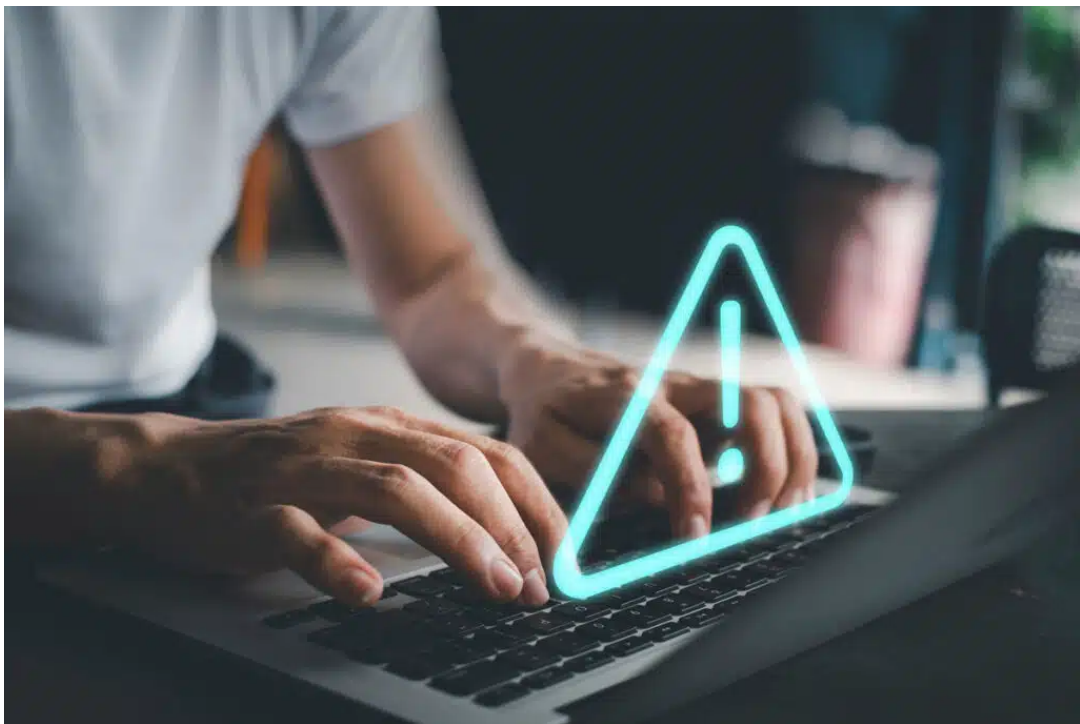




(<https://ttoydigital.agency>)



Common Security Issues with WordPress & How to Mitigate Them



i security (<https://ttoydigital.agency/tag/security/>),
WordPress (<https://ttoydigital.agency/tag/wordpress/>)

From our website, you can probably see that we use WordPress as our content management system of choice to build all of our websites.



Need Help? **Chat with us**

The reason we use WordPress is that it's one of the most popular website platforms in the world, but its widespread popularity can also leave websites vulnerable to malicious attacks.

What is a malicious attack?

A malicious attack is where somebody tries to take control of a WordPress site to commit acts that may put your, business or customers at risk, it might be your website is redirected to another site or customer data is stolen for example.

Fortunately, there are steps you can take to ensure your website remains safe and secure. This article will explain some of the most common security issues associated with WordPress and how you can mitigate them.



Brute Force Attacks

A brute force attack is a type of attack where an attacker tries to access a website by repeatedly trying different usernames and passwords until they find the correct combination.

To prevent these types of attacks, make sure you use strong passwords that contain a combination of letters, numbers and symbols – not only for the admin user but also for any other WordPress users on your site.

Additionally, it's worth considering installing two-factor authentication on your site as this will require an additional layer of security when logging in. Two-factor authentication is where you receive an email, use an authentication app or are sent a code via text message to input on the website before you're allowed into the WordPress dashboard and limit login attempts.

Need Help? [Chat with us](#)

Malware & Viruses

Malware and viruses are malicious code designed to infect the computer (server) your website lives and steal information. To reduce the risk, always keep your plugins, themes and WordPress core up-to-date – as many vulnerabilities arise from outdated software. We wrote an easy to follow guide in this **article** (<https://ttoydigital.agency/demystifying-malware-a-simple-guide-for-small-business-owners/>).

It's also important to be aware of suspicious links or emails in case they are infected with malicious code – if in doubt always check with someone else before clicking on anything.

Need Help? **Chat with us**

Phishing Scams

Phishing scams occur when hackers send emails imitating legitimate companies to collect user data such as usernames/passwords or payment details. We've had these targeting us in the past.

To protect yourself against this type of attack, always look for grammatical errors, and the 'from' address and think whether you were expecting the email. Additionally, never click on questionable links or respond to requests for personal information via email – if there's ever any doubt about the legitimacy of an email then contact the company directly using their official website/address instead.

Phishing attacks don't just come through from email either they're also prevalent on social media, I'm sure you've seen posts on Facebook that say something like comment on your first pet's name or something similar. These types of posts can be dangerous if you comment as if you are a business owner, you most likely going to have where you work on your Facebook page. It's then not a massive step to find out if you are a website owner too, and attempt to break into your website.

Unfortunately, most people don't use strong passwords and use the same one across all everything they need to log into which means if someone's got a password they've got access to everything.

You should always use a strong passwords, if you struggle to remember them try using a phrase and you can use a password manager to create them and remember them for you.

Need Help? [Chat with us](#)

Backups

It's always worthwhile having regular backups in place just in case something does go wrong (such as malware infection) so you can be up and running again in no time. There are many options available such as taking manual backups (via File Transfer Protocol) or you can set up automated backups through plugins such as UpdraftPlus or your hosting provider may take backups for you, for instance, we keep 60 days' worth of backups of your site automatically. You can learn more about backups in our **backup article**.

(<https://ttoydigital.agency/website-backups-why-theyre-important-and-how-to-create-them/>)

Backups should always be kept safe somewhere separate from your main site.

Need Help? **Chat with us**

WordPress Core, plugins and themes

There are three main components to a WordPress site. The WordPress core is the actual WordPress installation, WordPress themes are what are used to design your website for visitors and WordPress plugins help change or add functionality to a WordPress website.

Ensuring that your WordPress core plugins and themes are up-to-date is essential for the security of your website. Outdated software can leave your website vulnerable to malicious attacks and expose it to potential risks. You can learn more about WordPress in this **article** (<https://ttoydigital.agency/wordpress-what-is-it/>)

WordPress Core

Your WordPress installation is where your website databases and the code for running your website is stored. WordPress is open source so many WordPress developers support the content management system and are dedicated to keeping WordPress secure, but it is a constant battle as with any software. WordPress generally release two to three updates a year but will release security patches more frequently if security issues are found.

Need Help? **Chat with us**

WordPress Themes

Themes allow you to style your website there are lots of free and paid themes available from different companies. Before installing a new theme make sure it's from a reputable source and that is being kept up to date regularly by the developers. You can then update your theme when new updates are released.

WordPress Plugins

Plugins allow you to change or add functionality to WordPress, like themes they can be free or purchased from plugin developers the same advice above stands to help mitigate security threats.

You can find further detailed information on what WordPress is in this **article**. (<https://ttoydigital.agency/wordpress-what-is-it/>)

It's always best practice to keep all of your WordPress components (plugins, themes and core) up-to-date so that you have the latest security patches installed. This also ensures that you have access to the newest features and bug fixes.

Need Help? **Chat with us**

Updating plugins, themes and WordPress can be done easily from within the WordPress dashboard. When accessing the **dashboard** (<https://ttoydigital.agency/what-is-the-wordpress-admin-dashboard/>), you will see an orange alert icon in the top right-hand corner if there is anything available to update – simply click this and then follow the prompts to ensure everything is up-to-date. It's important to note that manual updates should only be done if you know what you're doing as they can potentially cause conflicts with other components on your site and break it. If in doubt, seek professional help and always take a backup of your WordPress website and test any updates on a staging site.

Website Contact Forms

Whilst not limited to contact forms, I wanted to mention a couple of other types of attacks that are used on WordPress websites that if you're attacked you'll need to know what they mean.

The first one is SQL injections and this can be used on any field that accepts input such as the login page or form fields. SQL stands for structured query language. It's essentially a way of extracting data from a database. What people do is write a piece of code that attempts to retrieve some information that's held within your WordPress website. This could be customer data or login information for example.

They copy and paste this code into a form field or login box in an attempt to retrieve information which is why it's known as an SQL injection attack.

The other common attack on WordPress websites is cross-site scripting or XSS attacks are where an attacker injects code into a website itself that's then executed in a user's browser.

Both attacks could be a serious security breach for your business.

Need Help? [Chat with us](#)

WordPress Security Plugin

You could also use WordPress security plugins like WordFence that are specifically designed to work on WordPress Websites. These plugins help combat common WordPress security issues like brute force attacks, SQL injection attacks and cross site scripting attacks.

These security plugins usually have an inbuilt web application firewall that blocks malicious IP addresses so they can't connect to your site helping to reduce security threats.

Secure WordPress Hosting

Ultimately there will be some actions that can only be done at the server level to help keep your WordPress website secure. Some of these are quite technical so we'll not go over these but web host might provide their security features like backup solutions and deploy their web application firewall to help keep WordPress users secure and try to mitigate security risks.

When setting up a new site or considering moving hosts you'll need to do your research to find out which secure WordPress hosting packages are best for you. you can find our rang of hosting packages by visiting our **hosting page** (<https://myaccount.ttoydigital.agency>).

Need Help? **Chat with us**

More Articles

I have an SSL Certificate, does that mean I'm protected?

No. An SSL Certificate protects connections from your website to a user's device so people can't see what's happening. However, attacks are usually against a WordPress site itself so an SSL certificate would do nothing.

Are WordPress Websites secure?
<https://ttoydigital.agency/web-design-packages-vs-just-paying-for-a-website-design/>

WordPress is a powerful platform that provides users with plenty of options

Web Design Packages Vs Just paying for a Website Design
[\(https://ttoydigital.agency/web-design-packages-vs-just-paying-for-a-website-design/\)](https://ttoydigital.agency/web-design-packages-vs-just-paying-for-a-website-design/)

On the internet, your website is your storefront. It's a way to showcase your products and services. It's usually the first impression potential customers have of your business. However, it's not immune to security issues such as brute force attacks, malware, viruses and phishing scams as no website whether its built on WordPress or another content management system is 100% secure.

Read More » [\(https://ttoydigital.agency/web-design-packages-vs-just-paying-for-a-website-design/\)](https://ttoydigital.agency/web-design-packages-vs-just-paying-for-a-website-design/)

As site owners, you have the responsibility to maintain a WordPress site so that you can reduce security risks. As we've discussed there are several things you can do to help secure WordPress sites:-

- Limit login attempts
- Update Plugins and Themes
- Remove outdated software
- Research security features that are deployed by your web host
- Enforce two factor Authentication
- Install security plugins to help prevent SQL injection, brute force attack or XSS attacks
- Ensure your WordPress installation is up to date
- Ensure users create secure passwords.

Need Help? [Chat with us](#)

[\(https://ttoydigital.agency/what-does-image-optimization-for-websites-mean/\)](https://ttoydigital.agency/what-does-image-optimization-for-websites-mean/)
 like anything you have to take precautions to make sure your site remains
What does Image Optimization for Websites mean? (https://ttoydigital.agency/what-
 secure drive a car without insurance would you?
does-image-optimization-for-websites-mean/)

There is no doubt that images are an essential part of any website. They can enhance the user experience, create a more compelling design and

Read More » (https://ttoydigital.agency/what-does-image-optimization-for-websites-mean/)

[\(https://ttoydigital.agency/common-security-issues-with-wordpress-how-to-mitigate-them/\)](https://ttoydigital.agency/common-security-issues-with-wordpress-how-to-mitigate-them/)

Common Security Issues with WordPress & How to Mitigate Them
[\(https://ttoydigital.agency/common-security-issues-with-wordpress-how-to-mitigate-them/\)](https://ttoydigital.agency/common-security-issues-with-wordpress-how-to-mitigate-them/)

From our website, you can probably see that we use WordPress as our content management system of choice to build all of our websites. The

Read More » (https://ttoydigital.agency/common-security-issues-with-wordpress-how-to-mitigate-them/)

« Previous Next » [\(https://ttoydigital.agency/common-security-issues-with-wordpress-how-to-mitigate-them/2/\)](https://ttoydigital.agency/common-security-issues-with-wordpress-how-to-mitigate-them/2/)


Need Help? **Chat with us**

Follow Us

(<https://ttoydigital.agency>)

 <https://www.facebook.com/ttoydigital>

 hello@ttoydigital.agency (mailto:hello@ttoydigital.agency?subject=Hello)

 <https://twitter.com/TtoyDigital>

 <https://www.linkedin.com/company/ttoydigital/>

 [WhatsApp](https://api.whatsapp.com/send?phone=+441773418300) (https://api.whatsapp.com/send?phone=+441773418300)

Services

Home

Web Design

SEO Service

Hosting

Domains

Review Management

Marketing360

Knowledge Centre

News

About Us

Legal

Privacy Policy

Need Help? [Chat with us](#)

Acceptable Use Policy

Cookie Policy



Our website is listed in [webdesignlistings.org](https://www.webdesignlistings.org)
(<https://www.webdesignlistings.org/Bespoke-Websites/C3-1-0.htm>)

©2023 TTOY Digital Ltd

TTOY Digital Ltd is a registered company in England and Wales. Registration number:
13324664

Need Help? [Chat with us](#)