European Economic Letters
ISSN 2323-5233
Vol 14, Issue 4 (2024)
http://eelet.org.uk

The Threat of Cybercrimes to Electronic Consumers and Strategies for their Protection

Fatma Zohra Settou[1*], Azeddine Ghobch[2]
1*University of El Oued, Algeria, settou-fatimazohra@univ-eloued.dz
2University of El Oued, Algeria, ghobch-azeddine@univ-eloued.dz

Received: 04/09/2024 **Accepted**: 05/11/2024 **Published**: 22/11/2024

Abstract:
This study aims to explore methods of protecting electronic consumers from the risks of cybercrimes, which are considered one of the most pressing challenges of the modern era. These crimes employ various malicious techniques, such as fraud, deception, forgery, and more. The study presents several mechanisms and strategies for consumer protection, including administrative, technical, and legal measures. Additionally, it offers recommendations and proposals that could serve as a protective barrier for consumers. These include enhancing oversight of various electronic transactions and agreements to safeguard consumers, enacting laws and regulations governing e-commerce and electronic transactions at the international level, and ensuring the security of commercial transactions and payments to strengthen consumer protection in the digital realm.

Keywords: Electronic Consumer, Cybercrimes, Electronic Transactions, Cyber Fraud.

Introduction:

Amid the significant transformations shaping the modern world, particularly in information and communication technology, advanced technological tools have emerged, dramatically reducing time and distance while reshaping the traditional business landscape. Commercial transactions have transitioned to a virtual realm, where a screen and a single click connect sellers and consumers. Goods and services are now exchanged, and payments processed, via computers, smart devices, and electronic payment systems. These advancements have enabled the development of a new paradigm for electronic transactions, transcending temporal and spatial limitations.

Despite the many advantages of electronic transactions, certain challenges prevent their full adoption as a complete alternative to traditional methods. Chief among these challenges are concerns about the confidentiality and security of information, as well as the privacy of consumer data shared online. Such vulnerabilities expose consumers to risks and cybercrimes, including forgery, fraud, and deception. Consequently, the need to protect electronic consumers has become a critical political, social, and economic priority in recent years. As internet usage continues to expand globally, the concept of electronic consumer protection has garnered increasing attention from scholars and researchers, underscoring the imperative to safeguard consumer rights.

Research Problem:

In light of the aforementioned context, the central question of this study arises:

How can electronic consumers be protected in the face of cybercrimes?

From this main question, the following sub-questions emerge:

- What is meant by cybercrimes, and what does electronic consumer protection entail?
- What justifies the need to protect electronic consumers?
- What are the most effective means to protect electronic consumers from cybercrimes?

Significance of the Study: The significance of this study stems from the critical role of the consumer as the cornerstone of any transaction and as the weaker party in the commercial process, particularly in electronic transactions. This necessitates identifying the key risks consumers may face in the context of cybercrimes and emphasizing the need to provide them with protection. Moreover, the study underscores the importance of establishing a set of rules to ensure the protection of all parties involved in electronic transactions, whether within national borders or internationally.

Objectives of the Study:

This study aims to:

1. Provide a theoretical framework that clarifies the concept of cybercrimes as a contemporary issue in the virtual world, as well as the concept of electronic consumer protection in this context.
2. Identify the key risks electronic consumers face from cybercrimes.
3. Propose the most effective measures to safeguard electronic consumers against cybercrimes.

Methodology:

To address the research problem and comprehensively explore the study's topics, a descriptive and analytical approach was adopted due to its relevance to the subject matter.

Structure of the Study:

To thoroughly examine the study's literature from various perspectives and attempt to answer its research question, the study is divided into the following sections:

1. The Conceptual Framework of Cybercrimes.
2. The General Framework of Electronic Consumers.
3. The Risks Faced by Electronic Consumers in the Context of Cybercrimes and Mechanisms for Their Protection.

First: The Conceptual Framework of Cybercrimes

Cybercrimes pose a significant challenge to the environment in which they are perpetrated. Cybercriminals can operate from anywhere in the world, targeting individuals or businesses across international borders. The challenges associated with these crimes are compounded by their scope and scale, the technical complexity of identifying perpetrators, and the necessity of international cooperation to bring offenders to justice. The internet provides new opportunities for criminals, often operating under the assumption that legal jurisdictions cannot effectively enforce laws in the virtual world.

1. Definition of Cybercrime:

There is no universally accepted definition of cybercrime, nor is there consensus on the types of offenses it encompasses. It is often referred to as the "crime of the era," "electronic crime," or "information systems misuse" (Hilal, 2014, p. 374). Broadly, cybercrime includes a range of behaviors directed against individuals with the intent to harm them using computers and communication networks. Cybercrime encompasses all types of criminal acts where information and communication technologies play a central role.

Etymologically, the term "cybercrime" is derived from the words *crime* and *cyber*, the latter originating from the Greek word *Kubernan*, meaning "governance" or "control." Despite the prevalence of the term, legal experts have not agreed on a unified definition. The European Union's guidelines on the European Arrest Warrant offer some direction, while the United Nations defines cybercrime as:

"All unlawful acts conducted through electronic operations that target the security of information systems and the data processed by them" (Beas, 2016, pp. 25–26).

Other definitions include:

- **"Crimes conducted using a computer or advanced technology against another computer or advanced technology, requiring a network connection between them."** (Bint Attiyah Allah, 2020, p. 8).
- **"Criminal activities where computer technology is used directly or indirectly as a tool or target to execute the intended offense."** (Al-Qar'an, 2017, p. 19).
- The Shanghai Cooperation Organization defines cybercrime as: **"The use of information resources and their manipulation within the information domain for unlawful purposes."** (Aissawi & Shekarda, 2020, p. 76).

Based on the above, cybercrime can be defined as: **"Any intentional act or omission involving the unlawful use of information technology to achieve personal gains, whether by infringing on material, financial, or moral assets, or by violating the privacy of individuals and institutions. Cybercrime also encompasses offenses where information systems are the primary means to commit traditional crimes, such as unauthorized electronic fund transfers or online defamation."** (Kirkouri, 2020, p. 12).

2. Characteristics of Cybercrimes:

Cybercrimes have distinctive features that differentiate them from traditional crimes:

- **Transnational Nature:** Cybercrimes often occur across multiple countries, bypassing geographical boundaries, similar to crimes like money laundering and drug trafficking. In the era of interconnected computers and the internet, perpetrators are often in one country, victims in another, and the impact felt in a third location.
- **Difficulty of Evidence Collection:** Cybercriminals use sophisticated, rapid techniques that may take only seconds to execute. Additionally, evidence can be easily manipulated or erased. In many jurisdictions, courts are reluctant to accept digital evidence, which consists of intangible magnetic fields and electrical impulses that cannot be perceived by human senses.
- **Ease of Commission:** Cybercrimes, often referred to as "soft crimes" or "white-collar crimes," require minimal effort or time when the necessary technology is available.
- **Reluctance of Victims to Report:** Many victims of cybercrime do not report incidents, either because they are unaware of the crime or due to fear of reputational harm. Consequently, most cybercrimes are discovered accidentally, often long after their occurrence. Furthermore, undiscovered crimes far outnumber reported ones, creating a "dark figure" that obscures the true scale of cybercrime (Abdulrahman, 2008, p. 9).

3. Causes of Cybercrime:

The proliferation of cybercrime can be attributed to several factors (Dris, 2017, pp. 31–32):

- **Obsession with Information Gathering:** Some individuals commit cybercrimes to access new or restricted information. Hackers often believe information should be unrestricted and dedicate significant effort to breaching protected systems. They frequently form groups to collaborate, share information, and exchange programs and news.
- **Financial Gains:** The desire for quick wealth motivates some individuals to exploit sensitive information for monetary benefits.
- **Personal Motives:** External influences, coupled with a person's immersion in an automated information-processing environment, can lead to cybercriminal behavior. Such influences might stem from amusement, revenge, or other personal triggers.

4. Objectives of Cybercrime:

The goals of cybercrime include (Gaballah, 2021, p. 653):

- Unlawful access to information, including theft, disruption, or destruction of data via the internet.
- Disabling or damaging servers that store critical information.

- Modifying website addresses to harm public institutions.
- Threatening or blackmailing individuals or entities that use technology.
- Exploiting information technology for financial, moral, or political gains, such as credit card fraud or website hacking.
- Using technology to support terrorism or promote extremist ideologies.

In summary, cybercrime is driven by illegitimate objectives aimed at harming others through threats, blackmail, data theft, or system sabotage to achieve personal gains.

5- Classification of Cybercrimes and Their Perpetrators

1-5 Classification of Cybercrimes:

Legal scholars have not agreed upon a unified criterion for classifying cybercrimes due to their complexity and rapid evolution. These crimes can be categorized based on the means of committing the crime, the criminal's motive, or the target of the crime. Accordingly, cybercrimes can be divided into the following categories (Hafouda & Gardain, 2017, pp. 93-94):

Crimes Against Financial Assets:

With the shift from traditional commercial transactions to electronic transactions and the development of online payment methods, financial exchanges over the internet have become vulnerable to various crimes, including:

- Theft of credit card numbers and unauthorized electronic transfers;
- Online gambling and money laundering;
- Theft and robbery of bank funds;
- Online drug trafficking.

Crimes Against Individuals:

As the internet has developed, personal information about individuals is now widely available, making it vulnerable to misuse by cybercriminals. This has exposed the reputation and honor of individuals to violations, including:

- Threats, harassment, and stalking;
- Identity theft, deception, and enticement;
- The production and dissemination of explicit content;
- Defamation, slander, and reputational damage.

Crimes Against National Security:

Cybercrimes that threaten the security of nations and societies include:

- **Terrorist Organizations:** Extremist groups exploit the communicative nature of the internet to disseminate their beliefs and ideologies, even engaging in practices that threaten the security of targeted states.
- **Organized Crime:** Organized crime syndicates utilize internet and communication technologies to plan, execute, and coordinate their criminal operations with ease and efficiency.
- **Crimes Targeting Intellectual Security:** The internet provides opportunities to influence the beliefs and traditions of entire societies, leading to intellectual defeat and creating chaos.
- **Cyber Espionage:** The internet has greatly facilitated espionage activities, allowing criminals to spy on individuals, states, organizations, or institutions at national or international levels. Cyber espionage primarily targets three areas: military, political, and economic intelligence.

The most significant classification of cybercrimes is provided by the **European Convention on Cybercrime (Budapest Convention, 2001):**

- **Category One:** Crimes targeting the confidentiality, integrity, and availability of data, including unauthorized access, disclosure, reproduction, or destruction of computer data.
- **Category Two:** Crimes involving the use of computers as a means, such as fraud and electronic forgery.

- **Category Three:** Crimes involving content, where computers serve as the medium for illegal activities, such as child exploitation, online gambling, money laundering, and drug trafficking.
- **Category Four:** Crimes related to intellectual property rights, including copyright violations, supplementing national and international intellectual property laws.

2-5 Perpetrators of Cybercrimes:

Perpetrators of internet crimes, often referred to as hackers, can be categorized into three main groups (Sira'a & Deqish, *Economic Dimensions of Electronic Crime*, 2018, p. 38):

Hackers:

Hackers, commonly referred to as pirates, engage in cybercrimes that may be either destructive or recreational out of curiosity. Most hackers are young individuals deeply interested in computers and the internet.

Crackers:

Crackers are professional hackers and among the most dangerous types of cybercriminals. These individuals often possess ordinary social status but have specialized knowledge in electronic sciences, making them highly capable of committing serious crimes.

Malicious Actors:

This group targets organizations, establishments, and employers, often motivated by revenge or the pursuit of financial or political benefits. These individuals may act out of extremism, espionage, or system hacking.

This classification highlights the diversity in the nature and intent of cybercrimes and the backgrounds of their perpetrators, reflecting the multifaceted challenges posed by cybercrime in modern society.

6- Methods of Combating Cybercrime

Effectively combating cyberattacks requires international cooperation and coordination to ensure cybersecurity, detect threats, mitigate potential adverse effects, and respond effectively. Below are some of the measures taken to combat internet and computer crimes (Aissawi & Shekarda, 2020, p. 81):

Media Efforts

The role of traditional media institutions and global electronic interactive platforms lies in their social and ethical responsibility to promote basic knowledge and educational principles for media literacy. This requires tools and capabilities that enable governments and nations to gradually and intensively reduce the negative effects of information and communication technologies. Such efforts must guide high levels of usage on interactive media platforms with awareness and rationality.

Legislative Efforts

Several European countries, including the UK, the Netherlands, France, Denmark, Hungary, Poland, Japan, and Canada, have enacted specific laws addressing internet and computer crimes. Many Western nations have also established specialized units to combat cybercrime and taken a step further by creating centers to support victims of these crimes.

In the Arab world, states signed the **Arab Convention on Combating Information Technology Offenses** on December 21, 2010. This convention led to the development of various laws aimed at combating electronic crimes in countries like Saudi Arabia, Jordan, Qatar, the UAE, Iraq, and Oman. The convention came into effect in 2015 after seven member states ratified it.

Security Measures

Combating the risks of cybercrimes heavily depends on adopting an integrated security-societal strategy. This approach involves official state crime-fighting agencies working alongside community members and private sector institutions to curb criminal activities in cyberspace. Studies conducted in various countries emphasize the importance of engaging multiple sources and private institutions to share responsibility for combating and controlling these crimes. Key contributors include:

- **Internet Service Providers (ISPs):** ISPs can identify the Internet Protocol (IP) addresses of users, enabling the monitoring of risky online activities and restricting access for users involved in such activities.
- **Ordinary Citizens:** Individuals can play a significant role by protecting themselves from cybercrimes through the use of antivirus software.
- **Commercial Banks and Credit Card Companies:** These institutions have significant responsibility in safeguarding their customers by implementing fraud prevention measures, installing monitoring software to track unusual activities on customer accounts, and alerting customers about transactions made on their accounts.
- **Private Investigators:** Working in coordination with criminal justice agencies, private investigators can play a vital role in addressing cybercrimes.

Second: General Framework for Electronic Consumer Protection

The rise of commercial transactions via electronic platforms has increased the risks consumers face due to the advanced technical tools used to lure them into transactions. Consumers often enter into agreements without sufficient knowledge of the product or service, necessitating the provision of mechanisms for their protection.

1. Definition of the Consumer

The consumer is a fundamental element of the marketing process. Market analysis begins and ends with the consumer, aiming to satisfy their needs and preferences. The consumer is the final party in the commercial process, which starts with producers and intermediaries and concludes with the consumer, the central figure in production and marketing activities (Ben Yaqoub, 2004, p. 6).

1.1. Definition of the Electronic Consumer

- The electronic consumer is defined as:
  “A natural or legal person who acquires goods and services of any kind, whether physically or virtually, with or without payment, to meet personal, familial, or public needs unrelated to their profession, via the internet.” (Mohammed, 2013, p. 35).
- Another definition describes the electronic consumer as:
  “Anyone who uses goods or services to meet their needs or those of their dependents without intending to resell, modify, or use them for professional activities, contracting for these goods or services via modern electronic means.” (Tijani & Amamra, 2018, p. 1204).
- A further definition states:
  “An individual who enters into various electronic contracts, such as purchases, rentals, loans, and usufruct agreements, to fulfill their personal or familial needs without intending to resell or market them, and without possessing the technical expertise to process or repair these items.” (Osama, 2005, p. 108).

Thus, the concept of the electronic consumer closely aligns with that of the traditional consumer but involves the use of modern tools for transactions. It represents a contemporary form of contracting, positioned between immediate and remote agreements.

Characteristics of the Electronic Consumer (Ben Dhahbiya et al., 2018, p. 1181):

- Ability to interact with and navigate websites available on the internet.
- Participation in designing goods and services through an organization's website by specifying desired features, enabling businesses to adjust their offerings to meet user needs and preferences.
- Flexibility in adapting to surrounding changes due to advancements in information and communication technology.
- Capacity to compare goods and services and choose the most suitable options.
- Proficiency in internet and IT usage, distinguishing electronic consumers from traditional consumers.

2. Protecting the Electronic Consumer

Electronic protection refers to safeguarding consumer rights against fraud, deception, or the purchase of counterfeit goods using digital tools. These tools, with their extensive reach, often surpass the influence of traditional methods.

Legal definitions and regulations concerning consumer rights generally apply to both traditional and electronic transactions. Thus, the electronic consumer is entitled to the same legal protections granted to traditional consumers, with specific rules tailored to the unique nature of electronic contracts executed remotely via digital platforms.

Additionally, some regulations address cybercrime-related issues where consumers might unknowingly fall victim during financial or commercial activities conducted electronically.

Main Pillars of Consumer Protection (Boufench Wassila & Boufench Raqia, 2018, p. 1647):

- **Regulatory Pillar:** Ensuring the safety of goods and services offered, adhering to global standards, and preventing fraud and deception through governmental and civil society efforts.
- **Legislative Pillar:** Revisiting and updating existing laws to establish mechanisms for safeguarding all consumer rights.
- **Educational and Awareness Pillar:** Raising consumer awareness about their rights and responsibilities, guiding their decisions, and providing protection against online risks through platforms that share stories, expert advice, and updates on fraudulent activities.

3. Justifications for Protecting the Electronic Consumer

The main reasons for protecting electronic consumers include (Washawesh et al., 2018, pp. 1895-1896):

- **Need for Electronic Services:** Consumers increasingly rely on online platforms offering diverse services such as real estate, travel, and banking. The competitive nature of these platforms necessitates safeguarding consumer interests.
- **Technological Advancements in the Internet:** New tools and techniques enhance user interaction with services and products, creating the need for robust consumer protection mechanisms.
- **Lack of Technical Knowledge:** Many consumers lack adequate technical knowledge to navigate the internet securely, exposing them to online fraud and deceptive practices like counterfeit websites or false agreements.

3- Objectives of Protecting Electronic Consumers

The primary objectives of protecting electronic consumers include (Al-Bakri, 2006, p. 237):

- Ensuring consumers are protected from fraud and deception practiced by producers or intermediaries during transactions within sales operations.
- Guaranteeing various consumer rights and shielding them from possible manipulations in the goods and services they need or desire.
- Providing security and assistance to low-income groups, enabling them to access the goods and services they require.
- Enhancing coordination and cooperation with business organizations to equip them with consumer-related information that they may not otherwise access due to limited communication capabilities.

4- Principles of Protecting Electronic Consumers

The United Nations has established principles to underpin consumer protection frameworks in alignment with the global nature of the internet, including (Talouch & Zein, 2018, p. 1861):

- **Justice and Equity:** Virtual space businesses must act honestly, striving to build loyalty across their consumer base, especially among vulnerable and underprivileged consumers, while integrating these principles into their corporate culture.
- **Fair Commercial Practices:** Virtual businesses must refrain from engaging in illegal, unethical, discriminatory, or misleading practices, such as aggressive sales techniques or unjustifiable actions that harm consumers.

- **Communication and Transparency:** Companies must provide complete, accurate, and non-deceptive information about products, particularly regarding terms and fees. This information must be easily accessible, especially regarding key terms and conditions, regardless of the level of technology used.
- **Education and Awareness:** Organizations should establish programs and tools to help consumers acquire the knowledge and skills necessary to understand the risks associated with electronic transactions, particularly those linked to payment processes, while offering professional advice and assistance.
- **Privacy Protection:** Businesses must safeguard consumer privacy through monitoring mechanisms, security measures, and transparency. They should also obtain consent for collecting and using personal data.
- **Complaints and Dispute Resolution:** Virtual businesses should establish fair, transparent, and cost-effective complaint mechanisms to resolve disputes efficiently. They must strive for amicable dispute resolution and ensure customer satisfaction.

5- Risks Facing Electronic Consumers in the Context of Cybercrimes and Protective Measures

1. Risks Facing Electronic Consumers

Consumers' reliance on goods and services offered online—such as travel, banking, insurance, flight ticket purchases, and hotel bookings—drives them to engage in online transactions. However, their limited expertise and knowledge in information technology, particularly the internet, often expose them to risks. These risks are varied but generally aim to compromise data or personal information for financial gain. Notable risks include (Abdel-Rahim & Abdel-Rahim, 2017, pp. 130-132):

- **Hacking:** Cybercriminals, such as crackers and hackers, breach websites to steal personal information and financial accounts. Hackers closely monitor security updates and form networks to exchange information. They bypass security measures to commit acts of sabotage, embezzlement, and forgery.
- **Fraud and Deception:** Fraudsters create fake commercial websites offering unrealistic discounts or deals on non-existent products to deceive consumers.
- **Use of Similar Names and Trademarks:** Some websites mimic well-known brands to lure and deceive consumers.
- **Fraudulent Product Purchases:** This involves shipping electronic goods or luxury items purchased using stolen credit cards to locations far from the theft's origin. These goods are sold at slightly higher prices abroad, and the proceeds are divided among the fraudsters.
- **Auction Fraud:** Online auctions often come with risks from both buyers and sellers. Buyers may receive inferior goods, or sellers may collect payment without delivering products. Fraud can also occur through fake bids to inflate the product's price, deceiving consumers.
- **Credit Card Data Theft:** Credit card information can be stolen through traditional theft, phishing, or hacking. Criminals use stolen data to make online purchases of goods or services.

Other risks include:

- **Malfunction of Electronic Payment Tools:** Payment tools may experience functional failures due to physical or electrical malfunctions, programming errors, or maintenance issues, leading to inaccurate payments.
- **Loss of Electronic Payment Tools:** Consumers may lose payment tools due to negligence, forgetfulness, or theft, resulting in potential misuse by others.

2- Methods of Protecting Electronic Consumers from Cybercrime Risks

The issue of protecting electronic consumers has become increasingly important, particularly in the digital economy, where consumers are more susceptible to manipulation and various ongoing threats. Hackers and malicious actors continuously develop new techniques to carry out their destructive activities, making consumer security a vital aspect of the success of digital economy projects. Below are key systems and methods used to secure transactions within the digital economy:

1-2 Administrative Measures to Protect Electronic Consumers

Administrative measures involve various tasks for senior management to ensure information security. These include oversight and supervision of information security systems. Key tasks include (Bouzokri, 2015/2016, pp. 154–155):

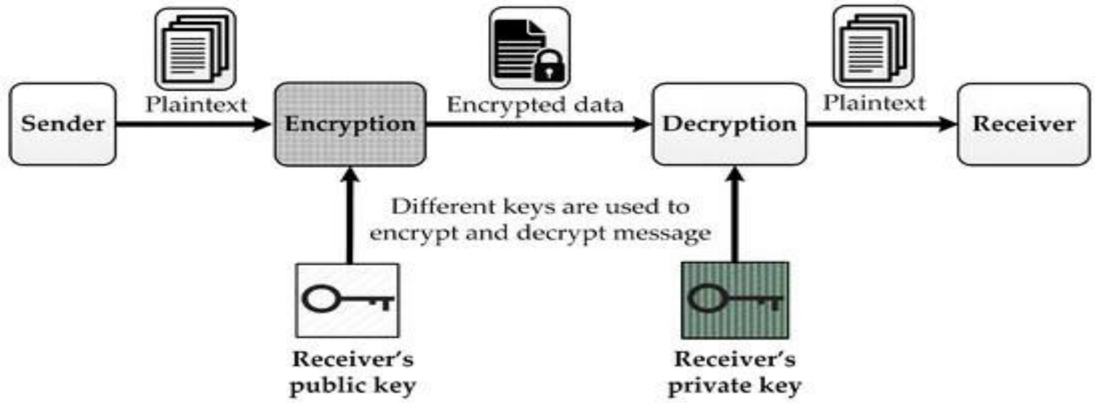
- **Educated Security Policies:** Webpage designers often employ hypertext techniques to enhance information security. This involves summarizing key security principles and standards in the first two pages of a website and linking to detailed guidelines.
- **Device Security:** Protecting devices requires securing the physical premises, such as restricting unauthorized access to computer rooms and storage areas. Advanced technologies, such as fingerprint or retina scanners and magnetic cards, should be used to control access to systems.
- **Data Security:** This involves assigning responsibilities based on organizational structure to enhance security levels and minimize crimes. Backup mechanisms must be implemented for external storage devices, ensuring their security and regular updates. Operational guidelines should be established for database programmers, administrators, network management, and input/output processes.
- **Employee Security:** Steps include:
  - Prohibiting temporary employment entirely.
  - Implementing strict procedures during employee termination, such as retrieving keys and magnetic cards and changing passwords.
  - Rotating employees among departments and requiring mandatory vacations to monitor system activities during their absence.
  - Organizing regular conferences, lectures, and workshops on information security.
  - Encouraging participation in international exhibitions and specialized security training courses.
  - Offering incentives and linking promotions to adherence to information security protocols.
- **Establishing a Dedicated Information Security Department:** Large organizations should appoint an information systems security manager reporting directly to senior management. This manager oversees a specialized team trained in data protection, programming, and handling cybercrime cases.
- **Network Access Authorization:** A robust security policy should regulate access to the network by allowing or denying certain files or activities.

2-2 Technical Measures to Protect Electronic Consumers

Technical measures involve a range of technical procedures followed by organizations to protect their information and customers. Key measures include (Sira'a, *Reality and Prospects of E-commerce in Algeria*, Master's Thesis, 2013/2014, pp. 77–82):

- **Secure Sockets Layer (SSL):** Developed by Netscape, SSL has increased confidence in digital economy applications, especially e-commerce. It provides a secure encryption protocol for transferring data between devices over the internet, ensuring data confidentiality. Most major internet browsers have incorporated SSL technology, making it a global standard for secure online transactions.
- **Secure Electronic Transactions (SET):** First used in the United States in 1997, SET relies on encryption and digital signatures, similar to SSL. It uses digital wallets containing cardholder details and digital certificates issued by certified banks. During online transactions, both merchants and cardholders authenticate each other's identities using their respective digital certificates.
- **Electronic Encryption:** Encryption converts information into unreadable codes to prevent unauthorized access. It transforms plaintext into ciphertext using keys based on complex mathematical formulas (algorithms). The strength of encryption depends on two factors: the algorithm and the key length (measured in bits).

The diagram below illustrates the electronic encryption process:

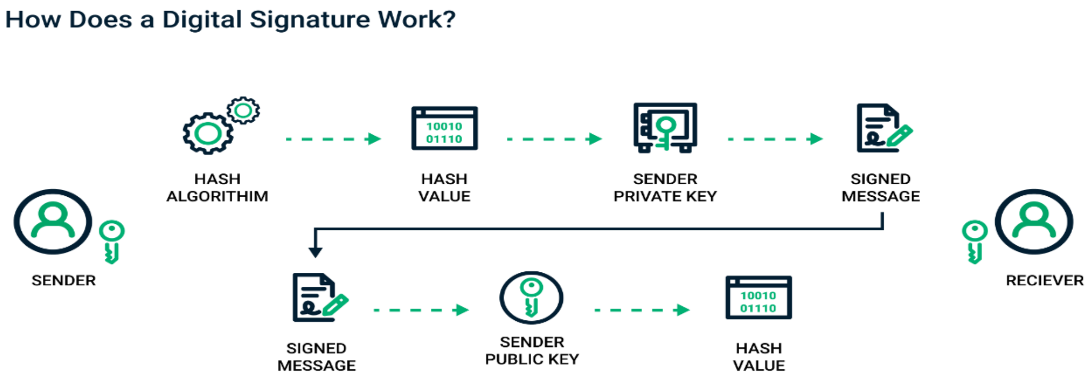


Source : https://www.mdpi.com/2079-9292/11/6/891, consulté le 17/10/2024.

Electronic Fingerprint:
An electronic fingerprint is a digital identifier derived using specific algorithms called hash functions. These algorithms perform mathematical calculations on a message to generate a small “fingerprint” representing the entire file or message. The electronic fingerprint consists of fixed-length data (typically between 128 and 160 bits) derived from variable-length messages. The uniqueness of each fingerprint depends on the private keys used to create them, which can only be decoded using the corresponding public key.

Electronic Signature:
An electronic signature ensures more secure and confidential transactions by acting as a digital identity seal accompanying the message online. It verifies that the message originates from its source and remains unaltered during transmission. The sender uses a private key to digitally sign the document, while the receiver verifies the signature's validity using the public key. The following diagram illustrates how electronic signatures work:

Figure 02: Mechanism of Electronic Signatures



Source: Sectigo, accessed 17/10/2021.

Electronic Certificate:

An electronic certificate is a digital document verifying the identity of users over the internet. It is issued by a trusted entity called a Certificate Authority (CA). Each digital certificate contains important details about its owner and the issuing authority.

Firewalls:

Firewalls are tools used to protect private networks from unauthorized access. They prevent illicit entry to networks and protect internet control and transmission units. Firewalls are critical for safeguarding private networks against various cyber threats.

Use of Intermediary Sites:

One example is **PayPal**, established in 1998 and later acquired by eBay in 2002 to facilitate its commercial transactions. PayPal is known for its ease of use and money transfer services. As a global leader in online payment solutions, PayPal supports over 169 million accounts in 203 markets and 26 currencies worldwide, making it a cornerstone for global e-commerce by offering diverse payment options across sites, currencies, and languages.

3-2 Legal Measures to Protect Electronic Consumers:

The success of electronic transactions in any country relies on building consumer, merchant, and business trust in this transaction model. Cybercrimes, which transcend geographic boundaries, pose the greatest threat to this trust.

Thus, creating a robust legal framework is essential to protect the rights and interests of all involved parties. It is insufficient to merely modify traditional laws with additional provisions; instead, it is necessary to develop an independent legal framework tailored to the new economic applications and to adequately protect electronic consumers.

Providing legal protections for electronic consumers in different countries reflects the technological and social advancements in these regions. Since electronic contracts are often international, suitable legal measures for global consumer protection must be established. To this end, the European Council has issued two directives:

1. **First Directive:** Encourages international conferences to address electronic commercial transactions, particularly those outside Europe.
2. **Second Directive:** Establishes rules to determine the most favorable jurisdiction for consumers, especially under the Rome Treaty of July 19, 1980. The European directive also addresses protecting consumers from unfair conditions imposed by sellers. (Belaatir & Ben Ameyrouche, 2018, p. 1605).

Conclusion:

In light of scientific and technological advancements and the growth of e-commerce, protecting electronic consumers from exploitation by cybercriminals has become essential. Strengthening mechanisms to protect electronic consumers locally and internationally is imperative, whether through raising consumer awareness or enacting appropriate laws and regulations.

Electronic consumers face numerous risks, such as hacking, fraud, credit card data theft, and deceptive use of brand names. Many legal frameworks focus on educating consumers before they enter contracts to protect them. Examples include initiatives by the International Consumer Organization, the European Directive, and the Organization for Economic Cooperation and Development (OECD).

However, there is no comprehensive legal framework guaranteeing consumer rights in electronic transactions, as electronic contracts often involve parties from different countries with varying laws. Additionally, not all protection mechanisms are practical or affordable, reducing the potential benefits of electronic transactions for consumers.

Recommendations:

1. Enact international laws and regulations governing e-commerce and electronic transactions while enhancing payment security to protect electronic consumers from fraud and deception.
2. Strengthen oversight of electronic transactions and agreements to safeguard consumers.
3. Standardize international legal frameworks to align the legal rights of contracting parties and expand consumer protection against cybercrimes.
4. Develop technical protections enhanced by legal safeguards to address risks related to electronic transactions and information technologies.
5. Update laws and regulations to address emerging cybercrimes threatening consumers' finances and well-being.
6. Leverage intermediary sites in electronic transactions to ensure consumer funds are safeguarded and credit card information remains confidential.
7. Encourage consumers to choose secure websites and reputable online merchants.

References:

1. Beas, R. (2016). *The fight against cybercrime in light of state actions* (Doctoral Thesis). Paris, Faculty of Law, France: University of Lorraine.
2. Ahmad Badr Osama. (2005). *Consumer Protection in Electronic Contracts.* Egypt: New University Publishing House.
3. El-Amir Abdel Kader Hafouda & Houssam Gardain. (2017). *Cybercrime and Mechanisms to Combat It* (National Symposium). Faculty of Economic, Commercial, and Management Sciences, Tlemcen: Abou Bekr Belkaid University.
4. Tayeb Aissawi & Hicham Shekarda. (2020). *Media Education as a Mechanism to Reduce Cybercrime on the Internet.* Algerian Journal of Research and Studies.
5. Ben Yaqoub, A. (2004). *The Role of Consumer Behavior in Enhancing Marketing Decisions.* Journal of Humanities, 81–95.
6. Boufench Wassila & Boufench Raqia. (2018, April 23–24). *Mechanisms for Consumer Protection in the Context of the Digital Economy.* Third National Symposium on the Consumer and the Digital Economy – Necessity of Transition and Protection Challenges. Mila, Faculty of Economic, Commercial, and Management Sciences, Algeria: Abdelhafid Bousouf University Center.
7. Thamer Al-Bakri. (2006). *Contemporary Principles and Concepts.* Amman: Dar Al-Yazouri Scientific Publishing and Distribution.
8. Jamil Muhammad Hussein Abdul Rahman. (2008). *Legal Protection of Computer Programs* (Master's Thesis). Nablus, Faculty of Graduate Studies, Nablus: An-Najah National University.
9. Djilali Bouzokri. (2015/2016). *Electronic Management in Algerian Institutions: Realities and Prospects* (Doctoral Dissertation). Faculty of Economic, Commercial, and Management Sciences, Algeria: University of Algiers 03.
10. Hakima Jaballah. (2021). *Impacts of Cybercrime on the Digital Environment: A Study on Mechanisms and Strategies to Combat It.* Annals of the University of Algiers 1, 649–667.
11. Hanan Mubaraka Kirkouri. (2020). *The Specificity of Committing Cybercrime in the Information System: An Analytical Study in Light of Algerian Law.* Journal of Strategic and Military Studies, 9–22.
12. Rawan Al-Sahfi Bint Attiyah Allah. (2020). *Cybercrimes.* Multidisciplinary Electronic Journal, 1–53.
13. Zouleikha Belaatar & Madihah Ben Ameirouche. (April 23–24, 2018). *Mechanisms for Protecting Electronic Consumers from Fraud and Breach Risks* (National Symposium). Mila, Faculty of Economic, Commercial, and Management Sciences, Algeria: Abdelhafid Bousouf University Center.
14. Shamseddine Al-Tijani & Mohammed Youssef Amamra. (April 23–24, 2018). *The Reality of Algerian Consumers in the Context of Information and Communication Technology Usage – Foundations, Realities, and the Sector's Role in*

Consumer Protection (National Symposium). Faculty of Economic, Commercial, and Management Sciences, Mila: Abdelhafid Bousouf University Center.

15. Sabah Abdel Rahim & Wahiba Abdel Rahim. (2017). *The Reality of Consumer Shopping on the Internet Between Protection and Crime.* Journal of Judicial Efforts, 121–138.
16. Fares Talouch & Younes Zein. (April 23–24, 2018). *A Study of Legal Protection for Consumers Within United Nations and Developed Nations' Legislations* (National Symposium). Mila, Faculty of Economic, Commercial, and Management Sciences, Algeria: Abdelhafid Bousouf University Center.
17. Fouad Washaoush et al. (April 23–24, 2018). *International Consumer Protection in the Context of E-commerce Risks* (National Symposium). Mila, Faculty of Economic, Commercial, and Management Sciences, Algeria: Abdelhafid Bousouf University Center.
18. Karima Sira'a. (2013/2014). *The Reality and Prospects of E-commerce in Algeria* (Master's Thesis). Oran, Faculty of Economic, Commercial, and Management Sciences, Algeria: Oran 2 Mohamed Ben Ahmed University.
19. Karima Sira'a & Jamal Deqish. (2018). *The Economic Dimensions of Cybercrime.* Journal of Marketing Studies and Business Administration, 35–53.
20. Mohammed Ben Dhahbiya et al. (April 23–24, 2018). *Risks of Electronic Payment Facing Consumers and Algeria's Strategy to Protect Them – E-signature and Certification Projects* (National Symposium). Faculty of Economic, Commercial, and Management Sciences, Mila: Abdelhafid Bousouf University Center.
21. Mohammed, M. (2013). *Electronic Consumer Protection in Private International Law.* Cairo: Dar Al-Nahda Al-Arabia for Publishing and Distribution.
22. Mahmoud Ahmed Al-Qur'an. (2017). *Electronic Crimes.* Amman: Dar Wael for Publishing and Distribution.
23. Manal Zahra Hilal. (2014). *Information and Communication Technology.* Jordan: Osama Publishing House.
24. Nabil Dris. (2017). *Cybercrime: Concepts and Legislative Texts – Algeria as a Model.* Journal of Law and Society, 20–40.
25. Younes Arab. (April 2–4, 2006). *Journal of Law and Courts.* Retrieved from a7wallaw.com: http://www.a7wallaw.com/10807.