Email Spoofability Across Veterinary Practices

A Passive Measurement of DMARC Enforcement in 124 US Veterinary Practices

Bridgham Technology Institute

June 2026

Abstract

Email sender authentication lets a receiving mail server decide whether a message that claims to come from a domain is legitimate. The Domain-based Message Authentication, Reporting, and Conformance standard (DMARC) is the control that tells receivers what to do with mail that fails authentication, and an enforcing DMARC policy is what prevents an outsider from sending mail that appears to come from a practice to that practice's own clients. We measured the published DMARC posture of 124 United States small-animal veterinary practices across three independently drawn sample frames, using only passively observable public DNS records and contacting no practice's systems.

Across every frame, a strong majority of practices publish no enforcing DMARC policy. The spoofable share ranged from 76.1 percent among accredited practices to 88.6 percent among North Carolina general practices. The strongest policy, p=reject, was rare everywhere, reached by fewer than one practice in thirteen in every frame. DNSSEC was effectively absent, signed by one domain of the 124. The accredited frame was directionally less spoofable than the two general-practice frames, but all pairwise confidence intervals overlapped, so the frames are not statistically distinguishable at this sample size and no causal claim is made. Because the observed mail provider mix is dominated by Microsoft 365 and Google Workspace, the distance between current posture and protected posture is, in most cases, a console configuration change rather than an infrastructure project.

The study is directional. All three frames are convenience samples compiled from public listings rather than official membership rosters, so the findings describe the practices observed and are not a definitive population estimate.

1. Introduction

A small professional practice runs on trust. Its clients open its email, click its appointment reminders, and pay its invoices because they believe 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 ever 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 this. The Sender Policy Framework (SPF) publishes which servers may send mail for a domain. DomainKeys Identified Mail (DKIM) attaches a verifiable signature to outgoing

mail. DMARC ties the two together and publishes a policy instructing receivers what to do when a message fails authentication: take no action (p=none), set it aside (p=quarantine), or refuse it (p=reject). Only the latter two are enforcing. A domain with no DMARC record, with a policy of p=none, or with a record a receiver cannot parse gives receivers no instruction to act, and is therefore spoofable in the operational sense used throughout this paper.

Adoption of these controls is uneven, and the practices most exposed are often the smallest, because configuration is a task that competes with running the business. This study asks a narrow, answerable question about one such field: among United States small-animal veterinary practices, what share publish an enforcing DMARC policy, and how does that share read across different ways of selecting the practices? We answer it from public DNS alone, report the level first, and treat differences between frames as descriptive rather than causal.

1.1. The Controls

SPF is a DNS TXT record listing the hosts authorized to send mail for a domain.[2] 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; receivers verify the signature against a public key published in DNS.[3] DKIM survives forwarding better than SPF but does not by itself bind the visible From address.

DMARC closes the gap.[1] 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 is therefore the control that determines whether a domain can be impersonated to its recipients, which is why it is the primary measure in this study.

DNSSEC is a separate control that cryptographically signs DNS records themselves, protecting the integrity of the lookups on which all of the above depend.[4] We measure it as a supporting indicator of overall DNS hygiene.

1.2. Measurability From Outside the Organization

Every one of these controls is, by design, published in public DNS so that any receiver in the world can read it. That is what makes a practice's authentication posture an attribute 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 drew three independent sample frames, each intended to read the same underlying question from a different angle:

- Frame A, accredited, multi-metro. Practices presenting as accredited by the American Animal Hospital Association, across multiple metropolitan areas. This is the conservative frame: the "even among the accredited" read.
- Frame B, general practice, multi-metro. General-practice veterinary clinics across multiple metropolitan areas, with no accreditation screen. This is the representative read of the broader field.
- Frame C, North Carolina general practice. General practices across four North Carolina metropolitan areas. This is the single-state read; it is a convenience sample, and a defined-population frame drawn from the state veterinary medical association's member directory is left to future work.

Each frame was compiled from public business listings. For each practice we recorded only the practice's own primary domain. Corporate veterinary chains and third-party aggregator domains were excluded so that each observation corresponds to an independently operated practice's own mail domain. The three frames share no domain in common; this was verified programmatically. The realized sizes were 46, 43, and 35 practices respectively, for a total of 124. No frame was padded to a target size; the realized count is reported as drawn.

These are convenience samples compiled by public search, not draws from official accreditation or licensure rosters. This is the central sampling limitation and is revisited in Section 5. It means the frame labels describe how the practices were found, not a verified population, and the results are directional rather than definitive.

2.2. Measurement

For each domain we queried public DNS through public resolvers and assessed 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 (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

Shares are reported with N equal to the number of domains conclusively assessed for that measure. Each share is accompanied by a 95 percent Wilson score interval, which gives more reliable coverage than the normal approximation at these sample sizes and near the boundaries of the proportion scale. No significance test is performed and no model is fitted; the study reports observed shares and their intervals.

2.5. Coverage and Scope

All 124 sampled domains resolved and were assessed for the primary DMARC measure, for 100 percent coverage in every frame. SPF and DNSSEC are recorded 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; this is why the SPF denominators are 45, 41, and 35 rather than 46, 43, and 35. The primary spoofable measure is unaffected, because DMARC, MX, and DNSSEC records are small and resolve without truncation. Where a value is unknown it is reported as not assessed, never as a pass and never as an inferred value.

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

2.6. Pre-Registration

The operational definitions, the per-frame cuts, and the cross-frame comparison plan were committed in a pre-registration before any aggregation was computed, including the single directional hypothesis that the accredited frame would show a lower spoofable share. Committing this in advance is what allows the comparison in Section 3.4 to be read as a stated prediction rather than a result selected after the fact.

3. Results

3.1. Overall Level

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

3.2. Per-Frame Results

Table 1 gives 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.

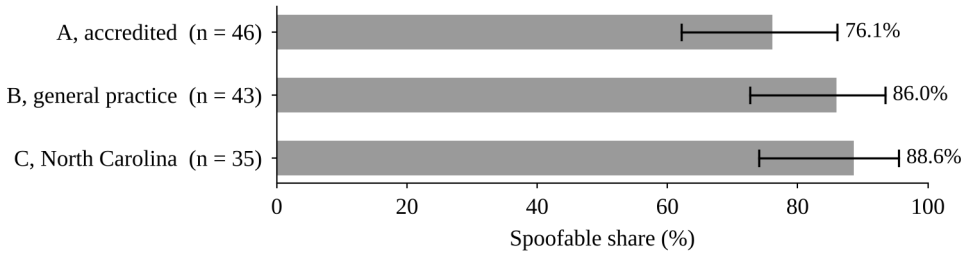


Figure 1: Spoofable Share by Frame. Bars are point estimates; whiskers are 95% Wilson intervals (A 62.1 to 86.1, B 72.7 to 93.4, C 74.1 to 95.5). The intervals overlap.

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

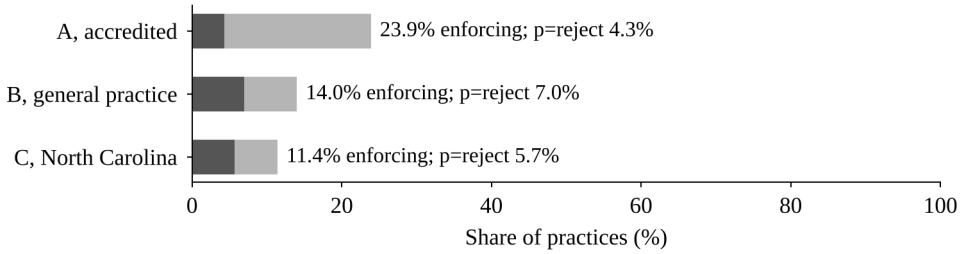


Figure 2: Enforcing DMARC Share by Frame. The full bar is the enforcing share (p=quarantine or p=reject); the darker segment is p=reject.

3.3. Supporting Controls and Provider Mix

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

DNSSEC is the clearest single result in the study: 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).

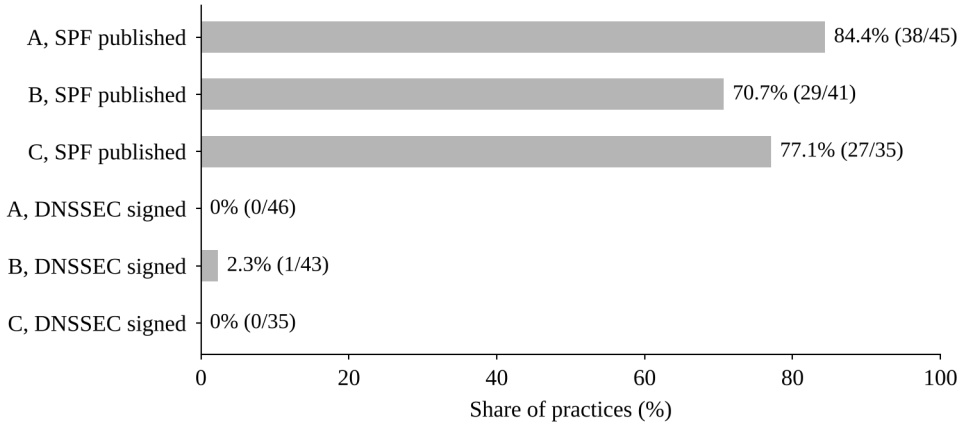


Figure 3: Supporting Controls by Frame. SPF published against DNSSEC signed (0 of 46, 1 of 43, and 0 of 35).

The observed mail provider mix is dominated by Microsoft 365 and Google Workspace. Per-provider counts were not part of the canonical run and are not estimated 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 this study measures is, for most practices in it, small and reversible.

3.4. Cross-Frame Comparison

The accredited frame (A) is directionally lower on spoofability than both general-practice frames, 76.1 percent against 86.0 and 88.6 percent. This matches the single pre-registered directional hypothesis. However, every pairwise Wilson interval overlaps, so the frames are not distinguishable at this sample size. Overlapping intervals are reported here as not distinguishable, and are not taken as evidence of no difference.

Three different 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 any single cause. In particular, this study does not show, and is not designed to show, that accreditation makes a practice safer. It shows that across three different ways of selecting practices, the level of exposure is consistently high.

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. An enforcing DMARC policy has not been published, on platforms where publishing one is a console setting. The pattern does not single out veterinary practices; an entire category of small professional businesses sits at the unenforced default, and the default is consequential because email is the channel through which these practices are trusted.

4.2. SPF Is Not Sufficient

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

4.3. Reading the Frame Comparison

The cross-frame reading should be held lightly. Accredited practices looked somewhat better, which is intuitive and 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 everywhere, and the differences between frames are a direction that warrants more data rather than a conclusion.

4.4. Future Work

The natural next studies are a roster-verified frame to convert the directional accreditation contrast into a clean one, larger per-frame samples to narrow the intervals, and a repeated measurement of the same domains over time to observe whether enforcement adoption is moving. A consented, longitudinal cohort would allow the published-posture proxy to be checked against deployed behavior directly.

5. Limitations

Convenience samples, not rosters. All three frames were compiled from public business listings rather than official accreditation or licensure rosters. The frame labels therefore describe how practices were found, not a verified population, and the shares are directional rather than definitive population estimates. Roster-verified frames are the most valuable hardening for future work.

Published record is not deployed behavior. This study reads 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, and not a direct observation of, how mail is handled in every case.

SPF indeterminates. A small number of SPF records could not be read in the observation environment and were excluded rather than guessed, which slightly reduces the SPF denominators. The primary DMARC measure is unaffected.

DKIM not assessed. DKIM selector discovery requires either sending mail or guessing selector names, both of which fall outside this study's passive, no-contact scope. DKIM is therefore not part of the posture measured here.

Sample size. With 35 to 46 practices per frame, intervals are wide and cross-frame differences are not resolvable. The overall level is robust to this; the comparison is not.

Single field, single country. The result describes United States small-animal veterinary practices and should not be generalized to other professions or jurisdictions without measurement.

6. Conclusion

Across three independently drawn frames 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; DNS-layer integrity protection is, for practical purposes, absent. The exposure is consistent across frames and, given the observed provider mix, is in most cases a console configuration change away from being closed. The differences between frames are consistent in direction but not distinguishable at this sample size, and no causal claim is made for them. The level is the result.

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. Crocker, D., Hansen, T. and Kucherawy, M. (2011). DomainKeys Identified Mail (DKIM) Signatures. RFC 6376. Internet Engineering Task Force.

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

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-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 Cyber, LLC. For questions regarding methodology or data, contact headofresearch@bridghamcyber.com.