

McAfee's 10-STAPPENPLAN VOOR EEN VEILIG INTERNET VOOR UW GEZIN

Hoe u het met kinderen, pre-tieners,
tieners en starters van elke
leeftijd over onlinebeveiliging
kunt hebben

A woman with dark hair tied back is smiling and looking at a laptop screen. A young child with curly hair is sitting next to her, also looking at the screen. The woman's hand is on the child's shoulder. The laptop is open on a white desk. In the background, there is a window with a white railing and a view of a green landscape.

10

Inhoud

- 3 Inleiding
- 4 Internet van nu:
voorzichtigheid is geboden
- 5 Een 10-stappenplan voor een
veilig internet voor al uw gezinsleden
- 17 Het abc van veiligheid op internet:
 - 17 Voor kinderen (3 tot 7 jaar)
 - 21 Voor pre-tieners (8 tot 12 jaar)
 - 26 Voor tieners (13 tot 19 jaar)
 - 30 Voor starters van elke leeftijd
- 33 Over McAfee

10





Inleiding

Miljoenen gezinnen over de hele wereld maken elke dag gebruik van internet om iets te leren, dingen op te zoeken, te winkelen, te kopen, te bankieren, te investeren, foto's uit te wisselen, games te spelen, films en muziek te downloaden, contact te hebben met vrienden, nieuwe mensen te ontmoeten en zich bezig te houden met nog veel meer activiteiten. Hoewel internet talloze voordelen, mogelijkheden en veel gemak biedt, wordt het ook steeds riskanter: elke dag duiken **vele nieuwe gevaren op**.

Het is dan ook geen verrassing dat cybercriminelen misbruik maken van internet en van de mensen die er gebruik van maken. U en uw gezinsleden moeten altijd uitkijken wanneer u online gaat. U moet niet alleen goede beveiligingssoftware van een betrouwbaar bedrijf installeren om uw gezin te beschermen tegen hackers, personen die identiteitsgegevens stelen, oplichters die via e-mail opereren en kinderlokken, maar ook een aantal **basisregels voor internetbeveiliging in acht nemen** en een ouderwets, gezond verstand gebruiken. U hebt een internetbeveiligingsplan voor uw gezin nodig.

Zodra gezinsleden online actief worden — en ongeacht hun leeftijd —, is het tijd om hen te onderwijzen over internet veiligheid. **U moet beseffen** dat pc's, ook al hebt u er thuis geen, bijna overal beschikbaar zijn: — op scholen, in bibliotheken, bij vriendjes thuis en zelfs in kelders van kerken. Het is voor iedereen belangrijk om de basisbeginselen van bescherming op internet te kennen.



Internet van nu: voorzichtigheid is geboden

- 50% van de tieners online hebben persoonlijke informatie bekendgemaakt¹
- Hackers vallen elke 39 seconden pc's aan met internettoegang²
- Volgens McAfee® Avert Labs®, zijn er momenteel 222.000 bekende computervirussen, en het aantal bedreigingen groeit dagelijks
- 30% van de tieners wordt tijdens de schoolperiode één of meerdere keren via internet gepest³
- Internetcriminaliteit is toegenomen met 33% in 2008 ten opzichte van 2007⁴
- 31% van de kinderen zijn blootgesteld aan schadelijke inhoud¹
- 3,2 miljoen mensen wereldwijd worden jaarlijks bedrogen door massale marketingzwendel⁵

1 EU Kids Online, vergelijkt de mogelijkheden en risico's van het internet voor kinderen in Europa (2006–2009)

2 Elke 39 seconden een aanval door hackers – James Clark School of Engineering aan de University of Maryland

3 theage.com.au

4 2008 Internet Crime Report, IC3

5 National Fraud Strategic Authority



Een 10-stappenplan
voor een veilig
internet voor al
uw gezinsleden



Stap 1

Geef de computer de juiste plek

In een huis met kinderen is de plek waar de gezinscomputer komt te staan een van de belangrijkste beslissingen die u kunt nemen. We raden u aan de computer neer te zetten op een **plek waar altijd wel iemand is** en het aantal uren dat kinderen achter de computer zitten, te beperken. Zorg ervoor dat u over **beveiligingssoftware** voor de computer beschikt met door ouders in te stellen beperkingen zoals aanwezig in McAfee-producten, of gebruik software die speciaal ontworpen is voor de bescherming van kinderen online, zoals McAfee Family Protection.

Stap 1



Stap 2

Stap 2

Werk samen als een team om grenzen te stellen

Bepaal precies wat mag en wat niet mag wat betreft:

- Het soort websites dat geschikt is om te bezoeken
- De chatrooms en forums die geschikt zijn om aan deel te nemen:
 - Gebruik alleen chatrooms die onder toezicht staan
 - Zorg ervoor dat uw kinderen “.alt”-chatrooms vermijden die gericht zijn op alternatieve onderwerpen die misschien niet geschikt zijn voor jonge mensen
- Het soort zaken dat uw kinderen online kunnen bespreken en taal die onbehoorlijk wordt geacht



Stap 3

Beslis samen over computer-regels voor het gezin

We raden het volgende aan:

- Log nooit in met een gebruikersnaam die de ware identiteit onthult of provocerend is
- Maak nooit je wachtwoorden bekend
- Maak nooit telefoonnummers of adressen bekend
- Plaats nooit informatie die je identiteit onthult
- Plaats nooit onbehoorlijke foto's of foto's die je identiteit kunnen onthullen (bijvoorbeeld: de naam van een stad of een school op een T-shirt)
- Wissel online nooit informatie uit met vreemden
- Spreek nooit af met vreemden die je online hebt ontmoet
- Open nooit bijlagen van vreemden

Zodra u de regels hebt vastgesteld, hangt u ze naast de computer.

Stap 3



Stap 4

Teken een contract over geschikt gedrag online

Maak een contract of **gebruik het contract op de volgende pagina**, zodat alle gezinsleden weten wat gepast computergebruik en **gepast gedrag op internet is**.

Stap 4



Contract voor veiligheid op internet

Omdat het gebruik van de computer en internet een voorrecht is dat ik niet wil kwijtraken,

- Zal ik veilig internetten, zoeken, werken, spelen en chatten als ik online ga
- Ik zal alle regels volgen waar we het over eens zijn geworden
- Ik zal mijn echte naam, mijn telefoonnummer, mijn adres, of mijn wachtwoorden niet bekendmaken aan online "vrienden"
- Ik zal nooit een afspraak voor een persoonlijke ontmoeting maken met mensen die ik online ben tegengekomen
- Als ik op internet in een onveilige of ongemakkelijke situatie terecht kom, beloof ik dat ik dat aan jou (mijn ouder/voogd/leraar) vertel, zodat je mij kunt helpen
- Ik houd me aan dit contract en weet dat elke beslissing die ik neem gevolgen heeft

Handtekening kind _____

- Als ouder/voogd/leraar beloof ik dat je op mij kunt rekenen als je hulp nodig hebt en zal ik je op alle mogelijke manieren helpen eventuele problemen op te lossen.

Handtekening ouder/voogd/leraar _____



Stap 5

Installeer beveiligingssoftware

Zorg ervoor dat u over goede beveiligingssoftware beschikt die uw computer beschermt tegen virussen, hackers en spyware. Die software moet ook aanstootgevende inhoud, afbeeldingen en websites filteren. Deze software **moet regelmatig worden bijgewerkt**, omdat er met de dag nieuwe gevaren opduiken. Ideaal gesproken is beveiligingssoftware die automatisch wordt bijgewerkt—zoals McAfee's **instellen-en-verder-geen-omkijken-meer-naar-software**—de beste keuze.

Stap 5



Stap 6

Gebruik ouderlijk toezicht

Alle grote fabrikanten van beveiligingssoftware bieden ouderlijk toezicht. Schakel dat toezicht ook in. Als u freeware of software zonder ouderlijk toezicht gebruikt, moet u overwegen software te kopen die daar wel over beschikt. **Neem de tijd om uit te zoeken hoe het werkt**, en gebruik opties die ongeschikt materiaal filteren.

Gebruik om uw kinderen op internet volledig te beschermen McAfee Family Protection software naast het ouderlijk toezicht in uw beveiligingssoftware. McAfee Family Protection software beschermt kinderen van alle leeftijden tegen blootstelling aan ongepaste inhoud, risico's van sociale netwerksites, vreemden en andere bedreigingen van het internet.

Natuurlijk hebben deze hulpmiddelen ook hun beperkingen. Niets kan de plaats innemen van oplettende en meelevende ouders die hun kinderen in de gaten houden als ze online zijn.

Stap 6



Stap 7

Stap 7

Herinner familieleden eraan dat mensen die ze via internet ontmoeten vreemden zijn

Iedereen die online gaat, moet het volgende begrijpen:

Hoe vaak je ook chat met 'vrienden' van internet, hoe lang je ook al met iemand chat en hoe goed je ze ook denkt te kennen: mensen die je online tegenkomt, zijn vreemden. **Liegen en je voordoen als iemand anders is gemakkelijk als je online bent.** Vooral kinderen moeten weten dat een nieuwe 'vriend' in werkelijkheid een man van 40 kan zijn in plaats van iemand van hun leeftijd.

Sociale netwerksites zoals Hyves en Facebook zijn een ideale manier om online nieuwe mensen te ontmoeten. U moet dit soort sites dus bezoeken en **het profiel van uw kinderen bekijken** om ervoor te zorgen dat er geen ongepaste gesprekken worden gevoerd en dat er geen onacceptabele foto's worden geplaatst. U moet ook de rechtstreekse berichtenconversaties van uw kinderen in de gaten houden om ervoor te zorgen dat ze niet online worden achtervolgd door een kinderlokker.



Stap 8

Maak sterke wachtwoorden

Als je een wachtwoord wilt maken dat moeilijk te kraken is, begin je door minstens 8 tekens te gebruiken en vervolgens een combinatie van letters, getallen en symbolen te kiezen. **Wachtwoorden moeten regelmatig worden gewijzigd** om te voorkomen dat een bepaald wachtwoord na verloop van tijd minder veilig wordt.

Methodes voor sterke wachtwoorden:

- Gebruik een gepersonaliseerde nummerplaat: "W8ff0pmy"
- Gebruik meerdere woordjes met leestekens: "Bindi#the^jungle@girl"
- Zet midden in een woord een leesteken: "Beck%ham"
- Gebruik een ongewone samentrekking van een woord: "vtblspln"
- Gebruik de eerste letter van elk woord in een zinnetje, met een willekeurig getal: 'moeilijk om dit wachtwoord te kraken' = 'modw5tk'
- Vertel je wachtwoord aan niemand!

Stap 8



Stap 9

Controleer de beveiligingssoftware op uw computer

Open de beveiligingssoftware die u gebruikt en controleer of uw computer wordt beschermd door de volgende **drie belangrijke zaken**: een **antivirusprogramma**, een **antispyswareprogramma** en een **firewall**.

Deze hoofdbeveiliging moet worden aangevuld met antispamssoftware en software voor veilig zoeken, zoals McAfee SiteAdvisor®, die voorzien zijn van antiphishingbescherming en beschermingsniveaus. Voor gezinnen is een compleet beveiligingspakket op thuis-pc's ideaal, met ouderlijk toezicht, zoals McAfee Family Protection software en hulpprogramma's om diefstal van identiteitsgegevens te voorkomen.

Stap 9



Stap 10

Blijf op de hoogte

Hoe meer u weet, hoe veiliger u bent. Ga naar het beveiligingsadviescentrum van McAfee voor makkelijk leesbare en leerzame informatie over computer- en internetbeveiliging: www.mcafee.com/advice.

Stap 10



Het abc van veiligheid op internet

Voor kinderen 3–7 jaar



A

Met jonge kinderen praten

Als u het met jonge kinderen over veiligheid op internet hebt, kunt u dat het beste doen met de computer uit, zodat u hun onverdeelde aandacht hebt. Begin met uitleggen dat een computer een hulpmiddel is en dat internet een soort elektronische reuzebibliotheek boordevol informatie is.

Leg uit waarom het belangrijk is om veilig online te zijn, omdat de computer eenvoudig toegang kan geven tot uw belangrijke persoonlijke gegevens. Praat met ze over hoe slechte mensen de besturing van uw pc kunnen overnemen en de computer kapot kunnen maken, waardoor u een nieuwe moet kopen.

Leg uit waarom het belangrijk is om geen persoonlijke gegevens uit te wisselen met mensen op internet. Vertel ze dat ze niet hun eigen naam moeten gebruiken en niet moeten zeggen waar ze wonen of naar welke school ze gaan.



B

Maak een speciale lijst met regels voor computergebruik door jonge kinderen

Op die lijst moet het volgende staan:

- Download geen muziek- of programmabestanden van websites zonder toestemming van de ouders
- Gebruik alleen chatrooms waarbij een volwassene toezicht houdt op de chat-conversatie
- Stuur nooit een foto van jezelf zonder eerst met je ouders te overleggen
- Gebruik geen grove taal
- Bezoek geen websites voor volwassenen
- Wissel alleen informatie uit met mensen die je in het echt kent, bijvoorbeeld klasgenoten, vrienden en familie
- Vul geen formulieren in op internet zonder de hulp van een ouder
- Gebruik alleen speciale zoekmachines, zoals KiddieSearch en Netwijs .nl



C

Gebruik browsers en zoekmachines die speciaal voor kinderen zijn bedoeld

Zorg ervoor dat uw kinderen browsers en zoekmachines gebruiken die geen ongepaste tekst of afbeeldingen weergeven. Controleer of de browser al is ingesteld op veilige websites en met woordfilters. Het enige wat u hoeft te doen, is de standaardwebsites en -woorden bekijken en goedkeuren.

Zorg er als uw kinderen een standaard zoekmachine gebruiken voor dat u het ouderlijk toezicht inschakelt in de zoekmachines om te voorkomen dat ongeschikte afbeeldingen en inhoud in de zoekresultaten verschijnen.



Het abc van veiligheid op internet

Voor pre-tieners 8–12 jaar



A

Met uw pre-tiener praten

Kinderen tussen acht en twaalf jaar zijn veel wereldwijzer dan ze vroeger waren in die leeftijd. De term 'pre-tiener' (Engels: 'tween') is speciaal verzonnen voor deze groep kinderen die niet meer als 'jonge kinderen' worden beschouwd, maar ook nog geen tieners zijn. Deze tweens zijn erg handig met de computer, omdat ze er thuis en/of op school mee zijn opgegroeid.

Voordat u met pre-tieners gaat praten, moet u een aantal beslissingen nemen, zodat u grenzen kunt stellen aan hun internetgebruik. Om duidelijk te kunnen overbrengen wat de regels zijn, moet u ze eerst vaststellen. Om uw pre-tiener veilig te laten internetten, moet u de volgende vragen kunnen beantwoorden:

- Staat de computer in een openbare ruimte of thuis?
- Welke websites kan uw pre-tiener veilig bezoeken?
- Hoe lang mogen onlinesessies duren?
- Wat mogen ze doen als ze online zijn?
- Met wie mogen ze contact hebben?
- Als u uw pre-tieners gaat controleren: wanneer moeten ze om uw hulp of toestemming vragen?



Zodra u de antwoorden op deze vragen weet, kunt u het gesprek met ze aangaan. Met de computer uit, zodat ze uw onverdeelde aandacht hebben, legt u uw pre-tiener uit dat de computer een hulpmiddel is en dat het belangrijk is dat ze veilig zijn op internet.

Heb het in elk geval over de volgende punten:

- Bespreek virussen, spyware en hackers
- Bespreek hoe kinderlokken kinderen willen verleiden om over zichzelf te praten
- Leg uit waarom het belangrijk is om veilig online te zijn, omdat de computer eenvoudig toegang kan geven tot uw belangrijke persoonlijke gegevens
- Bespreek hoe diefstal van identiteitsgegevens optreedt
- Bespreek het feit dat u of een computerexpert (als u dat zelf niet bent) alles kan nagaan wat er met uw computer is gedaan
- Praat met ze over hoe criminelen de besturing van uw pc kunnen overnemen en de computer kapot kunnen maken, waardoor u een nieuwe moet kopen



B

Vertel uw kind dat het om hulp moet vragen als er online iets vervelends gebeurt

Benadruk aan uw pre-tieners dat ze het moeten vertellen als ze rare of vervelende berichten krijgen tijdens het chatten en dat u dan niet boos op ze zult zijn of ze zult verbieden om internet te gebruiken. Maak het kind duidelijk dat u begrijpt dat ze geen invloed hebben over wat anderen tegen ze zeggen en dat zij niet de schuld kunnen krijgen als dat gebeurt.


Zorg er ook voor dat uw pre-tiener niet online wordt gepest of zelf andere kinderen pest. Als kinderen uit school komen, laten ze hun klasgenoten en hun problemen niet per se achter. Via computers, sms-berichten en mobiele-telefoongesprekken kunnen scholieren altijd in contact met elkaar blijven, en ze kunnen deze technologie misbruiken om anderen te pesten, te treiteren of schade te berokkenen.



C

Hoe u gebruikers blokkeert en problemen rapporteert

Als er tijdens het chatten van uw kind iets vervelends gebeurt, kunt het probleem melden en de gebruiker blokkeren. Kopieer eerst de chatberichten en plak de tekst in een tekstverwerkingsprogramma. Stuur de gekopieerde tekst vervolgens naar de moderator of beheerder van de chatroom. U vindt de contactgegevens van de moderator of beheerder in het help- of rapportageonderdeel van het programma. In de meeste chatprogramma's kunt u een gebruiker ook blokkeren door met de rechtermuisknop te klikken op de naam in de lijst met contactpersonen en de functie "Blokkeren" of "Negeren" te kiezen.



Het abc van veiligheid op internet

Voor tieners 13-19 jaar



A

Met uw tieners praten

Zoals u tieners verkeersveiligheid moet bijbrengen voordat ze gaan autorijden, moet u ze ook leren internet veilig te gebruiken, voordat u ze zonder toezicht op het web laat surfen.

Een belangrijk verschil tussen in de auto springen en online gaan is dat er geen echte 'verkeersregels' op internet bestaan. Daardoor is het een zeer krachtig en zeer gevaarlijk voertuig. Om computercrashes of erger te voorkomen, moet u dus regels opstellen en die aan hen opleggen. Het doel daarvan is om tieners hun gezond verstand te laten gebruiken, zodat ze uit de buurt te blijven van online gevaren.



Bespreek met uw tiener waarom het belangrijk is om veilig te internetten.

Heb het in elk geval over de volgende punten:

- Bespreek virussen, spyware en hackers en hoe ze te werk gaan
- Bespreek hoe kinderlokkeners kwetsbare jongeren willen verleiden om over zichzelf te praten
- Leg uit waarom het belangrijk is om veilig online te zijn, omdat de computer eenvoudig toegang kan geven tot uw belangrijke persoonlijke gegevens
- Bespreek hoe diefstal van identiteitsgegevens optreedt
- Bespreek het feit dat u of een computereexpert (als u dat zelf niet bent) alles kan nagaan wat er met uw computer is gedaan
- Praat met ze over hoe criminelen de besturing van uw pc kunnen overnemen en de computer kapot kunnen maken, waardoor u een nieuwe moet kopen



B

Herinner uw tiener eraan dat mensen die ze online ontmoeten vreemden zijn

Hoe vaak ze ook online met ze chatten en hoe goed ze hen ook denken te kennen: mensen die uw tieners online ontmoeten, zijn vreemden. Mensen kunnen liegen over hun leeftijd. De nieuwe 'vriend' van uw tiener kan dus een man van 40 zijn in plaats van iemand van hun eigen leeftijd.

C

Controleer het profiel van uw tiener op sociale netwerksites

Zorg ervoor dat uw tieners niet te veel informatie over zichzelf publiceren op Hyves of Facebook. Zorg ervoor dat de foto's die ze plaatsen niet provocerend zijn. Wijs ze erop dat ze de aandacht van kinderlokkers op internet kunnen trekken, vrienden en familie in verlegenheid kunnen brengen, een eventuele toelating op een universiteit kunnen bemoeilijken of een toekomstige werkgever negatief kunnen beïnvloeden.



Het abc van veiligheid op internet

Voor beginners van alle
leeftijden



Voor uw echtgenoot, partner, ouders, schoonfamilie of grootouders is het gebruik van een computer en internet misschien nieuw. Ze zijn misschien niet zo handig als u denkt en zouden het slachtoffer kunnen worden van oplichting op internet en cyberaanvallen. Daarom kunnen ze wel wat begeleiding van u gebruiken. Uw bespreking van veiligheid op internet moet de volgende punten bevatten:

A

Virussen, spyware en hackers

Definities van deze termen zijn makkelijk te vinden via een zoekmachine of de woordenlijst op www.mcafee.com/advice.



B

Gevaren van diefstal van identiteitsgegevens en phishing

Er is sprake van phishing als criminelen een nepwebsite of -e-mailadres maken van een legitiem bedrijf met als doel wachtwoorden en creditcardnummers te stelen. Controleer regelmatig uw creditcard- en bankafschriften.

C

Het belang van terughoudendheid bij het downloaden van 'gratis' dingen

Herinner de mensen die u lief zijn aan het oude gezegde dat voor niets de zon opgaat en dat 'gratis' niet bestaat! Waarschuw ze er ook voor dat ze bij het downloaden van software misschien ongevraagd adware en spyware bij de applicatie krijgen.

Meer advies over pc- en internetveiligheid

Bezoek voor meer informatie en advies over beveiliging voor pc en internet het beveiligingsadviescentrum van McAfee op www.mcafee.com/advice.

Over McAfee

McAfee Inc., gevestigd in Santa Clara, Californië, is het grootste gespecialiseerde bedrijf ter wereld inzake veiligheidstechnologie. McAfee is toegewijd om de moeilijkste veiligheidsuitdagingen ter wereld aan te gaan. Het bedrijf levert proactieve en bewezen oplossingen en diensten die helpen om systemen en netwerken over heel de wereld te beveiligen, zodat gebruikers veilig met het internet kunnen verbinden, en nog veiliger aankopen kunnen doen op het web. Gesteund door een met een prijs bekroond onderzoeksteam, creëert McAfee innovatieve producten die thuisgebruikers, bedrijven, de publieke sector en dienstverleners in staat stellen om aan de geldende regelgevingen te voldoen, gegevens te beschermen, storingen te voorkomen, kwetsbaarheden te identificeren en continue de beveiliging te bewaken en te verbeteren.

www.mcafee.nl

McAfee, Inc. 3965 Freedom Circle Santa Clara, CA 95054 1.888.847.8766 www.mcafee.com

McAfee en/of andere gerelateerde McAfee-producten hier vermeld, zijn gedeponeerde handelsmerken of handelsmerken van McAfee, Inc. en/of haar gelieerde bedrijven in de VS en/of andere landen. McAfee Red wijkt qua beveiliging af van McAfee-merkproducten. Alle andere niet-gerelateerde McAfee-producten, gedeponeerde en/of niet-gedeponeerde handelsmerken hierin zijn enkel ter referentie en zijn het eigendom van hun respectievelijke eigenaars.

© 2009 McAfee, Inc. Alle rechten voorbehouden.