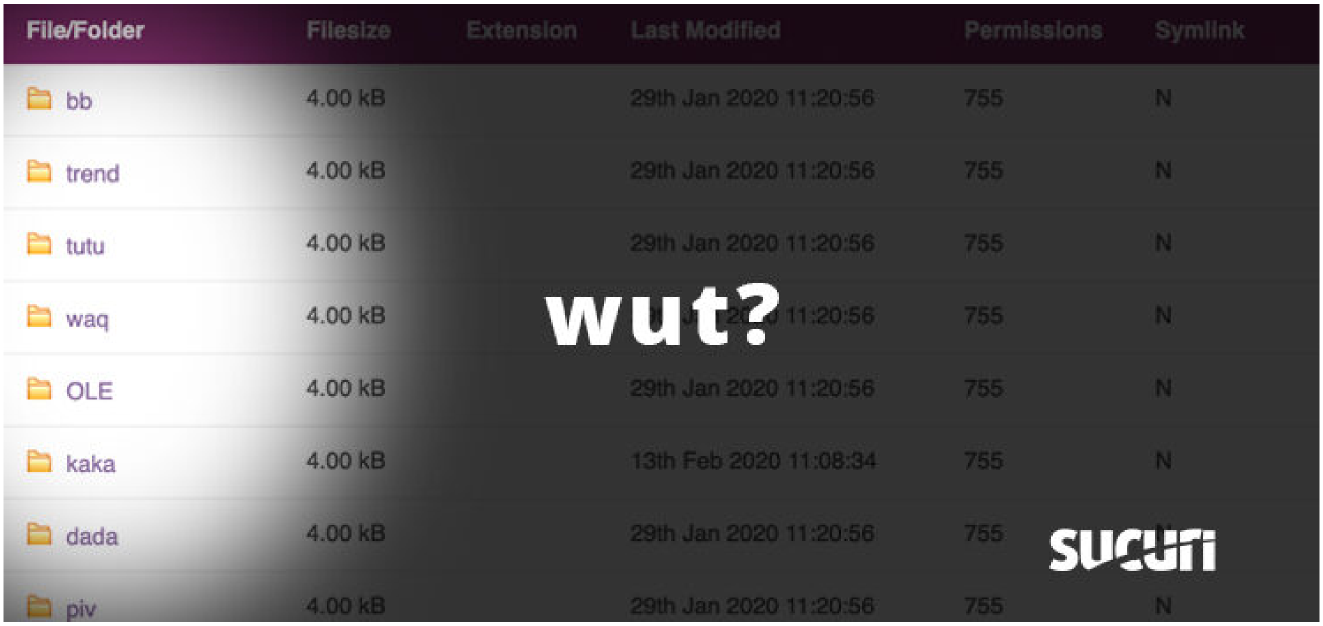
Sucuri Blog

blog.sucuri.net/2020/06/gibberish-hack.html

Justin Channell

June 12, 2020



File/Folder	Filesize	Extension	Last Modified	Permissions	Symlink
bb	4.00 kB		29th Jan 2020 11:20:56	755	N
trend	4.00 kB		29th Jan 2020 11:20:56	755	N
tutu	4.00 kB		29th Jan 2020 11:20:56	755	N
waq	4.00 kB		[illegible] 11:20:56	755	N
OLE	4.00 kB		29th Jan 2020 11:20:56	755	N
kaka	4.00 kB		13th Feb 2020 11:08:34	755	N
dada	4.00 kB		29th Jan 2020 11:20:56	755	N
piv	4.00 kB		29th Jan 2020 11:20:56	755	N

Discovering some random folder with numbers and letters you don't remember on your website would make any website owner put on their detective cap. At first, you may think, "Did I leave my FTP client open and my cat ran across the keyboard?"

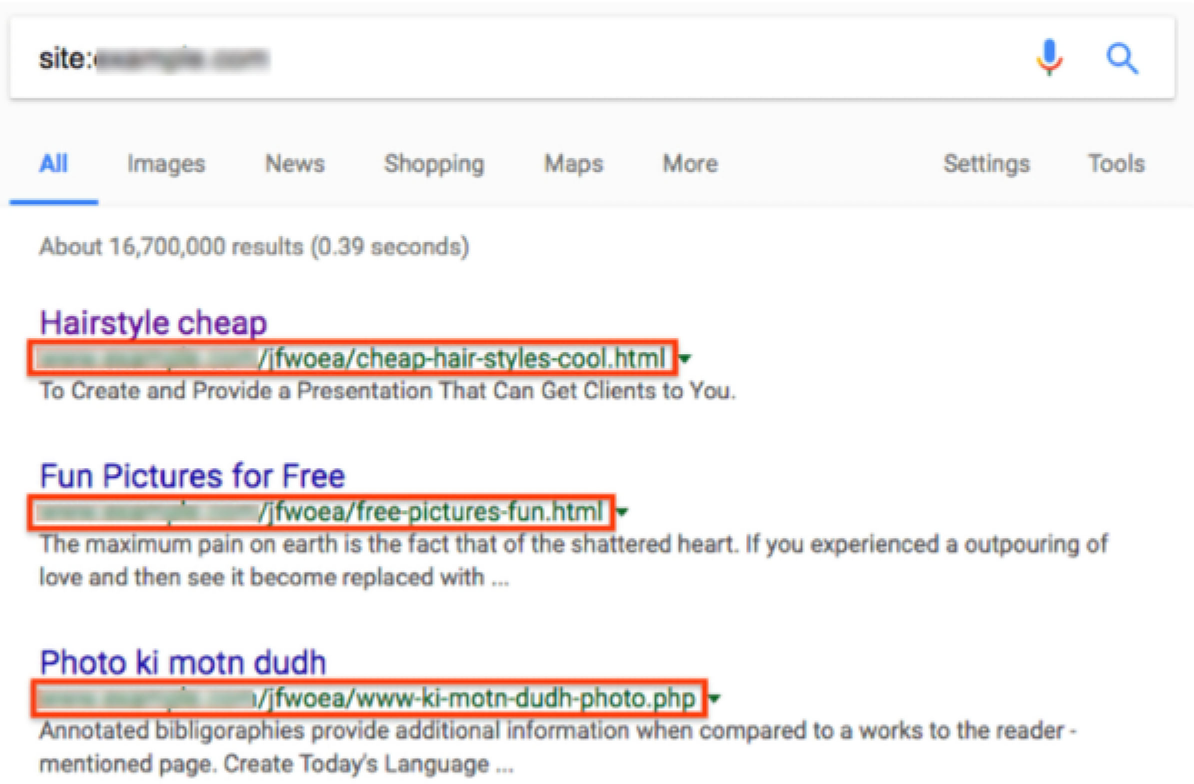
But when you open the folder, you find a series of HTML files, each named with some kind of nonsensical phrases like "cheap-cool-hairstyles-photos.html." If you open one of these files on the browser, you'll likely be redirected to something you're not expecting, such as a suspicious ecommerce site or an error page.

These are signs that your website was hit with a gibberish hack. Removing this hack is not just as easy as deleting a random folder. Even though it just seems like the hackers are putting a bunch of nonsense on your site as a defacement, these attacks are far more nefarious than you'd expect. It works similar to the Japanese keyword hack we covered on the blog earlier this month.

Random folder on a website

Hackers put random folders on websites to conceal pages with URLs that will look appealing in search results. Attackers sometimes store these URLs in folders with random numbers and letters. This is in the hope that less savvy website owners will assume that they are CMS core files.

The goal of a gibberish hack is to use a legitimate website's good standing with Google's search engine to generate traffic to another website. In the example from Google below, we see some of the examples like "cheap-hair-styles-cool.html" and "free-pictures-fun.html."



site:[redacted]

About 16,700,000 results (0.39 seconds)

Hairstyle cheap
[redacted]/jfwoea/cheap-hair-styles-cool.html
To Create and Provide a Presentation That Can Get Clients to You.

Fun Pictures for Free
[redacted]/jfwoea/free-pictures-fun.html
The maximum pain on earth is the fact that of the shattered heart. If you experienced a outpouring of love and then see it become replaced with ...

Photo ki motn dudh
[redacted]/jfwoea/www-ki-motn-dudh-photo.php
Annotated bibligoraphies provide additional information when compared to a works to the reader - mentioned page. Create Today's Language ...

Hackers will make money by sending traffic to their sites, so they want to keep the hack going as long as possible. They will do this through **cloaking** – or hiding the content on your site in a way that is hidden from you, but is visible to your visitors. There are many different methods of cloaking. A basic cloaking techniques include formatting text to blend into the background color. A more sophisticated method involves injected code that displays one page when a search engine indexes the page, and a different page for a human visitor.

These methods can also be targeted in order to keep the malicious code secret from the website owner. In this case, a gibberish page may display 404 error when the owner opens it, but redirect any visitors from a different IP address, location, or device.

If you are at all concerned about whether a random folder on your website is caused by a gibberish hack, you can use a free scanning tool like Sucuri's SiteCheck to scan your site. Alternatively, you can search your domain in Google with the **site:** *yourwebsiteurl*. However, you will have to manually check for any suspicious URLs and content if Google hasn't flagged your website yet.

How to remove folders with random numbers and letters

To clean up a gibberish hack, you may think it's as simple as just deleting the random folder with numbers and letters and any HTML files created by the hackers. Unfortunately, it is likely the hackers left an option to reinfect your website with more spammy content. As a result, you will want to make sure your site is completely clean by following these steps.

Check Core File Integrity

The core files of your CMS are vital to making your website run, so they should never be modified or removed. But hackers can make changes to these files, so you'll need to make sure they haven't been tampered with. If you're using WordPress, the Sucuri plugin is the quickest way to check your core files integrity.

For users of other CMS platforms, you can use the **diff** command in the terminal. If using the command line makes you nervous, you can check directories for recently modified files in your FTP client. Just make sure to use FTPS, SFTP, or SSH and not unencrypted FTP to keep that communication channel with your website secure. If you identify any core files that have been compromised, replace them with a fresh copy or a clean backup.

Clean Hacked Files and Database Tables

If you have a recent backup that's not infected, you're in luck! You can just replace any hacked website files with fresh copies from the backup. If you do not have a backup, you'll need to manually edit malicious code from your website. It's important to make a backup of the site before doing this, as removing code can cause your website to stop functioning entirely. Make sure to test and verify the site is still operational after making any changes to code.

You will also need to clean your database tables. The functions are used by plugins and extensions for legitimate reasons, but hackers can also take advantage of them. To do this yourself, it will require some manual searching and removal of suspicious content in your website's database. Again, make sure to do your backups before attempting.

Deal with the aftermath

After your website has been scrubbed, you'll have to deal with the aftermath, including your site's standing on Google's search results page. All those gibberish pages are still in Google's index. When users click those links, they will hit a **"404 Not Found"** error page, which can damage SEO for the site. There are multiple solutions to resolving this problem including the URL removal tool in Google and editing the robots.txt file on your server.

If you're feeling worried about breaking your website while trying to clean a gibberish hack, you may want to seek assistance from a website security professional.

Protect your website from the gibberish hack

Once you've cleaned up a gibberish hack, the last thing you'll want to do is go through it all again. That's why it's a good idea to protect and secure your website to prevent hackers from gaining access. While it's impossible to guarantee hackers won't find a way in, these best practices will be helpful in keeping your site away from bad actors.

- **Update everything –** When website software is updated – whether it be for the CMS, plugins, or themes – developers also patch vital security issues. Without these patches, your website will be vulnerable to attacks. Because most attacks are automated by bots that scan for any opportunities to exploit website vulnerabilities, it is important to update your software as soon as possible. If you need to use outdated software on your website for any reason, consider using a firewall option that allows for virtual patching of outdated software to ensure that those vulnerabilities are covered even without you updating the software.
- **Use strong passwords –** Don't reuse passwords on multiple accounts and make sure they are long and unique. Avoid using any distinguishable words, too. A good rule of thumb is that if you can say your password out loud, it can likely be compromised by hackers. If you're not using a password manager, get one. These services will both generate strong passwords and keep track of them. Some popular choices include LastPass, KeePass, and 1Password.
- **One site per server or hosting account –** Hosting many websites on a single account with your hosting provider seems like a great idea from a financial standpoint, but it's terrible for website security. Hosting many sites in the same location creates a large attack surface that will allow for cross-site contamination.
- **Principle of Least Privilege –** Your website users may be targeted by an attacker. As a result, you'll want to make sure to limit any administrator access and practice the principle of least privilege. This means only giving users a minimal set of privileges in order to perform an action and only granting them for the time required to complete their job.
- **Make frequent backups –** Backups are crucial for recovering a website after it has been compromised. Make sure your backups are stored off site, as you do not want hackers to be able to access and modify them in the event of an attack. Also, make sure you can set up automatic backups and create multiple backups for redundancy.
- **Get a website firewall –** All of these steps are helpful, but a fully robust website security plan will include a web application firewall (WAF) to stop website hacks and attacks. The Sucuri cloud-based WAF can instantly block attacks, while also providing virtual patching, protection from zero-day exploits, and faster load times through our CDN.

Conclusion

Finding a random folder on your website full of gibberish links is a nuisance that no website owner wants to deal with. But you'll want to get a gibberish hack cleaned up as soon as possible.

Leaving a compromised website online for an extended period of time will lead to a loss of visitor trust and search engine blacklisting that can destroy your website's good standing. If you feel overwhelmed by the cleanup process, we have you covered. Our malware removal experts can get your website up and running again.