TORQUE®

SO YOUR WORDPRESS SITE JUST GOT HACKED, NOW WHAT?

A Digital Marketing Guide

WHITE PAPER

WP engine®

Getting your WordPress site hacked is unarguably one of the worst things that can happen to a website owner. It's super stressful and impacts your business, reputation, search rankings, traffic and much more.

A while ago we talked about how WordPress websites get hacked and what you can do to prevent it from happening. However, what if it's already too late? How do you recover a WordPress website that has already been hacked?

In this white paper, we will look into how to spot whether your WordPress website has been compromised and what to do if it has.

Is It Hacked? How to Spot a Compromised WordPress Website

When it comes to getting your site hacked, it's important to keep in mind that this is not a WordPress-specific issue. Basically anything that is connected to the internet can potentially be hacked (just ask Sony) and no platform is one hundred percent secure.

That's just how it is. It's part of owning a website like the risk of having your car stolen is part of driving one. There are things you can do to prevent it, but it might still happen.

However, how can you even tell that your site has been hacked? What are the signs of a hacked website? Here are a few:

- **Security plugin sends you a warning** - If you are using one of the many security plugins out there, chances are good that you will get an email warning the moment your site gets compromised. As far as hacks go, this is the optimal scenario as it enables you to react immediately.
- **Unable to log into your admin panel** - One of the most common security breaches is someone stealing your login information (or obtaining it via brute force). In that case, they might hijack your administrator account so that you can no longer access your own site and you will have to take special measures to get back into it.
- **WordPress site redirects to another website** - A common way hackers use hijacked websites is by redirecting visitors to porn sites or other non-desirable web entities. If you notice this or a visitor emails you about it, you can be sure that someone got unauthorized access to your server.
- **Site displays strange links** - A more subtle variant of moving visitors to other websites is to place spammy links on the hacked site. For that reason, it makes sense to check your site regularly and see if everything is as you remember it.
- **Google marks site as insecure** - Google will sometimes mark hacked sites as insecure in the search results (if it doesn't remove them from the results page altogether). In addition to that, Google Search Console will also likely alert you under *Security Issues*.

- **Warning from your browser** - Chrome and other browsers warn users when they detect phishing attacks, malware, cross-referencing or other bad stuff on a website they are trying to access. If you or someone else gets a warning for your site, you will have some work to do.
- **Web host takes your site offline** - If your hosting company gets a notification that your site has been compromised, most likely you will me taken offline. Because they are managing your security, they will know before you will. Taking the site down will stop the hacker from accessing other sites the company manages.
- **Security scan shows problems** - Often infections are well hidden and not easily detectable. For that reason, proactive website owners do well to run a malware scan every now and then. Sucuri Site Check is a good option. This way, you will learn about compromises and can address them.
- **Sudden traffic spikes** - Hackers sometimes use hacked websites as clean fronts for their own malware-riddled and flagged sites. To avoid spam detection, they will link to your domain and then redirect visitors to another site. If you see some unexplained traffic spikes, consider running a malware scan.

While this list isn't exhaustive, it does cover a good number of ways to spot whether your site has been hacked or not. If in doubt, run a security check. However, what to do if it finds something? That's what we will get to now.

So, You Had Your WordPress Website Hacked - What to Do Now?

In the following, we will first give you some general advice on how to deal with your hacked website. After that, we will go through different scenarios that you might be confronted with and offer a step-by-step approach to fixing them.

1. Stay Calm

The best thing you can do in this kind of situation is to keep cool. While it's natural to want to fix the problem as quickly as possible, rash actions can cause as much damage as they can help get things under control.

For that reason, the first order of the day is to take a deep breath, try to relax and analyze the situation before jumping into action. This gives you a chance to develop a game plan and deal with things rationally without making it worse.

2. Make a Backup of What You Have Left

While it seems counterintuitive to make a backup of a hacked site, it's important to keep in mind that it contains a lot more than just the (corrupted) system files.

Some hosting providers will automatically delete websites from their servers that have been compromised. Since images and other media are hard to replace once they are gone, it's a good idea to keep a copy around in case you need to rebuild the site later.

For that reason, as a first step, try to salvage what you can. There are plenty of backup solutions for WordPress out there and you can also backup WordPress manually. Do this but be sure to mark it clearly as a hacked backup.

3. Scan Your Local Machine

In many cases, the hack can actually start on your computer. If a hacker has compromised your system, it's entirely possible for them to extend their reach to the websites you frequently log into (e.g. via a keylogger).

Install and run a full virus/malware scan on your local machine and make sure your OS is up to date. This way, you can make sure the problem didn't come from your computer and reduce the risk of being reinfected after cleaning up the mess.

4. Hire a Professional

Website security is a serious matter. If you are not comfortable dealing with code, servers and other technical stuff you might be better off hiring someone else to do it.

Hackers are also a sly bunch and sometimes hide things in several places to be able to reestablish the hack after your clean up. For that reason, paying a professional to take care of your site can be the best option and will often save you time.

Of course, for people who like to do things themselves, we also have plenty of material below. Just keep in mind that having someone else deal with the mess can also be an option.

5. Talk to Your Hosting Company

The first address in this kind of situation should always be your hosting company. Good quality providers are prepared for these emergencies and can offer assistance. They also have staff at hand who know their way around the hosting environment and might be able to fix things for you.

Also, your host will be interested in hearing about this as a hack can often affect more than one site. Especially in shared hosting environments, if a someone got unauthorized access to the server, they might have compromised more websites on the same machine.

At the very least, talking to your host might give you additional information on how to fix the situation.

6. Restore from Backup

If you regularly back up your site (which you know you should), recovering from a hack might be as simple as restoring an earlier version.

How to Recover a Hacked WordPress Site if You Still Have Access to the Backend

So, your site got hacked but you can still access the WordPress dashboard? In that case, you can assess the problem with the following steps.

1. Change Your Password

If you suspect or know that your site has been hacked, the first thing to do is to change your password. That way, it will keep anyone who has illegally obtained your login information from logging in again.

This isn't foolproof (in fact, we will ask you to change your password once more further below) but it's an important first step. So, do it now, I'll wait.

And while you are at it, force all other users with admin rights to change their passwords as well. The Expire Passwords plugin can do this for you. Alternatively, you can also simply change their passwords manually inside the Users menu and then email the new passwords to them.

2. Scan for Malware

Next up we want to find out where exactly the compromised files are on our site. A good first step to eliminate hiding places is to delete any inactive themes and plugins. This is often where hackers hide their backdoors (programs that allow them to access your site or server without normal authentication).

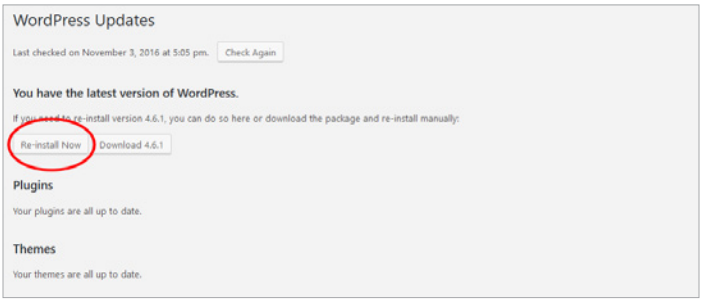
After that, it's time to scan the entire site. You can use the Sucuri Malware Scanner plugin for that. Once installed, it will scan all your WordPress core files for integrity and can also tell whether your site has been blacklisted for sending spam or some other reason.

If you don't want to use a plugin, below we also have a list of external scanners to use for this purpose. Also, as mentioned, Google Search Console might have some input on where to find the compromised files.

3. Replace Compromised Files with Originals

If malicious code is found in any of the files on your site, a simple fix is to delete and replace them with their original (unhacked) versions.

For example, you can replace WordPress core files with a fresh install without breaking your site. As long as the *wp-content* folder stays intact, everything should be able to go back to normal. In fact, the simplest way to do that is to just go and re-install WordPress from inside the dashboard.



The same goes for theme and plugin files (though you might lose theme customizations if you have made any and are not using a child theme). Of course, if there are files that have simply been added, you need to delete those.

4. Check User Permissions

WordPress user roles exist to control what users can and cannot do once logging into the dashboard. Administrator rights should only be given to people you explicitly trust.

For that reason, after a hack, it's a good idea to have a look around the *Users* menu to see if there is anything suspicious, like an administrator user you don't recognize.

5. Change SALTs (Secret Keys)

```
define('AUTH_KEY',         '3m i3Jb.1SsZ&>K)9CLY3IHzS)^blfsv#Zr+7+fuMQbZ(=|1.6.WUACa|pc].9Bw');
define('SECURE_AUTH_KEY',  '49Utvr.V$|H<VMtkRA=%+>]4d8nVg,@FpBvRP~nfPz230WAIsH376(1GZZ=r1g(U');
define('LOGGED_IN_KEY',    '=Gs^2-e-O([3DY+YK+G)WuwQbb3&$]XD6D M]94BjufwLzA9Z9P(P{ d|]#I#5rx');
define('NONCE_KEY',        '@xe|+NyU:0jkPKT~gEt!~*B2h^ElW*BMS~GkI_1YW:p_HR@V*t-QEl(]%b&&CtUe');
define('AUTH_SALT',        'w.son,2xz^JR3~f)n_jIdHIisM?eZ ckEt;X]%lI@q:?w?Y)=j4(w,c9a38Q(2S:');
define('SECURE_AUTH_SALT', 'IO)uL+$Tg|nwdxG$^4=}*f<CZEKDB)> 5M4(n>Ev1+J+w1Kpmo~K(bB14V_hDynT');
define('LOGGED_IN_SALT',   ';xKX$((o>Y/JA|Y+rIdoqR4/IL8`(vLLis9nguz6iOQvpjh76`:xa;%+X;Jx#(NR');
define('NONCE_SALT',       'mq8BIc@3dt*gh36ac(||bEIz_4+*k)sWZGQicpK2,]&Ok^d)Xj-%>Ms:I FX)Ht,');
```

We already mentioned SALTs in our article on how WordPress websites get hacked. These are secret keys which help encrypt important information inside cookies. If someone accessed your website after having stolen your password, they might still be logged into it. You can change this by generating new SALTs and replacing the ones present in your *wp-config.php* file.

Note that this happens on your server, so you will need FTP access or some other way to get into it.

6. Change Your Password Once More

Yes, we know you already changed your password in the beginning. However, now it's time to do it all over again including everything else that's important:

- Hosting admin backend credentials
- FTP login
- MySQL database password
- Admin email address

Only then can you be sure that you have plugged the security leak for the future.

7. Harden Your Security

The final step for dealing with a hacked WordPress website is to make sure it doesn't happen again. That means upping your security measures. Here are a few good places to get started:

- How WordPress Websites Get Hacked (And What to Do About It)
- Hardening WordPress
- WordPress Security: The Ultimate Guide

Seriously, do it now. It's the only way to keep stuff like this from happening again. While there is no absolute guarantee, it does make the worst case scenario a lot less likely.

8. Rebuild Your Site

After you have taken care of the hack and secured your site for the future, you might still have to roll back some things that got lost during recovery. We are talking about blog posts, theme customizations and other things that might have vanished due to the hack.

If you have them saved somewhere (such as on a local WordPress installation), you are golden. In that case, all you need to do is re-implement them. If not, it might take some time to get your site back to what it was before the hack.

A hint for lost blog posts: check if you can find them in your RSS reader. If you have subscribed your own feed, the posts might still be there so you can at least get those back quickly.

Site Recovery With No Access to the WordPress Dashboard

Things change a little if you discover you have been hacked but can no longer get into the WordPress backend.

1. Reset the Administrator Password via phpMyAdmin

If you can't log into your site, it might be because the hacker has changed the password of your admin account. The good news is that you can get around this by resetting the password inside your database via an admin tool like phpMyAdmin.

Another possibility is to replace your email address instead and then go back to the login screen to get a new password via the recovery function. Of course, this option only exists if you can still access the login screen. Should your site be gone altogether, you will have to go a different route.

2. Find Affected Files

Even if you can't access your backend at all anymore, the recovery process is still similar to what we described above. You first need find the corrupted files and then delete them or replace them with a clean version.

To find the corrupted files on your server, the best option is to use an external scanner. Here are some options:

- Unmask Parasites
- Web Inspector
- Sucuri Site Check
- Norton Safe Web
- Quttera
- Scan My Server
- Virus Total

Since each of these scanners has their own strengths, it's best to run several or all of the them to make sure you don't miss anything.

Apart from that, your web host can often help you find hacked files on the server. Other sources of information are Google Search Console your server logs. Jenni McKinnon has written an excellent article on the latter over at WPMU Dev.

3. Replace Corrupted Files

Once you have located them, replace or delete the hacked files.

For that, will need to have FTP access or an administration backend like cPanel that lets you access file system on your server. From here, go through the entire list of corrupted files and make sure you take care of each and every one of them.

4. Re-Run Security Checks

Once you are done with that, run the security scans again. That way, you can be sure you have not forgotten anything.

Here is another time to contact your hosting provider and make sure you're site is back online.

5. Finish Up

Once you have cleaned up the hack, you will have to take the same steps mentioned earlier to increase your website security and recover anything that has been lost in the process:

- Check user permissions
- Change passwords
- Replace secret keys inside wp-config.php
- Rebuild website

With the above steps you should be able to get your hacked WordPress site up and running again. Hopefully, this will never happen again.

Getting Hacked Sucks But It's not the End of the World

Having your WordPress website hacked is not a pleasant experience and nothing any of us hope for. However, it does happen, even to the best of us.

If the worst has come to pass, we hope this guide can help you figure things out and get back to normal. Should the above information not be enough to take back control of your site, don't hesitate to hire a professional. If your website is part of your livelihood (as it is for many of us), that's a sensible investment.

After that, please definitely make sure to improve your security and patch any holes you found in the process. Future you will thank you.

About WP Engine

WP Engine powers amazing digital experiences for websites and applications built on WordPress. The company's premium managed hosting platform provides the performance, reliability and security required by the biggest brands in the world, while remaining affordable and intuitive enough for smaller businesses and individuals. Companies of all sizes rely on WP Engine's award-winning customer service team to quickly solve technical problems and create a world-class customer experience. Founded in 2010, WP Engine is headquartered in Austin, Texas and has offices in San Francisco, California, San Antonio, Texas, Limerick, Ireland and London, England.

About Torque

Torque is a news site featuring all things WordPress. We are dedicated to informing new and advanced WordPress professionals, users, and enthusiasts about the industry. Torque focuses primarily on WordPress News, Business, and Development, but also covers topics relating to open source and breakthrough technology. Torque made its debut in July 2013, at WordCamp San Francisco, and has since produced valuable content that reflects the evolution of WordPress, both as a platform and a community. Torque is a WP Engine publication, though maintains complete editorial independence. [*torquemag.io*](torquemag.io)

WP Engine 504 Lavaca Street, Suite 1000, Austin, Texas 78701 info@wpengine.com wpengine.com

WP-WP-SoYourWordPressHacked-v02