FORTRA™

PLAYBOOK *(PhishLabs)*

How to Defend Against Look-Alike Domain Threats

A Digital Risk Protection Playbook

Look-alike domains are one of the most versatile tools a threat actor can use to attack an organization. They lay the foundation for a wide range of cyberthreats, including reputation abuse, phishing sites, and email scams.
To evade detection and increase the probability of success, criminals often move quickly after registering a domain.
According to Fortra™ reports, the average brand is targeted by 40 look-alike domains per month.
This playbook breaks down:

- The domain lifecycle and how domains are abused
- Threats criminals use to deceive and defraud their targets
- How look-alike domain attacks are created
- How to gather and monitor domain data to identify threats proactively
- Analysis and mitigation approaches that reduce the risk of compromise

By following this playbook, security professionals can minimize the risk look-alike domains pose to their organizations.

The Domain Life Cycle

In order to understand how domains can be abused, it is helpful to understand a few basics and the domain life cycle.

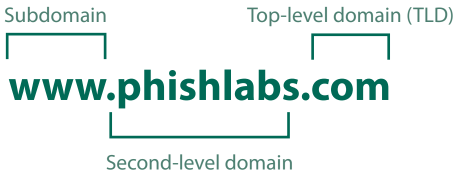
Domain Name Elements

Domain names give Internet users an easy way to communicate and visit websites. They define an area of authority for registrants, map to IP addresses that identify a web or mail server, and originate from the Domain Name System (DNS) root.

At the highest level of the DNS hierarchy, top-level domains (TLDs) are controlled by registries and make up the end portion of every domain name.

Second-level domains are the next level below. Managed by registrars, they are often selected by companies to represent a brand and establish a unique website address.

Subdomains, which make up the next or third level down, are controlled by a domain's registrant and can provide a means to differentiate areas or sections of a website.



Life Cycle of a Domain Name

Domain names are not technically bought or sold – registrants pay for the right to use them for a pre-determined period of time. Generic top-level domains (.com, .net, etc.) have a typical lifecycle made up of five phases:

Phase 1: Available.
During this phase, anyone can register the domain for 1-10 years.

Phase 2: Registered and Active
Once a registrant pays the registration fee, the domain is considered active and they can set up hosting for a website or email.

Phase 3: Expiration and Renewal Grace Period
If the domain is not renewed before its expiration date, a registrar will change the domain's status to Expired and turn off access.

Phase 4: Redemption Period
If the registrant still does not renew within 45 days after expiration, the domain goes into a redemption period. They still have the option to renew for 30 days if they pay a fee.

Phase 5: Pending Deletion
After the redemption period, requests to update domain information are denied. This phase is usually five days, then the domain is released and available again for anyone to register.

What Is a Look-Alike Domain?

Cybercriminals abuse domains by registering look-alike versions that are slightly altered from an original. Hundreds of thousands of look-alike domains are registered each year to leverage the existing trust of reputable companies, confuse customers, and make money by committing fraud.

Many attackers use similar tricks to create look-alike domains. The techniques below are often used to generate several variations for implementing attacks:

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**	phishlaЪs.com
Repetition	phishllabs.com	**Vowel-swap**	phishlebs.com
Replacement	ph1shlabs.com	**Addition**	phishlabss.com

How Look-Alike Domains Are Used

Look-alike domains are considered one of the most useful tools for bad actors because they serve as a foundation for a wide range of cyberthreats. Reaching millions of Internet users each year, look-alike domain attacks lead to significant brand damage, financial losses, and data compromise. Below are some of the most common examples.

Business Email Compromise

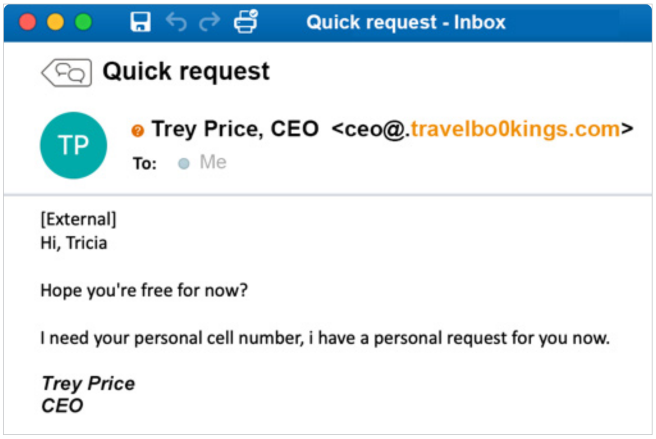
One widespread example is a Business Email Compromise (BEC) attack, which results in millions of dollars lost by businesses every year.

BEC threats target employees with access to an organization's sensitive information such as bank accounts or payroll administration.

They first receive a carefully crafted email appearing to be from an executive – usually the CEO – requesting a favor. The email does not contain links or attachments and the language creates a sense of urgency.

When the target replies to the email, the domain appears legitimate, and the conversation ultimately leads to a request for payment or sensitive data.

Attackers commonly use look-alike domains for BEC threats because they can send emails from legitimate servers that are likely to get through a company's authentication controls. There is nothing technically unauthorized about them, as the domains are legally registered, which leads to a high risk of compromise.



Quick request

Trey Price, CEO <ceo@.travelbo0kings.com>

To: Me

[External]
Hi, Tricia

Hope you're free for now?

I need your personal cell number, i have a personal request for you now.

Trey Price
CEO

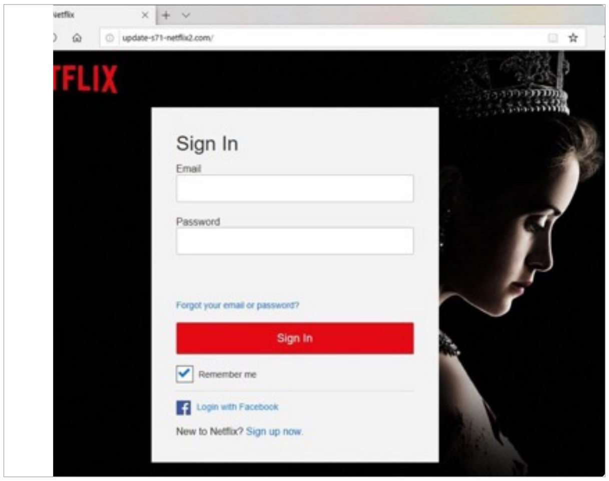
Business Email Compromise

Legitimate Domain: travelbookings.com
Fake Domain: travelbo0kings.com

Phishing Websites

Over half of phishing attacks use look-alike domains to impersonate trusted brands, send phishing emails, and trick account holders into entering login credentials on fake websites. These phishing scams often lead to account takeover, where cybercriminals compromise and control online accounts to engage in fraudulent activity. Account takeover (ATO) attacks can also use look-alike domains with Vishing or SMiShing to scam unsuspecting victims.

The image to the right shows how a domain was spoofed to look like a Netflix page where customers are prompted to enter their credentials.



Phishing Website

Legitimate Domain: netflix.com
Fake Domain: update-s71-netflix2.com/

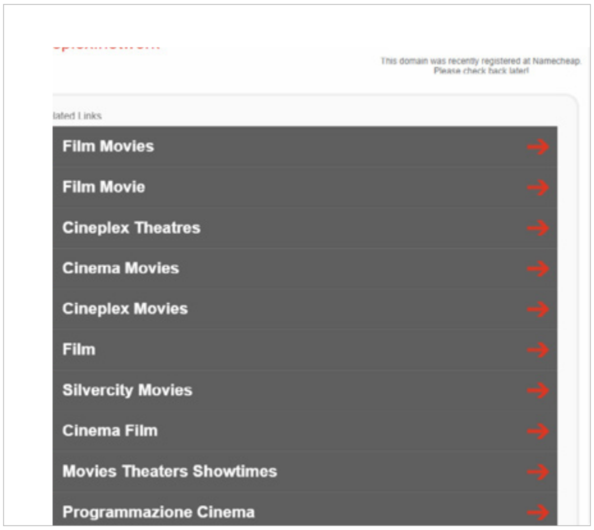
Monetized Links

At its most benign, a threat actor can register a domain that impersonates a legitimate brand, park it, and serve ads to visitors. This is called domain parking monetization.

Free domain service providers are particularly susceptible to abuse, along with a number of cheap registrars that provide low-cost bulk registration. These providers are appealing because many don't require attackers to identify themselves.

In 2019, PhishLabs observed a year-over-year increase in the use of free domains used to host phishing sites, making up 32.6% of the volume last year alone.

Unauthorized Brand Association is when attackers piggyback on the brand and reputation of legitimate organizations. They may post a reputable organization's logo to lend credibility to their company or event.


This domain was recently registered at Namecheap.
Please check back later!

Monetized Links on a Parked Domain

Free domain service provider

Proprietary | Copyright PhishLabs

Website Traffic Diversion leads users to a fake site where they may encounter a number of different schemes from that point forward like counterfeit products and services, phishing websites, or malware delivery.

How Look-Alike Domain Attacks Are Created

Most look-alike domain threats have a common structure. Below are the steps in the creation process:

Step 1: Register a look-alike domain

An attacker finds a domain they want to spoof, checks to see what variations are available, then registers a look-alike domain name with a registrar.

Step 2: Create DNS records

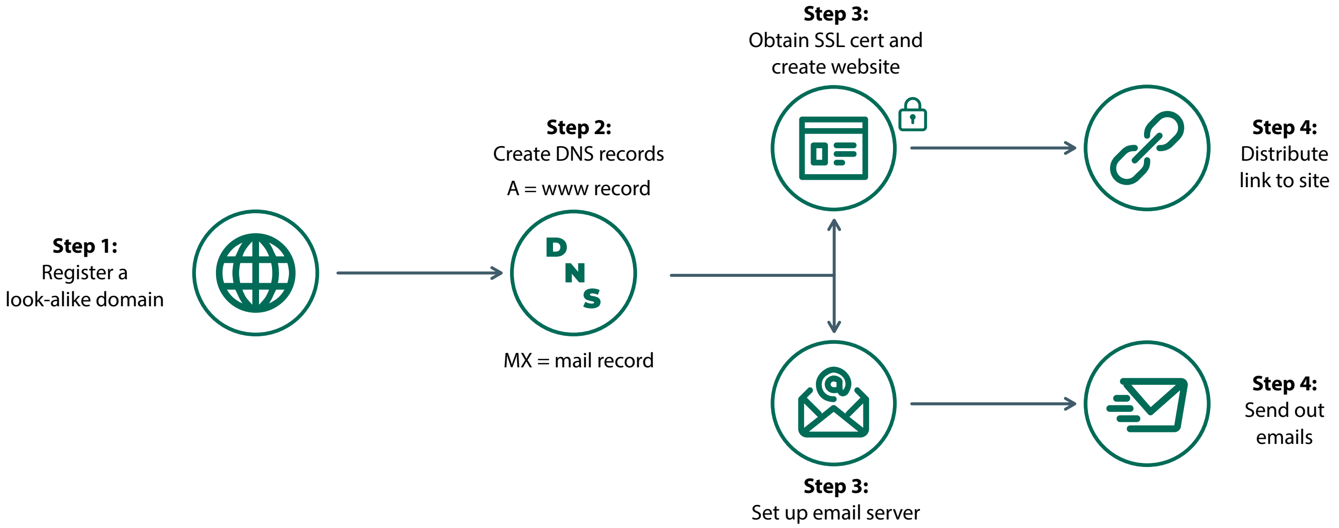
They then create an A record to point to a new website or an MX record for email delivery.

Steps 3 and 4 (website): Create website and distribute links

Most threat actors obtain SSL certificates for phishing sites (typically for free) then set up websites. They'll share the fake site link in various ways – via spam, SMS, blog comments, etc.

Steps 3 and 4 (email): Set up email server and send emails

When creating a BEC scam or ransomware attack, scammers will set up an email server, craft their emails, and send them out to targets.



How To Defend Against Look-Alike Domains

Enterprises can effectively manage domain threats by implementing a mature and ongoing process for collection, curation, and mitigation. The best practice is to take on a multipronged approach:

1. Collection - the sourcing of sufficient domain intelligence to identify potential threats.

2. Curation - the analysis and development of intelligence to identify real domain threats and compile sufficient evidence.

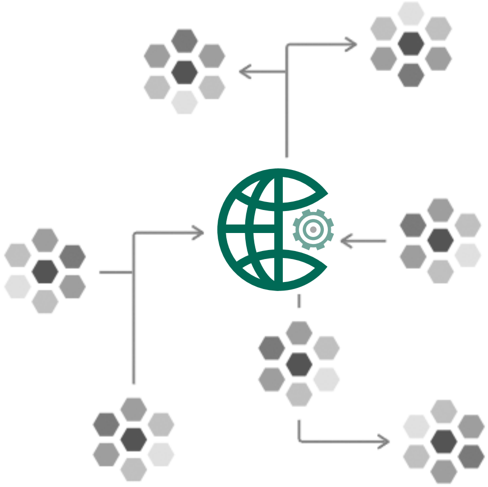
3. Mitigation - the actions taken to reduce the risk posed by identified domain threats.

Collection

To identify domain threats, organizations need visibility into new and existing registered domain names.

There are a number of useful sources for domain intelligence:

- TLD zone files list every registered domain as they are created on a daily basis.
- Secure Socket Layer (SSL) certificate transparency logs present domains, subdomains, third-level domains, fourth level, and so on for millions of new SSL certificates issued daily.
- DNS traffic contains domain names being queried and can be monitored for new domains.
- DNS queries can be performed using look-alike variations of legitimate domains to see if those look-alike variations currently exist.



Domain intelligence collected via the above sources can be monitored for indicators of domain impersonation.

Proprietary | Copyright PhishLabs

Curation

Collected domain intelligence must be analyzed to identify real threats. Searching domain intelligence for brand-related keywords and variations is necessary to find potential threats.

However, domain strings can often unintentionally contain keywords. Analysis is needed to remove these false positives from the process.

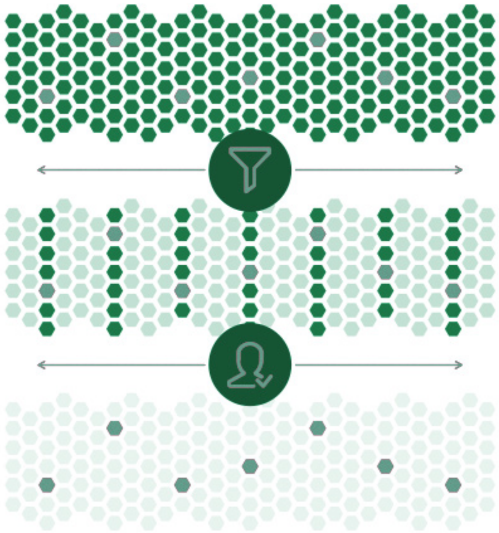
When analyzing a domain, two different aspects can show if it is truly a threat:

1. Analyze the domain string itself and score it based on its likelihood to be mistaken as legitimate brand use.

- How closely does it match keywords?
- Is it obvious that a word is different?
- Are there letters, symbols, or capitalization that would confuse an end user?

2. Observe the content by looking at each page hosted on the domain.

- Is there data present?
- Does it appear related to a legitimate brand?



Sometimes it is not clear if the content is related or not. Review by marketing, legal, or other business functions may be needed to determine if a questionable domain poses a threat.

Once the domain is deemed suspicious, two additional items must be analyzed:

1. All content on the domain should be analyzed to identify anything unauthorized or malicious. Security teams should actively review web pages in search of any element that suggests malicious activity.

2. The domain should be checked for a Mail Exchanger (MX) Record. This record specifies which mail servers accept email for the domain. A domain may lack content, but if it has a MX record, it is capable of sending email. This can be abused for BEC, email phishing, and spam campaigns. Establishing the presence of an MX record can help determine if the domain is malicious.

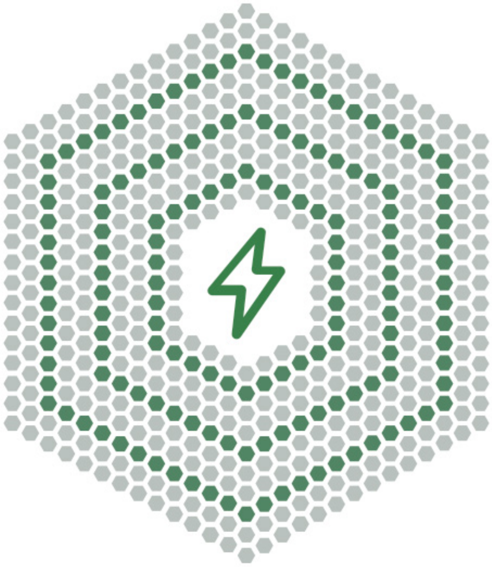
Mitigation

Once a domain has been established as a threat, it needs to be completely mitigated.

Security teams should adopt a comprehensive mitigation strategy for domains that includes taking the threat down and using indicators to prevent internal users from accessing it.

Look-alike domains should be incorporated into internal intelligence and workflow processes to detect and prevent attempts to access them by enterprise users and systems. Ideally, this should be done via automated integrations with intelligence tools and security controls.

This mitigation approach reduces risk of users being impacted when they are within the reach of security controls. However, it does not address the risk to users operating outside of security controls. It also does not address brand and customer fraud risks.



The only certain method of fully mitigating the risk posed by a look-alike domain is to take the domain offline. To quickly take down a domain, security teams need to have sufficient evidence that shows the domain is being used for malicious purposes. If no evidence is present when a potentially malicious domain is first detected, it should be monitored until suspicious content or activity is observed that can serve as evidence to support the site's removal.

Once sufficient evidence is collected to justify taking down a domain, security teams can pursue its removal. In general, domain registries have broad anti-abuse authority. When provided with evidence, they will typically remove domains being abused for:

- Hosting phishing sites
- Hosting malware
- Botnet command and control
- Distributing child exploitation materials
- Delivering spam

In these scenarios, it is clear to the registry that abuse is taking place. In other scenarios, however, the domain may involve fraud that is not clearly abusive to the registry. These could be viewed as intellectual property or trademark disputes that do not warrant a takedown without a court order or law enforcement request.

Unfortunately, legal action is not an ideal way to address these threats. Whether through lawsuits or arbitration, pursuing a domain takedown via legal action is exceedingly time consuming and costly. It is not a scalable option for mitigating domain threats. It should be a last resort.

In scenarios where the domain abuse may not be obvious, the fastest way to mitigate the threat is to remove all doubt that the domain in question is supporting fraudulent activity. This is where thorough intelligence collection and analysis pays dividends.
If provided with ample evidence that clearly demonstrates abuse, many registries will take action to remove the offending domain. Reputation and experience also increase the odds of a successful takedown request.

DMARC Protection For Email Security

Lastly, in order to protect against email spoofing, DMARC reject on email domains is vital. When a cybercriminal uses a domain for email threats, they can mislead an organization's customers which can create long-term damage. DMARC is an email authentication protocol that enables administrators to prevent hackers from hijacking domains for email spoofing, spear phishing, and other email threats.

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 — encompassing a complete domain protection strategy.

Conclusion

Look-alike domains have the ability to harm an otherwise healthy organization, sometimes permanently. Because of the various ways that domains can be abused, security teams must be both proactive and thorough in order to protect against malevolent activity.

By adopting the steps in this playbook, security teams should have a better understanding of domain threats, how to collect and analyze domain intelligence, and tactics to follow to mitigate threats.

To learn more about how PhishLabs helps organizations with external threats such as look-alike domains, visit phishlabs.com/digital-risk-protection.

To learn more about DMARC solutions, visit agari.com/products/dmarc-protection.

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.