**Introduction**

Today, privacy, security and trust are major concerns for electronic technologies. Ecommerce security is specifically applied to the components that affect e-commerce namely computer security, data security, integrity, availability and other wider realms of the Information Security framework.

* Web e-commerce applications that handle payments such as electronic transactions using credit cards or debit cards, online banking, PayPal or other tokens have more compliance issues and are at increased risk from being targeted than other websites as they suffer greater consequences if there is data loss or alteration.
* Mule, Trojan horse and worms if launched against client systems, pose the greatest threat to e-commerce privacy and security because they can subvert most of the authorization and authentication mechanisms used in an ecommerce transaction
* Viruses are a nuisance threat in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool.

**E-commerce usage all over the world**





Headha

**Technologies used for e-commerce Security**

1. Encryption algorithms like Public Key Infrastructure (PKI) systems which are based on asymmetric cryptography are highly secure as they are coupled with Secure Socket Layer (SSL) protocol and the interbank standard suite, ANSI X9. PKI often requires a centralized, highly available intermediary for key management, and especially for prompt notification about revoked key-pairs.
2. A digital signature, which can be used to sign contracts, to prove identity for access or to provide authenticity of an electronic distribution is the best example of PKI.
3. Smartcards can be used to store data about the bearer of the card, including identification credentials, financial data, medical records etc. Smartcards can allow POS transactions to be more intricate, because the entire user’s data is always available. This architecture can also avoid the centralized storage of personally sensitive data.
4. Digital cash and networked payments through which a consumer might buy electronic data or a digital service without revealing his purchases to a financial clearinghouse and identity to the merchant. Micropayments such as per-article newspaper subscriptions and PayPal, a payment intermediary, have also been financially successful.
5. Digital watermarking technology is another popular internet security mechanism where the technical goal is to find ways of cryptographically tagging electronic content (especially images and audio) in a way that is non-removable, non-forgeable, and recognizable. The watermark tag is generally designed to be invisible or unobtrusive.

**RISK MANAGEMENT TO REDUCE THE E-COMMERCE RISK**

Electronic payment is an easy, quick and cheap payment system based on electronic communication. Buyers and sellers do their deals without seeing each other. The rapid development of the internet brought e-commerce to public attention, and it was acknowledged to be full of potential. In ecommerce, there are many ways in which an unscrupulous person can cheat users. In the early days of the internet, the popularity of e-commerce hinged on whether data transfers could be made secure. Although the following options may not be helpful for ending risk in e-commerce, they may help to reduce it:

1. Training to team on e-commerce risks: Train your team in risk management policies and procedures, and the fraud and security risks involved in an e-commerce transaction. The more informed your organization is, the easier it will be to combat online threats and to carry out risk mitigating measures.
2. Spread organizational policies to customers: Make sure your website provides guidance to customers in the form of your privacy policy, information security, shipping & billing policies, and refund policies. This is also helpful to avoid dissatisfaction and disputes.
3. Ensure Payment Card Industry (PCI) compliance: All e-commerce organizations are required to be PCI-compliant and must adhere to the rules outlined by the Payment Card Industry Security Standards Council. If your organization is not PCI-compliant, it may be exposed to severe fines and the loss of its payment ability.
4. Protect your e-commerce business from intrusion: Check the system for viruses and hackers, change passwords, make software updates, and check sensitive data on a regular basis to make the system secure for e-commerce transactions.
5. Know the details of your payment service provider contract: Be familiar with your contract, particularly the areas that refer to holding funds and chargeback liability. Know the length of time and conditions under which your deposits may be held, and know your liability for fraudulent transactions.
6. Make strict laws: Classify e-commerce fraud as a type of crime in which perpetrators interfere with e-commerce for the purpose of ill-gotten gains.
7. Privacy-enhancing technologies: Although there are many technologies used for surveillance, the technologies for forming agreements (contracting) about the release of private data, the technologies for labelling and trust, and privacy-enhancing technologies (PETs) should be much stronger.

**CONCLUSION**

In the last few years, many researchers have offered solutions to the security and privacy issues that are the loopholes in e-commerce transactions. E-commerce includes the transmission and exchange of information, products, and services—online transactions and payment, and also resource-sharing between enterprises.

In the effort to make electronic business secure, there are many problems to be solved beyond privacy and security. Beyond buyers and sellers, financial institutions, government agencies, certification bodies, distribution centers, and other organizations must contribute solutions.

However, organizational policies and electronic signature technology may play as important a role in security and privacy as any other solution. Careful analysis will ultimately bring greater transparency and proficiency to the online process so that users can overcome risk and e-commerce can go on unhindered. This paper has proposed a set of guidelines for the benefit of users, so that those users can use online transactions in a safe and secure manner.

**References:**

https://www.sciencedirect.com/science/article/pii/S0378720603000995