This is a dated observation of publicly visible information. It is not a security audit within the meaning of the Estonian Cybersecurity Act, and not a penetration test. We do not log in, submit forms or attempt to bypass any protection.



**Real public observations — bounded sample, not a whole-site assessment.**

# Bounded public security review · oej.ee

**Main finding** **Your domain doesn't ask mailboxes to stop forged email.** Your DMARC rule is in monitoring mode only (p=none).

**24 of 29 checks · 27 Oct 2026**

16 complete · 8 partial or inventory · 5 not assessed

### Security at a glance

## Good. One finding needs review: protection against email spoofing.

The OEJ check score starts at 100 points, and every finding takes points off.

The score is based on 24 of the 29 checks. It is not a certificate.

Your result: 100 − 20 × 1 = 80. Levels: 90–100 Very good · 75–89 Good · 60–74 Fair · 40–59 Poor · 0–39 Weak.

“Needs review” costs 20 points: worth changing, but not high severity (see the method page).

## Status by area

Half-filled segment: a partly assessed check

**Connection & certificate** — Partly assessed
No findings in the connection checks. Partly assessed: connection versions (TLS).

**Email spoofing protection** — Needs review
Needs review: forged email rule (DMARC).

**Browser security settings** — Partly assessed
No findings in the browser settings checked. Partly assessed: script rule (CSP).

**Public information & contact** — Partly assessed
No findings in the public information checks. Partly assessed: domain signature (DNSSEC).

**Public code** — Partly assessed
No findings in the public code checked. Partly assessed: secrets in code, source maps, external scripts, JavaScript libraries, login.

**Not assessed in this version** — Not assessed
No results for these checks.

Each segment is one check. “No findings” applies only to the checks we ran.

**Summary 1 finding needs work.** A finding does not mean anyone has attacked your site. It shows what is worth putting right.

**1 finding needs review. This sample cannot show how well the whole website is protected.**

## What to do first

1. **Your domain doesn't ask mailboxes to stop forged email.** Ask your email administrator to read the DMARC reports for a few weeks, then tighten the rule (p=quarantine).

   Who and how long: email administrator with your DNS administrator · about 30 minutes with the mail provider or DNS administrator for each DNS change, then 2–4 weeks of reading reports before each tightening step (about 2–4 weeks to reach p=quarantine; a later move to p=reject, if chosen, takes longer). · When: Start within two weeks

   How to verify the fix: Look up the TXT record at _dmarc.oej.ee again: exactly one v=DMARC1 record with p=quarantine or p=reject and without t=y.

   **→ Technical appendix, card A1**

When the fixes are done, run your free re-check (until 26.11.2026). You'll see in writing whether the fixes work. For DMARC, the re-check confirms the step you have reached by then (for example p=quarantine). Whether to go on to p=reject is your decision with your email administrator; that step can take longer.

## Findings in detail

**Needs review** Start within two weeks

### Your domain doesn't ask mailboxes to stop forged email

`DMARC · p=none`

**What it means**

Your DMARC rule is in monitoring mode only (p=none). It does not ask mailboxes to hold back email that fails the check, even when it shows your address as the sender.

**Why fix it**

If someone sends email that shows your address as the sender, your domain does not ask mailboxes to hold it back.

> *p=none asks for no extra handling when a message fails DMARC; the receiving provider still decides.*

**→ Technical appendix, card A1**

## What is in good shape

- ✓ The HTTPS certificate passed the connection check (trusted issuer, matching name, within its dates).
- ✓ The unencrypted homepage address (http://) redirects to the secure one.
- ✓ The site sends browsers an HTTPS-only instruction (HSTS).
- ✓ An SPF record of allowed senders is published, and no syntax errors were found in it.
- ✓ Email signing keys (DKIM) were found at the selector names we looked up.
- ✓ The checked response limits which sites may show the page in a frame (frame-ancestors or X-Frame-Options).
- ✓ The checked response tells browsers not to guess file types (nosniff).
- ✓ The checked response sets a referrer rule (Referrer-Policy).
- ✓ A browser-permissions rule (Permissions-Policy) is published.
- ✓ A security contact file (security.txt) with a contact and an expiry date is published.
- ✓ A report address for failed email connections (TLS-RPT) is published.

## What we saw but did not fully assess

- Successful connections: TLSv1.2, TLSv1.3; we did not test whether older versions are refused.

- A DNS resolver reported a signed answer for your domain's key records (DNSKEY); we did not validate the signatures ourselves.
- The domain publishes no certificate issuing rules (CAA); this check does not count that as a weakness.
- No secret-key patterns were found in the public code we sampled; other files were not read.
- No source map references were found in the checked code; we did not request map files.
- The page declares a script rule (CSP); we checked it only for a few unsafe script settings, not its other rules.
- The checked response sends Access-Control-Allow-Origin: *. Browsers then let scripts on any website read responses to requests made without cookies or other credentials; it does not open responses to credentialed requests. This header does not control whether requests can be sent. This version does not assess that value.
- The checked response names its server software (cloudflare); this version does not assess software versions.
- The MTA-STS policy is published in testing mode (mode: testing): it helps find connection problems but does not yet ask senders to refuse unencrypted delivery.
- Scripts declared in the homepage HTML: 2, from other websites: 0. We did not run or judge them.
- No library versions were named in script addresses; libraries not named there were not checked.

### Scope and limits

Observed at: 27 October 2026, 02:10 (Tallinn time, UTC+02:00)

Method version: oej-security-check-2026-10-26 (rules public-security-v2, 29 checks; DMARC RFC 9989, May 2026).

Scope: public root responses, mail/DNS policy and two modern TLS offers. We read static HTML without executing it. Actual evidence and gaps are listed below. No login, forms, application attacks, external scripts or consent behavior were tested.

Check status: 16 fully done, 8 partly done, 5 not done. Not assessed does not mean a problem.

Why 5 checks are not assessed: 2 need separately agreed and authorised testing; 3 are not in this version yet. Not assessed is not evidence of danger or safety. “No findings” covers 23 checks, 8 of them partly done or inventory-only; it does not mean 23 security checks passed.

## Email signing keys (DKIM)

We looked up the selector names that mail providers most often use (brevo1, brevo2, google, selector1, selector2, default, k1, s1):

- `brevo1` — Key syntax observed without an error in the bounded parser. Verify a real signed email with the provider; this is not proof of working message authentication.
- `brevo2` — Key syntax observed without an error in the bounded parser. Verify a real signed email with the provider; this is not proof of working message authentication.

Only the names listed above were looked up. Other selectors and signed-message validation were not tested.

### Important limits

Not assessed does not mean a problem. DNSSEC is resolver-reported, not independently cryptographically validated. Legacy TLS rejection, pre-consent browser behavior, login and application access control remain unproven.

### Not assessed in this version

These conditions are not reported even when present, so their absence from this page does not mean they are fine:

> - HSTS lifetime: only whether a positive max-age is declared was checked; a short lifetime (for example below six months) is not reported.
> - security.txt: the local representation/Contact/Expires subset is assessed at observation time; contact reachability, soft 404 controls, signatures and full RFC conformance remain untested.
> - DNSSEC: whether the domain is signed is not graded; an unsigned domain is not reported.
> - Software versions in Server or X-Powered-By headers are not graded or reported.

No changes to the website. Original evidence is kept privately; hashes refer to it. Detailed evidence is in the separate technical appendix and matching report JSON.

### What we did not look at

- Hidden files on the server, such as backups: needs separately agreed and authorised testing.
- The application's internal logic and injection flaws: needs separately agreed and authorised testing.
- Cookie and tracking behaviour before consent: not in this version yet.
- Lookalike domains that someone could use to mislead your customers: not in this version yet.
- Subdomains listed in public certificate logs: not in this version yet.
- Not in this check's scope: logging in, filling in forms, and services on other domains, such as payment or booking systems.
- Server settings and installed plugin versions cannot be determined from this capture.

---

**OEJ OÜ · Meelis Sootalu · info@oej.ee · +372 5846 0000**

Want us to make the fixes for you? Write or call – we send a quote within one business day.

## Technical appendix

The full cards are in the technical appendix PDF.

A1 · Email spoofing policy (DMARC)

Sharing copy: credential and CSP nonce values are redacted. Original evidence is kept privately. Source hashes refer to the original bytes, not this sharing copy.