



# Three Quarters of 317 Million Graded Domains Fail Basic Security Checks

*The September 2026 Defaults Exposed census grades 316.6 million domains against 34 checks covering email, encryption, DNS, and web security.*

RAS AL-KHAIMAH, RAS AL-KHAIMAH, UNITED ARAB EMIRATES, September 8, 2026 /EINPresswire.com/ -- [Defaults Exposed](#), the independent domain security census, today published its September 2026 edition. The census scanned 347,691,016 domains and graded 316,600,902 of them. It found that 74.2% score a failing grade, and that most of those domains are exposed on more than one front at once.

The grade is a composite. Every domain is checked against 34 measures across five areas: email authentication, TLS and certificates, web security, DNS, and infrastructure. Twenty-five of the 34 count toward the score. A domain scoring below 60% receives an F, and one scoring 95% or above receives an A+. Reaching an F takes failures across several checks rather than one, because no single check is weighted heavily enough to drop a passing domain that far on its own. As of 5 September 2026, 234,955,475 domains, 74.2% of every domain graded, score F.

Where domains fall short

The failures are spread across the whole grade, not concentrated in one control.

A third of graded domains do not serve their website over HTTPS at all. Among those that do, 89.1% present a valid, trusted certificate, which leaves about 40% of all graded domains without one, so a visitor's browser cannot confirm it has reached the real site.

On the email side, 75.2% publish no DMARC record, the setting that lets a receiving mail server reject a message forged to look like it came from the domain, and only 11.6% publish an enforcing policy. A related gap sits in SPF, which 46.4% of domains publish in a valid form.

In DNS, 6.86% of domains have a working DNSSEC chain, the protection that stops an attacker pointing the domain at a fake copy of its site; the other 93% do not. Only 1.4% publish a CAA record limiting which authorities may issue certificates in their name.

On the web itself, of the 125.8 million domains whose page answered a request directly, fewer than one in five send the browser-hardening headers that blunt common attacks: 17.8% send X-

Content-Type-Options, 15.3% send clickjacking protection, 10.1% send a Content-Security-Policy, and 7.91% send a Referrer-Policy.

## What the email gap costs

Of these gaps, email forgery is the one with the clearest measured cost. A domain that publishes DMARC at p=none, the monitoring-only setting that 53% of domains with a record still use, asks the world's mail servers to deliver a forged message rather than block it. Across the census, 94.3% of the 233,574,031 domains that scored F fail the DMARC policy check.

The FBI's Internet Crime Complaint Center logged 21,489 business email compromise complaints in 2023, with \$2,946,830,270 in adjusted losses, an average of about \$137,000 per complaint. Business email compromise relies on a recipient trusting an email that appears to come from a known sender, and a domain that does not enforce DMARC offers no defence against the exact-domain impersonation these schemes use.

## The technical picture at a glance

Across the 316,600,902 graded domains, as of 5 September 2026:

74.2% score F (234,955,475 domains)

67.0% serve content over HTTPS, of which 89.1% present a valid, trusted certificate

46.4% publish a syntactically valid SPF record

11.6% publish an enforcing DMARC policy of p=quarantine or p=reject

6.86% have a valid, fully validating DNSSEC chain

Of the 125.8 million domains whose page answered directly, 12.7 million (10.1%) send an effective Content-Security-Policy header.

The aggregate dataset, with per-check and per-TLD figures, is at [defaults.exposed/v10/data](https://defaults.exposed/v10/data). The full methodology, with a citable page for every check, is at

<https://defaults.exposed/methodology>

## Checking and fixing a domain is free

Anyone can [check a domain](https://defaults.exposed) at <https://defaults.exposed>. The free scan runs the same 34-check engine as the census, returns a grade from A+ to F in about a second, and requires no account and no email address. The result names what failed in plain English, and every check has a free how-to fix guide at [defaults.exposed/fix](https://defaults.exposed/fix), with the exact record or header to publish. Most of the fixes are a single DNS record or one line of web-server configuration, and they cost nothing to apply.

## About Defaults Exposed

<https://defaults.exposed> is an independent domain security census and grading service operated by Defaults Exposed FZ-LLC (trade licence no. 47034427), Ras Al Khaimah Economic Zone, UAE. The census runs monthly. Its census data is stored and processed within the EU. The service publishes aggregate patterns only; it never publishes a list of named domains with their grades, and a single domain's grade is shown only to whoever runs the free scan of it. The current census data and full methodology are at [defaults.exposed](https://defaults.exposed).

Media contact [press@defaults.exposed](mailto:press@defaults.exposed)

Notes to editors

All figures in this release are from the September 2026 census, as of 5 September 2026. Census numbers update monthly, and the current figures are always at <https://defaults.exposed/data>.

Shares for the header checks (Content-Security-Policy and the other browser-hardening headers) are taken over the 125,815,036 domains whose page returned a direct response, the only ones on which those checks run. Every other share is taken over the 316,600,902 graded domains. Each figure names its base on the site.

The FBI Internet Crime Complaint Center figures (21,489 business email compromise complaints, \$2,946,830,270 in adjusted losses, 2023) are from the IC3 2023 Internet Crime Report, published by the Federal Bureau of Investigation and available at [ic3.gov](https://ic3.gov).

The free domain scan at <https://defaults.exposed> runs the same 34-check engine as the census, returns a grade from A+ to F, and requires no account or email address. A plain-English fix guide for every check is published at <https://defaults.exposed/fix>.

[press@defaults.exposed](mailto:press@defaults.exposed)

Defaults Exposed

[press@defaults.exposed](mailto:press@defaults.exposed)

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[Facebook](#)

[YouTube](#)

[TikTok](#)

[X](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/940557044>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.