A 10-POINT WEBSITE SECURITY AUDIT

TIPS FOR SECURING YOUR ONLINE STORE
Introduction

Running an ecommerce website means taking a more proactive approach to your site's security. As an online store owner, it's your responsibility to take the necessary precautions to protect customer accounts and data.

Plus, downtime related to a hack or security breach is even more expensive for ecommerce websites. That's why your website's uptime has never been more valuable.

Now is the time to perform a security audit of your website. At the end of your website security audit, you should be able to answer these 10 questions:

1. Is my store on the right platform?
2. Is my store on the right web host?
3. Is my shop PCI-DSS compliant?
4. Do I collect too much data on my customers?
5. Am I encrypting communication between my customers and my store?
6. Are my customer accounts secure?
7. Is the software running my online store up to date?
8. Am I regularly visiting the front-end of my site?
9. Am I using a CDN and WAF?
10. Do I protect my connection when working in public spaces?

Don't fret if you don't know how to answer some or all of these questions. You will know how to answer all of these questions by the end of this post.
1. Is my store on the right platform?

Shopify, Magento, and WordPress are three of the most popular platforms that people use to create their stores. None of these platforms would be popular eCommerce solutions if they weren't secure. All three platforms have their strengths and weaknesses, so you should do a little research to find out which one best fits your needs.

A quick audit of your current platform might include the following questions:

- 1. Does the platform frequently push out updates to address security vulnerabilities?
- 2. Does the platform employ/utilize a team who is devoted to ensuring security standards are met?
- 3. Does the platform have a history of large-scale data breaches or vulnerabilities that were left open?
- 4. What is the reputation of the platform as being secure?

One thing to keep in mind is how easy it would be to move your store to another platform or host. If you need to move away from Shopify, you can migrate Shopify to WooCommerce. However, it won't be as easy as moving a WordPress store to a new web host. WordPress also allows for more customization and flexibility for the tools you can use.
2. Is my store on the right web host?

Putting your website on the same shared hosting as your friend’s blog is a bad idea. Why? An eCommerce website adds a lot of complexity that requires higher expertise to properly secure. You didn’t create a store because you dreamed of becoming a cybersecurity expert, so you should offload that responsibility to your host.

Investing in an eCommerce focused hosting solution like Liquid Web’s Managed WooCommerce Hosting or Managed WordPress hosting is the way to go.

Full disclosure, Liquid Web is our parent company, but it is seriously great hosting for you. Go price shop and find another hosting company that competes with that value at that price.

Having a managed eCommerce host will save you a lot of time and hassle in managing your site—time you can use to grow your business instead.
3. Is my shop PCI-DSS compliant?

If you accept credit card payments, you must meet Payment Card Industry Data Security Standards (PCI-DSS). According to the official PCI Security Standards Council, “If you accept or process payment cards, the PCI Data Security Standards apply to you.”

These standards include over 300 different security requirements, but here’s an overview of PCI-DSS best practices.

<table>
<thead>
<tr>
<th>GOALS</th>
<th>PCI DSS REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and maintain a secure network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameter</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
</tbody>
</table>
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need-to-know  
8. Assign a unique ID to each person with computer access  
9. Restrict physical access to cardholder data |
|------------------------------------------|------------------------------------------------------------------------------------------------|
| Regularly Monitor and Test Networks      | 10. Track and monitor all access to network resources and cardholder data  
11. Regularly test security systems and processes |
| Maintain an Information Security Policy   | 12. Maintain a policy that addresses information security for employees and contractors |

When you elect to take people’s debit card numbers, meeting these requirements will go a long way in preventing a malicious attacker from draining their bank account. It's a good idea to get some expert advice to ensure you are meeting the PCI-DSS requirements.
4. Do I collect too much data on my customers?

The more information you collect on your customers, the more information that can be compromised during a breach. These days, we can hardly go a week without hearing that some company was the victim of a data breach that exposed customer data. For example, in the Doordash breach, customer’s phone numbers, email addresses, home addresses and hashed passwords were compromised. That combination of information could be all that is needed to take out a fraudulent loan.

You should never collect more information on your customers than you need. If you are selling digital products that do not automatically renew, why would you collect and store mailing address?

You should also consider using a payment gateway like Stripe. Payment gateways allow you to offload credit card payments, so your store can accept online payments without processing or storing credit card numbers. Stripe will also help you become PCI-DDS compliant.

Unfortunately, there will always be attackers online, and there will not be a lack of reports of sites being compromised. Limiting the information you collect on your customers will limit the amount of information exposed during a breach. You can’t lose sensitive customer data you don’t have.
5. Am I encrypting communication between my customers and my store?

SSL encrypts the communication that your customers type in their browser and send to your site. With SSL, when someone enters their account name and password, it will be protected when that information is sent to your site’s server for confirmation. Encrypting the username and password will make it harder for an attacker to intercept the username and password in transit from their browser to your server.

We aren’t going to spend too much time on this because we will assume that everyone is already using an SSL certificate on their site. You can check out our WordPress Https Training if you are unfamiliar with SSL. If you are using an ecommerce-specialized host, your site is likely already securely using SSL.
6. Are my customer accounts secure?

A brute force attack is the most common type of attack on your customer accounts. Brute force is a type of attack when a hacker tries to guess a random combination of usernames and passwords until they find the right one. The reason that brute force attacks are so popular is that the skill barrier of entry is very low. You can find plenty of free password cracking tools with a quick Google search.

The great news is that using a WordPress security plugin like iThemes Security Pro on your WordPress site makes it easy to prevent attacks on your customer’s login from being successful.

Based on research by Google security blog, you should follow these 5 rules to stop 100% of brute force attacks:

<table>
<thead>
<tr>
<th>RULE</th>
<th>DESCRIPTION</th>
<th>SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit Failed Login Attempts</td>
<td>Limit the number of incorrect login attempts a bot can try before being locked out.</td>
<td>The iThemes Security Pro WordPress Brute Force Protection feature gives you the power to set the number of allowed failed login attempts before a username or IP is locked out. A lockout will temporarily disable the attacker’s ability to make login attempts. Once the attackers have been locked out three times, they will be banned from even viewing the site.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Force Strong Passwords</td>
<td>A password that is at least 12 characters long, random and includes a large pool of characters like “ISt8XXal28X3” will make it very difficult to crack.</td>
<td>Require users that can make edits to WordPress to use strong passwords. Using a WordPress security plugin like iThemes Security Pro to force privileged users to use strong passwords will help to increase the WordPress login security.</td>
</tr>
<tr>
<td>Refuse Compromised Passwords</td>
<td>The more users you have that are reusing passwords, the weaker your WordPress login security will be.</td>
<td>Prevent your customers from using known compromised passwords. iThemes Security Pro takes advantage of the HaveIBeenPwned API to detect whether or not a password has appeared in a data breach. If a password was found in a data breach, iThemes Security will require you to update your account's password immediately.</td>
</tr>
<tr>
<td>Use Two-Factor Authentication</td>
<td>There is no better way to secure your customer accounts than by requiring WordPress two-factor authentication. Two-factor authentication requires an extra code along with your WordPress username and password to log in.</td>
<td>Using a WordPress security plugin, like iThemes Security Pro, you can add WordPress two-factor authentication to your WordPress site. Enable either the email or mobile app method of two-factor. You can also use the WordPress Passwordless Login feature to make it even easier to login with the security of two-factor.</td>
</tr>
</tbody>
</table>
You may be thinking that you would never make it harder for your customers to login. It is up to us, as store owners, to require strong passwords and two-factor authentication to secure customer accounts. Because when a customer’s account is hacked, store owners are likely to get the blame.

The good news is that the iThemes Security Pro plugin has a new WordPress passwordless login feature that allows you to require users to use strong passwords and two-factor authentication without ever entering a password or an extra authentication code. You can now offer all of the security without sacrificing any of the usability.
7. Is the software running my online store up to date?

Software updates are not just for new features or bug fixes. Updates can also include security patches for known security exploits. Running outdated software with known exploits is one of the most common reasons websites are hacked. It is crucial to the security of your WordPress site that you have an update routine. You should be logging into your sites at least once a week to perform updates.

Using the iThemes Security Pro plugin’s Version Management feature, you can enable automatic WordPress updates to ensure you are getting the latest security patches. Updating your software is the easiest thing you can do to help protect your online store.
8. Am I regularly visiting the front-end of my site?

When was the last time you ran through the front-end of your site or even looked at your homepage? As busy site owners, we typically log straight into the backend of our sites to add new products, content and perform site updates. Running through your site’s pages and products can help you find signs of infection. You should look for these 3 signs of infections when inspecting the front-end of your site or when asking *is my WordPress site hacked*.

- **Check your homepage for changes** – The primary goal of some hacks is to troll a website or gain notoriety. So they only change your homepage to something they find funny or to leave a hacked by calling card.
- **Look for any malicious pop-ups or spam** – Are there any products being advertised on your site that you don’t sell?
- **Find unexpected redirects** – Do you click on one of your product links only to be redirected to a malicious shop trying to harvest your customer’s data?

Using the iThemes Security Pro’s File Change Detection feature can help make you aware of any unexpected changes made to your site. It is crucial to be alerted to a successful attack on your site, the sooner the breach is identified the more you can mitigate the damage done.
9. Am I using a CDN and WAF?

Using a content delivery network (CDN) like Cloudflare CDN can help to protect your shop from DDoS attacks. The CDN is on a different server than your site and is able to inspect requests to your site before they ever make it to your site. A Denial of Service Attack (DDos) is when an attacker tries to disrupt or bring your site down with a flood of internet traffic. Depending on your hosting plan, it may not take very much extra traffic to bring your site down.

A CDN can help mitigate a DDoS attack in a couple of different ways. The first thing a CDN will do is actively monitor and identify that your site is under attack, which is critical. You can’t stop an attack that you aren’t set up to detect. Once the malicious IPs are identified the CDN will prevent any requests from the IPs from ever hitting your site.

You should also consider using a Web Application Firewall (WAF). A WAF is able to identify and filter out malicious traffic before it hits your site. Unlike a PHP Web Application Firewall, a WAF like the Cloudflare WAF provides isn’t on the same server as your site. So all of the security filtering is done offsite and doesn’t add any extra load or slow down your site.
10. Do I protect my connection when working in public spaces?

One of the great things about running an online shop is that you can work anywhere. Unfortunately, public wifi is known to be very insecure making public libraries, hotels, coffee shops and airports prime locations for hackers to intercept communication and harvest passwords.

I once worked with an iThemes Security Pro customer who couldn’t figure out how their admin account kept getting hacked even after they changed their password. After some back forth I found out that they like to work from their local library, and that they were connected to the wifi without using a virtual private network (VPN).

A virtual private network allows you to safely communicate with your bank or online shop by encrypting your internet traffic. Since the iThemes Security Pro customer wasn’t using a VPN their traffic wasn’t encrypted and their password kept getting intercepted by a malicious actor. After we suggested they try using a VPN at the local library, they reported back to us that using the VPN put a stop to the hacks.

If you need any more proof about the insecurity of public wifi, here is a great USA Today article where a journalist wrote about his experience being hacked while using inflight wifi: *I got hacked mid-air while writing an Apple-FBI story.*
Wrapping Up: Online Security
Best Practices

Most attacks on your online store can be prevented from being successful with a little action on your part. Right now is a great time to do a security audit of your website to be sure your site is secure!
Get started with our single site iThemes Security Pro plan for just $49* with coupon code SECUREMYWP

BUY NOW FOR $49 →

*Offer good on any *new* iThemes Security Pro (1 site) plugin purchase. Coupon can’t be used to renew or extend an existing iThemes Security Pro (1 site) plugin membership.