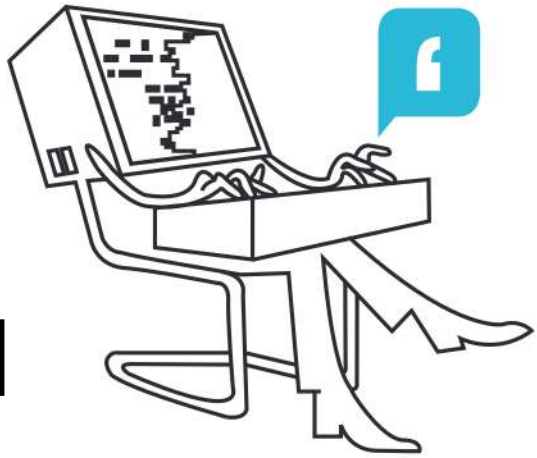
Midden West-Vlaamse Hobby
COMPUTER CLUB ROESELARE



Ons Kompjoeterblad

Jaargang 39 - Nummer 3 - mei 2024

Nieuwtjes

Midden West-Vlaamse Hobby
Computer Club Roeselare vzw
zetel: Skaldenstraat 27 - 8800 Roeselare

RPR Kortrijk
Ondernemingsnummer 432327416

info@hccr.be - https://www.hccr.be
Betalingen op rek MWVHCCR
BE12 0689 3213 7792

Midden West-Vlaamse Hobby
COMPUTER CLUB ROESELARE

☸ HCCR NIEUWS

* Onze kalender voor 2024

4 mei 2024	MacO vs Windows iPhone vs Android door Kevin *+ Alg. vergadering*
21 september 2024	Siri en Google Assistant door Kompuuter
16 november 2024	Canva door Willy
7 september 2024	Alles over Drones door Peter
5 oktober 2024	Raspberry PI Toepassingen door Christophe
7 december 2024	Betaalsystemen door Lenny

Ons clubbestuur is steeds op zoek om de bijeenkomsten zo interessant mogelijk te maken. - Hardware, software nieuwe gadgets en noem naar op.
Zoek jij meer info over een of ander onderwerp, laat het ons weten, wij zoeken dan binnen onze groep sprekers wie dit onderwerp kan/wil behandelen.
Heb jij weet van een vlotte spreker, laat het ons weten, in de mate van wat mogelijk is, zullen wij dan proberen contact te leggen om deze naar onze clubbijeenkomsten uit te nodigen.

☸ NIEUWTJES

* Uitnodiging Algemene Vergadering

Uitnodiging Algemene Vergadering

Roeselare, 27 april 2024

vzw Midden West-Vlaamse Hobby Computer Club Roeselare

Bij deze, nodigen wij graag,
alle leden uit op de jaarlijkse Algemene Vergadering
van de vzw Midden West-Vlaamse Hobby Computer Club Roeselare,
op zaterdag 4 mei 2024 om 16 uur in het clublokaal, Nijverheidsstraat te Roeselare *(ingang via parking OLV-Markt)*

AGENDA

1 Openingswoord door de Heer Voorzitter

2 Overzicht van de activiteiten van het afgelopen werkjaar 2023 - 2024.

3 Overzicht van de financiële toestand. Inkomsten en uitgaven v/h boekjaar 2023.

4 Ontlasting aan de beheerders voor de handelingen van het afgelopen werk- en boekjaar.

5 Begroting boekjaar 2025

6 Goedkeuring door de Algemene Vergadering van de begroting voor het boekjaar 2025.

7 Rondvraag

8 Slotwoord door de Heer Voorzitter

Deze Algemene Vergadering is een openboek omtrent de werking van de club.

Het is dan ook belangrijk op deze vergadering aanwezig te zijn.

De voorzitter

Kevin Florin

De secretaris

Rik Durnez

☸ NIEUWTJES

* Wat is RCS, en hoe te activeren?

Sinds een tijdje merk ik in mijn SMS-berichten een vreemd icoontje staan naast een van mijn contacten.
Ik wil nu een SMS-berichtje naar dat bewuste contact sturen, daar merk ik 'RSC-chat starten met …'.
Mijn interesse was gewekt, ik wilde een en ander uitzoeken.

John, Redactie HCCR

Berichtendienst RCS kan SMS, WhatsApp en Messenger vervangen. Lees hoe u chat met RCS, over de voor- en nadelen en hoe u het aan zet.

- ***Wat is RCS?***

RCS is de opvolger van SMS, maar het ziet eruit als een chatdienst zoals WhatsApp. RCS staat voor 'Rich Communication Services', Engels voor 'uitgebreide contactdienst'. Want in een SMS staat alleen tekst, maar in een RCS-bericht kunnen ook foto's, video's, audio en smileys verstuurd worden. Ook groepsgesprekken zijn mogelijk.

- ***De belangrijkste voordelen van RCS zijn:***

- Net als WhatsApp en Facebook Messenger is de service kosteloos. Het is niet nodig, zoals bij SMS, om per bericht te betalen. RCS maakt geen gebruik van de belbundel van een abonnement, maar van wifi of de databundel.
- Alle communicatie en het delen van bestanden kan via één app verlopen in plaats van via verschillende apps.
- RCS is verbonden aan een telefoonnummer en niet zoals bij Messenger of WhatsApp aan een profiel dat moet worden aangemaakt.

- ***Nadelen zijn er ook:***

- RCS wordt nog niet op alle telefoons ondersteund. Apple *(iPhone)* doet dit bijvoorbeeld *(nog)* niet, want het concurreert met Apple's eigen app iMessage. Stuurt u een RCS-bericht naar iemand zonder RCS-telefoon, dan verandert het in een gewone SMS. Dit gebeurt ook als u bijvoorbeeld in het buitenland bent en de provider daar RCS niet ondersteunt.
- Voorlopig werkt de dienst alleen via de smartphone, terwijl WhatsApp bijvoorbeeld ook voor de computer beschikbaar is.

- ***Kan ik RCS gebruiken?***

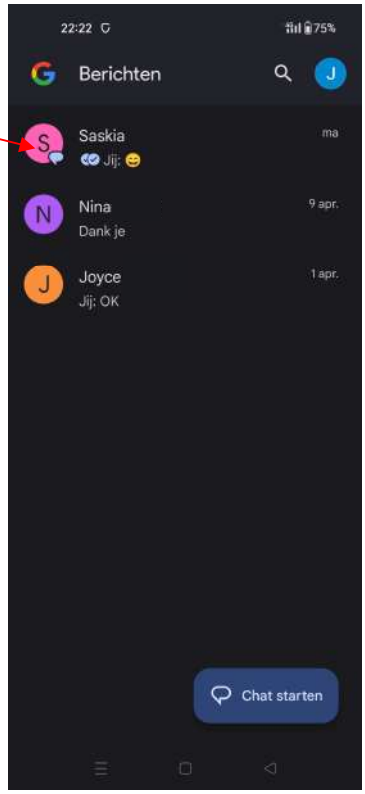
Of u RCS kunt gebruiken hangt af van wat voor apparaat u gebruikt en of de functie is ingeschakeld. Wie een Samsung Galaxy-toestel gebruikt of de app Google Berichten downloadt, kan het gebruiken. Google zorgt ervoor dat alle berichten *(eind-tot-eind)* versleuteld en dus veilig zijn.

De grootste speler op het gebied van RCS, is Google. RCS is in de Google Berichten-app ingebouwd. Samsung heeft ervoor gekozen om van Google Berichten de standaard berichten-app te maken. De verwachting is dat RCS op den duur 'gewoon' aan de Android berichten-app wordt toegevoegd. Dat het de nieuwe standaard wordt. Maar dat is tot op heden nog niet gebeurd.

- ***RCS via Google Berichten***

Met de app Google Berichten kunnen gebruikers RCS-berichten versturen. Meestal staat RCS standaard al aan. Controleer het als volgt of zet het als dat nodig is zelf aan:

- Open de Berichten-app die staat mogelijk in de map 'Google'. Of download en installeer Google Berichten in de Play Store.
- Tik op Standaard SMS-app maken om SMS in te wisselen voor RCS.
- Tik op Berichten *(de bovenste optie).*
- Tik op Standaard instellen.
- De Berichten-app gaat aan het werk. Het zet alle bestaande SMS-berichten over. Oude SMS'jes gaan dus niet verloren.
- Tik op pictogram 'Account', dat is een rondje met daarin uw voorletters of profielfoto.
- Tik op Instellingen voor Berichten.
- Tik op RCS-chats.
- Is het schuifje achter 'RCS-chats aanzetten' blauw? Dan staat RCS aan.
- Een bericht versturen? Tik op het pictogram van een tekstballon rechts onderin.
- U kunt het zien als de ontvanger geen RCS-functie heeft. Dan staat helemaal bovenaan de melding 'SMS'en met [naam] (SMS/MMS)' en bij het pictogram voor verzenden 'SMS' te staan. Als u het bericht als SMS verstuurt, gaat dit van uw bel- of SMS-bundel af.



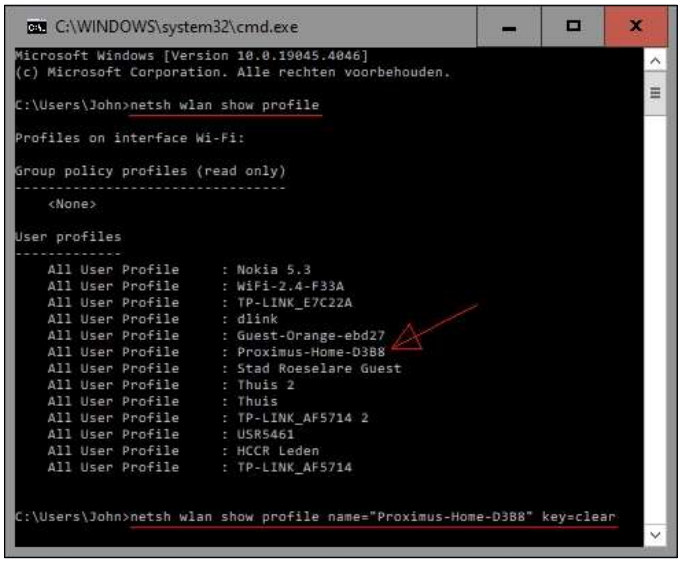
(Beschreven stappen zijn getest met een Samsung Galaxy-toestel met Android 14. De stappen kunnen op andere toestellen afwijken.)

Bron: https://www.seniorweb.nl

☸ NIEUWTJES

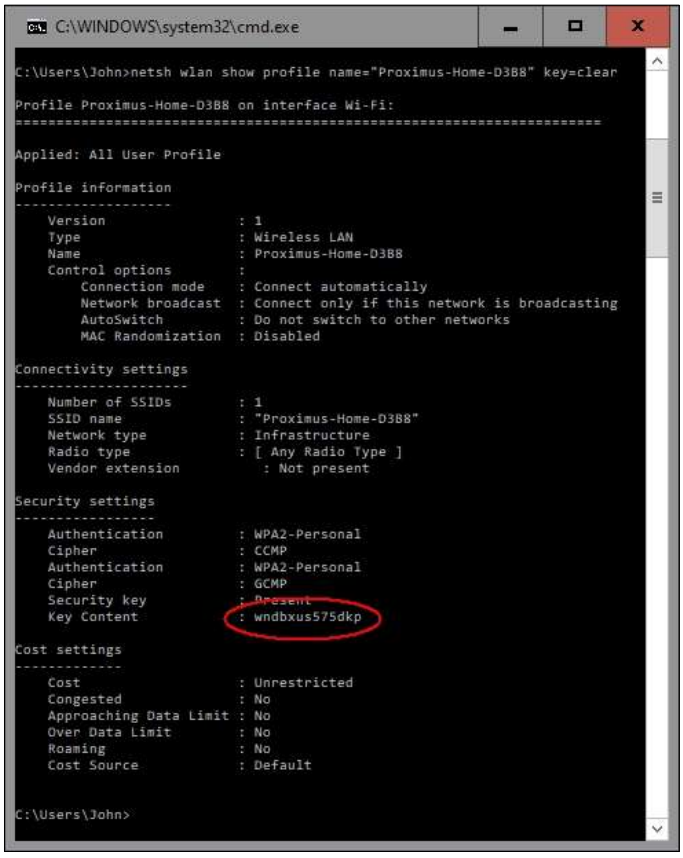
* WiFi-wachtwoorden achterhalen

Soms kan het gebeuren, dat wij om een of andere reden de opgeslagen WiFi-wachtwoorden op onze PC of laptop willen weten. Toegegeven, daar bestaan handige tooltjes voor.
Ikzelf gebruik daarvoor het mij vertrouwde CMD, wat reeds in Windows ingebakken zit.



- ***Probeer eens even mee:***

Windows-toets + R
het program 'Uitvoeren' gaat open
typ *CMD*, en geef 'n enter.
Typ:
netsh wlan show profile
Geef 'n enter en alle reeds opgeslagen netwerknamen komen in beeld. *(Bovenste afbeelding)*
Typ:
netsh wlan show profile name="Netwerknaam" key=clear
Geef vervolgens nogmaals een enter en onder de rubriek 'Security settings':
-> 'Key Content' wordt het Wifi-w8woord weergegeven.



- ***Let op:***

bij de prompt zijn de netwerknamen hoofdlettergevoelig. Zorg ervoor dat je de naam **exact** zo invoert als deze in de lijst wordt weergegeven !!

- Op onze bovenste afbeelding vinden wij alle, op mijn machine opgeslagen WiFi-netwerken.
- Verder zien wij in deze afbeelding duidelijk dat ik "Netwerknaam" heb vervangen door "Proximus-Home-D3B8", waarvan ik het wachtwoord wens te achterhalen.

Suc6,

Het WiFi-wachtwoord van je huidige netwerk bekijken

- Via Configuratiescherm
- Klik op Netwerk en internet > Netwerkcentrum
- Alle actieve verbindingen staan onder 'De actieve netwerken weergeven'.
- Klik op de blauwe link met de naam van het wifi-netwerk. Het venster 'Status van Wi-Fi' opent.
- Klik op Eigenschappen van draadloos netwerk.
- Klik op het tabblad Beveiliging.
  Achter 'Netwerkbeveiligingssleutel' staan bolletjes. Deze staan voor de tekens van het wachtwoord.
- Zet een vinkje voor Tekens weergeven.
  Soms moeten gebruikers toestemming geven voor deze handeling. Klik in dat geval op Ja.
  Het wachtwoord verschijnt. Hebt u het wachtwoord onthouden? Eventueel ergens veilig opgeschreven?
- Haal het vinkje dan weer weg om het wachtwoord te verbergen.
- Klik op Ok.

John, Redactie HCCR

☸ NIEUWTJES

* Veilig op het internet: 5 tips

Het wereldwijde web is een bron van vertier en informatie die niet meer weg te denken valt. De mogelijkheden breiden elke dag uit, maar dat geldt helaas ook voor mensen met minder goede bedoelingen.
Mediawijs, het Vlaams Kenniscentrum voor Digitale en Mediawijsheid, geeft 5 tips die kunnen helpen om veiliger te surfen op het internet.

- ***1. Beveilig je wifinetwerk***

Wanneer je wifi niet goed beveiligd is, kunnen anderen zomaar toegang krijgen tot jouw bestanden of andere apparaten die aangesloten zijn op het netwerk. Criminelen zouden je netwerk zo kunnen gebruiken voor illegale activiteiten of jouw internetverkeer onderscheppen.

Tip: pas het paswoord van je wifinetwerk regelmatig aan. Het is ook een goed idee om een extra gastennetwerk - met een ander paswoord - in te stellen voor mensen die bij jou thuis op bezoek komen.

- ***2. Kies verschillende wachtwoorden***

Het is geen goed idee om voor al je verschillende accounts *(e-mail, cloud, webshops, ...)* hetzelfde paswoord te gebruiken. Dat is natuurlijk best handig, maar veilig is dat niet. Wanneer er een datalek zou zijn bij één van die diensten, dan kunnen hackers jouw paswoord te weten komen en kunnen ze toegang krijgen tot alle diensten waar je dat ene wachtwoord voor gebruikt.


Freepik.com

Tip: kies voor een sterk wachtwoord *(minstens 15 tekens, combineer (hoofd)letters, cijfers en symbolen)* dat niet te hard voor de hand ligt. Dus beter niet je geboortedatum of je naam. (*)

Heb je problemen om al die verschillende wachtwoorden te onthouden? Gebruik een wachtwoordkluis. Dat is een programma dat alle verschillende wachtwoorden onthoudt en opslaat in de cloud. Bewaar ze niet zomaar in een *(onbeveiligd)* document op je computer.

- ***3. Gebruik tweestapsverificatie***

Tweestapsverificatie is een dubbele beveiliging voor je accounts. Kort samengevat betekent het dat je twee keer inlogt in je account, op twee verschillende manieren. Bijvoorbeeld door je wachtwoord te combineren met een vingerafdruk op je smartphone of een code die je via sms krijgt toegestuurd.

Als iemand jouw paswoord toch weet te bemachtigen, kan die persoon daardoor nog steeds geen toegang krijgen tot je account.

- ***4. Pas je privacy-instellingen aan***

Denk goed na over welke informatie of beelden je met wie deelt, want het internet vergeet niet. Op accounts van sociale mediakanalen zoals Facebook, Instagram, X en TikTok kan je de privacy-instellingen aanpassen. Zo kan je onder andere kiezen wie jouw profiel te zien krijgt en wie jou berichten kan sturen.

- ***5. Vergeet niet te updaten***

Het internet evolueert razendsnel, waardoor er regelmatig updates nodig zijn. Die nieuwe versies van besturingssystemen of software voegen niet alleen nieuwe functies toe, maar dichten ook eventuele beveiligingslekken. Op die manier proberen makers nieuwe bedreigingen zo snel mogelijk in de kiem te smoren. Op veel toestellen kan je instellen om updates automatisch te laten installeren. Vaak krijg je ook een melding wanneer er een nieuwe update beschikbaar is.

Bron: Harald Scheerlinck , vrt.be

(*) Daar uw redacteur graag eens bezig is met HTML-code te schrijven, is er een webpagina ontwikkeld geweest die een sterk wachtwoord kan genereren. - Je kunt zelf ingeven uit hoeveel karakters je wachtwoord moet bestaan. *(Standaard staat dit op 12)* Klik dan op "Genereer wachtwoord" en er wordt per direct een sterk wachtwoord gemaakt. Klik vervolgens op "Wachtwoord selecteren en kopieëren" en uw zopas aangemaakte wachtwoord kan je gebruiken waar je dit wenst. - Let op: dit is geen wachtwoord manager, deze pagina bewaart de wachtwoorden NIET !

https://ok.hccr.be/files/WWgen.html

❁ NIEUWTJES

* USB-stick beveiligen met een wachtwoord?

Een USB-stick is een handig en handzaam opslagmedium. Maar door zijn geringe formaat verlies je 'm ook vrij makkelijk. En als er gevoelige informatie of belangrijke gegevens op de USB-stick staan, dan wil je daar niet aan denken.

Gelukkig kun je relatief eenvoudig voorkomen dat onbekenden in de gegevens op je USB-stick gaan neuzen. Dit doe je door de bestanden die op je USB-stick staan te beveiligen met een wachtwoord.

- ***Hoe werkt het beveiligen van een usb-stick?***

De meest doeltreffende manier om een USB-stick te beveiligen is de inhoud ervan te versleutelen en te beveiligen met een wachtwoord. Het wachtwoord wordt gebruikt om de inhoud te ontsleutelen en wederom leesbaar te maken.

Dit wil je uiteraard op iedere computer kunnen doen. Want een van de voordelen van bestanden meenemen op een USB-stick is, dat je je bestanden via de USB-stick kunt benaderen en gebruiken op iedere computer die je wilt.

Echter, om data te kunnen versleutelen en ontsleutelen is software nodig. En wanneer je je USB-stick en de bestanden die erop staan overal wilt kunnen gebruiken, dan moet de software dus ook op de USB-stick staan. En niet alleen op de computer waarmee je de bestanden op de USB-stick versleuteld hebt.

Want dit zou betekenen dat je op iedere computer waarop je de USB-stick zou willen gebruiken, eerst de software zou moeten downloaden en zou moeten installeren, voordat je 'm kunt gebruiken. Dat is niet erg handig.

Software waarmee we eenvoudig en gratis een USB-stick kunnen beveiligen en waarmee we 'm overal kunnen blijven gebruiken is: Rohos Mini Drive.

(Rohos Mini Drive downloaden via link onder de afbeelding)

Rohos Mini Drive

https://rohos.com/products/rohos-disk-encryption/rohos-mini-drive/

Je dient Rohos Mini Drive wel eerst op je computer te installeren voordat je het kunt gebruiken.

Wat je verder op zal gaan vallen, als je Rohos Mini Drive in gebruik gaat nemen, is dat een aantal opties netjes in het Nederlands wordt weergegeven en een aantal niet. Het staat wat slordig, maar het beperkt de werking verder niet.
Bovendien weegt dit niet op tegen de voordelen en het gebruiksgemak van Rohos Mini Drive.

Aparte software om je USB-stick te beveiligen met een wachtwoord heb je overigens alleen nodig als de Home -editie van Windows op je pc staat.
Als je een Pro -of Enterprise-editie van Windows hebt, dan kun je BitLocker gebruiken, dat standaard onderdeel is van deze edities van Windows.

- ***Je USB-stick beveiligen met Rohos Mini Drive***

Zodra Rohos Mini Drive is gestart, zal het programma vragen wat je wilt doen.

Steek nu eerst de USB-stick in een vrije USB-poort in je computer en klik op de optie Encrypt USB drive.
Rohos zal de aangesloten USB-stick vanzelf vinden en je vervolgens een venster tonen waarin je om het wachtwoord wordt gevraagd dat je wilt gebruiken.

Tevens wordt in ditzelfde venster aangeboden om een snelkoppeling te maken op het Bureaublad van je computer. Dit is een slimme optie die je kunt gebruiken wanneer je je beveiligde USB-stick makkelijk en snel wilt kunnen benaderen op je computer.
Klik op de knop Maak schijf om de met een wachtwoord beveiligde partitie op je USB-stick aan te maken. Wees geduldig want het kan even duren voordat de partitie is aangemaakt.

Zodra Rohos klaar is met het aanmaken van de beveiligde USB-stick, zal een Verkennervenster geopend worden, waarin de beveiligde partitie wordt getoond.

Tevens wordt er een nieuw schijfstation in Verkenner weergegeven, Encrypted disk. Dit is het schijfstation op je USB-stick waarin je bestanden zet die versleuteld moeten worden en beveiligd moeten worden met een wachtwoord.

- ***Je USB-stick met Rohos Mini Drive gebruiken***

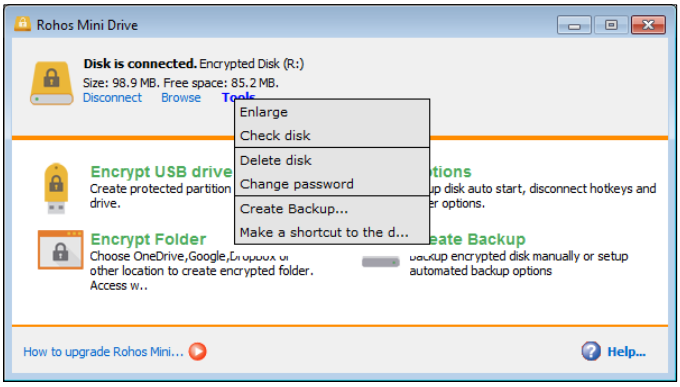
Klik je in Verkenner op de schrijfletter en de naam die je USB-stick heeft, dan zie je dat er slechts 2 bestandjes worden weergegeven:

☸ NIEUWTJES

- Rohos Mini Drive *(Portable)*.exe - Door op dit bestand te dubbelklikken kun je op een andere computer dan de computer waarop je je beveiligde USB-stick hebt gemaakt, en waarop je niet de rechten van Administrator hebt, uw beveiligde USB-stick gebruiken.

- Rohos mini.exe - Door op dit bestand te dubbelklikken kun je de USB-stick gebruiken op een computer waarop je wel Administrator rechten hebt, maar welke niet de computer is waarop je de beveiligde USB-stick hebt gemaakt.

Dit betekent in de praktijk dat, als je je beveiligde USB-stick hebt gemaakt op je pc, daar de Rohos software op geïnstalleerd is. Sluit je je USB-stick op de pc aan, dan kun je door middel van dubbelklikken op de snelkoppeling op het Bureaublad, en het invoeren van het wachtwoord dat je hebt aangemaakt voor de USB-stick, er direct toegang toe krijgen.



Heb je tevens een laptop en wil je je beveiligde USB-stick op je laptop gebruiken, dan start je Windows Verkenner en navigeer je naar je USB-stick in Verkenner en dubbelklik je op het bestand Rohos mini.exe. Ook nu zal je om je wachtwoord gevraagd worden, waarna je toegang krijgt tot je bestanden.
Echter, wil je je USB-stick op de computer van je werk gebruiken, dan zul je op deze computer vaak niet beschikken over Administrator rechten. In dat geval start je tevens Windows Verkenner, maar dubbelklik je op het bestand Rohos Mini Drive *(Portable)*.exe dat tevens op je USB-stick staat.

Op deze manier kun je werkelijk op iedere computer met een USB-aansluiting gebruik maken van je beveiligde USB-stick.

Een USB-stick beveiligen met een wachtwoord en de bestanden versleuteld op de USB-stick zetten, maakt het werken met een USB-stick iets ingewikkelder dan normaal gesproken. Het werken met een beveiligde USB-stick zal dan misschien ook best even wennen zijn.

Maar in ieder geval zijn je bestanden en gegevens veilig en vreemden kunnen niet zomaar met de inhoud van je USB-stick aan de haal.

Bekijk hier een YouTube-video:
https://ok.hccr.be/files/rohos.html

Bron: W. van Dreven, www.personalcomputercare.nl
https://rohos.com/

* App 112 BE - De app die levens redt

- ***Wist je dat?***

Het op 4 mei de Internationale Dag van de Brandweer is? Uiteraard, je ziet ze liever niet komen, maar ... een ongeluk zit steeds in een klein hoekje. Een gouden raad: installeer de gratis app 112 op je smartphone.
In geval van nood contacteer je zo gemakkelijk de brandweer, ambulance of politie.
De noodcentrale krijgt meteen je locatie door en andere info die je invulde: allergieën, bloedgroep, ...
Meer details in dit filmpje - https://ok.hccr.be/files/app112.html