eCommerce Security
Questionnaire

By Shawna Leigh Designs
www.shawnaleighdesigns.com

WRITTEN SPECIFICALLY FOR:
Owners of eCommerce Websites Built on WordPress

SHAWNALEIGH DESIGNS™

DISCLAIMER: The information provided within this document is for informational purposes only. The purpose of this document is to inform you about some of the basic responsibilities required for running a safe and secure eCommerce website. This is not necessarily a complete list of responsibilities and your specific situation may be different. This document is meant to be used as a guide and should not be solely relied on to make important business decisions without your full and educated understanding of the topic. Shawna Leigh Designs shall not be held responsible for your use of, or inability to use the information contained within this document.

OVERVIEW

When you run any kind of website, the security of your visitors is paramount. This is especially true with eCommerce websites since you're collecting and processing sensitive customer data. With ever increasing security concerns, it's absolutely necessary to be pro-active with your website's security.

Within this eCommerce Security Questionnaire, you'll find several questions that cover basic, yet important tasks associated with keeping your website secure and your customer's data safe.

If you're unable to answer any of these questions on your own, on a continual basis, you'll need the support of an eCommerce website expert to help you.

Remember, no one can prevent ALL cyber crimes.

Let's begin.

1. Is WordPress, your theme and all of your plugins up to date?

Out-dated versions of WordPress, themes and plugins is the #1 reason WordPress websites get hacked. Many updates include important security vulnerability patches, so failure to perform updates makes your website more vulnerable.

WHAT YOU SHOULD DO: Ensuring that WordPress, your Theme and all of your Plugins are up to date is essential. You should aim to perform all updates within a week of their release, or sooner if there's a known vulnerability.

IMPORTANT: Before making any updates, you should always create a full backup of your website and database. In fact, regular backups should be apart of your security and remediation plan. More on this later.

2. Are you using safe themes and plugins that were acquired through trustworthy sources?

You should always be cautious when adding new themes or plugins to your eCommerce WordPress website. If you acquire themes or plugins from unreputable sources, they may hide harmful malware and viruses that give hackers an open back door to your website.

WHAT YOU SHOULD DO: Only use themes and plugins from reputable marketplaces or developers. If you're unsure about a plugin, you should consult with an expert for advice.

3. Are you using complex and unique passwords and limiting access to your website?

Passwords need to be complex. Automated bots (and people) will try to hack into your website by trying different password combinations until they're in. This is what's known as a brute-force attack. If your passwords are weak, it's only a matter of time before they are compromised.

Here's just an example of what your password length and complexity should look like:
N*aYC&afj78GCC4wtQ *(do not use this sequence as a password)*

Additionally, sharing the same password across multiple accounts is a bad idea. Even the largest, most popular websites and apps aren't immune to hackers. So, if you're using the same password for another account and that password is leaked through a data breach, hackers will have access to all accounts using the same password.

Furthermore, sharing access to your website should be limited only to trusted individuals that need it. If you must share your own account password with someone, make sure it's 100% unique and change it as soon as their access is no longer required.

WHAT YOU SHOULD DO: Use complex and unique passwords for ALL of your online accounts, including your website. Never share your own password or access to your website unless it's absolutely necessary and change your password frequently or when you believe it's at risk.

You can use a service like LastPass to help you create and remember unique and complex passwords for all of your online accounts.

Click Here To Learn More About LastPass
Notice: This is an affiliate link and Shawna Leigh Designs may earn a commission if you make a purchase using this link.

4. Is your website protected with SSL from a reputable certificate authority?

SSL certificates encrypt data between your website visitor's web browser and the server your website is hosted on for a secure connection. Without an SSL certificate, it's possible for a hacker to intercept plain-text data, such as credit card numbers and passwords.

SSL Certificates are an absolute MUST for eCommerce websites. SSLs are most commonly offered as an add-on to your website hosting account. Therefore, your website hosting provider should be able to help you with most SSL related questions, setup and/or issues. If you're hosting with Shawna Leigh Designs, I'll handle all SSL tasks for you!

WHAT YOU SHOULD DO: Ensure that you have a valid SSL certificate from a reputable certificate authority at all times. Take immediate action to resolve any issues if or when the SSL certificate is not working correctly. Premium SSL certificates are usually renewed each year, so don't forget to renew when the time comes.

---

5. Are you familiar with PCI-DSS Compliance?

Through a collaboration of the large credit card brands like Visa, Mastercard, Discover, and American Express, the PCI Security Standards Council was born. The purpose of the council is to introduce industry standards for safely accepting, transmitting, and storing credit card and cardholder data. These standards are what's known as PCI-DSS Compliance.

PCI-DSS Compliance applies to anyone that accepts, transmits, and/or stores credit card data. The higher your credit card processing volume, the more steps you need to take to ensure that you are in compliance.

Businesses that process less than 20,000 credit card transactions annually can simplify their requirements by selecting a payment gateway that handles compliance technicalities for them and then completing a Self-Assessment Questionnaire.

For helpful information on PCI-DSS Compliance, please visit:
https://www.pcicomplianceguide.org/faq/ AND https://www.pcisecuritystandards.org/

WHAT YOU SHOULD DO: Visit the links above to learn more about PCI-DSS Compliance. Although it may seem confusing at first, the most important thing to remember is never activate a credit card payment gateway on your website without first understanding how it will affect your compliance level. For this, you should seek the advice from an eCommerce website expert.

6. Are you hosting your website on a shared server, or a VPS/dedicated server?

Understanding your hosting environment will help you determine which ways you can safely accept credit cards. This digs a little deeper into the PCI-DSS Compliance described in question 5.

Shared Hosting is the simplest and cheapest form of website hosting, therefore it's the most popular for smaller businesses. Unfortunately, Shared hosting is also the least secure. Because of this, you'll need to choose a payment gateway that does not store or transmit credit card data via the hosting server. This will also simplify PCI-DSS Compliance.

VPS/Dedicated Hosting is typically more suitable for larger-scale businesses. VPS and Dedicated hosting offers much more power, flexibility, and control when it comes to all areas of your website.However, they're also very expensive and require a tremendous amount of skill to run and maintain.When configured correctly, VPS and Dedicated hosting is more secure than Shared hosting. Therefore, you have the ability to use payment gateways that store and/or transmit credit card data via the hosting server. However, storing and/or transmitting credit card data this way will also increase your PCI-DSS Compliance requirements, something you should try to avoid, especially if you're a smaller business.

So, as you can see, determining what type of website hosting you have plays a big role in how you'll be able to safely accept credit cards AND vice-versa.

We always have clients asking how they can accept credit cards directly through their own bank account, a custom gateway, or through their own payment card terminal. In the end, it's much better (and easier) for small businesses to stick with simpler solutions like PayPal Standard and/or Stripe - all of which you can connect directly to your bank account anyway.

WHAT YOU SHOULD DO: Be realistic with your options in relation to your budget and resources available to you right now. Unless you're a large business with the budget and resources necessary to manage more complex hosting solutions and payment gateways, you should stick to simpler solutions.

It's also important to note that smaller businesses commonly migrate back and forth between hosting solutions at different providers. Make sure that IF you do change hosting plans or providers, that it does not affect your ability to safely accept credit cards.

7. Is your website protected with a firewall, preventing common security vulnerabilities?

To further protect your website, you should perform certain tasks to help protect against common vulnerabilities. Although most security protection begins at the server level, there are several things that you should (and need) to do to harden your WordPress website's security. In addition to using secure passwords and limiting access to your website, you should:

a. Protect the WordPress admin area with lockout protection that can automatically block malicious bots and users trying to break into your website with multiple failed login attempts.

b. Protect your WordPress admin area by masking the default admin area URL where yourdomain.com/wp-admin is changed to yourdomain.com/something-random

c. Enable 2-Factor Authentication that requires admin users to retrieve a code before logging into the WordPress admin area.

d. Enable 404 Lockout Detection which will help block malicious bots and users snooping for vulnerable files in order to compromise your website.

e. Ban the use of common usernames like admin, administrator, and your host name, so that anyone attempting to login to your website with these usernames are immediately blocked.

f. Enable Audit Logging if you have employees or other users that will be accessing your website, so that you can monitor their activities within it.

WHAT YOU DO SHOULD DO: Implement as many security features that you reasonably can, from the list above and beyond. To handle a majority of these tasks, Shawna Leigh Designs highly recommends installing and properly configuring Defender. Defender is a free (and upgradeable) security plugin that will help you harden your WordPress website.

Click Here To Learn More About Defender By WPMU DEV (click the link, then click on Plugins > Defender)
TIP: WPMU DEV (the creator of Defender) also has a few other useful plugins I recommend checking out. For A FREE 7-Day Trial, Click Here.

8. Do you have a backup and remediation plan in case something goes wrong?

It's important to have a plan of action IF something does go wrong. You can make a stressful situation a lot easier with some basic preparations. The most important piece to any remediation puzzle is regular website backups. Regular backups are a must! Not only can they save you from hackers, they can save you from your own catastrophic mistakes.

Backup Frequency: Daily backups are ideal, but even weekly backups are okay in some situations, especially for low traffic websites that don't receive a lot of customer orders - or if you otherwise have a generally static website.

Backup Storage: Where you store your backups is just as important as the backups themselves. You need to safely store your website backups away from your website, such as downloaded to your computer or uploaded to a third-party cloud storage service.

Backup Restoration: Properly restoring a backup is fairly technical, so you should always have help from an expert. This is especially true if you're restoring a backup due to a hack. If you don't find and patch the vulnerability that originally led to the hack, your website can easily be hacked again.

Pick Your Expert Now! If something goes wrong, do you know who you're going to call or email for help? You should figure this out long before something happens. Whoever they may be, call them up and ask them the what if kind of questions. This way, you can generally know what to expect if their assistance is needed.

Insider Tip: At Shawna Leigh Designs, we do not recommend the automatic malware and virus removal services that some hosting companies offer. In our experience, they usually end up leaving more of a mess and don't always fix the root cause. You need an expert on your team that will look at the data, find the root cause, offer a solution, and provide assistance going forward.

WHAT YOU DO SHOULD DO: Work with your website hosting provider or the expert that built your website to find the best backup solutions for your situation. Thinking about what could happen, will help you better prepare if something does happen.

Don't forget, backups will only help you get back up and running quicker. Backups won't always be the solution to every problem. Depending on the extent of any other damage done, there could be other issues to fix. These could include simple issues like your website's IP being blacklisted to more serious things such as notifying your customers of a data breach.

If you host your WordPress website with Shawna Leigh Designs, choose the Security Performance, and Backups (SPB) Add-On to handle backups for you!

WRAPPING UP

The takeaway of this questionnaire is that if you cannot confidently answer one or more of these important questions on a regular basis, you will need the help of an expert to run and maintain your eCommerce website - or some more learning to do before you setup shop on your own.

But, in a world of DIY, we can't forget or deny that sometimes we still need help. There's a lot of technical stuff that's covered in this questionnaire, and even more that's not that could still pertain to your situation.

At Shawna Leigh Designs, we want to help you! It's our goal and mission to help small businesses with ALL of their online needs. If we're ever unable to confidently answer your questions or help you, we'll do our best to guide you to someone that can!

So visit shawnaleighdesigns.com today to see how we can help you!

Feedback: All feedback is welcomed as it will serve only to improve this questionnaire. Please email support@shawnaleighdesigns with the subject FEEDBACK.