Advertenties blokkeren om pagina's sneller te laden

Als u advertenties te blokkeren, zal webpagina's sneller laden en kijk schoner.Door het blokkeren van advertenties, kunt u ook de bron van vele volgen van cookies blokkeren.

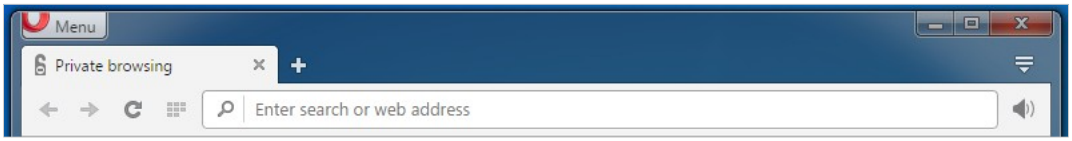
Om advertenties te blokkeren:

1. Vanuit het hoofdmenu, selecteer **Instellingen** .
2. Klik op **Privacy en veiligheid** op de zijbalk.
3. Onder **Advertenties blokkeren** , vinkt u het **blokkeren advertenties en surfen op het web tot drie keer sneller** schakelen.

Klik op de **Beheren Uitzonderingen** knop om site-specific voorkeuren in te stellen. Standaard zijn een paar sites niet geblokkeerd.

Wanneer ad blocking is ingeschakeld, ziet u een zien badge in de gecombineerde zoek- en adresbalk. Klik op de badge voor meer informatie, met inbegrip van het aantal geblokkeerde advertenties, een snelheidstest en een site-specific switch voor het ontstoppen advertenties.

Blijf veilig met private browsing



Private browsing zorgt ervoor dat uw internet geschiedenis en de activiteit zodra u alle particuliere vensters te sluiten worden verwijderd.

Om privé te bladeren, selecteer **Nieuwe particuliere window** in het hoofdmenu. Wanneer u alle particuliere vensters te sluiten, zal Opera de volgende bijbehorende gegevens te wissen:

- Browsegeschiedenis
- Items in de cache
- koekjes

Na te zijn gesloten, kan een eigen tabblad of venster niet worden verhaald op de **Onlangs gesloten** lijst in het menu tabblad.

Terwijl de particuliere ramen hebben geen record van de websites die u bezoekt, als je opzettelijk gegevens op te slaan, bijvoorbeeld als je een item op te slaan op uw Speed Dial, slaat een wachtwoord of downloaden van een bestand te verlaten, zal het nog steeds zichtbaar zijn nadat het venster is gesloten .

Privégegevens

Standaard, Opera bevat bepaalde browsing gegevens te helpen versnellen verbindingen, laadt gemeenschappelijke pagina-elementen, en in het algemeen communiceren beter met de sites die u

bezoekt. Misschien wilt u sporen van uw surfgedrag te verwijderen door het opruimen van uw persoonlijke gegevens.

Om privégegevens te wissen:

1. Vanuit het hoofdmenu, selecteer **Meer hulpmiddelen** > **Browsegegevens wissen** .
2. Selecteer de periode waarin u wilt geschiedenis items met behulp van de te verwijderen **Obliterate de volgende items van** drop-down menu.
3. Vink de selectievakjes naast de specifieke browsing gegevens die u wilt verwijderen.
4. Klik op **Browsegegevens wissen** .

Clearing surfgeschiedenis zal alle opgeslagen locatie-informatie over de pagina's die u hebt bekeken en de tijden die u hen toegang te verwijderen.

Clearing downloaden geschiedenis zal record van de bestanden die u via de browser hebt gedownload Opera's legen. Dit zal het bestand niet verwijderen uit uw lokale computer, maar het record van wanneer en waar je het gedownload.

Cookies verwijderen en andere sitegegevens zullen alle bijgehouden site data te verwijderen. Lees meer over het beheren van cookies .

Het legen van het cachegeheugen van uw browser zal geen tijdelijk opgeslagen gegevens verwijderen uit websites. De cache wordt gebruikt om tijdelijk op te slaan pagina-elementen, zoals afbeeldingen of zoekopdrachten, dus als je wilt weer toegang tot de site, kunt u laadtijden te verminderen. Het legen van deze cache zal duidelijk ruimte op uw lokale schijf.

Het wissen van gegevens van gehoste apps worden alle gegevens die zijn opgeslagen door de extensies die u in de browser geïnstalleerd te verwijderen.Bijvoorbeeld, als u een extensie weer aan snelkeuze en stel uw locatie in de instellingen, het wissen van deze gegevens zal de uitbreiding naar de standaardinstellingen te resetten geïnstalleerd en moet u de extensie opnieuw uw plaats vertellen.

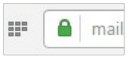
Let op: Zorg ervoor dat u nuttige gegevens per ongeluk wissen. Als u nog niet vertrouwd mee, probeer privé browsen. De gegevens voor privé browsen wordt automatisch gewist wanneer u alle particuliere vensters te sluiten.

Beheren hoe Opera winkels kunnen prive-gegevens nuttig zijn, als een alternatief voor het opruimen van alle privégegevens. Lees meer over het instellen van web voorkeuren .

Gebruik badges pagina veiligheid en meer vast te stellen

Opera waarschuwt u voor verdachte pagina's door het controleren van de pagina die u aanvragen tegen een database van bekende "phishing" en "malware" websites. Om jezelf te beschermen bij het invoeren van gevoelige informatie, altijd op zoek naar de sluis in de beveiliging badge.

Badges geven details over de pagina die u bekijkt. Wanneer een badge in uw gecombineerde zoek- en adresbalk verschijnt, klik erop om meer informatie, met inbegrip van beveiligingscertificaten en nog veel meer te zien.



Icoon	Geeft ...
	Versnelde (Turbo) verbinding
	Advertenties worden geblokkeerd
	cameratoegang
	Uitbreiding
	Fraude of malware waarschuwing
	lokaal bestand
	toegang locatie
	toegang microfoon
	MIDI toegang
	Opera pagina
	beveiligde verbinding
	onbeveiligde verbinding
VPN	VPN is

Wanneer de verbinding veilig is, wordt een slot weergegeven in de beveiliging badge, wat inhoudt dat niemand anders de informatie die verstrijkt tussen u en de site kunt lezen. Opera maakt gebruik van certificaten om de identiteit van de site-eigenaren te controleren. Een slot betekent dat er goede encryptie tussen u en de ontvanger, en de identiteit van de ontvanger is geverifieerd.

Als een website wordt gevonden op de zwarte lijst, wordt u gepresenteerd met een waarschuwing pagina, en u kunt beslissen of de website te bezoeken, of om te gaan om veilig terug naar de vorige pagina. Fraude en bescherming tegen malware geen vertraging bij de opening van de pagina's te veroorzaken.

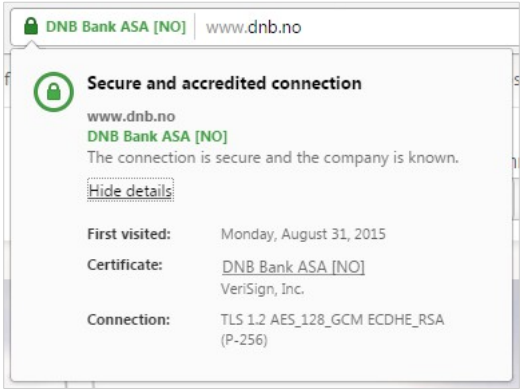
Deblokkeren en laat onveilige inhoud

Als je bekijkt op een versleutelde verbinding (`https://`), Opera controleert om ervoor te zorgen dat alle onderdelen van de site zijn gecodeerd. Als Opera herkent dat levende elementen van de pagina, bijvoorbeeld scripts, plugins, of frames, worden bediend door een open verbinding (`http://`), zal het onveilige inhoud te blokkeren. Dit betekent dat delen van de pagina mogelijk niet goed weergegeven.

Opera afraadt waardoor onveilige inhoud te laden in een versleutelde verbinding. De beste manier om uw gevoelige informatie te beschermen is om te communiceren alleen met beveiligde content. Bij Opera onveilige inhoud en blokkeert het detecteert, verschijnt er een waarschuwing in de rechterkant van de gecombineerde adres en de zoekbalk.

Als u niet de zorg over de veiligheid van uw verbinding met de site, kunt u de waarschuwing klikken om een tonen **Deblokkeren** knop. Met deze knop kan de geblokkeerde inhoud moet worden geladen op de pagina, en de veiligheid badge zal veranderen in een open hangslot te tonen, u eraan te herinneren dat je onveilige inhoud heeft toegestaan om te laten zien op een versleutelde verbinding.

Beheert u beveiligingscertificaten



Beveiligingscertificaten worden gebruikt om te controleren of een website veilig is om te gebruiken.De meeste van de tijd certificaten zijn volledig geldig. Als je een groene

hangslot security badge zien in uw gecombineerde zoek- en adresbalk, kunt u veilig doorgaan met uw browsen.

Indien u meer informatie wilt over het beveiligingscertificaat van een site, klik op de veiligheid badge en selecteer **Details** . Opera zal uitgever van het certificaat, het type certificaat en of een samenvatting van de emittent is publiekelijk bekend en geldig is.

Publiekelijk bekend emittenten en hun certificaten worden gevalideerd tegen een aantal veiligheids- en identiteitscontroles. Opera zal u waarschuwen als een deel van het certificaat van een publiekelijk bekende emittent is twijfelachtig. U kunt ervoor kiezen om door te gaan, maar Opera kan niet garanderen dat uw veiligheid.

Om beveiligingscertificaten beheren en hoe Opera omgaat met hen:

1. Vanuit het hoofdmenu, selecteer **Instellingen** .
2. Klik op **Privacy en veiligheid** op de zijbalk.
3. Onder **HTTPS / SSL** , klikt u op de **Certificaten beheren** knop.

Een opmerking over lokale certificaat emittenten

Sommige verbindingen kunnen worden gecertificeerd door certificaten van de lokale emittenten, hetzij van apps op uw machine of andere niet-openbare bronnen (zoals een lokaal intranet). De uitgevers kunnen worden gebruikt om beveiligde verbindingen in de browser te controleren. De meeste van deze verbindingen gelden. Zo kunnen debuggen toepassingen van derden beveiliging scannen, en ouderlijke filters rekenen op lokaal uitgegeven certificaten.

Connections gecertificeerd door certificaten van lokale emittenten worden niet gescreend door dezelfde veiligheidsnormen als algemeen bekende emittenten en certificaten. Een dergelijke screening is te strikt en kunnen niet toestaan verbindingen om te werken zoals bedoeld. Malware of virussen kunnen deze certificaten gebruiken om gecodeerde informatie te bekijken of te injecteren advertenties.

Als u wilt, kunt u Opera configureren om u te waarschuwen over de publieke sites die certificaten gebruik maken van lokale emittenten. Als je verder op deze verbindingen te bladeren, zich ervan bewust dat een aantal veiligheidsmaatregelen, zoals het certificaat pinning en Certificate Transparantie, zal worden uitgeschakeld voor al deze verbindingen tijdens uw browsersessie.

Vertel sites die niet aan uw activiteiten bijhouden

De meeste sites bijhouden van uw gedrag, terwijl je ze bezoekt. Als je niet van dit idee, kan Opera een extra header sturen met elk verzoek: "DNT: 1". Dit is een vlag naar websites die de gebruiker niet wil worden gevolgd. Sommige landen hebben DNT wetgeving die legaal uw verzoek en de meeste goed opgevoede websites te beschermen zal deze extra header respecteren.

U kunt Opera ingesteld op sites die u de voorkeur aan opt-out van online behavioral volgen vertellen. Om dit in te stellen:

1. Vanuit het hoofdmenu, selecteer **Instellingen** .

2. Klik op **Privacy en veiligheid** op de zijbalk.
3. Onder **Privacy** , vinkt u de **aanvraag sturen een 'Do Not Track' met je browsing verkeer** checkbox.

VPN

Normaal gesproken, uw browser rechtstreeks verbinding naar websites, waardoor websites om uw IP-adres en de locatie bij benadering te identificeren. Met VPN, u verbinding maakt met websites via een VPN-server.Daardoor uw schijnbare locatie verandert de locatie van de server.

Om VPN te schakelen:

1. Vanuit het hoofdmenu, selecteer **Instellingen** .
2. Klik op **Privacy en veiligheid** op de zijbalk.
3. Onder **VPN** , tik de **Enable VPN** checkbox.

Wanneer u VPN in te schakelen, het begint automatisch, en de blauwe VPNbadge verschijnt in de gecombineerde zoek- en adresbalk. Klik op de badge, en je krijgt een aan / uit schakelaar, informatie over de hoeveelheid gegevens die de virtuele locatie, en het virtuele IP-adres te zien.

Vanuit het point-of-view van de websites, wordt uw browser nu gevestigd in het land gegeven door de virtuele locatie. Aan uw virtuele locatie wijzigen, selecteert u een land uit de lijst. Als je niet een land te kiezen, wordt u automatisch een 'optimale locatie "toegewezen. Om VPN uit te schakelen, draait u de schakelaar.

Omdat de verbinding tussen uw browser naar de VPN-server wordt gecodeerd, zelfs als de lokale netwerk niet, VPN verbetert uw privacy op het lokale netwerk. U kunt uw het doorbladeren activiteiten te verbergen voor andere gebruikers van dat netwerk.

Om uw privacy te verbeteren met betrekking tot websites, waardoor het moeilijker voor hen om u te volgen, een combinatie van functies nodig. De kwestie is cookies . Zelfs als je je locatie te verhullen, kunnen websites die u toch identificeren als ze een cookie heeft ingesteld. Opmerking echter dat door het blokkeren van advertenties , de bron van vele volgen van cookies, en aan het einde van een blok private browsing sessie, wanneer u de browser sluit, worden alle cookies van die sessie verwijderd.

VPN is een gratis service, en de hoeveelheid gegevens die je mag overdracht is onbeperkt.