BRIDGHAM TECHNOLOGY INSTITUTE
BTI WORKING PAPER 320-26

Email Spoofability Across Insurance Agencies: A Passive Measurement of DMARC Enforcement in 60 US Independent Insurance Agencies

Bridgham Technology Institute

This work is made available under the rights statement In Copyright - Educational Use Permitted
https://rightsstatements.org/page/InC-EDU/1.0/
Raleigh, NC: Bridgham Technology Institute, November 2026.

Electronic copy available at: https://bridghaminstitute.com/research/working-papers/320-26

Email Spoofability Across Insurance Agencies: A Passive Measurement of DMARC Enforcement in 60 US Independent Insurance Agencies

Bridgham Technology Institute*

November 2026

Abstract: Clients of an insurance agency act on email that appears to come from the agency, and the agency's published DMARC policy determines whether a receiving mail server is told to refuse a message that falsely claims the agency's domain. We measure the published email-authentication records of 60 US independent insurance agencies in three samples, using only public DNS and contacting no one. Of the 60 agencies, 44 (73.3%, 95% Wilson interval [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 for each sample with its 95% interval, alongside SPF publication (93.3%) and DNSSEC signing (5.0%). An expectation stated in advance, that affiliated agencies would be better protected, did not hold: the three samples are not distinguishable at this sample size. For an agency without an enforcing policy, these results suggest that the corrective step is a single DNS policy change.

Keywords: DMARC, SPF, DNSSEC, email spoofing, insurance agencies, passive measurement

* Bridgham Technology Institute is a division of Bridgham Cyber, LLC, Raleigh, NC. Contact: headofresearch@bridghamcyber.com.

1. Introduction

Insurance agencies hold client personal information and carry errors-and-omissions exposure, and they 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 that publishes an enforcing DMARC policy allows mailbox providers to reject mail that fails authentication. An agency that publishes no enforcing policy leaves impersonating mail able to pass. Each policy is published in the public Domain Name System (DNS), where any receiving server can read it. A single record does not show how common enforcement is across agencies as a group.

In this paper, we measure the share of independent insurance agencies that publish no enforcing DMARC policy. We compile three sampling frames by public search: agencies that present Trusted Choice or Big "I" affiliation, general independent agencies, and independent agencies in North Carolina. For each of the 60 agencies measured, we read the DMARC record from public DNS. We also read the Sender Policy Framework (SPF) record, which declares who may send for a domain,[2] and we record whether the domain is signed with DNSSEC.[3] No mail was sent and no agency was contacted.

We document three main findings. First, 44 of the 60 agencies (73.3%, 95% confidence interval (CI) [61.0, 82.9]) publish no enforcing DMARC policy. Second, declaring senders is far more common than enforcing. SPF is published by 56 of the 60 agencies (93.3%), an enforcing DMARC policy by 16 (26.7%), and the strictest policy, p=reject, by 8 (13.3%). Third, the three frames are not distinguishable. We expected in advance that affiliated agencies would show a lower spoofable share, but the affiliated frame is higher (78.8%) than the general frame (64.3%) and the North Carolina frame (69.2%), and all pairwise intervals overlap. The aggregate level is also close to the 83.1% that a companion paper reports for veterinary practices, with overlapping intervals.[4]

These findings are directional. The three frames are convenience samples compiled by search, the comparison between them is underpowered at this sample size, and published DNS is a proxy for how mail is handled.

The paper proceeds as follows. Section 2 describes the measurement, the definitions and the three sampling frames. Section 3 presents the results. Section 4 compares the result with the veterinary paper and discusses what it means for an agency. Section 5 states the limitations, and Section 6 concludes.

2. Method

2.1. Measurement

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

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. Each share carries a 95% Wilson score interval. We use no significance test and no model.

2.3. Sampling Frames

All three frames are public and search-compiled. Frame A holds agencies that present 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 the mail domain of one independently operated agency. We excluded carriers, managing general agents, wholesalers, and rollup and aggregator domains. Of the 62 agencies supplied, we measured 60. Two had no MX record, which means they were not mail-active, and they are counted in no denominator.

2.4. Independent Reproduction

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

3. Results

3.1. Aggregate Level

Table 1 reports the spoofable share by frame, and Figure 1 shows each share with its interval. 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 an enforcing policy of either kind (quarantine or reject) at 16 of 60 (26.7%). SPF is published at 56 of 60 (93.3%), and DNSSEC is

signed at 3 of 60 (5.0%).

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.

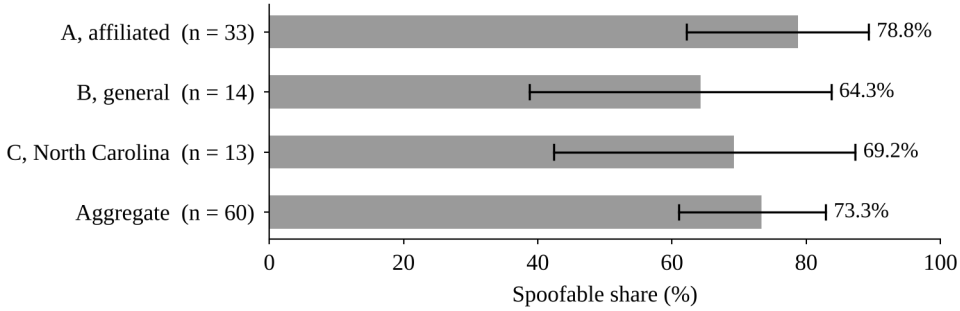


Figure 1: Spoofable Share by Frame and in Aggregate. Bars are point estimates; whiskers are 95% Wilson intervals. Every pairwise interval overlaps.

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%). 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 an 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).

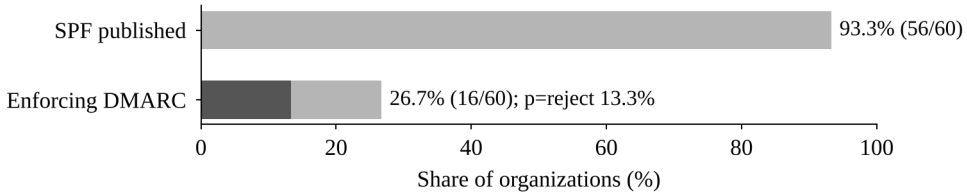


Figure 2: Declaring Versus Enforcing. SPF published (56/60) against any enforcing DMARC policy (16/60); the darker segment is p=reject (8/60).

4. Discussion

4.1. Comparison With the Veterinary Study

The companion paper on veterinary practices reports that 83.1% of practices are spoofable.[4] Insurance agencies are lower at 73.3%, with overlapping intervals, so the two sectors are not clearly distinguishable. Both show a clear majority of firms 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 that any client, or any attacker, can read from outside the agency.

5. Limitations

Our analysis has five limitations. First, the frames are search-compiled convenience samples, so the results are directional and not definitive. Second, the frame comparison is underpowered at this sample size, and the publishable result is the aggregate level. Third, published DNS is a proxy for deployed behavior. Fourth, we do not measure DKIM, which is outside the scope of a passive measurement. Fifth, two domains were excluded for having no MX record. Per-frame companion measures are included in the released data.

6. Conclusion

Clients of an insurance agency act on email that appears to come from the agency, and a published DMARC policy is the control that tells receiving servers whether to refuse a message that falsely claims the agency’s domain. 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.

The three samples are convenience samples, and they are not distinguishable from one another at this sample size, so the result is the overall level. For an agency without an enforcing policy, the results suggest that the exposure may be closed 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. https://www.rfc-editor.org/rfc/rfc7489

2. Kitterman, S. (2014). Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. RFC 7208. Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc7208

3. Arends, R. et al. (2005). DNS Security Introduction and Requirements. RFC 4033, with RFC 4034 and RFC 4035. Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc4033

4. Bridgham Technology Institute. (2026). Email Spoofability Across Veterinary Practices. BTI Working Paper 319-26. https://bridghaminstitute.com/research/working-papers/319-26

Disclaimer

This report is published by Bridgham Technology Institute 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 Technology Institute. For questions regarding methodology or data, contact headofresearch@bridghamcyber.com.