

Increase your email opt-ins by 87%. Dont believe me? :-)

[CLICK HERE for Proof!](#)

- [Home](#)
- [About](#)
- [New? Start Here](#)
- [Resources](#)
- [Videos](#)
- [Wordpress Services](#)
- [Contact](#)

# 14 Ways To Prevent Your WordPress Blog From Being Hacked

by [Salman Ahsan](#)

in [Wordpress Security](#)

Recommend { 150 }



There are over 5 million results in google for the keyword “**prevent wordpress hack**“. Everyone has their own opinion and I dont think all of these posts are updated frequently. It’s been a while I have posted here. If you have been following me on my [twitter](#) then you should know what I have been up to. First, here are few things you should know- I have made several changes to this blog.

Recently, some of my blogs were hacked. It was funny how the index file had an image of a smurf showing the middle finger with a text saying “where’s your security?” I was glad the hacker left his email address so I could thank him for mocking the security of my blogs and so, I did. The amazing part- This guy didn’t even touch the database; he didn’t even inject any shit virus. I felt it was weird but after checking out each files, I found they were all clean.

I was so involved in other projects that I didn’t pay much attention to security which is actually the most important thing here. If this dude didn’t breach my security, I wouldn’t have known it was vulnerable and hence wouldn’t have bothered to take action. Whatever it is, I have sent him a “Thank You” Note 😊

I have removed some shitty plugins, transferred to [HostGator](#), tweaked codes and more... Today, I have decided to write a post on how I did what I did- that is, strengthen the security of my blog to keep off hackers and all creepy people. I will have a video tutorial created for this later this month but for now, check this out. Some basic tweaks can help protect all your hard earned content. Check out the following tips to *prevent wordpress hack*.

## 14 Tips To Prevent WordPress Hack

### 1. Backup

This is the first step and the most important. Before you plan on making any changes, make sure you backup your entire DB. You can do this

manually or use an available plugin. I recommend [backup buddy](#) which backs up your entire wordpress blog. Unlike free plugins which only backup your database, backup buddy exports your entire database with images, files and whatever you have in your blog's content folder- Pretty sweet!

## 2. Update WordPress Version

Second crucial step after backing up your blog is to update it to the latest version. You should always make sure that your blog's version is up to date. WordPress team creates patches to help fix security holes. Follow wordpress feed to find out about the latest updates or you could simply login to your admin.

I would also recommend that you follow WordPress Development and BlogSecurity as they will inform you whenever a new patch/fix is released.

- [WordPress Development](#)
- [BlogSecurity.net](#)

## 3. Change your Login/Password

The default wordpress login is "admin" and most hackers know that. We should change this to something else that would be difficult to guess. Something like "rogers12" or "donhoe2" is good examples. The best thing to do is delete the default admin and create a new custom login.

I suggest that you use strong passwords which include upper/lower keys, numbers and symbols. Something like "rockSTAR19!@" or "Anabel2@!" is a great example of a strong password.

Most hackers try to brute force the password so if your password is really strong as I mentioned earlier, you should be fine.

Do not use birth days, names, pet names or hobbies as passwords. People who are close to you know a little more about you; you don't want any wild guesses 😊

## 4. WordPress Keys in wp-config.php

I didn't know much about wordpress keys but it is another important security measure. These keys work as salts for WordPress cookies thus, ensuring better encryption of user data.

Use the [WordPress Key Generator](#) to generate these keys. Now open up your wp-config.php, find the lines that look like below and simply replace with the generated ones:

```
define('AUTH_KEY', 'put your unique phrase here');
define('SECURE_AUTH_KEY', 'put your unique phrase here');
define('LOGGED_IN_KEY', 'put your unique phrase here');
define('NONCE_KEY', 'put your unique phrase here');
```

Save and you are done!

## 5. Install WP Security Scan

### WP - Security Admin Tools

Initial Scan

**WordPress version: 3.1** You have the latest stable version of WordPress.

Your table prefix is not wp\_.

Your WordPress version is successfully hidden.

WordPress DB Errors turned off.

WP ID META tag removed from WordPress core

No user "admin".

.htaccess exists in wp-admin/

\*\*\*WP Security Scan plugin must remain active for security features to remain\*\*\*

**Future Releases**

one-click change file/folder permissions

test for XSS vulnerabilities

intrusion detection/prevention

lock out/log incorrect login attempts

user enumeration protection

WordPress admin protection/security

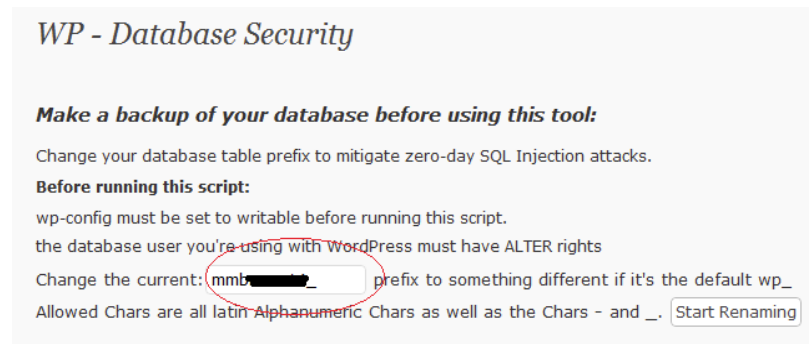
System Information Scan

- Operating System : Linu
- Server : Apache mod\_
- mod\_bwlimited/1.4 Fro
- Memory usage : 29.64 I
- MYSQL Version : 5.1.52
- SQL Mode : Not set
- PHP Version : 5.2.15
- PHP Safe Mode : Off
- PHP Allow URL fopen : C
- PHP Memory Limit : 256
- PHP Max Upload Size : 6
- PHP Max Post Size : 64



This plugin is the real deal. It's simple and automates stuff. It will scan your wordpress blog for vulnerabilities and inform you if it finds any malicious codes etc. If the texts are in green in the admin panel then you should be good. However, they will not just be green; sometimes you have to make them 😊. And I will tell you how.

## 6. Change Table Prefix



The default table prefix for wordpress is wp\_. I know that, you know it and I am sure the hacker does too. [SQL Injection](#) attacks are easier with the default table prefix because it is easier to guess. A good prefix would be "mashjg23\_" or "sasdoe265\_". Changing your database table prefix is highly recommended and you can do this in two ways. The manual way requires some work and is not suitable for newbie; here's when WP Security Scan Plugin makes your work much easier. It has a tab called "Database". Once you are in it, you have the option to rename your entire table prefix to something that is tough to guess. Do this and you will be a step closer to strengthening your blog's security.

DB Password: How strong is your database password? Both your wordpress login password and database password should be strong. Include upper/lower keys, numbers and symbols.

## 7. Prevent WordPress Hack by Blocking Search Engine Spiders from Indexing the Admin Section

Search engine spiders crawl over your entire blog and index every content unless they are told not to do so. We do not want to index the admin section as it contains all the sensitive information. The easiest way to prevent the crawlers from indexing the admin directory, is to create a robots.txt file in your root directory. Then place the following code in the file:

```
#
User-agent: *
Disallow: /cgi-bin
Disallow: /wp-admin
Disallow: /wp-includes
Disallow: /wp-content/plugins/
Disallow: /wp-content/cache/
Disallow: /wp-content/themes/
Disallow: */trackback/
Disallow: */feed/
Disallow: */feed/rss/$
Disallow: /category/*
```

## 8. .htaccess Hacks

[.htaccess](#) (hypertext access) is the default name of directory-level configuration files that allow for decentralized management of configuration when placed inside the web tree. .htaccess files are often used to specify the security restrictions for the particular directory. This is not an exact tip that falls under the list but you should know about .htaccess because you can do a lot with it to [prevent wordpress hack](#). I am not going to get in depth for this term but I found out some sweet .htaccess hacks which can tighten your wordpress security. See them below

## 9. Protect your .htaccess

After tweaking your .htaccess to protect your blog from hackers, you cannot simply leave the .htaccess open itself to attacks. The hack below prevents external access to any file with .hta. Simply place the code in your domain's root .htaccess file.

```
# STRONG HTACCESS PROTECTION</code>
<Files ~ "^.*\.[Hh][Tt][Aa]">
```



```
order allow,deny
deny from all
satisfy all
</Files>
```

## 10. No Directory Browsing

Its not a good idea to allow your visitors to browse through your entire directory. This is an easy way to find out about directory structures and this makes it easier for hackers to lookout for security holes.

In order to stop this, simply add the piece of 2 lines in your .htaccess in the root directory of your WordPress blog.

```
# disable directory browsing
Options All -Indexes
```

## 11. Secure wp-config.php

Wp-config.php is important because it contains all the sensitive data and configuration of your blog and therefore we must secure it through .htaccess. Simply adding the code below to the .htaccess file in the root directory can do the trick

```
# protect wp-config.php
<files wp-config.php>
Order deny,allow
Deny from all
</files>
```

The code denies access to the wp-config.php file to everyone (including me 😊)

## 12. Limit Access to the Wp-Content Directory

Wp-content contains everything. This is a very important folder and you should secure it. You don't want users to browse and get access to unwanted/other data. Users should be only able to view and access certain file types like images (jpg, gif, png), Javascript, css and XML.

Place the code below in the .htaccess file within the wp-content folder (not the root).

```
Order deny,allow
Deny from all
<Files ~ "(.xml|css|jpeg|png|gif|js)$">
Allow from all
</Files>
```

## 13. Protect WordPress Admin Files

Wp-admin should be accessed only by you and your fellow bloggers (if any). You may use .htaccess to restrict access and allow only specific IP addresses to this directory.

If you have static IP address and you always blog from your computer, then this can be a good option for you. However, if you run a multiple user blog then either you can opt out from this or you can allow access from a range of IPs. You can refer to Apache's documentation on mod\_access for complete instruction on how to set this up.

Copy and paste the code below to the .htaccess in wp-admin folder (not root folder)

```
# deny access to wp admin
order deny,allow
allow from xx.xx.xx.xx # This is your static IP
deny from all
```

The above code will prevent browser access to any file in these directories other than "xx.xx.xx.xx" which should be your static IP address.

There is another way you could restrict access to the directory and that is by using a password in the .htaccess. I am planning to write a detailed .htaccess hack where I will include all of these.

## 14. Prevent script injection



I found this code on [wprecipes](#) and it works like a charm. Now you can protect your WordPress blog from script injection, and unwanted modification of \_REQUEST and/or GLOBALS.

Simple copy and paste the code below to your .htaccess in the root

```
# protect from sql injection
Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (<|>|'|\".*script.*(>|'|\" [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|\\[|\\%{0-9A-Z}{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|\\[|\\%{0-9A-Z}{0,2})
RewriteRule ^(.*)$ index.php [F,L]
```

## Bonus

*WP - Security Scan*

Name	File/Dir	Needed Chmod	Current Chmod
root directory	../	0755	755.
wp-includes/	../wp-includes	0755	755.
.htaccess	../.htaccess	0644	644.
wp-admin/index.php	index.php	0644	644.
wp-admin/js/	js/	0755	755.
wp-content/themes/	../wp-content/themes	0755	755.
wp-content/plugins/	../wp-content/plugins	0755	755.
wp-admin/	../wp-admin	0755	755.
wp-content/	../wp-content	0755	755.

Take a note at the files permission. Wp Security scan shows this in a nice way. Browse the specific files on your root using your favorite ftp client and Chmod the files if required.

Last but not the least; you can install [WordPress Firewall 2](#) which actually protects your blog from malicious hackers. It blocks the attempts of the hacker and notifies you when abused. Only the negative point of this plug-in is, it sometimes even blocks our action. This can really get annoying and I do not really recommend this plug-in unless you have SUPER Hackers and bots screwing up your blog. Stick with the .htaccess hacks since they do the job pretty well and your blog should be just fine.

**Furthermore, Check out these amazing wordpress security posts written by others to prevent wordpress hack :**

1. [WordPress Security](#)
2. [11 Best Ways to Improve WordPress Security](#)
3. [How to Stop Your WordPress Blog Getting Hacked](#)

## Verdict

Prevention is better than cure. I cannot personally guarantee that your blog will not get hacked after implementing the methods I have mentioned but, I am sure the chances of getting attacked will be very less.

How secure is your wordpress blog? If you have a tip or a piece of code you would like to contribute then use the comment box. I bet after reading this post, you will know how to prevent wordpress hack to some great extent

Recommend 150

## Did you enjoy this article?

Signup for the Upcoming "VIP Blogging e-Course"

Be one of the FIRST ones to receive the VIP Blogging e-Course which includes HD Videos, Guides and much more for FREE.




FREE INSTANT ACCESS



**Leave a comment & let me know what you think!**



36 comments



Add a comment...

Comment

**Susan Gecek Ramos**

you really are a rockstar!

Reply · 1 · Like · September 19 at 9:28am

**Quinn Curtis** · Salt Lake City, Utah

Man, this is GREAT info. Thank you so much! Dealing with a big ol' messy hack job on all my sites and going BANANAS trying to get it to stop. Really appreciate your suggestions.

Reply · 1 · Like · October 18 at 1:45pm

**Salman Ahsan** · Rockstar at Salman Ahsan Consulting · 1,134 subscribers

There will be a video on this soon :) I have decided to create videos on popular tutorials. Hope it will help more people.

Reply · Like · October 18 at 1:47pm

**Quinn Curtis** · Salt Lake City, Utah

Sounds awesome! Count me IN. :)

Reply · 1 · Like · October 18 at 7:34pm

**Vikram Singh Rana** · Web Developer at ODesk

Extremely helpful articles. I would like to thank you for your efforts. Keep up the good work.

Reply · 1 · Like · October 11 at 6:55am

**Samuel Guebo** · Abidjan, Cote d'Ivoire

nice tips indeed..making sure you also have a good antivirus would not be a bad idea, I once got my websites infected just cuz my files were infected by some viruses before I uploaded them.

Reply · 1 · Like · September 3 at 8:32am

**Salman Ahsan** · Rockstar at Salman Ahsan Consulting · 1,134 subscribers

definitely. a good antivirus is necessary :)

Reply · Like · September 3 at 4:28pm

**Diana DeVargas** · Sydney, Australia

Thanks for the tips.

Reply · 1 · Like · August 14 at 7:13pm

**John O Gilmore Jr**

All my blogs hacked last night. Must start over. I know these suggestions may not stop all attempts – but, I do believe they sure as h\*ll will slow them down! Thank you so much for this info. This is the best "First Line of Defense" site I could find. Well done!

Reply · 1 · Like · June 24 at 11:25am

**Salman Ahsan** · Rockstar at Salman Ahsan Consulting · 1,134 subscribers

btw, I am working on another detailed post which will be the 2nd part.. Recently some of my websites were infected by malwares.. I havent talked much about these silly scripts which I think is actually quite important. Thank you all for your support

Reply · Like · June 28 at 8:50pm

**Emmanuel Hemmings**

Excellent post, will follow this advice.

Reply · 1 · Like · June 7 at 11:59pm

**Jocelyn Correa Wing** · Top Commenter · Gaithersburg, Maryland

Thanks for writing this post. This hackers just don't know what to do. They are the new website bullies.

Reply · 1 · Like · June 2 at 10:21pm

**Salman Ahsan** · Rockstar at Salman Ahsan Consulting · 1,134 subscribers

{ 59 comments... read them below or [add one](#) }



[Anita](#) [March 4, 2011 at 10:14 am](#)

Hm, this article is a little over my head at this time, and it will need some rereading, but I'm interested to know how come you came to HostGator? Is it because it is considered safer? Is there a "safe" host?

[Reply](#)



[Salman Ahsan](#) [March 4, 2011 at 11:55 am](#)

Im not sure how safe is hostgator but I always wanted to check them out. The fact is, I have 4 different hosting accounts and this blog was formerly hosted by JustHost. They are good but I think my blogs deserve [hostgator](#)? 😊 Btw, WpWebHost is awesome for blogs too. I have hosting with them for almost 2 years now and rarely had downtime issues. Web Hosting do matter when it comes to security and making some additional tweaks to your blog can be beneficial. If you ask for recommendation, I would say Gator and WpWebHost are real sweet for hosting wordpress and they don't hurt your wallet

[Reply](#)



[Anita](#) [March 6, 2011 at 1:03 am](#)

Thanks for replying! I'm using HostGator and I think they're good but again they are my first hosting company so...)

[Reply](#)



[topblogger](#) [July 17, 2011 at 10:41 pm](#)

how about in blogger.com domain? it is safe to apply on my Blog?

[Reply](#)



[Salman Ahsan](#) [July 20, 2011 at 6:59 am](#)

i guess not 😊 . you can try but this stuff is for wordpress 😊

[Reply](#)



[Chris](#) [September 20, 2011 at 5:08 pm](#)

thanks sooo much very well written and helpful too!

[Reply](#)



[Thanushka](#) [November 18, 2011 at 10:26 am](#)

My Wordpress site (blissfulinterfaces.com) was hacked a few weeks ago (just couple of days after it came live), since I had not changed the Wordpress keys.. Even though the site is not hacked anymore, I still see those hacker web domains directing to my host. When I go to those domains, they direct to my web site Pages with their domain in the URL. as an example, this below URL directs to my contact page under the domain name 'muggeltd dot com'.  
muggeltd dot com/index.php?page\_id=227

Do you know a way to prevent these stripping domains from redirecting to my server? These domains even appear on google search and I'm worried that it will affect my site's Seoul ranking...if you have any tips on how to prevent this, please help. Thank you in advance..





[Reply](#)[Salman Ahsan November 30, 2011 at 6:29 am](#)

First of all, scan your server for any security holes and worms. You need to remove them if found. Install the wordpress security plugins I mentioned. Try to modify the htaccess. As for redirecting, anyone can redirect to whatever they want 😊 at least that's what I know. I don't see much cases like that but if the problem still exist and you want to discuss this then use the contact tab on top and shoot me an email 😊 cheers

[Reply](#)[Husain November 25, 2011 at 9:44 pm](#)

Dear Salman,

I did not manage to insert all the code into .htaccess in the root folder. It ended up my blog displaying "Internal Server Error"

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator...bla..bla..bla"

I just copied the code from your blog here and pasted into .htaccess in the root folder but it failed. Seeking for your advice, please?

Thank you.

[Reply](#)[Salman Ahsan November 30, 2011 at 6:24 am](#)

Your blog seems to load OK. Did you copy the code properly and paste it onto notepad? If you are still facing problems then use the contact tab on top and shoot me an email. I will try to put all the codes together and compile a htaccess and will post the download link here for convenience.

[Reply](#)[pranoy sinha January 14, 2012 at 7:24 am](#)

Dear Salman,

Read all your useful tips. Very informative and useful.

I also have the same issue as Hussain had faced regarding the .htaccess issue. Can you pls post it as a downloadable link here. It would be a great help if you.

Best regards,  
pranoy

[Reply](#)[Salman Ahsan January 19, 2012 at 3:07 am](#)

I appreciate you like my posts. And since you requested, I will update the post shortly with a downloadable .htaccess file which I use on my blogs. 😊 Hope everyone is doing great

[Reply](#)[Yogesh December 4, 2011 at 4:27 am](#)

When I am trying your number 12 method, all the css and designing part of my site used to stop working. Rest all working fine. Can u fix this problem?

[Reply](#)



Adam [December 31, 2011 at 12:53 am](#)

I had this happen to me too, but I never did step 12. Turns out it was the WebsiteDefender WordPress Security plugin. As soon as I disabled it, all the css worked again. However, the WP – Security Scan by the same guy didn't have this problem.

[Reply](#)



Salman Ahsan [January 10, 2012 at 6:31 am](#)

you have to be careful with what plugins you install. Some are buggy while some may overlap

[Reply](#)



Web Aesthetics [June 6, 2012 at 2:00 am](#)

Hi, Thanks for all the great advice. But I am having the same problem as Yogesh when I do step 12. Any guess why this is happening?

[Reply](#)



Salman Ahsan [June 11, 2012 at 9:17 pm](#)

there was a typo which is now fixed 😊

[Reply](#)



Web Aesthetics [June 11, 2012 at 10:04 pm](#)

Hi Thanks to the update, but still having the same problem even when the typo is removed. Any guess why this is still happening?



Peter [June 7, 2012 at 8:23 am](#)

Number 12 has a typo for file type jpeg:

change to:

Awesome post Salman! Thank you.

[Reply](#)



Salman Ahsan [June 11, 2012 at 9:17 pm](#)

thanks for contributing 😊

[Reply](#)



john [December 6, 2011 at 9:19 pm](#)



cant most of this stuff be prevent by firewall

[Reply](#)



[Seo Futurity February 6, 2012 at 6:26 am](#)

One of the best article on the web about Hacking problems in wordpress.

I write post especially about problem, also mention this blog post as a great solution to this wordpress hack problem. Great Image also.

[Reply](#)



[Angel February 18, 2012 at 7:30 pm](#)

hi, my site was hacked just 3 days ago and now its back. Im just new to wp blogging. can you teach me how to prevent those spam comments? please and thank you...

[Reply](#)



[Salman Ahsan February 20, 2012 at 2:04 am](#)

Did you read the post? I have pretty much mentioned everything that you can do.. what is it that you don't understand?

[Reply](#)



[Carol Cody September 26, 2012 at 2:36 pm](#)

Try Askimet for preventing comment spam.

<http://akismet.com/>

[Reply](#)



[Ajnabii February 22, 2012 at 9:23 pm](#)

Hello Dear Salman,

You done very well done Job on you blog, nice blog and really helfull posts, after reading this post i have learned many new things how to protect wordpress blog from hackers, thanks for writing this nice article.

[Reply](#)



[saieshwar March 2, 2012 at 2:12 am](#)

Awesome man, it helps me much, how can I restore my data if my site is hacked and total database becomes empty (i have back up in my system)

[Reply](#)



[Salman Ahsan March 3, 2012 at 7:53 pm](#)

well of course, and with backup buddy its pretty easy. You just have to upload the backup to the root and then using the plugin click a few buttons and get your site restored 😊

[Reply](#)





Phil Tyler [March 4, 2012 at 6:45 pm](#)

Thank you soooo much.

[Reply](#)



Phone Arena India [March 5, 2012 at 4:27 am](#)

whew.. wish i had come upon this article a bit sooner. Had three sql injections carried on in th past couple of weeks and my site was totally messed up. Just spent the last hour implementing all the 14 steps mentioned above. Hopefully, my site's a lot more secure now. Fingers crossed.

[Reply](#)



onyou [March 10, 2012 at 2:12 am](#)

extremely useful tips.. thanks

[Reply](#)



Soccerwidow [April 15, 2012 at 10:58 am](#)

Very well written article, very logical and helpful. Thank you!

I implemented most of it and hope my blog will be now a little more secured. Thanks again 😊

[Reply](#)



Christopher Barnard [April 20, 2012 at 12:47 am](#)

Great post – WP Security can be a real problem.

Implementing No 12 though blocked my images on my site. Any ideas how to resolve that?

[Reply](#)



Salman Ahsan [April 28, 2012 at 4:40 pm](#)

you can just leave out #12 for now. Several people are having issues with it. 😊 I will be writing another post on wordpress security and will include a downloadable custom .htaccess

[Reply](#)



jocelyn [June 5, 2012 at 5:10 am](#)

My website was hacked last Saturday by devilhacker and that's what led me hear. My website (<http://optimizemediamarketing.com>) was defaced and the hosting company I'm using was not available to talk on the phone on weekend. It was a total disaster because I do wp web design but I don't do the hard core programming so I don't really know where to look for the malicious code that was installed on my website. (Fixed now)

I have the plug-in that supposed to protect my site but it's annoying because even myself can't modify the contents.

I also recommend hostgator for their excellent customer service. They are available 24/7 on phone/chat and email.

Thanks for posting this article. Now I know what to do to protect every website I'm managing.



[Reply](#)Salman Ahsan [June 11, 2012 at 9:21 pm](#)

I hope your blog is healthy and live. Let me know if you need any assistance. Good luck

[Reply](#)Ligo George [June 11, 2012 at 12:37 am](#)

Thanks for the share.....Very useful.....

[Reply](#)Primeinspiration [June 22, 2012 at 9:10 am](#)

Dear Salman,

This article was really nice. Is hostgator really good in their customer service? want change my sites too on that. Most of the things (wp admin files and preventing script injection sections) are really new to me and very useful. Thanks

[Reply](#)Michael [July 4, 2012 at 6:56 pm](#)

Nice article...I recently received an email notifying me that WP firewall detected/prevented a Mysql attacks, so figured it's a good time for me to fortify my site a bit more. On #14, where do I paste the code snippet in the .htaccess file? top, bottom, in-between? Thanks so much

[Reply](#)Salman Ahsan [July 7, 2012 at 1:17 am](#)

Check out the latest blog post on wordpress malware prevention

[Reply](#)George [July 6, 2012 at 10:39 am](#)

Hi Salman

Great post, extremely thorough.

Apologies if I am being a newbie but I have posted the code into my htaccess file and uploaded but then I cannot access the site and it returns Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Any help would be appreciated, I think the stress of malware hackers may have addled my brain!!

Many thanks in advance

This is the code I am using:

```
#BEGIN WordPress
```

```
RewriteEngine On
```

```
RewriteBase /
```

```
RewriteRule ^index\.php$ - [L]
```

```
RewriteCond %{REQUEST_FILENAME} !-f
```



```

RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]

# END WordPress

## protect wp-config.php

Order deny,allow
Deny from all

## STRONG HTACCESS PROTECTION

order allow,deny
deny from all
satisfy all

## disable directory browsing
Options All -Indexes

## protect from sql injection
Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (\%3E) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|\\|%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|\\|%[0-9A-Z]{0,2})
RewriteRule ^(.*)$ index.php [F,L]

```

[Reply](#)Salman Ahsan [July 7, 2012 at 1:16 am](#)

Check out the new blog post on prevent wordpress malware attack 😊 Hope that helps

[Reply](#)George [July 7, 2012 at 9:09 am](#)

Thanks for that, another excellent article.

Your blog is EXACTLY what happened to me. It has taken 3 weeks to get back to recover. Your advice is invaluable.

I have download your htaccess file but still my wesite returns server error when I upload it.  
Any advice would be appreciated.

htaccess file below:

AddDefaultCharset Off

BEGIN WordPress

```

RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]

```

# END WordPress

RewriteEngine On

```

# proc/self/environ? no way!
RewriteCond %{QUERY_STRING} proc/self/environ [OR]

```



```
# Block out any script trying to set a mosConfig value through the URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]

# Block out any script trying to base64_encode crap to send via URL
RewriteCond %{QUERY_STRING} base64_encode.*(*) [OR]

# Block out any script that includes a tag in URL
RewriteCond %{QUERY_STRING} (!%3E) [NC,OR]

# Block out any script trying to set a PHP GLOBALS variable via URL
RewriteCond %{QUERY_STRING} GLOBALS(=|\\%[0-9A-Z]{0,2}) [OR]

# Block out any script trying to modify a _REQUEST variable via URL
RewriteCond %{QUERY_STRING} _REQUEST(=|\\%[0-9A-Z]{0,2})

# Send all blocked request to homepage with 403 Forbidden error!
RewriteRule ^(.*)$ index.php [F,L]

Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (!%3E) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|\\%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|\\%[0-9A-Z]{0,2})
RewriteRule ^(.*)$ index.php [F,L]

#Options +FollowSymlinks
RewriteEngine On
RewriteCond %{http_host} ^basketballchat.co.uk
RewriteRule ^(.*) http://www.basketballchat.co.uk/\$1 [R=301,L]

# Protect from spam bots

RewriteEngine On
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{REQUEST_URI} .wp-comments-post\.php*
RewriteCond %{HTTP_REFERER} !.basketballchat.co.uk.* [OR]
RewriteCond %{HTTP_USER_AGENT} ^$
RewriteRule (.*?) ^http://%{REMOTE_ADDR}/$ [R=301,L]

# STRONG HTACCESS PROTECTION

order allow,deny
deny from all
satisfy all

CheckSpelling On

# disable directory browsing
Options All -Indexes

order allow,deny
deny from all
```

[Reply](#)[Hostinpk July 11, 2012 at 3:55 am](#)

Thanks for such a nice post. Actually, wordpress sites are getting hacked due to outdated versions. We have more than 2000 wordpress installations on our servers and hacked day by day. However, I am sending an email to all clients about this tutorial and I hope that it will prevent hack attempts to some extent.

[Reply](#)



[Alex](#) [July 17, 2012 at 10:16 am](#)

Ahmad, Thanks to the brief and wonderful post and hope it is very useful for me to implement some security measures.

[Reply](#)



[Daryl Austman](#) [July 26, 2012 at 4:33 pm](#)

Boy, sure wish I had found this information earlier. I've been hacked several times on 3 of my sites. I've spent countless hours removing "pharma" links from within posts (most recently they were the -ads- type that seems to hide in an invisible link and which is attached somehow to a hackers bogus .htaccess file.

TONS of wasted time which I hope some of these helpful hints are going to make harder for that crud to infiltrate my sites. Thanks!! this is appreciated probably a lot more than you think.

[Reply](#)



[Salman Ahsan](#) [July 31, 2012 at 2:08 am](#)

I really appreciate your appreciation 😊

[Reply](#)



[Stephan Rees](#) [July 28, 2012 at 12:53 pm](#)

Many thanks for the article. Excellent advice on beefing up Wordpress security. Points 1-9 I had implemented already, but 10,11 & 14 were just what I was looking for.

However, I have been unable to implement #12 'Limit access to WP content directory files', as when I copy the modified code (to include pdf) into the WP content .htaccess file I am unable to access public pdf files.

Order deny,allow  
Deny from all

Allow from all

Also, I am cautious about implementing #13 'Protect WP Admin', as I sometimes travel and log on from other IP address. Also, I have a forum where users can register, so I imagine that could cause difficulties for registered or guest users?

[Reply](#)



[Salman Ahsan](#) [July 31, 2012 at 2:14 am](#)

You can skip the ip restriction as it wont make much differences. If you don't want to mess with the htaccess, simply use "Better WP Security" plugin and give it access to modify your htaccess. With just a click of a button, you will be able to protect your directories and tweak a lot of other security stuff 😊

[Reply](#)



[AshleyTisdale.org](#) [August 16, 2012 at 7:14 pm](#)

This article sounds very helpful!

However, if you don't mind, I'd like talking to you about our site's situation. We recently moved from cutenews to wordpress and since that, we've been hacked twice in less than 1 week. The first time happened after we launched the new sites look, only 2 days after, and the 2nd time was today but weirdly the site got back safe and as usual.

What would you suggest us to do to keep the hacker away? Apparently the hacker is the same person who hacked us the first time.



Please a help would be REALLY appreciated.

Thanks for your time... keep up the great work!

[Reply](#)



Salman Ahsan [August 25, 2012 at 5:08 pm](#)

do you have some personal issues with the hacker? 😊 just asking. Usually there is no reason for someone to hack your stuff. Did you also implement all the tips mentioned on this blog. If the problem continues, you may want to check out [Sucuri](#)

[Reply](#)



AshleyTisdale.org [August 25, 2012 at 8:36 pm](#)

Well, not that we are aware of lol... but apparently the situation has calmed down. We haven't been hacked/attacked by that hacker since when we changed a few things in the site access.

But thanks so much for your tips- we did get backup buddy anyway, just to feel safer and protected 😊

[Reply](#)



chris [August 19, 2012 at 6:23 pm](#)

Uggghhh...Hacked again for about the 12th time. I've been doing all the basics like making sure I update everything, and clean out all the stuff not used, updated passwords and logins etc.... I feel like I am a target to hackers.

Thanks for posting these tips and taking the time to be very detailed. I am so glad there are advanced things I can do to stop the hacking! I sure hope it stops it once and for all!

You have no idea how much your efforts are appreciated. Having something more to do gives me hope! It so much better that not knowing if there is more I can do and then get hacked again. I have over 20 sites to repair everytime it happens. What a nightmare.

[Reply](#)



Salman Ahsan [August 25, 2012 at 5:33 pm](#)

did you implement all the tips? its really weird that you are experiencing this very often. Are you sure you know whats going on? I am not doubting your skills or expertise but you may want to check out [Sucuri](#) and hire them for monitoring your blog network. If you know the hacker, you can easily block them. If its a range of bots then you can block the ip range. Unless I know the specific problem, the solution might be vague.

[Reply](#)



Shah Nawaz [September 5, 2012 at 3:02 am](#)

This is amazing article on wordpress security to protect wordpress from assholes hackers

[Reply](#)



Brian [September 6, 2012 at 3:38 pm](#)

Just giving a heads up:

Order deny,allow  
Deny from all



Allow from all

— Gives an internal server error

```
# deny access to wp admin
```

```
order deny,allow
```

```
allow from xx.xx.xx.xx # This is your static IP
```

```
deny from all
```

— Gives a forbidden error even when not on the admin page (yes, I changed the IP too, haha)

[Reply](#)



Salman Ahsan [September 24, 2012 at 8:44 pm](#)

Thanks Brian, appreciate the contribution. I will check out all the codes and update this post very soon.

[Reply](#)



DG [October 11, 2012 at 5:58 am](#)

Thanks Salman for your specific details. You are different from other “experts” who just write general stuff like “install anti-virus” blah blah.

I have a non-wordpress site that has been hacked, and I will implement your tips.

[Reply](#)



Salman Ahsan [October 19, 2012 at 9:10 pm](#)

Thanks DG 😊 If you know a little coding or have some skills then you can easily modify this htaccess and use it on any non wordpress related sites

[Reply](#)

Leave a Comment

**Commenting Policy:**

\*Keywords instead of a real name? Comment gets deleted.

\*A fake name instead of your real name? Comment gets deleted.

\*1 liner "thank you" comment or offtopic? Comment gets deleted.

\*If the comment gets approved, we own all rights to it.

*All comments are subject to moderation.*

Name \*

E-mail \*

Website

Anti-Spam: What is 10 + 4 ?



☐ Notify me of followup comments via e-mail

Submit

- [← Previous Article](#)

[Top 3 WordPress Infographics](#)

- [Next Article →](#)

[5 Simple Tricks to Prevent WordPress Spam Comments](#)

- **looking for something?**

To search, type and hit ente

- **Latest Blog Posts**



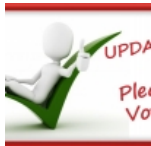
#### [How to Use Facebook Timeline without Annoying Your Friends](#)

Facebook Timeline is probably one of the biggest tweaks to this social networking service. Wheth[...]



#### [10 Methods that will Increase your Twitter Followers by 75%](#)

Twitter is getting big and it will continue to get bigger. Their interface has improved as well [...]



#### [You Ask, I Give : Please Vote!](#)

Hello friends, hope everyone is doing well :). It's been a while since I made my last post on th[...]



#### [9 Killer Ways to Make Your Blog Popular](#)

I have been working on my blogs for a while and every time I tweak something, I learn something [...]





#### [4 Methods to Gain More Twitter Followers for Free](#)

Twitter is huge, no doubt. And this giant microblogging platform is growing rapidly. Its users a[...]

- **Connect & Subscribe**



- 

SignUp for the  
Upcoming "VIP  
Blogging  
e-Course"

Email Address

Free Instant Access

We hate spam as much as you do.



- 

[Disclaimer](#) | [Privacy Policy](#) | [Advertise](#) | [DMCA](#)

© 2009 Onwards MastermindBlogger.com & Ahsan Media LLC

