# Instal : Jurnal Komputer

**E-ISSN: 2808-683X**
**Edisi : Volume 16 Nomor 03 | 2024**

Available online at https://journalinstal.cattleyadf.org/index.php/Instal/index


# Information Technology Crime


**Amiruddin[1], M. Haziq Annabil[2], Rio Ananata Putra Panjaitan[3], Budi Hasiholan Sitanggang[4]**

[1]Universitas Muhammadiyah Sumatera Utara, [2,3,4]Univeristas Islam Negeri Sumatera Utara



**ARTICLEINFO**

***Keywords:***
IT crime, security, digital threats, technology



## ABSTRACT

Information technology crime, or cybercrime, has become a serious threat as technology develops and reliance on the internet increases. These crimes include various illegal acts such as data theft, privacy violations, and attacks on systems. To deal with these threats requires in-depth understanding and mitigation measures that include cybersecurity training, updated security policies, and the use of advanced technology. Cooperation between the public and private sectors is also important in building an effective defense strategy. Education and training in cybersecurity must be improved to prepare future generations to face these digital challenges.





***Corresponding Author:***
Amiruddin
Universitas Muhammadiyah Sumatera Utara
E-mail: amiruddin.spdi@umsu.ac.id


## INTRODUCTION

In the ever-growing digital era, information technology crime has become an increasingly greater threat. This includes various types of illegal acts that use technology and the internet as a means to violate privacy, steal information, damage systems, or even threaten national security. The background to this increase in information technology crime is very complex and involves various factors. One of them is the rapid development of technology, which provides opportunities for criminals to infiltrate the system more easily and without being detected. In addition, increasing dependence on technology makes us increasingly vulnerable to cyber attacks. Widespread internet use, the use of smart devices, and the need for digital connectivity increasingly open up opportunities for criminals to access our networks and steal important data.

With the passage of time and advances in technology, cyber crime has developed into various new types of crime with new operational methods [1]. Apart from that, the motives behind information technology crimes also vary. Some are motivated by financial gain, such as stealing credit card information or committing online fraud. There are also those who have political or ideological motives, using technology to spread messages or carry out

Pages : 192-197
Doi. 10.54209/jurnalinstall.v16i03.235

attacks against specific targets. No less worrying, cybercrime is also increasingly being carried out by organized criminal organizations that use technology to carry out various illegal acts, including money laundering and trading of illegal goods.

In this context, a deeper understanding of information technology crimes becomes very important. Only with a solid understanding of these threats can we take proactive steps to protect ourselves, our companies, and society at large from increasingly sophisticated and costly cyberattacks. Therefore, further research on information technology crime is critical in our efforts to face the challenges of this complex digital era.

Mitigation measures should include increasing awareness of cybersecurity at all levels, from individuals to large companies. This can be done through regular training, security policy updates, and the implementation of advanced security technologies such as data encryption, firewalls, and intrusion detection systems. Cooperation between the public and private sectors is also critical to building an effective defense strategy. The government can play a role by making strict regulations and supporting strict law enforcement against cybercriminals.

Additionally, companies should regularly conduct security audits to identify and close security gaps in their systems. The use of technology such as artificial intelligence and machine learning can help detect and respond to cyber threats more effectively and quickly. Thus, a holistic and coordinated approach in dealing with information technology crimes is the key to protecting digital assets and ensuring security in this digital era.

Knowledge about cybercrime and how to prevent it must be an integral part of education and training in the field of information technology. Curricula in schools and universities must include aspects of cybersecurity to prepare future generations to face this growing threat. With comprehensive and sustainable efforts, we can create a safer digital environment and avoid the detrimental impacts of information technology crime.

## METHODS

This research uses a Normative Juridical approach to analyze information technology crimes. The data collection technique in this research was carried out through literature study, which involves collecting, reviewing and analyzing relevant literature. Data sources include laws, government regulations, scientific journals, textbooks, and other publications related to information technology crimes. By using this method, the research aims to understand how to deal with crime in the field of information technology.

## RESULTS AND DISCUSSION

### Types of IT Crimes

In the ever-growing digital era, information technology crime is a threat that cannot be ignored. From clever phishing attacks to destructive malicious software, the variety of cybercrime continues to grow and become more complex. Criminal acts such as identity theft, online fraud, and DDoS attacks are becoming more common, causing huge financial losses for individuals and companies. A deep understanding of these various threats is becoming increasingly important, because every day thousands of people become victims of criminal activity in cyberspace. Therefore, in this article, we will review some common types of information technology crimes and how we can protect ourselves from the dangers that lurk in the digital environment. There are several types of crimes in information technology as follows:

The most common and frequently occurring cyber crimes today include the following categories:

1. Phishing: This is a form of cybercrime that often occurs. Phishing attacks are often carried out via email, text messages, or social media to steal personal information

Pages : 192-197
Doi. 10.54209/jurnalinstall.v16i03.235

such as passwords, credit card numbers, and other sensitive data. These attacks are difficult to distinguish from official communications.
2. Malware: Types of malware, including viruses, ransomware, and trojans, are a common threat to computer users. Ransomware, in particular, is increasingly common, where the perpetrator encrypts the victim's data and demands a ransom to restore access.
3. Identity Theft: Identity theft is increasing as more personal data is stored and shared online. Cybercriminals use stolen information to commit fraud or illegal activities in the name of victims.
4. Fraud: Online fraud, such as credit card fraud and online auctions, is becoming common. Cybercriminals often target unwary users to steal financial information and carry out illegal transactions.
5. Data Breach: A data breach involves the theft of sensitive data from a company or organization, which can result in significant financial and reputational losses.
6. Denial of Service (DoS) and Distributed Denial of Service (DDoS): DDoS attacks aim to make online services unavailable by flooding traffic. Business websites and gaming platforms are often targeted.
7. Online Harassment and Stalking: Online harassment and stalking are becoming more common with the increasing use of social media. Perpetrators often use the anonymity of the internet to intimidate or harass victims.
8. Cryptojacking: Although new, cryptojacking is becoming more common with the increasing popularity of cryptocurrencies. Cybercriminals target users' computers to mine cryptocurrency without permission.

The importance of awareness of these types of information technology crimes fuels prevention efforts, such as the use of up-to-date security software and safe online practices. Apart from that, it is important to always be alert to potential threats.

**Reasons for the Rise in IT Crime**

The rise of information technology crimes is caused by several factors. First, with increasing digitalization and use of the internet in everyday life, the number of potential targets for cybercriminals is also increasing. Second, increasingly sophisticated technological developments provide more effective tools for cybercriminals to carry out their actions. Law enforcement officials' lack of understanding of information technology is a major factor in the difficulty of ensnaring cybercriminals.

In addition, the anonymity provided by the internet makes it difficult for criminals to be tracked and caught. Lack of cybersecurity awareness and practices among users also contributes to the increasing rate of these crimes. Economic factors also play a role, because cybercrime can provide large financial benefits with relatively low risks for the perpetrator.

Several factors are the reasons for the rise in IT crime, namely public legal awareness, security factors, law enforcement factors, and psychological factors [2]:

**Community legal awareness**

Until now, Indonesian society's legal awareness in responding to cybercrime is still low. This is caused by a lack of understanding and knowledge about this type of crime. This lack of information hampers efforts to combat cybercrime, especially in law enforcement and monitoring activities suspected to be related to cybercrime.

**Safety factor**

The perpetrator's activities are difficult for outsiders to know, in contrast to conventional crimes which are easily visible. In an open place like an internet cafe without partitions, the perpetrator looks like he is using a normal computer. This condition makes perpetrators

Pages : 192-197
Doi. 10.54209/jurnalinstall.v16i03.235

bold, and they can easily erase traces of crimes on the internet, making it difficult for law enforcement to find evidence when the perpetrator is caught.

**Law enforcement factors**

The rise of cybercrime is often caused by law enforcement's lack of understanding of information technology, making it difficult for them to find evidence when arresting perpetrators. Many regional authorities are not ready to deal with cyber crime due to lack of access and knowledge about the internet, while this crime can have a widespread impact abroad.

**Psychological factors**

The Guardian cites psychological research showing that perpetrators of online insults or hate speech seek to improve their status by provoking anger, sparking debate and seeking support. They seek attention because they have a narcissistic personality and fail to attract attention in the real world.

**IT Criminals**

In the ever-growing digital era, information technology (IT) or cyber crime has become a major threat to individuals, companies and governments throughout the world. IT criminals use computer technology and internet networks to carry out various illegal acts, ranging from identity theft to cyber attacks that damage critical infrastructure. The types of IT criminals vary widely, including hackers, crackers, phishers, and malware developers, each using different methods and goals. To overcome this threat, high awareness, a strong security system and effective law enforcement are needed. International cooperation is also very important in fighting cybercrime, which is often cross-border. By understanding the profile and modus operandi of IT criminals, we can take appropriate preventive steps and protect ourselves from potential dangers in cyberspace.

Information technology (IT) criminals, or often referred to as cybercrime perpetrators, are individuals or groups who commit illegal acts using computer technology and internet networks. Here are some types of IT criminals:

1. Hackers
   Someone who attempts to access a computer system or network without permission.
2. Crackers
   Someone who breaks into a computer security system with the aim of damaging it or carrying out illegal activities.
3. Phishers
   Actors who attempt to obtain sensitive information such as passwords or credit card numbers by pretending to be trusted entities in electronic communications.
4. Spammers
   Perpetrators who send unwanted mass messages via email or other media.
5. Cyberbully
   Perpetrators who use technology to harass, threaten, or embarrass others.
6. Scammers
   Perpetrators who defraud others to gain financial gain via the internet.
7. Identify Thief
   Perpetrators who take someone's personal information to commit fraud or other crimes.
8. Cyberterrorist
   Perpetrators who use computer and internet technology to carry out acts of terrorism.
9. Malware Developer

Pages : 192-197
Doi. 10.54209/jurnalinstall.v16i03.235

Actors who create and distribute malicious software.

10. Insider Threats
    A person within an organization who abuses authorized access to commit cybercrime.

By understanding the types of IT criminals and their examples, we can be more alert and take appropriate steps to protect ourselves and our systems from cyber threats.

**How to Overcome IT Crime in Companies**

Cybercriminals use a variety of methods to attack corporate systems, steal sensitive data, and disrupt business operations. Therefore, companies need to take proactive steps to protect themselves from these threats. Combating IT crime requires not only advanced technology, but also awareness and active participation from all employees. By implementing a comprehensive security strategy, from employee training to the use of cutting-edge technology, companies can strengthen their defenses against cyber threats and ensure business continuity in this digital era. One of the efforts that the government has made is to establish the National Cyber and Crypto Agency (BSSN) [3].

Cybercriminals use a variety of techniques to attack corporate systems, steal sensitive data, and disrupt business operations. Therefore, companies must immediately take proactive measures to protect themselves from these threats. Tackling IT crime requires more than advanced technology; awareness and active participation of all employees is also very important. By implementing a comprehensive security strategy, from employee training to using the latest technology, companies can strengthen their defenses against cyber attacks and maintain business continuity in this digital era.

Efforts to overcome crime are actually ongoing efforts and never stop. Along with the progress of human civilization, which is the result of developments in science and technology, various new types of crime have emerged, including cyber crime [4]. Companies need to take proactive steps to protect themselves from increasingly sophisticated cyberattacks, as cybercriminals use a variety of methods to steal sensitive data and disrupt business operations. Not only advanced technology is needed, but also awareness and active participation from all employees. Implementing a comprehensive security strategy, including employee training and implementing cutting-edge technology, is key to strengthening a company's defenses against cyber threats and ensuring business continuity in this digital era.

Increasingly complex cyberattacks are targeting companies to steal sensitive data and disrupt business operations. Therefore, it is important for companies to take proactive measures to protect themselves from these threats. Tackling IT crime requires more than advanced technology; Active participation and awareness of all employees is also very important. By implementing a comprehensive security strategy, including employee training and the use of the latest technology, companies can strengthen their defenses against cyberattacks and maintain business continuity in this digital era.

In today's digital era, companies must face the threat of cybercrime that uses various techniques to attack systems, steal sensitive data, and disrupt business operations. Proactive steps are needed to protect companies from these threats. Tackling IT crime requires more than just advanced technology; awareness and active participation of all employees is also very important. By implementing a comprehensive security strategy, from employee training to using the latest technology, companies can strengthen their defenses against cyberattacks and maintain business continuity.

Some important steps that must be taken in responding to cybercrime are [5]:

1. Updating national criminal laws and legal procedures in accordance with international agreements related to cybercrime.

Pages : 192-197
Doi. 10.54209/jurnalinstall.v16i03.235

2. Improving the national computer network security system to comply with international standards.
3. Increase the knowledge and expertise of law enforcement officials in preventing, investigating and prosecuting cases related to cyber crime.
4. Increase public awareness about the problem of cyber crime and the importance of prevention efforts.
5. Increase international cooperation, both bilateral, regional and multilateral, to overcome cybercrime, including through extradition treaties and mutual assistance treaties.

## CONCLUSSION

Law enforcement against criminal acts of defamation via electronic media involves prevention and enforcement strategies. Prevention is carried out through socialization using electronic media connected to the internet, while enforcement is carried out through a legal approach [6]. The punishment for perpetrators of criminal acts of insulting via electronic media is regulated in Article 27 paragraph (3) of the ITE Law and the criminal threat is heavier than the Criminal Code. In Article 310 paragraph (1) of the Criminal Code the penalty is 9 (nine) months and in Article 310 paragraph (2) of the Criminal Code the penalty is 1 (one) year 4 (four) months with a fine of four thousand five hundred rupiah. Meanwhile, in Article 45 paragraph (1) of the ITE Law, the maximum prison sentence is 6 (six) years and a maximum fine of 1 (one) billion rupiah.

## REFERENCES

[1] Ekawati, D. (2018). Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan skimming ditinjau dari perspektif teknologi informasi dan perbankan. *UNES Law Review*, *1*(2), 157-171.

[2] Lompoliuw, B. O. S. (2020). Analisis Penegakan Hukum Pidana Tentang Penghinaan Di Media Sosial Ditinjau Dari Undang-Undang Ite Dan Kuhp. *Lex Crimen*, *8*(12).

[3] Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Kom, N. A. R. S. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal Information Engineering and Educational Technology) ISSN*, *2549*, 869X.

[4] Djarawula, M., Alfiani, N., & Mayasari, H. (2023). Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Cakrawala Ilmiah*, *2*(10), 3799-3806.

[5] Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400-426.

[6] Mulyadi, T., Raziah, H. F., & Semedi, C. A. P. (2022). Penegakan Hukum Terhadap Tindak Pidana Penghinaan Dalam Sosial Media Platform Tiktok. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia*, *4*(1), 21.