Heart Internet Presents

YOUR GUIDE TO WEBSITE SECURITY

Information on website security for small businesses

Heart Internet

Contents

Foreword

The web is not a safe place - there is a hacking attack every 39 seconds, and 65 per cent of these attacks are aimed at small and medium sized business, often because cybercriminals see them as soft targets.

And the threats that businesses face are ever changing - 230,000 new malware samples are produced every day **[1]**, while in 2017 the number of cryptojacking attacks increased by 8,500 per cent **[2]**.

Website security is one of the most important aspects of doing business online, but for many of your clients it's an issue they don't think about until something goes wrong.

And if things do go wrong for a client, they're likely to turn to you to help them out.

In this book, we'll explore ways you can help your clients keep their sites secure, and how you can fix things if they do become the victim of a cyberattack.

You'll also be able to use the tips and advice to better protect your own website against security threats.

1. https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/
2. https://www.symantec.com/security-center/threat-report

Top 10 Security Risks for Websites in 2019

Gil Press talked to a range of cybersecurity experts in his article "60 Cybersecurity Predictions for 2019" **[1].** Out of that, we pulled 10 that can definitely affect your website and your business.

1. Security starts at the developer

Don't tack your security fixes at the end of the project – include it every step of the way. More companies will keep in mind that the code, the design, and all the processes need to have security at heart.

2. Customers get more data savvy

As they become more aware about how much their data is worth, they will want you to take better care of it. GDPR didn't just stop in May 2018 – it's a continuous exercise.

3. Social engineering emails get smarter

As natural language and AI capabilities get easier and more powerful, phishing emails will get harder and harder to spot. Always check where an email has come from before entering in personal data.

4. Attacks move along supply chains

As larger businesses develop better security, attackers will discover they can still cause disruption by targeting the rest of the supply chain, especially small businesses without the resources for better security.

5. The Internet of Things becomes the Internet of Hacks

As more devices become "smart", there are more opportunities for hackers to get into your business. That Google Home Mini looks great in the office, but what is it listening to?

6. Exploits found in large data pools

The breaches won't be from super-elite hackers, but from gaps left by developers in large data pools. Be extra vigilant with who has access to your data, especially using APIs and web apps.

7. Smaller e-commerce sites get targeted

As brute force attacks get faster and easier to implement, smaller e-commerce sites will be targeted, especially those without proper protection. Make sure all your software is updated and secure.

8. Hijacked chatbots take over sites

Flaws on websites can allow hackers to install chatbots onto your site, getting customers to click links, download files, and share information – all looking like they're from your business.

9. Bigger and smarter attacks thanks to machine learning

Cybercriminals will be able to do more damage with even less, building complex and elusive adversaries through machine learning and AI. On the other hand, cybersecurity experts will be doing the same thing.

10. Spending 20% on security essentials will provide 80% of improvements

Make sure everything is up to date, and make sure everything is locked down. Spend a little time on the basics, and you've essentially solved the problem.

Resources:

[1] Gil Press, Forbes
60 Cybersecurity Predictions for 2019
https://www.forbes.com/sites/gilpress/2018/12/03/60-cybersecurity-predictions-for-2019/

7 Steps for Cleaning Your Hacked Site

Would it surprise you to know that the one of the main reasons websites get hacked is not to steal customer data?

Believe it or not, SEO spam is why hackers target vulnerable websites. By hijacking a vulnerable site, they can redirect your visitors to malicious sites, causing you to not just lose customers, but penalising you on search engines. Including showing "this site may be compromised" whenever someone tries to visit.

No matter how much hard work you put into optimising your site for users and search engines, no matter how perfect your copy is or your code, if security is not a priority, all that work will be for nothing the moment a hacker gets into your site.

What do I do if my site's been hacked?

If you act fast, you can save your site and save your search engine results.

Google has an in-depth guide on the steps you need to take **[1]**, but here's an overview:

Step 1: Verify that you own the site

The road to recovery starts with verifying ownership in the Search Console. Sign into the Search Console **[2]**, click "Add a Site", enter in your site's URL and then continue through the process.

Choose the verification process that works for you and continue through the process. As a verified website, you'll be notified of any security issues. Once you are verified, you can also go into your Search Console and manage users. Some hackers might try to claim ownership of your site, and if you see any users you're not aware of, delete them immediately.

Step 2: Inform your web host

Once you have verified your site with Google, you need to let your web host know that your site has been hacked. This allows them to take measures to protect their other customers, and they can also help you find out how your site was compromised and how to recover.

Step 3: Take your site offline

This prevents hackers from causing further damage and also prevents visitors from seeing a malware alert when they visit your site. If you have control over your webserver, stop it entirely. Or point your domain's DNS entries to an entirely different server, with a 503 HTTP response code, showing that your site is temporarily unavailable.

Step 4: Review and clean all accounts

Once your site is offline review user accounts, especially the newest ones. Anything that looks suspicious, delete. And change all the passwords for all site users, accounts, FTP, database access, system administrators, CMS, and anything else that requires a password.

Step 5: Determine how you were hacked

Check the messages in your Search Console to see if you received any information on what your site was used for. Was it serving spamming pages or links? Phishing? Distributing malware? You can also go to Security Issues to get more information.

Step 6: Clean everything up

Remove anything that was added by the hacker – content, links, images, users, whatever. Do a clean install of your software and program updates and eliminate the third-party widgets you rarely use. If you have access to the root of your server, do a clean installation from the ground up. And if you have any backups, make sure you only upload the files you know are clean.

Step 7: Ask Google to review your site

Have you verified your site's ownership? Is your site all cleaned up and back online?

Once you know you're ready, it's time for a Google review. This is important to have all the warnings removed from your site. Just follow Google's instructions **[3]** on requesting a review, making sure you show all the steps you've taken. Once Google determines your site is clean, they'll approve the review, remove the "this website is not safe" warning, and everything will be up and running again!

Resources:

[1] Google
Help, I think I've been hacked!
https://developers.google.com/web/fundamentals/security/hacked/

[2] Google Search Console
https://search.google.com/search-console

[3] Google
Request a review
https://developers.google.com/web/fundamentals/security/hacked/request_review

5 Easy WordPress Security Tips

As WordPress becomes more and more popular, it's a lot more likely that hackers will write scripts specifically to attack WordPress sites.

If you're worried about how secure your WordPress site is, don't worry – there are very simple things you can do that keeps your site protected.

1. Keep WordPress up to date

This is the most obvious one and yet everyone forgets to do it. If you don't have to check the site regularly, it can often get several versions behind. But this is your chance. Stop reading this, log into your WordPress site, and update your site.

Right now.
Update your plugins too.
That was easy, wasn't it?

2. Make sure your passwords are strong

This is another obvious one, but it's also the one people forget. And it's not just a matter of adding in as many special characters and numbers you can remember – it's about having unique passwords for each site. No longer having the same email address and password combination for Netflix/Steam/WordPress/Google/DropBox/whatever.

Check Have I Been Pwned [1] first. If you show up, change your passwords. Even if you don't show up, change your passwords anyway. Use KeePass [2] or another password management tool and keep that password secure as well.

Once you've sorted out your passwords, make logging into WordPress even more secure by adding two-factor authentication. MiniOrange's Google Authenticator [3] is a good one.

3. Clean up your users

Have people left your company? Did you hire guest authors? How many users do you have on your WordPress installation? And what are their permissions?

This might not seem like a big deal, but ICO fined Carphone Warehouse £400,000 for their data breach **[4]**, and that was the result of someone using a valid WordPress login on an outdated site.

So what do you do with these unwanted users? If they haven't posted anything, delete them. There's no reason to keep them around and they're just a risk.

If they have posted something, and you would like to keep them as an author, you can set their role to "No role for this installation". They can still log in, but once they have, they can't access the Admin screen or do anything else.

4. Get a good plugin

There are hundreds of security-related plugins **[5]** available, containing everything under the sun, from firewalls to brute force testers to two-factor authentication and anti-spam measures. Luckily, most of them are free or have trial versions, so you can test them and see which works best for you. Here are four that are generally considered to be good:

- Sucuri Security **[6]**
- Wordfence Security **[7]**
- All in One WP Security & Firewall **[8]**
- iThemes Security **[9]**

Don't forget that Jetpack **[10]** comes with a lot of security features, and it's automatically installed on your installation of WordPress.

You should also double-check all your existing plugins to make sure they're still regularly maintained and kept secure. Thousands of sites, including the NHS and ICO, were recently turned into cryptominers by one third-party script that had been hijacked **[11]**.

5. Back up regularly

Of course, no matter how much you lock things down, no matter how many plugins or security measures you take, your site can still get hacked.

This is where regular backups come in. Even if you do get hacked, you can just revert back to a previous version with a minimum of data loss.

You can manually back up your entire site on a regular basis, but you'll need to remember to take those backups as well as remembering to back up the database separately. Jetpack also has a backup feature, which you can set to do a daily backup.

Or you can get a separate plug-in, many of which will back up your site to another cloud service, such as AWS, DropBox, or Google Drive. Updraft Plus **[12]** is a popular one, as is BackWPup **[13]**.

So there you go – five easy steps to make your WordPress site even more secure!

Resources:

[1] Have I Been Pwned
https://haveibeenpwned.com/

[2] KeePass
https://keepass.info/

[3] miniOrange's Google Authenticator Plugin
https://wordpress.org/plugins/miniorange-2-factor-authentication/

[4] Alex Hern, The Guardian
Carphone Warehouse fined for "striking" number of failures that led to data breach
https://www.theguardian.com/technology/2018/jan/10/carphone-warehouse-fined-400000-pounds-security-failures-information-commissioners-office-hack-customers

[5] WordPress.org
Security Plugins
https://wordpress.org/plugins/search/security/

[6] Wordfence Security Plugin
https://wordpress.org/plugins/wordfence/

[7] Sucuri Security Plugin
https://wordpress.org/plugins/sucuri-scanner/

[8] All In One WP Security and Firewall Plugin
https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/

[9] iThemes Security Plugin
https://wordpress.org/plugins/better-wp-security/

[10] Jetpack Plugin
https://wordpress.org/plugins/jetpack/

[11] Chris Williams, The Register
UK ICO, USCourts.gov... Thousands of websites hijacked by hidden crypto-mining code after popular plugin owned
https://www.theregister.co.uk/2018/02/11/browsealoud_compromised_coinhive/

[12] UpdraftPlus WordPress Backup Plugin
https://wordpress.org/plugins/updraftplus/

[13] BackWPup WordPress Backup Plugin
https://wordpress.org/plugins/backwpup/

How To Prepare Your Business For Almost Anything

Are you prepared for disaster?

If you're running a small business, you probably don't want to think about what could go wrong. You could be too busy with the day-to-day aspects. You might be planning for the future, but focusing on the positive aspects, like expanding or raising revenue. Or you might be thinking about disasters, but focusing on giant disasters, staying up late at night thinking about supervolcanoes and asteroids.

When we're talking about disaster recovery and business continuity, we don't mean cinematic epics. We're talking about the small disasters that can change your business permanently. A single hard drive failing. The power going out. Even a new employee rewriting over a file. Without a business continuity plan, these tiny problems can spiral out into giant disasters – maybe not worldwide, but definitely for your business.

Your business continuity plan gives your company the information it needs when something goes wrong. With contact information, lists of suppliers, backup plans, and detailed instructions, a good business continuity plan provides the structure people need right when they're about to start panicking.

What can a business continuity plan include?

It might seem impossible creating business continuity plans. You think you have everything you need, then you start thinking about new possible problems, all the ways things could go wrong, and the next thing you know, you're writing about what to do in case of alien attack.

You don't need to provide detailed plans for all possibilities – a basic guide can give you the strong framework you need to apply to any problem. The same guide that tells you what to do in case of a hard drive failing can work just as well for when the entire computer is stolen or when a targeted electromagnetic pulse has wiped out all the electronics across your city.

We're going to focus on the technical side of your business continuity planning, but if you want to make sure you're prepared for all types of disasters, look at the British Red Cross's guides on preparing for emergencies **[1]**.

What should an IT plan include?

The first version of your IT plan should include:

- The list of people in the company to contact in case of a problem, in order of importance
- The location of utilities in the building (gas, electric, water, etc.) and how to turn them off

- The list of vendors that can replace your technology quickly
- The location of important documents, serial numbers, and other important details
- Where your backups are located and how to retrieve them
- How to make sure all staff are aware of this plan and what to do in case of a problem

TechTarget, as part of their Essential Guide to Business Continuity and Disaster Recovery Plans **[2]**, have produced a free IT Disaster Recovery Plan **[3]** you can download and adapt to your own business. Including everything from contact trees to external communications, this plan can be the detailed template you need to make your own planning easy. Everyday Tech has also produced a collection of templates **[4]** to aid with your plans, including logging all your IP addresses, mapping out server dependencies, and scheduling backups.

What about backups?

You should have a backup plan for every single piece of technology you have on hand – from your company mobile to your web server to that ancient fax machine you only use once a year. Whether backing up your individual computer, running a file server, or keeping your website running, a good backup can make recovering from any disaster a million times easier.

And with the advent of cloud hosting, it's even more convenient to keep your backups safe and separate from your files. No more worrying about tape drives, stacking up CDs, or keeping everything on a very easy to lose USB stick.

Many people use VPS or Dedicated Servers as web hosting platforms, but they also make excellent file hosting platforms, giving you a secure and easy way to store your important files in a location separate from your office.

Purchasing a VPS or a Dedicated Server from a hosting company also gives you extra peace of mind, as that company should already have business continuity plans in place, with redundancy measures for power, data, connection, and more.

A Good Plan Makes A Good Business

So take a few minutes out of your day to build a business continuity plan. It might seem like a waste of time now, but it definitely won't when the robot uprising happens.

Resources:

[1] British Red Cross
Prepare for emergencies
https://www.redcross.org.uk/get-help/prepare-for-emergencies

[2] TechTarget
Essential guide to business continuity and disaster recovery plans
https://searchdisasterrecovery.techtarget.com/essentialguide/Essential-guide-to-business-continuity-and-disaster-recovery-plans

[3] TechTarget
IT disaster recovery (DR) plan template
https://searchdisasterrecovery.techtarget.com/feature/IT-disaster-recovery-DR-plan-template-A-free-download-and-guide

[4] Everday Tech
Disaster Recovery Plan Templates & Sample Documents
https://everyday-tech.com/disaster-recovery-plan-templates-and-sample-documents/

WEBSITE SECURITY

Malware can strike at any time. Secure your website today.

Never worry about the safety of your site again

With Website Security, you'll never be compromised

Action

Remove malware from your website as soon as it appears.

Alert

Get immediate updates about issues on your site.

Prevent

Stop future hacks with our Web Application Firewall.

Improve

Make your site even faster with our built-in CDN.

See more at www.heartinternet.uk/website-security

Heart Internet