

CREATIVE/STUDIO

WEBSITE & EMAIL SECURITY SNAPSHOT

CREATIVESTUDIO.GROUP

Sample report. We ran our own \$99 Snapshot on our own domain so you can see exactly what you get. Every result below is real.

SAMPLE REPORT · OUR OWN SITE

DOMAIN

creativestudio.group

CHECKED

19 October 2026, 07:12-07:20
UTC

METHOD

Passive, public checks only

SUMMARY



Short version: the encryption (SSL/HTTPS) is excellent and the email domain is set up, but the website doesn't send most of the browser security headers, and our DMARC policy only watches, so it doesn't block anyone faking our address. None of this is an emergency. All of it can be fixed in about an hour.

SSL / HTTPS		A+ (SSL Labs)
Security headers		C, 50/100 (Mozilla)
Email authentication		2.5 of 3
DNS hardening		1 of 2 (2 warnings)

How the score works: we run 15 checks. A pass scores 1 point, a warning ½ point, a fail 0. Result: 8 passes, 5 warnings, 2 fails = 10.5 / 15 = 70 / 100. Grade bands: A 90+, B 80+, C 70+, D 60+, F below 60.

ALL CHECKS AT A GLANCE

CHECK	RESULT	WHAT WE SAW
SSL certificate	PASS	Let's Encrypt (ECDSA P-256), covers creativestudio.group and www, valid until 14 Jan 2027
TLS versions	PASS	Only TLS 1.2 and 1.3 offered. SSL Labs grade A+, no Heartbleed/POODLE
HTTP → HTTPS redirect	PASS	Mozilla Observatory: redirects to HTTPS. www redirects (301) to the main domain
HSTS	PASS	max-age=31536000 (1 year). No includeSubDomains or preload
Mixed content	PASS	0 insecure http:// resources on the homepage
Content-Security-Policy	FAIL	Header not sent
Clickjacking protection	FAIL	No X-Frame-Options and no CSP frame-ancestors

X-Content-Type-Options	WARN	Header not sent (failed in Observatory, low impact on a static site)
Referrer-Policy	WARN	Header not sent (browser default applies)
Permissions-Policy	WARN	Header not sent
SPF	PASS	<code>v=spf1 include:_spf.mail.hostinger.com ~all</code>
DKIM	PASS	Selector <code>hostingermail-a</code> publishes a 2048-bit RSA key
DMARC	WARN	<code>v=DMARC1; p=none</code> , monitoring only, no report address
CAA record	WARN	None published
DNSSEC	WARN	Not enabled (no DS record)

Also confirmed: mail is handled by Hostinger (MX: mx1/mx2.hostinger.com). The website is hosted on Netlify.

FINDINGS AND HOW TO FIX THEM

1. No Content-Security-Policy

MEDIUM

WHAT IT MEANS A CSP is a list that tells browsers which sources of scripts, styles and fonts your site is allowed to load. Without one, if a bad script ever gets onto the page (through a compromised plugin, a widget, or a form bug), the browser runs it without question, and it could steal form entries or redirect visitors.

HOW TO FIX Add a `Content-Security-Policy` header that allows only our own domain plus Google Fonts. Test it on a staging copy first so nothing breaks.

2. No clickjacking protection

MEDIUM

WHAT IT MEANS Any other website can load our pages inside an invisible frame and trick visitors into clicking things they can't see, like our contact form button. It's an old trick, but it's still used in phishing.

HOW TO FIX Send `X-Frame-Options: DENY` and `frame-ancestors 'none'` in the CSP.

3. DMARC is set to "watch only"

MEDIUM

WHAT IT MEANS We have a DMARC record, which keeps us inside Gmail's, Yahoo's and Outlook's rules. But `p=none` tells them to deliver fake emails "from" @creativestudio.group anyway, and with no report address we would never hear about it. A scammer could email our clients pretending to be us.

HOW TO FIX Add a report address (`rua=`) and watch the reports for 2–4 weeks. Once everything legitimate passes, move to `p=quarantine` , then `p=reject` .

4. Missing smaller security headers

LOW

WHAT IT MEANS `X-Content-Type-Options` , `Referrer-Policy` and `Permissions-Policy` aren't sent. Each one closes a small gap: browsers guessing file types, our page addresses leaking to other sites, and unused features like camera or microphone being available to scripts. They're cheap to add, and security scanners and insurers look for them.

HOW TO FIX Add all three headers in the host's config file (shown on the next page).

5. No CAA record

LOW

WHAT IT MEANS A CAA record lists which companies may issue SSL certificates for our domain. Without one, any certificate authority can issue one, which makes it slightly easier for a mistake or a scam to produce a valid-looking certificate for our name.

HOW TO FIX Add a DNS record `CAA 0 issue "letsencrypt.org"`, matching the issuer we use today.

6. DNSSEC off, and HSTS could go further

INFO

WHAT IT MEANS DNSSEC signs our DNS answers so they can't be forged in transit. HSTS already forces HTTPS for a year. Adding `includeSubDomains` and joining the browser preload list would protect visitors on their very first visit too.

HOW TO FIX Turn on DNSSEC in the DNS provider's panel (one click at most registrars). Extend HSTS once we've confirmed every subdomain works over HTTPS.

What's already good

- SSL Labs **A+**: modern TLS only, strong certificate, forward secrecy.
- All traffic is forced to HTTPS, and HSTS is on for a year.
- No mixed content, so the padlock never breaks.
- SPF and DKIM are both in place, so our real emails are authenticated.

HOW WE CHECKED

Passive checks only. We read what the domain already shows to everyone:

- Public DNS lookups for MX, SPF, DKIM, DMARC, CAA, DS and NS records.
- One normal page request, to read the response headers and check for mixed content.
- A TLS handshake to read the certificate.
- Qualys SSL Labs, with results kept off the public boards.
- Mozilla HTTP Observatory.

No attack tools, no login attempts, no scanning of ports or folders. Blacklist and breach lookups are part of the paid Snapshot but weren't included in this sample. Results reflect 19 Oct 2026 and can change whenever the site or DNS changes.

WHAT THE FIX PACK (\$349) WOULD DO HERE

Email

Add DMARC reporting, review 2–4 weeks of reports, then move to `p=quarantine` and `p=reject` so spoofed mail gets blocked. Double-check that SPF and DKIM pass for every service that sends as us.

Security headers

Add CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy and Permissions-Policy, then test every page and form so nothing breaks.

DNS

Add a CAA record for Let's Encrypt and switch on DNSSEC.

Proof

Re-run every check and send a before/after report. The target is Mozilla Observatory A or better while keeping SSL Labs at A+.

For this site (hosted on Netlify), the header fix is one small config file:

```
/*
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=()
Content-Security-Policy: default-src 'self'; script-src 'self';
  style-src 'self' https://fonts.googleapis.com; font-src https://fonts.gstatic.com;
  img-src 'self' data:; form-action 'self'; frame-ancestors 'none';
  base-uri 'self'; object-src 'none'
```

And one DNS change for DMARC:

```
_dmarc TXT "v=DMARC1; p=none; rua=mailto:dmarc@creativestudio.group; fo=1"
(after 2–4 clean weeks → p=quarantine → p=reject)
```

On WordPress, the Fix Pack also covers updates, removing unused plugins and themes, Wordfence, 2FA for admins, and turning off XML-RPC and file editing. On Shopify and Wix, it covers account security and the email DNS records.

Want this for your domain? Email julia@creativestudio.group with your domain name. Snapshot \$99, delivered in 48h, fully credited if you upgrade to the Fix Pack within 14 days.

Julia, Creative Studio · <https://creativestudio.group/security.html>