Website Security For Ecommerce Merchants

September 2020

everywhere
you want to be

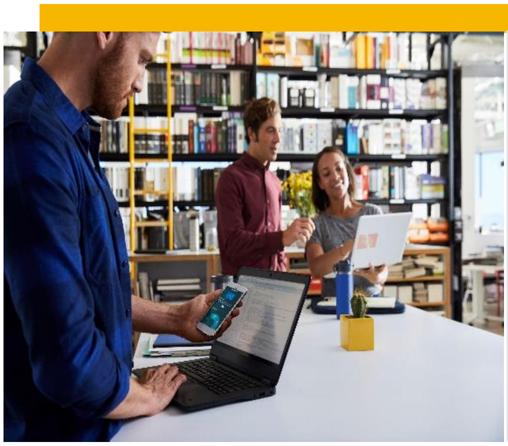
ABOUT THIS GUIDE:

Useful information to help merchants keep their ecommerce websites secure.

Overview

With the recent Magento 1 'end-of-life' support, merchants with online stores deployed on Magento 1 will lose all access to new features, functionality updates, bug fixes, and support from Adobe/Magento. Most importantly, any future vulnerabilities will no longer be addressed with new security patches from the company, leaving the unsupported versions of Magento exposed to security or data compromise incidents.

However, Magento is not the only targeted website platform so now is a good time to provide ecommerce merchants with some recommendations to keep their websites secure and avoid a security or data compromise incident:



This guide is designed to assist merchants in securing their ecommerce websites and protect their customer's payment card data.

Content Section

With the recent Magento 1 ‘end-of-life’ support, merchants with online stores deployed on Magento 1 will lose all access to new features, functionality updates, bug fixes, and support from Adobe/Magento. Most importantly, any future vulnerabilities will no longer be addressed with new security patches from the company, leaving the unsupported versions of Magento exposed to security or data compromise incidents.

However, Magento is not the only targeted website platform and so the purpose of this guide is to provide ecommerce merchants with recommendations to keep their websites secure in order to avoid a security or data compromise incident:

1. Keep all your Software Up-to-Date:

It is crucial to keep all platforms, applications or scripts you have installed up-to-date. Attackers aggressively target security flaws in popular web software, and the software needs to be updated and patched where security vulnerabilities are identified. Remember to maintain, update, and patch every software product you use.

2. Enforce Strong Authentication for Users:

It is important to use strong passwords. Software packages often come with default (preset) passwords such as “password” or “admin,” which are commonly known. Attackers are also known to frequently utilize automated ‘brute force’ software to guess and crack passwords. To help protect against brute force attacks, passwords should be complex, containing uppercase letters, lowercase letters, numerals, special characters and should be changed regularly.

Implementing a multi-factor authentication (MFA) solution for all remote network access and for users with privileged access rights can significantly reduce the likelihood of unauthorized access. Only provide users with access rights necessary to perform job functions.

3. Encrypt and protect your Login Pages:

Use SSL encryption on your login pages. SSL allows sensitive information such as credit card numbers and login credentials to be transmitted securely. Information entered on a page is encrypted so that it is meaningless to any third party who might intercept it. This helps to prevent attackers from accessing confidential data, for example, login credentials that they can then use to access the website’s administrative page. The attacker could then make changes to the website, add malicious code or compromise payment data, Personally Identifiable Information (PII), or other data.

It is also important to change the URL of the administrative webpage. This can make it more difficult for attackers to find the login page and therefore reduces the chance of an attack.

4. Use a Secure and PCI compliant Hosting Provider:

Choosing a secure and reputable web hosting company is critical to website security. Make sure the chosen hosting provider is aware of threats and devoted to keeping your website secure. Your hosting provider should also back up your data to a remote server and make it easy to restore in case your site is hacked. They should provide you with a Web Application Firewall (WAF) and anti-virus protection, which intercepts and inspects incoming data and removes malicious code, preventing damage or unauthorized intrusion to your website. Choose a hosting provider who offers ongoing technical support including any technical support of your company's incident response procedures, where applicable. Note that shared hosting environments carry added risks and sharing hosting providers would need to comply with additional requirements to protect each customer's hosted environment. Ensure the hosting provider you use is PCI compliant and the contract clearly identifies the hosting provider's responsibilities in securing the cardholder data.

5. Keep your Website Clean:

Every database, application, or plugin on your website is another possible point of entry for attackers. Delete any files, databases, or applications from your website that are no longer in use. It is also important to keep the file structure organized in order to track changes and make it easier to delete old files.

6. Backup your Data:

Back up your site regularly. You should maintain backups of all of your website files in case your site becomes inaccessible e.g. from system failure or ransomware. Your web host provider should provide backups of their own servers, but you should still backup your files regularly. Some content management programs have plugins or extensions that can automatically back up your site, but you should also be able to back up databases and content manually.

7. Scan your Website for Vulnerabilities:

It is important to perform regular web security scans to check for website and server vulnerabilities. Perform website security scans on at least a quarterly basis and after any change or addition to your website. It is recommended a Payment Card Industry (PCI) Authorized Scanning Vendor (ASV) - a company that is qualified and officially certified by the PCI Security Standards Council (SSC) performs external vulnerability assessments for entities as required by the Payment Card Industry (PCI) Data Security Standards (DSS).

A security scan provides an assessment of vulnerabilities on your website. However, a scan may not detect all security flaws on your website, system or back end databases because vulnerabilities are reported on an ongoing basis.

8. Monitor your Website:

If your website is attacked, it is important that an ‘alert’ is created for any unauthorized activity so that responsible personnel are notified and appropriate remediation can be implemented in a timely manner; there are a number of things that can be done to monitor the security and activity of your website:

File Integrity Monitoring (FIM) solutions are specifically designed to monitor for changes in files. The software typically takes a “snapshot” of your system, and then periodically compares that to the system’s current state. When it detects changes to files that suggest unauthorized intrusion it can alert you to take action to minimize the threat.

Website Logging – A web log file is a log file automatically created and maintained by a web server. Every "hit" to the website, including each view of a HTML document, image or other object, is logged. The raw web log file format is essentially one line of text for each hit to the website. This contains information about who was visiting the site, where they came from, and exactly what they were doing on the website. Regular review of these log files can provide you an opportunity to uncover suspicious website activities and these log files should be kept for at least 12 months.

9. Secure Payment Account Data:

Ecommerce merchants should consider outsourcing all payment processing to PCI DSS validated payment service providers that can directly receive cardholder data and therefore help reduce the risk of compromise should a website become vulnerable or even hacked. No electronic storage, processing, or transmission of any cardholder data on the merchant’s systems can reduce the attractiveness of a website being targeted and help to reduce the PCI DSS security requirements required in the first instance. For advice on securing payment account data speak to a Payment Card Industry (PCI) Qualified Security Assessor (QSA) or your acquiring bank.

Ensure payment data is not stored. If you must store payment data for reoccurring payments or other purposes you should utilize a payment card tokenization solution.