Presentatie Internet & Privacy

Privacy in het dagelijks leven is niets nieuws. Wie iets koopt bij de groenteboer, kan dat doen zonder zich te hoeven legitimeren. Het versturen van een brief kan zonder dat het postkantoor controleert of het adres van de afzender wel correct is. En wie zou er niet boos worden als de postbode alle brieven leest?

Op het Internet is privacy een stuk minder vanzelfsprekend. Als u op het internet aan het surfen bent, vindt u het dan normaal dat de websites die u bezoekt uw surfgedrag en nog veel meer “persoonlijke” gegevens van u vastlegt voor puur zakelijk gewin?

Bedenk wel dat zodra u uw computer, smartphone of tablet met Internet verbind, u verbinding heeft met de hele wereld (het grote “boze” **W**ereld **W**ijde **W**eb), maar dat de hele wereld dan ook de kans heeft om in uw computer, smartphone of tablet in te breken.

Zorg daarom voor een veilige computer

Als criminelen je computer binnendringen is dat heel slecht voor je privacy. Je kunt je pc wel wapenen tegen zulke hackers.

Installeer een goede virusscanner

Natuurlijk heb je een virusscanner die voorkomt dat allerhande 'malware' (kwaadaardige software) jouw pc binnendringt. Sommige malware stelt hackers in staat te volgen wat jij op de pc doet. We kunnen niet zeggen welke virusscanner de beste is, want de resultaten van onze test verschillen elk jaar. Wel zien we een kleine kopgroep van virusscanners die het keer op keer goed doet. Het gaat om de scanners van G-Data, Kaspersky, F-Secure en ESET.
Maar geen enkele scanner zorgt voor een waterdichte beveiliging. Je moet meer doen.

Zorg dat je programma's up-to-date zijn

Software wordt niet alleen maar geüpdatet omdat de maker een leuke nieuwe functie heeft bedacht. Regelmatig wordt een update noodgedwongen uitgebracht omdat er een lek is gevonden waardoor criminelen je pc kunnen binnendringen. Laat dat knipperende update-icoontje dus niet te lang staan maar voer de update uit.

Windows zelf is niet meer het grootste gevaar, omdat nieuwe updates standaard automatisch worden geïnstalleerd. Gevaarlijker is veelgebruikte software als Flash, Adobe Reader en Java. Die worden veel minder snel door computergebruikers bijgewerkt. Een radicalere oplossing is om de genoemde kwetsbare software helemaal te verwijderen.

Adobe reader is nog steeds een populair programma onder hackers. Denk eens aan een alternatief. Zoals Sumatra PDF, Foxit, of de ingebouwde PDF lezer van Google Chrome of Firefox 20 (of hoger).

En heb je **Java** op je computer? Vroeger was dit nodig om veel websites te laten werken, maar tegenwoordig wordt het nauwelijks meer gebruikt. Java is dan vooral een zwakke plek in je PC. Schakel Java uit.

Gedraag je veilig

Klik nooit zomaar op links

Phishing is en blijft een populaire manier van criminelen om je geld afhandig te maken. Traditioneel gebeurt dat via de phishingmail, bijvoorbeeld een mail die zogenaamd van je bank afkomstig is met een link om in te loggen. Die link leidt dan naar een nagebouwde website. Maar zo'n foute link kan in principe overal opduiken. Hij kan bijvoorbeeld ook verstopt zitten in een Twitter- of Facebookbericht.

Download software uit een goede bron

Heb je iemand de naam van een leuk nieuw tooltje of plug-in doorgekregen? Klik dan niet op de eerste de beste link in Google en ook niet op de Google-advertenties die boven en naast de resultaten verschijnen. Zoek eerst uit wie de maker is van de software, ga naar de website van de maker en download het daar.

Ook dan is het van belang om goed op te letten dat er geen ongewenste Toolbars en dergelijke zogenaamde hulp-programmaatjes mee geinstalleerd worden. Haal in voorkomend geval de **vinkjes** weg of klik zo nodig op **I do not accept** c.q. **Decline** of **I do not Agree** of welke uitdruking daar ook voor wordt gebruikt.

Wantrouw bedrijven die bellen

Het zal jou misschien ook intussen overkomen zijn: gebeld worden door de helpdesk van Microsoft met de melding dat je computer besmet is. Hang dan meteen op. Het gaat hier om oplichters die uit India opereren die proberen je computer over te nemen.

Er zijn ook gevallen bekend van mensen die gebeld werden door hun bank, tenminste dat dachten ze. Geef nooit door de telefoon je rekeningnummer en inlogcode door. Banken zullen hier nooit om vragen.

Gebruik goede, unieke wachtwoorden

Wel 6 op de 10 mensen gebruiken voor internetdiensten nog steeds wachtwoord dat je makkelijk kunt raden, zoals een naam met een geboortedatum erachter. Een goed gekozen wachtwoord is moeilijk te raden, maar met een ezelsbruggetje toch makkelijk te onthouden. Je kunt bijvoorbeeld een zin gebruiken, en daar dan de eerste letters van nemen. Je kunt ook werken met hele zinnen. Je wachtwoord wordt dan dus een wachtzin.

Gebruik verder niet voor elk account hetzelfde wachtwoord. Anders word je wachtwoord een soort 'masterkey' waarmee een kraker overal kan inloggen als hij het eenmaal in handen heeft. En gebruik dan niet varianten op hetzelfde
wachtwoord, maar echt verschillende wachtwoorden.

Tem de sociale netwerken

Wat deel je bewust en vooral ook onbewust met de rest van de wereld via Twitter, Facebook, Hyves, Instagram, Google+ Linkedin of een van de andere sociale netwerken?

Twitter wil bijvoorbeeld je locatie meesturen met je tweets. Is dat nodig? En Facebook wil jouw naam gebruiken in advertenties van merken die jij ooit hebt 'geliked'. Zitten jij en je vrienden daar op te wachten? Vast niet.

De sociale netwerken hebben allemaal privacy-opties die het rondpompen van jouw gegevens kunnen beperken, als je dat aangeeft. Loop deze opties regelmatig eens langs, want ze veranderen nogal eens (en niet in jouw voordeel). Een tip: Je kunt bij zowel Facebook als Google+ je profielpagina bekijken zoals niet-vrienden dat kunnen zien (bijvoorbeeld je werkgever).

- In **Facebook:** ga naar de Privacyinstellingen (hangslotsymbool), kies Meer instellingen weergeven, kies links Tijdlijn en taggen en klik bij 'Wie kan dingen op mijn tijdlijn zien?' op de link 'Weergeven als'. Je ziet nu hoe je profiel er uitziet voor de rest van de wereld.
- Voor **Google+**: surf naar google.nl en log uit je Google-account. Google nu je eigen naam en klik op je Google+-vermelding. Je ziet nu je profiel zoals niet-vrienden dat zien.

Gebruik de Beveiligings- & Privacy mogelijkheden van je browser

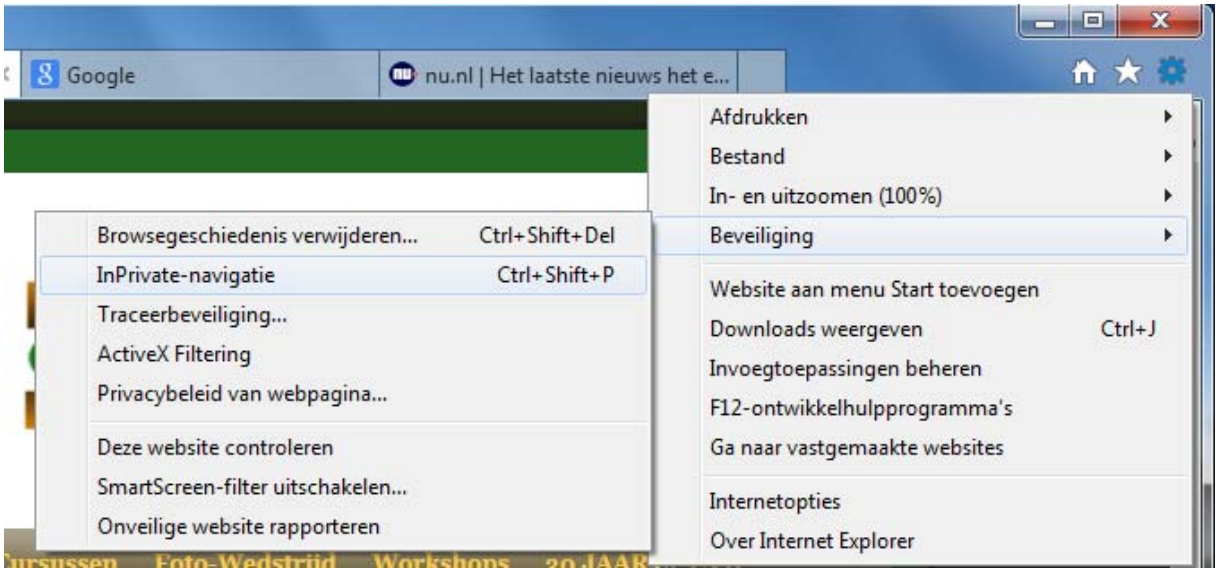
Naast een goede virusscanner, het up to date houden van de software, het niet zo maar klakkeloos klikken op links, het niet reageren op mailtjes en telefoontjes die zogenaamd van uw bank afkomstig zijn, het gebruik van goede wachtwoorden en het bewust omgaan met uw privacy op Sociale media, is het ook zeer wenselijk om na te gaan welke mogelijkheden de browser die u gebruikt heeft om uw Privacy zo goed mogelijk te beschermen en te waarborgen.

Internet Explorer en Privacy

Als voorbeeld gebruik ik de mogelijkheden van Internet Explorer , maar ook de andere bekende browsers zoals Firefox en Google Chrome hebben vergelijkbare opties.

1. InPrivate-navigatie

Hoewel veel mensen weten dat tijdens het ***surfen*** op Internet cookies op hun eigen computer worden opgeslagen waarin gegevens over hun surfgedrag worden vastgelegd, zijn er maar weinig computer gebrui8kers die weten dat er buiten cookies ook tijdelijke internet bestanden worden aangemaakt waarin onder andere de geschiedenis van het gebruik van internet, informatie uit ingevulde formulieren en ook op internet gebruikte wachtwoorden en nog meer gegevens worden opgeslagen.

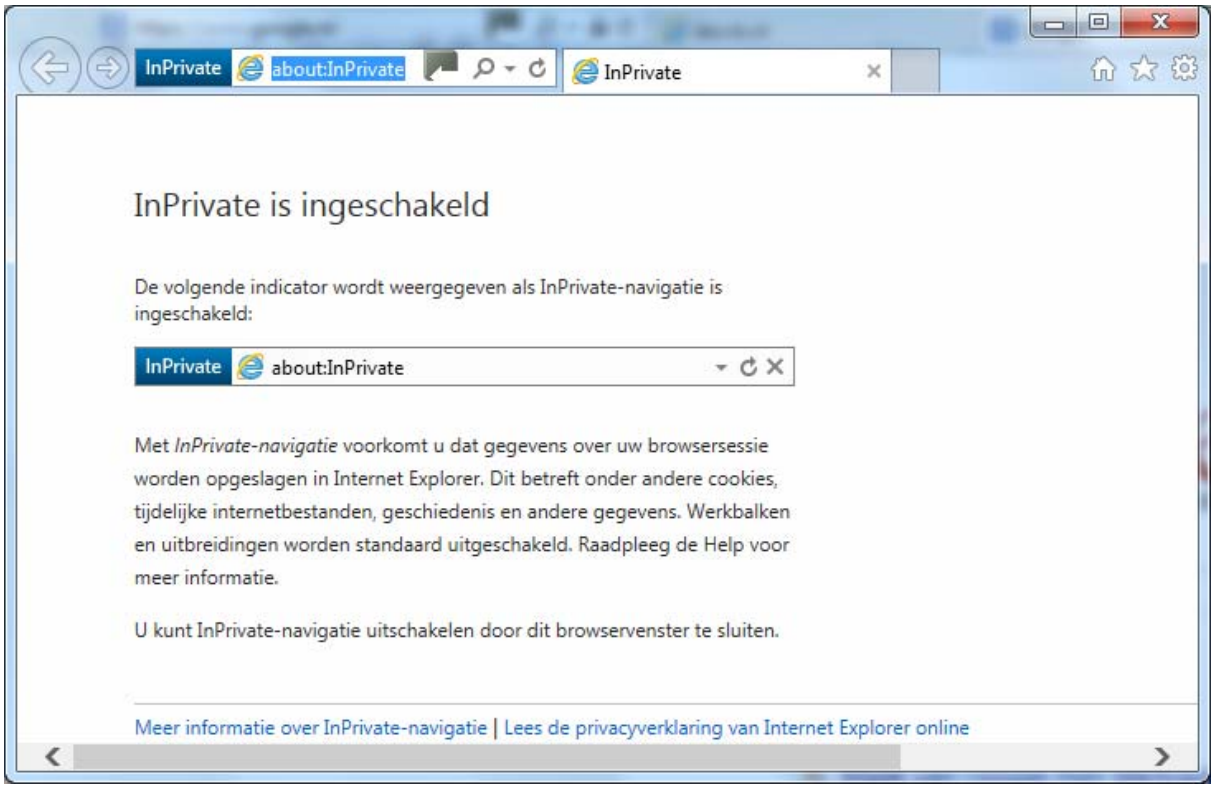


Met **InPrivate-navigatie** worden een deel van deze gegevens, die bij normaal gebruik van Internet Explorer of een andere browser allemaal op uw computer worden opgeslagen, of helemaal niet opgeslagen of tijdelijk opgeslagen en direct bij het afsluiten van Internet Explorer van uw computer verwijderd.

InPrivate-navigatie kunt u in Internet Explorer inschakelen door op de knop **Extra** (het radarwieltje) te klikken, vervolgens **Beveiliging** aan te wijzen en in het volgende menu op **InPrivate-navigatie** te klikken.

U kunt **InPrivate-navigatie** ook inschakelen met de toetsen combinatie **Ctrl+Shift+P**.

Er wordt, als u **InPrivate-navigatie** inschakeld in Internet Explorer een nieuw venster geopend waarin duidelijk staat dat **InPrivate** is ingeschakeld en een korte uitleg wordt gegeven wat het doet.

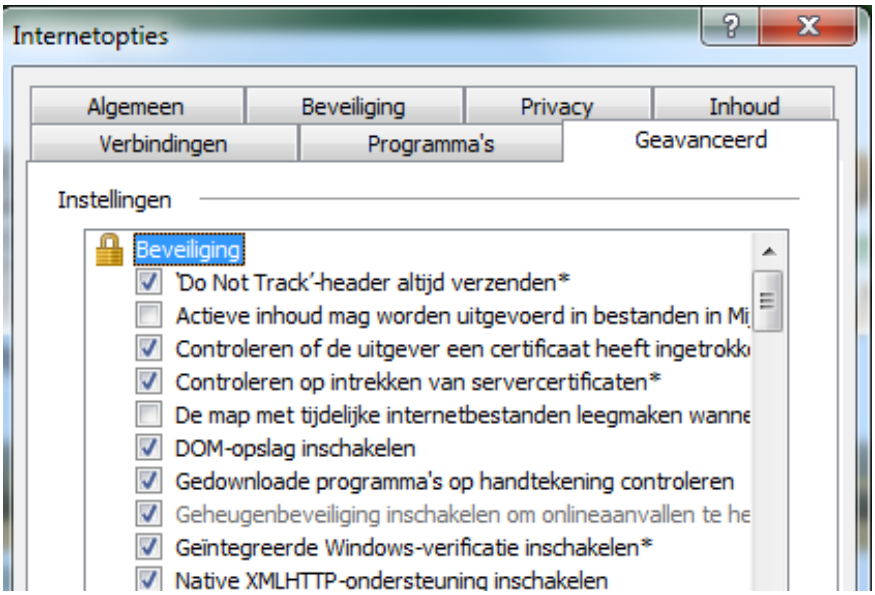


2. Traceerbeveiliging

Met **Traceerbeveiliging** stuurt u via Internet Explorer een ***Do Not Track***-verzoek naar de websites die u bezoekt. Met een ***Do Not Track***-verzoek kunt u uw surfgedrag beter privé houden, maar kan het voorkomen dat u bepaalde inhoud van die websites niet kunt zien.

Let wel: het is een verzoek en websites zijn niet verplicht om het verzoek op te volgen, maar alle **"nette"** websites zullen zich er wel aan houden.

Traceerbeveiliging kunt u permanent instellen via de knop **Extra** , **Internetopties** en op het Tabblad **Gavanceerd** vervolgens een vinkje ✓ te zetten bij de regel **Do Not Track-header altijd verzenden** en de wijziging te bevestigen met de knop OK.



3. ActiveX Filtering

ActiveX-besturingselementen en **invoegtoepassingen** voor webbrowsers zijn kleine programma's die op grote schaal worden gebruikt op internet. Met deze programma's kunt u tijdens het surfen werkbalken, tikkers, video's en nog veel meer gebruiken. Deze programma's kunnen echter ook fouten bevatten of ongewenste inhoud weergeven. In sommige gevallen kunnen ze worden gebruikt om gegevens van uw computer te verzamelen, gegevens op uw computer te beschadigen, zonder uw toestemming software op uw computer te installeren of iemand anders in staat te stellen uw computer op afstand te besturen.

Stel uzelf de volgende vragen voordat u toestaat dat een website een **ActiveX-besturingselement** op uw computer kan installeren:

- Is de website waarop dit besturingselement beschikbaar wordt gesteld te vertrouwen?
- Waarvoor is het besturingselement bedoeld en wat doet het op de computer?

Als het goed is, kunt u op de website meer lezen over de functie van de **invoegtoepassing** of het **ActiveX-besturingselement** en eventuele bijzonderheden die u moet weten voordat u het besturingselement installeert. Als deze informatie **niet** beschikbaar is, moet u het besturingselement **niet** installeren.

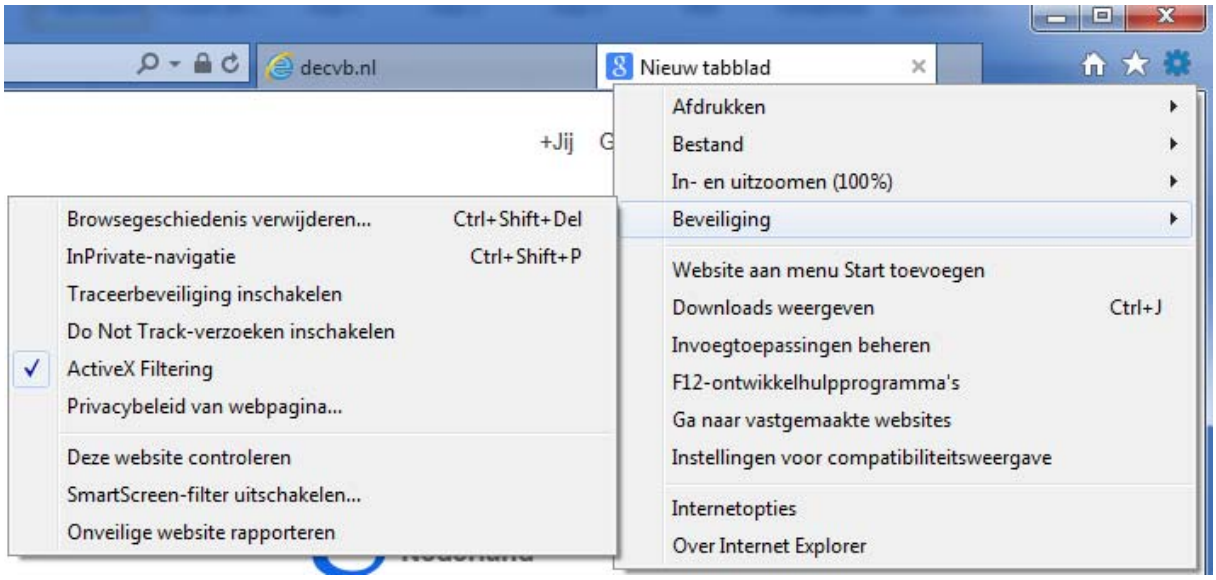
ActiveX-filtering in Internet Explorer kan u helpen een weloverwogen besluit te nemen over elk **ActiveX-besturingselement** dat u gebruikt doordat u de mogelijkheid krijgt om ActiveX-besturingselementen voor alle sites te blokkeren en/of weer in te schakelen bij sites die u vertrouwt.

Door hier weloverwogen mee om te gaan kunt u zich beter beveiligen tegen risicovolle en onbetrouwbare ActiveX-besturingselementen. Aan de andere kant is het wel zo dat inschakeling van **ActiveX-filtering** als neveneffect heeft dat u dan op de meeste websites weer minder kan doen.

De voor- en nadelen van het inschakelen van **ActiveX-filtering** moet u goed afwegen.

Op deze site van Microsoft: http://windows.microsoft.com/nl-nl/internet-explorer/use-activex-filtering#ie=ie-10-win-7 kunt meer lezen over het gebruik van **ActiveX-filtering**.

ActiveX-filtering kunt u in Internet Explorer inschakelen door op de knop **Extra** (het radarwieltje) te klikken, vervolgens **Beveiliging** aan te wijzen en in het volgende menu op **ActiveX-filtering** te klikken.



Er komt dan een vinkje ✓ voor te staan ten teken dat het ingeschakeld is.. Op dezelfde wijze kunt u ActiveX-filering ook weer uitzetten, dan sataat er geen vinkje ✓ bij.

4. SmartScreen-filter

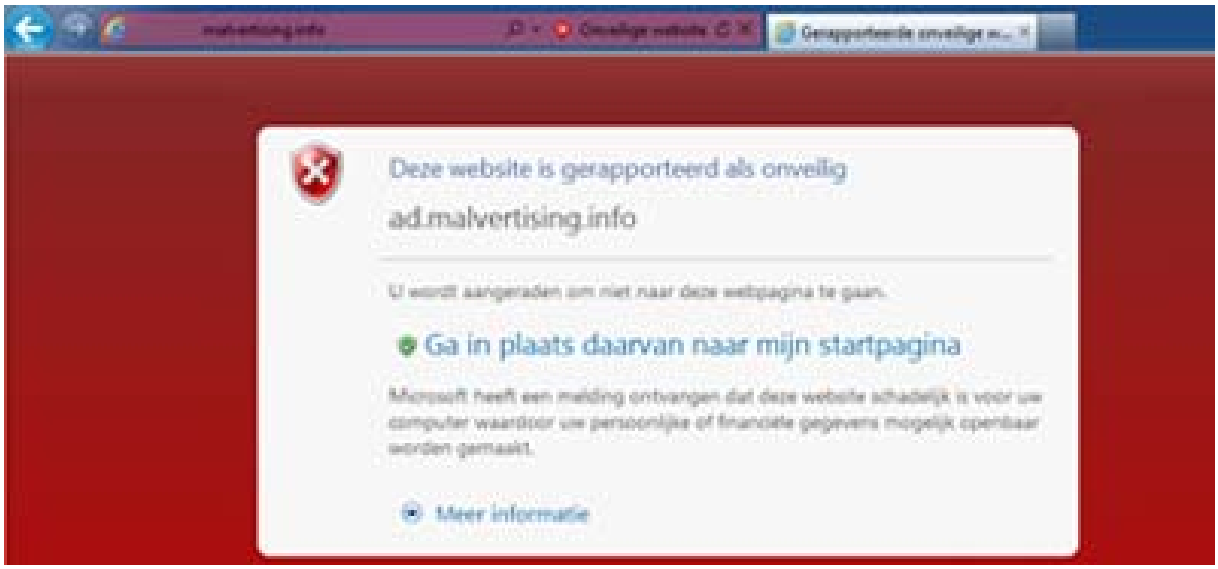
Internet Explorer is ontworpen om u te beschermen tegen de steeds omvangrijker wordende dreigingen op internet en bij social engineering. De dreigingen kunnen bestaan uit koppelingen in een e-mail die afkomstig lijkt van uw bank, nepmeldingen van sociale netwerksites, zoekresultaten voor populaire inhoud of schadelijke advertenties. U kunt het zo gek niet bedenken of het wordt uitgeprobeerd.

Met SmartScreen-filter kunt u veiliger browsen in de gedachte dat u beter beschermd bent ingeval u het doelwit wordt van deze aanvallen.

SmartScreen-filter bestrijdt deze dreigingen met een aantal geavanceerde hulpmiddelen.

- **Bescherming tegen phishing** − voor het screenen van bedreigingen afkomstig van misleidende websites die persoonlijke gegevens willen verzamelen, zoals gebruikersnamen, wachtwoorden en rekeninggegevens.
- **Application Reputation** − verwijdert alle onnodige waarschuwingen voor bekende bestanden en geeft dringende waarschuwingen bij risicovolle downloads.
- **Bescherming tegen malware** − helpt voorkomen dat potentieel schadelijke software uw computer infiltreert.

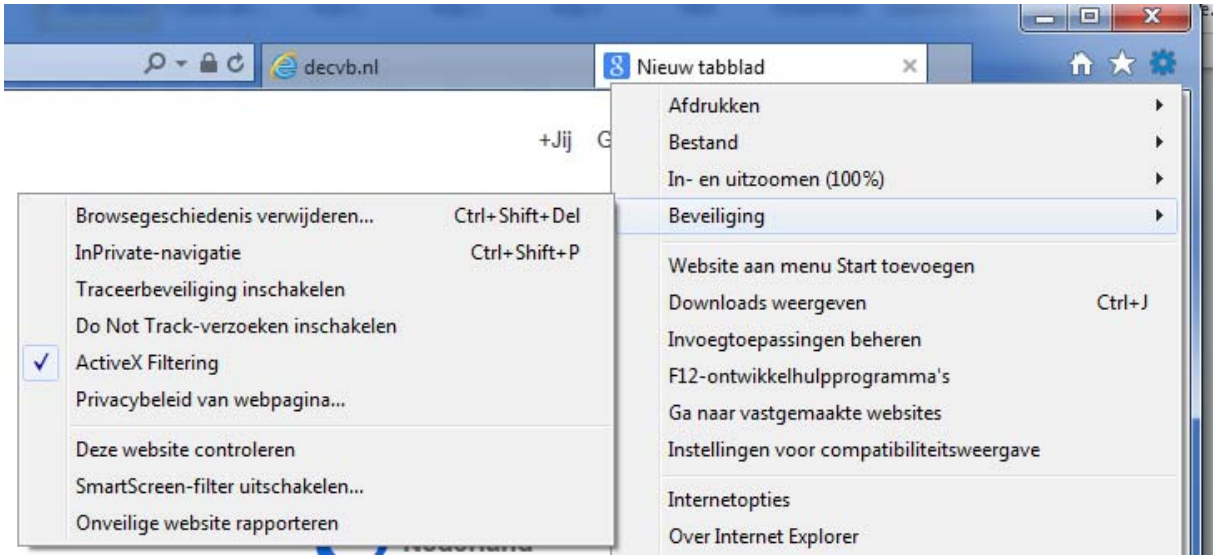
Als er een schadelijke website wordt ontdekt, zal Internet Explorer zo nodig de complete site blokkeren. Daarnaast kan het malware of phishing die wordt gehost op legitieme websites, ook "in quarantaine" plaatsen en zo de schadelijke pagina's blokkeren zonder de rest van de site te treffen.



Smartscreen-filter werkt ook samen met Downloadbeheer om u te beschermen tegen schadelijke downloads. Potentieel riskante downloads worden direct geblokkeerd. Downloadbeheer geeft duidelijk aan of een programma een groot risico vormt, zodat u zelf kunt beslissen of u het wilt wissen, uitvoeren of opslaan.

Het Smartscreen filter kent drie kleuren: **ROOD** = onveilig, **GROEN** = veilig en **ORANJE** = (nog) niet gecontroleerd. U kunt die website dan eerst controleren voor u verder gaat (zie **Website controleren**).

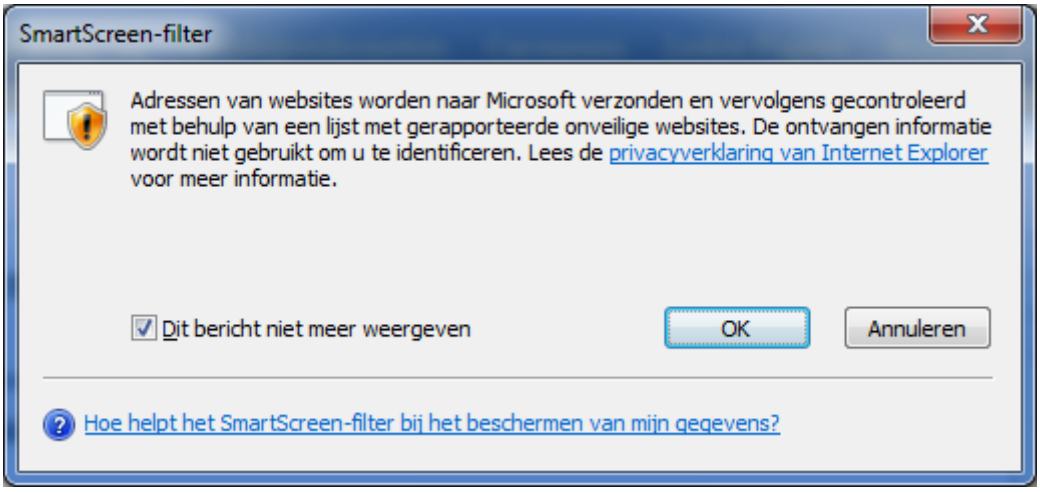
Controleer of in uw Internet Explorer het **SmartScreen-filter** ingeschakeld is door op de knop **Extra** (het radarwieltje) te klikken, vervolgens **Beveiliging** aan te wijzen en in het volgende menu **SmartScreen-filter uitschakelen** vermeld staat. Dit betekend dat het **SmartScreen-filter** ingeschakeld is.



Door op de tekst **SmartScreen-filter uitschakelen** te klikken kunt het weer uitschakelen, maar ik raad u in uw eigen belang aan om het ingeschakeld te laten. Anders kan het u duur komen te staan!!!!!

5. Website controleren

Komt u tijdens het surfen en op een website terecht die niet vertrouwd, maar ook niet door het **SmartScreen-filter** als onveilig wordt aangemerkt of dat u het **SmartScreen-filter** uitgeschakeld heeft**,** dan kunt u de betrouwbaarheid controleren door op knop **Extra** (het radarwieltje) te klikken, vervolgens **Beveiliging** aan te wijzen en in het volgende menu op **Deze website controleren** te klikken.



Zoals u ziet heeft Microsoft heel wat beveiligingsopties in Internet Explorer ingebouwd maar zo als met alle zaken behoudt zelf een gezonde dosis wantrouwen en klik niet klakkeloos op allerlei linken, want voor u het weet……..

Cookies

Sinds enige jaren zijn websites verplicht u om toestemming te vragen, alvorens zij Cookies over uw surfgedrag op uw computer mogen vastleggen.

Ook de Consumentenbond die onderzoek heeft gedaan naar het gebruik van Cookies houdt zich, zoals u hiernaast kunt zien aan deze wettelijke regeling.

Uit onderzoek van de Consumentenbond blijkt dat websites op grote schaal surfgegevens aan elkaar doorspelen, via zogeheten cookies op de pc. Tvgids.nl staat op kop met 68 cookies van 'derde partijen' die meekijken tijdens het surfen. Wat zijn cookies en hoe werken ze?

Een cookie (ook wel een HTTP cookie genoemd) is een klein tekstbestandje dat een website op de harde schijf van je computer zet op het moment dat je de site bezoekt. De belangrijkste functie van cookies is om de ene gebruiker van de andere te onderscheiden. Je komt cookies dan ook veel tegen bij websites waarbij je moet inloggen. Een cookie zorgt er dan voor dat je ingelogd blijft terwijl je de site gebruikt.

Looptijd van cookies

Cookies hebben een looptijd. Sommige cookies worden verwijderd als je je browser afsluit. Andere (bijvoorbeeld die met inloggegevens) kunnen jaren op je computer blijven staan als je ze niet verwijdert.
Je kunt meestal niet zien waar een cookie precies voor dient. Cookies zijn tekstbestandjes, maar de inhoud van die bestandjes is meestal onleesbare computercode. De echte gegevens over je staan dan in de database van de website.

Advertenties op maat

De mogelijkheid om gebruikers te identificeren en te volgen is voor veel websites waardevol. Door te volgen wat voor pagina's de gebruiker bezoekt, kan het aanbod aan de gebruiker worden aangepast. Denk aan webwinkels die producten 'aanraden'.

Cookies van derden

Sommige websites staan toe dat andere websites ook cookies kunnen plaatsen op de pc van de gebruiker. Dat soort cookies noemen we *cookies van derden* (3rd party cookies).

Tracking cookies

Hoe werkt dit? Een website (A) kan bijvoorbeeld een adverteerder toestemming geven om een cookie te plaatsen. Die adverteerder weet dan ook dat je de website of pagina hebt bezocht. Het echte voordeel voor die derde partij (de adverteerder) ontstaat als de gebruiker ook op een andere site (B) komt die ook toestemming heeft gegeven aan de adverteerder om cookies te plaatsen. De adverteerder kan het cookie van site A dan uitlezen, en op die manier weet de adverteerder dat deze gebruiker zowel sites A en B bezocht heeft. En hij heeft meer informatie dan website A of B los van elkaar over de gebruiker hebben.
Cookies die het 'volgen' van mensen mogelijk maken, noemen we tracking cookies.

Flash Cookies

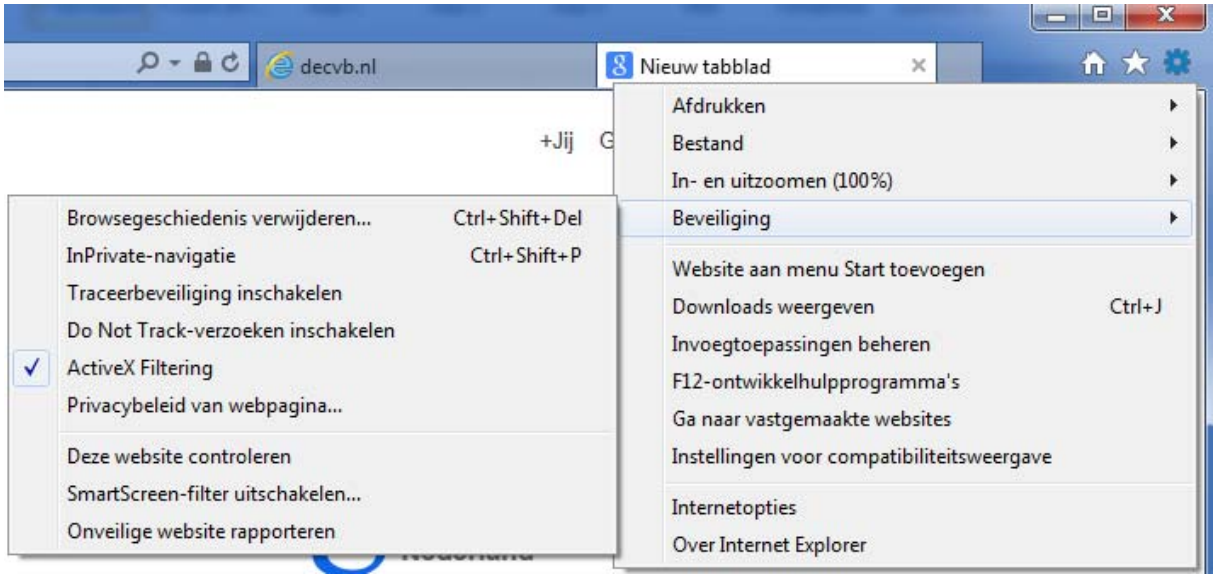
Flashcookies zijn een ander soort cookies die gebruik maken van Adobe Flash, een techniek om websites mooier weer te geven. Vroeger waren ze lastig te verwijderen en niet tegen te houden. Door medewerking van Adobe behandelen de nieuwe generatie browsers (vanaf 2011) flashcookies wel gewoon als gewone cookies, en worden ze dus op verzoek ook geblokkeerd en verwijderd. Sinds Adobe Flash versie 10.3 is dat mogelijk. Deze Flash-versie is beschikbaar sinds medio 2011. Om veiligheidsredenen is het belangrijk om Adobe Flash zo in te stellen dat deze altijd bijgewerkt blijft naar de nieuwste versie. De nieuwste Flash-speler is te downloaden van: http://www.adobe.com/nl/ .

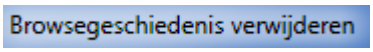
Cookies wel- of juist niet accepteren

Internet Explorer biedt verschillende mogelijkheden om de cookies te beheren die op uw computer zijn opgeslagen. U kunt cookies blokkeren of toestaan, of u kunt specifieke sites opgeven waarvan u cookies wilt accepteren. Wanneer u dit soort wijzigingen aanbrengt, heeft dit geen invloed op de cookies die al op uw computer zijn opgeslagen. Het is dus raadzaam om eerst alle cookies die al op de computer zijn opgeslagen, te verwijderen, voordat u de volgende stappen uitvoert.

Cookies verwijderen

Klik op de knop **Extra** (het radarwieltje) en wijs vervolgens **Beveiliging** en klik in het volgende menu **op Browsergeschiedenis verwijderen…**



In het nieuw geopende venster Browsergeschiedenis verwijderen 

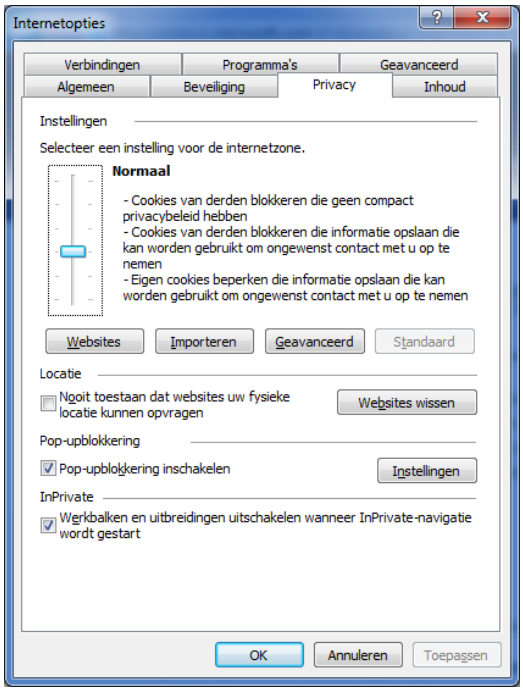
staan standaard al vier vinkjes ✓, die u laat staan. Het volstaat om onderin te klikken op de knop 

om niet alleen alle “oude” cookies te verwijderen, maar ook de tijdelijke internet bestanden en de geschiedenis (welke websites u in de afgelopen periode heeft bezocht).

Alle cookies blokkeren of toestaan

- Klik in Internet Explorer op de knop **Extra** en klik vervolgens op **Internetopties**.
- Klik op de tab **Privacy** en verplaats onder **Instellingen** de schuifregelaar naar boven om alle cookies te blokkeren of naar beneden om alle cookies toe te staan. Klik vervolgens op **OK**.

Als u alle cookies blokkeert, worden sommige webpagina's mogelijk niet meer juist weergegeven.



Cookies blokkeren op basis van type

In plaats van cookies van specifieke websites te blokkeren of toe te staan, kunt u ook bepaalde algemene typen cookies opgeven die u wilt toestaan. U kunt er bijvoorbeeld voor kiezen om cookies toe te staan van websites die een privacy beleid hanteren, of om cookies te blokkeren van websites die zonder uw toestemming persoonlijke gegevens opslaan. Meer informatie over de verschillende typen cookies vindt u in.

- Klik in Internet Explorer op de knop **Extra** en klik vervolgens op **Internetopties**.
- Klik op de tab **Privacy**, verplaats de schuifregelaar naar het gewenste privacy niveau en klik op **OK**.

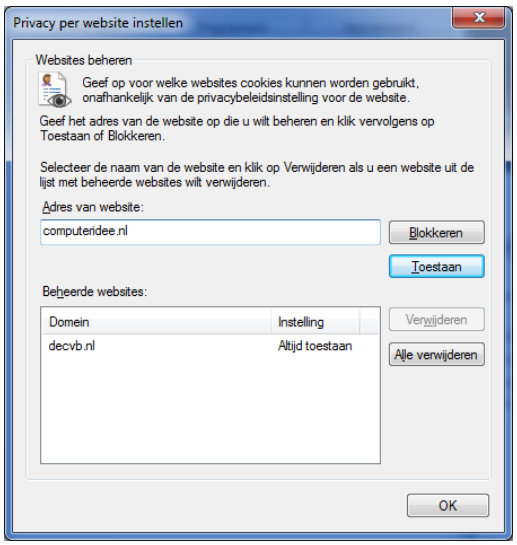
Terwijl u de schuifregelaar verplaatst, wordt een beschrijving gegeven van de typen cookies die op dat privacy niveau worden geblokkeerd of toegestaan.

Cookies van bepaalde websites blokkeren

- Klik in Internet Explorer op de knop **Extra** en klik vervolgens op **Internetopties**.
- Klik op de tab **Privacy** en plaats de schuifregelaar op een positie tussen het bovenste en onderste niveau, zodat u niet alle cookies blokkeert of toestaat.
- Klik op **Websites**.
- Typ het adres van een website in het vak **Adres van website** en klik op **Blokkeren** of **Toestaan**.

  Terwijl u typt, wordt een lijst weergegeven met de webpagina's die u al hebt bezocht. U kunt op een adres klikken om dit weer te geven in het vak **Adres van website**.

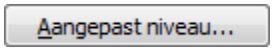
- Herhaal stap 5 voor elke website die u wilt blokkeren of toestaan. Klik op **OK** als u klaar bent.
- Plaats de schuifregelaar weer op de oorspronkelijke positie en klik op **OK**.



Beveiligde modus

Als u in Internet Explorer op de knop **Extra** klikt en vervolgens op **Internetopties** en daarna in het venster Internetopties op het tabblad Beveiliging, controleert u of een vinkje ✓ geplaatst is bij de optie **Beveiligde modus inschakelen (hiervoor moet Internet Explorer opnieuw opgestart worden**).

Staat er geen vinkje ✓ bij, dan moet u daar een vinkje ✓ plaatsen en Internet Explorer afsluiten en opnieuw openen.

Op hetzelfde tabblad kunt u door op de knop Aangepast niveau 

te klikken nog meer instellingen aanpassen, maar dat heeft alleen zin als u ter zake deskundig bent en terdege weet wat de gevolgen daarvan zijn.

Schroeft u de beveiliging te hoog op, dan zult u vrijwel niets meer kunnen doen op internet.

U hoeft ook lang niet altijd Cookies te accepteren. U merkt vanzelf of u de betreffende website verder kunt bekijken en doorzoeken of dat u niet verder komt. In dat geval kan u altijd nog overwegen of het bekijken en doorzoeken van de bewuste website belangrijk genoeg is om de cookies alsnog te accepteren.

In dat geval opent u die bewuste website opnieuw en accepteert u alsnog cookies.

Er valt nog veel meer te vertellen over Internet & Privacy, maar daarvoor ontbreekt de tijd.

Heeft u, nu of later nog vragen over dit onderwerp, dan kunt u die per mail aan mij voorleggen.

De bekendste vorm van computercriminaliteit is het **opzettelijk en wederrechtelijk binnendringen** in een computersysteem of netwerk. Dit heet computervredebreuk (soms ook wel computerinbraak of **hacken**) en is een misdrijf. Hierop staat een straf van maximaal 1 jaar cel of geldboete van 16.750 euro (art. 138ab lid 1). Wilt u hier meer over weten, bekijk dan eens de info over Computervredebreuk c.q. hacken op deze site:
http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/computervredebreuk/

Andries Vermeulen
Redacteur en Vicevoorzitter van de CVB
redactie@decvb.nl