Drieentwintigste jaargang nummer 01: Jan 2022

De COMPUTERCLUB

Nissewaard

Computerclub Nissewaard is voortgekomen uit een samenwerking van CcUpd@te en Stichting Wijkgroep de Akkers

Colofon

Dagelijks bestuur

Voorzitter:	**H.Kubbinga**	**Tel. 0181-640669**
Penningmeester:	**B.W.Tijl**	**Tel. 0181-630859**
Secretariaat:	**A van Bronckhorst**	**Tel. 06-36147051**

Vrijwilligers Computerclub Nissewaard

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

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

Correspondentieadres is:
computerclubnissewaard@gmail.com
Tel. 06-54692942
Internet: Aan website wordt gewerkt

Computerclub Nissewaard is voortgekomen uit een samenwerking van CcUpd@te en Stichting Wijkgroep de Akkers

Bestuursmededeling
Januari 2022

Beste leden,

Het is wel weer een raar en hectisch kwartaal geweest. Het goede nieuw was de clubstart die toch redelijk bezet was. We konden elkaar weer fysiek ontmoeten al was het met enigszins beperkende maatregelen. Helaas zijn we allen vlak voor de kerst verrast door een nieuwe lockdown. Dus geen club meer. Voor ons is het nog te overzien, maar je zal maar een eigen zaak hebben. Hoe de Omicrom zich gaat gedragen is maar afwachten. Max heeft ons wel vermaakt met zijn formule-1 winst.
Wij hopen dat jullie toch allemaal een mooi kerstfeest met het beperkte aantal visite heeft kunnen vieren.
Arie heeft in dit blad weer leuke leerzame artikelen gezet om wat van op te steken.
Iedereen wensen we een rustiger en zeker gezond 2022 toe, ook voor jullie familie en tot in 2022.

Groet van uw voorzitter: Hans Kubbinga en de andere lesgevenden.

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 ineens voor een heel jaar, betaalt U **€ 90,00**
U kunt bij ons een cursus volgen.
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 betaalt dan een bijdrage van: **€ 10.00 per keer, excl. materiaalkosten.**

Vraag aan de penningmeester naar de diverse mogelijkheden,

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: T.a.v. Secretaris Computerclubnissewaard, MFC De Akkers, Lenteakker 5, 3206 TB Spijkenisse

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 uit komen.

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

Inhoudsopgave

Hoe zit het met veiligheid en privacy in de cloud?

Seniorweb

Bestanden kunnen veilig opgeslagen worden in de cloud. De grote gratis aanbieders doen er alles aan hun opslag te beveiligen. Gebruikers dienen zelf hun account te beveiligen.

Wat is de cloud?

De term ‘cloud’ wordt gebruikt voor online werken en opslaan. In dit artikel beperken we ons tot de diensten die gratis online opslag aanbieden: **OneDrive**, **Google Drive**, **iCloud** en **Dropbox**.

Accountbeveiliging

Alle opslagdiensten werken via een gebruikersaccount. OneDrive met een Microsoft-account, Google Drive met een Google-account, iCloud met een Apple ID en Dropbox met een Dropbox-account.
De grote drie (**Microsoft, Google en Apple**) gebruiken het gebruikersaccount ook voor andere dingen. Bijvoorbeeld voor hun mailprogramma's of als gebruikersaccount van een smartphone. Wie zo'n andere dienst gebruikt heeft dus al een account voor de opslagdienst van het bedrijf. Voor alle accounts gelden de volgende aanbevelingen:

- Maak een uniek en sterk wachtwoord**.**
- Beveilig het account met **tweestapsverificatie**. Komen de accountgegevens onverhoopt op straat te liggen, dan houdt tweestapsverificatie de deur naar alle bestanden gesloten.
- Let op voor phishing en kwaadaardige programma's. Via e-mail tracht men de inloggegevens van een account te ontfutselen. Trap er niet in, wees alert.
- Sla geen gevoelige persoonlijke informatie op in de cloud, zoals een document met inloggegevens of een fotokopie van een paspoort.

Ransomware

Bij **ransomsware** komt er kwaadaardige software op de computer, waarmee de bestanden op de pc worden versleuteld. Als een cloudprogramma op de computer is geïnstalleerd, kan ransomware ook de bestanden bij de clouddienst versleutelen. Veel diensten wapenen zich hiertegen.

Bij **Dropbox** kunnen gebruikers eerdere versies van bestanden terugzetten. Je kan dan terug naar een bestand dat niet versleuteld is door de ransomware. In de **gratis** versie van Dropbox kan dit alleen per

bestand**. Betalende** gebruikers kunnen hele mappen en zelfs een heel account in één keer herstellen.

OneDrive kent deze herstelmogelijkheid ook, maar alleen voor **betalende Microsoft 365-abonnees**.
Google Drive heeft eveneens een mogelijkheid tot bestandsherstel, maar deze blijft achter bij Dropbox of OneDrive.

Ransomware voor de Mac (en dus **iCloud)** is er nauwelijks.

Geeft de dreiging van ransomware een onveilig gevoel, dan kunt u de map van de clouddienst handmatig synchroniseren in plaats van automatisch. Dan weet u zeker dat de clouddienst alleen start als de bestanden niet zijn versleuteld. Natuurlijk kunt u ook alle bestanden alleen in de online omgeving bewaren, en niet op de lokale schijf van de computer.

Beveiliging van de diensten

Alle diensten beveiligen de online opslag van bestanden.

Veilige verbinding

De opslagdiensten beveiligen de verbinding zodat niemand mee kan kijken.

Versleuteling van de bestanden

Alle bestanden die online bewaard worden, zijn versleuteld. De sleutel is gekoppeld aan het account. Zonder sleutel zijn de bestanden onleesbaar. Ook voor medewerkers van de opslagdienst. Alle gegevens zijn daarom veilig voor de ogen van derden.

Dubbele opslag

Ook de computers van de opslagdiensten kunnen kapotgaan. Door een crash van de harde schijf, maar ook als gevolg van een brand of andere ramp. Daarom worden de bestanden op meer dan één plek opgeslagen. Zo kunnen ze nooit kwijtraken.
De aanbieders van online opslag hebben belang bij het beschermen van de data van hun klanten. Met hun beveiliging zit het wel snor. Vergelijk het met uw eigen financiën. Wat is veiliger volgens u: uw geld laten beheren door een bank of uw geld thuis verbergen in uw driezitsbank?

Zit het wel goed met de privacy?

De bestanden zijn versleuteld en daarom alleen leesbaar voor de gebruiker. Dus de privacy van bestanden is wel gewaarborgd. Alle diensten slaan alleen wel informatie over de gebruiker op.

Deze informatie is in Europa beschermd door de Algemene Verordening Gegevensbescherming (AVG). Persoonsgegevens mogen niet worden ingezien of gebruikt.

Diensten moeten aangeven waarom ze welke gegevens opslaan. Er moet bijvoorbeeld een duidelijke reden zijn om te vragen naar iemands leeftijd. De diensten mogen gegevens die niet direct te herleiden zijn tot een persoon, wel gebruiken om gericht advertenties te tonen. Microsoft, Apple en Google staan hierom bekend.

Wie alleen de opslagdienst van deze partijen gebruikt, merkt daar niet veel van. Maar de meeste mensen gebruiken meerdere diensten.

Foto's van Android-telefoon op pc zetten

Seniorweb

Bewaar de foto's gemaakt met uw Android-smartphone ook op de computer. Er is dan een goede back-up.

Smartphone foto's back-uppen

Foto's van een Android-smartphone of tablet overzetten naar de computer kan op verschillende manieren: via de cloud (online opslagruimte) of via de meegeleverde kabel.

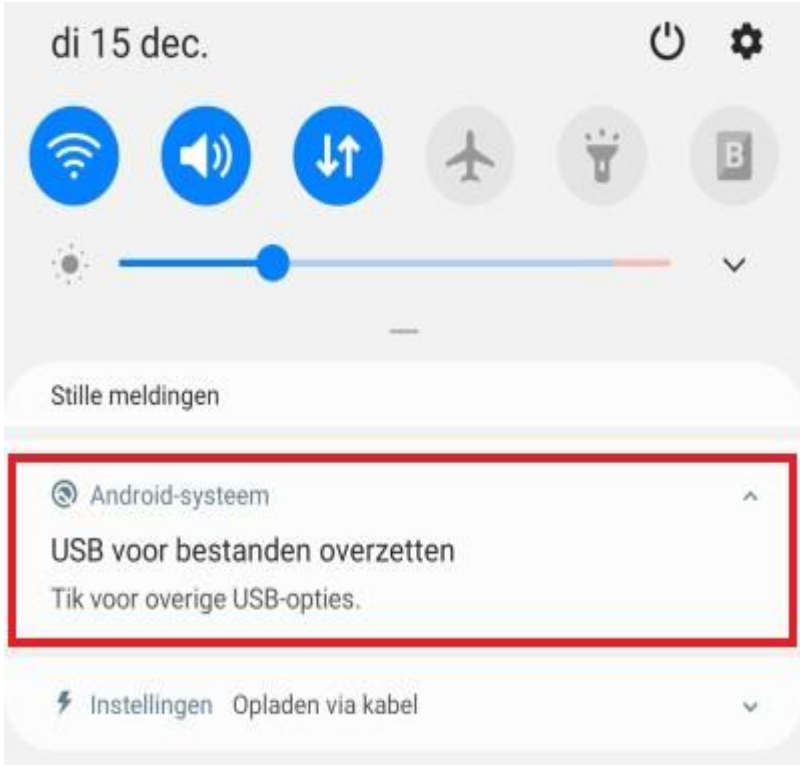
Foto's overzetten via de cloud

Wie geen zin heeft in gedoe met snoertjes die niet passen of kwijt zijn, kan het beste kiezen om foto's over te zetten via de **cloud.** U slaat de foto's dan op internet op, bij een gratis of betaalde dienst. Omdat ze online staan, kunt u vanaf elk apparaat bij de beelden, dus ook vanaf de computer.

Foto's overzetten via kabel smartphone

Foto's van de Android-smartphone handmatig overzetten naar de computer, gaat met een USB-kabel. Deze kabel hebt u gekregen bij de telefoon. Dit is hetzelfde snoertje waarmee u het apparaat oplaadt. Zet als volgt foto's en video's over van de smartphone naar de computer:

- Verbind de telefoon met de computer via de USB-kabel.
- Op de telefoon verschijnt de melding 'Toegang tot apparaatgegevens toestaan'. Tik op Toestaan.
- Verschijnt er geen melding, veeg dan van de bovenrand van het scherm naar beneden. Tik in het snelmenu op USB voor bestanden overzetten.



- Kies onder 'USB bediend door' of u de smartphone wilt bedienen vanaf de computer wanneer die is aangesloten, of zoals altijd vanaf de telefoon.
- Kies onder 'USB gebruiken voor' voor Afbeeldingen overzetten.
- Open op de computer de Verkenner**.**
- Klik in de linker kolom op Deze pc.
- De verkenner toont de inhoud van 'Deze pc'. Onder 'Apparaten en stations' staan de schijven en externe apparaten die met de computer zijn verbonden. Daartussen staat ook de naam van de telefoon. Dubbelklik hierop.
- Elk merk telefoon gebruikt andere mappenindelingen. Bij sommige telefoons staan alle foto's in de map 'Pictures'. Blader eventueel door de mappen om de map met foto's te vinden. Dubbelklik op de Samsung Galaxy A50 op de map Phone > DCIM > Camera.
- Klik op de foto die u wilt kopiëren naar de computer. Wilt u meerdere foto's kopiëren, houd dan de Ctrl-toets ingedrukt terwijl u op de foto's klikt.
- Rechtsklik op een geselecteerde afbeelding.
- Klik in Windows 10 op Kopiëren. Klik in Windows 11 bovenin het menu op het pictogram Kopiëren.
- Open in de Verkenner de map op de computer waarnaar u de foto's wilt kopiëren.
- Rechtsklik op een leeg (wit) stuk in de map.
- Klik in Windows 10 op Plakken. Klik in Windows 11 bovenin het menu op het pictogram Plakken.

De foto's worden in de map geplaatst. U kunt deze methode ook andersom gebruiken, dus om foto's van de computer naar de smartphone te kopiëren.

In deze tip gaan we uit van een Samsung Galaxy A50 en een computer met Windows 10. Maar op andere Android-toestellen en Windows-versies werkt het ongeveer hetzelfde.

Collecties beheren met Excel

Seniorweb

Een boeken-, film-, of muziekcollectie is eenvoudig te beheren via Excel. Gebruik gewoon de tabellen in het rekenprogramma.

Lijstjes

De gasten op een groot feest, de muziek die die avond gedraaid moet worden, een boeken-, film- of wijnverzameling, wat er in de koffer moet op vakantie. Het is allemaal te ordenen en beheren met behulp van lijstjes. En Excel is kampioen lijstjes maken. Dankzij de vele mogelijkheden van de tabellen in het programma.

Kant-en-klare lijsten

Helemaal gemakkelijk zijn de vele kant-en-klare sjablonen. Maak een nieuw werkblad op basis van een sjabloon, pas het sjabloon naar wens aan en vullen maar. Hieronder wat voorbeelden van sjablonen.

- Boekencollectie: typ de zoekterm 'Boekencollectie' en gebruik het sjabloon 'Lijst met boekencollectie'.
- Gastenlijst: typ de zoekterm ‘Gastenlijst’ en gebruik het sjabloon ‘Gastenlijst voor bruiloft’.
- Filmlijst: typ de zoekterm ‘Filmlijst’ en gebruik het sjabloon ‘Filmlijst’.
- Muzieklijst: typ de zoekterm ‘Muzieklijst’ en gebruik het sjabloon ‘Muzieklijst bruiloft’.
- Wijncollectie: typ de zoekterm ‘Wijnverzameling’ en gebruik het sjabloon ‘Lijst met wijnverzameling’.
- Vakantie: typ de zoekterm ‘Vakantie’ en gebruik het sjabloon ‘Vakantie checklist’.

Laat uw fantasie de vrije loop en blader eens door alle voorbeelden van lijsten. Natuurlijk sluiten de meeste sjablonen niet exact aan op uw wensen. Dat hoeft ook niet want de gebruiker kan elk sjabloon naar wens aanpassen,

Sjabloon zoeken

Zoek zo een geschikt sjabloon:

- Start Excel.
- Klik aan de rechterkant, bovenin, op Meer sjablonen.
- Typ in het zoekveld een zoekterm. Bijvoorbeeld 'Boekencollectie'.
- Druk op de Enter-toets.
- Klik op een geschikt sjabloon.
- Klik op Maken.
- Het sjabloon opent.

Sjabloon aanpassen

We gebruiken als voorbeeld het sjabloon ‘Lijst met boekencollectie’. Open dit om ermee te oefenen. De acties die we bespreken zijn van toepassing op elk sjabloon in Excel.

Kolom verwijderen

Het sjabloon ‘Lijst met boekencollectie’ bevat de kolom ‘Locatie boekenplank’. Weinig mensen zullen behoefte hebben aan deze informatie. Weg met die kolom!

- Klik met de rechtermuisknop op de kolom die u wilt verwijderen.
- Kies voor Verwijderen > Tabelkolommen.

Kolom toevoegen

Voeg een missende rubriek zelf toe. Bepaal eerst vóór welke bestaande kolom de nieuwe rubriek geplaatst moet worden.

- Klik met de rechtermuisknop op de bestaande kolom.
- Klik op Invoegen > Tabelkolommen links.
- Geef de nieuwe kolom een naam. Klik op de nieuwe kolom.
- Typ de naam.
- Druk op de Enter-toets.

Titel wijzigen

Het voorbeeldsjabloon heeft de titel ‘Lijst met boekencollectie’. Pas dit naar wens aan. Omdat de individuele cellen niet zichtbaar zijn is het even zoeken naar de juiste cel. Het blijkt ‘C1’ te zijn. Klik op die cel, typ en andere naam en druk op de Enter-toets.

Sjabloon opslaan

Vergeet niet het voorbeeld op te slaan onder een eigen naam.

- Klik op Bestand > Opslaan als.
- Klik op Bladeren.
- Selecteer de map waarin de lijst moet worden opgeslagen.
- Typ naast ‘Bestandsnaam’ de nieuwe naam.
- Klik op Opslaan.

Teller toevoegen

Wie een collectie beheert houdt graag overzicht. Hoeveel boeken

staan er bijvoorbeeld op de plank? Voeg daarom een teller toe aan het sjabloon ‘Lijst met boekencollectie’.

- Klik op cel H1 zodat deze geselecteerd is.
- Klik op het tabblad Formules.
- Klik op Functie invoegen  .
- Klik op het uitklapmenu naast ‘Of selecteer een categorie’.
- Kik op Alles.
- Klik in de lijst op AANTALARG.
- Klik op Ok.
- Klik op de eerste titel (in het voorbeeld is dat ‘The Call of the Wild’).
- Gebruik de sneltoets Ctrl+Shift +pijl naar beneden.
- Klik op Ok.
- Cel H1 toont het aantal boeken in de lijst. Voegt u boeken toe dan loopt de teller mee.
- Klik op cel C1.
- Klik op het tabblad Start > Opmaak kopiëren/plakken.
- Klik op cel H1.
- De cel heeft nu dezelfde opmaak als de titel. Wie het helemaal af wil maken doet het volgende:
- Kopieer deze tekens: *&” boeken”*
- Dubbelklik op cel H1.
- Zorg dat de muisaanwijzer aan het eind staat. Dus na het tweede haakje.
- Plak de gekopieerde tekens met de sneltoets Ctrl+V.
- Druk op de Enter-toets.

Lijst vullen

Het sjabloon is nu omgewerkt tot een lijst die u kunt gaan vullen. Veel succes daarmee!

Zo bescherm je je externe schijf met een wachtwoord

Dirk

Je telefoon en computer zijn beveiligd met een pincode, wachtwoord of biometrische authenticatie, maar hoe zit het met je externe opslagapparaten? Ook die dingen kunnen in handen raken van onbevoegden. Er zijn enkele manieren om zo'n externe schijf te beschermen met een wachtwoord.

Externe harde schijven en usb-sticks zijn bijzonder handig vanwege hun draagbaarheid. Je neemt grote bestanden heel gemakkelijk met je mee, zonder dat je met een laptop hoeft te zeulen. Om de veiligheid in het oog te houden, kun je natuurlijk hardware-gecodeerde opslagapparaten met vingerafdruklezers aanschaffen. Deze schijven bieden een veilige vorm van wachtwoordvrije biometrische codering die makkelijk in gebruik is en ook eenvoudig in te stellen is. Maar die zijn duur.

Wij bekijken vergrendelingssoftware die je geen cent kost. Voor alle duidelijkheid, we hebben het hier niet over tools waarmee je selectief één of meerdere mappen versleutelt. In dit artikel leggen we je uit hoe je de volledige gegevensdrager met een wachtwoord beveiligt. Hierdoor vermijd je dat je op een hectische dag per ongeluk gegevens opslaat buiten die paar beveiligde mappen waardoor ze open en bloot voor iedereen beschikbaar zijn die de schijf in handen krijgt.

BitLocker inschakelen

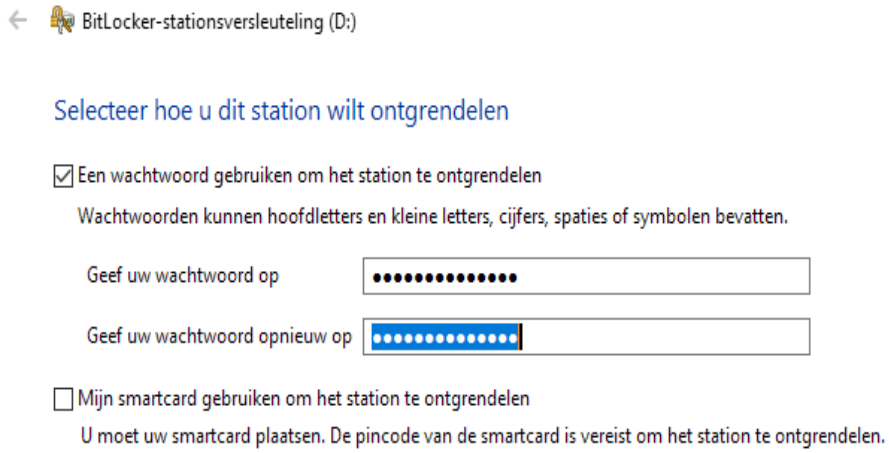
BitLocker is de gemakkelijkste Windows-oplossing, want dan hoef je geen software van derden te gebruiken. Hier zit helaas wel een 'maar'

aan verbonden, want deze tool is alleen beschikbaar in Windows 10 Pro, Enterprise en Education. Wie dus met Windows 10 Home werkt, moet een andere oplossing, bijvoorbeeld VeraCrypt – ook besproken in dit artikel – gebruiken.

Maak je gebruik van een andere versie dan Home, open dan Windows Verkenner en klik met de rechtermuisknop op de externe schijf of usb-stick en kies BitLocker inschakelen. Er verschijnt een mededeling dat BitLocker wordt geïnitialiseerd. Wacht even tot dat klaar is en zorg ervoor dat je de schijf niet ontkoppelt tijdens de BitLocker-codering.

Wachtwoord

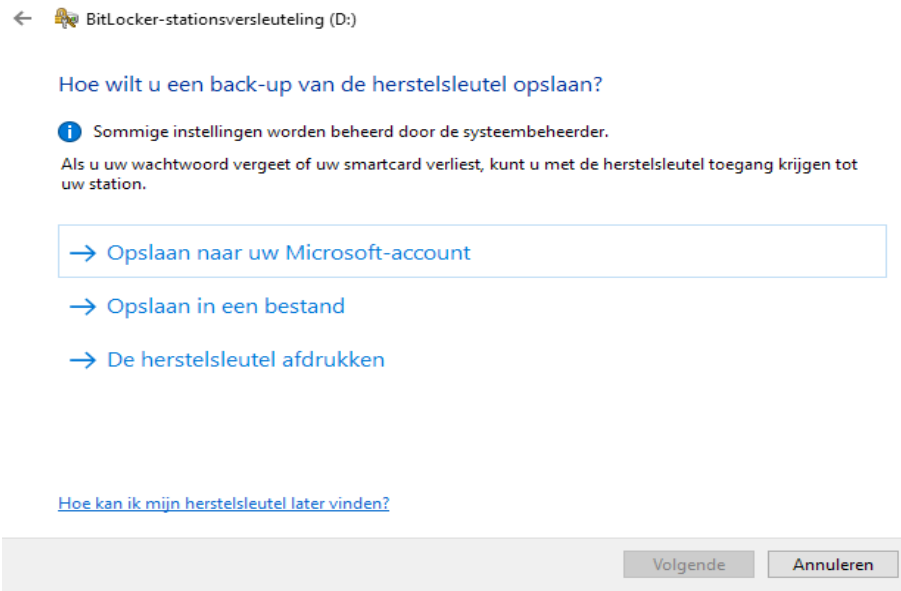
Daarna zet je een vinkje bij de tekst Een wachtwoord gebruiken om het station te ontgrendelen. Voeg een sterk wachtwoord in en herhaal dit. Selecteer daarna Volgende om door te gaan. Het wachtwoord moet aan een aantal criteria voldoen, anders ontvang je een foutmelding. Het moet minimaal acht tekens bevatten, minstens één hoofdletter en één kleine letter en er moet ten minste één symbool, cijfer of spatie in staan.



Het wachtwoord moet uit minstens acht tekens bestaan.

Herstelsleutel

Windows maakt automatisch een **herstelsleutel** aan als je het wachtwoord bent vergeten. Je kunt die herstelsleutel op drie manieren vastleggen: je kunt hem opslaan in je Microsoft-account, in een tekstbestand ergens op de harde schijf of afdrukken. Kies een van de drie manieren en klik op Volgende. Nadat je het bericht hebt ontvangen dat de herstelsleutel is opgeslagen of afgedrukt, ga je verder.



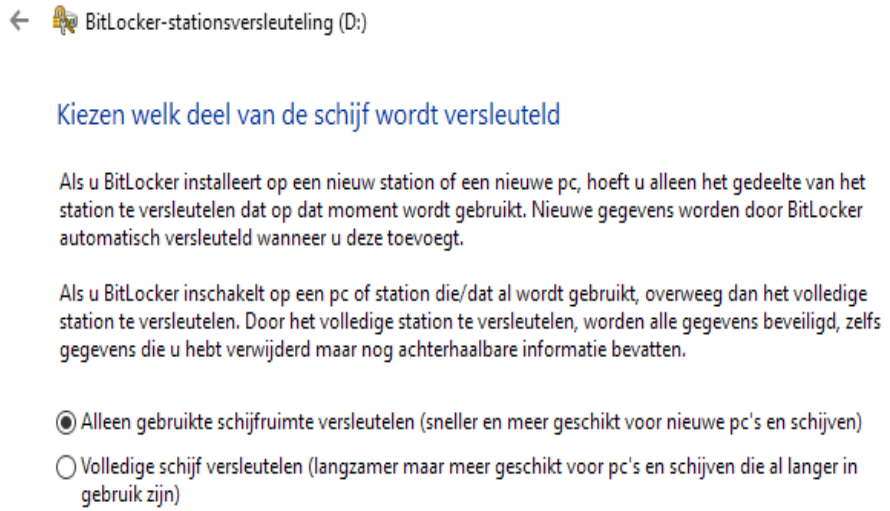
Zo'n herstelsleutel bestaat uit 48 unieke tekens.

Versleuteling starten

BitLocker vraagt welk deel van de externe gegevensdrager beveiligd moet worden. Als het gaat om een nieuwe schijf of usb-stick, dan hoef je alleen het gedeelte van het station te versleutelen dat je op dat moment gebruikt. Alle nieuwe gegevens zal BitLocker automatisch versleutelen wanneer je ze naar dit station wegschrijft. Dit is de snelste

methode. Afhankelijk van de hoeveelheid gegevens op de schijf een paar seconden tot minuten.
Schakel je BitLocker in op een station dat al wordt gebruikt, dan kun je het volledige station versleutelen, zodat alle gegevens beveiligd zijn. Dat geldt ook voor gegevens die je van dit station hebt verwijderd, maar die nog niet overschreven zijn. Deze methode verloopt langzamer en kan zelfs uren in beslag nemen.

Heb je je keuze gemaakt, klik dan op de knop Versleuteling starten.



Welk deel van de schijf moet BitLocker versleutelen?

Geavanceerde opstartopties

Verwijder de schijf niet, want dan onderbreek je de codering en hierdoor zou de schijf beschadigd kunnen raken. Je kunt het versleutelingsproces wel even pauzeren, maar de bestanden zijn pas volledig beschermd als je het bericht ziet dat de versleuteling is afgerond.

Wanneer je later **de schijf of usb-stick** verwijdert en opnieuw in de computer plugt, verschijnt er een pop-upvenster van BitLocker die naar het wachtwoord vraagt. In het pop-upvenster zie je ook nog twee andere opties: het opgeven van de herstelsleutel en de schijf automatisch laten ontgrendelen op de pc. De eerste optie gebruik je als je je wachtwoord vergeten bent, je voert dan de herstelsleutel van 48 tekens in om weer toegang tot je schijf te krijgen. Door de tweede optie aan te vinken zorg je ervoor dat de huidige pc de schijf altijd automatisch herkent en ontgrendelt.

Je kunt aangeven dat BitLocker deze pc kan vertrouwen zodat je niet keer op keer het wachtwoord hoeft in te geven.

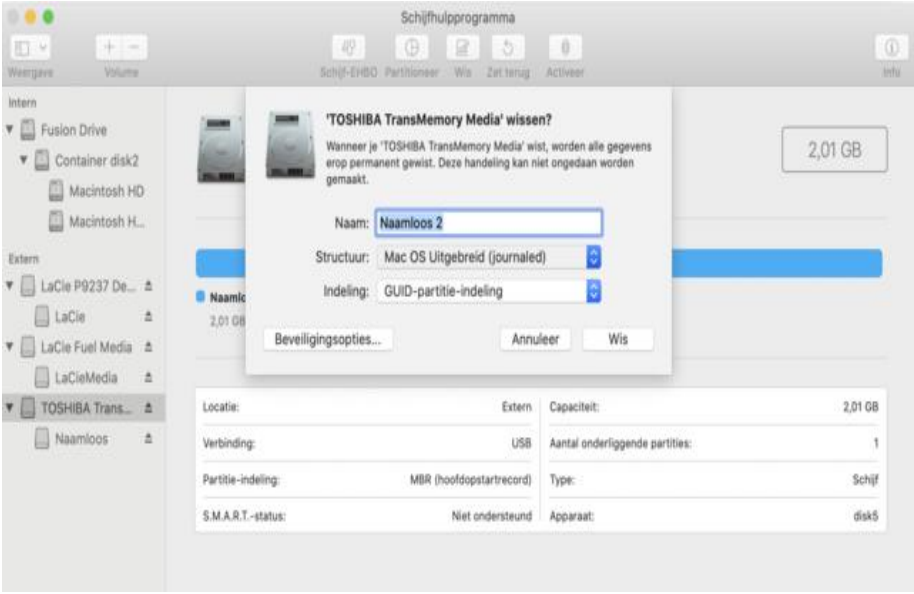
MacOS via Schijfhulpprogramma

Ook voor de Mac heb je geen externe **software** nodig om de toegang tot een externe harde schijf te beveiligen. De beveiliging moet je wel instellen voordat je de gegevens op het opslagmedium plaatst.

Open de tool Schijfhulpprogramma dat op iedere Mac staat. Selecteer in de **linkerkolom** de schijf of de usb-stick die je wilt beveiligen en gebruik dan de knop **Wis**. Je gaat hiermee dit station formatteren en je kunt dan meteen het station een nieuwe naam geven. In hetzelfde venster moet je ook een Structuur en een Indeling selecteren.

Bij Indeling ga je voor GUID-partitie-indeling. Als je dat hebt gedaan, kun je bij Structuur de optie Mac OS Uitgebreid (journaled) kiezen. Het systeem zal vragen om een wachtwoord dat je moet bevestigen en waarvoor je ook een aanwijzing moet opgeven als geheugensteuntje.

Als je dat allemaal gedaan hebt, klik je op de knop Wis. MacOS zal de gegevensdrager nu formatteren en versleutelen. Dit kost tijd, dus heb geduld. Als de versleuteling is afgerond, zul je iedere keer het wachtwoord moeten invoeren als je de gegevensdrager aan een pc koppelt.



In macOS moet je de schijf eerst formatteren, zodat je daarop later de gegevens kunt plaatsen die versleuteld moeten blijven.

Volume aanmaken

Naast de eigen programma's van Windows en Apple is er het externe programma **VeraCrypt**. Deze gratis coderingssoftware werkt vlot op **Windows**, macOS en Linux. Beschik je niet over BitLocker omdat je systeem op Windows Home draait, dan is dit een prima alternatief.

Na de installatie start je het programma op en sluit je de externe schijf aan op je computer. In het menu Instellingen kun je het programma bij Taal op Nederlands zetten. Wanneer je het programma uitvoert, verschijnt er een venster met een aantal stationsletters en enkele knoppen. Die heb je straks nodig om het versleutelde volume te koppelen. Negeer die lijst voorlopig en klik op de knop Volume aanmaken. Je komt vervolgens in de wizard terecht die je helpt een volume aan te maken.

De eerste optie, Een versleutelde bestandscontainer aanmaken, creëert een virtueel versleuteld gedeelte op de schijf, de rest van de schijf kan niet-versleutelde gegevens bevatten. Wij willen juist dat de volledige schijf versleuteld wordt, dus kiezen we voor de tweede optie: Een niet-systeempartitie/schijf versleutelen.

Vink de juiste optie aan om de volledige externe schijf te versleutelen.

Apparaat selecteren

In het volgende scherm van de wizard krijg je de keus tussen een Standaard VeraCrypt-volume of een Verborgen VeraCrypt-volume. De tweede optie gebruik je eigenlijk alleen als iets top secret moet blijven; het programma zal dan een tweede versleuteld volume binnen het eerste versleutelde volume creëren. In de meeste gevallen zal dat niet nodig zijn.

Maak het dus niet te complex en selecteer Standaard VeraCrypt-volume en klik weer op Volgende. Daarna moet je de externe gegevensdrager selecteren met de knop Apparaat selecteren. In het volgende venster kun je een bepaalde partitie selecteren of de volledige schijf.

Als er slechts één partitie op de schijf staat, is het mogelijk dat er een foutmelding verschijnt als je aangeeft dat de volledige schijf versleuteld moet worden. Dat los je op door die ene partitie te selecteren. Je komt dan terug in het vorige scherm waar het pad naar partitie op de juiste manier is ingevuld.

Ga door, zodat je in het scherm Modus volume aanmaken komt. De eerste optie zorgt ervoor dat VeraCrypt alle gegevens zal verwijderen die op de harde schijf zijn opgeslagen, voordat het de schijf gaat versleutelen.

De tweede optie houdt in dat VeraCrypt de gegevens die op de schijf staan, versleutelt zonder iets te verwijderen. De eerste optie is veel sneller, dus kies voor Versleuteld volume aanmaken en formatteren.

VeraCrypt toont het pad naar de partitie die het zal versleutelen.

Bewegen bewegen

In het scherm Versleutelingsopties moet je het coderingsalgoritme en het hash-algoritme kiezen. Heb je geen idee wat dit betekent, laat dit dan gerust op de standaardwaarden staan en klik op Volgende. Daarna volgt er nog een scherm om de grootte van het volume te dubbelchecken. Daarna is het eindelijk tijd om het wachtwoord voor de schijf op te geven.

VeraCrypt geeft duidelijk aan waaruit het wachtwoord moet bestaan. En tot slot is het de beurt aan het formatteren van de schijf. Hier moet je een tijdlang de muisaanwijzer willekeurig binnen het venster bewegen. Door onvoorspelbare bewegingen creëer je entropie. Dat is

een random nummergenerator in de software die willekeurige getallen genereert op basis van jouw bewegingen. Een groene progressiebalk geeft aan wanneer het algoritme klaar is. Wacht tot het versleutelingsproces is afgelopen, en klik op Formatteren.

Door muisbewegingen te maken, creëer je random getallen voor het encryptie-algoritme.

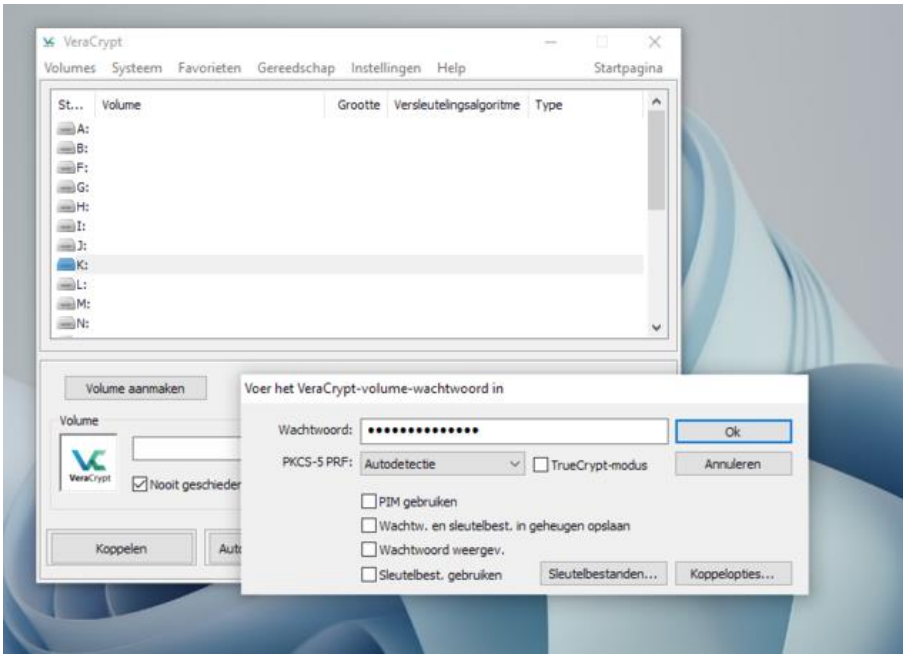
Koppelen

Wanneer de schijf is gecodeerd kun je uitsluitend toegang krijgen tot de inhoud door eerst de VeraCrypt-software te gebruiken. Het programma moet dus op iedere pc staan waarmee je iets op de schijf wilt kunnen opslaan. Het is belangrijk dat je weet dat je dit volume niet langer kunt benaderen via de oorspronkelijke stationsletter. Had het

volume voor de encryptie de letter D, dan ontvang je na de encryptie de melding dat dat station onleesbaar is. Om het versleutelde volume beschikbaar te maken, moet je de schijf via VeraCrypt koppelen met de pc.

Open VeraCrypt en selecteer een andere stationsletter uit de lijst, bijvoorbeeld H. Vervolgens klik je op de knop Automatisch koppelen. Nadat je het volume wachtwoord hebt opgegeven, klik op je op OK. De koppeling duurt eventjes en VeraCrypt waarschuwt zelfs dat je niet moet denken dat de applicatie is vastgelopen.

Ten slotte zie je dat het volume is gekoppeld aan de geselecteerde schijfletter. Je kunt het volume vervolgens openen vanuit VeraCrypt door erop te dubbelklikken. Of je kunt in Windows Verkenner de beveiligde schijf vinden met als schijfletter H.



Je kunt de versleutelde gegevensdrager openen vanuit VeraCrypt of –na koppelen –vanuit Windows Verkenner.

Back-up terugzetten op de iPad

Seniorweb

Maak regelmatig een back-up van de iPad. Die kunt u terugzetten als er iets heel erg misgaat op het apparaat of als u een nieuwe iPad hebt.

Back-up maken

In dit artikel bespreken we hoe gebruikers van iPadOS 14 en 15 via iCloud een eerder **gemaakte back-up op een iPad** terugzetten. U moet dus al een back-up hebben ingesteld.

iPad terugzetten naar fabrieksinstellingen (iOS 15)

Is er iets misgegaan en moet u de iPad helemaal opnieuw installeren? Dat werkt op onderstaande manier. Dit is echt een noodgreep, als er

iets heel erg fout is gegaan met het apparaat. De huidige inhoud en alle instellingen worden gewist.

- Tik op Instellingen > Algemeen.
- Tik op Zet over of stel iPad opnieuw in.
- Tik op Wis alle inhoud en instellingen.
- Tik op Ga door.
- Tik op Wis toch.
- Typ als erom wordt gevraagd, het wachtwoord van uw Apple-ID.
- Tik op Schakel uit.
- Tik op Wis iPad.
- Typ eventueel uw toegangscode.

De inhoud en alle instellingen worden gewist en de iPad start opnieuw op.

iPad terugzetten naar fabrieksinstellingen (iPadOS 14)

Is er iets misgegaan en moet u de iPad helemaal opnieuw installeren? Dat werkt op onderstaande manier. Dit is echt een noodgreep, als er iets heel erg fout is gegaan met het apparaat. De huidige inhoud en alle instellingen worden gewist.

- Tik op Instellingen > Algemeen.
- Tik op Stel opnieuw in.
- Tik op Wis alle inhoud en instellingen.
- Mogelijk meldt de iPad dat niet van alle apps een reservekopie is gemaakt. Bijvoorbeeld omdat u bepaalde apps hebt uitgesloten van de reservekopie. Tik op Ga door > Wis nu.
- Typ eventueel uw toegangscode.

- Tik in de twee volgende vensters op Wis om de inhoud en instellingen ook daadwerkelijk te wissen.
- Typ uw Apple ID-wachtwoord en tik op Wis.

De inhoud en alle instellingen worden gewist en de iPad start opnieuw op.

Back-up terugzetten (iPadOS 15 en 14)

Neem de volgende stappen om een eerder gemaakte back-up terug te zetten op de iPad:

- Schakel het apparaat in.
- Selecteer uw taal. Wij tikken op Nederlands.
- Selecteer uw land. Wij tikken op Nederland.
- Typ, indien gevraagd, de code van de simkaart en tik op Ok.
- Tik op Configureer handmatig.
- Tik op uw wifi-netwerk en voer eventueel het wachtwoord in.
- Tik op Verbind > Volgende.
- Apple geeft informatie over het gebruik van gegevens en privacy. Lees deze informatie en tik op Ga door.
- Stel eventueel op nieuwere apparaten Touch ID of Face ID in als toegangscode.
- Vul een toegangscode in en herhaal de code.
- Tik op Zet iCloud-reservekopie terug.
- Tik op achter 'Apple ID' op E-mail en vul uw Apple ID in.
- Tik op Volgende.
- Voer uw wachtwoord in en tik op Volgende.
- Eventueel krijgt u op een ander Apple-apparaat een verificatiecode. Vul deze code dan in.
- Lees eventueel de Algemene Voorwaarden en tik op Akkoord.
- De iPhone/iPad wordt geconfigureerd. Dit kan even duren. Daarna ziet u een aantal reservekopieën. Staat de reservekopie

die u wilt gebruiken hier niet tussen, tik dan op Toon alle reservekopieën.

Tik op de reservekopie die u wilt terugzetten. Dit is waarschijnlijk de meest recente.

- Tik op Ga door iPad up-to-date te houden.
- Stel eventueel de iCloud-sleutelhanger in. Wij doen dit nu niet en tikken op Gebruik iCloud-sleutelhanger niet.

Apple vraagt eventueel of u een creditcard of betaalkaart aan Pay wilt toevoegen. Wij doen dit nu niet en tikken op Configureer later in Instellingen. Had u op een gekoppeld apparaat (iPhone) al een betaalkaart toegevoegd, dan krijgt u in iPadOS 15 de suggestie om deze ook op de iPad te gebruiken. Wij willen dit niet en kiezen voor Configureer later in Instellingen.

- Nu komt eventueel de vraag of u audio-opnamen wilt delen met Apple om Siri te verbeteren. Wij doen dat niet en tikken op Niet nu.
- Bepaal of Apple uw gebruiksgegevens mag analyseren.
- De reservekopie wordt teruggezet. Dit kan even duren. De iPad start daarna opnieuw op. Typ, indien gevraagd, de code van de simkaart en tik op Ok.
- Typ uw zojuist ingestelde ontgrendelcode in.

Alle apps worden opnieuw gedownload en geïnstalleerd. Dit kan even duren.

Stichting Wijkgroep De Akkers

Namens Stichting wijkgroep de Akkers

Inlichtingen: tel: 0654692942
computerclubnissewaard@gmail.com