

Table of Contents

Inleiding	3
Belangrijkste bevindingen	4
Wat maakt sommige zoektermen risicovol?	4
Methodologie van de studie	5
Evaluatiemethodologie van McAfee SiteAdvisor	6
Gegevensbronnen	6
Rankings	7
Landspecifiek overzicht van de samenvatting van de risico's	7
Grondig onderzoek met gegevens van Hitwise	7
Beperkingen van de studie	8
Discussie over het gerelateerde werk	9
Conclusie	10
De gevaarlijkste zoektermen per land	11
Europa	
Oostenrijk, België, Tsjechische republiek, Denemarken, Finland, Frankrijk, Duitsland, Italië, Polen, Zuid-Afrika, Spanje, Zweden, Zwitserland, Nederland, Verenigd Koninkrijk	11
Noord-Amerika	
Verenigde Staten	16
Over McAfee	16

Inleiding

Tenzij u werkt voor of eigenaar bent van een online onderneming, is er kans dat u nog nooit hebt gehoord van de termen "search engine optimization" (SEO) en "search engine marketing" (SEM). Toch worden deze twee afkortingen – SEO (de moeite die eigenaars van websites doen om hun website hoger te rangschikken bij zoekmachines) en SEM (het gebruik van betaalde advertenties om een opvallende plaats te verkrijgen bij zoekmachines) steeds belangrijker voor bedrijven die op het web willen groeien. Helaas zijn het niet alleen legitieme bedrijven die met deze nieuwe tool steeds meer invloed winnen.

De oplichters – van individuen tot georganiseerde misdadigers – hebben zich snel gerealiseerd dat de zoekmachines, die legitieme bedrijven in staat stellen meer gebruikers te bereiken, ook gebruikt kunnen worden door criminelen om meer slachtoffers van hun geld te beroven.

Deze paper onderzoekt een nieuw fenomeen – het gebruik van zoekmachines door hackers, die op winst uit zijn, door het analyseren van het risico bij het zoeken naar meer dan 2.000 van de populairste woorden en uitdrukkingen ("sleutelwoorden"), ingevoerd in zoekmachines gedurende 2008. Van "Jonas Brothers tickets" (Tickets voor de Jona Brothers) en "game cheats" tot "Viva la vida lyrics" (songtekst Viva la Vida), deze sleutelwoorden zijn een ruime representatie van wat John Battelle onze "database van intenties" noemt.

Samen met onze "intenties", geeft deze database ook weer aan welk risico we ons blootstellen iedere keer we onze favoriete zoekmachine gebruiken. Welk risico? Voor sommige sleutelwoorden zoals "popular screensavers" (populaire schermbeveiligingen) en "descargar google" (download google) en hun pagina's met resultaten, kan het risico reëel zijn – 75% of meer van de resultaten (drie uit vier) kan leiden tot verhoogde veiligheidsrisico's op het web.

Dit is niet verrassend voor observatoren van de trends in beveiliging. Sinds het hacken voor eer plaats heeft moeten ruimen voor het hacken voor winst, is het aantal malafide spelers sterk gegroeid en worden hun manieren om grote groepen van potentiële slachtoffers te vinden steeds complexer. Door het relatieve risico van de populaire zoektermen te meten, bevestigt deze studie dat de oplichters nog steeds proberen om een zo groot mogelijke groep van slachtoffers te bereiken.

Maar deze studie toont ook interessant bewijs van het tegendeel. Vorige studies van McAfee® over webbeveiliging tonen aan dat 4% van de sites risicovol zijn. Dit is een algemene meting van het totale risico waaraan we blootstaan wanneer we het web gebruiken. Contrasterend is dat het algemene risiconiveau van alle resultatenpagina's slechts 1,7% was.

Deze studie is breed en richtinggevend. Nieuwe hulpmiddelen en onderzoeksmethoden moeten gebruikt worden om beter te begrijpen via welke methodes de zoekresultaten worden misbruikt. We hopen dat deze studie mee helpt aan de manier waarop andere studies een antwoord kunnen geven op deze belangrijke vragen.

De oplichters – van individuen tot georganiseerde misdadigers – hebben zich snel gerealiseerd dat de zoekmachines, die legitieme bedrijven in staat stellen meer gebruikers te bereiken, ook gebruikt kunnen worden door criminelen om meer slachtoffers van hun geld te beroven.



Belangrijkste bevindingen

McAfee onderzocht meer dan 2.600 populaire sleutelwoorden. Voor elk sleutelwoord onderzochten we de vijf eerste pagina's met resultaten van de vijf grootste zoekmachines. Gemiddeld leverde dit voor elk sleutelwoord iets meer dan 250 resultaten op. In totaal hebben we meer dan 413.000 unieke URLs onderzocht. We hebben elk sleutelwoord aan een categorie en een land toegewezen en hebben ze gerangschikt volgens het risico van hun resulterende URLs. Daarnaast hebben we gebruik gemaakt van gegevens van Hitwise, een bedrijf dat zich bezighoudt met zoekintelligentie, om een grondiger onderzoek van bepaalde sleutelwoorden uit te voeren.

De sleutelwoorden zijn gerangschikt op twee manieren: 1) het gemiddelde risico van alle resultaten en 2) het maximale risico van de meest risicovolle pagina van de resultaten.

- In totaal was het algemene risiconiveau van alle resultatenpagina's slechts 1,7%. In andere woorden, in een lijst van 250 resultaten zijn er slechts iets meer dan vier risicovol.
- Maar wanneer we het gemiddelde berekenden van de meest risicovolle pagina's (de pagina van elk sleutelwoord dat het meeste risicovolle resultaten had), dan steeg het gemiddelde risico tot 10,0%. In andere woorden, in een lijst van 250 resultaten zijn er iets meer dan 25 risicovol.
- We hebben Hitwise gebruikt om een gedetailleerde lijst van sleutelwoordvarianten te genereren voor 12 zoektermen. Zoals gedefinieerd door McAfee, de meest risicovolle set van variaties van sleutelwoorden was "screensavers" (schermbeveiliging) met een maximaal risico van 59,1% en een gemiddeld risico van 34,4%, substantieel hoger dan de gemiddeldes van de studie van 10,0% en 1,7%. Verrassend was dat zoekopdrachten met het sleutelwoord Viagra, een populair sleutelwoord dat vaak in onze spamfilters wordt tegengehouden, minder risicovolle sites opleverde.
- Populaire sleutelwoorden in landen buiten de VS zijn significant risicovoller dan de populaire sleutelwoorden in de Verenigde Staten. 14 landen hadden lijsten met sleutelwoorden die een hoger maximaal risico inhielden dan het gemiddelde, inclusief de Tsjechische Republiek (14,2%) en Brazilië (12,1%). En 12 landen waren in totaal risicovoller dan het gemiddelde, inclusief Mexico (1,9%) en India (1,8%). Deze bevindingen kunnen uitzonderingen zijn, maar als andere studies deze bevestigen, kan dit een vroeg bewijs zijn van een verontrustende trend dat oplichters zich nu ook op slachtoffers buiten de VS richten.

Hackers zijn het meest succesvol wanneer ze grote aantallen van slachtoffers kunnen aantrekken. Een manier om een grote online doelgroep te bereiken zijn actuele gebeurtenissen – alles van nieuws over bekende sterren en natuurrampen tot vakanties en populaire muziek.

Wat maakt sommige zoektermen risicovol?

Waarom zijn sommige sleutelwoorden of zoektermen risicovoller dan andere? Terwijl het niet steeds mogelijk is om de denkwijze en motivatie van de hedendaagse hackers te begrijpen, kan McAfee inzichten verschaffen die gebaseerd zijn op gekende technieken die door cybercriminelen worden gebruikt.

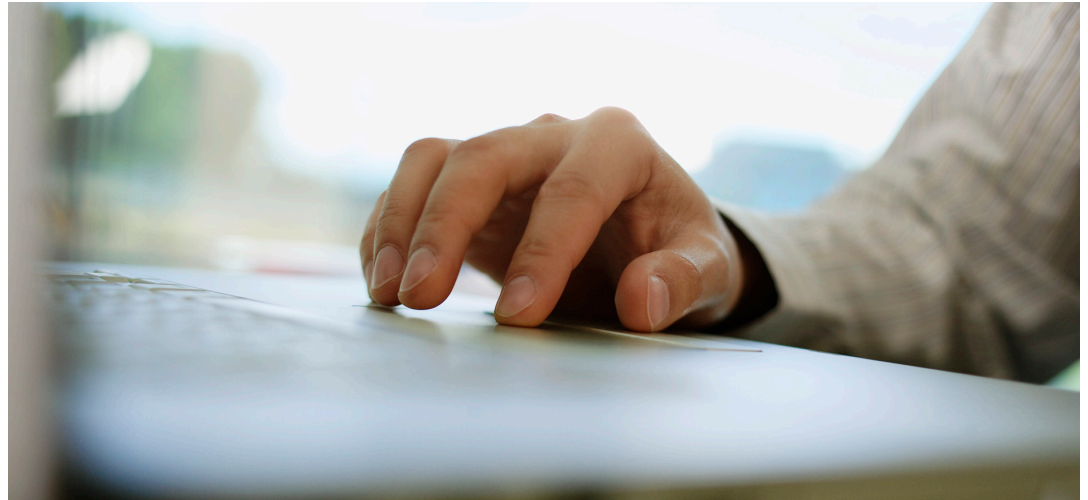
Hackers zijn het meest succesvol wanneer ze grote aantallen van slachtoffers kunnen aantrekken. Een manier om een grote online doelgroep te bereiken zijn actuele gebeurtenissen – alles van nieuws over bekende sterren en natuurrampen tot vakanties en populaire muziek.

Een belangrijke manier waarop cybercriminelen hun slachtoffers in de val lokken, is door ze een computerbestand of programma met een schadelijke inhoud te laten downloaden.

Nu deze twee concepten zijn geïntroduceerd, kijken we naar één van onze meest risicovolle zoektermen: gratis muziekdownloads. Ongeveer 20,7% van de resultaten waren risicovol (te vergelijken met slechts 1,7% voor alle zoektermen) en op één van de 25 resultatenpagina's die we evalueerden, waren 42,9% van alle resultaten risicovol. Omdat consumenten steeds vaker hun muziekbibliotheken digitaliseren met MP3-bestanden, worstelen ze ook met de kost om muziek te kopen die ze reeds bezitten op cassette, LP of in andere formaten. Gevangen tussen deze twee noden, hebben vele consumenten gehoord dat het web een bron kan zijn voor gratis muziek. Als de consument op zoek is naar muziek, dan zijn ze reeds overtuigd om iets te downloaden - en dat maakt het werk van de auteur van schadelijke programma's natuurlijk eenvoudiger.

Het onderwerp of de inhoud van een website heeft ook een invloed op het risico. Twee van zulke voorbeelden zijn minder bekende pornografische en goksites die gebruikt kunnen worden om schadelijke software zoals exploits, dialers, trojans en andere malware te verspreiden. Dit soort inhoud kan consumenten naar de donkere plekjes van het internet leiden en consumenten blootstellen aan meer risico wanneer zij naar deze termen op zoek zijn.

Bij het bepalen van de "marktgrootte" voor hun oplichting, kunnen cybercriminelen kijken naar het totale aantal links naar een website dat bepaalde zoektermen opleveren. Googlebattle.com is een goed voorbeeld om dit aan te tonen. McAfee vond dat "Brad Pitt" gevaarlijker was om te zoeken dan "Hugh Jackman" (14,3% maximaal risico ten opzicht van 9,1%). Gelijkwaardig levert Googlebattle 26,4 miljoen hits voor "Brad Pitt" en slechts 5,5 miljoen voor "Hugh Jackman".



Het is belangrijk op te merken dat het aantal links naar websites slechts één factor is die een cybercrimineel gebruikt bij bepalen van een sleutelwoord. Bijvoorbeeld, Googlebattle geeft aan dat Olympisch voetbal meer links heeft dan Olympisch zwemmen, maar voor de VS was "Michael Phelps" toch een populairdere - en risicvollere - zoekterm.

Op dezelfde manier kunnen hoofdpunten in het nieuws ook consistent populaire sleutelwoorden uit de "risicozone" halen. Bijvoorbeeld, drie populaire, vrouwelijke sterren zijn Angelina Jolie (8,3% maximaal risico) Oprah Winfrey (10%) en Beyoncé Knowles (10%). Maar zoekopdrachten naar Zuma Rosedale, de dochter van Gavin Rossdale en Gwen Stefani, kunnen een risico tot 25% inhouden. Dit is een voorbeeld om aan te geven dat malafide hackers zonder scrupules ook aandacht besteden aan het nieuws.

Methodologie van de studie

Elke uitdrukking en sleutelwoord is opgezocht in de vijf grootste zoekmachines uit de VS – Google, Yahoo!, Live, AOL en Ask. We hebben de eerste vijf resultatenpagina's voor elk sleutelwoord bekeken en hebben het aantal rood en geel geëvalueerde sites (zoals bepaald door McAfee SiteAdvisor®) op elke pagina geteld en ze vergeleken met het totaal aantal geëvalueerde sites. We hebben de sites die nog niet geëvalueerd zijn, niet meegeteld. We hebben zowel gesponsorde als organische links geteld en hebben ze hetzelfde gewicht meegegeven. McAfee SECURE™ sites die op dagelijkse basis getest worden op kwetsbaarheden, zijn als groen geëvalueerde sites geteld voor deze studie.

We hebben het risico van bepaalde zoektermen op twee manieren gerangschikt. Het gemiddelde risico is het totaal aantal rood en geel geëvalueerde sites gedeeld door het aantal rood, geel en groen geëvalueerde sites op de 25 resultatenpagina's die we onderzochten. Het maximale risico is de pagina met het hoogste percentage aan rood en geel geëvalueerde sites.

Bijvoorbeeld, een sleutelwoord dat tien geëvalueerde resultaten per pagina genereert, zou in totaal 250 geëvalueerde sites opleveren. Het gemiddelde risico zou dan gelijk zijn aan (rood + geel geëvalueerde sites / rood + geel + groen geëvalueerde sites). 10 rood, 15 geel en 225 groen geëvalueerde sites zouden een gemiddeld risico van 10% opleveren (25/250). Als één pagina twee rood, twee geel en zes groen geëvalueerde sites zou weergeven, is het maximale risico gelijk aan 40% (4/10).

Evaluatiemethodologie van McAfee SiteAdvisor

De veiligheidsopinions van de sites zijn afkomstig van onze evaluatiedatabank uit McAfee SiteAdvisor. Deze database bevat evaluaties voor meer dan 20 miljoen sites die ongeveer 95% van het totale webverkeer uitmaken. Evaluaties van websites zijn gebaseerd op tests voor veiligheidsrisico's:

De beoordelingen van de websites door SiteAdvisor worden bepaald door de volgende veiligheidsrisico's en overwegingen:

- *Risicovolle downloads*
- *Browsermisbruik*
- *E-mailactiviteiten*
- *Phishing*
- *Excessieve aantallen pop-ups*
- *Linken*

- *Risicovolle downloads*—Downloadbare bestanden die virussen, spyware of adware bevatten of niet-gerelateerde wijzigingen aan de computer aanbrengen.
- *Browsermisbruik*—Ook gekend als een drive-by download, dit type van schadelijke code schakelt virussen, toetsaanslagloggers of spyware in op de computer van een consument zonder zijn toestemming of medeweten.
- *E-mailactiviteiten*—Registratieformulieren en andere inschrijvingen die resulteren in massa's e-mails, sterk commercieel gerichte e-mails of beide. We hebben ook getest hoe moeilijk het was om uit te schrijven.
- *Phishing*—Oplichtingsites om bezoekers te misleiden die geloven dat het een legitieme website is.
- *Excessieve aantallen pop-ups*—Sites die op een agressieve manier pop-ups oproepen of een groot aantal pop-ups weergeven
- *Linken*—Sites die agressief andere rood of geel geëvalueerde sites linken.

De meeste van deze tests worden uitgevoerd door testcomputers. In sommige gevallen treed het personeel van McAfee dit automatisch testen bij met handmatige controles.

Rode evaluaties worden gegeven aan websites die in één of meer van deze tests falen. Gele evaluaties worden gegeven aan sites waarvoor, volgens onze mening, de nodige voorzichtigheid moet geboden worden. Groene evaluaties worden gegeven aan sites met weinig tot geen risico.

Gegevensbronnen

Deze studie onderzoekt het relatieve risico van het zoeken naar ongeveer 2.658 unieke, populaire sleutelwoorden en uitdrukkingen in 413.368 unieke URLs. In alle gevallen waren de volwassenenfilters ingeschakeld. Het merendeel van de gegevens is gecreëerd door zoektermen te verzamelen van de volgende bronnen:

2008 Year-End Google Zeitgeist

<http://www.google.com/intl/en/press/zeitgeist2008/>

Yahoo! 2008 Year in Review (Jaaroverzicht 2008)

<http://buzz.yahoo.com/yearinreview2008/>

AOL 2008 Year End Hot Searches (Populairste zoektermen jaareinde 2008)

<http://about-search.aol.com/hotsearches2008/index.html>

Ask Top 2008 Searches (Top 2008 zoektermen)

<http://about.ask.com/en/docs/2008/topqueries.shtml>

Hitwise

<http://www.hitwise.com/>

Voor elk van de 12 sleutelwoorden, gebruiken we Hitwise om de 25 populairste varianten van de laatste 12 weken van 2008 eindigend op 27 december, te genereren.

Wordtracker Top 1000

<https://www.wordtracker.com>

Voor woorden en uitdrukkingen buiten de VS, hebben we slechts één bron gebruikt - Google Zeitgeist's Around the World list.

<http://www.google.com/intl/en/press/zeitgeist2008/world.html>

Rankings

For convenience, we have grouped the keywords we studied by category and by country of popularity.

Landspecifiek overzicht van de samenvatting van de risico's

Land	Maximaal risico (gemiddeld)	Risicocategorie (gemiddeld)
Tsjechië	14,2%	2,4%
Finland	13,1%	2,3%
Chili	13,0%	2,2%
Frankrijk	12,8%	2,1%
Spanje	12,6%	1,8%
Polen	12,2%	1,9%
Brazilië	12,1%	1,5%
Columbia	11,9%	1,8%
Denemarken	11,6%	1,9%
India	11,3%	1,8%
Zuid-Afrika	11,2%	1,7%
Nederland	11,1%	1,6%
Zweden	10,4%	1,6%
Mexico	10,3%	1,9%
Italië	9,7%	1,1%
Maleisië	9,6%	1,5%
Singapore	9,5%	1,1%
Canada	9,4%	1,3%
België	9,4%	0,9%
Argentinië	9,2%	1,4%
Filipijnen	9,1%	1,5%
Nieuw-Zeeland	7,9%	1,1%
Australië	7,7%	0,9%
Oostenrijk	7,7%	0,8%
Verenigd Koninkrijk	7,4%	0,8%
Zwitserland	7,0%	0,9%

Grondig onderzoek met gegevens van Hitwise

De meeste lijsten van sleutelwoorden die we voor deze studie hebben gebruikt zijn vereenvoudigd door de personen die deze lijsten hebben samengesteld. De lijsten groeperen gerelateerde zoektermen in één woord of uitdrukking, dat representatief is. Bijvoorbeeld, "Miley Cyrus" is zeker en vast een populaire zoekterm. Maar zo is ook "Miley Cyrus lyrics" (songteksten Miley Cyrus), "Miley Cyrus videos," "Miley Cyrus and Nick Jonas" (Miley Cyrus en "Nick Jonas) en "Miley Cyrus pictures" (foto's van Miley Cyrus). Voor Yahoo! en AOL was de enige zoekterm die in hun jaareinde lijst terecht kwam de eerste - "Miley Cyrus."

We weten ook dat gebruikers bij het selecteren van zoektermen en het gebruik van zoekmachines soms op ongebruikelijke manieren handelen. Volgens Google is "www.google.com" ongeveer vijf miljoen keer ingevoerd op Google zelf!

Om deze variaties beter op te vangen, gebruikt McAfee variaties van het gegevensbedrijf Hitwise¹ om een gedetailleerder beeld van het risico van bepaalde sleutelwoorden te krijgen. Als we in detail kijken naar één uitdrukking en zijn variaties, is dit het begin om de zoekrisico's beter te begrijpen. Dit grondige onderzoek keek naar de 25 populairste variaties voor zoekwoorden voor 12 populaire sleutelwoorden in de Verenigde Staten.

Volgens Google is "www.google.com" ongeveer vijf miljoen keer ingevoerd op Google zelf!

Categorie	Maximaal risico (gemiddeld)	Risicocategorie (gemiddeld)
Screensavers (Schermbeveiligingen)	59,1%	34,4%
Free Games (Gratis games)	24,7%	6,8%
Work From Home (Werk van thuis uit)	15,6%	3,1%
Rihanna	12,6%	2,4%
Webkinz	11,4%	1,9%
Powerball	9,3%	1,5%
iPhone	7,9%	1,2%
Jonas Brothers	7,9%	1,2%
Twilight	6,8%	0,9%
Barack Obama	6,2%	0,7%
Taxes (Belastingen)	4,9%	0,4%
Viagra	1,6%	0,1%

Beperkingen van de studie

Deze studie is beperkt door de brongegevens en de methodes die zijn gebruikt.

Zoals opgemerkt is de “top van de zoektermen” van het jaareinde vereenvoudigd door de zoektermen te groeperen onder één woord of uitdrukking. Ja, er zijn vele songteksten gezocht in 2008, maar in vele gevallen voegden de gebruikers de titelnaam of artiest bij het woord “lyrics” (songtekst). Dus lijst Google “lyrics” op als een populaire zoekterm in zeven landen. De Olympische Usain Bolt was daarentegen ongetwijfeld een populaire zoekterm, al was het voor beelden van zijn races. Maar het is onwaarschijnlijk dat vele personen gezocht hebben naar “Usain Bolts WR Breaking Win in 200m Final” (Usain Bolts WR in 200m finale) en daarom categoriseert AOL deze zoekterm onder “Live video moments” (Live video momenten).

Een aantal prominente webschrijvers hebben deze lijsten bekritiseerd omwille van verschillende redenen. TechCrunch concludeert:

“Als Google aan het einde van de dag de top duizend van zoektermen neemt, een aantal interessante zoekopdrachten op subjectieve wijze eruit filtert en vervolgens opnieuw de volgorde bepaalt op basis van de groeisnelheid in plaats van algemene rangschikkingen, dan eindigen we met een lijst die op het einde helemaal zinloos is.”

In 2006 antwoordde één zoekmachine, Google:

“[[W]e verzamelen niet alleen de meest opgezochte zoektermen voor een bepaalde periode – deze wijzigen immers helemaal niet zo vaak gedurende de jaren. Deze lijst zou gedomineerd worden door zeer generieke zoektermen, zoals “ebay”, “dictionary” (woordenboek), “yellow pages” (gele gids), “games”, “maps” (kaarten)– en natuurlijk een aantal volwassenen zoektermen. Deze zijn constanten en zonder twijfel zeer populair, maar we denken niet dat ze effectief de Zeitgeist (tijdgeest) weergeven.”

Hieronder volgen enkele links naar de interpretaties en analyses door enkele critici:

- Search Engine Watch: <http://blog.searchenginewatch.com/061219-105250>
- Rough Type: http://www.rough.type.com/archives/2006/12/dweebs_horndogs.php
- CenterNetworks: <http://www.centernetworks.com/top-searches-compared>
- GigaOM: <http://gigaom.com/2006/12/28/google-explains-wack-zeitgest-criteria/>

We kunnen akkoord gaan met beide argumentaties, maar merk op dat onze studie de rangschikking van de zoekmachines slechts gebruikt als startpunt om het belangrijkste aandeel in sleutelwoorden te voorzien. Of een woord nu of de 5de of 15de plaats van populaire zoektermen is gerangschikt, is voor onze studie niet van belang. Hetgeen belangrijk is, is dat de zoekterm populair is. In deze zin geloven we dat deze lijsten nuttig zijn.



Onze bevindingen voor landen buiten de VS zijn op twee manieren beperkt. We gebruiken Google als onze enige bron voor populaire zoekwoorden in landen buiten de VS. Zoals eerder aangehaald, lijken deze lijsten wat te zijn gegeneraliseerd. Daarnaast gebruiken we dezelfde zoekmachines voor alle zoekopdrachten. Bijvoorbeeld, we hebben google.com en niet .fr gebruikt voor de Franse zoekopdrachten.

Discussie over het gerelateerde werk

McAfee is niet het enige bedrijf of instituut dat vaststelt dat oplichters gebruik maken van populaire trends om een steeds groter aantal potentiële slachtoffers te bereiken. Afgelopen mei bijvoorbeeld, vond het bedrijf Sophos Trojans in bijlagen van e-mails over bekende sterren.

In 2006 wees een studie van onderzoekers aan de Universiteit van Washington uit dat game en celebrity sites "... een groter risico bleken te zijn voor piggybacked spyware, terwijl sites die gepirateerde software aanbieden de lijst van drive-by aanvallen aanvoerde."

In hetzelfde jaar, ging Microsoft een rechtszaak aan tegen een bedrijf dat gebruik maakte van screensavers van bekende sterren om spyware te distribueren, door de volgende uitspraak te doen:

"Veel van deze programma's worden voorgesteld als screensavers met mooie foto's van bekende sterren zoals Jessica Simpson. Maar de programma's van de beschuldigde bevatte veel meer dan enkel en alleen mooie foto's. Eens geïnstalleerd zou de software contact opnemen met "thuis" en verschillende andere programma's downloaden die gebruikers bombarderen met ongewenste pop-up advertenties, die hun activiteit op internet volgen, die hun internet browsers doorverwijzen naar ongewenste pagina's, die pictogrammen toevoegen aan het Bureaublad van Microsoft Windows en de instellingen van het Windows-register van de gebruiker wijzigen. Microsoft beweert dat deze programma's zijn gedownload en geïnstalleerd zonder medeweten of goedkeuring van de gebruikers. Blijkbaar installeert de software van de beschuldigde zelfs indien gebruikers de installatie proberen tegen te houden door het selecteren van de gepaste opties."

Recenter meldde Trend Micro reported dat ze oplichting hadden ontdekt rond vacatures. Gegeven de globale economische crisis, zijn we niet verbaasd dat oplichters zich ook richten op deze steeds groter worden groep van slachtoffers.

Op eenzelfde manier ontdekte Gary Warner, een forensisch computeronderzoeker dat oplichters de economische crisis in de VS gebruikten om slachtoffers te zoeken. Symantec vond ook stimuli in e-mails, die indien ze beantwoord zouden worden, konden leiden tot het verlies van persoonlijke identiteitsinformatie en identiteitsdiefstal.

In februari was Digg, een populaire nieuwssite, meermaals het slachtoffer van honderdduizenden valse commentaren die de bezoekers naar websites met malwares leidden.

Een onafhankelijke veiligheidsonderzoeker, Shanmuga genaam, analyseerde een bestand dat de nieuwe videoclip van Paris Hilton beloofde maar eigenlijk een list was om kijkers te lokken.

Conclusie

Algemeen gesproken, bevestigt deze studie dat oplichters populaire trends zeker niet links laten liggen wanneer ze op zoek zijn naar slachtoffers. Dat is eigenlijk heel logisch. Als hackers nu hoofdzakelijk gemotiveerd worden door winst, kunnen de grootste winsten behaald worden als de grootst mogelijk groep van slachtoffers wordt aangesproken. En op het web zijn populaire trends en hoge bezoekersaantallen sterk met elkaar gecorreleerd.

Nu dit gezegd is, weten we niet waarom een bepaald populair sleutelwoord meer of minder risicovol is dan een ander populaire sleutelwoord. En we hebben slechts een beperkt begrip van de manier waarop oplichters te werk gaan. Ja, we weten dat ze spam versturen, websites opzetten, anderen infecteren enzovoort. Maar problemen met webbeveiliging evolueren even snel als het web zelf. Bijvoorbeeld, enkele jaren geleden maakten oplichters steeds vaker gebruik van technieken zoals "Google bombing" om een hogere rangschikking in de zoekmachines te verkrijgen:

"Fraudeurs hoopten om geld te kunnen stelen dat bestemd was voor ... (tsunami) liefdadigheid door de paginarangschikking van Google te manipuleren zodat hun namaaksite hoger in de zoekmachines verscheen dan de officiële website van het liefdadigheidsdoel."

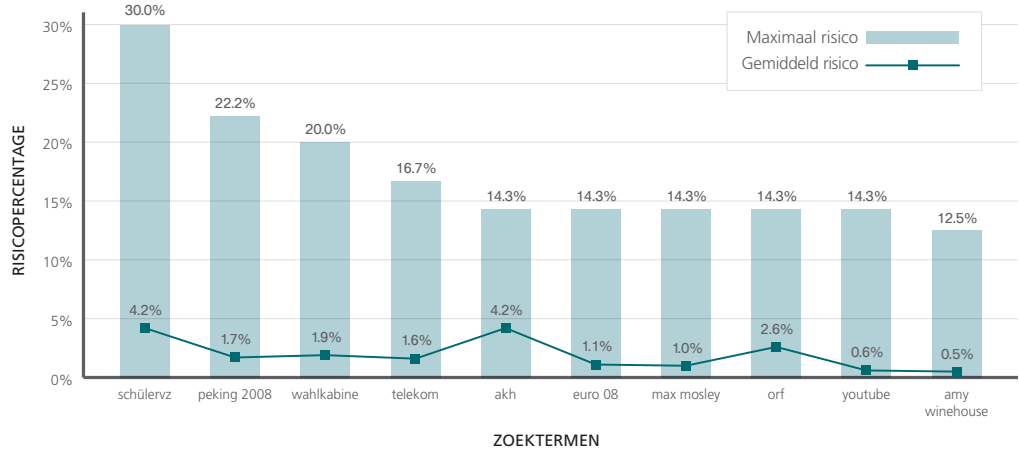
De zoekmachines reageerden en deze soorten van aanvallen komen vandaag minder frequent voor en zijn niet zo effectief als in 2005. Maar er ontstaan elke week nieuwe manieren van oplichting, die de oudere vervangen. En op deze manier blijft de strijd steeds verdergaan.

Voor consumenten betekent dit dat ze moeten vertrouwen op intuïtie of kennis van vroegere risico's maar dat is niet voldoende om veilig van het web gebruik te kunnen maken. Technisch aangelegde gebruikers lopen nog meer risico. De beste bescherming is een computerbeveiligingsprogramma te installeren en dit up-to-date te houden en door gebruik te maken van een veilig zoekprogramma zoals McAfee SiteAdvisor.

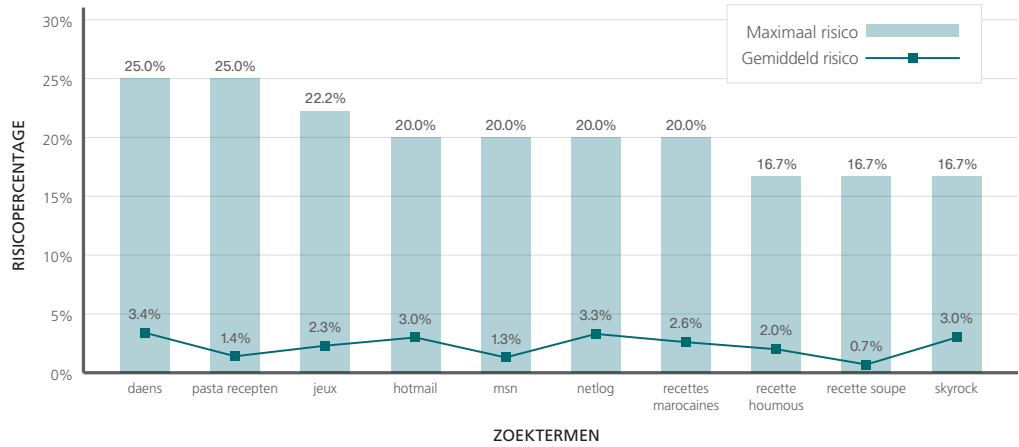
De gevaarlijkste zoektermen per land

Europa

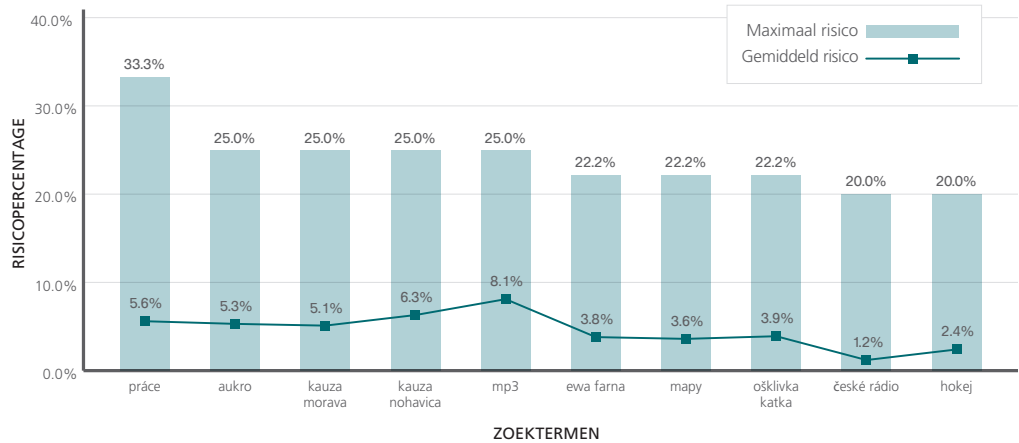
Gevaarlijkste zoektermen – Oostenrijk



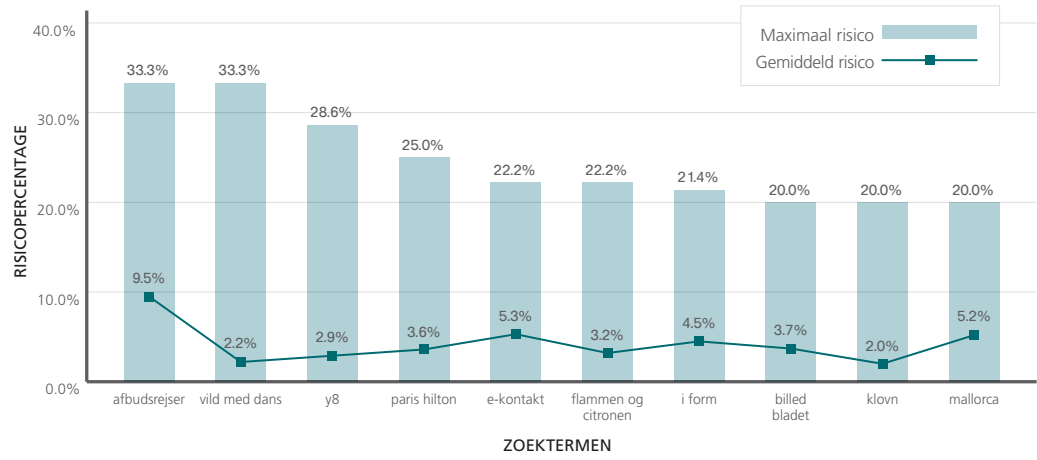
Gevaarlijkste zoektermen - België



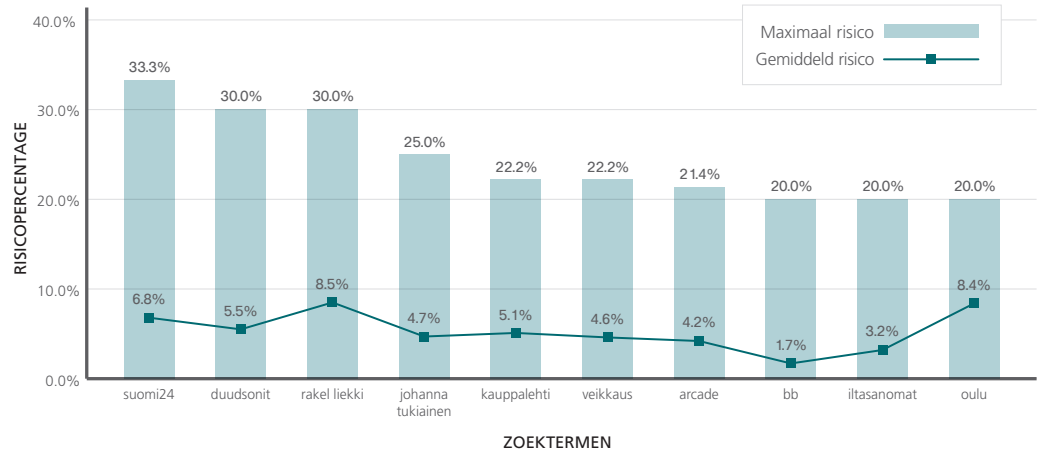
Gevaarlijkste zoektermen - Tsjechische republiek



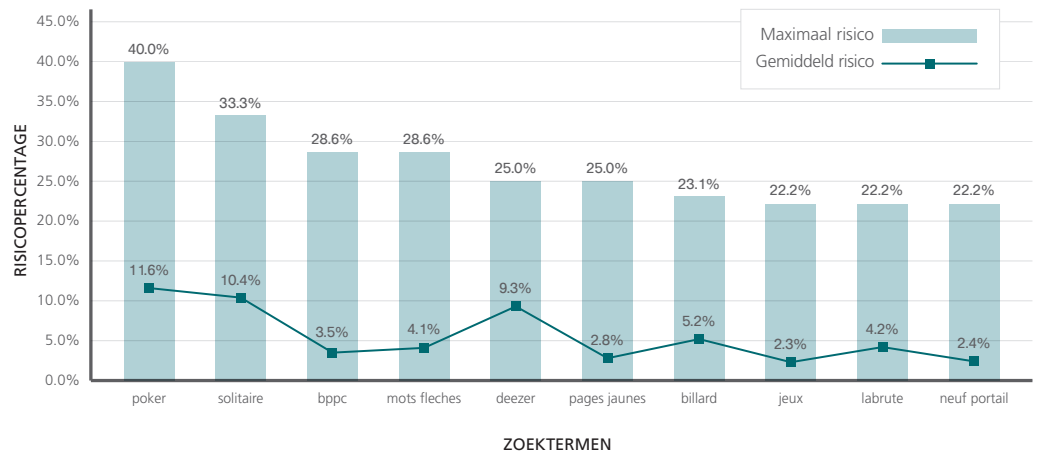
Gevaarlijkste zoektermen – Denemarken



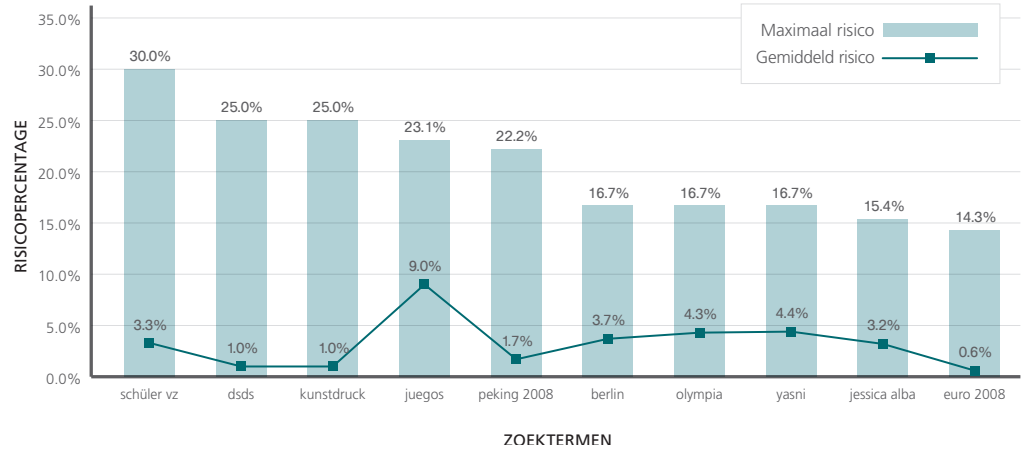
Gevaarlijkste zoektermen - Finland



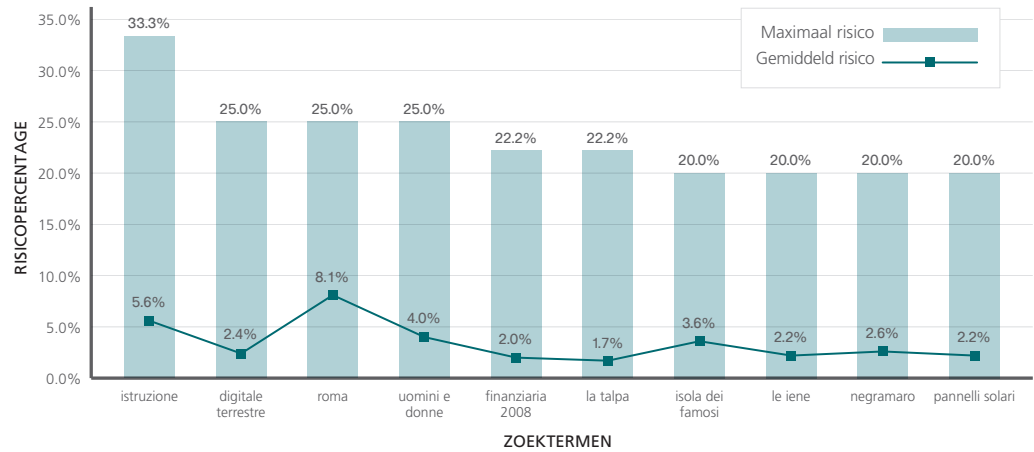
Gevaarlijkste zoektermen – Frankrijk



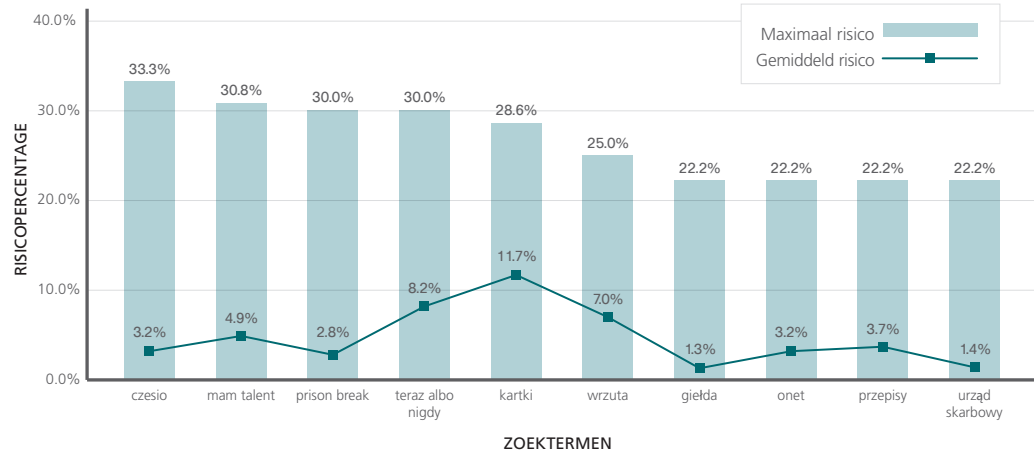
Gevaarlijkste zoektermen – Duitsland



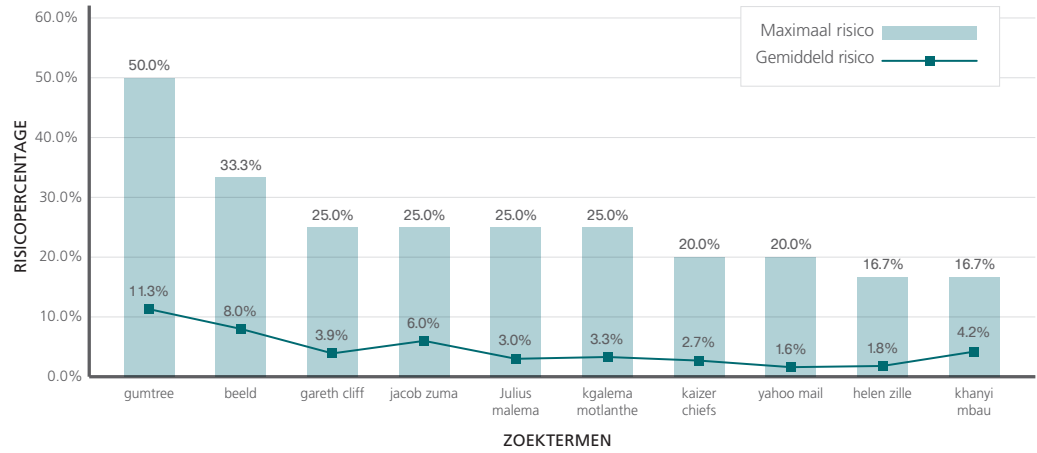
Gevaarlijkste zoektermen – Italië



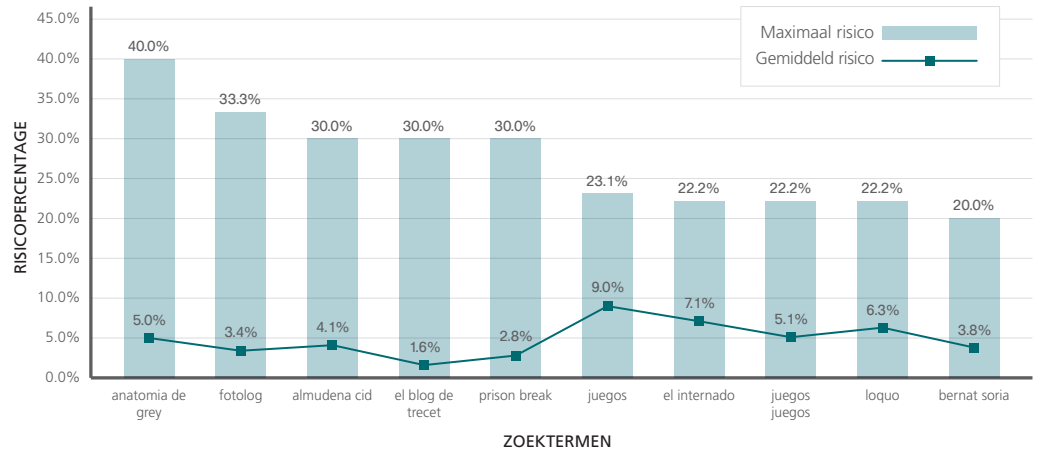
Gevaarlijkste zoektermen - Polen



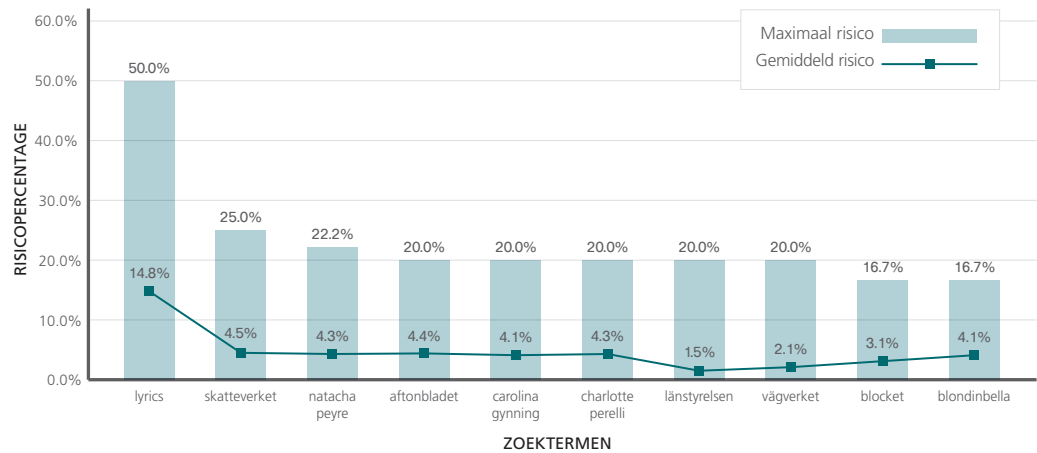
Gevaarlijkste zoektermen - Zuid-Afrika



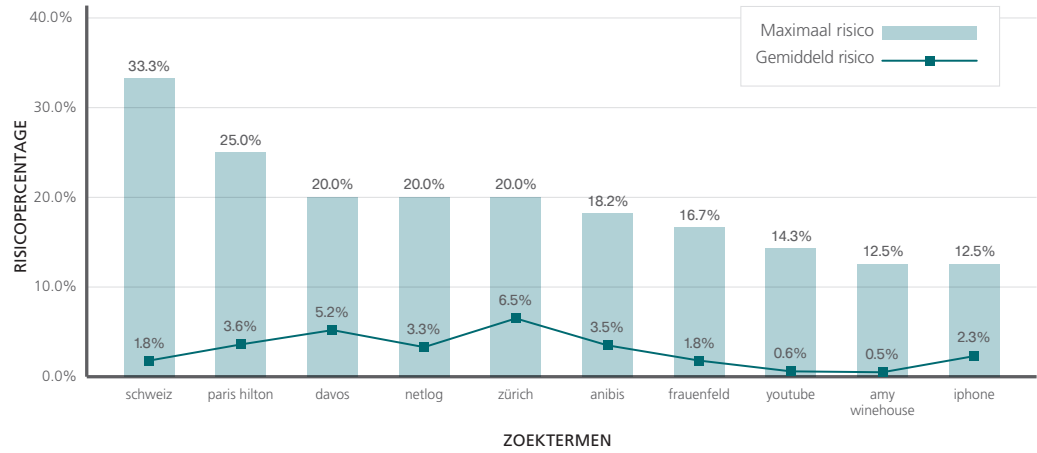
Gevaarlijkste zoektermen - Spanje



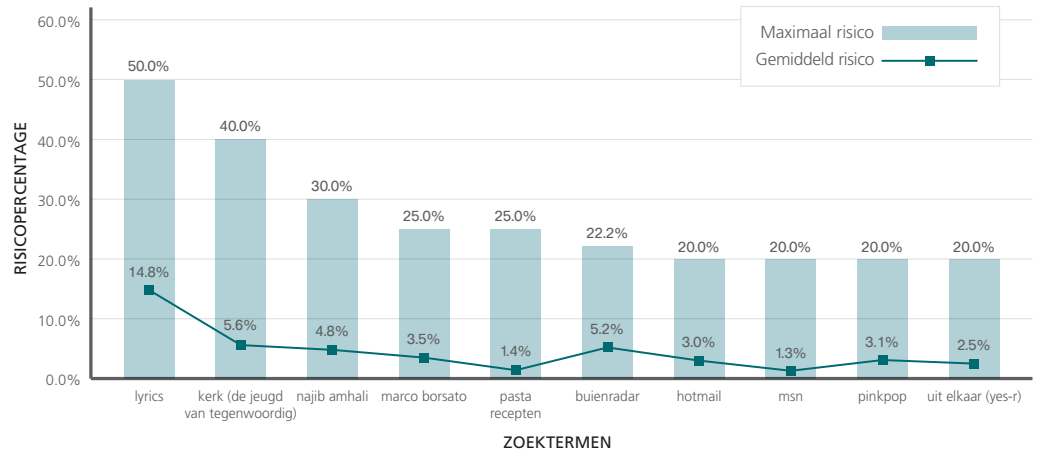
Gevaarlijkste zoektermen - Zweden



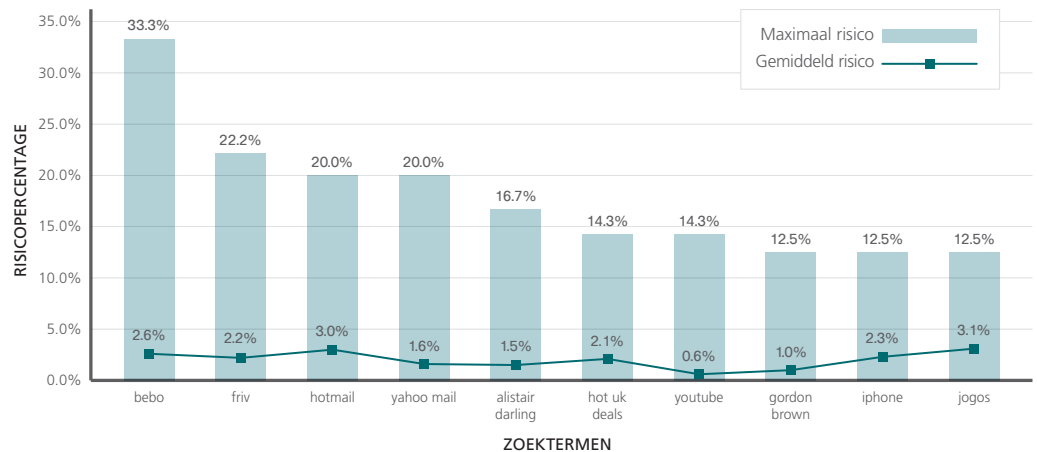
Gevaarlijkste zoektermen – Zwitserland



Gevaarlijkste zoektermen - Nederland

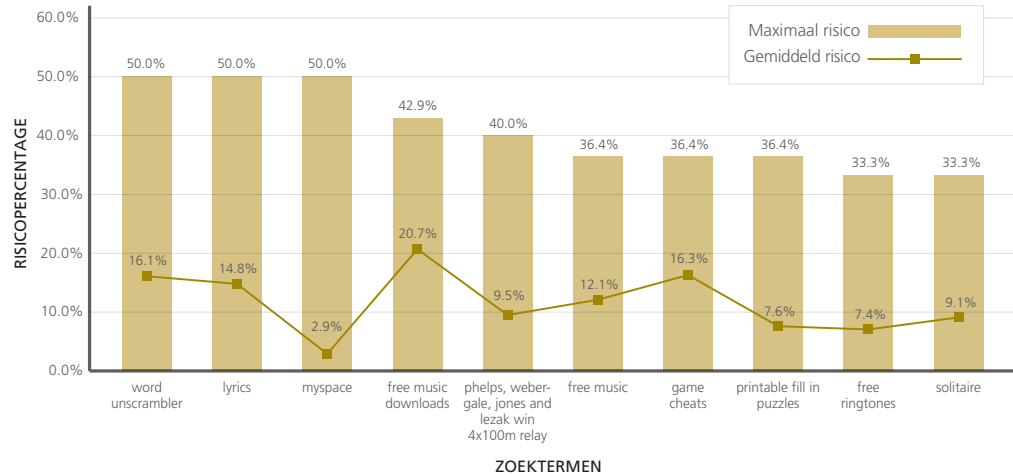


Gevaarlijkste zoektermen - Verenigd Koninkrijk



Noord-Amerika

Gevaarlijkste zoektermen - Verenigde Staten



Over McAfee

McAfee Inc., gevestigd in Santa Clara, Californië, is het grootste, gespecialiseerde bedrijf ter wereld inzake veiligheidstechnologie. McAfee is toegewijd om de moeilijkste veiligheidsuitdagingen ter wereld aan te gaan. Het bedrijf levert proactieve en bewezen oplossingen en diensten die helpen om systemen en netwerken over heel de wereld te beveiligen, zodat gebruikers veilig met het internet kunnen verbinden, en nog veiliger aankopen kunnen doen op het web. Gesteund door een met een prijs bekroond onderzoeksteam, creëert McAfee innovatieve producten die thuisgebruikers, bedrijven, de publieke sector en dienstverleners in staat stellen om aan de geldende regelgevingen te voldoen, gegevens te beschermen, storingen te voorkomen, kwetsbaarheden te identificeren en continue de beveiliging op te volgen en te verbeteren. <http://www.mcafee.com>.

