WEBSCOOT

EASIEST WAYS TO IMPROVE

MAGENTO SECURITY

Step-by-Step Guide for Your Website

Table of Contents

This workbook is designed to help you with tips and strategies on how to increase your website speed.

Introduction to **Magento Security**

eCommerce websites are extremely vulnerable to cyber threats. They store sensitive information (passwords, addresses, credit card details, etc) which is why hackers pull on a lot of strings to execute a successful data breach.

Cyber attacks on eCommerce websites have seen a consistent uptick in the past few years.

Even leading platforms like Magento can't ensure bulletproof security. However, there are a lot of measures you can take, in order to tighten your store's security to a large extent and reduce exposure to hacking incidents.

This guide will touch upon all the steps you can take to air-tight your Magento store's security.

Benefits of **Secured Magento Store**?

- Encrypted User Data
- Better SEO Rankings
- Increased Conversions
- Enhance Website Trust
- Better Customer Retention
- Increased Customer Confidence

01.

Important **Pre-requisites**

1.1 Things to Know About Magento Security

- The Magento team regularly keeps releasing security patches that fix bugs or add extra protection to Magento storefronts. These must be updated and installed diligently
- Magento is not the most secure eCommerce platform out there.
- It has a large repository of modules and extensions that can offer you advanced security.

1.2 PCI Compliance

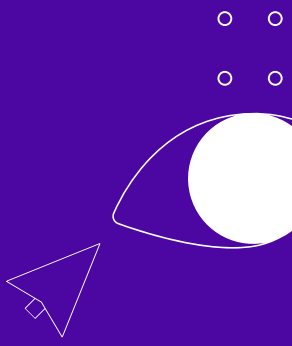
The Payment Card Industry Data Security Standard (PCI DSS) is applicable to all businesses that accept credit card payments.

Since your online business will be accepting card payments and transmitting credit card details, you need to ensure that your data is hosted on secure servers by web hosts that are PCI Compliant. If a merchant is found to be non-compliant, payment industry regulators might impose heavy penalties and restrictions (like suspension of credit card payment processing).

The latest version of PCI DSS includes 12 requirements that must be followed by all merchants. Discussing all of them in detail is beyond the scope of this article. In brief, PCI-DSS covers measures like:

- Installing and maintaining a firewall configuration to protect cardholder data
- Encrypting transmission of cardholder data across open, public networks
- Identifying and authenticating access to system components
- Restricting access to cardholder data
- Regularly testing security systems and processes
- Protecting all systems against malware and regularly updating antivirus software or programs
- Not using vendor-supplied defaults for system passwords and other security parameters

An eCommerce host that offers website security will make sure that all the above requirements have been met properly.



1.3 TLS & HTTPS

The 'S' in the HTTPS protocol stands for SSL (Secure Socket Layer) certificate. An SSL (now TLS) certificate will encrypt the communication that is happening between your website servers and client computers.

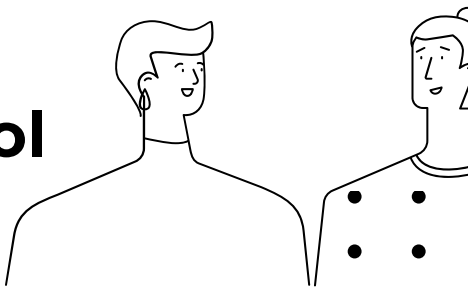
It's mandatory for all websites to operate in an HTTPS environment. Without it, any interaction your customers have with your website can be intercepted and sensitive data can get stolen easily.

Moreover, not having an HTTPS protocol can also affect the SEO rankings of your website as Google considers websites without SSL certificates to be insecure, affecting their rankings on the search engine.

One of the requirements of PCI DSS is also to encrypt the transmission of cardholder data across open networks. You can easily purchase and set up an SSL certificate online while buying the domain of your website.

02.

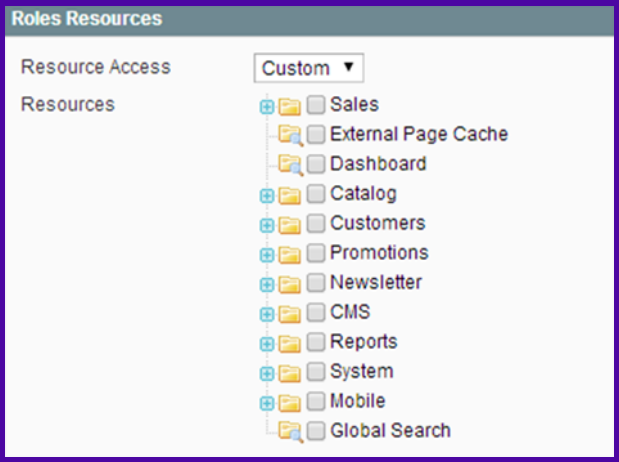
Access Control Measures



Proper access control measures will help you tighten the security for your Magento storefront. You can reduce the possibility of a data infiltration by setting strong passwords, restricting access to admin area, setting up 2FAs, etc.

2.1 Define User Roles

When giving access of your Magento storefront try and give privileges to a very small number of people, preferably for a limited amount of time. In Magento 1 & 2 you can create custom roles and decide which resources those roles will be able to access from your website.



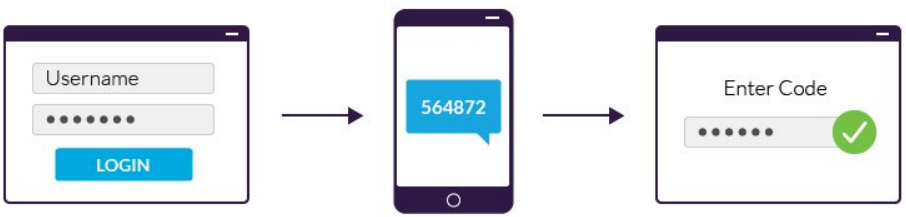
Here's how you can create a new custom role:

- Log into Magento as Administrator.
- Navigate to the Admin menu and select System > Permissions > Roles.
- Select the Add New Role button.
- Enter a name to describe your new Role.
- On the left-hand panel, select Role Resources.
- Select the admin resource checkboxes that you want to grant for this role

Two-Factor Authentication (2FA/MFA)

2FA's are quite common these days. After you've entered the username and password to an account, you're asked to provide another code or pin that only you can access. Usually, these One Time Passwords (OTPs) are received on your phone or email.

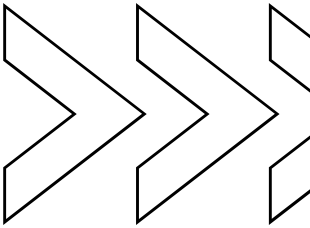
How **Two Factor Authentication** Works?



The user enters in their username and password.

An authentication code is sent to the user's mobile device.

The user enters in their authentication code to log into the application.



Sometimes double verification could also mean fingerprint scans or face detection once you've entered your password.

This step will easily fail any password guessing hacking scheme, because the hacker will not be able to login to your account even if they've guessed your password.

2FAs are inbuilt in Magento's core module. If you enable 2FAs, then admin users have to go through a two-step process in order to login to the Admin backend.

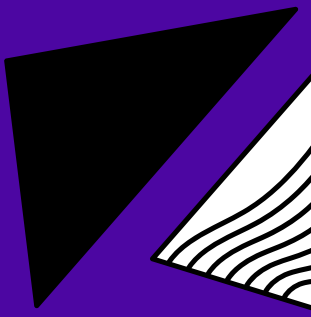
This feature is not applicable to customer accounts. You can also add 2FA to any page on your storefront using Google authenticator.

2.3 Restrict Access

- You can install extensions or modules that block unauthorized IP addresses
- **IP Whitelisting**: you can limit access only to trusted IP addresses by creating lists or IP ranges that can access your store's backend.

03.

Basic Magento **Security Measures**



3.1 Backups

Backups will revive your system to the last known configuration. This means, you need to run backups for your data as often as you can. In case your store is compromised, you will can restore your data without having to start from scratch.

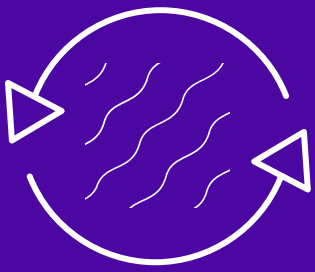
Make sure your secure these assets while taking backups:

- Server log files
- Magento file system
- Magento database
- Custom files and configurations

Here a few tips:

- Always **automate** backup tasks, so that they run in the background when your e-store is functioning.
- Store your backups in an **offsite location** (a different server perhaps) so that your backup doesn't get infected in case of compromise
- Be clear on what file types you want to include while backing up your data. Some files (like archives) may be excluded.

Web Application Firewall



3.2 Web Application Firewall (WAF)

A WAF is a thick layer of security that detects unwanted traffic and blocks it before can reach your network. For example, we use Sucuri firewalls on our servers to protect our client websites and their data.

Apart from the techniques we mentioned above, our Sucuri WAFs use IP whitelisting, signature detection, and bot & scan blocking to prevent brute force attacks. Bots attempting to log in are proactively detected and blocked, without affecting the normal traffic to our client websites.

3.3 SFTP/SSH

Transferring your files securely to and from your server is essential for security as it minimizes the chances of interception. SFTP/SSH will encrypt your data during transmission so that hackers can't steal it. Here's a brief explanation of the two:

Here's a brief explanation of the two:

- **SSH** or Secure Socket Shell is a secure transport layer that encrypts all kinds of file transfers and authentication procedures.
- **SFTP** is just an extension of SSH. It is a network protocol that facilitates file transfer and file management over any reliable network.

Using the above two protocols while logging into the Magento admin panel and adding backend data and files will ensure that important information doesn't leak into the wrong hands.

3.4 Choose the Right Hosting Service

The environment you host your website will greatly affect the security of your website servers and data. You have four options:

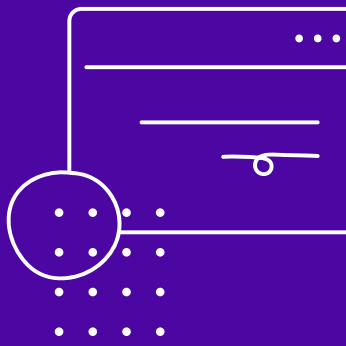
- Shared hosting
- Fully managed hosting
- VPS hosting environment
- Dedicated servers

For Magento, it is recommended to go for fully managed or dedicated hosting services. A fully managed host will provide an all-inclusive service where you won't have to worry about the hosting side of operations at all. Apart from security, the uptime and scalability of your website will also be looked after.

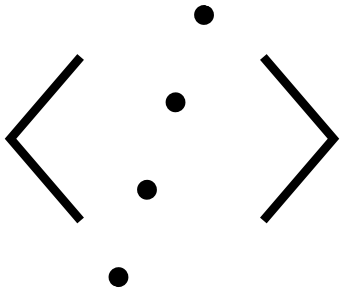
Fully managed hosting services will monitor your website at all times, and take all proactive measures necessary to create a sturdy layer of security for your website. For example, this is what we offer for security to our clients:

- WAFs, SFTP, SSL,
- Proactive monitoring
- Immediate response in case of attacks
- Regular scanning for malware and viruses
- Daily backups

If you're a large company and have an IT department that can handle the hosting side of operations on their own, then you can go for VPS (Virtual Private Server) hosting as well.



Pro tip: Shared hosting plans for Magento are not advisable. Magento is a heavy platform that requires dedicated resources for maximum performance and easy scalability. The most optimum solution would be to go for a fully managed cloud hosting service.



3.5 .htaccess Configurations

If you're using the Apache web server, you can employ a .htaccess configuration file to protect the system.

In order to verify that .htaccess protection is working like it should try the following request: **http://www.example.com /app/etc/local.xml.**

Remember to replace example.com with your own domain name.

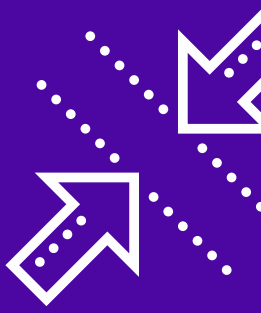
If the contents of the local.xml file are returned, you'll need to change your web server settings.

You can use the .htaccess configuration system for password protection, blocking offline browsers and 'bad bots', restricting access to certain IP addresses, and more.

Related read: Choosing the Best Magento Hosting: The Ultimate Guide

04.

Magento Security Best Practices



4.1 Use Strong Passwords

Surprisingly, 80% of hacking related breaches are because of weak passwords.

in March 2018, around 1000 Magento open source accounts were compromised due to brute force attacks. The attackers used those accounts to steal credit card information and cryptocurrency mining

Your password needs to be:

- **Unique**: This means it hasn't been set on any other website with your username. If you use the same password for many websites, then hackers can use it to breach other accounts you have on the web and steal more information.

- **Long**: a four-digit pin (using only numbers) can have 10,000 possible combinations. Using software, this pin can be cracked in a matter of minutes. Which is why it's advisable to set a password that has around 15-20 characters to make guessing harder.

- **Less obvious**: people usually use birth dates, their own names, names of things, or people close to them, etc in their passwords. Finding personal information is easier nowadays. Choose terminology which might not be directly related to you but is easy to recall.

- **Complex**: use a combination of upper case and lower case letters, along with signs, numbers and symbols.

4.2 Limit Login Attempts for Magento Admin

Hackers sometimes attempt brute force attacks in order to gain access to your Magento admin panel. If you limit login attempts per user, the hacker's chance of breaking in will reduce considerably.

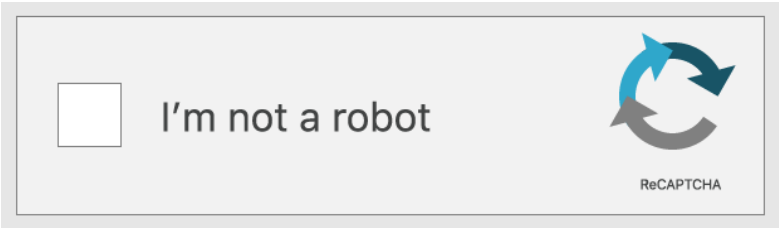
Remember that different accounts and IP addresses can be used for each attempt. A common practice is to temporarily block an IP or account from attempting to log in after 4 or 5 failed attempts. Each time 4-5 failed attempts have been made, you can increase the temporary block duration. This will buy you time and your systems will be able to detect brute force bots and block them before they can do damage.

Enable Captcha

Adding Captcha to your Magento login page can make it difficult for bot attacks to succeed, as its challenges are designed for humans to solve. Captcha is used on all pages where users have to enter sensitive information.

To enable Captcha on your Magento store, do the following:

- Navigate to **Stores>Settings**
- Click on **Configuration**
- Go to **Advanced>Admin** in the left-most panel
- Expand the **Captcha** section; Select 'Yes' to enable CAPTCHA



Captcha

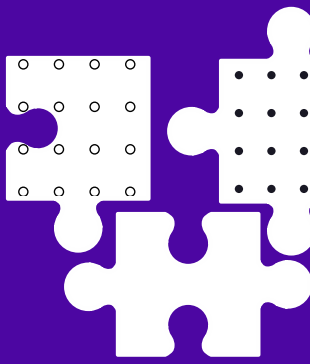
4.4 Regular Audits and Scans

You can integrate various tools to proactively monitor your website's security. Regular audits will inform you if there are any issues that need to be addressed.

- **Alerting tools**: if a user logs in to your Magento account or makes changes, and alerting tool will immediately notify you of the activity. You'll easily be able to detect unusual activity.
- **Security scanner**: this tool will check if all your security patches are up to date and if there are any loose ends in your website's security, leaving you vulnerable to an attack.
- **File integrity scanner**: you will keep adding files to your Magento backend. It's possible that those new files are compromised or infected. This tool will help you scrutinize all those files and ensure their core integrity.

05.

Protection Against **Software Vulnerabilities**



5.1 Regular Security Patching

As we've mentioned above, Magento keeps releasing security patches. Installing these promptly after release is the most crucial step you will take to tighten your Magento storefront's security. These patches contain bug fixes and protect your Magento platform from any recent security vulnerabilities. Along with that, it may include some new security features as well.

Before installing, make sure that you have the latest backup of your store's data ready. Also carefully read the version notes of the security patch you're about to download. Read the changes being introduced and assess how they will impact your store operations.

5.2 Monitoring & Updating Modules & Extensions

A Magento storefront requires a lot of third party extensions for better functioning. Faulty plugins are the main source of hacking on Magento, as they can infect your site with Malware or leave it open to attacks. Here's how you can prevent this from happening:

- Keep updating all third-party modules, extensions, themes, and plugins regularly.
- Choose extensions from trusted or verified vendors only. You can easily find Magento's premier and technology partners in the Magento marketplace. Also, be sure to read customer reviews carefully before making a call.
- You can use tools like MageReport, where you can scan your website to find out if there are any known vulnerabilities.
- Install tools that till regularly scan and audit your store's third-party extensions and identify security issues, if any.

- Install tools that till regularly scan and audit your store's third-party extensions and identify security issues, if any.

- Keep removing unused components if you don't feel you will use it in the near future. Simply disabling them will not eliminate the risk of compromise.
- Monitor your extensions regularly. Check their functioning and look for updates. If there is an extension where the vendor hasn't provided an update for a long time, look for alternatives.

Finally...

Evidently, there is a lot one can do when it comes to Magento Security. No store is completely safe from cybercriminals, but if you take all the steps you can in the right direction, then the risk gets reduces considerably.

Get fully-managed hosting that takes care of speed, security, monitoring with Webscoot.io.

Run on AWS for fixed cost >>

WEBSCOOT
Faster eCommerce

SCAN THIS QR CODE FOR MORE EBOOKS ON ECOMMERCE