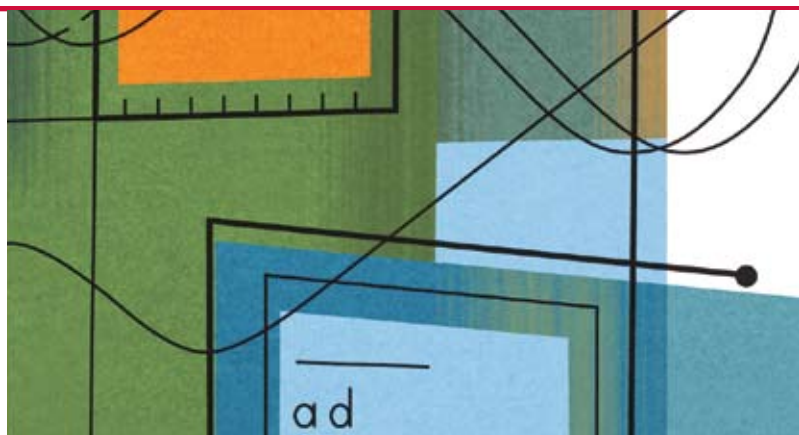


Unintended Adventures In Browsing

By Benjamin Edelman



Browse the web, and you may be exposed to a variety of attacks that are well chronicled in the *McAfee Security Journal*.

From malicious banners to adware bundlers, the sites you *intend* to visit may cause remarkable harm. But users should also be aware of the sites they do not intend to visit—the sites they stumble across by accident.

Basic Strategy

For those of us who sometimes slip up when typing a URL, there's a special kind of security threat to watch out for. This plague of the imperfect typist is called typosquatting. The typosquatter strategy is to anticipate domain names users might accidentally "request." Consider a user who misspells "bankofamerica.com" by doubling the "k" and dropping the "e" to yield "bankkofamrica.com." Ordinarily, that user would receive a browser error message, directing the user to the real Bank of America site. But suppose a typosquatter had anticipated the user's error. The typosquatter might register the misspelled domain (and several other inaccurate names) in hopes that users will eventually wander in.

Historically, typosquatters primarily focused on spelling errors—inserting a stray letter, dropping a letter, or transposing two letters. But recently typosquatters have found other tricky ways to attract unintended traffic. Suppose a user omits the period that separates "www" from a site's domain name, for example, "wwwmcafee.com" instead of "www.mcafee.com." Typosquatters can register that domain. (As it turns out, someone did! And McAfee is working to recover it.) In the case of trailing periods, typosquatters rightly anticipate that web browsers will automatically append a ".com" to a domain with no top-level domain—

so squatters also claim domains such as "www.mcafeecom.com." Still other squatters focus on adding "http" prefixes, or registering the corresponding .com's for domains that actually reside in other top-level domains.

How do users end up at these typosquatting sites? Some users may forget a site's correct spelling. Others make typing errors. (Consider non-native English speakers, users with poor eyesight, and users still improving their typing skills.) Novice users may not realize the correct punctuation of a site's full address, and hurried users may wrongly enter part of a URL. Even the most sophisticated user can make an entry error on a mobile device with a small keyboard, on a handwriting-recognition tablet, or during a bumpy ride in a moving vehicle. So it would be wrong to blame the users who "request" typosquatting sites. On the contrary, although users certainly end up at these sites, they generally get there by mistake.

The Scope of Typosquatting

With many users making a wide variety of errors, typosquatting has become remarkably widespread. The McAfee SiteAdvisor® service runs ongoing searches for typosquatters, and in the McAfee Avert Labs' May 2008 examination, we found more than 80,000 domains typosquatting on just the top 2,000 web sites. Go deeper into the web, and typosquatting grows even more.

Domains frequented by kids are particularly rich targets for typosquatters. For example, a recent analysis identified 327 different typosquatting registrations that are all close variants of “cartoonnetwork.com.” Freecreditreport.com led the list compiled with SiteAdvisor technology; also popular were YouTube, Craigslist, Wikipedia, and Bank of America. (For the numbers, see Figure 1. And for examples of creative misspellings, see Appendix.)

Legal Response

In general, typosquatting is illegal in the United States. The 1999 Anti-cybersquatting Consumer Protection Act (ACPA), 15 USC §1125(d), prohibits registering, trafficking in, or using domain names that are identical to, or confusingly similar to, a trademark or famous name. The ACPA grants damages of a typosquatter’s ill-gotten profits (15 USC §1117(a)(1)), or statutory damages of \$1,000 to \$100,000 per typosquatting domain (as the court considers just) (§1117(d)).

Other countries’ laws treat typosquatting somewhat differently, but most nations view typosquatting as a genre of trademark infringement—hence it is prohibited. Furthermore, the Uniform Dispute Resolution Policy (UDRP) establishes arbitration for

complaints about infringing domains. To register a site in a major top-level domain, a registrant must agree to the UDRP’s jurisdiction, so the UDRP applies regardless of the location of the typosquatting site. That said, UDRP remedies are limited to the forfeiture of an infringing domain without a payment of money damages.

Although the ACPA imposes significant penalties, typosquatters seem to realize that enforcement is unlikely. So despite the threat of major sanctions, typosquatters continue to operate with abandon.

Typosquatters’ Profit Strategy

Once a user arrives at a typosquatting site, the squatter wants to make as much money as possible.

Some years ago, notorious typosquatter John Zuccarini forced his unwitting visitors to view sexually explicit web sites they did not want and had not requested. Zuccarini registered at least 8,000 domains, which I documented at length.¹ But he didn’t get away with this scam forever: In September 2003, Zuccarini was arrested for violation of the Truth in Domain Names Act, which specifically prohibits any action that “uses a misleading domain name with the intent to deceive a person into viewing obscenity.”

These days, the typosquatters standard approach is advertising. Among the thousands of typosquatting domains I’ve examined in the past several years, it’s rare to find one *not* showing ads.

DOMAIN	NUMBER OF TYPOSQUATTING DOMAINS
freecreditreport.com	742
cartoonnetwork.com	327
youtube.com	320
craigslist.org	318
blogspot.com	276
clubpenguin.com	271
wikipedia.com	266
runescape.com	264
miniclip.com	263
bankofamerica.com	251
dailymotion.com	250
metrolog.com	249
addictinggames.com	248
friendster.com	246
myspace.com	239
verizonwireless.com	238
facebook.com	235

Figure 1: Typosquatting’s most-popular list. This table reports a selection of trademarks highly targeted by typosquatters. The data comes from the May 2008 examination of the SiteAdvisor service data set.

The McAfee SiteAdvisor service runs ongoing searches for typosquatters, and in the McAfee Avert Labs’ May 2008 examination, we found more than 80,000 domains typosquatting on just the top 2,000 web sites.

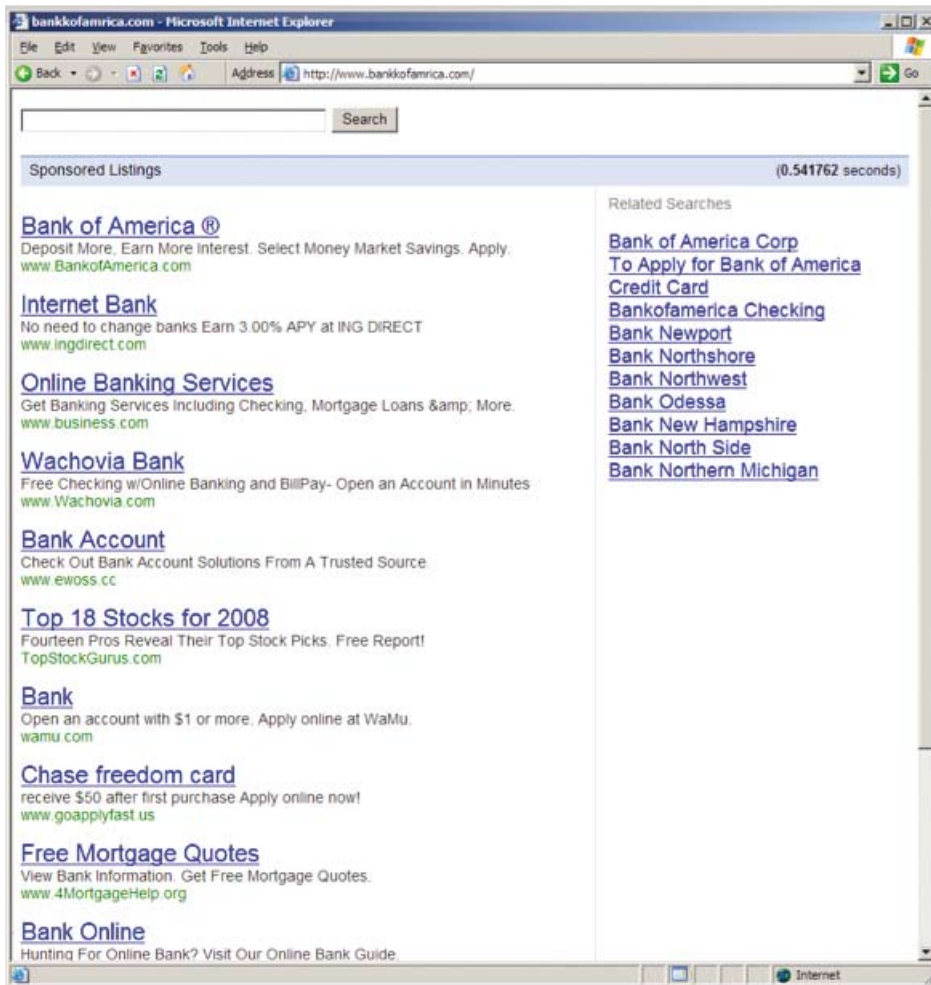


Figure 2: A typosquatter registers a domain name similar to a leading bank's, and then—indirectly—sells advertising links to that and other banks.

When typosquatting sites show ads, they typically attempt to select ads “relevant” to the site the user was (in all likelihood) trying to reach. So in the bankkofamrica.com example we mentioned, the resulting ads promote—predictably—banks. Which banks? First on the list is Bank of America itself. (See Figure 2.) Surprised? On the one hand, that ad placement is useful for Bank of America: At least they manage to reach the customer, despite the customer’s typographic error. But on the other hand, it’s remarkable for this typosquatter to ask Bank of America to pay to reach a customer who already requested Bank of America by name. After all, the typosquatter is infringing Bank of America’s trademark, exactly in violation of the ACPA, which says that the typosquatter can’t register such domains and that

the typosquatter even has to pay Bank of America high statutory damages if the bank files a suit. But instead, the typosquatter ends up selling advertising space to Bank of America—which, at least initially, may be none the wiser.

How is this possible? Typosquatters don’t directly sell space to advertisers. (Imagine the conversation: “We’d like to show your ads on our typosquatting site?” “You want to put our ads where?”) Instead, typosquatters sell their inventory to ad networks, which in turn recruit advertisers. The largest network in this space is Google, whose AdSense for Domains product and other domain-syndication products serve ads on more than 80 percent of the typosquatting sites recently uncovered by SiteAdvisor technology.

What's Next for Typosquatters?

In June 2008, the Internet Corporation for Assigned Names and Numbers (ICANN) voted to speed the process of creating more top-level domains. Beyond the familiar domains most users know, there are already lesser-used domains such as .info, .biz, .museum, and .travel. Soon, we can expect new domains like .nyc or .lib (as some have suggested). More top-level domains mean more opportunities for cybersquatting—for exact registration of famous trademarks, or for close typographic variations of famous names. When users request these domains—whether in misguided attempts to reach the “real” sites, or in mistaken attempts to recall sites’ true addresses—typosquatters can jump in with their infringing interlopers.

But there are signs that typosquatting may soon be on the decline. For one, some major web sites have taken action to protect themselves and their customers from typosquatters. For example, in 2006, Neiman Marcus sued domain registrar Dotster. Neiman Marcus alleged that Dotster registered scores of domains infringing Neiman Marcus marks, showing ads to maximize its revenues from these typosquatting sites. Neiman Marcus claimed Dotster acted not just as registrar for these domains, but also as registrant, choosing which domains to register, and reaping the profits from resulting ads. The case settled in 2007 on confidential terms, and Neiman Marcus has since gone on to sue other large squatters. (Disclosure: I served as a consultant to Neiman Marcus in some of these cases.) Verizon and Microsoft have also been vigilant in similar litigation. On one hand, these cases aren’t particularly prevalent. But the ACPA’s statutory damages—\$1,000 and more per domain—can force typosquatters to pay big money for their large-scale infringements. Microsoft alone has received more than \$2 million in typosquatting settlements.

Further, persistent rumors suggest top ad networks, particularly Google, may abandon the typosquatting industry. Recent trademark-holder class-action litigation has challenged Google’s role in funding the typosquatting industry, and these typosquatting placements have been a repeated source of advertiser and trademark-holder complaints. If Google ceased funding typosquatting,

typosquatters would have far less incentive to register infringing domains; no other ad network is likely to pay typosquatters as much as Google does. (Disclosure: I serve as co-counsel in *Vulcan Golf, et al., v. Google, et al.*, trademark-holder class-action litigation regarding Google’s responsibility for the typosquatting sites where Google pays to place ads.)

Defenses

Though the typosquatting battles continue, concerned users can do plenty to protect themselves. First, be careful when you type. Be alert for typosquatting, particularly when requesting a site that’s hard to spell. Guessing a domain name may not be the best choice; consider using a search engine instead.

Second, after arriving at a site, look twice before you proceed. Is this really the site you intended to reach? Is this link an ordinary pointer, or a paid advertisement? Should this government site really be a .com, or did you want the corresponding .gov? A bit of critical thinking may serve you well as a defense against typosquatting or other attacks.

Appropriate software can also help protect users from typosquatters. SiteAdvisor technology identifies many typosquatting sites. A typo-protection service, such as OpenDNS, provides additional protection. Search engines typically offer help—“Did you mean? ...” spelling correction—so that users can avoid many typosquatting sites by running searches instead of typing domain names directly into a browser’s address bar.



Benjamin Edelman is an assistant professor at the Harvard Business School, where he studies electronic marketplaces and online fraud. He is also a special advisor to McAfee for the SiteAdvisor service, offering an independent perspective to supplement SiteAdvisor site ratings. Though a fast and accurate typist, Professor Edelman has occasionally embarked on unintended browsing adventures.

ENDNOTES

- 1 “Large-Scale Registration of Domains with Typographical Errors,” January 2003. Harvard Law School. (http://cyber.law.harvard.edu/archived_content/people/edelman/typo-domains/)

APPENDIX

Examples of Typosquatting Sites: Cartoonnetwork.com

Among the more than 80,000 domains in SiteAdvisor’s May 2008 examinations we found these typosquatting variations of cartoonnetwork.com:

c卡通network.com	ck卡通network.com	ca卡通network.com
dc卡通network.com	jc卡通network.com	cu卡通network.com
nc卡通network.com	vc卡通network.com	ac卡通network.com
cf卡通network.com	ca卡通network.com	bc卡通network.com
ce卡通network.com	ca卡通network.com	can卡通network.com