WordPromise
Expert Website Maintenance & Support™

# Why Hackers are real threat to My Website?

Email us at info@wordpromise.com

# Good Cyber security is not only about technology, but much more than that.

To safeguard a website, we need to understand the enemies first. By understanding the psychological phenomena of Hackers, we can truly keep our website and its data safe from those who wish to harm it intentionally for their evil deeds.

Let’s explore more in detail about Hacker’s activity and their motivation…

# Who is Hacker?

Hacker is a person who breaks into the system without any permission and change or steel website information to commit crime. Similarly, Hacking is the activity of identifying weaknesses in a website or a network associated with Website to exploit the security to gain access to private data or confidential business data.

An example of Website hacking can be using a password cracking algorithm to gain access into the system.

Unfortunately, there are people & systems actively working to hack websites. There are many types of hacking from low to high end but they're unlikely to target your personal WordPress website directly.

They may be tempted to personify attacks, but the reality is, a "**hacker**" is more like a mindless robot. By robots, we mean "bots," or automated code that has a connection to the internet. Just like a robotic arm at a manufacturing plant is programmed to do specific tasks, these bots work every second of every day to perform their programmed tasks as often as they can, on as many sites as they can.

The goal of attacks is often to make the attacked site into yet another bot that can be given tasks. The tasks can range from attacking other sites to sending spam or phishing emails. In other words, these bots don't know what your site is about, nor do they care. To the creator of the bot, each compromised site gives them access to more resources to create a revenue stream in one way or another.

# Hacker’s Motivation

Hackers are augmenting their skills day by day. They’re constantly finding new ways to trick system's vulnerabilities and peep into our networks. So, what is it that motivates the hackers to hack a website?

It has nothing to do with a specific website, what business it offers, what type of user it covers etc. In fact, hackers target the software upon which your website is built & hosted. They look for minute mismatch or weakness in the software which they can tweak and use it for their unauthorized entry into the system. By gaining the access, they can change the website data or even steal it for their benefit.

**Hackers generally exploit common vulnerabilities in the software and execute hacks on a broader scale hoping it succeeds on as many websites as possible.** In fact, 44 percent of all cyberattacks are aimed at small businesses. What makes it worse is that only 14 percent are prepared for an attack, which explains why they're targeted.

**WordPress, being the leading content management system for the Websites; makes it a popular target for attackers.** It is important to mention that the threat is not with WordPress itself, but the wide range of third-party plugins that are being used by WordPress users. While WordPress is constantly updating its core framework, improved security does not extend to its plugins which are built by third-party developers. If a popular WordPress plugin has a serious vulnerability, then there are all chances of getting it exploited by the hacker.

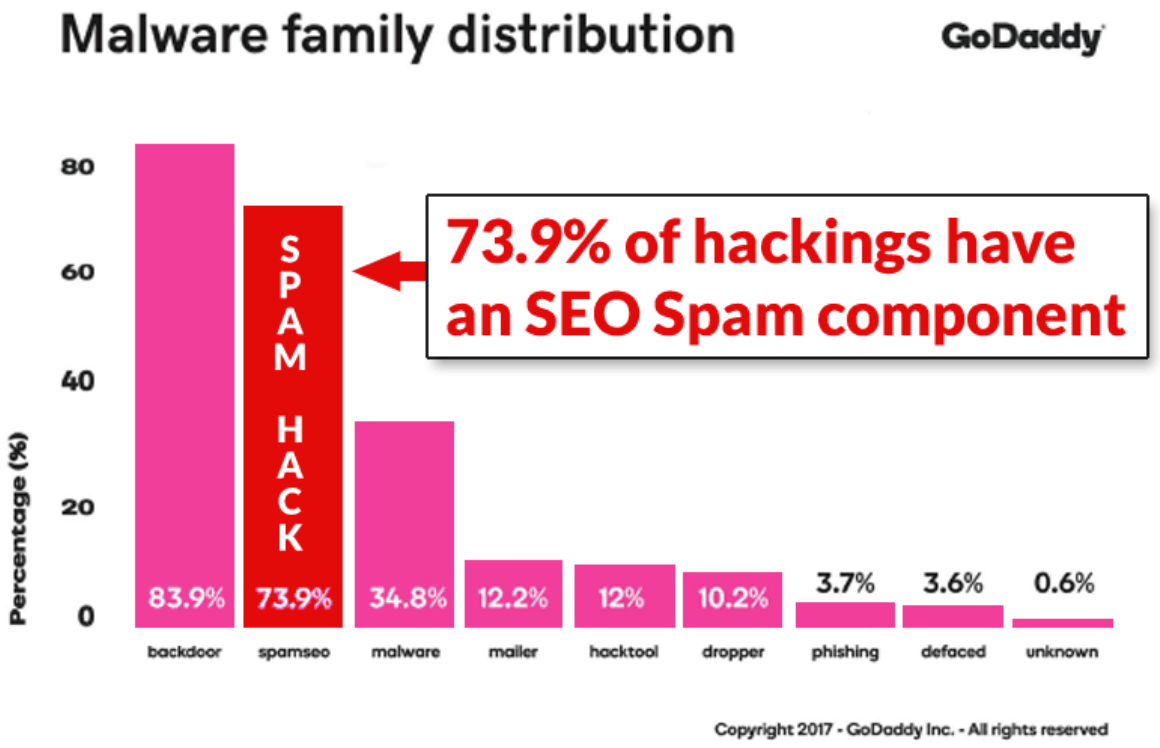
Fortunately, most plugin vulnerabilities are quickly patched by their developers

The obvious motive is financial gain. If you do have sensitive information, like payment details, then security should be a top priority.

# Have you heard of SEO Spam?

SEO spamming or also known as spamdexing is the intentional attempt to manipulate the search engine indexes without the knowledge or permission of the website owner. There are many methods such as link building and repeating unrelated keywords, to manipulate the relevance of content indexed, in a manner you would not do generally.

According to a study by GoDaddy, 73.9% of hacked sites are hacked for SEO purposes. Hackers add links to a website, add new web pages and can even start showing a different site altogether just to Google.




This means SEO is a major reason to compromise a website's security.

Hackers know all these technical details about SEO, and they use it in their favour. When your website has been compromised, hackers do install a malware into your website that allows them to control your content and keywords remotely. More dangerously, they can redirect traffic from your website, funnelling it straight to theirs, passing over yours completely.

You might think SEO spam would be easy to spot, but that isn’t so easy. Hackers do everything to hide their work, and often the malware is coded in a way that the spam is only shown to search engine crawlers. Normal users — including the website owners — only see the surface content.

Of course, if your site has been compromised with SEO spam, you want to know about it as soon as possible.

WordPress security plugin with malware scanning can only help in such scenario. **Sucuri** and **WordFence** are good plugin to address the same.

# Malware Injections

Malware Injections or malware attack is a common cyber security threat where malware (normally a piece of software commands compiled together in a script to) executes unauthorized actions on the targeted software platform or websites.

**Malware Injections** at specific levels includes many specific types of attacks such as SQL injections, cross site scripting (XSS), spyware, command, and control, and more.

Hacker's point of view, once the injection is completed, the malicious scripted file is executed as a legitimate file on the hosting server. Hackers can then manipulate or steal the data as per their benefit and they can keep a direct link to the data at their system. Whenever any new data gets generated, hackers do have access to it, if they have compromised the system.

It is important to note that amongst all of the malware injection attacks, it is the Structured Query Language (SQL) injection attack and the cross-site scripting attack which are the two most common forms that can be launched against a cloud computing infrastructure.

# Spyware

Spyware also belong to the family of Malware; a type of malicious software that is installed on target system without any authorization or permission. If successful, It invades the hardware & software firewall, access or steals information, and transmit it to Hacker.

Spyware also belong to the family of Malware; a type of malicious software that is installed on target system without any authorization or permission.

If successful, it invades the hardware & software firewall, access or steals information, and transmit it to Hacker.

Any piece of code can be classified as spyware if it is downloaded without the user's authorization. Spyware is a kind of malware that secretly gathers information about a person or organization and relays this data to other parties.

Spyware can be difficult to detect; often, Signs of a spyware infection can include unwanted behaviours of your webpages along with slow system performances. Substantial or very heavy consumption of hosting server or your local computer system.

Some prominent issues such as websites freezing, failure to load, difficulty connecting to the internet and web pages crashes are also common.

# Website Defacement

Website defacement as its name suggest is to change the look and feel of the website pages.

**Website defacement** as its name suggest is to change the look and feel of the website pages. In short, hacker finds a way to modify the content of webpages without your permission. Usually, they do change the contents of your website as per their state of mind and to embarrass you. Sometimes, hackers deface websites of companies or organizations with whom they have some disagreement on any sort of issues whether personal, political, business related.

Eventually, Website defacement attacks differ from other malware attacks because the hacker rarely stands to gain from the action.

Sometimes, they simply do the acts to false satisfaction of their false identity. They are different from other sort of hackers, in a way they want the websites of companies or organizations, to notice their mischievous deeds. Most malicious hackers try to hide their activities, but not those who choose defacement as a weapon. They're doing it to show off.

Your website is the virtual face of your business, and website defacement attacks can easily ruin your business. It will also bring financial dent to your business as obviously the clients would not want to be the part of all this.

The cost of re-fixing your website from defacement is also another burden you have to face, in case of any occurrence of website defacement. This is why website defacement prevention strategies are also important for your business.

# Quick Tips to Protect and Secure Your Website

**Keep all software & plugin versions up to date:**

It may seem obvious, but ensuring you keep **all software up to date is vital** in keeping your site secure. Running outdated software is the number one reason a WordPress website or blog gets hacked. Keeping your WordPress website up to date should be at the top of your list of security checklist.

WordPress core and any theme or plugin you have installed on your website should always be running the latest version. Version updates are not just for new features or bug fixes; they can also include security patches for known exploits. Bots will scour the internet looking for WordPress sites running outdated software with known WordPress vulnerabilities. When you leave software out of date, you are giving a would-be hacker the blueprint to bypass all other security measures you have added to the site.

**Use HTTPS**:

We've all seen the green padlock in our browser next to the URL we are accessing, but why is it so important? SSL stands for Secure Sockets Layer and creates an encrypted connection between your web server and your visitors' web browser. HTTPS stands for Hyper Text Protocol Secure. When using.

HTTPS if anyone is able to intercept it, they still won't be able to decipher it because it's encrypted. SSL certificates range in price but are absolutely necessary to keep information on your website secure. There are also several places to buy SSL

certificates, but the easiest route is to buy it from your host and let them install it.

**Strong Password always helps**:

You should always use a strong password for your WordPress admin password. A strong password is a minimum of 12 characters, using a combination of alphanumeric and ASCII characters. Using only lower-case letters limits the pool of possible characters to 26, so it is vital to include alphanumeric, upper-case letters and common ASCII special characters to increase the pool of characters needed to crack the password to 92.

To make a password truly secure, even more characters or more than one uppercase letter, number or symbol can be added. A twelve-character password with one uppercase letter, one number and one symbol is almost unbreakable, taking a computer 34,000 years to crack.

**Avoid File Uploads**:

File uploads are essential for any business services and applications. It is important to note that file uploads are an important function for content management systems, IT portals, General sites, and messaging applications. As technology advanced, it becomes increasingly critical to implement measures to ensure the security of file uploads, since leaving file uploads unrestricted can create a major risk to the business. Through unrestricted file upload, hackers can target your IT infrastructure by overwriting an existing file or simply by putting malicious content. To avoid these types of

attacks, always ensure to allow specific file types only with the specified minimum and maximum allowed file size.

**Website Security Plugins**:

Security vulnerability can affect the health index of your website in the eyes of Google as well as your readers. A good plugin will help protect your WordPress website from brute force attacks, malware, and spammers. While the WordPress core software is very secure, the plugins and themes you install can leave your website open to vulnerabilities.

A security plugin is highly recommended to protect your website against brute force attacks. Security plugins keep confidential website files secure and it block spam from contact form plugins. Security plugins do notify you when a security threat is detected.

**Backup Your Website**:

When it comes to security, we should be prepared for the worst. In worst scenario, your site can be hacked even if you follow the WordPress security best practices. If an attacker successfully compromises your site, having a backup will allow you to restore your site to a clean state. Since WordPress doesn't have a built-in backup tool, having a solid backup strategy is your disaster insurance.

# Wrapping Up

At **WordPromise**, we provide WordPress Auditing Services that include WordPress Security, Speed, Support and Maintenance Plan for Website Owners and agencies. We offer the most comprehensive Audit information based on 90-point inspection checklist that covers security, speed performance, and analytics on the Websites of our clients.

At WordPromise, we are a team of contributors from a variety of backgrounds within the WordPress community that offers a standard subscription plan that includes all technical elements related to Firewall, Malware scanner and remedial actions, IP/Country blockers, GDPR etc. With WordPromise, you can protect your website from various type of malware infiltration into your website.

With so many threats to your website, it's important to make your WordPress site as secure as possible. Running a WordPress security audit of your website helps you prepare for and prevent successful attacks on your site.

You can't protect your site from every possible issue, but you can make sure you're prepared for the most common threats by running a WordPress security audit.

***Don't believe, try us!***