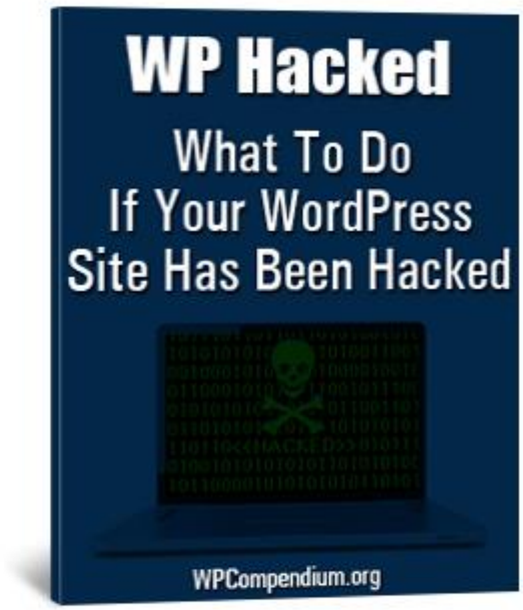
What To Do If Your WordPress Site Has Been Hacked



WPCompendium.org

What To Do If Your WordPress Site Has Been Hacked

Backups are absolutely vital for website security and peace of mind!

As Benjamin Frankin once famously declared, “an ounce of prevention is worth a pound of cure.”

WordPress is a secure platform. If, however, your website has been compromised and you did not back up your WordPress site and data, then, unfortunately, there is very little you can do other than to reinstall WordPress and start again from scratch, or go through the painstakingly difficult process of trying to clean and recover your WordPress installation.

If you have set up the WordPress Maintenance System recommended in our WordPress Management Tutorials, then you should have all of your website’s data and files backed up, as well as a record of your email accounts, copies of any downloadable files you offer on your site (e.g. bonus reports for subscribers, etc.), additional content, etc. and this will make getting everything back up and running a lot easier, a lot faster and a lot less painful.

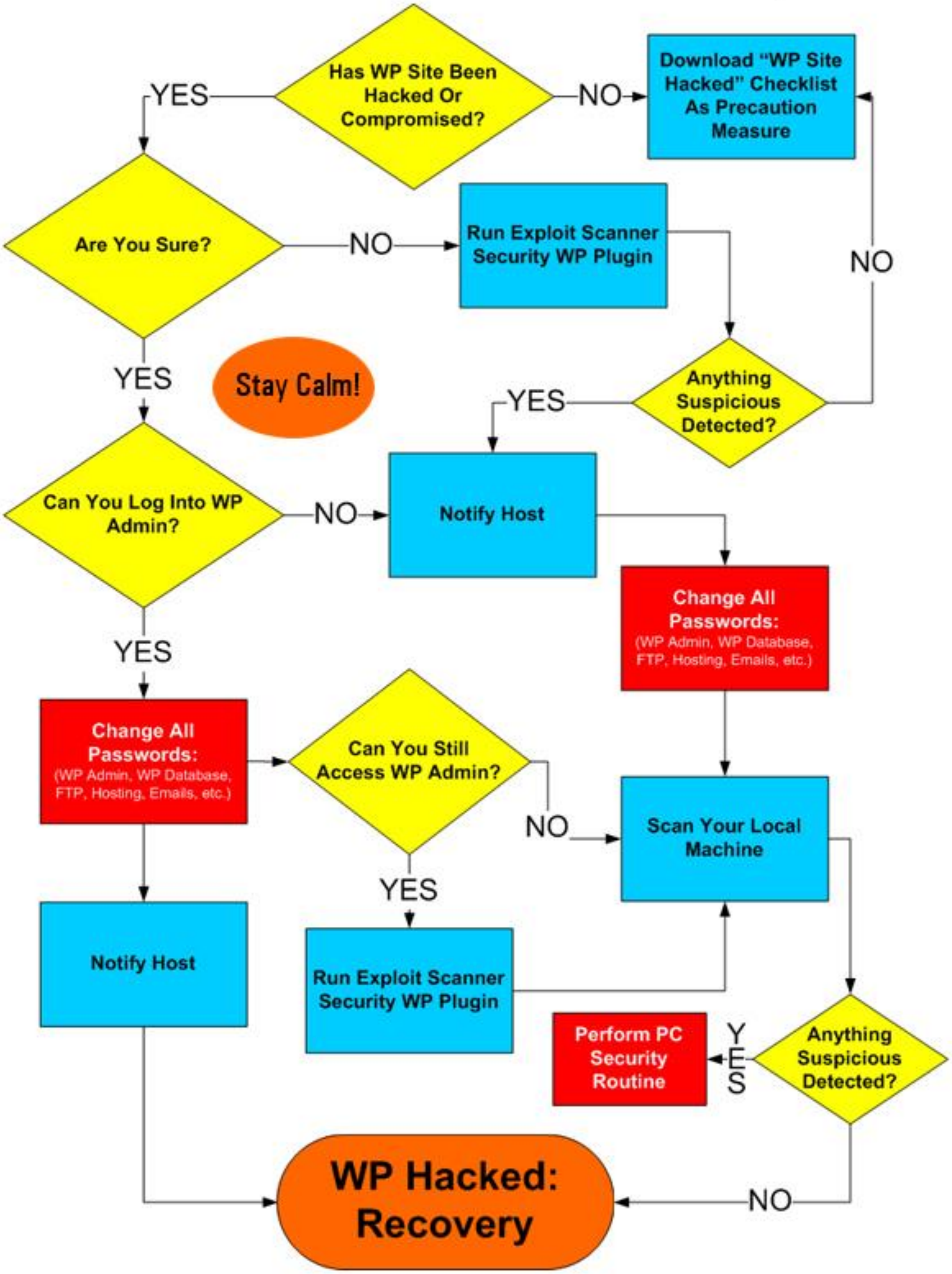
▶ **WordPress Management Tutorials:** http://wpcompendium.org/wordpress-management-tutorials

If your WordPress site has been hacked, or if you suspect that someone has compromised the security of your site, then follow the immediate steps provided below.

Note: Depending on your site, the urgency and nature of the attack, and the level of damage caused, you may not want to go through the process below yourself. If so, we recommend using the services of a professional website security expert!

***

WordPress Site Hacked: Immediate Action Steps


Has WP Site Been Hacked Or Compromised?
YES
NO
Download "WP Site Hacked" Checklist As Precaution Measure
Are You Sure?
NO
Run Exploit Scanner Security WP Plugin
NO
YES
Stay Calm!
Anything Suspicious Detected?
YES
Can You Log Into WP Admin?
NO
Notify Host
Change All Passwords:
(WP Admin, WP Database, FTP, Hosting, Emails, etc.)
YES
Change All Passwords:
(WP Admin, WP Database, FTP, Hosting, Emails, etc.)
Can You Still Access WP Admin?
NO
Scan Your Local Machine
YES
Notify Host
Run Exploit Scanner Security WP Plugin
Perform PC Security Routine
YES
Anything Suspicious Detected?
WP Hacked: Recovery
NO

WordPress Site Hacked – Immediate Action Steps

Here are the immediate action steps to take if you suspect that your WordPress site has been hacked:

Stay Calm

The first thing you need to do with any incident that involves security is to stay calm. This will help you think clearly as you go through the next steps, and prevent you from making any mistakes that can make your situation worse.

So … take a deep breath and calm yourself down before you do anything else …

Assess The Situation

The next step is to assess the situation. You want to be sure that your site has indeed been hacked before you take any drastic measures like shutting your entire business down online and/or deleting your entire site.

Sometimes things just act up. It could be that a plugin or application displays a weird WordPress error message, or your server temporarily goes down and your database stops working, or something just goes screwy.

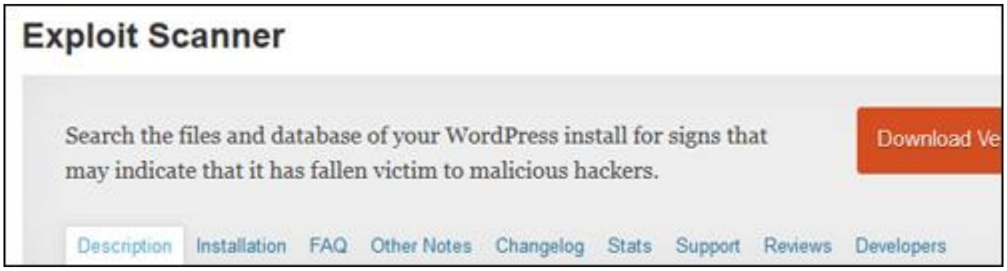
For this reason, it’s important to stay calm. If you are not sure whether your site has indeed been hacked or not, then do the following:

1. *(Optional):* Go through our WordPress Troubleshooting Section information and make sure that you’re not just experiencing an error with your site that can be easily fixed.

▶ *To learn how to fix common WordPress errors, see the tutorial below:*

▶ **How To Fix Common WordPress Errors:** http://wpcompendium.org/wordpress-management-tutorials/wordpress-troubleshooting-tutorials

2. Download and install the **Exploit Scanner** plugin if you can log into your site. This plugin can help detect any damage to your site so that it can be cleaned up.



Exploit Scanner

Search the files and database of your WordPress install for signs that may indicate that it has fallen victim to malicious hackers.

- **Exploit Scanner:** https://wordpress.org/plugins/exploit-scanner

3. If you can’t log into your site or if you detect anything suspicious, notify your host immediately.

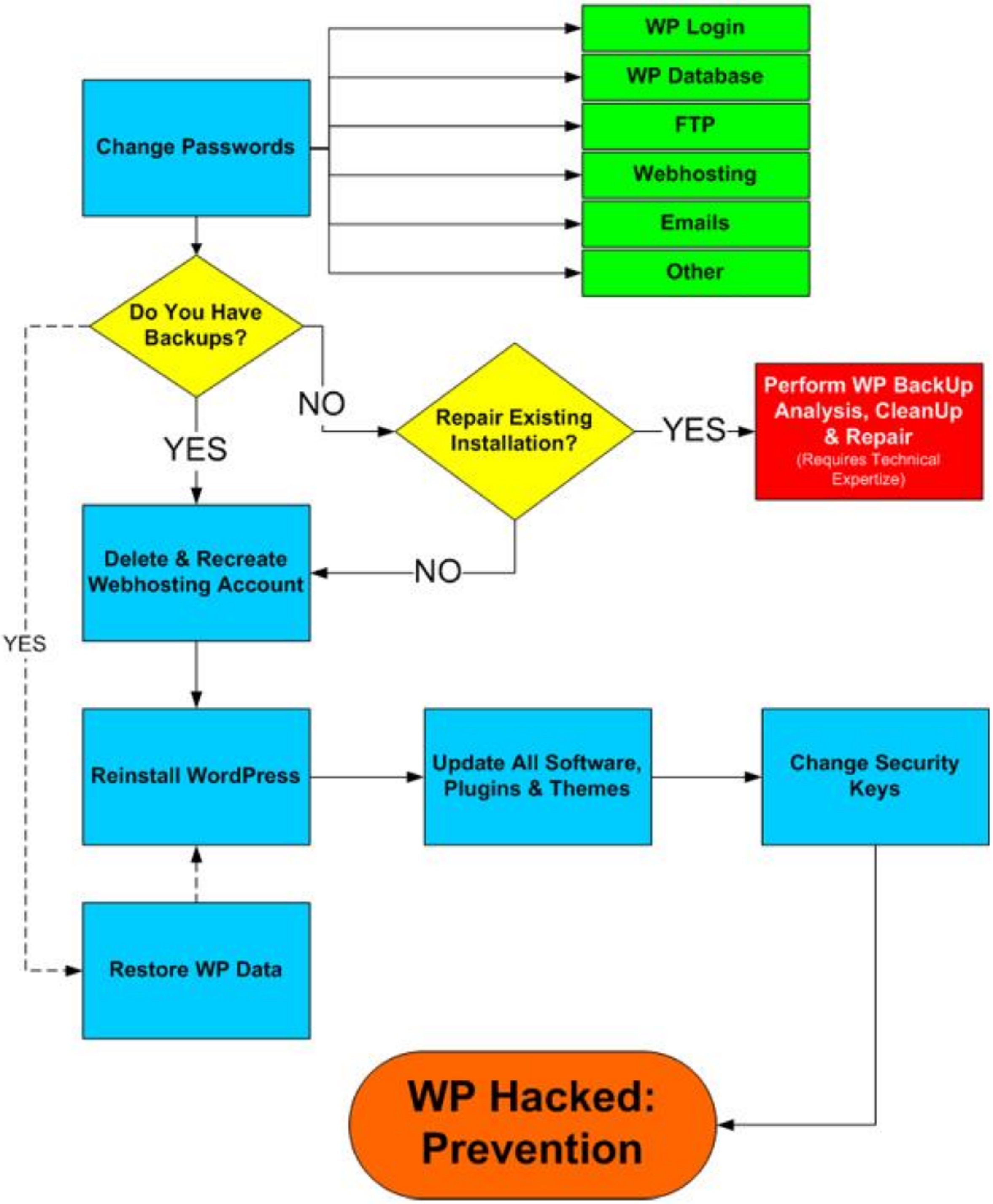
4. If you detect or suspect that any malicious code may have been injected into your website, then your machine may have been compromised. You will need to scan your hardware devices (e.g. laptop) for malware.

- *To learn more about securing your devices, see the tutorial below:*

- **Your Device - Computer Security:** http://wpcompendium.org/wordpress-security-tutorials/your-devices-computer-security

***

WordPress Site Hacked: Recovery Action Steps


Change Passwords
WP Login
WP Database
FTP
Webhosting
Emails
Other
Do You Have Backups?
NO
YES
Repair Existing Installation?
YES
Perform WP BackUp Analysis, CleanUp & Repair
(Requires Technical Expertize)
NO
Delete & Recreate Webhosting Account
YES
Reinstall WordPress
Update All Software, Plugins & Themes
Change Security Keys
Restore WP Data
WP Hacked: Prevention

WordPress Site Hacked – Recovery Action Steps

Try To Regain Control

The next step is to try and get control of the situation if you can.

Depending on the nature of the attack, you may or may not be able to access your site.

In some cases, it may be possible to 'clean' up your WordPress installation and remove any malicious code your site has been infected with.

Tip: If you can't login to your site, try simply deleting your .htaccess file. This usually solves many WordPress-related problems. If you have followed our WordPress maintenance tutorials, you should a backup of your files, including a copy of your .htaccess file.

▶ **WordPress Maintenance Tutorials:** http://wpcompendium.org/wordpress-management-tutorials/wordpress-maintenance-tutorials

If you can access any of your hacked files and database, then we recommend backing these up to a removable stick drive before deleting them from your hard drive or server.

This way, you can analyze your files for problems later (open source tools like OSSEC - http://www.ossec.net - can analyze your logs and help you find where/how the attack happened), or send them off to a security expert for a 'forensic' investigation, or refer to them if you ever need to. Just remember to label the files as your 'hacked site backup' to avoid recreating the problem.

If you can access your site and you have determined that you site has been compromised, then do the following:

1. Change Passwords

Change passwords immediately for all of the following:

- Your WordPress Site Login Password. Change passwords for all users, especially Administrators and Editors. This is especially important if you upload files to your site via FTP.
- Your WordPress Database Password.
- Your FTP Password
- Your Webhosting Account Password.
- Your Email Account Passwords.

- Any other passwords associated with your site.

Note: Changing some of the above passwords will most likely “break” your site (i.e. your website will stop being visible). Given the nature of the circumstances, however, this may not necessarily be a bad thing.

If your site has indeed been compromised and unwanted messages (e.g. spam) were being displayed on your site, then having your site no longer being visible will prevent your site visitors from seeing any offensive, disturbing or inappropriate content, protect the reputation of your site and help you avoid getting blocked by search engines, or even shut down by your host.

2. Reinstall WordPress

In the most severe of circumstances, if your site has been badly compromised, or you have been locked out of your own site and can’t get back in, the safest thing to do is to simply delete everything and reinstall the latest version of WordPress.

If you have a recent back up of all of your site’s data and files, you can simply delete and recreate your hosting account, then perform a new WordPress installation and re-import all of your backed up data.

Note: Finding and removing malicious code from web files is a technically difficult area, and, therefore, outside the scope of these tutorials.

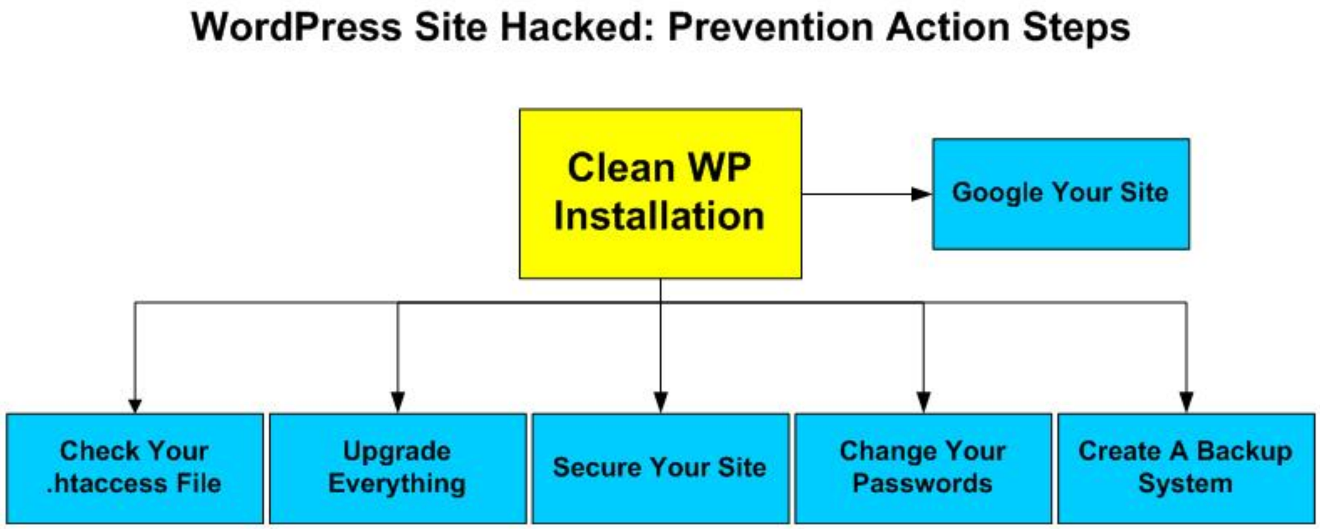
3. Update Plugins And Themes

After reinstalling WordPress, make sure that all of the plugins and themes you have reimported are up-to-date.

4. Update Your Security Keys

If a hacker steals your login details and they are logged into your site, they will remain logged in even if you change your password, because their browser cookies are still valid, and WordPress stores login session information using browser cookies.

To disable the cookies, you will need to create a new set of ‘security keys’ and replace your existing keys with the newly-created ones.



WordPress Site Hacked – Prevention Action Steps

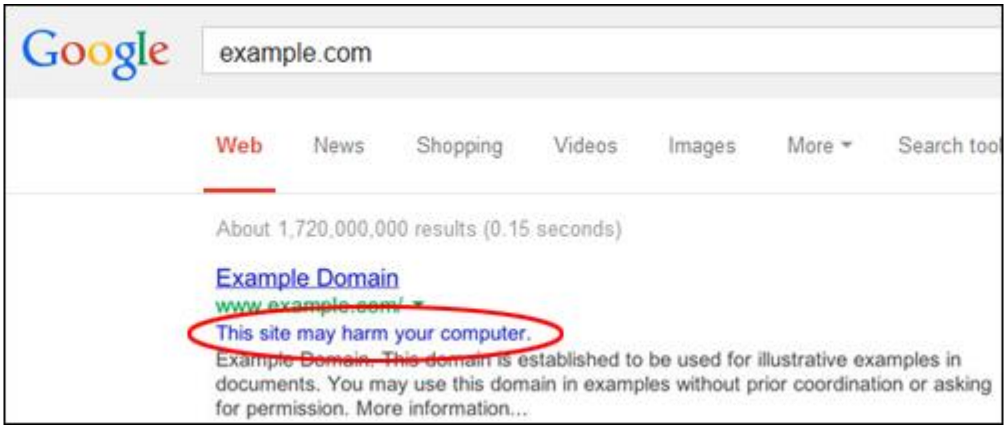
Analyze What Happened

If you can find out how your website was hacked, you can help to prevent it from happening again (or at least try and prevent it from happening again *in the same way!*)

Here are some things you can do:

Google Your Site

Google your site address to see if your site has been blacklisted.



About 1,720,000,000 results (0.15 seconds)

Example Domain
www.example.com/
This site may harm your computer.
Example Domain. This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information...

To remove your site from Google's blacklist you will need to make sure that all of the security issues listed have been addressed and fixed before requesting Google to review your site.

Check Your .htaccess File For Hacks

Hackers can use your .htaccess file to redirect your site visitors to malicious sites.

If your WordPress installation is located in a subdirectory of your domain (e.g. yourdomain.com/blog), then look in the main folder's .htaccess file as well. Hackers will try to hide their code at the bottom of the file, so scroll down.

Something else that a hacker may do is change the permissions of the .htaccess file to prevent you from editing the file. To make your file editable, change the file permission back to 644.

Upgrade Everything

Once you have a clean WordPress installation, make sure you upgrade your WordPress installation, plugins and themes to their latest version. Older versions are more prone to hacks than newer versions.

Secure Your Site

After successfully recovering or reinstalling your site, make sure you secure it by implementing at least some of the recommended security measures in this training module (WordPress Security Tutorials).

Change Your Passwords Again

If you only changed your passwords after discovering the hack, change them again after securing your new WP installation and making sure that your new site is clean.

Start Backing Up Regularly

After recovering from the nightmare and heartache of having your website hacked, it's vitally essential that you learn how to start performing regular backups of your WordPress database and files.

This way, if your site ever gets hacked again, all you will need to do is restore your data and files from your last clean backup, and change your passwords and secret keys, and you'll be back to normal again.

To ensure continuous WordPress site security, complete all of the WordPress Security Tutorials at WPCompendium.org

http://wpcompendium.org