FORTRA

WHITE PAPER (DIGITAL RISK PROTECTION)

Preventing Domain Impersonation: How to Stop Look-Alike Domains and Spoofing

Arguably, a domain is a cornerstone to any organization's digital presence and IT infrastructure. This important asset is also a desired by cybercriminals who use look-alike domains and spoofing for lucrative gains. This article examines domain impersonation and the steps an organization can take to protect one of their most valuable assets.

Why organizations should care about domain impersonation

Domain impersonation is a tactic used by cybercriminals where fake email addresses or website domains are created based off valid organizations. The impersonated assets are used to trick individuals for money or sensitive data. According to Fortra's 2023 Domain Impersonation Report, of look-alike domain threat types, 54% hosted brand content, 37% redirected to a third-party site, and 10% hosted malicious content. The two common types of domain impersonation are look-alike domains and email spoofing.

Look-alike domains

Domains nearly identical, or confusingly similar, but slightly altered are registered with intent to deceive. These domains are known as look-alike domains, and they can be created in many ways. For example, with use of internationalized domain name (IDN)/homoglyph domains, a popular domain can be altered with a character or two to look similar but obviously not the same: arnazon.com or amazön.com.

Domains are the key to internet communication

TECHNIQUES TO CREATE LOOK-ALIKE DOMAIN NAMES			
TLD swap	phishlabs.tech	Omission	phshlabs.com
Subdomains	phish.labs.com	Transposition	phsihlabs.com
Typosquatting	phishlavs.com	Insertion	phishxlabs.com
Hyphenation	phish-labs.com	Homoglyph	phishlaƄs.com
Repetition	phishllabs.com	Vowel-swap	phishlebs.com
Replacement	ph1shlabs.com	Addition	phishlabss.com

This chart shows the various ways a domain can be altered.

Once a look-alike domain is registered, A DNS records are created. The cybercriminal can then create a website and an SSL certificate. Now the website is ready for distribution. This can lead to phishing attacks, malware, and various scams as well as a tarnished reputation and loss of trust for the legitimate organization. While all of this can happen quickly, sometimes the cybercriminals may wait on the look-alike domain to obtain a better trust score. Just because a look-alike domain isn't in plain sight, doesn't mean it isn't lurking for future use.

Monetized links, adult content, unauthorized brand association, credential theft phishing, and counterfeit activity are all the various types of domain impersonation.

Email spoofing

One of the most common forms of cybercriminal activity, specifically a form of identity deception that's widely used in phishing and spam attacks, is email spoofing. It underpins the mechanism required to conduct hacking activities, and it can take many forms. Unfortunately, most email users will eventually receive an email that has been spoofed — whether they know it or not.

Email spoofing does not require a registered domain as it is a forgery of an email sender address. Once a look-alike domain is registered, MX DNS records are created for mail. This can lead to a setup of a mail server and the cybercriminals can send emails.

Display name deception is often successful because email clients usually show only the display name. Cybercriminals can insert the identity of a trusted individual or trusted brand into the display name. This type of attack is simple and cheap to stage.

In addition to manipulating the display name, cybercriminals may also use the actual email address of the impersonated identity in the From header, such as "United Customer Service" <noreply@united.com>. This type of attack, known as a domain spoofing attack, does not require compromising the account or the servers of the impersonated identity, but exploits the security holes in the underlying email protocols. They often use public cloud infrastructure or third-party email sending services that do not verify domain ownership to send such attacks.

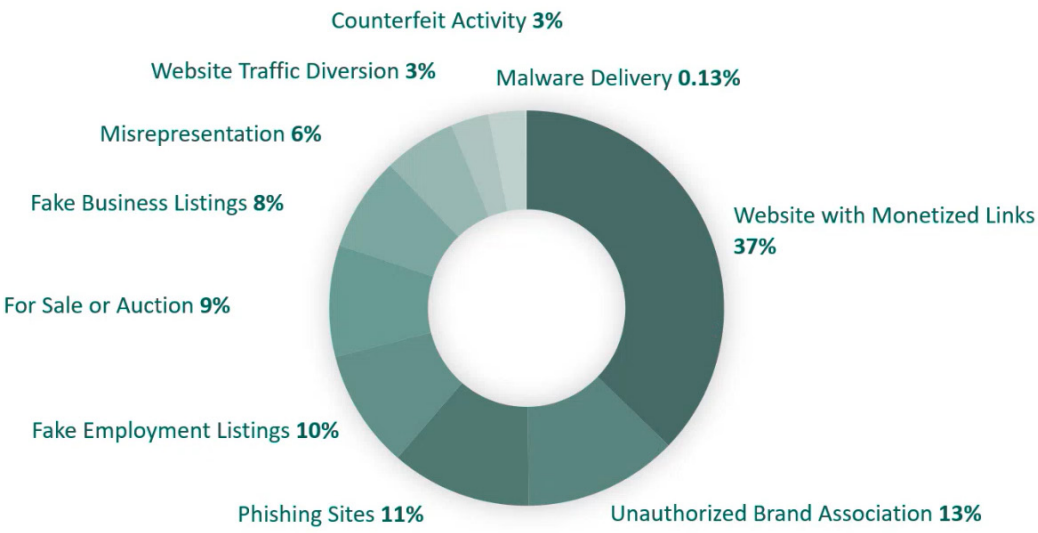
Do domain impersonations work?

These impersonation schemes are gaining traction. Fortra's 2023 Domain Impersonation Report also reported that the average brand is targeted by 40 look-alike domains per month.

And the organizations effected by brand impersonation are staggering. In a BleepingComputer article, Bill Toulas explained how a malicious group named "Fangxiao" created more than 42,000 impersonated domains from popular brands such as Coca-Cola, McDonald's, Knorr, Unilever, Shopee, and more. The domains redirected users to sites promoting dating apps, "free" giveaways, and adware apps.[1]

Fortra™ took a sample from intel based on 50,000 incidents across all industries and found the following information.

Look-Alike Domain Threats



Sampling of 50,000 Incidents

Common Challenges

There are also some serious resource issues that make domain impersonation difficult to stop for most organizations. The following are common challenges affecting a majority of businesses.

Lack of visibility

Insufficient intelligence across digital channels caused by an absence of resources brings a lack of visibility needed to identify domain abuse. It is near impossible for organizations to monitor everything on their own as there are numerous registrars to manage (contacts, procedures, relationships, etc.).

Too Much Noise

The volume of data can be overwhelming, making it difficult to accurately detect domain threats. Most organizations lack the refined curation and their submitted abuse reports may get ignored.

Ineffective Mitigation

Slow, costly, and often unsuccessful, mitigations can be near impossible for organizations on their own. A lack of a step-by-step procedural playbook for each registrar and an overwhelming number of relationships to maintain are just some of the reasons mitigations and proper takedowns are usually unsuccessful.

Limited resources

If the previous challenges do not deter organizations from mitigations on their own, the results might be just enough. Underestimated time, staff, and budget, regardless of the organization's size, can produce mediocre results as they simply don't have the wherewithal to do it.

What can organizations do to protect themselves from domain impersonation?

Monitor external domain data for look-alikes (look-alikes are not always taking advantage of the root domain, it can also impersonate the sub-domains). Organizations can use a Domain Monitoring Service. The scope of the domain service component includes detection, analysis, mitigation, and monitoring of domains for the following:

a. Domains that contain brands or identified terms

b. Being used in a "malicious" manner where the purpose is used to steal customer data, alter customer transactions, or exhibits other properties indicative of fraudulent activity.

c. Being used in an "unauthorized" manner

What is needed for successful domain monitoring?

The following steps are essential for effective domain monitoring.

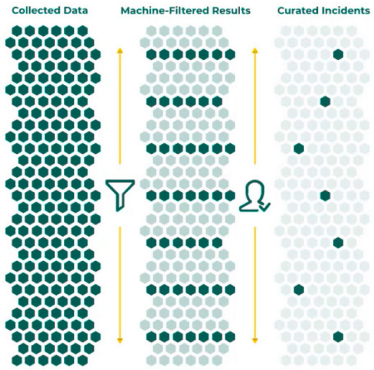
Collection of Domain Data

- Use DNS zone files and/or third-party domain services to review newly registered domains
- Use SSL transparency logs to find new SSL certificate registrations that contain key terms.
- Active DNS: Generate DNS queries to see if a domain exists.
- Passive DNS: Monitor DNS traffic to learn about new names
- Client Submission and Client Intelligence

Curation

- Review new gTLDs and ccTLDs
- Search new SSL cert registrations for key terms
- Identify typo-squatting and/or imposter domains
- Monitor domains for changes to website content, MX records and WHOIS data

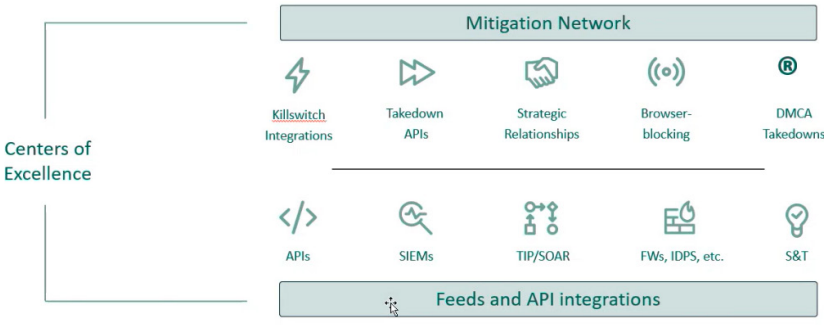
- Use technology to find look-alike domain matches.
- Review matches for web content and DNS information to determine if there are any active threats.
- Considered during domain analysis:
  - ✓ Resolved content
  - ✓ WHOIS
  - ✓ DNS Records (MX)
  - ✓ Domain name match % or suspicion level



Mitigation

- Legitimate abuses lead to takedown or suspension
- Internal security tools block malicious domains
- Brand infringement can be mitigated or monitored

The takedown of malicious domains is fundamental for successful protection against impersonation. Having a cybersecurity solution that streamlines takedowns – take immediate action on domains hosting phishing attacks – will reduce corporate spend on defensive efforts monitoring/managing registrations.



> *"Speed of take down for fraudulent sites is amazing."*
> - Security Executive at Large Financial Institution

DMARC protection for email authentication

Another way to combat impersonation is to implement DMARC reject on your email domains. When a cybercriminal uses your domain for email threats, they can mislead an organization's customers causing long-term damage to the organization's brand and customer trust. DMARC is an essential email authentication protocol that enables administrators to prevent hackers from hijacking domains for email spoofing, executive impersonation, and spear phishing. But email is complicated and getting email authentication correct is critical, so that only the spoofing is blocked.

A solution that protects from email spoofing is important. Strong email authentication can usually detect a spoofed email. Email authentication standards, such as DMARC, can be used by a domain owner to prevent spoofing of their domain, but unfortunately, have not been adopted widely by many retail companies.

A complete domain protection strategy

Fortra™ provides the solutions needed to stop domain impersonation and email spoofing all under one name. With some of the fastest takedowns in the industry and DMARC superior to most, organizations can be confident in their one stop cybersecurity ally.

Learn about solutions that protect your brand.

DOMAIN MONITORING **DMARC PROTECTION**

Sources:
[1] https://www.bleepingcomputer.com/news/security/42-000-sites-used-to-trap-users-in-brand-impersonation-scheme/

FORTRA®

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.