

Mijn Norton™

Gebruikershandleiding



Gebruikershandleiding voor Mijn Norton

De software die in deze handleiding wordt beschreven, wordt geleverd met een licentieovereenkomst en mag alleen worden gebruikt in overeenstemming met de voorwaarden in deze overeenkomst.

Documentatieversie 22.20.1

Copyright © 2020 Symantec Corporation. Alle rechten voorbehouden.

Het product dat in dit document wordt beschreven, wordt gedistribueerd onder licenties waarmee het gebruik, het kopiëren, het distribueren en het decompileren/toepassen van reverse-engineering ervan wordt beperkt. Geen enkel deel van dit document mag worden gereproduceerd in enige vorm op enige wijze zonder voorafgaande schriftelijke toestemming van Symantec Corporation en zijn eventuele licentiegevers.

DE DOCUMENTATIE WORDT GELEVERD 'ZOALS DEZE IS' EN ALLE EXPLICIETE OF IMPLICIETE VOORWAARDEN, REPRESENTATIES EN GARANTIES, WAARONDER IMPLICIETE GARANTIES VAN VERKOOPBAARHEID, GESCHIKTHEID VOOR EEN BEPAALD DOEL OF NIET-SCHENDING WORDEN AFGEWEEZEN, TENZIJ DERGELIJKE DISCLAIMERS NIET WETTELIJK ZIJN TOEGESTAAN. SYMANTEC CORPORATION IS NIET AANSPRAKELIJK VOOR INCIDENTELE OF GEVOLGSCHADE IN VERBAND MET DE VERSTREKKING, PRESTATIES OF HET GEBRUIK VAN DEZE DOCUMENTATIE. DE INFORMATIE IN DEZE DOCUMENTATIE KAN ZONDER VOORAFGAANDE KENNISGEVING WORDEN GEWIJZIGD.

De Gelicentieerde Software en Documentatie worden beschouwd als commerciële computersoftware zoals gedefinieerd in FAR 12.212 en zijn onderhevig aan beperkte rechten zoals gedefinieerd in FAR Sectie 52.227-19 'Commercial Computer Software - Restricted Rights' en DFARS 227.7202, e.v. 'Commercial Computer Software and Commercial Computer Software Documentation,' al naar gelang van toepassing, en eventuele verdere voorschriften, ongeacht of die door Symantec zijn geleverd op locatie of als hosted services. Het gebruiken, wijzigen, uitgeven van een reproductie, uitvoeren, weergeven of openbaar maken van de gelicentieerde Software en Documentatie door de Amerikaanse regering zal uitsluitend gebeuren in overeenstemming met de voorwaarden van deze Overeenkomst.

Symantec Corporation
350 Ellis Street,
Mountain View, CA 94043
<http://www.symantec.com>

Gedrukt in Tsjechië.

10 9 8 7 6 5 4 3 2 1

Inhoudsopgave

Hoofdstuk 1	Welkom bij Norton LifeLock	6
	Systeemvereisten voor de nieuwe Norton 360	6
	Uw Norton-account openen	8
Hoofdstuk 2	Uw beveiliging instellen	9
	Apparaatbeveiliging configureren	9
	Norton Password Manager instellen	10
	Cloudback-up configureren	15
	LifeLock Identity Theft Protection configureren	15
	Toezicht op het dark web wordt mogelijk gemaakt door LifeLock**	17
	Uw Veilige VPN instellen	18
	Ouderlijk toezicht instellen	19
	Bescherm uw bankgegevens met Norton Safe Web	22
Hoofdstuk 3	Uw apparaatbeveiliging beheren	24
	Wat te doen als uw apparaat gevaar loopt	24
	LiveUpdate uitvoeren	25
	Beveiligingsbedreigingen voor apparaten die Norton detecteert weergeven of verhelpen	26
	Risico's of bedreigingen in quarantaine verwerken	27
	Norton gebruiken om de prestaties van de computer te optimaliseren en te verbeteren	29
	Norton-scans uitvoeren om uw pc op bedreigingen te controleren	33
	Uw eigen aangepaste Norton-scans maken	36
	Norton-scans plannen	37
	Realtimebedreigingen bekijken die door Norton SONAR-beveiliging worden gedetecteerd	38
	Bestanden en mappen uitsluiten van de scans Norton Auto-Protect, SONAR en Downloadinformatie	39
	Bestanden met handtekening voor laag risico van Norton-scans uitsluiten	40
	Automatische taken in- of uitschakelen	41
	Aangepaste taken uitvoeren	42

Beveiligings- en prestatiescans plannen	42
Gegevensbescherming configureren om schadelijke processen te blokkeren die uw pc beïnvloeden	43
Norton instellen om scripts die door phishing-pogingen kunnen worden misbruikt te verwijderen	46
Veelgestelde vragen: Scriptbeheer van Norton	49
Uw Password Manager beheren	51
Norton Safe Web in- of uitschakelen	52
Op het web zoeken met Norton Safe Search	54
Norton Password Manager openen	55
Norton Password Manager-safe in de cloud maken	56
Uw Norton Password Manager-safe in de cloud verwijderen	57
Uw Norton Password Manager-gegevens exporteren	58
Uw Norton Password Manager-gegevens Importeren	59
De Norton Security-werkbalk in- of uitschakelen	61
Bescherm uw apparaat tegen misbruik, hackers en zero-day aanvallen.	61
Norton Firewall in- of uitschakelen	63
Programmaregels aanpassen	63
De volgorde van firewallregels wijzigen	64
Een verkeersregel tijdelijk uitschakelen	65
Een geblokkeerd programma toestaan	66
Melding van firewallblokkering uitschakelen	66
Lijst met uitsluitingen voor Inbraakpreventie	67
Browserbeveiliging inschakelen	68
Stel Norton Firewall in om waarschuwingen over blokkering van een aanval in of uit te schakelen	69
AutoBlock in- of uitschakelen	70
De blokkering opheffen van computers die door AutoBlock zijn geblokkeerd	70
Een apparaat toevoegen aan Apparaatvertrouwen	71
Downloadinformatie in- of uitschakelen	72
Filteren van spam in- of uitschakelen	73
Internetgebruik definiëren voor Norton	74
Beperken van netwerkgebruik in- of uitschakelen	75
Norton instellen om toezicht te houden op toepassingen en schadelijke websites te blokkeren op uw computer	76
Aan de slag met Norton Cloudback-up	78
Bestanden en mappen toevoegen aan of uitsluiten van uw back-upsets	79
Foto's, muziek of andere belangrijke bestanden herstellen uit Norton-back-upsets	80
Norton Backup inschakelen	81

De instellingen van uw Norton-product aanpassen	82
Instellingen voor Realtimebeveiliging aanpassen	83
Instellingen voor scans en risico's	85
Instellingen van Inbraakpreventie en browserbeveiliging	87
Norton zo instellen dat u uw beschermde apparaten op afstand kunt beheren	88
Instellingen voor Norton-apparaatbeveiliging beschermen tegen onbevoegde toegang	88
Een sneltoets instellen om in Norton-apparaatbeveiliging te zoeken naar informatie	89
Hoofdstuk 4 Extra oplossingen vinden	91
Apparaatbeveiliging verwijderen	91
Disclaimers	92

Welkom bij Norton LifeLock

Dit hoofdstuk bevat de volgende onderwerpen:

- [Systeemvereisten voor de nieuwe Norton 360](#)
- [Uw Norton-account openen](#)

Systeemvereisten voor de nieuwe Norton 360

Alleen licenties voor Norton-apparaatbeveiliging

- Norton™ AntiVirus Plus dekt één pc of Mac

Licenties voor Apparaatbeveiliging en Norton Secure VPN

Ondersteunt apparaten die draaien op Windows, Mac, Android en iOS

- Norton™ 360 Standard dekt één apparaat
- Norton™ 360 Deluxe dekt maximaal 5 apparaten
- Norton™ 360 met LifeLock Select dekt maximaal 5 apparaten
- Norton™ 360 met LifeLock Advantage dekt maximaal 10 apparaten
- Norton™ 360 met LifeLock Ultimate Plus dekt een onbeperkt aantal apparaten (beperkingen zijn van toepassing*)

Apparaatbeveiliging

Opmerking: Niet alle functies zijn beschikbaar op alle platforms.

Opmerking: Ouderlijk toezicht, Cloudback-up en SafeCam worden momenteel niet ondersteund op Mac OS.

Windows™-besturingssystemen

- ◆ ■ Microsoft Windows® 10 (alle versies)
 - Microsoft Windows® 10 in S-modus (32-bits, 64-bits of ARM32) versie 1803 en hoger
 - Microsoft Windows® 8/8.1 (alle versies)
Sommige beschermingsfuncties zijn niet beschikbaar in browsers in het startscherm van Windows 8.
 - Microsoft Windows® 7 (alle versies) met Service Pack 1 of later

Opmerking: Norton AntiVirus Plus wordt niet ondersteund op Windows 10 in S-modus.

Mac®-besturingssystemen

- ◆ Mac OS X 10.10.x of later voor een Norton-product met versie 8.0 of later.

Opmerking: Ouderlijk toezicht van Norton Family en Cloudback-up worden momenteel niet ondersteund op Mac OS.

Android™-besturingssystemen

- ◆ Android 4.1 of hoger
Google Play moet zijn geïnstalleerd.
Automatisch scannen van apps op Google Play wordt ondersteund op Android 4.1 of later, met uitzondering van Samsung-apparaten. Samsung-apparaten met Android 4.2 of later worden ondersteund. Voor eerdere versies van Android moet de functie Delen van Google Play gebruiken om apps op Google Play te scannen.

iOS-besturingssystemen

- ◆ iPhones of iPads met de huidige en laatste twee versies van Apple iOS

Systeemvereisten voor Norton™ Secure VPN

Beschikbaar voor Windows™-pc's, Macs®, iOS- en Android™ -apparaten:

Norton Secure VPN is compatibel met pc's, Macs, Android-smartphones en tablets, iPads en iPhones. Norton Secure VPN kan op het opgegeven aantal apparaten worden gebruikt - met onbeperkt gebruik tijdens de abonnementsperiode.

Windows™-besturingssystemen

- ◆ ■ Microsoft Windows® 10 (alle versies behalve Windows 10 S)
 - Microsoft Windows® 8/8.1 (alle versies)

- Microsoft Windows® 7 (alle versies) met Service Pack 1 of later
150 MB beschikbare schijfruimte.

Mac®-besturingssystemen

- ◆ Mac OS X 10.10.x of later.
150 MB beschikbare schijfruimte.

Android™-besturingssystemen

- ◆ Android 4.4 of later
Google Play moet zijn geïnstalleerd.

iOS-besturingssystemen

- ◆ iPhones of iPads met de huidige en laatste twee versies van Apple iOS

Uw Norton-account openen

Via uw Norton-account kunt u uw Norton-abonnementsgegevens beheren, uw productsleutel ophalen, opties voor automatische verlenging instellen of beveiligingsfuncties upgraden. Uw apparaat moet met internet zijn verbonden om uw account te openen.

Uw Norton-account openen

Opmerking: Als u een product via de online winkel heeft gekocht, heeft u als onderdeel van het aankoopproces al een Norton-account aangemaakt, zelfs als dit lang geleden was. Gebruik het e-mailadres en wachtwoord die u bij de aankoop heeft opgegeven. Als u het wachtwoord voor uw Norton-account bent vergeten, raadpleegt u [Het wachtwoord voor uw Norton-account opnieuw instellen](#).

- 1 Open uw browser en ga naar:
<https://my.norton.com>
- 2 Klik op **Aanmelden** en voer vervolgens op de pagina **Welkom bij Norton** een van de volgende handelingen uit:
 - Voer op het tabblad **Aanmelden** het e-mailadres en wachtwoord van uw account in en klik vervolgens op **Aanmelden**.
 - Vul op het tabblad **Een account maken** de verplichte velden in en selecteer **Account maken**. Raadpleeg [Een Norton-account aanmaken](#) voor uitgebreide instructies.

Uw beveiliging instellen

Dit hoofdstuk bevat de volgende onderwerpen:

- [Apparaatbeveiliging configureren](#)
- [Norton Password Manager instellen](#)
- [Cloudback-up configureren](#)
- [LifeLock Identity Theft Protection configureren](#)
- [Uw Veilige VPN instellen](#)
- [Ouderlijk toezicht instellen](#)
- [Bescherm uw bankgegevens met Norton Safe Web](#)

Apparaatbeveiliging configureren

U moet Apparaatbeveiliging van Norton installeren om uw apparaat te beschermen. U kunt Apparaatbeveiliging installeren op Windows-desktops en -laptops, Mac-computers en mobiele apparaten met Android en iOS.

Apparaatbeveiliging downloaden en installeren

- 1 Open uw browser op elke computer, laptop en smartphone en typ het volgende adres:
<https://norton.com/setup>
- 2 Meld u aan bij uw Norton-account.

- 3 Klik in het venster **Norton instellen** op **Akkoord en downloaden**



- 4 Klik op de sectie die de pijl op het scherm aanwijst en volg de instructies op het scherm. Uw service wordt automatisch gedownload, geïnstalleerd en geactiveerd.

Opmerking: Als u een foutmelding ziet wanneer u uw service downloadt, of als uw download niet wordt voltooid, kunt u de download opnieuw starten.

Norton Password Manager instellen

Nadat u Apparaatbeveiliging heeft geïnstalleerd, wordt u gevraagd browserextensies toe te voegen. U moet de extensies aan de Internet Explorer-, Firefox- en Chrome-browsers toevoegen om ervoor te zorgen dat de functies werken.

U moet de Norton-browserextensies inschakelen voor toegang tot alle browserspecifieke functies. De Norton-browserextensies omvatten:

Norton Safe Web	Een beveiligde zoekervaring waarmee u veilig op internet kunt surfen, zoeken en winkelen. Het analyseert de websites die u bezoekt en detecteert of er virussen, spyware, malware of andere bedreigingen op staan. Kom meer te weten over Norton Safe Web
Norton Safe Search	Een beveiligde zoekmachine die Ask.com en Yahoo! gebruikt om zoekresultaten te genereren. Norton Safe Search rangschikt de zoekresultaten op basis van de beveiligingsstatus van de site en de Norton-beoordeling.
Norton-startpagina	Een website die gebruik maakt van de functie Norton Safe Search om uw zoekervaring op internet te verbeteren. U ziet de beveiligingsstatus van de website en de Norton-beoordeling voor het gegenereerde zoekresultaat.
Norton Password Manager	Een veilige locatie waar u al uw vertrouwelijke gegevens kunt opslaan, zoals aanmeldingen, persoonlijke gegevens en financiële informatie. U kunt deze informatie gebruiken wanneer u zich aanmeldt bij websites, automatisch online formulieren invult en online betaalt.

Internet Explorer

De Norton-browserextensie toevoegen in Internet Explorer

- 1 Nadat u Apparaatbeveiliging voor het eerst heeft geïnstalleerd, wordt de pagina **Browserbeveiliging** automatisch in een nieuw venster geopend wanneer u Internet Explorer start.
- 2 Klik op de pagina **Browserbeveiliging** op de optie **Inschakelen** van de **Norton Security-werkbalk**.
- 3 In de pop-up van de extensies klikt u op **Extensie toevoegen**.

- 4 Nadat u de Norton Security-werkbalk heeft ingeschakeld, kunt u de extensies van Norton Safe Search, Norton-startpagina en Norton Password Manager voor uw browser inschakelen.

Gebruik de optie **Klik om toe te voegen** en volg de instructies op het scherm om deze functies in te schakelen.

- 5 Als u deze extensies niet heeft geïnstalleerd, wordt de melding **Internet Explorer-beveiligingswaarschuwing** weergegeven wanneer u Internet Explorer na een week start.

Klik op **Nu installeren** en volg de instructies op het scherm om de extensies te installeren.

Opmerking: Als u de Norton-extensie op een later tijdstip wilt activeren, klikt u op **Melding later herhalen**. Als u wilt dat de melding niet meer wordt weergegeven, klikt u op **Niet meer vragen**.

Google Chrome

De Norton-browserextensies toevoegen in Google Chrome

Opmerking: U moet de nieuwste versie van Norton 360 hebben om de browserextensies van Google Chrome te installeren. Als u de nieuwste versie niet heeft, moet u LiveUpdate uitvoeren in uw Norton-product. We bieden de volgende extensies voor de Google Chrome-browser:

- Norton Safe Web
- Norton Password Manager
- Norton Safe Search
- Norton-startpagina

Volg de onderstaande instructies om de browserextensies voor Chrome te installeren.

- 1 Nadat u Apparaatbeveiliging voor het eerst heeft geïnstalleerd, wordt de pagina **Browserbeveiliging** automatisch in een nieuw venster geopend wanneer u Google Chrome start.

U kunt de pagina **Browserbeveiliging** ook openen door onder **Internetbeveiliging** op de optie **Nu instellen** te klikken.

- 2 Klik op de pagina **Browserbeveiliging** op de optie **Klik om toe te voegen** van **Norton Safe Web**.
- 3 In de pop-up van de extensies klikt u op **Extensie toevoegen**.
- 4 Nadat u Norton Safe Web heeft ingeschakeld, kunt u de extensies Norton Safe Search, Norton-startpagina en Norton Password Manager voor uw browser inschakelen. Gebruik

de optie **Klik om toe te voegen** en volg de instructies op het scherm om deze extensies in te schakelen.

Klik op **Alle Norton-extensies gratis toevoegen** en volg de instructies op het scherm om alle Norton-extensies in Google Chrome in te schakelen.

- Als u de Norton Safe Web-extensie niet heeft geïnstalleerd, wordt de waarschuwing **Chrome-bescherming verwijderd** weergegeven wanneer u Google Chrome na een week start.
- Als u deze extensies niet heeft geïnstalleerd, wordt de melding **Google Chrome-beveiligingswaarschuwing** weergegeven wanneer u Google Chrome na een week start.

5 Klik op **Nu installeren** en volg de instructies op het scherm om de extensies te installeren.

Opmerking: Als u de Norton-extensie op een later tijdstip wilt activeren, klikt u op **Melding later herhalen**. Klik op **Niet meer vragen** als u wilt dat de melding niet meer wordt weergegeven.

Mozilla Firefox

De browserfuncties van Norton toevoegen in Mozilla Firefox

Opmerking: U moet de nieuwste versie van Norton 360 hebben om de webgebaseerde, zelfstandige browserextensies van Mozilla Firefox te installeren. Als u de nieuwste versie niet heeft, moet u LiveUpdate uitvoeren in uw Norton-product. We bieden de volgende extensies voor de Firefox-browser:

- Norton Safe Web
- Norton Safe Search
- Norton-startpagina
- Norton Password Manager

Volg de onderstaande instructies om de browserextensies voor Firefox te installeren of upgraden.

- 1 Nadat u Apparaatbeveiliging voor het eerst heeft geïnstalleerd, wordt de pagina **Browserbeveiliging** automatisch in een nieuw venster/tabblad geopend wanneer u Mozilla Firefox start.

Als u een upgrade heeft uitgevoerd voor Apparaatbeveiliging van Norton, klikt u in het waarschuwingsvenster **Browserbeveiliging** op **OK** om de extensiepagina weer te geven.

Opmerking: U kunt de pagina **Browserbeveiliging** ook openen door onder **Internetbeveiliging** op de optie **Nu instellen** te klikken.

- 2 Klik op de pagina **Browserbeveiliging** op de optie **Inschakelen** van **Norton Safe Web**.
- 3 In de pop-up van de extensies klikt u op **Toestaan**.

Nadat u Norton Safe Web heeft ingeschakeld, kunt u de functies van Norton Safe Search, Norton-startpagina en Norton Password Manager voor uw browser inschakelen. Gebruik de optie **Inschakelen** en volg de instructies op het scherm om deze functies te activeren.

Klik op **Alle Norton-extensies gratis toevoegen** en volg de instructies op het scherm om alle Norton-extensies in Firefox in te schakelen.

Als u deze extensies niet heeft geïnstalleerd, wordt de melding **Firefox-beveiligingswaarschuwing** weergegeven wanneer u Firefox na een week start. Als u de Norton-extensie op een later tijdstip wilt activeren, klikt u op **Melding later herhalen**. Als u wilt dat de melding niet meer wordt weergegeven, klikt u op **Niet meer vragen**. Als u de optie **Melding later herhalen** kiest, wordt na een week een beveiligingswaarschuwing in Firefox weergegeven. Klik in de melding op de optie **Nu installeren** en volg de instructies op het scherm om de extensies te installeren.

Microsoft Edge

De Norton-browserextensie toevoegen in Microsoft Edge

Opmerking: Norton Password Manager is een onafhankelijke extensie waarvoor geen Norton-product in de Microsoft Edge-browser hoeft te zijn geïnstalleerd. De extensie is alleen compatibel met computers waarop Windows 10-makersupdate en latere versies worden uitgevoerd.

- 1 Start de Microsoft Edge-browser.
- 2 Klik in de rechterbovenhoek op de knop **Meer** en selecteer **Extensies**.
- 3 Klik in het venster **Extensies** op **Extensies downloaden uit de Store**.
- 4 Typ in het venster **Store** het woord **Norton** in het zoekvakje en klik op **Norton Password Manager** in de resultaten.

- 5 Klik op **Installeren**.
Klik op **Starten** wanneer de extensie is geïnstalleerd.
- 6 Klik in het pop-upvenster **U heeft een nieuwe extensie** op **Inschakelen**.
- 7 Als u het Norton Password Manager-pictogram wilt weergeven op de adresbalk, klikt u op de knop **Meer** in de rechterbovenhoek van de browser, en vervolgens op **Extensies**.
- 8 In het venster **Extensie** selecteert u **Norton Password Manager**.
- 9 In het venster **Norton Password Manager** zet u de schuifregelaar onder **Knop weergeven naast de adresbalk** op **Aan**.

Cloudback-up configureren

Cloudback-up werkt preventief om gegevensverlies door ransomware, malware of ernstige hardwareproblemen met uw pc te voorkomen. Uw abonnement geeft u recht op een bepaalde hoeveelheid opslagruimte in Norton Cloudback-up. De hoeveelheid gratis cloudopslag hangt af van het abonnement dat u heeft aangeschaft.

Opmerking: De functie Norton Cloudback-up is alleen beschikbaar op Windows.

Voordat u uw eerste back-up uitvoert, moet u Cloudback-up activeren.

Opmerking: Als u Cloudback-up wilt gebruiken, moet u de optie **Beperken van netwerkgebruik** in het venster **Firewallinstellingen** instellen op **Geen limiet**.

Cloudback-up activeren

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** naast **Cloudback-up** op **Instellen**.
- 3 Klik in het venster dat verschijnt op het tabblad **Waar** op **Gratis activeren**.
- 4 Voer de gegevens van uw Norton-account in wanneer u daarom wordt gevraagd en klik op **Aanmelden**.
- 5 Klik op **Instellingen opslaan** en vervolgens op **Sluiten**.

LifeLock Identity Theft Protection configureren

Nu LifeLock en Norton hun krachten in één bedrijf hebben gebundeld, kunnen we u nu helpen uw identiteit te beschermen.

U kunt de volgende persoonlijke gegevens aan LifeLock toevoegen voor toezicht:

- Rijbewijs
- Burgerservicenummer, geboortedatum, meisjesnaam van moeder
- 5 verzekerings-id's
- 5 adressen
- 5 telefoonnummers
- 10 bankrekeningen
- 10 creditcards*

U kunt aanvullende informatie toevoegen voor toezicht, zoals telefoonnummers, e-mailadressen of accounts.

Het LifeLock Identity Alert System waarschuwt u wanneer uw identiteit door iemand anders wordt gebruikt. Dit kunnen bijvoorbeeld mensen zijn die proberen op uw naam een telefooncontract of een autolening af te sluiten.

Opmerking: LifeLock Identity Theft Protection biedt geen bescherming voor bedrijven. Onze technologie en service zijn ontworpen om individuen te beschermen die burgerservicenummers en andere persoonlijk identificeerbare informatie hebben die bedrijven niet hebben.

*U kunt bekende creditcards, zoals Visa, MasterCard, American Express en Discover toevoegen. Helaas worden andere kaarten, zoals winkelkaarten of cadeaukaarten, op dit moment niet ondersteund.

Niemand kan identiteitsdiefstal of cybercriminaliteit volledig voorkomen.

LifeLock houdt geen toezicht op alle transacties bij alle bedrijven.

LifeLock Identity Theft Protection configureren

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** naast **Identiteitsbescherming** op **Instellen**.
- 3 Klik op de pagina **LifeLock-ledenaanmelding** op de optie **Aanmelden met Norton**.
- 4 Voer uw accountgegevens in en meld u aan.
- 5 Volg de instructies op het scherm.

LifeLock voor Norton 360 installeren op Android

- 1 Start de **Play Store** -app op uw Android-apparaat en zoek **LifeLock Identity Theft Protection**.
- 2 Zodra u de app-pagina in de Play Store heeft gevonden, tikt u op **Installeren** en vervolgens op **Accepteren**.
- 3 Open de app nadat deze is geïnstalleerd en meld u aan met uw accountgegevens.

LifeLock voor Norton 360 installeren op iOS

- 1 Open de **App Store** -app op uw iOS-apparaat en zoek **LifeLock Identity Theft Protection**.
- 2 Zodra u de app-pagina in de App Store heeft gevonden, tikt u op **Download** en vervolgens op **Installeer**.
- 3 Open de app nadat deze is geïnstalleerd en meld u aan met uw accountgegevens.

Toezicht op het dark web wordt mogelijk gemaakt door LifeLock**

Wat is toezicht op het dark web?

We houden toezicht op het gebruik van uw persoonlijke gegevens** op moeilijk te vinden sites en forums op het dark web. Wanneer we uw informatie op het dark web vinden, stellen we u hiervan op de hoogte.

Waarom is dit belangrijk?

Identiteitsdieven kunnen uw persoonlijke informatie verkopen op moeilijk te vinden sites en forums op het Dark Web.

Wat moet ik doen?

Staat er informatie over uzelf in het bericht, raadpleeg dan de onderstaande stappen.

- **Betaalpas/creditcard gecompromitteerd** : als de rekening is gesloten, hoeft u niets te doen. Als het account actief is, neemt u contact op met uw creditcard-/betaalkaartbedrijf en vraagt u een nieuwe kaart aan. Houd uw afschriften goed in de gaten.
- **E-mail gecompromitteerd** : wijzig uw huidige e-mailwachtwoord. Heeft u accounts met hetzelfde wachtwoord, wijzig die dan ook. Houden de problemen aan, dan is het misschien verstandig een nieuw e-mailaccount te openen. Het helpt de beveiliging van uw accounts wanneer u uw wachtwoorden elke 30 dagen wijzigt.
- **Burgerservicenummer gecompromitteerd** : het is raadzaam fraudemeldingen in te stellen bij een van de drie kredietbureaus om uw identiteit verder te beschermen.
- **Naam/adres/telefoonnummer gecompromitteerd** : gelukkig zijn in dit geval geen mogelijk gevoeligere gegevens zoals uw burgerservicenummer gedeeld. Omdat sommige van uw persoonlijke gegevens echter openbaar zijn gemaakt, raden we u aan om uw kredietrapport nauwlettend in de gaten te houden.

We blijven in de gaten houden of uw persoonlijke gegevens** op het dark web staan. Als we uw gegevens vinden, sturen we een nieuwe e-mail.

Opmerking: Niemand kan identiteitsdiefstal volledig voorkomen.

Bij Toezicht op het dark web in Norton 360-abonnementen wordt alleen toezicht gehouden op uw e-mailadres. Meld u aan bij de portal om te controleren of u extra informatie kunt toevoegen voor toezicht.

Uw Veilige VPN instellen

Openbare wifi is overal: vliegvelden, koffiezaken, winkelcentra en hotels. Gratis 'hotspots' zijn zo wijdverspreid en handig dat mensen er vaak verbinding mee maken zonder erover na te denken. Maar e-mails lezen, uw banksaldo checken en andere activiteiten waarvoor u zich moet aanmelden, zijn riskant wanneer u openbare wifi gebruikt. Als u openbare wifi gebruikt, kunnen anderen uw online activiteiten volgen. Cybercriminelen kunnen persoonlijke gegevens stelen zoals uw gebruikersnamen, wachtwoorden, locatiegegevens, chats, e-mails of rekeningnummers.

Met Secure VPN kunt u de verbinding beveiligen wanneer u een openbare draadloze verbinding gebruikt. Er wordt een VPN (Virtual Private Network) gemaakt dat uw gevoelige gegevens versleutelt.

Secure VPN beschermt als volgt de gegevens die u via openbare wifi verstuurt en ontvangt:

- Uw verbinding wordt beschermd met versleuteling van bankkwaliteit zodat u openbare wifihotspots veilig kunt gebruiken.
- U kunt anoniem internetten zodat uw online privacy geen gevaar loopt.
- U kunt overal werken met uw favoriete apps en inhoud, alsof u thuis bent.
- Uw gegevens worden versleuteld op een privénetwerk waar uw activiteiten niet worden gevolgd of opgeslagen.
- U kunt rekenen op de uitstekende klantondersteuning van Norton LifeLock, een leider in online consumentenbeveiliging.

Opmerking: De functie Secure VPN is niet met alle abonnementen beschikbaar.

Volg de onderstaande instructies om Secure VPN te configureren.

Secure VPN configureren

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** naast **Veilige VPN** op **Instellen**.
- 3 Klik op de webpagina die verschijnt op **Aanmelden**.
- 4 Voer uw accountgegevens in en meld u aan.

- 5 Als u wordt gevraagd om de toepassing te downloaden, klikt u op **Downloaden**.
- 6 Volg de instructies op het scherm.

Doe hier mee aan de discussie met andere desktopgebruikers: [Norton Community](#).

Ouderlijk toezicht instellen

U kunt Ouderlijk toezicht nu instellen zodat uw kinderen veiliger kunnen internetten. Het is gemakkelijk en er zijn maar drie stappen.

Ouderlijk toezicht biedt alles wat u nodig heeft om de online activiteiten van uw gezin te beschermen tegen gevaren op het internet en ongeschikte content. Het helpt u er zelfs voor te zorgen dat uw kinderen geen vertrouwelijke gegevens doorgeven via internet.

Aanmelden bij uw Norton-account

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** naast **Ouderlijk toezicht op Instellen**.
- 3 Als u wordt gevraagd om u aan te melden, voert u uw accountgegevens in en meldt u zich aan.
- 4 Klik op de pagina die verschijnt op het tabblad **Family**.
- 5 Lees de **Servicevoorwaarden** en klik op **Akkoord en doorgaan** om uw gezin te configureren.
- 6 Volg de instructies op het scherm.

Een kind toevoegen aan uw account

Op ieder kind dat u toevoegt, past Ouderlijk toezicht de vooraf gedefinieerde huisregels toe die zijn gebaseerd op de leeftijd van het kind. U kunt de huisregels op elk moment aanpassen zodat deze beter aansluiten op de volwassenheid van ieder kind.

Opmerking: U kunt tot 15 kinderen aan uw account toevoegen. U kunt een kind op elk moment aan uw Norton Family-account toevoegen of hieruit verwijderen.

- 1 Typ de naam van uw kind in het vak **Naam van kind**.

Opmerking: De naam mag geen speciale tekens bevatten zoals &, # of \$.

- 2 Selecteer het geboortjaar van uw kind.

Huisregels worden op basis van de leeftijd van het kind toegepast.

- U kunt **een avatar selecteren** of **een foto uploaden** om een profielafbeelding voor uw kind in te stellen.

Opmerking: Nadat u de configuratie voor uw eerste kind heeft voltooid, kunt u [meer kinderen toevoegen](#) aan uw account.

- Klik op **Volgende**.

Norton Family installeren op het apparaat van uw kind

Installeer Norton Family op elk apparaat dat uw kind gebruikt. Als u niet op het apparaat van uw kind zit, klikt u op **Nee** om een downloadlink te verzenden in een e-mail. Open deze e-mail op het apparaat waarop u Norton Family wilt installeren.

Norton Family installeren op Windows

- Klik onder **Gebruikt uw kind dit apparaat?** op **Ja** en vervolgens op **Volgende**.
- Klik op het gedownloadte installatiebestand of voer dit uit.
- Norton-downloadbeheer installeert Norton Family automatisch op het apparaat.
- Lees de licentieovereenkomst en klik op **Akkoord en installeren**.
Het apparaat wordt automatisch aan uw account gekoppeld.
- Klik op **Doorgaan**.
- Klik in het venster Accounts bewerken op **Bewerken** naast het kind aan wie u dit apparaat wilt toewijzen.
- Klik op **meldt zich aan als** en kies het account dat het kind gebruikt om zich op dit apparaat aan te melden. Als uw kind meerdere gebruikersaccounts heeft, moet u het kind voor al die gebruikersaccounts selecteren.
- Klik op **Opslaan > OK**.

De Norton Family-app installeren op Android

- Tik in het venster **Norton Family installeren** op **Ja** en vervolgens op **Doorgaan**.
- Tik op **Norton Family-app downloaden**.
- Voltooi de handeling met **Play Store** als u hierom wordt gevraagd.
- Tik op **Installeren** en volg de instructies op het scherm.
- Open de Norton Family-app voor ouderlijk toezicht.
- Lees de **Norton-licentieovereenkomst** en tik op **Accepteren en doorgaan Aan de slag**.
- Klik op **Aanmelden** en voer uw accountgegevens in.

- 8 Tik op **Kind** om de modus Kind te activeren en tik vervolgens op **Doorgaan**.
In de modus Kind kunt u een kind toevoegen en huisregels toewijzen aan dit apparaat.
- 9 Tik op **Een kind toevoegen** en voer in het venster **PROFIEL** de gegevens van uw kind in om een kind toe te voegen.
Kies een avatar voor het profiel van uw kind door op de avataraafbeelding te tikken. U kunt een afbeelding uit uw galerie kiezen of direct een foto nemen voor het profiel van uw kind.
- 10 Tik op **Doorgaan** en vervolgens op **Opslaan**.
Norton Family heeft standaardhuisregels ingesteld op basis van het geboortjaar van uw kind. U kunt op **Huisregels** tikken om de regels te zien die aan uw kind zijn toegewezen.
- 11 Selecteer het kind aan wie u dit apparaat wilt toewijzen, geef een handige naam op om dit apparaat te identificeren, en tik vervolgens op **Gereed**.
- 12 Als u daarom gevraagd wordt, schakelt u de opties **App-gebruik** en **Toegankelijkheid** in.
- 13 In de melding die wordt weergegeven, tikt u op **Activeren** om Norton Family als de apparaatbeheerder in te stellen.

De Norton Family-app installeren op iOS

- 1 Tik in het venster **Norton Family installeren** op **Ja** en vervolgens op **Doorgaan**.
- 2 Tik op **Norton Family-app downloaden**.
- 3 Tik om **Norton Family** te installeren.
- 4 Tik op **Openen**.
- 5 Tik op **OK** om Norton Family toe te staan meldingen te sturen.
- 6 Lees de **Norton-licentieovereenkomst** en het **Privacybeleid**. Tik vervolgens op **Accepteren en doorgaan**.
- 7 Meld u aan met uw accountgegevens.
- 8 Voer in het venster **Kind toevoegen** de gegevens van uw kind in. Tik vervolgens op **Toevoegen**.
Tik op **Een nieuw kind toevoegen**, voer in het venster **Kind toevoegen** de gegevens van uw kind in en tik op **Toevoegen** om nog een kind toe te voegen.
Kies een avatar voor het profiel van uw kind door op de avataraafbeelding te tikken. U kunt een afbeelding uit uw galerie kiezen of direct een foto nemen voor het profiel van uw kind.
- 9 Selecteer het kind aan wie u dit apparaat wilt toewijzen. Geef ook een naam op waarmee u dit apparaat gemakkelijk kunt identificeren.
- 10 Tik op **Toewijzen**.

- 11 Tik op **Installeren** en volg de instructies op het scherm om een profiel te installeren.
Profielinstallatie is vereist om Direct vergrendelen en andere functies in te schakelen op het apparaat van uw kind.
- 12 Volg de instructies op het scherm om beperkingen in te stellen.

Norton Family installeren op het apparaat van een ouder

Nadat u de configuratie heeft voltooid, downloadt en installeert u de volgende mobiele app op uw apparaat:

- Android-apparaat: installeer de app **Norton Family voor ouderlijk toezicht**.
- iOS-apparaat: installeer de app **Norton Family voor ouders**

De Norton Family-app voor ouderlijk toezicht op Android downloaden en installeren

- 1 Open de Play Store-app en zoek naar **Norton Family voor ouderlijk toezicht**.
- 2 Selecteer de **Norton Family-app voor ouderlijk toezicht** en tik vervolgens op **Installeren**.
- 3 Open de app nadat deze is geïnstalleerd.
- 4 Lees de **Norton-licentieovereenkomst** en andere beleidsdocumenten. Tik vervolgens op **Doorgaan**.
- 5 Meld u aan met uw accountgegevens.
- 6 Tik op **Apparaat van ouder**. Als u het apparaat met uw kind deelt, moet u naar de modus **Kind** overschakelen voordat u het apparaat aan uw kind geeft.

De Norton Family-app voor ouders installeren op iOS

- 1 Open de App Store-app en zoek naar **Norton Family voor ouders**.
- 2 Selecteer **Norton Family voor ouders** en tik vervolgens op **Installeer**.
- 3 Open de app nadat deze is geïnstalleerd.
- 4 Lees de **Norton-licentieovereenkomst** en andere beleidsdocumenten. Tik vervolgens op **Doorgaan**.
- 5 Meld u aan met uw accountgegevens.

Bespreek alles met uw gezin

Communicatie is de sleutel tot de online veiligheid van uw gezin. Hiertoe kunt u een gesprek voeren met uw kind waarin u het belang van verantwoordelijk internetgebruik uitlegt.

Bescherm uw bankgegevens met Norton Safe Web

Bescherming tijdens het bankieren in Norton Safe Web biedt verhoogde beveiliging wanneer u transacties uitvoert via bankwebsites. Wanneer u een bankwebsite bezoekt met de browsers

Google Chrome, Mozilla Firefox of Microsoft Edge, ontvangt u een melding om de Norton Safe Web-extensie te installeren of in te schakelen. Klik op **Installeren** of **Inschakelen** in de melding en volg de instructies op het scherm om de Norton Safe Web-extensie te installeren of in te schakelen.

U kunt de waarschuwing melding voor bescherming tijdens het bankieren uitschakelen door in de melding te klikken op **Niet meer weergeven** of door naar het venster **Instellingen** te gaan.

Meldingen voor bescherming tijdens bankieren in- of uitschakelen

1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.

3 Klik in het venster **Instellingen** op **Firewall**.

4 Onder het tabblad **Inbraak- en browserbeveiliging**, in de rij **Meldingen voor bescherming tijdens bankieren**, zet u de **Aan / Uit**-schakelaar op **Uit** of **Aan**.

5 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

Uw apparaatbeveiliging beheren

Dit hoofdstuk bevat de volgende onderwerpen:

- [Wat te doen als uw apparaat gevaar loopt](#)
- [Norton gebruiken om de prestaties van de computer te optimaliseren en te verbeteren](#)
- [Norton-scans uitvoeren om uw pc op bedreigingen te controleren](#)
- [Uw Password Manager beheren](#)
- [Bescherm uw apparaat tegen misbruik, hackers en zero-day aanvallen.](#)
- [Norton instellen om toezicht te houden op toepassingen en schadelijke websites te blokkeren op uw computer](#)
- [Aan de slag met Norton Cloudback-up](#)
- [De instellingen van uw Norton-product aanpassen](#)

Wat te doen als uw apparaat gevaar loopt

In het hoofdvenster van Norton geeft de kleur van de tegels Beveiliging, Internetbeveiliging, Back-up en Prestaties de status van elke categorie als volgt aan:

- **Groen** : u bent beschermd.
- **Oranje** : uw computer vereist aandacht.
- **Rood** : uw computer loopt gevaar.

Opmerking: De back-upcategorie is alleen beschikbaar bij de abonnementen Deluxe, Premium en Norton 360.

Norton verhelpt automatisch alle problemen die uw beveiliging of de systeemprestaties verminderen en geeft de status 'Beveiligd' weer in het hoofdvenster. Norton geeft kwesties die uw aandacht vereisen weer als **Kwetsbaar** of **Aandacht vereist**.

Reageren op de aanduidingen Aandacht vereist of Kwetsbaar

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik op de rode of oranje tegel die **Kwetsbaar** of **Aandacht vereist** aangeeft in het hoofdvenster van Norton.

- 3 Klik op **Nu verhelpen** en volg de aanwijzingen op het scherm.

Als u nog steeds problemen ondervindt, klikt u op **Help > Ondersteuning** om het diagnostische hulpprogramma uit te voeren.

U kunt ook de [Norton Rescue Tools](#) proberen als u denkt dat uw computer ernstig is geïnfecteerd.

LiveUpdate uitvoeren

Het is raadzaam LiveUpdate regelmatig uit te voeren in de volgende gevallen:

- Als u de optie **Automatische LiveUpdate** heeft uitgeschakeld
- Als uw computer al geruime tijd niet met internet is verbonden

Opmerking: Voor LiveUpdate heeft u een geldig abonnement en een internetverbinding nodig.

LiveUpdate handmatig uitvoeren

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Beveiliging** en klik vervolgens op **LiveUpdate** in het hoofdvenster van het Norton-product.

- 3 Klik op **OK** in het venster **Norton LiveUpdate** wanneer de LiveUpdate is voltooid.

Beveiligingsbedreigingen voor apparaten die Norton detecteert weergeven of verhelpen

Wanneer Norton een bedreiging detecteert, wordt deze automatisch verwijderd, tenzij uw invoer vereist is om te bepalen hoe u de dreiging wilt oplossen. Als u informatie moet invoeren, geeft Norton de waarschuwing Bedreigingen gedetecteerd of Beveiligingsrisico weer met suggesties voor wat u kunt doen.

Risico's bekijken die automatisch zijn opgelost tijdens een scan

Risico's bekijken die automatisch zijn opgelost tijdens een scan

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 In het venster **Beveiligingsgeschiedenis** selecteert u **Opgeloste beveiligingsrisico's** in de vervolgkeuzelijst **Weergeven**.
- 4 Selecteer een risico in de lijst en bekijk vervolgens in het deelvenster **Details** de actie die is ondernomen.

Gedetecteerde beveiligingsrisico's verhelpen die tijdens een scan zijn gedetecteerd

In sommige gevallen wordt een risico niet automatisch opgelost door Norton, maar ziet u een aanbevolen actie die u kunt uitvoeren om het risico te verhelpen.

Gedetecteerde beveiligingsrisico's verhelpen die tijdens een scan zijn gedetecteerd

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 In het venster **Beveiligingsgeschiedenis** selecteert u **Onopgeloste beveiligingsrisico's** in de vervolgkeuzelijst **Weergeven**.
- 4 Selecteer een risico in de lijst als er onopgeloste risico's worden weergegeven.
- 5 Volg de **Aanbevolen actie** in het deelvenster **Details**.

Norton Power Eraser uitvoeren als u een gedetecteerd risico niet kunt verhelpen

Voer Norton Power Eraser als u het vermoeden heeft dat uw systeem is geïnfecteerd. Norton Power Eraser is een krachtig verwijderingsprogramma voor malware waarmee u de beveiligingsrisico's kunt elimineren die moeilijk te verwijderen zijn. Voor meer informatie: Zie ["Norton-scans uitvoeren om uw pc op bedreigingen te controleren"](#) op pagina 33.

Opmerking: Norton Power Eraser is een agressief verwijderingsprogramma voor malware. Soms verwijdert Norton Power Eraser niet alleen malware maar ook legitieme bestanden. Zorg dus dat u de scanresultaten grondig doorneemt voordat u een bestand verwijdert.

Een bestand herstellen dat onterecht als beveiligingsrisico is aangemerkt

Beveiligingsrisico's worden standaard door Norton van uw computer verwijderd en in quarantaine geplaatst. Als een bestand onterecht is verwijderd, kunt u het vanuit de quarantaine terugplaatsen op de oorspronkelijke locatie en het uitsluiten van latere scans.

Een bestand uit quarantaine herstellen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het Norton-hoofdvenster op **Beveiliging**. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** onder het vervolgkeuzemenu **Weergeven** de optie **Quarantaine**.
- 4 Selecteer het bestand dat u wilt herstellen.
- 5 Klik in het deelvenster **Details** op **Opties**.
- 6 Klik op **Dit bestand herstellen en uitsluiten** in het venster **Bedreiging gedetecteerd**.
- 7 In het venster **Uit quarantaine herstellen** klikt u op **Ja**.
- 8 Selecteer in het dialoogvenster **Zoeken naar map** de map of het station waarnaar u het bestand wilt herstellen, en klik dan op **OK**.

Opmerking: Sluit een programma alleen uit van Norton-productscans als u zeker weet dat het programma veilig is. Als een programma bijvoorbeeld afhankelijk is van een ander programma dat een beveiligingsrisico vormt, kunt u besluiten dat programma toch op uw computer te laten staan.

Risico's of bedreigingen in quarantaine verwerken

Items die in quarantaine worden geplaatst worden van de rest van uw computer geïsoleerd, zodat ze zich niet kunnen verspreiden en de computer niet kunnen infecteren. Als u van een item vermoedt dat het is geïnfecteerd, maar niet door Norton als een risico is geïdentificeerd, kunt u het handmatig in quarantaine plaatsen. U kunt een item uit de quarantaine terugzetten als u denkt dat het een laag risico heeft. Norton herstelt het item dat u terugzet niet. Norton kan de teruggezette items echter wel desinfecteren tijdens de daaropvolgende scans.

Een item uit de quarantaine terugzetten

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** in de vervolgkeuzelijst **Weergeven** de categorie **Quarantaine**.
- 4 Selecteer een item dat u wilt beheren.
- 5 Klik in het deelvenster **Details** op **Opties**.

Gebruik de link **Meer opties** om meer details over het item te bekijken voordat u een actie voor het item selecteert. Via de link wordt het venster **Bestandsinformatie** geopend dat meer informatie over het risico bevat.

- 6 Kies een van de volgende opties in het venster **Bedreiging gedetecteerd** :
 - **Herstellen** : hiermee worden de bestanden teruggezet naar de oorspronkelijke locatie op uw computer. Deze optie is alleen beschikbaar voor items die handmatig in quarantaine zijn geplaatst.
 - **Dit bestand herstellen en uitsluiten** : hiermee wordt het item zonder reparatie teruggeplaatst op de oorspronkelijke locatie en wordt uitgesloten van detectie in latere scans. Deze optie is beschikbaar voor gedetecteerde bedreigingen die wel en geen virussen zijn.
 - **Uit geschiedenis verwijderen** : hiermee kunt u het geselecteerde item uit het logbestand van de **Beveiligingsgeschiedenis** verwijderen.
- 7 Als u ervoor kiest het terug te zetten, klikt u in het venster **Uit quarantaine herstellen** op **Ja**.
- 8 Selecteer in het dialoogvenster **Zoeken naar map** de map of het station waarnaar u het bestand wilt herstellen, en klik dan op **OK**.

Een item naar Symantec verzenden voor analyse

Wanneer u bestanden opgeeft waarvan u denkt dat deze een beveiligingsrisico vormen, draagt u bij aan de doeltreffendheid van uw Norton-product. Symantec Security Response analyseert het bestand, bepaalt of het een risico vormt en voegt het toe aan latere beveiligingsdefinities.

Opmerking: Persoonlijke identificatiegegevens worden nooit in inzendingen opgenomen.

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.

- 3 Selecteer in het venster **Beveiligingsgeschiedenis** in de vervolgkeuzelijst **Weergeven** de categorie **Quarantaine**.
- 4 Selecteer een item dat u wilt beheren.
- 5 Klik in het deelvenster **Details** op **Opties**.
Gebruik de link **Meer opties** om meer details over het item te bekijken voordat u een actie voor het item selecteert. Via de link wordt het venster **Bestandsinformatie** geopend dat meer informatie over het risico bevat.
- 6 Klik op **Verzenden aan Symantec** in het venster **Bedreiging gedetecteerd**.
- 7 Klik op **OK** in het dialoogvenster dat verschijnt.

Een item handmatig in quarantaine plaatsen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** in de vervolgkeuzelijst **Weergeven** de categorie **Quarantaine**.
- 4 Klik op **In quarantaine plaatsen**.
- 5 Voeg in het venster **Handmatige quarantaine** het bestand toe dat u in quarantaine wilt plaatsen en voer een beschrijving in ter referentie.

Opmerking: Als u een bestand dat aan actieve processen is gekoppeld in quarantaine plaatst, worden de processen beëindigd. Sluit dus alle geopende bestanden en actieve processen voordat u een bestand in quarantaine plaatst.

Norton gebruiken om de prestaties van de computer te optimaliseren en te verbeteren

We weten hoe frustrerend het is wanneer uw computer langzamer wordt en het een eeuwigheid duurt om eenvoudige taken uit te voeren. Sommige gebruikers zijn van mening dat de prestaties van hun computer verslechteren na installatie van Norton. Maar feit is dat Norton gestroomlijnd is om een bescherming van wereldklasse te bieden zonder in te boeten op prestaties.

U kunt uw computer ook sneller maken met de tools van Norton voor prestatiebeheer en optimalisatie zodat u dagelijkse taken sneller kunt uitvoeren.

De opstarttijd van computer versnellen

Vele toepassingen zijn zo ingesteld dat ze worden gestart wanneer u uw computer start. Er worden programma's gestart die u zelden of nooit gebruikt, of waarvan u niet eens wist dat u ze had. En hoe meer programma's worden gestart, hoe langer alles duurt. Met **Opstartbeheer van Norton** kunt u opstartprogramma's uitschakelen of vertragen zodat u sneller aan de slag kunt gaan.

Opstartitems uitschakelen of vertragen

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Prestaties** in het Norton-hoofdvenster. Klik vervolgens op **Opstartbeheer**.

- 3 Doe het volgende in het venster **Opstartbeheer** :

- Hef in de kolom **Aan/Uit** de selectie op van de programma's die u niet gebruikt zodat deze niet worden gestart wanneer u uw computer start.
- Selecteer in de kolom **Opstartvertraging** de programma's die pas moeten worden geladen nadat het opstarten is voltooid.

- 4 Klik op **Toepassen** en vervolgens op **Sluiten**.

De laadtijd voor programma's en bestanden verbeteren

Met het hulpprogramma **Schijf optimaliseren** worden bestandsfragmenten die mettertijd over uw computer verspreid zijn geraakt, weer bij elkaar gezet. Het verbetert de prestaties van de computer, zodat u efficiënter werkt.

Schijf optimaliseren uitvoeren

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Prestaties** in het hoofdvenster van Norton. Klik vervolgens op **Schijf optimaliseren**.

- 3 Klik op **Sluiten** wanneer het proces is voltooid.

Tijdelijke bestanden en mappen verwijderen die de computer vertragen

Telkens wanneer u internet of bestanden downloadt, worden tijdelijke bestanden op uw computer opgeslagen. U hoeft ze niet te bewaren. Toch bouwt u in de loop van de tijd een hele verzameling op wat de prestaties van uw computer kan aantasten. Met het hulpprogramma Bestandsopruiming kunt u onnodige bestanden verwijderen om uw computer sneller te maken.

Tijdelijke bestanden en mappen verwijderen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Prestaties** in het hoofdvenster van Norton. Klik vervolgens op **Bestandsopruiming**.
- 3 Klik op **Sluiten** wanneer het proces is voltooid.

Uw computer optimaliseren

U kunt de prestaties en betrouwbaarheid van uw computer verbeteren door de vaste schijven te optimaliseren. Met Norton worden uw vaste schijven automatisch gecontroleerd op fragmentatie en geoptimaliseerd als ze meer dan 30% zijn gefragmenteerd. U kunt altijd de recentste rapporten raadplegen om te bepalen of optimalisatie noodzakelijk is.

U kunt Schijfoptimalisatie alleen uitvoeren wanneer de schijf meer dan 15 procent vrije ruimte heeft. Tijdens het schijfoptimalisatieproces worden SSD's (Solid-state drives) alleen in Windows 8 of latere besturingssystemen gedefragmenteerd.

Uw vaste schijven optimaliseren

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Prestaties** in het hoofdvenster van Norton. Klik vervolgens op **Schijf optimaliseren**.
- 3 Wanneer de activiteit is voltooid, klikt u op **Sluiten**.

Het opstartvolume optimaliseren

Wanneer u het opstartvolume optimaliseert, worden bestandsfragmenten in aansluitende of aangrenzende clusters herschikt, waardoor de bruikbare vrije ruimte wordt gemaximaliseerd. Wanneer de stationskop van de vaste schijf alle bestandsgegevens op één locatie vindt, kan het bestand sneller in het geheugen worden gelezen.

Het opstartvolume optimaliseren

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Prestaties** in het hoofdvenster van Norton. Klik vervolgens op **Grafieken**.
- 3 Klik boven aan de beveiligingsstatusgrafiek in het venster **Grafieken** op **Optimaliseren**.

Prestaties verbeteren wanneer ik game of films kijk

Is het u wel eens gebeurd dat uw beveiligingssoftware midden in een game of film werd gestart zodat het scherm op het meest ongelegen moment bevroor? U kunt instellen dat

Schermvullende detectie bepaalt wanneer er een programma actief is dat niet mag worden onderbroken. De achtergrondtaken die u beschermen, gaan dan pas van start wanneer u klaar bent met de app.

Zorg dat Schermvullende detectie is ingeschakeld.

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 Zet onder **Instellingen voor Stille modus** in de rij **Schermvullende detectie** de schakelaar op **Aan**.
- 5 Klik op **Toepassen** en vervolgens op **Sluiten**.

Onderbrekingen stoppen wanneer ik mijn favoriete apps gebruik

Als u van mening bent dat Norton uw favoriete programma's langzamer maakt, kunt u de **Stille modus** instellen zodat Norton niet wordt uitgevoerd wanneer u de programma's gebruikt. De achtergrondtaken die u beschermen, gaan dan pas van start wanneer u klaar bent met de programma's.

Mijn favoriete programma's in Stille modus uitvoeren

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 Klik op **Configureren** in de rij **Gebruikergedefinieerde programma's** onder **Instellingen voor Stille modus**.
- 5 Klik in het venster **Programma's met stille modus** op **Toevoegen**.
- 6 Ga naar uw programma in het dialoogvenster **Programma toevoegen**.
- 7 Selecteer het bestand en klik op **Openen**. Klik vervolgens op **OK**.

Programma's weergeven die veel systeembronnen gebruiken en mijn computer trager maken

Met Norton houdt u toezicht op uw computer en kunt u instellen dat een waarschuwing verschijnt wanneer een programma of proces een ongewone hoeveelheid bronnen gebruikt. U kunt deze programma's afsluiten om prestaties te verbeteren wanneer u ze niet gebruikt.

Processen identificeren die veel systeembronnen gebruiken

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Prestaties** in het hoofdvenster van Norton. Klik vervolgens op **Grafieken**.
- 3 Klik in het venster **Grafieken** in het linkerdeelvenster op **Gebruik**.
- 4 Voer een van de volgende handelingen uit:
 - Klik op de tab **CPU** als u de CPU-grafiek wilt weergeven.
 - Klik op de tab **Geheugen** als u de geheugengrafiek wilt weergeven.
- 5 Klik op een willekeurige plaats op de grafiek om een lijst met resource-belastende processen weer te geven.
Klik op de naam van een proces als u aanvullende informatie over dat proces wilt zien in het venster **Bestandsinformatie**.

Norton-scans uitvoeren om uw pc op bedreigingen te controleren

Virusdefinities worden automatisch bijgewerkt en uw pc wordt regelmatig op een reeks bedreigingen gescand. Als u offline bent geweest of vermoedt dat u een virus heeft, kunt u handmatig het volgende uitvoeren:

- **Snelle scan** om gebieden van uw computer te analyseren die het meest kwetsbaar zijn voor bedreigingen.
- **Volledige systeemsan** om uw hele systeem te analyseren, inclusief minder kwetsbare toepassingen, bestanden en actieve processen die tijdens een snelle scan niet worden gecontroleerd.
- **Aangepaste scan** om afzonderlijke bestanden, mappen of stations te analyseren als u vermoedt dat ze gevaar lopen.

Opmerking: Nadat u Norton heeft geïnstalleerd, kan de eerste scan een uur of langer duren om uw volledige systeem te analyseren.

Een Snelle scan, Volledige systeemsan of Handmatige scan uitvoeren

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.

- 3 In het venster **Scans** naast **Scans en taken** selecteert u een van de volgende:
 - **Snelle scan > Start**
 - **Volledige systeemsan > Start**
 - **Aangepaste scan > Start**. Klik vervolgens op **Uitvoeren** naast **Scan van station**, **Scan van map** of **Scan van bestand** om naar de onderdelen te gaan die u wilt scannen.
- 4 Klik in het venster **Resultatenoverzicht** op **Voltooien**.

Als items aandacht vereisen, kunt u de risico's beoordelen in het venster **Bedreigingen gedetecteerd**.

Volledige systeemsan

Met een volledige systeemsan wordt een uitvoerige scan uitgevoerd van de computer om virussen en andere beveiligingsbedreigingen te verwijderen. Hierbij worden alle opstartrecords, bestanden en actieve processen gecontroleerd waartoe de gebruiker toegang heeft. Hiermee wordt uw computer grondig en langduriger onderzocht.

Opmerking: Wanneer een volledige systeemsan wordt uitgevoerd door iemand met beheerdersrechten, worden er meer bestanden gescand dan wanneer de scan zonder beheerdersrechten wordt uitgevoerd.

Een volledige systeemsan uitvoeren

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Volledige systeemsan**.
- 4 Klik op **Start**.

Aangepaste scan

U wilt misschien zo nu en dan een bepaald bestand, verwisselbare stations, een vaste schijf, of alle mappen of bestanden op uw computer scannen. Wanneer u bijvoorbeeld met verwisselbare media werkt en vermoedt dat een virus aanwezig is, kunt u die specifieke schijf scannen. Heeft u in een e-mailbericht een gecomprimeerd bestand ontvangen en vermoedt u dat het een virus bevat, dan kunt u dat specifieke element scannen.

Afzonderlijke elementen scannen

- 1 Start Norton.
 Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste scan**.
- 4 Klik op **Start**.
- 5 In het venster **Scans** voert u een van de volgende handelingen uit:
 - Als u specifieke stations wilt scannen, klikt u op **Uitvoeren** naast **Scan van station**, vervolgens selecteert u de stations die u wilt scannen en tot slot klikt u op **Scannen**.
 - Als u specifieke mappen wilt scannen, klikt u op **Uitvoeren** naast **Scan van map**, vervolgens selecteert u de mappen die u wilt scannen en tot slot klikt u op **Scannen**.
 - Als u specifieke bestanden wilt scannen, klikt u op **Uitvoeren** naast **Scan van bestand**, vervolgens selecteert u de bestanden die u wilt scannen en tot slot klikt u op **Toevoegen**. U kunt ook de **Ctrl** -toets ingedrukt houden om meerdere bestanden te selecteren die u wilt scannen.
- 6 Klik in het venster **Resultatenoverzicht** op **Voltooien**.
 Als items aandacht vereisen, kunt u deze beoordelen en de aanbevolen actie ondernemen.

Norton Power Eraser-scan

Norton Power Eraser is een krachtig verwijderingsprogramma voor malware waarmee u beveiligingsrisico's kunt opruimen die moeilijk te verwijderen zijn. Norton Power Eraser maakt gebruik van agressievere technieken dan het normale scanproces. Daardoor bestaat er soms het risico dat Norton Power Eraser een betrouwbaar programma voor verwijdering markeert. Controleer scanresultaten zorgvuldig voordat u bestanden met Norton Power Eraser verwijdert.

Scannen met Norton Power Eraser

- 1 Start Norton.
 Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het hoofdvenster van het Norton-product. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Norton Power Eraser** op **Norton Power Eraser**.
- 4 Klik op **Start**.
- 5 Klik in het venster **Norton Power Eraser** op **OK**.
- 6 Klik in het hoofdvenster van **Norton Power Eraser** op **Geavanceerde scans**.

- 7 Klik op **Systeemsan**.
- 8 Controleer de scanresultaten en volg de instructies op het scherm om de gedetecteerde beveiligingsrisico's te verhelpen.

Uw eigen aangepaste Norton-scans maken

Hoewel de standaard automatische scaninstellingen van Norton voor de meeste gebruikers goed werken, is het mogelijk dat sommige gebruikers opties willen aanpassen om specifieke schijven, mappen of bestanden volgens een door hen gekozen schema te scannen.

Een aangepaste scan maken

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste scan**. Klik vervolgens op **Start**.
- 4 Klik in het venster **Scans** op **Scan maken**.
- 5 Voer in het venster **Nieuwe scan** naast **Scannaam** een naam in voor uw aangepaste scan en geef de instellingen als volgt op:
 - Klik op het tabblad **Scanitems** op **Stations toevoegen**, **Mappen toevoegen** of **Bestanden toevoegen** om naar de onderdelen te gaan die u in de scan wilt opnemen.
 - Selecteer op het tabblad **Scan plannen** onder Wanneer moet de scan worden uitgevoerd? een interval en selecteer vervolgens de timingopties.
Selecteer een optie onder **De scan uitvoeren**. Voor de meeste gebruikers is het het beste om alle vakjes aangevinkt te houden. Dit zorgt ervoor dat scans alleen worden uitgevoerd wanneer u uw computer niet gebruikt of wanneer u geen batterijvoeding gebruikt, en het voorkomt dat uw computer tijdens een scan naar de slaapstand overschakelt.
 - Verplaats op het tabblad **Scanopties** de schakelaars om het gedrag aan te passen voor gecomprimeerde bestanden of bedreigingen met een laag risico tijdens de scan.
- 6 Klik op **Opslaan**.

Een aangepaste scan van Norton bewerken of verwijderen

U kunt een aangepaste scan die u heeft gemaakt, bewerken om de naam te wijzigen, bestanden toe te voegen of te verwijderen of het schema aanpassen. U kunt de scan verwijderen als u deze niet meer nodig heeft.

Een aangepaste scan bewerken of verwijderen

- 1 Start Norton.
 Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste scan**. Klik vervolgens op **Start**.
- 4 Voer in het venster **Scans**, in de kolom **Scan bewerken**, naast de aangepaste scan die u wilt wijzigen een van de volgende taken uit:
 - Klik op het bewerkingspictogram en verschuif de schakelaars in het venster **Scan bewerken** om de scanopties in of uit te schakelen. De standaardinstellingen werken goed voor de meeste gebruikers. Klik op **Standaardwaarden gebruiken** om aangepaste instellingen te verwijderen.
 - Klik op het prullenbakpictogram en dan op **Ja** om te bevestigen dat u de scan wilt verwijderen.
- 5 Klik op **Opslaan**.

Norton-scans plannen

Norton detecteert wanneer u niet achter uw computer zit en voert automatisch scans uit om te zorgen dat uw systeem regelmatig op bedreigingen wordt gecontroleerd. U kunt ook uw eigen Snelle scan, Volledige systeemscan of Aangepaste scan plannen om op door u gewenste tijdstippen te worden uitgevoerd.

Een Snelle scan, Volledige systeemscan of Handmatige scan van Norton plannen

- 1 Start Norton.
 Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste scan**.
- 4 Klik op **Start**.
- 5 Klik in het venster **Scans**, in de kolom **Scan bewerken**, op het bewerkingspictogram naast Snelle scan, Volledige systeemscan of een Aangepaste scan die u eerder heeft gemaakt.
- 6 In het venster **Scan bewerken** op het tabblad **Scanplanning** doet u het volgende:
 - Selecteer onder **Wanneer moet de scan worden uitgevoerd?** een interval en selecteer vervolgens de timingopties.

- Selecteer een optie onder **De scan uitvoeren**. Voor de meeste gebruikers is het het beste om alle vakjes aangevinkt te houden. Dit zorgt ervoor dat scans alleen worden uitgevoerd wanneer u uw computer niet gebruikt of wanneer u geen batterijvoeding gebruikt, en het voorkomt dat uw computer tijdens een scan naar de slaapstand overschakelt.
- 7 Klik op **Volgende**.
 - 8 Klik op het venster **Scanopties** op **Opslaan**.

Realtimebedreigingen bekijken die door Norton SONAR-beveiliging worden gedetecteerd

Symantec Online Network for Advanced Response (SONAR) biedt realtimebeveiliging tegen bedreigingen en detecteert proactief onbekende beveiligingsrisico's. SONAR identificeert nieuwe bedreigingen op basis van het gedrag van toepassingen. Dit gaat sneller dan de traditionele bedreigingsdetectie op basis van handtekeningen. Het beveiligt u al tegen schadelijke code voordat virusdefinities via LiveUpdate beschikbaar zijn.

Het is raadzaam SONAR-beveiliging altijd ingeschakeld te laten.

Opmerking: Wanneer Auto-Protect is uitgeschakeld, is SONAR-beveiliging ook niet actief en is uw computer niet beschermd tegen nieuwe bedreigingen.

Zorg dat SONAR-beveiliging is ingeschakeld

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Zet op het tabblad **Automatische bescherming** onder **Realtimebeveiliging** de schakelaar **SONAR-beveiliging** op **Uit** of **Aan**.
Als u de schakelaar uitschakelt, zelfs voor een korte duur, zijn functies voor realtimebeveiliging uitgeschakeld en is uw computer mogelijk kwetsbaar.
- 5 Klik op **Toepassen**.
- 6 Als u de schakelaar heeft uitgeschakeld, selecteert u hoelang u wilt dat SONAR uit staat en klikt u op **OK**.
- 7 Klik in het venster **Instellingen** op **Sluiten**.

Risico's weergeven die zijn gedetecteerd door SONAR

- 1 Start Norton.
 Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 In het venster **Beveiligingsgeschiedenis** selecteert u **SONAR-activiteit** in de vervolgkeuzelijst.
- 4 Selecteer een risico in de lijst als er risico's worden weergegeven.
- 5 Volg de **Aanbevolen actie** in het deelvenster **Details**.
 Binnen deze categorie worden ook alle activiteiten vermeld die de configuratie of instellingen van uw computer aanpassen. De optie **Meer informatie** voor deze categorie biedt details over de resources die van invloed zijn op de activiteit.

Bestanden en mappen uitsluiten van de scans Norton Auto-Protect, SONAR en Downloadinformatie

U kunt Norton configureren om bepaalde programma's van de Auto-Protect- en SONAR-scans uit te sluiten. U kunt de vensters **Scanuitsluitingen** en **Realtime-uitsluitingen** gebruiken om virussen en andere beveiligingsbedreigingen met een hoog risico van scans uit te sluiten. Wanneer u een bestand of map aan de lijst met uitsluitingen toevoegt, negeert Norton het bestand of de map wanneer op beveiligingsrisico's wordt gescand.

Selecteer een map en download het bestand in de geselecteerde map om het bestand uit te sluiten van Downloadinformatie. Wanneer u bijvoorbeeld een onveilig uitvoerbaar bestand in deze map downloadt, laat Norton u het bestand downloaden en wordt het niet van uw computer verwijderd. U moet een nieuwe map maken speciaal voor uitsluitingen van Downloadinformatie.

Opmerking: Wanneer u een bestand van Norton-scans uitsluit, wordt het beveiligingsniveau van uw computer verlaagd. Doe dit alleen als u hier een specifieke reden voor heeft. Sluit items alleen uit als u zeker weet dat ze niet zijn geïnfecteerd.

Beveiligingsbedreigingen met een hoog risico van scans uitsluiten

- 1 Start Norton.
 Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik op de tab **Scans en risico's** in het venster **AntiVirus**.
- 5 Voer onder **Uitsluitingen/Lage risico's** een van de volgende handelingen uit:

- Klik in de rij **Items uitsluiten van scans** op **Configureren**.
 - Klik in de rij **Items die van Auto-Protect-, Scriptbeheer-, SONAR- en downloadinformatiedetectie moeten worden uitgesloten** op **Instellen**.
- 6 Klik in het weergegeven venster op **Mappen toevoegen** of **Bestanden toevoegen**.

U kunt uitsluitingen toewijzen aan lokale stations, mappen, groepen bestanden, afzonderlijke bestanden en netwerkstations. Het uitsluiten van bestanden op een netwerk wordt echter niet ondersteund door Norton. Als u een netwerkstation aan de lijst met uitsluitingen toevoegt, moet u ervoor zorgen dat het station met uw computer is verbonden.
 - 7 Klik op het bladerpictogram in het dialoogvenster **Item toevoegen**.
 - 8 Selecteer het item dat u van de scan wilt uitsluiten, in het dialoogvenster dat verschijnt.

U kunt ook opgeven of submappen moeten worden opgenomen wanneer u mappen toevoegt.
 - 9 Klik op **OK**.
 - 10 Klik op **OK** in het dialoogvenster **Item toevoegen**.
 - 11 Klik in het opgeroepen venster op **Toepassen** en vervolgens op **OK**.

Bestanden met handtekening voor laag risico van Norton-scans uitsluiten

Via de Uitsluitingen van handtekeningen kunt u specifieke bekende beveiligingsrisico's selecteren om deze uit te sluiten van Norton-scans. Als bijvoorbeeld een legitieme app, zoals een gratis game, afhankelijk is van een ander programma, zoals adware, om te functioneren zou u kunnen besluiten om de adware te behouden, zelfs als deze u blootstelt aan risico's. Ook kunt u aangeven dat waarschuwen niet meer nodig is bij toekomstige scans.

Opmerking: Uitsluitingen verlagen uw bescherming. Gebruik ze alleen als u ze specifiek nodig heeft en volledig begrijpt wat de risico's zijn wanneer u bekende bedreigingen uitsluit van Norton-scans.

Een handtekening voor laag risico toevoegen aan Uitsluitingen van handtekeningen

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik op het tabblad **Scans en risico's** in het venster met instellingen voor **AntiVirus**.

- 5 Klik op **Configureren** in de rij **Handtekeningen die van alle detecties worden uitgesloten** onder **Uitsluitingen/Lage risico's**.
- 6 Klik op **Toevoegen** in het venster **Uitgesloten handtekeningen**.
- 7 Klik in het venster **Beveiligingsrisico's** op een beveiligingsrisico dat u wilt uitsluiten, en klik op **Toevoegen**.
- 8 Klik in het venster **Uitgesloten handtekeningen** op **Toepassen** en vervolgens op **OK**.

Automatische taken in- of uitschakelen

Uw Norton-product voert automatische taken uit om uw pc zo onopvallend mogelijk te beveiligen. Deze automatische taken omvatten het scannen op virussen, controleren van uw internetverbinding, downloaden van beveiligingsupdates en andere belangrijke taken. Deze activiteiten worden op de achtergrond uitgevoerd wanneer uw computer is ingeschakeld.

Als een item uw aandacht vereist, wordt een bericht weergegeven met informatie over de huidige status of om u te vragen iets te doen. Als u geen berichten ziet, is uw computer beveiligd.

U kunt uw Norton-product altijd openen om de status van uw computer te bekijken of beveiligingsdetails weer te geven.

Wanneer een achtergrondactiviteit in voortgang is, wordt een bericht weergegeven in het meldingsgebied uiterst rechts op de taakbalk. De resultaten van de recentste activiteiten worden weergegeven wanneer u het hoofdvenster van Norton de volgende keer opent.

Automatische taken in- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Instellingen van Taakplanner**.
- 4 Voer de volgende handelingen uit op het tabblad **Automatische taken** van het venster **Taakplanner** :
 - Selecteer de functie die u automatisch wilt laten uitvoeren.
Schakel het selectievakje **Taken** in om alle functies aan te vinken.
 - Hef de selectie op van de functie die u niet automatisch wilt laten uitvoeren.
Schakel het selectievakje **Taken** uit om alle functies uit te schakelen.
- 5 Klik op **Toepassen** en vervolgens op **Sluiten**.

Aangepaste taken uitvoeren

Norton controleert uw systeem automatisch en kiest de beste instellingen om uw systeem beveiligd te houden. U kunt echter ook een aantal specifieke taken uitvoeren. U kunt de specifieke taken die u wilt uitvoeren, selecteren aan de hand van de opties in het venster **Aangepaste taken**.

U kunt voor eenmalige scans zelf een combinatie van taken kiezen. U kunt LiveUpdate uitvoeren, een back-up maken van uw gegevens, uw browsergeschiedenis wissen, schijfruimte vrijmaken door ongewenste (schijf)bestanden op te ruimen en uw schijven optimaliseren.

Aangepaste taken uitvoeren

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het hoofdvenster van Norton. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste taak**. Klik vervolgens op **Start**.
- 4 Selecteer in het venster **Aangepaste taken** de taken die u wilt uitvoeren.
Selecteer de optie **Taken** om alle taken te selecteren.
- 5 Klik op **Start**.

Beveiligings- en prestatiescans plannen

Via de instellingen van Taakplanner kunt u uw systeem automatisch op beveiligings- en prestatieproblemen laten controleren door Norton. Norton

De volgende opties zijn beschikbaar voor het plannen van beveiligings- en prestatiescans:

Automatisch (Aanbevolen)

Met deze optie wordt uw pc op beveiligings- en prestatieproblemen gecontroleerd wanneer de pc niet actief is.

Deze optie biedt maximale beveiliging.

Wekelijks

Met deze optie wordt uw pc een of meer keer per week gecontroleerd op beveiligings- en prestatieproblemen.

U kunt de dagen van de week en het tijdstip van de dag selecteren waarop de scan moet worden uitgevoerd.

Maandelijks

Met deze optie wordt uw pc een keer per maand gecontroleerd op beveiligings- en prestatieproblemen.

U kunt de dag van de maand en het tijdstip van de dag selecteren waarop de scan moet worden uitgevoerd.

Handmatige planning

Met deze optie wordt geen geplande beveiligings- of prestatiescan van uw pc uitgevoerd.

Als u deze optie kiest, moet u regelmatig handmatige beveiligings- en prestatiescans van uw pc uitvoeren om de beveiliging in stand te houden.

Uw computer presteert optimaal als u belangrijke bewerkingen laat uitvoeren op momenten waarop uw computer niet actief is. Wanneer u de scans wekelijks of maandelijks plant en de optie **Alleen uitvoeren tijdens inactiviteit** selecteert, wordt uw computer door Norton gescand wanneer deze niet actief is. Het is raadzaam de optie **Alleen uitvoeren tijdens inactiviteit** te selecteren om computerprestaties te optimaliseren.

Beveiligings- en prestatiescans plannen

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik in het hoofdvenster van Norton op **Instellingen**.

- 3 Klik in het venster **Instellingen** op **Instellingen van Taakplanner**.

- 4 Selecteer een optie op het tabblad **Planning** onder **Plannen**.

Wanneer u de optie **Wekelijks** of **Maandelijks** selecteert, moet u het tijdstip en de datum selecteren waarop de automatische taken moeten worden uitgevoerd. U kunt ook opgeven dat de automatische taken alleen mogen worden uitgevoerd wanneer de pc niet actief is.

- 5 Klik op **Toepassen** en vervolgens op **Sluiten**.

Gegevensbescherming configureren om schadelijke processen te blokkeren die uw pc beïnvloeden

Gegevensbescherming beschermt uw pc tegen schadelijke processen die uw pc destabiliseren, uw gegevens beschadigen en/of stelen, en hun schadelijke aard aan andere goede processen doorgeven. Het maakt gebruik van Norton-reputatietechnologie om een proces als veilig, schadelijk of onbekend te identificeren. Op basis van deze identificatie, voorkomt Smartlisting dat schadelijke processen bewerkingen op uw pc uitvoeren. Deze tool is agressiever bij het beschermen van uw bestanden en blokkeert zelfs veilige processen als er tijdens de runtime een schadelijk bestand in wordt geïnjecteerd. Gegevensbescherming is standaard ingeschakeld

en beschermt vooraf ingestelde mappen en extensies. Afhankelijk van uw situatie kunt u meer mappen en/of extensies toevoegen, en processen uitsluiten van scans en bescherming.

Waarschuwing: Als u deze functie uitschakelt, wordt uw pc minder beveiligd. We raden u dus aan om deze functie altijd ingeschakeld te houden. Als u deze functie echter wilt uitschakelen, doe het dan slechts tijdelijk en zorg dat de functie ook weer wordt ingeschakeld.

Gegevensbescherming in- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.
- 3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.
- 4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan** of **Uit**.
- 5 Voer een van de volgende handelingen uit in de rij **Meldingen weergeven** :
 - Zet de schakelaar op **Aan** om een melding te krijgen telkens wanneer Gegevensbescherming een bedreiging blokkeert.
 - Zet de schakelaar op **Uit** om meldingen te onderdrukken. U kunt de details van de geblokkeerde bedreigingen echter bekijken in het venster **Beveiligingsgeschiedenis**. U opent het venster **Beveiligingsgeschiedenis** door in het hoofdvenster van Norton te dubbelklikken op **Beveiliging** en dan op **Geschiedenis > Gegevensbescherming**.
- 6 Klik op **Toepassen**.
- 7 Indien u daarom wordt gevraagd, geeft u op na hoeveel tijd de functie Gegevensbescherming moet worden uitgeschakeld en klikt u op **OK**.

Een map voor Gegevensbescherming toevoegen of bewerken

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.
- 3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.
- 4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan**.
- 5 Ga als volgt te werk om een map toe te voegen of te bewerken:
 - Klik naast **Beveiligde mappen** op **Configureren**.
 - Voer de volgende stappen uit in het venster **Beveiligde mappen** :
 - Klik op **Toevoegen** om een nieuw item toe te voegen.

- Als u een bestaand item wilt toevoegen, kiest u het item en klikt u op **Bewerken** om het te wijzigen.

Opmerking: Vooraf ingestelde mappen kunnen niet worden bewerkt.

- Klik in het venster **Item toevoegen** of **Item bewerken** op



- om naar de map te bladeren en deze te selecteren.
- Klik op het selectievakje om de submappen ook op te nemen.
- Klik op **OK**.

- 6 Klik op **Toepassen** en vervolgens op **OK**.

Een extensie toevoegen voor Gegevensbescherming

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.
- 3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.
- 4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan**.
- 5 Ga als volgt te werk om een extensie toe te voegen:
 - Klik naast **Beschermde bestandstypen** op **Configureren**.
 - Klik in het venster **Beschermde bestandstypen** op **Toevoegen**.
 - In het venster **Item toevoegen** typt u de extensie die u wilt beschermen. Als u bijvoorbeeld uitvoerbare bestanden wilt beschermen, typt u **.exe** in het vak. Alle bestanden met een **.exe**-extensie op de pc zijn beschermd.
 - Klik op **OK**.

- 6 Klik op **Toepassen** en vervolgens op **OK**.

Een map of extensie uit Gegevensbescherming verwijderen

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.
- 3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.

- 4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan**.
- 5 Klik naast **Beschermde mappen** of **Beschermde bestandstypen** op **Configureren**.
- 6 In het venster **Beschermde mappen** of **Beschermde bestandstypen** kiest u het item dat u wilt verwijderen.

Opmerking: U kunt geen vooraf ingestelde map of extensie verwijderen.

- 7 Klik op **Verwijderen**.
- 8 Klik op **Toepassen** en vervolgens op **OK**.

Een proces toevoegen aan of verwijderen van de uitsluitingslijst van Gegevensbescherming

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.
- 3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.
- 4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan**.
- 5 Klik in de rij **Uitgesloten processen** op **Configureren** en voer de volgende stappen uit:
 - Als u een proces wilt toevoegen voor uitsluiting van Gegevensbescherming, klikt u op **Toevoegen** en kiest u vervolgens het proces.
 - Als u een proces wilt verwijderen van uitsluiting van Gegevensbescherming, klikt u op het proces en vervolgens op **Verwijderen**.
- 6 Klik op **Toepassen** en vervolgens op **OK**.

Norton instellen om scripts die door phishing-pogingen kunnen worden misbruikt te verwijderen

Scriptbeheer helpt u te beschermen tegen malware die u downloadt of als bijlage ontvangt in phishingmails. De functie verwijdert standaard verdachte scripts uit bestanden en schoont de bestanden op **. U kunt de originele bestanden echter nog met het script herstellen. Ook kunt u instellen hoe Norton documenten met ingesloten scripts moet afhandelen.

Opmerking: **Deze functie wordt voor de browsers Chrome, Edge en Internet Explorer alleen ondersteund op Windows 10 RS2 en later.

Scripts worden gebruikt om documenten dynamisch en interactief te maken. Hoewel het primaire doel van scripts is de documentervaring te verbeteren, kunnen cybercriminelen deze gebruiken om stiekem malware op uw computer te zetten. Scripts zijn over het algemeen niet

belangrijk voor het functioneren van een document en worden door veel softwareprogramma's standaard uitgeschakeld.

U kunt instellen dat Norton specifieke bestanden van Scriptbeheer uitsluit als u zeker weet dat deze geen schadelijke inhoud bevatten. Zie voor meer informatie Zie "[Bestanden en mappen uitsluiten van de scans Norton Auto-Protect, SONAR en Downloadinformatie](#)" op pagina 39.. U kunt de originele bestanden herstellen door de opgeschoonde bestanden te vervangen. Sluit alleen bestanden uit als u zeker weet dat ze geen schadelijke inhoud bevatten.

Scriptbeheer identificeert mogelijke bedreigingen op basis van het gedrag van bestanden. Als Norton mogelijk gevaarlijke activiteiten detecteert wanneer u een document met ingesloten script opent, blokkeert de toepassing het script. U kunt instellen hoe Norton de scripts moet afhandelen wanneer u documenten met ingesloten scripts opent.

Het originele bestand herstellen

- 1 Start Norton.
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** de optie **Weergeven** in de keuzelijst. Selecteer vervolgens **Scriptbeheer**.
- 4 Selecteer in de weergave **Scriptbeheer** het item dat u wilt herstellen.
- 5 Klik in het rechterdeelvenster onder **Details** op **Herstellen**.
- 6 Klik in het venster **Scriptbeheer herstellen** op **Ja**.
- 7 Selecteer **Ja** in de prompt die verschijnt.
- 8 Klik in het venster **Beveiligingsgeschiedenis** op **Sluiten**.

Scriptbeheer in- of uitschakelen

- 1 Start Norton.
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik in het venster **Antivirus** op het tabblad **Scriptbeheer**.
- 5 In de rij **Scripts verwijderen bij het downloaden van documenten** zet u de **Aan/uit**-schakelaar op **Aan** of **Uit**.
Als u deze uitschakelt, doet u het volgende:
 - Selecteer in het venster **Beveiligingsverzoek** in de keuzelijst **Selecteer de duur** hoelang u de optie wilt uitschakelen.

- 6 In de rij **Scripts blokkeren wanneer documenten worden geopend** zet u de **Aan/Uit**-schakelaar op **Aan** of **Uit**.

Als u deze uitschakelt, doet u het volgende:

- Selecteer in het venster **Beveiligingsverzoek** in de keuzelijst **Selecteer de duur** hoelang u de optie wilt uitschakelen.

- 7 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

Alle items van Scriptbeheer permanent verwijderen

- 1 Start Norton.

Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.

- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** de optie **Weergeven** in de keuzelijst. Selecteer vervolgens **Scriptbeheer**.
- 4 Klik in de weergave **Scriptbeheer** op **Items wissen**.
- 5 Klik in het venster **Items wissen** op **Ja**.
- 6 Klik in het bevestigingsvenster op **Ja**.
- 7 Klik in het venster **Beveiligingsgeschiedenis** op **Sluiten**.

Stel in hoe Norton documenten met ingesloten scripts moet afhandelen

- 1 Start Norton.

Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.

- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik in het venster **Antivirus** op het tabblad **Scriptbeheer**.
- 5 Klik onder **Scripts blokkeren wanneer documenten worden geopend** in de rij **Microsoft Office** op **Configureren**.
- 6 Selecteer in het venster **Voorkeuren voor Microsoft Office** onder **Acties** de actie die Norton voor elke toepassing moet uitvoeren.

U kunt kiezen uit:

- **Blokkeren**
- **Toestaan**
- **Mij vragen**

U kunt voor elke toepassing een andere actie kiezen.

- 7 Klik op **OK** in het bevestigingsvenster dat verschijnt.
- 8 Klik op **Toepassen** in het venster **Voorkeuren voor Microsoft Office** en klik vervolgens op **OK**.
- 9 Selecteer in de rij **Adobe-document** de actie die Norton voor Adobe-documenten moet uitvoeren.
- 10 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

Veelgestelde vragen: Scriptbeheer van Norton

Wat zijn scripts en waarom worden ze door Norton verwijderd?

Scripts worden gebruikt om documenten dynamisch en interactief te maken. Ze kunnen ook functionaliteit toevoegen door bepaalde taken te automatiseren.

Scripts kunnen het volgende bevatten:

- ActiveX-besturingselementen
- Add-ins
- Gegevensverbindingen
- Macro's
- Gekoppelde OLE-bestanden (Object Linking and Embedding)
- Kleurthemabestanden

Hoewel het primaire doel van scripts is de documentervaring te verbeteren, kunnen cybercriminelen deze gebruiken in phishing-pogingen om stiekem malware op uw computer

te zetten. Scripts zijn over het algemeen niet belangrijk voor het functioneren van een document en worden door veel softwareprogramma's standaard uitgeschakeld.

Kan het verwijderen van scripts problemen veroorzaken?

Dat hangt ervan af. Als een document op scripts vertrouwt voor interactiviteit of het downloaden van extra inhoud, werkt die functionaliteit niet als het script wordt verwijderd.

Word ik nog steeds beschermd zelfs als ik Scriptbeheer uitschakel?

Norton detecteert wanneer wordt geprobeerd malware in een document uit te voeren, waaronder malware ingesloten door scripts, dus u moet worden beschermd. Scriptbeheer biedt een extra beveiligingslaag door scripts te verwijderen en documenten op te schonen.

Hoe krijg ik het originele bestand terug?

- 1 Start Norton.
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** de optie **Weergeven** in de keuzelijst. Selecteer vervolgens **Scriptbeheer**.
- 4 Selecteer in de weergave **Scriptbeheer** het actieve contentitem dat u wilt herstellen.
- 5 Klik in het rechterdeelvenster onder **Details** op **Herstellen**.
- 6 Klik in het venster **Scriptbeheer herstellen** op **Ja**.
- 7 Selecteer **Ja** in de prompt die verschijnt.
- 8 Klik in het venster **Beveiligingsgeschiedenis** op **Sluiten**.

Welke toepassingen blokkeert Norton als het een mogelijke bedreiging detecteert?

Norton voorkomt dat u de volgende toepassingen kunt openen als het mogelijk gevaarlijke activiteiten detecteert:

- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Word

Naast deze toepassingen detecteert en blokkeert Norton scripts van Adobe-documenten, veelvoorkomende hulpprogramma's van ontwikkelaars, WMI-tools (Windows Management Instrumentation), opdrachtregelinterfaces en scriptinterfaces.

Scripts blokkeren bij het downloaden vs. openen van documenten: wat is het verschil?

Wanneer u een document met een ingesloten script downloadt, gebruikt Scriptbeheer **Auto-Protect** om verdachte scripts op te sporen. **Auto-Protect** gebruikt de bedreigingshandtekeningen die Norton tijdens het updaten van virusdefinities ontvangt, en andere beveiligingsupdates om de veiligheid van ieder bestand dat u downloadt te bepalen.

Wanneer u een document met een ingesloten script opent, gebruikt Scriptbeheer **SONAR-bescherming** om mogelijk gevaarlijke activiteiten op te sporen. Het identificeert mogelijke bedreigingen op basis van het gedrag van bestanden en zorgt ervoor dat de toepassing het script niet kan uitvoeren.

Opmerking: De optie **Scripts verwijderen bij het downloaden van documenten** is voor de browsers Chrome, Edge en Internet Explorer alleen beschikbaar op Windows 10 RS2 en later.

Norton raadt aan beide Scriptbeheeropties altijd ingeschakeld te houden.

Uw Password Manager beheren

Met Password Manager kunt u uw wachtwoorden beheren en van extra beveiliging bij online transacties profiteren. Met de verschillende functies in Password Manager kunt u persoonlijke gegevens beheren, zoals adressen, geboortedatum en creditcardgegevens.

U kunt Password Manager in- of uitschakelen op de pagina Extensies in Google Chrome of op de pagina Add-ons in Mozilla Firefox.

Password Manager in- of uitschakelen op de pagina Extensies in Google Chrome

- 1 Start Google Chrome.
- 2 Klik in de rechterbovenhoek op **Instellingen**.
- 3 Ga in de optie **Instellingen** naar **Meer tools** en klik op **Extensies**.
- 4 Als op de pagina **Extensies** de optie **Norton Password Manager** is **Ingeschakeld**, heft u deze selectie op.

Als Norton Password Manager is uitgeschakeld, selecteert u het vakje **Ingeschakeld**

- 5 Start Google Chrome opnieuw

Password Manager in- of uitschakelen op de pagina Add-ons in Mozilla Firefox

- 1 Start Mozilla Firefox.
- 2 Klik op het **Firefox** -menu en vervolgens op **Add-ons**.
- 3 Klik op het tabblad **Extensies** op **Norton Password Manager**.
- 4 Als **Norton Password Manager** grijs wordt weergegeven, klikt u op **Inschakelen**.
Als Norton Password Manager niet grijs wordt weergegeven, klikt u op **Uitschakelen**.
- 5 Start Mozilla Firefox opnieuw.

Password Manager in- of uitschakelen op de pagina Extensies in Safari

- 1 Start Safari.
- 2 Klik in het menu Safari op **Safari** en vervolgens op **Voorkeuren**.
- 3 Klik **Extensies**.
- 4 Als optie Norton Password Manager in het linkerdeelvenster is **Ingeschakeld**, heft u deze selectie op. Als Norton Password Manager is uitgeschakeld, selecteert u het vakje **Ingeschakeld**

Norton Safe Web in- of uitschakelen

Norton Safe Web beschermt u wanneer u online surft, zoekt of winkelt in Internet Explorer, Firefox, Google Chrome of Microsoft Edge. Het analyseert de beveiligingsniveaus van de websites die u bezoekt en geeft de websites aan die geen bedreiging vormen. Aan de pictogrammen voor siteclassificatie naast de zoekresultaten kunt u zien of een website schadelijk is voordat u deze bezoekt.

Norton Safe Web in- of uitschakelen via extensiepagina in Google Chrome

- 1 Start Google Chrome.
- 2 Klik in de rechterbovenhoek op **Instellingen**.
- 3 Ga in de optie **Instellingen** naar **Meer tools** en klik op **Extensies**.
- 4 Als Norton Safe Web op de pagina **Extensies** is ingeschakeld, schakelt u het selectievakje **Ingeschakeld** uit.
Als Norton Safe Web is uitgeschakeld, schakelt u het selectievakje **Ingeschakeld** in.
- 5 Start Google Chrome opnieuw.

Norton Safe Web in- of uitschakelen via de pagina Add-ons in Mozilla Firefox

- 1 Start Mozilla Firefox.
- 2 Klik in het Firefox-menu op **Add-ons**.

- 3 Klik op het tabblad **Extensies** op **Inschakelen**.

Als Norton Safe Web niet grijs wordt weergegeven, klikt u op **Uitschakelen**.

- 4 Start Mozilla Firefox opnieuw.

Norton Safe Web in- of uitschakelen op de pagina Extensies in Safari

- 1 Start Safari.
- 2 Klik in het menu **Safari** op **Safari** en vervolgens op **Voorkeuren**.
- 3 Klik op **Extensies**.
- 4 Als optie Norton Safe Search in het linkerdeelvenster is **Ingeschakeld**, heft u deze selectie op.

Als Norton Safe Search is uitgeschakeld, selecteert u het vakje **Ingeschakeld**.

Norton Safe Web in- of uitschakelen via extensiepagina in Microsoft Edge

- 1 Start Microsoft Edge.
- 2 Klik in de rechterbovenhoek op de knop **Meer**



en selecteer **Extensies**.

- 3 Klik in het venster **Extensies** op **Extensies downloaden uit de Store**.
- 4 Typ in het venster **Store** de naam Norton in het vak Zoeken.
- 5 Klik in de resultaten op **Norton Safe Web** en klik op **Installeren**.
- 6 Klik op **Starten** wanneer de extensie is geïnstalleerd.
- 7 Klik in het pop-upvenster **U heeft een nieuwe extensie** op **Inschakelen**.

Als het pop-upvenster ontbreekt, klikt u in de rechterbovenhoek van Microsoft Edge op **Meer**



, en selecteert u **Extensies**.

- 8 Verplaats in het venster **Norton Safe Web** onder **Norton Safe Web** de schuifregelaar naar **Aan**.

Verplaats de schuifregelaar naar **Uit** om Norton Safe Web uit te schakelen.

Op het web zoeken met Norton Safe Search

Norton Safe Search vormt een verrijking van uw zoekacties op internet. Wanneer u op internet zoekt met behulp van Norton Safe Search, wordt er gebruikgemaakt van Ask.com en Yahoo! om zoekresultaten te genereren. Norton Safe Search toont de beveiligingsstatus van de website en de Norton-beoordeling voor alle gegenereerde zoekresultaten.

Norton Safe Search biedt ook een intelligente functie om te zoeken terwijl u typt, zodat zoeksuggesties direct worden weergegeven wanneer u een aantal letters van de zoekterm intypt.

Opmerking: De functie Norton Safe Search is alleen beschikbaar voor sommige regio's, met inbegrip van Australië, België, Brazilië, Canada, Denemarken, Finland, Frankrijk, Duitsland, Italië, Japan, Nederland, Noorwegen, Spanje, Zweden, Zwitserland, de Verenigde Staten en het Verenigd Koninkrijk. De functie Privacy Safeguard is alleen beschikbaar voor de Verenigde Staten, het Verenigd Koninkrijk en Canada.

U kunt Norton Safe Search zelfs gebruiken wanneer u de functies van Password Manager heeft uitgeschakeld.

Opmerking: Norton Safe Search wordt alleen ondersteund door de browsers Internet Explorer, Firefox en Chrome.

Op het web zoeken met Norton Safe Search

- 1 Open uw browser.
- 2 Typ uw zoekopdrachten in het vak **Norton Safe Search** op de Norton Security-werkbalk.
- 3 Voer een van de volgende handelingen uit:
 - Klik op **Safe Search**.
 - Selecteer in het pop-upvenster een suggestie die overeenkomt met uw zoekreeks.

Het Norton Safe Search-vak inschakelen op de werkbalk

Opmerking: Deze functie is alleen beschikbaar voor Internet Explorer.

Wanneer u Norton installeert, wordt de Norton Security-werkbalk toegevoegd aan Internet Explorer. Wanneer u Internet Explorer opent, wordt u gevraagd het vak **Norton Safe Search** op uw werkbalk in te schakelen.

Als u het zoekvak van Norton Safe Search handmatig heeft uitgeschakeld en u het weer wilt inschakelen, doet u het volgende:

- 1 Open uw browser.
- 2 Klik op het pictogram Instellingen (...) op de Norton Security-werkbalk.
- 3 In het menu dat verschijnt, zet u de schakelaar naast **Norton Safe Search** op **Aan**.

Als u het Norton Safe Search-vak wilt uitschakelen, doet u het volgende:

- 1 Open uw browser.
- 2 Klik op het pictogram Instellingen (...) op de Norton Security-werkbalk.
- 3 In het menu dat verschijnt, zet u de schakelaar naast **Norton Safe Search** op **Uit**.

Norton Password Manager openen

U kunt Password Manager vanuit de volgende gebieden openen:

- Via de sectie **Internetbeveiliging** in het hoofdvenster van het product in Windows
- Via de Norton Password Manager-extensie
- Via de Norton Password Manager-app in Android en iOS

U kunt de opties **Aanmeldingen** en **Kaarten** in het deelvenster **Webbeveiliging** gebruiken voor toegang tot respectievelijk het venster **Aanmeldingen beheren** en **Kaarten beheren**.

U kunt alle Password Manager-gegevens openen, zelfs nadat het product is verlopen. Dit zijn de functies die u kunt bekijken of openen nadat het product is verlopen:

Aanmeldingen	U kunt de opgeslagen aanmeldingsinformatie bekijken, zoals de aanmeldingsgegevens van uw online bankrekening, uw gebruikersnaam voor e-mail en uw wachtwoord.
Adressen	U kunt uw opgeslagen persoonlijke gegevens bekijken, zoals uw naam, uw geboortedatum, uw postadres, uw e-mailadres en uw telefoonnummers.
Portemonnee	U kunt uw opgeslagen financiële gegevens bekijken, zoals uw creditcardgegevens, bankrekeninggegevens en betalingsgegevens.
Opmerkingen	U kunt de opgegeven tekst later raadplegen.

Opmerking: U moet zijn aangemeld bij Password Manager om de Password Manager-functies te kunnen gebruiken. De Password Manager-functies worden ondersteund in de browsers Internet Explorer, Firefox, Safari en Chrome.

De Norton Password Manager-app in Android of iOS downloaden en installeren

- 1 Voer een van de volgende handelingen uit:

- Ga op Android naar **Play Store**. Als u Play Store voor het eerst opent, wordt het scherm met de servicevoorwaarden weergegeven. Tik op **Accepteren** om door te gaan.
 - Tik in iOS op het pictogram **App Store** op uw startscherm.
- 2 Zoek en selecteer de Norton Password Manager-app.
 - 3 Voer een van de volgende handelingen uit:
 - Tik in Android op het scherm met toepassingsdetails op **Installeren** en tik op **Accepteren en downloaden**.
 - Tik in iOS op **Gratis** en vervolgens op **INSTALLEER APP**. Typ het wachtwoord van uw Apple-account in het vak **Apple ID-wachtwoord**.

Norton Password Manager-safe in de cloud maken

Met Password Manager kunt u een safe in de cloud maken om uw Password Manager-gegevens in op te slaan. Per Norton-account kunt u één safe in de cloud maken. Met een safe in de cloud heeft u uw Password Manager-gegevens gemakkelijk bij de hand wanneer u onderweg bent.

U heeft toegang tot Password Manager in de cloud vanaf elke computer die met internet is verbonden.

Safe in de cloud maken via de browser

- 1 Open uw browser.
- 2 Klik in de rechterbovenhoek van de browser op **Norton Password Manager**.
- 3 Klik op het aanmeldingsscherm van Norton Password Manager op **Aanmelden**.
- 4 Klik in het venster **Welkom bij Norton** op **Een account maken**.
- 5 Vul de velden op het tabblad **Een account maken** in en klik op **Account maken**.
- 6 Klik in het venster **Geen safe gedetecteerd** op **Safe maken**.
- 7 In het venster **Uw safe maken** voert u uw wachtwoord in en klikt u op **Volgende**.
Het wachtwoord moet aan alle vermelde vereisten voldoen om te worden geaccepteerd.
- 8 Voer uw wachtwoord nogmaals in en klik op **Volgende**.
- 9 Voer een geheugensteun voor uw wachtwoord in en klik op **Safe maken**.
- 10 Klik in het venster **Instellen voltooid** op **Ga naar safe**.

Safe in de cloud van Norton maken

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik in het hoofdvenster van Norton op **Internetbeveiliging** en klik vervolgens op **Password Manager**.
- 3 Meld u in het venster **Aan de slag** aan met uw accountgegevens.
- 4 Geef in het venster **Nieuwe safe maken: safewachtwoord** in het vak **Safewachtwoord** uw wachtwoord op en klik op **Volgende**.
- 5 Geef in het venster **Nieuwe safe maken: wachtwoord bevestigen** het wachtwoord nogmaals op om het te bevestigen en klik dan op **Volgende**.
- 6 Geef in het venster **Nieuwe safe maken: geheugensteun** een hint voor het wachtwoord op. Klik dan op **Volgende**.
Als u al een back-up van uw Password Manager-gegevens heeft, klikt u op **Importeren** en selecteert u het back-upbestand om dat met het nieuwe account samen te voegen.
- 7 Klik op **Voltooien**.

Een safe in de cloud maken op Android of iOS

- 1 Meld u aan bij de **Norton Password Manager** -app.
- 2 Typ in het venster **Aanmelden** het e-mailadres en wachtwoord van uw Norton-account.
- 3 Tik op **Aanmelden** en volg de instructies op het scherm.

Uw Norton Password Manager-safe in de cloud verwijderen

Uw cloudsafe is gecodeerd en kan alleen worden opgeroepen via uw Norton-account en safewachtwoorden. Uw safe in de cloud kunt u alleen handmatig verwijderen. Zelfs als u Norton van uw apparaat verwijdert, kunt u uw safe blijven gebruiken op andere apparaten.

Waarschuwing: Wanneer u een safe verwijdert, worden alle Password Manager-gegevens die u in de safe heeft opgeslagen, permanent verwijderd. Als u denkt dat u uw safegegevens in de toekomst zult gebruiken, moet u uw safe niet verwijderen.

Uw safe in de cloud verwijderen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik in het hoofdvenster van Norton op **Internetbeveiliging** en klik vervolgens op **Password Manager**.

- 3 Geef in het venster **Safe gesloten** uw wachtwoord driemaal fout op.
- 4 Klik op de link **Klik hier** naast **Wilt u uw safe verwijderen?**.
- 5 Klik in het venster **Safe verwijderen** op **Ja, mijn safe verwijderen**.
- 6 Klik op **Ja** in het dialoogvenster Waarschuwing.
- 7 Typ uw Norton-accountwachtwoord en klik op **Aanmelden**.
- 8 Klik in het bevestigingsvenster op **OK**.

Hoe krijg ik toegang tot mijn 'safe in de cloud'-account na het verwijderen van Norton?

- 1 [Meld u aan](#) bij de Norton Password Manager-website met uw Norton-accountgegevens.
- 2 Typ het wachtwoord van uw safe in het venster **Uw safe openen** en klik vervolgens op **Safe openen**.

Uw Norton Password Manager-gegevens exporteren

U kunt uw Password Manager-gegevens exporteren ter beveiliging, voor gegevensherstel, of wanneer u uw Password Manager-gegevens naar een nieuwe computer overzet. Het wachtwoord van uw safe kan niet opnieuw worden ingesteld. Het is dus raadzaam regelmatig een back-up te maken van uw safegegevens. Wanneer u de automatische back-upfunctie inschakelt, worden er automatisch back-ups van uw safe gemaakt en lokaal opgeslagen op uw apparaat.

Wanneer uw product verloopt, kunt u de Password Manager-gegevens ophalen.

Opmerking: In Norton Password Manager is het exporteren van NPM-bestanden (Norton Password Manager) niet toegestaan.

Uw Norton Password Manager-gegevens exporteren via de browser

- 1 Open uw browser.
- 2 Klik in de rechterbovenhoek van de browser op **Norton Password Manager**.
- 3 Klik in het weergegeven pop-upvenster op **Safe openen**.
- 4 Typ het wachtwoord van uw safe in het venster **Uw safe ontgrendelen** en klik vervolgens op **Safe openen**.
- 5 Klik op het pictogram voor de Norton Password Manager-extensie en vervolgens op **Safe**.

- 6 Klik in het venster van Norton Password Manager op



en klik op **Safe exporteren**.

- 7 In het venster **Actie voor beschermde safe** voert u het wachtwoord van uw safe in om de Norton Password Manager-gegevens te exporteren.

Uw Norton Password Manager-gegevens exporteren via Norton

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik in het hoofdvenster van Norton op **Internetbeveiliging** en klik vervolgens op **Password Manager**.
- 3 Klik onder in het venster **Norton Password Manager** op het pictogram **Instellingen**.
- 4 Klik op de tab **Importeren/exporteren**.
- 5 Selecteer in het deelvenster **Exporteren** de bestandsindeling.
U kunt een van de volgende opties selecteren:
 - **Back-upindeling voor Password Manager – DAT-bestand**
Als u de back-up van uw gegevens extra wilt beveiligen met een wachtwoord, moet u het wachtwoord typen en bevestigen.
 - **Zonder opmaak – CSV-bestand (alleen aanmeldingen en opmerkingen)**
- 6 Klik op **Exporteren**.
U kunt de back-ups van uw safe oproepen via **My Documents\Norton Password Manager Backups\<Norton-accountnaam>**.
- 7 Voer in het venster **Wachtwoord voor Password Manager valideren** uw safewachtwoord in om uw Password Manager-gegevens te exporteren.
- 8 Klik op **OK** in het bevestigingsvenster.

Uw Norton Password Manager-gegevens Importeren

U kunt uw gegevens van Wachtwoordbeheer importeren uit het bestand waarvan u eerder een back-up heeft gemaakt. Er wordt alleen een automatische back-up van de safe gemaakt wanneer de betreffende functie is ingeschakeld. Standaardlocatie van map voor automatische back-up is C:\Documents\Norton Password Manager.

De opties **Bestaande gegevens samenvoegen met geïmporteerde gegevens** en **Bestaande gegevens vervangen door geïmporteerde gegevens** verschijnen wanneer u Norton Password Manager-gegevens vanuit een back-upbestand importeert. U kunt de geïmporteerde gegevens

samenvoegen met de safe waarbij u momenteel bent aangemeld, of de bestaande gegevens vervangen die in uw safe zijn opgeslagen

Opmerking: Wanneer u een bestand wilt importeren, mag dit niet groter zijn dan 15 MB voor CSV-bestanden. Bovendien staat Norton Password Manager het importeren van NPM-bestanden (Norton Password Manager) niet toe.

Uw Norton Password Manager-gegevens importeren via Norton

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik in het hoofdvenster van Norton op **Internetbeveiliging** en klik vervolgens op **Password Manager**.
- 3 Klik onder in het venster **Norton Password Manager** op het pictogram **Instellingen**.
- 4 Klik op de tab **Importeren/exporteren**.
- 5 Klik in de rij **Importeren** op **Importeren**.
- 6 Selecteer in het venster **Importeren in safe** een van de volgende opties:
 - **Bestaande gegevens samenvoegen met geïmporteerde gegevens**
 - **Bestaande gegevens vervangen door geïmporteerde gegevens**
- 7 Klik op **Importeren**.
- 8 Navigeer naar de locatie van het bestand dat u wilt importeren.
U kunt de back-ups van uw safe oproepen via **My Documents\Norton Password Manager Backups\<Norton-accountnaam>**.
- 9 Selecteer het bestand en klik op **Openen**.
- 10 Als u verschillende wachtwoorden heeft voor de aanmeldingen die u heeft opgeslagen in de safe die u momenteel gebruikt en de safe waarnaar u importeert, geeft Norton een bevestigingsbericht weer. Selecteer een van de volgende opties:
 - Klik op **Bestaand wachtwoord behouden** om het wachtwoord in de safe in de cloud te behouden.
 - Klik op **Geïmporteerd wachtwoord behouden** om het wachtwoord in de safe in de cloud te overschrijven met het wachtwoord van de safe waarnaar u importeert.
- 11 Klik op **OK** in het bevestigingsvenster.

De Norton Security-werkbalk in- of uitschakelen

Wanneer de Norton Security-werkbalk is ingeschakeld, geeft Norton Password Manager het pop-upvenster van Norton Safe Web en een beveiligingsclassificatie weer voor de websites die u bezoekt. Wanneer de werkbalk is uitgeschakeld, geeft Norton Password Manager het pop-upvenster Norton Safe Web niet weer, maar wordt u wel nog steeds gewaarschuwd over verdachte of frauduleuze websites.

De Norton Security-werkbalk in- of uitschakelen

- ◆ Open uw browser:
 - In Internet Explorer klikt u met de rechtermuisknop op de menubalk. Schakel de **Norton Security-werkbalk** in of uit en volg de instructies op het scherm.
 - Klik in Safari op **Weergave > Pas knoppenbalk aan**. Sleep vervolgens de extensies van de Norton Security-werkbalk die u wilt in- of uitschakelen.

Bescherm uw apparaat tegen misbruik, hackers en zero-day aanvallen.

Een zero-day-exploit is een techniek die een hacker gebruikt om van kwetsbaarheden in een programma te profiteren en schadelijke acties op uw computer uit te voeren. Behalve dat deze exploits uw computer vertragen of programma's laten vastlopen, kunnen deze exploits uw persoonlijke gegevens en vertrouwelijke informatie blootstellen aan hackers.

De functie Misbruikpreventie in uw Norton-product beschermt toepassingen en bestanden die kwetsbaar zijn voor misbruikpogingen. Misbruikpreventie van Norton is standaard ingeschakeld en blokkeert aanvallen op kwetsbare programma's door die programma's te sluiten. Norton stuurt de melding Aanval geblokkeerd wanneer een programma wordt afgesloten en geeft links naar informatie over de aanval.

Misbruikpreventie in- of uitschakelen

Opmerking: Wanneer **Misbruikpreventie** is uitgeschakeld, is uw computer kwetsbaar voor zero-day-exploits en andere vormen van misbruik.

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster Instellingen op **Misbruikpreventie**.
- 4 In de rij Misbruikpreventie zet u de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 5 Klik in het venster Instellingen op **Toepassen** en klik vervolgens op **Sluiten**.

Technieken voor misbruikpreventie

Norton gebruikt proactieve technieken voor misbruikpreventie om uw computer te beschermen tegen de nieuwste zero-day-aanvallen. U kunt technieken afzonderlijk in- of uitschakelen via het venster **Instellingen**. Standaard zijn alle technieken ingeschakeld.

Opmerking: Norton raadt aan om alle afzonderlijke technieken voor misbruikpreventie ingeschakeld te houden om u te beschermen tegen de meest uiteenlopende exploits.

Technieken voor misbruikpreventie omvatten:

- **Bescherming van Java-processen**
Voorkomt dat hackers op afstand schadelijke code gebruiken via Java-processen en staat alleen de uitvoering van vertrouwde Java-processen toe.
- **Structured Exception Handler Overwrite-bescherming**
Beschermt tegen exploits voor het afhandelen van gestructureerde uitzonderingen, die een toepassing in gevaar brengen door de pointer van een uitzonderingshandler te overschrijven met een door een aanvaller beheerd adres.
- **Stack Pivot-detectie**
Blokkeert exploitaanvallen waarbij de stackpointer wordt veranderd door een geheugen van de aanvaller om een ROP-aanvalscode (Return Oriented Programming) uit te voeren.
- **Handhaving van preventie van gegevensuitvoering**
Blokkeert aanvallers tegen het uitvoeren van schadelijke code vanuit het stack- of heap-geheugen van uw computer.
- **Handhaving van Memory Layout Randomization**
Dwingt dynamisch geladen toepassings-DLL's of modules af om altijd op willekeurige locaties te worden geladen ter bescherming tegen aanvallers.
- **Heap Spray-bescherming**
Beschermt vaak aangevallen geheugenlocaties waarbij exploits of aanvallers hun shellcode toewijzen met behulp van heap-spray-aanvalstechnieken.
- **Verbetering van Memory Layout Randomization**
Verbeterd het ASLR-gedrag (Address Space Layout Randomization) van het besturingssysteem bij het toewijzen van kritieke geheugenlocaties van de toepassing. Hierdoor zijn die geheugenlocaties minder voorspelbaar voor aanvallers.
- **Null Page-bescherming**
Wijst de null-geheugenlocatie van tevoren toe, wat helpt bij het voorkomen van aanvallen op null-pointer-dereference-kwetsbaarheden.
- **Remote DLL Injection-detectie**

Voorkomt dat hackers op afstand schadelijke uitvoerbare code invoegen via externe netwerken zoals openbare IP-adressen of domeinen.

- De technieken **Stack-uitvoerpreventie**, **Detectie van verdachte API-aanroepen** en **Heap Payload-detectie** beschermen uw computer tegen ROP-aanvallen (Return-Orienting Programming) die niet worden tegengehouden door de misbruikbeperkings technieken Address Space Layout Randomization en Preventie van gegevensuitvoering.

Norton Firewall in- of uitschakelen

De Slimme firewall controleert de communicatie tussen uw computer en de andere computers op internet. Daarnaast beveiligt de firewall uw computer tegen veelvoorkomende beveiligingsproblemen. Wanneer de Slimme firewall is uitgeschakeld, is uw computer niet tegen internetbedreigingen en beveiligingsrisico's beveiligd.

Als u Slimme firewall wilt uitschakelen, doet u dit alleen voor een bepaalde duur, waarna de firewall automatisch weer wordt ingeschakeld.

Norton Firewall in- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Zet in de rij **Slimme firewall** op het tabblad **Algemene instellingen** de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 5 Klik op **Toepassen**.
- 6 Indien u daarom wordt gevraagd, geeft u op na hoeveel tijd de firewallfunctie moet worden uitgeschakeld en klikt u op **OK**.

Norton Firewall uitschakelen of inschakelen vanuit het Windows-meldingsgebied

- 1 Rechtsklik op het Norton-pictogram in het meldingsgebied op de taakbalk, en klik vervolgens op **Slimme firewall uitschakelen** of **Slimme firewall inschakelen**.
- 2 Indien u daarom wordt gevraagd, geeft u op na hoeveel tijd de firewallfunctie moet worden uitgeschakeld en klikt u op **OK**.

Programmaregels aanpassen

Nadat u Norton een tijdje heeft gebruikt, moet u de toegangsinstellingen voor bepaalde programma's misschien aanpassen.

Programmaregels aanpassen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Op het tabblad **Programmabeheer** selecteert u in de kolom **Programma** het programma dat u wilt wijzigen.
- 5 In de vervolgkeuzelijst naast het programma dat u wilt wijzigen, selecteert u het gewenste toegangsniveau voor dit programma. U kunt kiezen uit:

Toestaan	Alle toegangspogingen van dit programma worden toegestaan.
Blokkeren	Alle toegangspogingen van dit programma worden geblokkeerd.
Aangepast	Maak de regels waarmee wordt bepaald hoe dit programma toegang tot internet krijgt.
- 6 Klik op **Toepassen**.

De volgorde van firewallregels wijzigen

Elke lijst met firewallregels wordt van boven naar beneden verwerkt. U kunt bepalen hoe deze regels worden verwerkt door de volgorde te wijzigen.

Opmerking: Wijzig de volgorde van de algemene verkeersregels niet, tenzij u een ervaren gebruiker bent. Wanneer u de volgorde van standaard verkeersregels wijzigt, kan dit de firewallfunctionaliteit beïnvloeden en de beveiliging van uw computer verminderen.

De volgorde van verkeersregels wijzigen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Selecteer op het tabblad **Verkeersregels** de regel die u wilt verplaatsen.
- 5 Voer een van de volgende handelingen uit:
 - Als u deze regel een positie vóór de regel erboven wilt verplaatsen, klikt u op **Omhoog**.

- Als u deze regel een positie na de regel eronder wilt verplaatsen, klikt u op **Omlaag**.
- 6 Wanneer u de gewenste regels heeft verplaatst, klikt u op **Toepassen**.

De volgorde van programmaregels wijzigen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Selecteer op het tabblad **Programmabeheer** het programma dat de regel bevat die u wilt verplaatsen.
- 5 Klik op **Wijzigen**.
- 6 Selecteer in het venster **Regels** de regel die u wilt verplaatsen.
- 7 Voer een van de volgende handelingen uit:
 - Als u deze regel een positie vóór de regel erboven wilt verplaatsen, klikt u op **Omhoog**.
 - Als u deze regel een positie na de regel eronder wilt verplaatsen, klikt u op **Omlaag**.
- 8 Wanneer u de gewenste regels heeft verplaatst, klikt u op **OK**.
- 9 Klik op **Toepassen** in het venster **Firewall**.

Een verkeersregel tijdelijk uitschakelen

U kunt een verkeersregel tijdelijk uitschakelen als u iemand specifieke toegang tot een computer of programma wilt verlenen. Vergeet niet deze regel weer in te schakelen wanneer u klaar bent met het programma of de computer waarvoor u deze wijziging moest doorvoeren.

Opmerking: Enkele standaard firewallregels in die lijst kunnen niet worden uitgeschakeld. U kunt de instellingen van deze regels alleen bekijken via de optie **Weergeven**.

Een verkeersregel tijdelijk uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Op het tabblad **Verkeersregels** heft u de selectie op van de regel die u wilt uitschakelen.
- 5 Klik op **Toepassen**.

Een geblokkeerd programma toestaan

Soms blokkeert de Slimme firewall de toegang tot internet voor bepaalde programma's. Dit kunnen soms bepaalde programma's zijn voor streaming media, netwerkgames of aangepaste zakelijke toepassingen die door uw werkgever worden geleverd. Als u zeker weet dat de internetactiviteiten van het programma geen beveiligingsrisico vormen, kunt u de blokkering van internettoegang voor het programma uitschakelen.

Een geblokkeerd programma toestaan

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Op het tabblad **Programmabeheer** selecteert u het programma waarvoor u internettoegang wilt toestaan.
- 5 Klik op **Toestaan** in de vervolgkeuzelijst **Toegang** voor de programma-ingang.
- 6 Klik op **Toepassen**.

Instellingen voor internettoegang worden standaard automatisch voor webprogramma's geconfigureerd door Norton Firewall. Dit gebeurt wanneer deze voor het eerst worden uitgevoerd. Wanneer een programma voor het eerst verbinding met internet probeert te maken, maakt Automatisch programmabeheer hier regels voor. Als u instellingen voor internettoegang van uw programma's wilt bepalen, kunt u Automatisch programmabeheer uitschakelen. Wanneer een programma voor het eerst internettoegang probeert te krijgen, verschijnt een waarschuwingsvenster waarin u wordt gevraagd toeganginstellingen te configureren.

Automatisch programmabeheer uitschakelen

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Klik in het venster **Firewall** op **Automatisch programmabeheer**.
- 5 In de rij **Automatisch programmabeheer** zet u de **Aan/Uit** -schakelaar op **Uit**.

Melding van firewallblokkering uitschakelen

Wanneer Automatisch programmabeheer ingeschakeld is, voorkomt Slimme firewall automatisch dat kwaadaardige toepassingen of toepassingen met een negatieve reputatie verbinding maken met internet of communiceren met andere computers in uw netwerk.

Norton stelt u op de hoogte wanneer Slimme firewall voorkomt dat een toepassing verbinding met het netwerk maakt. U kunt deze optie uitschakelen via **Geavanceerd programmabeheer** als u de melding niet wilt zien.

Melding van firewallblokkering uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Zet op het tabblad **Geavanceerd programmabeheer** de schakelaar **Melding firewallblokkering weergeven** op **Uit**.

Lijst met uitsluitingen voor Inbraakpreventie

Als u zeker weet dat een apparaat in uw netwerk veilig is, kunt u het vertrouwensniveau voor het apparaat op Volledig vertrouwd instellen. U kunt het vertrouwensniveau van een apparaat met behulp van Apparaatvertrouwen onder Netwerkinstellingen configureren. U kunt deze vertrouwde apparaten van de inbraakpreventiescan uitsluiten. Wanneer u volledig vertrouwde apparaten van de inbraakpreventiescan uitsluit, wordt de scantijd korter en de netwerksnelheid van uw computer verbeterd. Wanneer u een volledig vertrouwd apparaat uitsluit, wordt informatie die van dat apparaat wordt ontvangen, niet gescand. Volledig vertrouwde apparaten die van de inbraakpreventiescan zijn uitgesloten, worden aan de lijst met uitsluitingen voor Inbraakpreventie toegevoegd.

Merkt u dat een van de apparaten die u van de inbraakpreventiescan heeft uitgesloten, is geïnfecteerd, dan kunt u de opgeslagen lijst met uitsluitingen leegmaken. Wanneer u dit doet, verwijdert uw Norton-product alle door de inbraakpreventiescan uitgesloten apparaten van deze lijst.

U kunt de opgeslagen lijst met uitsluitingen in de volgende omstandigheden leegmaken:

- Een van de apparaten die u van inbraakpreventiescans heeft uitgesloten, is geïnfecteerd.
- Een van de apparaten die u van inbraakpreventiescans heeft uitgesloten, probeert de computer te infecteren.
- Uw thuisnetwerk is geïnfecteerd.

Hoe kan ik alle apparaten verwijderen van de inbraakpreventielijst met uitsluitingen?

Alle apparaten uit de lijst met uitgesloten items voor Inbraakpreventie verwijderen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster Instellingen op **Firewall**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Klik op **Leegmaken** in de rij Lijst met uitsluitingen onder Inbraakpreventie.
- 6 Klik op **Ja** in het bevestigingsvenster.
- 7 Klik in het venster Instellingen op **Sluiten**.

Browserbeveiliging inschakelen

Schadelijke websites detecteren en misbruiken zwakke punten in browsers om malware te downloaden. Wanneer u Browserbeveiliging inschakelt, blokkeert Norton malware voordat deze kan aanvallen. Het beschermt uw gevoelige gegevens en voorkomt dat aanvallers toegang kunnen krijgen tot uw computer.

Browserbeveiliging is standaard ingeschakeld. Houd Browserbeveiliging ingeschakeld om bescherming tegen schadelijke websites te waarborgen.

Opmerking: De functie Browserbeveiliging is beschikbaar voor de browsers Google Chrome, Microsoft Internet Explorer, Mozilla Firefox en Microsoft Edge.

Hoe kan ik Browserbeveiliging inschakelen?

De functie Browserbeveiliging is standaard ingeschakeld om uw browser tegen schadelijke websites te beschermen. Wanneer u de functie echter had uitgeschakeld, kunt u deze weer inschakelen.

Browserbeveiliging inschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster Instellingen op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 In de rij Browserbeveiliging zet u de **Aan/Uit** -schakelaar op **Aan**.

- 6 Klik op **Toepassen**.
- 7 Klik in het venster **Instellingen** op **Sluiten**.

Stel Norton Firewall in om waarschuwingen over blokkering van een aanval in of uit te schakelen

U kunt kiezen of u een waarschuwing wilt ontvangen wanneer Inbraakpreventie van Norton een verdachte aanval blokkeert.

Als u ervoor heeft gekozen geen waarschuwingen te ontvangen, kunt u nog steeds in uw beveiligingsgeschiedenis bekijken welke aanvallen Norton heeft geblokkeerd.

Waarschuwingen voor Inbraakpreventie in- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Onder **Inbraakpreventie**, in de rij **Meldingen**, zet u de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 6 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

Afzonderlijke waarschuwingen voor Inbraakpreventie in- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Klik op **Configureren** in de rij **Handtekeningen voor inbraakbeveiliging** onder **Inbraakpreventie**.
- 6 Schakel in het venster **Handtekeningen voor inbraak** de optie **Waarschuwen** in of uit voor de individuele handtekening.
- 7 Klik op **OK**.
- 8 Klik in het venster **Handtekeningen voor inbraak** op **Toepassen** en klik vervolgens op **OK**.
- 9 Klik in het venster **Instellingen** op **Sluiten**.

AutoBlock in- of uitschakelen

Norton AutoBlock stopt al het verkeer tussen een apparaat in uw netwerk en elke andere computer die probeert dat apparaat te misbruiken. Aangezien dit verkeer omvat dat mogelijk niet schadelijk is, stopt AutoBlock de verbinding slechts voor beperkte tijd nadat een bedreiging is gedetecteerd. Hier kunt u opgeven hoelang uw Norton-product de verbindingen van aanvallende computers moet blokkeren. Standaard wordt al het verkeer tussen uw computer en de aanvallende computer 30 minuten geblokkeerd.

Als u toegang wilt krijgen tot een of meer computers die door AutoBlock worden geblokkeerd, kunt u AutoBlock uitschakelen.

AutoBlock in- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Klik op **Configureren** in de rij **Beveiliging tegen inbreuk met AutoBlock** onder **Inbraakpreventie**.
- 6 In het venster **Beveiliging tegen inbreuk met AutoBlock** voert u onder **AutoBlock** een van de volgende handelingen uit:
 - Klik op **Uit** om Beveiliging tegen inbreuk met AutoBlock uit te schakelen.
 - Klik op **Aan (aanbevolen)** om Beveiliging tegen inbreuk met AutoBlock in te schakelen. Selecteer vervolgens in de vervolgkeuzelijst **AutoBlock aanvallende computers voor** hoelang automatische blokkering ingeschakeld moet blijven.
- 7 Klik in het venster **Beveiliging tegen inbreuk met AutoBlock** op **OK**.
- 8 Klik in het venster **Instellingen** op **Sluiten**.

De blokkering opheffen van computers die door AutoBlock zijn geblokkeerd

Als Norton Firewall netwerkverkeer stopt op een computer waarvan u weet dat deze veilig is, kunt u de verbindingen met de computer herstellen door deze te verwijderen uit de AutoBlock-lijst in de Norton Firewall-instellingen.

De blokkering opheffen van computers die door AutoBlock zijn geblokkeerd

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Klik op **Configureren** in de rij **Beveiliging tegen inbreuk met AutoBlock** onder **Inbraakpreventie**.
- 6 Selecteer het IP-adres van de computer in het venster **Beveiliging tegen inbreuk met AutoBlock** onder **Computers die momenteel door AutoBlock worden geblokkeerd**.
- 7 Selecteer onder de kolom **Actie** de optie **Blokkering opheffen** in de vervolgkeuzelijst.
- 8 Klik in het venster **Beveiliging tegen inbreuk met AutoBlock** op **OK**.
- 9 Klik in het venster **Instellingen** op **Sluiten**.

Een apparaat toevoegen aan Apparaatvertrouwen

U kunt handmatig een apparaat aan Apparaatvertrouwen toevoegen. U kunt een apparaat toevoegen door het volgende op te geven:

- De naam of beschrijving van het apparaat
- Het IP-adres of fysieke adres van het apparaat

Opmerking: Als u een apparaat vertrouwt dat zich niet in uw netwerk bevindt, kunt u uw computer aan potentiële beveiligingsrisico's blootstellen.

Een apparaat toevoegen aan Apparaatvertrouwen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Op het tabblad **Algemene instellingen** in de rij **Apparaatvertrouwen** klikt u op **Configureren**.
- 5 Klik in het venster **Apparaatvertrouwen** op **Toevoegen**.

- 6 Typ in het vak **Naam** van het venster **Apparaat toevoegen** de naam van het apparaat dat u aan uw netwerk wilt toevoegen.
De apparaatnaam mag niet meer dan 15 tekens bevatten.
- 7 Typ in het tekstvak **IP-adres of fysiek adres** het IP-adres of fysieke adres van het apparaat dat u aan Apparaatvertrouwen wilt toevoegen.

U kunt de volgende indelingen gebruiken in het tekstvak **IP-adres of fysiek adres** :

IPv4-adres	172.16.0.0
IPv6-adres	fe80::12ac:fe44:192a:14cc
Fysiek adres	11-22-c3-5a-fe-a4
Herleidbare host	ftp.myfiles.com

Het adres wordt pas geverifieerd wanneer het apparaat fysiek op het netwerk wordt gevonden.

- 8 Selecteer een optie in de vervolgkeuzelijst **Vertrouwensniveau**. U kunt kiezen uit:

Volledig vertrouwd

Hiermee wordt een apparaat aan de lijst Volledig vertrouwd toegevoegd.

Apparaten met dit vertrouwensniveau worden alleen op bekende aanvallen en infecties gecontroleerd. Selecteer deze instelling alleen wanneer u zeker weet dat het apparaat helemaal veilig is.

Beperkt

Hiermee wordt een apparaat aan de lijst Beperkt toegevoegd.

Beperkte apparaten hebben geen toegang tot uw computer.

- 9 Zet een vinkje bij **Uitsluiten van Inbraakpreventie-scans** als u het apparaat wilt uitsluiten van Inbraakpreventie-scans.

- 10 Klik op **Apparaat toevoegen**.

Downloadinformatie in- of uitschakelen

Downloadinformatie beschermt uw computer tegen onveilige bestanden die u op uw computer kunt uitvoeren nadat u deze heeft gedownload met een ondersteunde browser. De optie **Downloadinformatie** is standaard ingeschakeld. In dit geval verschaft Downloadinformatie informatie over het reputatieniveau van alle uitvoerbare bestanden die u downloadt. De door

Downloadinformatie verstrekte reputatiedetails geven aan of het gedownloade bestand veilig kan worden geïnstalleerd.

Het kan voorkomen dat u Downloadinformatie moet uitschakelen. U wilt een onveilig bestand misschien downloaden. In dat geval moet u Downloadinformatie uitschakelen, zodat u het bestand kunt downloaden zonder dat het door uw Norton-product van uw computer wordt verwijderd.

U kunt de optie **Downloadinformatie** gebruiken om Downloadinformatie in of uit te schakelen.

Downloadinformatie in- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 In de rij **Downloadinformatie** zet u de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 6 Klik op **Toepassen**.
- 7 Indien u daarom wordt gevraagd, geeft u op na hoeveel tijd de functie Downloadinformatie moet worden uitgeschakeld en klikt u op **OK**.
- 8 Klik in het venster **Instellingen** op **Sluiten**.

Filteren van spam in- of uitschakelen

Met het toenemende gebruik van e-mail ontvangen veel gebruikers grote hoeveelheden ongewenste en ongevraagde commerciële e-mailberichten, ook wel spam genoemd. Spam maakt het niet alleen moeilijk legitieme e-mailberichten te identificeren, sommige spamberichten bevatten bovendien stuitende teksten en afbeeldingen.

U kunt filteren op spam om deze spammails in de hand te houden. Spambeveiliging blijft standaard actief. Mocht u deze beveiliging willen uitschakelen, dan kunt u dit vanuit het programma zelf doen.

Opmerking: Wanneer u Norton AntiSpam uitschakelt, verhoogt u de kans op ongewenste e-mailberichten.

Filteren van spam in- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.

- 3 Klik in het venster **Instellingen** op **AntiSpam**.
- 4 Zet op het tabblad **Filter** in de rij **AntiSpam** de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 5 Als u filteren van spam wilt uitschakelen, doet u het volgende:
 - Selecteer in het venster **Beveiligingsverzoek** in de vervolgkeuzelijst **Selecteer de duur** hoelang u filteren van spam wilt uitschakelen.
- 6 Klik op **Toepassen**.
- 7 Klik op **OK**.
- 8 Klik in het venster **Instellingen** op **Sluiten**.

Internetgebruik definiëren voor Norton

Met **Beperken van netwerkgebruik** kunt u bepalen hoeveel bandbreedte Norton gebruikt. Beperken van netwerkgebruik is standaard ingeschakeld en ingesteld op Automatisch. In Windows 7 of eerder is de standaardinstelling **Geen limiet**. Als u een trage internetverbinding heeft, kunt u de bandbreedte die Norton gebruikt, verlagen. U kunt ook het communicatiebeleid instellen voor alle netwerkverbindingen die door uw computer worden gebruikt, door de instellingen van Beperken van netwerkgebruik te wijzigen.

Internetgebruik definiëren voor Norton

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Op het tabblad **Algemene instellingen** in de rij **Beperken van netwerkgebruik** klikt u op **Configureren**. Als de optie **Configureren** is uitgeschakeld, zet u de schakelaar **Aan/Uit** op **Aan**.
- 5 Klik in het venster met instellingen voor **Beperken van netwerkgebruik** onder de kolom **Beleid** op de vervolgkeuzelijst naast de netwerkverbinding waarvoor u een beleid wilt instellen.
- 6 Selecteer een van de volgende opties:
 - **Auto** Met behulp van deze optie kan Norton het beleid voor het observeren van kosten van Windows gebruiken om alle updates van virusdefinities en producten te ontvangen.

Opmerking: De optie Automatisch is alleen beschikbaar in Windows 8 of later.

- **Geen limiet** Hiermee kan uw Norton-product de netwerkbandbreedte gebruiken die nodig is om alle product- en virusdefinitie-updates te ontvangen. Als u Windows 7 of eerder gebruikt, is het standaardbeleid ingesteld op **Geen limiet**.
 - **Beperkt** Hiermee krijgt Norton alleen toegang tot internet om essentiële productupdates en virusdefinities te ontvangen. Als u een beperkte internetverbinding heeft, kunt u de optie **Beperkt** selecteren om te zorgen dat u tegen de belangrijkste beveiligingsbedreigingen wordt beschermd.
 - **Geen verkeer** Hiermee kunt u voorkomen dat door Norton verbinding met internet wordt gemaakt. Als u dit beleid kiest, kan Norton geen essentiële virusdefinities en programma-updates ontvangen, wat tot potentiële internetgevaren en virusaanvallen kan leiden.
- 7 Klik op **Toepassen** en vervolgens op **OK**.
 - 8 Klik in het venster **Instellingen** op **Sluiten**.

Beperken van netwerkgebruik in- of uitschakelen

U kunt beleidsregels instellen om het internetgebruik van Norton te beperken. Als u het internetgebruik van uw Norton-product niet wilt beperken, kunt u **Beperken van netwerkgebruik** uitschakelen.

Als u vindt dat Norton te veel netwerkbandbreedte gebruikt, kunt u **Beperken van netwerkgebruik** inschakelen. Vervolgens kunt u beleidsregels instellen om het internetgebruik van Norton te beperken. Norton maakt verbinding met internet op basis van het beleid dat u instelt in het venster **Beperken van netwerkgebruik**. **Beperken van netwerkgebruik** is standaard ingeschakeld.

Beperken van netwerkgebruik in- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
Klik op **Netwerk** als u Norton AntiVirus heeft.
- 4 Zet op het tabblad **Algemene instellingen** in de rij **Beperken van netwerkgebruik** de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 5 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

Norton instellen om toezicht te houden op toepassingen en schadelijke websites te blokkeren op uw computer

Enkele schadelijke websites kunnen proberen ongeautoriseerde toegang te krijgen tot uw apparaatgegevens wanneer u freeware- of sharewaretoepassingen installeert en opent. Schadelijke websites detecteren en exploiteren kwetsbaarheden om malware te downloaden, zoals malware voor **crypto mining**, waarmee uw apparaatgegevens aan cybercriminelen kunnen worden onthuld.

Als **Toezicht op app-URL's** is ingeschakeld, controleert Norton alle toepassingen die op uw computer zijn geïnstalleerd en worden schadelijke websites geblokkeerd zodat ze geen toegang krijgen tot uw computer. Norton waarschuwt u wanneer een schadelijke website wordt geblokkeerd en u kunt de informatie over de aanval in het venster Beveiligingsgeschiedenis bekijken.

Opmerking: Browsertoepassingen worden niet door **Toezicht op app-URL's** gecontroleerd. U moet Norton-browserextensies toevoegen om uw browsertoepassing tegen schadelijke websites te beschermen.

Toezicht op app-URL's inschakelen om schadelijke websites te blokkeren

Toezicht op app-URL's is standaard ingeschakeld. Houd Toezicht op app-URL's ingeschakeld om bescherming tegen schadelijke websites te waarborgen.

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster Instellingen op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Onder **Inbraakpreventie**, in de rij **Toezicht op app-URL's**, zet u de Aan/Uit-schakelaar op Aan.

Een URL of domein uitsluiten van toezicht

Inbraakpreventie maakt gebruik van een uitgebreide lijst met aanvalshandtekeningen om schadelijke websites te detecteren en blokkeren. In sommige gevallen kunnen goedaardige websites als verdacht worden geïdentificeerd, omdat ze een vergelijkbare aanvalshandtekening hebben. Als u meldingen over een mogelijke aanval ontvangt en weet dat de websites of

domeinen die deze meldingen activeren veilig zijn, dan kunt u de handtekening van toezicht uitsluiten.

Meldingen voor een URL of domein uitschakelen

- 1 Klik in de waarschuwing melding op **Details weergeven**.
- 2 Klik op **Blokkering van URL opheffen** in het venster **Beveiligingsgeschiedenis - Geavanceerde details**.

Een URL of domein uitsluiten met uw Norton

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Klik op **Configureren** in de rij **Uitsluitingen van Toezicht op app-URL's** onder **Inbraakpreventie**.
- 6 Klik op de knop **Toevoegen** en voer de URL of de domeinnaam in die u van toezicht wilt uitsluiten.
- 7 Als u een URL of domein wilt bewerken of verwijderen, doet u het volgende:
 - Selecteer een URL of domein in de lijst en klik op de knop **Bewerken**. Wijzig de URL of de domeinnaam.
 - Selecteer de URL die of het domein dat u wilt verwijderen en klik op de knop **Verwijderen**.

Informatie over de geblokkeerde URL weergeven

Informatie in de waarschuwing melding weergeven

- 1 Klik in de waarschuwing melding op **Details weergeven**.
- 2 In het venster **Beveiligingsgeschiedenis - Geavanceerde details** kunt u meer informatie bekijken over de geblokkeerde URL.

Informatie weergeven met behulp van het venster Beveiligingsgeschiedenis

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het hoofdvenster van het Norton-product. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** in de keuzelijst **Weergeven** de optie **Inbraakpreventie**.

- 4 Klik op een rij om de details voor dat item te bekijken.
- 5 Dubbelklik op een rij of klik op **Meer opties** om de Geavanceerde details van beveiligingsgeschiedenis te openen. Hier vindt u meer informatie over de activiteit en kunt u indien nodig actie ondernemen.

Aan de slag met Norton Cloudback-up

Met Cloudback-up slaat u belangrijke bestanden en documenten op als preventieve maatregel tegen gegevensverlies als gevolg van een defecte vaste schijf, gestolen apparaten en zelfs ransomware.

Opmerking: Norton Cloudback-up is alleen beschikbaar op Windows.

Voordat u Norton Cloudback-up uitvoert, maakt u een back-upset waarmee u opgeeft van welke bestanden u een back-up wilt maken. U kunt ook opgeven waar en wanneer de back-up van de bestanden moet worden gemaakt. U kunt een back-up van uw bestanden naar de cloud maken via Norton Cloudback-up, of naar uw eigen externe stations.

Opmerking: De eerste keer dat u een back-up uitvoert, kan het even duren voordat alle bestanden op uw computer door Norton zijn gecontroleerd en gekopieerd. Dit proces kan nog langer duren als u een trage internetverbinding heeft.

Een back-upset maken

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van Norton. Klik vervolgens op **Back-upsets**.
- 3 Klik op het tabblad **Overzicht** onder **Dingen die u kunt doen** op **Nieuwe back-upset maken**.
In het venster dat verschijnt, typt u een naam voor uw Back-upset en vervolgens klikt u op **OK**.
- 4 Selecteer op het tabblad **Wat** onder **Bestandstypen** een of meer bestandscategorieën.
- 5 Klik in het venster **Back-upsets beheren** op **Instellingen opslaan**.
- 6 Selecteer een back-uplocatie op het tabblad **Waar** in de kolom **Doel**.
Als u Secure Cloud Storage heeft gekozen, klikt u op de link en volgt u de instructies om u bij uw Norton-account aan te melden en online back-up te activeren.

Met de instelling Bandbreedtebeperking kunt u de internetbandbreedte configureren die Norton gebruikt om een back-up van uw bestanden naar online opslag te maken. U kunt kiezen voor een van de volgende niveaus voor bandbreedtebeperking:

- **Snelste (aanbevolen)**
- **Intensief gebruik**
- **Gemiddeld gebruik**
- **Weinig gebruik**

Opmerking: Wanneer u de aanbevolen instelling selecteert, wordt voor het maken van back-ups de volledige internetbandbreedte benut, zodat andere internetactiviteiten langzamer gaan.

- 7 Kies in de lijst **Schema** op het tabblad **Wanneer** het back-upschema dat het beste aan uw behoeften voldoet.

Norton Cloudback-up uitvoeren

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van het Norton-product. Klik vervolgens op **Back-up uitvoeren**.
- 3 Volg de instructies op het scherm in het venster **Back-up uitvoeren**.
- 4 Klik op **Sluiten**.

Opmerking: Als de back-up niet kan worden voltooid, biedt Norton mogelijke oorzaken zoals onvoldoende opslagcapaciteit of snelheidsbeperkingen. Controleer steeds of u met het internet bent verbonden wanneer u een back-up uitvoert, en dat opslagapparaten verbonden en ingeschakeld zijn.

Bestanden en mappen toevoegen aan of uitsluiten van uw back-upsets

Met Norton kunt u in uw back-upsets back-ups zetten van verschillende bestandstypen, zoals foto-, muziek- of videobestanden. U kunt bestanden of mappen specificeren die bestandstypen bevatten die normaal in uw back-upsets worden opgenomen en deze uitsluiten van back-ups. U kunt ook bestandsextensies toevoegen of verwijderen die normaal deel uitmaken van de standaardbestandstypen.

Bestanden en mappen toevoegen aan of uitsluiten van uw back-upset

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van Norton. Klik vervolgens op **Back-upsets**.
- 3 Selecteer de back-upset die u wilt configureren op het tabblad **Overzicht** in het venster **Back-upsets beheren**.
- 4 Ga naar het tabblad **Wat** en vink **Bestandstype bewerken** aan om de extensies in bestandstypen voor afbeeldingen, muziek, video en andere bestandstypen te wijzigen.
- 5 Klik onder **Bestandstypen** op **Configureren** naast een bestandstype. In het venster dat verschijnt, voert u een van de volgende handelingen uit:
 - Selecteer extensies in de lijst om ze uit het bestandstype te verwijderen.
 - Klik op **Nieuwe toevoegen** om extra extensies aan de lijst toe te voegen.
 - Klik op **Opslaan**.
- 6 Klik op **Bestanden en mappen toevoegen of uitsluiten** op het tabblad **Wat**. In het venster dat verschijnt, voert u een van de volgende handelingen uit:
 - Klik op **Bestand opnemen** of **Bestand uitsluiten**. Ga in het venster **Zoeken naar bestanden** naar een bestand om toe te voegen of te verwijderen en klik op **Openen**.
 - Klik op **Map opnemen** of **Map uitsluiten**. Ga in het venster **Zoeken naar mappen** naar een bestand om toe te voegen of te verwijderen en klik op **OK**.
- 7 Klik in het venster **Back-upsets beheren** op **Instellingen opslaan**.

Bestanden en mappen toevoegen aan of uitsluiten van een back-upset in Windows Verkenner

- 1 Klik met de rechtermuisknop in Windows Verkenner op de map of het bestand, selecteer **Norton Security** en navigeer naar **Aan back-up toevoegen / Van back-up uitsluiten**.
De optie **Aan back-up toevoegen / Van back-up uitsluiten** in het snelmenu wordt pas ingeschakeld nadat u uw back-up heeft geconfigureerd en wanneer de vensters **Back-upsets beheren** en **Bestanden herstellen** zijn gesloten.
- 2 Klik op de back-upset met het bestand dat of de map die u wilt uitsluiten.

Foto's, muziek of andere belangrijke bestanden herstellen uit Norton-back-upsets

U kunt uw Norton Back-upgegevens gemakkelijk herstellen als u het slachtoffer wordt van ransomware of andere malware, of als u met onherstelbare hardwareproblemen te maken krijgt. U kunt volledige back-upsets of specifieke bestanden in een back-upset herstellen. U kunt ook bepalen waar de back-upbestanden moeten worden hersteld.

Norton-back-upbestanden of volledige back-upsets herstellen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van Norton. Klik vervolgens op **Bestanden herstellen**.
- 3 In het venster **Bestanden herstellen** klikt u onder **Herstellen vanaf** op **Alles weergeven**.
Klik op een back-upset en klik vervolgens op **OK**.
- 4 In het venster **Bestanden herstellen** onder **Bestanden** klikt u op **Naar bestanden en mappen bladeren**.
Selecteer de bestanden die u wilt herstellen en klik op **OK**.
- 5 In het venster **Bestanden herstellen** klikt u onder **Herstellen naar** op **Oorspronkelijke locatie**.
Klik op **Locatie wijzigen** en volg de instructies als u niet naar de oorspronkelijke locatie wilt herstellen.
- 6 Klik op **Bestanden herstellen** en vervolgens op **Sluiten**.

Norton Backup inschakelen

Wanneer de optie **Back-up** is ingeschakeld, maakt uw Norton-product automatisch een back-up van uw bestand wanneer uw computer niet actief is. Mocht u het programma tijdelijk willen uitschakelen, dan kunt u dit vanuit het programma zelf doen.

Wanneer u de back-up uitschakelt, verandert de back-upstatus in het hoofdvenster van het Norton-product van **Beschermd** in **Uitgeschakeld**. In de status **Uitgeschakeld** schakelt uw Norton-product alle automatische back-ups van bestanden uit. U kunt de optie **Back-up uitvoeren** in het hoofdvenster gebruiken als u een back-up wilt maken van de bestanden uit alle back-upsets.

U kunt Back-up in- of uitschakelen vanuit het venster **Instellingen**, vanuit het venster **Back-upinstellingen** of vanuit het venster **Details van back-up**. Dit gaat als volgt:

Back-up in- of uitschakelen vanuit het venster Instellingen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Onder **Snelle besturingselementen** in het venster **Instellingen** kunt u het volgende doen:
 - Schakel het selectievakje **Back-up** uit als u Back-up wilt uitschakelen.

- Schakel het selectievakje **Back-up** in als u Back-up wilt inschakelen.

Back-up in- of uitschakelen vanuit het venster Back-upinstellingen van Norton

1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

2 Klik in het hoofdvenster van Norton op **Instellingen**.

3 Klik in het venster **Instellingen** op **Back-upinstellingen**.

4 In het venster **Back-upinstellingen** voert u een van de volgende handelingen uit:

- Als u back-up wilt uitschakelen, zet u de **Aan/Uit** -schakelaar op **Uit**.
- Als u back-up wilt inschakelen, zet u de **Aan/Uit** -schakelaar op **Aan**.

5 Klik in het venster **Instellingen** op **Toepassen**.

Back-up in- of uitschakelen vanuit het venster Details van back-up

1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

2 Klik in het hoofdvenster van Norton op **Back-up** en vervolgens op **Details weergeven**.

3 Onder **Dingen die u kunt doen** in het venster **Details van back-up** voert u een van de volgende handelingen uit:

- Klik op **Back-up uitschakelen** als u Back-up wilt uitschakelen.
- Klik op **Back-up inschakelen** als u Back-up wilt inschakelen.

De instellingen van uw Norton-product aanpassen

In het venster **Instellingen** kunt u de volgende services voor **Snelle besturingselementen** in- of uitschakelen:

- **Stille modus**
- **Back-up**
- **Overlays van back-upstatus**
- **Automatische LiveUpdate**
- **Slimme firewall**
- **Norton Tamper Protection**

Het is raadzaam alle services behalve Stille modus ingeschakeld te laten.

Snelle besturingselementen in- of uitschakelen

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik in het hoofdvenster van Norton op **Instellingen**.

- 3 Onder **Snelle besturingselementen** in het venster **Instellingen** kunt u het volgende doen:

- Als u een service wilt inschakelen, schakelt u het bijbehorende selectievakje in.
- Als u een service wilt uitschakelen, schakelt u het bijbehorende selectievakje uit. Als een waarschuwing of bericht verschijnt, selecteert u de duur in het vervolgkeuzemenu en klikt u vervolgens op **OK**.

Instellingen voor Realtimebeveiliging aanpassen

Realtimebeveiliging detecteert onbekende beveiligingsrisico's op uw computer en laat u bepalen welke actie moet worden ondernomen wanneer u een risico vindt.

Opmerking: Voor de meeste gebruikers worden standaardinstellingen aanbevolen. Als u een functie tijdelijk wilt uitschakelen, moet u hem zo snel mogelijk weer inschakelen. Als u wilt dat items met een laag risico automatisch worden verwijderd, configureert u de Geavanceerde modus van SONAR. Auto-Protect controleert op virussen en andere beveiligingsrisico's telkens wanneer u programma's op uw computer uitvoert. Zorg dat Auto-Protect altijd ingeschakeld is.

Auto-Protect instellen om verwisselbare media te scannen

Scan van verwisselbare media controleert op virussen wanneer u verwisselbare media gebruikt en wordt in enkele seconden voltooid. Zijn de verwisselbare media eenmaal gescand, dan worden ze pas weer gescand wanneer ze opnieuw worden geplaatst of geformatteerd. Als u nog steeds denkt dat uw verwisselbare media is geïnfecteerd, schakelt u Auto-Protect in, plaatst u de verwisselbare media en opent u het in Windows Verkenner zodat Auto-Protect het opnieuw kan scannen. U kunt de verwisselbare media ook handmatig scannen.

Instellingen voor Automatische bescherming aanpassen

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik in het hoofdvenster van Norton op **Instellingen**.

- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Zet onder **Scan van verwisselbare media** de schuifregelaar op **Aan**.

SONAR instellen om bedreigingen automatisch te verwijderen

Symantec Online Network for Advanced Response (SONAR) biedt realtimebeveiliging tegen bedreigingen en detecteert proactief onbekende beveiligingsrisico's op uw computer. SONAR identificeert nieuwe bedreigingen op basis van het gedrag van toepassingen. U kunt opgeven hoe SONAR een bedreiging verwijdert via de instellingen van de Geavanceerde modus van SONAR.

SONAR instellen om bedreigingen automatisch te verwijderen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Zet onder **Risico's automatisch verwijderen** de schuifregelaar op **Altijd**.
- 5 Zet onder **Risico's verwijderen als ik weg ben** de schuifregelaar op **Altijd**.
- 6 Klik op **Toepassen**.

Auto-Protect instellen om bekende goede bestanden uit te sluiten van Norton-scans

Als u vindt dat een legitieme toepassing ten onrechte als een beveiligingsrisico is aangemerkt door Norton, kunt u het bestand uitsluiten van Norton-scans.

Bestanden van Norton-scans uitsluiten

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik op de tab **Scans en risico's** in het instellingenvenster voor AntiVirus.
- 5 Voer onder **Uitsluitingen/Lage risico's** een van de volgende handelingen uit:
 - Klik in de rij **Items uitsluiten van scans** op **Configureren**.
 - Klik in de rij **Items die van Auto-Protect-, SONAR- en downloadinformatiedetectie moeten worden uitgesloten** op **Configureren**.
- 6 Klik in het weergegeven venster op **Mappen toevoegen** of **Bestanden toevoegen**.

- 7 Klik op het bladerpictogram in het dialoogvenster **Item toevoegen**. In het dialoogvenster dat wordt geopend, selecteert u het item dat u van de scan wilt uitsluiten.
- 8 Klik op **OK**.

Instellingen voor scans en risico's

Via de instellingen voor **Scans en risico's** kunt u de scans aanpassen die door Norton op uw computer worden uitgevoerd. U kunt een scan configureren aan de hand van de digitale handtekening en het vertrouwensniveau van de bestanden op uw computer. U kunt opgeven wat moet worden gedaan tijdens het scannen van e-mailberichten.

U kunt de volgende instellingen voor **Scans en risico's** gebruiken:

Computerscans

U kunt verschillende typen scans uitvoeren om virusinfecties op uw computer te detecteren en voorkomen. Dit zijn Snelle scan, Volledige systeemscan en Aangepaste scan. U kunt de verschillende opties van **Computerscans** gebruiken om de scans te verbeteren die door Norton op uw computer worden uitgevoerd. U kunt ook aangeven dat u gecomprimeerde bestanden wilt scannen.

Via de opties voor **Computerscans** kunt u ook instellen dat scans rootkits, andere onzichtbare items, tracking-cookies en onbekende beveiligingsbedreigingen scannen. U kunt kiezen uit:

- **Scan van gecomprimeerde bestanden**
Met deze optie scant en herstelt u de bestanden in gecomprimeerde bestanden. Wanneer u deze functie inschakelt, worden virussen en andere beveiligingsrisico's in de bestanden in de gecomprimeerde bestanden gescand en gedetecteerd, en worden de gecomprimeerde bestanden verwijderd.
- **Scan van rootkits en onzichtbare items**
Hiermee kunt u op rootkits en andere beveiligingsrisico's scannen die misschien op uw computer zijn verborgen.
- **Scan van netwerkstations**
Hiermee worden de netwerkstations gescand die op uw computer zijn aangesloten. Norton voert een **Scan van netwerkstations** uit tijdens een **Volledige systeemscan** en **Aangepaste scan**. De optie **Scan van netwerkstations** is standaard ingeschakeld. Als u de optie uitschakelt, worden netwerkstations niet gescand.
- **Heuristische beveiliging**
Hiermee wordt uw computer gescand om deze tegen onbekende beveiligingsbedreigingen te beschermen.
Norton maakt gebruik van heuristische technologie om verdachte eigenschappen van een bestand te controleren zodat het als geïnfecteerd kan worden gecategoriseerd. De technologie vergelijkt de eigenschappen van een bestand met die van een bekend

geïnfecteerd bestand. Als voldoende verdachte eigenschappen worden gevonden, identificeert Norton het bestand als geïnfecteerd met een bedreiging.

- **Scan van trackingcookies**

Hiermee kunt u op kleine bestanden scannen die door programma's op uw computer kunnen worden geplaatst om uw computeractiviteiten te volgen.

- **Volledige systeemscaan**

Met een volledige systeemscaan wordt de volledige computer uitgebreid gescand op virussen, spyware en andere beveiligingskwetsbaarheden. Met de optie **Configureren** kunt u de volledige systeemscaan plannen.

Beveiligde poorten

Met de instellingen voor deze optie kunt u de POP3- en SMTP-poorten van uw e-mailprogramma beveiligen.

U kunt deze optie gebruiken om uw POP3- en SMTP-e-mailpoorten handmatig te configureren voor e-mailbeveiliging. Als de SMTP- en POP3-poortnummers die u van uw internetaanbieder heeft ontvangen voor uw e-mailprogramma afwijken van de standaard SMTP- en POP3-poortnummers, moet u Norton configureren om de poorten te beveiligen.

Antivirusscan voor e-mails

Antivirusscan voor e-mails beveiligt u tegen de bedreigingen die via e-mailbijlagen worden verzonden of ontvangen.

Met de opties van Antivirusscan voor e-mails kunt u bepalen wat Norton moet doen tijdens het scannen van e-mailberichten. Norton scant automatisch de e-mailberichten die u verzendt of ontvangt aan de hand van de opties die u kiest.

Uitsluitingen/Lage risico's

Met uitsluitingsopties geeft u de items zoals mappen, bestanden en stations op die u van Norton-scans uitsluit. Scanhandtekeningen en items met laag risico zijn enkele items die u van scans kunt uitsluiten.

Met behulp van uitsluitingsopties kunt u ook kiezen welke risicocategorieën Norton moet detecteren. U kunt kiezen uit:

- **Lage risico's**

Hiermee kunt u de items met een laag risico beheren die op uw computer zijn gevonden. U kunt instellen hoe Norton op items met een laag risico moet reageren.

- **Items uitsluiten van scans**

Hiermee bepaalt u welke schijven, mappen of bestanden moeten worden uitgesloten van risicoscans.

U kunt nieuwe uitsluitingsitems toevoegen of de toegevoegde items bewerken in de lijst met uitgesloten items. U kunt items ook uit de lijst met uitgesloten items verwijderen.

- **Items die van Auto-Protect-, SONAR- en downloadinformatiedetectie moeten worden uitgesloten**

Hiermee bepaalt u welke schijven, mappen of bestanden moeten worden uitgesloten van Auto-Protect-scans en SONAR-scans.

U kunt nieuwe items die moeten worden uitgesloten, toevoegen of de items die u al heeft uitgesloten, aanpassen. U kunt items ook uit de lijst met uitgesloten items verwijderen.

- **Handtekeningen die van alle detecties worden uitgesloten**

Via Uitsluitingen van handtekeningen kunt u bekende risico's op naam selecteren en een risiconaaam uit de lijst met uitgesloten items verwijderen.

U kunt ook de risicogevolgen bekijken op basis van de impact op prestaties, privacy, verwijdering en onzichtbaarheid.

- **Bestands-id's wissen die van scans worden uitgesloten**

Hiermee kunt u de reputatiegegevens van bestanden die van scans zijn uitgesloten, verwijderen.

U kunt de optie **Alles wissen** gebruiken om de reputatiegegevens van de bestanden die van scans zijn uitgesloten, te wissen.

Opmerking: Uitsluitingen verlagen uw beveiligingsniveau. Gebruik ze alleen als u ze specifiek nodig heeft.

Instellingen van Inbraakpreventie en browserbeveiliging

Inbraakpreventie scant alle netwerkcommunicatie van en naar uw computer en vergelijkt deze informatie met een verzameling aanvalshandtekeningen. Dit zijn gegevens aan de hand waarvan aanvalspogingen kunnen worden geïdentificeerd van aanvallers die bekende zwaktes in programma's of besturingssystemen uitbuiten. Inbraakpreventie beveiligt uw computer tegen de meeste internetaanvallen.

Als de informatie overeenkomt met een aanvalshandtekening, wordt het pakket automatisch door Inbraakpreventie verwijderd en wordt de verbinding verbroken met de computer waarvan de gegevens afkomstig zijn. Op die manier is uw computer volledig beveiligd.

Inbraakpreventie maakt gebruik van een uitgebreide lijst met aanvalshandtekeningen om verdachte netwerkactiviteiten te detecteren en te blokkeren. Het Norton-product voert LiveUpdate automatisch uit zodat uw lijst met aanvalshandtekeningen actueel blijft. Als u Automatische LiveUpdate niet gebruikt, dient u LiveUpdate eenmaal per week uit te voeren.

Het Norton-product biedt ook de functie Browserbeveiliging om uw browser tegen schadelijke programma's te beschermen.

Opmerking: De functie Browserbeveiliging is beschikbaar voor de browsers Google Chrome, Microsoft Internet Explorer, Mozilla Firefox en Microsoft Edge.

Internet wordt steeds intensiever gebruikt, waardoor uw webbrowser kwetsbaarder wordt voor aanvallen door kwaadaardige websites. Deze websites detecteren de zwakke plek in uw webbrowser en maken hier misbruik van door zonder uw toestemming of medeweten malwareprogramma's op uw systeem te downloaden. Deze malwareprogramma's worden ook wel 'drive-by downloads' genoemd. Het Norton-product beveiligt uw browser tegen 'drive-by downloads' van schadelijke websites.

De instellingen voor **Inbraak- en browserbeveiliging** bevatten ook de optie **Downloadinformatie** om uw computer te beveiligen tegen onveilige bestanden die u downloadt. Downloadinformatie verschaft informatie over het reputatieniveau van alle uitvoerbare bestanden die u downloadt via de webbrowser. Downloadinformatie biedt alleen ondersteuning voor downloads via het HTTP-protocol, Internet Explorer 6.0 of later, Edge 40.15063 of later, Chrome 10.0 of later en Firefox 3.6 of later. De door Downloadinformatie verstrekte reputatiedetails geven aan of het gedownloade bestand veilig kan worden geïnstalleerd. Aan de hand van deze details kunt u bepalen of u het uitvoerbare bestand wilt installeren.

Norton zo instellen dat u uw beschermde apparaten op afstand kunt beheren

Extern beheer van Norton verzendt de status van uw apparaat en andere informatie naar de Norton Studio-app voor Windows. U kunt deze app gebruiken om op afstand uw Norton-producten te bekijken, te beheren of te verkennen en een aantal beschermingsproblemen met uw apparaat op te lossen. Extern beheer is standaard uitgeschakeld.

Extern beheer inschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 In de rij **Extern beheer** zet u de schakelaar op **Aan**.
- 5 Klik op **Toepassen** en vervolgens op **Sluiten**.

Instellingen voor Norton-apparaatbeveiliging beschermen tegen onbevoegde toegang

U kunt onbevoegde wijzigingen van uw instellingen voor Norton-apparaatbeveiliging voorkomen door **Wachtwoordbeveiliging voor instellingen** en **Norton Tamper Protection** in te schakelen.

- Met **Wachtwoordbeveiliging voor instellingen** kunt u een wachtwoord instellen om de apparaatbeveiligingsinstellingen te kunnen bekijken of wijzigen.

- **Norton Tamper Protection** controleert op wijzigingen in uw instellingen door onbekende of verdachte apps.

Wachtwoordbeveiliging voor instellingen en Norton Tamper Protection aan- of uitschakelen

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 Onder **Productbeveiliging** :
 - Zet de schakelaar in de rij **Wachtwoordbeveiliging voor instellingen** op **In** of **Uit**.
 - Zet de schakelaar in de rij **Norton Tamper Protection** op **In** of **Uit**.
Indien u daarom wordt gevraagd, geeft u op hoelang de functie uit moet staan en klikt u op **OK**.
- 5 Klik op **Toepassen**.
- 6 Als u het venster **Wachtwoord instellen** ziet, typt u een wachtwoord en bevestigt u het. U moet een wachtwoord instellen telkens wanneer u deze functie in- en uitschakelt.
- 7 Klik op **OK**.
- 8 Klik in het venster **Instellingen** op **Sluiten**.

Een verloren of vergeten wachtwoord voor Wachtwoord-beveiliging voor Norton-instellingen opnieuw instellen

U moet uw Norton opnieuw installeren om toegang te krijgen tot de instellingen en een nieuw wachtwoord in te stellen.

Een sneltoets instellen om in Norton-apparaatbeveiliging te zoeken naar informatie

Wanneer u zoekt met behulp van het



pictogram in de app Norton-apparaatbeveiliging, kunt u online informatie vinden over Norton-functies en ondersteuning, evenals algemene onderwerpen. U kunt de standaard-sneltoets **Ctrl + F** gebruiken om sneller te zoeken of een sneltoets instellen.

Een sneltoets voor zoeken configureren

- 1 Start Norton.
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 Zet in de rij **Sneltoets voor Zoeken** de schakelaar op **Aan**.
- 5 Klik op de pijl en kies de toets waaraan u Zoeken in product wilt toewijzen.
- 6 Voer een van de volgende handelingen uit:
 - Als de sneltoets alleen moet werken wanneer uw Norton-product is geselecteerd, moet u de **selectie ongedaan maken** van de optie **Algemeen**.
 - Moet de sneltoets ook werken wanneer uw Norton-product **niet** is geselecteerd, dan moet u de optie **Algemeen selecteren**.
- 7 Klik op **Toepassen** en vervolgens op **Sluiten**.

Extra oplossingen vinden

Dit hoofdstuk bevat de volgende onderwerpen:

- [Apparaatbeveiliging verwijderen](#)
- [Disclaimers](#)

Apparaatbeveiliging verwijderen

U kunt Apparaatbeveiliging op de volgende manieren van uw computer verwijderen:

- In het **Configuratiescherm** van Windows.
- Via het menu **Start**.
- Via het **Start** -scherm (Windows 8/8.1).

Opmerking: Het is raadzaam dit Help-onderwerp af te drukken alvorens de verwijdering voort te zetten. Tijdens de verwijdering kunt u de online Help niet oproepen.

Apparaatbeveiliging verwijderen via het Configuratiescherm van Windows.

- 1 Voer een van de volgende handelingen uit:
 - Klik op de Windows-taakbalk op **Start > Configuratiescherm**.
 - Ga in Windows 8 naar **Toepassingen** en klik onder **Windows-systeem** op **Configuratiescherm**.
 - In Windows 10 klikt u op **Start > Alle apps** en klikt u onder **Windows-systeem** op **Configuratiescherm**.
- 2 In het **Configuratiescherm** van Windows voert u een van de volgende handelingen uit:
 - Klik in Windows 7 en Windows 8 op **Programma's > Programma's en onderdelen**.

De optie **Programma's** is beschikbaar wanneer u de optie **Categorie** selecteert in de vervolgkeuzelijst **Weergeven op**.

- Klik in Windows 10 op **Een programma verwijderen**.
- 3 Voer in de lijst met momenteel geïnstalleerde programma's een van de volgende handelingen uit:
 - Klik in Windows 7, Windows 8 of Windows 10 op uw Norton-product en klik vervolgens op **Verwijderen/wijzigen**.
 - 4 Volg de instructies op het scherm.

Apparaatbeveiliging wordt pas volledig verwijderd wanneer u de computer opnieuw opstart.

Apparaatbeveiliging verwijderen via het menu Start

- 1 Klik in de taakbalk van Windows op **Start > Alle programma's/Alle apps > Norton > Norton verwijderen**.
- 2 Als u de Norton-startpagina niet als uw standaardstartpagina en Norton Safe Search niet als uw standaardzoekmachine wilt behouden, schakelt u het selectievakje in dat onderaan wordt weergegeven.
- 3 Volg de instructies op het scherm.

Apparaatbeveiliging wordt pas volledig verwijderd wanneer u de computer opnieuw opstart.

Apparaatbeveiliging verwijderen via het startscherm in Windows 8/8.1

- 1 Klik met de rechtermuisknop op uw Norton-product in het **Start** -scherm en klik dan op **Verwijderen**.
- 2 Klik in de lijst met momenteel geïnstalleerde programma's op uw Norton-product, en klik vervolgens op **Verwijderen/wijzigen**.
- 3 Volg de instructies op het scherm.

Uw Norton-product wordt pas volledig verwijderd wanneer u de computer opnieuw opstart.

Disclaimers

Copyright © 2019 Symantec Corporation. Alle rechten voorbehouden. Symantec, het Symantec-logo, het keurmerkviengkje, Norton en Norton by Symantec, LifeLock en het LockMan-logo zijn handelsmerken of gedeponeerde handelsmerken van Symantec Corporation of haar dochterondernemingen in de Verenigde Staten en andere landen. Firefox is een handelsmerk van de Mozilla Foundation. Google Chrome en Android zijn handelsmerken van Google, LLC. Mac, iPhone en iPad zijn handelsmerken van Apple Inc. Microsoft en het Windows-logo zijn handelsmerken van Microsoft Corporation in de Verenigde Staten en/of andere landen. De Android Robot wordt gereproduceerd of aangepast op basis van werk gemaakt en gedeeld door Google, en wordt gebruikt volgens de voorwaarden die zijn beschreven in de Creative Commons 3.0 Attribution License. Andere namen kunnen handelsmerken zijn van de respectieve eigenaars.