Science, Education and Innovations in the Context of Modern Problems
Issue 12, Vol. 8, 2025

Title of research article

The Role of the Family in Preventing Cybercrime: A Socio-Legal and Criminological Analysis of Family-Based Strategies for Combating Emerging Digital Crimes in Contemporary Society

Mezioud Salim
Doctor
Department of Law and Criminal Sciences, Faculty of Law and Political Science, University of Dr. Yahia Farès, Médéa
Algeria
E-mail: lotani.salim@gmail.com

Issue web link https://imcra-az.org/archive/387-science-education-and-innovations-in-the-context-of-modern-problems-issue-12-vol-8-2025.html

Keywords Family; Cybercrime; Emerging Crimes; Digital Safety; Crime Prevention; Criminology

Abstract

Cybercrime has emerged as one of the most pressing global security and social challenges of the 21st century. Its borderless, dynamic, and constantly evolving nature threatens individuals, institutions, and states alike. Among the most vulnerable victims is the family, the foundational social institution entrusted with safeguarding values, norms, and ethical stability. The proliferation of digital platforms, mobile technologies, and artificial intelligence has created new opportunities for interaction but also for exploitation, manipulation, and crime. Traditional prevention mechanisms are no longer sufficient to protect individuals from crimes committed in cyberspace, including identity theft, online fraud, cyberbullying, illegal content distribution, and sexual exploitation.

This study seeks to highlight the preventive role of the family in combating cybercrime. It adopts a descriptive-analytical methodology, combining legal, sociological, and criminological perspectives, to analyze the multifaceted dimensions of cybercrime and the protective functions of the family. The findings demonstrate that the family is not merely a private entity but a primary defense line against cyber threats. By fostering digital literacy, instilling ethical values, supervising online behavior, and collaborating with state institutions and civil society, the family can significantly reduce exposure to online risks. The study further emphasizes that the family must adapt its preventive strategies to the rapidly changing technological environment, becoming both a cultural transmitter and a proactive guardian of digital safety.

The research contributes to scholarly debates by positioning the family as a central actor in cybercrime prevention, complementing legislative, institutional, and technological measures. Policy implications call for strengthening family-oriented educational programs, integrating cybercrime awareness into curricula, and fostering cooperation between families and governmental cybercrime prevention agencies.

Citation. Mezioud S. (2025). The Role of the Family in Preventing Cybercrime: A Socio-Legal and Criminological Analysis of Family-Based Strategies for Combating Emerging Digital Crimes in Contemporary Society. *Science, Education and Innovations in the Context of Modern Problems*, 8(12), 108–120. https://doi.org/10.56352/sei/8.125.10

Received: 08.03.2025 | Accepted: 29.087.2025 | Published: 19.09.2025 (available online)

1. Introduction

The exponential growth of digital technologies and the increasing reliance on the internet have fundamentally reshaped social, economic, and cultural life. Alongside these benefits, however, cybercrime has emerged as one of the most pressing threats to individuals, families, and societies. Cybercrime is distinguished from traditional forms of crime by its **borderless, intangible, and highly adaptive nature**, posing significant challenges to law enforcement, judicial systems, and preventive institutions.

Against this backdrop, the family remains the **primary social institution** responsible for nurturing values, guiding behavior, and safeguarding individuals from risks. The central research question guiding this study is therefore:

What role does the family play in protecting individuals and society from the dangers of cybercrime?

The aim of this paper is to (i) define cybercrime, (ii) analyze its nature, forms, and characteristics, and (iii) highlight the preventive measures that families can adopt to mitigate exposure to cyber threats. To achieve this objective, the study employs a **descriptive-analytical methodology**, combining legal, criminological, and sociological perspectives.

Actuality of the Study

The relevance of this study lies in the unprecedented **rise of cybercrime worldwide** and its direct impact on the stability of family structures. Algeria, like many countries, is experiencing rapid technological penetration across all social strata, making families increasingly exposed to online risks. Given that cybercrime transcends territorial borders and legal systems, prevention must begin within the family unit. Recognizing the family as a **cornerstone of social order** ensures that individuals are equipped with moral, cultural, and digital tools necessary to confront emerging threats. This research is timely, as policymakers and scholars alike seek **integrated approaches** to addressing cybercrime, blending **legal frameworks, technological solutions, and socio-cultural prevention mechanisms**.

Method and Methodology

This research employs a **descriptive-analytical approach**:

1. **Descriptive Dimension:**
   - Defines cybercrime and reviews competing jurisprudential, sociological, and international definitions.
   - Outlines the nature, forms, and evolving characteristics of cybercrimes, including identity theft, online fraud, child exploitation, hacking, and financial crimes.
2. **Analytical Dimension:**
   - Examines the role of the family as a preventive actor in combating cybercrime.
   - Investigates the extent to which parental supervision, family cohesion, and ethical upbringing reduce vulnerability to cyber threats.
   - Analyzes case studies from Algeria and comparative legal frameworks to evaluate the efficiency of family-based prevention.
3. **Sources of Data:**
   - Review of criminological, legal, and sociological literature.
   - Reports from international organizations (Interpol, UNODC, ITU).
   - National cybercrime laws and preventive campaigns in Algeria and abroad.

The methodology thus allows for a multidimensional understanding of how families can transform from passive social entities into **active guardians of digital security**.

Findings

The study reveals several key findings:

1. **Family as First Line of Defense:** Families that actively supervise online behavior and cultivate awareness among children significantly reduce the likelihood of victimization by cybercriminals.
2. **Education and Digital Literacy:** Preventive success depends on equipping family members—especially children and adolescents—with digital skills, critical thinking abilities, and awareness of online risks.
3. **Value Transmission:** Strong family bonds and moral education help instill values of responsibility, honesty, and respect for privacy, which serve as shields against deviant online behavior.
4. **Weaknesses in Family Prevention:** Many Algerian families lack adequate awareness of cyber risks, resulting in exposure to fraud, online harassment, and harmful digital content.
5. **Complementary Role of State Institutions:** While the family is critical, effective prevention requires support from governmental cybercrime units, legal frameworks, schools, and civil society organizations.
6. **Recommendations:** Families should:
   - Foster open communication with children regarding online activities.
   - Establish household digital rules.
   - Collaborate with schools, community organizations, and law enforcement.
   - Participate in national cyber awareness programs.

In summary, the family functions as a **micro-social unit** whose proactive engagement strengthens the overall resilience of society against cybercrime.

2. Concepts Related to Cybercrime

2.1. Definition of Cybercrime

There is no universally agreed-upon definition of cybercrime in criminal jurisprudence. Scholars variously refer to it as *electronic crime*, *information crime*, *computer crime*, or *emerging crime*. This diversity of terminology reflects different jurisprudential schools of thought and legal interpretations.

At its core, cybercrime consists of two elements: *crime*—defined as behavior that violates the law—and *cyber*, referring to the use of computer technologies and networks. As such, cybercrimes involve unlawful acts committed through or against computer systems, often with the intent to cause harm, gain illicit benefit, or undermine trust (Hijazi, 2002).

The German jurist Tadman defined cybercrime as "all forms of unlawful or harmful behavior to society committed using a computer." Similarly, Al-Bashri (2005) emphasized that such crimes involve situations in which the computer plays an active role, rather than being merely incidental to the act.

In sum, cybercrime may be defined as **any unlawful activity in which a computer system or network serves as the instrument, target, or environment for committing the offense**.

2.2. International Definitions of Cybercrime

International organizations, including the **United Nations Office on Drugs and Crime (UNODC)**, generally define cybercrime as unlawful actions targeting the **confidentiality, integrity, and availability** of data and systems. These include hacking, malware distribution, online identity theft, financial fraud, and crimes involving the dissemination of illicit content (Houri, 2003).

Dr. Abdel Fattah Murad further elaborated on internet crimes as encompassing "all actions that violate law and Sharia, committed using a computer through the internet, requiring specialized knowledge of information systems." Examples include hacking, economic espionage, intellectual property violations, identity theft, online extortion, and money laundering.

3. Characteristics of Cybercrime

Cybercrime is characterized by features that distinguish it from conventional crimes:

- **High technical skill of perpetrators:** Offenders often possess advanced expertise in computing and information systems, unlike traditional criminals, who may have limited formal education.
- **Motivations beyond financial gain:** While some perpetrators seek economic benefit, many are motivated by the desire to challenge or undermine digital systems.
- **Intangible targets:** Cybercrime typically affects digital assets (data, information, intellectual property) rather than physical property.
- **Difficulty of detection and prosecution:** Perpetrators leave minimal physical evidence, complicating investigation and judicial processes.
- **Global dimension:** Cybercrimes transcend territorial boundaries, raising complex legal, technical, and political challenges, particularly regarding international cooperation (Ali Al-Araban, 2004).

4. Types of Cybercrime

Cybercrime encompasses a broad range of activities. For analytical clarity, it may be classified into the following categories (Dierschl, 2017; Al-Hamdan, 2017):

4.1. Cybercrimes against Individuals

These involve unauthorized access to personal data, email accounts, or online identities. Offenses include identity theft, impersonation, and online harassment. Perpetrators may also threaten victims by exploiting stolen files, photos, or sensitive information.

4.2. Cybercrimes against Governments

Such crimes target official websites and critical information infrastructures, often aiming to disrupt operations or compromise national security. Motivations are frequently political, and perpetrators are commonly referred to as *hacktivists* or cyber-terrorists.

4.3. Cybercrimes against Property

These target institutions, both public and private, with the aim of destroying, stealing, or manipulating data. Common methods include malware attacks, unauthorized file transfers, and data corruption.

4.4. Political Cybercrimes

Political cybercrimes involve attacks on military or defense systems, theft of classified information, or infiltration of encrypted government communications. They are often linked to cyberterrorism and international espionage.

4.5. Fraud and Financial Cybercrimes

This category includes phishing, unauthorized transfers, manipulation of financial databases, insider abuse by employees, and exploitation of e-commerce systems. Financial cybercrimes are among the most widespread and economically damaging forms of cybercrime.

3.6. Cyber Extortion

Cyber extortion involves deliberate attacks on computer systems or websites to disrupt or deny access to services, often through *Distributed Denial of Service (DDoS)* attacks. Perpetrators typically demand ransom payments to cease their attacks. These offenses are usually carried out by organized groups or professional hackers with advanced technical expertise (Al-Hamdan, 2017).

3.7. Defamation Crimes

Cyber defamation crimes aim to tarnish an individual's reputation through slander, insults, or the unauthorized dissemination of sensitive information. A common form is **cyberstalking**, which involves electronically tracking or harassing individuals in ways that result in personal distress or public embarrassment. Offenders frequently exploit social media platforms, chat rooms, and other interactive forums to collect personal data and manipulate it for defamatory purposes.

4. Objectives of Cybercrime

The objectives of cybercrime vary depending on the perpetrator's motivation and level of sophistication. They can be summarized as follows:

- **Unauthorized access to information:** Stealing, viewing, deleting, or modifying information to achieve criminal objectives.
- **Disabling information servers:** Gaining access to online servers and interrupting their ability to provide services.
- **Extortion:** Obtaining confidential information from individuals, banks, or government institutions to blackmail them.
- **Illicit gains:** Securing financial, political, or moral benefits through fraudulent activities such as credit card fraud, website destruction, and unauthorized bank account transfers.

5. Tools of Cybercrime

Cybercriminals employ a wide range of tools and techniques, including:

- **Internet access:** The essential platform enabling cybercrime activities.
- **Specialized software:** Programs designed to copy or retrieve information stored on a victim's device.
- **Espionage devices:** Hardware such as cameras linked to communication systems.
- **Barcode readers and decoders:** Used to intercept and manipulate digital codes.
- **Peripheral devices:** Printers and mobile phones adapted for fraudulent purposes.
- **Malicious software:** Programs such as *Trojan horses*, worms, or ransomware, which deceive users into installing them and cause extensive damage.

6. Causes of Cybercrime

The causes of cybercrime span **individual, societal, and global levels**, reflecting the multifaceted nature of this phenomenon.

6.1. Individual-Level Causes

6.1.1. Seeking Recognition

Some cybercrimes are committed by reckless youth or minors seeking status, recognition, or media attention. Such behavior is often temporary, declining with age and maturity.

6.1.2. Opportunity

The accessibility of modern technologies creates abundant opportunities for criminal exploitation. Inadequate monitoring, combined with weak protective measures, increases the likelihood of cybercrime, as sensitive information can be stolen or manipulated with minimal risk of detection.

6.1.3. Low Self-Control

Drawing on **Gottfredson and Hirschi's General Theory of Crime**, individuals with low self-control are more likely to engage in reckless or deviant behavior when opportunities arise. Such individuals prefer immediate gratification through bribery, theft, or deception rather than long-term lawful rewards.

6.1.4. Routine Activities

According to **Cohen and Felson's Routine Activity Theory**, crime occurs when three conditions converge: (i) a motivated offender, (ii) a suitable target, and (iii) the absence of capable guardianship. Increased use of social networks, email, and other online platforms provides ideal conditions for this convergence, thereby amplifying the risks of cybercrime.

6.2. Societal-Level Causes

6.2.1. Urbanization

Rapid urbanization, particularly in developing countries, creates social pressures that drive individuals toward crime. With limited economic opportunities, some turn to cybercrime, which requires minimal initial investment but offers high potential returns. For example, in Nigeria, this phenomenon is commonly referred to as "Yahoo Yahoo."

6.2.2. Unemployment

High unemployment rates, especially among young populations, are directly correlated with cybercrime. The proverb *"An idle mind is the devil's workshop"* aptly illustrates how youth with technical skills may resort to online crime when legitimate opportunities are absent.

6.2.3. General Social Pressures

Poverty, illiteracy, and economic instability create negative coping mechanisms, including involvement in electronic human trafficking, online sexual exploitation, and financial cybercrimes.

6.2.4. Pursuit of Wealth

Consistent with **Merton's Anomie Theory**, individuals who cannot achieve socially approved goals through legitimate means may resort to illegitimate ones. Cybercrime becomes particularly attractive because it promises larger targets, quicker returns, and lower risks compared to traditional crimes.

6.2.5. Weak Law Enforcement

In many countries, legislation and judicial mechanisms have not kept pace with technological advancements. Insufficient capacity to manage digital evidence, weak cross-border cooperation, and limited technical expertise among law enforcement agencies contribute to the persistence of cybercrime.

6.3. Global-Level Causes

6.3.1. Transition to a Digital Society

The **information age** is marked by quantitative and qualitative changes in the flow of information, instantaneous communication, and global connectivity. With basic technical knowledge and access to the internet, individuals can now participate in complex social, political, and criminal activities within cyberspace. The transformation to a digital society, therefore, creates new vulnerabilities requiring global security measures.

6.3.2. Globalization

Globalization amplifies cybercrime by enabling anonymity, flexibility of identity, and weak deterrence in cyberspace. Individuals who would not commit crimes in the physical world may find it easier to engage in illegal activities online due to reduced risks of detection and punishment.

6.3.3. Global Interconnectedness

The emergence of global interconnectedness in the context of demographic and economic transformations has created unprecedented opportunities for criminals. By 2050, the world's urban population is expected to reach **6.2 billion people**, or nearly 70% of the total population. The **National White-Collar Crime Center** reports that the internet allows offenders to instantly communicate with multiple victims via chat rooms, email, or websites, making large-scale fraud and exploitation accessible with only basic computing skills.

6.3.3. Exposure of Global Information Infrastructure

Global information infrastructures differ markedly in their exposure to **natural hazards, human negligence, and managerial failures**. The U.S. Presidential Report on protecting critical infrastructure identifies five sectors sharing common risk characteristics:

- **Information and Communication Sector:** Public telecommunications networks (PTN), the internet, and computers in household, academic, governmental, and commercial use.
- **Physical Distribution Sector:** Highways, railways, ports, waterways, airports, transport companies, and shipping services that enable the movement of people and goods.
- **Energy Sector:** Industries producing and distributing electrical power, petroleum, and natural gas.
- **Banking and Finance Sector:** Banks, non-bank financial services, payroll systems, investment companies, mutual loans, and securities exchanges.
- **Vital Human Services Sector:** Potable water systems, emergency services, and core government services (e.g., unemployment, social security, disability compensation, and civil registration).

7. Information Crimes in Algerian Legislation

7.1. Investigation of Information Crimes

Effective response requires **specialized units** within all security services (police, gendarmerie, military security). Because judicial police officers are typically the first to be notified of cyber incidents, comparative experience is instructive. For instance, France established the **Central Office for Combating Crime Related to Information and Communication Technologies (OCLCTIC)** in 2000.

7.2. Central Brigade for Combating Information Crime (BCRCI)

Established in **September 1994**, the BCRCI operates alongside regional units, including:

- **Research Brigade for Crimes Related to Information Technologies.**
- **Juvenile Brigade**, specializing in crimes against minors in online indecency.

Administrative services also play preventive roles—e.g., the **Central Directorate for Information Systems Security** at the Ministry of Finance—and various **awareness associations**. Police services maintain regional and central units with officers trained for diverse cyberoffenses.

To address legal gaps, the Algerian legislature enacted **Law No. 09-04** (5 August 2009) on preventing and combating ICT-related crimes (low09-04, 2009). The law comprises six chapters; Chapter I defines terminology

and scope, sets **technical arrangements for monitoring electronic communications**, enables **real-time collection and recording** of content, and regulates **searches and seizures**.

7.3. Monitoring Electronic Communications

Article 4 specifies when electronic monitoring is permitted (low09-04, 2009):

- Prevention of acts categorized as terrorism, sabotage, or crimes against state security.
- When credible information indicates a potential attack on an information system threatening public order, national defense, state institutions, or the national economy.
- Where judicial investigations require monitoring to be effective.
- To execute **international mutual legal assistance** requests.

This procedure requires **written authorization** from the competent judicial authority. The **Public Prosecutor at the Algiers Court** may grant a **six-month renewable** authorization to judicial police officers of the **National Agency for Preventing Crimes Related to Information and Communication Technologies**, based on a technical report detailing the arrangements and purposes.

7.4. Searching Information Systems

Competent judicial authorities and judicial police officers may **access and search** an information system (or part thereof) and its stored data—including remotely. If the required data are accessible only via systems located **outside national territory**, the authorities must seek assistance from the relevant foreign bodies in accordance with **international agreements** and the **principle of reciprocity**.

7.5. Seizing Data

Data under investigation—and any data necessary to interpret it—may be **copied to an electronic storage medium** for seizure and custody under the Code of Criminal Procedure. Technical means necessary to **assemble and reconstruct** data may be used to render it intelligible for investigative purposes, provided the **content is not altered**; misuse beyond investigative necessity incurs sanctions. **Law 04/09** also permits **access-blocking seizure** via an order instructing qualified persons to apply appropriate technical measures (Qashqoush, 2000).

7.6. Preserving Traffic Data

Law 09-04 obliges service providers to assist judicial investigations by enabling **real-time collection and recording** of communications content and by making preserved data available—under strict confidentiality. Providers must retain, for **one year** from recording date:

- Data identifying service users.
- Data relating to **terminal equipment** used.
- **Technical characteristics**, date, and duration of each communication.
- Data concerning **supplementary services** requested, used, or provided.
- Data identifying the **recipient** and **addresses of accessed sites**.

Obstructing investigations incurs **criminal liability**: natural persons face **6 months to 5 years** imprisonment and a **50,000–500,000 DZD** fine; legal persons are fined per the Penal Code. Providers must **remove unlawful content** immediately upon awareness (direct or indirect), **store it** or **block access**, implement **technical filters** against content violating public order or morals, and **inform subscribers** of such measures.

Search, inspection, and seizure are executed under **Article 47(3)–(4)** of the Code of Criminal Procedure, allowing judicial police to act—**with prior authorization** from the public prosecutor—**at any time**. The investigating judge may undertake these measures anywhere in the national territory under **Article 65 bis et seq.** Procedures for

intercepting correspondence, **audio recording**, **image capture**, and **leak operations** require authorization by the public prosecutor (preliminary stage) or the investigating judge (judicial stage).

Finally, **Law 09-04** created the **National Agency for Preventing ICT-Related Crimes**, though it has yet to be established. The law affirms **international cooperation** and **mutual legal assistance**.

Observations. Many technical terms remain **insufficiently defined** (except those in Article 2). A **dedicated statute** clarifying all ICT-crime terminology and delineating **rights/obligations** of users of computer systems, internet, and intranets would (i) reduce avenues for evading liability and (ii) assist legal practitioners, judges, and researchers through clearer allocation of responsibilities. The absence of such a consolidated law remains a salient challenge in Algerian legislation. By contrast, **France's 1978 Law on Data Protection, Freedoms, and Information Technology** established foundational concepts and clarified criminal/civil responsibilities, with subsequent enactments building on that framework.

8. Prevention of Cybercrime

Cybercrime accompanies all societies—**developed and developing**—though its manifestations vary. International reports indicate a **global rise** in crime, with novel forms emerging from rapid advances in communication technologies (Brooks, 2018). While research remains ongoing, key **preventive priorities** include:

8.1. Providing Opportunities for Healthy Personality Development

Crime has deep developmental roots. Parents can limit antisocial tendencies by maintaining a **supportive emotional climate** in the home during childhood.

8.2. Building Friendly Relationships with Children (Ahmed Mohamed, 1980)

Parents should actively guide moral and personality development. **Schools**, **youth centers**, and **community organizations** are crucial partners in parent education.

8.3. Early Detection of Delinquency and Crime

Delinquency typically **emerges gradually**. **Timely identification** and guidance can prevent escalation into criminality.

8.4. Removing Factors that Encourage Crime

Reduce exposure to **harmful environments**, eradicate **slum conditions**, and expand **recreational facilities** (e.g., sports and youth clubs) to provide constructive outlets for children and adolescents.

8.5. Preparing Parents for Their Roles

Contemporary parenting requires **modern skills**. Parents should receive **structured guidance** through training programs delivered by specialized institutions.

8.6. Enforcing the Law Strictly

Effective **deterrence** depends on precise and consistent application of legal provisions.

8.7. Establishing Effective Government Rehabilitation Systems

Strengthen the **legal framework** to ensure proportionate punishment and close loopholes that enable offenders to evade justice.

8.8. Creating Rehabilitation Centers

Invest in centers that **socially, culturally, and economically** rehabilitate juvenile offenders, converting them into **productive citizens** through educational and restorative models.

9. The Role of the Family in Preventing Cybercrime

The family is the **primary unit of socialization**; its strength or fragility reverberates through the entire social order. Families bear a **frontline responsibility** for cultivating values and preparing children to uphold societal norms. As noted: *"O you who have believed, protect yourselves and your families from a Fire whose fuel is people and stones ..."* ("At-Tahrim, Verse 06). The Prophet Muhammad (peace be upon him) said: *"Each of you is a shepherd, and each of you is responsible for his flock. The man is a shepherd over his family, and the woman is a shepherd over her husband's house and children."* (Al-Bukhari, (n.d.))

Families help achieve **societal security** by instilling principles that guide **self-regulation**, thereby preventing crime **at its source**. In cyber contexts, parents contribute to **cybersecurity** by educating, supervising, and promoting responsible digital behavior. Practical focus areas include:

9.1. Electronic Games

While attractive, some games **normalize violence** or harmful behaviors and can contribute to psychological harm and, in extreme cases, self-harm. Parents should **curate content**, encourage **constructive games**, and monitor usage.

9.2. Social Media and "Electronic Friendships"

"Virtual friends" are often **anonymous** and may include **extremists**, **extortionists**, or **manipulators**. Parents should cultivate **open, trusting communication**, monitor activity, and provide **warmth and guidance** to prevent victimization or offending.

9.3. Cyberterrorism Awareness

Extremists exploit online platforms to **disseminate ideology** and **recruit** vulnerable youth. Parents should ensure **sound religious education** from **trusted sources** and caution against **unverified content**.

9.4. Information Quality and Critical Thinking

The internet's vast resources are **uneven in reliability**. Parents should promote **verification skills** and **critical thinking** to evaluate sources.

9.5. News Literacy

Some outlets spread **rumors, disinformation, and hate speech**. Direct children to **trusted official sources** and discuss **verification practices**.

9.6. Healthy Technology Use

Encourage **moderation** to avoid overuse and **digital addiction**, emphasizing balance, sleep hygiene, and offline activities.

Every family can turn the home into a **micro-school** where children learn to **make sound decisions** and avoid professional cybercriminals' traps (ahmed mohamed, 2005). Practical guidelines include:

- **Promote good conduct** and explicitly warn against risky online behaviors; educate about the **dangers of technology and the internet**.
- Foster an environment of **dialogue and respect**, where children can **exercise judgment** and feel valued.
- **Instill responsibility** to strengthen psychological stability and purpose.
- Recognize the **challenges of adolescence** and address them sensitively.
- **Learn the technology** yourselves—deploy parental controls and **content filters** where appropriate.

Summary of the family's role:

- Cultivate **scientific literacy** about technology and its positive societal uses through family discussions and friendly competitions.
- Teach a **correct understanding** of technology's purposes and the risks of misuse using real-life examples.
- **Monitor and guide** children's technology use toward responsible practices.
- Instill **religious and ethical values**, including respect for others' property and privacy.
- Emphasize **honesty, mutual help, and compassion**, following the principle: *"None of you truly believes until he loves for his brother what he loves for himself."*

10. Conclusion

In the contemporary digital era, cybercrime has evolved into a **global security challenge** that transcends geographic boundaries and affects all aspects of social, economic, and political life. The rapid diffusion of internet technologies, social networks, and digital devices has provided unprecedented opportunities for communication and development, but it has also created fertile ground for new forms of crime. These crimes threaten not only individual rights and freedoms but also the stability of families, institutions, and societies at large.

The findings of this study underscore that the **family occupies a central position in cybercrime prevention**, serving as the first and most influential social institution in shaping values, behaviors, and resilience against external threats. By instilling ethical and religious values, encouraging responsible use of technology, and fostering open communication, families act as a **protective shield** against the risks of cyberspace. Families that are engaged, vigilant, and digitally literate are far more capable of guiding their children and adolescents away from harmful online practices such as cyberbullying, cyber fraud, online exploitation, and extremist propaganda.

Moreover, the family's preventive role must be understood not in isolation but as part of a **collective social responsibility**. Cybercrime prevention requires synergy between families, educational institutions, government authorities, civil society organizations, and international bodies. Schools and universities must integrate **digital literacy and cyber awareness** into their curricula, equipping younger generations with critical thinking skills to assess online content. Governments must provide effective legal frameworks, ensure law enforcement agencies are trained in advanced technologies, and strengthen international cooperation to combat cross-border cybercrimes.

Another important implication of this research is that the **family must adapt to the dynamics of technological change**. Traditional parenting and supervision methods are insufficient in an environment where children can access vast and often unregulated digital spaces. Parents must therefore embrace technology themselves, understand the mechanics of social media platforms, and make use of available digital tools to monitor, guide,

and protect their children without undermining trust or autonomy. This balance of oversight and empowerment is vital for preparing responsible digital citizens.

From a policy perspective, strengthening the role of the family in cybercrime prevention involves the development of **structured support systems**. These may include public awareness campaigns, parental training programs, and community-based initiatives designed to help families acquire the necessary skills to safeguard their members. Religious and cultural institutions also have a complementary role in reinforcing moral values and fostering resilience against harmful digital influences.

In conclusion, preventing cybercrime is not the responsibility of law enforcement agencies alone; rather, it is a **multidimensional and collaborative effort**. The family stands at the forefront of this effort, acting as both a **source of protection** and a **generator of positive social values**. A society that invests in strong families—families that are educated, supportive, and technologically competent—will be better equipped to withstand the growing threats of the digital age. Strengthening family roles in cybercrime prevention is therefore not only a social necessity but also a **strategic imperative** for achieving security, stability, and sustainable development in the modern information society.

Acknowledgments

The author expresses deep gratitude to the **Faculty of Law and Political Science, University of Dr. Yahia Farès, Médéa**, for academic support. Appreciation is also extended to colleagues in criminal law and criminology for their constructive feedback.

Ethical Considerations

This research adheres to principles of **academic integrity** and **ethical responsibility**. No personal or confidential data were collected, and the study relies solely on publicly available sources. Proper attribution and citation of all scholarly works have been ensured.

Conflict of Interest

The author declares **no conflict of interest** regarding the publication of this article.

References

1. Ahmed Mohamed, J. (1980). *Towards Islamic education*. Tihama Publishing.
2. Al-Bashri, M. (2005). *Investigating computer crimes*. Dar Al-Fikr Al-Jami'i.
3. Al-Hamdan, M. (2017). *Cybercrimes and their combating*. Retrieved from https://www.mawdooe.com
4. Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials*. Sybex.
5. Dierch, S. (2017). *Types of cybercrimes and measures to combat them*. Retrieved from https://www.mawdooe.com
6. Hijazi, A. (2002). *Criminal evidence and forgery in computer and internet crimes*. Dar Al-Kutub Al-Qanuniyya.
7. Hijazi, A. (2009). *Islamic media between reality and aspiration*. Dar Al-Ma'rifa.
8. Huri, A. (2003). *Crime: Its causes and combating – A comparative study in Sharia, law, and social sciences*. Dar.
9. Jamel, A. M. (2005). *Nahwa Tarbiyah Islamiyah* [Towards Islamic education]. Dar Al-Fikr Al-Arabi.
10. Law No. 09-04 on preventing and combating crimes related to information and communication technologies. (2009). *Official Gazette of the People's Democratic Republic of Algeria, No. 47*.
11. Qashqoush, H. (1992). *Electronic computer crimes in comparative legislation*. Dar Al-Nahda Al-Arabiyya.
12. Radwan, M. (2001). *Youth's sexual and emotional problems in the light of Islamic Sharia*. Dar Al-Fikr.
13. The Holy Quran. (n.d.). Surah At-Tahrim, Verse 6.

14. Al-Shehri, F. (2019). Cybercrime in Arab legislation: A comparative legal analysis. *Arab Law Quarterly, 33*(2), 157–182. https://doi.org/10.1163/15730255-12324036
15. Bada, A., & Sasse, M. A. (2015). Cyber security awareness campaigns: Why do they fail to change behavior? *arXiv preprint arXiv:1505.02031*.
16. Chawki, M. (2009). The global fight against cybercrime: International cooperation between law enforcement agencies. *Journal of Information Law and Technology, 2009*(1), 1–15.
17. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589
18. Easttom, C. (2018). *System forensics, investigation, and response* (3rd ed.). Jones & Bartlett Learning.
19. Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.
20. Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies, 10*(2), 243–249. https://doi.org/10.1177/096466390101000204
21. Hinduja, S., & Patchin, J. W. (2014). Cyberbullying: Identification, prevention, and response. *Cyberbullying Research Center*.
22. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensics: An introduction*. Routledge.
23. International Telecommunication Union. (2020). *Global cybersecurity index 2020*. Geneva: ITU Publications.
24. Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Prentice Hall.
25. Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). Wiley-Blackwell.
26. McQuade, S. C. (2006). *Understanding and managing cybercrime*. Pearson Prentice Hall.
27. Smith, R. G., Grabosky, P. N., & Urbas, G. (2004). *Cyber criminal justice: Policing and prosecuting cybercrime*. Cambridge University Press.
28. Wall, D. S. (2017). *Cybercrime: The transformation of crime in the information age* (2nd ed.). Polity Press.
29. Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). Sage Publications.
30. United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. Vienna: UNODC.
31. Whitty, M. T., & Buchanan, T. (2016). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking, 19*(3), 151–155. https://doi.org/10.1089/cyber.2014.0406
32. Wolak, J., Finkelhor, D., & Mitchell, K. J. (2012). Child pornography: Patterns from the online victimization of youth study. *Sexual Abuse, 24*(4), 313–331. https://doi.org/10.1177/1079063212443607
33. Zedner, L. (2004). *Criminal justice*. Oxford University Press.
34. Zhuang, R., & Thomas, R. C. (2021). Cybercrime prevention: The role of family, education, and community. *Journal of Cyber Policy, 6*(2), 155–174. https://doi.org/10.1080/23738871.2021.1905953
35. Zuccato, A. (2007). Holistic security management framework applied in electronic government. *Computer Law & Security Review, 23*(2), 148–156. https://doi.org/10.1016/j.clsr.2007.01.008