ENUCLEA

Digital Trust Audit

2026 · PRINCE WILLIAM CHAMBER OF COMMERCE

What was measured

This briefing reports public email-authentication posture across 814 unique local small-to-midsize businesses in Prince William Chamber of Commerce, Virginia. Fortune 500 chains, duplicate regional-bank branches, and government agencies were separated from the community scorecard. Each entity is bound to one primary sending domain. The unit of analysis is the published DNS identity of that domain, not an internal network review.

UNIVERSE
814 unique local SMBs

SOURCE
Chamber regional list

CONTROLS
SPF · DKIM · DMARC · DNSBL

ACCESS
Public DNS only

Acronym Definitions

SPF (Sender Policy Framework) — publishes which mail servers are authorized to send on behalf of a domain

DKIM (DomainKeys Identified Mail) — cryptographically signs outbound mail so recipients can verify it was not altered in transit

DNSBL (DNS Blocklist) — a real-time list of IP addresses known to send spam or malicious mail; a hit indicates reputation damage

DMARC (Domain-based Message Authentication, Reporting & Conformance) — ties SPF and DKIM together and tells receiving servers what to do with mail that fails both checks

p=none — monitoring mode only; failing mail is still delivered

p=quarantine — failing mail is sent to spam/junk

p=reject — failing mail is blocked entirely; the strongest enforcement level

How the scores are read

Scoring methodology

Scores come from non-intrusive interrogation of public DNS: SPF authorization, DKIM selector presence, DMARC policy, and — in this run — DNSBL / IP reputation (blocklist checks) where an outbound identity was visible. 'Enforced' means a DMARC policy of p=quarantine or p=reject. A record of p=none is monitoring, not protection. No mail was sent to or from audited domains. No mailbox was accessed. No private system was in scope. This is intentional — the audit is bounded by public DNS and respects the line between observable identity and private infrastructure. The snapshot is point-in-time. Where no DKIM selector was advertised, domains were checked against a common selector dictionary — results reflect an educated estimate, not a confirmed absence.

How to read a sector page

Each sector page holds the same instruments: headcount, mean, median, enforcement rate, missing DMARC, missing DKIM, and the fault that defines the vertical. "Why it matters" is the business-risk path for that vertical. "Why the data looks different" is the operating reason the numbers diverge from the regional mean — vendor mix, tenant type, who owns DNS, and whether the firm's real sending fleet is aligned. Individual private businesses are not named.

Grade scale

Score Range	Grade	Trust Classification
95–100	**A+**	Precise (High Trust)
90–94	**A**	**Robust (High Trust) *Recommended Goal**
75–89	**B**	Good (Moderate Protection)
60–74	**C**	Vulnerable (Basic Only)
45–59	**D**	At Risk (High Exposure)
0–44	**F**	Critical (No Spoofing Protection)

Scores are derived from a 100-point rubric across five weighted pillars — see the Scoring Rubric addendum at the end of this document for the full breakdown.

Community posture is a C+.

Basic authentication is present. Spoof protection is not yet the regional default.

814

ENTITIES

unique local SMBs · providers held out

66.2

MEAN / MEDIAN

Mean 66.2 · Median 65.0 · −13.8 vs Good (80)

C+

GRADE

basic auth / monitoring

23.3%

ENFORCED

76.7% open or inactive

What the region shows

Across 814 unique local entities the community mean is 66.2 and the median is 65.0. That is a tight center: most firms are neither catastrophically unconfigured nor fully enforced. Only 23.3% publish an enforcing DMARC policy. The rest can still be impersonated with a lookalike From line that surviving filters will treat as ordinary local mail.

The sector spread is orderly, not random. Technology & Defense, Financial Services, Professional Services, and Construction & Trades sit above the line because tenant maturity, regulatory scrutiny, and high-value invoice flows pull authentication forward. General Commercial, Non-Profit & Community, and Hospitality sit below it because DNS is nobody's job and extra senders are unsigned. General Commercial, at 596 firms, is the gravitational center of the study.

Providers were measured on the same instruments and kept out of the community mean so they would not inflate it.

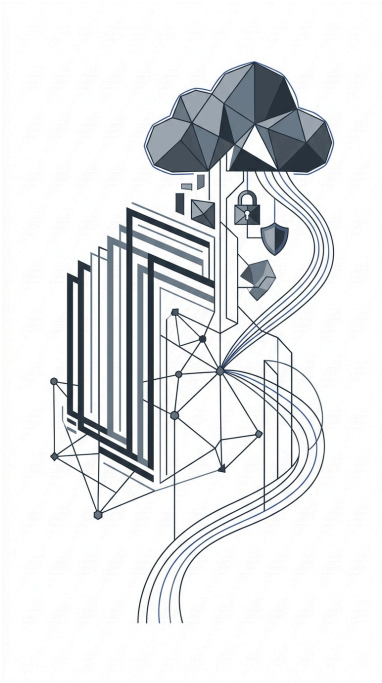
How to use the pages that follow

Read each sector as an operating system, not a leaderboard. The interesting question is not "who scored lowest." It is why a vertical with the same public DNS toolkit produces a different enforcement rate. Those reasons — field-first admin, donated tenants, unsigned vendor senders, unclicked M365 DKIM — are what make a community grade movable.

SECTOR PAGE · N = 5

+10.6 VS REGIONAL MEAN

IT Providers & MSPs



76.8

MEAN / MEDIAN

Mean 76.8 · Median 82.0 · +10.6 vs 66.2

20%

ENFORCING

1 of 5 quarantine or reject

80%

MONITORING ONLY

4 of 5 stalled at p=none (3/5 RUA)

4 of 5

OPEN TO SPOOF

monitoring mode delivers forged mail

Why it matters

- Every business in this study is a downstream client of an IT provider — their posture sets the floor for the region
- A spoofed or impersonated MSP domain is a master key: clients accept email from their provider without question
- Fake invoices, remote-access requests, and credential resets sent from a trusted IT domain convert at the highest rate of any vertical

Why the data looks different

- Highest mean in the region (76.8) with 100% SPF and DKIM adoption across all audited providers
- 4 of 5 providers (80%) remain stalled in passive monitoring (p=none) — only 1 provider has advanced to quarantine or reject
- The gap is purely a policy decision: telemetry is active (60.0% RUA reporting), but the enforcement switch remains unflipped

SECTOR PAGE · N = 2

+8.8 VS REGIONAL MEAN

Technology & Defense

75.0

MEAN / MEDIAN

Mean 75.0 · Median 75.0 · +8.8 vs 66.2

50%

ENFORCING

1 of 2 quarantine or reject

50%

NO DMARC

1 of 2 no policy published

50%

DNSBL LISTED

1 of 2 blocklist reputation hits

Why it matters

- Defense, aerospace, and government IT contractors operate under strict DFARS / NIST SP 800-171 and CMMC mandates
- Contractors handle Controlled Unclassified Information (CUI) and defense logistics where domain spoofing represents a national security threat
- Prime contractors and DoD agencies increasingly require verified SPF, DKIM, and DMARC before issuing subcontractor task orders

Why the data looks different

- 100% Microsoft 365 cloud email deployments with 50.0% enforcement rate
- Unconfigured secondary domains lower what should otherwise be a uniform A-grade defense-adjacent posture

SECTOR PAGE · N = 39 | +7.3 VS REGIONAL MEAN

Financial Services

73.5

MEAN / MEDIAN

Mean 73.5 · Median 75.0 · +7.3 vs 66.2

46%

ENFORCING

18 of 39 quarantine or reject

28%

NO DMARC

11 of 39 no policy published

21 of 39

OPEN TO SPOOF

p=none or no DMARC

Why it matters

- Financial advisors, CPAs, lenders, and wealth managers are high-priority targets for wire fraud and account takeover schemes
- A single spoofed invoice or wire-instruction email can cause catastrophic, unrecoverable capital loss for local clients
- SEC, FINRA, and FTC Safeguards Rules mandate strict domain and message authentication for customer data protection

Why the data looks different

- Highest commercial enforcement rate in the county (46.2% — 18 of 39 firms) driven by enterprise broker-dealer mandates
- Highest telemetry adoption in the study, with 61.5% (24 of 39 firms) publishing active DMARC RUA aggregate reporting
- 11 of 39 boutique firms still publish no DMARC policy, creating a bifurcated risk landscape between branch offices and independents

SECTOR PAGE · N = 15

+7.3 VS REGIONAL MEAN

Professional Services: Legal & CPA

73.5

MEAN / MEDIAN

Mean 73.5 · Median 75.0 · +7.3 vs 66.2

27%

ENFORCING

4 of 15 quarantine or reject

53%

NO DMARC

8 of 15 no policy published

53%

MISSING DKIM

8 of 15 unsigned outbound mail

Why it matters

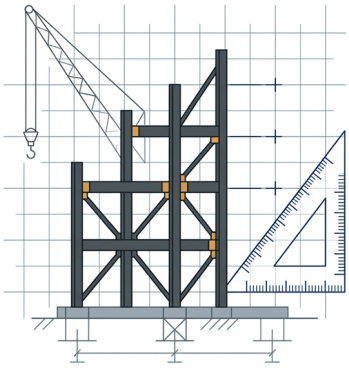
- Attorneys, legal practices, title companies, and CPAs handle confidential client privileged communications and escrow/settlement funds
- Real estate closing wire fraud represents one of the fastest-growing cybercrime categories targeting legal settlement coordinators
- State bar ethics rules require reasonable technical measures to protect confidential client data in transit

Why the data looks different

- Strong 73.5 mean score, but 53.3% of firms (8 of 15) publish no DMARC record and 53.3% lack DKIM cryptographic signatures
- Only 4 of 15 practices (26.7%) enforce anti-spoofing policies despite handling high-risk financial and escrow transactions
- Practices assume standard cloud setups (Microsoft 365: 9, Google Workspace: 3) automatically enforce protection without manual DNS activation

SECTOR PAGE · N = 45 +1.4 VS REGIONAL MEAN

Construction & Trades



67.6

MEAN / MEDIAN

Mean 67.6 · Median 65.0 · +1.4 vs 66.2

20%

ENFORCING

9 of 45 quarantine or reject

36%

NO DMARC

16 of 45 no policy published

47%

MISSING DKIM

21 of 45 unsigned outbound mail

Why it matters

- In construction and contracting, financial transactions are high-value and episodic (draw requests, subcontractor disbursements, change orders)
- Threat actors monitor unauthenticated email threads to execute wire-redirection right before progress payments or closing
- A single intercepted payment can paralyze active project job sites and result in mechanics' liens

Why the data looks different

- 44.4% of the cohort (20 of 45 firms) is stalled in passive monitoring (p=none), leaving 80.0% open to lookalike forgery
- Trade contractors rely heavily on standard cloud defaults (Microsoft 365: 19, Google Workspace: 13) without completing DKIM/DMARC alignment
- 11 of 45 trade firms (24.4%) suffer from DNSBL blocklist hits caused by shared hosting and unauthenticated field dispatchers

SECTOR PAGE · N = 40

+1.3 VS REGIONAL MEAN

Healthcare & Medical

67.5

MEAN / MEDIAN

Mean 67.5 · Median 67.0 · +1.3 vs 66.2

25%

ENFORCING

10 of 40 quarantine or reject

45%

NO DMARC

18 of 40 no policy published

25%

DNSBL LISTED

10 of 40 blocklist reputation hits

Why it matters

- Medical practices, dental clinics, specialty surgery centers, and therapy groups transmit HIPAA-regulated electronic Protected Health Information (ePHI)
- Spoofed clinical emails can facilitate fraudulent prescription routing, medical identity theft, and vendor payment diversion
- OCR (HHS Office for Civil Rights) penalizes unauthenticated transmission of patient health identifiers

Why the data looks different

- Solid 67.5 mean score across 40 practices, with primary email on Google Workspace (15) and Microsoft 365 (13)
- 10 of 40 practices (25.0%) show DNSBL blocklist hits or SPF lookup penalties triggered by unaligned third-party EHR appointment reminders
- 18 of 40 practices (45.0%) publish no DMARC record at all, leaving clinical communications vulnerable to impersonation

SECTOR PAGE · N = 596

−0.5 VS REGIONAL MEAN

General Commercial

65.7

MEAN / MEDIAN

Mean 65.7 · Median 65.0 · −0.5 vs 66.2

23%

ENFORCING

136 of 596 quarantine or reject

48%

NO DMARC

287 of 596 no policy published

54%

MISSING DKIM

323 of 596 unsigned outbound mail

Why it matters

- As the largest sector cohort, General Commercial represents the core economic circulatory system of the county
- Local B2B supply chains, regional wholesalers, equipment distributors, and commercial vendors transact via recurring email billing
- Weak domain hygiene across this cohort enables widespread invoice interception and vendor impersonation fraud

Why the data looks different

- At 596 of 814 entities (73.2%), this single cohort anchors the county mean score (65.7 vs 66.2 regional mean)
- 287 of 596 domains (48.2%) publish no DMARC record, and 323 domains (54.2%) lack DKIM outbound signatures
- 225 firms operate on Microsoft 365 and 157 on Google Workspace, but softfail (~all) configurations leave 77.2% open to lookalike forgery

SECTOR PAGE · N = 40 | −1.9 VS REGIONAL MEAN

Non-Profit & Community

64.3

MEAN / MEDIAN

Mean 64.3 · Median 65.0 · −1.9 vs 66.2

18%

ENFORCING

7 of 40 quarantine or reject

43%

NO DMARC

17 of 40 no policy published

58%

MISSING DKIM

23 of 40 unsigned outbound mail

Why it matters

- Non-profits, charities, foundations, and community associations hold high public trust and process donor contributions and grant distributions
- Attackers frequently spoof non-profit leadership during fundraising galas and capital campaigns to divert donor wire transfers
- Compromised reputations directly impair grant eligibility, donor goodwill, and community board confidence

Why the data looks different

- 0% reject enforcement across 40 community organizations (7 quarantine, 16 monitoring p=none, 17 no DMARC)
- 58% of non-profits (23 of 40) lack DKIM cryptographic signatures, sending unauthenticated donor solicitations
- Heavy reliance on donated Microsoft 365 (18) and Google Workspace (4) grants without dedicated technical administration to activate DNS keys

SECTOR PAGE · N = 37 | −4.8 VS REGIONAL MEAN

Hospitality, Dining & Retail

61.4

MEAN / MEDIAN

Mean 61.4 · Median 62.0 · −4.8 vs 66.2

14%

ENFORCING

5 of 37 quarantine or reject

62%

NO DMARC

23 of 37 no policy published

54%

MISSING DKIM

20 of 37 unsigned outbound mail

Why it matters

- Restaurants, event venues, boutique retailers, and hospitality operators manage large customer contact lists and private event bookings
- Spoofed banquet and catering deposit invoices directly defraud event clients and damage local brand goodwill
- Customer trust is fragile: recipient mail gateways increasingly route unauthenticated promotional emails directly to spam folders

Why the data looks different

- Lowest-scoring sector in the region (61.4 mean), with 62% of storefronts (23 of 37) publishing no DMARC record at all
- 86% of hospitality businesses (32 of 37) are open to spoofing, with only 5 storefronts (14%) enforcing DMARC
- Storefronts manage marketing separate from core operations, creating unaligned transactional sending services on DIY website builders

Free-mail is a second, stable failure.

13.3% of the wider chamber set still use consumer or ISP mail as a public business identity.

1086

CHAMBER IDENTITIES

wider set including chains and agencies

144

FREE-MAIL USERS

13.3% of the wider chamber set

90

PURE FREE-MAIL

Gmail, Yahoo, or similar as primary

54

SHADOW-MAIL

own a domain, publish free-mail for inquiries

What it is

- A separate identity failure from missing DMARC — the domain itself is absent
- Concentrates in trades, salons, and owner-operated services
- Consistent across Northern Virginia chambers — this figure is stable, not improving

Why it matters

- A DMARC record on a domain nobody uses does not fix a Gmail address on the truck wrap
- Free-mail identities cannot be authenticated, monitored, or enforced against
- The business is invisible to any email-security tooling the recipient deploys

All sectors against the regional mean

IT Providers & MSPs lead the region — and multiple providers are still open to impersonation. The top of the table is not a ceiling to aspire to. It is a floor that needs raising.

Sector	Mean Score	vs Regional Mean
IT Providers & MSPs	76.8	+10.6
Technology & Defense	75.0	+8.8
Financial Services	73.5	+7.3
Professional Services: Legal & CPA	73.5	+7.3
Construction & Trades	67.6	+1.4
Healthcare & Medical	67.5	+1.3
Regional Mean	*66.2*	—
General Commercial	65.7	−0.5
Non-Profit & Community	64.3	−1.9
Hospitality, Dining & Retail	61.4	−4.8

The bulk of the work is in the middle. Most sectors sit within a few points of 66.2 — close enough that a single policy change moves the regional grade. But no sector, including the leaders, has closed the impersonation window.

What holds, and what to do with it

The region is configured, not enforced.

A 66.2 mean with 23.3% enforcement means most domains can send mail and most domains can still be forged. Monitoring records and missing DKIM are the common state, not the exception.

Sector gaps follow operations, not slogans.

Construction is a payment-path problem. Legal and CPA is an unclicked DKIM problem. Healthcare is an unaligned vendor-sender problem. Hospitality is an unsigned storefront. Treat them as different jobs.

General Commercial sets the grade.

At 596 of 814 entities, this cohort is the community. If only the regulated and defense-adjacent firms harden DNS, the regional number will not move.

Free-mail is a second, stable failure.

13.3% of the wider chamber set still use consumer or ISP mail as a public identity. It will not be fixed by a DMARC record on a domain nobody uses.

The lift is DNS, not capital.

SPF, DKIM, a DMARC record at p=none, two weeks of reports, then quarantine or reject. The same three steps apply to every page in this book. The sector narratives only change why the owner should care this week.

Domain check **enuclea.com/email-security-check**

Research Enuclea · Stafford, Virginia

Addendum: Scoring Rubric

Each domain is scored across five positive pillars (max 100 pts) with deductions applied for broad sending scope and blocklist presence. The final score is clamped between 0 and 100.

What adds points

Pillar	Points
Domain Identity [1]	+35
DMARC Enforcement	+25
Reverse DNS / Infrastructure	up to +15
SPF Record & Hygiene	up to +15
DKIM Validity	+10

What removes points

Condition	Penalty
Broad SPF network block (>/28)	−5
Large authorized IP range (>4,096)	−10
Excessive IP range (>65,536)	−20
IP listed on DNSBL blocklist	−15

Partial credit is awarded within each pillar based on configuration quality — e.g. p=none with reporting earns +10 of the available +25 for DMARC. The final score is clamped between 0 and 100.

[1] Domain Identity measures whether the business operates on a dedicated custom domain (e.g. acmeplumbing.com) or relies on a free consumer address (e.g. Gmail, Yahoo). A custom domain is the prerequisite for all other authentication controls — without it, SPF, DKIM, and DMARC cannot be meaningfully applied.