Security Issues in E-Commerce: Need and Concept

E-commerce is an important revenue stream for many businesses, especially with legions of customers who prefer to use computers or tablets to complete shopping from home comfortably. Security is one of the biggest concerns of customers shopping online. To avoid jeopardizing your ecommerce transactions, you should remain vigilant with your security measures. Without robust mechanisms to protect their financial information, customers feel frightened easily - and often go to competitors to meet their shopping needs. Choosing a fast and secure hosting solution is key to protecting your customer data from hackers and phishing attacks so common today.

E-commerce security is a set of protocols that protect e-commerce transactions. Safety requirements must be provided to protect customers and businesses alike from threats such as credit card fraud, fraud and malware.

Here are essential e-commerce security features your website needs -

1. SSL Certification

SSL certificates encrypt sensitive information to ensure that any data is not readable to everyone other than the destination server.

When site visitors send data (such as credit card details or other personal information) over the Internet, it is passed across multiple computers before reaching the destination server. If this data is not SSL certified, it may be stolen at any time during this chain.

2. Use HTTPS

Easy to check. Take a look at your website. In the upper left corner of the URL fields, you will see either "http: //" gray or "https: //" gray.

If you have the latter! If you have a previous one, then you need to fix this! HTTPS is a data transmission protocol over the web that should be used instead of HTTP on all pages where data is generated while data is encrypted. It's all about coding. With HTTP, the information is not encrypted - instead, it is sent as plain text, which means that anyone can intercept it and read what has been sent.

Many customers now know about this security feature and people will avoid ecommerce websites that still use HTTP. HTTP preservation can have a negative impact on your site before the hacker can read your personal information. HTTPS should only be used on pages that collect data and other sensitive information - you do not have to include it on Our About pages etc.

3. Monitor Your Site

Without someone like Quentosity watching your website, you can be prone to constant attacks on the website. If you are constantly monitoring your site, you will be able to quickly identify and close any potential piracy activity, thus preventing any data loss and theft of information that can all be exposed to safety and customer confidence.

4. Scan for Malware

Regular checking your site for malware will pick up a bad code on the website hackers put there.

A provider like Quentosity will run a malware scan repeatedly and choose from every 6 months, monthly, or even weekly to ensure your site is secure.

5. Ask for a CVV Number

CVV indicates the value of card verification. CVV is the three or four digit code on the back of a credit or debit card. If the hacker has a credit card number and not the physical card, CVV requirements will make it more difficult to complete a fraudulent transaction.