

Checkliste: SEO & Sicherheit

1. Check Security Headers

X-Content-Type-Options present?

Set header: X-Content-Type-Options: nosniff

X-Frame-Options configured?

Recommended: SAMEORIGIN

Content-Security-Policy in place?

At least: default-src 'self'; allow others explicitly

Referrer-Policy enabled?

Recommended: strict-origin-when-cross-origin

HSTS configured?

Use header: Strict-Transport-Security with max-age & includeSubDomains

2. Secure Content & Resources

All resources loaded via HTTPS?

Do not embed HTTP content on HTTPS pages

External content with Subresource Integrity?

Use integrity attribute for external JS/CSS

Any HTTP links (internal or external)?

Replace with https:// where possible

Scripts from trusted sources?

Only load verified and necessary third-party scripts

Content-Security-Policy restricting sources?

Use CSP to define trusted content sources

3. Secure Forms & Data Submission

Forms only available via HTTPS?

Page and form action must use HTTPS

Browser warnings present?

Avoid mixed content or insecure form submissions

No sensitive data in referrer?

Set a proper Referrer-Policy

Google reCAPTCHA properly embedded?

Load via HTTPS and match CSP rules

External form services using HTTPS?

Only use providers that serve over HTTPS

4. Safe Link Structure

External links with target='_blank' secured?

Always use rel='noopener noreferrer'

HTTP redirects to HTTPS in place?

Set up 301 redirects for all HTTP requests

Canonical tags use HTTPS?

Canonical URLs should always be HTTPS

Sitemap uses HTTPS URLs?

Only include HTTPS links in your XML sitemap

target='_blank' links protected?

Prevent reverse tabnabbing via rel='noopener' or 'noreferrer'