

# Module 4:

# Veiligheid op het internet

Werkinstrument voor leerkrachten

---

## Korte omschrijving thema

Het internet is een zeer mooi instrument om informatie te zoeken en te delen, om met mensen te connecteren, om grappige dingen te doen. Het is een wereld waarin kinderen vandaag almaar actiever zijn. Ze zijn er dan ook heel bedreven in en staan niet altijd stil bij de risico's die ze eventueel lopen.

In de module 'Veiligheid op het internet' belichten we een aantal risico's van het internet en hoe we kinderen weerbaar kunnen maken voor wat er mogelijk fout gaat online.

## Doelstellingen

Met deze module beogen we volgende doelstellingen:

1. Inzicht geven in risico's op besmetting van computers, tablets en smartphones
  2. Manieren aanleren om computers en sociale media te beveiligen
  3. Bewustzijn creëren rond assertief gedrag online
  4. Middelen aanreiken om cyberpesten te melden
- 

## ICT-eindtermen

In deze module komen de volgende ICT-eindtermen aan bod:

- De leerlingen gebruiken ICT op een veilige, verantwoorde en doelmatige manier.
- De leerlingen kunnen ICT gebruiken om op een veilige, verantwoorde en doelmatige manier te communiceren.

Bovendien wordt aandacht besteed aan de eindtermen 'Sociale vaardigheden'

- De leerlingen kunnen zich weerbaar opstellen naar leeftijdsgenoten en volwassenen toe door signalen te geven die voor anderen begrijpelijk en aanvaardbaar zijn.

## Doelgroep

- Lager onderwijs derde graad
- Middelbaar onderwijs eerste graad

## Benodigheden

- Min. 5 computers / laptops met Windows 10-besturingssysteem
- Antivirussoftware Windows Defender
- Toegang tot internet en webbrowser
- Digg-it-module 'Safety first'

## Lesduur

2 lessen (2 x 50')

## Vorbereiding

- Computers / laptops opladen
- Dummyinformatie klaarmaken voor aanmaken Facebook-account
- Klaarzetten van de diggit-module 'Safety first' op interactief bord

## Belangrijke begrippen

Hieronder vind je een overzicht van een aantal relevante termen en definities m.b.t. veilig internetgebruik:

### Worm

Een worm is een computerprogramma dat zichzelf vermenigvuldigt. Via het computernetwerk worden kopieën van deze worm doorgestuurd zonder tussenkomst van een gebruiker. Zo brengt die aanzienlijke schade toe aan alle toestellen die op dat netwerk zijn aangesloten.

Het verschil met een computervirus is dat een worm zichzelf verspreidt over het internet, terwijl een virus dat op zichzelf niet kan. Een computervirus heeft een gastheer nodig, zoals een bestand of e-mail om zich te kunnen verspreiden (zie ook: virus)

### Firewall

Een firewall is een beveiligingssysteem om je lokale computernetwerk te beschermen tegen toegang door onbevoegden.

### Hacking

Hacking is zonder toestemming inbreken in de computer(s) van iemand anders of van een bedrijf door de beveiliging te omzeilen. Hackers hebben niet altijd de bedoeling om illegaal informatie te verkrijgen. Soms willen ze aantonen dat het netwerk onvoldoende beveiligd is.

Bedrijven zetten vaak ethische hackers in om gaten te ontdekken in de beveiliging van hun computernetwerken. Zo helpen deze hackers in de strijd tegen cybercriminaliteit en zijn ze bijgevolg de 'good guys' van het internet.

### Internettrol

Een internettrol is iemand die met opzet anonieme berichten op internet plaatst om onrust te zaaien. Het kan gaan om relatief onschuldige zaken, maar vaak ook om minder onschuldige, provocerende meningen.

## Belangrijke begrippen

Hieronder vind je een overzicht van een aantal relevante termen en definities m.b.t. veilig internetgebruik:

### Malware

Verzamelnaam voor **kwaadaardige en- of schadelijke software**. Het woord is een samentrekking van het Engelse 'malicious software' (kwaadwillige software). Voorbeelden van malware: virus, worm, Trojaans paard en spyware.

### Trojaans paard

Een **computerprogramma** dat er **bedrieglijk echt uitziet**. Via een Trojaans paard worden virussen en wormen het computersysteem binnengesmokkeld, alsook onzichtbare programma's die vertrouwelijke gegevens op een computer verzamelen om die vervolgens naar de afzender van het Trojaanse paard te sturen, die er kwade bedoelingen mee heeft.

### Spyware

Spyware is de naam voor computerprogramma's die informatie verzamelen over een computergebruiker en die doorsturen naar iemand anders. Het doel van spyware is meestal om geld te verdienen. De term komt van het Engelse woord 'spy', dat spion betekent, en het achtervoegsel 'ware', geeft aan dat het om software gaat.

### Virus

Een virus is een computerprogramma dat zich in een bestand op je computer kan vasthechten. Het komt ongemerkt binnen via een 'gastheer', bijvoorbeeld een besmet bestand of een besmette e-mail. Het is schadelijk omdat het schijfruimte en computertijd in beslag neemt van de besmette computers. In ernstige gevallen kan een virus ook gevoelige informatie wissen en verspreiden. In zeer ernstige gevallen kan de gebruiker zelfs de totale controle over de computer verliezen.

## Interessante links

[www.lokalopolitie.be/5412/vragen/criminaliteit-op-internet](http://www.lokalopolitie.be/5412/vragen/criminaliteit-op-internet)

[www.veiligonline.be/](http://www.veiligonline.be/)

[www.childfocus.be/nl/preventie/veilig-internetten/professionelen](http://www.childfocus.be/nl/preventie/veilig-internetten/professionelen)

## **Draaiboek**

Hieronder vind je een overzicht van het verloop van de les over het veilig gebruik van internet:

**5'** | **Deel 1: Introductie**

**15'** | **Deel 2: Conversatiestarters**

**15'** | **Deel 3: Je computer beveiligen**

**45'** | **Deel 4: Een sterk wachtwoord creëren**

**30'** | **Deel 5: Zelf veilig online**

## Deel 1: Introductie

1. Schetsen van de context: internet is een heel mooi instrument, maar er zijn ook wel wat risico's aan verbonden
2. Doel van de les uitleggen

## Deel 2: Conversatiestarters

Leerlingen zijn digitaal vaak heel actief. Het is dan ook belangrijk om hun ervaringen te delen: Wat doen ze online? Wat vinden ze interessant? Wat gaat goed en wat loopt soms fout? Onder begeleiding in klasverband het gesprek op gang brengen is een stap in het digitaal nog wijzer maken van leerlingen. Hieronder vind je een paar vragen als 'conversatiestarters' voor het thema 'Internet veilig gebruiken'.

- Stel: iemand steelt de wachtwoorden van je Facebook en Instagram. Wat is dan het ergste dat er zou kunnen gebeuren?
- Een faker is iemand die zich voordoeft als iemand anders. Soms om je in te palmen en rare dingen te laten doen voor de webcam. Hoe herken je een faker, op bijvoorbeeld Facebook, Instagram of WhatsApp? Wat zijn jouw gouden tips?
- Het komt voor dat kinderen inbreken op elkaars account en een grappige post plaatsen op de Facebook-pagina van een ander. De bedoeling is niet om iemand kwaad te doen. Maar op iemands account inbreken is wel strafbaar. Wat is voor jou het verschil tussen een grapje en crimineel gedrag op internet? Wanneer gaat het te ver?

## Deel 3: Je computer beveiligen

### Korte omschrijving

Computers die aangesloten zijn op een netwerk, hoe klein of hoe groot ook, zijn kwetsbaar voor malware. Gebruikers moeten zich ervan bewust zijn dat de manier waarop ze met hun computers, bestanden en mails omgaan, een significant verschil kan maken in de manier waarop ze blootgesteld worden aan die schadelijke invloeden.

In dit deel van de les geven we je een inzicht in de risico's op besmetting van computers, tablets en smartphones.

### Stap voor stap

Stap voor stap beschrijving van de informatie, inclusief screenshots en illustraties.

Inhoud per stap	Werkvorm in de klas	Media
<p><b>Opdracht:</b> Zoek de definitie op voor de volgende woorden.</p> <ul style="list-style-type: none"><li>• Malware</li><li>• Trojaans paard</li><li>• Hacking</li><li>• Virus</li><li>• Internettrol</li></ul>	<p>Werk in groepjes + klassikale bespreking</p>	<p>Google search</p>





Inhoud per stap	Werkvorm in de klas	Media
<b>Opdracht:</b> Probeer dit nu ook op de computer in de klas.	Werk in groepjes aan de computer	
<b>Vraag en antwoord:</b> Wat kan je nu allemaal doen om je computer beter te beveiligen? <b>Tips:</b> <ol style="list-style-type: none"><li>1. Open nooit een e-mail of bijlage die vreemd lijkt. Bijvoorbeeld een gekke titel, geen onderwerp, een onbekende afzender, fouten in de tekst. Gebruik dus je gezond verstand en check ook met een volwassene.</li><li>2. Klik in een mail of een post op sociale media nooit op een link die er vreemd uitziet. Vraag altijd aan de afzender of deze mail of post wel van hem/haar komt.</li><li>3. Als je op een website persoonlijke gegevens moet ingeven, check dan snel even of er https:\\ staat in de link bovenaan je browservenster. Zo ben je zeker dat de website goed beveiligd is. En je gegevens in veilige handen zijn.</li></ol>	Vraag en antwoord + klassikaal afronden met de tips	

## Deel 4: Een sterk wachtwoord creëren

### Korte omschrijving

Een heel belangrijk aspect van onlineveiligheid is een sterk wachtwoord kiezen. Op die manier wordt het cybercriminelen heel wat moeilijker gemaakt om in te breken in je computer, tablet en/of smartphone. Sommige websites en apps gaan hier nog een stapje verder in, met tweestapsverificatie.

In dit deel van de les leren we je een aan de hand van tips en tricks hoe je dat het beste aanpakt.

### Stap voor stap

Stap voor stap beschrijving van de informatie, inclusief screenshots en illustraties.

Inhoud per stap	Werkvorm in de klas	Media
<p><b>Vraag:</b> Wat is een ZWAK wachtwoord volgens jullie?</p> <p><b>Uitleg:</b> Een zwak wachtwoord is een wachtwoord dat iemand snel kan raden.</p> <ol style="list-style-type: none"><li>1. Je eigen naam</li><li>2. De naam van je huisdier</li><li>3. Je geboortedatum</li><li>4. Je straatnaam en huisnummer</li><li>5. Logische rijtjes zoals 'abcdefg' of '12345678'</li></ol> <p>Ook: een opgeschreven wachtwoord is een zwak wachtwoord</p> <ol style="list-style-type: none"><li>1. Schrijf nooit je wachtwoord op een briefje of post-it of in je agenda.</li><li>2. Tip nummer 2 : geef je wachtwoord nooit aan iemand anders, ook niet aan je beste vriend of vriendin.</li></ol>	<p>Werk in groepjes + klassikale bespreking</p>	<p>Google search</p>

Inhoud per stap	Werkvorm in de klas	Media
<p><b>Vraag:</b> Wat is dan wel een STERK wachtwoord?</p> <p><b>Uitleg:</b></p> <ol style="list-style-type: none"><li>1. Een sterk wachtwoord bestaat uit minstens 12 karakters</li><li>2. Het bestaat uit een combinatie van hoofdletters, kleine letters, nummers en speciale tekens.</li><li>3. Het is origineel: MijnHondBl@ft20Keer!</li><li>4. Het zit in je hoofd.</li><li>5. Je hebt verschillende wachtwoorden, want als het dan toch eens mis gaat met een ervan, kan het niet gebruikt worden om al je sociale media, e-mailaccounts, apps en dergelijke binnen te dringen.</li></ol>	<p>Groepsdiscussie in klasverband + overzicht met “do’s”</p>	

Inhoud per stap	Werkvorm in de klas	Media
<p><b>Vraag:</b> Bedenk een sterk wachtwoord voor jezelf in je hoofd?</p> <p><b>Uitleg: Tweestapsverificatie:</b> verschillende platformen zoals Facebook en Instagram gaan nog een stap verder om de veiligheidsrisico's te verkleinen, dankzij tweestapsverificatie. Het klinkt moeilijker dan het in werkelijkheid is.</p> <p><b>Voorbeeld aan de hand van Facebook</b></p> <ol style="list-style-type: none"><li>1. Log in op Facebook en klik rechtsboven op het pijltje.</li><li>2. Kies nu 'Instellingen' en vervolgens 'Beveiliging en aanmelding'.</li><li>3. Klik in het deel 'Tweestapsverificatie' op 'Bewerken' en dan op 'Aan de slag'.</li><li>4. Vink 'Sms' aan om de veiligheidscode te ontvangen op je gsm en klik op 'Volgende'.</li><li>5. Je krijgt nu een code op het telefoonnummer dat je opgaf. Geef die hier in. Klik op 'Volgende'. Nu is de tweestapsverificatie actief!</li></ol> <p>Vanaf nu krijg je altijd een code als jijzelf of iemand anders inlogt van een onbekende smartphone of computer.</p>	Groepsdiscussie in klasverband	Bijlage 3, 4, 5, 6 en 7.

## Deel 5: Zelf veilig online

### Korte omschrijving

In de onlinewereld worden kinderen geconfronteerd met mensen die hun grenzen niet respecteren, gemeen doen of zelfs geld vragen. Het is belangrijk om dit bespreekbaar te maken en hun manieren aan te reiken om hiermee om te gaan.

In dit deel van de les willen we bij leerlingen bewustzijn creëren rond assertief onlinegedrag en hun middelen aanreiken om cyberpesten aan te kaarten.

### Stap voor stap

Stap voor stap beschrijving van de informatie, inclusief screenshots en illustraties.

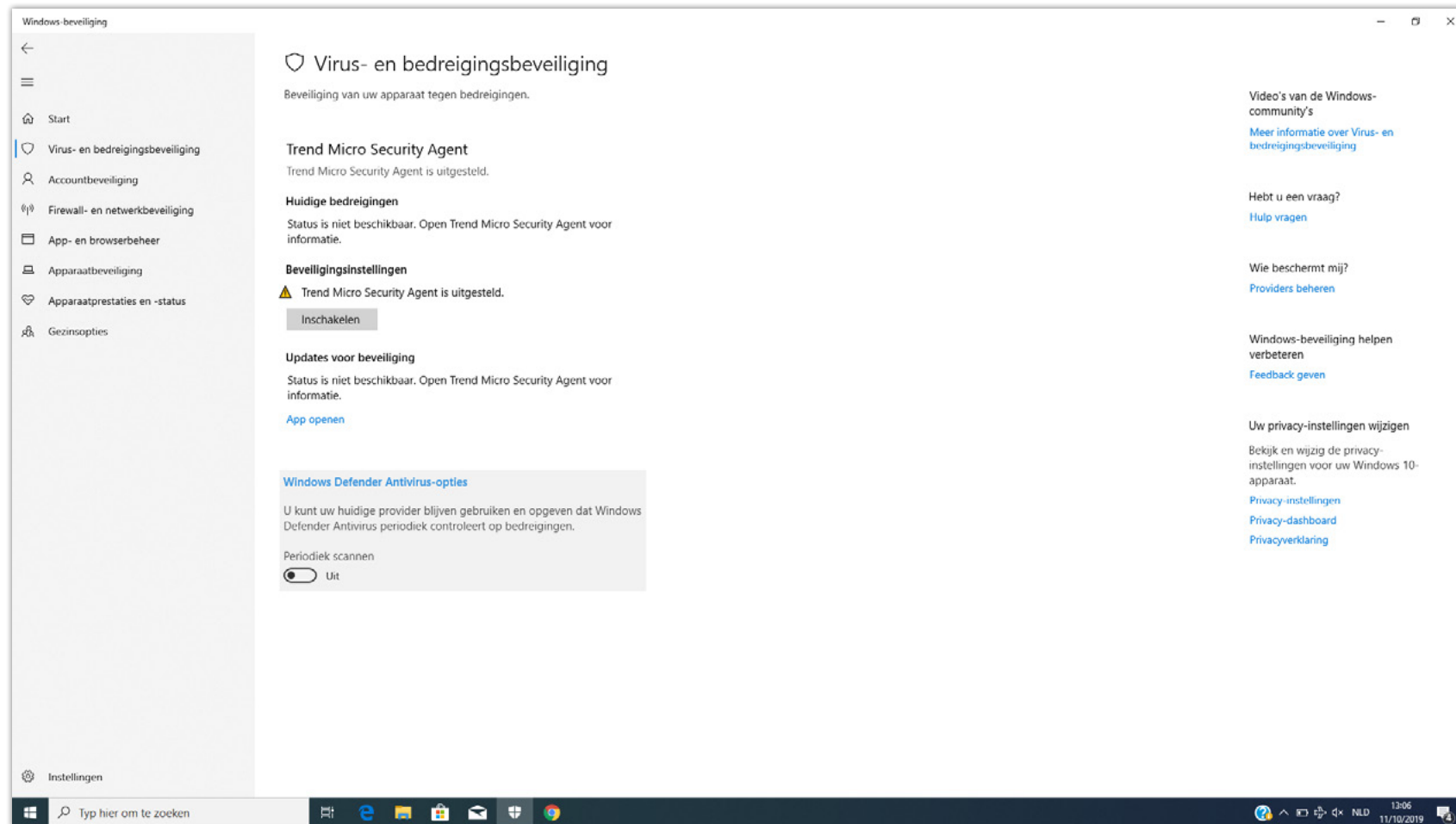
Inhoud per stap	Werkvorm in de klas	Media
<p><b>Vraag:</b> In films als Batman en Superman draait het om de held en de boef. Het goede tegen het kwade. Wat is voor jou op internet 'het goede' en wat is 'het kwade'?</p> <p><b>Uitleg:</b> Online ben je aan niemand iets verplicht, ook niet als je hem of haar als vriend hebt toegevoegd op je sociale media. Bij twijfel check je altijd met iemand die je vertrouwt, zoals je ouders of je leerkracht.</p>	Groepsdiscussie in klasverband + overzicht met "dont's"	

Inhoud per stap	Werkvorm in de klas	Media
<p><b>Een aantal extra tips:</b></p> <ol style="list-style-type: none"><li>1. Stuur geen ongepaste foto's of video's door, als iemand je dat vraagt (ook iemand die je heel goed kent)</li><li>2. Wees op je hoede voor valse informatie (ook 'fake news' genoemd).</li><li>3. Gebruik altijd je gezond verstand als je iets leest wat ongelooflijk lijkt op sociale media of in een e-mail</li></ol> <p><b>Meenemertje:</b> als het te goed lijkt om waar te zijn, is het dat meestal ook!</p>		
<p><b>Vraag:</b> Wat is voor jou de definitie van cyberbesten?</p>	Werk in groepjes	
<p><b>Opdracht:</b> Surf naar de site van Child Focus en zoek hoe je cyberpesten kan melden?</p>	Werk in groepjes aan de computer. Eén groepje stelt voor, de andere groepen kunnen aanvullen.	

Inhoud per stap	Werkvorm in de klas	Media
<p><b>Uitleg:</b> Er bestaan verschillende mogelijkheden om cyberpesten te melden:</p> <ol style="list-style-type: none"><li>1. Je vindt een luisterend oor en een vertrouwenspersoon bij de hulplijn van Child Focus: via de website, telefonisch op het gratis nummer 116000, per mail of via Facebook.</li><li>2. Op de website awel.be kan je een mailtje sturen of chatten met iemand. Je kan ook bellen op het gratis nummer 102.</li><li>3. Dat kan ook op het socialemediaplatform. Op Facebook bijvoorbeeld kan je niet alleen pestgedrag melden, je kan zelfs de hulp inroepen van een ouder, vriend of leraar.</li></ol>	Klassikaal	Bijlage 8, 9, en 10.

## Bijlagen

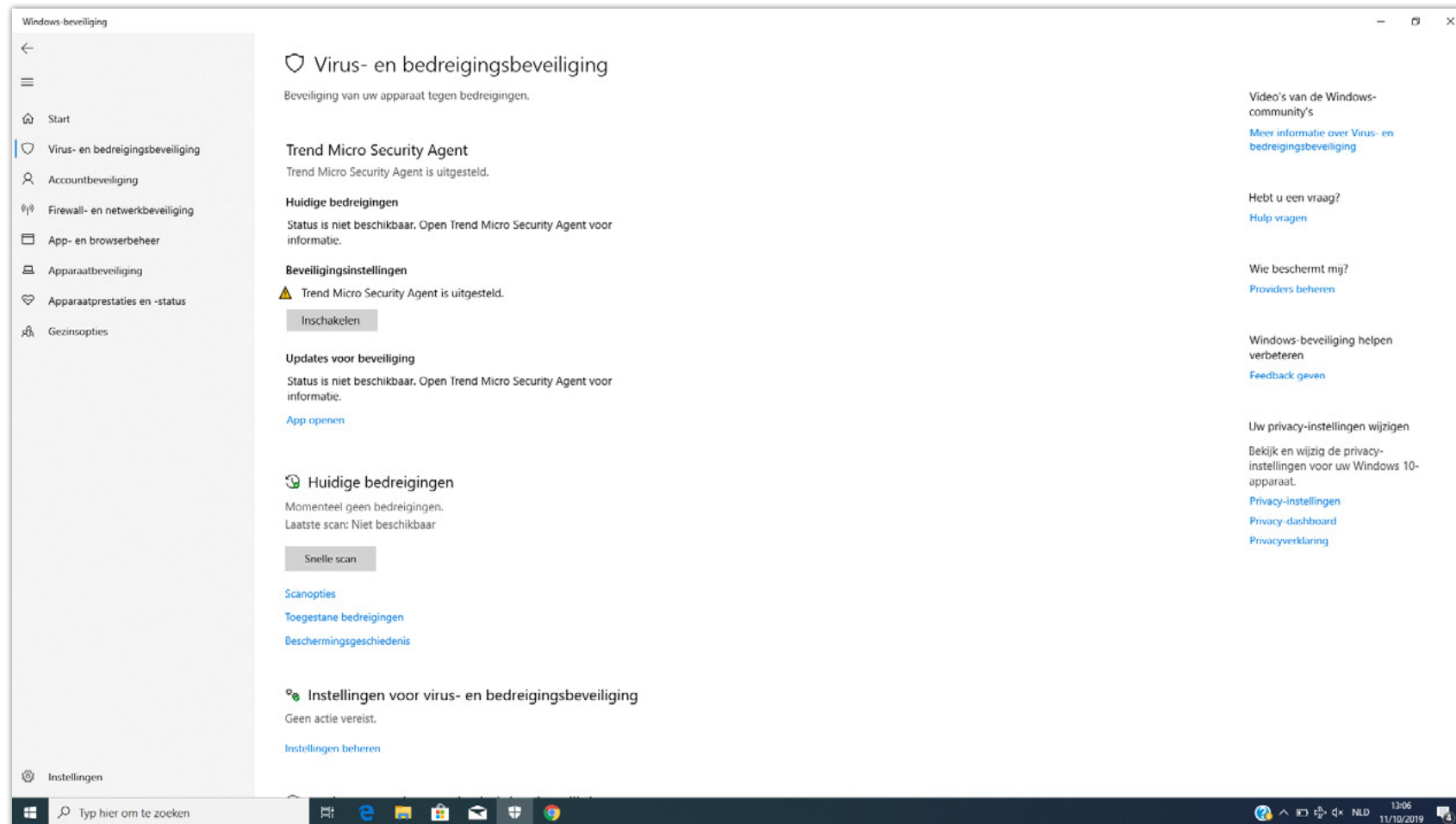
1.





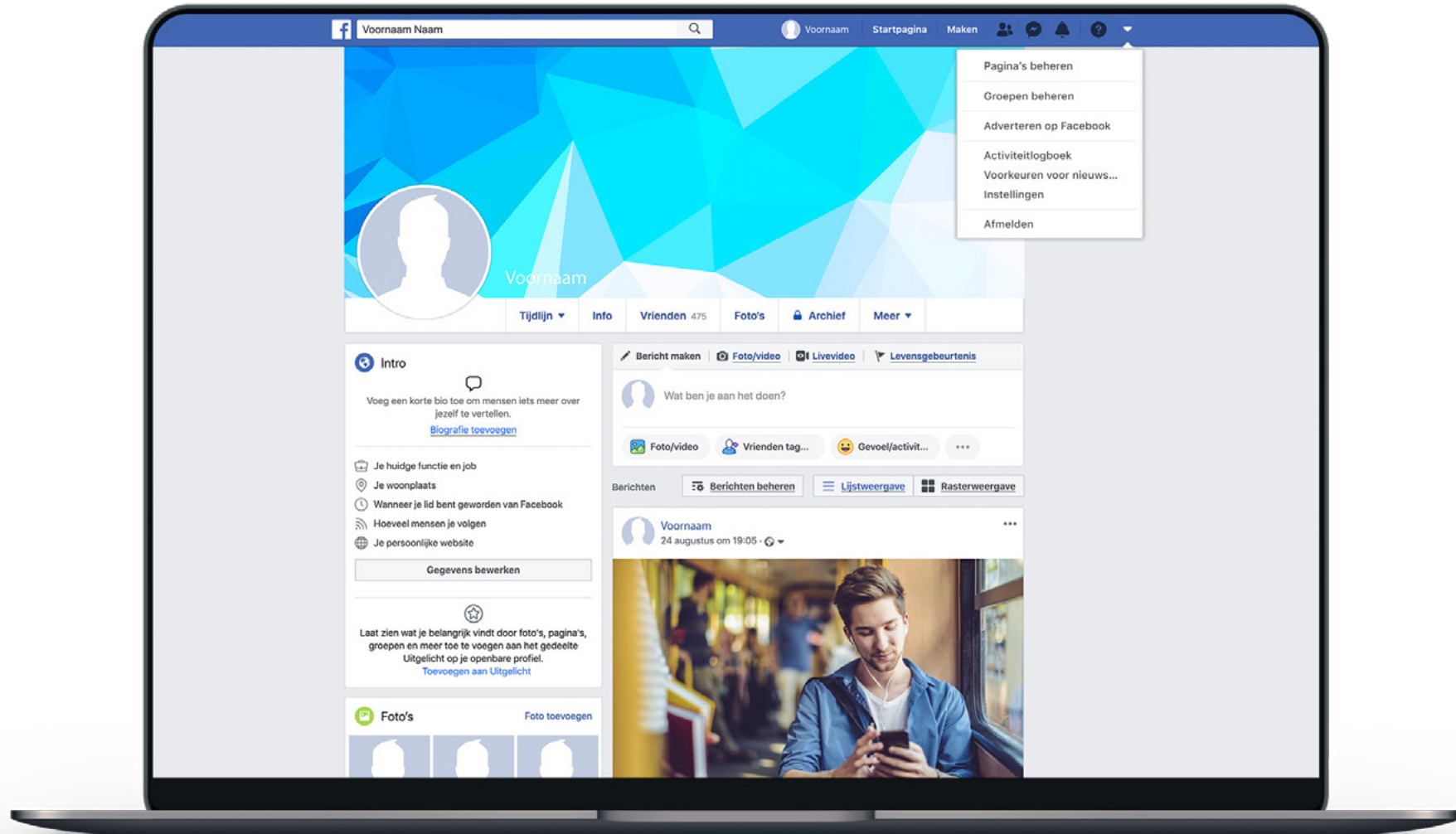
## Bijlagen

2.



## Bijlagen

3.



## Bijlagen

4.

The screenshot shows the Facebook 'Beveiliging en aanmelding' (Security and Login) settings page. The left sidebar contains navigation options: Algemeen, Beveiliging en aanmelding (selected), Je Facebook-gegevens, Privacy, Tijdlijn en taggen, Verhalen, Locatie, Blokkeren, Taal en regio, Gezichtsherkenning, Meldingen, Mobiel, Openbare berichten, Apps en websites, Instant Games, Bedrijfsintegraties, Advertenties, Betalingen, Support-inbox, and Video's.

The main content area is titled 'Beveiliging en aanmelding' and is divided into several sections:

- Aanbevolen**
  - Kies vrienden om contact mee op te nemen als je niet meer in je account kunt**: A notification to nominate three to five friends who can help log in if you're locked out. Includes a 'Bewerken' button.
- Waar je bent aangemeld**
  - Mac**: Chrome - Nu actief
  - iPhone 6s**: Facebook-app - 15 uur geleden
  - [Meer weergeven](#)
- Aanmelden**
  - Wachtwoord wijzigen**: A reminder to use a strong password. Includes a 'Bewerken' button.
  - Je aanmeldgegevens opslaan**: Option to save login data for browsers and devices. Includes a 'Bewerken' button.
- Tweestapsverificatie**
  - Tweestapsverificatie gebruiken**: Option to use two-step verification. Includes a 'Bewerken' button.
  - Geverifieerde aanmeldingen**: Option to view devices that don't require a code. Includes a 'Weergeven' button.
  - Appwachtwoorden**: Option to use special passwords for apps. Includes a 'Toevoegen' button.

## Bijlagen

5.

Tweestapsverificatie > **Tweestapsverificatie**

### Voeg extra beveiliging toe met tweestapsverificatie

Help je account te beschermen, zelfs als iemand je wachtwoord in handen krijgt.

**Aan de slag**

#### Hoe tweestapsverificatie werkt

##### Extra beveiliging

Als we een aanmelding zien via een apparaat dat we niet herkennen, vragen we om een aanmeldcode voordat je toegang krijgt tot je account.

##### Via sms of een verificatieapp

We sturen een sms-bericht met een aanmeldcode of je kunt een zelfgekozen beveiligingsapp gebruiken.


## Bijlagen

6.

### Tweestapsverificatie


Een beveiligingsmethode kiezen

Elke keer dat je je aanmeldt vanaf een telefoon of computer die we niet herkennen, vragen we je om je wachtwoord en een aanmeldcode.



**Verificatieapp**

Stel een app in zoals Google Authenticator of Duo Mobile om aanmeldcodes te genereren.



**Sms-bericht**

We sturen een code naar +32 \*\*\*\*\*23 voor je configuratie.  
[Ander nummer gebruiken](#)

## Bijlagen

7.

### Tweestapsverificatie ✕



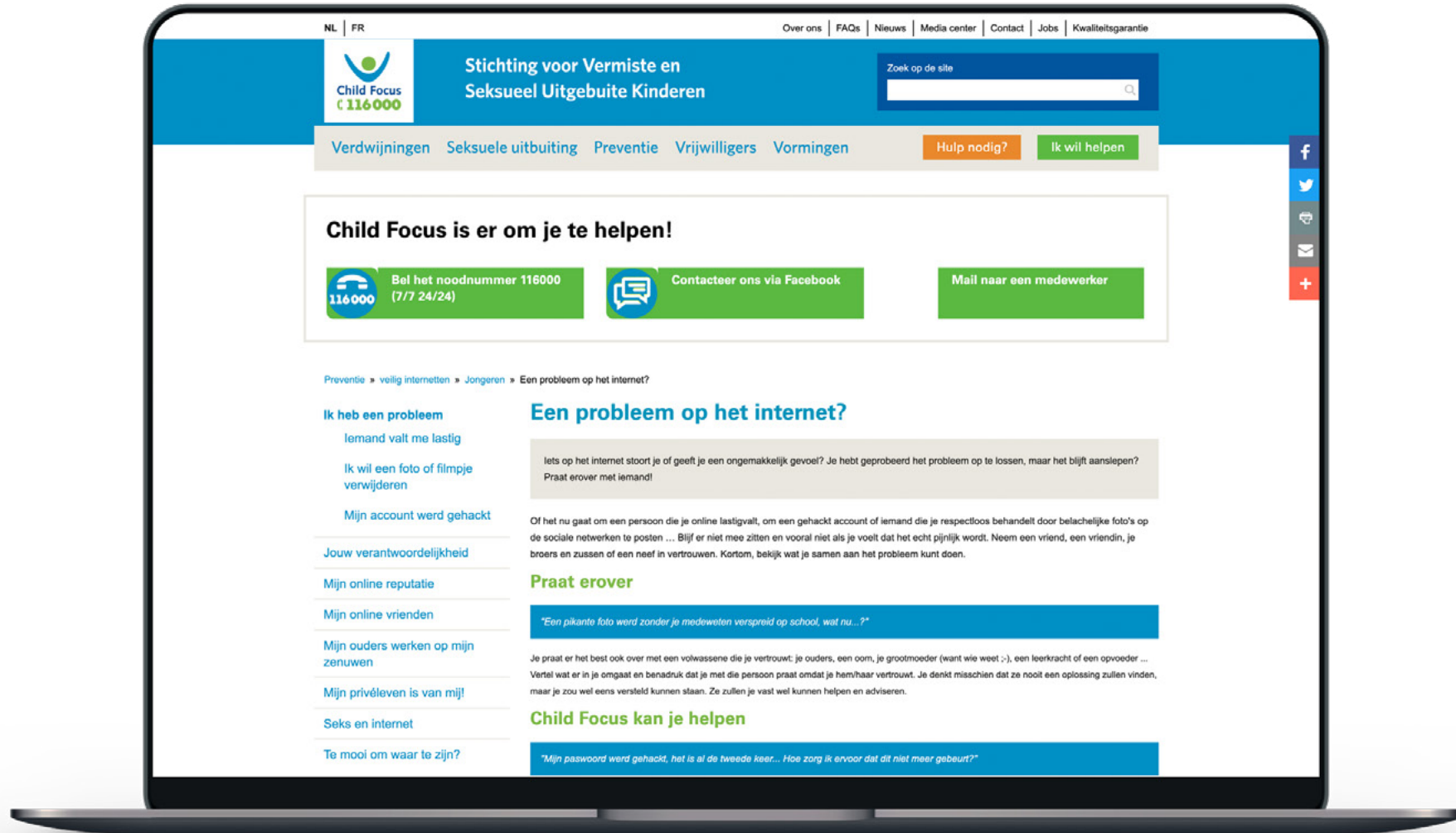
#### Bevestigingscode invoeren

Voer de bevestigingscode in die in je verificatieapp wordt weergegeven

Terug Volgende

## Bijlagen

8.



Bijlagen

9.





## Bijlagen

10.

