MOORLI BrandGuardDiagnostic

Brand: MOORLI (moorli.io) **Audit ID:** bgd_f9…062c **Generated:** May 15, 2026, 01:31 AM **Plan:** Executive
Lookalike Candidates: 100 **Client:** SAMPLE REPORT

POSTURE SCORE

0–100 (higher = safer). Computed as 100 minus the average risk score of the 25 highest-priority registered lookalike domains found. Unregistered variants are excluded.

Immediate action required: 21 lookalike domains show active web or mail signals on confusable domains. Prioritize review, containment, and evidence capture, then rescan to confirm.

Key Findings

- ! 21 candidates showed active threat signals (live content or mail infrastructure).
- ! 18 active domains publish MX records (inbound mail infrastructure observed).
- ! 1 active domain contains login forms (credential harvesting risk).
- • 3 registered lookalike domains appear recently registered (< 90 days).

Next 7 Days

1 CONTAIN

Block active lookalike domains at email/web gateways, and alert finance/HR/executive assistants about impersonation patterns.

2 EVIDENCE

Capture screenshots, DNS snapshots, and headers for any suspicious domains to support registrar/host abuse reports.

3 REMEDIATE

Report to registrar/hosting/CDN abuse contacts. If trademark infringement is clear, consult counsel for UDRP / cease-and-desist.

4 DEFEND

Register priority variants defensively and enforce SPF/DMARC alignment on your legitimate domains to reduce spoofing success.

WHY THIS MATTERS

Lookalike domains are commonly used for **invoice fraud**, **credential theft**, and **brand reputation attacks**. This report prioritizes candidates that show live web/mail signals so you can contain risk quickly.

What This Means for Your Business

We scanned 100 domains that closely resemble moorli.io — the kinds of misspellings and look-alike addresses that attackers register to impersonate your organization. Of these, 21 confusable domains showed active web or mail infrastructure. These domains require review because they materially increase impersonation risk. Specifically: 18 publish MX records and show inbound mail infrastructure on lookalike domains (a high-priority BEC/phishing signal); 1 hosts login forms that could be used for credential harvesting. Your brand posture score of 78/100 reflects this exposure. The detailed findings and recommended actions below are prioritized so your team can address the highest-risk domains first.

HOW TO READ THE SCORES IN THIS REPORT

Posture Score (0–100)

Your overall brand impersonation exposure. Calculated as 100 minus the average risk across the highest-priority registered lookalike domains found. **Higher = safer.** Above 80 is strong; below 50 indicates significant active threat signals. Unregistered domains are excluded. Registered domains are included regardless of whether they show active infrastructure, because inactive or parked domains can be weaponized at any time.

Risk Score (0–100, per domain)

How dangerous a specific lookalike domain is. Each domain is evaluated against all applicable diagnostics in the 36-rule set (registration, DNS, web, mail, SSL, reputation). Rules that fire as FAIL contribute maximum risk; WARN contributes partial risk; PASS reduces risk. Not-applicable or inconclusive results are excluded so they never inflate the score. **Higher = riskier.** Domains you own (defensive holds) are capped at 10.

Business Impact Summary

18 domains publish MX records and show inbound mail infrastructure on lookalike domains. IC3 reported **$3.05B** in BEC losses in 2025 (FBI IC3, 2025). These figures provide industry context and are not a forecast of your direct losses.
→ `mooli.org` , `moori.info` , `mooli.online` , `moorla.io` , `moorii.net` +13 more

1 domain hosts login forms that could harvest credentials from your employees, customers, or partners.
→ `mooli.org`

1 lookalike domain expire within 30 days. These are short-window acquisition opportunities if the domains are not renewed.
→ `morli.top`

69 high-risk variants (edit distance ≤1) are unregistered and available for defensive registration. Pricing varies by TLD and registrar.
→ `moorli.net` , `moorli.org` , `moorli.co` , `moorli.app` , `moorli.info` +64 more

⚡ Act Now — Top 5 Priorities

These are the domains that require the fastest response, ranked by severity and attack capability.

Priority	Domain	Action	Why
CRITICAL	mooli.org	**Block at gateway + report to registrar immediately**	Hosts a login form — strong credential-harvesting signal.
HIGH	moori.info	**Block at email gateway + watch for phishing campaigns**	Publishes MX records — supports inbound mail handling and increases phishing/BEC relevance.
HIGH	mooli.online	**Block at email gateway + watch for phishing campaigns**	Publishes MX records — supports inbound mail handling and increases phishing/BEC relevance.
HIGH	moorla.io	**Block at email gateway + watch for phishing campaigns**	Publishes MX records — supports inbound mail handling and increases phishing/BEC relevance.
HIGH	moorii.net	**Block at email gateway + watch for phishing campaigns**	Publishes MX records — supports inbound mail handling and increases phishing/BEC relevance.

Defensive Registration Recommendations

These unregistered domains are close enough to your brand to be weaponized. Defensive registration pricing varies by TLD and registrar; validate current pricing before purchase.

Domain	Edit Distance	Similarity Type	Risk Level
moorli.net	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL
moorli.org	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL
moorli.co	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL
moorli.app	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL
moorli.info	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL
moorli.biz	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL
moorli.dev	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL
moorli.online	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL
moorli.site	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL
moorli.top	0	TLD variation of your primary domain. Common defensive gap.	CRITICAL

Defensive registration pricing varies materially by TLD and registrar. Validate current pricing before purchase. For common low-cost TLDs, the total annual cost is often modest relative to a single BEC incident.

Classification

AVAILABLE **69** (69%) ACTIVE_THREAT **21** (21%) INACTIVE **7** (7%)

PARKED **3** (3%)

HOW TO INTERPRET CLASSIFICATION

ACTIVE_THREAT indicates the domain is registered and shows active web or mail infrastructure on a confusable domain (highest review priority).
PARKED and **INACTIVE** are registered and can be activated quickly—consider defensive registration or acquisition.
DEFENSIVE_HOLD indicates observed or user-verified benign ownership.
AVAILABLE means the domain is unregistered.

Top Priority Candidates

Domain	Classification	Risk	Signals	Highlights
mooli.org	ACTIVE_THREAT	30	● MX ● Web ● Login ○ Brand	FAIL BGD-COMP-080 — Privacy-protected registrant plus login form on a lookalike domain. High-priority credential-harvesting risk. FAIL BGD-WEB-022 — Lookalike domain contains a login form or credential input. This is a strong credential-harvesting signal that warrants immediate review. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand.
moori.info	ACTIVE_THREAT	27	● MX ● Web ○ Login ○ Brand	FAIL BGD-COMP-080 — Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review. FAIL BGD-REG-002 — Domain was registered within the last 90 days. High risk of active phishing or brand abuse. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand.

Domain	Classification	Risk	Signals	Highlights
mooli.online	ACTIVE_THREAT	24	● MX ● Web ○ Login ○ Brand	FAIL BGD-REG-002 — Domain was registered within the last 90 days. High risk of active phishing or brand abuse. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand. WARN BGD-COMP-080 — Domain is parked or for-sale with privacy-protected WHOIS. Brand references on parked marketplace pages are common and do not indicate active abuse. Review periodically for activation.
moorla.io	ACTIVE_THREAT	28	● MX ○ Web ○ Login ○ Brand	FAIL BGD-COMP-080 — Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand. WARN BGD-MAIL-030 — MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.
moorii.net	ACTIVE_THREAT	25	● MX ○ Web ○ Login ○ Brand	FAIL BGD-COMP-080 — Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand. WARN BGD-MAIL-030 — MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.

Domain	Classification	Risk	Signals	Highlights
moorki.com	ACTIVE_THREAT	25	● MX ● Web ○ Login ○ Brand	FAIL BGD-COMP-080 — Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand. WARN BGD-MAIL-030 — MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.
morli.com	ACTIVE_THREAT	24	● MX ● Web ○ Login ○ Brand	FAIL BGD-COMP-080 — Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand. WARN BGD-MAIL-030 — MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.
mourli.com	ACTIVE_THREAT	23	● MX ● Web ○ Login ○ Brand	FAIL BGD-COMP-080 — Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand. WARN BGD-MAIL-030 — MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.

Domain	Classification	Risk	Signals	Highlights
morli.info	ACTIVE_THREAT	23	● MX ● Web ○ Login ○ Brand	FAIL BGD-COMP-080 — Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand. WARN BGD-MAIL-030 — MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.
morli.top	ACTIVE_THREAT	23	● MX ● Web ○ Login ○ Brand	FAIL BGD-COMP-080 — Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review. FAIL BGD-SIM-061 — Edit distance is 1 — extremely close to your brand. WARN BGD-MAIL-030 — MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.

All candidates — Registered

Domain	Classification	Risk	FAIL	WARN	NA	Flags
mooli.org	ACTIVE_THREAT	30	3	11	2	privacy mx web login
moori.info	ACTIVE_THREAT	27	3	11	2	privacy mx web
mooli.online	ACTIVE_THREAT	24	2	12	2	privacy mx web
moorla.io	ACTIVE_THREAT	28	2	9	11	privacy mx
moorii.net	ACTIVE_THREAT	25	2	7	12	privacy mx
moorki.com	ACTIVE_THREAT	25	2	13	0	privacy mx web
morli.com	ACTIVE_THREAT	24	2	8	6	privacy mx web
mourli.com	ACTIVE_THREAT	23	2	12	2	privacy mx web
morli.info	ACTIVE_THREAT	23	2	8	6	privacy mx web
morli.top	ACTIVE_THREAT	23	2	11	2	privacy mx web
moori.net	ACTIVE_THREAT	23	2	11	2	privacy mx web
mooli.net	ACTIVE_THREAT	20	1	7	12	privacy mx
moori.co	ACTIVE_THREAT	20	1	10	7	mx web
mooli.com	ACTIVE_THREAT	19	1	9	6	privacy mx web
morli.co	ACTIVE_THREAT	19	1	11	5	mx web
moorle.com	ACTIVE_THREAT	18	1	10	2	privacy mx web
moroli.com	ACTIVE_THREAT	25	2	10	2	privacy mx web
moorii.com	ACTIVE_THREAT	16	1	8	3	privacy mx web
mooeli.com	ACTIVE_THREAT	20	1	7	12	privacy web

Domain	Classification	Risk	FAIL	WARN	NA	Flags
mooli.io	ACTIVE_THREAT	18	1	9	8	privacy, web
mooli.app	ACTIVE_THREAT	18	1	8	8	privacy, web
moorla.com	PARKED	24	3	10	6	privacy, web
moorli.com	PARKED	22	1	12	6	privacy, web, brand
moori.shop	PARKED	14	1	6	13	web
moofli.com	INACTIVE	24	1	6	24	privacy
moorli.xyz	INACTIVE	15	1	3	24	—
noorli.com	INACTIVE	17	1	4	19	privacy
moarli.com	INACTIVE	17	1	6	11	privacy
moofli.org	INACTIVE	17	1	6	11	privacy
moofli.online	INACTIVE	17	1	6	11	privacy
morli.shop	INACTIVE	14	1	6	14	—

Note: This audit uses deterministic DNS/registration + lightweight HTTP/TLS checks. Some domains may be blocked by WAF/captcha or unreachable; those signals are marked Inconclusive (NA).

Unregistered Variants (69)

These domains are not currently registered. Variants with edit distance ≤2 are marked as defensive registration candidates.

Domain	Similarity Type	Edit Distance	Recommendation
moorli.net	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.org	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.co	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.app	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.info	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.biz	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.dev	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.online	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.site	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.top	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REGISTER
moorli.click	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REVIEW
moorli.link	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REVIEW
moorli.shop	TLD variation of your primary domain. Common defensive gap.	Identical name on a different TLD. Very high deception risk.	REVIEW

Domain	Similarity Type	Edit Distance	Recommendation
m-oorli.io	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
mo-orli.io	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moo-rli.io	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moor-li.io	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
m-oorli.com	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
mo-orli.com	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moo-rli.com	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moor-li.com	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
m0orli.io	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
mo0rli.io	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moor1i.io	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorii.io	Similarity pattern does not match common squatting vectors. Review lower priority unless other signals indicate abuse.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorl1.io	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorll.io	Similarity pattern does not match common squatting vectors. Review lower priority unless other signals indicate abuse.	Edit distance is 1 — extremely close to your brand.	REVIEW

Domain	Similarity Type	Edit Distance	Recommendation
m0orli.com	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
mo0rli.com	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moor1i.com	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorl1.com	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorll.com	Similarity pattern does not match common squatting vectors. Review lower priority unless other signals indicate abuse.	Edit distance is 1 — extremely close to your brand.	REVIEW
m-oorli.net	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
m-oorli.org	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
m-oorli.co	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
mo-orli.net	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
mo-orli.org	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
mo-orli.co	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moo-rli.net	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moo-rli.org	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moo-rli.co	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW

Domain	Similarity Type	Edit Distance	Recommendation
moor-li.net	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moor-li.org	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moor-li.co	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
mmoorli.io	Doubled or dropped letter. Common squatting technique.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorlii.io	Doubled or dropped letter. Common squatting technique.	Edit distance is 1 — extremely close to your brand.	REVIEW
m-oorli.app	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
mo-orli.app	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moo-rli.app	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
moor-li.app	Hyphen insertion/removal. Used to create plausible lookalikes.	Identical name on a different TLD. Very high deception risk.	REVIEW
mmoorli.com	Doubled or dropped letter. Common squatting technique.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorlii.com	Doubled or dropped letter. Common squatting technique.	Edit distance is 1 — extremely close to your brand.	REVIEW
m0orli.net	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
m0orli.org	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
m0orli.co	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW

Domain	Similarity Type	Edit Distance	Recommendation
mo0rli.net	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
mo0rli.org	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
mo0rli.co	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moor1i.net	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moor1i.org	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moor1i.co	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorii.org	Similarity pattern does not match common squatting vectors. Review lower priority unless other signals indicate abuse.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorii.co	Similarity pattern does not match common squatting vectors. Review lower priority unless other signals indicate abuse.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorl1.net	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorl1.org	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorl1.co	Homoglyph substitution (e.g., rn→m, l→1, 0→O). Extremely hard to distinguish. High deception risk.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorll.net	Similarity pattern does not match common squatting vectors. Review lower priority unless other signals indicate abuse.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorll.org	Similarity pattern does not match common squatting vectors. Review lower priority unless other signals indicate abuse.	Edit distance is 1 — extremely close to your brand.	REVIEW
moorll.co	Similarity pattern does not match common squatting vectors. Review lower priority unless other signals indicate abuse.	Edit distance is 1 — extremely close to your brand.	REVIEW

CHANGES SINCE LAST SCAN

This is the **baseline scan** for MOORLI. When you run a rescan (recommended: 30 days), the rescan report will show posture score changes, new threats, resolved threats, and domain-level risk movement.

Executive plan includes a 30-day rescan with full delta analysis.

Methodology

MOORLI BrandGuardDiagnostic performs automated, passive analysis of publicly observable signals across 36 rules in 9 categories. No intrusive testing is performed. All checks use standard DNS, RDAP, HTTP, and TLS protocols. SMTP catch-all acceptance testing remains out of scope in passive mode.

REGISTRATION & OWNERSHIP

RDAP/WHOIS: registration age, expiry, privacy/proxy, registrar reputation, registrant match.

DNS & HOSTING

A/AAAA/NS/MX resolution, hosting provider identification, redirect detection, wildcard DNS, shared hosting.

WEB PRESENCE

Live content detection, parked page identification, login form detection, brand mention scanning, CDN analysis.

MAIL INFRASTRUCTURE

MX records, SPF, DMARC policy and enforcement, DKIM selector discovery, mail provider identification.

BROWSER-TRUSTED SSL/TLS CERTIFICATES

Certificate validity, issuer analysis, free CA detection, brand mention in SAN, certificate age.

THREAT INTELLIGENCE

Internal reputation checks from commercial threat-intelligence and security-DNS sources, plus a corroboration rule when independent sources agree. Provider outputs are used as internal scoring signals and are not redistributed verbatim. These sources are provided "as is": some risky sites may not be identified, and some safe sites may be identified in error.

Detailed Findings

25 domains are included in the detailed findings section below. **21 active lookalikes** showed observable infrastructure (MX records, web content, or login forms) — these are your highest priority for review, containment, and evidence capture.

Each domain on the following pages includes a signal summary, threat narrative, and a prioritized findings table. One domain per page.

HOW TO READ THE SIGNAL STRIP

● Signal detected (risk indicator) ○ Signal not detected (safer) — Not applicable / inconclusive

Signals checked per domain: **DNS** · **MX Records** · **Live Web** · **Login Form** · **Brand Mention** · **Browser-Trusted SSL** · **Privacy WHOIS**

mooli.org

30/100

ACTIVE_THREAT • Risk 30 • FAIL 3 • WARN 11

● DNS ● MX Records ● Live Web ● Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

This domain accepts email (MX), serves web content, hosts a login form and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus login form on a lookalike domain. High-priority credential-harvesting risk.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-WEB-022	Web Presence & Content	Lookalike domain contains a login form or credential input. This is a strong credential-harvesting signal that warrants immediate review.	Review immediately. Preserve screenshots, capture the page URL, and report to the host/registrar if the page is deceptive or abusive.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-MAIL-032	Mail Infrastructure (Phishing Readiness)	DMARC record detected with monitoring/non-reject policy. This is a mail-readiness signal, but not proof of fully authenticated phishing.	Review the DMARC policy value and correlate it with SPF/DKIM and other impersonation indicators before escalating.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.

Status	Rule	Category	Details	Recommendation
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-WEB-024	Web Presence & Content	Wildcard DNS is configured — any subdomain (e.g., login.fakebrand.com, portal.fakebrand.com) will resolve. This vastly expands the phishing attack surface.	Wildcard DNS means attackers can create unlimited convincing subdomains without any additional configuration. Add *.domain to blocklists, not just the root domain.

19 passed, 2 inconclusive / not applicable (21 rules omitted for brevity — no scanner data or no material findings).

moori.info

27/100

ACTIVE_THREAT • Risk 27 • FAIL 3 • WARN 11

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

> This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-REG-002	Registration & Ownership	Domain was registered within the last 90 days. High risk of active phishing or brand abuse.	Review this domain periodically. Recently registered lookalikes are frequently used for phishing campaigns shortly after creation.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-MAIL-035	Mail Infrastructure (Phishing Readiness)	MX records point to a mail-forwarding or hosted routing provider. This is a passive mail-readiness signal, not proof of malicious use or catch-all acceptance.	Treat as corroborating mail-readiness evidence, not proof of abuse and not an SMTP catch-all result. Review alongside SPF, DKIM, DMARC, live web content, brand references, recent registration, and reputation signals.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

19 passed, 2 inconclusive / not applicable (21 rules omitted for brevity — no scanner data or no material findings).

mooli.online

24/100

ACTIVE_THREAT • Risk 24 • FAIL 2 • WARN 12

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-REG-002	Registration & Ownership	Domain was registered within the last 90 days. High risk of active phishing or brand abuse.	Review this domain periodically. Recently registered lookalikes are frequently used for phishing campaigns shortly after creation.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-COMP-080	Composite High-Risk Signals	Domain is parked or for-sale with privacy-protected WHOIS. Brand references on parked marketplace pages are common and do not indicate active abuse. Review periodically for activation.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-MAIL-032	Mail Infrastructure (Phishing Readiness)	DMARC record detected with monitoring/non-reject policy. This is a mail-readiness signal, but not proof of fully authenticated phishing.	Review the DMARC policy value and correlate it with SPF/DKIM and other impersonation indicators before escalating.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-WEB-021	Web Presence & Content	Domain is parked or showing a generic registrar/advertising landing page. Parked domains can be weaponized at any time.	Lower immediate risk, but parked domains can be activated quickly. Consider a defensive acquisition if the domain closely matches your brand.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

19 passed, 2 inconclusive / not applicable (21 rules omitted for brevity — no scanner data or no material findings).

moorla.io

28/100

ACTIVE_THREAT • Risk 28 • FAIL 2 • WARN 9

• DNS • MX Records — Live Web — Login Form — Brand Mention ○ SSL Signals • Privacy WHOIS

This domain accepts email (MX) and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Vowel substitution. Moderately deceptive in quick reading.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.

Status	Rule	Category	Details	Recommendation
WARN	BGD-WEB-024	Web Presence & Content	Wildcard DNS is configured — any subdomain (e.g., login.fakebrand.com, portal.fakebrand.com) will resolve. This vastly expands the phishing attack surface.	Wildcard DNS means attackers can create unlimited convincing subdomains without any additional configuration. Add *.domain to blocklists, not just the root domain.
WARN	BGD-MAIL-035	Mail Infrastructure (Phishing Readiness)	MX records point to a mail-forwarding or hosted routing provider. This is a passive mail-readiness signal, not proof of malicious use or catch-all acceptance.	Treat as corroborating mail-readiness evidence, not proof of abuse and not an SMTP catch-all result. Review alongside SPF, DKIM, DMARC, live web content, brand references, recent registration, and reputation signals.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-REG-005	Registration & Ownership	Domain is registered with a registrar commonly associated with bulk/cheap domain squatting. This is weak corroboration only, not proof of abuse.	Informational corroboration only. Bulk/cheap registrars are frequently used by squatters due to low cost. Combined with stronger threat indicators, this can increase suspicion.

13 passed, 11 inconclusive / not applicable (24 rules omitted for brevity — no scanner data or no material findings).

moorii.net

25/100

ACTIVE_THREAT • Risk 25 • FAIL 2 • WARN 7

• DNS • MX Records — Live Web — Login Form — Brand Mention — SSL Signals • Privacy WHOIS

This domain accepts email (MX) and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-WEB-024	Web Presence & Content	Wildcard DNS is configured — any subdomain (e.g., login.fakebrand.com, portal.fakebrand.com) will resolve. This vastly expands the phishing attack surface.	Wildcard DNS means attackers can create unlimited convincing subdomains without any additional configuration. Add *.domain to blocklists, not just the root domain.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-REG-005	Registration & Ownership	Domain is registered with a registrar commonly associated with bulk/cheap domain squatting. This is weak corroboration only, not proof of abuse.	Informational corroboration only. Bulk/cheap registrars are frequently used by squatters due to low cost. Combined with stronger threat indicators, this can increase suspicion.

14 passed, 12 inconclusive / not applicable (26 rules omitted for brevity — no scanner data or no material findings).

moorki.com

25/100

ACTIVE_THREAT • Risk 25 • FAIL 2 • WARN 13

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

> This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-MAIL-032	Mail Infrastructure (Phishing Readiness)	DMARC record detected with monitoring/non-reject policy. This is a mail-readiness signal, but not proof of fully authenticated phishing.	Review the DMARC policy value and correlate it with SPF/DKIM and other impersonation indicators before escalating.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.

Status	Rule	Category	Details	Recommendation
WARN	BGD-MAIL-034	Mail Infrastructure (Phishing Readiness)	DKIM selector responds with a valid key. This is a mail-readiness signal that supports higher deliverability when combined with SPF/DMARC. Absence of DKIM does not imply safety.	Escalate if DKIM is present alongside MX + SPF/DMARC, especially if the domain is new or has brand/login indicators.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Keyboard-adjacent typo. Common user mistake that drives traffic to squatters.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

20 passed (20 rules omitted for brevity — no scanner data or no material findings).

morli.com

24/100

ACTIVE_THREAT • Risk 24 • FAIL 2 • WARN 8

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention — SSL Signals ● Privacy WHOIS

> This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-MAIL-032	Mail Infrastructure (Phishing Readiness)	DMARC record detected with monitoring/non-reject policy. This is a mail-readiness signal, but not proof of fully authenticated phishing.	Review the DMARC policy value and correlate it with SPF/DKIM and other impersonation indicators before escalating.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

19 passed, 6 inconclusive / not applicable (25 rules omitted for brevity — no scanner data or no material findings).

mourli.com

23/100

ACTIVE_THREAT • Risk 23 • FAIL 2 • WARN 12

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.

Status	Rule	Category	Details	Recommendation
WARN	BGD-SIM-060	Similarity & Permutation Type	Vowel substitution. Moderately deceptive in quick reading.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-MAIL-033	Mail Infrastructure (Phishing Readiness)	MX points to a recognized email provider. Domain is set up for real email operations.	A recognized email provider indicates this domain is set up for real email operations, not just placeholder MX records. Report to the provider's abuse team directly.
WARN	BGD-SSL-043	SSL/TLS Configuration	Certificate issued within the last 14 days. Recently activated domain.	Treat this as a timing signal. Pair it with stronger indicators (live content, login forms, MX/email auth, blocklists). If those are present, escalate quickly.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

19 passed, 2 inconclusive / not applicable (21 rules omitted for brevity — no scanner data or no material findings).

morli.info

23/100

ACTIVE_THREAT • Risk 23 • FAIL 2 • WARN 8

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention — SSL Signals ● Privacy WHOIS

> This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-DNS-012	DNS Resolution & Hosting	Domain redirects to an unrelated URL outside both the protected brand and the candidate family. Review the destination, but do not treat the redirect alone as conclusive phishing evidence.	Review the final destination and pair this redirect with stronger evidence such as live impersonation content, login forms, brand references, or reputation flags before treating it as an active phishing redirect.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

19 passed, 6 inconclusive / not applicable (25 rules omitted for brevity — no scanner data or no material findings).

morli.top

23/100

ACTIVE_THREAT • Risk 23 • FAIL 2 • WARN 11

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

> This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-MAIL-032	Mail Infrastructure (Phishing Readiness)	DMARC record detected with monitoring/non-reject policy. This is a mail-readiness signal, but not proof of fully authenticated phishing.	Review the DMARC policy value and correlate it with SPF/DKIM and other impersonation indicators before escalating.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-SSL-041	SSL/TLS Configuration	SSL certificate was issued by a free/automated CA (for example, Let's Encrypt). Legitimate sites use free CAs too, so this is minor corroboration only.	Minor corroboration only. Free CAs are not inherently suspicious, but combined with stronger indicators (new registration, brand mention, login form), they can modestly raise the risk profile.

20 passed, 2 inconclusive / not applicable (22 rules omitted for brevity — no scanner data or no material findings).

moori.net

23/100

ACTIVE_THREAT • Risk 23 • FAIL 2 • WARN 11

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

> This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.

Status	Rule	Category	Details	Recommendation
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-WEB-024	Web Presence & Content	Wildcard DNS is configured — any subdomain (e.g., login.fakebrand.com, portal.fakebrand.com) will resolve. This vastly expands the phishing attack surface.	Wildcard DNS means attackers can create unlimited convincing subdomains without any additional configuration. Add *.domain to blocklists, not just the root domain.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-SSL-041	SSL/TLS Configuration	SSL certificate was issued by a free/automated CA (for example, Let's Encrypt). Legitimate sites use free CAs too, so this is minor corroboration only.	Minor corroboration only. Free CAs are not inherently suspicious, but combined with stronger indicators (new registration, brand mention, login form), they can modestly raise the risk profile.

20 passed, 2 inconclusive / not applicable (22 rules omitted for brevity — no scanner data or no material findings).

mooli.net

20/100

ACTIVE_THREAT • Risk 20 • FAIL 1 • WARN 7

• DNS • MX Records — Live Web — Login Form — Brand Mention — SSL Signals • Privacy WHOIS

This domain accepts email (MX) and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure. Suspicious, but not enough on its own to prove intentional abuse.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-005	Registration & Ownership	Domain is registered with a registrar commonly associated with bulk/cheap domain squatting. This is weak corroboration only, not proof of abuse.	Informational corroboration only. Bulk/cheap registrars are frequently used by squatters due to low cost. Combined with stronger threat indicators, this can increase suspicion.

15 passed, 12 inconclusive / not applicable (27 rules omitted for brevity — no scanner data or no material findings).

moori.co

20/100

ACTIVE_THREAT • Risk 20 • FAIL 1 • WARN 10

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals — Privacy WHOIS

This domain accepts email (MX) and serves web content. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.
WARN	BGD-MAIL-034	Mail Infrastructure (Phishing Readiness)	DKIM selector responds with a valid key. This is a mail-readiness signal that supports higher deliverability when combined with SPF/DMARC. Absence of DKIM does not imply safety.	Escalate if DKIM is present alongside MX + SPF/DMARC, especially if the domain is new or has brand/login indicators.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.

Status	Rule	Category	Details	Recommendation
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-SSL-041	SSL/TLS Configuration	SSL certificate was issued by a free/automated CA (for example, Let's Encrypt). Legitimate sites use free CAs too, so this is minor corroboration only.	Minor corroboration only. Free CAs are not inherently suspicious, but combined with stronger indicators (new registration, brand mention, login form), they can modestly raise the risk profile.
WARN	BGD-REG-004	Registration & Ownership	Some core RDAP/WHOIS registration metadata could not be determined. Treat ownership and timing conclusions more cautiously.	Use this as review context only. When registration metadata is incomplete, rely more heavily on active infrastructure signals such as MX records, live web content, login forms, TLS certificate signals, and reputation corroboration.

17 passed, 7 inconclusive / not applicable (24 rules omitted for brevity — no scanner data or no material findings).

mooli.com

19/100

ACTIVE_THREAT • Risk 19 • FAIL 1 • WARN 9

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention — SSL Signals ● Privacy WHOIS

> This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure. Suspicious, but not enough on its own to prove intentional abuse.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.

Status	Rule	Category	Details	Recommendation
WARN	BGD-MAIL-033	Mail Infrastructure (Phishing Readiness)	MX points to a recognized email provider. Domain is set up for real email operations.	A recognized email provider indicates this domain is set up for real email operations, not just placeholder MX records. Report to the provider's abuse team directly.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-WEB-025	Web Presence & Content	Domain is behind a CDN. Remediation requires reporting to the CDN provider in addition to the origin host.	Operational corroboration only. If the domain is behind a CDN, report to both the CDN provider and the registrar/origin host. Do not treat CDN usage by itself as proof of abuse.

19 passed, 6 inconclusive / not applicable (25 rules omitted for brevity — no scanner data or no material findings).

morli.co

19/100

ACTIVE_THREAT • Risk 19 • FAIL 1 • WARN 11

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals — Privacy WHOIS

This domain accepts email (MX) and serves web content. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-MAIL-032	Mail Infrastructure (Phishing Readiness)	DMARC record detected with monitoring/non-reject policy. This is a mail-readiness signal, but not proof of fully authenticated phishing.	Review the DMARC policy value and correlate it with SPF/DKIM and other impersonation indicators before escalating.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.

Status	Rule	Category	Details	Recommendation
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-SSL-041	SSL/TLS Configuration	SSL certificate was issued by a free/automated CA (for example, Let's Encrypt). Legitimate sites use free CAs too, so this is minor corroboration only.	Minor corroboration only. Free CAs are not inherently suspicious, but combined with stronger indicators (new registration, brand mention, login form), they can modestly raise the risk profile.
WARN	BGD-WEB-025	Web Presence & Content	Domain is behind a CDN. Remediation requires reporting to the CDN provider in addition to the origin host.	Operational corroboration only. If the domain is behind a CDN, report to both the CDN provider and the registrar/origin host. Do not treat CDN usage by itself as proof of abuse.
WARN	BGD-REG-004	Registration & Ownership	Some core RDAP/WHOIS registration metadata could not be determined. Treat ownership and timing conclusions more cautiously.	Use this as review context only. When registration metadata is incomplete, rely more heavily on active infrastructure signals such as MX records, live web content, login forms, TLS certificate signals, and reputation corroboration.

18 passed, 5 inconclusive / not applicable (23 rules omitted for brevity — no scanner data or no material findings).

moorle.com

18/100

ACTIVE_THREAT • Risk 18 • FAIL 1 • WARN 10

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-COMP-080	Composite High-Risk Signals	Domain is parked or for-sale with privacy-protected WHOIS. Brand references on parked marketplace pages are common and do not indicate active abuse. Review periodically for activation.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Vowel substitution. Moderately deceptive in quick reading.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.

Status	Rule	Category	Details	Recommendation
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-WEB-021	Web Presence & Content	Domain is parked or showing a generic registrar/advertising landing page. Parked domains can be weaponized at any time.	Lower immediate risk, but parked domains can be activated quickly. Consider a defensive acquisition if the domain closely matches your brand.
WARN	BGD-MAIL-033	Mail Infrastructure (Phishing Readiness)	MX points to a recognized email provider. Domain is set up for real email operations.	A recognized email provider indicates this domain is set up for real email operations, not just placeholder MX records. Report to the provider's abuse team directly.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

22 passed, 2 inconclusive / not applicable (24 rules omitted for brevity — no scanner data or no material findings).

moroli.com

25/100

ACTIVE_THREAT • Risk 25 • FAIL 2 • WARN 10

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure with authentication signals. This is stronger than MX alone and warrants immediate review.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
FAIL	BGD-MAIL-032	Mail Infrastructure (Phishing Readiness)	Restrictive DMARC policy plus SPF indicates deliberate mail-authentication setup on a lookalike domain.	Review the DMARC policy value and correlate it with SPF/DKIM and other impersonation indicators before escalating.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-DNS-012	DNS Resolution & Hosting	Domain redirects to an unrelated URL outside both the protected brand and the candidate family. Review the destination, but do not treat the redirect alone as conclusive phishing evidence.	Review the final destination and pair this redirect with stronger evidence such as live impersonation content, login forms, brand references, or reputation flags before treating it as an active phishing redirect.
WARN	BGD-MAIL-031	Mail Infrastructure (Phishing Readiness)	Lookalike domain has an SPF record published. This suggests deliberate outbound email configuration beyond a bare parked domain.	Escalate when SPF is present alongside MX, DKIM, restrictive DMARC, brand references, or login-form evidence.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Adjacent character swap (transposition). Common typo-squatting vector that can fool hurried users.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 2 — close to your brand. Likely confusable at a glance.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

21 passed, 2 inconclusive / not applicable (23 rules omitted for brevity — no scanner data or no material findings).

moorii.com

16/100

ACTIVE_THREAT • Risk 16 • FAIL 1 • WARN 8

● DNS ● MX Records ● Live Web ○ Login Form ○ Brand Mention ○ SSL Signals ● Privacy WHOIS

> This domain accepts email (MX), serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active mail infrastructure. Suspicious, but not enough on its own to prove intentional abuse.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-MAIL-030	Mail Infrastructure (Phishing Readiness)	MX records are configured. This supports inbound mail handling and increases phishing/BEC relevance, but does not by itself prove outbound impersonation.	Treat as a priority mail-risk signal. Document the MX provider, add the domain to watch/block lists as appropriate, and correlate with SPF/DMARC/DKIM or other impersonation signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.

Status	Rule	Category	Details	Recommendation
WARN	BGD-MAIL-035	Mail Infrastructure (Phishing Readiness)	MX records point to a mail-forwarding or hosted routing provider. This is a passive mail-readiness signal, not proof of malicious use or catch-all acceptance.	Treat as corroborating mail-readiness evidence, not proof of abuse and not an SMTP catch-all result. Review alongside SPF, DKIM, DMARC, live web content, brand references, recent registration, and reputation signals.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-WEB-025	Web Presence & Content	Domain is behind a CDN. Remediation requires reporting to the CDN provider in addition to the origin host.	Operational corroboration only. If the domain is behind a CDN, report to both the CDN provider and the registrar/origin host. Do not treat CDN usage by itself as proof of abuse.

23 passed, 3 inconclusive / not applicable (26 rules omitted for brevity — no scanner data or no material findings).

mooeli.com

20/100

ACTIVE_THREAT • Risk 20 • FAIL 1 • WARN 7

● DNS ○ MX Records ● Live Web ○ Login Form ○ Brand Mention — SSL Signals ● Privacy WHOIS

This domain serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active web infrastructure. Suspicious, but not enough on its own to prove intentional abuse.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-DNS-012	DNS Resolution & Hosting	Domain redirects to an unrelated URL outside both the protected brand and the candidate family. Review the destination, but do not treat the redirect alone as conclusive phishing evidence.	Review the final destination and pair this redirect with stronger evidence such as live impersonation content, login forms, brand references, or reputation flags before treating it as an active phishing redirect.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Keyboard-adjacent typo. Common user mistake that drives traffic to squatters.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.

15 passed, 12 inconclusive / not applicable (27 rules omitted for brevity — no scanner data or no material findings).

mooli.io

18/100

ACTIVE_THREAT • Risk 18 • FAIL 1 • WARN 9

● DNS ○ MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

This domain serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active web infrastructure. Suspicious, but not enough on its own to prove intentional abuse.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-SSL-041	SSL/TLS Configuration	SSL certificate was issued by a free/automated CA (for example, Let's Encrypt). Legitimate sites use free CAs too, so this is minor corroboration only.	Minor corroboration only. Free CAs are not inherently suspicious, but combined with stronger indicators (new registration, brand mention, login form), they can modestly raise the risk profile.
OPP	BGD-REG-006	Registration & Ownership	Domain expires within 90 days. Set a reminder and prepare for acquisition.	Acquisition opportunity only. If this domain closely matches your brand and is expiring within 90 days, consider a defensive purchase, reminder, or backorder.

17 passed, 8 inconclusive / not applicable (25 rules omitted for brevity — no scanner data or no material findings).

mooli.app

18/100

ACTIVE_THREAT • Risk 18 • FAIL 1 • WARN 8

● DNS ○ MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

This domain serves web content and WHOIS is privacy-protected. It represents active infrastructure on a confusable domain and should be reviewed immediately with corroborating evidence.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-COMP-080	Composite High-Risk Signals	Privacy-protected registrant plus active web infrastructure. Suspicious, but not enough on its own to prove intentional abuse.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-WEB-020	Web Presence & Content	Non-parked live web content detected on a confusable domain. This is meaningful active-infrastructure evidence and warrants review.	Review the content promptly. If it impersonates your brand or hosts suspicious workflows, capture evidence and report the host/registrar. Generic parking/for-sale pages should be handled under the parked-page rule instead.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.

Status	Rule	Category	Details	Recommendation
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-SSL-041	SSL/TLS Configuration	SSL certificate was issued by a free/automated CA (for example, Let's Encrypt). Legitimate sites use free CAs too, so this is minor corroboration only.	Minor corroboration only. Free CAs are not inherently suspicious, but combined with stronger indicators (new registration, brand mention, login form), they can modestly raise the risk profile.

18 passed, 8 inconclusive / not applicable (26 rules omitted for brevity — no scanner data or no material findings).

moorla.com

24/100

PARKED • Risk 24 • FAIL 3 • WARN 10

● DNS ○ MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals ● Privacy WHOIS

> This domain serves web content and WHOIS is privacy-protected. Rescan periodically to track changes.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-REG-002	Registration & Ownership	Domain was registered within the last 90 days. High risk of active phishing or brand abuse.	Review this domain periodically. Recently registered lookalikes are frequently used for phishing campaigns shortly after creation.
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
FAIL	BGD-SSL-043	SSL/TLS Configuration	SSL certificate was issued in the last 7 days. Very recent cert on a lookalike domain is a strong indicator of active setup.	Treat this as a timing signal. Pair it with stronger indicators (live content, login forms, MX/email auth, blocklists). If those are present, escalate quickly.
WARN	BGD-COMP-080	Composite High-Risk Signals	Domain is parked or for-sale with privacy-protected WHOIS. Brand references on parked marketplace pages are common and do not indicate active abuse. Review periodically for activation.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-DNS-012	DNS Resolution & Hosting	Domain is parked or for-sale and redirects to a marketplace or registrar landing page. Lower immediate risk than an active phishing redirect, but the domain could be weaponized if acquired by a threat actor.	Review the final destination and pair this redirect with stronger evidence such as live impersonation content, login forms, brand references, or reputation flags before treating it as an active phishing redirect.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.

Status	Rule	Category	Details	Recommendation
WARN	BGD-SIM-060	Similarity & Permutation Type	Vowel substitution. Moderately deceptive in quick reading.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-WEB-021	Web Presence & Content	Domain is parked or showing a generic registrar/advertising landing page. Parked domains can be weaponized at any time.	Lower immediate risk, but parked domains can be activated quickly. Consider a defensive acquisition if the domain closely matches your brand.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-SSL-041	SSL/TLS Configuration	SSL certificate was issued by a free/automated CA (for example, Let's Encrypt). Legitimate sites use free CAs too, so this is minor corroboration only.	Minor corroboration only. Free CAs are not inherently suspicious, but combined with stronger indicators (new registration, brand mention, login form), they can modestly raise the risk profile.

16 passed, 6 inconclusive / not applicable (22 rules omitted for brevity — no scanner data or no material findings).

moorli.com

22/100

PARKED • Risk 22 • FAIL 1 • WARN 12

● DNS ○ MX Records ● Live Web ○ Login Form ● Brand Mention ● SSL Signals ● Privacy WHOIS

This domain serves web content, mentions your brand and WHOIS is privacy-protected. Rescan periodically to track changes.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Identical name on a different TLD. Very high deception risk.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-COMP-080	Composite High-Risk Signals	Domain is parked or for-sale with privacy-protected WHOIS. Brand references on parked marketplace pages are common and do not indicate active abuse. Review periodically for activation.	Prioritize for analyst review, containment, and evidence capture when privacy shielding appears alongside corroborating web or mail signals.
WARN	BGD-SSL-042	SSL/TLS Configuration	Certificate SAN/CN includes the brand token or primary-domain string. This increases impersonation confidence.	Treat as corroborating evidence. Escalate more aggressively when certificate naming aligns with live content, login forms, or mail-authentication signals.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-DNS-012	DNS Resolution & Hosting	Domain is parked or for-sale and redirects to a marketplace or registrar landing page. Lower immediate risk than an active phishing redirect, but the domain could be weaponized if acquired by a threat actor.	Review the final destination and pair this redirect with stronger evidence such as live impersonation content, login forms, brand references, or reputation flags before treating it as an active phishing redirect.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	TLD variation of your primary domain. Common defensive gap.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.

Status	Rule	Category	Details	Recommendation
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-WEB-021	Web Presence & Content	Domain is parked or showing a generic registrar/advertising landing page. Parked domains can be weaponized at any time.	Lower immediate risk, but parked domains can be activated quickly. Consider a defensive acquisition if the domain closely matches your brand.
WARN	BGD-WEB-024	Web Presence & Content	Wildcard DNS is configured — any subdomain (e.g., login.fakebrand.com, portal.fakebrand.com) will resolve. This vastly expands the phishing attack surface.	Wildcard DNS means attackers can create unlimited convincing subdomains without any additional configuration. Add *.domain to blocklists, not just the root domain.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-SSL-041	SSL/TLS Configuration	SSL certificate was issued by a free/automated CA (for example, Let's Encrypt). Legitimate sites use free CAs too, so this is minor corroboration only.	Minor corroboration only. Free CAs are not inherently suspicious, but combined with stronger indicators (new registration, brand mention, login form), they can modestly raise the risk profile.

16 passed, 6 inconclusive / not applicable (22 rules omitted for brevity — no scanner data or no material findings).

moori.shop

14/100

PARKED • Risk 14 • FAIL 1 • WARN 6

● DNS ○ MX Records ● Live Web ○ Login Form ○ Brand Mention ● SSL Signals — Privacy WHOIS

This domain serves web content. Rescan periodically to track changes.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Doubled or dropped letter. Common squatting technique.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-SSL-040	SSL/TLS Configuration	Lookalike domain has a browser-trusted SSL/TLS certificate for this hostname. This gives the site a padlock icon and 'https://' prefix, increasing victim trust.	A browser-trusted SSL certificate can make a phishing site appear more legitimate. Users trained to 'look for the padlock' can be deceived. Factor this into your risk assessment.
WARN	BGD-WEB-021	Web Presence & Content	Domain is parked or showing a generic registrar/advertising landing page. Parked domains can be weaponized at any time.	Lower immediate risk, but parked domains can be activated quickly. Consider a defensive acquisition if the domain closely matches your brand.
WARN	BGD-REG-004	Registration & Ownership	Some core RDAP/WHOIS registration metadata could not be determined. Treat ownership and timing conclusions more cautiously.	Use this as review context only. When registration metadata is incomplete, rely more heavily on active infrastructure signals such as MX records, live web content, login forms, TLS certificate signals, and reputation corroboration.

15 passed, 13 inconclusive / not applicable (28 rules omitted for brevity — no scanner data or no material findings).

moofli.com

24/100

INACTIVE • Risk 24 • FAIL 1 • WARN 6 • Light Scan

• DNS — MX Records — Live Web — Login Form — Brand Mention — SSL Signals • Privacy WHOIS

This domain WHOIS is privacy-protected. Rescan periodically to track changes.

Status	Rule	Category	Details	Recommendation
FAIL	BGD-SIM-061	Similarity & Permutation Type	Edit distance is 1 — extremely close to your brand.	Domains with edit distance of 1-2 are the highest risk for user confusion and should be prioritized for review.
WARN	BGD-DNS-010	DNS Resolution & Hosting	Domain resolves to an IP address. Infrastructure is present.	Visit the domain carefully (use a sandboxed browser or screenshot service) to determine what content is being served. If impersonating your brand, report to the hosting provider via their abuse contact.
WARN	BGD-REG-001	Registration & Ownership	Registered lookalike detected. Ownership and intent must be validated.	Investigate the registrant. If unauthorized, consult legal counsel about a UDRP (Uniform Domain-Name Dispute-Resolution Policy) filing or cease-and-desist.
WARN	BGD-SIM-060	Similarity & Permutation Type	Keyboard-adjacent typo. Common user mistake that drives traffic to squatters.	Higher similarity scores indicate domains more likely to deceive users. Prioritize remediation of high-similarity domains.
WARN	BGD-WEB-024	Web Presence & Content	Wildcard DNS is configured — any subdomain (e.g., login.fakebrand.com, portal.fakebrand.com) will resolve. This vastly expands the phishing attack surface.	Wildcard DNS means attackers can create unlimited convincing subdomains without any additional configuration. Add *.domain to blocklists, not just the root domain.
WARN	BGD-REG-003	Registration & Ownership	Registrant information is hidden behind a privacy/proxy service. Cannot determine if this is your organization or a third party.	Privacy-protected WHOIS is common but prevents easy identification. If the domain shows active threat indicators (web content, MX records), escalate for legal review.
WARN	BGD-REG-005	Registration & Ownership	Domain is registered with a registrar commonly associated with bulk/cheap domain squatting. This is weak corroboration only, not proof of abuse.	Informational corroboration only. Bulk/cheap registrars are frequently used by squatters due to low cost. Combined with stronger threat indicators, this can increase suspicion.

4 passed, 24 inconclusive / not applicable (28 rules omitted for brevity — no scanner data or no material findings).

Disclaimer

MOORLI BrandGuardDiagnostic is an automated intelligence service provided by **MOORLI LLC** that evaluates **publicly observable signals** related to lookalike domains and brand impersonation risk. Risk scores, classifications, and recommendations are generated by software algorithms and are provided solely for **informational and educational purposes**.

Passive analysis only. This Service performs passive analysis of public DNS/registration records and lightweight HTTP/TLS checks. We do not attempt authentication, probe internal networks, perform penetration testing, exploit vulnerabilities, or conduct intrusive security testing. SMTP catch-all acceptance testing is not performed in passive mode.

No professional advice. MOORLI is not a cybersecurity firm, MSSP, insurer, registrar, or law firm. Nothing in this report constitutes legal advice, compliance advice, or professional cybersecurity guidance. Consult qualified professionals as appropriate, including counsel for trademark and enforcement actions.

Accuracy limits & false positives/negatives. Results depend on DNS propagation, public record availability, and reachability at scan time. Some domains may be blocked by WAF/captcha, geofencing, or temporary outages, which can result in *Inconclusive (NA)* signals. Adversaries can activate infrastructure quickly or conceal signals that are not observable during the scan window.

Third-party threat intelligence. We may submit candidate URLs/domains to third-party reputation providers as a corroborating input in our analysis of potentially malicious activity. These external sources are provided **"AS IS"**, are not redistributed verbatim, and are used as one factor within our own scoring and findings. Some risky sites may not be identified, and some safe sites may be identified in error.

No guarantee. Absence of detected threats does not guarantee safety. This report reflects conditions only at the time of scanning and does not provide continuous monitoring unless you run subsequent rescans.

Third-party actions. Remediation steps (e.g., registrar/hosting abuse reports, takedown requests, mail gateway blocks, UDRP/URS actions) may involve third parties. Outcomes are controlled by those parties and may vary by jurisdiction, policy, and evidence requirements. You are responsible for all enforcement decisions and actions.

External references. Any third-party tools, registrars, hosting providers, or referenced resources are provided for convenience only and do not constitute endorsement. MOORLI has no control over third-party systems or their availability.

Warranty disclaimer. Reports are provided **"AS IS"** and **"AS AVAILABLE"**, without warranties of any kind (express or implied), including merchantability, fitness for a particular purpose, non-infringement, or accuracy.

Limitation of liability. To the fullest extent permitted by law, MOORLI LLC shall not be liable for any indirect, incidental, special, consequential, punitive, or exemplary damages arising from use of this report or reliance on its contents. In any event, MOORLI LLC's total aggregate liability for any claim shall not exceed the amount paid for the specific audit/report.