KEY TAKEAWAYS

Mapping the Mal Web

The world's riskiest domains

McAfee

The Web's Riskiest Places To Visit

Here's a real-world situation. Your new Facebook friend sends you a link or you do a web search that leads you to a funny photo of Cameron Diaz. Should you click or close?

Somewhere in the back of your mind, you recall the advice: "Think before you click." That so-called friend may be a cyberscammer, and that link could take you to a site that will install a nasty piece of software called Koobface (an anagram of Facebook). What's the safe decision? How do you pick?
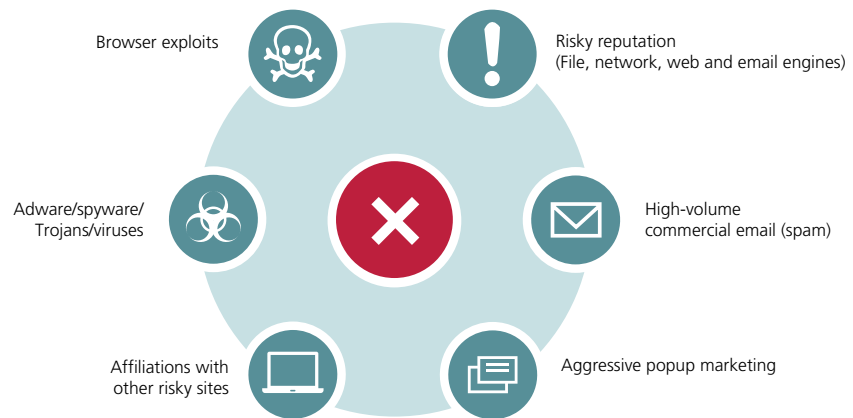
What if we told you that the letters at the end of the URL give you a *huge* clue about the right decision? What if we told you that among these four websites …

- Yourfavoritestore.jp
- Yourfavoritestore.info
- Yourfavoritestore.fr
- Yourfavoritestore.hk

… one of them was more than 100 times more likely to contain malware that could send spam, breach your browser's security, or worse?

Those letters—.JP for Japan, .INFO for the generic Information domain, .FR for France, .HK for Hong Kong, and more than 200 others, including .COM and .EDU—are called top-level domains (TLDs). They are a vital piece of information that the web uses to organize its addresses and are an important clue about where to click.

Clicking search results at random is like playing Russian roulette with your computer, your privacy, and your identity. Based on this year's findings, it's like having one out of 16 chambers loaded.

Security Threats Evaluated by McAfee® Global Threat Intelligence™

Browser exploits

Risky reputation
(File, network, web and email engines)

Adware/spyware/
Trojans/viruses

High-volume
commercial email (spam)

Affiliations with
other risky sites

Aggressive popup marketing

We calculate risk level based on multiple characteristics of each website, including its reputation for good behavior and clean living—healthy or unhealthy associations with other sites and Internet services.

For the fourth year in a row, McAfee has studied millions of websites (27 million this year!) to create the "Map of the Mal Web." This year, risk reached the highest levels ever, with 6.2% of the sites we evaluated showing signs of risk. Compare that to 5.8% in 2009 and 4.1% the previous two years.

What you do not know is that scam artists, cybercrime bosses, hackers, and other assorted bad guys are selective. They like some TLDs better than others. And McAfee has figured out which ones.

It turns out that scammers and hackers register their operations in the places where it is easiest to do business or where they see a profit opportunity from misspellings or logical associations. For instance, since it is easy to leave out the "O" in a .COM address, an unscrupulous player might register in Cameroon (.CM) for the www.mcafee.cm address, hoping to skim traffic from anyone concerned about security.

Why Should You Care?

Simply viewing a web page can return malicious code that steals your password and identity information, takes advantage of security holes in your computer, or takes over your computer. It can be expensive, embarrassing, and really tricky to get your computer—or your identity—back.

We think that if you know in advance that three out of five sites in one TLD are risky, you can choose a different place to download that photo you are searching for. For instance, despite Vietnam's growing allure as a vacation destination, visitors to sites registered in Vietnam (.VN) should consider it a "no fly" zone. This year, .VN splashed into our top five as one of the riskiest TLDs on the Internet, with 58% of the sites we track containing malicious or potentially dangerous content and activities.

This year Vietnam (.VN) splashed into our top five riskiest TLDs, with 58% of the sites we track containing malicious or potentially dangerous content and activities.
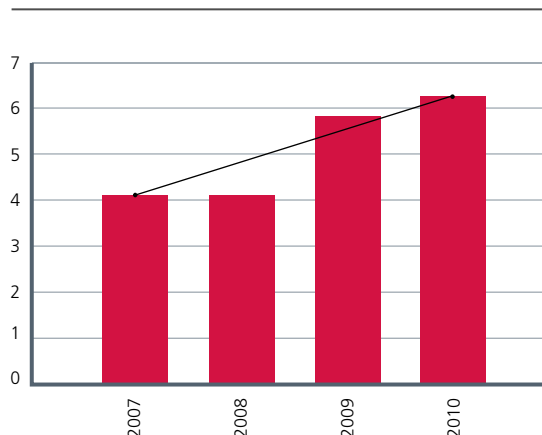
The 2010 Results

Generally, Internet threats are increasing. Criminals are working to make their activities harder to detect—and harder to police.

- **Risk is rising**—The overall weighted average of risky sites rose from 5.8% (2009) to 6.2% (2010). The web is getting trickier to navigate safely, even for the savviest users.

- **Heavy traffic = big risk at .COM**—With a 3 in 10 chance of hitting a risky site, .COM (Commercial—the most heavily trafficked TLD) was the riskiest TLD this year (using our weighted risk system).[1] Koobface malware, dangerous code that spreads through social networking sites like Facebook and Twitter, was associated more with .COM than any other TLD.

- **.INFO records risky information**—.INFO (Information) moved up to second place from fifth place last year. Spammers continue to plague this TLD. Many risky .INFO sites assist with the hosting of content used for spam campaigns, from pharmaceuticals and watches to malware and fake anti-virus.

Percentage of Risky Sites on the Web

- **The worst offenders**—Overall, the five TLDs with the greatest percentage of risky registrations were:
  - .COM (Commercial)   31.3%
  - .INFO (Information)   30.7%
  - .VN (Vietnam)   29.4%
  - .CM (Cameroon)   22.2%
  - .AM (Armenia)   12.1%

- **A world of risk**—Our leading risky TLDs include TLDs from three continents, from Asia to Europe to Africa, and two generic TLDs, both operated from the Americas. The Europe, Middle East, and Africa (EMEA) region again won the dubious distinction of having the most risky TLDs in the top 20, with seven entrants, including top 20 newcomers Armenia (.AM) and Poland (.PL).

- **Some big improvements**—Singapore (.SG) deserves recognition for falling in risk from last year's number 10 slot to number 81 this year; Venezuela (.VE) dropped from 21 to 88 this year; and the Philippines (.PH) moved from number 6 in 2009 to number 25 this year.

- **Squeaky clean**—The five TLDs with the fewest domains rated risky were:
  - .TRAVEL (Travel and Tourism Industry) .02%
  - .EDU (Educational)   .05%
  - .JP (Japan)   .08%
  - .CAT (Catalan)   .09%
  - .GG (Guernsey)   .10%

Lessons to Learn

Although risks are up, by taking a few precautions when you travel online, you can still search and surf the Internet with confidence.

This year, 6.2% of the sites we track contained malicious or potentially dangerous content and activities such as:

- **Malware**—Code that can damage your system, steal data, or allow your computer to be controlled by someone else.

- **Browser exploits**—Attacks and malware that take advantage of vulnerable software on your computer.

- **Phishing**—Fake sites designed to "phish" for information or install malicious code.

- **Spamminess**—Sign-up forms that will lead to lots of commercial email, or spam.

- **Risky affiliations**—Sites with links that take you to a malicious site, and sites that have suspicious relationships, such as shady hosting services.

- **Pay attention to the TLDs**—Look at the TLD license plates you encounter while driving the Internet. Use the charts that follow to steer toward safety and bypass risk.

- **Don't assume that the "most popular" sites are safe havens**—Expect risk in high-traffic zones, such as .COM (the riskiest TLD) and sites listed on popularity charts like Alexa. Some malware-infested sites use search engine optimization techniques to jet into the top Internet listings.

- **Be suspicious: some threats are silent**—Invisible content is easy to place on an innocent-seeming web page. When you visit, malware downloads without your clicking to accept any software. It's best to use safe searching software like McAfee SiteAdvisor® before you visit a new site. Don't click if the site is rated red or yellow.

- **Look out for risky pages on safe domains**—Our site ratings are based on overall site assessments, rather than ratings of individual pages. You should be aware that there are still risks within individual URLs on generally safe domains; we find quite a few risky page-level URLs on .EDU (Educational) sites, for instance.

- **Look for disguised threats**—The URL you can see is just the front door. A URL shortening service (like TinyURL or bit.ly) might disguise the real location of the content. It could be anywhere, including a shareware site like RapidShare. While anti-virus updates help against some kinds of malicious content, you also need comprehensive security software that constantly analyzes the files you are downloading, looking for the very newest malicious content. One example is McAfee Total Protection™ software, which checks every file for up-to-the-minute versions of freeloading spyware, keyloggers, and Trojans.

- **Choose your "friends" wisely**—Many Facebook users accept "friend" requests from total strangers or unknown friends of friends. This lax attitude makes a criminal's work easy, since malicious or disguised links can be included in posts and messages from friends who enjoy "transitive trust." I trust you, so I can trust your recommendations, right? Since 2008, the malicious Koobface code has been exploiting these trust networks to find new victims.[2] Don't "friend" people you don't know.

[2]Craig Schmugar, "Koobface remains active on Facebook," McAfee Labs Blog.
www.avertlabs.com/research/blog/index.php/2008/12/03/ koobface-remains-active-on-facebook/

Proceed with Care

The Internet has become the focal point of social networking, entertainment, and information—as well as criminal activity. Risk is widely distributed throughout the web. Risks are growing, changing quickly, and getting harder to detect. Yet the security community and the TLD registrar community continue to fight back, and win. Some of the worst offenders on last year's report were some of the most improved this year.

You can surf carefully—even confidently—if you keep your eyes open for risky activities. And consider a little real-time guidance. Today, even the most experienced users rely on the assistance of comprehensive, up-to-date security software with safe search functionality.

To read the full *Mapping the Mal Web* report and learn more about threats and how to counter them, visit the McAfee Security Advice Center.

Rankings

Top 10 Riskiest TLDs

HIGH RISK ▮▮▮▮▮▮▮▮ **LOW RISK**

Country or Name	Region	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	Total Domains Tracked	Total Risky Domains
Commercial	Generic	COM	1	31.3%	6.1%	2	32.2%	-2.8% ↓	15,530,183	948,995
Information	Generic	INFO	2	30.7%	46.6%	5	15.8%	94.5% ↑	533,711	248,806
Vietnam	APAC	VN	3	29.4%	58.0%	39	0.9%	3,107.9% ↑	24,988	14,492
Cameroon	EMEA	CM	4	22.2%	44.2%	1	36.7%	-39.5% ↓	3,947	1,746
Armenia	EMEA	AM	5	12.1%	24.2%	23	2.0%	512.9% ↑	3,145	760
Cocos (Keeling) Islands	APAC	CC	6	10.5%	20.2%	14	3.3%	215.4% ↑	58,713	11,869
Asia-Pacific	APAC	ASIA	7	10.3%	20.6%	N/A	N/A	N/A	3,122	642
Network	Generic	NET	8	10.1%	10.5%	7	5.8%	73.7% ↑	1,556,813	163,466
Russia	EMEA	RU	9	10.1%	16.8%	9	4.6%	116.7% ↑	329,136	55,373
Western Samoa	APAC	WS	10	8.6%	16.9%	4	17.8%	-51.8% ↓	22,070	3,734

Top 10 Least Risky TLDs

HIGH RISK ▮▮▮▮▮▮▮▮ **LOW RISK**

Country or Name	Region	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	Total Domains Tracked	Total Risky Domains
Travel and Tourism Industry	Generic	TRAVEL	106	0.0%	0.0%	92	0.2%	-88.6% ↓	2,013	1
Educational	Generic	EDU	105	0.1%	0.1%	102	0.1%	-48.6% ↓	14,002	15
Japan	APAC	JP	104	0.1%	0.1%	103	0.1%	6.6% ↑	464,408	547
Catalan	Sponsored	CAT	103	0.1%	0.2%	99	0.1%	-31.6% ↓	3,936	7
Guernsey	EMEA	GG	102	0.1%	0.2%	57	0.6%	-81.1% ↓	12,092	25
Croatia	EMEA	HR	101	0.1%	0.2%	100	0.1%	-11.1% ↓	22,511	50
Ireland	EMEA	IE	100	0.1%	0.2%	101	0.1%	-5.7% ↓	32,120	71
Switzerland	EMEA	CH	99	0.1%	0.3%	95	0.2%	-13.3% ↓	217,863	572
Australia	APAC	AU	98	0.2%	0.3%	93	0.2%	-4.3% ↓	256,103	871
Slovenia	EMEA	SI	97	0.2%	0.4%	79	0.3%	-36.6% ↓	11,339	48

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse and shop the Web more securely. Backed by unrivaled McAfee Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee secures your digital world.

www.mcafee.com