Computerveiligheid

MINI COMPUTER CLUB ALMELO

Wat is computerveiligheid?

Beveiliging van computers, randapparatuur, software, data en ict-installaties tegen diefstal, verlies, beschadiging, misbruik en/of ongeauthoriseerd gebruik.

Wat kan je daaraan doen?

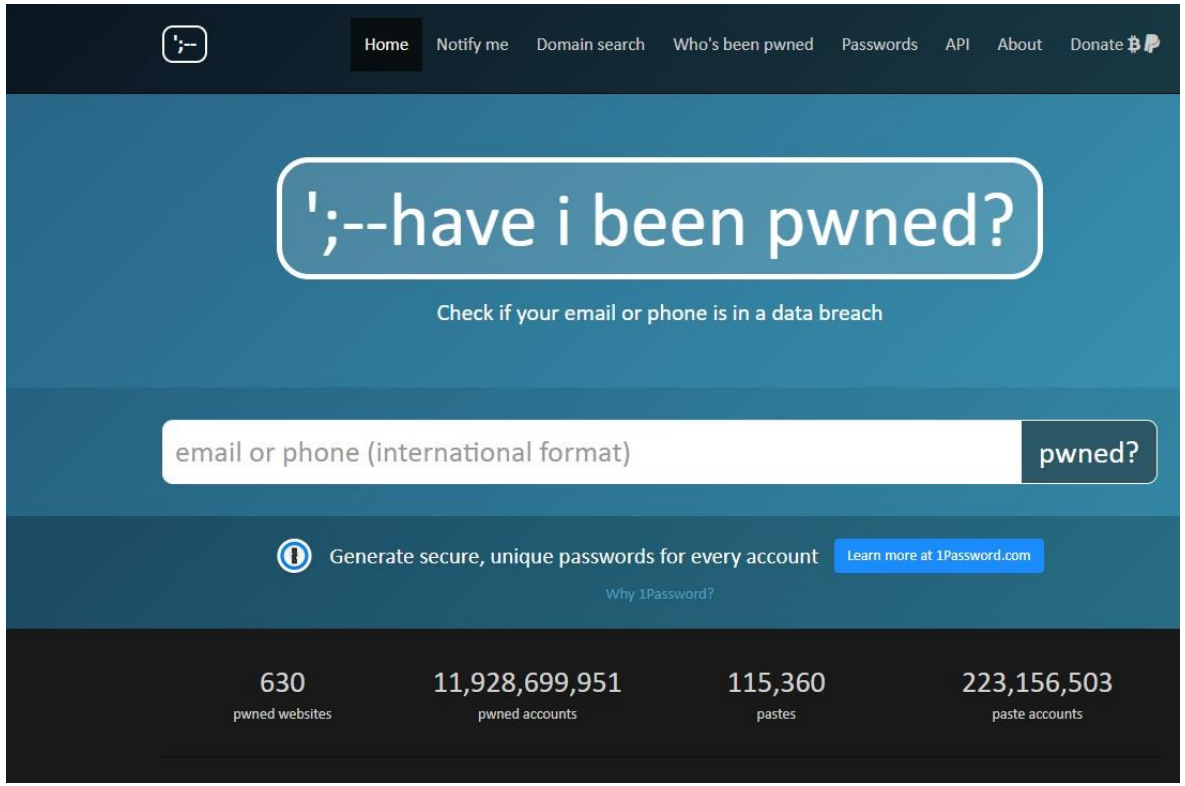
- Gebruik vooral je boerenverstand
- Controleer bij tijd en wijle of je gehackt bent
- Wees bedacht op phishing
- Zorg ervoor dat Windows up-to-date is
- Activeer een goede virusscanner
- Maak wachtwoorden niet te makkelijk, zo mogelijk met 2 stapsverificatie
- Gebruik officiële software
- Maak periodiek een back-up

MINI COMPUTER CLUB ALMELO

Ben ik gehackt?

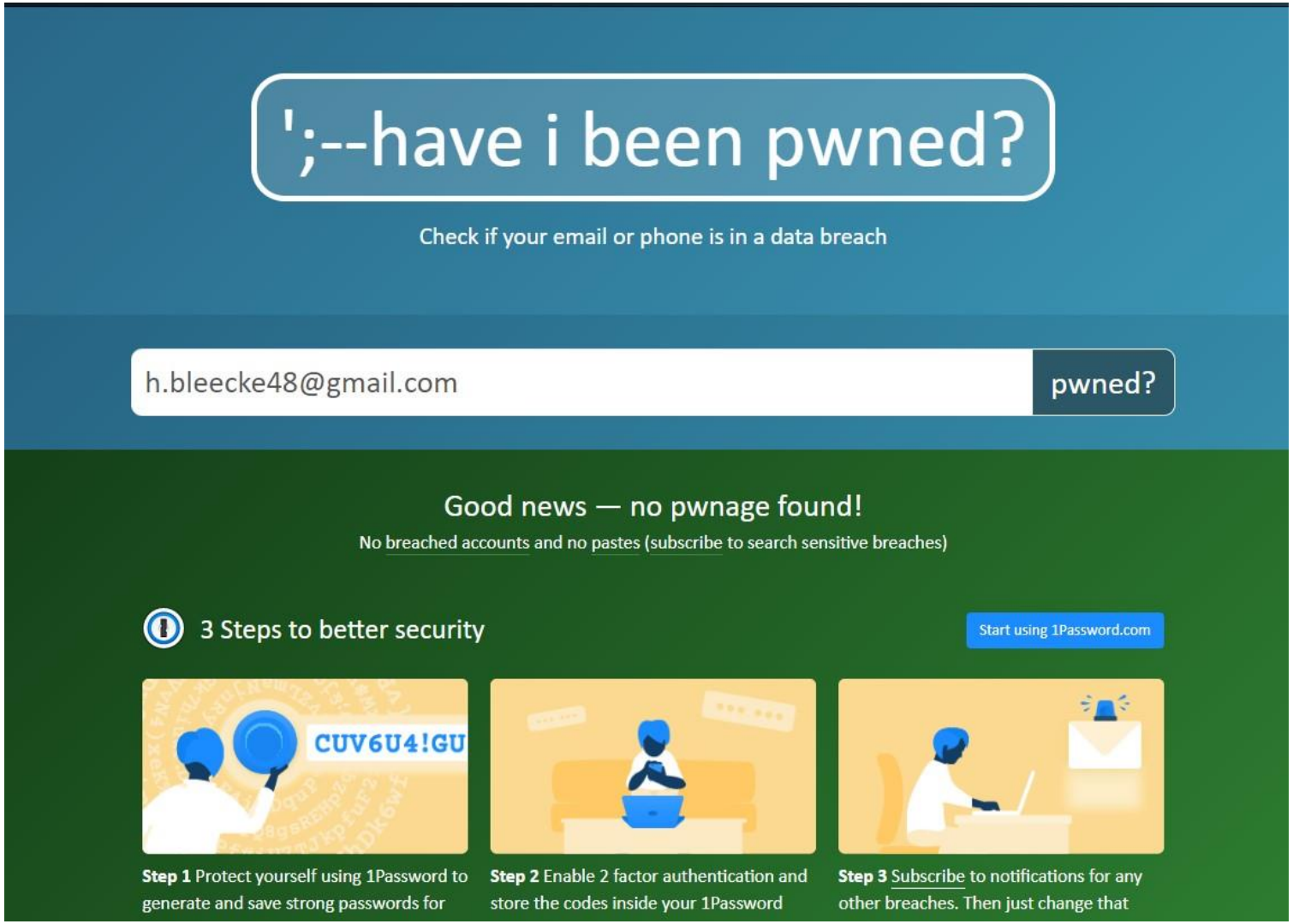
Controle of je e-mailadres of eventuele andere gegevens zijn buitgemaakt door hackers na een datalek.

De link hiernaast geeft daartoe de mogelijkheden: https://haveibeenpwned.com/



MINI COMPUTER CLUB ALMELO

Met als resultaat:



MINI COMPUTER CLUB ALMELO

Help! Ik ben gehackt

Probeer kalm te blijven

Hoewel het verleidelijk is om nu in paniek te raken, zal dat je zeker niet helpen. Merk je dat je gehackt bent, neem dan vijf minuten de tijd om op adem te komen en ga de boel niet overhaast proberen te redden. Het kwaad is al geschied en wat je nu doet is belangrijk. Als je het hoofd koel houdt kun je beter en gerichter handelen en zo de schade (misschien) enigszins beperken.

Verbreek de verbinding met het wifi-netwerk

Een veelgemaakte fout is dat mensen denken dat ze het apparaat moeten uitzetten. Zo kunnen bestanden en/of gegevens echter verloren gaan. Laat het apparaat dus aan staan, maar verbreek wel meteen de verbinding met het wifi-netwerk. Doe dit niet alleen voor het gehackte apparaat, maar voor al je apparaten die met het internet verbonden zijn. Hackers krijgen meestal toegang via het internet, dus zo zet je hen (voor nu) buitenspel. De kans dat ze al gegevens en/of bestanden in handen hebben is er dan helaas nog wel.

Verander je wachtwoorden

Als het je nog lukt om in te loggen bij je accounts, verander je wachtwoorden dan onmiddellijk. Kies voor wachtwoorden met zowel tekens als cijfers en symbolen. Hoe meer tekens, hoe beter. Mits mogelijk, kies dan voor een tweestapsverificatie. Verander je wachtwoorden nooit vanaf het gehackte apparaat, want misschien kijkt de hacker mee.

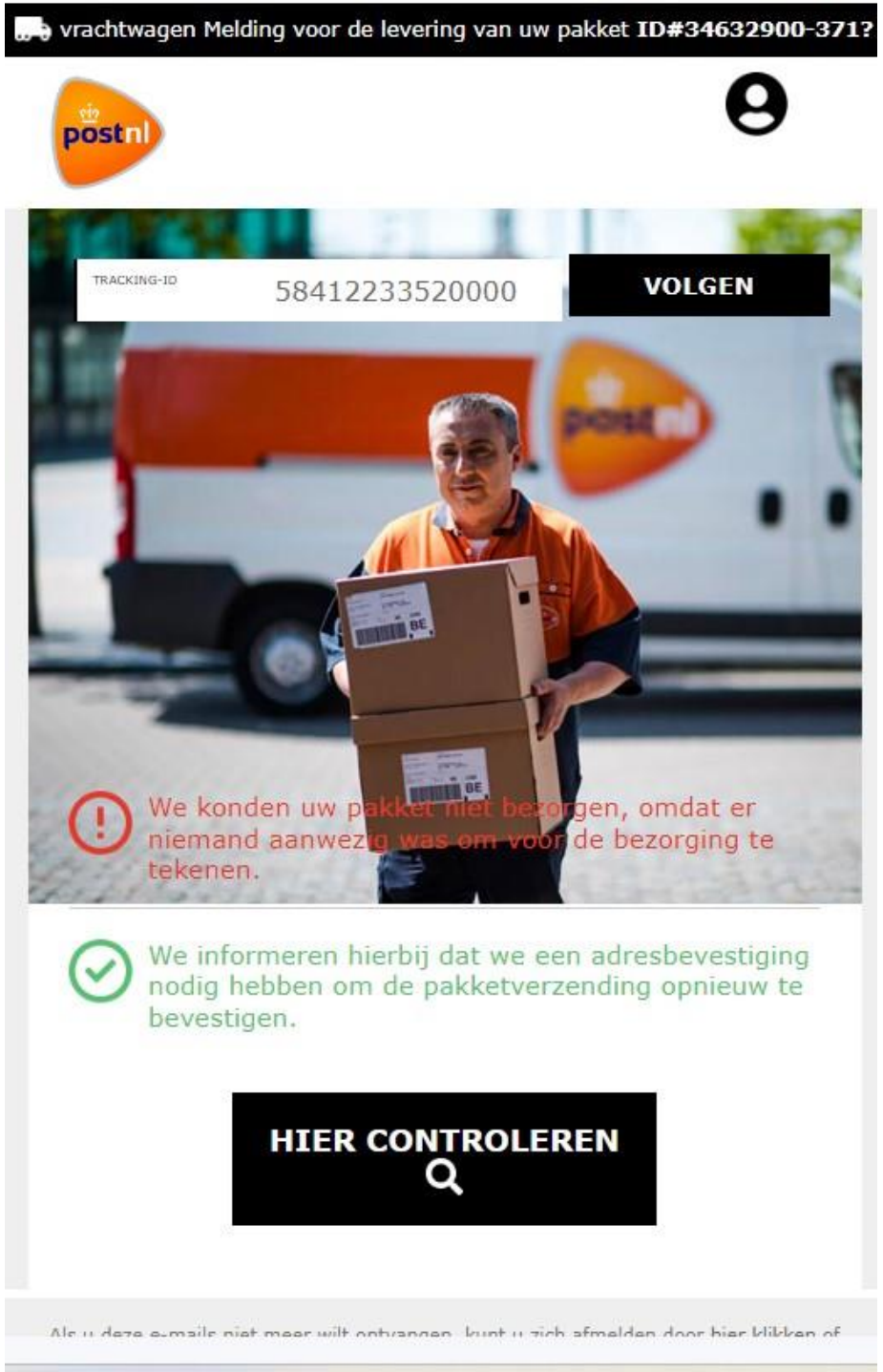
Zoek uit wat er precies aan de hand is en onderneem actie

Cybercriminaliteit is er in vele soorten en maten. De acties die je moet ondernemen verschillen per vorm van cybercriminaliteit. Hieronder vind je de meest voorkomende vormen.

Malware
Malware is een verzamelnaam voor slechte software met kwaadaardige bedoelingen. Een goede malware scanner kan malware opsporen. Doe een uitgebreide scan en verwijder de software.
Ransomware
Bij ransomware blokkeren cybercriminelen je computer en/of gegevens en moet je betalen om weer toegang te krijgen. Betaal niet! Op de website van het No More Ransom project, een initiatief van onder andere de Nederlandse politie, vind je decryptietools. Doe ook online aangifte, zodat de politie op jacht kan naar de daders.

Phishing

Bij phishing lokken criminelen je per e-mail, sms of WhatsApp naar een valse website, waar ze gegevens of geld stelen. Heb je per ongeluk op een link geklikt? Laat je apparaat controleren op schadelijke software en verander zo snel mogelijk je wachtwoorden. Wacht sowieso met internetbankieren totdat je zeker weet dat je apparaat schoon is. Neem daarnaast contact op met de instantie waar het om gaat.
Heb je alles geprobeerd, maar kom je er niet uit? Als er veel op het spel staat, is het raadzaam een specialist die zich bezighoudt met cybersecurity voor bedrijven in te schakelen.



MINI COMPUTER CLUB ALMELO

Phishing herkennen

Hoewel oplichters goed zijn in het namaken van officiële e-mails, zijn er wel een aantal dingen die kunnen opvallen:

- Phishing gebeurt meestal uit naam van banken, de overheid, bedrijven en abonnementsdiensten.
- Er wordt gevraagd op een link of betaalverzoek te klikken.
- Er is haast geboden.
- Er staan taal- en stijlfouten in het bericht.
- Het e-mailadres lijkt op dat van het nagemaakte bedrijf, maar is vaak net iets anders. Bijvoorbeeld 'Zigggo' (met een extra ‘g’) of 'ING-betalen.nl' (een domein dat niet van ING zelf is).
- Vreemde bijlages. Klik hier vooral niet op, ze kunnen virussen bevatten.

Ik heb (per ongeluk) een bijlage geopend uit een nepmail

- Sluit het e-mailprogramma af.
- Laat de virusscanner een uitgebreide scan van de computer uitvoeren en schadelijke software verwijderen.
- Wijzig voor de zekerheid (belangrijke) wachtwoorden. Zeker die van uw e-mail en de bank.
- Gebruik een ander apparaat (bijvoorbeeld via de internetverbinding van uw smartphone) voor internetbankieren totdat u er zeker van bent dat er geen schadelijke software op de pc aanwezig is.

MINI COMPUTER CLUB ALMELO

Voorkomen is beter dan genezen

Zodra de hackers de deur zijn gewezen, kun je je focussen op het voorkomen van toekomstige cyberaanvallen. Met deze tips behoed je jezelf zoveel mogelijk tegen cybercriminaliteit:

- Installeer een goede antivirussoftware en firewall. Zorg dat deze up-to-date blijven.
- Let goed op voordat je op een link klikt of je inloggegevens invult. Zet tweestapsverificatie aan voor al je online accounts. Naast het invoeren van je wachtwoord, krijg je dan een unieke code op je telefoon die je ook moet invoeren. Zo creëer je een extra beveiligingslaag.
- Voer software-updates altijd meteen uit zodra je een melding krijgt.
- Gebruik geen wachtwoorden, maar wachtzinnen. Hoe langer je wachtwoord, hoe moeilijker het te kraken is. Gebruik bijvoorbeeld: ”Ik ben in 2019 op vakantie geweest naar Spanje!” in plaats van “Spanje2019!”. Wijzig ze bij tijd en wijle.
- Kijk uit met openbare wifi-netwerken. Kwaadwillenden kunnen gemakkelijk met je meekijken op zo’n netwerk en je mogelijk omleiden naar sites met kwaadaardige code. Gebruik bij voorkeur je mobiele dataverbinding.
- Zet je computer/laptop niet op slaapstand, maar helemaal uit.
- Maak regelmatig back-ups van je bestanden.
- Scherm de toegang tot belangrijke bestanden af.

MINI COMPUTER CLUB ALMELO

Windows update

Via Start>Instellingen> Windows update kunnen we controleren of uw systeem geheel bij de tijd is. Eventueel kunt u via de knop “Alles installeren” de laatste wijzigingen aanbrengen.

MINI COMPUTER CLUB ALMELO

Virusscanners

Een van de manieren om je computer te controleren op virussen en malware is het gebruik van een virusscanner. Er zijn verschillende virusscanners te verkrijgen. Daarvoor moet je echter wel een abonnement afsluiten. Een goed alternatief is tegenwoordig Microsoft Defender.

Microsoft Defender

Microsoft Defender (voorheen Windows Defender genoemd) had in het verleden een matige reputatie. Maar tegenwoordig scoort het programma best goed in de tests. Er zijn uitgebreidere virusscanners, maar Defender is een aanrader: het is gratis, werkt goed en krijgt geregeld nieuwe updates.
Defender is goed in het opmerken van malware op de computer. Het programma blokkeert echter geen phishingsites, terwijl andere (gratis) virusscanners dat wel doen.

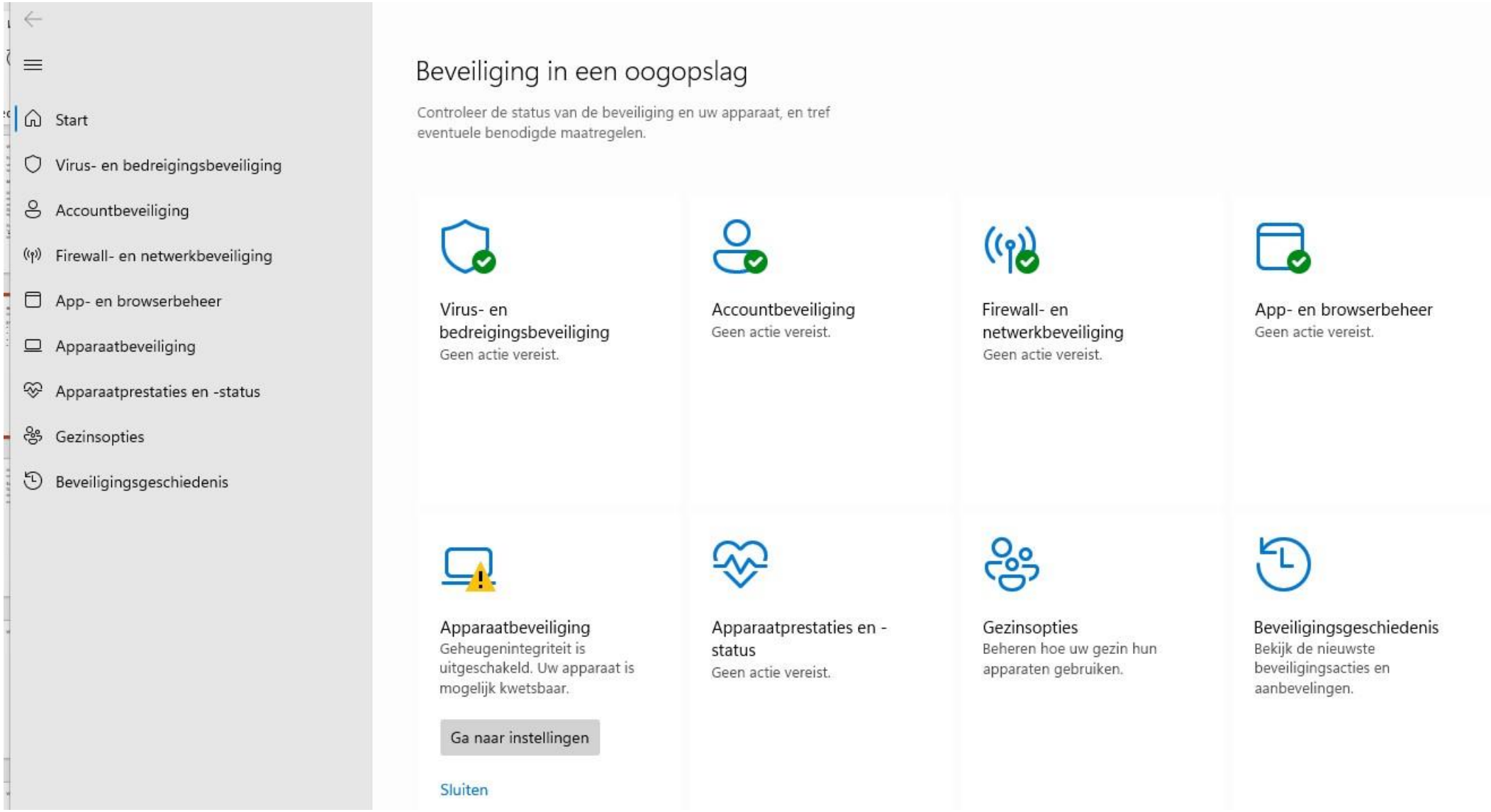
Een directe reden om een ander programma te installeren is dit niet, maar wie optimaal beschermd wil zijn kan eens de 'Keuzehulp virusscanner' doorlopen. Houd het wel bij één alternatief. Meerdere virusscanners installeren is een slecht idee; ze gaan elkaar in de weg zitten en geven dan problemen.

Het Microsoft Defender-beveiligingscentrum

In het Microsoft Defender-beveiligingscentrum staat onder meer wanneer de computer voor het laatst is gescand op virussen en wanneer de laatste update was. Open het beveiligingscentrum zo:

- Klik op de Startknop.
- Klik op **Instellingen**.
- Klik op **Privacy en beveiliging**.
- Klik links op **Windows-beveiliging** > **Windows-beveiliging openen**.

Het Defender-beveiligingscentrum bestaat uit zeven/acht onderdelen. Als alles oké is, staat er bij de meeste onderdelen een groen vinkje. Als een onderdeel actie van u vraagt, staat dit er duidelijk bij. U kunt door de verschillende links aan te klikken de werking ervan onderzoeken.



MINI COMPUTER CLUB ALMELO

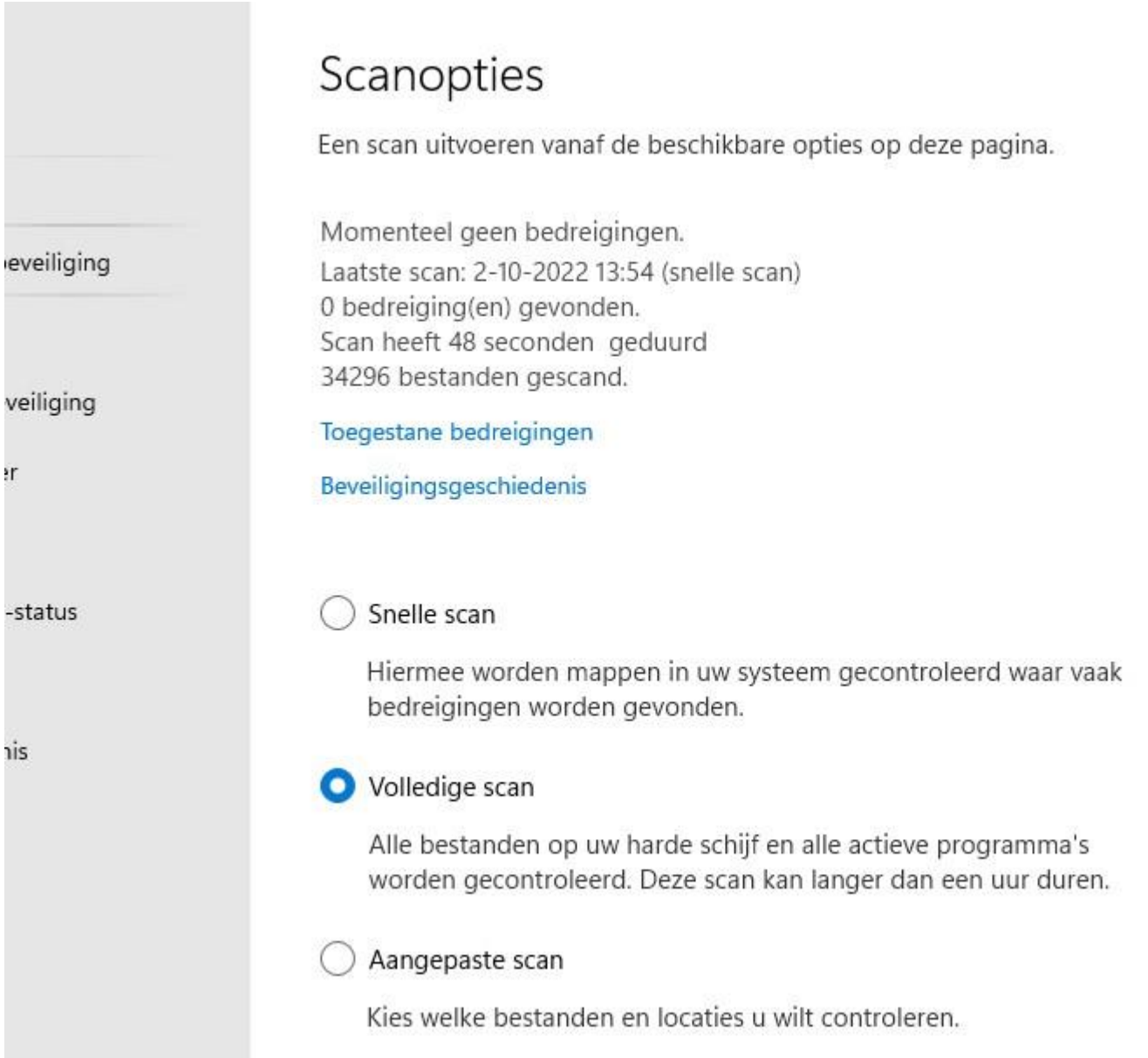
Scannen op virussen

Defender scant als de computer regelmatig op virussen. U merkt er niks van, tenzij het programma een dreiging vindt. U kunt ook zelf een scan starten. Bijvoorbeeld als de computer ineens gek doet. Of als u op een verdachte link of bijlage klikte, en denkt dat er nu een virus actief is.

- Klik in het Microsoft Defender-beveiligingscentrum op **Virus- en bedreigingsbeveiliging**.
- Bij 'Huidige bedreigingen' staat wanneer de laatste scan is uitgevoerd, hoeveel bestanden zijn gescand en of er bedreigingen zijn gevonden.
- Klik op **Snelle scan** om direct een scan van de computer te starten. De scan duurt meestal hooguit een paar minuten. U kunt de computer gewoon gebruiken tijdens het scannen.

- Wilt u een grondige scan van de computer, klik dan op **Scanopties**.

- Klik op uw keuze, bijvoorbeeld **Volledige scan**.
- Klik op **Nu scannen**.



In het eerder getoonde venster is duidelijk dat de geheugenintegriteit is uitgeschakeld. Dit kan je inschakelen door op de link eronder te klikken.

Deze kernisolatie is een beveiligingsfunctie van Microsoft Windows die belangrijke kernprocessen van Windows beveiligt tegen schadelijke software door ze in het geheugen te isoleren.

Kernisolatie

Beveiligingsfuncties beschikbaar op uw apparaat met beveiliging op basis van virtualisatie.

Hiervoor moet uw apparaat opnieuw worden opgestart.

Geheugenintegriteit

Voorkomt dat bij aanvallen kwaadaardige code wordt ingevoegd in streng beveiligde processen.

⚠ Geheugenintegriteit is uitgeschakeld. Uw apparaat is mogelijk kwetsbaar. Sluiten

Aan

Meer informatie

Blokkeringslijst voor Microsoft-kwetsbare stuurprogramma's

Stuurprogramma's met beveiligingsproblemen kunnen niet worden uitgevoerd op uw apparaat, omdat dit wordt geblokkeerd door Microsoft.

Aan

Meer informatie

Veilig met een wachtwoord

Een wachtwoord is een combinatie van cijfers, letters en leestekens waarmee u online informatie beveiligt. Het is de sleutel tot allerlei gegevens en diensten: uw e-mailaccount, een internetabonnement of internetbankieren. Zo'n wachtwoord zorgt dat alleen u dingen kunt wijzigen of aanvragen.

Valkuilen bij wachtwoorden
Er is een aantal dingen erg belangrijk als het om wachtwoorden gaat.

- **Wijzig het standaardwachtwoord**
  Soms krijgt u als u een account aanmaakt een wachtwoord toegewezen. Het is verstandig dit wachtwoord te wijzigen, want lijsten met standaardwachtwoorden worden wel eens gestolen door hackers.
- **Kies geen makkelijk wachtwoord**
  Wachtwoorden moet u onthouden, daarom kiezen veel mensen een makkelijke. Denk aan een geboortedatum of eenvoudige cijferreeks. Dat is niet veilig, want een computercrimineel die accounts van anderen wil hacken, probeert altijd eerst de veelgebruikte wachtwoorden.

MINI COMPUTER CLUB ALMELO

- **Gebruik niet één wachtwoord voor alles**
  Hetzelfde wachtwoord voor alles betekent minder om te onthouden. Toch is het niet verstandig: mocht het bekend raken, dan kunnen andere mensen ook bij al uw accounts inbreken.

Makkelijke wachtwoorden vragen dus om moeilijkheden. Maak bij voorkeur hele zinnen voor belangrijke gegevens. Hou uw gegevens uptodate wanneer u ergens uw wachtwoorden opschrijft. Maar al te vaak worden wachtwoorden ergens opgeschreven en zijn ze op het “moment surpreme” niet terug te vinden.

Gebruik indien mogelijk 2 stapsverificatie.

Wat is tweestapsverificatie?

Tweestapsverificatie is een extra beveiliging en legitimatie. Stel het in om de online toegang tot gevoelige zaken, zoals internetbankieren, beter te beschermen.

MINI COMPUTER CLUB ALMELO

Tweestapsverificatie

Het is veiliger als iemand op meerdere manieren zijn identiteit moet bevestigen. Daarin onderscheidt men drie opties:

1. **Wat iemand weet**
   Bijvoorbeeld een gebruikersnaam met wachtwoord.
2. **Wat iemand heeft**
   Bijvoorbeeld een telefoon. Waar een sms-code naartoe kan worden gestuurd of via een app uw identiteit kan worden bevestigd.
3. **Wat iemand is**
   Bijvoorbeeld een vingerafdruk of een gezicht.

Combineer twee van deze zaken en voilà; dat is tweestapsverificatie. Gebruikers moeten bijvoorbeeld eerst hun gebruikersnaam en wachtwoord invullen. Daarna krijgen ze een sms op hun smartphone. Pas wie de sms-code invult, krijgt toegang.

Voorbeelden

Misschien bent u al eens tegen tweestapsverificatie aangelopen. Sommige sites met een DigiD-inlog gebruiken deze extra beveiliging. Ook veel grote bedrijven als Apple, Google, Facebook en Microsoft doen dat. Hieronder staan een aantal bedrijven die informatie geven over de manier waarop ze tweestapsverificatie toepassen:

- Apple
- DigiD
- Dropbox
- Facebook
- Google
- LinkedIn
- Microsoft
- Twitter
- WhatsApp

Bijvoorbeeld inloggen bij ZGT Almelo.

www.zgt.nl

Klik “MijnZGT”.

Inloggen

DigiD staat voor Digitale Identiteit; het is een gemeenschappelijk systeem waarmee de overheid op internet uw identiteit kan verifiëren. U kunt zelf uw DigiD aanvragen op https://www.digid.nl. Met uw DigiD kunt u bij steeds meer overheidsinstellingen terecht.
Bij Ziekenhuis Groep Twente kunt u inloggen met uw DigiD. Voortaan kunt u met DigiD naar steeds meer overheidsinstellingen op internet.

DigiD

Inloggen

EN | NL

DigiD **Inloggen bij**
Ziekenhuisgroep Twente - Patientenportaal

Hoe wilt u inloggen?

Met de DigiD app
De makkelijkste manier om veilig in te loggen ›

Met een sms-controle ›

Met mijn identiteitskaart ›

MINI COMPUTER CLUB ALMELO

Inloggen bij
Ziekenhuisgroep Twente - Patientenportaal

Vul hieronder uw gebruikersnaam en wachtwoord in

DigiD gebruikersnaam

Wachtwoord

Onthoud mijn DigiD gebruikersnaam

‹ Vorige

Inloggen ›

Inloggen bij
Ziekenhuisgroep Twente - Patientenportaal

Er is een sms-code gestuurd naar: XXXXXXX978

Verzonden op: 1 oktober 2022, 16:34 uur (Nederlandse tijd).

Vul de sms-code in die u heeft ontvangen.

U heeft een sms-code ontvangen. Deze bestaat uit 6 cijfers. Vul de code in de 6 invoervelden hieronder in.

Geen code ontvangen?

‹ Annuleren

Volgende ›

MINI COMPUTER CLUB ALMELO

zgt

Home | Agenda | Dossier | E-Consult | Vragenlijsten | Mijn gegevens

- Agenda
- Veel gestelde vragen
- Mijn gegevens
- Nieuw in mijn dossier

Welkom op MijnZGT,

U kunt hier:
- uw afspraken met ZGT bekijken
- een vraag stellen aan uw behandelaar
- uw medische gegevens inzien
- de medische gegevens inzien van iemand die u heeft gemachtigd

Heeft u vragen over het gebruik van mijnZGT? Stuur dan een e-mail naar mijnzgt@zgt.nl
Op werkdagen kunt u tijdens kantooruren ook bellen naar 088 708 57 77.

Ook bent u op werkdagen welkom op ons Informatiepunt MijnZGT op onze locatie Hengelo en Almelo.

Aankomende afspraak

Vijf principes voor veilig internetbankieren

De Nederlandse banken houden zich aan vijf principes voor veilig internetbankieren. Deze principes zijn begin 2014 opgesteld door de Nederlandse Vereniging van Banken (NVB) in overleg met de Consumentenbond. In 2019 zijn ze aangepast in verband met de Europese betaalwet PSD2.

De vijf principes die de NVB heeft opgesteld luiden:

- Houd uw beveiligingscodes geheim
- Zorg ervoor dat uw bankpas nooit door een ander wordt gebruikt
- Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor bankzaken
- Controleer uw bankrekening
- Meld incidenten direct aan de bank en volg aanwijzingen van de bank op

Houd uw beveiligingscodes geheim

- Gebruik beveiligingscodes alleen zelf en schrijf ze niet op.
- Kies een beveiligingscode die niet eenvoudig te raden is.
- Geef beveiligingscodes nooit per telefoon, e-mail of andere wijze door. Banken en andere dienstverleners vragen nooit om deze codes.

Zorg ervoor dat uw bankpas nooit door een ander wordt gebruikt

- Klanten moeten zich tijdens het gebruik van de bankpas niet laten afleiden.
- Berg de bankpas altijd op een veilige plaats op. Controleer regelmatig of u de bankpas nog in uw bezit hebt.

Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor bankzaken

- Voorzie de geïnstalleerde software en het besturingssysteem op de computer, tablet en/of smartphone van de laatst mogelijke (beveiligings-)updates.
- Installeer geen illegale programma's.
- Beveilig de toegang tot de apparaten met een wachtwoord, pincode of anderszins.
- Zorg ervoor dat niemand anders op uw apparaten kan internetbankieren.
- Log altijd uit bij internetbankieren.

MINI COMPUTER CLUB ALMELO

Controleer uw bankrekening

- Controleer minimaal elke twee weken uw digitale rekeninginformatie. Wie nog papieren afschriften ontvangt moet die het liefst binnen twee weken na ontvangst controleren.

Meld incidenten direct aan de bank en volg aanwijzingen van de bank op

Denk daarbij aan:

- Uw bankpas is gestolen of kwijt.
- U weet of vermoedt dat anderen uw beveiligde gegevens hebben gebruikt.
- In het rekeningoverzicht staan transacties waarvoor u geen toestemming hebt gegeven.
- Uw mobiele apparaat met daarop een banktoepassing is gestolen of kwijt.

Mocht u toch slachtoffer worden van fraudeurs, dan hebt u grotere kans op schadevergoeding door de bank als u zich aan deze principes houdt.

MINI COMPUTER CLUB ALMELO

Windows 11: een back-up maken en terugzetten

Windows 11 kan automatisch een back-up van de belangrijkste mappen maken. Het besturingssysteem bewaart de gegevens in Microsoft OneDrive, een usb-stick of externe harde schijf.

Online back-up maken

Sinds Windows 11 kunnen we een online back-up te maken in OneDrive. Dat is veilig en de bestanden zijn ook nog eens op ieder Windows-apparaat beschikbaar. Bezit u zowel een laptop als computer, dan staan daarop dezelfde gegevens van de back-up. Maak op een Windows 11-computer automatisch een online back-up van de belangrijkste mappen. Dat werkt zo:

- Klik op **Starten**.
- Klik op **Instellingen**.
- Klik op **Accounts**.
- Klik op **Windows back-up**.

Accounts › **Windows back-up**

AsusvanHenk

OneDrive
Synchroniseren

Lijst met apps
Er is een back-up gemaakt

Voorkeuren
Er is een back-up gemaakt

OneDrive-map synchroniseren
De geselecteerde mappen worden beveiligd en zijn beschikbaar op al uw apparaten

Synchronisatie-instellingen beheren

Mijn apps onthouden
Snel toegang krijgen tot uw apps op elk apparaat

Aan

Mijn voorkeuren onthouden
Krijg snelle toegang tot uw voorkeuren in alle Microsoft-producten

Aan

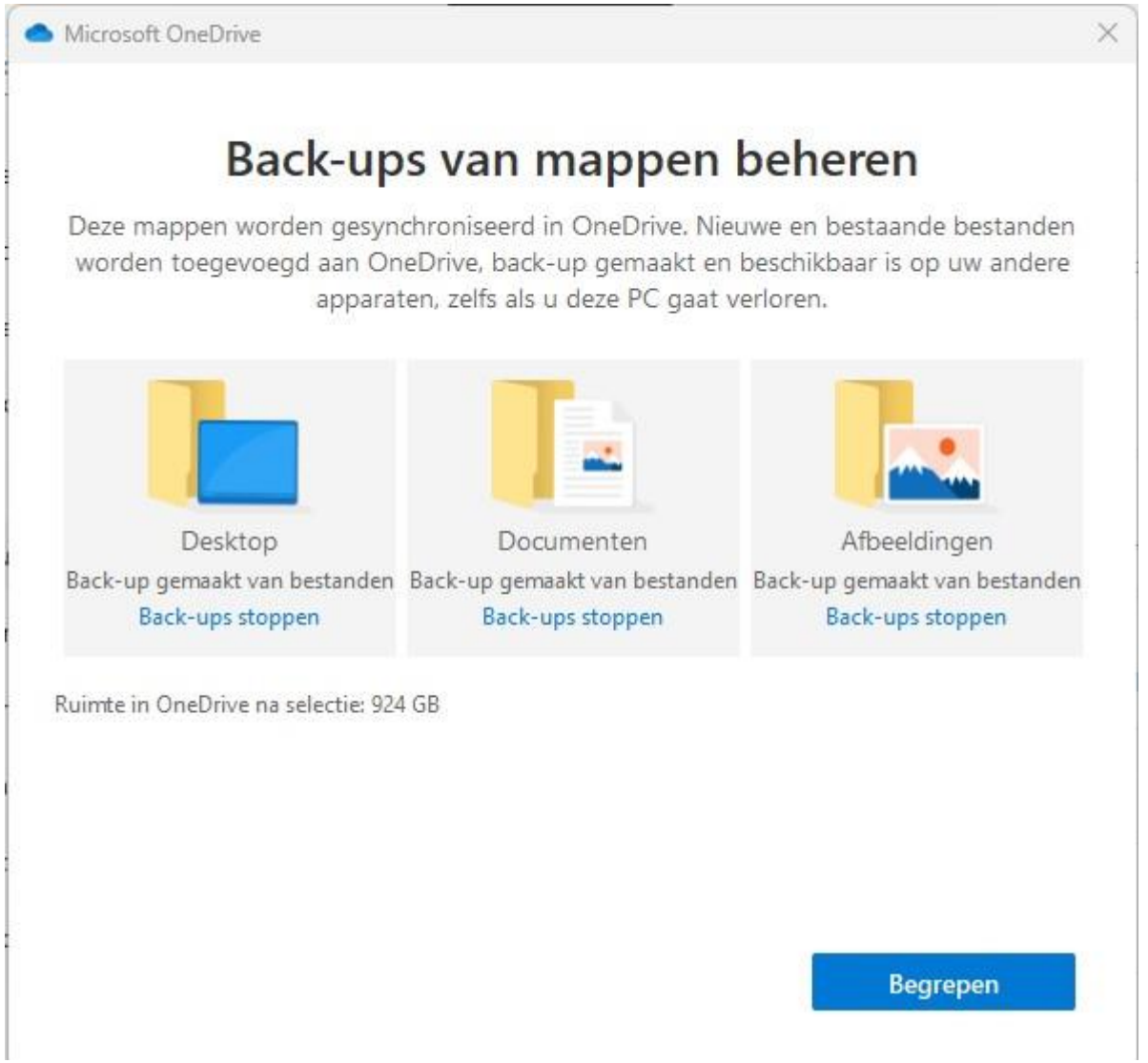
Privacybronnen
Over deze instellingen en uw privacy | Privacydashboard | Privacyverklaring

Verwante ondersteuning

Hulp bij Windows back-up

Kies voor “Synchronisatie-instellingen beheren”. U kunt hier kiezen om de back-up te stoppen.

Door “Begrepen” aan te klikken sluit u het venster.



De verschillende mappen kunt u vervolgens terugvinden in OneDrive. Let u wel op dat U het aantal te back-uppen bestanden niet te groot maakt. Standaard is heeft u 5GB tot uw beschikking. Met een abonnement op Microsoft 365+ heeft u 1TB om bestanden op te slaan.

Als u een back-up hebt gemaakt met het hulpprogramma voor Back-up maken en terugzetten in Windows 7, werkt deze ook in Windows 10/11. Ga via het configuratiescherm naar Back-up maken en terugzetten (Windows 7). Na het instellen van Back-up wordt een back-up gemaakt.

De presentatie Windows-Backup onder Tips op onze site laat zien hoe u te werk moet gaan.

Wilt u het maken van een Backup automatiseren kunt u ook de synchronisatietool SyncBackFree gebruiken. Dit kunt u downloaden via www.2brightsparks.com/download-synbackfree.html