Asian Crime and Society Review

Original Research Article

Received: 23 September 2024 **Revised:** 12 November 2024 **Accepted:** 12 November 2024

COMPUTER CRIME: FORMS AND IMPACT OF VICTIMIZATION

Trynh PHORAKSA[1] and Samanan RATTANASIRIVILAI[2*]

1 Faculty of Social Sciences and Humanities, Mahidol University, Thailand; trynh.p@gmail.com

2 Graduate School, Suan Sunandha Rajabhat University, Thailand; samanan.ra@ssru.ac.th (Corresponding Author)

Handling Editor:
Professor Dr.Christian KAUNERT Dublin City University, Ireland
(This article belongs to the Theme 1: Law, Crime & Justice in the Age of AI)

Reviewers:
1) Professor Dr.Attapol KUANLIANG Midwestern State University, USA.
2) Professor Police Major General Dr.Patchara SINLOYMA RPCA, Thailand
3) Associate Professor Police Lieutenant Colonel Dr.Patchara SANTAD RPCA, Thailand

Abstract

Computer crimes are illegal acts committed using computers or electronic devices connected to a network. This research was conducted using a qualitative methodology with two main objectives: (1) to study the forms of computer crime that have occurred in Thai society and (2) to examine the impact of being a victim of computer crime. The key informants for this research were 15 police officers from the Metropolitan Police Bureau, Royal Thai Police who had experienced computer crime themselves. The research tool used was a semi-structured interview. Data were validated through triangulation and analyzed using content analysis. The research findings revealed that the main forms of computer crime in Thai society included email fraud, online sales scams, romance scams, investment fraud, phone scams by call center gangs, and pyramid schemes. The impacts of being a victim of computer crime can be summarized into two main areas: psychological effects and social effects. Urgent guidelines for preventing and addressing computer crime include strengthening the protection of citizens' data by relevant agencies, clearly defining laws and penalties, and enhancing the authority of government officials to monitor and control violations of data security. Additionally, raising awareness and understanding of computer crime across all dimensions and promoting the use of technology with robust security measures are essential steps for the public.

Keywords: Computer Crime, Victimization, Police Officer

Citation Information: Phoraksa, T., & Rattanasirivilai, S. (2025). Computer Crime: Forms and Impact of Victimization. *Asian Crime and Society Review, 12*(1), Article 1. https://doi.org/10.14456/acsr.2025.1

Background and Significance of the Issue

The transition to a "new normal" lifestyle has not only increased public access to online goods and services but has also led criminals to increasingly adapt their fraud methods to online platforms. During the COVID-19 pandemic, in the range of 81% of global organizations reported an increase in cyber threats, with 79% experiencing operational disruptions (Dolezal, 2021). In Thailand, statistical data from the Technology Crime Suppression Division (TCSD) from 2018 to 2021 indicates that defamation was the most frequently reported computer crime, with 698 complaints filed in 2021, predominantly resulting from online harassment and defamatory social media posts. Due to the increased access to social media, resulting in a higher volume of harmful content being posted and shared, this has led to more victims. The approximate damages from defamation cases in 2021 reached an estimated 1.6 billion baht (SpringNews, 2022).

The second most prevalent crime was hacking in relation to data manipulation, theft, or destruction, with 585 reported cases and damages nearing 67 million baht. Ranked third were online sales scams, with 445 cases and an approximate financial loss of 45 million baht. From March to December 2022, the Thai Police Online portal received over 163,000 cybercrime reports, totaling 27.3 billion baht in damages. More than half of these complaints are related to international call center gangs, as well as other cybercrimes, for example, online fraud, data ransom, hacking, and online sexual harassment. In 2022, almost 120,000 phone numbers and 60,000 bank accounts were frozen in response to the surge in cybercrime incidents, highlighting an increase in cybercrime activities within the country, including efforts by police officers, the Ministry of Digital Economy and Society, and various agencies leading to the suppression of such crime channels. This could be seen that cybercrime has increased rapidly. However, the sectors that swiftly respond to combating cybercrime are the private sectors, while government agencies might lack sufficient cybersecurity skills (Phuriwikrai, 2020).

Based on the above circumstances, the research team is interested in studying cybercrimes in Thailand and examining their effects on police officers who become victims. The study also aims to explore appropriate responses when facing such incidents and to reduce the likelihood of fraud victimization in the future.

Literature Review

Computer Crime

Computer crime refers to illegal or criminal acts conducted within computer systems or using computers for unlawful activities. The computer systems in this context refers to computer networks and any devices connected to these networks as well. Computer-based or network-based crimes (such as those occurring online) may often be called "cybercrime." An individual committing such crimes is called a "cracker," which refers to an individual who illegally breaks into the computer systems of others to damage, steal, or misuse information.

Cybercrimes can be classified into two main categories:

1) The act involves using computers to gain personal gain from the victims, with the perpetrators gaining benefits in return.

2) The crime of using any form of technology as a tool to execute unlawful actions. In such incidents, officers' investigation to bring perpetrators to justice requires technological knowledge as well.

Cybercrime can be classified into nine main forms (Nakhon Pathom Rajabhat University, n.d.); 1) Internet data theft, which includes the theft of benefits through such unauthorized access; 2) Criminals utilize communication systems to conceal their illegal actions; 3) Unauthorized replication or imitation of software systems; 4) Using computers to disseminate obscene images, sounds, or unsuitable content; 5) Using computers for money laundering; 6) Attacking and disrupting public utility systems, such as water supply, electricity, or traffic management

systems; 7) Deceiving individuals into fraudulent trade or investment scams; 8) Unauthorized data alteration to secure a personal advantage; 9) Secretly using computers to transfer funds from others' accounts into personal accounts.

Crime Triangle Theory

The Crime Triangle Theory explains the components involved in the occurrence of a crime, consisting of three elements: the Criminal, the Target/ Victim, and the Opportunity. The Criminal refers to the individual with the intent or desire to commit a crime. The Target/Victim is the person, place, or object that the offender intends to act upon or aims to harm. Opportunity represents the suitable time or location that enables the offender to carry out the criminal act or offense.

The Crime Triangle Theory consists of three key components. Firstly, for the Criminal side, there must be offender control involving reducing the number of potential offenders by enforcing laws, such as arresting suspects under arrest warrants, implementing measures to control vice-related establishments or places that may foster criminal activity, and monitoring individuals recently released from penitentiary who enter the area.

The second part is Victim or Target, including victims or the public, who should protect themselves by gaining support from the community and police to provide knowledge and useful information to protect themselves from crimes, such as the criminals' tactics, avoiding displaying valuable jewelry or wearing enticing clothing.

Lastly, on the Opportunity side, preventing criminals from committing offenses requires removing opportunities by controlling environmental factors that may contribute to crime risks. For example, using technology to install CCTV cameras or lighting in high-risk areas can reduce the chances of crime (Cullen & Wilcox, 2010).

Since crime occurs when all three elements are present, this theory suggests that crime prevention is the effort to eliminate at least one side of the triangle, thereby reducing the likelihood of criminal acts.

Forms of Computer Crime in Foreign Countries

In the United States, it was found that the top five forms of computer crime in 2020 were as follows: 1) Phishing attacks; 2) Non-Payment/Non-Delivery fraud; 3) Data breaches involving unauthorized access to personal information; 4) Identity theft (Extortion); and 5) Cyber extortion (Internet Crime Complaint Center, 2020).

In Nigeria, Ayub and Akor (2022) studied the trends, forms, and impacts of computer crime in the country using secondary data from the Nigerian Police and the Economic and Financial Crimes Commission (EFCC). The Nigerian government has attempted to tackle computer crime issues by enacting and enforcing the Cybercrime Act (Prohibition, Prevention, etc.) of 2015. Nevertheless, the constant evolution of computer crime tactics has limited the effectiveness of apprehending cybercriminals.

In Bangladesh, Shahjahan and Miah (2023) studied the forms of computer crime committed by juveniles in the country using a cross-sectional study from a sample of 167 individuals, with data collected through semi-structured questionnaires. The findings indicated that hacking was the prevalent form of computer crime among adolescents. The main factors contributing to these crimes included weak legal frameworks, flawed socialization, peer influence, easy internet access, corruption, unemployment, and poverty. Moreover, most youths used password-cracking programs, with techniques such as key loggers, network sniffers, exploiting vulnerabilities, vulnerability scanners, and port scanners. To solve computer crime, government, and private sectors should collaborate to update existing laws to control this type of crime effectively.

Methodology

Documentary Study

The documentary method is the study of books, journals, and various documents both in Thailand and abroad. It also includes research, theses, news, and newspapers that contain content related to the forms of computer crimes in Thailand.

In-Depth Interview

The interviewees in this research were 15 police officers who had been victims of computer crimes, affiliated with the Metropolitan Police Bureau, Royal Thai Police.

Research Instruments

The researcher conducted a semi-structured interview that took approximately 45 minutes and involved open-ended questions that were flexible, similar to everyday conversations.

Data Validation

Data triangulation refers to the validation of data from three sources including 1) data from books, journals, related documents in both Thai and foreign languages, research and theses 2) data from personnel in the criminal justice process related to computer crimes, and 3) data from documents obtained from inquiries, notes and audio recordings of conversations (if permitted).

Human Research Ethics Review

The researcher has received human research ethics approval from the Human Research Ethics Committee in Social Sciences, Faculty of Social Sciences and Humanities, Mahidol University.

Results

The Forms of Computer Crimes in Thai Society

The forms of computer crimes that occur in Thai society can be summarized as follows: email scams, Sales scams, Romance scams, Hybrid scams, Phishing or Voice Phishing by call center gangs, and Ponzi schemes.

The Effects of Being a Victim of Computer Crime

According to the results, the effects of being a victim of computer crime can be summarized into 2 main areas: psychological effects - victims felt stressed, anxious, and paranoid in daily life, and social effects - victims were absent from work, resulting in loss of income and property, and felt embarrassed in front of the public and their police colleagues.

Discussions

The forms of computer crimes that occur in Thai society can be divided into 6 main forms.

1) Email Scams occur when criminals deceive victims through SMS or fake emails that appear to be from a well-known source. They usually claim that the victims won a lottery, received a donation, or received a large inheritance. They also invite the victims to work with them by only clicking the link sent by them. The scammers want the most to trick the victims into filling in their personal information on a fake website or replying to a fake email with their private data.

2) Sales Scams occur when criminals deceive victims into buying or selling products online. The victims are required to transfer money for products or services. However, the criminals do not send any products to them or send products that are not what the victims ordered or that are not up to standard.

3) Romance Scams involve criminals deceiving victims into falling in love by creating fake profiles that make them look attractive, rich, and trustworthy. The criminals talk and build a relationship with the victims over time. When the victims fall in love or trust that they really love them, the criminals trick them into transferring money or assets to them. In some cases, the victims may be tricked into transporting drugs or illegal items on behalf of the criminals.

4) A Hybrid Scam is similar to a romance scam, but the victims will be deceived and driven by their own greed for money. The criminals will create fake profiles as investors with much

money and assets. Later, they will invite the victims to be business partners and trick them into investing with high returns. If the victims are reckless and greedy, without considering that "Nothing comes easy. Otherwise, everyone in the country would be rich by now," they will be tricked into investing continuously, gradually increasing money for investment. Their money will be invested through fake websites created by the criminals. In addition, they may use a famous politician or businessman's name to assure them, and in the end, the victims will be tricked until they lose everything.

5) Vishing or Voice Phishing is when criminals form call center gangs and try to invent a situation and prey on the victims' emotions. They often impersonate government officials or agencies, claiming that the victims are involved in illegal activities, that their bank accounts have been used to launder money, or that their parcels have illegal items found in shipping services or have smuggled goods. Subsequently, when the victims are so scared and shocked that they are not in their right senses, the criminals will trick the victims into giving their personal information or transferring their money to prove their innocence.

6) The Ponzi Scheme has evolved into a more modern and convincing scheme in the form of applications and websites. The criminals entice the victims to become new investors with high short-term rates of return. In the beginning, the victims will get returns on their investment. However, as the membership pool expanded, they finally did not get the returns as claimed, and the criminals fled with the victims' funds.

The Effects of Being a Victim of Computer Crime

The effects of being a victim of computer crime can be divided into 2 types, including psychological effects and social effects. For psychological effects, the victims felt stressed, anxious, and paranoid in daily life. In agreement with Ahe (2022), victims of computer crime suffer from mental health problems and financial loss, which can sometimes lead to suicide and other forms of depression. It has also been found that computer crime victims tend to have a high risk of mental illness, and they do not get mental health care services from the government. Moreover, computer crime laws are not very effective.

In terms of social effects, the victims were absent from work, resulting in loss of income and property, and felt embarrassed in front of the public and their police colleagues. This is consistent with the study of Cybercrime: Case Study of Factors Affecting Electronic Banking by Sucharajit et al. (2018). The study results showed that computer crimes seriously threaten electronic banking systems. In addition to financial loss, it damages the credibility of electronic banking systems, banks, and users' confidence in using electronic banking services. Besides, police officers who had been victims of computer crimes felt embarrassed and ashamed. This may affect public confidence and trust in the police since the police have a duty to prevent and stop crimes. However, in this case, the police become victims, resulting in social effects - the lack of trust in the police duties and responsibilities.

Urgent Recommendations to Prevent and Solve Computer Crime Problems

Based on the forms of computer crimes and the effects of becoming a victim of computer crime, relevant agencies and sectors should take action according to the following recommendations:

1) Enhancing data security systems to protect citizens' identity information: Relevant government agencies should improve protection measures such as access control systems, encryption, and monitoring to prevent unauthorized access to information.

2) Imposing clear laws and penalties: Strict regulations and enforcement can prevent and reduce computer crimes, such as the penalty for unauthorized access to personal information and the penalty for attacking computer systems.

3) Strengthening authority: Government officials should have the authority and capability to investigate and take action on sensitive data breaches, i.e., investigating data breach-related cases.

4) Educating the public: Raising awareness and improving the understanding of computer crime, such as learning about online scams, can help reduce the chances of becoming a victim.
5) Promoting the use of computer security technologies: The use of technologies with good security measures should be supported, such as antivirus software, intrusion detection tools, and cloud services that have security measures.
6) Developing international cooperation: Computer crime is considered an international problem. International cooperation is vital to effectively prevent and solve computer crime problems.

References

Ahe, L. (2022). *Mental Wellbeing and Cybercrime: The Psychological Impact of Cybercrime on Victims*. Retrieved from http://essay.utwente.nl/91014/4/vonderAhe_BA_BMS.pdf.

Ayub, A., & Akor, L. (2022). Trends, Patterns and Consequences of Cybercrime in Nigeria. *Gusau International Journal of Management and Social Sciences, 5*(1), 241-262.

Cullen, F., & Wilcox, P. (eds.). (2010). *Encyclopedia of Criminological Theory*. California: SAGE Publishing.

Dolezal, A. (2021). *Cyber Threats Have Increased 81% Since Global Pandemic*. Retrieved from www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic.

Internet Crime Complaint Center. (2020). *2020 Internet Crime Report*. Retrieved from www.ic3.gov/AnnualReport/Reports/2020_IC3Report.pdf.

Nakhon Pathom Rajabhat University. (n.d.). *Law and Computer Ethics*. Retrieved from https://pws.npru.ac.th/signal/data/files/Chapter3_Law.pdf.

Phuriwikrai, K. (2020). *Cybercrime: A Challenging Problem for ASEAN in the 21st Century*. Retrieved from www.the101.world/cybercrime-in-21st-century/.

Shahjahan, M., & Miah, A. (2023). Pattern of Cybercrime among Adolescents: An Exploratory Study. *International Journal of Information Security and Cybercrime, 12*(2), 43-48.

SpringNews. (2022). *Police Technology Crime Suppression Division Releases CyberCrime statistics for 2021 and Trends for This Year*. Retrieved from www.springnews.co.th/spring-life/819659.

Sucharajit, W., Ketchaya, S., & Kulnides, N. (2018). *Cyber Crime: Case Study of Factors Affecting Electronic Banking*. Retrieved from www.journalgrad.ssru.ac.th /index.php/miniconference/article/view/1646.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.