

The Role of Cyber Security in Protecting E-Commerce from Cybercrimes

Ismahan Saadi
Strategic Studies and Political
Research , University of Tlemcen Abu
Bekr Belkaid (Algeria)

Receipt Date: 04/ 11/ 2024

Review period: 08/ 11/ 2024

Publication Date; 30/ 12/ 2024

Abstract:

The rapid growth of e-commerce has exposed it to a wide range of cybercrimes such as: phishing, malware, ransom ware, identity theft, and online fraud. This study highlights the crucial role of cyber security in protecting e-commerce by using tools like encryption, two-factor authentication, firewalls, and intrusion detection systems to safeguard sensitive data and ensure user trust. Effective cyber security measures are essential for protecting financial transactions and maintaining the privacy and security of customer information. However, challenges persist due to the rapid evolution of cyber threats, limited awareness of security risks, and gaps in legal frameworks. By examining international regulations, such as the General Data Protection Regulation (GDPR), this study emphasizes the need for stronger security practices and international cooperation. It concludes with recommendations for investing in advanced cyber security solutions and developing legal standards to ensure a secure e-commerce environment.

Keywords: Cyber security, E-commerce, Cybercrimes, Data Encryption, Security Awareness

Introduction

In recent decades, the world has witnessed a profound transformation in the way commercial transactions are conducted, largely due to rapid technological advancements. These widespread adoptions of the internet and the increasing reliance on digital technology have led to the flourishing of e-commerce. Its platforms have emerged as prominent channels for buying and selling, used by both businesses and individuals alike. Amidst this significant growth, e-commerce has become not only a dynamic market and a source of vast economic opportunities, but also a battleground for new and unprecedented security challenges.

As the number of users conducting transactions online continues to rise, alongside the growing volume of financial and personal data exchanged, the risks associated with cybercrimes have also escalated. Cybercriminals are increasingly targeting e-commerce platforms to steal sensitive data and commit crimes such as online fraud and identity theft, posing serious threats to users' trust in these systems.

In this context, and amid the rapid expansion of e-commerce, cyber security plays a pivotal role in reinforcing the trust of users and businesses in the digital environment, thereby contributing to the sustainable growth of this vital sector. However, e-commerce continues to face persistent challenges due to the fast-evolving nature of cyber attacks, necessitating ongoing responses from both businesses and governmental institutions alike.

In light of this reality, a crucial issue emerges: **How can cyber security effectively protect e-commerce from the rising tide of cybercrimes? Furthermore, how can available tools and technologies be applied to counter evolving threats and ensure the sustainability and security of this growing sector?**

To address this issue, the study has been divided into three main axes; first, it examines cybercrimes and their impact on e-commerce, analyzing common types such as fraud and identity theft, and how these affect user trust. Second, it discusses the tools and technologies used in cyber security. The third axis includes the challenges faced, such as a lack of awareness and legal gaps, while offering proposed solutions to enhance protection and ensure the security of e-commerce.

1. Common Cybercrimes and Their Impact on E-Commerce

To begin with, it is important to clarify that e-commerce has become an essential part of daily life for both individuals and businesses. It is defined as “commercial transactions conducted over open networks, such as the internet. E-commerce encompasses transactions between businesses (B2B), as well as transactions between businesses and consumers (B2C)” (منظمة التعاون الاقتصادي والتنمية، 2023). This definition reflects the comprehensive nature of e-commerce, as it allows companies to offer their products and services directly to consumers, thereby facilitating the buying and selling process.

The widespread adoptions of the internet and the increased reliance on digital tools have contributed to the enhancement of this type of commerce, making transactions faster, more flexible, and time-efficient. This shift especially enables access to new markets and expands business opportunities in innovative and rapid ways. However, at the same time, this growth has opened the door to new threats in the form of cybercrimes.

Cybercrimes pose a real threat to this vital sector, and they are defined as: “the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.” (Dennis, 2024)

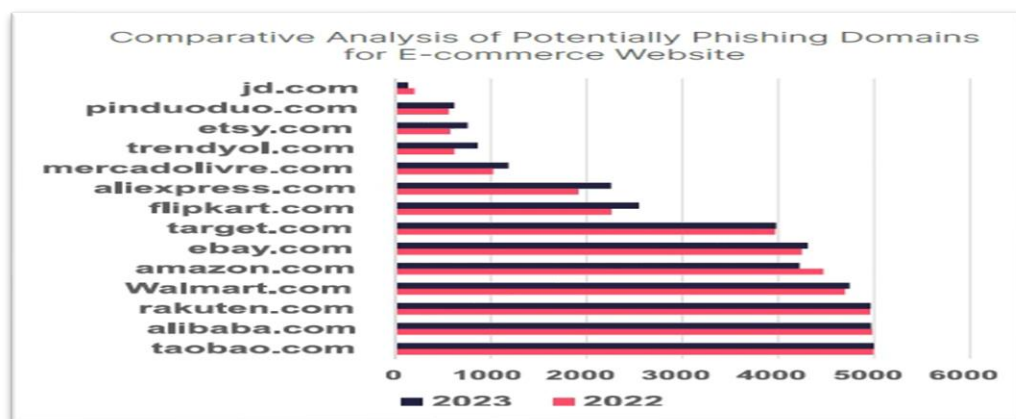
This definition highlights the diversity of cybercrimes, reflecting the significant challenges that societies face in protecting individuals and businesses from these criminal activities. Here, we will review the most prominent common cybercrimes and their negative impact on e-commerce:

1.1 Phishing

It is considered one of the fundamental elements of cyber security threats, aimed at deceiving individuals into revealing sensitive information and data, including personal details, usernames, and passwords. In e-commerce, this often translates to attempts to steal credit card information. It is consistently referred to as one of the most prevalent forms of cyber attacks. (SOCRadar, 2023)

In phishing attacks, attackers impersonate a trusted entity to send messages that appear legitimate, aiming to deceive users into clicking on malicious links or downloading harmful files. These links may prompt users to provide sensitive information, such as account details. In 2020, *Twitter* experienced a massive phishing attack targeting high-profile individuals, including former U.S. President Barack Obama and *Apple* CEO Tim Cook. The attackers used phishing tactics to gain control over verified accounts and access sensitive information. This attack not only compromised the privacy of the individuals involved but also led to significant reputational damage for Twitter and a loss of user trust. (The Verge, 2020)

Figure 01: Comparative analysis of Phishing for E-commerce Web (SOCRadar, 2023)



The graph illustrates a comparison of the number of potential domains associated with phishing attempts targeting e-commerce sites in 2022 and 2023. The data indicates a clear increase in the number of malicious domains in 2023 compared to the previous year, reflecting a rise in security threats to these platforms. Websites such as taobao.com, alibaba.com, and Walmart.com topped the list, indicating that they were primary targets for attackers due to their popularity and large user bases, as well as the financial transactions conducted daily on these platforms. This creates an ideal environment for attackers to exploit the trust users place in these sites.

Additionally, both amazon.com and ebay.com experienced a notable rise in phishing attempts, attributed to their expanding user bases and financial transactions, coupled with the high level of trust users have in these platforms. This combination has made it easier for attackers to deceive users with seemingly legitimate messages, contributing to the increase in targeting.

Phishing attacks vary in terms of techniques and targets. Based on the targets, there are: *spear phishing* conducted through email or electronic communications targets an individual, organization, or specific company. Although cybercriminals often seek to steal data for malicious purposes, they may also attempt to install malware on the victim's computer.

Whale phishing (Whaling): is a term used to describe a phishing attack specifically aimed at gaining access to sensitive and confidential information from influential individuals who are wealthy, powerful, or prominent. In cyber security, whaling is a subset of phishing attack that employs a targeted approach, crafted by cybercriminals to impersonate a specific member of a company or organization. Attackers target these companies to steal confidential information or persuade the victim to send funds or gift cards to the impersonator.)RMG(2023 ‘

As for the method or techniques, SMS phishing (*smishing*) is gaining popularity due to the increased reliance on text messaging. Meanwhile, voice phishing (*vishing*) occurs through phone calls, where attackers use recorded messages or conversations to persuade victims to disclose their personal data. (Interpol, 2023)

Given the significant impact that phishing attacks have on individuals and the theft of their financial data, this has directly affected the e-commerce sector. The sector now faces numerous challenges from various aspects, including the loss of consumer trust, financial damages, and increased costs associated with strengthening cyber security measures to protect platforms and users from these constantly evolving threats. Phishing attacks result in significant financial losses for both companies and individuals, as attackers steal bank account details and sensitive information, leading to financial theft and fraud. For example, the Federal Bureau of Investigation (FBI) reported that phishing-related scams caused losses amounting to approximately 3.5 billion Dollars in 2019 alone. Moreover, these attacks contribute to a decline in consumer trust in e-commerce platforms, with individuals becoming more cautious about sharing their personal or financial information online. Businesses are also compelled to invest substantial resources in enhancing their security and cyber security systems, which increases operational costs. Lastly, companies may face legal penalties if they fail to adequately protect customer data, further exacerbating the consequences of these attacks. (SOCRadar, 2023)

1.2 Malware (malicious software)

It refers to any software that can infect computers and cause harm, often used by cybercriminals to target specific websites with the goal of obtaining personal data, such as passwords, account details, stealing money, or blocking the system owner from using it. Malware attacks are carried out in a deceptive manner, misleading users and redirecting them to harmful websites or pages .In a report published by CyberArk (2022), approximately 670 million types of malware were recorded in 2017 alone, reflecting the increasing frequency of cyber attacks worldwide. This significant rise indicates an escalating threat to online commercial systems. (CyberArk Glossary) And these are the most common ones:

.Viruses: Infect or modify files, leading to system disruption and data loss. In e-commerce, viruses can result in the shutdown of operations or transactions, causing significant harm to a

company's reputation. For example, in 2014, Sony experienced a cyber attack involving a virus that disrupted its services across several systems (New York Times, 2014)

.Worms: Spread automatically across networks, causing performance slowdowns and service disruptions. In e-commerce, worms can negatively impact user experience, potentially driving customers away from the platforms due to poor functionality and reliability. In 2003, the "Blaster Worm" targeted thousands of online systems by exploiting vulnerability in the "Windows XP" operating system. This worm caused widespread disruptions, shutting down devices and impacting both individuals and major corporations, including tech companies and financial institutions. The financial losses from this attack were significant, with an estimated 2.5 Billion Dollars in damages, according to a study by *Computer Economics* in 2003. This figure includes the direct costs for businesses to repair affected systems and the temporary halting of business operations. (Computer Economics, 2023)

.Trojan Horse: Disguised as legitimate software, it allows other malicious programs to enter the system. This can lead to the compromise of sensitive data and the theft of financial information, heightening security concerns among customers.

.Ransom ware: Encrypts files and demands a ransom for their recovery. This can result in business shutdowns and substantial financial losses, with companies often forced to pay the ransom to regain access to critical data. *WannaCry (2017)* is a prominent example of ransom ware malware that affected hundreds of thousands of systems globally, including businesses in the e-commerce sector. The attack disrupted services worldwide, notably impacting the UK's National Health Service (*NHS*), and highlighting the significant disruption that such attacks can cause to business operations. (BBC News, 2017) . A more recent and notable example of the significant impact of malware, particularly ransom ware, is the attack on *JBS Foods* in May 2021. JBS, one of the world's largest meat suppliers, was forced to shut down its operations in North America and Australia due to a cyber attack attributed to the *REvil ransomware* group. This attack disrupted global meat supplies and caused significant financial losses, with JBS paying an 11 million dollars ransom to regain access to its systems. The incident underscored the vulnerabilities in critical infrastructure and the far-reaching consequences of cyber attacks on essential industries like food production and distribution. The attack on *JBS Food* highlights how ransom ware can affect not only individual companies but also entire industries and global supply chains. The impact on the food sector, in particular, led to concerns about the growing threat to the world's supply of essential goods, with significant economic and operational ramifications. (BBC News, 2021)

.Spyware: Gathers sensitive information without the user's knowledge, posing a threat to customer privacy and data confidentiality. This can lead to identity theft and a loss of trust in e-commerce platforms.

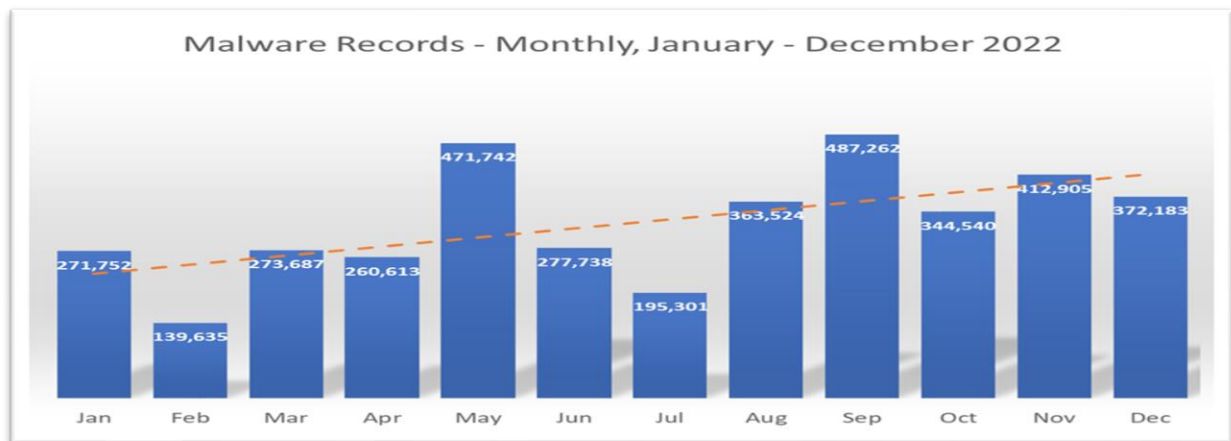
.Adware: Displays unwanted advertisements, negatively affecting user experience. This can drive customers away from e-commerce sites due to the annoyance caused by intrusive ads.

.Malvertising: Involves delivering malicious software through legitimate advertisements, putting users' devices at risk. It can lead to data theft and severely damage the reputation of e-commerce websites.

.Hybrid Malware: Combines features from multiple types of malicious software, making it a complex threat. It affects systems in various ways, increasing the difficulty of detection and mitigation.

All of these threats pose a serious problem for e-commerce, as the number of attacks has been increasing significantly each year. For instance, approximately 670 million types of malware were recorded in 2017. Addressing these threats requires multifaceted defensive strategies, such as antivirus software and firewalls, since each type of malware has unique characteristics that necessitate diverse approaches for detection and mitigation. (Xiang Liu, 2022)

Figure 02: Monthly Malware Records Statistics for 2022 (Cybercrime Information Center, 2023)



The chart illustrates the monthly malware records from January to December 2022, showing a general increase in the number of incidents over the months. Starting in January with around 271,752 records, the figures steadily rose, peaking in May with 471,742 records. Following this peak, there was a noticeable decline in June, with records dropping to 195,301. However, the numbers resumed their upward trend in the subsequent months, continuing to rise toward the end of the year.

September recorded the highest level of activity, with 487,262 malware incidents, indicating a significant surge in malicious activity during that month. The overall upward trend, despite some fluctuations, suggests that cyber threats remain a growing concern. This reinforces the need to strengthen security measures across all sectors, including e-commerce, to protect sensitive data and information effectively.

1.3 Identity Theft and Electronic Fraud

The U.S. Department of Justice provided a specific definition for these terms, describing them as: “terms that encompass all forms of criminal activity in which an

individual unlawfully acquires and utilizes another person's personal information in a manner that involves fraud or deception, typically with the intent of achieving financial gain". (Criminal Division, 2023)

Electronic fraud encompasses any form of illegal deception and exploitation targeting internet users, whether through chat rooms, blogs, e-commerce stores, or mobile applications. Fraudsters aim to infiltrate these platforms to steal users' personal accounts and banking data. Common forms of fraud include the use of stolen or counterfeit credit cards, identity theft, and fraudulent advertisements. These activities negatively impact user experience and e-commerce profits. Fraud is not limited to data thieves but also includes customers committing what is known as friendly fraud, where a customer deliberately retrieves their payment after receiving the product without paying for it. Financial fraud remains one of the most prominent types in e-commerce, where fraudsters exploit fake websites and insecure transactions to steal bank accounts and funds. To safeguard electronic transactions, e-commerce stores rely on encrypted payment gateways and fraud detection systems (عبد، 2021)

Identity Theft is one of the most prevalent forms of fraud in e-commerce, where fraudsters steal shoppers' personal data and use it for unauthorized purchases. According to a study conducted by World pay involving 274 merchants across various industries in six countries, identity theft is the leading source of concern among merchants at 71%, followed by phishing at 66% and account theft at 63%. (Hayes, 2020)

Fraudsters in this type of fraud exploit vulnerabilities in the security systems of certain e-commerce stores, benefiting from existing identities rather than inventing new ones, as this is easier and faster to execute. This type of fraud complicates the process of tracking down the culprits or recovering funds or goods, resulting in significant damage to both customers and store owners.

To protect e-commerce from these attacks, cyber security systems play a crucial role by providing a secure and continually updated infrastructure. For example, platforms like Expand Cart offer online stores that rely on cloud servers secured with SSL certificates, ensuring the encryption and protection of customer data and transactions from illicit attacks. Thus, enhancing cyber security is an essential necessity to safeguard both users and e-commerce stores from the financial and reputational risks associated with fraud and identity theft.

2. Cyber security Tools and Techniques for Protecting E-commerce

E-commerce is one of the most vulnerable sectors to cyber threats, necessitating the implementation of advanced strategies to protect and ensure its seamless operation. In this context, safeguarding the digital infrastructure and securing sensitive data are essential for maintaining trust between users and online platforms. These strategies focus on reinforcing security frameworks and ensuring the integrity of transmitted information, thus mitigating risks and addressing the emerging challenges posed by the digital environment

2.1 Firewalls

They are considered one of the fundamental tools in the field of cyber security, playing a vital role in protecting e-commerce from increasing and evolving threats. Firewalls act as a defensive barrier between a company's internal systems and external networks, allowing for the monitoring and examination of data traffic to determine whether it is trustworthy before granting access to servers. (Scarefone, 2009)

This technology helps prevent unauthorized access to sensitive information, such as customer data and payment information, thereby protecting this data from cyber attacks that could lead to financial losses or damage to the companies' reputations. Additionally, firewalls play a crucial role in countering various attacks, such as Distributed Denial of Service (DDoS) attacks aimed at disrupting electronic services and malware attacks that exploit vulnerabilities in e-commerce systems. (Scarefone, 2009)

Moreover, firewalls are part of a broader protection strategy that includes multiple tools and techniques, such as intrusion detection systems and data encryption. Firewalls also enhance compliance with global cyber security standards, such as PCI-DSS standards for payment data protection, ensuring that e-commerce platforms adhere to best security practices. (بلال، 2022) Furthermore, firewalls contribute to improving system performance by reducing unwanted activities and regulating internet traffic, which helps decrease server load and increase transaction processing speed. Although investing in advanced firewalls may seem costly, their benefits outweigh the expenses, as they reduce the likelihood of successful breaches and attacks, thereby lowering costs associated with responding to and recovering from security incidents. (Stallings, 2018)

There are several types of Firewalls such as:)RMG(2024 ،

-Proxy Firewall: The Proxy Firewall acts as a gateway between networks for a specific application. Proxy servers provide additional functions, such as content caching and enhanced security by preventing direct external connections to the internal network. However, this type of firewall can impact performance and the applications it supports, and is considered an older type of firewall.

-Stateful Inspection Firewall: This type of firewall allows or blocks data traffic based on specific factors such as the state, transport, and protocol. It monitors all activities from the initiation of a connection to its termination and makes filtering decisions based on rules defined by the administrator, as well as "context." The term "context" refers to the use of information from previous connections and packets that belong to the same connection.

-Unified Threat Management (UTM) Firewall: UTM, or Unified Threat Management, combines the functions of a stateful inspection firewall with antivirus programs. It may also include additional services, such as cloud service management.

-Next-generation Firewall (NGFW): These advanced firewalls go beyond simple packet filtering or state inspection. Most organisations use NGFWs to block modern threats such as advanced malware and application-layer attacks.

Firewalls are an integral part of cyber security infrastructure, directly contributing to the protection of e-commerce from increasing threats and ensuring a secure digital environment that allows users to trust in completing their online transactions.

2.2 Data Encryption

It is an essential component of cyber security, particularly within the realm of e-commerce. It serves as the second line of defence after firewalls and antivirus software, playing a crucial role in protecting sensitive information. If cyber attacks manage to breach these defences, encryption can effectively safeguard the data. It involves transforming data from its readable format into encoded text that can only be understood with a decryption key. (Kaspersky, 2020)

In the context of e-commerce, encryption is necessary for several reasons. First, the continuous evolution of cyber attackers' techniques poses a significant threat to online businesses, as they seek to exploit vulnerabilities in systems to access sensitive information. Therefore, encryption is a means of protecting data even in the event of a breach. Second, the likelihood of data theft increases during online transactions, making encryption an effective tool to prevent unauthorized access and illegal exploitation of sensitive information, such as credit card details and personal identification. (Electric, 2023)

Moreover, the prevalence of unreliable software on the internet can lead to the infiltration of malware that jeopardizes data security. Here, encryption plays a critical role in safeguarding information, ensuring that even if malicious software manages to penetrate the system, the data remains unreadable to unauthorized users. Additionally, encryption is vital for protecting intellectual property, business plans, and patents from theft that may be orchestrated by competitors.

Furthermore, certain regulations require organizations to implement stringent data protection measures. Encryption serves as a means to ensure compliance with these requirements, helping to avoid legal repercussions. Finally, encryption can protect inactive data from unauthorized access, even from within the organization itself, thereby enhancing the overall security of the data. Encryption is a fundamental method for bolstering cyber security measures in e-commerce, ensuring that businesses can operate securely, maintain customer trust, and comply with legal obligations, thereby contributing to a safe online shopping experience.

2.3 Two-Factor/Multifactor Authentication

Two-factor authentication (2FA) or multifactor authentication (MFA) is an effective method for enhancing cyber security, particularly in the field of e-commerce. These

techniques aim to add an extra layer of security on top of the traditional password-based authentication.

In two-factor authentication, users are required to provide two different forms of identity verification before gaining access to their accounts. This usually involves something the user knows (such as a password) and something the user possesses (such as a code sent via text message or a dedicated app). This process enhances account security, as even if the password is compromised, accessing the account still requires the second form of authentication. (Loshin, 2024)

Multifactor authentication takes this a step further by involving more than two verification factors. These can include something the user knows, something the user possesses, and something inherent to the user (such as a fingerprint or facial recognition). This approach makes it much harder for attackers to access accounts, even if they obtain the password. (Yasar, 2023). These techniques are essential in e-commerce, where platforms handle sensitive information, such as payment details and personal identification data. By implementing two-factor or multifactor authentication, online stores can strengthen data protection, reduce fraud risks, and increase customer trust in online shopping.

Two-factor and multifactor authentication also contribute to compliance with global security standards, such as the PCI-DSS standard, which sets requirements for protecting payment card data. Therefore, adopting these strategies is a crucial step in securing e-commerce platforms and ensuring a safe shopping environment for customers. (PCI Security Standards Council, 2017)

While these are some of the most commonly used tools, there are numerous other technologies available that contribute to a comprehensive defence strategy. Together, these tools help protect e-commerce platforms from cyber threats by preventing unauthorized access, safeguarding user data, and ensuring a secure transaction environment.

3. Challenges and Proposed Solutions

Despite the existence of advanced tools and techniques for protecting e-commerce, challenges persist. The rapid evolution of cybercrimes, changing attack methods, and gaps in legal frameworks all pose significant and varied obstacles to cyber security. Among these challenges are:

3.1 The Rapid Evolution of Cyber security Threats:

There is a direct relationship between threats and cyber security; as cyber threats such as new attacks and advanced hacking techniques increase and evolve, there is an urgent need to continuously develop cyber security tools and techniques to combat them. In other words, as threats become more sophisticated and dangerous, there is a persistent necessity to enhance cyber security measures correspondingly. Each new level of cyber security threats drives continuous evolution and improvement in order to effectively address these challenges.

Simultaneously, there is an adaptive relationship regarding threats; (i, e) every advancement in cyber security is met with corresponding developments in hacking attempts. Attackers will always strive to find new methods for infiltration, fraud, data theft, and targeting businesses and consumers. Consequently, the relationship between threats and cyber security remains one of ebb and flow.

3.2 Weak Awareness of Cyber security Risks:

This poses a significant challenge in protecting e-commerce from cyber attacks, as many users and companies remain unaware of the real risks surrounding online commerce. This lack of awareness leads to neglect in implementing basic security measures, such as using strong passwords or enabling two-factor/multi-factor authentication. Additionally, insufficient awareness and a lack of understanding of threats leave them vulnerable to phishing attacks, as they struggle to identify suspicious messages and links.(2024، الضوي)

Furthermore, companies often lack clear policies for protecting sensitive data, which increases the risk of data breaches. Therefore, it is essential to intensify efforts to raise public awareness through awareness campaigns and training programs. This will contribute to fostering a culture of cyber security and effectively protecting systems and data.

3.3 Insufficient Collaboration and Coordination :

The lack of collaboration and coordination among stakeholders in the field of cyber security presents a significant challenge in protecting e-commerce from cyber attacks. The absence of coordination among governments, companies, and security institutions weakens the response to attacks, as attackers exploit these gaps to navigate through different systems and regulations.

The lack of shared platforms for exchanging information about threats and cyber attacks, along with the absence of coordinated security policy frameworks among nations and corporations, makes it difficult to effectively confront threats. This results in slow response times to attacks, or each entity's response to these threats becomes limited and ineffective, leaving room for attackers to exploit the legal and operational gaps between countries or organizations. (United Nations Office on Drugs and Crime, n.d)

To overcome this challenge, it is essential to strengthen international and regional collaboration among various stakeholders in e-commerce. This includes the exchange of information regarding potential threats, coordination of security policies, and the establishment of shared platforms to develop effective strategies for countering cyber attacks.

3.4 Deficiencies in Legal Framework :

The deficiencies in legal frameworks related to e-commerce in the face of cyber attacks represent a significant challenge amid the rising threat landscape. Security laws vary from one country to another, leading to disparities in standards and leaving gaps that international attackers can exploit. Furthermore, while technology evolves rapidly, legal frameworks lag

behind in keeping pace with new technologies such as artificial intelligence, exacerbating the vulnerability of protection systems. As previously discussed, the lack of international cooperation in law enforcement complicates the pursuit of criminals across borders, particularly in light of certain countries imposing non-deterrent penalties.(2011، عاقل)

Moreover, some legal frameworks focus solely on the protection of personal data while neglecting other areas such as financial transactions or small e-commerce platforms, putting them at risk. There is an urgent need to continuously update laws, making them more flexible, standardizing international regulations, and enhancing cooperation among countries to effectively combat cyber attacks.

Conclusion

In conclusion, cyber security stands as a vital pillar in protecting e-commerce, securing its sustainability, and building the trust of users who rely on these platforms daily. The rapid expansion of digital commerce has brought with it a significant increase in cyber threats, which have evolved in complexity and impact. Consequently, safeguarding e-commerce now requires a multi-dimensional approach, combining advanced technologies with robust legal frameworks. These measures not only enhance protection against immediate cyber threats but also strengthen the resilience of e-commerce platforms against potential future risks.

As e-commerce continues to play a critical role in the global economy, maintaining security is fundamental to preserving its reliability and accessibility. Cyber security measures must evolve to counter increasingly sophisticated cybercrimes, including threats like phishing, identity theft, malware attacks, and electronic fraud. Failure to address these risks could undermine consumer confidence, leading to diminished participation in e-commerce and substantial economic losses for businesses. Additionally, the costs associated with data breaches from financial damages to reputational harm underscore the urgent need for a comprehensive cyber security strategy.

Effective cyber security strategies must be forward-thinking, incorporating cutting-edge technologies such as artificial intelligence and machine learning to proactively detect and respond to threats. Alongside these technological advancements, it is essential to establish robust legal structures that can adapt to the rapidly changing cyber threat landscape. Standardized, enforceable policies across regions will provide a more cohesive approach, creating a secure environment for cross-border transactions and reducing the legal ambiguities that attackers often exploit.

Ultimately, an integrated approach to cyber security not only safeguards e-commerce platforms but also reinforces their indispensable role in today's economy. Ensuring the sustainability, reliability, and security of these platforms benefits businesses and consumers alike, fosters a secure online marketplace that can thrive in the digital era.

Recommendations

-Enhance Cyber security Awareness: Implement widespread awareness campaigns aimed at educating businesses and consumers about cyber security risks and best practices. Training programs should focus on recognizing threats such as phishing and understanding the importance of strong password policies.

-Strengthen Legal Frameworks: Governments must update and harmonize legal frameworks to keep pace with the evolving landscape of cyber threats. This includes enacting comprehensive legislation that addresses various aspects of e-commerce, such as financial transactions and data protection. For instance, the *General Data Protection Regulation (GDPR)* of the European Union serves as a global benchmark, enforcing stringent standards to safeguard user privacy. Furthermore, developing laws to regulate digital transactions, such as electronic signatures and smart contracts, is essential to ensure that online buying and selling processes are reliable and secure. In this regard, the *Uniform Electronic Transactions Act (UETA)* (Reuters) in the United States stands out as a prominent example, offering a legal framework that recognizes electronic signatures and fosters trust in digital transactions.

Addressing cross-border cybercrimes also necessitates international legal alignment. Instruments like the *Budapest Convention on Cybercrime* (Council of Europe) provide a critical framework for enhancing global cooperation in combating such threats. Updating and harmonizing these legal frameworks not only fortifies user security but also boosts corporate confidence in the digital economy.

-Foster International Cooperation: This is necessitates the establishment of platforms that bring together governments, law enforcement agencies, and the private sector to exchange information on cyber threats and vulnerabilities. Such partnerships enhance incident response mechanisms and promote the adoption of best practices. However, the effectiveness of these collaborations faces significant challenges, particularly the intensifying great power rivalries, such as the ongoing tensions between China and the United States, which hinder international coordination. Despite these challenges, there are notable success stories, such as the *Budapest Convention on Cybercrime (2001)* (Council of Europe), which provides a unified legal framework for addressing cyber threats, and organizations like *Interpol*, which facilitate global coordination efforts, exemplified by operations such as *Operation Pangea* (INTERPOL, 2020). Nonetheless, political conflicts, including state-sponsored cyber attacks like those between the United States and Russia or disputes over data governance and cyber espionage between China and the United States, often undermine these efforts.

To address these obstacles, regional initiatives such as the *ASEAN Cyber security Cooperation Framework* (ASEAN) offer a promising alternative. These initiatives demonstrate the potential for effective collaboration that transcends geopolitical tensions, strengthening collective efforts to safeguard nations and individuals against escalating cyber threats.

-Invest in Advanced Technologies: Organizations should invest in cutting-edge cyber security technologies, including artificial intelligence (AI) and machine learning, to enhance

their capabilities in threat detection and response. For instance, Microsoft leveraged AI to identify over 30 billion cyber threats in 2020, highlighting the effectiveness of AI in rapidly and accurately detecting potential security risks. Additionally, the company has developed AI-driven security tools, such as *Microsoft Defender*, which are designed to detect anomalous patterns in digital activity and provide immediate responses to mitigate potential cyber attacks (Microsoft, 2020). Regular updates and improvements to security systems are crucial to keeping pace with the evolving threat landscape, ensuring that organizations can respond swiftly and effectively to emerging threats.

-Develop Incident Response Plans: Organizations should establish and continuously update incident response plans to ensure timely and efficient actions in the event of a cyber attack. For example, in the case of a data breach, such a plan should encompass well-defined procedures for the rapid restoration of compromised data, alongside clear communication protocols with affected parties, including customers and regulatory authorities. A pertinent illustration of this is the 2013 *data breach* at *Target*, wherein the company promptly notified impacted customers, provided credit monitoring services, and coordinated with law enforcement agencies for an investigation. Furthermore, Target undertook significant upgrades to its security infrastructure to fortify defences against future breaches (Target , 2013). This case underscores the critical importance of maintaining a robust and adaptive incident response framework to effectively manage cyber threats.

-Engage Stakeholders: It is essential to engage all relevant stakeholders, including industry leaders, cyber security experts, and policymakers, in the development of comprehensive strategies to combat cyber threats. For instance, within the framework of public-private collaboration, numerous governments and companies have formed partnerships aimed at enhancing cyber security and sharing threat-related information. One such initiative is the "Cyber security Forum," which brings together representatives from both the public and private sectors to exchange best practices and coordinate responses to cyber attacks (Brown, 2024). These types of partnerships are crucial in strengthening the effectiveness of measures taken to secure e-commerce and ensure its sustainability.

-Encourage Research and Development: It is essential to encourage research initiatives that focus on the challenges of cyber security and innovative solutions. For instance, new algorithms have been developed for detecting malware through ongoing research in machine learning, which helps identify threats such as phishing before they cause significant damage. A prominent example of this is the development of advanced machine learning models by companies like Google and Microsoft to detect phishing emails and fraudulent websites. These models are capable of analyzing communication patterns and detecting anomalies indicative of phishing attempts, enabling rapid response to such threats (Microsoft, 2021). Furthermore, cyber security research has contributed to the creation of real-time threat detection systems, such as the Darktrace system (Darktrace, 2021), which employs artificial intelligence to detect emerging cyber threats in real-time and proactively respond. These types of research efforts significantly contribute to identifying emerging threats and developing proactive measures to counteract them.



References

ASEAN. *ASEAN Cyber Security Cooperation: 2021-2025*.

BBC News. (2017, 05 13). *BBC News*. Massive RansomeWare infection hits computers in 99 countries: <https://www.bbc.com/news/technology-39901382> Retrieved 11 10, 2024.

BBC News. (2021). *BBC News*. CYber Attack on JBS: Company pays Ransome after Hackers Disrupt Meat Production: <https://www.bbc.com/news/world-us-canada-57374817> Retrieved 2024.

Computer Economics. (2023). *Computer Economics*. The economic impact of Blaster Worm: <https://www.computereconomics.com/> Retrieved 11 2024,

Council of Europe. (n.d.). *Council of Europe*. Retrieved from The Budapest Convention on Cybercrime: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

Criminal Division. (2023). *Identity Theft*. USA: US Department of Justice.

CyberArk Glossary. (n.d.). *What is a Malware Attack?* cyberark: <http://www.cyberark.com/what-is/malware/> Retrieved oct 20, 2024.

Cybercrime Information Center. (2023). *The Malware Landscape 2023*. Cybercrime Information Center.

Darktrace. (2021). *Darktrace*. Darktrace: AI-Powered Cyber security for the Digital Era: <https://www.darktrace.com> Retrieved 11 7, 2024.

Dennis, M. A. (2024, oct 22). *Cybercrime*. Britannica: <https://www.britannica.com/topic/cybercrime/Hacking> Retrieved oct 27, 2024,

Electric. (2023, march 29). *Why is Encryption Important? Every Reasons It's Necessary.*, Electric.com: <http://www.electric.ai/blog/why-is-encryption-important> Retrieved oct 17, 2024

GDPR. (n.d.). *GDPR.eu*. Retrieved from General Data Protect Regulation : <https://gdpr-info.eu/>

INTERPOL. (2020). *INTERPOL*. Operation Pangea: Interpol's global fight against online pharmaceutical crime: <https://www.interpol.int/en/Crimes/Pharmaceutical-crime/Operation-Pangea>

Kaspersky. (2020). *What is Data Encryption*. Kaspersky.com: <http://www.kaspersky.com/resource-center/definitions/encryption> Retrieved Oct 19, 2024.

Loshin, P. K. (2024, oct). *What is two-factor authentication (2FA)*. techTarget: <https://www.techtarget.com/searchsecurity/definition/two-factor-authentication> Retrieved oct 17, 2024.

Microsoft. (2020). *Microsoft Security Intelligence Report* .

Microsoft. (2021). *Microsoft tech Community* . Advancing Phishing Protection with Machine Learning : <https://techcommunity.microsoft.com> Retrieved 11 10, 2024,

New York Times. (2014, 12 19). *New York Times*. Sony Cyber Attack was Act of Cyberterrorism, U.S Says: <https://www.nytimes.com/2014/12/20/us/sony-hack-fbi.html> Retrieved 10 15, 2023,

PCI Security Standards Council. (2017, jan). Guidance Multifactor-Factor Authentication.

Reuters, T. (n.d.). *Westlaw*. Uniform Electronic Transactions Act (UETA): [https://content.next.westlaw.com/Glossary/PracticalLaw/l66e3df587a6611e498db8b09b4f043e0?transitionType=Default&contextData=\(sc.Default\)](https://content.next.westlaw.com/Glossary/PracticalLaw/l66e3df587a6611e498db8b09b4f043e0?transitionType=Default&contextData=(sc.Default))

RMG: (2023). *ابرز أنواع الهجمات السيبرانية حتى عام 2021*. تاريخ الاسترداد 27 أكتوبر، 2024، RMG /<http://www.rmg-sa.com>

RMG: (2024). *الحماية من الهجمات الالكترونية عبر 6 أدوات للأمن السيبراني*. تاريخ الاسترداد 18 أكتوبر 2024 : -<https://www.rmg-sa.com/6>

Scarefone, P. H. (2009). *Guidelines on Firewalls and Firewalls Policy*. USA: National Institute of Standards and Technology.

SOCRadar. (2023, dec 23). *Phishing in E-commerce: Understanding Digital Threats Effectively*. SOCRadar: <http://socradar.io/phishing-in-e-commerce-understanding-digital-threats-effectively/> Retrieved oct 20, 2024.

Stallings, W. a. (2018). *Computer Security: Principles and Practice (4th ed)*. Pearson.

Target . (2013, Dec 19). *Target Corporation*. Target Confirms Unauthorized Access to Payment Card Data in U.S Stores: <https://corporate.target.com/news-features/article/2013/12/target-confirms-unauthorized-access-to-payment-car#:> Retrieved 11 2024, 5,

The Verge. (2020). *The Verge*. Twitter hack: How hackers took over high-profile accounts to steal bitcoin: <https://www.theverge.com/2020/7/16/21327689/twitter-hack-high-profile-accounts-bitcoin-attack-explained>

United Nations Office on Drugs and Crime. (n.d). *International cooperation on cybersecurity matters*. qatar.

Xiang Liu, S. F. (2022). Cyber security threats: A never-ending challenge for e-commerce. *frontiers in psychology* , 09.

Yasar, K. (2023, oct). *Multifactor authentication*. TechTarget: <https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA> Retrieved oct 2024,

احمد الضوي. (02 09, 2024). *قلة الوعي والهجمات الالكترونية أبرز 5 عيوب للأمن السيبراني*. بوابة الهرم .

جناجرة بلال. (2022). *أمن الشبكات وحمايتها*. فلسطين: قسم تكنولوجيا المعلومات جامعة فلسطين.

فضيلة عاقل. (2011). الاطار القانوني للتجارة الالكترونية وواقع استخدامها في الدول العربية. مجلة الاقتصاد الجديد ، 185.

محمد عبود. (Apr, 2021 26). الاحتيايل في التجارة الالكترونية: الأنواع الشائعة وطرق الحماية والمواجهة. تاريخ الاسترداد 22 oct, 2024
Expand Card : [http:// expandcart.com/ar/56745](http://expandcart.com/ar/56745)

منظمة التعاون الاقتصادي والتنمية. (2023). التجارة الالكترونية. تاريخ الاسترداد 14 اكتوبر, 2024، من الاسكوا:
<https://www.unescwa.org/ar/sd-glossary>