

Wil je niet dat bedrijven weten naar welke sites je surft? Met deze trucjes laat je minder sporen na op het internet.



Blokkeer (sommige) cookies

Bedrijven slagen erin om veel kennis over jou te vergaren door cookies te gebruiken. “Dat zijn virtuele post-its die op je digitale ik geplakt worden om bij te houden wie je bent”, zegt Heyman. “Ze weten in welke taal je een website bekijkt, houden een winkelwagentje bij in een webshop en onthouden wachtwoorden voor je.”

De bovenstaande voorbeelden zijn directe cookies. Daarnaast zijn er ook *third party cookies*, en daar ligt het gevaar. “Dat zijn de cookies waarmee adverteerders je surfgedrag kunnen volgen op het internet, en zien wat je aanklikt, opzoekt, koopt, ... Het is verstandig om die te blokkeren met een cookie blocker.” Voorbeelden daarvan zijn *Purify*, *Ghostery* en *uBlock Origin*. Let wel op dat je in de instellingen aangeeft dat je alleen de *third party cookies* blokkeert. “Anders gaan enkele websites, die directe cookies nodig hebben, niet meer werken”, zegt professor Bart Preneel (KU Leuven).

Gebruik een andere zoekmachine dan Google

Met je zoekopdrachten geef je Google en adverteerders de pap in de mond: ze weten dan exact wat je zoekt. Als je een incognitovenster gebruikt voor zoekopdrachten, worden cookies automatisch verwijderd na de sessie. “Maar zeker ben je nooit”, zegt doctor Ralf De Wolf (UGent). “Als dat incognitovenster van Google is, belanden je gegevens toch bij Google. Je vertrouwt erop dat ze die verwijderen, maar je weet het niet.”

“Er zijn alternatieven”, zegt Preneel. “Duck Duck Go gebruik ik zelf bijvoorbeeld veel. Dat is een zoekmachine die je verzekert dat je informatie niet bij andere partijen belandt.” Het nadeel is wel dat minder bekende zoekmachines minder goede zoekresultaten opleveren.

Verwijder cookies, zoekgeschiedenis en locatiegegevens

Wanneer je in de instellingen van de browser je cookies, zoekgeschiedenis en locatiegegevens verwijdert, verdwijnen die. “Ik raad mensen aan om dat geregeld te doen”, zegt Preneel. Heyman waarschuwt evenwel. “Als je de post-it verwijdert, wordt bij je volgende bezoek aan die website een nieuwe aangemaakt. Je zal

dan opnieuw de vraag krijgen of de website cookies mag gebruiken. Als je de discipline niet hebt om dan aan te geven dat je ze niet wil, ben je eigenlijk niet vooruitgegaan. Dus verwijderen heeft alleen zin als je ze niet opnieuw installeert.”

Probeer Google te misleiden

Wat je kan proberen, is Google en co. op het verkeerde been zetten door valse zoekopdrachten en je profielen op allerlei webshops en sites geregeld van naam en eventueel van geslacht te veranderen. Zo is het veel moeilijker om in kaart te brengen wie je bent en wat je interesseert. “Je hebt ook tools die op alle websites automatisch alle advertenties aanklikken, waardoor het onmogelijk is om te weten wat je echt leuk vindt”, zegt De Wolf.

Die techniek werkt een beetje, zegt Preneel. “Maar je zal er heel veel moeite voor moeten doen. Ze zullen snel doorhebben dat je hen probeert te misleiden, maar als het je lukt loont het de moeite.”

Maak een lijst met wachtwoorden

Wanneer een website je vraagt om je te registreren, krijg je standaard de opties ‘Inloggen met Facebook’ en ‘Inloggen met Google’. Zo laat je hen de gegevens invullen, wat handig is: je hoeft niet nog een login en paswoord te onthouden. Toch doe je het volgens Preneel beter niet. “Je ruilt je privacy in voor gebruiksgemak.” Log je bijvoorbeeld in op een webshop met Google of Facebook, weten zij ook meteen wat je er koopt, terwijl die informatie anders binnen de webshop blijft. “Daarom is het beter om een lijst met wachtwoorden te maken en op elke site een ander te gebruiken dan Google verantwoordelijk te maken voor al je logins.”

Wie de tijd neemt om te registreren met een e-mailadres en alles invult, geeft minder gegevens prijs. “Je moet je tijd nemen als je je gegevens wilt beschermen”, aldus Heyman.

Bankieren doe je beter niet via wifi

Op niet al te goed geconfigureerde wifi-netwerk, zoals bijvoorbeeld in hotels of winkels, kan wie dat ook wil makkelijk in de gaten houden welke websites je bezoekt en wat je doet. Zo kan het hotel of de winkel die informatie bijvoorbeeld doorverkopen. “Als je gevoelige dingen doet – een overschrijving bijvoorbeeld – doe je dat beter via 3G of 4G. Een mailtje lezen is geen probleem”, zegt Preneel.

Mobiele websites in plaats van apps

Zoek je op Google de weg, dan zal het je aanmoedigen de app van Google Maps te installeren. Ook webshops maken je er graag op attent dat ze een app hebben. Ze doen dat niet zomaar. “Apps op je telefoon kunnen veel meer informatie over jou verzamelen dan wanneer je gewoon naar de mobiele website surft”, zegt Preneel. “Het is alles of niets: je hebt daar bijvoorbeeld niet de optie om cookies te blokkeren.”

De experts:

Rob Heyman (VUB), onderzoeker en privacy-expert
Bart Perneel (KU Leuven), professor data-encryptie
Ralf De Wolf (UGent), doctor verbonden aan de vakgroep communicatie

Bron: Nieuwsblad van woensdag 16 oktober 2019 (digitale weergave).