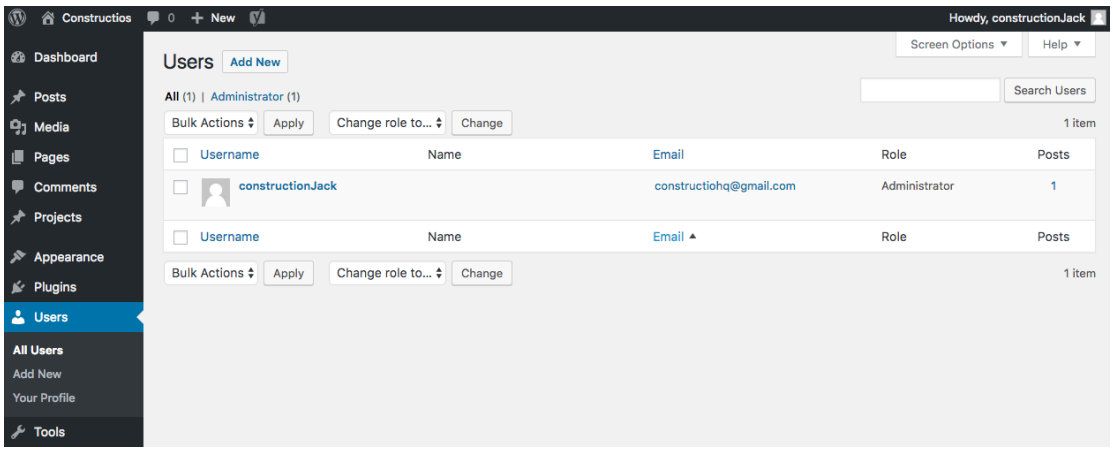
3.5.3 Security

You are in charge of keeping your website secure from hackers. There are some simple ways to keep your website secure that are worth considering and implementing right from the start:

1. Login Information

This sections refers to the User profiles area of your website. (Dashboard Menu > Users >).



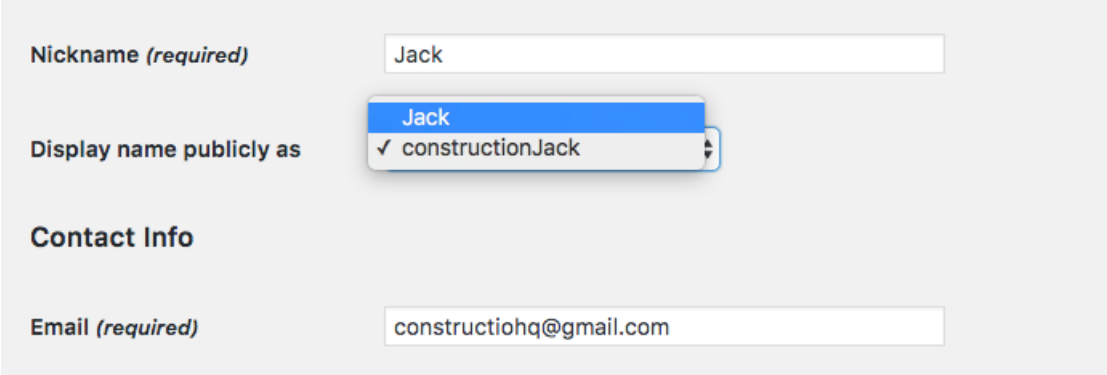
The easiest way for a hacker to gain entry to your site is to guess your username and password. Having a unique username and a strong password are your number 1 line of defense. This is so important to me and my websites that I do not reuse passwords – instead I use Lastpass.com to keep record of individual, complex, random passwords for each and every website.

1.1 Username

The easiest username to hack is admin – this should never, I repeat EVER be used on your website. If a hacker guesses that is your

username then all they have to do is run a program to guess your password if it is short.

You can make your public username different to your login username by clicking into your profile and changing your Nickname to something else (ex: Jack). Scroll down and ***Update Profile***, then scroll back up and change ***Display name publically as***: to your new Nickname.



Now a hacker cannot guess what your actual admin login is (In this case constructionJack).

1.2 Passwords

My strongest recommendation would be to start using a service like lastpass.com to manage your passwords. If you want to manage your passwords manually you can use a strong password generator like http://passwordsgenerator.net/

To understand a little more about how hackers crack passwords this article makes for interesting reading: http://lifehacker.com/5505400/how-id-hack-your-weak-passwords

Now that you know more about password security it might be worth testing some of your existing passwords using this site: http://random-ize.com/how-long-to-hack-pass/

2. Plugins & Updates

Plugins are great aren't they – adding all that extra functionality without needing developers! Well there is a dark side to plugins. Poorly written, supported and updated plugins are a very easy way for hackers to access your website. Make sure you check plugins reviews and how popular they are before installing them and after installation make sure they are updated regularly (I recommend a weekly website update practice).

The same goes for the Wordpress Core – all of those incremental updates you get notified of are generally security updates to patch weaknesses that could be exploited by hackers.

With themes, make sure to use highly recommended themes that are regularly updated by their developers and have a robust support community. This is why I love Elegant Themes, the are constantly innovating, securing and improving their plugins and their popularity ensures that there is an incredibly supportive community growing up around them.

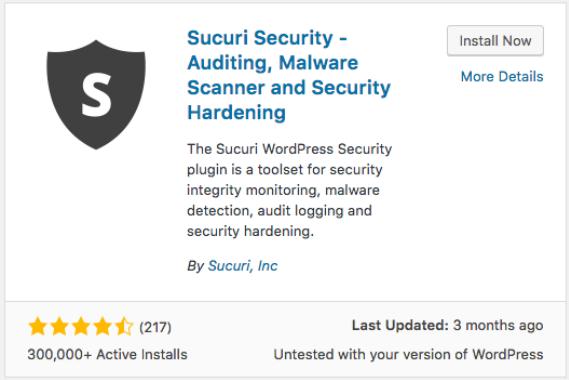
3. Add an SSL Certificate

This is a more advanced step and I would recommend hiring a professional to do this for your website. Siteground provide a free SSL certificate through their partner LetsEncrypt but implementing it can be tricky and requires some additional technical knowledge. You could implement it with the help of Siteground's excellent support staff but for piece of mind – this is one step I would recommend outsourcing if you can.

Once the certificate is installed all of the links on your site need to be secured so the certificate is valid. For a new site this can be done in 1-2 hours of work so budget accordingly.

4. Install Sucuri

There is a dizzying array of security plugins for you to choose from but the one I recommend is Sucuri Security.



Dashboard Menu (mysite.com/wp-admin) > Plugins > Add New and type Sucuri into the search bar. Install Now & Activate.

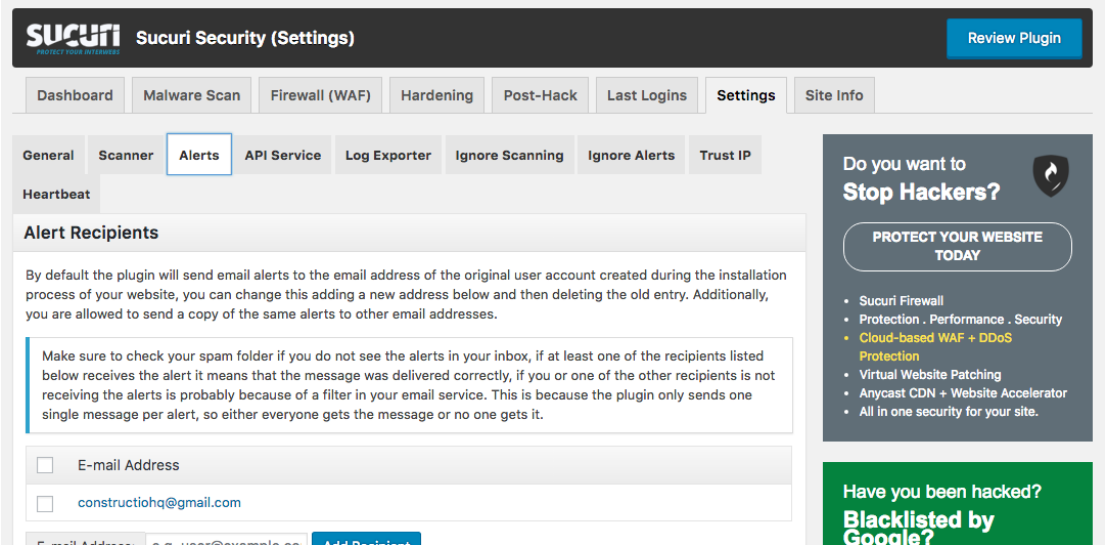
On activation you will be prompted to create a free API key. This isn't necessary but it does give you access to additional features and gets rid of an annoying prompt that is otherwise always present. Click Generate API, untick Enable DNS lookups on startup (unless your are going to be using a reverse firewall as it states) and click proceed. That is all you really need to do.

4.1 Managing Email Alerts

You will now start getting emails that tell you when someone successfully logs in.

To change your notification settings go to Sucuri Security > Settings > Alerts and scroll down to Event Description. If the login attempts are

annoying you can switch them off by unticking ***Receive email alerts for successful login attempts*** and click ***Save***

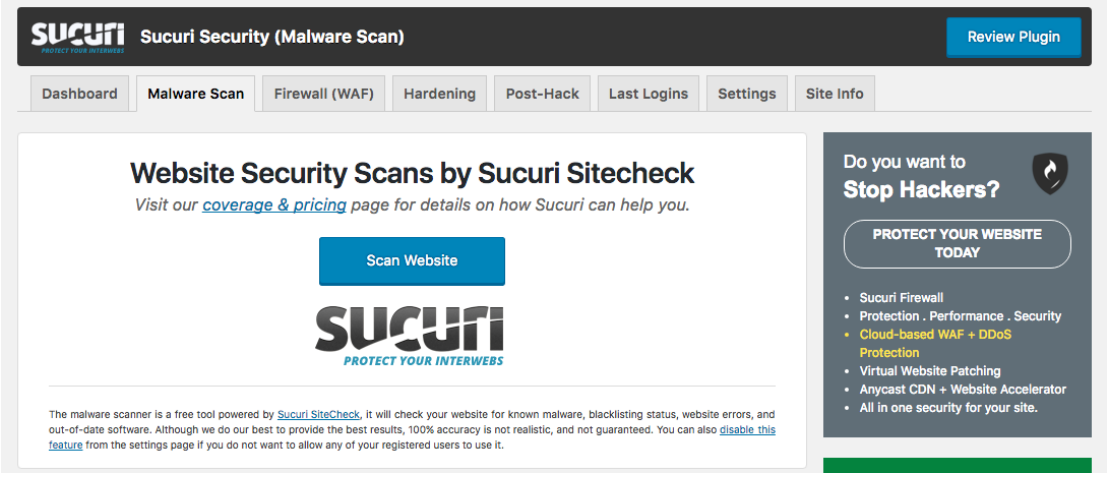


4.2 Manual Malware Scanning

Malware is software that is specifically designed to disrupt, damage or gain unauthorized access to your website. It can be hard to detect but Sucuri have a Malware Scanning function in their plugin.

Go to Sucuri > Malware Scan and press ***Scan Website***.

I would recommend doing this once a month just to be sure and especially if you have received a warning about changes to your site if you have not been logged in yourself.



4.3 Website Hardening

Some steps you can take to make your site even more secure are to go to the Hardening tab. These measures block backend access to certain sections of your site and I recommend switching on the following:

- Verify Wordpress version
- Verify PHP version
- Remove Wordpress versionBa
- Protect uploads directory
- Restrict wp-content access
- Restrict wp-includes access
- Security keys (should be default)
- Information Leakage
- Default admin account – this checks what I recommend in Step 1 of this guide – no 'admin' usernames.

Final Thoughts

There is no way to make your site 100% secure – even with the expensive paid security services. However, by having high quality hosting and following the guidelines above as well as keeping an

offsite backup of your site (in Dropbox or Drive) you are covered for most eventualities and these measures don't take a lot of effort to maintain once initially implemented.

If you are ever hacked, contact a professional as soon as possible for assessment and remedial work. The sooner the hack is caught the easier it is to fix. If the site is beyond fixing or the cost is too high – it might be more cost effective to just restore an earlier version of the website that was hack free. Again, this is something you will need to discuss with a web design professional, who has experience with hacking.