Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Email Authentication Posture of Iraqi Higher Education: A Passive DNS Census of University and College Domains

Rafid Ahmed Khalil

rafid@goldennetai.com

Golden Net https://orcid.org/0000-0002-9083-680X

Balqis Alamori

Golden Net https://orcid.org/0009-0006-5004-6770

Research Article

Keywords: email security, SPF, DKIM, DMARC, DNSSEC, spoofing, internet measurement, higher education, Global Cybersecurity Index, Iraq

Posted Date: November 2nd, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11563211/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare potential competing interests as follows: R. A. Khalil heads the Department of Cybersecurity Engineering Techniques at Al-Qabas Private College, one of the institutions in the measured population, and is also affiliated with Golden Net, which provided the computing infrastructure used in this study and whose own domain served as the measurement control. B. Alamori is affiliated with Golden Net. Golden Net offers email…

Abstract

Sender-authentication mechanisms for email (SPF, DKIM and DMARC) are the only widely deployed defence against exact-domain spoofing of institutional email and are named as baseline countermeasures in International Telecommunication Union (ITU) guidance, yet their deployment in the higher-education sectors of developing countries has not been measured at census scale. We present the first complete census of email-authentication posture for Iraqi higher education: all 103 federally recognised universities and colleges with a resolvable official domain (36 public, 67 private). Measurement was strictly passive: MX, SPF, DKIM (fixed selector dictionary), DMARC and DNSSEC records were retrieved through two independent public resolvers, every raw answer was stored and timestamped, and no packet was sent to any institutional host. The primary outcome is a binary spoofability criterion; a study-specific 0–9 posture score is a secondary summary. Of the 103 domains, 93 (90.3%) are spoofable, only 10 enforce a DMARC policy and only 2 reach the highest grade. The finding is robust: bounding all 15 excluded or unmeasured institutions gives 78.8–91.5%, and the verdict does not depend on DKIM discovery. Posture is strongly structured by mail-provider concentration rather than by the public/private distinction: 89.3% of institutions, including every public one, receive mail on a single provider, 91.3% of those tenants are spoofable, and one third publish SPF records that omit the provider — a systemic weakness that is equally a single remediation channel. DNSSEC is nominal (13 signed zones, none with a DS record). A documented incident shows the operational cost: an official message from a sampled institution, failing DMARC under a monitoring policy, was filtered as spam. We relate the findings to Iraq's Tier 4 standing in the ITU Global Cybersecurity Index 2024 (Technical Measures 9.6 of 20) and report the responsible-disclosure protocol under which per-institution results were delivered to the responsible ministry before publication, with a post-notification re-measurement planned as the longitudinal follow-up.

1. Introduction

Electronic mail remains the primary channel of formal communication between universities and the students, staff, ministries, suppliers and peer institutions they serve. The protocol that carries it, SMTP, provides no sender authentication: any host can present any address in the From field. Three DNS-published mechanisms retrofit authentication onto this substrate. The Sender Policy Framework (SPF) enumerates the hosts authorised to send on behalf of a domain [1]; DomainKeys Identified Mail (DKIM) binds a cryptographic signature to the message and publishes the verification key in DNS [2]; and Domain-based Message Authentication, Reporting and Conformance (DMARC) ties both to the visible From domain, instructs receivers what to do with messages that fail, and returns aggregate reports to the domain owner [3]. When a domain publishes no DMARC policy, or publishes a policy of none, a receiving system has no instruction to reject a forged message bearing that domain, and the domain is, in the terminology adopted throughout this paper, spoofable.

Large-scale measurements of these mechanisms exist for the global population of popular domains [4–11], and several national governments have mandated their deployment across the public sector [12, 13].

At the international level, ITU-T Recommendation X.1236 lists SPF and DKIM validation among the countermeasures against forged-header email attacks [26], and an ITU-D study-group report identifies SPF, DKIM and DMARC as practices for interrupting the transmission of spam and malware [27]. No measurement of their deployment exists for Iraq, and, to the best of our knowledge, none exists at census scale for the higher-education sector of any Arab state. The gap matters for two reasons. First, the ITU Global Cybersecurity Index (GCI) 2024 places Iraq in Tier 4 (Evolving, overall score 20–55) of five tiers [14]. Iraq's pillar scores, each out of 20, are 11.21 (Legal), 9.6 (Technical), 15.77 (Organizational), 8.38 (Capacity Development) and 8.11 (Cooperation), whose sum is 53.07 of 100 (the report publishes the tier and the pillar scores, not a single overall score; the sum is ours); among the Arab States, eight countries are in Tier 1 and only one ranks below Tier 4 [14]. The index records commitments and capacities, not deployed controls, so the actual state of a basic, well-understood technical control in the country's institutions is unknown. Second, in 2026 the Iraqi Ministry of Higher Education and Scientific Research (MoHESR) circulated cybersecurity guidance to all institutions that references the GCI and incident reporting through the National Cybersecurity Center, but does not mention email authentication [15]. A census provides the baseline against which any future sector policy can be evaluated.

This paper reports such a census. It is a complete enumeration rather than a sample: every federally recognised university and college with an official domain is included, subject to explicit and consistently applied exclusion rules. Measurement is passive DNS only. Each record is queried through two independent public resolvers, every raw answer is stored with a UTC timestamp, and no packet is sent to any institutional host. Results are reported in aggregate; no institution is named, and per-institution findings were delivered to MoHESR before publication.

Research questions. RQ1 (prevalence): what proportion of Iraqi higher-education domains publish SPF, DKIM and DMARC records, how are those records configured, and what proportion of domains is spoofable? RQ2 (structure): how does posture vary by institutional type (public versus private), by mail-service provider and by record quality?

Contributions. (i) The first census of email-authentication posture for Iraqi higher education, 103 domains, with a documented and reproducible roster construction. (ii) A passive, dual-resolver measurement instrument with a fixed DKIM selector dictionary, explicit permerror rules and a versioned re-scoring policy. (iii) A binary spoofability outcome, a study-specific 0–9 posture rubric as a secondary summary, and robustness analyses bounding the effect of unmeasured institutions, undiscovered DKIM keys and partial DMARC enforcement. (iv) A structural finding with direct policy consequences: sector posture is strongly structured by concentration on a single mail provider whose tenants do not complete configuration, so that the same concentration that spreads the weakness also offers a single channel for its remediation. (v) An explicit link between a deployed technical control and the Technical Measures pillar of the GCI, in which Iraq scores 9.6 of 20, together with a measurement design that can be reused for the higher-education sectors of other countries at a similar GCI tier. (vi) A responsible-disclosure design with pre-publication notification, a grace period and a scheduled re-measurement.

The remainder of the paper is organised as follows. Section 2 summarises the mechanisms, prior measurement work, the international normative framework and the governance of the .edu.iq name space. Section 3 describes the population, the instrument, the rubric and the validation. Section 4 reports results. Section 5 discusses structural explanations, policy implications and threats to validity. Section 6 concludes.

2. Background and Related Work

2.1 Sender Policy Framework

SPF [1] is a TXT record at the domain apex that lists the IP addresses, address ranges and referenced domains (include, a, mx mechanisms) permitted to use the domain in the SMTP envelope sender. The record ends with an all mechanism whose qualifier determines the disposition of non-matching sources: -all (fail), ~all (softfail), ?all (neutral) and + all (pass, which authorises every host). The specification limits a record to ten DNS-resolving mechanisms; a record that exceeds this limit, that is published more than once at the same name, or that contains a syntactically invalid term yields a permanent error (permerror) at the receiver, which is treated as the absence of a valid policy. SPF authenticates the envelope sender, not the From header, and therefore does not by itself prevent spoofing of the visible address.

2.2 DomainKeys Identified Mail

DKIM [2] signs selected headers and the body with a private key held by the sending system and publishes the public key at <selector>._domainkey.<domain>. The selector is chosen by the domain owner or provider and is not discoverable from the domain alone; measurement studies therefore probe a dictionary of common selectors and can only establish the presence of a key, never its absence. A TXT record at a selector name that contains no key material (for example a wildcard TXT record answering every name) is not a DKIM key.

2.3 Domain-based Message Authentication, Reporting and Conformance

DMARC [3] is a TXT record at _dmarc.<domain> that requires SPF or DKIM to pass and, in addition, to be aligned with the From-header domain. Its p tag requests a receiver disposition for failing messages: none (deliver and report), quarantine or reject. The pct tag (default 100) requests that the policy be applied to only that percentage of failing messages, with the remainder treated as if the policy were the next weaker one; a policy of reject with pct = 5 therefore requests rejection of 5% of failing messages and delivery of the rest. The rua tag names the address to which receivers send aggregate reports, which are the domain owner's only visibility into forgery attempts, since forged messages never traverse the impersonated domain's own infrastructure. As with SPF, multiple DMARC records at the same name constitute a permerror and no policy is applied [3, 16].

2.4 DNS Security Extensions

DNSSEC [17–19] signs the DNS records on which the three mechanisms depend. A zone that publishes DNSKEY records but has no DS record at its parent is signed but not validated: no resolver can construct a chain of trust to it, and the signatures provide no protection. Following Chung et al. [11], we distinguish zones with DNSKEY only (signed), zones with a DS record at the parent (validatable) and answers returned with the AD flag by a validating resolver (validated).

2.5 Threat model

We consider exact-domain spoofing: an attacker sends a message whose From header carries the institution's own domain to a third party. The mechanisms above, when correctly deployed and enforced, allow the receiving system to reject such a message. They do not address lookalike domains, display-name deception, compromised accounts or messages from the institution's own authorised infrastructure, and the paper makes no claim about those vectors. Spoofable, as used here, denotes the absence of a valid DMARC record or a policy of none; it is a statement about published DNS configuration, not about any observed attack or compromise.

2.6 Prior measurement studies

Durumeric et al. [4] and Foster et al. [5] measured the deployment of SPF, DKIM and DMARC across popular domains and mail providers in 2015 and found adoption concentrated among large providers, with enforcement rare. Hu and Wang [6] demonstrated end-to-end that major receivers deliver forged messages when senders publish no or weak policies. Tatang et al. [7] and Shen et al. [8] examined the interaction of the three mechanisms and the ambiguity of receiver behaviour. Liu et al. [9] characterised the concentration of mail service on a small number of providers and its consequences for authentication. Wang et al. [10] reported, for the Alexa top-million domains that publish MX records, SPF on 69.8%, DKIM discoverable on 37.0% and DMARC on 15.1%. The Lazy Gatekeepers study [20] examined SPF configuration across roughly 12 million domains and found SPF on 56.5% and DMARC on 13.6%, with widespread permissive records. Ashiq et al. measured DMARC reporting and its security implications [21] and the operational challenges of SPF management across 176 million domains [22]. Chung et al. [11] provided the longitudinal view of DNSSEC deployment that motivates our three-level DNSSEC classification. These studies characterise the global population of popular domains; sector-specific censuses of public institutions are rare, and none covers Iraq or the Arab region.

2.7 Governance context of the .iq name space

The .iq country-code top-level domain is administered by the Communications and Media Commission (CMC) following its redelegation in 2005 [23, 25]. Registration under .edu.iq is limited to institutions recognised by MoHESR, so the set of .edu.iq registrants coincides closely with the population studied here. Two government programmes provide the policy precedents for a sector-wide authentication baseline, and they represent two different models. The United States Binding Operational Directive 18 – 01, issued by the Department of Homeland Security on 16 October 2017, is a mandate: federal executive agencies were required to submit a plan of action within 30 days, to publish valid SPF and DMARC records with a policy of at least none and an aggregate-report address within 90 days, to add a central

DHS address as a recipient of every agency's DMARC aggregate reports, and to reach a DMARC policy of reject at pct = 100 within one year, with status reported to DHS every 30 days and progress verified by DHS scanning [12]. The directive required SPF and DMARC; it advised agencies to plan DKIM for mail-sending hosts but did not require it, since a reject policy can be met through SPF alignment alone [12]. The United Kingdom's model was a service rather than a mandate: from 2017 until its retirement on 31 March 2026 [24], the NCSC Mail Check service assessed the SPF, DKIM and DMARC records of participating public-sector organisations from public DNS, explained configuration errors, notified owners of changes and supported phased enforcement, alongside government guidance that sets out DKIM signing of outgoing mail and a DMARC rollout from none to quarantine or reject [13, 28]. Mail Check was extended to the education sector, where the number of academic organisations using it rose from 515 to 1,258 during 2022 [29]. No comparable instrument exists in Iraqi higher education; the 2026 MoHESR circular [15] references the GCI and incident reporting but is silent on email authentication.

2.8 International normative framework

Three ITU instruments frame the study. ITU-T Recommendation X.1236 (11/2023) specifies security requirements and countermeasures for targeted email attacks and is addressed in particular to IT security managers in countries beginning to engage actively in IT development; among its countermeasures for forged-header attacks it lists communication-protocol authentication that detects forged sender addresses by validating the message against SPF and DKIM [26, § 9.2.1]. The ITU-D Study Group 2 output report on Question 3/2 (2018–2021) recommends Sender Policy Framework, DomainKeys Identified Mail and DMARC, alongside real-time blocking lists, as policies through which service providers can break the chain of spam and malware transmission [27, § 1.3.1]. The GCI 2024 [14] measures national commitment across five pillars (Legal, Technical, Organizational, Capacity Development and Cooperation) and groups countries into five tiers, from Tier 1 (Role-modelling, 95–100) to Tier 5 (Building, 0–20). The present census does not measure any GCI indicator directly; it measures the deployment of controls that these instruments recommend, in the sector that the 2026 MoHESR circular addresses, and thereby supplies evidence on a component of national technical capacity that the index itself does not observe.

3. Methodology

3.1 Design

The study is a cross-sectional census of the Iraqi federal higher-education (HE) sector, with a planned longitudinal follow-up (Section 3.9). Measurement is passive: the instrument queries public DNS only and never contacts institutional hosts. All measurements were completed within a single session (26 September 2026) so that the snapshot is internally consistent.

3.2 Population and roster construction

Population. The roster was built from the official MoHESR list of recognised public and private universities and colleges (121 entries). Three exclusion rules were applied and are stated so that the population is reproducible. Rule A: institutions of the Kurdistan Region, which fall under a separate ministry, were excluded (2). Rule B: religiously affiliated institutions, defined as those owned by a religious endowment (waqf), a shrine authority or a religious foundation, or whose primary mission is religious instruction, were excluded (13), because their governance, funding and IT provisioning differ systematically from the federal system. Rule C: duplicate and renamed entries were merged (1). The resulting population comprises 105 institutions (36 public, 69 private). Official domains were established by the three-part rule of Section 3.3; 103 were accepted. Two private colleges could not be measured: one publishes a domain that does not exist in DNS (NXDOMAIN at both resolvers), and one has no discoverable official website. These are reported as a limitation, not excluded from the population.

Table 1
— Population and measured domains.

Group	Pop.	Meas.	Not	Note
Public universities and colleges	36	36	0	
Private universities and colleges	69	67	2	NXDOMAIN (1); no official site (1)
Total	105	103	2	after rules A, B, C from 121 entries

3.3 Domain identification

A domain was accepted for an institution only if all three parts of the following rule held: (a) the domain is published by the institution itself on its official website or official social-media page as its web or mail domain; (b) the domain has NS records at both resolvers; (c) the domain has MX records, or, if it has none, the absence is recorded and the domain is retained as measured_no_mx rather than discarded. Website hosts were reduced to their registrable domain.

3.4 Measurement instrument

The instrument is a Python program that queries, for each domain, the following records: MX; TXT at the apex, from which the SPF record(s) are selected by the v=spf1 prefix; TXT at _dmarc.<domain>; TXT at <selector>._domainkey.<domain > for a fixed dictionary of ten selectors (google, default, selector1, selector2, k1, mail, dkim, s1, s2, dkim1); and DNSKEY at the apex, DS at the parent and the AD flag of a validating resolver. Every query was issued to both 1.1.1.1 and 8.8.8.8 over UDP with TCP fallback; both raw answers were stored verbatim with a UTC timestamp. A lookup that returned SERVFAIL or timed out was retried once and otherwise recorded as inconclusive; inconclusive values are never imputed (there were none in the final snapshot). The instrument issues no HTTP, SMTP or TLS connections and performs no port or subdomain probing. In this it differs from trustymail, the open-source scanner published by DHS for BOD 18 – 01, which also connects to mail servers to test STARTTLS [30]; the present census is restricted to what can be read from public DNS.

Record classification. SPF and DMARC records are classified as present (exactly one syntactically valid record), absent, or malformed. Malformed follows the permerror conditions of the specifications: more than one record at the name, an unknown or syntactically invalid term, more than ten DNS-resolving mechanisms, or an invalid ip4/ip6 argument. DKIM is classified as found (a record containing key material at at least one dictionary selector), revoked-only (records with empty p= only) or not_discovered; the last is explicitly not absence. DNSSEC is classified as signed (DNSKEY present), validatable (DS at parent) and validated (AD flag).

Instrument versioning. During the census, version 1.0 of the instrument accepted an SPF ip4 term whose argument was not a valid address (an address concatenated with a following mechanism through a missing space). Version 1.1 requires ip4 and ip6 arguments to parse as valid addresses or CIDR prefixes and otherwise classifies the record as malformed. The snapshot was re-scored under v1.1 from the stored raw answers without new queries; exactly one institution changed (SPF present to malformed, score 4 to 2, spoofability unchanged). All results in this paper are v1.1; v1.0 files are retained.

3.5 Scoring rubric and spoofability

The primary outcome of the study is binary: a domain is spoofable if it has no valid DMARC record or its policy is none, because in that case a receiver has no instruction from the domain owner to reject a message that forges the From domain. The verdict depends on the DMARC record alone; it does not depend on SPF, on DKIM, or on the completeness of DKIM selector discovery. As a secondary summary for comparison across institutions, each domain also receives an SPF score (0–3), a DMARC score (0–4) and a DKIM score (0–2), summed to a posture score of 0–9 (Table 2), with grades A (8–9), B (6–7), C (3–5) and D (0–2).

The posture score is an operational rubric developed for comparative analysis in this study; it is not proposed as a validated security metric, and no headline conclusion rests on it. Its weights follow the role of each mechanism in exact-domain spoofing: DMARC carries the largest range because it alone binds authentication to the visible From domain and expresses the owner's disposition request, and it gains a point for aggregate reporting, which is the owner's only visibility into forgery; SPF is scored by the strictness of its qualifier; DKIM carries the smallest range because a key can be shown to exist but not to be absent (Section 2.2). The rubric deducts one DMARC point for an enforcing policy with pct < 100 but retains the domain as not spoofable, because a policy is published; a variant that counts such domains as spoofable is reported in Section 4.6. MX presence and DNSSEC state are reported but not scored.

Table 2
— Posture rubric.

Component	Condition	Points
SPF	absent, malformed, or + all	0
	?all, no all mechanism, or redirect	1
	~all	2
	-all	3
DMARC	absent or malformed	0
	p=none	1
	p=quarantine	2
	p=reject	3
	+ 1 if rua present; −1 if quarantine/reject with pct < 100; clamped 0–4	± 1
DKIM	not discovered	0
	revoked key(s) only	1
	key found at a dictionary selector	2
Total	sum; grades A 8–9, B 6–7, C 3–5, D 0–2	0–9

3.6 Provider classification

The primary MX host (lowest preference) classifies each domain's mail-service provider as google, microsoft, hostinger, self-hosted (MX under the institution's own domain), other, mixed (primary and secondary hosts of different classes) or none.

3.7 Validation

Three checks were applied. (i) Pilot stability: the ten institutions of the pilot region were re-measured after the full census; 519 of 520 stored values were identical, the single difference being the v1.1 reclassification described above. (ii) Resolver agreement: the two resolvers agreed on every stored value for all 103 domains. (iii) Control domain: a domain operated by the authors' institutional partner was measured in every session and returned the same posture (6/9, B) each time.

3.8 Ethics and responsible disclosure

The measurement is passive and public: it reads records that the institutions themselves publish for exactly this purpose and sends nothing to their systems. No institution is named in the paper; results are aggregated by institutional type and provider class, and any group smaller than five is merged into a larger one. Before publication, per-institution results with remediation guidance are delivered to MoHESR, with a grace period of 60–90 days before re-measurement. A free, provider-specific remediation guide

accompanies the notification. The authors' research is separate from any commercial activity; see the competing-interests statement.

3.9 Planned longitudinal follow-up

The planned follow-up adopts the measure–notify–remediate–re-measure cycle common to both programmes described in Section 2.7: a mandate with deadlines and verification scanning in the U.S. case, and continuous assessment with owner notification in the U.K. case [12, 29]. Per-institution results were delivered to MoHESR in October 2026 (Section 3.8). A second snapshot with the identical instrument and roster is planned shortly after the notification, to establish short-term stability, and a third after the notification grace period, to measure change attributable to the notification. The follow-up will compare snapshots per domain — improved, worsened, unchanged, new or resolved records, with value-level detail (DMARC policy and pct, SPF qualifier, DKIM discovery) — and will test the structural prediction of Section 5.2 that remediation concentrates on the single provider. Its results will be reported separately; the present paper is the cross-sectional baseline against which they will be read.

3.10 Data management and reproducibility

Raw resolver answers, timestamps and per-institution scores are retained by the authors and are not published. The instrument, the roster construction rules, the selector dictionary, the rubric and all aggregate result tables are released with the paper. The re-scoring from raw data under a new instrument version was performed with DNS access disabled in code so that no new query could enter the stored snapshot.

4. Results

4.1 Overall posture

Table 3 summarises the census. Of the 103 domains, 93 (90.3%) are spoofable and the mean posture score is 4.07. Only 2 domains reach grade A, 28 grade B, 49 grade C and 24 grade D. Public institutions score marginally higher than private ones (mean 4.39 versus 3.90; spoofable 91.7% versus 89.6%), a difference too small to interpret. Both grade-A domains belong to private institutions; three public institutions are not spoofable but none reaches grade A.

Group	n	Spoofable	A	B	C	D	Mean
Public	36	33 (91.7%)	0	13	17	6	4.39
Private	67	60 (89.6%)	2	15	32	18	3.90
All	103	93 (90.3%)	2	28	49	24	4.07

Table 3 — *Spoofability, grade distribution and mean posture score (0–9) by institutional type, Snapshot 1.*

4.2 Per-mechanism results

Table 4

and Fig. 2 report each mechanism. SPF is present on 80.6% of domains, but the qualifier is -all on only 10.8% of present records and ~ all on 88.0%; no + all record exists. DMARC is present on 54.4% of domains; among present records, 82.1% of policies are none, 14.3% quarantine and only 2 institutions publish reject. Aggregate reporting (rua) is configured on 60.7% of present records. DKIM keys were discovered for 69.9% of domains, predominantly at the google selector. DNSSEC is signed but unvalidatable throughout: 13 zones publish DNSKEY records and none has a DS record at the parent.

Mechanism / state	All (n = 103)	Public (36)	Private (67)
SPF present	83 (80.6%)	30	53
SPF absent	13 (12.6%)		
SPF malformed (permerror)	7 (6.8%)		
of present: -all	9 (10.8%)		
of present: ~all	73 (88.0%)		
of present: ?all / no all	1 / 0		
DMARC present	56 (54.4%)	21	35
DMARC absent	45 (43.7%)		
DMARC malformed (duplicate)	2 (1.9%)		
of present: p=none	46 (82.1%)		
of present: p=quarantine	8 (14.3%)		
of present: p=reject	2 (3.6%)		
of present: rua set	34 (60.7%)		
enforcing with pct < 100	1		
DKIM found	72 (69.9%)	28	44
DKIM not discovered	31 (30.1%)		
DNSSEC signed (DNSKEY)	13 (12.6%)	8	5
DNSSEC validatable (DS)	0	0	0

Table 4 — *Per-mechanism results, Snapshot 1.*

Figure 2 — *Record state per mechanism for the 103 measured domains, Snapshot 1, with segments ordered from the strongest to the weakest state. SPF: -all 9, ~all 73, ?all 1, malformed 7, absent 13. DMARC:*

reject 2, quarantine 8, none 46, malformed 2, absent 45. DKIM: key found 72, not discovered 31. DNSSEC: signed without a DS record 13, unsigned 90.

4.3 Provider structure

Table 5
and Fig. 3 give the primary-MX provider distribution. The sector is a single-provider population: 92 of 103 institutions (89.3%), including every public institution, receive mail on Google, and 84 of those 92 (91.3%) are spoofable. The remaining 11 institutions are divided among self-hosted mail (4), Microsoft (2), Hostinger (2), mixed host classes (2) and one other provider; 9 of them (81.8%) are spoofable. The provider therefore does not separate protected from unprotected institutions — spoofability is high under every provider class — and the significance of the concentration lies elsewhere: because almost nine-tenths of the sector sits on one platform with one documented configuration path, the weakness is systemic, and so is the opportunity to remove it.

Primary MX class	Institutions (n = 103)
google	92 (89.3%)
microsoft	2 (1.9%)
hostinger	2 (1.9%)
self-hosted	4 (3.9%)
other	1 (1.0%)
mixed	2 (1.9%)

Table 5 — *Primary-MX provider class.*

Figure 3 — *Mail-provider concentration and spoofability, Snapshot 1: the single dominant provider (92 institutions, 84 spoofable) against all other provider classes combined (11 institutions, 9 spoofable).*

Provider class predicts configuration errors as well as posture. Of the 92 Google-hosted institutions, 31 publish an SPF record that does not include the provider's sender range (include:_spf.google.com); their records enumerate web-hosting addresses only, so SPF cannot pass for their actual mail. Such a record also exposes the institution's own legitimate mail to filtering, as Section 5.4.1 shows.

4.4 Record quality

Self-inflicted errors that void a policy are common (Table 6). Nine malformed records in eight institutions comprise six duplicate SPF records, two duplicate DMARC records and one invalid SPF term. Three

institutions answer wildcard TXT records at DKIM selector names; these were not counted as keys. Thirteen institutions publish DNSKEY without DS. Thirteen institutions publish MX sets that mix host classes, including two cases of mistyped Google MX host names.

Table 6
— Record-quality anomalies.

Anomaly	Count	Effect
Duplicate SPF record (permerror)	6	SPF void
Duplicate DMARC record (permerror)	2	DMARC void
Invalid SPF term	1	SPF void
Provider-hosted mail, SPF omits provider	31 (Google)	SPF cannot pass
Enforcing DMARC with pct < 100	1 (pct = 90)	partial enforcement
DNSKEY without DS at parent	13	unvalidatable
Wildcard TXT at DKIM selectors	3	not a key
Mixed MX host classes	13	alignment risk
Mistyped Google MX host name	2	delivery risk

4.5 Pilot region

The ten institutions of the pilot region (Nineveh governorate), measured first and re-measured after the census, span the full range of the rubric (from 0/9 to 7/9) and are all spoofable; they are reported only as a validation set and are not identified individually.

4.6 Sensitivity and robustness

Partial enforcement. Only one domain publishes an enforcing policy with pct < 100 (quarantine at pct = 90). Counting it as spoofable raises the headline figure from 93 (90.3%) to 94 (91.3%); the result is insensitive to the treatment of partial enforcement. Treating pct < 100 as partial is consistent with BOD 18 − 01, which counted a reject policy as compliant only at pct = 100 [12].

Unmeasured and excluded institutions. Two institutions of the population could not be measured, and Rule B excluded 13 religiously affiliated institutions. Bounding the two unmeasured institutions alone, the spoofable share of the 105-institution population lies between 93/105 (88.6%) and 95/105 (90.5%). Bounding all 15 — that is, extending the population to every recognised federal institution before Rule B — gives between 93/118 (78.8%), if every one of them enforced DMARC, and 108/118 (91.5%), if none did. Even under the most favourable assumption, which is implausible given the measured base rate, roughly four in five institutions would remain spoofable; the headline conclusion does not depend on the exclusion rule.

Undiscovered DKIM keys. DKIM was not discovered for 31 domains. Because the spoofability verdict depends on DMARC alone, this limitation cannot change the 90.3% figure. Its only effect is on the secondary posture score: if every undiscovered domain in fact held a key, each would gain two points and the mean score would rise from 4.07 to at most 4.67, which leaves the sector's position in grade C unchanged.

5. Discussion

5.1 Prevalence and structure

On RQ1, the answer is unambiguous: nine in ten Iraqi universities and colleges can be impersonated by exact-domain spoofing, and the result holds under every bound examined in Section 4.6. On RQ2, posture is strongly associated with the structure of mail provision rather than with institutional type: the public/private difference is small, while the concentration of the sector on one provider shapes both its configuration errors and the means of correcting them. The design is observational, and we describe these as structural associations, not causal effects.

5.2 A single-platform failure mode

One platform, one fix. The sector runs on a single provider. That provider signs DKIM by default when enabled, publishes a documented SPF include, and supports phased DMARC enforcement; yet 91% of its Iraqi institutional tenants are spoofable and a third of them publish SPF records written for their web host rather than their mail. As a policy interpretation rather than a causal estimate, the pattern points to the absence of any actor responsible for the configuration step between tenant onboarding and enforcement, not to a lack of technical capacity. A single provider-specific remediation sequence (add the provider include; enable DKIM; publish DMARC none with reporting; raise to quarantine and then reject) would cover 89% of the sector.

Nominal DNSSEC and self-inflicted errors. Thirteen zones are signed and none is validatable, a pattern also reported globally by Chung et al. [11]; here it is complete. Duplicate records, invalid terms and mistyped provider host names void policies that were evidently intended to exist. They are the cheapest findings to fix and the clearest evidence that no monitoring of published records takes place. The same class of self-inflicted error — a provider-hosted domain whose SPF omits the provider, or whose DKIM aligns to the provider's shared domain rather than its own — is not only a spoofability finding but a deliverability risk for the institution's own outbound mail, as Section 5.4.1 illustrates.

5.3 Comparison with global baselines

Against the population of popular domains [10, 20], Iraqi higher-education institutions are not laggards in presence: DMARC is present on 54.4% of domains, against 13.6–15.1% in global samples. They are laggards in enforcement and correctness: only 9.7% of domains enforce a policy, in line with the global picture of policies published at none. The comparison should be read with the caveat that global

samples are dominated by domains that do not send mail at all, whereas every domain in this census belongs to an institution that does.

Sector benchmark. The closest sector comparison is U.K. higher education under Mail Check. Among 164 U.K. universities, university colleges and other degree-awarding bodies, the share with a strict DMARC policy — quarantine or reject, the policy the NCSC recommends — rose from 23% at the end of 2021 to 29% at the end of 2022 [29]. In Iraqi higher education in 2026, 10 of 103 institutions (9.7%) enforce a DMARC policy. The two figures differ in year, measurement population and operator, and the comparison is indicative only; it nonetheless places the Iraqi sector at roughly one third of the level that a comparable sector had reached four years earlier with a central monitoring service. The same report illustrates the scale of the threat to academic domains: in one 30-day period, receivers reported 4,112,819 spoofed messages against the 762 academic organisations in the service, of which 50% were blocked by DMARC [29].

5.4 The protection asymmetry and why it needs a baseline

The mechanisms imply an asymmetry that is central to the policy argument. When a domain owner raises the domain to an enforcing policy, the benefit accrues to other organisations: their receivers can reject messages that forge the fixed domain. The fixed domain's own inbox gains nothing against a forged sender whose domain publishes no enforcing policy, because authentication-based rejection of an incoming forgery requires the sender's domain to have published a policy to enforce; the receiving domain's own configuration cannot supply it. This is a collective-action problem, not a technical gap: each domain that enforces protects others but not itself, so voluntary adoption under-provides inbound safety for the whole sector. A sector-wide baseline resolves the misalignment by making enforcement the default for all domains at once, which is the rationale of BOD 18 – 01 [12] and of the sector-baseline recommendation in Section 5.5. The measured prevalence of spoofable domains (Section 4.1) is therefore not only a description of exposure but the direct quantitative case for a coordinated mandate over voluntary remediation. The same reasoning applies in reverse to deliverability: a sending domain whose SPF or DKIM is misconfigured, even where a DMARC record exists, produces messages that fail authentication and are therefore exposed to reputation-based filtering at strict receivers — a failure mode we observed directly, and document next.

5.4.1 A documented deliverability incident

The operational cost of misconfiguration — as opposed to total absence — is illustrated by a documented incident involving an official invitation dispatched by a public academic institution in the sample. The message was misclassified into the recipient's spam folder by a receiver that evaluates DMARC (Gmail). Inspection of the Authentication-Results header in the raw message revealed a dual-layer authentication failure: an SPF softfail, because the originating relay IP address was not listed in the sending domain's published SPF record; and a DKIM identifier-alignment failure, because although the DKIM signature validated successfully, it was generated under the service provider's shared third-party domain (a *.gappssmtp.com name) rather than the organizational domain, so the authenticated identifier

did not align with the From domain under DMARC. With neither SPF nor DKIM aligned, the message produced an explicit DMARC failure (dmarc=fail). Because the domain's policy was p=none, no protective enforcement instruction was communicated to the receiving mail server, and the message was left to the receiver's reputation-based filtering. The misconfiguration produced concrete operational friction: the legitimate invitation was unavailable to the recipient at the access checkpoint of a ministry-supervised event until a replacement copy was issued and delivered by hand. The incident shows that administrative misconfiguration can pose a deliverability threat as critical as the complete absence of DMARC enforcement — a domain that publishes records but misaligns them fails in both directions: it can be forged to others, and its own legitimate mail can be refused.

5.5 Policy implications

Three instruments follow from the structure of the findings. (i) A sector baseline for .edu.iq requiring SPF with a fail qualifier, DKIM, and DMARC at reject with pct = 100 within a fixed schedule. The baseline combines the staged enforcement model of BOD 18 − 01 — SPF and DMARC published first at none with reporting, then raised to reject within one year [12] — with the U.K. government guidance, which additionally sets out DKIM signing of outgoing mail [28], and is consistent with ITU-T X.1236 [26] and the ITU-D practices of [27]; the baseline would be inexpensive to meet because one provider guide covers 89% of institutions. (ii) Registration-level hygiene: since registration under .edu.iq already requires MoHESR recognition, valid SPF and DMARC records could be made a condition of registration or renewal, with automated permerror detection. (iii) A sector monitoring function of the kind the United Kingdom operated for its public sector and, from 2022, for its education sector, from 2017 to 2026 [24, 29], with the aggregate reports of every institution delivered to a central sector address, as BOD 18 − 01 required of federal agencies [12], since the record-quality findings show that published policies drift and break without anyone observing it; the retirement of that service in favour of commercial monitoring platforms does not remove the need, only the provider. Where the GCI [14] records what a country commits to, this study measures what one sector has actually deployed. The two are complementary: Iraq's lowest-scoring pillars include Technical Measures (9.6 of 20), and a measured, repeatable improvement in a basic technical control across an entire sector is the kind of evidence that strengthens a country's account of its technical capacity, although the census does not by itself change any GCI indicator.

5.6 Threats to validity

- Roster completeness: two private colleges could not be measured (one non-existent domain, one without an official website); the figures describe 103 of 105 institutions in the population, bounded in Section 4.6.
- DKIM discovery: the fixed selector dictionary establishes presence but not absence; not_discovered (31 domains) is an upper bound on DKIM absence. It affects the secondary posture score only; the spoofability verdict does not depend on DKIM (Section 4.6).
- Receiver behaviour: spoofability is defined on published policy, not on observed receiver disposition, which varies across receivers [6, 8]; the measure is conservative in that it counts as protected any

domain with an enforcing policy, including partial ones.

- Domain identity: institutions may send official mail from domains other than the one confirmed from their official presence; such domains were not measured and their posture is unknown.
- Temporal validity: a snapshot describes one day; DNS caching at public resolvers could in principle return stale records, mitigated by dual-resolver agreement on every value.
- Observational design: the study associates posture with provider structure but does not manipulate either; statements about provider concentration are structural associations, and the remediation prediction of Section 5.2 is tested only by the planned post-notification re-measurement.
- Exclusion rules: Rule B removes 13 religiously affiliated institutions from the HE population; their posture is unknown and the figures apply to the federal system as defined. The bounding analysis of Section 4.6 shows that no assumption about them reduces the spoofable share below 78.8%.

6. Conclusion

A complete, passive census of 103 Iraqi university and college domains shows that exact-domain spoofing is possible against 90% of the sector, a figure that remains above 78% under the most favourable assumption about every institution not measured. Posture is strongly structured by the concentration of the sector on one mail provider whose tenants do not complete configuration. The same concentration that spreads the weakness makes it unusually tractable: one provider-specific sequence would move almost nine-tenths of the sector to full enforcement. The controls concerned are those recommended by ITU guidance [26, 27], and their deployment bears on the technical capacity that the GCI assesses, in which Iraq currently scores 9.6 of 20 [14]. Because the instrument is passive, inexpensive and fully specified, the same census can be repeated over time and applied to the higher-education sectors of other countries at a similar stage. The responsible-disclosure protocol and scheduled re-measurement of this study are designed to test the remediation prediction directly in the planned follow-up.

Declarations

Preprint note. *This is the authors' preprint of a measurement study (snapshot of 26 September 2026); it has not been peer reviewed. An extended article with expanded related work and statistical analysis is in preparation.*

Ethics approval and consent to participate. Not applicable. The study reads publicly published DNS records and sends no traffic to any institutional system; no personal data is processed and no human participants are involved. No institution is named; aggregates below five are merged. Per-institution results were delivered to the Ministry of Higher Education and Scientific Research before publication, with a remediation guide and a grace period, under the responsible-disclosure protocol of Section 3.8.

Competing interests. R. A. Khalil heads the Department of Cybersecurity Engineering Techniques at Al-Qabas Private College, one of the institutions in the measured population, and is also affiliated with

Golden Net, which provided the computing infrastructure used in this study and whose own domain served as the measurement control. B. Alamori is affiliated with Golden Net. Golden Net offers email-security services, including domain-posture assessment. The study was designed, conducted and analysed by the authors; the company provided infrastructure only. No institution in the measured population was a client of the company at the time of measurement, and the authors' own institution received no treatment different from any other institution in the census. Should any measured institution later engage the company for remediation, that engagement will be disclosed in the longitudinal follow-up.

Authors' contributions. R. A. Khalil: conceptualisation, methodology, software, validation, formal analysis, investigation, writing (original draft), supervision. B. Alamori: investigation, data curation (roster construction and domain verification), validation, formal analysis (international policy comparison), methodology (longitudinal design), visualisation, writing (review and editing). Both authors read and approved the final manuscript.

Availability of data and materials. The measurement instrument, roster construction rules, selector dictionary, rubric and all aggregate result tables will be deposited in a public repository upon acceptance and are available from the corresponding author during review. Per-institution raw data are withheld under the disclosure protocol.

Acknowledgements. The authors thank Golden Net for computing infrastructure and for permitting the use of its domain as the measurement control, and Al-Qabas Private College for institutional support.

Funding. No external funding was received for this study.

Consent for publication. Not applicable.

Use of generative AI. A generative-AI assistant (Claude, Anthropic) was used for language editing and drafting support under the authors' direction. All measurements, analyses, interpretations and conclusions are the authors' own and were verified by them.

References

1. Kitterman S (2014) Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, RFC 7208, IETF, Apr
2. Crocker D, Hansen T, Kucherawy M (2011) DomainKeys Identified Mail (DKIM) Signatures, RFC 6376, IETF, Sep
3. Kucherawy M, Zwicky E (2015) Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC 7489, IETF, Mar
4. Durumeric Z, Adrian D, Mirian A, Kasten J, Bursztein E, Lidzborski N, Thomas K, Eranti V, Bailey M, Halderman JA (2015) Neither Snow Nor Rain Nor MITM… An Empirical Analysis of Email Delivery

Security, in Proc. ACM Internet Measurement Conference (IMC), pp. 27–39. 10.1145/2815675.2815695

5. Foster ID, Larson J, Masich M, Snoeren AC, Savage S, Levchenko K (2015) Security by Any Other Name: On the Effectiveness of Provider Based Email Security, in Proc. ACM Conference on Computer and Communications Security (CCS), pp. 450–463. 10.1145/2810103.2813607
6. Hu H, Wang G (2018) End-to-End Measurements of Email Spoofing Attacks, in Proc. 27th USENIX Security Symposium, pp. 1095–1112
7. Tatang D, Zettl F, Holz T (2021) The Evolution of DNS-based Email Authentication: Measuring Adoption and Finding Flaws, in Proc. 24th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), pp. 354–369
8. Shen K, Wang C, Guo M, Zheng X, Lu C, Liu B, Zhao Y, Hao S, Duan H, Pan Q, Yang M (2021) Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks, in Proc. 30th USENIX Security Symposium, pp. 3201–3217
9. Liu E, Akiwate G, Jonker M, Mirian A, Savage S, Voelker GM (2021) Who's Got Your Mail? Characterizing Mail Service Provider Usage, in Proc. ACM Internet Measurement Conference (IMC), pp. 122–136. 10.1145/3487552.3487820
10. Wang C, Shen K, Guo M, Zhao Y, Zhang M, Chen J, Liu B, Zheng X, Duan H, Lin Y, Pan Q (2022) A Large-scale and Longitudinal Measurement Study of DKIM Deployment, in Proc. 31st USENIX Security Symposium, pp. 1185–1201
11. Chung T, van Rijswijk-Deij R, Chandrasekaran B, Choffnes D, Levin D, Maggs BM, Mislove A, Wilson C (2017) A Longitudinal, End-to-End View of the DNSSEC Ecosystem, in Proc. 26th USENIX Security Symposium, pp. 1307–1322
12. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), Binding Operational Directive 18 – 01: Enhance Email and Web Security, 16 Oct. (2017) https://www.cisa.gov/news-events/directives/bod-18-01-enhance-email-and-web-security
13. U.K. National Cyber Security Centre, Email Security and Anti-Spoofing, version 2.0, 7 Oct. (2019) https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing
14. International Telecommunication Union (2024) Global Cybersecurity Index 2024, 5th ed., Geneva: ITU, ISBN 978-92-61-38751-8
15. Ministry of Higher Education and Scientific Research (Iraq) Information Technology Directorate, circular no. 1414/6604 on cybersecurity and incident reporting, 21 June 2026 (official circular; copy held by the authors)
16. Martin F, Lear E, Draegen T, Zwicky E, Andersen K (Sep. 2016) Interoperability Issues between DMARC and Indirect Email Flows, RFC 7960. IETF
17. Arends R, Austein R, Larson M, Massey D, Rose S (2005) DNS Security Introduction and Requirements, RFC 4033, IETF, Mar
18. Arends R et al (2005) Resource Records for the DNS Security Extensions, RFC 4034, IETF, Mar

19. Arends R et al (2005) Protocol Modifications for the DNS Security Extensions, RFC 4035, IETF, Mar
20. Czybik S, Horlboge M, Rieck K (2023) Lazy Gatekeepers: A Large-Scale Study on SPF Configuration in the Wild, in Proc. 23rd ACM Internet Measurement Conference (IMC), pp. 344–355. 10.1145/3618257.3624827
21. Ashiq MI, Li W, Fiebig T, Chung T (2023) You've Got Report: Measurement and Security Implications of DMARC Reporting, in Proc. 32nd USENIX Security Symposium, pp. 4123–4137
22. Ashiq MI, Li W, Fiebig T, Chung T (2024) SPF Beyond the Standard: Management and Operational Challenges in Practice and Practical Recommendations, in Proc. 33rd USENIX Security Symposium, pp. 3081–3098
23. Internet Assigned Numbers Authority (IANA) (2005) IANA Report on the Redelegation of the.IQ Top-Level Domain, 5 Aug. https://www.iana.org/reports/2005/iq-report-05aug2005.pdf
24. U.K. National Cyber Security Centre, NCSC to retire Web Check and Mail Check, 6 Nov. (2025) (services retired 31 Mar. 2026). https://www.ncsc.gov.uk/blog-post/retiring-mail-check-web-check
25. Internet Corporation for Assigned Names and Numbers (ICANN) Redelegation of.IQ (Iraq), Board resolution 05.70, 28 July 2005 (redelegation to the National Communications and Media Commission, NCMC). https://www.icann.org/en/board-activities-and-meetings/materials/minutes-special-meeting-of-the-board-28-07-2005-en
26. International Telecommunication Union (2023) Security requirements and countermeasures for targeted email attacks, Recommendation ITU-T X.1236 (11/2023. ITU, Geneva
27. International Telecommunication Union Securing information and communication networks: Best practices for developing a culture of cybersecurity — Output Report on ITU-D Question 3/2 for the study period 2018–2021, Geneva: ITU, 2021. ISBN 978-92-61-34101-5
28. U.K. Government Digital Service and Central Digital and Data Office, Set up government email services securely, GOV.UK guidance, last updated 4 Mar. (2024) https://www.gov.uk/guidance/set-up-government-email-services-securely
29. U.K. National Cyber Security Centre, Active Cyber Defence — The Sixth Year, NCSC, (2023) https://www.ncsc.gov.uk/files/ACD6-full-report.pdf
30. Cybersecurity and Infrastructure Security Agency (CISA) trustymail: scan domains and return data based on trustworthy email best practices, open-source software. https://github.com/cisagov/trustymail

Figures

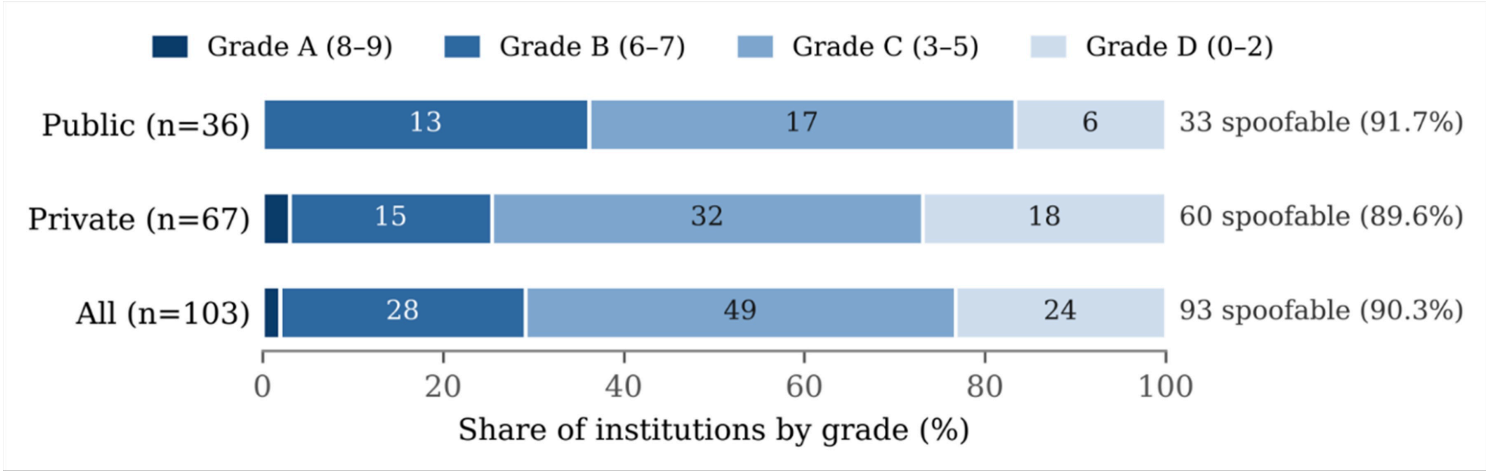


Figure 1

Grade distribution (count of institutions per grade) and spoofability, public versus private institutions, Snapshot 1.

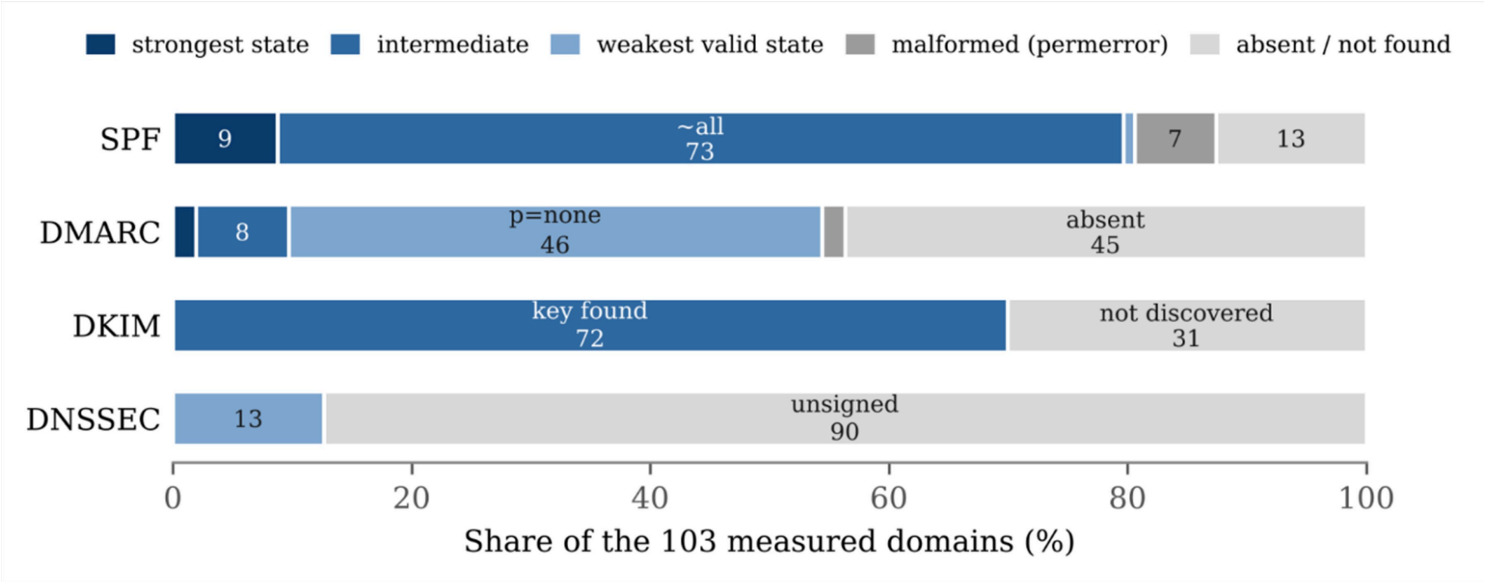


Figure 2

Record state per mechanism for the 103 measured domains, Snapshot 1, with segments ordered from the strongest to the weakest state. SPF: -all 9, ~all 73, ?all 1, malformed 7, absent 13. DMARC: reject 2, quarantine 8, none 46, malformed 2, absent 45. DKIM: key found 72, not discovered 31. DNSSEC: signed without a DS record 13, unsigned 90.

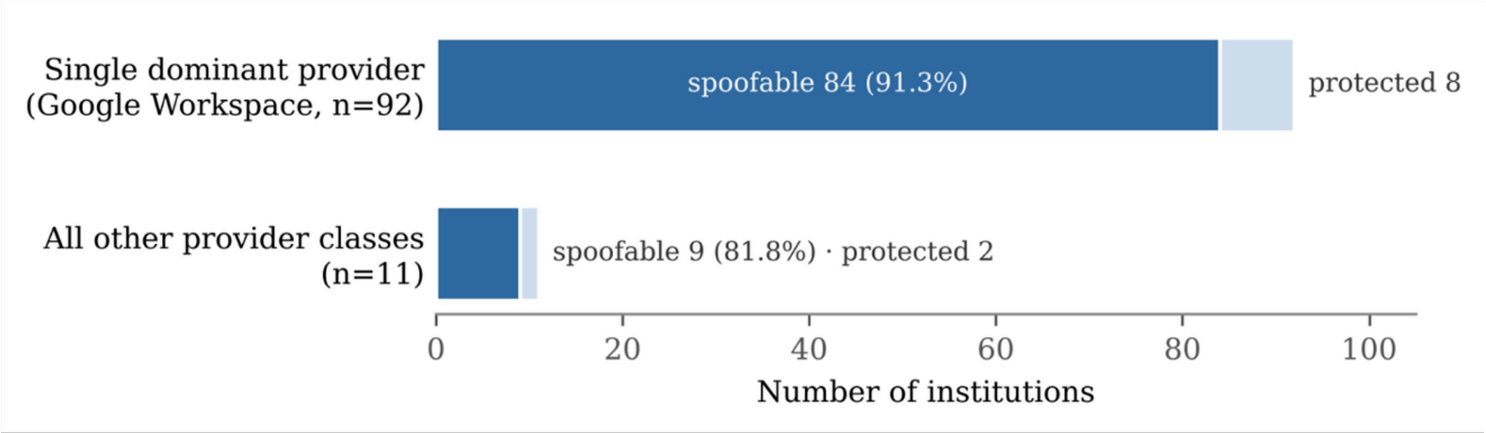


Figure 3

Mail-provider concentration and spoofability, Snapshot 1: the single dominant provider (92 institutions, 84 spoofable) against all other provider classes combined (11 institutions, 9 spoofable).