BRIDGHAM TECHNOLOGY INSTITUTE
BTI WORKING PAPER 319-26

Email Spoofability Across Veterinary Practices: A Passive Measurement of DMARC Enforcement in 124 US Veterinary Practices

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/319-26

Email Spoofability Across Veterinary Practices: A Passive Measurement of DMARC Enforcement in 124 US Veterinary Practices

Bridgham Technology Institute*

November 2026

Abstract: Clients of a veterinary practice act on email that appears to come from the practice, and an enforcing policy under the Domain-based Message Authentication, Reporting, and Conformance standard (DMARC) is the control that tells a receiving mail server to act on a message that falsely claims the practice's domain. We measure the published DMARC records of 124 United States small-animal veterinary practices in three separately compiled samples, using only passively observable public DNS records and contacting no practice's systems. In every sample, a strong majority of practices publish no enforcing DMARC policy: the spoofable share ranges from 76.1% among accredited practices to 88.6% among North Carolina general practices. The strongest policy, p=reject, is published by fewer than one practice in thirteen in every sample, and DNSSEC is signed by one domain of the 124. The accredited sample shows a lower spoofable share than the two general-practice samples, but all pairwise confidence intervals overlap, so the samples are not statistically distinguishable at this sample size and we make no causal claim. All three are convenience samples compiled from public listings and not from official membership rosters, so the findings are directional: they describe the practices observed and are not a definitive population estimate. Because the observed mail provider mix is dominated by Microsoft 365 and Google Workspace, the results suggest that the distance between current posture and protected posture is, in most cases, a console configuration change and not an infrastructure project.

Keywords: DMARC, SPF, DNSSEC, email spoofing, veterinary practices, passive measurement

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

1. Introduction

Clients of a veterinary practice open its email, follow its appointment reminders and pay its invoices because they believe that the message in front of them came from the practice. Email sender authentication is the set of public, standardized controls that lets a receiving mail server check that belief mechanically, before a person sees the message. When those controls are absent or unenforced, a domain can be impersonated: a message that did not originate with the practice can still arrive in a client's inbox appearing to come from it.

Three standards govern sender authentication. The Sender Policy Framework (SPF) publishes which servers may send mail for a domain.[1] DomainKeys Identified Mail (DKIM) attaches a verifiable signature to outgoing mail.[2] Domain-based Message Authentication, Reporting, and Conformance (DMARC) ties the two together and publishes a policy that instructs receivers what to do when a message fails authentication: take no action (p=none), set it aside (p=quarantine) or refuse it (p=reject).[3] Only the last two policies are enforcing. A domain with no DMARC record, with a policy of p=none, or with a record that a receiver cannot parse gives receivers no instruction to act, and it is therefore spoofable in the operational sense used throughout this paper.

Each of these records is public, but a single record does not show how common enforcement is across a field. In this paper, we measure the share of United States small-animal veterinary practices that publish an enforcing DMARC policy, and we examine how that share reads across three ways of selecting the practices. We compile three sample frames from public business listings: 46 practices that present as accredited, 43 general practices across multiple metropolitan areas, and 35 general practices in North Carolina, for 124 practices in all. We read each practice's published records from public DNS alone, report the level first, and treat differences between the frames as descriptive and not causal.

We document three main findings. First, most practices in every frame are spoofable. Pooled across the three frames, 103 of the 124 practices (83.1%, 95% confidence interval (CI) [75.5, 88.6]) publish no enforcing DMARC policy, and the share by frame runs from 76.1% to 88.6%. Second, strict enforcement and DNS signing are rare. Fewer than one practice in thirteen, in every frame, publishes p=reject, and one domain of the 124 is signed with DNSSEC, a separate control that protects DNS records themselves.[4] Third, the accredited frame shows a lower spoofable share (76.1%) than the two general-practice frames (86.0% and 88.6%), as we predicted before any aggregation was computed, but every pairwise interval overlaps and the frames are not distinguishable at this sample size.

These findings are directional. All three frames are convenience samples compiled by public search, not draws from official accreditation or licensure rosters, so the shares describe the practices observed and are not a population estimate. The measurement reads published records and does not observe how mail is handled.

The paper proceeds as follows. The remainder of this section describes the four controls and explains why they can be measured from outside an organization. Section 2 describes the frames, the measurement and the definitions. Section 3 presents the results. Section 4 discusses what the results mean for a practice and outlines future work. Section 5 states the limitations, and Section 6 concludes.

1.1. The Controls

SPF is a DNS TXT record that lists the hosts authorized to send mail for a domain.[1] It authenticates the envelope sender path but does not, on its own, protect the visible From address.

DKIM signs selected message headers with a private key, and receivers verify the signature against a public key published in DNS.[2] DKIM survives forwarding better than SPF does, but it does not by itself bind the visible From address.

DMARC closes this gap.[3] It requires that an authenticated identifier align with the visible From domain, and it publishes a policy that tells receivers how to treat mail that fails. DMARC therefore determines whether a domain can be impersonated to its recipients, which is why it is the primary measure in this paper.

DNSSEC is a separate control. It cryptographically signs DNS records themselves, and so it protects the integrity of the lookups on which the other three controls depend.[4] We measure it as a supporting indicator of overall DNS hygiene.

1.2. Measurability From Outside the Organization

These controls are, by design, published in public DNS so that any receiver in the world can read them. A practice's authentication posture is therefore an attribute that an outsider can assess without authorization, without sending mail, and without touching the practice's systems. A passive reader sees exactly what a receiving mail server sees. This paper measures only that public surface.

2. Method

2.1. Sampling and Frames

We compiled three independent sample frames, each intended to read the same underlying question from a different angle. Frame A is the accredited, multi-metro frame. It holds practices that present as accredited by the American Animal Hospital Association, across multiple metropolitan areas, and it is the conservative frame: the "even among the accredited" reading. Frame B is the general-practice, multi-metro frame. It holds general-practice veterinary clinics across multiple metropolitan areas, with no accreditation screen, and it is intended as the reading of the broader field. Frame C is the North Carolina general-practice frame. It holds general practices across four

North Carolina metropolitan areas and is the single-state reading. Frame C is a convenience sample, and a defined-population frame built from the member directory of the state veterinary medical association is left to future work.

We compiled each frame from public business listings, and for each practice we recorded only the practice's own primary domain. We excluded corporate veterinary chains and third-party aggregator domains, so that each observation corresponds to the mail domain of an independently operated practice. The three frames share no domain, which we verified programmatically. The realized sizes are 46, 43 and 35 practices, for a total of 124. We padded no frame to a target size, and each count is reported as realized.

These frames are convenience samples compiled by public search, not draws from official accreditation or licensure rosters. This is the central sampling limitation, and Section 5 returns to it. The frame labels describe how the practices were found, not a verified population, and the results are directional and not definitive.

2.2. Measurement

For each domain we queried public DNS through public resolvers and assessed four records: DMARC (presence, policy and parseability at the standard _dmarc location), SPF (presence of a published policy), DNSSEC (a DNSKEY record at the apex) and MX (as mail-active context). The DMARC and SPF assessments use established, RFC-conformant parsers without modification. The DNSSEC assessment is the one new probe.

2.3. Operational Definitions

A domain is *spoofable* if it publishes no enforcing DMARC policy: the record is absent, its policy is p=none, or the record cannot be parsed. A domain is *protected* if it publishes an enforcing policy (p=quarantine or p=reject), and *strictly protected* if it publishes p=reject. The enforcing share is the complement of the spoofable share by construction.

2.4. Statistical Treatment

We report each share with N equal to the number of domains conclusively assessed for that measure, and with a 95% Wilson score interval. The Wilson interval gives more reliable coverage than the normal approximation at these sample sizes and near the boundaries of the proportion scale. We perform no significance test and fit no model. The paper reports observed shares and their intervals.

2.5. Coverage and Scope

All 124 sampled domains resolved and were assessed for the primary DMARC measure, so coverage is 100% in every frame. We record SPF and DNSSEC as a tri-state: present, absent or indeterminate. A record that cannot be read conclusively is marked indeterminate and excluded from

its denominator, never silently counted as absent, which is why the SPF denominators are 45, 41 and 35 and not 46, 43 and 35. The primary spoofable measure is unaffected, because DMARC, MX and DNSSEC records are small and resolve without truncation. An unknown value is reported as not assessed, never as a pass and never as an inferred value.

The measurement reads published public DNS records only, through public resolvers, with throttled and resumable queries. We sent no mail, probed no DKIM selectors and enumerated no subdomains. The assessment is passive and makes no contact with any practice's systems.

2.6. Pre-Registration

We committed the operational definitions, the per-frame cuts and the cross-frame comparison plan in a pre-registration before any aggregation was computed. The pre-registration includes a single directional hypothesis: that the accredited frame would show a lower spoofable share. Because the hypothesis was committed in advance, the comparison in Section 3.4 can be read as a stated prediction and not as a result selected after the fact.

3. Results

3.1. Overall Level

Most practices in all three frames are spoofable, and very few reach an enforcing policy. This result holds however the frame was compiled. Between roughly three-quarters and seven-eighths of the practices in each frame publish no enforcing DMARC policy, and 103 of the 124 practices pooled across frames (83.1%, 95% CI [75.5, 88.6]) are spoofable. Fewer than one practice in thirteen, in every frame, reaches the strongest policy, p=reject. DNSSEC is effectively absent across the whole sample: exactly one of the 124 domains is signed.

3.2. Per-Frame Results

Table 1 reports every measure by frame, and Figure 1 shows the spoofable share with its interval.

Frame	N	Spoofable	95% Wilson	p=reject	SPF	DNSSEC
A, accredited	46	76.1% (35/46)	62.1 to 86.1	4.3% (2/46)	84.4% (38/45)	0% (0/46)
B, general practice	43	86.0% (37/43)	72.7 to 93.4	7.0% (3/43)	70.7% (29/41)	2.3% (1/43)
C, North Carolina	35	88.6% (31/35)	74.1 to 95.5	5.7% (2/35)	77.1% (27/35)	0% (0/35)

Table 1: DMARC, SPF, and DNSSEC Posture by Sampling Frame. Frames A and B are multi-metro; Frame C is North Carolina general practice. The interval is the 95% Wilson score interval for the spoofable share.

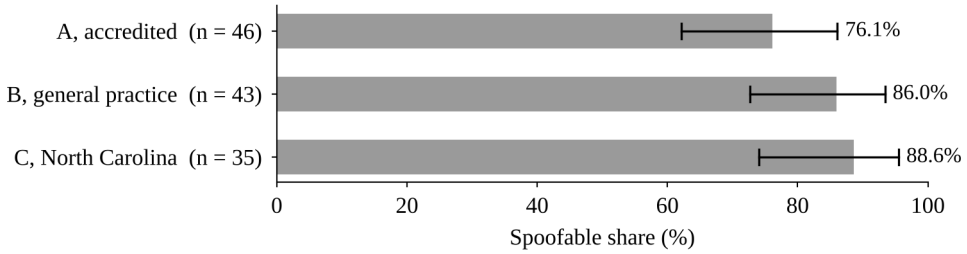


Figure 1: Spoofable Share by Frame. Bars are point estimates; whiskers are 95% Wilson intervals (A 62.1 to 86.1, B 72.7 to 93.4, C 74.1 to 95.5). The intervals overlap.

The enforcing share is the complement of the spoofable share: 23.9% in Frame A, 14.0% in Frame B and 11.4% in Frame C. Only a fraction of that already small enforcing share reaches p=reject, and the remainder rests at p=quarantine (Figure 2).

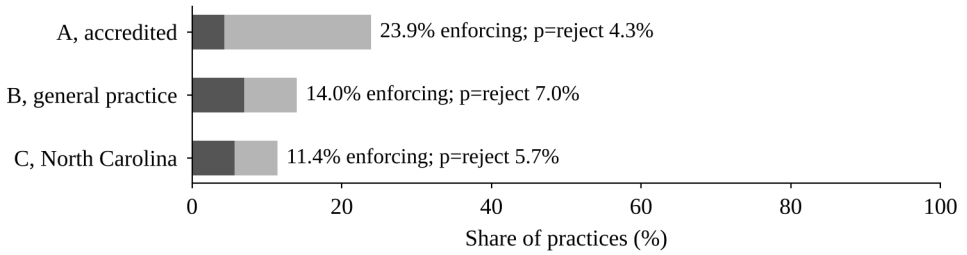


Figure 2: Enforcing DMARC Share by Frame. The full bar is the enforcing share (p=quarantine or p=reject); the darker segment is p=reject.

3.3. Supporting Controls and Provider Mix

SPF is published more often than DMARC is enforced, at between roughly 71% and 84% across the frames. This pattern is consistent with SPF being the older and more widely deployed control. SPF alone does not protect the visible From address, however, so a high SPF share does not change the spoofability that DMARC governs.

DNSSEC gives the clearest single result in the paper: one signed domain of 124, in the general-practice multi-metro frame. For practical purposes, DNS-layer integrity protection is not in use in this field (Figure 3).

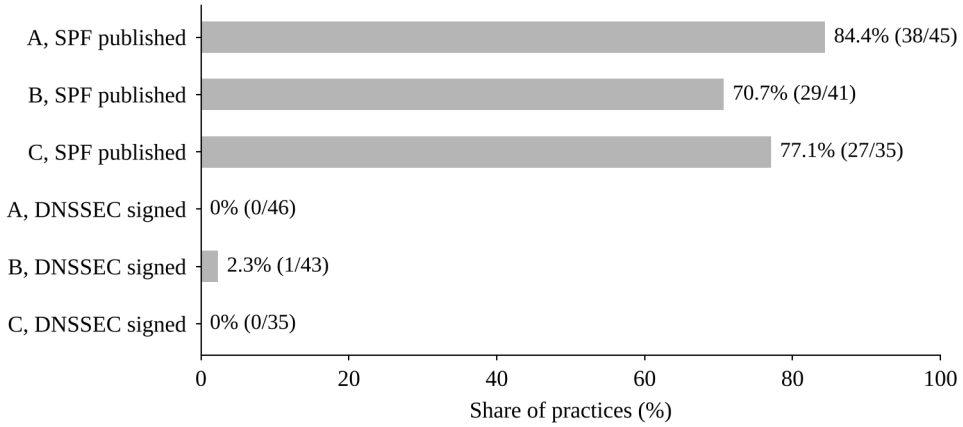


Figure 3: Supporting Controls by Frame. SPF published against DNSSEC signed (0 of 46, 1 of 43, and 0 of 35).

The observed mail provider mix is dominated by Microsoft 365 and Google Workspace. Per-provider counts were not part of the canonical run, and we do not estimate them here. The mix matters for interpretation. For a practice on one of these platforms, moving from no enforcing policy to an enforcing DMARC policy is a configuration change made in an administrative console, not a migration or an infrastructure build. The gap that this paper measures is, for most of the practices in it, small and reversible.

3.4. Cross-Frame Comparison

The accredited frame (A) shows a lower spoofable share than both general-practice frames: 76.1% against 86.0% and 88.6%. This direction matches the single pre-registered hypothesis. Every pairwise Wilson interval overlaps, however, so the frames are not distinguishable at this sample size. We report overlapping intervals as not distinguishable, and we do not take them as evidence of no difference.

Three frames are not a controlled experiment. The frames differ on more than one dimension at once (accreditation status, metropolitan mix, and single-state versus multi-metro composition), so any contrast between them is descriptive and cannot be attributed to a single cause. In particular, this paper does not show, and is not designed to show, that accreditation makes a practice safer. It shows that the level of exposure is consistently high across three ways of selecting practices.

4. Discussion

4.1. Common and Inexpensive to Correct

The exposure is both common and, in most cases, inexpensive to correct. A strong majority of practices in every frame can have mail sent in their name to their own clients, and the reason is almost never a hard technical constraint. These practices have not published an enforcing DMARC policy, on platforms where publishing one is a console setting. Nothing in the measurement is specific to veterinary medicine, and the same unenforced default may hold in other professional practices on the same platforms, which this paper does not measure. The default is consequential because email is the channel through which these practices are trusted.

4.2. SPF Is Not Sufficient

The primary measure matters more than its individual components for the same reason. SPF adoption is reasonably high, which may give a false sense of completion, but SPF does not govern the address that a client sees. DMARC does, and DMARC enforcement is where the field is thin. A practice can publish SPF and still be fully spoofable in the sense that matters to its clients.

4.3. Reading the Frame Comparison

The comparison between frames supports only a tentative reading. Accredited practices looked somewhat better, which is consistent with the idea that accreditation correlates with operational maturity, but the data do not separate the frames cleanly and the comparison confounds several variables. Exposure is high in every frame, and the differences between frames are a direction that warrants more data, not a conclusion.

4.4. Future Work

Three further studies follow from these results. A roster-verified frame would convert the directional accreditation contrast into a clean one. Larger samples per frame would narrow the intervals. A repeated measurement of the same domains over time would show whether enforcement adoption is moving. Beyond these three, a consented, longitudinal cohort would allow the published-posture proxy to be checked against deployed behavior directly.

5. Limitations

Our analysis has six limitations. First, the frames are convenience samples and not rosters. All three were compiled from public business listings and not from official accreditation or licensure rosters. The frame labels therefore describe how practices were found, not a verified population, and the shares are directional and not definitive population estimates. Roster-verified frames are the most valuable improvement for future work. Second, a published record is not deployed behavior. We

read what a domain publishes. A published enforcing policy is strong evidence of protection, and a missing one is strong evidence of exposure, but DNS posture is a proxy for how mail is handled and not a direct observation of it.

Third, a small number of SPF records could not be read in the observation environment. We excluded them and did not guess, which slightly reduces the SPF denominators. The primary DMARC measure is unaffected. Fourth, we do not assess DKIM. DKIM selector discovery requires either sending mail or guessing selector names, and both fall outside the passive, no-contact scope of this paper. Fifth, the samples are small. With 35 to 46 practices per frame, the intervals are wide and differences between frames cannot be resolved. The overall level does not depend on this limitation; the comparison does. Sixth, the result covers a single field in a single country. It describes United States small-animal veterinary practices and should not be generalized to other professions or jurisdictions without measurement.

6. Conclusion

Clients of a veterinary practice rely on email that appears to come from the practice, and an enforcing DMARC policy is the published control that tells receiving servers to act on a message that falsely claims the practice’s domain. Across three separately compiled samples of United States small-animal veterinary practices, a strong majority publish no enforcing DMARC policy and can therefore be impersonated by email to their own clients. Enforcing policy is uncommon and the strongest policy is rare, and DNS-layer integrity protection is, for practical purposes, absent.

The differences between the samples are consistent in direction but not distinguishable at this sample size, and we make no causal claim for them. All three are convenience samples, so the level describes the practices observed. Given the observed provider mix, the results suggest that the exposure is, in most cases, a console configuration change away from being closed.

References

1. 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

2. Crocker, D., Hansen, T. and Kucherawy, M. (2011). DomainKeys Identified Mail (DKIM) Signatures. RFC 6376. Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc6376

3. 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

4. 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

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-practice 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.