Search

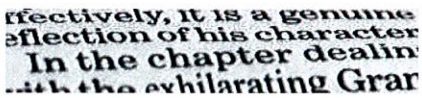
CADNA
The Coalition Against Domain Name Abuse
EDUCATION · ADVOCACY · COLLABORATION

OUR MISSION

CADNA works on behalf of the public interest to combat cybersquatting and cyber criminals for a safer, more rewarding online experience. Through education, advocacy, and collaboration, we seek a strong and effective national policy to deter online criminals and protect all Internet users.

Events

Read More »



Newsroom

Read More »

Blog

Read More »

About Us
Contact Us
Privacy Policy

1000 Potomac Street. NW
Suite 350
Washington, DC 20007

(202) 503-8649

Developed by Think Up Themes Ltd. Powered by Wordpress.

Search

CADNA
The Coalition Against Domain Name Abuse
EDUCATION | ADVOCACY | COLLABORATION

ABOUT CADNA

Our Mission

CADNA works on behalf of the public interest to combat cybersquatting and cyber criminals for a safer, more rewarding online experience. Through education, advocacy, and collaboration, we seek a strong and effective national policy to deter online criminals and protect all Internet users.

Think you might be a victim of cybersquatting? Start here.

Our Goals

The Coalition Against Domain Name Abuse, Inc. (CADNA), a 501(c)(6) not-for-profit corporation founded in 2007, seeks to make the Internet a safer and less confusing place for consumers and businesses alike. Its goal is to decrease instances of cybersquatting in all its forms by facilitating dialogue, effecting change, and spurring action on the part of policymakers in the national and international arenas.

Led by Joshua S. Bourne, President, and Amalia Feld, Director, CADNA is dedicated to building awareness about and advocating action to stop illegal and unethical infringement of brands/trademarks online. Taking action against the practices of cybersquatting, CADNA provides a framework for brand owners to protect themselves—as well as their investors, customers and partners—from illegal trademark infringement. CADNA works to reduce online infringement across all top-level domains (TLDs).

The Coalition also holds educational forums, where leading brand owners gather to confront the challenges of cybercrime and to learn about best practices and strategies to combat it.

CADNA has held 15 events in 10 cities across the globe, featuring such speakers as Representative Bob Goodlatte, Representative Tom Marino, and Senator Bob Dole; Utah State Senator Stephen Urquhart; law enforcement specialists; and

brand owners across a spectrum of industries whose common goal is to protect the overall integrity of the Internet for brand owners and consumers.

U.S. LEGISLATION

Through education and advocacy, CADNA works with U.S. federal and state legislatures to update appropriate laws and increase deterrents against cybersquatting, a practice that enables malware, phishing schemes, counterfeit sales, and confusion. Read about our proposed U.S. federal legislative reform here.

CADNA works to:

- Increase penalties for cybersquatting and cybercrime to deter these practices
- Educate elected officials about domain-related policy reform that will improve consumer safety
- Make the monitoring and enforcement of online infringements more manageable for trademark owners so they can better protect consumers in a timely manner

INTERNATIONAL LEGISLATION

Cybersquatting and cybercrime are international problems that can only be reduced through a coordinated, international effort. CADNA works with international policy makers to move towards a global solution for cybersecurity.

INTERNATIONAL CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN)

ICANN "defines policies for how the 'names and numbers' of the Internet should run" through a "bottom-up, consensus-driven, multi-stakeholder model". CADNA supports ICANN's multistakeholder approach to policy development and participates in the process through ICANN's Business Constituency.

CADNA works to:

- Implement policies within ICANN that discourage registrants and others who enable domain abuses.

Our Members

CADNA member organizations represent a cross-section of global brand leaders that recognize the critical important of protecting brands and Internet users from cybersquatting.

Search

CADNA
The Coalition Against Domain Name Abuse
EDUCATION | ADVOCACY | COLLABORATION

KNOW YOUR NET – BUSINESSES

In 2014, Internet users who were used to seeing .COM or .ORG websites are starting to also see things like .CLOTHING and .GURU. In fact, the Internet will expand to over a thousand of these new gTLDs that users will have to navigate online.

Brands – whether or not they applied for a .BRAND of their own – will find themselves on a level playing field. The most secure, innovative, and exciting places online will be up for grabs. But as brands and entrepreneurs try new ways to deliver content to Internet users, consumers will be navigating potentially dangerous territories.

Cybersquatters register domain names containing brand names, or typos of brand names, to take advantage of consumers' trust in those brands and consumers' confusion when they land on a cybersquatted page – they do it now in extensions like .COM and .INFO, and they are already starting to do so new extensions as well.

According to recent research, 1 out of 20 Internet users know nothing about new gTLDs. However, with just a small amount of information, comfort with new extensions rose by 11%. Consumer education is a major tool for protecting brands and their consumers from bad actors who could take advantage of Internet user confusion.

- Educating them about the new gTLD program and what to look for: they can start here.
- Maintaining clear and consistent branding and naming conventions across your domain name portfolio.
- Defensively registering domain names that your consumers are likely to visit.
- Keeping track of popular scams and provide that information to your consumers.
- Having a clear place for customer service, where consumers can report suspicious activity on potentially cybersquatted sites.
- Coordinate with law enforcement – contact the Internet Crime Complain Center to let them know your consumers are being misled by a cybersquatted site: http://www.ic3.gov/default.aspx.

Search

CADNA
The Coalition Against Domain Name Abuse
EDUCATION | ADVOCACY | COLLABORATION

About CADNA | What is the Problem? | What Can You Do? | Blog | Newsroom | Glossary

Contact Us

KNOW YOUR NET – INTERNET USERS

TheInternet is preparing for its largest expansion in a generation with the imminent addition of 1,400 Top Level Domains (TLD) to the approximately 22 that are now in common use in the United States, including .COM, .EDU, .INFO, .BIZ and others. Internet users will be able to navigate, for example, to new generic TLDs, such as .SHOP or .NYC and to branded TLDs, such as .AMERICANEXPRESS OR .ATHLETA.

This expansion, while anticipated to bring innovation to the web, will also expand the opportunity for bad actors to take advantage of unwary consumers. The expansion will impact Internet use in many other ways, in terms of safety, security, consumer targeting, product branding, navigation, and advertising.

Internet users can arm themselves with information abot this coming change and practice caution to make the experience safe and rewarding.

Fact 1:

Many major brands will launch .BRANDS. Many will stick with their .COM sites.

What does that mean for you?

There will be no standard way to look for your favorite brands. But you can also be sure of the authenticity and security of a .BRAND site because all the content provided on that gTLD is assuredly from that brand

Fact 2:

Many new generic TLDs will be open, such as .SHOPPING, or .SKI, where entrepreneurs will sell second-level domains to the public. Others will be closed, such as .MERCK or .NISSAN, owned and operated by major brands with no second-level domains for sale. A third category such as .Pharmacy, will sell second-level domains to specific categories of registrants.

What does this mean for you?

Unless you are sure that an extension is owned by a trustworthy source – say, a brand or a trade association – new TLDs should be treated with the same caution that you would exercise navigating to a .COM or a .INFO site. Know where you are going and

with whom you are communicating.

Fact 3:

New geographic extensions, such as .NYC and .PARIS, will be available, owned and operated by entrepreneurs who will sell secondary domain names to the general public.

What does this mean for you?

Geographic extensions should be visited with the same caution you would use in visiting a .COM site.

Staying Safe Online – Now, and in the Future

1. **Stay Alert**
   Just because a domain name seems to have a brand name in it, does not necessarily mean that it is providing authentic content. Cybersquatters register domain names containing brand names, or typos of brand names, to take advantage of consumers' trust in those brands. They do it now in extensions like .COM and .INFO, and they will in some of the new extensions. Cybersquatters divert traffic away from legitimate sites, cost businesses in lost revenue and consumer trust, link to advertisements that frustrate consumers, send malware, and deceive consumers into divulging personal information.
2. **Be skeptical**
   Small, subtle changes to a website with which you were familiar may mean it is cybersquatted. Any website that offers a chance to win a free product may be cybersquatted. A website that prompts you to submit personal information may be cybersquatted. A website that resolves to a page with nothing but advertisements may be cybersquatted.

Tips for Navigating Content Online

When looking for branded content, navigate to domain names that have been clearly advertised, that you trust, or that are trusted by people you trust.

Scrutinize websites that you aren't familiar with before divulging personal information.
If you come across a cybersquatted website, contact law enforcement through this portal: http://www.ic3.gov/default.aspx.