***E-Commerce Secure Site***

**Introduction -**

This report will Discuss the technologies involved in setting up a secure E-Commerce site. It will also examine the strategies employed and the impact of E-Commerce on business organisations

Given how common hacking and breaches are, ecommerce websites are a real challenge from the security perspective. Though startup ecommerce businesses are tech savvy, they often lack the expertise to tighten their website’s security.

If the breaching issue is not dealt with, aspiring online shop owners are at risk of losing their site and customer data. Fortunately, there are several ways in which businesses can secure ecommerce websites and this article will elaborate on them.

**1. Choose a Better Ecommerce Hosting Service**

Choosing a web hosting service for your ecommerce site is important and security should be the top priority. Other than keeping hackers away, your hosting service must have a good backup service so that your ecommerce site can be easily restored after a security breach.

Ensure that the web host is operational 24/7, has maximum uptime and has RAID data protection that creates backup copy of your website on multiple disks. As a result, your website will perform faster.

For the purpose of hosting a secure ecommerce website, I recommend choosing a managed cloud-hosting platform. The engineers operating the managed cloud-hosting platform take care of your website’s security. Additionally, the admin can use the website’s admin panel can add further layers of security.

**2. Use HTTPS**

It would be best to move your website to HTTPS to avoid online frauds. Before you move your ecommerce website to HTTPS, you must have an SSL certificate. Once you purchase the certificate from a recognized SSL vendor or hosting company, install it and change the settings on your site.

Google uses HTTPS as a ranking signal to give your website a higher SERP ranking and hence, more visitors. HTTPS is essential for user protection as it creates a secure link between the users’ browsers and your servers to prevent hackers from stealing your data.

**3. Choose a Secure Ecommerce Platform**

Before choosing an ecommerce, you have to account for various factors such as support, performance and features. However, security must be given higher priority, otherwise all of the previously mentioned factors will be useless. Ensure that your ecommerce platform uses secure payment gateways, releases security patches and includes shipping method extensions.

There are plenty of secure ecommerce platforms available such as Magento, Prestashop and WooCommerce.

**4. Secure User Level Information**

Hackers can do a lot of damage to a website once they have access to user login information. You as the admin must ensure your customers are taking various precautions when using your ecommerce website.

The most secure approach I can recommend is automating the process of reminding the consumers to change their passwords after a month. Ensure that customers use unique passwords. The unique passwords must consist of at least 8 characters, a number, an upper and a lowercase letter and a symbol.

**5. Don’t Store Sensitive Customer Data**

You must make sure that you haven’t stored any sensitive data like customer credit card information on your website. Storing sensitive information is very risky because if your systems are compromised, then you could lose your customers’ trust. To prevent such incidents, you can use the process of tokenization. Tokenization generates random numbers called tokens in place of customer information. Tokenization also helps prevent credit card fraud.

**6. Run Vulnerability Tests On Your Website**

Performing regular vulnerability scans on your ecommerce website will leave very little opportunities for hacking. Each ecommerce platform comes with different tools that allow you to scan for vulnerabilities.

Choose a program that scans not only your website, but also your network so that you know the risks and issues that should be addressed and fixed. Consider well-known scanning programs such as Retina CS Community, OpenVAS and MBSA.

**7. Ensure Your Website is PCI DSS Compliant**

You as the admin must ensure that your site is PCI DSS compliant. PCI DSS is a security standard that increases admin control of customer card data in order to reduce credit card frauds. Your website will be able to detect and prevent potential breaches and hacks before it leads to an account data compromise (ADC) event.

**8. Keep Your Website Updated**

Hackers are always looking for vulnerabilities that can get them inside your website. When new vulnerabilities are discovered by developers, they release new software updates. Quickly update your website because you never know when the hackers will begin their attack.

**9. Take Regular Backups**

Ensure that you backup your ecommerce website frequently. After a hacking incident, you can then retrieve your website’s backup from your hosting provider and restore your website. Ensure that your hosting provider has an automatic backup service in case you forget to manually backup your data.

**10. Use Content Delivery Network**

A content delivery network is a network of distributed servers that delivers content to users based on the servers closest to their locations. CDNs store copies of your website’s content and learn to identify traces of malware. CDNs are deployed at the edge of your network for blocking DDoS attacks.

**Conclusion -**

In conclusion this tips given above and you will have a secure ecommerce website. Your ecommerce site will be safe for service, fast and efficient. If you have anything to say, do let me know in the comments below. repost talks about the use of business intelligence tools and technologies associated with it. This report will discuss the choice for dashboards/visuals to help management in their decision-making process.