E-COMMERCE SECURITY: SECURING AGAINST CYBER THREATS

(Ms. Neha Arora GCW, Karnal, hardik.neha22@gmail.com)
(Ms Preeti GCW, Karnal ,prtkathuria89@gmail.com)

Abstract
Cyber security is a necessary consideration for information technology as well as Internet services. We need to recognize the importance of different types of risks that exist in the online world Enhancing cyber security and protecting critical information are essential to nation's security and economic being. Whenever we think about the cyber security we think - taking many measures to prevent the cyber-crime. This paper mainly focuses on trends, challenges and cyber ethics in the field of cyber security. Cyber incidents emphasize the importance of staying up-to-date on global cybercrime trends, especially concerning the use of mobile and personal computing devices.

Cyber Security
Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.
Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.
Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

What is E-Commerce Security?
E-Commerce security refers to the principles which guide safe electronic transactions, allowing the buying and selling of goods and services through the Internet, but with protocols in place to provide safety for those involved. Successful business online depends on the customers trust that a company has E-Commerce security basics in place.

Privacy
One of the most obvious E-Commerce security basics is privacy, which in this situation means not sharing information with unauthorized parties. When you shop online, your personal details or account information should not be accessible to anyone except the seller you have chosen to share it with. Any disclosure of that information by the merchant would be a breach of confidentiality. The business is responsible to provide at least the minimum in encryption, virus protection, and a firewall so that bank details and credit card information remain private.

Integrity
A second concept which is crucial within secure E-Commerce is the idea of integrity—that none of the information shared online by the customer will be altered in any way. This principle states that a secure transaction includes unchanged data—that the business is only using exactly what was entered into the Internet site by the buyer. Any tampering with information is breaking the confidence of the buyer in the security of the transaction and the integrity of the company in general.

Authentication
For E-Commerce to take place, both seller and buyer have to be who they say they are. A business cannot sell unless it's real, the products are real, and the sale will go through as described online. The buyer must also provide proof of identification so that the merchant can feel secure about the sale. In E-Commerce, fraudulent identification and authentication are possible, and many businesses hire an expert to make sure these kinds of E-Commerce security basics are in place. Common solutions include technological solutions—customer logins and passwords or additional credit card PINs.

ISBN 978-93-82529-14-9

Non-repudiation

Repudiation is denial, and good business depends on both buyers and sellers following through on the part of the transaction which originated with them—not denying those actions. Since E-Commerce happens in cyberspace, usually without any live video, it can feel less safe and sure. The legal principle of non-repudiation adds another level of security by confirming that the information which was sent between parties was indeed received and that a purchase or email or signature cannot be denied by the person who completed the transaction.

Customers who don't feel transactions are secure won't buy. Hesitation on the part of the buyer will destroy E-Commerce potential. Any breach will cost a business in lost revenues and consumer trust. These E-Commerce security basics can guide any business owner regarding safe online transaction proto

Why is cyber security important?

In today's connected world, everyone benefits from advanced cyber defense programs. At an individual level, a cyber security attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Everyone also benefits from the work of cyber threat researchers, like the team of 250 threat researchers at Talos , who investigate new and emerging threats and cyber attack strategies. They reveal new vulnerabilities, educate the public on the importance of cyber security, and strengthen open source tools. Their work makes the Internet safer for everyone.

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism.

Threats in cyber security:-

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. **Elements of cyber** encompass all of the following:

- Network security
- Application security
- Endpoint security
- Data security
- Identity management
- Database and infrastructure security
- Cloud security
- Mobile security
- Disaster recovery/business continuity planning
- End-user education

Types of Cyber security threats

Ransomware
Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.

Malware
Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.

Social engineering
Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.

Phishing
Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyber attack. You can help protect yourself through education or a technology solution that filters malicious emails.

FEATURED SERVICES

- **Managed Firewall** - provides multiple layers of security from entry level border protection to advanced deep packet inspection intrusion detection with URL and web filtering.
- **DDoS Monitoring & Mitigation** - offers organizations 24×7 proactive monitoring of their network infrastructure and a unique DDoS Mitigation plan based on baseline traffic pattern analysis.
- **Vulnerability Assessments** - scan of internal and external networks for known vulnerabilities and provide step-by-step remediation instructions.
- **Web Application Security** - provides critical web protection and cost-effective management as well as state-of-the-art firewall protection and blocking capabilities.
- **Real-time Log Flow Analysis** - boosts real-time security monitoring and alert users of critical security issues in advance of or during a breach.
- **Event Log Management -** collects Windows event log, syslog and flat file logs, running multiple searches for forensic analysis and storing logs securely in redundant off-site data centers

THE BENEFITS

- **Block Unwanted Traffic**
  Help free up bandwidth for legitimate business traffic
- **Reduce Costs**
  Eliminate the need to buy and manage premises-based security devices and appliances
- **Buy What You Need**
  Pay-as-You_Go services let you scale the solution easily as your organization grows
- **24/7 Monitoring and Management**
  By experienced, certified Cyber security professionals
- **Always On**
  Proactive security keeps you ahead of threats and changing conditions to stay in control
- **Manage Risk**
  An essential risk mitigation step for life in the online world

Conclusion
The future of cyber security will in one sense be like the present: hard to define and potentially unbounded as digital technologies interact with human beings across virtually all aspects of politics, society, the economy, and beyond. We built this project on the proposition that both the "cyber" and the "security" components of the concept "cyber security" will be in rapid motion during the back half of the 2010s. That motion is more likely to accelerate than to decelerate, but its direction varies widely among our scenarios. That is no artifact of our research process; it is the

central point of the work. We hypothesize that, at some point in the not-so-distant future (if it is not already true at present), cyber security will be recognized widely as the "master problem" of the internet era. That puts it at the top of any list of problems that societies face, more similar to a nearly existential challenge like climate change than to an operational concern that technology companies have to manage. That recognition also will bring major changes to how human beings and digital machines interact

References

1) **https://cltc.berkeley.edu/scenario-back-matter**
2) **https://www.wikipedia.org/**
3) **https://digitalguardian.com/blog/what-cyber-security**
4) **https://www.incapsula.com/web-application-security/social-engineering-attack.html**