Website Security

Steps to protect your site

STEP 1: Start With Your Theme And Plugins

Themes and plugins are updated regularly by their creators for a reason – to protect against the latest malware going around. Running an update is like giving them a flu vaccine, to prevent them from getting a virus.

Start by logging in to your WordPress site. Select **Dashboard** in the menu on the left, then click on **Updates**. It will take you to a page that shows any theme or plugin updates to run. Tick **Select All**, then click on **Update Plugins**. You will get a message to say that **All updates have been completed**.

Now clean up by deleting any themes or plugins that you don't use, to prevent attacks from creeping in there. Install a security plugin such as iThemes Security Pro (which I use and love), Sucuri or Wordfence, to amp up your overall security.

STEP 2: Get A Secure Password

Did you know? It takes no more than 10 minutes for software to crack a password that's 6 characters and all lower case. It's time to make your password more secure!

In the WordPress menu to the left, go to **Users** – **All Users**. Find your username and hover your mouse over it. Click **Edit**, which will now show up below your username. Scroll down to **Account Management** and click on the **Generate Password** button.

WordPress will create a good, strong password for you. Make sure you copy and save this directly into a password manager or wherever you store your passwords (I use LastPass to manage all my passwords). Scroll down to the bottom of the page and click on **Update Profile** (the blue button). You now have a strong, fairly secure new password.

Don't give this password to anyone. You can update it every now and then for extra protection.

Steps to protect your site

STEP 3: Get Two-Step Authentication

On the same page where you set your password for your username above, scroll down to **Two-Factor Authentication Options**. Two-factor authentication means you need to confirm with WordPress twice that it's really you logging in to the site – making it more difficult for hackers to trick the system.

Enable all three providers under two-factor authentication options (**mobile app**, **email** and **backup authentication codes**) by ticking the blocks in the **Enabled** column.

Now make **Mobile App** your primary method of two-factor authentication by clicking on the circle in the far-right column, under **Primary**. This is what WordPress recommends and I agree that it works well.

Click the gray button that says **View QR Code & Secret Key**. Now install Google Authenticator on your phone, as this will be your mobile app for two-factor authentication. You can do this by going to your app store on your phone, searching for 'Google Authenticator', and downloading it for free. Once Google Authenticator is installed and open on your phone, click on the plus sign in the bottom-right corner. You can either scan the barcode that WordPress shows you (your QR code) or you can type the WordPress secret key under the QR code into Google Authenticator.

Now copy the code from Google Authenticator into WordPress, to link the two. Click on **Verify** to finish setting this up.

From now on, whenever you sign in to WordPress, you will use your new WordPress password that you created in Step 2 and then fill in the latest Google Authenticator code from your mobile app. Authenticator changes the code about every 15 minutes for security purposes.

STEP 4: Set Up A Second Admin Account

Now it's time to set up a second WordPress admin account for yourself. You will use this account if you're ever locked out of your main account and cannot access your website. Don't worry, it's easy!

.

Steps to protect your site

In the main WordPress menu under **Users**, click on **Add New**. Now fill in the following info:

- **Username**: Make this something like 'Backup User Account', so you can tell the difference between your main admin account and this secondary account. Never use ‘admin’ or ‘info’ as these are super-easy for hackers to crack.
- **Email**: Use a different email account from the one you use for your main admin account.
- **First Name** and **Last Name**: Use your real names here.
- **Show Password**: Copy your new password into your password manager or save it wherever you safely store your passwords.
- **Role**: Make this ‘**Admin**’ so you have full rights, in case you ever have a problem and need to use this profile to sort it out.

Now click the blue button that says **Add New User**. This will bring you to the new user page. Well done!

Scroll down to **Two-Factor Authentication Options** and repeat Step 3 above, from where you click on the plus sign in the bottom-right corner to secure a new user profile. You now have two profiles in the Google Authenticator app – make sure you use the right code when you sign in. Use your main profile as usual, keeping this secondary admin profile as a backup if your main profile doesn’t give you access.

STEP 5: Backup, Backup, Backup

Realtors love *location, location, location*. Online business experts love *backup, backup, backup*.

Set up automatic backups to regularly save all the content and data for you website. I backup every day as I’m very active on Tiara Tribe. I don’t take any chances with this. Run backups as often as you work on your website, but no more than once a day as you don't want to slow it down.

For great backup plugins, choose between **Backup Buddy** (another great paid offer from iThemes that I use) or **Updraft** (free). Take responsibility for your backups and never assume your hosting service will backup for you!

And there you have it: 5 simple steps to ramp up your WordPress site's security. Get this done and dusted so you don't have to worry about getting hacked. You've now made your website more secure and you have access and backups in case anything does go wrong. It's well worth it!