Email Spoofability Across Insurance Agencies

A Passive Measurement of DMARC Enforcement in 60 US Independent Insurance Agencies

Bridgham Technology Institute

June 2026

Abstract

We measured the published email-authentication posture of 60 US independent insurance agencies across three sampling frames, using only public DNS and contacting no one. Of the 60 agencies, 44 (73.3%, 95% Wilson CI [61.0, 82.9]) publish no enforcing DMARC policy, which means a message that did not originate with the agency can still reach a client's inbox appearing to come from it. We report the level per frame with 95% intervals, alongside SPF publication (93.3%) and DNSSEC signing (5.0%). The corrective step is a single DNS policy change. A pre-registered expectation that affiliated agencies would be better protected did not hold: the three frames were not distinguishable at this sample size.

1. Introduction

Insurance agencies hold client personal information, carry errors-and-omissions exposure, and depend on clients trusting that an emailed policy document or payment request came from the agency. Email authentication is the public, checkable control that supports that trust.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) lets a domain owner tell receiving mail servers what to do with a message that claims the domain but fails authentication.[1] An agency either publishes an enforcing DMARC policy, in which case mailbox providers can reject mail that fails authentication, or it does not, in which case impersonating mail can pass. This study measures which, across three frames of independent agencies.

2. Method

2.1. Measurement

The study is passive and uses public DNS only. No mail was sent and no agency was contacted. For each domain we resolved DMARC at the _dmarc label (presence, policy, and parseability),[1] the Sender Policy Framework record (presence, tri-state, with indeterminate reads excluded rather than counted absent),[2] DNSSEC by the DNSKEY-at-apex definition,[3] and MX as a mail-active context check.

2.2. Operational Definitions

A domain is *spoofable* when it has no enforcing DMARC policy: the record is absent, set to p=none, or unparseable. A domain is *protected* at p=quarantine or p=reject, and *strictly protected* at p=reject. Shares carry 95% Wilson score intervals. No significance test and no model are used.

2.3. Sampling Frames

All three frames are public and search-compiled. Frame A holds agencies presenting Trusted Choice or Big "I" affiliation across several metropolitan areas. Frame B holds general independent agencies across several metropolitan areas, with no affiliation screen. Frame C holds independent agencies in North Carolina.

Each row is one independently operated agency's own mail domain. Carriers, managing general agents, wholesalers, and rollup and aggregator domains were excluded. Of 62 agencies supplied, 60 were measured; 2 were excluded for having no MX record (not mail-active) and are not counted in any denominator.

2.4. Independent Reproduction

Two checks agreed. A from-scratch classifier over the same findings produced 0 disagreements, and a second resolution pass through reordered resolvers and Quad9 agreed domain-for-domain on all 60.

3. Results

3.1. Aggregate Level

Across all frames, 44 of 60 agencies (73.3%, 95% CI [61.0, 82.9]) publish no enforcing DMARC policy. Strict protection (p=reject) is present at 8 of 60 (13.3%), and any enforcing policy (quarantine or reject) at 16 of 60 (26.7%). SPF is published at 56 of 60 (93.3%). DNSSEC is signed at 3 of 60 (5.0%). Table 1 gives the level by frame.

Frame	N	Spoofable	95% CI
A, affiliated	33	78.8% (26/33)	[62.2, 89.3]
B, general	14	64.3% (9/14)	[38.8, 83.7]
C, North Carolina	13	69.2% (9/13)	[42.4, 87.3]
Aggregate	60	73.3% (44/60)	[61.0, 82.9]

Table 1: Spoofable Share by Sampling Frame, with 95% Wilson Score Intervals.

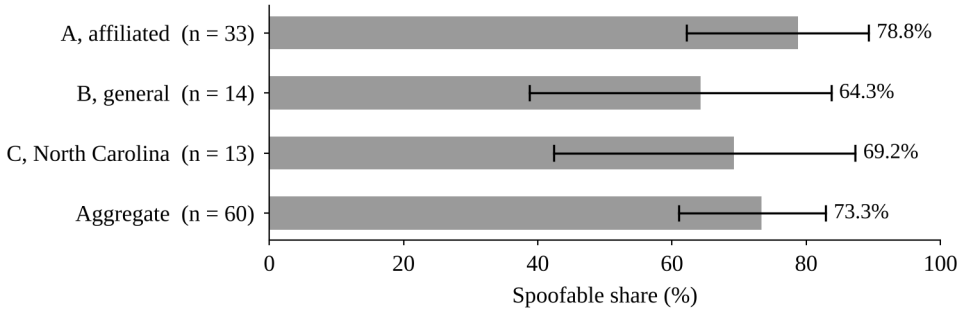


Figure 1: Spoofable Share by Frame and in Aggregate. Bars are point estimates; whiskers are 95% Wilson intervals. Every pairwise interval overlaps.

3.2. Frame Comparison

The pre-registered directional expectation was that affiliated agencies (Frame A) would show a lower spoofable share than the general frames. The data run the other way: the affiliated frame is directionally higher (78.8%) than the general frame (64.3%) and the North Carolina frame (69.2%), and all pairwise intervals overlap, so no frame is distinguishable at this sample size. We report the level and make no causal claim; affiliation is shown neither to protect nor to harm.

3.3. Declaring Versus Enforcing

The central pattern is the gap between publishing a sender record and enforcing it. SPF is nearly universal (93.3%), while any enforcing DMARC policy is the exception (26.7%, and 13.3% at p=reject). Agencies broadly declare who may send for them, but most do not tell receiving servers to act when a message fails that check, which is the step that stops impersonation (Figure 2).

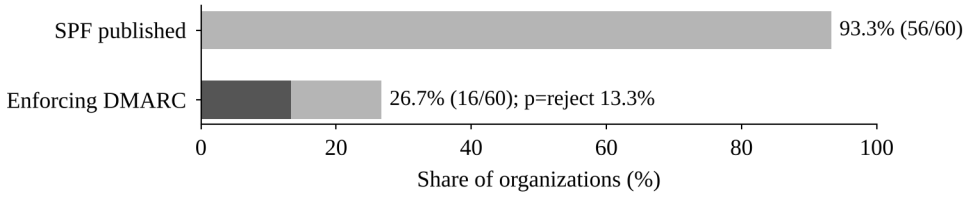


Figure 2: Declaring Versus Enforcing. SPF published (56/60) against any enforcing DMARC policy (16/60); the darker segment is p=reject (8/60).

4. Discussion

4.1. Comparison With the Veterinary Study

The companion veterinary study found 83.1% of practices spoofable.[4] Insurance agencies here are lower at 73.3%, with overlapping intervals, so the two sectors are not clearly distinguishable. Both show a clear majority of businesses exposed to impersonation.

4.2. Implications for Practice

Publishing an enforcing DMARC policy is a single DNS change, available in Microsoft 365 and Google Workspace without new software, after a short monitoring period at p=none to confirm that legitimate mail aligns. The measurement reported here is the same one any client, or any attacker, can read from outside the agency.

5. Limitations

The frames are search-compiled convenience samples, so results are directional rather than definitive, and the frame comparison is underpowered at this sample size; the publishable result is the aggregate level. Published DNS is a proxy for deployed behavior. DKIM is outside passive scope. Two domains were excluded for having no MX record. Per-frame companion measures are included in the released data.

6. Conclusion

Nearly three in four of the independent insurance agencies measured publish no enforcing DMARC policy, while more than nine in ten publish SPF. The gap between declaring authorized senders and instructing receivers to act on failures is the measurable exposure, and it closes with one DNS change.

References

1. Kucherawy, M. and Zwicky, E. (2015). Domain-based Message Authentication, Reporting, and Conformance (DMARC). RFC 7489. Internet Engineering Task Force.

2. Kitterman, S. (2014). Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. RFC 7208. Internet Engineering Task Force.

3. Arends, R. et al. (2005). DNS Security Introduction and Requirements. RFC 4033, with RFC 4034 and RFC 4035. Internet Engineering Task Force.

4. Bridgham Technology Institute. (2026). Email Spoofability Across Veterinary Practices. Vigil Library.

Disclaimer

This report is published by Bridgham Cyber, LLC for informational and analytical purposes only. It does not constitute investment advice, legal counsel, or a solicitation of any kind. The measurement is passive and uses public DNS only; no mail was sent and no organization was contacted. Results are reported in aggregate, and no per-agency result is published. The method and aggregate data are open. Reproduction or redistribution of this report, in whole or in part, requires attribution to Bridgham Cyber, LLC. For questions regarding methodology or data, contact headofresearch@bridghamcyber.com.