SunTzu CyberSecurity Labs LLC

SECURITY INTELLIGENCE & RISK ANALYSIS

Email Trust & Impersonation Review

External email authentication, impersonation resistance, and identity exposure assessment

Sanitized copy. Selected identifying or technical details have been replaced or removed.

CLIENT Client Organization	CUSTOMER ID Redacted
PRIMARY TARGET target1.example (192.0.2.1)	ASSESSMENT ID SAMPLE
COMPLETED Aug 31, 2026	REPORT GENERATED Sep 01, 2026

Public website sample. Customer-identifying and sensitive technical details have been sanitized.

Executive Summary

Why this matters: Fraudulent email that appears to come from your domain can be used to steal credentials, redirect payments, impersonate executives, and damage customer trust. This assessment tests whether receiving mail systems have enough externally visible evidence and policy direction to distinguish authorized mail from spoofed mail.

What This Means for Your Domain

target1.example was rated strong for externally observable email impersonation resistance. SPF is published with a hard-fail policy; DKIM capability was observed (2 selectors observed); DMARC is published with p=quarantine and reporting configured. Mail routing appears to use TitanHQ. MTA-STS was not observed; SMTP TLS reporting was not observed; BIMI was not observed; it is optional and should follow mature DMARC enforcement. Inspect a representative production message to confirm SPF or DKIM alignment and DMARC pass behavior.

target1.example's published SPF, DKIM, and enforcing DMARC controls materially reduce direct spoofing of the domain. They do not prevent lookalike domains, compromised mailboxes, or phishing sent from another trusted service, so phishing-resistant MFA and user/payment verification processes remain important.

What the Scan Found

ASSESSED DOMAIN

target1.example

Mail provider: TitanHQ

IMPERSONATION RESISTANCE

Strong

No material weakness was confirmed.

Next owner action: No material email-authentication weakness was confirmed. Maintain the current SPF, DKIM, and DMARC controls; add MTA-STS and TLS-RPT as the next practical hardening step; and validate alignment from production mail.

Continuous service recommended: For this strong posture, continuous service should preserve the current protections, detect configuration regression, and verify that new sending services do not weaken alignment or enforcement.

Scope and Observed Assets

Consolidated identity view

Related hostnames, addresses, services, and URLs are consolidated using evidence-backed relationships so one host is not repeated as several unrelated report assets.

Asset	Observed forms	Scope	Findings
target1.example (192.0.2.1)	hostname, ip 5 linked records	In scope	0

Email Trust and Impersonation Posture

Passive external assessment

DOMAIN IMPERSONATION RESISTANCE

Strong

SPF, observable DKIM capability, and enforcing DMARC were identified. Message-level authentication and alignment should still be validated from a qualifying production email when available.

Target Domain

Domain	Mail Provider	Mail Routing	Observed MX Hosts
target1.example	TitanHQ	Enabled	target2.example, target3.example

Authentication Controls

Control	Assessment	Evidence Found	Interpretation
SPF	PRESENT	v=spf1 a:target4.example include:target5.example -all	Sender Policy Framework was externally confirmed.
DKIM	PRESENT	Selectors: selector1, selector2	DomainKeys Identified Mail was externally confirmed.
DMARC	PRESENT	v=DMARC1; p=quarantine; rua=mailto:contact1@example.test; ruf=mailto:contact1@example.test; fo=1;	DMARC was externally confirmed.
DMARC Enforcement	PRESENT	v=DMARC1; p=quarantine; rua=mailto:contact1@example.test; ruf=mailto:contact1@example.test; fo=1;	DMARC Enforcement was externally confirmed.
DMARC Reporting	PRESENT	v=DMARC1; p=quarantine; rua=mailto:contact1@example.test; ruf=mailto:contact1@example.test; fo=1;	DMARC Reporting was externally confirmed.

Public Identity Exposure

0
Target-domain identities observed

0
Role accounts observed

0
Potential high-value identities

0

Highest targeting score

Publicly observable email identities can assist legitimate customers and partners, but they can also provide targeting information for phishing, business email compromise, and impersonation attempts. Exposure is therefore reported as context rather than treated automatically as a vulnerability.

Additional Mail Security Controls

Control	Assessment	Owner Action	Security Context
Mail Routing	Present	Maintain and revalidate after DNS or provider changes.	Email Mail Routing was externally confirmed.
MTA-STS	Not observed	Consider implementing MTA-STS with a valid published policy to strengthen inbound SMTP transport security.	No MTA-STS DNS signaling record was observed.
TLS-RPT	Not observed	Publish a TLS-RPT policy and monitor reports for SMTP transport-security failures.	No SMTP TLS reporting policy was observed.
BIMI	Not observed	Consider BIMI only after SPF, DKIM and DMARC enforcement are mature and operationally validated.	No BIMI record was observed. BIMI is an optional identity enhancement rather than a core email-authentication requirement.

Methodology and Limitations

Assessment Activities

- Authorized domain normalization and passive DNS review
- Mail exchanger and provider identification
- SPF, DMARC, and commonly published DKIM selector assessment
- MTA-STS, TLS reporting, and BIMI record review
- Passive email exposure correlation when data is available

Scope Boundary

Testing was limited to the authorized email domain and externally observable email-security information. Related or third-party domains and addresses observed on authorized public content were retained as evidence but were not automatically treated as customer-owned infrastructure or authorization to assess those domains.

Limitations

Results represent a point-in-time passive external assessment. DNS records, mail-routing information, public email identities, and commonly used DKIM selectors were reviewed without sending mail, authenticating to customer systems, accessing mailboxes, or attempting to deliver spoofed messages.

DKIM selectors are not globally predictable. Failure to discover a selector through passive testing does not prove DKIM is absent. Production message headers can provide stronger evidence of DKIM signing and DMARC alignment when such evidence is available.

Public email-address exposure is reported as targeting context. The presence of a publicly listed email address is not, by itself, treated as a vulnerability.

Recommended Use

Use this report to prioritize remediation and follow-up validation. Findings should be evaluated alongside asset ownership, business criticality, compensating controls, and operational context.

Tech Findings, Remediations and Recommendations

Owner action register

This final register consolidates the scan evidence into technical findings, the corrective action indicated by the evidence, and a practical owner recommendation. Confirmed protections are included so the report documents what should be preserved as well as what should change.

Technical Evidence Summary

Evidence	Observed Value	Meaning
Mail routing	`target2.example, target3.example`	Identifies the externally published inbound mail path and apparent provider.
SPF record	`v=spf1 a:target4.example include:target5.example -all`	Defines which systems are authorized to send mail for the domain.
DKIM selectors	`selector1, selector2`	Shows discoverable public keys; production message validation is still required.
DMARC record	`v=DMARC1; p=quarantine; rua=mailto:contact1@example.test; ruf=mailto:contact1@example.test; fo=1;`	Defines authentication policy, enforcement, and reporting destinations.
MTA-STS / TLS-RPT	MTA-STS not observed; TLS-RPT not observed	These controls improve and monitor transport security for inbound SMTP.

Technical Action Register

Domain impersonation resistance — Present

CONFIRMED PROTECTION

Finding: SPF, observable DKIM capability, and enforcing DMARC were identified. Message-level authentication and alignment should still be validated from a qualifying production email when available.

Remediation: No corrective action indicated by this external scan.

Recommendation: Validate a representative production message for SPF/DKIM alignment and DMARC pass behavior.

SPF — Present

CONFIRMED PROTECTION

Finding: Sender Policy Framework was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Maintain one valid SPF record, inventory every authorized sender, and revalidate after sender or DNS changes.

DKIM — Present

CONFIRMED PROTECTION

Finding: DomainKeys Identified Mail was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Confirm each production sending platform signs with an aligned domain; rotate keys according to provider guidance.

DMARC — Present

CONFIRMED PROTECTION

Finding: DMARC was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Continue reviewing DMARC reports and progress toward p=reject when all legitimate mail streams are validated.

DMARC reporting — Present

CONFIRMED PROTECTION

Finding: DMARC Reporting was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Confirm the reporting mailbox is monitored and that aggregate reports are retained for trend review.

DMARC enforcement — Present

CONFIRMED PROTECTION

Finding: DMARC Enforcement was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Treat quarantine as active enforcement and evaluate a controlled move to reject after validating legitimate senders.

Mail routing — Present

CONFIRMED PROTECTION

Finding: Email Mail Routing was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Confirm the observed MX provider and records remain authorized and remove stale routing entries.

MTA-STS — Not confirmed

RECOMMENDED HARDENING

Finding: No MTA-STS DNS signaling record was observed.

Remediation: Consider implementing MTA-STS with a valid published policy to strengthen inbound SMTP transport security.

Recommendation: Implement MTA-STS after confirming the production MX endpoints support the required TLS behavior.

TLS-RPT — Not confirmed

RECOMMENDED HARDENING

Finding: No SMTP TLS reporting policy was observed.

Remediation: Publish a TLS-RPT policy and monitor reports for SMTP transport-security failures.

Recommendation: Publish TLS-RPT and monitor reports for inbound SMTP transport security failures.

BIMI — Not confirmed

OPTIONAL ENHANCEMENT

Finding: No BIMI record was observed. BIMI is an optional identity enhancement rather than a core email-authentication requirement.

Remediation: No core security remediation is required.

Recommendation: Consider BIMI only as a later brand-trust enhancement after DMARC enforcement and operational monitoring are mature.

Public email identity exposure — Not confirmed

EVIDENCE GAP

Finding: No execution-scoped contact-surface evidence was available. Public email exposure cannot be determined from this historical execution.

Remediation: No corrective action can be concluded from passive data alone.

Recommendation: Perform a manual public-footprint review and retain only the organizational addresses that serve a business need.

High-value identity exposure — Not confirmed

EVIDENCE GAP

Finding: No normalized email-address observations were available for high-value exposure assessment.

Remediation: No corrective action can be concluded from passive data alone.

Recommendation: Manually review exposure of executive, finance, privileged, and other high-value identities and apply phishing-resistant MFA.

Recommended Continuous Protection

Continuous Email Trust Monitoring

This assessment is a point-in-time baseline. Email providers, DNS records, authorized sending platforms, DKIM keys, and publicly exposed identities change over time. Continuous monitoring detects control drift and suspicious sending activity before the next scheduled assessment.

For this strong posture, continuous service should preserve the current protections, detect configuration regression, and verify that new sending services do not weaken alignment or enforcement.

- Alert on SPF, DKIM, DMARC, MX, MTA-STS, and TLS-RPT record changes
- Collect and review DMARC aggregate reports for authorized and suspicious senders
- Maintain the inventory of services permitted to send as the domain
- Validate representative production headers after provider or DNS changes
- Track public and high-value email identity exposure
- Provide a recurring owner summary of posture, changes, incidents, and next actions

SunTzu CyberSecurity Labs can operate this service as the ongoing control layer after remediation, with alerts and recurring reporting tied to the assessed domain.

Confused or Unsure What to Do Next?

Email security can feel like evil wizardry: DNS records, authentication alignment, provider settings, reporting feeds, and delivery risk all have to work together. You do not need to translate or implement this report alone.

SunTzu CyberSecurity Labs can identify your legitimate sending services, prepare provider-safe DNS changes, implement SPF, DKIM, DMARC, MTA-STS, and TLS-RPT, validate production mail, and operate the continuous monitoring program.

Contact SunTzu CyberSecurity Labs to schedule an Email Security Remediation and Continuous Monitoring consultation.