Website Health & Security Checkup

aztc.it

November 17, 2026 at 3:34 PM (Arizona time) | Prepared for Sample Report



A

Grade

Your checkup at a glance

0	critical
0	fix now
4	fix soon
3	notes
22	looking good

A read-only check of your public homepage, security settings, email protection and public unsafe-site lists. We never log in, never test passwords and never change anything.

Executive summary

aztc.it is in good shape: no critical issues, not flagged by the unsafe-site lists we checked, and modern encryption. The remaining 4 items are tightening, with no visible change to the site.

Category (points)	Result	Summary
Blacklist & Safe Browsing (15 / 15)	GOOD	Not flagged by the unsafe-site lists we could check
Secrets & exposed files (20 / 20)	GOOD	No problems found
Encryption (18 / 20)	FIX SOON	Strict HTTPS rule
Email spoofing protection (16 / 20)	FIX SOON	SPF; DMARC
Browser protections (13.8 / 15)	FIX SOON	Content rule
Software & domain (10 / 10)	GOOD	No problems found

Fix order

Fix	Priority	Effort | Who usually does it
1. Strict HTTPS rule (HSTS)	FIX SOON	20 min | Web host or developer
2. SPF (allowed senders)	FIX SOON	10-20 min | Whoever manages your DNS

Book a free 15-minute review Call (888) 512-9899

Fix	Priority	Effort | Who usually does it
3. DMARC (policy)	FIX SOON	15 min + 2-week wait | Whoever manages your DNS
4. Content rule (CSP)	FIX SOON	45 min | Developer
5. Encrypted delivery rules (MTA-STS) and reports (TLS-RPT)	NOTE	30 min | DNS + web host
6. Security contact file	NOTE	10 min | Developer

Blacklist & Safe Browsing

Checked November 17, 2026 at 3:34 PM (Arizona time). Browsers, search engines and email filters check these lists before showing your site. A listing shows visitors a full-page warning, and email with your links gets filtered. Site Watch repeats this every week and alerts you the same day if any list adds your site.

List	Result	What we found
Malware-blocking public DNS	GOOD	Your domain resolves normally on a security filtering resolver.
Spam and phishing domain list (URI list)	GOOD	Not listed.
Community phishing feed	GOOD	Not in today's public feed.
Google's unsafe-site list (used by Chrome, Safari, Firefox)	GOOD	No unsafe content found. Google's public status lookup
Microsoft's browser warning list (Edge)	NOT CHECKED	There is no public lookup, so we check it by hand when you book a review. Site Watch members get it checked each month.
Domain reputation list (spam blocklist)	NOT CHECKED	Needs a registered data feed; checked by hand in a review.

Secrets & exposed files

Keys, passwords and private files that anyone can download. These are the issues attackers look for first.

Check	Result	What we found
Cross-site data sharing (CORS)	GOOD	No sharing headers sent to outside sites.
Public API leaks	GOOD	No public site API that lists users or settings.
Config, code-history and backup files	GOOD	6 common paths (environment file, code history, backup archive, server info page, and others) are not reachable.
Keys or passwords in page code	GOOD	Scanned the homepage and 2 script files (97 KB) for payment, cloud, AI, email and code-hosting key patterns: 0 matches.
Open database	GOOD	No database passwords or full-access database keys in page code.

Book a free 15-minute review

Call (888) 512-9899

Encryption

Whether every visit is encrypted, and stays that way.

Check	Result	What we found
Secure connection (HTTPS)	GOOD	The secure address loads with a valid certificate. https://aztc.it answered 200
HTTP redirects to HTTPS	GOOD	The insecure address forwards to the secure one. Enforced at the network edge
Strict HTTPS rule (HSTS)	FIX SOON	The strict HTTPS rule skips subdomains, so a first visit to a subdomain can begin unencrypted. max-age=31536000 (no includeSubDomains)
Mixed content	GOOD	0 insecure resources on the homepage.
Security certificate	GOOD	Valid, with 85 days left on the newest certificate. Covers *.aztc.it, aztc.it; newest certificate expires 2027-02-11 (85 days)

Fix: Strict HTTPS rule (HSTS)
Why: The strict HTTPS rule skips subdomains, so a first visit to a subdomain can begin unencrypted.
How: Confirm every subdomain loads over HTTPS, then set Strict-Transport-Security: max-age=31536000; includeSubDomains.
Effort: 20 min | Who usually does it: Web host or developer

Email spoofing protection

These DNS records decide whether someone can send email that looks like it came from you. Provider names are replaced in the records shown.

Check	Result	What we found
Mail servers (MX)	GOOD	1 mail server set.
SPF (allowed senders)	FIX SOON	SPF is present but ends with a soft fail (~all). A hard fail (-all) is stronger once all senders are listed. v=spf1 include:(mail provider) include:(email forwarding) ~all
DMARC (policy)	FIX SOON	DMARC is set to quarantine: fakes go to spam, where people still find them. "reject" stops them. v=DMARC1; p=quarantine; pct=100; sp=quarantine; rua=mailto:james@aztc.it
DKIM (signing key)	GOOD	Found at your mail provider's standard name; 2048-bit key. 2048-bit key at the standard name
Brand logo in inboxes (BIMI)	GOOD	Logo record published.
Encrypted delivery rules (MTA-STS) and reports (TLS-RPT)	NOTE	No delivery rules; no reports. Optional: makes other mail servers use encryption when they deliver to you.

Book a free 15-minute review

Call (888) 512-9899

Fix: SPF (allowed senders)
Why: SPF is present but ends with a soft fail (~all). A hard fail (-all) is stronger once all senders are listed.
How: List every service that sends mail as your domain, keep it under 10 lookups, then change the ending to -all.
Effort: 10-20 min | Who usually does it: Whoever manages your DNS

Fix: DMARC (policy)
Why: DMARC is set to quarantine: fakes go to spam, where people still find them. "reject" stops them.
How: Read 2 weeks of DMARC reports, confirm every real sender passes, then set p=reject; pct=100.
Effort: 15 min + 2-week wait | Who usually does it: Whoever manages your DNS

Browser protections

Instructions your site sends to browsers so injected code, framing and data leaks are blocked.

Check	Result	What we found
Content rule (CSP)	FIX SOON	A strict content rule is present, but the style rule still allows inline styles ('unsafe-inline'). style-src 'self' 'unsafe-inline' (an outside service)
Clickjacking protection	GOOD	Other sites cannot show your pages inside a frame. X-Frame-Options: DENY; frame-ancestors 'none'
File-type sniffing	GOOD	Browsers are told not to guess file types. X-Content-Type-Options: nosniff
Referrer rule	GOOD	Full page addresses are not leaked to other sites. Referrer-Policy: strict-origin-when-cross-origin
Device permissions rule	GOOD	Camera, microphone and location are limited to what the site needs. Permissions-Policy present
Cookie settings	GOOD	The homepage sets no cookies.
Security contact file	NOTE	No security contact file. Optional, but it gives researchers a way to warn you before anyone else finds an issue.

Fix: Content rule (CSP)
Why: A strict content rule is present, but the style rule still allows inline styles ('unsafe-inline').
How: Move inline styles into your stylesheet (or use hashes), then remove 'unsafe-inline' from style-src.
Effort: 45 min | Who usually does it: Developer

Book a free 15-minute review

Call (888) 512-9899

Software & domain

Outdated software is the most common way small business sites get hacked. Domain renewal keeps your site and email from going dark.

Check	Result	What we found
Outdated CMS, plugins or server software	GOOD	No CMS detected; no version numbers exposed.
Payments page	NOTE	No payment page found on the homepage. Checked again when you add online payments.
Domain renewal and transfer lock	NOT CHECKED	This domain ending has no public lookup service; we confirm it from the registrar account in a review.

Optional improvements

Note: Encrypted delivery rules (MTA-STS) and reports (TLS-RPT)
Why: No delivery rules; no reports. Optional: makes other mail servers use encryption when they deliver to you.
How: Add TXT _smtp._tls.aztc.it: v=TLSRPTv1; rua=mailto:(report address). Then publish an MTA-STS policy in testing mode.
Effort: 30 min | Who usually does it: DNS + web host

Note: Security contact file
Why: No security contact file. Optional, but it gives researchers a way to warn you before anyone else finds an issue.
How: Publish /.well-known/security.txt with a Contact: email and an Expires: date.
Effort: 10 min | Who usually does it: Developer

Book a free 15-minute review

Call (888) 512-9899

What we can do next

Fix Pack

$300 flat. We make the fixes in this report for you (DNS, email protection, security headers, exposed files), then re-run the checkup to prove it.

Site Watch

$49/month, or $29/month for Essentials and hosting clients; included with Partner and Growth. A weekly re-check of everything in this report, including the unsafe-site lists, with a same-day alert if anything changes. Billed monthly, first month up front, cancel anytime.

Malware Cleanup

$395, or $195 for Site Watch members; one per year included with Partner and Growth. Weekend or after-hours rush +$150. We remove the infection, close the hole it came through, and request removal from the warning lists.

Book a free 15-minute review and we will go through this report with you, confirm anything we could not check from outside, and give you a fixed quote. No obligation.

What this checkup does not do: it does not log in, test passwords, scan every page, or look inside your server. A clean result means we found no problems from the outside, not that none exist. Results are a snapshot of the time above.

Book a free 15-minute review **Call (888) 512-9899**