DNS Intelligence Report

2911.us

DNS & Trust Posture: **SECURE (Monitoring)**

Security controls present but some in monitoring mode.

1 monitoring

Analyzed: 2026-02-07 19:50 UTC Duration: 2.7s

EMAIL SPOOFING	BRAND IMPERSONATION
Protected	Not Setup
DNS TAMPERING	**CERTIFICATE CONTROL**
Protected	Open

Monitoring
DKIM (MailChimp only — not verified for Microsoft 365)

Configured
DMARC (email spoofing protection), DNSSEC (DNS responses signed), MTA-STS (policy present), TLS-RPT (reporting configured)

Not Configured
CAA (certificate authority control), BIMI (brand logo in inboxes)

REGISTRAR (RDAP)
GoDaddy.com, LLC
Where you pay to own domain

EMAIL SERVICE PROVIDER
Microsoft 365
Where email is hosted (MX)

WEB HOSTING
GoDaddy
Where website is hosted

DNS HOSTING
GoDaddy
Where DNS records are edited

Email Security

Can this domain be impersonated by email? No

Verdict: DMARC policy is reject - spoofed messages will be blocked by receiving servers. Note: DKIM found for MailChimp only — primary mail platform (Microsoft 365) DKIM not verified.

SPF Record

RFC 7208

Success -all 1/10 lookups

SPF valid with strict enforcement (-all), 1/10 lookups

```
v=spf1 include:spf.protection.outlook.com -all
```

⚠ RFC 7489 §10.1: -all may cause rejection before DMARC evaluation, preventing DKIM from being checked

⚠ SPF hard fail (-all): compliance-strong, but can short-circuit DMARC. RFC 7489 §10.1 notes that -all can cause some receivers to reject mail during the SMTP transaction — before DKIM is checked and before DMARC can evaluate the result. A message that would pass DMARC via DKIM alignment may be rejected prematurely. For most domains, ~all + DMARC p=reject is the strongest compatible posture — it ensures every authentication method (SPF, DKIM, DMARC) is fully evaluated before a decision is made.
DMARC is set to reject — enforcement is strong. However, some receivers may still reject messages on SPF hard fail before DKIM alignment is checked. Switching to ~all + p=reject

DMARC Policy

RFC 7489

Success p=reject

DMARC policy reject (100%) - excellent protection

```
v=DMARC1; p=reject; pct=100; sp=reject; rua=mailto:81a9c434@in.mailhardener.com; ruf=mailto:81a9c434@in.mailhardener.com; adkim=r; aspf=r; fo=1; rf=afrf; ri=86400
```

Alignment: SPF relaxed DKIM relaxed sp=reject

⚠ Forensic reports (ruf) configured - many providers ignore these

Reported to Mailhardener

DKIM Records

RFC 6376

Third-Party Only 2048-bit

Found DKIM for 2 selector(s) (2048-bit) but none for primary mail platform (Microsoft 365)

⚠ DKIM verified for MailChimp only — no DKIM found for primary mail platform (Microsoft 365). The primary provider may use custom selectors not discoverable through standard checks.

✓ k1._domainkey MailChimp 2048-bit

```
k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDbNrX2cY/GUKIFx2G/1I00ftdAj713WP9AQ1xir85i89sA2guU0ta4UX1Xzm06XIU6iBP41VwmPwBGRNofhBVR+e6WHUoNyIR4Bn84LVcfZE20rmDeXQblIupNWBqLXM1Q+VieI/eZu/7k9/vOkLSaQQdml4Cv8lb3PcnluMVIhQIDAQAB;
```

✓ k2._domainkey MailChimp 2048-bit

would provide the same enforcement with full DMARC compatibility.

```
v=DKIM1; k=rsa; p=MIIB
IjANBgkqhkiG9w0BAQEFAA
OCAQ8AMIIBCgKCAQEAv2aC
2KjGKLOwTweBY5A9RpjsxA
BXR9r7OAU6U8/zn92ivImI
75naUujWbItRI/QmL1jy5P
WGqLwoUA0b90ObWaLDc+i9
MtTNmGeWO009hr20fIxhGg
6XBT2kjZ1DTThopSe1nAnd
supmcBwlQ5Q6LJ+ZAxLcuj
nPIxM0ZBLmgpkv8u6RfY4e
FP8OLvdAW3oSuB0DyLDigQ
X4Sj8wBO4YIdQH6AAmBeOs
idsKAFNFUCpc3vCxtBDR12
U+cBg724l3sBkMQ8evnz6i
dnqxq9QAVYh8k4kJ+RP+6c
qTdy7LjIm8xY/bQNpQIpGU
AuDo2DjLcCDun9DAI4Q/3z
+Q0o9QuQIDAQAB;
```

MTA-STS

RFC 8461 | Success | ENFORCE | Policy Verified

MTA-STS enforced - TLS required for 1 mail server(s)

```
v=STSv1; id=20260207191811
```

Policy Details:

- Mode: `enforce`
- Max Age: 14 days (1209600 seconds)
- MX Patterns: 2911-us.mail.protection.outlook.com

TLS-RPT

RFC 8460 | Success

TLS-RPT configured - receiving TLS delivery reports

```
v=TLSRPTv1; rua=mailto:81a9c434@in.mailhardener.com
```

Reported to Mailhardener

Email Security Management

Actively Managed

Intelligence: This domain uses dedicated email security management — indicating continuous monitoring and professional oversight, not a "set and forget" configuration. Most tools ignore reporting destinations; we extract the operational security partner network directly from DNS.

Mailhardener

DMARC TLS-RPT

- DMARC aggregate (rua) and forensic (ruf) reports
- TLS-RPT delivery reports

Brand Security

Can this brand be convincingly faked? Partially

Verdict: No brand protection controls - attackers could obtain certificates or impersonate visually.

BIMI

BIMI Spec Warning

No BIMI record found

CAA

RFC 8659 Warning

No CAA records found - any CA can issue certificates

Domain Security

Can DNS itself be tampered with? **No**

Verdict: DNS responses are authenticated from the root downward. Delegation is verified.

DNSSEC

RFC 4033 · Signe · ECDSA P-256/SI

DNSSEC fully configured and validated - AD flag confirmed by resolver

Chain of trust: Root → TLD → Domain. DNS responses are authenticated and tamper-proof.

AD Flag: Validated - Resolver (8.8.8.8) confirmed cryptographic signatures

DS Record (at registrar):

```
17048 13 2 3FCCDEBAFA765AF4F6254CED78E58
635944DC88C76A3E82FDDA2DF68A09ECF78
```

```
40611 13 2 24284E985302282351AA791F81059
E778C5B93ED4EA9536EB68832C9599CF6DB
```

NS Delegation

Verified

2 nameserver(s) configured

Nameservers:

- pdns01.domaincontrol.com
- pdns02.domaincontrol.com

Multi-Resolver Verification: Consensus reached - 4 resolvers (Cloudflare, Google, Quad9, OpenDNS) agree on DNS records

Traffic & Routing

Where traffic flows & how services resolve

A IPv4 Address

```
23.185.0.3
```

Where the domain points for web traffic

AAAA IPv6 Address

```
2620:12a:8001::3
```

```
2620:12a:8000::3
```

✓ IPv6 ready

MX Mail Servers

```
0 2911-us.mail.protection.outlook.com.
```

Priority + mail server for email delivery

SRV Services

— No SRV records

No service-specific routing configured

Web: Reachable (1 IPv4, 2 IPv6) **Mail:** 1 server **Services:** None

Δ No Propagation Issues: All DNS records are synchronized between resolver and authoritative nameserver.

Live DNS Diff

Real-time propagation comparison | See exactly what public resolvers return vs. what your authoritative nameserver has. Spot propagation delays, stale cache, and DNS misconfigurations instantly.

DNS Evidence Diff

Side-by-side comparison

Resolver Records (Public DNS cache)	Authoritative Records (Source of truth)
A Synchronized — 1 / 1 records	
23.185.0.3	23.185.0.3
AAAA Synchronized — 2 / 2 records	
2620:12a:8001::3	2620:12a:8000::3
2620:12a:8000::3	2620:12a:8001::3
MX Synchronized — 1 / 1 records	
0 2911-us.mail.protection.outlook.com.	0 2911-us.mail.protection.outlook.com.
TXT Synchronized — 5 / 5 records	
v=spf1 include:spf.protection.outlook.com -all	openai-domain-verification=dv-8fTZweKgrwn7udZbUlatxIuV
facebook-domain-verification=rtkwfzcjtrjgnz02y6nz0btld5a9q1	google-site-verification=cnKBmgtuqnLMn2LbH_RbjL3OfRZMzVJgA8YiGZwauJo
openai-domain-verification=dv-8fTZweKgrwn7udZbUlatxIuV	v=spf1 include:spf.protection.outlook.com -all
MS=ms63238513	facebook-domain-verification=rtkwfzcjtrjgnz02y6nz0btld5a9q1
google-site-verification=cnKBmgtuqnLMn2LbH_RbjL3OfRZMzVJgA8YiGZwauJo	MS=ms63238513
NS Synchronized — 2 / 2 records	
pdns01.domaincontrol.com.	pdns01.domaincontrol.com.
pdns02.domaincontrol.com.	pdns02.domaincontrol.com.

Confirm Your Email Configuration

This tool analyzes DNS records, but to verify actual email delivery, send a test email to Red Sift Investigate. Their tool shows exactly how your emails arrive, including SPF/DKIM/DMARC pass/fail results in the headers.

Report reflects evaluated DNS security posture at time of generation.

Made by IT Help San Diego Inc.

Need help with DNS? Call 619-853-5008