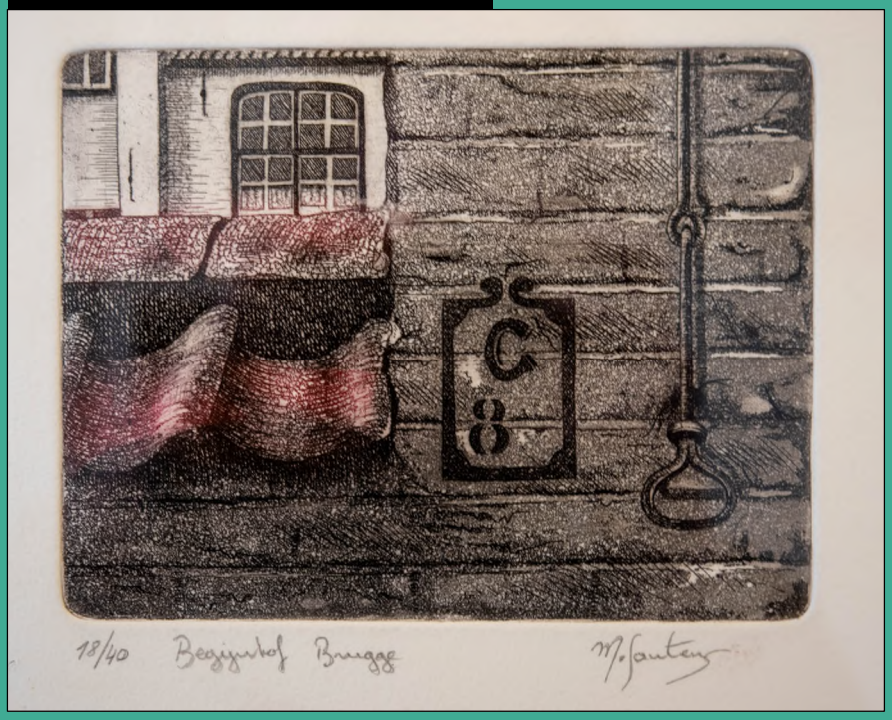
Midden West-Vlaamse Hobby
COMPUTER CLUB ROESELARE

Ons Kompjoeterblad

Jaargang 35 - Nummer 2 - maart / april 2020



Klik op bovenstaande afbeelding
en bezoek de Facebook pagina van Marc Santens, de kunstenaar.

Nieuwtjes

* VINK - Digitaal boodschappenlijstje maken
* Ransomware en cryptoware
* De duurste diskette ooit ?
* Browsers voor op de USB-stick
* Tombola januari-bijeenkomst

Met steun van ROESELARE IS 'R VOOR JOU

VRIJE TIJDSPAS

Midden West-Vlaamse Hobby
Computer Club Roeselare
Skaldenstraat 27
8800 Roeselare

info@hccr.be
http://www.hccr.be

☸ HCCR NIEUWS

* Onze kalender voor - 2020

7 maart 2020	OneNote door Olivier
4 april 2020	Backup en herstel Macrium Reflect door Peter
2 mei 2020	Beveiliging i/d Cloud door Lenny *+ Algemene Vergadering*
21 maart 2020	***Bedrijfsbezoek*** *meer info, kader onderaan*
18 april 2020	Linux Mint door Luc
16 mei 2020	

VERVANGING CLUBNAMIDDAG ...

Onze clubbijeenkomst van zaterdag 21 maart wordt vervangen door een bedrijfsbezoek op dinsdag 24 maart 2020 van 14 tot 16 uur.

Dan zijn wij te gast bij Inagro, het praktijkcentrum voor onderzoek en voorlichting in land- en tuinbouw.

Ieperseweg 87 - te 8800 Rumbeke-Beitem

Inschrijvingen kan - *UITSLUITEND* - via ons webformulier:

http://inagro.hccr.be/

Er kunnen maximaal 50 personen deelnemen.
Inschrijven en deelnemen is gratis.

inagro
ONDERZOEK & ADVIES IN LAND- & TUINBOUW

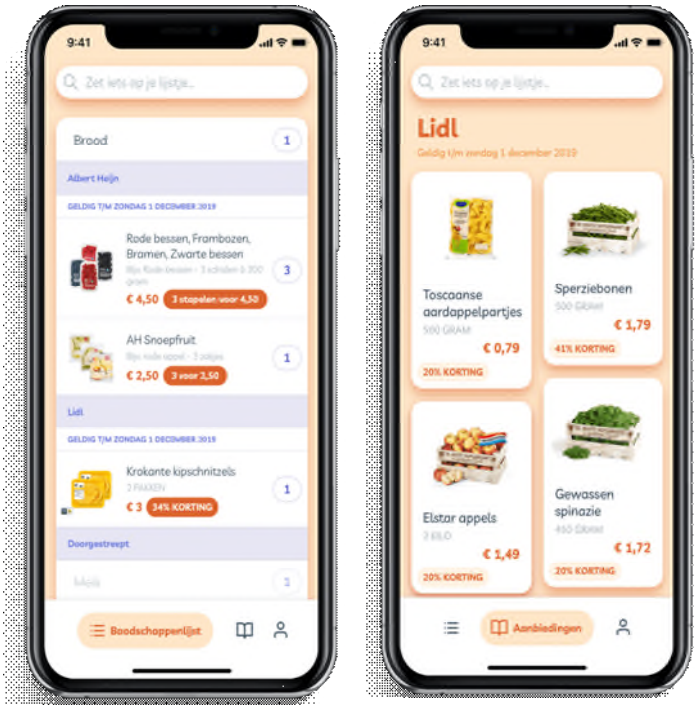
❁ NIEUWTJES

* VINK - Digitaal boodschappenlijstje maken

Boodschappenlijstjes werden vroeger altijd met de hand gemaakt, maar tegenwoordig zijn daar apps voor, zoals Vink. Vink is gratis te gebruiken en beschikbaar voor iOS en Android.

Iedereen moet wel eens boodschappen doen en de ene keer is dat wat meer dan een andere keer. Een paar artikelen zijn nog wel te onthouden, maar wanneer u een heleboel of wat meer specifieke producten nodig heeft, dan is dat wat lastiger. Een lijstje is dan erg handig. Boodschappenlijstjes werden vroeger altijd met de hand gemaakt, maar tegenwoordig zijn daar apps voor, zoals Vink. Met deze app maakt u eenvoudig een boodschappenlijstje, waar artikelen uit folders op te plaatsen zijn, maar waarbij u dat net zo goed met de hand doet. Alle artikelen zijn direct af te vinken, waardoor u gelijk weet wat u nog moet pakken in de winkel.

Het doen van boodschappen is door de jaren heen behoorlijk veranderd. Mensen maken vaker gebruik van maaltijdboxen en die bieden al veel ingrediënten. De bezorgdiensten van supermarkten zijn daarnaast aan een flinke opmars bezig. Toch gaan veel mensen nog wel zelf naar de supermarkt om daar hun boodschappen te doen. Vink zorgt ervoor dat dit wat makkelijker gaat en dat u uw boodschappen overzichtelijk op een rijtje heeft. Bovendien heeft de app een flink aantal aanbiedingen van bekende winkels, waardoor u geen aanbiedingen meer misloopt. Hiervoor zijn al veel grote winkelketens aangesloten, waardoor u alle meest recente aanbiedingen direct te zien krijgt. Dat scheelt u allemaal weer een hoop tijd en zelfs geld. Om de app te gebruiken moet u wel ingelogd zijn en u maakt een account aan met uw e-mailadres.



Vink heeft een duidelijke interface. In principe krijgt u meteen een overzicht van alle aangesloten winkels te zien, maar in uw profiel is het mogelijk om bepaalde winkels uit te vinken, bijvoorbeeld winkels waar u toch nooit komt. U ziet de aanbiedingen van die winkels dan niet meer in uw overzicht. Om iets op uw lijst te zetten voert u het product in de zoekfunctie van de app in en als u daarna op het plus icoontje klikt wordt het op uw lijst gezet. Een product hoeft niet in de aanbiedingen van winkels terug te komen. Verder worden per winkel de aanbiedingen getoond en door op een aanbieding te klikken wordt het product aan uw lijst toegevoegd. De app geeft aan tot wanneer de aanbiedingen geldig zijn. Aan de bovenkant van uw scherm veegt u simpel door de aangesloten winkels heen.

U heeft zo in een handomdraai uw boodschappenlijst samengesteld. Wanneer u in de winkel het gewenste product gepakt heeft klikt u op uw lijst in de app op dat product, waarna het wordt doorgestreept en in principe uit is afgevinkt. Dat is het dan wel. Vink is namelijk een duidelijke boodschappenlijst en niets meer en niets minder. Voordeel is sowieso dat u geen papieren lijst meer nodig heeft.

Vink heeft de volgende kenmerken:
- gratis boodschappenlijst-app voor iOS en Android,
- maak een account aan met uw e-mailadres,
- zoek producten en voeg deze toe aan uw boodschappenlijst,
- werkt met veel bekende winkelketens,
- heeft de meest recente aanbiedingen van de aangesloten winkels,
- voeg aanbiedingen met een simpele klik toe aan uw lijst,
- vink een product af als u het in de winkel heeft gepakt.

Bron: gratissoftware.nu/ https://vink.ai/

☸ NIEUWTJES

* Ransomware en cryptoware

Ransomware en cryptoware behoren tot de grootste internetgevaren. Wat is het, wat doet het precies en hoe kun je jezelf er tegen wapenen?

- ***Wat is ransomware?***

Ransomware is een type malware, ofwel kwaadaardige software, die een computer blokkeert of bestanden versleutelt. Pas als je losgeld (*ransom*) betaalt zou je de computer of de bestanden weer kunnen gebruiken. De Nederlandse term is daarom gijzelsoftware.

Ransomware is erg vervelend. Door de variant die al je bestanden versleutelt (*ook wel cryptoware genoemd*) kun je ongemerkt bijvoorbeeld je hele foto-archief of muziekverzameling, inclusief aangesloten back-ups, verliezen. Oudere, en nu minder vaak voorkomende, varianten van ransomware, blokkeren alleen de internetbrowser of het opstarten van de computer.

- ***Kenmerken cryptoware (ransomware die versleutelt)***

- Gijzelt bestanden door ze te versleutelen. Dit houdt in dat je bestanden niet meer kunt openen.
- Er wordt betaling geëist in de digitale munteenheid Bitcoin. Omgerekend wordt vaak een bedrag van honderden euro's gevraagd. Met een tijdslimiet wordt het bedrag steeds hoger gesteld.
- Besmetting verloopt via kwaadaardige bestanden (*meestal in e-mailbijlages*) of via een lek op de pc door niet-bijgewerkte software. In dat laatste geval kan de ransomware op de pc komen zonder dat je zelfs ergens op hoeft te klikken. Verdachte bestanden in e-mails zijn: zip-, exe-, js-, lnk- en wsf-bestanden. Ook Word-bestanden die vragen om macro's in te schakelen zijn gevaarlijk.
- Kijk uit voor nepmedewerkers van Microsoft die je opbellen. Je pc heeft zogenaamd een probleem en daarom willen ze op afstand inloggen, waarna ze je pc of bestanden blokkeren.
- Losgeld betalen is af te raden, maar kan een laatste redmiddel zijn.
- De versleuteling is meestal niet zonder de sleutel ongedaan te maken. Als je geluk hebt is er wel een oplossing, zie de paragraaf Bestanden redden.
- Cryptoware kan ook bestanden besmetten op aangesloten externe harde schijven of netwerkopslag die in Windows Verkenner een schijfletter heeft (*zoals E:, F:, G:*). Bewaar een back-up daarom gescheiden van de pc.
- Van enkele varianten zijn de sleutels door politie buitgemaakt, zie de paragraaf Bestanden redden.
- Namen van ransomware-varianten die bestanden versleutelen zijn bijvoorbeeld: Cerber, CTB-locker, Coinvault, CryptoLocker, Locky, Petya, Teslacrypt, TorrentLocker, WannaCry en Wildfire

- ***Praktijkvoorbeelden ransomware-mails***

Nepmails met ransomware proberen je te verleiden op een link te klikken of bevatten een besmette bijlage. In de mails worden bijvoorbeeld (*te hoge*) factuurbedragen, boetes, incasso's of mislukte afleverpogingen genoemd, waarvan de details in de bijlage of achter een link zouden staan. De bijlages of links bevatten onder andere vermomde uitvoerbare bestanden (*factuur.pdf.exe*), javascript(*.js*)-bestanden of Word-bestanden met kwaadaardige macro's. Soms zijn ze verpakt in een zip-bestand.
Bedrijfsnamen die hierbij als zogenaamde afzender worden misbruikt zijn onder meer KPN, Ziggo, Intrum Justitia en transportbedrijven. Ook zogenaamde scans van (*Xerox-*)kopieerapparaten en melding van autoschade komen voor. Lees meer over het herkennen van phishing (*nepmails*). Voorbeelden van meer nepmails vind je bij de Fraudehelpdesk.

- ***Bestanden redden***

Helaas zijn bij een ransomware-besmetting bestanden vaak niet te redden als je geen back-up hebt. Doorloop de volgende stappen als je bestanden versleuteld zijn:

- Verwijder eerst de malware, zodat bestanden niet opnieuw worden versleuteld. Doe een uitgebreide scan met je virusscanner en een second opinion met vertrouwde software als Malwarebytes of Hitman Pro.
- Plaats een back-up van de bestanden terug. Voorwaarde is natuurlijk dat er een (recente) back-up is en dat deze niet versleuteld is door de cryptoware.
- Als je geluk hebt, zijn de makers van de cryptoware

NIEUWTJES

opgepakt of heeft de politie ontsleutelingsgegevens weten te bemachtigen. In april 2015 achterhaalde de politie en antivirusmaker Kaspersky sleutels voor Coinvault.
Sinds mei 2016 zijn er reeds herstelprogramma's voor de Teslacrypt cryptoware varianten. Voor een overzicht van decryptors, waarmee je zonder hulp van criminelen je bestanden kunt redden, kun je kijken op nomoreransom.org, een initiatief van onder meer EuroPol. Voor de meeste ransomware is er helaas geen oplossing.

- Zoek verborgen back-ups. Heb je geen back-up gemaakt, dan is er een kleine kans dat Windows dit automatisch heeft gedaan. Zoek deze schaduwkopieën als volgt:
  Klik met je rechterknop een bestand of map.
  Klik op Eigenschappen > tabblad Vorige versies.
  Kijk of er een oudere versie staat die hersteld kan worden. Soms werkt dataherstelsoftware zoals het gratis Recuva.
- Betaal losgeld. Uiteraard raden we deze optie sterk af, maar als de getroffen data erg belangrijk voor je zijn, kunnen we ons voorstellen dat je overstag gaat. Ervaringen tonen aan dat slachtoffers de sleutels vaak krijgen, maar er is geen garantie.

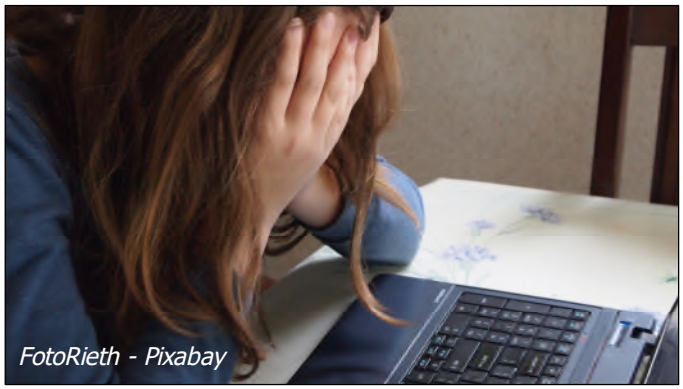
- ***Kenmerken politievirus (ransomware zonder versleuteling)***

- Direct zichtbaar: toegang tot de computer of internetbrowser is geblokkeerd.
- Doet zich vaak voor als bericht van een officiële instantie, zoals de politie of justitie. Er wordt bijvoorbeeld gezegd dat er illegale software of pornografisch materiaal is aangetroffen. Na een betaling van een boete zou de blokkering worden opgeheven.
- Er wordt meestal betaling geëist via prepaid betaalkaarten zoals Paysafecard of soms via Bitcoin.
- Besmetting verloopt meestal via besmette bestanden, bijvoorbeeld een e-mailbijlage of via een lek op de pc door niet-geüpdatete software.
- Losgeld betalen is zinloos (*de pc kan vaak niet eens meer door de criminelen worden gedeblokkeerd*).
- Het virus is te verwijderen zonder dat gegevens verloren gaan.

- ***Politievirus verwijderen***

- Betaal nooit. De kans dat je computer vrijgegeven wordt is nihil, in tegenstelling tot bij de variant die bestanden versleutelt *(cryptoware*).
- Probeer eerst Windows systeemherstel. Hierbij wordt Windows teruggezet naar de stand van een eerder moment, zonder dataverlies.
- Werkt systeemherstel niet? Kijk of je de pc in veilige modus kunt starten.
- Lukt dat? Probeer de ransomware dan te verwijderen met het gratis Malwarebytes.
- Wordt de computer geblokkeerd bij het opstarten of lukt verwijderen op een andere manier niet, probeer het dan met HitmanPro.Kickstart, onderdeel van HitmanPro en volg de Kickstart handleiding (*van Surfright, de makers van HitmanPro*). Door de computer via Kickstart op een usb-stick op te starten, kan de pc worden ontdaan van het virus. Op de website van Fraudehelpdesk zijn veel voorbeelden te vinden, met instructies hoe de blokkering van de pc op te heffen en het virus te verwijderen.

Lukt ook dat niet, dan blijft er maar 1 optie over: de pc opnieuw (*laten*) installeren. Dat is ook de enige manier om er 100% zeker van te zijn dat het virus weg is. Dat gaat het eenvoudigst met een herstelschijf of -partitie. Let op: alle data op de computer wordt gewist.


FotoRieth - Pixabay

- ***Ransomware en andere malware voorkomen***

De kans op dataverlies bij ransomware is groot, daarom is het belangrijk om besmetting te voorkomen en regelmatig te back-uppen voor als dit toch gebeurt. Volg onderstaande tips om de kans op virussen en cryptoware te verkleinen:

- Installeer een goede virusscanner en zorg dat deze minimaal 1 keer per dag automatisch bijwerkt.
- Houd alle software up-to-date, waaronder besturingssysteem, internetbrowser, browseraanvullingen en populaire programma's, zoals Adobe Reader. Met ScanCircle zie je snel hoe je pc ervoor staat. Voor software als Adobe Flash of Javascript is uitschakelen of beperkt instellen aan te raden.
- Klik niet op bijlagen en links in e-mails, tenzij je zeker weet dat het vertrouwd is. Twijfel je, kijk dan op Fraudehelpdesk op de Opgelicht website of de e-mail daar voorkomt. Zo niet, wacht dan een dag en controleer nogmaals.
- Cryptoware is vaak een uitvoerbaar .exe-bestand, vermomd als ander soort bestand, bijvoorbeeld een pdf-document. Schakel daarom bestandsextensies weergeven in.
- Er is ook software die zich speciaal richt op het voorkomen en stoppen van ransomware-versleuteling.

☸ NIEUWTJES

- En nogmaals: back-ups maken. Dat is sowieso verstandig, maar bij ransomware besmetting vaak het enige redmiddel om verlies van al je gegevens te voorkomen.

Met macOS en Linux loop je veel minder risico. Maar ook deze systemen kunnen besmet worden.

- ***Anti-ransomware programma's***

Er is software die specifiek gericht is op het voorkomen van ransomware besmetting en die als aanvulling op een virusscanner gebruikt moet worden. Helemaal uitontwikkeld zijn deze programma's niet. Met sommige virusscanners geven ze problemen. Een 100% garantie op bescherming is er niet en ze zorgen soms ook voor extra vertraging. Ook zijn sommige aardig aan de prijs. Om de kans op besmetting tegen ransomware te verkleinen kun je het installeren ervan toch overwegen, maar het is belangrijker om je te houden aan de andere punten uit het lijstje hierboven.
Enkele voorbeelden van anti-ransomware :

- CryptoPrevent: Gratis of $15-$20 per jaar (*Premium-versie*). Gericht op de wat gevorderde computergebruiker. De Premium versie zou beter moeten beschermen tegen nieuwe varianten van gijzelsoftware.
- Cybereason Ransomfree: gratis. Werkt door op willekeurige plaatsen mappen met bestanden aan te maken en deze in de gaten te houden. Stopt niet alle ransomware.
- HitmanPro.Alert: €30 per jaar, werkt tegen de meeste varianten. Eenvoudig in gebruik, maar lijkt soms te conflicteren met antivirussoftware.

- ***Niet versleutelbare back-up maken***

Er zijn verschillende manieren om een back-up te maken. Maar, let wel op dat niet elke manier van een back-up geschikt is om de versleuteling door cryptoware te herstellen. Cryptoware kan namelijk niet alleen de gegevens op het besmette apparaat versleutelen, maar ook externe opslagpunten.

- Sluit voor het maken van een back-up, de usb-stick of externe harde schijf alleen aan op het moment van een back-up en koppel hem daarna los.
- Bij een netwerkopslag kun je ervoor kiezen dat alleen de back-upsoftware bestanden mag opslaan op de netwerkschijf (*bvb via FTP*) en dat via Windows verkenner alleen bestanden gelezen worden.
- Bij een cloud back-up, en ook sommige andere vormen van back-up, kun je bestanden terughalen als er versiebeheer aanwezig is. Als in de meest recente versie van een back-up bestanden zijn versleuteld, kun je nog altijd terug naar een oudere versie van de back-up.

- ***Ook op Apple en Linux?***

De meeste ransomware/cryptoware die tot op heden is gesignaleerd, is gericht op Windows-systemen. Maar er zijn bijvoorbeeld ook gevallen bekend dat de telefoon van iPhone-gebruikers was geblokkeerd. Kortom, waar je ook mee op internet gaat, houd dat apparaat up-to-date, gebruik altijd je gezonde verstand en een kritische blik. Zeker als iets ook maar een kleine twijfel oproept.

Bron: Consumentenbond.nl/

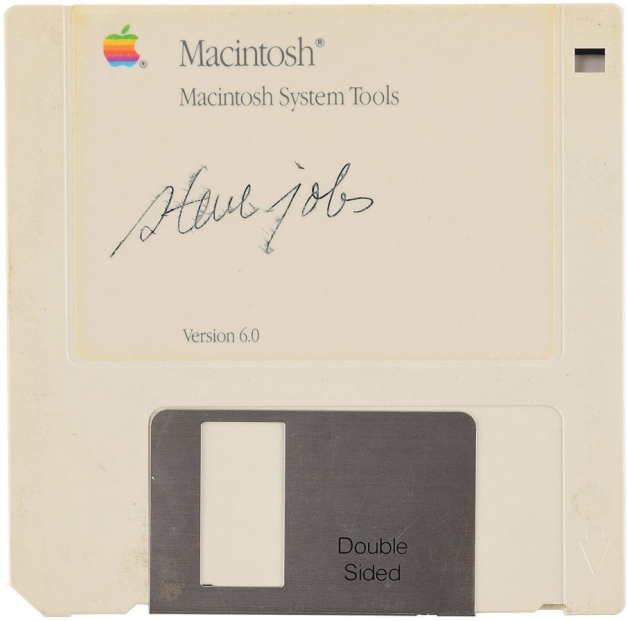
* De duurste diskette ooit ?

Een diskette ondertekend door Steve Jobs is op een veiling verkocht voor een verbluffende $ 84.115.
Het bieden begon bij slechts $ 1.000 en het item zou naar verwachting rond de $ 7.500 halen. Dat bleek een beetje een onderschatting te zijn.

De schijf werd als authentiek bevestigd en was duidelijk zeer gewild. In de itembeschrijving wordt opgemerkt dat Jobs zijn handtekening niet vaak op memorabilia plaatste, waardoor dit een bijzonder zeldzame vondst is. (*Jobs was gekend als een zeer terughoudend ondertekenaar, hij weigerde vaak om te voldoen aan de verzoeken van verzamelaars*).

Dit stukje Apple's iconische Mac OS-software, met Steve Jobs's elegante stijlvolle kleine handtekening is een stuk computergeschiedenis van museumkwaliteit.

Bron: Imore.com



☸ NIEUWTJES

* Browsers voor op de USB-stick

Of je nu uw privacy wilt verbeteren, of uw instellingen wilt behouden wanneer u een andere computer gebruikt, of gewoon verschillende versies van populaire browsers wil uittesten, het uitvoeren van een draagbare versie is een top idee. Wij testen enkele browsers op zakformaat.

- ***Opera***

De draagbare versie van Opera is verborgen tussen de standaard installatie-instellingen van de browser. Download de software zoals normaal en klik op het installatiescherm op het vervolgkeuzemenu naast 'Install for' en kies 'Stand-alone installatie (*USB*). Vanaf hier kiest u de map of USB-geheugenstick.

Deze draagbare versie bevat dezelfde tools en opties als de desktopbrowser, maar zonder zich aan uw besturingssysteem te hechten. Opera is perfect geschikt voor draagbaarheid en de minimalistische interface stopt een schat aan functies achter pictogrammen en panelen, neem een kijk naar de onopvallende zijbalk, versmald tot een enkele rij pictogrammen. Elk pictogram, wanneer erop wordt geklikt, onthult opties die over de pagina schuiven die u bekijkt, zodat u uw bladwijzer of item uit de geschiedenis kunt kiezen en vervolgens alles weer kunt verbergen We houden vooral van de optie Direct zoeken, die een Google-zoekvak op de huidige pagina overlapt, wordt uitgebreid met de zoekresultaten en vervolgens wordt uitgebreid naar een nieuw tabblad, als u dat wilt. De browser wordt aangevuld met een selectie van eenvoudig toegankelijke privacy kenmerken.

U kunt advertenties en trackers van pagina's verwijderen met een druk op de knop, en zelfs Opera's gratis VPN inschakelen, (*hoewel het goed is om te onthouden dat dit niet zo veilig is als een betaalde VPN*). Al deze tools en meer zijn beschikbaar via de briljante 'Easy setup'-zijbalk, waar abdere browsers iets van kunnen leren.

- Wat kan beter:

Onze belangrijkste klacht over Opera is dat ze erop staan, de Facebook Messenger- en WhatsApp pictogrammen, bovenaan de zijbalk. Je kunt ze zelf verwijderen door eenvoudig met de rechtermuisknop te klikken en de selectie ongedaan te maken, maar het is teleurstellend dat ze er nog steeds zijn, onzichtbaar op de achtergrond op de loer liggend en er waardevolle ruimte in beslag nemen.

- Ons oordeel

Opera voelt als de perfecte draagbare browser. De interface is schoon en gericht op de inhoud, maar ook rijk aan functies - het kiest er gewoon voor niet te veel opties zichtbaar te zetten. Het heeft ook elegante, ingebouwde privacytools om u te helpen beter op internet te surfen, probeer het eens - met deze versie heeft u niets te verliezen.

- ***Vivaldi***

Om Vivaldi draagbaar in te stellen in plaats van op uw pc te installeren, download u de software gewoon, voert u het installatieprogramma uit en klikt u op de eerste pagina van het installatievenster op Geavanceerd. Kies 'Standalone installeren' in het menu 'Installatietype', dit is de draagbare versie.

Als u op zoek bent naar een lichtgewicht en snelle draagbare browser, is dit het niet. Vivaldi is eerder een browser voor kenners, schitterend met luxe functies. Terwijl het werd afgesplitst van Opera en er nog steeds aan doet denken, is Vivaldi's 2.9 een interessante en innovatieve richtingen uitgegaan. De vertrouwde zijbalk vol met functies zit op het scherm, ervan uitgaande dat de gebruikers zijn uitgerust met royale brede schermen en willen dat hun browsesessies zijn uitgerust met alles erop en eraan.

De draagbare versie is dan ook ideaal om Vivaldi een serieuze proefperiode te geven, maar als je serieus bezig bent met surfen op het web, kun je beter de volledige browser op je gewenste computer installeren.

- Wat kan beter:

We houden van Vivaldi, maar het kan nooit worden omschreven als een pocketbrowser en is niet het meest geschikte om op elk apparaat te draaien.

- Ons oordeel

De draagbare editie van Vivaldi behoudt de uitgebreide reeks opties die u krijgt in de installeerbare versie. Het is een geweldige manier om de browser uit te proberen, maar is niet ideaal om mee te nemen, omdat het misschien niet erg geschikt is voor sommige schermen en apparaten waarop u het uiteindelijk gebruikt.

- ***SRWare Iron***

Iron is gebouwd op Chromium, maar het belooft meer privacy dan Chrome. De draagbare versie is rechtstreeks beschikbaar via de Iron-website, zodat u niet hoeft te rommelen tijdens de installatie. In feite hoeft u het niet eens te installeren, verplaats de bestanden gewoon van de gedownloade map naar waar u de browser wilt bewaren. De interface is identiek aan Chrome, maar verschilt, doordat het veel van de privacy compromitterende functies heeft verwijderd die Google in zijn browser toevoegt. Het is een goede ba-

☸ NIEUWTJES

lans tussen de snelheid en website compatibiliteit van Chrome en de privacyopties die je krijgt als je van Google weggaat.

- Wat kan beter:

Bij het sluiten, inspectie, was de versie van Iron die we hadden gedownload één versie achter op Chrome. Het wordt ook niet automatisch bijgewerkt, dus je moet het zelf in de gaten houden en steeds zelf handmatig de installatie bijwerken. Je kunt niet noodzakelijkerwijs verwachten dat een kleinere ontwikkelaar elke veranderingen van Google bijhoudt, maar een stap of meer achter de nieuwste updates aanlopen, geeft ons een beetje een ongemakkelijk gevoel.

- Ons oordeel

Je zou een draagbare versie van Chrome kunnen krijgen via het PortableApps-systeem, maar waarom zou je moeite doen als deze versie meer privé is? Het nadeel is wel dat je jezelf op de hoogte moet houden van updates, zodat je geen gecompromitteerde browser gebruikt.

* Onze januari-tombola …. En de winnaars zijn !

Links boven: Walter Decruy met een Raspberry Pi 4 set
Rechts boven: Erik Dupont met een pentekening van Marc Santens. Erik, samen met de kunstenaar op onze foto.
Een duidelijk beeld van deze tekening is te vinden op de eerste pagina van dit clubblad.
Links onder: Johny Verschaeve met een Raspberry Pi 4 set
Rechts onder: Jenny Degryse met een Raspberry Pi 4 set