ZEROFOX®

6 STEPS FOR PROTECTING YOUR COMPANY'S DOMAIN NAME

What can you do today to strengthen your domain security efforts?

Your company's domain name is the centerpiece of your online presence and a key component of critical applications that allow you to do business on the Internet.

WHAT IS DOMAIN SECURITY?

Policies & Controls ✚ **Technologies** ✚ **Visibility**

Domain security is the practice of implementing security measures, controls, and technologies that protect your company domain name against malicious cyber threats.

A comprehensive approach to domain security should be multifaceted, covering everything from domain name registration and access controls, to DNS security, encryption, email authentication, and domain monitoring.

This approach can help prevent digital adversaries from gaining unauthorized access to your company domain, hijacking DNS requests to your domain, or executing successful domain/email spoofing attacks.

The importance of domain security is in direct proportion to the diversity and potential impact of cyber attacks launched against company domains by digital threat actors.

HOW AN ATTACKER DEPLOYS A PHISHING SITE

DOMAIN.COM

STEP 1
Register a domain

STEP 2
Build a convincing website

STEP 3
Spread the fraudulent site via social and digital platforms

STEP 4
Obtain sensitive information from the unsuspecting user

Types of Domain Cyber Attacks

Consider the following types of cyber attacks that can be prevented or mitigated with a comprehensive approach to domain security:

Domain Hijacking

Also known as domain theft, this is a type of account takeover attack where a cyber adversary gains unauthorized access to your company domain control panel.

Typosquatting

Typosquatting is when a cyber adversary registers a domain name that is similar to yours, but contains a common spelling error that your customers might make when attempting to access your website.

Email Spoofing

Email spoofing tricks the recipient of an email into thinking that it came from your official company domain, when it was really sent by a cyber adversary.

Domain Spoofing

When a cyber adversary creates a copy of your website on a domain that they control and impersonates your brand in an attempt to scam your customers.

DNS Spoofing

DNS Spoofing is when an unauthorized cyber adversary exploits the DNS system to change the responses to DNS queries and divert web traffic from the target domains.

Denial of Service (DoS) Attacks

A DoS or Distributed Denial of Service (DDoS) attack attempts to disrupt the availability of your company website by flooding your IP address and network infrastructure with junk traffic.

Registrar Hacking

When the designated registrar for your company domain name is hacked and attackers gain administrative access to your domain. Web traffic can then be diverted to a malicious website.

A Comprehensive Approach to Domain Security

The following best practices described will help your organization get started with a comprehensive approach to domain security that protects your organization, employees, and customers against a variety of domain-based cyber attacks.

1 CHOOSE A REPUTABLE DOMAIN NAME REGISTRAR

The first step to shoring up your domain security should always be choosing a reputable domain name registrar with accreditation from registry operators and the Internet Corporation for Assigned Names and Numbers (ICANN). Even better, choose a registrar that can demonstrate investment and expertise in cybersecurity, including controls, processes, technologies, and staff training.

It's also important to list yourself as the owner of record to ensure that nobody else can hold your domain name hostage against your will. If you're registering an LLC before you own the corresponding domain name, there's a good chance it will be snapped up by an opportunistic squatter who may try to sell it back to you at an exorbitant cost.

The Trademark Clearinghouse (TMCH) is a centralized database of verified trademarks maintained by the Internet Corporation for Assigned Names and Numbers (ICANN). Registering your trademark data with the TMCH gives you first priority to register your trademark domain on newly released TLDs.
It also gives you standing to respond to any domain squatting attacks you detect by launching a Uniform Rapid Suspension (URS) with the National Arbitration Forum under the Uniform Domain-Name Dispute-Resolution Policy (UDRP).

FOX TIP

By registering your domain with TMCH, you will have the ability to take action on abusive registrations of domain names. Under the UDRP, disputes that arise from abusive registration of domain names (e.g. domain squatting abuses) can be resolved through an accelerated administrative process initiated by the trademark holder. This allows trademark holders to fight back against domain squatters without the time, cost, and complexity of taking legal action or winning in arbitration.

This action can be done by filing a complaint in court against the domain-name holder or submitting a complaint to an ICANN-approved dispute-resolution service provider.

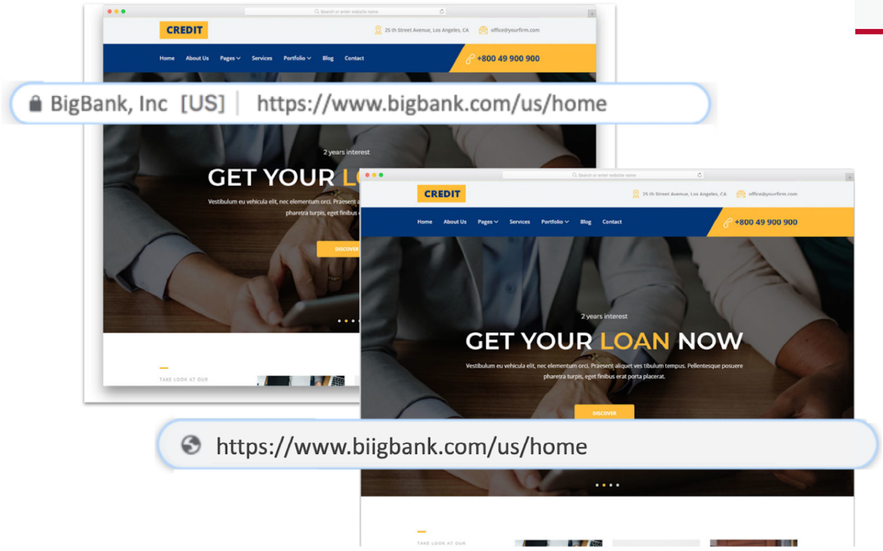
A Comprehensive Approach to Domain Security

2 REGISTER LOOKALIKE DOMAIN NAMES

The easiest way to start defending against typosquatting and domain spoofing attacks is to register look-alike domains yourself and redirect them to your company's real website. Registering these domains on your own means that they can't be registered by cyber adversaries who would use them to divert traffic away from your website and potentially scam your customers.

As you work to register domain names similar to yours, you may wish to include:

- Domain names that are typographical errors of your domain name.
- Domain names that look similar to your domain name, with just one or two character differences,
- Similar or identical domain names under other top-level domains (e.g. dot-info, dot-co, dot-biz, etc.)



FOX TIP

Domain hijacking can sometimes happen when your domain registrations unexpectedly expire, or when a cyber attacker successfully impersonates your business to your designated registrar.

To help mitigate the risk, we recommend:

- Registering your domains for the longest term possible – usually up to ten years.
- Registering your company's domain name directly to the corporation instead of an individual.
- Registering your company's domain name with a company credit card instead of an individual person's payment information.
- Enabling domain privacy protection to exclude your personal data from the WHOIS directory.
- Enabling Registry Lock, a security feature that requires your registrar to manually verify any requested changes to your DNS records.

A Comprehensive Approach to Domain Security

3 SECURE ACCESS TO YOUR DOMAIN

Securing access to your domain control panel and controlling user permissions are important steps to preventing domain hijacking attacks. Most registrars offer features like two-factor authentication and IP validation that can help verify the identity of a user logging into your domain control panel.

A number of employees at your organization may require access to your domain control panel to fulfill their job duties, but only trusted individuals should be assigned elevated permissions to modify staff permissions or implement DNS configuration changes.

Cyber attackers may attempt to gain access to your domain control panel by contacting your domain name registrar and impersonating your business. Your registrar should prevent these attacks by following your authorized contact policy and implementing DNS changes only when requested by trusted, verified individuals at your company.

FOX TIP

What is DNS… "The proper functioning of the Internet is critically dependent on the DNS . Every web page visited, every email sent, every picture retrieved from a social media: all those interactions use the DNS to translate human-friendly domain names (such as icann.org) to the IP addresses (such as 192.0.43.7 and 2001:500:88:200::7) needed by servers, routers, and other network devices to route traffic across the Internet to the proper destination." SOURCE

4 FORTIFY YOUR DNS SECURITY

The best way to strengthen your defenses against DNS spoofing and related DNS attacks is by enabling the DNS Security Extensions (DNSSEC) for your organization's DNS servers.

DNSSEC adds data origin authentication and data integrity protection to the core DNS protocol, cryptographically verifying both the identity of the sender and the integrity of the data received. These features make your domain less susceptible to DNS attacks.

A Comprehensive Approach to Domain Security

5 VALIDATE EMAILS WITH DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a protocol that leverages the Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) standards to validate the authenticity of email communications and protect against email spoofing attacks that impersonate your domain.

With SPF, your company can detail the specific IP addresses that are authorized to send mail on behalf of your domain. Recipients of an email from your company can compare the sender's IP address to those listed on your SPF records. When the addresses match, the email is determined to be authentic. With DKIM, individual email messages are cryptographically signed and can be authenticated by the recipient on arrival.

FOX TIP

When email sender addresses are spoofed (as is often the case with phishing campaigns), this can trigger a DMARC authentication failure report containing valuable information that can be used to determine the nature of the failure/violation. And while DMARC can instruct how to handle non-authenticated email, the information within such failure reports is often ignored or underutilized. This is unfortunate as the information within these reports can help identify abuses that other protections miss. Outsourcing through a third party, such as ZeroFox Adversary Disruption, can process this information easily, adding significant protection and minimizing impact on IT staff and users.

6 IMPLEMENT CONTINUOUS DOMAIN MONITORING AND PROTECTION

Digital threat actors are becoming increasingly innovative in their attempts to target organizations, their employees, and their customers with domain-based cyberattacks. Often, these attacks impersonate the organization's website and domain name to fool unsuspecting victims into compromising their data.

Because the attack surface is so large, and attacks against domains are so common, it is easy for organizations to feel inundated with alerts. Because of this, it is crucial that organizations continuously monitor for domains that may be impersonating or pirating their brand, products, trademarks or other intellectual property.

Continuous domain monitoring uses fullstring/substring matching, content matching, and AI-driven processes (such as OCR, image comparison and fuzzy-matching) to constantly monitor the public attack surface and detect potentially fraudulent domains and subdomains associated with your company, brand, and executives. Additionally, it checks for potentially malicious parked domain registrations and can alert on them when they subsequently become active.

FOX TIP

What is a Web Beacon?

A web beacon is a cloud-hosted tracker that can be added to web pages to gather information on how that page is being loaded. There are a variety of techniques that you can use, such as a 1x1 transparent pixel, to avoid detection.

Why should I use it?

A common tactic leveraged in phishing attacks is to directly clone an organization's website, and to redirect the login form in order to gather the victim's credentials. These credentials can be used to access an individual's account and steal money or sensitive information. While it can't catch every phishing page, a web beacon is one of the fastest and most reliable ways to detect this type of threat.

Enhance Domain Security And Counteract Digital Adversaries With Zerofox

Domain Monitoring and Threat Detection

Detect emerging and evolving threats with comprehensive and continuous domain protection coverage.

Benefit From:

- **Continuous domain monitoring** checks for potentially malicious domain registrations and triggers new alerts/escalations when they subsequently become active
- **Subdomain monitoring** detects impersonating subdomains
- **Typosquatting/homoglyph detection** finds domains registered to exploit common misspellings, typos, punycode homoglyphs, and different TLDs
- **Web Beacons** enable the rapid detection and identification of cloned content/material from protected web pages
- **Domain Content Search** enables you to search across extensive industry threat feeds for potential brand abuse

Rules and Domain Sources

Quickly fine-tune domain alert rules and define custom policies to meet your organization's targeted protection requirements.

Benefit From:

- **Easily definable domain alert rules** such as setting fullstring/substring URL text matching or prioritizing alerts based on domain relevance
- **Ingestion and alerting from many sources** including top PassiveDNS, domain registrars, and network security solutions
- **Domain Threat Submission Tool** provides a dedicated in-application utility for submitting phishing domains for alerting and takedowns

Alerts and Analysis

Gain context and intelligence via streamlined automation and advanced AI-enabled technologies.

Benefit From:

- **An easy-to-use UI and domain alerts enriched with contextual items** including DNS, WHOIS, A and MX records, website snapshots, etc.
- **AI-enabled domain analysis** such as OCR, Image Comparison, and fuzzy-matching
- **Daily Domain Summary Email** summarizing all newly observed, newly live, and newly expired domains related to your enterprise

Remediation and Disruption

Take action against phishing pages and impersonations by removing malicious sites and dismantling attack infrastructures.

Benefit From:

- **Automated takedown requests and processing** using streamlined, in-application controls
- **A team of specialists** that work on your behalf to remove fraudulent domains
- **Disruption/Dismantling phishing campaigns** at all points along the killchain via the ZeroFox Global Disruption Network of partner hosts, registrars, CDNs, ISPs and more
- **Disruption Actions view** providing best-practice attestation and detailed visibility into every takedown/disruption action taken in the remediation process

Enhance Domain Security and Counteract Digital Adversaries with ZeroFox

ZeroFox Domain Protection leverages artificial intelligence to detect and identify typosquatting and domain phishing attacks that target your brand, employees, and customers. Once detected, ZeroFox works on your behalf to takedown fraudulent cyber attacker infrastructure and discourage future domain spoofing or impersonation attacks against your brand community.

Our customers are able to find and eliminate typosquatting and domain phishing targeting employees and customers, making it easier than ever to protect domains against spoofed phishing URLs and other attempts to exploit employees and enterprise clients. Continuously monitoring for newly registered domains that closely resemble your brand, ZeroFox Domain Protection provides comprehensive protection against fraudulent domains, from identification to takedown.

Find out how ZeroFox targeted domain scams for the Civil Aviation Authority (CAA).

Schedule a Demo Today!

Sign up on zerofox.com

Learn More

Visit zerofox.com/products/domain-monitoring-tools/

Contact us sales@zerofox.com / 855.736.1400