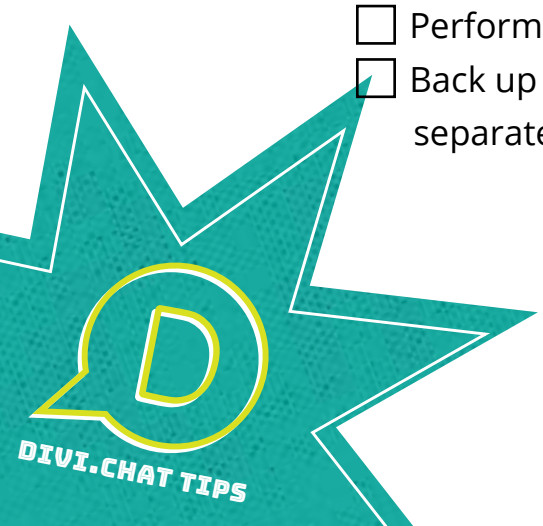
BEST SECURITY PRACTICES TO KEEP YOUR SITE SAFE

1. WordPress Security Checklist

Steps you can take to secure your site mentioned in the Divi Chat podcast episode 16.

- [ ] Hosting. Get reputable hosting and if you are really serious about your site security, **avoid shared hosting if possible**.
- [ ] Make sure you are using clean uninfected installs of WordPress.
- [ ] Use unique username, secure password and change passwords often not only on your WordPress website but on website hosting as well.
- [ ] Enable 2 Factor Authentication. Two recommended applications on this Divi Chat episode were Clef: https://getclef.com/ and Google Authenticator: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en
- [ ] Change/move the WordPress login URL.
- [ ] Keep all your plugins, themes and WP core files updated.
- [ ] Use plugins and themes from reputable and trusted developers.
- [ ] DO NOT keep deactivated plugins/themes on your website. If you are not using it – delete it.
- [ ] DO NOT give out your website login to anyone who needs to access your site (for example when you hire a developer). Create a new user account for them and delete the account immediately after they finish.
- [ ] Perform regular security audits.
- [ ] Back up your site regularly and keep all files in a safe location, separate from your server.



Be sure to watch the full episode for all the site security chat https://www.youtube.com/watch?v=uky4524mGOQ

BEST SECURITY PRACTICES TO KEEP YOUR SITE SAFE

2. Security Plugins

There are 2 types of WordPress security plugins: **Hardening** plugins and plugins that do **Active Scanning and Defense** of your site. As a minimum, you should have a combination of both types.

Hardening security plugins:

- GOTMLS: https://wordpress.org/plugins-wp/gotmls/
- AIO WP Security: https://wordpress.org/plugins-wp/all-in-one-wp-sercurity-and-firewall/

Plugins that actively scan files on your site:

- iThemes: https://wordpress.org/plugins-wp/better-wp-security/
- Sucuri*: https://wordpress.org/plugins-wp/sucuri-scanner/
- WordFence: https://wordpress.org/plugins-wp/wordfence/

3. How Attackers Get Access to WP Sites

If you ever wondered how the attackers entered the site check out this blog post by Dan Moen on the Wordfence blog:

How Attackers Gain Access to WordPress Sites:
https://www.wordfence.com/blog/2016/03/attackers-gain-access-wordpress-sites/

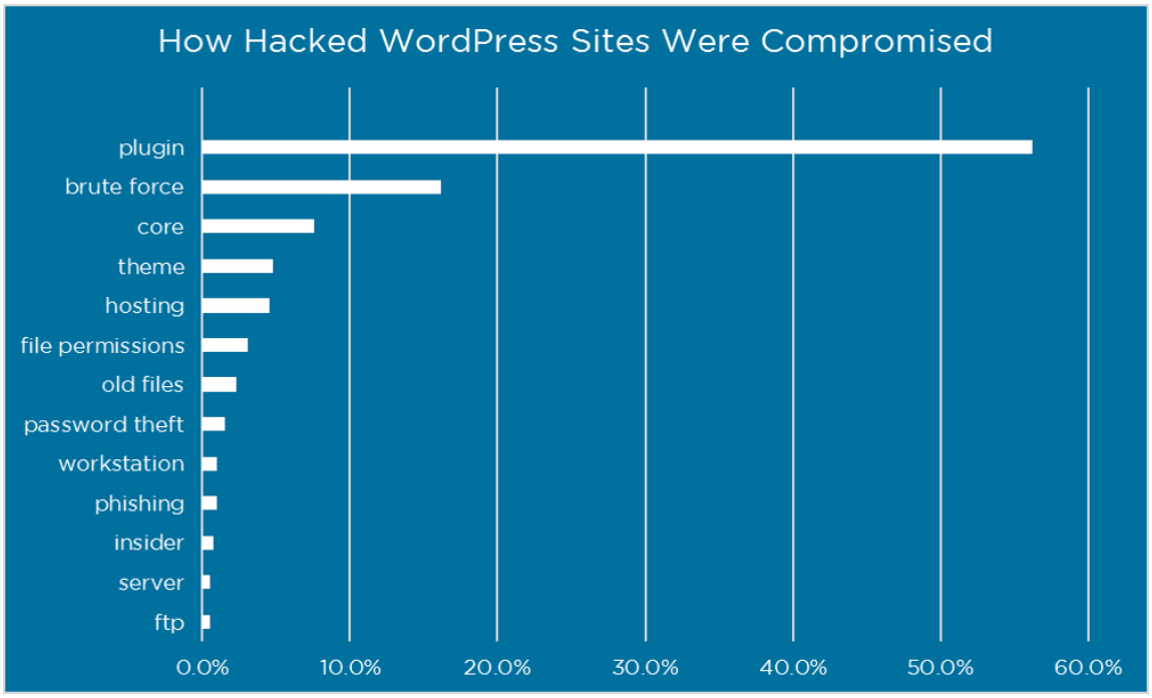
**Sucuri does also have a hardening feature*

DIVI.CHAT TIPS

Be sure to watch the full episode for all the site security chat
https://www.youtube.com/watch?v=uky4524mGOQ

BEST SECURITY PRACTICES TO KEEP YOUR SITE SAFE

Here is what the breakdown looks like:



https://www.wordfence.com/blog/2016/03/attackers-gain-access-wordpress-sites/

As you can see from the image above most hacks happen due to plugin vulnerabilities. This brings us back to the very important steps in regards to plugins:

- Make sure all plugins are updated.
- DO NOT leave deactivated plugins installed.
- Only use plugins (and themes) from reputable developers/studios
- Make sure that plugins are not abandoned, always check how long ago the last plugin update was before you install it and check the support section to make sure that the plugin developer is active.

DIVI.CHAT TIPS

Be sure to watch the full episode for all the site security chat https://www.youtube.com/watch?v=uky4524mGOQ

BEST SECURITY PRACTICES TO KEEP YOUR SITE SAFE

4. What To Do If Your Site Got Hacked

- First, don't stress, you can fix it.
- Change your WordPress salt keys to make sure that everyone is logged out. You can find more information about salts and how to change them in WordPress codex: https://codex.wordpress.org/Function_Reference/wp_salt
- Check all your users to make sure that no one has administrative rights (that shouldn't).
- Replace Core WordPress files via FTP. Make sure you replace them with fresh files downloaded from WordPress.org
- Change all passwords: for WordPress, Hosting and your email.
- Make sure that you always back up your site and keep all files away from your website/hosting so when you get hacked, you can quickly replace all hacked files with clean backup files.
- Check your .htaccess file. Even if you don't understand what is in there have a look for something that's heavily indented or for a really long code. If something doesn't look right you will need to replace this file.
- If you don't know what you are doing you will benefit greatly from getting professional help. You can pay companies like Sucuri and SiteLock to clean your hacked website for you.

Be sure to watch the full episode for all the site security chat
https://www.youtube.com/watch?v=uky4524mGOQ