

Mini Guide to WordPress Security

Protect your website with simple steps, best practices, and essential tools.

Why WordPress Security Matters

- WordPress powers over 40% of the web → making it a common target for hackers.
- A vulnerable site can lead to data loss, downtime, or even blacklisting.
- Good news: with the right practices, you can secure your site in minutes.

Backup Essentials

- **Always keep backups** before making changes.
- Use plugins like:
 - **UpdraftPlus** (free & easy to set up)
 - **BlogVault** (premium, reliable cloud backups)
- Store backups offsite (Google Drive, Dropbox, or external storage).

Must-Have Security Plugins

- **Wordfence** → Firewall & malware scanner.
- **iThemes Security** → Easy hardening options.
- **Sucuri Security** → Great for monitoring & alerts.

Tip: Don't overload with too many plugins. Pick one reliable option.

Strong Login Practices

- Use **unique, strong passwords** (consider a password manager like 1Password or Bitwarden).
- Change your **admin username** from “admin.”
- Enable **Two-Factor Authentication (2FA)**.

Keep Everything Updated

- Regularly update:
 - WordPress core
 - Themes
 - Plugins
- Outdated software is the #1 entry point for hackers.

Extra Security Best Practices

- Limit login attempts (plugins or hosting settings).
- Use SSL (https://). Many hosts like Hostinger or SiteGround provide free SSL.
- Remove unused themes and plugins.
- Check file permissions and disable file editing inside WordPress.

Quick Security Checklist

- Weekly backups
- Security plugin active
- Strong password & 2FA enabled
- SSL certificate installed
- Regular updates

Final Note

Securing your WordPress site doesn't need to be complex. By setting up backups, using one good security plugin, and following these best practices, you'll drastically reduce risks and keep your site safe.