Electronics Commerce Security Environment

E-commerce security refers to the principles that guide safe electronic transactions, allowing the purchase and sale of goods and services online, but with protocols to provide security for participants. The success of an online business depends on customer confidence that the company has the fundamentals of e-commerce security.

E-commerce embodies many business transactions using electronic systems. An e-commerce website includes an intranet that may interact with the World Wide Web. E-commerce has presented both external and internal risks to businesses and the websites they link to.

- External threats to the e-commerce website arise from various sources related to the electronic economic environment in addition to the risks related to the external Internet.

- Internal threats come from employees, internal network, management, and business operations. The most common risks are security issues that relate to the interface between consumer and network transactions.

Privacy

Privacy is one of the most obvious basics of e-commerce security, which in this case means not sharing information with unauthorized parties. When you shop online, no one should have access to your personal details or account information except the seller you choose to share with. Any disclosure of this information by the merchant will be a breach of confidentiality. The company is responsible for providing at least minimum encryption, virus protection, and firewall so that bank details and credit card information remain private.

Integrity

The second important concept in secure e-commerce is the idea of integrity - that none of the information that a customer shares online will be altered in any way. This principle states that a secure transaction involves unchanging data - since the business uses only exactly what was entered on the website by the buyer. Any manipulation of the information breaks the buyer's confidence in the safety of the transaction and the integrity of the company in general.

Authentication

In order for e-commerce to take place, both the seller and the buyer must be what they say. A business can only sell if it's real, the products are real, and the sale will go through as shown online. The buyer must also provide proof of identity in order for the merchant to feel safe about the sale. In e-commerce, identification and fraudulent authentication are possible, and many companies hire an expert to ensure these types of e-commerce security fundamentals exist. Common solutions include technology solutions - customer logins and passwords or additional credit card PINs.

Techniques to combat e-commerce threats

1. Encryption:

It is defined as a mechanism for converting regular information into encrypted content that cannot be read by others except for the person who sends or receives this message.

2. Having digital certificates:

It is known as a digital certificate issued by a trustworthy third-party company. An SSL certificate is necessary because it gives a high level of authentication to the website. The main function of this certificate is to secure an e-commerce website from unintended attacks such as Man-in-middle attacks.

Risk in social media marketing

1. Time intensive :

Maintaining an interactive presence on social media is time consuming and stressful. There is a need to monitor every social network, respond to inquiries and post valuable updates.

2. Negative feedback:

Social media users are free to post what they want. Sometimes, the unhappy customer leaves anger associated with your business. Moreover, some negative comments come from disaffected employees of the company which make the whole business look bad.

3. The possibility of embarrassment:

It's easy to get involved on social media and post anything that comes to mind, which greatly affects any business.