# The Challenge of Digital Citizenship for Youth in Cybercrimes
# ความท้าทายของการเป็นพลเมืองดิจิทัลสำหรับเยาวชนในอาชญากรรมไซเบอร์

**Kanchana Meesilapavikkai[1*]**
**กาญจนา มีศิลปวิกกัย**

[1] School of Communication Arts, Sripatum University
คณะนิเทศศาสตร์ มหาวิทยาลัยศรีปทุม
* Corresponding author e-mail: kanchana.me@spu.ac.th

Received: 06/01/2023 Revised: 16/03/2023 Accepted: 27/03/2023

## Abstract

Today's world is surrounded by the enormous use of the Internet. This creates an opportunity to "learn" and at the same time "take risks" which arising from cyber, especially youth. Academics have been created and designed the special content of digital citizenship to help and protect them not to be "victims" of cybercriminals. Cybercrime takes many forms as cyber fraud, cyber gambling, cyber blackmail/extortion or even cyber murder. The challenge of digital citizenship for youth in cybercrimes, something to be aware of at all times: "situation control" are 1) Self-Apperception, 2) Digital Literacy (able to distinguish), 3) Social Awareness and 4) Self- Management, as a habit to create a cyber-savvy identity.

**Keywords:** Digital Citizenship, Cybercrime, Victim, Youth, Cyber-savvy Identity

## บทคัดย่อ

โลกปัจจุบันที่แวดล้อมไปด้วยการใช้อินเทอร์เน็ตอย่างมากมายมหาศาลของประชาชน ทำให้เกิดโอกาสในการ "เรียนรู้" และในขณะเดียวกันก็เกิด "ความเสี่ยง" ที่เกิดขึ้นจากไซเบอร์ โดยเฉพาะเยาวชน ความเป็น "พลเมืองดิจิทัล" ได้ถูกสร้างและออกแบบด้วยนักวิชาการหลากหลายท่านเพื่อช่วยและป้องกัน ไม่ให้ตกเป็น "เหยื่อ" ของอาชญากรไซเบอร์ อาชญากรรมไซเบอร์มีหลากหลายรูปแบบตั้งแต่การหลอกลวง การพนัน การขู่ว่าจะเปิดโปงความลับ จนกระทั่งถึงการฆาตกรรม ความท้าทายของพลเมืองดิจิทัลโดยเฉพาะเยาวชนในโลกไซเบอร์เป็นสิ่งที่ต้องตระหนักอยู่ตลอดเวลา คือ "การควบคุมสถานการณ์" ซึ่งประกอบด้วย 1) มีสติสัมปชัญญะ 2) รู้เท่าทันสื่อดิจิทัล 3) รู้บริบทของสังคม 4) สามารถจัดการทุกอย่างได้ เพื่อเป็นการสร้างตัวตนที่มีความสามารถ มีความรอบรู้เท่าทันในโลกไซเบอร์

**คำสำคัญ:** การเป็นพลเมืองดิจิทัล อาชญากรรมไซเบอร์ เหยื่อ เยาวชน ตัวตนที่เข้าใจโลกไซเบอร์

## 1. Introduction

There has been an increase in Internet use of young people; digital skills, levels of use, and combination of activities vary. They are surrounded by digital media delivered through different devices such as computers, smartphones, and tablets. However, the important issues are the increasingly individualized, privatized, and mobile.

Mbanaso and Dandaura (2015) mention about cyberspace is driven by information systems and the Internet transforming. The environment is in extraordinary ways by which people connect, interact and collaborate with one another. They also point that more and more cybercitizens globally will ultimately rely on the effective functioning of the Internet to survive and prosper with unremitting upsurge. An example of cyberspace is the home of Google, Yahoo and Facebook.

Nowadays, cybercrime is at an all-time high that its scope and number of its forms with no sign of declining. There are many different forms of cybercrime, all with severe impacts for the finances, mental health, and physical safety of people, and negative impacts for the economy and political orderliness of whole nations. Cyberattacks can spell the death of an organization. Consequently, several concerns have been raised about possible adverse effects of ICT. Digital citizenship for youth "do not fall victim" in cybercrimes is challenge.

## 2. Digital Citizenship

The world that has been transformed by digital technologies, makes young people effortlessly enabling connectedness through social media and access to vast quantities of information. How do they learn and face? Digital citizenship will make young people as citizens to engage and response effectively in the affairs of the community.

Ribble and Bailey (2007) mention about how technology influences the way students interact and the concept of digital citizenship in the classroom. They define nine elements of digital citizenship, which are Digital Access, Digital Commerce, Digital Communication, Digital Literacy, Digital Etiquette, Digital Law, Digital Rights and Responsibilities, Digital health and wellness, and Digital Security. They are related to technology usage inside and outside the school environment as in Table 1:

Table 1 Nine elements of digital citizenship

| Nine elements | | Concept |
|---|---|---|
| 1. | Digital Access | Digital divide: suitable alternatives for each student's needs |
| 2. | Digital Commerce | Tackle safety issues: various career and how e-commerce works |
| 3. | Digital Communication | Given a voice: empathy and appropriate reactions |
| 4. | Digital Literacy | Differentiate between real and fake content: lead a balanced life |
| 5. | Digital Etiquette | Digitally Fluent: positively online attitude |
| 6. | Digital Law | Need to know the law |
| 7. | Digital Rights and Responsibilities | Protection against cyberbullying |
| 8. | Digital Health and Wellness | Protect themselves: potential harm |
| 9. | Digital Security | Aware of potential malware attacks |

Although, Davis (2017) mentions in Proactive Knowledge "9 Key Ps" and Experience Knowledge in digital citizenship. Proactive Knowledge shows below:

1. *password*, as secure password
2. *private information*, as information identify a person
3. *personal information*, as call numbers, favorite food
4. *photographs*, as some private details may show up
5. *property,* as understand copyright
6. *permission*, as how to get permission for work they use
7. *protection*, as malware
8. *professionalism,* as skill to work problem out
9. *personal brand*, as what they share refer "Digital Tattoo"

He still mentions Experience Knowledge about truth or fiction, turn students into teachers, and collaborative learning communities.

Council of Europe (2022) defines digital citizenship as the ability to engage positively, to critic and compete in the digital environment, to draw on the skills of effective communication and creation, to practice forms of social participation. Respectful of human rights and dignity through the responsible use of technology are challenges.

Digital citizenship is skills and knowledge to guide youth to experience situation which they need to navigate the world today. A core competency of digital citizenship should address how to use technologies in an ethical, safe, and responsible way without restricting users from fully participating in and contributing to the knowledge society.

### 3. Cybercrimes

Cybercrime is any criminal activity involving a computer, networked device or a network. Most cybercrimes are carried out in order to generate profit for the cybercriminals, anyhow as some cybercrimes are carried out against computers or devices directly to damage or disable them (Brush et. al., 2022) Wikipedia (2022) shares the definition of cybercrime as it involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target which cybercrime may harm someone's security and financial health.

There are many different types of cybercrime which are carried out with the expectation of financial gain by the attackers, though the ways cybercriminals aim to get paid can vary. Some specific types of cybercrimes include Phishing, Identity Theft, Theft and sale of corporate data, Hacking, Cyber extortion and Cyber espionage (Pacific Prime Thailand, 2020).: which as in Table 2:

Table 2 Types of Cybercrime

| Types of Cybercrime | Examples |
|---|---|
| Phishing | As: sending fake emails to get personal information |
| Identity Theft | As: involving the misuse of personal information |
| Theft and Sale of Corporate Data | As: selling corporate data which not legal |

| Types of Cybercrime | Examples |
|---|---|
| Hacking | As: shutting down or misusing of websites or computer networks |
| Cyber Extortion | As: demanding money to prevent a threatened attack |
| Cyber Espionage | As: hackers access government or company data |

Anyhow, types of cybercrime can define in details as cyber fraud, cyber gambling, cyber (child) pornography, cyber prostitution, cyber impersonation, cyber blackmail/extortion, cyber harassment, cyber defamation, cyber malware, cyber illicit business/transaction, cyberjacking, cyber piracy/copyright, cyber terrorism, and cyber murder. Youth are surrounded by many types of cybercrime; how to learn and live, and how to protect and save themselves, are very challenge.

## 4. The Challenge of Digital Citizenship for Youth in Cybercrimes

There is a clear need for specific training on the risks related to ICT use. A core competency of digital citizenship should address how to use these technologies in an ethical, safe, and responsible way without restricting users from fully participating in and contributing to the knowledge society. The challenges, young digital citizens need to provide themselves with the knowledge, skills, attitude to take advantage of the opportunities and be springy in the face of risks. A careful balancing act, which recognizes children's online experiences is important to support children's capacity to cope themselves, thereby building resilience for digital citizens.

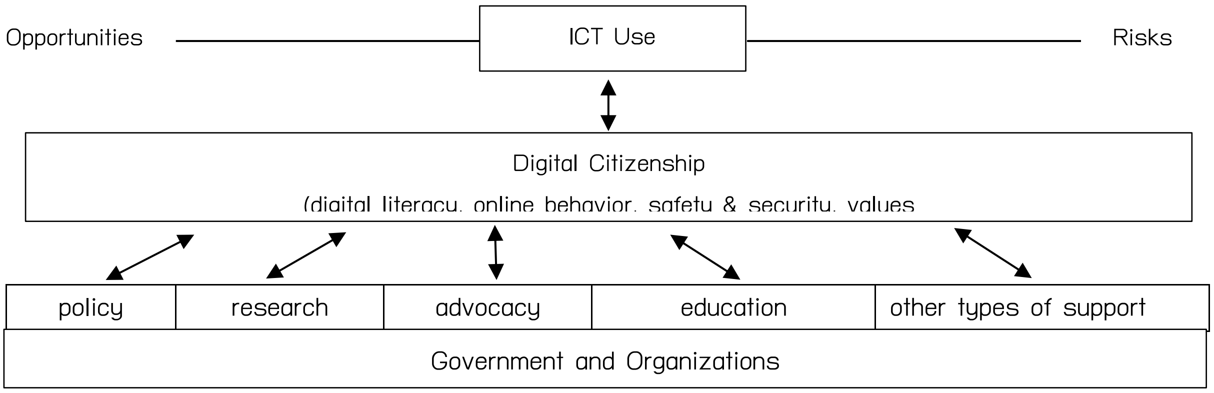


Figure 1 Guiding Framework for UNESCO' Mapping Exercise

Source: Tan, M.M., Park, J., Patravanich, S., and Cheong, J. (2014)

A group of experts and practitioners were gathered through this Guiding Framework, shown in Figure 1. Various key players in the Asia-Pacific region led to involve a desk review of online reports, studies, and other resources, to gather information about current digital citizenship and cyber wellness initiatives and programs.

The challenge for youth, not to be as a sufferer, in cybercrimes is very important. Digital citizenship, types of cybercrime, and the challenges for youth are related, see figure 2.

The digital citizenship provides an overview by creating "Cognition" the possibilities of the information technology world to the people involved, especially youth by developing knowledge and skills. From this article, I would like to use nine elements of digital citizenship (Ribble and Bailey, 2007) which are related to digital; as access, commerce, communication, literacy, etiquette, law, rights and responsibilities, health and wellness, and security.

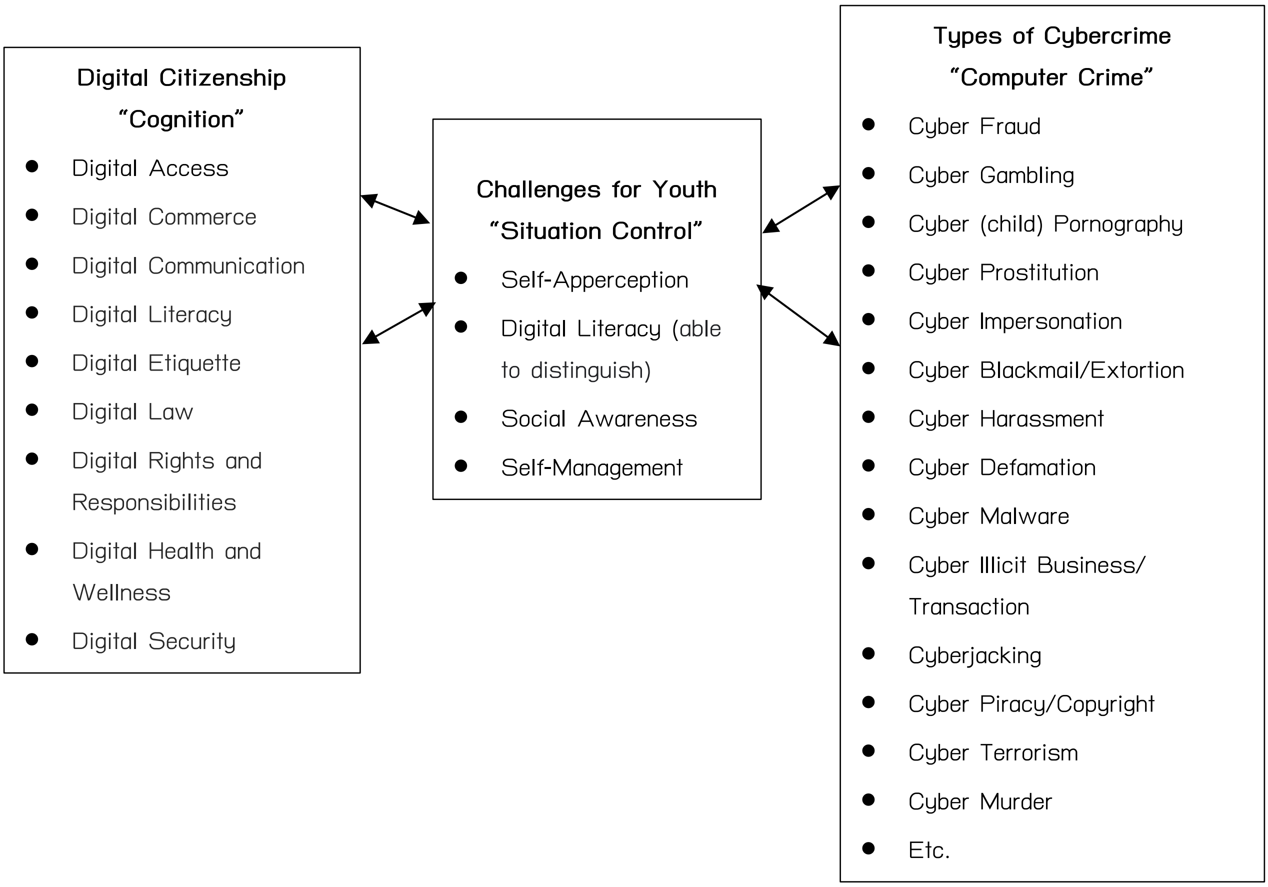
Cybercrime also known as "Computer crime," there are many types from the simplest to the more mysterious; such as fraud, gambling, pornography, prostitution, blackmail, jacking, copyright, murder etc. It is becoming increasingly diverse and frightening for children. Being a "victim" is "easy" and "possible" because the owner of the pitfall has ingeniously created a "path" to directly follow.

The challenge for cyber youth to be aware of when entering computers is to have the ability to: "Take control of the situation" themselves.

1) Self-apperception: Have apperception all the time; know what they are doing and what is displayed on the computer screen.

2) Digital literacy: Have the ability to distinguish what they see or perceive as being credible, true or false.

3) Social awareness: Understand the possibilities of society in order to assess what is seen or the situation from computer.



**Digital Citizenship**
**"Cognition"**

- Digital Access
- Digital Commerce
- Digital Communication
- Digital Literacy
- Digital Etiquette
- Digital Law
- Digital Rights and Responsibilities
- Digital Health and Wellness
- Digital Security

**Challenges for Youth**
**"Situation Control"**

- Self-Apperception
- Digital Literacy (able to distinguish)
- Social Awareness
- Self-Management

**Types of Cybercrime**
**"Computer Crime"**

- Cyber Fraud
- Cyber Gambling
- Cyber (child) Pornography
- Cyber Prostitution
- Cyber Impersonation
- Cyber Blackmail/Extortion
- Cyber Harassment
- Cyber Defamation
- Cyber Malware
- Cyber Illicit Business/ Transaction
- Cyberjacking
- Cyber Piracy/Copyright
- Cyber Terrorism
- Cyber Murder
- Etc.

Figure 2 Challenges of Digital Citizenship for Youth in Cybercrimes

4) Self-Management: Have the ability to deal with what is assessed as a whole from items 1-3. All skills and knowledge from digital citizenship must be fully applied.

Challenges are effective in cyberspace, when youth can create their own "Active" not "Passive" identity.

## 5. Conclusions and Recommendations

Overall, every country has laws to support cyber security for citizens. However, cybercrime still exists and tends to increase. With cybercriminals having expertise and a thorough understanding of computer systems, a crime game can be created to find the "victim" all the time. Youth are always "interesting" victims, with not much life experience and "optimism"

Today's world is changing rapidly. Youth use mobile phones as part of their lives. Therefore, from this article, computer can mean smart phones, which are more convenient to use for cyber access.

The challenge of digital citizenship for youth in cybercrimes; it is very important that youth need to be aware of and practice, "situation control" (figure 2) as a habit to create a cyber-savvy identity.

## 6. References

Adorjan M. & Ricciardelli R. (2019). *Cyber – risk and youth: Digital citizenship, privacy, and surveillance.* Routlrdge: Taylor & Francis Group

Brush, K., Rosencrance L., and Cobb M. (2022). *Cybercrime.* Available from URL: https://www.techtarget.com/searchsecurity/definition/cybercrime#:~:text=Cybercrime%20is%20any%20criminal%20activity,to%20damage%20or%20disable%20them.

Council of Europe. (2022). *Digital citizenship and digital citizenship education.* Available from URL: https://www.coe.int/en/web/digital-citizenship-education.

Davis V. (2017). *What your students really need to know about digital citizenship.* Available from URL: https://www.edutopia.org/blog/digital-citizenship-need-to-know-vicki-davis.

Ibrahim, S., Nnamani, D.I., and Okosun, O. (2021). Types of cybercrimes and approaches to detection. *IOSR Journal of Computer Enginerring (IOSR-JCE),* 23(5), 24-26.

Mbanaso, U. & Dandaura, E. (2015). *The cyberspace: Redefining a new world.* Available from URL: https://www.researchgate.net/publication/280101879_The_Cyberspace_Redefining_ANew_World.

Pacific Prime Thailand. (2020). *Cybercrime in Thailand: Current trends and solution.* Available from URL: https://www.pacificprime.co.th/blog/cybercrime-thailand-trends/.

Ribble M. and Bailey G.D. (2007). *Digital citizenship in schools.* International Society for Technology in Education.

Tan, M.M., Park, J., Patravanich, S., and Cheong, J. (2014). *Foster digital citizenship through safe and responsible use of ICT: A review of current status in Asia and the Pacific as of December 2014.* UNESCO Bangkok APEID- ICT in Education.

Wikipedia. (2022). *Cybercrime.* Available from URL: https://en.wikipedia.org/wiki/Cybercrime.

**ผู้เขียน**

**ผู้ช่วยศาสตราจารย์ ดร.กาญจนา มีศิลปวิกกัย**
อาจารย์ประจำ คณะนิเทศศาสตร์ มหาวิทยาลัยศรีปทุม

**การศึกษา:**

| | |
|---|---|
| ปริญญาตรี | บธ.บ. การโฆษณา |
| ปริญญาโท | นศ.ม. การโฆษณา |
| ปริญญาเอก | Ed.D. Higher Education Administration<br>(Administrative and Policy Studies) |