Let’s talk about 7 tips to improve website security.

Use a password manager

Number 1. Use a password manager and secure passwords for your logins. Password managers such as 1Password and Bitwarden are worth exploring. Unfortunately, one of the most common areas for security failure is the human one. No two passwords should ever be the same, and ensure passwords are at least 10 to 12 characters and include numbers and symbols. Remember, never use admin as a username. Password managers store your passwords securely and allow you to generate unique secure passwords for each login without needing to remember each one.

Two-Factor Authentication

Number 2. Use a two-factor authentication. Two-factor authentication can significantly enhance the security of your WordPress site by adding an extra layer of protection to the login process. This way, even if someone else gets your password, they still can’t log into your account without that second factor. Two-factor authentication may seem like a small step, but it can greatly improve the security of your online account and help protect your personal information.

You can search for a two-factor authentication plugin such as WP2FA, Two Factor Authentication, or Mini-orange’s Google Authenticator. Some security plugins also include two-factor authentication, but we will talk more about security plugins in a minute.

Review user base

Number 3. Always review your user base, remove unnecessary users, and be very selective of admin users. Let’s make our way to Users in the dashboard. User roles such as editors, authors, and contributors should be monitored. Typically, the administrative role is reserved for the website’s owner. Removing unnecessary users will minimize the potential attack surface or entry points that attackers can exploit.

Install trusted themes and plugins

Number 4. Only install plugins and themes from trusted developers and uninstall what you are not using. There are a few things to review to assess the reliability of a theme or plugin. Check user feedback and reviews. Note when it was last updated. Look at the number of active installs, explore their support and documentation, and double-check that it is compatible with the latest version of WordPress.

Keep plugins and themes updated

Number 5. Keep your plugins and themes updated, and remember to back up your site before updating. But you might be asking why. Keeping your WordPress themes and plugins up to date is important for maintaining your site’s security, stability, and compatibility. Updates often include security patches that fix software vulnerabilities and bug fixes that could cause your site

to malfunction or break. Attackers could also exploit these bugs to gain unauthorized access to your site. By keeping your website up to date, you can ensure that your site is protected against the latest security threats and runs smoothly with the latest web technologies.

Use a security plugin

Number 6. Install a security plugin like WordFence, Jetpack Security, or i-Themes to scan your site for any reported vulnerabilities. Many other plugins, such as PatchStack, All-in-One Security, are also available in the Plugins Directory. A website security plugin can help protect your website from common cyber threats, block malicious traffic, and alert you to potential security issues. In essence, a security plugin will help you maintain the security and integrity of your website.

Follow security-focussed blogs

Number 7. Something for more advanced users. Follow security-focused blogs like PatchStack, WPScan, or blog.sucuri, which report any new vulnerabilities for which there are updates and emerging web threats.

Extra steps

Then, there are also some other steps worth exploring. Firstly, choosing a reliable web host. Secondly, installing an SSL certificate if your host has not already installed one will allow you to enable HTTPS, which ensures that no information is passed in plaintext. And thirdly, use a spam detector, especially if you have a blog or allow comments on posts.