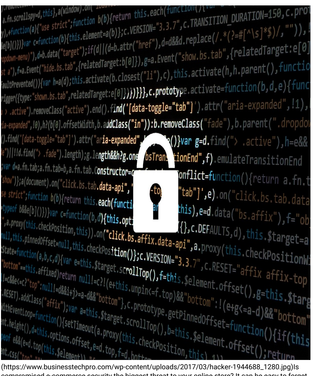
16 Things You Need to Ensure E-commerce Security

Mar

Whether you fear being hacked or losing the confidence of your customers, providing them with robust e-commerce security measures is just as important as getting conversions.



(https://www.businesstechpro.com/wp-content/uploads/2017/03/hacker-1944688_1280.jpg)Is compromised e-commerce security the biggest threat to your online store? It can be easy to forget about securing your website when you are trying to grow your business and reach new customers. However, leaving your e-commerce site open to cyber-attacks is not only the quickest way to being hacked but also losing your customer base and credibility. Protecting your website with substantial e-commerce security measures not only protects your customers and their information, but also the trust you have worked hard to build with them. People are less apt to buy from a website that has been compromised, so be sure that your e-commerce security has these things in place:

Adhering to PCI Compliance

The PCI Security Standards Council (https://www.pcisecuritystandards.org/) is a group of credit providers that includes American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc., established to maintain, improve, and evangelize the Payment Card Industry Data Security Standards (https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security) (PCI DSS). This set of standards was developed by the founding members of the PCI Security Standards Council and seeks to address the ever-changing landscape of data security in financial transactions.

Merchants who request, process, or store credit card information must adhere to these guidelines to ensure the security of customer information and your own site's trustworthiness. A good way of complying with the PCI DSS is through tokenization (https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf), or substituting the primary account number (PAN) from a customer's card with a surrogate value called a "token" to reduce the risk of the actual data being stolen by hackers.

Obtain an SSL Certificate

A Secure Sockets Layer (SSL) Certificate (https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/) is a small data file that applies a cryptographic key to the details of a website that activates the "green padlock" and the HTTPS protocol in the search bar. The SSL certificate provides a secure connection between a browser and a web server for processing credit card transactions, data exchanges, website logins, and secure browsing for social media websites. By obtaining an SSL certificate for improved e-commerce security, you can ensure that customers will be much safer when entering their critical information for purchases.

Encrypt Your Site with HTTPS

One of the more overlooked details when securing your site, getting an application protocol, or HTTPS (Hypertext Transport Protocol Secure (https://en.wikipedia.org/wiki/HTTPS)), is part of acquiring an SSL certificate and protects against most cyber-attacks. HTTPS provides encryption for your site to allow for secure data transfer while a regular HTTP can be intercepted and read. While using an HTTPS to secure your site is not 100% full-proof as is with anything else, it will drastically reduce the risk against your e-commerce store.

You will know you are protected when there are a green padlock and HTTPS in the top search box of a browser. However, it is important to note that while it can boost your e-commerce security, adding an HTTPS should only be reserved for web pages that collect customer information because it can slow load time a bit.

Prevent DoS and DDoS Attacks

Denial of Service (DoS) (https://www.us-cert.gov/ncas/tips/ST04-015) and Distributed Denial of Service (DDoS) (https://www.us-cert.gov/ncas/tips/ST04-015) can be a very big annoyance for any e-commerce website trying to reach customers. DoS and DDoS attacks can block out real users from your site by inundating your network with a flood of requests. This act can overwhelm the bandwidth of your network, making it very difficult for legitimate requests to get through, frustrating customers and cause them to leave the site.

The main difference between a DoS and DDoS attack is that a DoS uses one computer and network to spam you while a DDoS uses multiple machines and networks, making the latter more difficult to trace. One solution, though impractical and expensive, is to get more bandwidth. A more practical approach to protecting yourself from these attacks is to install a good firewall and maintain guarded control on your email filters for added e-commerce security.

Install a Firewall

While this for of e-commerce security may seem like a given in today's digital landscape, this protective measure cannot be understated. Using a strong firewall can prevent malicious or unwanted network access to your website and protect against the DoS and DDoS attacks mentioned above. Firewalls are an e-commerce site's first line of defense from unauthorized entry and come in many varieties. One of the more effective firewall types for e-commerce is application gateways, which serve as a checkpoint of sorts that hides your internal information from other outside networks and filters the appropriate information through.

However, the best option for keeping out cyber-attacks is a proxy firewall system; as opposed to a simple checkpoint, a proxy firewall is not directly connected to your data system and doesn't provide a clear path for hackers. The secret to any good firewall is proper installation and programming, so be sure whoever sets up your firewall correctly programs it to recognize crucial threats and keep it updated.

Layer Your Security

While a strong firewall is a good first line of defense against malicious cyber-attacks, you shouldn't depend only on the firewall for total e-commerce security. Adding multiple layers of roadblocks for would-be hackers reduces the risk to your stored data. Other layers can include account logins, submission forms, search boxes, CAPTCHA quizzes, and secondary verification systems.

Keep Your Site Updated and Patched

New loopholes and exploitable weak points are always being discovered on websites and network platforms, so it is very important to be vigilant in keeping your website as up-to-date as possible. Install patches when they become available and always be on the lookout for any weaknesses on your own to continuously improve your e-commerce security levels.

Backup Often

Sometimes losing all customer data due to a mishap can be worse than being hacked because it put the blame directly on you. Data can be lost due to power failure, natural disaster, or a malfunction of the system, and you need to be prepared should the worst happen. Put a recovery backup plan into place in which data is copied into an external system in the cloud or elsewhere where it can be easily restored.

Require Strong Passwords

If users log in to your website (and they should be logging in for security purposes), or for employees logging into the backend, requiring strong passwords makes it more difficult for hackers to get into your backend easily. Why fight the firewall if they can just enter your birthdate (not a good password, by the way)? Some widgets will autogenerate very long and complicated passwords for you, but here are some good guidelines to follow:

- Make passwords longer than the minimum
- Do not use something that is tied to you personally (spouse's name, birthdate, address, etc.) as someone can begin guessing at your passwords more easily
- Do not use sequential characters (123, ABC, etc.)
- Intersperse capital letters, lower-case letters, numbers, and symbols; the more random, the better (ex. 1tT]k_+53J) because these are next to impossible to guess

Obtain and Store Necessary Information Only

Not all information collected needs to be stored on in your data. You should only ever store what is necessary to maintain a user's account to minimize the risk to a customer. This idea can be done by not asking for frivolous or irrelevant information that does not concern the transaction. Keeping the bare minimum on file also makes you less liable should someone get past your cyber defenses because there is not much to steal in the first place.

Use external payment source service to mitigate risk

Using outside sources such as PayPal, Apple Pay, Samsung Pay or similar payment platforms virtually removes the risk of exposure from you since you are not collecting nor storing any customer data. By having customers go through another service, you may have to give a kickback to the service, but you are not liable if they are compromised.

Stay Vigilant

Sometimes the best defense you have is you and any staff you employ. Consistently keeping a sharp eye on your website and network will give you a better idea of normal traffic patterns and anomalies that need closer examination. Learning your website in and out will let your intuition detect things that do not seem right or outside the ordinary, and possibly helping you to prevent any major damage before it begins.

Properly Train Your Staff

If you employ staff members to help you run your site and daily operations, getting them up to speed on what to look for and what is considered normal can put more eyes on your processes, thus increasing your chances of spotting oddities when they happen and reduce your risk of exposure. You and your staff should always stay on top of current threats out there and fixes to keep them at bay.

Require Secondary Verification

An easy way to add more layered security, secondary verification methods are an added step to verify if a user is authentic or not. Authenticator apps such as Google Authenticator use autogenerated number codes that change every 30 seconds on a mobile device and are separate from the network. Secondary verification is very difficult to fake, particularly if access codes change constantly. Your website can employ secondary apps, CAPTCHA puzzles, and other external sources to complete verifications.

Use Tracking Numbers for All Transactions

If you have ever ordered something online from a reputable source, you will receive an email with a tracking number to track your package. These numbers also can prevent chargeback fraud perpetrated by malicious attacks to your site. These numbers confirm the transaction and make dealing with odd charges easier to fix.

Choose a Reliable Web Host

You can do your due diligence in maintaining your e-commerce store, but if the network you are using has weak security and is already compromised, you may still be in real trouble. Choose web host providers that take security just as serious as you should, and you've found a match made in e-commerce heaven.

For more information on keeping your e-commerce website safe from external threats, contact Business Tech Pro at (888) 326-6856 or support@businesstechpro.com (mailto:support@businesstechpro.com).

By application gateway (https://businesstechpro.com/tag/application-gateway/), backup (https://businesstechpro.com/tag/backup/), business tech pro (https://businesstechpro.com/tag/business-tech-pro/), captcha (https://businesstechpro.com/tag/captcha/), ddos (https://businesstechpro.com/tag/ddos/), dos (https://businesstechpro.com/tag/dos/), e-commerce security (https://businesstechpro.com/tag/e-commerce-security/), external payment method (https://businesstechpro.com/tag/external-payment-method/), firewall (https://businesstechpro.com/tag/firewall/), https (https://businesstechpro.com/tag/https/), layered security (https://businesstechpro.com/tag/layered-security/), patch (https://businesstechpro.com/tag/patch/), pci compliance (https://businesstechpro.com/tag/pci-compliance/), proxy (https://businesstechpro.com/tag/proxy/), recovery (https://businesstechpro.com/tag/recovery/), secondary verification (https://businesstechpro.com/tag/secondary-verification/), ssl certificate (https://businesstechpro.com/tag/ssl-certificate/), strong password (https://businesstechpro.com/tag/strong-password/), tracking number (https://businesstechpro.com/tag/tracking-number/), update (https://businesstechpro.com/tag/update/), web host (https://businesstechpro.com/tag/web-host/) 0 comment

Recent Posts

Gamification Adds Value to Marketing Strategies (https://businesstechpro.com/gamification-adds-value-marketing-strategies/)

5 Ways to Deal With Negative Comments Online (https://businesstechpro.com/5-ways-deal-negative-comments-online/)

Shorten Tweets in 10 Simple Ways (https://businesstechpro.com/shorten-tweets-10-simple-ways/)

Create Better Press Releases With These 12 Tips (https://businesstechpro.com/create-better-press-releases-12-tips/)

5 Digital Marketing Mistakes That Will Cost You (https://businesstechpro.com/5-digital-marketing-mistakes-cost/)

Recent Comments

Archives

August 2017 (https://businesstechpro.com/2017/08/)

July 2017 (https://businesstechpro.com/2017/07/)

June 2017 (https://businesstechpro.com/2017/06/)

May 2017 (https://businesstechpro.com/2017/05/)

March 2017 (https://businesstechpro.com/2017/03/)

February 2017 (https://businesstechpro.com/2017/02/)

January 2017 (https://businesstechpro.com/2017/01/)

December 2016 (https://businesstechpro.com/2016/12/)

November 2016 (https://businesstechpro.com/2016/11/)

September 2016 (https://businesstechpro.com/2016/09/)

August 2016 (https://businesstechpro.com/2016/08/)

July 2016 (https://businesstechpro.com/2016/07/)

April 2016 (https://businesstechpro.com/2016/04/)

March 2016 (https://businesstechpro.com/2016/03/)

February 2016 (https://businesstechpro.com/2016/02/)

October 2015 (https://businesstechpro.com/2015/10/)

Categories

BizTech Blog (https://businesstechpro.com/category/biztech-blog/)

Business Solutions (https://businesstechpro.com/category/business-solutions/)

E-Commerce (https://businesstechpro.com/category/e-commerce/)

Technology (https://businesstechpro.com/category/technology/)

Uncategorized (https://businesstechpro.com/category/uncategorized/)

Popular Recent

A brand new site for a brand new adventure (https://businesstechpro.com/hello-world-2/) Oct 09, 2015

Yappy for Business Communications: Insider Promo (https://businesstechpro.com/yapppy-business-communications-promo/) Feb 03, 2017

Shorten Tweets in 10 Simple Ways (https://businesstechpro.com/shorten-tweets-10-simple-ways/) Aug 16, 2017