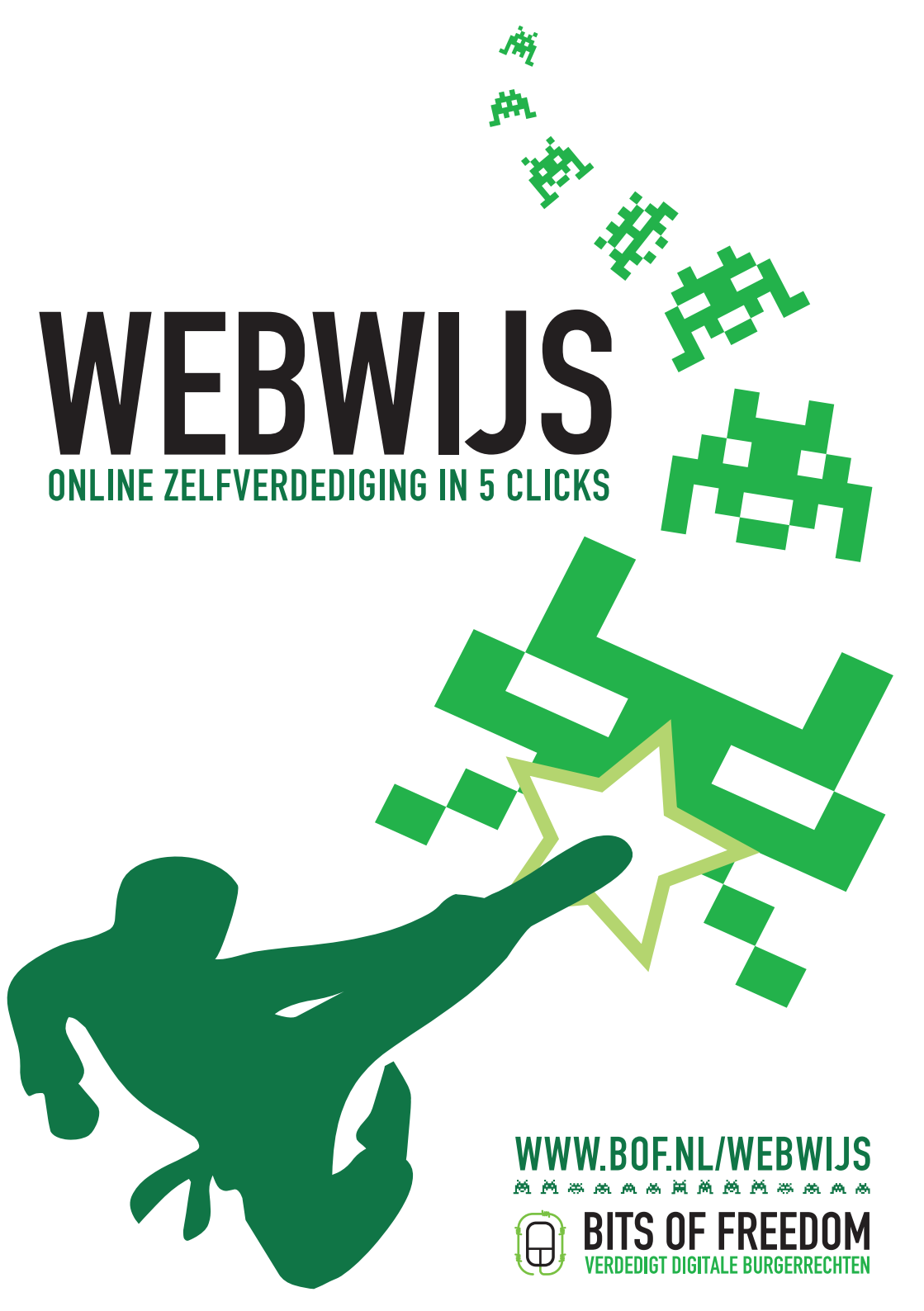
WEBWIJS

ONLINE ZELFVERDEDIGING IN 5 CLICKS



WWW.BOF.NL/WEBWIJS

BITS OF FREEDOM

VERDEDIGT DIGITALE BURGERRECHTEN

WEBWIJS – ONLINE ZELFVERDEDIGING IN 5 CLICKS
IS EEN INITIATIEF VAN

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

WEBWIJS

03/20

WEBWIJS

ONLINE ZELFVERDEDIGING IN 5 CLICKS

WAAROM WEBWIJS?

Waarschijnlijk gebruik jij het internet iedere dag. Maar internetgebruik is niet zonder problemen: dagelijks worden computers besmet door virussen, de inbox van je e-mail overspoeld door spam en privégegevens misbruikt. Denk je dat het duur, moeilijk of zelfs onmogelijk is om dit te voorkomen? Dan heb je het mis!

Digitale burgerrechtenbeweging Bits of Freedom heeft de gids Webwijs – Online Zelfverdediging in 5 clicks ontwikkeld. Ontdek in 5 clicks hoe je jezelf beschermt tegen de meest voorkomende problemen. Webwijs internetten is namelijk simpel, gratis en kost weinig tijd.

WAAROM ZOU IK?

Virussen, spammers en identiteitsdieven richten vooral schade aan bij de makkelijkste prooien. Als je slim bent, voorkom je dat jij die makkelijkste prooi bent. Dan geniet je nog steeds van alle mogelijkheden, maar heb je veel minder kans op schade.

Met Webwijs internetten help je niet alleen jezelf. Je doet je collega's, vrienden en familie ook een groot plezier. Want spam en virussen verspreiden zich meestal onder mensen die elkaar kennen. Deel de gids met je omgeving. Dan zijn jullie allemaal beter af.

ONLINE ZELFVERDEDIGING IN 5 CLICKS

In samenwerking met experts van Security.nl en dexlab.nl, ontwikkelde Bits of Freedom vijf simpele 'clicks'. Met deze vijf clicks geeft iedere internetter een verstandige impuls aan zijn online zelfverdediging:

Click 1 – IJzersterke wachtwoorden
bof.nl/click1
Click 2 – Een beveiligde computer
bof.nl/click2
Click 3 – Tijdelijke e-mailadressen
bof.nl/click3
Click 4 – Privacy op Facebook
bof.nl/click4
Click 5 – Anoniem Googlen
bof.nl/click5

AAN DE SLAG!

Ga direct aan de slag op de website van Bits of Freedom. Webwijs – Online Zelfverdediging in 5 clicks verschijnt ook als folder, die je gratis kunt downloaden en verder verspreiden. En als poster, die je in één oogopslag een rondleiding geeft langs de vijf clicks. Deel de folder uit, hang de poster op. Bij je werk, in het internetcafé of in je klas.

Website: *bof.nl/webwijs*
Folder: *bof.nl/webwijsfolder*
Poster: *bof.nl/webwijsposter*

Het is aan te raden steeds de website erbij te houden. In de tekst wordt namelijk vaak gelinkt naar instructiefilmpjes, uitleg op andere websites en achtergrondinformatie. Via de website hoef je alleen maar te clicken op de link, in plaats van de hele tekst over te nemen in je webbrowser.

SMAAK TE PAKKEN? CLICK VERDER!

Ben je door de eerste vijf stappen gekomen? Gefeliciteerd, je hebt je online zelfverdediging een flinke boost gegeven! Als je benieuwd bent geraakt naar nog meer maatregelen, click dan verder voor aanvullende maatregelen op het gebied van surfen, e-mail, sociale media, bellen/chatten en downloaden.

Click verder: *bof.nl/clickverder*
Surfen: *bof.nl/surfen*
E-mail: *bof.nl/email*
Sociale media: *bof.nl/socialemedia*
Bellen/Chatten: *bof.nl/bellenchatten*
Downloaden: *bof.nl/downloaden*

SCHRIJF MEE AAN DE WIKI VAN WEBWIJS

Het kan natuurlijk gebeuren dat nieuwe ontwikkelingen om nieuwe maatregelen vragen. Via de wiki van Bits of Freedom houden wij samen met jullie de gids actueel. Dat werkt precies hetzelfde als Wikipedia, iedereen kan de wiki lezen en er aan meeschrijven. Als je tijd en zin hebt, surf dan naar onze wiki en bouw mee aan de volgende gids!

Wiki Webwijs:
http://wiki.bof.nl/wiki/Webwijs

HULP NODIG? HELP ELKAAR IN DE REACTIES

Mocht je bij het zelfverdedigen hulp nodig hebben, kijk dan eerst of je een antwoord kan vinden op je vraag bij de wiki. Anders kun je op iedere pagina van de webgids vragen stellen via de 'reacties' onderaan. En als het je gemakkelijk afging, kijk dan eens in de reacties of je anderen kunt helpen. Bits of Freedom is een kleine organisatie en kan niet garanderen iedere individuele gebruiker te helpen. Maar wij zullen ons wel inzetten voor zoveel mogelijk ondersteuning, en daarbij gebruik maken van onze brede groep vrijwilligers. Wat ook helpt, is je vraag te stellen aan je zoekmachine. Meestal is het antwoord op je vraag ergens op internet te vinden.

CLICK 1

IJZERSTERKE WACHTWOORDEN

HOUD MEEGLUURDERS EN HACKERS BUITEN DE DEUR. GEBRUIK IJZERSTERKE WACHTWOORDEN.

WAAROM ZOU IK?

Of het nu gaat om je e-mail, Hyves of internetbankieren – je hebt een wachtwoord nodig. Dit wachtwoord is de sleutel tot je persoonlijke informatie en houd je geheim voor anderen.

Je wilt namelijk niet dat bijvoorbeeld je werkgever je persoonlijke mailtjes leest. En je wilt al helemaal niet dat een hacker uit jouw naam mailtjes naar anderen stuurt. Of zelfs iets uit jouw naam kan kopen en je bankrekening kan plunderen. Dit noem je identiteitsfraude, een ernstige vorm van criminaliteit die helaas razendsnel toeneemt. Behalve veel geld, kan een hack ook ernstige emotionele schade met zich brengen: als de overheid per abuis denkt dat je een crimineel bent.

Met een zwak wachtwoord ben je een makkelijk doelwit. Toch gebruiken veel mensen een wachtwoord dat eenvoudig te raden of kraken is. Zoals '123456' of de naam van een partner of hond. Bovendien gebruiken veel mensen voor alles hetzelfde wachtwoord, wat extra onveilig is. Om meegluurders en hackers buiten de deur te houden, gebruik je dus verschillende ijzersterke wachtwoorden.

STAP I. BEDENKEENLANGEZIN

Maak een zin, die bestaat uit verschillende woorden. Onderzoek toont namelijk aan dat je dit soort zinnen makkelijk onthoudt, terwijl een ander zo'n zin weer moeilijker kan raden of kraken.

Bijvoorbeeld:
• 'groenekikkerszijnmooi'
• 'blijmetmijnkuifjecollectie'
• 'inderegendoeikeendansje'

Maak de zin niet té lang, want bij sommige diensten mogen wachtwoorden maar een maximum aantal karakters hebben. Het toevoegen van cijfers, vreemde karakters en hoofdletters maakt de lange zin veiliger en kan verplicht zijn. Het is ook belangrijk dat de zin niet als geheel in het woordenboek staat, omdat de zin dan makkelijker geraden kan worden door hackers. Gebruik dus geen spreekwoorden. En: plak de zin nooit met een papiertje op je beeldscherm!

STAP II. EZELSBRUGGETJE PER GEVAL

Aangezien voor bijna alles een wachtwoord nodig is, kan het onthouden van al die wachtwoorden per specifieke dienst lastig zijn. Verzin daarom een ezelsbruggetje: vul de lange zin aan met een woord of teken, dat bij de specifieke website of dienst past.

Stel: 'mooieblauweluchtover' is je lange zin. Het ezelsbruggetje voor een hotmailaccount zou kunnen zijn: 'mooieblauweluchtoverhotmail'.

STAP III. PAS JE NIEUWE WACHTWOORD TOE

Nu moet je jouw nieuwe wachtwoord ook echt gaan aanpassen. Je hebt waarschijnlijk al voor zoveel diensten een wachtwoord opgegeven, dat je niet precies meer weet waarvoor. Wij adviseren je om je wachtwoord direct te veranderen bij je belangrijkste webdiensten. Denk aan:
• Je e-mail en sociale netwerken;
• Je financiële gegevens, zoals internetbankieren, online shoppen en verzekeringsdiensten;
• Je zakelijke gegevens, zoals je wachtwoord voor je werkcomputer of studenten account.

Nu ben je veel beter beschermd tegen meegluurders en hackers. En dat binnen vijf minuten!

Over de geheime vraag: veel websites geven je de mogelijkheid om, als je je wachtwoord vergeten bent, een geheime vraag te beantwoorden. Het gaat dan om je huisdier, meisjesnaam of favoriete kleur. Maar dit soort informatie is vaak te herleiden uit andere bronnen, zoals een Hyves- of Facebookprofiel. Dan kan een hacker het antwoord vrij eenvoudig raden. Het is daarom beter willekeurige onzin in te vullen, dan met een eenvoudig antwoord je wachtwoord prijs te geven.

WAT KAN IK DOEN?

MEER WETEN?

De Pers, 'Man jarenlang slachtoffer van identiteitsfraude' (03.09.09)
http://www.depers.nl/binnenland/334037/Man-jarenlang-slachtoffer-van-identiteitsfraude.html

Big Brother Awards, 'Bekijk en lees Vincent Icke en Renate Tromp' (10.05.10)
http://www.bigbrotherawards.nl/?p=589

CLICK 2

EEN BEVEILIGDE COMPUTER

MET AUTOMATISCHE BEVEILIGINGSUPDATES BESCHERM JE JEZELF TEGEN VIRUSSEN EN HACKERS.

WAAROM ZOU IK?

Hackers zijn uit op jouw computer, je mail-accounts en je privé-gegevens. Via iedere computer kan spam verspreid worden en met je gegevens verdienen zij grof geld. Ooit gemerkt dat je computer traag loopt, zomaar stilvalt of ineens uitgaat? Meestal net als je aan een belangrijk document zit te werken? Dan is de kans groot dat je gehackt bent. Je zou al je gegevens kunnen verliezen. Bovendien is je privacy niet zeker: met virussen verzamelen hackers jouw gegevens om er zelf rijk van te worden.

Dit heeft allemaal te maken met de beveiliging van je computer en je software. Als daar een lek inzit, kan een hacker toegang krijgen tot je computer om er bijvoorbeeld virussen op te installeren. Die vervolgens via jou de computers van vrienden en familie infecteren. Dit gebeurt zonder dat je het ziet. Daarom is het belangrijk om alle computerprogramma's op je computer altijd up-to-date te houden.

Om je te beschermen tegen virussen en hackers moet je allereerst de gratis automatische beveiligingsupdates van je besturingssysteem aanzetten. Zo krijg je vanzelf de meest actuele bescherming, zonder dat je hoeft na te denken. Bij veel mensen zijn deze automatische updates niet ingeschakeld, ook al is het zo gepiept.

AUTOMATISCHE BEVEILIGINGSUPDATES

Windows
http://windowsupdate.microsoft.com

Mac OS X
http://support.apple.com/kb/ht1338

Linux (Ubuntu)
https://help.ubuntu.com/community/InstallingSoftware#Automatic%20updates:%20Update%20Manager

Gebruik je Windows? Surf dan naar de Secunia Online Software Inspector voor een eerste volledige check:
http://secunia.com/vulnerability_scanning/online/?task=load

Wij adviseren Windows gebruikers om de Secunia Personal Software Inspector te downloaden, daarmee zijn alle risico's afgedekt: *http://secunia.com/vulnerability_scanning/personal/*

ADOBE UPDATE MANAGER

De Adobe Update Manager is ook van groot belang. Dit programma beschermt je tegen virussen in de producten van het bedrijf Adobe. Deze producten zijn een belangrijke prooi voor virussen omdat zij door iedereen worden gebruikt. Denk aan het lezen van .pdf bestanden en het bekijken van YouTube waarbij zogenaamde Flash software draait.

Windows
http://www.adobe.com/support/downloads/detail.jsp?ftpID=3185&promoid=DTEHP

Mac OS X
http://www.adobe.com/support/downloads/detail.jsp?ftpID=3184&promoid=DTEHO

Voor het besturingssysteem Linux is dit product helaas niet beschikbaar.

CLICK 3

TIJDELIJKE E-MAILADRESSEN

OOK GENOEG VAN SPAM IN JE INBOX? TIJDELIJKE E-MAILADRESSEN VOORKOMEN VEEL SPAM.

WAAROM ZOU IK?

Soms is voorafgaande registratie verplicht als je bepaalde websites of forums wilt bezoeken. Die registratie moet je dan bevestigen 'door te klikken op de link in een bevestigingsmailtje'. Vaak volgt in de dagen na je registratie ineens een hoop spam in je mailbox. Komt bekend voor? Door die registratie is je privé e-mailadres opgeslagen in een databank en op spamlijsten gekomen. Tegen de spam, die je inbox in de komende maanden gaat vervuilen, kun je dan niets meer doen.

WAT KAN IK DOEN?

Maak voor iedere dienst tijdelijke e-mailadressen aan. Via de website www.10minutemail.com krijg je zo'n e-mailadres en inbox voor tien minuten. Op de site krijg je direct een uniek e-mailadres. Hiermee kun je de aanmelding voltooien, en het bevestigingsmailtje krijg je dan in de inbox die je van 10minutemail hebt gekregen. Je klikt op de link en activeert je profiel.

Nu ben je binnen, zonder je privé e-mailadres te hebben gegeven. Zo kun je een forum of game een eerste keer uitproberen. Als je de website vertrouwt en denkt vaker terug te komen, kun je je opnieuw aanmelden met je echte e-mailadres.

Tijdelijke e-mailadressen zijn vooral handig voor online games, chatsites en fora. Voor online webwinkels en andere belangrijke websites kun je beter een permanent e-mailadres gebruiken. Zo worden ontvangstbevestigingen van vluchten en garantiebewijzen op producten vaak alleen via e-mail verstuurd.

CLICK 4

PRIVACY OP FACEBOOK

WAAROM ZOU IK?

Facebook heeft miljoenen gebruikers. Het sociale netwerk levert al die mensen veel plezier en vriendschappen op. Maar Facebook is steeds vaker negatief in het nieuws, omdat het weinig hecht aan jouw controle over de persoonlijke informatie op je profiel. Daarmee staat je privacy op het spel.

Uit een peiling blijkt dat driekwart van de Nederlanders zijn baas weigert als vriend op sociale netwerken. De meeste mensen hebben liever niet dat werkgevers via Facebook zo een blik in hun privéleven kunnen werpen. En wat te denken van ex-partners, hypotheekverstrekkers of ziektekostenverzekeraars? Het is dus van groot belang dat je zelf controle houdt over je profiel en je gegevens, omdat de informatie en foto's van jou zijn, niet van Facebook.

Facebook geeft jou liever zo min mogelijk controle, omdat jouw privacy op gespannen voet staat met hun bedrijfsmodel: je informatie doorverkopen aan adverteerders. Facebook verandert steeds van privacybeleid, zodat het bedrijf meer gegevens kan doorverkopen en het tegelijkertijd voor gebruikers volstrekt onduidelijk is welke informatie nu privé en welke publiek toegankelijk is.

JOUW LEVEN OP FACEBOOK IS NIET VAN FACEBOOK, MAAR VAN JOU.

In mei 2010 leidde de privacy-perikelen bij Facebook tot zulke heftige kritiek in de pers en op internet, dat Facebook moest buigen. Het sociale netwerk veranderde haar privacy-instellingen opnieuw. Facebook zette een aantal goede stappen, maar leverde helaas half werk. Als gebruiker zul je alsnog zelf je bescherming moeten regelen. Alleen zo blijft de kans dat jouw persoonlijke informatie in handen komt van je (toekomstige) werkgever, marketeers of hackers tot een minimum beperkt.

WAT KAN IK DOEN?

Hoog tijd om het heft in eigen hand te nemen. Sinds kort is dat heel makkelijk. Surf naar de website reclaimprivacy.org en volg de instructies. In drie heel simpele stappen weet je hoe je privacy-instellingen ervoor staan. Deze scan is open source, betrouwbaar en kost je niet meer dan één minuut.

De scan is klaar, wat nu? De scan geeft met de kleuren rood, geel en groen direct aan hoe je profiel erbij staat en levert de mogelijkheid een aantal aanpassingen te maken op je instellingen. Bij een groen resultaat hoef je niks te doen, bij geel en rood is het verstandig even te bekijken wat je kunt veranderen.

De keuze wat je wilt delen met anderen is natuurlijk aan jou. Na het volgen van de scan, biedt het overzicht een aantal simpele vervolgopties. Bits of Freedom adviseert:
(i) Instant Personalization uit te zetten;
(ii) Je vrienden geen informatie over jou te laten delen met derden, en
(iii) De applicaties op je profiel geen informatie te laten delen met anderen.

Van deze drie opties heb je namelijk weinig tot geen voordeel, terwijl het je profiel wel via de achterdeur openzet voor anderen. Verder raden wij je aan heel voorzichtig te zijn met het bekendmaken van je contactgegevens en adres. Dit is namelijk heel interessante informatie voor cybercriminelen en inbrekers.

Als je niet zeker weet wat je moet doen, raden wij aan om het instructiefilmpje van onze zusterorganisatie de Electronic Frontier Foundation te volgen. Dan ben je binnen een paar minuten klaar en weet je dat het goed zit.

Bij de keuze wat je deelt met anderen, moet je verder nog bedenken dat vrienden van vrienden niet alleen 'oude bekenden die je weer eens tegenkomt op een verjaardag' zijn. Het kan al gauw om een groep van 40.000 mensen gaan, als jouw 200 vrienden zelf ook 200 vrienden hebben. Onder die 40.000 'vrienden van vrienden' bevinden zich waarschijnlijk ook de werkgevers, marketeers en hackers die je juist niet wilde toelaten. Let wel: 40.000 is een gemiddelde. Als je meer vrienden hebt, ligt het aantal 'vrienden van vrienden' natuurlijk vele malen hoger.

N.B. Tijdens het schrijven van Webwijs, voert Facebook nieuwe privacy-instellingen door. Daarom bestaat er een kleine kans dat de 'Reclaim Privacy' scan niet werkt, omdat deze nog gebaseerd is op de oude instellingen terwijl bij jouw profiel de nieuwe instellingen al zijn doorgevoerd. Reclaim Privacy heeft laten weten hier hard aan te werken. Deze tijdelijke lacune moet bij het verschijnen van 'Webwijs' opgelost zijn.

MEER WETEN?

Instructiefilmpje Electronic Frontier Foundation, 'HOWTO: Maximize Facebook Privacy' (26.05.10, Engels) *http://www.eff.org/deeplinks/2010/05/more-privacy-facebook-new-privacy-controls*

Bits of Freedom, 'Facebook's Privacy-aanpassingen: goed begin, maar half werk [video]' (28.05.10) *https://www.bof.nl/2010/05/28/facebooks-privacy-aanpassingen-goed-begin-maar-half-werk-video/*

Pleaserobme.com, waarom je voorzichtig moet zijn met het posten van je contactgegevens *http://pleaserobme.com/why*

De Telegraaf, 'Baas geen vriend op Facebook' (22.04.10) *http://www.telegraaf.nl/digitaal/6575613/__Baas_geen_vriend_op_Facebook__.html?sn=digitaal*

The Guardian, 'Facebook, Google and Twitter: custodians of our most intimate secrets' (25.05.10) *http://www.guardian.co.uk/commentisfree/2010/may/25/personal-secrets-to-internet-companies*

CLICK 5

ANONIEM GOOGLEN

WEL DE GOOGLE RESULTATEN, NIET DE MASSALE GEGEVENSOPSLAG

WAAROM ZOU IK?

De kans is groot dat je Google gebruikt als zoekmachine. Maar weet jij nog wat je bijvoorbeeld negentien dagen geleden om één uur 's nachts bezig hield? Nee? Google wel, tot op de seconde. Daarmee weet Google bijna meer over jou dan jijzelf. Zoekopdrachten, Google Maps en Street View locaties, je e-mails in Gmail en zelfs de websites die je via Google bezoekt; alles wordt voor lange tijd opgeslagen.

En jouw leven wordt niet alleen door adverteerders, maar misschien ook wel door je verzekeringsmaatschappij, kredietverstrekker of de overheid ingezien. Of door criminelen, als de database van Google gehackt wordt of op straat komt te liggen door een fout.

Zoekresultaten zijn al vaker op het internet beland. Bij het zogenaamde 'America Online Search Data Scandal' belandden ruim 20 miljoen zoekopdrachten van 650.000 gebruikers van zoekmachine America Online (AOL) online. Nog steeds kun je op de website www.aolstalker.com van al die mensen zien, waar zij naar hebben gezocht.

Denk dus goed na voordat je al jouw zoekgedrag aan één bedrijf geeft. Je zoekgedrag bevat namelijk je meest persoonlijke en intieme informatie. Zoals je politieke voorkeur, gezondheid en liefdesleven. Kortom, je diepste geheimen. Informatie die niemand anders iets aangaat, ook Google niet.

WAT KAN IK DOEN?

Gebruik de onderstaande twee zoekmachines voor het zoeken naar informatie op internet. Zij slaan je zoektermen niet of nauwelijks op, en het ip-adres waarmee je geïdentificeerd kan worden evenmin. Als ze dit al doen, worden deze gegevens binnen 48 uur definitief verwijderd.

ALTERNATIEF I: SCROOGLE

Zoekmachine Scroogle gebruikt Google als zoekmachine, maar verwijdert alle persoonlijk identificeerbare informatie. Scroogle fungeert eigenlijk als tussenpersoon: de zoekopdrachten die Scroogle ontvangt, stuurt het weer door naar Google. Google ziet niet jouw IP-adres en kan ook niet zien welke zoekopdrachten van een bepaalde persoon zijn.

Scroogle kun je gebruiken via ***https://ssl.scroogle.org/***. Bovendien wordt Scroogle door de meeste grote browsers ondersteund, zodat je deze anonieme versie van Google rechtsboven in het zoekveld van je browser kunt zetten. Wel zo handig. Hier volgen de handleidingen voor:

Mozilla Firefox
https://addons.mozilla.org/en-US/firefox/addon/12506/

Microsoft Internet Explorer 7 / 8
plak ***http://www.scroogle.org/cgi-bin/nbbw.cgi?Gw=TEST*** in de navigatiebalk en volg de stappen op het scherm.

Chrome
Ga naar Preferences (Voorkeuren) > Basic Settings (Standaardinstellingen) > Default Search Manage (Standaardbrowser) > beheren. Klik op Add (toevoegen of plusje bij Mac OS X). Plak ***https://ssl.scroogle.org/cgi-bin/nbbwssl.cgi?Gw=%s*** in de balk.

Opera
Ga naar menu Tools > Preferences > Search > Add. Kies een zoekterm ("x"?) en gebruik ***http://www.scroogle.org/cgi-bin/nbbw.cgi?Gw=%s*** voor het "Address".

ALTERNATIEF II: IXQUICK

Ixquick kun je gebruiken via ***https://www.ixquick.nl***. Het is een meta-zoekmachine, waarbij meerdere zoekmachines gebruikt worden om per zoekterm de beste resultaten te gegeven. Dat zie je aan de sterretjes: hoe meer er achter een zoekresultaat staan, hoe vaker die site voorkwam bij de ongeveer 12 zoekmachines die Ixquick gebruikt.

Bovendien neemt Ixquick privacy serieus. Zo worden bijvoorbeeld geen IP-adressen van gebruikers opgeslagen. Wat Ixquick ook speciaal maakt, is het aanbieden van een 'proxy' optie bij alle zoekresultaten. Hiermee kun je zoekresultaten anoniem bezoeken, via de proxyserver van Ixquick. Met Ixquick kan je ook zoeken op afbeeldingen en filmpjes, net als bij Google.

MEER WETEN?

Meer informatie over zoekmachine Scroogle:
https://ssl.scroogle.org/sslnote.html

Meer informatie over zoekmachine Ixquick:
http://www.ixquick.nl/eng/protect-privacy.html

Meer informatie over het belang van anoniem Googlen:
The Guardian, 'Facebook, Google and Twitter: custodians of our most intimate secrets' (25.05.10) ***http://www.guardian.co.uk/commentisfree/2010/may/25/personal-secrets-to-internet-companies***

CLICK VERDER!

Je bent de eerste vijf clicks doorgekomen? Gefeliciteerd! Nu kan je jezelf nóg beter beschermen met extra beveiligingsmaatregelen. Hier vind je links naar extra tips, geselecteerd voor vijf gangbare online handelingen: surfen, e-mail, sociale media, bellen/chatten en downloaden. Deze tips vergen iets meer tijd en computervaardigheden dan de eerste 5 clicks. Ook hier geldt: de maatregelen bieden geen volledige bescherming. Maar je kan er wel van op aan dat je nóg beter beschermd bent.

Ontdek hoe je nog verder kunt zelfverdedigen bij:

SURFEN
https://www.bof.nl/surfen

E-MAIL:
https://www.bof.nl/email

SOCIALE MEDIA
https://www.bof.nl/socialemedia

BELLEN/CHATTEN
https://www.bof.nl/bellenchatten

DOWNLOADEN
https://www.bof.nl/downloaden

SURFEN

Surfen over het web is zo gebruikelijk geworden, dat je er nauwelijks bij stilstaat hoeveel informatie je over jezelf blootgeeft. Met de volgende tips help je jezelf een eind op weg deze informatie privé te houden:

– Gebruik altijd de meest recente versie van je webbrowser. Dan ben je beschermd tegen de nieuwste virusaanvallen en hacks. Als je een update wordt aangeboden van je webbrowser, doe je er verstandig aan om deze te installeren.

– Check of er een 's' achter http staat voor https-versleuteling. Zo kan je communicatie tussen jou en bijvoorbeeld internetbankieren, online winkelen en e-mailen niet worden onderschept voordat het daadwerkelijk bij de bank, bol.com of je inbox terecht komt: ***http://www.nederlandveilig.nl/veiliginternetten/tips/*** (tip 3)

– Waarschuw jezelf voor riskante website met de Web of Trust plug-in voor Internet Explorer, Firefox en Google Chrome: www.mywot.com

– Ontdek webbrowser Firefox en de privacy-vriendelijke add-ons:
• Installeer de open source webbrowser Firefox: ***http://www.mozilla.com/nl/***
• Maak een einde aan reclames en gegevens-trackers met Firefox add-on Adblock Plus: ***http://adblockplus.org/en/***
• Verwijder hardnekkige Flashcookies met Firefox add-on BetterPrivacy: ***https://addons.mozilla.org/en-US/firefox/addon/6623/***
• Weet wie toegang krijgt tot je computer en surf veilig met Firefox add-on NoScript: ***https://addons.mozilla.org/en-US/firefox/addon/722/***
• Verbeter de privacy-instellingen van je Firefox browser: ***http://www.simplehelp.net/2010/04/07/how-to-improve-your-privacy-settings-in-mozilla-firefox/nl/***

– Surf volledig anoniem over het internet met TOR:
http://www.torproject.org/index.html.en

E-MAIL

Waar we een zakelijke brief altijd in een envelop doen, zijn we met onze e-mail veel minder voorzichtig. Weinig mensen zijn zich ervan bewust dat zij hun e-mails open en bloot over het internet verzenden. Zo is de zogenaamde header van je e-mail bijvoorbeeld altijd leesbaar, met daarin bijvoorbeeld al het onderwerp van je mailtje en het tijdstip van verzending. Vaak genoeg zijn er redenen om toch een digitale envelop te gebruiken, ook voor je elektronische post. Hier is wat je daarvoor moet doen.

– Stop je webmail berichten, zoals Gmail en Hotmail berichten, in een digitale envelop met Firefox add-on FirePGP: http://getfiregpg.org/s/install (webbrowser Firefox vereist)

– Ontdek de open source e-mail client Thunderbird 3:
• Installeer de open source e-mailclient Thunderbird 3: *http://www.mozillamessaging.com/nl/thunderbird/*
• Verzend je e-mailberichten en wachtwoorden standaard met SSL-encryptie: *http://yakpost.net/files/yakpost_thunderbird_setup.pdf* (PDF)
• Versleutel je e-mailberichten met Thunderbird Enigmail: *https://addons.mozilla.org/en-US/thunderbird/addon/71/*

– Stop je e-mailberichten in een versleutelde envelop met GnuPG encryptie:
Windows en Linux gebruikers: *http://www.gnupg.org/*
Mac OS X gebruikers: *http://macgpg.sourceforge.net/*

SOCIALE MEDIA

Diensten als Hyves, Facebook en Twitter zijn een onlosmakelijk deel van onze internetervaring en dagelijks leven geworden. Hoe mooi deze vormen van communicatie ook zijn, soms zijn er valkuilen en privacylekken in de sites die niet overeenkomen met je verwachtingen, of weet je zelf nog niet goed hoe je je nu wel en niet moet gedragen binnen sociale media. Leer meer hierover via onderstaande links:

– Excite.nl, 'Tips voor meer privacy op Hyves en Facebook' (18.11.09)
http://webspinnen.excite.nl/nieuws/2014/Tips-voor-meer-privacy-op-Hyves-en-Facebook

– Tien Tips voor Facebook-privacy van RTL Nieuws, met medewerking Bits of Freedom (28.05.10):
http://www.rtl.nl/%28/actueel/rtl-nieuws/%29/components/actueel/rtl-nieuws/2010/05_mei/26/verrijkingsonderdelen/facebook_privacy_beschermen.xml

BELLEN / CHATTEN

De open source plug-ins die hieronder worden genoemd, geven je een maximale privacybescherming bij bellen en chatten. Zo weet je zeker dat privé ook écht privé is.

– Wél bellen via het internet, maar geen opslag van jouw gegevens of afgeluisterde gesprekken met Zfone:
http://zfoneproject.com/getstarted.html

– Veilig chatten op alle platforms met Pidgin en de OTR plug-in:
http://www.pidgin.im/ en
http://www.cypherpunks.ca/otr/

DOWNLOADEN

Miljoenen Nederlanders maken gebruik van filesharing, oftewel peer-to-peer technologie (p2p). Toch staan veel gebruikers onvoldoende stil bij wat er precies zichtbaar wordt als zij onderling gegevens met elkaar uitwisselen. Met deze maatregelen voorkom je privacyschendingen tijdens het gebruik van programma's als LimeWire en Bittorrent.

– Bescherm je anonimiteit in p2p netwerken met een onherkenbare gebruikersnaam voor je computer:

Veel mensen hanteren verschillende gebruikersnamen als er meerdere mensen gebruikmaken van dezelfde computer. Of hebben hun eigen naam als gebruikersnaam ingevuld. Zij realiseren zich niet, dat deze gebruikersnaam van de computer vaak wordt meegezonden met internetverkeer, in het bijzonder tijdens downloaden. Je kunt nog zoveel maatregelen nemen om je anonimiteit te beschermen, maar als je deze maatregel niet treft geef je op deze manier alsnog je eigen identiteit prijs, of die van je partner en kinderen.

Stel daarom een onherkenbare gebruikersnaam in. Vaak gebruikte opties zijn: 'user1', 'user2', 'user3'. Het veranderen van gebruikersnamen is erg eenvoudig:

Windows XP:
http://support.microsoft.com/?scid=kb%3Bnl%3B279783&x=9&y=16#appliesto

Mac OS X:
Klik op appeltje linksboven > System preferences (Systeemvoorkeuren) > Accounts > Klik op het hangslot linksonder om de instellingen te wijzigen > Typ je wachtwoord. Nu kun je een andere gebruikersnaam intoetsen. Klik op het hangslot om de wijzigingen op te slaan.

Linux (Ubuntu): surf naar
http://www.freesoftwaremagazine.com/articles/users_in_ubuntu

– Voorkom onbewuste datalekken via je 'shared folder' bij p2p programma's:
http://webwereld.nl/nieuws/65250/vs-waarschuwt-voor-datalekken-via-p2p.html

– Bescherm je privacy in p2p netwerken met PeerGuardian:
http://sourceforge.net/projects/peerguardian/

COLOFON

De totstandkoming van 'Webwijs – Online Zelfverdediging in 5 clicks' is afgerond op 1 juni 2010.

'Webwijs – Online Zelfverdediging in 5 clicks' is een initiatief van Stichting Bits of Freedom, de digitale burgerrechtenbeweging die opkomt op voor jouw vrijheid en privacy op internet. Bits of Freedom zorgt ervoor dat jouw internet jouw zaak blijft en dat je digitale grondrechten gerespecteerd worden. Omdat grondrechten onmisbaar zijn voor de zelfontplooiing van het individu, innovatie in het bedrijfsleven en de democratische rechtsstaat.

Website Bits of Freedom:
https://www.bof.nl

Speciale dank aan onze vrijwilligers, in het bijzonder:
Niels Arnbak, copywriter bij Euro RSCG 4D
Jeroen van Beek, IT security consultant bij dexlab.nl
Sander Hermsen, freelance grafisch ontwerper bij sander-hermsen.nl
Joran Polak, security expert en journalist bij Security.nl

Meer informatie over Online Zelfverdediging
Bits of Freedom blog: *https://www.bof.nl/category/zelfverdediging/*
Electronic Frontier Foundation, 'Surveillance Self-Defense Project': *https://ssd.eff.org/*
Front Line, 'Security in a Box': *http://security.ngoinabox.org/*
Postbus 51, 'Veilig Internetten': *http://www.nederlandveilig.nl/veiliginternetten/*

WEBWIJS – ONLINE ZELFVERDEDIGING IN 5 CLICKS
IS EEN INITIATIEF VAN

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

mijn kind online

Ouders Online

dexlab
it security audit, advisory & research

thuiswinkel
waarborg

STEUNEN 'WEBWIJS – ONLINE ZELFVERDEDIGING IN 5 CLICKS'