DOMAIN SECURITY RECOMMENDATIONS TO SAFEGUARD YOUR DOMAINS AND BRANDS FROM ONLINE ABUSE AND FRAUD

Adopt a defense-in-depth approach for domain management and security

- [ ] Eliminate third-party risk by assessing your domain registrar's security, technology, and processes along with your company's domain name system (DNS) management provider
- [ ] Secure vital domain names, DNS, and digital certificates through:
  - [ ] Implementing two-factor authentication
  - [ ] Regulating permissions—both normal and elevated—and watching for any changes, as well as adding an authorized contact policy
  - [ ] Monitoring DNS activity and deploying distributed denial of service (DDoS) protection
  - [ ] Using security measures like domain registry locks, DNS security extensions (DNSSEC), domain-based message authentication reporting and conformance (DMARC), certificate authority authorization (CAA) records, and redundancy on DNS hosting

Continuously monitor the domain space and key digital channels

Within marketplaces, apps, social media, and email for brand abuse, infringements, phishing, and fraud:

- [ ] Identify domain and DNS spoofing tactics, such as homoglyphs (fuzzy matches and international domain names), cousin domains, keyword match, and homophones
- [ ] Register domains that could be high-value targets related to your brands (i.e., homoglyphs, or country domains) to mitigate the risk of bad actors using them
- [ ] Identify trademark and copyright abuse on web content, online marketplaces, social media, and apps

---

Request a free consultation here and one of our experts will contact you.

cscdbs.com

DOMAIN SECURITY RECOMMENDATIONS TO SAFEGUARD YOUR DOMAINS AND BRANDS FROM ONLINE ABUSE AND FRAUD

Use global enforcement, including takedowns and internet blocking

- ☐ Use phishing monitoring and a fraud-blocking network of browsers, partners, internet service providers (ISPs), and security information and event management (SIEM) systems
- ☐ Use a range of technical and legal approaches for enforcement, selecting the most appropriate approach per case
- ☐ Use a combination of actions to enforce on IP infringements and fraud, including:

  Primary enforcement: Marketplace delistings, social media page suspensions, mobile app delistings, cease and desist letters, fraudulent content removal, and complete threat vector mitigation

  Secondary enforcement: Registrar-level domain suspensions, invalid WHOIS domain suspensions, and fraud alerting

  Tertiary enforcement: Uniform Domain Name Dispute-Resolution Policy (UDRP) and Uniform Rapid Suspension (URS) procedures, domain acquisitions, in-depth investigations, and test purchasing

Confirm vendor business practices aren't contributing to fraud and brand abuse

The following issues are often common with consumer-grade domain registrars:

- ☐ Operating domain marketplaces that drop catch, auction, and sell domain names containing trademarks to the highest bidder
- ☐ Domain name spinning and advocating the registration of domain names containing trademarks
- ☐ Monetizing domain names containing trademarks with pay-per-click sites
- ☐ Frequently occurring breaches resulting in DNS attacks, phishing, and business email compromise

---

Request a free consultation here and one of our experts will contact you.

cscdbs.com