



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CE-37 Cyber security Challenges in the Digital Commerce Ecosystem

Ms. Rajashri S. Shekokare¹, Mrs. Shital Y. Borole², Mr. Pravin G. Bhangale³,
Mrs Kajal P. Visrani⁴

¹²³⁴Assistant Professor, ,KCE'S COEM ,Jalgaon , India , 425001

shekokareraajashri@gmail.com, sejal.borole@gmail.com , pravinbgangale55@gmail.com, kajalvisrani@gmail.com

Abstract –Now a day, World Wide Web has become a popular medium to search information, business, trading and so on. Various organizations and companies are also employing the web in order to introduce their products or services around the world. Therefore E-commerce or electronic commerce is formed. E-commerce is any type of business or commercial transaction that involves the transfer of information across the internet. In this situation a huge amount of information is generated and stored in the web services. This information overhead leads to difficulty in finding relevant and useful knowledge, therefore web mining is used as a tool to discover and extract the knowledge from the web. Besides, the security issues are the most precious problems in every electronic commercial process. This massive increase in the uptake of e-commerce has led to a new generation of associated security threats. In this paper we use techniques for security purposes, in detecting, preventing and predicting cyber-attacks on virtual space

Keywords: Ecommerce, Cybercrime, threats, security ,attacks.

INTRODUCTION

E-commerce (Electronic Commerce) Refers to Companies and Individuals Which Buy and Sell Goods and Services or Transmitting Funds and data primarily over Internet or on any electronic Network , E-Commerce Conducted Over Computers, Tablets , Smartphone's and Other Smart Devices.

Providing Goods and Services Is Not Easy. It Requires a lot of Research work about Product And Service you Wish to sell E-commerce also Called as Online-Commerce.

It is a transaction between buyers and sellers That leverages Technology. The Term E-Commerce and E-business use Interchangeably . E-commerce Platform like Amazon and E-bay Contributed Substantial growth in Online Retail.

E-Commerce Provides huge business opportunities From Small Scale Industry to Large Scale Industries .Many Organizations want to want to host their business on web to reach new market as they could not reach with its Sales Force Or Advertising Campaigns. There is an Internet Security Threat Cyber Crimes Enable E-Commerce Transaction Which face Significant financial and Information Loss.

software for customers and deploy it over the Web. In the software on demand model, the provider provide customers network-based approach to a single copy of an application created specifically for SaaS distribution.

E-Commerce Suffer From Cyber-Security treat called as Cyber-Crime .Cyber-Crime becomes Rapidly Growing underground business built by savvy criminals who can buy and sell valuable financial Information from Unsuspecting users. Cyber Attacks mostly comes from phishing , malware, malicious Software Which Handle Control of your Computer .

Some Business may try to avoid e-commerce due to challenges like :

Limited Face to Face Iteration

Technical difficulties

Data Security Concern

Challenges of Shipping and Fulfilling Orders.

Basically we are focusing on Data Security Concerns

Customers Concern about how Information Stored and Shared By Providing details on Privacy Policy Built Trust for Customers . To demonstrate Transparency and resources Customers Which Safeguards Personally Identifiable Information .

Amazon Has Worked to Create a Secure Shopping Experience and Business which sell on Amazon gives Benefits from long-standing Customer Trust.

E-Commerce Vs. E-business

E-Commerce and E-Business used Interchangeably

E-Commerce Refers To Conducting Online Transactions, While E-business Encompasses all Business activity and Services Conducted Using Web.

There are Six Types of E-Commerce.

- 1.B2B – Business To Business
- 2.B2C – Business To Consumer
- 3.C2C – Consumer To Consumer
- 4.C2B – Consumer To Business
- 5.B2A – Business To Administration
- 6.C2A – Consumer To Administration

eCommerce business models

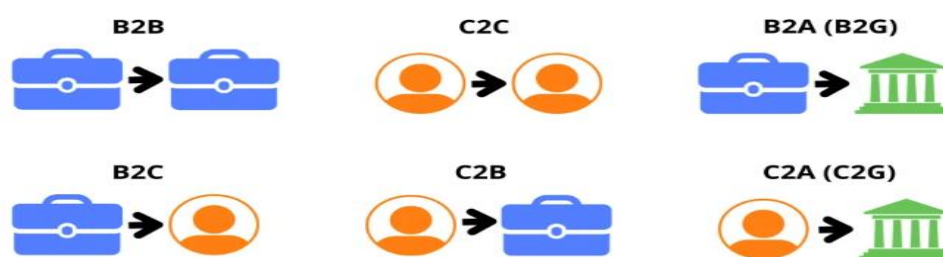


Fig 1: E-Commerce Business Model

Here are Several Popular Business Models Depending on Goods and Services Of an E-Commerce Company

1. Business to Consumer (B2C)

This Type of Business model may be use to sell product or services .

B2C E-Commerce Companies Sell Directly to Product End User . Instead of Distributing To Intermediary.

2. Business To Business (B2B)

An E-Commerce Business Can Directly sell Goods to a user may be another Company

3. Business to Government (B2B):

B2G E-Commerce Companies must Often Meet Government Request for Personal Requirement Some Entities Specialize as Government Contractor Providing Goods Or Services to Agencies or Administrators.

4. Consumer To Consumer (C2C):

E-Commerce Platform Such as Digital Marketplace Connect Consumers with Other Consumers Who Can List Their Own Product And Execute Their Own Sales.

5.Consumer-To-Buisness(C2B)

Consumer use Modern Platform to Easily Engage with Companies And Offer Their Services Especially Related to Short term Contract, Gigs, Freelance Opportunity Example : Listening On Up work

6. Consumer-To-Government(C2G):

Consumers Can Interact With Administration

Literature review

The development and convergence of technology gave rise to the rapidly expanding field of e-commerce.

and the internet, where people engage in a variety of business-related activities. E-commerce, to put it another way, is the selling and purchasing of goods using the internet. In return for finishing the business activity, there is an online money transfer. E-commerce develops and executes various activities and transactions between groups or organizations or between a business and a client. A survey estimates that there are between 12 million and 24 million e-commerce websites worldwide.

In e-commerce, the internet is used to facilitate the purchasing and selling business process. Data interchange, money transfers, and product selection are some of the major e-commerce activities.

Online marketing, online management platforms, and automated data collection systems are additional activities.

In order to give suppliers and customers better services, the companies modernized their networks, operations, etc. as a result of their rapid expansion. E-commerce technology allowed businesses to achieve previously unachievable objectives by giving them numerous chances to locate and seize new markets and draw clients from across borders. Despite the fact that e-commerce offers both consumers and businesses several benefits, it is not feasible without a competent security strategy. E-commerce functions in four primary market segments. Business to Business, which deals with product sales between companies; Business to Consumer,

which deals with sales between companies and customers; Consumer to Consumer, which permits sales between individuals; and Consumer to Business, which deals with sales between individuals and organizations. It's crucial to remember that e-commerce sales were 4.28 trillion USD in 2020 and are predicted to grow to 5.4 trillion USD. In the United States, e-commerce accounted for just 469.2 billion USD in 2021.

History Of E-Commerce

E-Commerce Began in the 1960's When Business Started Using EDI(Electronic Data Exchange) Is the Electronic Interchange of Business Information Using Standardized Format a Process Which allows one Company To Send Information To Another Company Electronically Rather than with Paper.

Applications Of E-Commerce

E-retailing done through use of Tools Such as Virtual Shopping Carts And E-catalogs , Banks and stock Exchanges make extensive use of E-Commerce in Their Operations . Applying E-Commerce to trade elevate it to a Higher Level Allow Individuals To Participate Without Regard For Geographical Borders Development And Commercialization Strategies Like Pricing , Product Characterization And Customer Relationship Can Boosted by Using E-Commerce.

Cyber Attacks and Security For E-Commerce

Since Birth Of Internet And Rise Of Online Technology Cyber Attacks Are Common. Cybercrime is on the Rise too, over 2.3million Cyber-attacks were reported in UK in 2023.

Over 2.3 million Cyber-attacks Were Reported in UK In 2023.

Cyber Attacks are Common like Malware, Phishing, Ransom ware, From Small Scale to Large Scale can Have Significant Impact on Individuals Business And Government.

There Are Many Types Of Cyber Attacks, Some Kinds Of Cyber Attacks listed Below:

1. Phishing : Phishing is a type of Social Engineering Attack Which were attempts to steal sensitive Information like Passwords, Credit Card Numbers , phishing attacks are Carried out through Mail , Phone Calls, Text Messages .
2. Malware: Malware is a Special Type of Malicious Software that can be installed on a Computer System Without Users Knowledge Malware Can Steal Data , Damage File s Or Disrupts System Operations .
3. Zero-Day Attack:
Zero-Day Attacks are attacks that exploits Vulnerability in software that Software Vendors aware about .
4. Distributed Denial Of Service Attacks(DDOS)
DOS attacks are to fool traffic, Making it unavailable to legitimate users.
5. Man In Middle Attacks (MITM)
Man In Middle Attack Occur when attack Intercepts Communication Between Two Parties allow them to Modify Data being Exchange or Eavesdrop On Conversation.

BIGGEST CYBER ATTACKS IN HISTORY

1.Merriot Hotel Data Breach

1. The Marriott Hotel Group revealed in 2018

That it had been hit by massive database Breach Revealing Personally Identifiable Information around 500 Million Guests.

2. Want to Cry Ransom ware

Want to Cry Ransom ware attack It Was a global event took place in 2017. It Was Implemented by Want to Cry Ransom ware Crypto worm This Worm attack various Computers Running the Microsoft Windows Operating System Users Had Their Encrypted And Criminals Ask Bit coin In Payment.

3. Ukraine Power Grid Attack

Major Cyber Event Which Ended up affecting an entire Country, The Ukraine Power Grid Attack took place in 2015. The issue was attributed to an advanced Persistent threat Group Known As “ Sandworm “ And Become the First Publically Acknowledge attack on a Power Grid.

4. MOVEit

In My 2023, Progress Software Disclosed a Zero Day Vulnerability in its MOVE it Transfer Software That allows attacker to gain access to MOVE it Servers and steal Customer data.

5. The NASA Cyber Attack

Major Cyber Security Event to take place in 1999.the NASA Cyber Attack involved the breach and Subsequent Shutdown of NASA’S Crucial Computers For Around 21 Days around 1.7 Million Pieces Of

Software were also Downloaded During Attack Which Cost Space Company Around \$41000 on repairs.

CHOICE OF E-COMMERCE PLATFORM

There are so many Possibilities when it comes to the different e-commerce platform available.

Understanding different business needs and carefully planning how to launch your site are key items to Consider when Choosing E-Commerce Software.

Some Best E-Commerce Platforms Designed for being and selling of online goods and services.

Big E-Commerce Platforms Designed for buying and selling of online goods and services. Big Commerce , Shopify, Adobe Commerce Cloud, Commerce Tools, Magneto, Shoplift, Big Commerce, Woo Commerce, Petra shop. Each Platform has its own native features and extensions. While making final choice check for scalable security Provision .Third Party Security extensions also easily integral with platform. Also not to pick a platform which run on expired or nearly Expired Versions.

Magneto Has Several Versions Starting From 1.x to 2.x.

CHOICE OF HOSTING PROVIDES

It is Best Option to choose host Provider who off
ers all or most of the following.

1. AES ENCRYPTION (ADVANCED ENCRYPTION STANDARD)

It is an algorithm which uses same key to encrypt and Decrypt Protected data.

AES Encryption uses a ‘Symmetric Block Cipher’ or encryption algorithm. Encryption is one of the most basic cyber security strategies available to keep hackers always and make sensitive information safe .Encryption Process turns plain text into Code that can only be understand by Someone with Cipher (Key) to decode code into Plain Text.

2. SWIFT SERVICES

3. NETWORK MONITORING

4. SCHEDULED REGULAR BACKUP PROGRAM

Immediate Disaster Recovery

Round the Clock technical assistance

Stay Safe With PCI (Payment Card Industry) Compliance

As Per number of transactions of your business in year PCI Compliance level may vary. If Online Store has more or Less 20,000 Transactions then it required to conduct an annual Risk Assessment Questionnaire.

TIPS TO KEEP YOUR ACCOUNT SAFE

1. USE A UNIQUE AND STRONG PASSWORD:

You have to set Strong and Unique Password For Your E-Commerce Account .Do not Use Easily Guessable Password Such as “12345” or “ Your Name”. Instead of that use Contribution of numbers, letters and special Characters.

2. AVOID USING PUBLIC WI-FI

Public Wi-Fi networks are less secure than Private Network , Its Good to Avoid Accessing your accessing account.

3. BE CAUTIOUS OF PHISHING ATTACKS

Be Aware of Emails Or messages which are claiming to be from one of the popular E-Commerce site Which ask you to enter Your Login Credentials or other Sensitive data. If You Receive a Suspicious messages do not Click on any Link or enter any Information.

4. USE OF SECURE DEVICE

Use a Device which is more Secure and up to date with latest Security patches and Antivirus Software . Which help you to protect against malware and other cyber threats.

5. ENABLE TWO FACTOR AUTHENTICATION

Two Factor Authentication add an extra Layer of Security to your account by Entering Code Sent to your Phone or Email in addition to your password. This will help you to prevent Unauthorized access to your account if Someone Else Has Your Password.[WWW.Quora.Com].

Above screenshot are for showing two way authentication.

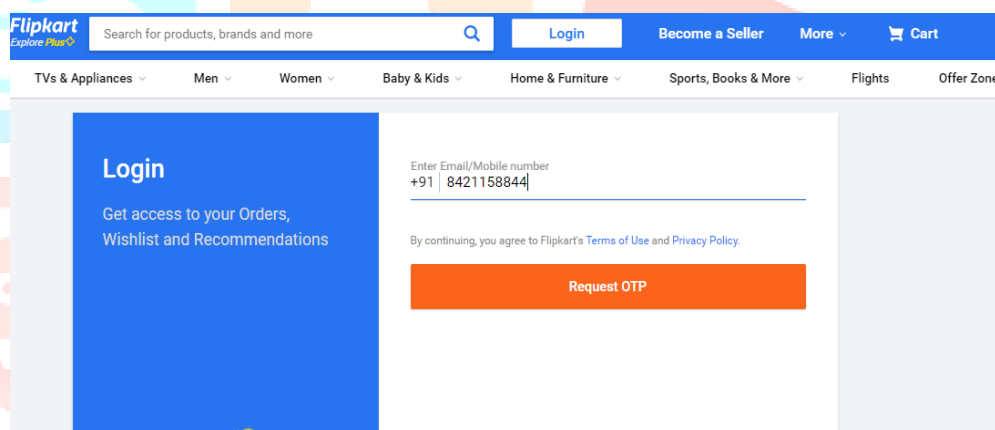


Fig 2: Screenshot Showing Login to the Ecommerce Platform For Example Flip kart

This could simply be a username and password or it includes some other form of authentication like a One-Time Password (OTP). In above screenshot authenticated user tried to log in to ecommerce platform such as Flip kart but to verify authenticity of user. he has to enter his contact number or email address here .

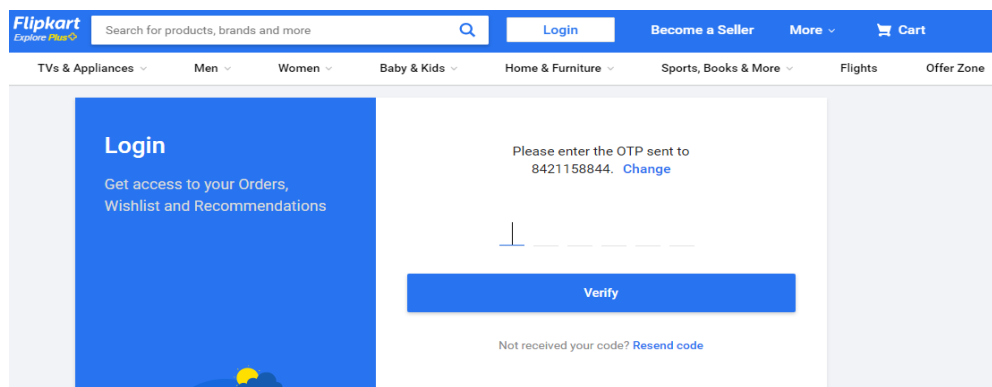


Fig 3: Screenshot Showing Login To The Ecommerce Platform For Example Flipkart

user has entered his mobile number , after providing mobile number he get One Time Password(OTP) on his mobile number In this way authorization has proved

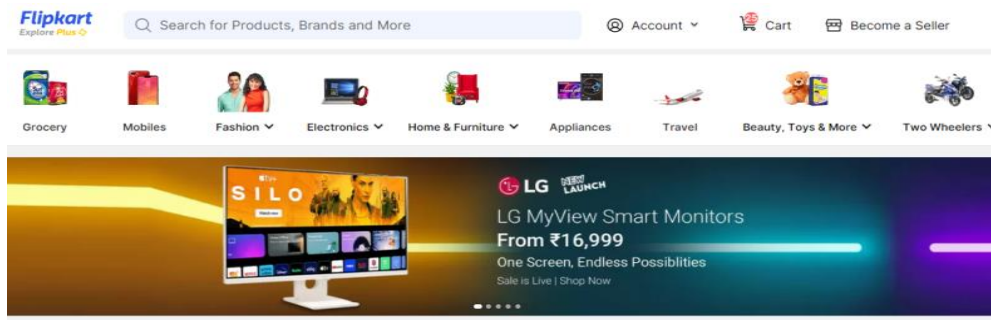


Fig 4: Screenshot Showing Login To The Ecommerce Platform For Example Flip kart With Two Factor Authentication.

After That only authorized user can login to his account.

Providing OTP is part of two-factor authentication only when used along with another factor like a password.

Here's a **real-world example of Two-Factor Authentication (2FA)**:

Example : Logging into your Gmail account

You go to gmail.com and enter your email and password. This is **something you know** (your password). Google sends a **One-Time Password (OTP)** to your registered mobile phone via SMS or through the Google Authenticator app. This is **something you have** (your phone or authenticator app). **Result: Access Granted** Only if **both steps succeed**, you're allowed to log in.

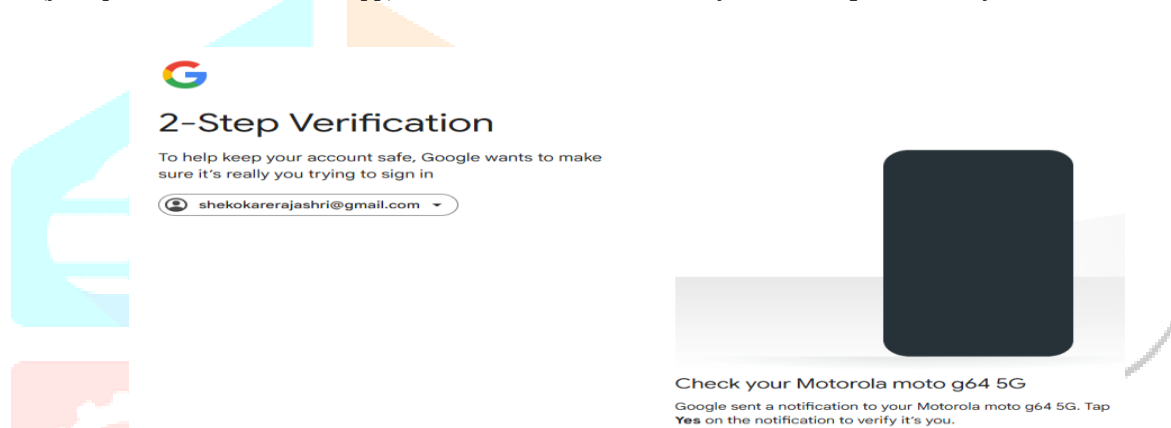


Fig 7: Screenshot Showing Login To Gmail Account With Two Factor Authentication.

WHAT IS SINGLE SIGN-ON?

Single sign-on (SSO) is an authentication method Which enables users to securely authenticate with multiple websites and application by using just one set of credentials.

SSO works Relay upon a trust relationship set up between an application, known as the service provider, and an identity provider, like One Login.

In SSO, this identity data takes the form of tokens which contain identifying bits of information about the user like a user's Username or email address. If the user hasn't logged in, they will be allowed to do so by providing the credentials required by the Identity Provider. This could simply be a username and password or it includes some other form of authentication like a [One-Time Password \(OTP\)](#).

V. RESULT & DISCUSSION

Concerns over the possibility of cyber attacks up setting international relations and national security have been raised by the growing usage of technology and digital infrastructure in vital industries including defense, energy, and banking.

As commerce becomes more digitally connected, cyber security becomes essential to e-commerce's functionality and confidence. Traditional defense strategies aren't working well against sophisticated, contemporary cyber threats.

They tackle both current and new cyber threats by providing scalable, intelligent, and adaptable defenses. These technologies have the potential to serve as the cornerstone of safe online commerce in the years to come with sustained development, moral application, and cooperative industry activities.

VI. CONCLUSION

E-commerce develops and executes various activities and transactions between groups or organizations or between a business and a client. A survey estimates that there are between 12 million and 24 million e-commerce websites worldwide.

REFERENCES

1. Lech J. Janczewski, Andrew Colarik, *Managerial Guide For Handling Cyber-terrorism and Information Warfare*, IGI publishing, Hershey, PA, 2005.
2. http://en.wikipedia.org/wiki/E-mail_bomb. http://legal.practitioner.com/computer-crime/computercrime_3_2_7.html.
- Borenstein, J.; Everett, H.R. & Feng, L. (1996). *Navigating Mobile Robots: Sensors and Omni directional Mobile Robot – Design and Implementation* Ioan Doroftei, Victor Grosu and Veaceslav Spinu “Gh. Asachi” Technical University of Iasi Romania Techniques. A K Peters, Ltd, MA, USA.
3. Dr. Subhash Chandra Gupta, ‘Information technology Act, and its Drawbacks’, *National Conference on Cyber laws & legal Education*, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad (2000).
4. Dr. Farooq Ahmed, ‘Cyber Law in India (laws on Internet)’, *Pioneer Books, Delhi* U.S. App (1992). Dupont, B. (2012). *The cyber security environment to 2022: Trends, drivers and implications*. Available online at: <https://ssrn.com/abstract=2208548> (accessed February 20, 2022).
5. Dykstra, J. (2017). *Cyber issues related to social and behavioral sciences for national security*. National Security Agency. White Paper. Available online at: https://sites.nationalacademies.org/cs/groups/dbasse/site/documents/webpage/dbasse_177250.pdf (accessed January 2, 2022).
6. Ahmadian, S. (2021). Review of e-commerce service delivery models. *Arman Process J.* 2, 14–20.
7. Dahiya, A., and Gupta, B. B. (2020). An economic incentive-based risk transfer approach for defending against DDoS attacks. *Intl. J. E-Serv. Mob. Appl.* 12, 60–84. doi: 10.4018/IJESMA.2020070104
8. Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76, 101795. <https://doi.org/10.1016/j.irfa.2021.101795>
9. Li, K., Kim, D. J., Lang, K. R., Kauffman, R. J., & Naldi, M. (2020). How should we understand the digital economy in Asia? Critical assessment and research agenda. *Electronic commerce research and applications*, 44, 101004. <https://doi.org/10.1016/j.elerap.2020.101004>
10. Lis, P., & Mendel, J. (2019). Cyber-attacks on critical infrastructure: An economic perspective. *Economics and Business Review*, 5(2), 24–47. <https://doi.org/10.18559/eb.2019.2.2>
11. Litvinenko, V. S. (2020). DE as a factor in the technological development of the mineral sector. *Natural Resources Research*, 29(3), 1521–1541. <https://doi.org/10.1007/s11053-019-09568-4>

