



HUB
SOFTWARE

A HUB SOFTWARE STUDY

State of Tax Firm Email Security 2026

How 3,612 small US tax practices protect their clients from email that fakes the firm's name.

34%

of small US tax practices tell Gmail, Outlook and other mail systems to block or quarantine email that fakes their name.

Almost every firm has set up the first layer of protection. Fewer than half have switched on the one that stops fake email.

97%

publish a sender list (SPF)

65%

publish a DMARC policy at all

30%

of all firms set DMARC to "none", which blocks nothing (45% of firms that have DMARC)

29%

fully protected: SPF, enforced DMARC and DKIM

Jim Taczy, Founder, Hub Software, LLC

Scan date September 26, 2026 · Published October 13, 2026 · Corrected edition

jim@cpa-hub.com · 949.288.3022

cpa-hub.com

What we found

Only 34% of small US tax practices stop criminals from sending email in their name. Almost every firm has set up the first layer of protection; fewer than half have switched the important one on.

We checked the public email settings of 3,612 US tax practices with 2 to 8 credentialed preparers on September 26, 2026. 3,609 answered; the 3,603 of those that receive email are the basis for the figures below.

Finding	Share of firms
Publish a basic sender list (SPF)	97%
Publish a DMARC policy (the setting that tells Gmail, Outlook and others what to do with email faking your address)	65%
Set DMARC to "none" — it reports fakes but blocks nothing	30%
Set DMARC to block or quarantine fakes	34%
Fully protected: SPF, enforced DMARC and DKIM signing	29%

Two things stand out:

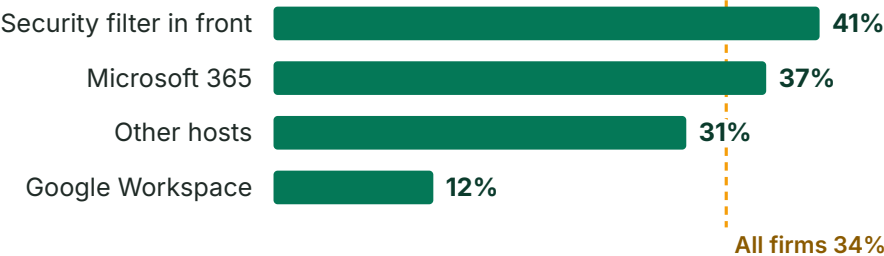
- **Half the work, none of the protection.** 45% of the firms that published a DMARC policy left it on "none". Their clients' inboxes still accept email that fakes the firm's address.
- **The smallest firms are the most exposed.** 32% of 2–3-preparer firms block fakes, against 45% of firms with 6–8 preparers.

Share of firms that block fake email

BY FIRM SIZE



BY EMAIL PROVIDER



Source: Hub Software scan of public DNS records for 3,612 US tax practices, September 26, 2026. Method and limits are at the end of this report.

Why it matters

A tax firm's email address is a key to its clients' trust. If a criminal can send email that looks like it came from the firm, clients will open the attachment, click the link or send the documents.

- **The IRS has warned tax pros about this directly.** Its July 2025 Security Summit alert describes spear phishing and a “new client” scam built to “trick practitioners into opening email links or attachments that infect computer systems to steal existing client information” ([IR-2025-75](#)).
- **The FTC tells small businesses to use these exact tools.** Its email authentication guidance names SPF, DKIM and DMARC, and says DMARC lets you “tell other servers what to do” with fake email: reject it, flag it as spam, or take no action ([FTC](#)). A DMARC policy of “none” is the “take no action” choice.
- **A breach now has a federal clock.** Since May 13, 2024, a tax preparation firm covered by the FTC Safeguards Rule must notify the FTC within 30 days of discovering a breach affecting 500 or more people ([FTC](#)).

The Safeguards Rule itself does not name DMARC. It requires a written security plan that addresses the risks a firm can reasonably foresee, and impersonation by email is one the IRS has named for years.

The findings in detail

By firm size

The fewer preparers a firm has, the less likely it is to block fake email. Firms with 2–3 preparers are 77% of the practices we checked. In these tables, Firms counts every firm that answered; the percentages are of the firms among them that receive email.

Preparers	Firms	Publish DMARC	Left on “none”	Block fakes	DKIM found	Fully protected
2–3	2,772	62%	29%	32%	61%	27%
4–5	540	75%	31%	42%	73%	37%
6–8	297	77%	31%	45%	77%	40%

By email provider

Email providers differ more than firm sizes do. 12% of firms on Google Workspace block fakes, against 37% on Microsoft 365, which hosts 59% of these firms. The scan shows the gap, not its cause.

Email provider	Firms	Publish SPF	Publish DMARC	Block fakes	DKIM found	Fully protected
Security filter in front (e.g. Proofpoint, Mimecast)	444	99%	75%	41%	61%	31%
Microsoft 365	2,122	99%	67%	37%	71%	34%
Other hosts	746	96%	60%	31%	53%	24%
Google Workspace	261	80%	50%	12%	52%	11%

17% of the Google Workspace firms have neither SPF nor DMARC, the two most basic settings. Twenty-three firms use GoDaddy email and seven use Zoho; those groups are too small to report on their own.

Websites

91% of firm websites load over a valid secure (HTTPS) connection. 5% present a certificate browsers reject, which puts a warning in front of any client who visits. 29% send the header that tells browsers to always use the secure version of the site (HSTS).

What a firm should do this week

Three changes close most of the gap. Each is a setting in the firm's domain registrar or DNS host, or in the email admin console, and an IT provider can make all three in an afternoon.

1. **Turn on DKIM signing** in Microsoft 365 or Google Workspace. Both have a switch for it; the firm then publishes the two records it gives you.
2. **Publish DMARC at "none" with reports turned on**, and read the reports for two to four weeks. They show every service that sends email as the firm: payroll, e-signature, the tax software's client portal.
3. **Move DMARC to "quarantine", then "reject"**, once every legitimate sender is covered. This is the step that stops fake email. The 45% of firms with DMARC that left it on "none" have not taken it.

Then write it down. The firm's written security plan should say which email protections are in place and who checks the reports.

How the numbers were gathered

Everything in this report comes from records any member of the public can look up. Nothing was logged into, probed or tested for weaknesses, and no firm is named.

Who is in it. The IRS's public file of preparer tax identification number (PTIN) holders, in the release dated February 23, 2026, lists each preparer's credential, business address and website. We grouped the preparers who list a CPA or attorney credential into firms by the website domain they give, and kept firms with 2 to 8 of them: 4,412 firms. We then left out 669 firms made up only or mostly of attorneys, and 131 more before the scan: 123 whose domain had no mail server or no longer existed, and 8 removed while the list was cleaned. That left 3,612 firms; 3,609 answered the lookups, and the 3,603 of those that receive email are the basis for every percentage. The other six answered but take no email: three have no mail server, and three publish a record saying they accept none.

What we checked, per firm:

- Who hosts the firm's email (its MX records).
- Its SPF record, and whether it ends in a hard fail.
- Its DMARC record and policy. "Block fakes" means a policy of quarantine or reject applied to all mail.
- DKIM signing keys, looked up under ten common names used by Microsoft 365, Google Workspace and major email services.

- One request to the firm's home page, to check for a valid HTTPS certificate and the HSTS header.

How we checked the checker. Lookups went to three public DNS services (Cloudflare, Google and Quad9). A lookup that failed was left out of every percentage rather than counted as a missing record; 3 firms were excluded this way. We then re-checked 50 randomly chosen firms with a separate tool through a different path; SPF, DMARC and the DMARC policy matched on all 50.

Limits.

- **DKIM is a floor.** A firm can sign under a key name we did not try, so the real DKIM figure, and the “fully protected” figure, may be somewhat higher.
- **Firm size counts credentialed preparers only.** The size bands count the CPAs and attorneys in the IRS file; a firm's other preparers and staff are not counted, so some firms are larger than their band.
- **Firms without a website, or whose domain had no mail server, are not in the count.** Those firms may be less protected, not more.
- **This is one day.** The scan ran on September 26, 2026. Records change.
- **Small groups are withheld.** Any state or provider with fewer than 10 firms is not reported.

Sources

- [IRS IR-2025-75: Tax pros should watch out for phishing emails and other attacks](#) (July 15, 2025)
- [FTC: Cybersecurity for Small Business — Email Authentication](#)
- [FTC: Safeguards Rule notification requirement now in effect](#) (May 2024)
- Hub Software scan of public DNS records, 3,612 US tax practices, September 26, 2026



About Hub Software. Hub Software, LLC builds software for small tax and accounting practices: CPA Hub, practice management built around the firm's written security plan and client consent, and WISP Creator, which builds the written information security plan the FTC Safeguards Rule requires.

Questions about this study: Jim Taczy, Founder · jim@cpa-hub.com · 949.288.3022 · cpa-hub.com

Appendix: results by state

44 states with 10 or more firms, largest first. 52 firms in smaller states are counted in the totals but not shown here. Treat states with fewer than 30 firms as a rough indication only.

State	Firms	Publish DMARC	Block fakes	Fully protected
CA	507	63%	36%	32%
TX	265	65%	35%	29%
FL	244	61%	33%	28%
NY	231	69%	36%	31%
IL	162	72%	37%	32%
PA	140	66%	31%	28%
NC	115	62%	22%	19%
WA	115	65%	35%	31%
NJ	111	63%	29%	25%
CO	110	63%	33%	26%
MA	109	67%	39%	30%
MD	102	73%	38%	33%
OH	101	63%	38%	31%
MI	97	67%	45%	37%
GA	94	65%	27%	24%
VA	79	61%	27%	25%
AZ	73	67%	29%	26%
MN	72	62%	30%	27%
OR	66	67%	29%	26%
WI	61	74%	38%	34%
MO	60	67%	40%	38%
UT	56	54%	29%	23%

State	Firms	Publish DMARC	Block fakes	Fully protected
IN	51	76%	45%	37%
KY	44	66%	34%	30%
TN	43	70%	49%	44%
AL	41	71%	34%	27%
SC	41	59%	20%	20%
KS	37	70%	43%	32%
ID	36	56%	33%	31%
NV	34	62%	47%	44%
CT	33	67%	24%	21%
OK	28	64%	29%	21%
LA	26	62%	35%	27%
NE	24	83%	42%	38%
HI	23	61%	30%	26%
MS	20	50%	25%	15%
IA	19	74%	58%	58%
NM	18	39%	22%	17%
RI	16	81%	38%	31%
ME	12	50%	33%	17%
DE	11	73%	45%	36%
MT	10	70%	40%	20%
ND	10	90%	30%	30%
WV	10	60%	30%	20%