+44 204 591 6648

Research report for law firms in London, the South East and the East of England

The Law Firm Fraud and Breach Report 2026

What 998 SRA scam alerts, 1,072 ICO breach reports and the email records of 4,323 firms say about the risks facing firms like yours.

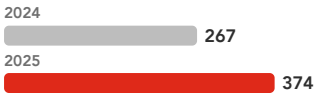
November 2026



AT A GLANCE

Six numbers worth reading before your next partners' meeting

+40%



More SRA scam alerts in 2025 than in 2024: 374, up from 267. 2026 is running at the same higher level.

92%



Of alerts in the last 12 months involved the name of a real, regulated firm or solicitor.

1,072



Data breaches reported to the ICO by the legal sector in the year to September 2026, up 16%. The last two quarters are the highest on record.

37%



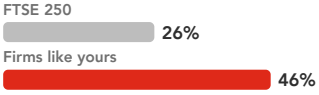
Of those reports reached the ICO more than 72 hours after the firm found the breach.

46%



Of law firms with 25 to 55 staff have email that a criminal can fake in their name.

26%



The same figure for FTSE 250 companies.

How this report was put together

Most of the figures quoted about law firm cyber risk are years old. The "£7m lost to Friday afternoon fraud" line that still does the rounds dates from 2016. So we went back to the raw data.

We counted every scam alert the Solicitors Regulation Authority has online, all 998 of them, back to November 2023. We cut the Information Commissioner's Office breach data down to the legal sector. And on 12 November 2026 we read the public email settings of 4,323 law firms in London, the South East and the East of England. Every figure has its source in the margin beside it. Where a number is our own analysis, the margin says so.

SOURCES

SRA scam alerts. All alerts online at sra.org.uk/consumers/scam-alerts, 1 Nov 2023 to 11 Nov 2026. Counted by AIS Technology.

ICO breach reports. ICO data security incident trends, Q1 2019 to Q3 2026, open data published 26 Oct 2026. Legal sector, one record per report. Analysis by AIS Technology.

Email settings. Public DNS records read by AIS Technology on 12 Nov 2026. The 46% covers 267 firms of 25 to 55 staff with no in-house IT team we could find.

FTSE 250. Red Sift, "FTSE 250 DMARC report", 12 May 2026: 18.8% monitor only plus 7.2% no record.

£7m. Legal Futures, 8 Dec 2016, reporting the SRA.

INSIDE THIS REPORT

01 Someone is using your name 3

02 Breaches at record levels 6

03 Your name in someone else's inbox 9

04 Cost and cover 12

05 Nine things to do 13



PART ONE

Someone is using your name

When fraudsters want a client to send money, they borrow the name of a firm the client already trusts. Each time one of these scams is reported, the SRA publishes a warning. We counted all of them.

998

SRA scam alerts counted, November 2023 to November 2026

415

different firms named in the last two years, 65 of them more than once

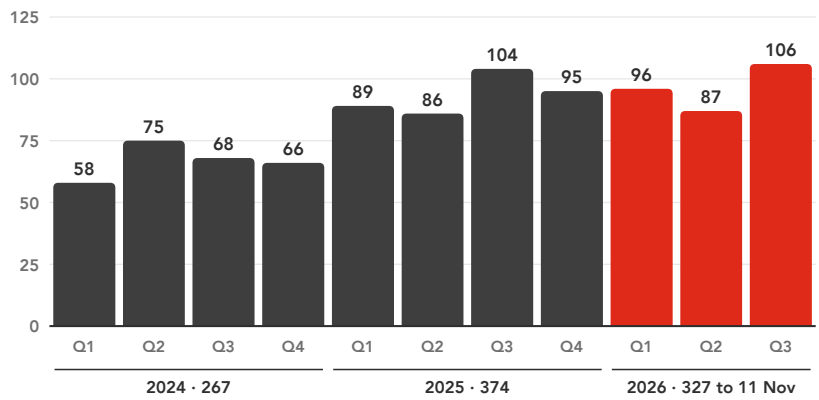
1 in 5

alerts in 2025 involved a property transaction

The jump came in 2025, and it hasn't gone away

The SRA published 374 scam alerts in 2025, 40% more than the 267 it put out in 2024. This year has held at that level: 319 alerts from January to October, against 313 for the same months of 2025. It isn't still climbing. It just hasn't come back down.

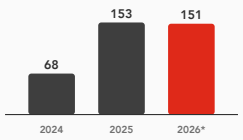
SRA scam alerts published, by quarter



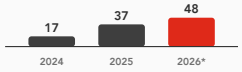
2026 quarters in red. Q4 2026 is not shown because it is incomplete.

The toolkit has changed faster than the total. Alerts that involve a fake website more than doubled in 2025, and WhatsApp turns up in more alerts every year. Email still features in about three alerts out of four.

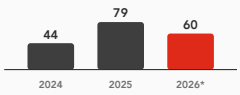
FAKE WEBSITE



WHATSAPP



PROPERTY DEAL



Alerts mentioning each channel or setting. *2026 runs to 11 November. An alert can mention several.

92% of alerts in the 12 months to October 2026 misused a real firm or solicitor. Only 14 described a firm that doesn't exist.

SOURCES

Source. SRA scam alerts, sra.org.uk/consumers/scam-alerts, fetched 12 Nov 2026. 998 alerts, 1 Nov 2023 to 11 Nov 2026. Counted and classified by AIS Technology.

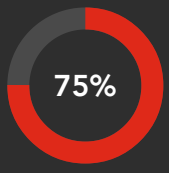
What an alert measures. An alert is a scam someone reported and the SRA wrote up. These figures track reported impersonation, not every attempt.

Channels. Classified by keyword from each alert's text. Email appears in 211 of 267 alerts in 2024 and 282 of 374 in 2025.

92%. 350 of 380 alerts, Nov 2025 to Oct 2026, where the SRA says there is a genuine firm or person whose details were misused.

Older alerts. The SRA removes alerts over time. The NCSC counted 278 published in Jan 2022 to Jan 2023, but those are no longer online, so the series starts in November 2023.

EMAIL IS STILL THE WAY IN



of SRA scam alerts in 2025 involved email: 282 of 374.

One letter is all it takes

Many of the alerts describe a lookalike domain: an email address that differs from the real firm's by a single character. The SRA's alert of 6 November 2026 is typical. It describes emails about a property transaction sent from a domain using an "l" in place of the "i" in the firm's name.

ILLUSTRATION · FICTIONAL FIRM

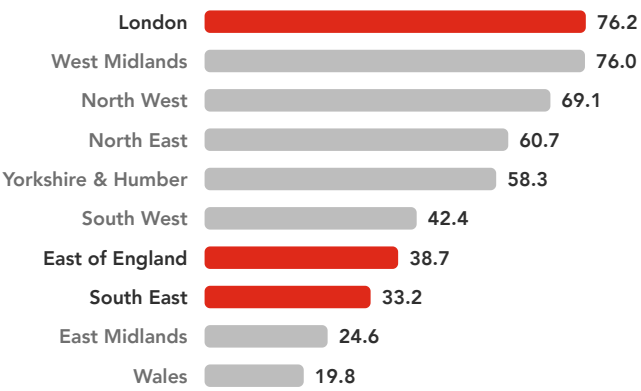
completions@marlowehirst.co.uk	GENUINE
completions@marlowehlrst.co.uk	LOOKALIKE
completions@rnarlowehirst.co.uk	LOOKALIKE

Nothing on your own systems stops a criminal registering a domain like that. What stops the money moving is the person at the other end checking the details before they pay, and your firm telling clients, often and plainly, how you will and won't ask for funds.

Where it happens

London firms are named far more often than anyone else: 76 alerts for every 1,000 firms over two years. The South East and the East of England sit at less than half that rate. Big national firms with London offices push the London figure up, and 415 different firms were named over the period. It happens in every region, to firms of every size.

Alerts per 1,000 SRA-authorised firms, Nov 2024 to Oct 2026



SOURCES

The alert quoted. SRA scam alert, 6 Nov 2026, describing a lookalike domain using "'l' in place of the 'i'". The domains shown here are invented to illustrate the technique.

Regions. AIS Technology analysis. 520 of 740 alerts in the 24 months matched to a firm's head office, using the SRA number, a postcode in the alert or a unique name match. Firm counts from the SRA register, 11 Nov 2026.

Repeat targets. 65 of the 415 firms were named in more than one alert.

Property. A property transaction features in about one alert in five: 79 of 374 in 2025.

NAMED MORE THAN ONCE

65

of the 415 firms named in two years were impersonated in more than one alert.



PART TWO

Breaches are being reported at record levels

A firm must tell the Information Commissioner about a serious personal data breach within 72 hours. The ICO publishes every report it receives as open data. We took out the legal sector and looked at what it shows.

1,072

breach reports from the legal sector in the 12 months to September 2026

354

of them were an email sent to the wrong person, the commonest breach of all

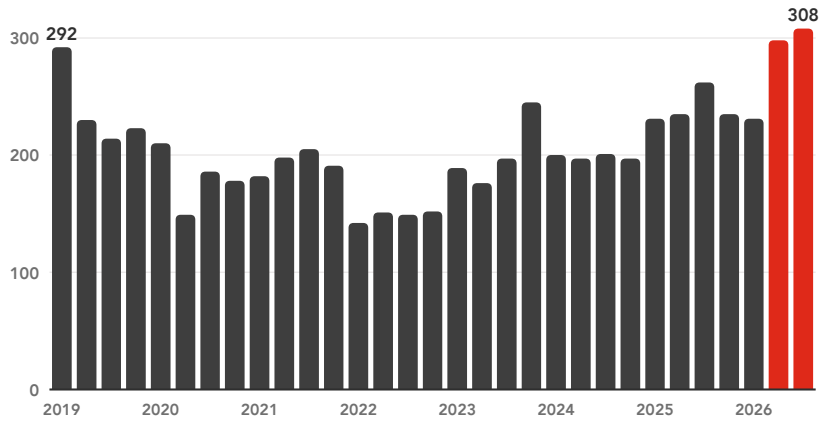
43 days

to report a cyber attack, in a case that cost one firm a £60,000 fine

1,072 reports in a year, and the two busiest quarters on record

The legal sector reported 1,072 breaches to the ICO in the 12 months to September 2026, up 16% on the year before. The two latest quarters, with 298 and 308 reports, are the highest since the data begins in 2019.

Breach reports from the legal sector to the ICO, by quarter



Q1 2019 to Q3 2026. Q2 and Q3 2026 in red.

12 months to September	2025	2026	Change
All reports	925	1,072	**+16%**
Classed by the ICO as cyber incidents	223	271	**+22%**
Email sent to the wrong person	340	354	+4%
Phishing	160	221	**+38%**
Reported more than 72 hours after discovery	331	398	**+20%**

The commonest breach is still an email sent to the wrong person. Phishing is second, and it is rising fast. Then there's the clock: 37% of reports reached the ICO more than 72 hours after the firm found out, which is outside the deadline unless the delay can be explained.

SOURCES

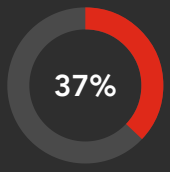
Source. ICO, Data security incident trends, open data file Q1 2019 to Q3 2026, published 26 Oct 2026. Sector "Legal". De-duplicated to one record per report reference, as the ICO advises. Analysis by AIS Technology.

What the data is. Breaches firms chose to report. It shows what is being reported, not everything that happens. The ICO notes its cyber and non-cyber categories are under review.

The 72-hour rule. UK GDPR Article 33: notify "without undue delay and, where feasible, not later than 72 hours after having become aware of it".

Previous peak. Q1 2019, 292 reports.

LATE TO THE ICO



of legal-sector breach reports arrived more than 72 hours after discovery: 398 of 1,072.

Two case files

Both firms were regulated and of a size many readers will recognise. Neither attack needed anything clever.

DPP Law Ltd

Fined £60,000

ICO penalty notice, April 2025 · turnover £3.49m · offices in Bootle, Birmingham, Liverpool, London and Tolworth

19 February 2022
The first of 400 brute-force attempts on an administrator account for a legacy case management system. The account dated from 2001 and had no multi-factor sign-in, because it was a service account.

4 June 2022
The email server stops. Files across the firm's servers are found corrupted.

15 July 2022
The National Crime Agency tells the firm that 32.4GB of its data is on the dark web, including court bundles and police body-camera footage.

17 July 2022
The firm reports the breach to the ICO, 43 days after the attack. It had not realised that losing access to data counted as a breach.

✓ The firm had multi-factor sign-in on its remote access. The way in was an old account nobody was watching.

Levales Solicitors LLP

Reprimanded

ICO reprimand, 2024 · Ash Vale, Hampshire

8,234 people affected, 863 of them judged high risk, with data published on the dark web. The ICO found no multi-factor sign-in on the account that was compromised, and no password policy.

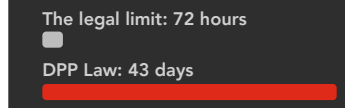
✓ Two basic controls were missing. Neither costs much to put right.

SOURCES

DPP Law. ICO monetary penalty notice, 14 Apr 2025, ico.org.uk. Fine for breaches of UK GDPR Articles 5(1)(f), 32(1), 32(2) and 33(1). Turnover from para. 146; timeline from paras. 18 to 25.

Levales. ICO reprimand, Levales Solicitors LLP, ico.org.uk/media2/k4mlpkrm/levales-reprimand.pdf. Quotes: "8,234 UK data subjects were affected, of which 863 were deemed to be at 'high-risk'"; no "Multi-Factor Authentication (MFA) in place for the affected domain account".

HOW LATE IS LATE?



DPP Law told the ICO 43 days after the attack. The limit is 72 hours.



PART THREE

Your name, in someone else's inbox

One email setting, called DMARC, tells Microsoft, Google and every other provider to reject messages that fake your firm's address. It costs nothing, and anyone can look it up. So we looked it up for 4,323 law firms.

4,323

law firms in London, the South East and the East of England checked on 12 November 2026

95%

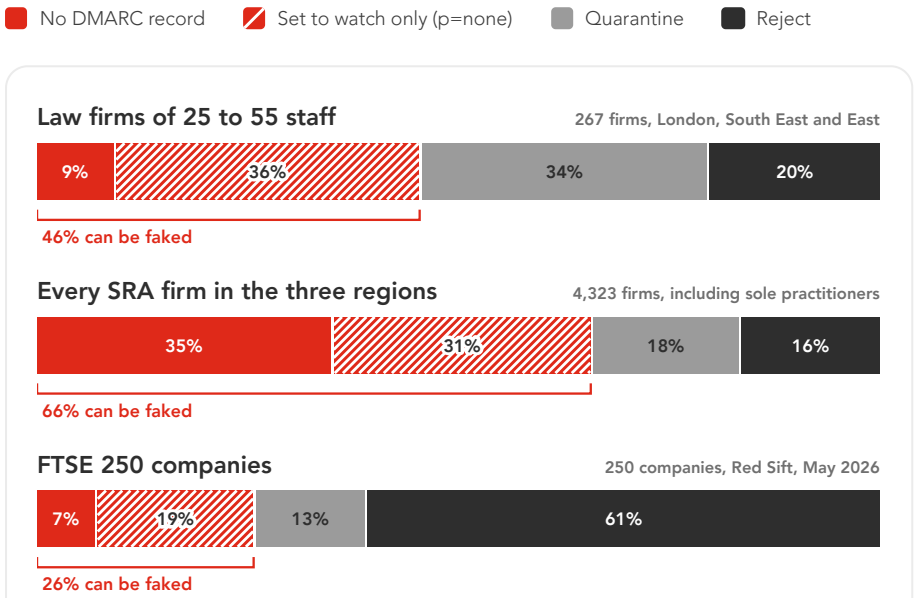
of firms with 25 to 55 staff run their email on Microsoft 365

46%

of those firms have email that can be faked in their name

Almost half of firms like yours haven't switched it on

We looked at 267 law firms with 25 to 55 staff and no in-house IT team that we could find. 46% either have no DMARC record or have it set to "none", which watches and does nothing. Either way, an email can claim to come from the firm's own address and nothing tells the recipient's provider to stop it. For FTSE 250 companies the figure is 26%.



Across every SRA firm in the three regions the figure rises to 66%, mostly because sole practitioners rarely set it up. Two more findings stood out.

44 of 97

firms on "watch only" haven't given an address for the reports. Nobody is watching.

32 of 83

firms paying for an email filter such as Mimecast or Proofpoint can still be faked. A filter guards your inbox. DMARC guards your name in everyone else's.

SOURCES

Method. Public DNS records read by AIS Technology on 12 Nov 2026. Each firm scored on the domain its staff send email from. No firm was contacted and no system was tested.

The 267 firms. Law firms in London, the South East and the East of England with about 25 to 55 staff on LinkedIn and no in-house IT role we could find. 95% run their email on Microsoft 365.

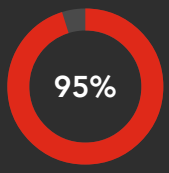
4,323 firms. Every SRA-authorised firm with a head office in the three regions and an email domain on the register.

FTSE 250. Red Sift, 12 May 2026.

Two years ago. A study of 3,964 SRA firms published in Feb 2024 found 2,225 with no DMARC record (Solicitors Journal, 5 Feb 2024). Most firms now have a record. Many stopped at "none".

Snapshot. Settings can change at any time. We publish totals only and never name a firm.

ONE PLATFORM



of firms of 25 to 55 staff run their email on Microsoft 365, where DMARC is a free setting.

What this setting won't do

DMARC stops one trick: email that claims to come from your exact address. It does nothing about a lookalike domain, a client's hacked mailbox, or a phone call from someone pretending to be your conveyancer. Those are behind a lot of the scams in part one.

So treat it as the cheapest fix on the list rather than the whole answer. Each trick has its own defence.

The trick	What it looks like	What stops it
Your exact address, faked	An email that really does show @yourfirm.co.uk as the sender	**DMARC set to reject**
A lookalike domain	One letter changed, or a different ending such as .com for .co.uk	Clients who know you never change bank details by email, and domain monitoring
A hacked mailbox	A real account, yours or a client's, sending real-looking mail	Multi-factor sign-in, and a phone call before any payment

CHECK YOUR OWN FIRM IN TWO MINUTES

01 Open any free DMARC lookup site. MXToolbox has one at `mxtoolbox.com/dmarc.aspx`.

02 Type your email domain: everything after the @ in your own address.

03 Find the value after `p=` in the result and read it against the list below.

p=reject	Fake email using your address is refused. This is where you want to be.
p=quarantine	Fake email goes to junk. Good, and one step from finished.
p=none	Watching only. Nothing is blocked.
Nothing found	No protection at all.

Moving from "none" to "reject" needs care. If a service that sends email on your behalf (your case management system, your accounts package, your marketing tool) isn't set up first, its messages will start to bounce. Read the reports for a few weeks, fix what they show, then tighten the policy.

SOURCES

NCSC. "Having a DMARC policy of 'reject' on all of your domains is the best way to prevent spoofing of your email." NCSC, Email security and anti-spoofing guidance.

Other domains. If your firm uses more than one domain, check each one. In our wider sample, 72% of firms that send email from a second domain left their website's domain open.

THE NCSC'S ADVICE

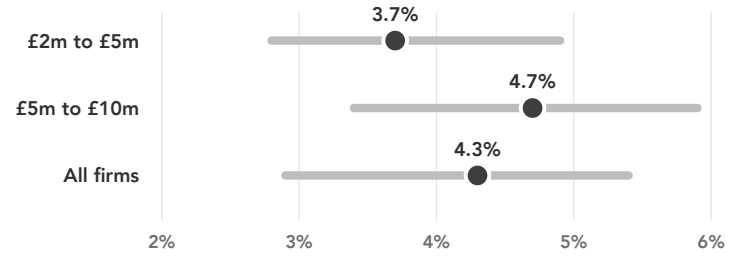
"Having a DMARC policy of 'reject' on all of your domains is the best way to prevent spoofing of your email."

National Cyber Security Centre

IT is now the biggest bill after salaries

The Law Society's 2026 benchmarking survey found that IT costs "have now overtaken everything else" among firms' non-salary overheads, driven by software suppliers consolidating and by spending on AI. Most of the same firms named cyber security as their biggest concern.

IT spend as a share of fee income, by firm turnover



Dot: median. Bar: lower to upper quartile. Includes IT support, consultants and cloud storage.

For a firm turning over £2m to £5m, the median is 3.7% of fee income. On £3.5m, that is roughly £130,000 a year.

Insurance won't cover all of it

Only 28% of firms bought cyber insurance in the Law Society's last survey of the market, in 2023. Brokers say take-up is still low. Even where a policy is in place, the Law Society points out that theft from a firm's office account isn't covered by cyber insurance, and the SRA's minimum terms for indemnity insurance don't include a firm's own losses from a cyber event.

If this happens	Indemnity insurance (SRA minimum terms)	Cyber insurance
Money is stolen from the client account	**Covered**	**Covered**
Money is stolen from the office account	**Not covered**	**Not covered.** Crime (fidelity) cover may be needed
Your own losses from a cyber attack, such as downtime or ransomware	**Not included**	Often, under first-party cover. Check the wording.

Insurers are also asking harder questions. Some now ask what a firm has done to protect itself against scams, including its security, its IT systems and any cyber accreditations it holds.

SOURCES

Benchmark. Law Society, Financial Benchmarking Survey 2026 (Hazlewoods, Leadership and Management Section), 121 firms. Quotes from the survey text; percentages from Figure 6.12.

£130,000. Our arithmetic: 3.7% of £3.5m.

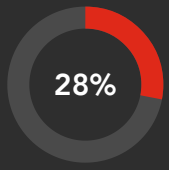
28%. Law Society, "Cyber insurance for law firms", citing its 2023 PII research. No newer survey has been published.

Cover table. Law Society, same page: "A cyber policy and the organisation's PII policy will cover theft from the client account. However, it will not cover theft from the office account." The SRA's minimum terms "don't include first-party losses resulting from a cyber event." General guidance only; your policy wording decides.

Take-up. Howden, April 2026 solicitors' PII renewal review, 7 May 2026: "adoption of cyber insurance remains low amongst the legal profession".

Concern. SRA research "Risk in the legal profession", Dec 2024: 58% of solicitors at firms turning over £500k to £10m see cybercrime as a risk to their firm, against 40% at smaller firms. 515 solicitors, fieldwork Sept to Dec 2023.

CYBER COVER



of firms bought cyber insurance in the Law Society's 2023 survey, the latest there is.

PART FIVE · WHAT TO DO

Nine things, in the order we'd do them

This week

- **Look up your DMARC setting.** Two minutes, using the steps in part three.
- **Search the SRA scam alerts for your firm's name.** If someone is already using it, you want to know before a client does.
- **Check multi-factor sign-in covers every account.** Include admin, shared and service accounts, and anything set up years ago. That is how DPP Law was breached.

This month

- **Write down the bank details rule.** Your firm never changes its bank details by email, and staff never act on an emailed change without calling a number already on file. Then tell every client, in writing, at the start of every matter.
- **Decide who reports a breach.** Name the person who decides whether the ICO must be told, and their deputy. 37% of legal-sector reports are late.
- **Register the obvious lookalikes of your domain,** or set up monitoring so you hear when someone else does.

This quarter

- **Take DMARC from "none" to "reject".** Read the reports, fix the services that send email for you, then tighten the policy.
- **Run phishing training with a real test.** Phishing reports to the ICO from law firms are up 38% in a year.
- **Close the old doors.** List every system and account that is still switched on but no longer used, and switch it off.

SOURCES

SRA scam alerts. sra.org.uk/consumers/scam-alerts. The page has a keyword search.

A plan template. AIS Technology's free business continuity plan template includes a section on declaring an incident and the 72-hour rule: aistech.co.uk/guides.

Cyber Essentials. The government-backed scheme covers several of these controls, including multi-factor sign-in and removing unused accounts. ncsc.gov.uk/cyberessentials.

TALK IT THROUGH

020 4591 6648

If something in this report raised a question about your own firm, call AIS Technology. We're happy to talk it through.

info@ais.london · aistech.co.uk

SOURCES AND METHOD

Where every number comes from

SRA scam alerts. sra.org.uk/consumers/scam-alerts, fetched 12 Nov 2026. 998 alerts dated 1 Nov 2023 to 11 Nov 2026, collected month by month with the page's own date filter and each alert's detail page read. Channels and settings classified by keyword. Regions matched to the SRA register by SRA number, postcode or unique name; 70% of alerts in the two-year window matched. Analysis by AIS Technology.

SRA register. SRA Data Share API, pulled 11 Nov 2026: 8,871 authorised firms, 4,669 with a head office in London, the South East or the East of England. Regions from postcodes.io.

ICO breach data. ico.org.uk/action-weve-taken/data-security-incident-trends, open data file Q1 2019 to Q3 2026, updated 26 Oct 2026. Sector "Legal". One record per report reference. Analysis by AIS Technology.

DPP Law Ltd. ICO monetary penalty notice, 14 Apr 2025.

Levales Solicitors LLP. ICO reprimand, 2024.

Email settings. Public DNS lookups (DMARC, SPF, MX) through public resolvers on 12 Nov 2026, by AIS Technology. 267 law firms of 25 to 55 staff, and 4,323 SRA firms in the three regions. Results published as totals only. A setting shows what a firm has told other providers to do; it doesn't prove that a given fake email would arrive, because Microsoft and Google run their own checks too.

FTSE 250. Red Sift, "FTSE 250 DMARC report", 12 May 2026.

2024 study. Solicitors Journal, "Legal IT audit reveals significant flaws in law firm security", 5 Feb 2024.

NCSC. Email security and anti-spoofing guidance, ncsc.gov.uk.

Law Society. Financial Benchmarking Survey 2026; "Cyber insurance for law firms", updated 2026, citing 2023 PII research.

Howden. "1 April 2026 solicitors' PII renewal review", 7 May 2026.

SRA research. "Risk in the legal profession", BMG Research for the SRA, published 13 Dec 2024, 515 solicitors.

Legal Futures. "Friday afternoon fraud cost profession at least £7m", 8 Dec 2016. Quoted only to show its age.

NCSC. Cyber threat report: UK legal sector, June 2023, for the count of alerts published in 2022.

A note on the sample. The 267 firms are law firms in London, the South East and the East of England with roughly 25 to 55 staff on LinkedIn and no in-house IT role that we could find. They are not a random sample of all UK law firms.

This report is general information and isn't legal advice. Figures are correct as at 12 November 2026.

HOW THE NUMBERS WERE BUILT

998

Alerts read

Every SRA scam alert online, November 2023 to November 2026, each detail page read and matched to the register.

89,591

Reports filtered

The ICO's full breach file, one record per report, cut down to the 1,072 legal-sector reports in the latest year.

4,323

Domains checked

Public email settings for every SRA firm in London, the South East and the East of England, read on 12 November 2026.



ABOUT AIS TECHNOLOGY

IT support and cyber security for firms that don't have an IT department

AIS Technology looks after the IT of professional firms across Essex, London and the South East: Microsoft 365, cyber security, a 24/7 help desk and on-site engineers. Our founder, Chris Dunham, worked in network security for the Home Office and for financial institutions before starting AIS.

We help our managed clients reach Cyber Essentials and Cyber Essentials Plus, and we help firms put the controls in this report in place, from DMARC to multi-factor sign-in.

If anything in this report raised a question about your own firm, call us. We're happy to talk it through.

CALL

020 4591 6648

EMAIL

info@ais.london

WEB

aistech.co.uk

AIS TECHNOLOGY

The Law Firm Fraud and Breach Report 2026. Published by AIS Technology, Wickford, Essex, November 2026. This report includes data supplied by the Solicitors Regulation Authority (sra.org.uk/sra/how-we-work/web-service/attribution.page). Contains public sector information licensed under the Open Government Licence v3.0. Images are illustrative. This report is general information and isn't legal advice.