Flanders Computer Club

Flanders Nieuwsflash Bulletin

Werk jaar 38 – Editie: Januari 2023

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

FREEWARE – 25/01/2023

PDF24 TOOLS – GRATIS EN MET VEEL FUNCTIONALITEIT

Het pdf-formaat moeten we niet meer voorstellen. Alle gebruikers hebben ondertussen wel software op hun computer staan om pdf-bestanden te lezen. Iedereen kan ondertussen ook zelf pdf-bestanden maken met de in Windows aanwezige pdf-printer. Vind je die te beperkt dan zijn er tal van pdf-printers te vinden op het internet.
Maar je kan heel wat meer doen met pdf-bestanden. Daar heb je dan weer andere tooltjes voor nodig.
PDF24 Tools kan hierbij helpen.
PDF24 is een verzameling van tools voor het oplossen van pdf-gerelateerde problemen en dit in een installeerbare app voor Windows.
Het is de ultieme gereedschapskist als het om pdf gaat.
Even ter info:
Het getal 24 komt voort uit het feit dat de eerste versies van het programma 24 verschillende componenten bevatten, maar inmiddels zijn het er al ruim dertig.
Je kan de toepassing gebruiken om elk afdrukbaar bestand naar pdf te converteren, om pdf's samen te voegen of te splitsen, om pagina's te extraheren (*eruit halen*), te verplaatsen, te verwijderen en te roteren. Je kan pdf's beschermen en ontgrendelen. Je kan ze comprimeren, watermerken en paginanummers toevoegen.
Je kan ook **pdf/X**-bestanden aanmaken. De X staat voor *Blind Exchange*. Dit wil zeggen dat een drukkerij jouw bestand blindelings kan verwerken omdat het voldoet aan een afgesproken standaard.
Ook het aanmaken van **pdf/A**-bestanden is mogelijk. Pdf/A (*Portable Document Format Archivable*), ook bekend als ISO 19005-1, is een speciale variant van het gewone PDF-formaat die specifiek ontwikkeld is voor de archivering van digitale documenten.
Er is bovendien ook nog een volledig uitgeruste en lichtgewicht pdf-lezer aanwezig.
Alle aanwezige tools zijn offline te gebruiken en volledig gratis.

In onze programmabibliotheek vind je het programma samen met de nodige info.
U kan het programma ook zelf downloaden via onderstaande link.
https://tools.pdf24.org/nl/

(FVG)

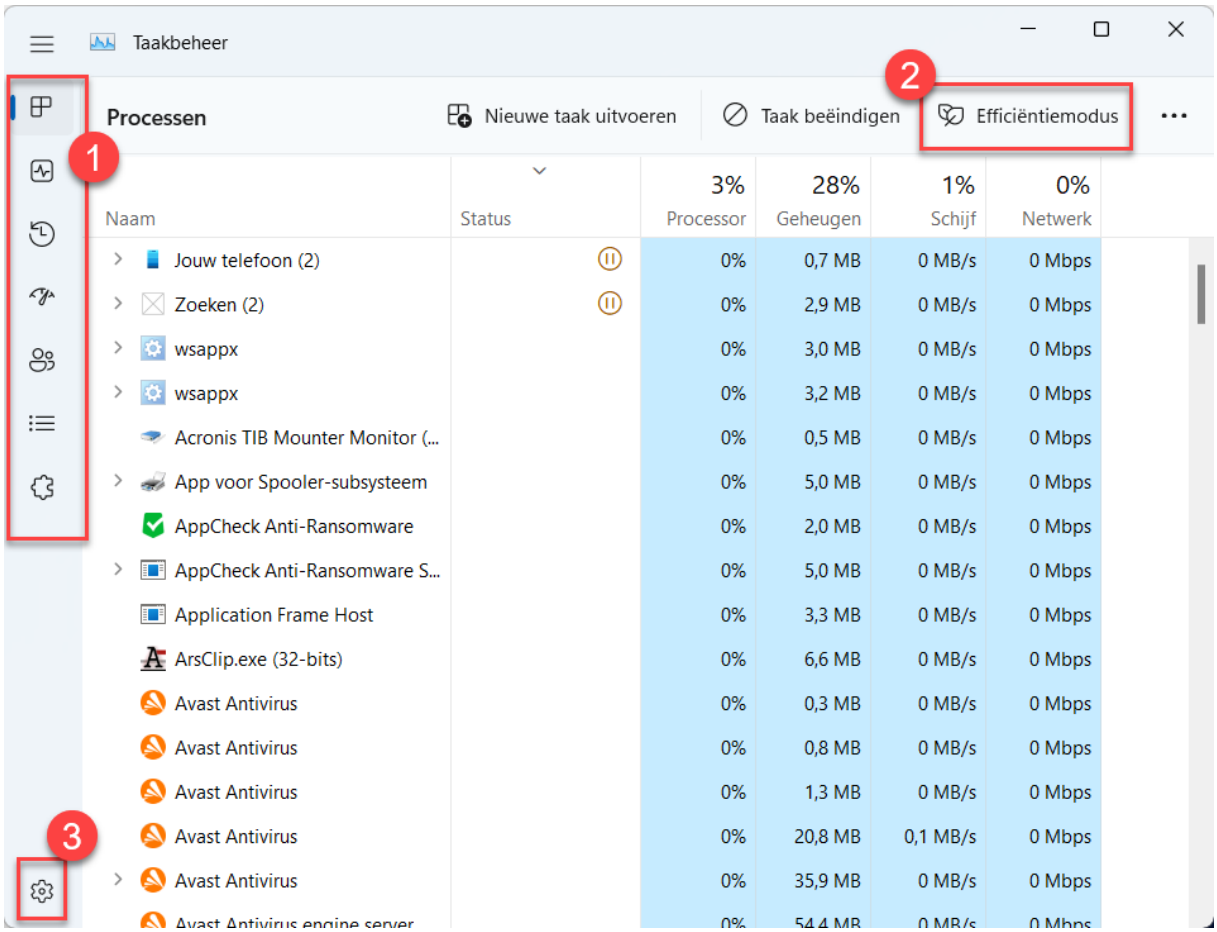
WINDOWS 11 – 19/01/2023
NIEUW TAAKBEHEER

Met de laatste grote Windows 11 update (*22H2*) heeft Microsoft de Taakbeheer-toepassing grondig onder handen genomen. Maar waarvoor dient Taakbeheer?
Kort samengevat geeft het een overzicht van alle geopende programma's. Als één van die programma's niet goed werkt of is vastgelopen, dan kan je Taakbeheer gebruiken om het af te sluiten. Verder zijn er in Taakbeheer allerlei overzichten te vinden over de prestaties van je computer.

Taakbeheer kan je op verschillende manieren snel opstarten. We sommen de belangrijkste even op:

- Met de sneltoetsen: **Ctrl+Shift+Esc**
- Met het PowerUser-menu (***Win+X***) → Taakbeheer kiezen in de lijst
- Met **Ctrl+Alt+Del** → Taakbeheer kiezen in de lijst
- Met het venster '***Uitvoeren***' (***Win+R***) → Open '***taskmgr.exe***'

Na het starten van Taakbeheer valt meteen de andere look op. De volledige applicatie heeft nu de look van de andere Windows 11 apps gekregen, waarbij de tabbladen zijn vervangen door een icoontjes-menu aan de linkerkant (1).



Er is een nieuwe optie **Efficiency Mode** (2), die ervoor zorgt dat apps op de achtergrond minder stroom en rekenkracht opeisen. Dit kan spijtig genoeg bij sommige toepassingen instabiliteit met zich meebrengen.

Via de knop instellingen (3) kan je een aantal persoonlijke voorkeuren instellen zoals de standaard opstartpagina of kiezen om taakbeheer altijd bovenaan te plaatsen.
Bij één van de volgende maandelijkse updates zal Taakbeheer ook eindelijk een zoekfunctie krijgen. Hierdoor zal het niet langer nodig zijn om door een ellenlange lijst van processen te scrollen om de juiste te vinden. Door simpelweg de naam of ID van een proces in te typen zal die dan onmiddellijk uit de lijst gefilterd worden.
Ook zal in de toekomst het mogelijk worden om de donkere modus voor Taakbeheer afzonderlijk in te stellen. Taakbeheer hoeft dan niet langer meer het systeemthema van Windows te volgen. De instellingen voor donkere modus zullen gesynchroniseerd worden met je Microsoft-account zodat je dit niet elke keer moet instellen.
Er zijn dus nog extra verbeteringen in zicht, maar toch is deze nieuwe versie al een grote vooruitgang.

(FVG)

SNELCURSUS → ANDROID – 10/01/2023
IS JOUW TELEFOON BESMET MET MALWARE?

Over het algemeen is Android heel veilig, maar geen enkel systeem is onfeilbaar en de laatste tijd steekt ook hier malware de kop op.
Twee recente malwarevirussen zijn **FluBot**, dat de bankrekening van slachtoffers probeert leeg te halen en **GriftHorse** dat probeert om ontzettend dure telefoonabonnementen aan te smeren.
En zoals bij Windows-malware kom je als slachtoffer hier meestal te laat achter.
Het is daarom de moeite waard om ook op je Android-toestel een aantal zaken in het oog te houden.

Op je toestel staan een hele reeks van app's. Vermoedelijk weet je zelfs niet van elke app wat die precies doet. Malwaremakers proberen dan ook om schadelijke apps stiekem te installeren, want door de grote hoeveelheid aanwezige apps, valt dit meestal niet op.
Het is daarom geen slecht idee om regelmatig te controleren welke apps zoal op je toestel staan. Staat er iets tussen dat je niet herkent, Google dan even de naam ter controle.
Het kan zelfs nuttig zijn een lijst van alle apps te maken (*eventueel via schermkopies*) zodat je af en toe kan controleren of er apps zijn bijgekomen die jijzelf niet geïnstalleerd hebt.
Maar wees wel voorzichtig en verwijder niet zomaar alle onbekende apps, want sommige zijn nodig om het toestel goed te laten functioneren.
Dit is een voorzorgmaatregel, maar wat als het kwaad al geschied is?

Hoe merk je dat er malware op je toestel staat?

Als je plots bestookt wordt met allerlei pop-ups die zomaar uit het niets opduiken en ineens zo goed als je hele scherm overnemen, dan is het toestel bijna zeker besmet met adware, een vorm van malware.
Bij adware worden gebruikers bestookt met allerlei advertenties.
Meestal promoten ze dubieuze praktijken zoals de aankoop van cryptomunten of dure ondoorzichtige abonnementen.
Heel dikwijls zijn de advertenties heel lastig of helemaal niet weg te klikken.

Wat je zeker ook moet in het oog houden zijn je mobiele data.
Dat kan via de ***Instellingen*** en ***Wifi en Netwerk*** en dan ***Dataverbruik***.
Als je plotseling veel meer data verbruikt dan normaal, dan is er zeker iets aan de hand.
Hackers zijn altijd op één ding uit: geld.
Via malware kunnen hackers stiekem je toetsaanslagen uitlezen.
Ook wordt er dikwijls gewerkt met een nepversie van je bank-app om zo achter je pincode te komen.
Hackers hebben ook dikwijls interesse in in gesprekken, foto's en chatberichten, zoekend naar bezwarend materiaal waarmee ze de slachtoffers kunnen afpersen.
Al deze data moet verzonden worden en daar is meestal een hoop dataverkeer voor nodig.
Dus als je verbruik zonder verklaarbare reden erg gestegen is, dan heeft een hacker mogelijk malware op je toestel geïnstalleerd.

Nog een indicatie die kan wijzen op de aanwezigheid van malware is wanneer je toestel zonder reden erg warm aanvoelt of wanneer de batterij supersnel leegloopt.
Malware blijft op de achtergrond altijd werken en is constant bezig met data verzamelen. Dat heeft impact op je toestel.
Android zal namelijk standaard bij niet gebruik van het toestel, altijd achtergrondprocessen stilleggen, zodat het toestel niet onnodig wordt belast. Malware draait juist continu door op de achtergrond waardoor een besmet toestel soms erg warm kan worden.
Wanneer je toestel regelmatig buitensporig warm wordt zonder aanleiding (*zoals opladen of het kijken van een film*), dan is er mogelijk iets mis.
In de meeste gevallen zal je toestel ook merkelijk trager worden want de malware draait altijd op de achtergrond en dat is erg belastend.

Kan je er iets aan doen?

Als je via de ***Instellingen*** en de optie ***Apps*** in combinatie met ***Mr.Google*** te weten komt welke app's er malware zijn, dan kan je ze verwijderen door uw Androidtoestel te starten in **veilige modus**.

Dat doe je zo:

- Zet het toestel aan door op de ***Powerknop*** te drukken.
- Zodra het toestel is opgestart hou je de ***Powerknop*** ingedrukt en druk je vervolgens ook op de ***Uitschakelen***-knop. Je krijgt dan een venster waar je kan aangeven dat je in veilige modus wil opstarten.
- Via de ***Instellingen*** en de optie ***Apps*** kan je dan de boosdoeners verwijderen.

Heb je geen idee wie de boosdoeners zijn, dan zijn er ook apps verkrijgbaar om malwarebesmettingen te verwijderen en te voorkomen.

Een aanrader is **Malwarebytes Mobile Security**, dat je beschermt tegen malware, ransomware en andere schadelijke software. De app geeft bijvoorbeeld een melding zodra je op het punt staat om een dubieuze link te openen.

Voorkomen is uiteraard beter dan genezen, dus let altijd goed op met wat je installeert. En installeer enkel vanuit de **Google Play Store**.

Wat doet Google zelf?

Google zelf probeert gevaarlijke apps op je toestel sneller en beter te herkennen. Dat doen ze met **Play Protect**, een functie die sinds Android 8.0 (*Oreo*) ingebouwd zit op alle Android-toestellen.

Play Protect scant op regelmatige basis je toestel en alle apps die erop staan. Wanneer er een schadelijke app wordt ontdekt, dan krijg je daar een waarschuwing over. Daarenboven worden apps die bij Google reeds bekend zijn als ‘zeer schadelijk’ automatisch van je toestel verwijderd. Bij minder schadelijke apps kan je zelf kiezen.
Helaas is Google Play Protect niet perfect. Uit een onderzoek blijkt dat de dienst slechts zo’n 70 procent van alle malware stopt. Google doet er alles aan om dat percentage te verhogen, en als je enkel vanuit de Play Store downloadt dan blijf je aardig veilig.
Je kan zelf controleren of Google Protect aan staat op jouw toestel. Ga daarvoor naar de Play Store en klik rechts bovenaan op je profiel-icoontje. Daarna kies je voor het item ***Play Protect***. Hier kan je zien of de optie aan staat en wanneer er voor de laatste keer een controle gebeurd is.

Moet ik dan toch nog een virusscanner installeren?

Heel lange tijd hebben we gerust kunnen beweren dat dit niet nodig was. Een app bestaat in Android slechts uit één enkel apk-bestand, dit in tegenstelling tot een Windows-toepassing die uit een hele reeks bestanden bestaat. Bovendien is elk apk-bestand voorzien van een ‘checksum’ om te controleren of er geen wijzigingen aangebracht zijn aan het origineel bestand.
Maar tijden veranderen en hackers zoeken telkens nieuwe manieren. Zo wordt er nu meestal gebruik gemaakt van eigen fake-apps die in stilte en zonder medeweten van de gebruiker worden geïnstalleerd.

Veel gebruikers hebben waarschijnlijk genoeg aan de ingebouwde virusherkenning van de meeste Android-toestellen. Wil je toch graag nog wat extra bescherming dan is het gratis **Bitdefender Mobile Security** een aanrader.

Dit gratis pakket heeft onder andere een malwarescanner en kan een pincode over je gevoelige apps plaatsen. Ook houdt de app goed in de gaten of er in je browser niets raars gebeurt.

De apps kan je terugvinden in de Play Store van Google of via onderstaande links:

https://play.google.com/store/apps/details?id=org.malwarebytes.antimalware&pli=1

https://play.google.com/store/apps/details?id=com.bitdefender.security

(FVG)

Secretariaat	Informatie	Lidgelden
p/a	Per post: via secretariaat	60 EUR voor 1 jaar
Moretuslei 3	Per telefoon: 0032 3 2895573	IBAN: BE23 9731 6510 9491
B-2180 Ekeren	Per e-mail: info@flanderscomputerclub.be	BIC: ARSPBE22

Redactie: Frank Van Goolen