域名安全建议

以保护您的域名及品牌免受线上滥用和欺诈

采用深度防御方法进行域名管理并保护域名安全

- ☐ 通过评估您域名注册商的安全性、技术和流程以及您的域名系统 (DNS) 管理服务提供商，消除第三方风险
- ☐ 通过以下方式保护关键域名、DNS和数字证书：
  - ☐ 执行双重验证
  - ☐ 监管权限——包括正常权限和提升权限——跟踪任何变化，并添加授权联系人政策
  - ☐ 监管 DNS 活动并部署分布式拒绝服务 (DDoS) 保护
  - ☐ 采用域名注册局锁、DNS 安全扩展 (DNSSEC)、基于域名的消息身份认证、报告和一致性 (DMARC)、证书认证机构授权 (CAA) 记录和 DNS 主机冗余等安全措施

持续监控域名空间和关键数字渠道

如市场、应用程序、社交媒体和电子邮件，防止品牌滥用、侵权、网络钓鱼和欺诈

- ☐ 识别域名和 DNS 欺骗策略，例如同形文字（模糊匹配和国际域名）、相似域名、关键字匹配和同音异义词
- ☐ 那些可能成为与您品牌有关的高价值目标的域名（即：同形文字或国家/地区域名），降低不法分子恶意利用这些域名的风险
- ☐ 识别网站内容、线上市场、社交媒体和应用程序上的商标和版权滥用行为

点此获取免费咨询，我们将派一名专家与您联系。

cscdbs.com/cn

域名安全建议

以保护您的域名及品牌免受线上滥用和欺诈

实行全球维权，包括关停和高级网络封锁技术

- ☐ 使用网络钓鱼监管以及由浏览器、合作伙伴、互联网服务提供商 (ISP)、安全信息或事件管理 (SIEM) 系统组成的欺诈封锁网络
- ☐ 使用各种技术和法律方法进行维权，并按具体情况选择最适合的方法
- ☐ 使用对知识产权侵权和欺诈行为的多种维权行动：

  第一类维权行动：在市场上下架，暂停显示社交媒体页面，使移动应用程序下架，下达停止令，删除欺诈性内容，以及全面规避威胁载体

  第二类维权行动：注册商层面的域暂停、无效 WHOIS 域暂停，以及欺诈警报

  第三类维权行动：统一域名争议解决规则和统一快速暂停程序、域名收购、深入调查和测试购买

确认您的域名注册商的业务实践不会助长欺诈和品牌滥用行为

消费级域名注册商通常有以下问题：

- ☐ 运营域名市场，在其中搜罗放弃的品牌或商标域名、将其拍卖并出售给出价最高的竞标者
- ☐ 从事域名筛选业务，并提倡注册可引发大量误植域名的商标化域名
- ☐ 通过包含商标的点击付费类网站的域名赚钱
- ☐ 频繁发生导致 DNS 攻击、网络钓鱼和商业电子邮件入侵的泄露事件

点此获取免费咨询，我们将派一名专家与您联系。

cscdbs.com/cn

DBS09092022