Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Best Practices for Use of Look-Alike Domains for Security Purposes

September 2025

The reference URL for this document: m3aawg.org/lookalike-domains-bcp-2025

Table of Contents

Introduction

The goal of this document is to recommend best practices to parties who are considering the registration of look-alike domain names for legitimate, active security, or security-related research purposes. Below, we explore the legal and operational issues associated with the registration and use of such domains. This document is **not** intended for legal advice; please consult your company's legal counsel.

Background

Cybersecurity companies and security researchers sometimes register and use domain names that contain trademarks owned by other organizations. These "look-alike" domains may contain letter-for-letter representations of a trademarked brand name or term, or misspellings or variations thereof.[1] These domains are registered and used for purposes including security simulations, training that helps employees learn to recognize phishing attempts, spam traps, and sinkholing techniques. (Criminals also register domain names that infringe on brand names, notably to perpetrate phishing and scams.) The registration and use of look-alike domains for security-related purposes can cause confusion and difficulties for various parties – including the brand owner, internet users, and reputation blocklist providers – and may present legal issues.

This guidance does not apply to domain registrations made solely for brand protection, trademark defense, or marketing-related objectives.

Legal Considerations

Trademarks are a form of intellectual property. Their primary function is to identify the source of goods or services and prevent consumers from confusing them with those from other sources.

The registration and/or use of a domain containing a trademark, or a confusingly similar variation, can pose problems for both the registrant and the trademark holder. Trademark infringement is the unauthorized use of a trademark (or service mark) on, or in connection with, goods and/or services in a manner that is likely to cause confusion, deception, or mistakes about the source of the goods and/or services. Most countries have laws that cover trademark infringement, and their criteria vary. Courts typically consider evidence addressing various factors such as the likelihood of consumer confusion, how and where the parties' goods or services are used, and the defendant's intent when it adopted the trademark's use.

The Uniform Domain Name Dispute Policy (UDRP)

The UDRP[2] is used to adjudicate disputes about domain names that contain a complainant's trademark or a confusingly similar variant. The UDRP is used in all generic top-level domains (gTLDs) and some country-code TLDs (ccTLDs), and all registrants in those TLDs are required to submit to the UDRP

[1] Variations of the term *Trademark* would include *tradmark.com, trademark-mail.org, securetrademark.de,* etc.
[2] UDRP https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/uniform-domain-name-dispute-resolution-policy-01-01-2020-en

procedure. Mark owners can also use the courts to seek relief. For example, the U.S. Anticybersquatting Consumer Protection Act (ACPA)[3] contains criteria similar to the UDRP.

Under the UDRP, the criteria establishing bad faith includes "by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your website or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location." A registrant can establish its legitimate interest to use the domain if it is making "a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue."[4,5]

UDRP decisions and lawsuits under various national trademark laws have consistently found that violating domains do not need to exactly match the spelling of the trademark. The addition of other terms in the domain name (whether descriptive, geographical, pejorative, meaningless, or otherwise) may not prevent a finding of confusing similarity.

In UDRP cases, the presence of a DNS mail exchange (MX) record can be considered "use" of the domain. The complainant need not prove that such a communication has been sent; it is sufficient that such a communication *could* be sent. Precedent-setting cases have stated, "Where the use of the disputed domain name sets up the Respondent to engage in behaviour that would falsely imply an affiliation with the Complainant, that is a use of the disputed domain name in bad faith."[6]

Cases involving look-alike domain names used for anti-phishing training illustrate how registrants and trademark holders may differ in their opinions, and how legal outcomes may depend on case-specific details. In one UDRP case, the trademark owner prevailed, with the UDRP panelist finding the registration and use were in bad faith.[7] In a similar case, the UDRP panel found that the respondent did not act with obvious bad faith and the respondent was allowed to keep the domains. However, the panel noted that it made "no findings concerning the parties' rights under applicable national law," a matter that was perhaps "better suited for determination by a court."[8]

---

[3] 15 U.S.C. § 1125(d). https://www.law.cornell.edu/uscode/text/15/1125

[4] UDRP, section 4. https://www.icann.org/resources/pages/policy-2024-02-21-en

[5] For more about fair use, see "Fair Use of Trademarks (Intended for a Non-Legal Audience)," International Trademark Association. https://www.inta.org/fact-sheets/fair-use-of-trademarks-intended-for-a-non-legal-audience/

[6] Regarding MX records, see *bioMérieux v. Registration Private, Domains By Proxy, LLC / Milton Bardmess,* WIPO Case No. D2020-3499. https://www.wipo.int/amc/en/domains/decisions/text/2020/d2020-3499.html and *PrideStaff, Inc. v. Privacy service provided by Withheld for Privacy ehf / Mike Gregor,* WIPO Case No. D2021-2030. https://www.wipo.int/amc/en/domains/decisions/text/2021/d2021-2030.html

[7] *Facebook, Inc. and Instagram, LLC v. WhoisGuard Protected, WhoisGuard, Inc. / Phishing Operations, Wombat Security Technologies*, WIPO Case No. D2020-3218. https://www.wipo.int/amc/en/domains/decisions/text/2020/d2020-3218.html
The respondent in the UDRP case (Wombat, a.k.a. Proofpoint) then filed a U.S. court case against Facebook, seeking to establish that its actions were "not unlawful" under the Anticybersquatting Consumer Protection Act (ACPA) and Lanham Act (*Proofpoint Incorporated v. Facebook Incorporated*, 2:21-cv-00226). The plaintiff dismissed the case without prejudice and the merits of the case were never adjudicated.

[8] See *Aetna Inc. v. On behalf of help-aetna.com owner / Whois Privacy Service / Manager / Knowbe4,* WIPO Case No. D2021-1565. https://www.wipo.int/amc/en/domains/decisions/text/2021/d2021-1565.html

Typosquatting

Typosquatting is the practice of registering a misspelling of a brand owner's domain name. Internet users sometimes make typographical errors when they type a domain name into a web browser or email client; this directs traffic to the look-alike domain. For example, this can allow a party to harvest misaddressed e-mail messages mistakenly sent to the typo domain. While this practice has some practical uses, such as enabling email administrators to observe misconfigurations and to correct data leakage, handling such data presents legal and ethical issues.

The practice of typosquatting is more often associated with taking web users to ad pages. This can cause user confusion and involves collecting money for impressions or clicks, so it is considered a bad-faith use of a domain name, and it runs afoul of the UDRP and ACPA.

Operational Issues

Domain Contact Data

The domain name's registration record (available via a domain directory service, i.e., WHOIS and RDAP) is often the first resource a brand owner consults when it learns of a domain name that is a potential intellectual property violation, or is being used to perpetrate an abuse such as phishing. But the domain record usually will not reveal *who* registered the domain name, making it difficult for the brand owner to judge the registrant's purposes or motives. As of this writing, only 10.8% of gTLD domain records reveal the identity of the actual registrant. (About 58% of all gTLD domains have the real registrant's identity hidden behind a proxy service, and 30% have the contact data redacted by the registrars.) These identity protections are usually applied by the registrars automatically.[9] This situation can force a brand owner to file a UDRP case without knowing the hidden identity of the domain registrant. The UDRP then requires the domain registrar to reveal the underlying registrant's identity to the UDRP dispute provider.

As stated in the GDPR and ICANN policy, users with a legitimate purpose can request that a domain registrar provide the registrant's contact data if it is hidden behind a proxy contact or redaction.[10] Legitimate purposes include, but are not limited to, the investigation of cybercrime, fraud prevention, intellectual property protection, and coordination of dispute resolution services related to domain names, i.e., UDRP. However, contact data disclosure decisions depend entirely upon the judgment of each registrar and registry operator, who have varying evaluation methods and standards.[11] About two-thirds of contact data requests made via ICANN's contact data request system were denied by the registrars.[12] There is no ICANN appeal process, and the only legal recourse is through courts or the European Data Protection Board, which is expensive and time-consuming.

---

[9] "Domain Name Contact Data Availability and Registrant Classification Study," Interisle Consulting Group, 4 June 2024. https://www.dnib.com/media/downloads/reports/Interisle_gtld_contact_data_study_final.pdf

[10] See GDPR Article 6 and Recitals 47 and 49; ICANN Data Registration Policy, Section 10, https://www.icann.org/resources/pages/registration-data-policy-2024-02-21-en

[11] See *SAC112: "*Minority Statement on the Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process (EPDP)," ICANN Security and Stability Advisory Committee (SSAC), 20 August 2020. Page 5. https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-112-en.pdf

[12] "Registration Data Service Request (RDRS) Usage Metrics Report," ICANN, March 2025. https://www.icann.org/en/system/files/files/rdrs-usage-metrics-13mar25-en.pdf

Brand owners can attempt to contact a registrant to initiate a conversation. gTLD registrars are required to forward messages to domain registrants with proxy-protected or redacted contact information. This contact mechanism should be stated in the domain's WHOIS or RDAP output.

Domain Blocking and Suspension

Some brand owners stay alert for domain names that may be registered by cybersquatters or phishers.[13] Brand owners or their vendors report infringing domains to hosting providers and registrars for suspension. This may disable domains being used for useful purposes, such as sinkhole domains.

The operators of reputation blocklists (RBLs) look for dangerous and potentially dangerous domains and URLs, and recommend that customers block them. Domains on these blocklists may become unreachable or unresolvable by some internet users due to the domain being listed in the RBL. This can reduce the utility of domains being used for legitimate purposes, such as sinkhole and spam trap domains.

Many RBL providers publish their own procedures to appeal blocklistings, which are listed on their websites, and domain removal is at their discretion. Parties that register look-alike domains for legitimate purposes should therefore assume that their domains may be subject to blocklisting and disruption.

Use of Domain Names by Phishers and for Anti-Phishing Training

Many large organizations hire security companies to provide phishing awareness and training. These vendors simulate phishing attacks against employees, register domains where they place fake phishing sites or warning messages, and advertise the URLs to employees in simulated phishing emails.

Some parties, including training companies, red teams, pentesters, and security researchers[14], use phishing kits for legitimate security and safety purposes. These sites may get blocklisted, because those kits are used by both benevolent and malevolent actors, and it is often difficult to distinguish the intent behind the use. See the Recommendations sections below for more about how to manage such deployments.

A definite minority of domain names registered by real phishers contain a brand name. This suggests that the use of domains containing trademarks is not strictly necessary for successful phishing training products and simulations. One study found that out of 1.1 million domain names used for phishing, only about 53,000 – less than 5% – contained the correct spelling of a brand keyword.[15] Many phishers know that brand owners and their vendors search for infringing domains, and avoid registering them to evade detection. Instead, they often embed the names of brands elsewhere in the URLs, where users may see

[13] Monitoring for look-alike domains is a recommended best practice for brand owners. See "M[3]AAWG Brand Protection Kit Domain Management," February 2022. Pages 6-7.
https://www.m3aawg.org/sites/default/files/m3aawgbrandprotectionkit_domainmanagement.pdf

[14] For example, see a GoPhish kit deployment option from the U.S. Cybersecurity and Infrastructure Security Agency (CISA), https://hub.docker.com/r/cisagov/gophish

[15] This counted extended domains such as *amazon-login.click*. In addition, more domains contained misspellings of brand keywords. "Phishing Landscape 2024: A Study of the Scope and Distribution of Phishing," Interisle Consulting Group, 23 July 2024. https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing

them and be fooled.[16] Some are found in subdomains, such as: *https://**login-apple**.please--verify.com* while others appear in the URL path, such as: *https://encontrardispositivos.info/**apple-eng**.php.*

Recommendations

When considering registering a look-alike domain for security or research purposes:

1. Be aware of the legal and operational risks involved.

2. Consider whether the use of a look-alike domain name is necessary or worth the risks. For some purposes, alternatives may fulfill the need.

3. Publish one's actual contact data in WHOIS or RDAP output. This can signal the registrant's professional credentials, indicate receptiveness to contact, and will facilitate direct contact not mediated by or dependent upon the domain name registrar. Note that ICANN requires that all gTLD registrars offer registrants a way to opt out of proxy protection or contact redaction.

4. If the registrant of a look-alike domain decides to use a proxy contact service or allows redaction of its contact data in RDAP or WHOIS, the registrant should test the registrar's contact mechanism to ensure effectiveness and timely email message delivery. Registrants should also ensure that someone in their company is monitoring for such incoming emails.

5. Consider contacting the trademark owner for awareness, coordination, and agreement to help avoid confusion, takedown efforts, unnecessary costs, wasted time, and animosity. In a cooperative solution, the registrant of a look-alike domain name can transfer ownership of the look-alike domain to the trademark owner, who can then point the look-alike domain to the researcher's nameservers of choice. This allows the trademark owner to permit use of the domain, while retaining some control.

6. Operators of sinkhole domains or nameservers should notify others of those services by adding them to lists shared by the security community.[17] This can help avoid accidental takedowns.

7. When operating phishing education programs, avoid consumer confusion by placing appropriate language on the look-alike domain's website home and landing page(s). State that the domain is not being used for actual phishing and do not present fields that ask for user credentials, such as username and password fields. A simulated phishing attack does not necessarily need to spoof a brand owner's site. Instead, the landing page can notify the user that they have clicked on a simulated phishing link and that users should be careful of phishing lures.

---

[16] Per some studies, a brand name appears somewhere in the URL (but not in the domain name) in almost 50% of phishing URLs. "Branded Domains are the Focal Point of Many Phishing Attacks." CSC. https://www.cscdbs.com/blog/branded-domains-are-the-focal-point-of-many-phishing-attacks

[17] Such as abuse.ch's SinkDB, https://sinkdb.abuse.ch See "M^{3}AAWG DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries," January 2024. Page 20. https://www.m3aawg.org/sites/default/files/dns_abuse_prevention_remediation_and_mitigation_practices_for_registrars_and_registries.pdf

8. When operating a phishing site for training or research purposes, limit site accessibility by imposing IP-based limits or other techniques. Prevent access to the site from the general public, making it accessible only from a relevant network.

9. Consider whether the look-alike domain needs to be configured to receive mail or should have an MX record. An MX record signals that the domain is enabled for email, which may raise concerns from brand owners and can be used as evidence of bad faith in a UDRP case. While an MX record can be useful if the look-alike domain is used as an email sinkhole, other uses may not require an MX record.

10. When conducting a phishing training exercise within, or on behalf of, an enterprise, expect security vendors to treat look-alike domains as hostile phishing attempts and block them. Prior to beginning the training exercise, consider a) ensuring delivery of email by a mail gateway through exceptions or configuration changes, and b) setting up appropriate DNS configurations and firewall entries within the enterprise to direct traffic to the phishing training site.

11. After using a look-alike domain for a phishing training exercise or other temporary use, ensure the domain does not prompt complaints or continued blocklisting by removing the associated website and preventing it from resolving in the DNS.

As with all documents that we publish, please check the M^{3}AAWG website (www.m3aawg.org) for updates.