Website Security Checklist

Simple hardening steps for safer hosting and websites.

Account Security

- Use unique, long passwords for the Client Area, Plesk, FTP/SFTP, databases and applications.
- Enable two-factor authentication wherever available.
- Do not share passwords in tickets or email.
- Remove access for users who no longer need it.

Website Security

- Keep CMS, themes, plugins and extensions updated.
- Remove unused software instead of leaving it disabled indefinitely.
- Use least-privilege user roles.
- Protect administrator login areas from brute-force attacks.

Files & Server Access

- Prefer SFTP/SSH over unencrypted FTP.
- Avoid world-writable file permissions.
- Review logs when unexpected changes occur.
- Do not run unsupported or abandoned PHP applications.

SSL & Backups

- Use HTTPS for all login and account pages.
- Renew or replace invalid certificates promptly.
- Keep backups separate from the live website.
- Test restores periodically rather than assuming backups are usable.

Warning Signs

- Unexpected administrator accounts.
- Spam or phishing pages appearing on the site.
- Redirects to unknown websites.
- Unexplained modified files or sudden performance problems.

Security Checklist
✓ Unique passwords
✓ 2FA enabled

✓ Software updated
✓ Unused software removed
✓ SFTP used
✓ Permissions reviewed
✓ SSL valid
✓ Backups off-server
✓ Logs monitored
✓ Recovery plan documented