Encryptie, het beveiligen van uw gegevens

Binnen de cryptografie staat **encryptie** voor het coderen (versleutelen) van gegevens op basis van een bepaald algoritme. Deze versleutelde gegevens kunnen nadien weer gedecrypteerd (ontcijferd of gedecodeerd) worden zodat men de originele informatie weer terugkrijgt. Dit proces wordt **decryptie** genoemd.

Eén van de bedoelingen van cryptografie is dat gegevens veilig **uitgewisseld** kunnen worden tussen twee personen over een onveilig communicatiekanaal, dat wil zeggen een communicatiekanaal waar ook derden toegang toe kunnen hebben, zoals het internet. De versleuteling zorgt er dan voor dat deze derden de gegevens niet kunnen lezen. Dit gebeurt meestal door het gebruik van sleutels. Wat precies een sleutel vormt verschilt per algoritme, maar meestal is een sleutel een bepaald heel groot getal van enkele tientallen decimalen, tegenwoordig minimaal 2048 bits. Het doel van het cryptografische algoritme is dan om er voor te zorgen dat alleen de personen met de juiste sleutel de versleutelde gegevens weer kunnen ontcijferen. Je kunt dit natuurlijk ook gebruiken om informatie versleuteld **op te slaan**, zodat alleen degeen die de sleutel kent toegang heeft tot die informatie.

Er zijn grofweg twee vormen van cryptografie: symmetrische en asymmetrische.

Bij symmetrische cryptografie gebruiken zender en ontvanger dezelfde sleutel. Die sleutel moet van tevoren uitgewisseld worden via een veilig kanaal (waarbij zender en ontvanger elkaars identiteit kunnen controleren en onderschepping van de sleutel door derden niet mogelijk is). Bij opslag is duidelijk dat degeen die informatie opslaat dezelfde sleutel dient te gebruiken om de informatie weer te lezen.

Voor veilige verzending is de asymmetrische cryptografie, ook wel *public key encryption* genoemd. Hierbij hebben zender en ontvanger elk een eigen set van twee sleutels, waarvan er één publiek is en één geheim. Het is in theorie mogelijk, maar niet praktisch haalbaar, om de geheime sleutel uit de publieke sleutel af te leiden.

Berichten die met een publieke sleutel worden versleuteld, kunnen alleen met de geheime sleutel worden ontcijferd. Met andere woorden: onbevoegden kunnen het bericht niet lezen.

Andersom geldt dit ook: informatie die is vercijferd met de geheime sleutel van iemand, kan alleen met de bijbehorende publieke sleutel worden ontcijferd. Dit laatste wordt gebruikt bij het digitaal ondertekenen van berichten (bij voorbeeld betaalopdrachten van bedrijf naar bank): men heeft de zekerheid dat het bericht afkomstig is van degene die zich de afzender noemt.

De publieke sleutel mag aan iedereen bekend zijn en kan dus uitgewisseld worden over een onveilig kanaal zoals internet. Om een bericht te coderen en digitaal te ondertekenen, heeft de zender zijn eigen geheime sleutel nodig én de publieke sleutel van de ontvanger. Om het ontvangen bericht te decoderen en te verifiëren of de handtekening wel van de zender is, heeft de ontvanger zijn eigen geheime sleutel nodig én de publieke sleutel van de zender.

Een nadeel van asymmetrische cryptografie is dat grote sleutellengtes nodig zijn (bijvoorbeeld 4096 bits), waardoor coderen en decoderen veel rekenkracht vergen. Dit kan dan ook niet zonder een computer. De sleutels moeten groot zijn, omdat het anders mogelijk wordt met een snelle computer de geheime sleutel te vinden.

Hashing

Cryptografische hashing is in strikte zin geen versleuteling, omdat bij hashing uit de verkregen hash code de oorspronkelijke gegevens niet meer terug kunnen worden gehaald. Wel wordt bij hashing gebruikgemaakt van dezelfde technieken als bij versleuteling en vormt hashing ook vaak een onderdeel van versleutelingsprotocollen. Het verschil tussen hashing en encryptie is dus dat hashing maar 1 kant op kan (alleen hashen) en dat er bij encryptie twee kanten op gewerkt kan worden (coderen en decoderen). Hashen wordt met name gebruikt om de ongewijzigde staat van berichten te verifiëren (integriteit).

Hashing van wachtwoorden

Voor de aanmelding bij een computer zijn vaak een naam en een wachtwoord nodig. Deze wachtwoorden worden vaak versleuteld opgeslagen, zodat de wachtwoorden niet bekend worden als het bestand met wachtwoorden door een onbevoegde gelezen wordt. Dit gebeurt door middel van een hashing-algoritme, dat het onmogelijk maakt de versleutelde gegevens te decoderen. Dat is ook niet nodig, aangezien het voldoende is te controleren of de gebruiker het juiste wachtwoord heeft opgegeven.

> De lengte en complexiteit van wachtwoorden die mensen in de praktijk gebruiken is beperkt, terwijl computers steeds sneller worden. Daardoor wordt het voor iemand die probeert hashcodes voor wachtwoorden te kraken steeds makkelijker om een computer allerlei mogelijkheden te laten uitproberen. Hash-algoritmen voor wachtwoorden blokkeren deze methode, doordat voor deze algoritmen in te stellen is hoeveel rekentijd ze moeten kosten. De algoritmen worden dan zo ingesteld dat het uitrekenen ervan bijvoorbeeld één milliseconde kost, terwijl het berekenen van een hashcode met een gewoon hash-algoritme minder dan een microseconde kan kosten. Bij het controleren van een wachtwoord is het meestal geen probleem als dit een milliseconde in plaats van een microseconde kost, terwijl iemand die wil proberen de hashcodes te kraken meer dan duizend keer zo veel rekenwerk moet doen, en dus meer dan duizend keer langer bezig is.

Encryptie van bestanden

Door bestanden middels encryptie te versleutelen, kunnen ze alleen worden geopend door personen die in bezit zijn van de bijbehorende unieke sleutel en/of het wachtwoord. Encryptie kan erg nuttig zijn wanneer vertrouwelijke informatie wordt gedeeld, bijvoorbeeld als bijlage via e-mail of WeTransfer voor het verzenden van grote bestanden of opgeslagen via een online dienst als OneDrive, Skydrive, Google Drive of Dropbox. En wat te denken van makkelijk kwijt te raken mobiele middelen als smartphones, tablets, USB-sticks en DVD's. Pas wel op met het toepassen van encryptie: raakt de unieke sleutel en/of het wachtwoord kwijt dan zijn de bestanden ook voor u niet meer toegankelijk!

Houd het offline?

Als het een **grote ramp** zou zijn als een bepaald bestand openbaar wordt, dan hoort dat bestand waarschijnlijk überhaupt niet in de cloud te staan. Hoewel we regelmatig gebruikmaken van clouddiensten om onze data op te slaan, is er geen garantie dat er niet op je dienst zal worden ingebroken. Je hebt geen enkele controle over de beveiliging van

cloudservers, dus als er eentje gehackt wordt kun je niet veel meer doen om de schade te beperken. Tenzij je de informatie vooraf hebt versleuteld!

Bovendien moet je er maar op vertrouwen dat een clouddienst alle kopieën van je bestand van haar servers verwijdert wanneer je een bestand van je clouddienst verwijdert. Zorg dat je de servicevoorwaarden en het privacybeleid van het bedrijf goed doorneemt en begrijpt voordat je de dienst gebruikt om gevoelige informatie op te slaan.

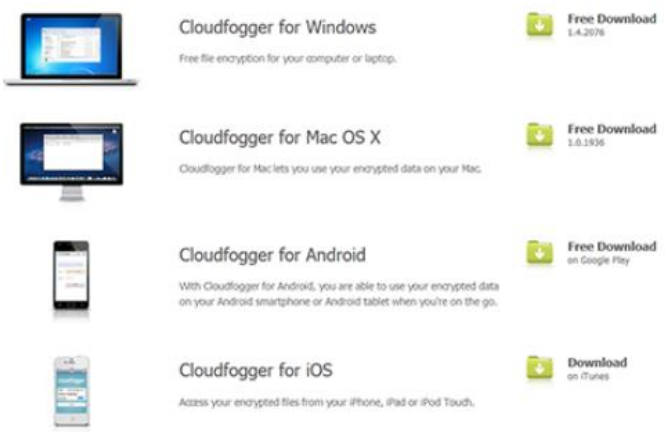
Maar soms heb je toch een plek nodig om je bestanden neer te zetten. Verwisselbare media apparaten zijn een relatief veilige optie - zolang je ze niet in vreemde computers of netwerken plugt of verliest- en ze geven je meer fysieke controle over je data. Behandel het zoals je een back-up behandelt en houd het niet in je computer geplugd.

Encryptie biedt dan de beste beveiliging. Er zijn tegenwoordig veel manieren om bestanden te versleutelen, maar ik bespreek hier enkele methodes. Elke methode heeft zijn eigen kenmerken, toepassingen en beperkingen.

Encryptiemogelijkheden met Cloudfogger

De gratis tool Cloudfogger (download: www.cloudfogger.com) past 256 bits AES-encryptie (Advanced Encryption Standard) toe op mappen en bestanden, zowel handmatig als volledig geautomatiseerd. Laatstgenoemde eigenschap maakt Cloudfogger bijzonder interessant bij gebruik van online opslagdiensten als OneDrive, Google Drive, Sky Drive, Dropbox e.d. Door de inhoud van de “online” map automatisch te laten versleutelen, wordt alleen nog de versleutelde data gesynchroniseerd. Cloudfogger is zeker niet de enige dienst die bestanden versleuteld in de cloud plaatst (zgn. client-side encryption), maar veel alternatieven zorgen ervoor dat die versleuteling plaatsvindt in de cloud zelf (zgn. server-side encryption). De makers van Cloudfogger vinden dat (terecht) niet de meest veilige manier en bieden een methode die ervoor zorgt dat de versleuteling al lokaal op je computer gebeurt.

Nadeel daarvan is uiteraard dat je op elke computer waarop je toegang wilt hebben tot de versleutelde bestanden, de software van Cloudfogger moet installeren. Je bestanden zijn te ontsleutelen met een wachtwoord. Het is dus van groot belang een sterk wachtwoord te kiezen en dit te onthouden.

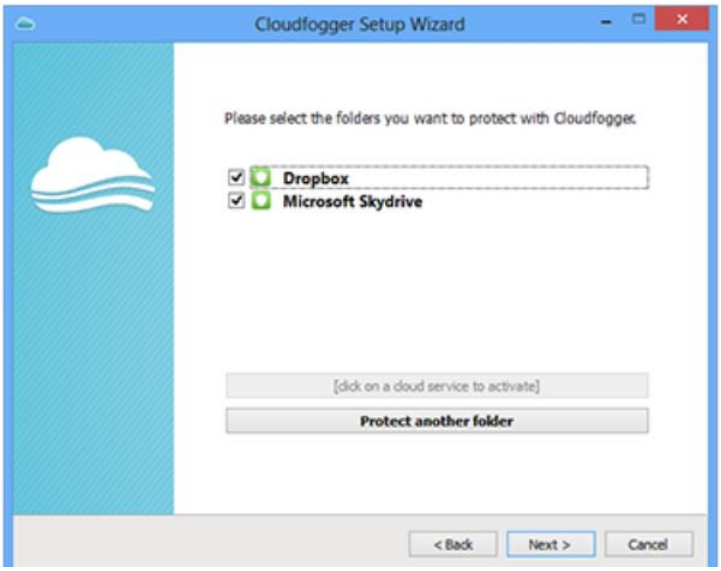


Wat we erg fijn vinden van Cloudfogger, is dat er niet van uit wordt gegaan dat we meerdere computers willen gebruiken. Ben je namelijk van plan slechts één pc te gebruiken in combinatie met de versleutelde opslagdienst, dan hoef je geen account aan te maken (dit is een optie binnen het programma), en kan je direct aan de slag; wel zo handig.

Meerdere computers

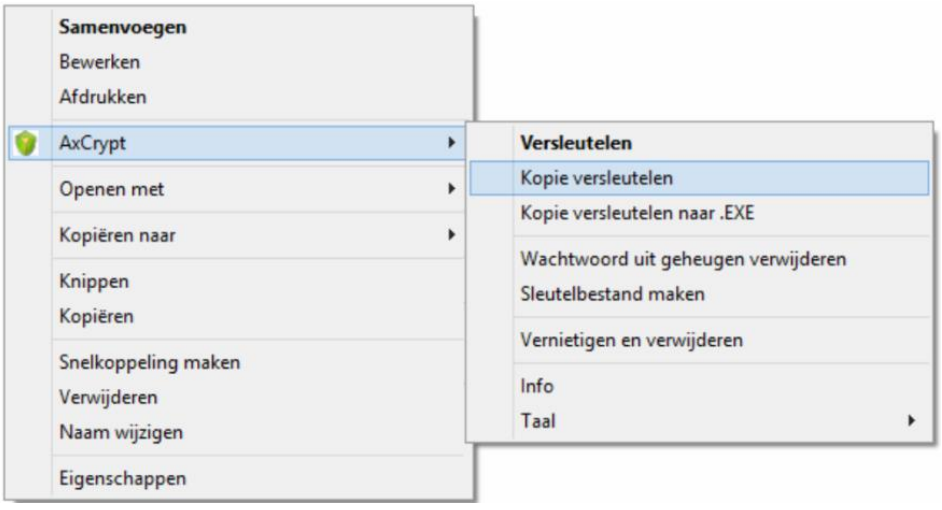
De kans is natuurlijk groot dat je wel meerdere computers wilt gebruiken om toegang te hebben tot je opgeslagen gegevens. Tijdens de installatie detecteert het programma zelf welke Cloud-diensten je gebruikt, waarna je encryptie voor deze diensten activeert (dit kan je altijd achteraf wijzigen). Verder hoef je helemaal niets te doen. Bestanden worden nu automatisch versleuteld wanneer je ze uploadt. **Ook wordt de huidige inhoud van de cloud-opslag gedownload en versleuteld weer teruggeplaatst.**

Wanneer je de software op een andere pc installeert en koppelt aan hetzelfde account, kan je die bestanden probleemloos weer downloaden en openen. De kracht van dit programma is naast veiligheid dan vooral ook de onzichtbaarheid. Installeren en direct weer vergeten, omdat het op de achtergrond z'n werk doet. Dat is ideale beveiliging.
Bestanden delen met anderen is overigens ook mogelijk, maar daarvoor moeten de ontvangers ook een Cloudfogger-account hebben.
Cloudfogger detecteert zelf welke Cloud-diensten je gebruikt, je hoeft zelf alleen maar aan te geven welke diensten je wilt beveiligen.



Encryptiemogelijkheden met AxCrypt

De gratis tool AxCrypt (download: www.axantum.com/AxCrypt) kan bestanden op twee manieren voorzien van encryptie: met een wachtwoord of met een zogenaamd sleutelbestand. Bijkomend voordeel van AxCrypt: het bestand wordt tegelijkertijd gecomprimeerd. Het versleutelen gaat heel eenvoudig door in de Windows Verkenner met rechts op een bestand te klikken en te kiezen voor de toegevoegde optie AxCrypt.



De eerste optie (Versleutelen) versleutelt het bestand zelf (het originele bestand krijgt nu de extensie AXX). Door deze

optie is er dus geen -zonder sleutel- leesbare versie van het bestand meer. De tweede optie (Kopie versleutelen) maakt een kopie van het originele bestand en versleutelt deze tot een AXX-bestand. De derde optie versleutelt een kopie van het origineel naar een EXE-bestand. Voor de ontvanger van dit EXE-bestand is installatie van het programma niet noodzakelijk, het wachtwoord weten is voldoende om het bestand te openen (enig nadeel is dat menig e-mailprogramma dergelijke EXE-bestanden als onveilig beschouwt en daarom voor de zekerheid ontoegankelijk maakt). Beschikt de ontvangende partij wel over dit programma (en het sleutelbestand), dan kan beter gebruik worden gemaakt van Kopie versleutelen.

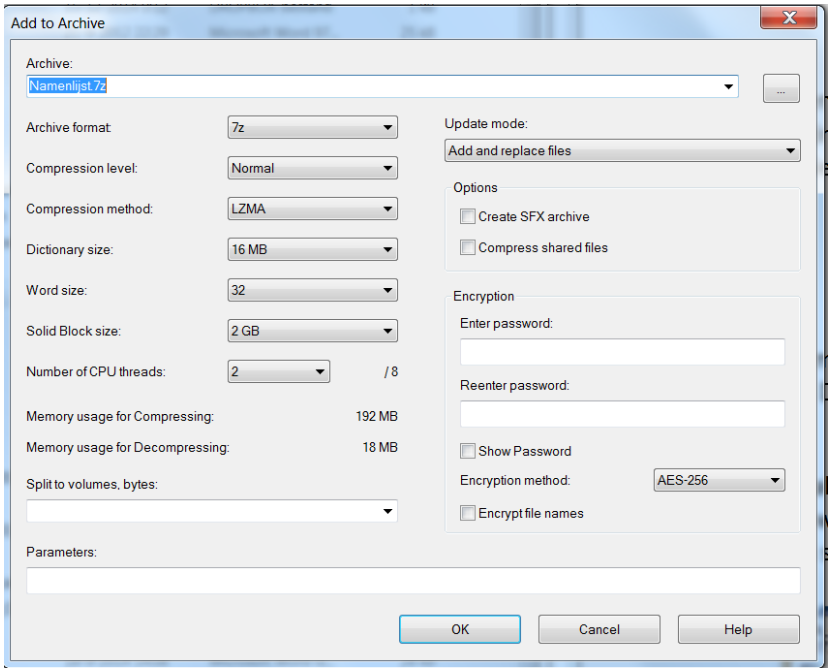
> TIP: Het is verstandig om, naast het sleutelbestand, ook de installatiesoftware van AxCrypt goed te bewaren zodat deze altijd weer geïnstalleerd kan worden wanneer toegang moet worden verkregen tot een in het verre verleden eens versleuteld bestand. Je weet namelijk nooit of de software dan nog te downloaden is...

Dat geldt wel voor **BoxCryptor,** wat voor alle platforms en cloudservices beschikbaar is. Kijk op http://computertotaal.nl/apps-software/beveilig-je-cloudopslag-met-boxcryptor-50745 voor een complete cursus hoe je BoxCryptor installeert en gebruikt, ook op Android. Opvalt, dat BoxCryptor van de versleutelde map een virtuele drive maakt in Windows, waardoor deze zich gedraagt zoals verder beschreven onder **Een hele schijf automatisch laten versleutelen.**
De gratis versie heeft beperkingen, maar deze zijn voor een relatief gering bedrag op te lossen.

Eenvoudige modus: 7-Zip

7-Zip is een snelle manier om je bestanden te versleutelen in een ZIP-archief. Het 7z formaat ondersteunt AES 256-bit encryptie, wat sterk genoeg is voor de meeste doeleinden. De bestanden in het archief worden versleuteld door middel van een wachtwoord.

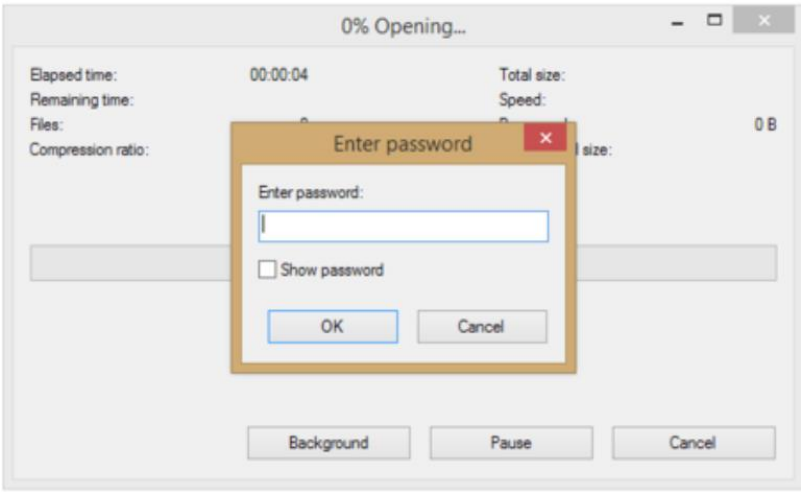
Voor Windows, download de 7-Zip software van de website van het project. De installatie zou slechts een paar seconden moeten duren. Daarna heeft de File Explorer (Windows Explorer voor Windows 7 gebruikers) een nieuw 7-Zip submenu in het contextmenu staan.



Om één of meer bestanden te versleutelen, selecteer ze, klik erop met de rechtermuisknop en selecteer **7-Zip > Add to archive...** in het dialoogvenster dat verschijnt, geef het archief een naam en voer een wachtwoord in om het te versleutelen. Je kunt ervoor

kiezen om ook de bestandsnamen te versleutelen als je bang bent dat ze de inhoud van de bestanden onthullen.

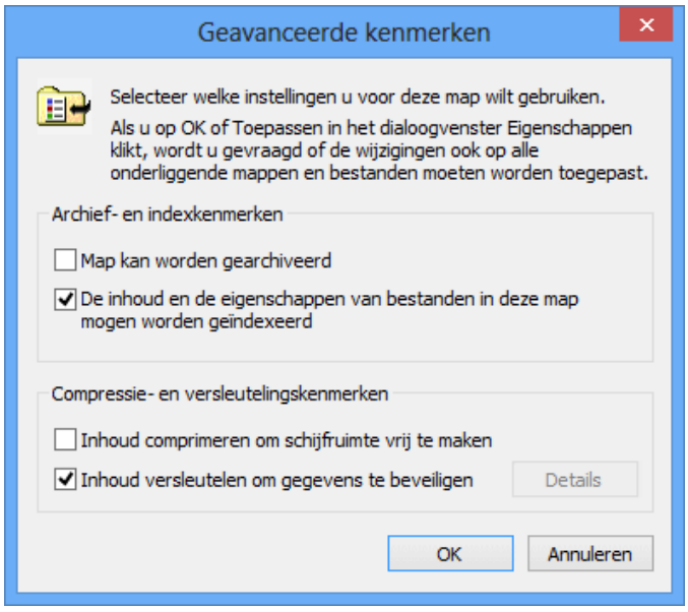
Als je klaar bent, klik op **OK** en 7-Zip zal het archief aanmaken en versleutelen. Het enige wat je hoeft te doen is het archief in de cloud of in een e-mail zetten. Of versleuteld op je computer te laten staan… maar het origineel bestaat ook nog!



Als je een wachtwoord met iemand moet delen, moet je zorgen dat de manier waarop je dat doet ook veilig is. (En nee, een privébericht op Facebook is niet veilig.) Gebruik in plaats daarvan een versleutelde e-mail of schrijf het op een stukje papier.

Het Encrypted File System (EFS) van Windows

Windows 7/8 Pro heeft ook de mogelijkheid bestanden te beveiligen door middel van encryptie, het gaat dan alleen om de bestanden die op de computer staan. Deze methode staat ook wel bekend onder de naam Encrypted File System (EFS) en is alleen bruikbaar voor partities met een NTFS-indeling. Een bestand of map kan worden voorzien van EFS-encryptie door er met rechts op te klikken en te kiezen voor Eigenschappen, knop Geavanceerd, activeer de optie Inhoud versleutelen om gegevens te beveiligen.



Zolang het mogelijk is in te loggen met het gebruikersaccount, behoudt de gebruiker toegang tot de versleutelde bestanden. Het is dus voor het ontsleutelen van de bestanden niet noodzakelijk een code te onthouden. Het account wordt namelijk gekoppeld aan een unieke EFS-sleutel. Is het echter niet meer mogelijk Windows op te starten en in te loggen met het gebruikersaccount (om wat voor redenen dan ook), dan is er ook geen toegang meer tot de met EFS versleutelde bestanden. Voor u er erg in heeft zijn de gegevens dus echt niet meer toegankelijk!

Door de unieke EFS-sleutel te kopiëren naar een USB-stick kan op een andere PC of onder een andere gebruikersnaam weer toegang worden verkregen tot de versleutelde bestanden. Stel de sleutel daarom veilig via het configuratiescherm, onderdeel Gebruikersaccounts, taak Uw certificaten voor bestandsversleuteling beheren. Gebruik hiervoor wel een veilige, gemakkelijk te onthouden locatie die niet 'encrypted' is ;-).

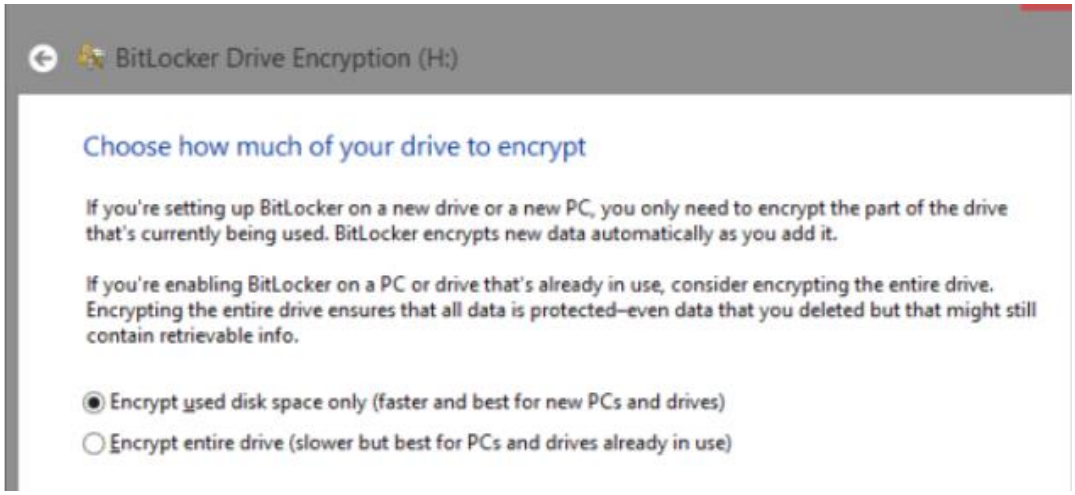
Een hele schijf automatisch laten versleutelen.

In plaats van het versleutelen van een of meer bestanden of zelfs mappen, zijn er ook mogelijkheden om een hele schijf (drive letter) in te richten zodat alles wat er op staat of op geschreven wordt automatisch versleuteld wordt.

Encryptie van een schijf: BitLocker

BitLocker versleutelt alleen harde schijven, maar het doet dat erg goed. BitLocker, beschikbaar in de Windows versies Ultimate en Enterprise, is verbeterd voor Windows 7 en 8 en biedt bescherming voor alles, van documenten tot wachtwoorden, door het gehele station met Windows en uw gegevens te versleutelen. Zodra BitLocker is ingeschakeld, worden alle bestanden die u op dit station opslaat automatisch versleuteld.

BitLocker zal je niet helpen als je dingen in de cloud moet opslaan, maar als iemand je harde schijf in handen krijgt kan hij of zij niet zien wat erop staat.
U kunt met behulp van BitLocker-stationsversleuteling alle bestanden beveiligen die zijn opgeslagen op het station waarop Windows is geïnstalleerd (het station van het besturingssysteem) en op **vaste gegevensstations** (zoals interne harde schijven).



Anders dan bij EFS (Encrypting File System), waarmee u afzonderlijke bestanden kunt encrypten wordt met BitLocker het gehele station versleuteld. U kunt zich normaal aanmelden en op de gebruikelijke wijze met uw bestanden werken, maar dankzij BitLocker krijgen hackers geen toegang tot de systeembestanden waaruit ze uw wachtwoord zouden kunnen achterhalen. Ook krijgen ze geen toegang tot uw harde schijf als ze deze uit de computer verwijderen en in een andere computer installeren.

Wanneer u nieuwe bestanden toevoegt aan een station dat is versleuteld met BitLocker, worden deze automatisch versleuteld. Bestanden blijven alleen versleuteld terwijl ze zijn opgeslagen op het versleutelde station. Bestanden die naar een ander station of naar een andere computer worden gekopieerd, worden ontsleuteld. Als u bestanden deelt met andere gebruikers, bijvoorbeeld via een netwerk, zijn deze bestanden versleuteld terwijl ze op het versleutelde station zijn opgeslagen. Ze kunnen door bevoegde gebruikers echter normaal worden geopend.

Met behulp van BitLocker To Go (beschikbaar op Windows 7 en8 Professional en Enterprise versies) kunt u alle bestanden beveiligen die zijn opgeslagen op **verwisselbare** gegevensstations (zoals externe harde schijven of USB-flashstations).

Zo zet je die sexy selfies veilig in de cloud

Zoals sommige sterren onlangs op een pijnlijke manier hebben ondervonden, zijn je privébestanden niet per se veilig omdat je ze naar de cloud hebt geüpload. Computersystemen kunnen gekraakt worden, en die handige cloud kan al snel roet in het eten gooien.

Iedereen heeft gevoelige bestanden die ze graag privé willen houden: medische dossiers, liefdesbrieven, fiscale documenten, en ja, misschien zelfs een paar naaktfoto's van jezelf of een dierbare. Het probleem is dat als je bestanden eenmaal naar de cloud uploadt, je de controle over wie ze kan zien enigszins uit handen geeft.

Maar er zijn een aantal stappen die je kunt nemen om je meest persoonlijke data tegen pottenkijkers te beschermen. Er is alleen wat tijd en focus voor nodig...

Voor bestanden, documenten hebben we hiervoor uitgelegd hoe je deze zelf beveiligt door versleuteling toe te (laten) passen.

Als je cloud-apps op je telefoon geïnstalleerd hebt, is de kans groot dat ze automatisch elke foto die je maakt naar de cloud uploaden. Dropbox, Google+, en iCloud doen dit standaard. Dat klinkt eng, maar het is eigenlijk als handigheid bedoeld: Als je telefoon gewist, gestolen of kapotgemaakt wordt, heb je de foto's nog altijd online staan. Maar dit betekent dat je moet nadenken voordat je een foto maakt. Als je een afbeeldingen liever niet deelt, open dan de instellingen van je app, zoek naar 'automatische foto-uploads', en schakel deze optie uit. Kopieer vervolgens handmatig de foto’s naar de versleutelde “online” map voor een beveiligde kopie.

En vergeet niet dat een foto die je van je telefoon verwijdert niet noodzakelijk ook meteen uit de cloud verwijderd wordt. Als je wilt dat een foto voor eens en voor altijd weg is, zorg dan dat je inlogt op de clouddienst en controleer het handmatig. Verwacht niet zomaar dat alles in orde is. Controleer het gewoon even.