DIRKJAN VAN ITTERSUM

ONLINE PRIVACY & VEILIGHEID

editie 2015

+28 online-video's

oprecht consumentenbond

Onlineprivacy & -veiligheid

DIRKJAN VAN ITTERSUM

ONLINE PRIVACY & VEILIGHEID

editie 2015

oprecht consumentenbond

2e geheel herziene druk, september 2015

Auteur: Dirkjan van Ittersum
Verder werkten mee: Vincent van Amerongen, Peter Kulche, Yvo Verschoor
Eindredactie: Vantilt Producties, Nijmegen
Grafische verzorging: PUUR Publishers
Beeld omslag: iStock
Foto auteur: Michel Walraven

ISBN 978 90 5951 3310
NUR 988

INHOUD

INLEIDING

Digitale technieken leveren veel gemak op, maar er zijn ook gevaren. Iedereen kent wel de verhalen over slachtoffers van phishing, bij wie de hele bankrekening werd leeggeroofd. Ook op subtieler niveau is er gevaar. Uw privacy wordt continu bedreigd, of u nu surft op internet of apps downloadt. Adverteerders doen dit om u te kunnen te bestoken met 'gepersonaliseerde advertenties' zonder te vragen of u daar wel op zit te wachten. En waar wordt al die informatie precies voor gebruikt en hoe veilig wordt ze bewaard? Stel dat de informatie uitlekt: kan de verzekeraar u weigeren omdat u vaak zoekt op een bepaald ziektebeeld? Berekent een webwinkel u een hogere prijs omdat uit uw profiel blijkt dat u het wel kunt betalen? Het zijn maar een paar redenen om niet te willen dat bedrijven en overheid informatie over u verzamelen.

Omgekeerd geven we via sociale netwerken massaal vrijwillig informatie over onszelf prijs. Volgens het Centraal Bureau voor de Statistiek behoort Nederland tot de koplopers als het gaat om het gebruik van Facebook, Twitter, LinkedIn en Pinterest. Vooral het uitwisselen van berichten is populair, mede dankzij de sms-vervanger WhatsApp. Al deze netwerken bouwen in meer of mindere mate profielen van gebruikers op.

Gelukkig kunt u uw privacy beschermen. Denk goed na over wat u op internet zet. De gouden regel is: als het niet mag uitlekken, hoort het niet op internet. Daarnaast kunt u privacyinstellingen optimaal instellen om ongenode gasten

Als informatie niet mag uitlekken, hoort ze niet op internet thuis

(of het nou hackers of adverteerders zijn) buiten de deur te houden. In dit boek leggen we uit met welke gevaren u rekening moet houden en hoe u zich zo goed mogelijk beschermt.

Dit boek staat vol met tips en stappenplannen. Daarbij verwijzen we regelmatig naar filmpjes op onze website. Als een stappenplan is voorzien van een video-icoon, kunt u op www.consumentenbond.nl/onlineprivacy-videos terecht voor een instructiefilmpje.

Tot slot: onlineprivacy is volop in beweging. Webdiensten passen regelmatig hun beleid en werkwijze aan. Het kan daarom voorkomen dat bepaalde tips en instructies in dit boek inmiddels achterhaald zijn of op een net iets andere manier werken.

Ook op onze website vindt u veel informatie over onlineprivacy en -veiligheid. Zie www.consumentenbond.nl/internet-privacy en www.consumentenbond.nl/veilig-online.

Komt u in dit boek begrippen tegen waar u wat meer over wilt weten? Kijk dan eens naar de woordenlijst op www.digitaalgids.nl.

Dirkjan van Ittersum is webondernemer, IT-journalist en auteur van computerboeken. Hij geeft graag uitleg over de mogelijkheden van nieuwe technologie.

1

PRIVACY

Over privacy wordt soms lacherig gedaan. Ten onrechte, want er zijn serieuze gevaren voor wie niet goed oplet wat hij op internet zet. In dit hoofdstuk leggen we uit waarom privacy belangrijk is en hoe de wettelijke bescherming is geregeld.

1.1 Hoezo privacy?

Het belang van privacy wordt nog weleens afgedaan met de opmerking: 'Ik heb toch niets te verbergen.' Maar privacy is voor iedereen belangrijk, ook als u ogenschijnlijk niets te verbergen heeft.
Stelt u zich eens voor dat uw hele handel en wandel zichtbaar is voor vreemden en uw naaste omgeving. Al uw zoekopdrachten van het afgelopen jaar. Heeft u daar echt geen moeite mee? Privacy is het recht met rust gelaten te worden, los van het feit of je iets te verbergen hebt. Dat geldt ook online.
Een extra probleem met onlineprivacy is dat informatie niet zomaar weg is. Iets staat snel online, maar het van internet halen gaat niet zo makkelijk (zie par. 1.4). Bovendien kan iets wat nu onschuldig is in de toekomst een probleem vormen. Een 'grappige' foto van een uit de hand gelopen feestje kan bijvoorbeeld een sollicitatie laten stuklopen.
Het wordt pas echt vervelend als gegevens die niets met elkaar te maken hebben, gekoppeld worden. Bezoekt u wel eens activistische websites? Dan kunnen inlichtingendiensten u als verdacht persoon markeren. Foute conclusies zijn vlug getrokken. Zie dat maar eens recht te zetten.

Veel overheden luisteren massaal af, al is de praktijk omstreden. In mei 2015 lag de Amerikaanse regering onder vuur door plannen voor een verplicht achterdeurtje in sterke encryptie. President Obama pleit daarvoor, maar veel technologiebedrijven zijn tegen.

Op internet hebben we vaak niet in de gaten dat we worden afgeluisterd en we weten al helemaal niet wat er met de informatie gebeurt. Alleen dankzij klokkenluider Edward Snowden weten we het een en ander over de National Security Agency (NSA). Deze Amerikaanse veiligheidsdienst zou een directe lijn hebben met bedrijven als Google, Microsoft, Facebook en Apple. Alle commotie over de NSA heeft ervoor gezorgd dat de Amerikaanse overheid iets voorzichtiger is geworden met het massaal afluisteren van Amerikanen, maar gegevens over buitenlanders (ook wij dus) zijn in Amerika nog steeds vogelvrij.

Wat kunt u zelf doen?

Onlineprivacy begint bij uzelf. In een gesprek zijn woorden snel vervlogen, maar op internet blijft informatie lang staan

en kan ze bij personen terechtkomen waarvoor ze niet bedoeld is. Het is zaak uw gezond verstand te gebruiken. Enkele algemene tips:

- Zet niets online dat niet in verkeerde handen mag vallen. Dus ook niet in een e-mail of een afgeschermde omgeving.
- Bedenk altijd dat u informatie makkelijk online zet, maar lastig offline kunt halen.
- Maak privégegevens niet openbaar.
- Houd rekening met de privacy van anderen. Zet geen foto's of filmpjes van anderen online zonder toestemming.
- Gebruik voor ieder account een ander, sterk wachtwoord (zie par. 2.2a).
- Gebruik een versleutelde verbinding als u zeker wilt weten dat anderen niet meekijken. Versleuteling is de enige remedie tegen spiedende overheden en bedrijven (zie par. 2.4).

De cloud

Tegenwoordig kunt u via steeds meer diensten uw bestanden opslaan in 'de cloud'. Uw gegevens worden dan op internet opgeslagen. Het voordeel is dat u er altijd bij kunt, maar het nadeel is dat uw gegevens kwetsbaarder zijn dan wanneer u ze op uw eigen computer bewaart. Ook al zijn de bestanden beveiligd met een wachtwoord. In hoofdstuk 4 gaan we dieper in op de cloud.

Opensourcesoftware

Door opensourcesoftware te gebruiken, is de kans groter dat uw privacy wordt beschermd. De broncode van deze software is openbaar, waardoor het lastig is voor overheden of bedrijven om stiekem achterdeurtjes in te bouwen om mee te kijken. Bekende opensourceprogramma's zijn Linux, Firefox en OpenOffice.

1.2 De gevaren

Wat zijn eigenlijk de gevaren die u loopt op internet? De meeste mensen hoeven van inlichtingendiensten niet veel kwaad te verwachten. Tenzij ze u specifiek op het oog hebben, heeft u van hen niet veel last. We bespreken hierna andere, meer reële gevaren.

Oplichting en identiteitsfraude

Hackers zijn meestal uit op uw geld. Een virus boekt bijvoorbeeld achter uw rug om geld over naar een andere rekening. Een hacker kan zich ook voor u uitgeven, dat noemen we identiteitsfraude. Een goede beveiliging beperkt het risico op oplichting en identiteitsfraude (zie hoofdstuk 2).

Reputatieschade

Een sociaal risico is reputatieschade. Als u een foto of bericht online zet, kunt u er nog lang door achtervolgd worden. U kunt zelf veel ellende voorkomen door voorzichtig om te gaan met sociale netwerken (zie hoofdstuk 5), maar het wordt al lastiger als een ander bewust of onbewust iets over u heeft geplaatst. U kunt proberen de informatie te verwijderen (zie par. 1.4). Er is sprake van laster als iemand bewust kwalijke berichten verspreidt. Zeker als het van uzelf afkomstig lijkt, bijvoorbeeld doordat een rancuneuze ex-partner uw wachtwoord weet. Dan is er sprake van identiteitsdiefstal.

Verzamelen persoonsgegevens

De datahonger van webdiensten en andere bedrijven is niet direct schadelijk, maar wel een aantasting van uw privacy. Met cookies, apps en andere technieken verzamelen en verhandelen ze onze privégegevens. In de volgende hoofdstukken gaan we hier dieper op in.

Misbruik van uw computer en internet

U hoeft niet zelf het doelwit te zijn van hackers of spionagediensten. Veel computers worden gehackt om als springplank te dienen om andere computergebruikers te bestoken met spam of aanvallen. Ze zijn dan onderdeel van een botnet.