

Índice

Introdução	3
Principais descobertas	4
O que torna alguns termos de busca arriscados?	4
Metodologia do estudo	5
Metodologia de classificação do McAfee SiteAdvisor	6
Fontes dos dados	6
Classificações	7
Resumo de Descobertas de Risco por País	7
Análise minuciosa com dados da Hitwise	7
Restrições estudo	8
Análise de trabalhos relacionados	9
Conclusão	10
Palavras-Chave de Busca Mais Perigosas por País	
América Latina	
Argentina, Brasil, Chile, Colômbia, México	11
Sobre a McAfee	13

Introdução

A menos que você seja proprietário ou trabalhe para uma empresa cujos negócios são realizados de modo on-line, é provável que você nunca tenha ouvido sobre os termos “otimização de sites” (Search Engine Optimization - SEO) e “marketing de busca” (Search Engine Marketing - SEM). Mas, estas duas expressões — SEO (o esforço do proprietário do site para que este receba uma classificação mais alta pelos mecanismos de busca) e SEM (o uso de publicidade paga para conseguir um local de destaque em mecanismos de busca) são termos cada vez mais importantes no vocabulário de negócios que procuram prosperar na web. Infelizmente, negócios legítimos não são os únicos que estão ganhando destaque com essa nova linguagem.

Os *scammers*, que podem ser desde operadores independentes até criminosos organizados, perceberam rapidamente que os mesmos mecanismos de busca utilizados por negócios legítimos para alcançar maior número de consumidores também podem ser usados por criminosos para tirar mais dinheiro de suas vítimas.

Este documento examina um novo fenômeno que é o uso de mecanismos de busca como um canal para fins lucrativos pelos hackers, analisando o risco de procurar mais de 2.000 palavras e frases mais populares (“palavras-chave”) utilizadas em mecanismos de busca em 2008. De “Jonas Brothers tickets” (ingressos para os Jonas Brothers), passando por “game cheats” (trapaças virtuais nos jogos) até “Viva la Vida lyrics” (letra de Viva la Vida). Estas palavras-chave representam uma parte considerável daquilo que o especialista em buscas John Battelle chama de “banco de dados de intenções”.

Além de nossas “intenções”, esse banco de dados também revela o risco a que nos expomos toda vez que usamos nosso mecanismo de busca favorito. Qual é o risco? No caso de algumas palavras-chave, como “screensavers” (protetores de tela populares) e “descargar google” (baixar google), e algumas de suas páginas de resultados, o risco pode ser imenso, 75% ou mais dos resultados (três em cada quatro) podem aumentar o risco à segurança na Internet.

Isso não surpreende quem acompanha as tendências de segurança. Uma vez que os hackers em busca de fama foram substituídos pelos hackers em busca de lucro, essas pessoas mal intencionadas foram sofisticando cada vez mais sua habilidade de encontrar grandes grupos de vítimas em potencial. Ao medir o risco relativo de termos de busca populares, esse estudo confirma que os *scammers* continuam a visar grandes grupos de vítimas.

Mas esse estudo também encontrou interessantes evidências contrárias. Estudos anteriores da McAfee® sobre segurança da Internet demonstraram que cerca de 4% dos sites apresentavam risco. Essa é uma medida ampla do risco geral que enfrentamos ao utilizar a web. Em contrapartida, o nível de risco médio de todas as páginas de resultados que estudamos foi de apenas 1,7%.

Esse estudo é amplo e direcional. Precisam ser criados novos métodos de pesquisa e ferramentas que nos permitam entender melhor a mecânica de como as pesquisas estão sendo mal utilizadas. Esperamos que este estudo ajude a abrir caminho para outros estudos sobre essas questões importantes.

Os scammers, que podem ser desde operadores independentes até criminosos organizados, perceberam rapidamente que os mesmos mecanismos de busca utilizados por negócios legítimos para alcançar maior número de consumidores também podem ser utilizados por criminosos para tirar mais dinheiro de suas vítimas.



Principais descobertas

A McAfee pesquisou mais de 2.600 palavras-chave populares. Em cada uma delas, examinamos as primeiras cinco páginas de resultados nos cinco principais mecanismos de busca. Em média, cada palavra-chave gerou pouco mais de 250 resultados. Ao todo, examinamos mais de 413.000 URLs diferentes. Atribuímos a cada palavra-chave uma categoria e um país e depois as classificamos pelo risco de suas URLs resultantes. Além disso, usando dados da Hitwise, uma empresa de inteligência em buscas, fizemos análises mais detalhadas de palavras-chave específicas.

As palavras-chave foram classificadas de duas maneiras: 1) o risco médio de todos os resultados e 2) o risco máximo da página de resultados mais arriscada.

- No geral, o nível de risco médio de todas as páginas de resultados foi de apenas 1,7%. Em outras palavras, em uma lista de 250 resultados, apenas um pouco mais de quatro eram arriscados.
- Contudo, quando fizemos a média das páginas mais arriscadas (a página de cada busca por palavra-chave que tinha os resultados mais arriscados), o risco médio saltou para 10,0%. Ou seja, em uma lista de 250 resultados, apenas um pouco mais de 25 eram arriscados.
- Adotamos ferramenta da Hitwise para gerar uma lista detalhada de variações de palavras-chave para 12 termos de busca. Conforme definido pela McAfee, o conjunto mais arriscado de variações de palavras-chave foi "screensavers" (protetores de tela), com risco máximo de 59,1% e risco médio e 34,4%, resultados consideravelmente maiores do que as médias do estudo, de 10,0% e 1,7%. Surpreendentemente, buscas usando a palavra-chave Viagra, que é popular e frequente em nossos filtros de spam, apresentou o menor número de sites arriscados.
- As palavras-chave populares em outros países foram significativamente mais arriscadas do que aquelas populares nos Estados Unidos. Verificamos que 14 países tiveram listas de palavras-chave que expõem os usuários a risco máximo mais alto do que a média, incluindo a República Tcheca (14,2%) e o Brasil (12,1%). E 12 países foram mais arriscados no geral do que a média, incluindo México (1,9%) e Índia (1,8%). Essas descobertas talvez sejam anomalias, mas se estudos subsequentes as confirmarem, pode ser uma primeira evidência de uma nova tendência preocupante: os *scammers* estão visando mais vítimas fora dos EUA.

Os hackers têm mais êxito quando conseguem atrair um grande número de vítimas. Um modo de visar grandes grupos on-line é acompanhar eventos atuais, desde um surto de uma celebridade até desastres naturais, de feriados a música popular.

O que torna alguns termos de busca arriscados?

Por que algumas palavras-chave ou termos de busca são mais arriscados que outros? Embora nem sempre seja possível entender a mente e as motivações dos sofisticados hackers atuais, a McAfee pode fornecer alguns insights com base nas técnicas conhecidas utilizadas pelos cibercriminosos.

Os hackers têm mais êxito quando conseguem atrair um grande número de vítimas. Um modo de visar grandes grupos on-line é acompanhar eventos atuais, desde um surto de uma celebridade até desastres naturais, de feriados a música popular.

Uma das principais ferramentas que os cibercriminosos utilizam para enganar suas vítimas é fazê-las baixar um arquivo ou programa de computador que traz uma carga útil maliciosa.

Com esses dois conceitos em mente, vamos dar uma olhada em um de nossos termos de busca mais arriscados: downloads de música gratuita. Em média, 20,7% dos resultados foram arriscados (comparados com apenas 1,7% de todos os termos de busca) e em uma página de resultados entre cada 25 páginas classificadas pelo mecanismo de busca, encontramos absurdos 42,9% de resultados arriscados. À medida que os consumidores continuam a converter suas bibliotecas de música para formatos digitais, como arquivos de MP3, eles também se deparam com o custo de comprar música que já possuem em fitas, LPs ou outros formatos. Apanhados entre essas duas necessidades, muitos consumidores ouviram falar que a web pode ser uma fonte de música gratuita. Se o consumidor já estava procurando por música, ele também está mentalmente preparado para fazer o download de algo, o que facilita muito o trabalho de um autor de malware.

O assunto ou tipo de conteúdo do web site também afeta seu risco. Dois exemplos típicos são sites pornográficos ou de apostas menos conhecidos que podem ser utilizados para hospedar software malicioso, como exploits, dialers, cavalos de Tróia, e outros malwares. Esse tipo de conteúdo pode conduzir os consumidores pelos becos escuros da Internet, e ao buscar por esses termos, eles se expõem a mais riscos.



Ao determinar o “tamanho do mercado” para seus *scams*, os cibercriminosos talvez procurem o número total de links para web sites que resulta de um termo de pesquisa. O Googlebattle.com é uma boa ferramenta para ilustrar isso. A McAfee descobriu que é mais perigoso procurar por “Brad Pitt” do que por “Hugh Jackman” (14,3% de risco máximo contra 9,1%). De modo similar, o Googlebattle produz 26,4 milhões de resultados para “Brad Pitt” e apenas 5,5 milhões para “Hugh Jackman”.

É importante notar que o número de links para o web site é apenas um fator que os cibercriminosos podem utilizar ao decidir visar determinada palavra-chave. Por exemplo, Googlebattle mostra que futebol olímpico tem mais links do que natação olímpica, mas para o público dos EUA em especial, “Michael Phelps” é um termo de busca mais popular e mais arriscado.

De modo similar, picos de cobertura das notícias também podem levar até palavras-chave consistentemente populares para fora da “zona de maior risco”. Por exemplo, três celebridades populares do sexo feminino são Angelina Jolie (8,3% de risco máximo) Oprah Winfrey (10%) e Beyoncé Knowles (10%). Mas buscas por Zuma Rossdale, filha de Gavin Rossdale e Gwen Stefani, pode ter um risco de até 25%, sugerindo que pessoas mal intencionadas e inescrupulosas prestam bastante atenção aos eventos noticiados.

Metodologia do estudo

Cada frase e palavra-chave foi procurada nos cinco principais mecanismos de busca localizados nos EUA: Google, Yahoo!, Live, AOL e Ask. Analisamos as cinco primeiras páginas de resultados de cada palavra-chave, e contamos o número de sites classificados em vermelho e amarelo em cada página (conforme determinado pelo McAfee SiteAdvisor®) e os comparamos ao número total de sites classificados. Não consideramos sites para os quais ainda não temos uma classificação. Contamos tanto links patrocinados como “orgânicos” e os pesamos igualmente. Os sites com o selo McAfee SECURE™, que passam por testes diários de vulnerabilidade, foram contados como sites classificados em verde para os fins deste estudo.

Depois, classificamos o nível de risco de determinado termo de busca em duas maneiras. O risco médio é o número total de sites classificados em vermelho e amarelo dividido pelo número total de sites classificados em vermelho, amarelo e verde nas 25 páginas de busca que examinamos. O risco máximo é a página única com a mais alta porcentagem de sites classificados em vermelho e amarelo.

Por exemplo, uma palavra-chave que gerou dez resultados classificados por página daria um total de 250 sites classificados. O risco médio seria igual (sites classificados em vermelho e amarelo / sites classificados em vermelho, amarelo e verde). Dez sites classificados em vermelho, mais 15 em amarelo e 225 em verde resultariam em um risco médio de 10% (25/250). Se uma página exibiu dois sites classificados em vermelho, mais dois em amarelo e seis em verde, o risco máximo seria igual a 40% (4/10).

As classificações do web site do SiteAdvisor são determinadas pelas seguintes preocupações e riscos de segurança:

- Downloads arriscados
- Exploits de navegador
- Práticas de email
- Phishing
- Pop-ups excessivos
- Práticas de criação de links

Metodologia de classificação do McAfee SiteAdvisor

Nossas opiniões sobre segurança de sites vêm do banco de dados de classificação de sites do McAfee SiteAdvisor. Esse banco de dados inclui classificações para mais de 20 milhões de sites que, juntos, respondem por aproximadamente 95% do tráfego na web. As classificações de web sites se baseiam em testes das seguintes ameaças e preocupações com a segurança:

- *Downloads arriscados* — Arquivos que podem ser baixados e que contêm vírus, spyware ou adware ou fazem mudanças não relacionadas no computador para os quais são baixados.
- *Exploits de navegador* — Também conhecidos como “download drive-by”, esse tipo de código malicioso permite que vírus, criadores de logs de teclado, ou spywares se instalem no computador do consumidor sem o seu consentimento e/ou conhecimento.
- *Práticas de email* — Formulários de registro e outras inscrições que resultam em altos volumes de mensagens, emails altamente comerciais ou ambos. Também testamos a dificuldade de cancelar a inscrição.
- *Phishing* — Sites de *scam* que tentam enganar o visitante para que ele acredite que o site é legítimo.
- *Pop-ups excessivos* — Sites que têm comportamento insistente no uso de pop-ups ou mostram um número muito grande de pop-ups.
- *Práticas de criação de links* — Sites que criam links para outros sites classificados em vermelho ou amarelo insistentemente.

A grande maioria dos testes são feitos em computadores dedicados para esta finalidade. Em alguns casos, a equipe da McAfee aumenta esses testes automáticos fazendo exames manuais.

A classificação em vermelho é aplicada a web sites que não passam em um ou mais desses testes. A classificação em amarelo é aplicada a sites que, em nossa opinião, merecem cuidado no uso. A classificação em verde é aplicada a sites com riscos mínimos ou nenhum risco detectado.

Fontes dos dados

Este estudo examinou o risco relativo de procurar aproximadamente 2.658 palavras-chave e frases populares diferentes em 413.368 URLs diferentes. Em todos os casos, os filtros para conteúdo adulto estavam ativados. O *corpus* (coleção) de dados foi criado pela coleta de termos de busca das seguintes fontes:

Zeitgeist de Fim de Ano do Google — 2008

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

Yahoo! — Year in Review — 2008

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

AOL 2008 Year End Hot Searches

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

Ask Top 2008 Searches

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

Hitwise

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

Para cada uma das 12 palavras-chave, utilizamos a consultoria Hitwise para gerar as 25 variações mais populares para as 12 semanas que findaram em 27 de dezembro de 2008.

Wordtracker Top 1000

<https://www.wordtracker.com>

Para palavras-chave e frases fora dos EUA, usamos uma única fonte: a lista Google Zeitgeist's Around the World.

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

Classificações

Por conveniência, agrupamos as palavras-chave que estudamos por categoria e por país de popularidade.

Resumo de Descobertas de Risco por País

País	Risco Máximo (Média)	Risco da Categoria (Média)
República Tcheca	14,2%	2,4%
Finlândia	13,1%	2,3%
Chile	13,0%	2,2%
França	12,8%	2,1%
Espanha	12,6%	1,8%
Polônia	12,2%	1,9%
Brasil	12,1%	1,5%
Colômbia	11,9%	1,8%
Dinamarca	11,6%	1,9%
Índia	11,3%	1,8%
África do Sul	11,2%	1,7%
Holanda	11,1%	1,6%
Suécia	10,4%	1,6%
México	10,3%	1,9%
Itália	9,7%	1,1%
Malásia	9,6%	1,5%
Cingapura	9,5%	1,1%
Canadá	9,4%	1,3%
Bélgica	9,4%	0,9%
Argentina	9,2%	1,4%
Filipinas	9,1%	1,5%
Nova Zelândia	7,9%	1,1%
Austrália	7,7%	0,9%
Áustria	7,7%	0,8%
Reino Unido	7,4%	0,8%
Suíça	7,0%	0,9%

Análise minuciosa com dados da Hitwise

A maioria das listas de palavras-chave que utilizamos para este estudo foram simplificadas pelas pessoas que as compilaram. As listas agrupam frases de busca relacionadas sob uma única palavra ou frase representativa. Por exemplo, “Miley Cyrus” sem dúvida é um termo de busca popular. Mas “Miley Cyrus lyrics” (letras de Miley Cyrus), “Miley Cyrus videos” (vídeos de Miley Cyrus), “Miley Cyrus and Nick Jonas” (Miley Cyrus e Nick Jonas) e “Miley Cyrus pictures” (fotos de Miley Cyrus) também são populares. No caso do Yahoo! e AOL, o único termo de busca incluído nas suas listas de fim de ano foi o primeiro: “Miley Cyrus”.

Também sabemos que, algumas vezes, as pessoas escolhem palavras para buscas e utilizam os mecanismos de busca de formas incomuns. De acordo com o Google, a expressão “www google com” foi procurada aproximadamente cinco milhões de vezes no próprio Google!

Para capturar melhor essa variedade, a McAfee utilizou variações de palavras-chave da empresa Hitwise¹ para obter um quadro mais detalhado da natureza do risco de certas palavras-chave. Se analisarmos com mais cuidado uma frase e suas variações, podemos começar a entender melhor o risco das buscas. Essas análises minuciosas avaliaram as 25 variações de palavras de busca mais populares de 12 palavras-chave populares nos Estados Unidos.

De acordo com o Google, a expressão “www google com” foi procurada aproximadamente cinco milhões de vezes no próprio Google!

Categoria	Risco Máximo (Média)	Risco da Categoria (Média)
Screensavers (Protetores de tela)	59,1%	34,4%
Free Games (Jogos grátis)	24,7%	6,8%
Trabalho em casa	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%
Crepúsculo	6,8%	0,9%
Barack Obama	6,2%	0,7%
Taxes (Impostos)	4,9%	0,4%
Viagra	1,6%	0,1%

Restrições do estudo

O estudo é restrito aos dados da fonte e pelos métodos utilizados.

Como mencionado, as listas de “maiores buscas” do ano simplificam os termos de busca agrupando palavras-chave relacionadas sob uma única palavra ou frase. De fato, as pessoas procuraram muitas letras de música em 2008, mas com muita frequência elas acrescentaram o nome da música ou do artista à palavra “letras”. Mas o Google lista “letras” como uma busca popular em sete países. De modo similar, o atleta olímpico Usain Bolt foi sem dúvida uma figura popular nas buscas, bem como os vídeos de suas corridas. Mas é improvável que muitas pessoas tenham procurado “Usain Bolts WR Breaking Win in 200m Final” (Quebra do recorde mundial na vitória de Usain Bolts na final dos 200 m), embora esse seja um termo de busca que o AOL incluiu em sua categoria “Momentos ao vivo em vídeo”.

Diversos escritores de destaque na Internet criticam essas listas por várias razões. TechCrunch concluiu:

“Se no final das contas, o Google pega alguns milhares de buscas principais, escolhe subjetivamente algumas que são interessantes e depois volta a determinar a ordem com base na velocidade de crescimento, em vez de na classificação geral, acabamos com uma lista que é, ao final, completamente inútil.”

Em 2006, um mecanismo de busca, o Google, respondeu:

“Nós não retomamos simplesmente os termos mais frequentemente procurados no período. A verdade é que eles não mudam muito de um ano para outro. Essa lista teria, predominantemente, buscas muito genéricas, como “ebay”, “dictionary” (dicionário), “yellow pages” (páginas amarelas), “games” (jogos), “maps” (mapas), e, é claro, diversas palavras-chave pornográficas. Essas são constantes e, embora sejam inquestionavelmente populares, não achamos que elas realmente definam o Zeitgeist.”

Abaixo, se encontram os links para interpretações e análises de vários críticos:

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

Reconhecemos ambos os lados dessa discussão, mas indicamos que nosso estudo utilizou as classificações dos mecanismos de busca como ponto inicial que nos forneceu o *corpus* de palavras-chave. Para os fins deste estudo, não importa se a palavra é classificada em quinto ou quinquagésimo lugar entre as mais populares. O que é importante é apenas que é popular. Nesse sentido, acreditamos que essas listas são úteis.



Nossas descobertas em outros países são limitadas por dois motivos. Utilizamos o Google como nossa única fonte de palavras-chave populares nesses países. Como mencionado, essas listas parecem um pouco generalizadas. Também, utilizamos o mesmo mecanismo de busca em todas as buscas. Por exemplo, usamos o google.com, não o google.fr, para buscas em francês.

Análise de trabalhos relacionados

A McAfee não é a única empresa ou instituição a descobrir que os *scammers* estão usando a cultura e as tendências populares para alcançar grupos maiores de vítimas em potencial. No último mês de maio, por exemplo, a empresa de segurança Sophos encontrou cavalos de Tróia em anexos de emails relativos a celebridades.

Em 2006, um estudo realizado por pesquisadores da Universidade de Washington identificou que sites de jogos e celebridades "... pareciam apresentar o maior risco de spywares, enquanto sites que ofereciam softwares piratas ficam no topo da lista de ataques drive-by".

No mesmo ano, a Microsoft apontou uma empresa que supostamente utilizava protetores de tela de celebridades para distribuir spyware, afirmando:

"Muitos desses programas são apresentados como protetores de tela com fotos de celebridades conhecidas, como Jessica Simpson. No entanto, estes programas sobre ela incluíam muito mais do que belas fotos. Depois de instalado, o software 'ligava para casa' e fazia secretamente o download de inúmeros outros programas que bombardeavam os usuários com anúncios pop-up indesejados, acompanhavam a atividade do usuário na Internet, redirecionavam seus navegadores de Internet para páginas indesejadas, acrescentavam ícones ao desktop do Microsoft Windows e mudavam configurações do registro do Windows do usuário. A Microsoft alega que esses programas eram baixados e instalados sem aviso adequado aos usuários ou sem o consentimento deles. O interessante é que os softwares dessa artista foram instalados mesmo quando os usuários tentaram parar a instalação escolhendo as opções adequadas."

Mais recentemente, a Trend Micro informou ter detectado *scams* que tinham por alvo pessoas em busca de emprego. Devido à difícil economia global, não ficamos surpresos em que os *scammers* se concentrassem nesse crescente grupo de vítimas.

De modo similar, um pesquisador forense de tecnologia da Gary Warner descobriu que *scammers* utilizaram o estímulo econômico dos EUA para encontrar vítimas. A Symantec também encontrou convites em emails que, se respondidos, poderiam levar à perda de informações de identificação pessoal e ao roubo de identidade.

E, recentemente, o Digg, um site de notícias muito popular, foi vítima de centenas de milhares de comentários falsos que levaram os visitantes a Web sites que hospedavam malware.

Um pesquisador de segurança independente chamado Shanmuga analisou um arquivo que prometia um novo vídeo de Paris Hilton, mas era de fato uma isca para injetar viewers.

Conclusão

No geral, este estudo confirma que os *scammers* consideram as tendências populares ao decidir as vítimas que serão seu alvo. Isso faz sentido. Se os hackers agora são motivados basicamente pelo lucro, pode-se obter muita lucratividade com maiores grupos de vítimas em potencial. E na web, as tendências populares e o tráfego de visitantes são altamente correlacionados.

Ainda assim, não sabemos por que determinada palavra-chave popular é mais ou menos arriscada do que outra. E só temos um entendimento limitado sobre os modos de operação dos *scammers*. De fato, sabemos que eles utilizam spam, criam web sites e infectam outros, e assim por diante. Mas as questões de segurança na Internet se alteram tão rapidamente quanto a própria web. Por exemplo, há alguns anos, os *scammers* começaram a utilizar as técnicas "Google bombing" para obter colocação de destaque no mecanismo de busca:

"Fraudadores que queriam furtrar dinheiro voltado para a ... instituição de caridade para as vítimas do tsunami manipularam as classificações das páginas do Google para assegurar que seu site falso aparecesse primeiro do que o site oficial da instituição."

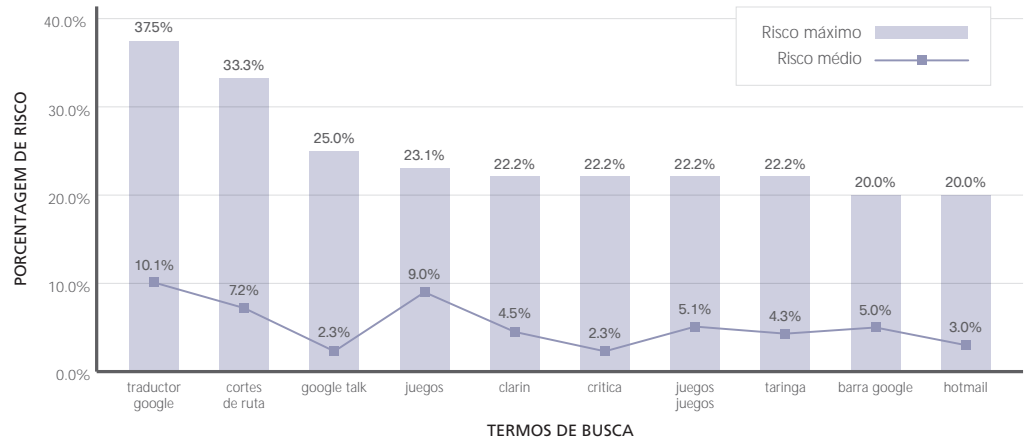
Os mecanismos de busca reagiram e esse tipo de ataque é menos comum e com pouca eficiência hoje do que em 2005. Mas, novos *scams* surgem toda semana para tomar o lugar dos antigos. E assim, a corrida continua.

Para os consumidores, isso significa que confiar na intuição ou conhecer riscos do passado não é o bastante para continuar seguro ao utilizar a web. Até os usuários tecnicamente mais sofisticados correm risco. A melhor proteção é instalar um conjunto de segurança no computador e mantê-lo atualizado, além de utilizar uma ferramenta de busca segura, como o software McAfee SiteAdvisor.

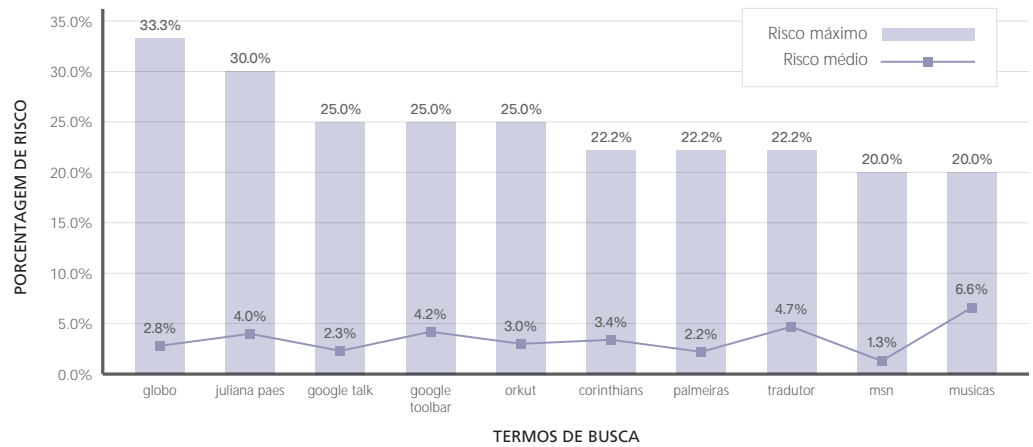
Palavras-Chave de Busca Mais Perigosas por País

América Latina

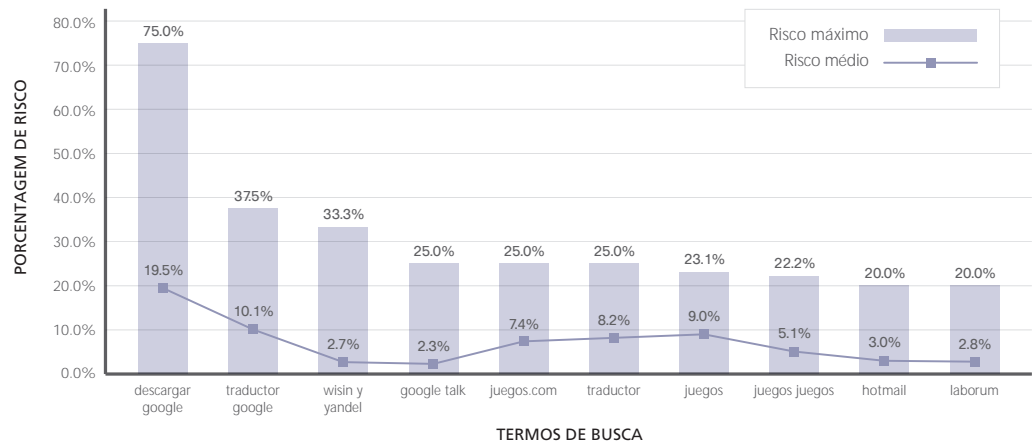
Termos de busca mais perigosos – Argentina



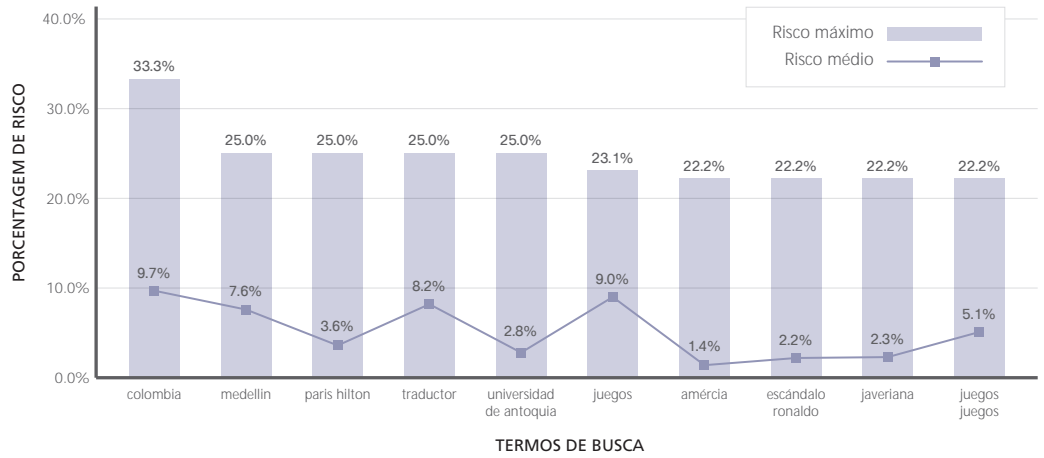
Termos de busca mais perigosos – Brasil



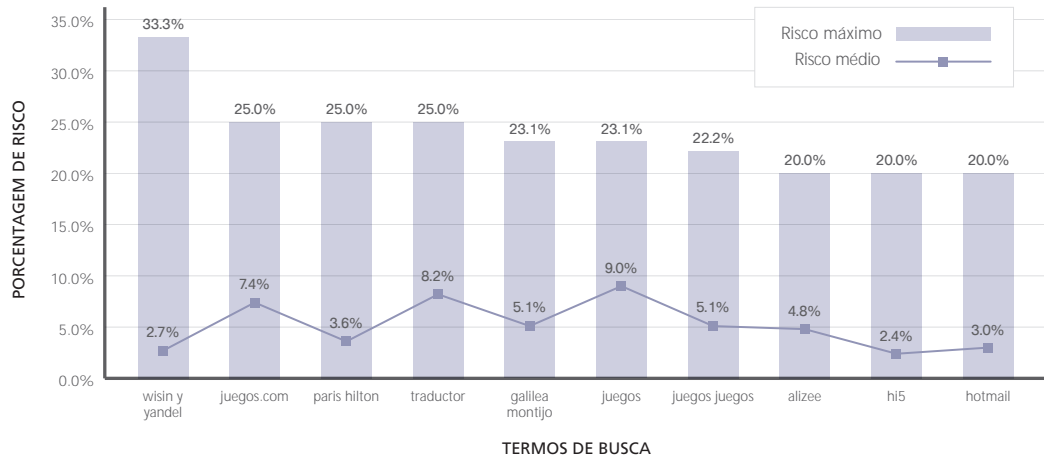
Termos de busca mais perigosos – Chile



Termos de busca mais perigosos – Colômbia



Termos de busca mais perigosos – México



Sobre a McAfee

A McAfee, Inc., com sede em Santa Clara, Califórnia (EUA), é a maior empresa do mundo dedicada à tecnologia de Segurança da Informação. Totalmente comprometida em combater os rigorosos desafios de segurança globais, a McAfee provê soluções proativas e com qualidade comprovada e serviços que ajudam a manter sistemas e redes protegidos mundialmente, permitindo aos usuários conectarem-se à Internet, navegarem e realizarem compras pela Web com segurança. Apoiada por uma equipe de pesquisas premiada, a McAfee desenvolve produtos inovadores que capacitam os usuários domésticos, as empresas dos setores público e privado e os provedores de serviços, permitindo-lhes manter a conformidade com as regulamentações de mercado, proteger dados, prevenir interrupções, identificar vulnerabilidades e monitorar continuamente, além de incrementar a segurança em TI.

<http://www.mcafee.com.br>.

