

HTTPS Self-Check

Companion worksheet to "Why HTTPS Is a Non-Negotiable Starting Point"

HTTPS is invisible when it works and costly when it does not: browsers flag an insecure site as "Not Secure" right where visitors see it. Run these checks yourself in a few minutes, and if any fail, hand the result to your site platform or hosting support, who resolve this routinely.

1. Run the three checks

Open your site in a browser and work through all three. Check the box only when it passes.

☐ Certificate is present and valid

Click the site information icon just left of the web address. A warning means the certificate is expired, mismatched, or broken.

☐ The site auto-redirects HTTP to HTTPS

Type the `http://` version of your address. It should switch to `https://` on its own. If it loads as HTTP, the setup is incomplete.

☐ No mixed content in the page source

Right-click, choose View Page Source, and search for `http` without the `s`. Any results point to mixed content somewhere on the page.

2. Hunt the mixed content

A page can read as secure while individual elements still load over HTTP. Count what you find in each common hiding spot.

Old image URLs in older blog posts _____

Third-party widgets (reviews, MLS, social, analytics) _____

External font or script libraries _____

3. Note what to hand off

HTTPS clears the lowest bar; it does not fix speed, sitemaps, or schema. For anything that failed above, write the specific item to send to your platform or hosting support.

The exact issue and which page or element it appears on:

4. Your commitments

Turn the check into three concrete moves.

This week.

Click the site information icon and confirm HTTPS is present with a valid certificate. What I found:

This month.

Run all three checks, and if any fail, send the specifics to your platform or hosting support. First item to send:

Ongoing.

Each time you add content, confirm new images, scripts, and widgets load over HTTPS. The publishing habit I will keep:
