Website security checklist

Mark each item Pass, Fix, or N/A as you audit your site. Created by Tech Help Canada - techhelp.ca.

#	Security check	What to check	Pass	Fix	N/A	Pass when
1	**HTTPS is enforced sitewide**	HTTP pages, HTTPS pages, redirects, and mixed content	☐	☐	☐	All website traffic is sent to HTTPS without browser warnings
2	**SSL/TLS certificate is healthy**	Validity, domain coverage, trust, expiration, and renewal	☐	☐	☐	The certificate is valid and renewal is working
3	**Website software is up to date**	CMS, plugins, themes, frameworks, libraries, and server software	☐	☐	☐	No security updates are waiting
4	**Unused software and accounts are removed**	Inactive plugins, themes, extensions, test sites, and old users	☐	☐	☐	Only software and accounts you still need remain
5	**Known vulnerabilities are checked**	Installed software and dependencies against disclosed vulnerabilities	☐	☐	☐	No unresolved known vulnerability affects the site
6	**Admin accounts use MFA**	CMS, hosting, registrar, DNS, and other privileged accounts	☐	☐	☐	MFA protects every account that can make major site changes
7	**Passwords are strong and unique**	Website, hosting, database, registrar, email, and related accounts	☐	☐	☐	Sensitive accounts don't share passwords

Tip: anything marked Fix becomes your remediation list. Use N/A only when the control genuinely does not apply.

Website security checklist

Mark each item Pass, Fix, or N/A as you audit your site. Created by Tech Help Canada - techhelp.ca.

#	Security check	What to check	Pass	Fix	N/A	Pass when
8	**User permissions follow least privilege**	Administrators, editors, developers, agencies, and other users	☐	☐	☐	Every user has only the access needed for their role
9	**Login and registration systems resist automated attacks**	Failed logins, password resets, account creation, and bot activity	☐	☐	☐	Rate limiting or other automated-abuse protection is active
10	**Backups are automatic and recoverable**	Website files, databases, storage location, frequency, and restoration	☐	☐	☐	Recent backups exist outside the live site and a restore has been tested
11	**Malware and unexpected file changes are monitored**	Malicious files, injected code, redirects, and unexplained changes	☐	☐	☐	No unexplained malicious or unauthorized changes are present
12	**Security headers are configured**	Browser security headers and their settings	☐	☐	☐	Appropriate headers are active without breaking legitimate site functions
13	**Cookies and sessions are protected**	Authentication cookies, session settings, expiration, and security attributes	☐	☐	☐	Sensitive sessions aren't unnecessarily exposed
14	**Forms, uploads, and user input are secured**	Validation, database queries, output handling, CSRF protection, and file uploads	☐	☐	☐	User-controlled data is handled safely on the server

Tip: anything marked Fix becomes your remediation list. Use N/A only when the control genuinely does not apply.

Website security checklist

Mark each item Pass, Fix, or N/A as you audit your site. Created by Tech Help Canada - techhelp.ca.

#	Security check	What to check	Pass	Fix	N/A	Pass when
15	**Sensitive files and information aren't public**	Backups, configuration files, logs, credentials, repositories, and debug output	☐	☐	☐	Sensitive resources can't be accessed from the public web
16	**File permissions and server access are restricted**	Files, directories, FTP/SFTP, SSH, hosting, and deployment accounts	☐	☐	☐	Access is limited to the people and processes that require it
17	**Third-party scripts and services are reviewed**	Analytics, widgets, APIs, payment tools, embeds, and external scripts	☐	☐	☐	Every external service is still needed and trusted
18	**Security logging and alerts are working**	Logins, account changes, configuration changes, errors, and suspicious activity	☐	☐	☐	Security events are recorded and serious activity can trigger an alert
19	**Domain and DNS accounts are protected**	Registrar access, DNS access, MFA, permissions, and domain locking	☐	☐	☐	Unauthorized users can't easily take control of the domain
20	**Firewall and traffic protection match the site's risk**	Malicious requests, bots, exploit attempts, and traffic attacks	☐	☐	☐	Appropriate protection is active for the site's exposure
21	**A recovery plan exists**	Backups, credentials, contacts, containment, restoration, and investigation	☐	☐	☐	You know how to regain control and restore the site after a compromise

Tip: anything marked Fix becomes your remediation list. Use N/A only when the control genuinely does not apply.