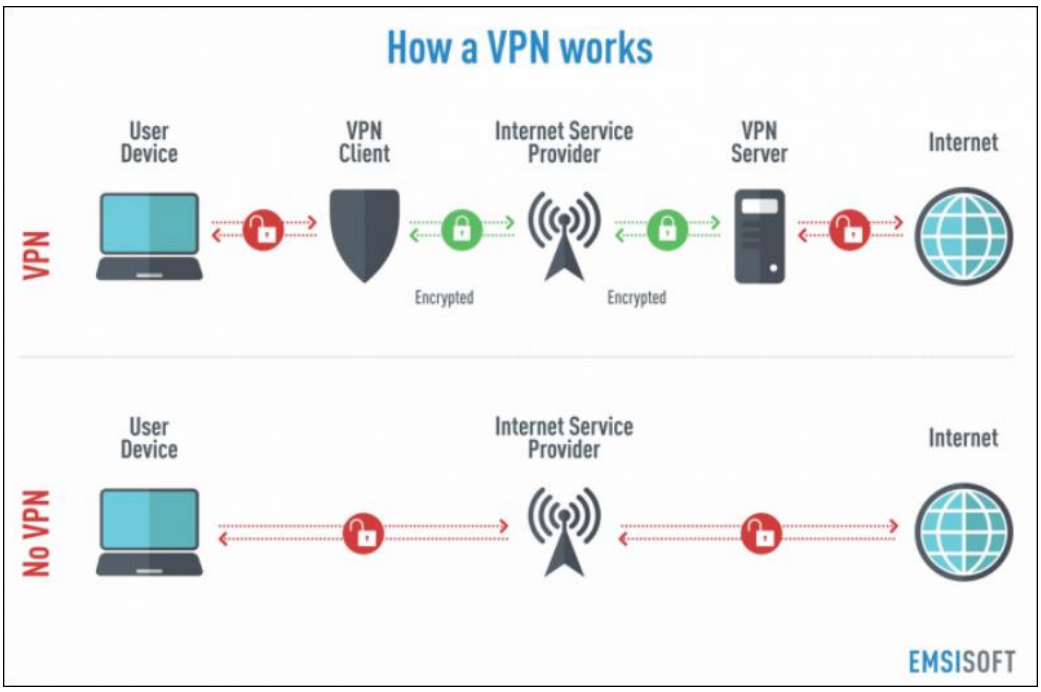
In deze tijden van hacking en tracking maken steeds meer mensen gebruik van VPN. Mogelijk ben ook jij als internetgebruiker nieuwsgierig naar wat deze services voor jou zouden kunnen doen.

Wat is VPN?
VPN staat voor ***Virtual Private Network*** (*Virtueel Privaat Netwerk*). Het is eigenlijk een virtuele tunnel met een versleutelde verbinding tussen jou en je bestemmeling. Noch uw provider, noch de sites die je bezoekt kunnen zien wat je aan het doen bent omdat alle transport gecodeerd is. Het kraken van die codering is in de praktijk zo goed als onmogelijk.
Dat is natuurlijk de eenvoudige uitleg. In werkelijkheid is het wat ingewikkelder. Daarvoor moeten we wat dieper ingaan op de werking van het internet.
Wanneer je een internetsite bezoekt dan maak je een verbinding tussen jouw toestel en je provider (*ook ISP genoemd*). Uw provider stuurt het signaal vervolgens door naar de site die je bezoekt. Dus eigenlijk kunnen zowel uw provider als de site waar je naar toe gaat bijhouden hoe u zich op internet gedraagt.
Een VPN-dienst gaat dit trachten te voorkomen op twee manieren.

Eerst en vooral gaat uw aanvraag niet rechtstreeks doorgezonden worden naar uw provider maar naar één van de eigen servers van de VPN-dienst. Hierdoor verandert uw IP-adres in dat van de server van die VPN-dienst, waardoor het lijkt alsof u zich op een andere locatie bevindt. Door dit te doen wordt het moeilijker om je in de gaten te houden. Een tweede voordeel is dat

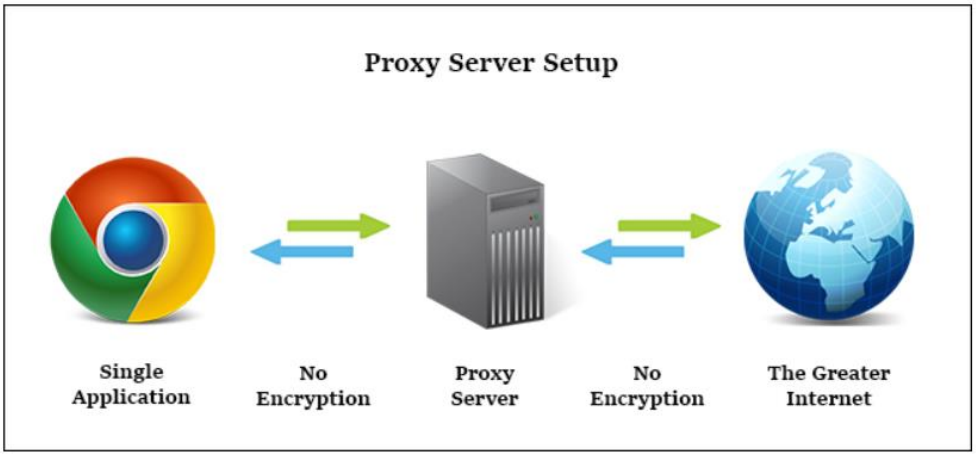
je ook de regionale beperkingen kan omzeilen omdat de VPN-diensten samenwerken met servers in verschillende landen en continenten.
Dit lijkt allemaal nogal ingewikkeld. Daarom deze handige manier om een VPN-tunnel te visualiseren.
Doe even alsof je in een auto rijdt. Zolang je op de openbare weg rijdt, kan iedereen je zien. Maar op het moment dat je een tunnel in rijdt, wordt het een stuk moeilijker. Als die tunnel bovendien ook nog bewakers heeft staan aan elk uiteinde dan wordt de vergelijking met een VPN-tunnel volledig.

De tweede manier die een VPN-dienst gebruikt om jou als individu te beschermen is het coderen van alle over te brengen data.
Als je een verbinding maakt via een VPN-dienst, dan is alles wat iedereen van uw activiteit kan zien een willekeurig gekrabbel.
Om je verbinding te versleutelen wordt gebruik gemaakt van een zogenaamd protocol. Dit is een soort overeenkomst tussen twee machines over hoe ze met elkaar kunnen 'praten' met behulp van specifieke regels.
In het geval van een VPN-protocol moet er rekening gehouden worden met regels zoals het type van encryptie dat wordt gebruikt en ook via welke netwerkpoorten het verkeer moet worden omgeleid.
De meest voorkomende vorm van encryptie op dit ogenblik is **AES**.
AES bestaat in twee versies, een 128-bits en 256-bits. Theoretisch geeft de 256-bits de beste bescherming, maar in de praktijk blijkt er niet veel verschil te zijn als het om de beveiliging gaat. Beide varianten hebben duizenden (sommige beweren miljoenen tot miljarden) jaren nodig om te kraken.
Het type protocol dat wordt gebruikt heeft vooral invloed op de snelheid. Als gebruiker van een VPN-dienst moet je er vooral op letten dat de VPN-provider van uw keuze werkt met het **OpenVPN**-protocol. Dit protocol is in de meeste situaties de beste keuze voor de meeste mensen.
Ook moet je er van uit gaan dat betalende VPN-diensten een hogere snelheid garanderen dan de gratis diensten.



Heb je een VPN eigenlijk wel nodig?
Dit is natuurlijk een vraag die ieder voor zichzelf moet beantwoorden.

Een VPN-dienst is niet de enige mogelijkheid om je verbinding om te leiden. Het kan ook via **proxy's** zoals ***Tor***.
VPN's en proxy's hebben één ding gemeen: bij allebei lijkt het alsof je vanaf een andere locatie verbinding maakt met het internet.
Maar proxyservers verbergen alleen uw IP-adres. Ze versleutelen het internetverkeer tussen uw computer en de proxyserver niet. Er zijn dus geen extra privacy- of beveiligingsoverwegingen ingebouwd.



Dan bestaat er ook nog in elke browser de mogelijkheid om te surfen in **incognitomodus**. Ook deze zorgt voor een zekere anonimiteit.
Hoewel incognitomodus samen met gezond verstand en een aantal voorzorgsmaatregelen zoals het niet klikken op verdachte links, zeer nuttig is, zal een goede VPN-service je veel beter beschermen tegen bewaking en andere vormen van inbraak.

(FVG)

Secretariaat
p/a
Moretuslei 3
B-2180 Ekeren

Informatie
Per post: via secretariaat
Per telefoon: 0032 3 2895573
Per e-mail: info@flanderscomputerclub.be

Lidgelden
60 EUR voor 1 jaar
IBAN: BE23 9731 6510 9491
BIC: ARSPBE22

Redactie: Frank Van Goolen