BASIC WORDPRESS SECURITY

It all depends on you

About Me

- I was involved in security in a law enforcement environment for years
- I built my first website in 1996 and built my first money-making website in 1998
- I’ve been interested in website security all that time.
- I’m appalled at how few website owners even think about the security of their websites.

Today’s Takeaways

1. You will know why your website is a target and why it is vulnerable

2. You will know how to protect yourself

3. You will know how to respond quickly to simple hacks and be able to help the experts get you back online in more complex hacks

Google finds around 100,000 hacked websites every month

And they instantly drop them from the search results

First Things First

- There is nothing sexy or exciting about website security at this level – nobody dies and we all get to go home at night.

- It’s repetitive, boring, gritty work - there are no fist-pumping wins and you just keep doing the same thing over and over again. The moment you stop you lose!

- In fact there are no wins at all … the best you can hope for is that you’ve just had one more day when the bad guys didn’t get into your website.

- BUT … if you don’t get interested in the ongoing security of your website you can see your website get trashed, your reputation destroyed and your business wiped out.

That’s your motivation for going on

Deceptive site ahead

Attackers on [redacted] may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

☐ Automatically report details of possible security incidents to Google. Privacy policy

Details

Back to safety

Reported Attack Page!

This web page at ..au has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Get me out of here! | Why was this page blocked?

Ignore this warning

Hacked By 7OP-H4ck3R ..:: Libyana ::..

Group ToP-TeaM = 7OP-H4CK3R + AWH3D4 + A.d.A.m + H4mz4-Abd Alnabi

Bany-Walid FreeDom

Www.Facebook.com/ToPTeaM.Ly

Thanx Bro :) ALansary Hacker [LY] + Chadinas24 [CH]

Skype : Top-eam

./Ly

But Hackers Won't Be Bothered With Me!

Think again:

Health and Beauty site – 40,000 attempts to gain access in 3 weeks

Very small land subdivision site – just 9 blocks – Over 3,000 attempts in a weekend plus many more since then

A brand new bed and breakfast – over 3,000 attempts in the first couple of weeks after the site went live

A site about personal relationships – just 4 pages – currently 3,456 in just over a year

A poly welding site – over 2,000 attempts in the first week

A signwriter's site – over 5,000 attempts in the last 5 or six months

The threat from hackers is very real and they don't care who they target

Know your enemy

There are basically 6 types of hacker:

1. **The Script Kiddie** – they just want to show their friends how cool they are and how they can make you look dumb

2. **The Activist** – they want to make a religious or political statement

3. **The Link Dropper** – they want to add links to porn, pills and potions … or even a genuine website.

4. **The Spammer** – they want to add code to your site that will enable them to send out millions of spam emails that will look as though they came from you.

5. **The Trojan Dropper** – they will add code to your site that will immediately infect the computer of anyone who visits your website.

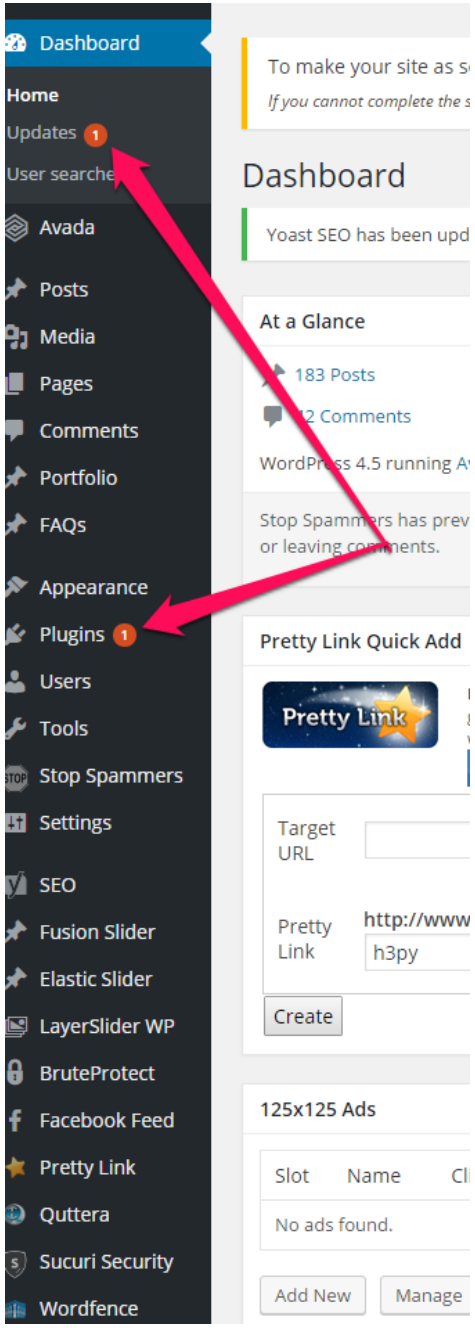
How do they get in?

Weak usernames and passwords

A Wordpress core that’s not been updated

Old plugins that have not been updated

Vulnerabilities at the server level


Dashboard
Home
Updates 1
User searche
Avada
Posts
Media
Pages
Comments
Portfolio
FAQs
Appearance
Plugins 1
Users
Tools
Stop Spammers
Settings
SEO
Fusion Slider
Elastic Slider
LayerSlider WP
BruteProtect
Facebook Feed
Pretty Link
Quttera
Sucuri Security
Wordfence
To make your site as s
If you cannot complete the s
Dashboard
Yoast SEO has been upd
At a Glance
183 Posts
12 Comments
WordPress 4.5 running A
Stop Spammers has prev
or leaving comments.
Pretty Link Quick Add
Pretty Link
Target URL
Pretty Link
http://www
h3py
Create
125x125 Ads
Slot
Name
No ads found.
Add New
Manage

MOSSACK FONSECA

Securing Your Website

Strong username and password

Add plugins that will make it harder for hackers to gain access

Add plugins that will alert you to hacker activity

Add plugins that will make recover easier when you’re hacked

Monitor your website

Securing Your Website

Username – Password - Nickname

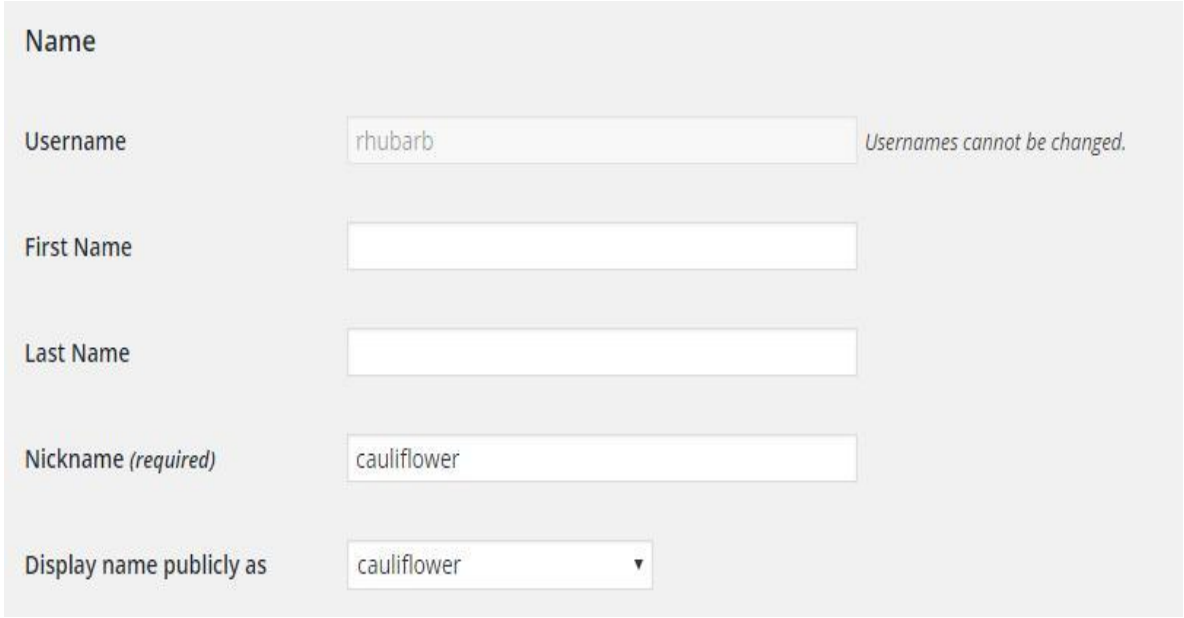
- Such a simple step
- But so many people ignore it because they are dumb
- Don’t use your real name, the name of your dog or cat
- Don’t use a simple password – use a combination of letters characters and symbols

2%raO4B#0r#"42!

Securing Your Website

Username – Password - Nickname

Setting up your user profile



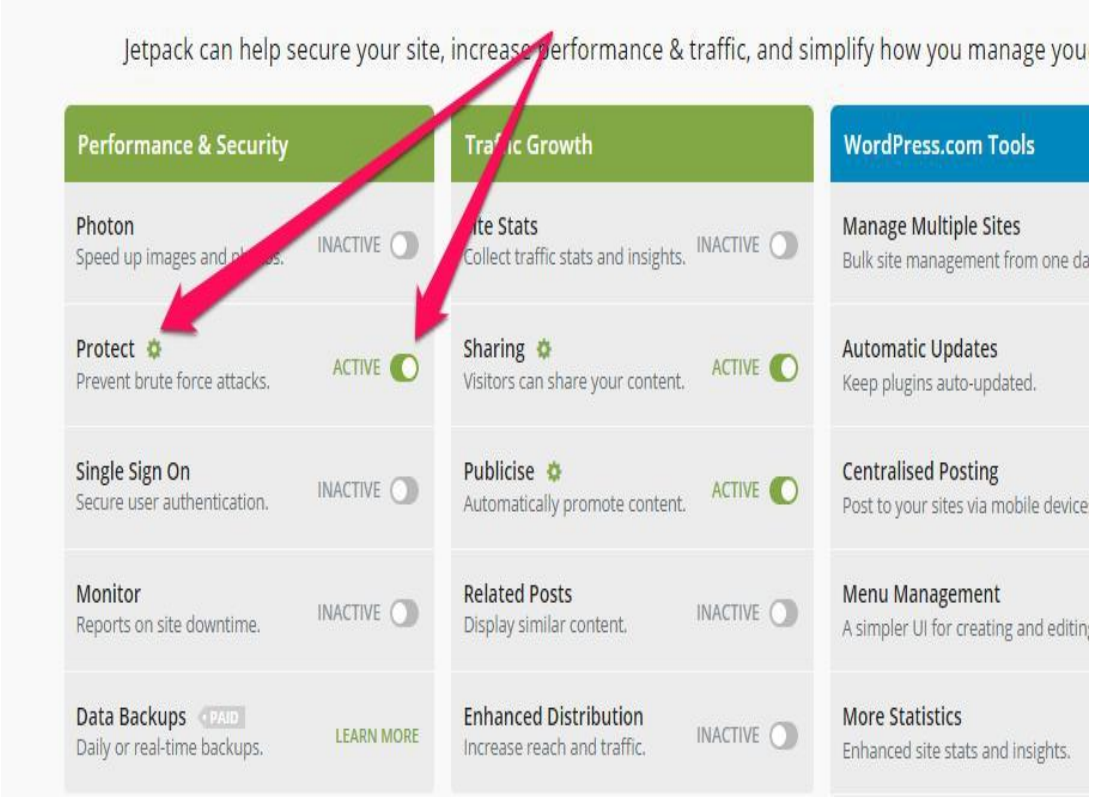
Securing Your Website

- ✓ Strong username and password
- Add plugins that will make it harder for hackers to gain access
- Add plugins that will alert you to hacker activity
- Add plugins that will make recovery easier when you’re hacked
- Monitor your website

Securing Your Website

- Install Jetpack

… and activate the “Protect” option



Securing Your Website

Install the Wordfence Security plugin

- Go to the Options tab and add your email address in the email alerts field
- Look for the Login Security section and change the amount of time a user is locked out to some period longer than 5 minutes.
- Go to the Firewall tab and activate the Firewall
- Now you will have protection and you will get email notifications every time something needs updating.

Don’t ignore those emails

Securing Your Website

Install the Google Captcha (reCAPTCHA) plugin by BestWebSoft

- There are a few simple steps to setting it up and once you have done those then you too will have one of those horrible captchas on your website.

Securing Your Website

- ✓ Strong username and password
- ✓ Add plugins that will make it harder for hackers to gain access
- Add plugins that will alert you to hacker activity
- Add plugins that will make recovery easier when you're hacked
- Monitor your website

Securing Your Website

Install the Sucuri Security - Auditing, Malware Scanner and Hardening – plugin.

- Apply for an API key – don’t panic – it’s easy.
- Go to Settings > Alerts and make sure your email address is listed and then tick every alerts box you can find
- Go to Settings> Hardening – ignore the Firewall option but harden every other option you see there with the exception of the database prefix

Securing Your Website

The Wordfence Security plugin will also alert you to attempts to break into your website.

You need to know what is happening so don’t turn off any security alerts – anyone of them could be the one that is warning you of impending disaster.

Securing Your Website

- ✓ Strong username and password
- ✓ Add plugins that will make it harder for hackers to gain access
- ✓ Add plugins that will alert you to hacker activity
- Add plugins that will make recovery easier when you're hacked
- Monitor your website

Securing Your Website

Install a database backup plugin such as **WordPress Database Backup** by Matzko or **Updraft Plus Backup/Restore**

- Set up is simple and the plugin to email you a copy of your database at intervals that suit you. They can be from hourly to weekly.
- Keep those database copies somewhere safe and keep them for a few months.

Install the **Quttera Web Malware Scanner** plugin

- Regularly run both the external AND internal scans

Securing Your Website

- ✓ Strong username and password
- ✓ Add plugins that will make it harder for hackers to gain access
- ✓ Add plugins that will alert you to hacker activity
- ✓ Add plugins that will make recovery easier when you're hacked
- Monitor your website

Securing Your Website

- Regularly visit the front of your website
  - Skim through a few pages and look for any changes

- Set up a Google Webmaster Tools account
  - Link your site to the account (the Yoast SEO tool can help)
  - Visit the account often because Google will use it to tell you if they have found malicious code on your website.

Recovering From a Hack

So you have been hacked – what do you do?

Have your pity party

Get angry

Wail and gnash your teeth

And then get over it and fix the problem

Recovering From a Hack

- Check the list of Users in the Admin area and delete any that you don't know – and delete their content too – don't add it to another user's content.
- Completely change your WordPress passwords
- If other people have access to your site change their passwords too
- If you have FTP access to your website change that password and if you have access but can't then ask your host to change it for you.

Recovering From a Hack

Assess the damage

- If it was a simple defacement then you should be able to repair the damage yourself.

- If a link dropper paid you a visit then you will need to go through every single page and post and remove the links … and look for hidden links too.

- If it was an email spammer or a Trojan was installed then you need professional help … and it could cost you a lot of money

- If the hack came through the server then your host may repair the damage for you.

Recovering From a Hack

The bottom line:

- If you have been hacked and you don’t know how to fix it then get help.

- Don’t just leave it and hope it will all go away … because it won’t!

For links to all the plugins I’ve mentioned here please visit:

Wpsecurityworkshop.com/mypod