FACTORS INFLUENCING CYBERCRIMES OF SOCIAL MEDIA USERS IN NONTHABURI PROVINCE

Thawat Sairahu[*], Koblap Areesrisom[**], Krittapol Thongdonpum[***]
Division of Resources Management and Development,
Faculty of Agricultural Production, Maejo University, Chiangmai, Thailand 50290

Introduction
Statement and Significance of the Problem

Nowadays, the use of social media is an important communication channel along with people daily life. Both in communication between people and communication between organizations. peoples use social media to chat, search for information, transact and buy goods. This can be done anytime, anywhere via the Internet. As a result, various agencies and organizations have changed their operational guidelines to be in line with the arrival of this social media . however found that most social media users Often met with ill-wishers who come to deceive, steal various data to be used in illegal ways, leading to cybercrime, which is one of the major crimes that occur to users . Social media jobs in Thailand the nature of cybercrime is partly due to the carelessness of users themselves, such as revealing passwords to others. Trusting strangers who communicate through social media, unauthorized access to information having curious behavior exposing vulnerabilities that allow criminals to gain access to personal information and not knowing and not understanding cyber threats, etc.

Cybercrime is a crime that anyone can fall victim to and impact on life well-being of the people at large scale. (DSI's Bureau of Development and Logistics, 2021). Due to crime patterns that use modern technology, computers, internet networks. and electronic devices as a means of misconduct (UNODC , 2019) . The increase in cybercrime is due to several factors. But the noteworthy point is Cybercrimes exploiting the COVID-19 crisis It's not just individual cybercriminals. But it is likely that organized crime has expanded and adapted to the cybercrime scene (Radoini , 2020 ; Marelli, 2020 ; Ahmed, 2020 ; Thailand Institute of Justice , 2020 ; Zivotic & Trajkovski, 2020). that engages in cybercrime. greater personnel capacity and capital to commit crimes In addition, cybercrime organizations also have transnational forms of crime. Therefore, it is likely to cause more damage to the people and the economy and it should be foreseen that Thailand will also be affected by the same problem with crime. It is a chronic problem and has been close to Thai society for a long time. At present, the various crimes that surround people in society There are causes and factors of the likelihood of committing a crime. and intensified more and more violence affecting the safety of people's lives and property who were the victims of many crimes

Thai society has stepped into a society affected by innovation. The invention modern technology and internet system which has a positive impact and contributes to the people's livelihoods more on the other side of modern technology that has been created to meet the needs of people beings better. It is indeed a double-edged sword that hides a dark side, that can be used in illegal and immoral ways of the country not only negatively affecting the victims, but also creates a wide-ranging impact on society and the safety of people's lives and property. This has resulted in a modern crime problem whose form has evolved to become more complex and difficult to study the problem and preventive measures. especially cybercrime which is an important problem for the safety of life and property of the people, society and national security cybercrime that is special and has developed a more complex model, approach and method. Cybercrime rate in Thailand has been rising. The rate of occurrence during the year 2021 from January to December. Number of 135 events, as for the

rate of "cyber threats" in 2022 from January to December. There were a total of 772 incidents, which increased more than 3 times because it was a new type of crime that had not yet been discovered and could not be analyzed for prevention and suppression methods. For this reason, collaboration in the form of Collaborative Networks is required from other relevant agencies that are responsible for oversight and responsibility. Thailand's cybercrime problem come together to create a network of cooperation between various agencies together to design ideas and exchange useful information about the context of the crime problem and use those opinions to formulate policies . Measures and guidelines for the prevention and suppression of cybercrime more efficiently by Nonthaburi Province Classified as a province that is the metropolitan area of Bangkok and has the highest density of people living in the area and latent population 2nd place after Bangkok. And from the physical characteristics of Nonthaburi Province, there are areas that are prosperous in education, economy, society, transportation, industry and important technologies close to Bangkok .These developments have creeped up and led to channels and opportunities that are vulnerable to cybercrime. Especially in cases of fraud through online financial transactions which has a tendency to increase within the area of Nonthaburi province undeniably and still cannot find a way or guidelines for management and correction It is imperative to urgently study the factors contributing to the rapid increase in cybercrime in order to find further protection.

Research Question

From problems that arise rapidly and intensify The researcher is therefore interested in what

1）What are the basic characteristics of social media users in Nonthaburi? influencing the rate of cybercrime

2）What is the behavior of social media users in Nonthaburi Province that influences the cybercrime rate?

3）What is the knowledge and understanding of cybercrime of social media users in Nonthaburi Province that influences the cybercrime rate?

Research Objective

1) To study personal information of social media users in Nonthaburi Province influencing the rate of cybercrime

2) To study the behavior of social media users in Nonthaburi Province influencing the rate of cybercrime

3) To analyze the level of knowledge and understanding of cybercrime of social media users in Nonthaburi province that influences the cybercrime rate.

Research Hypothesis

This research formulated a hypothesis based on 6 related theoretical frameworks as follows:

1. Personal data affects the behavior of social media users differently.
2. Personal data affects our understanding of cybercrime differently.
3. Personal data results in different cybercrime rates
4. How Social Media User Behavior Influences Cybercrime Cognition
5. How Social Media User Behavior Influences Cyber Crime Rates
6. Cybercrime Awareness Influences Cybercrime Rates

Scope of the Study

The method of conducting research in this research uses a mixed method that consists of Quantitative Research in conjunction with Qualitative Research , with details as follows

population boundary

1) Population, sample group, quantitative

(1) Population includes people who use services on social media in Nonthaburi Province without limiting personal factors

(2) The sample group is users of social media services in Nonthaburi Province without limiting personal factors by randomly selecting 400 people/sample from the Office of Civil Registration, Department of Provincial Administration, 2022, Nonthaburi Province, with a population of 1,288,637 people. By using the method from calculating the sample size with the formula of Yamane (1973) with a confidence level of 95% and a margin of error of 0.05, with a sample size of 400 samples. The researcher selected the sample group by random method. (Accidental Sampling) by defining the proportion as Nonthaburi City 113 people, Bang Krai District 46 people, Bang Yai District 38 people, Bang Bua Thong District 87 people, Sai Noi District 38 people and Pak Kret District 78 people.

2) Population and qualitative samples

to give insights from the interview, including 10 experts with specific qualifications, consisting of two teachers in cybersecurity-related subjects, two researchers and academics involved in the use of electronic media and social media, three cybercrime-related law enforcement officers . and 3 online business operators. All 10 key informants must have at least 5 years of work experience in the specified line of work

This research aims to study and analyze factors influencing the cybercrime rate of social media users. The scope of the population is social media users in Nonthaburi Province. And analyzing the relationship of 4 factors: 1) personal information about gender, age, occupation, religion, status, highest level of education. and average monthly income. 2) Behavior of social media users, including expressions on social media. Activities on social media Choosing the time to access social media and trading of goods and services via social media. 3) Knowledge and understanding of cybercrime, namely knowledge and understanding of computer use Knowledge and understanding of using social media knowledge and understanding of computer networks and the Internet knowledge and understanding of digital technology and understanding of cyber law ; and 4) the cybercrime rate of related to hacking Data capture, malware attacks ransom attack Social media fraud and scams; and Unauthorized access to information and for in-depth interviews will cover comments on relevant issues Open-ended questions to express opinions about the current use of social media by Thai people. Commenting on the current cybercrime happening in Thailand. Describe the privacy factors that influence and contribute to the cybercrime of social media users in Nonthaburi Province Explain about social media user behavioral factors that influence and contribute to the cybercrime of social media users in Nonthaburi Province explains about cognitive factors in cybercrime that influence and contribute to the cybercrime of social media users in Nonthaburi Province Additional comments and suggestions on Factors influencing cybercrime of social media users in Nonthaburi Province which will bring all comments to be processed and explained together with the results from the questionnaire responses

Significance of the study

Expected benefits from research policy benefits Administrative benefits and academic benefits

Policy The findings of the research will be proposed to determine the role of the government in preventing cybercrime for security purposes. economic and social create legal measures Including supervision to create safety for the public. in which people can lead a normal life

Administrative The results of the research are important information to provide social media users. became more aware and cautious

Academic The research findings should be expanded to include additional variables that affect the occurrence of crime. Because when the situation changes, the causal factors will change.

Definition of term

Expressions on social media Refers to the user's behavior or reaction to social media media, including reading (Read) or visiting (View) , liking (Like). Writing text (Post) , commenting sharing (Share), labeling (Tag) Conversation (Chat) and follow-up

Choosing to use social media Refer to the user chooses to use social media according to your skills and preferences. The most popular social media include Facebook. ,Twitter, YouTube Instagram), Line and webboards

Using communication tools to connect to social media Refers to the use of social media by users through various communication tools, which include Computers, mobile phones, tablets and other electronic devices.

Activities on social media Refers to the forms of activities that Users take and interact with via social media, including conversations, status updates (information, pictures, and Others) Recreation such as playing games, listening to music, watching movies, searching for information and exchanging information. electronic transactions and business operations

Choosing the time to access social media Refers to the most appropriate time for users to access social media, divided into 4 periods: 00.01-06.00 hrs., 06.01-12.00 hrs., 12.01-18.00 hrs. and 18.01 hrs. -24.00

Knowledge of malware attacks means knowledge, skills and experience about various malicious programs known as malware The malware works in a way that attacks the system. system damage Including data theft, malware can be divided into various types such as Virus (Virus) Worm or Internet Worm (Worm) Trojan Horse (Trojan Horse) secretly intercepting information (Spyware) , key logger (Key Logger) , as well as data stealing programs (Cookie) and embedded Malicious Mobile Code (MMC) through various vulnerabilities.

Understanding of cheating and scams on social media Means knowledge, skills andExperiences about the dangers of ill-wishers who try to deceive, talk, persuade, defraud and deceive the victims.to do something unprofitable, such as transferring money, sending photos or sending personal information to criminals; and Criminals take those information for further use.

Knowledge of hacking systems means knowledge, skill and experience relating to hacking into computer programs illegally This is a password protected system. But there are people who do not wish to hack into the system without permission.

Knowledge of data capture Refers to knowledge, skills, and experience with data capture programs. on computer network Because computer networks are shared communication systems. The bad guys can get information from one computer sent to another computer. by capturing data that runs between networks

Knowledge of ransom attacks Refers to knowledge, skill and experience in relation to ransom demands on the Internet. by those who do not wish to access the information of the victim and encrypt those data until it cannot be used And will demand a ransom in which the victim pays to decrypt the encrypted data.

Knowledge of unauthorized access to information Refers to knowledge, skills and experience relating to hacking into personal data. Or sneak into the system that the owner does not allow access.

Cybercrime means data capture malware attack ransom attack Social media fraud and scams; and Unauthorized access to information
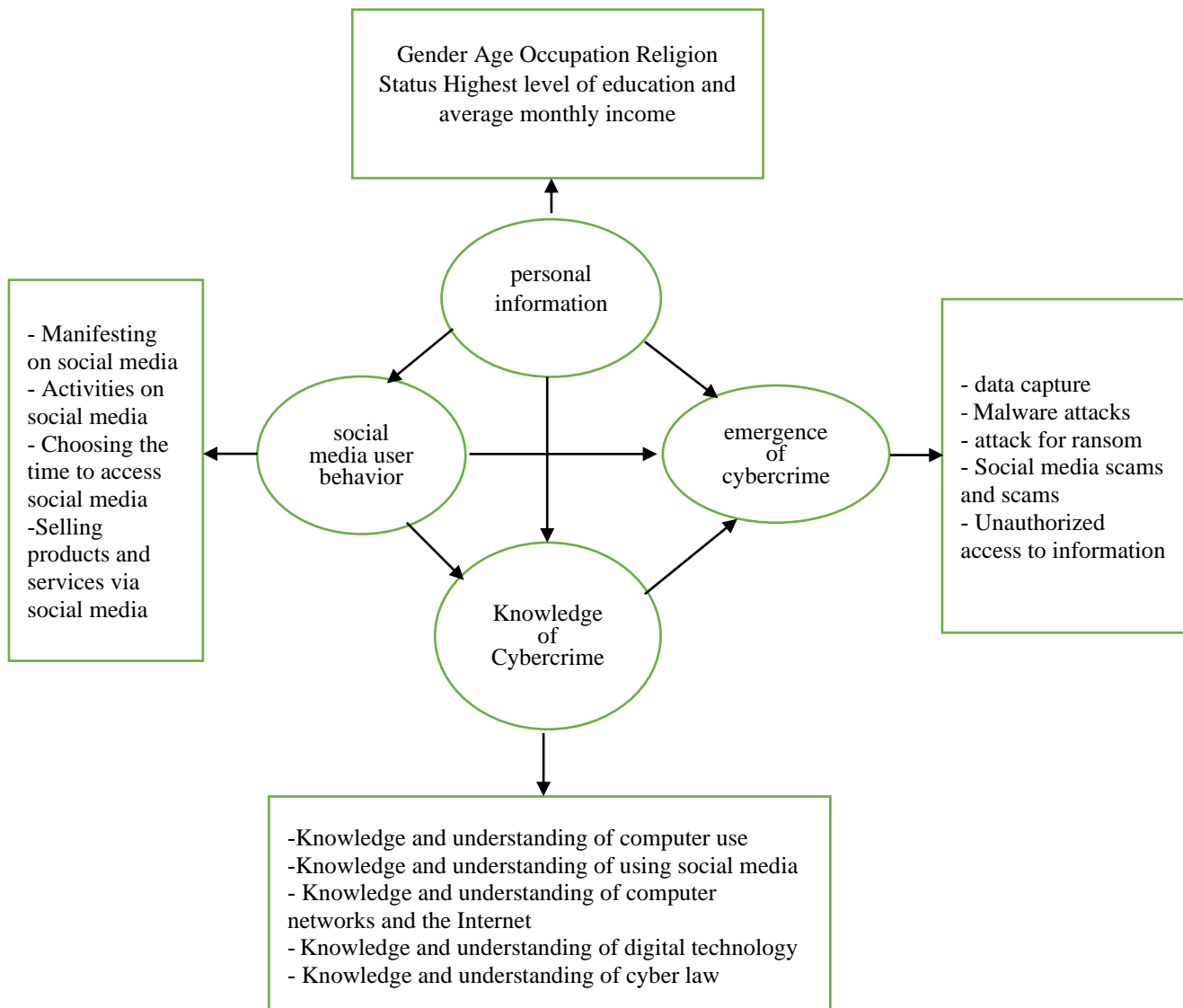
Theoretical Concept

subject research Factors Influencing Cyber Crimes of Social Media Users in Nonthaburi Province The researcher has studied the following theoretical concepts.

1. The concept of development management
2. The concept of human resource development
3. Theoretical concepts about social media user behavior
4. Computer Crime
5. Protection Motivation Theory
6. Cybersecurity Act 2019
7. Theoretical concepts of demographics
8. Concepts and theories about development management
9. The concept of perception theory
10. Behavioral theory concepts
11. Cybercrime Threat Management Concepts
12. The concept of crime and crime prevention The concept of cybercrime threats.
13. The concept of national security
14. Related research The concept of government roles
15. Conceptual Framework

Conceptual Framework

conceptual framework for research It has been determined according to the research hypothesis and the structural equation is shown in the figure.

Bibliography

Albladi , SM and Weir, GRS (2016). Vulnerability to Social Engineering in Social Networks: A Proposed User-Centric Framework. IEEE International Conference on Cybercrime and Computer Forensic (ICCCF).

Chena, R. and Sharma, SK (2013). Understanding Member Use of Social Network-working Sites from a Risk Perspective. Procedia Technology 9 (2013), 331-339.

Department of Administrative Affairs. (2018). Population statistics of Thailand. The Bureau of Registration Administration, Department of Administrative Affairs. (In Thai).

Hadlington , L. and Chivers , S. (2018). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. Journal of Policy and Practice

Hootsuite. (2018). Social Media Management Platform in Thailand 2018. Social Media and Marketing Solutions.

Keardsri, W., Meethongjan, K. and Kulnides, N. (2 0 1 8). A Survey of the Variables Influencing Cybercrime among Social Media Users in Thailand. SSRU Graduate School Mini-Conference 2018. (In Thai).

Leukfeldt, R. (2 0 1 7). Research agenda the people factor in cybercrime and cybersecurity. Eleven International Publishing.

Riek, M. and Bohme, R. (2 0 1 4). Understanding the influence of cybercrime risk on the e-service adoption of European Internet users. 13th Annual Workshop on the Economic of Information Security.

Smitherson , D. (2012). Impact of Cyber Crime and Security on Social Media. Social Media Today.

Wayuparb, S. (2 0 1 8). Thailand Internet User Profile 2 0 1 8. Electronic Transactions Development Agency Publication. (In Thai).

Yamane, T. (1973). Statistics: An Introductory Analysis. Third Edition, New York Harper and Row Publication