# A review of cyber crime

**Trung Nam Nguyen**
Faculty of Economic, People's Police University, University in Ho Chi Minh City, Vietnam
Correspondence Author: Trung Nam Nguyen
Received 16 Nov 2022; Accepted 23 Dec 2022; Published 6 Jan 2023

**Abstract**
As we all know, cybercrime is one of the most common activities performed by computer professionals. I have discussed some of the effects of cybercrime in my work. Cybercrime refers to the activities perpetrated by individuals for the purpose of harming organizations and stealing important data, documents, and banking information. My paper contains extensive information on cyber crime and cyber crime methods. Finally, I will conduct study on the crimes committed by misusing the Internet in areas such as financial crimes, cyber pornography, spoofing, bombing, and viral attacks. I shall obtain my paper's primary objectives. In this manner, my paper will be finished.

**Keywords:** cyber crime, humanism philosophy, scientist

## 1. Introduction

Cybercrime, often known as computer crime, is the use of a computer for criminal purposes, such as fraud, trafficking in child pornography and intellectual property, identity theft, and invasion of privacy. As the computer has become fundamental to commerce, entertainment, and government, cybercrime, particularly via the Internet, has increased in significance [3]. Since the 1970s, computer crime has been a concern in criminal justice and criminology; offenders use computers to commit crimes. Cybercrime is a criminal conduct committed utilizing a computer and the Internet [6]. The Internet has become a breeding ground for a variety of criminal activities and techniques. The many sorts of cybercrime can be loosely classified into three groups. First, the Internet facilitates the establishment and upkeep of cybercrime markets. The Internet also provides a place for fraudulent activity (i.e., cyberfraud). Thirdly, the Internet has become a breeding ground for cybercriminal communities.

Information regarding the Cybercrime market: Given the rich market for cyber thieves, the World Economic Forum (WEF) has ranked cyber attacks as the third most likely global risk for 2018, and this is unlikely to diminish in the future years. According to Forbes, global investment on information security will reach $124 billion by 2019, driven primarily by privacy concerns and legislation. The scenario of a significant increase in cybercriminal activity has placed enormous pressure on industry participants. If cyberattacks have escalated, it must be highlighted that attack vectors have also multiplied – from emails and websites to IoT devices and the weaponization of AI-enabled gadgets, the attack vectors are omnipresent, leaving the targets susceptible. Lethal dangers in the modern era include ransomware, cryptojacking for cryptomining, and attacks on cyber-physical systems involving key infrastructure like power grids, transportation systems, and other areas. Similarly, outdated methods such as phishing assaults and malware infestation are detrimental to any firm.

The costs of cybercrimes are mind-boggling-loss, theft, manipulation of data, data processing infrastructure, theft of money, identity, intellectual property, personally identifiable data, digital forensic investigations, loss of productivity, reputation loss for organizations, fines, penalties, damages, and lawsuits for organizations, loss of customers resulting in a decline in revenues, and the cost of restoring business operations to normalcy [1]. There have been instances in which businesses were unable to recognize a malicious code built in a complicated manner and, as a result, suffered substantial losses or had to temporarily cease commercial operations. The removal of the senior executives from their jobs and the possibility of prison time significantly weakened their standing in the eyes of the general public.

## 2. Most prevalent forms of cybercrime

It has already been asserted that cybercriminal activity will pose the greatest threat to humanity over the next few decades. Cybercrimes are projected to cost $6 trillion annually by 2021, up from $2 trillion in 2015. According to the 2018 Cost of Data Breach Report by the Ponemon Institute, the average total cost grew from $3.62 million to $3.86 million, a 6.4% rise from 2017, while the average cost per lost record increased from $141 to $148 in 2018. In the coming years, it is anticipated that these figures will continue to rise [4].

### a) Malware

According to the survey, more over half (55 percent) of all types of cybercrime involve malware. These threats include spyware and malware for remote administration. From there, they are able to obtain login passwords, critical corporate data, or information that can aid them in conducting social engineering assaults. The third most prevalent type of malware assault is the infamous ransomware, which often encrypts your device or holds your data hostage until you pay the culprit [5].

### b) Social engineering

31% of social engineering assaults rely more on trust than

technical sophistication. This sort of cybercrime is particularly challenging to defend against since it exploits human vulnerabilities rather than technological ones. Phishing and more complex physical techniques are examples of social engineering attack types [4].

**c) Hacking**

Typically, the phrase hacking refers to a broad range of attacks. Positive Technologies defines it more narrowly in its report: "attacks that exploit vulnerabilities in software and services, holes in protection measures, and other system flaws that do not entail social engineering or malware [2]."

**d) Web attacks**

Web-based attacks account for five percent of cybercrimes against businesses. These attacks exploit website vulnerabilities to gain access to the data of other users. For instance, hackers may insert malicious code into an e-commerce website in order to steal credit card information from users [2].

**e) Credential compromise**

Seventeen percent of attacks involved credential compromise, which is when a hacker uses your login information to access your accounts without permission. An adversary can obtain your credentials by phishing, social engineering, malware (such as key loggers), or hacking (gaining access to a database of credentials and cracking the passwords) [3].

**f) Distributed denial of service (DDoS)**

Although just 2 percent of firms will ever be the subject of a DDoS assault, these can be exceedingly costly and disruptive. DDoS assaults overwhelm a network with traffic, preventing authorized users or staff from accessing the service. After hackers have effectively disabled a network, they often demand a ransom to restore service [5].

**g) Malicious code-viruses, worms and trojans**

Virus: A computer virus is a program that alters other software. These alterations ensure that the virus will be replicated by the infected program. Not all viruses are harmful to their hosts. Typically, a virus is transmitted from one computer to another by email or an infected disk. However, a computer cannot be infected by a virus until the application is executed. When a computer user is deceived into opening a virus-infected file attached to an e-mail, believing the file to be a harmless program from a trustworthy source, this is a frequent technique of virus execution. The Melissa virus, which was released in March 1999, is the most popular example of a virus. The Melissa virus was concealed in a Microsoft Word attachment that appeared to originate from a known sender. The application triggered a macro that emailed itself to the top fifty e-mail addresses found within Microsoft Outlook. It was estimated that the virus caused $80 million in damages [6].

Worms: A worm is a program that replicates independently. Unlike viruses, a worm can spread throughout a network system without needing to be linked to a file. For example, the estimated loss caused by the I love you worm in 2001 was $10.7 billion.

Trojans: A Trojan Horse is a computer application that appears harmless but has secret functionality. They loaded onto the hard drive and ran concurrently with the main software. However, the harmless program contains a hidden subprogram that performs an unlawful purpose. The Trojan horse is the most frequent method for introducing viruses onto computer systems. Back Orifice 2000, for instance, is a program built for misuse and attack on another computer [3].

**3. Some of the security measures**

Utilize Internet Security Software: If you know anything about computers and the internet, there is a great likelihood that you are already running an antivirus (And if not then do not take the risk unless you are seasoned cyber security professional with data backups in place). A combination of antivirus and internet security software assists you in:

1. Utilize an Internet Security Suite: If you know anything about computers and the internet, you're probably already utilizing an antivirus (And if not then do not take the risk unless you are seasoned cyber security professional with data backups in place). An antivirus tool integrated with an internet security suite aids in: Preventing accidental malicious downloads. Preventing accidental malicious installations. Protection against Man in the Middle (MITM) attacks Protection against phishing [2].
2. Use Strong Passwords: This point cannot be overstated. If your bank password is "qwerty123" and you have a substantial amount of money in your account, you must be prepared for an unexpected transaction. You should not rely solely on the rate-limiting mechanisms used by the websites you visit. Your password should be sufficiently robust to be almost uncrackable. A strong password is at least 12 characters long and contains a variety of uppercase and lowercase letters, numbers, and symbols (and spaces). Setting a really unbreakable password should not be difficult, especially with random password generators accessible [3].
3. Maintain Software Continuity: Regrettably, despite the developer's best efforts to create secure software and the security teams' thorough evaluations, a significant number of zero-day vulnerabilities are identified after the program has been widely used. Companies are aware of this, which is why they often release patches to address these vulnerabilities. These changes, notwithstanding their inconvenience, are important for this reason. They prevent attacks that can readily circumvent antivirus software.
4. Avoid Identity Theft: Identity theft occurs when someone uses your personal information to impersonate you on any platform in order to receive advantages in your name while your bills are paid on your behalf. It's just an example, but identity theft can inflict more severe harm than monetary loss. Inappropriate management of sensitive personal data is the leading cause of identity theft. Avoid the following while working with personally identifiable information: Never disclose your Aadhar or PAN number (in Vietnam) with someone you do not know or trust. Never disclose your SSN (in the United States) with someone you do not know or trust. Do not share confidential information on social networking sites. Do not make all of your personal information public on social networking platforms. Never share an Aadhar OTP received via phone call with another individual. Ensure that you do not receive Aadhar-related OTP SMS that are unneeded (if you do, your Aadhar

number is already in the wrong hands) Do not provide personal information on websites that pretend to deliver perks in exchange.

How Vietnam employs a variety of preventative measures against cybercrime: In general, Vietnam has enacted a number of Cyber Laws to combat cybercrime. These laws are designed to safeguard all Vietnamese citizens from heinous acts. All of these laws are in place to safeguard citizens from harm. Traditional criminal actions such as theft, fraud, forgery, libel, and mischief exist in internet. Vietnam's Cyber Laws prohibit any crime committed through the use of technology, when a computer is a tool for cybercrime. Cybercrime rules prevent citizens from sharing sensitive information with strangers online [5].

**Among the laws are the following**

1. Copyright law pertaining to software, source code, internet, cell phone content, etc.
2. In terms of software and source code, licensing law. Regarding domain names, meta tags, mirroring, framing, and linking, etc., trademark law.
3. The Semiconductor Law protects the designs and layouts of semiconductor integrated circuits.
4. Regarding computer hardware and software, patent law.
5. Aim for a balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, and email service providers.

Since the establishment of cyber laws in Vietnam, the IT Act 2000 was passed in 2000 and revised in 2008 to cover all sorts of cyber offences in Vietnam.

The primary objective of this act is to legalize electronic trade and expedite the filing of electronic documents with the government.

The Information Technology Act 2008, as the updated version of the Information Technology Act of 2000 is commonly known, has increased the emphasis on Information Security. Several new sections on offenses, including Cyber Terrorism and Data Protection, have been included.

## 4. Conclusion

Cybercrime, or criminal behavior on the Internet, is one of the future's major issues for Vietnam and international law enforcement. It is already involved in numerous international crimes, such as drug trafficking, human smuggling, terrorism, and money laundering. Even in traditional crimes, digital evidence will become more prevalent, and we must be prepared for this new challenge. To maintain the safety and security of the Internet, law enforcement agencies from around the world are collaborating to build new alliances, new forensic procedures, and new responses to cybercrime. To detect, prevent, and respond to cybercrime, it will be necessary to apply globally applicable new investigative techniques, technology, and talents. This "new business" will be characterized by new types of crime, a considerably greater scope and scale of offending and victimization, the need to respond in a much more rapid manner, and difficult technological and legal difficulties. Innovative measures, such as the development of "cyber police," "cyber courts," and "cyber judges," may ultimately be required to address the enormous jurisdictional difficulties. To prevent all of these web-based attacks, there exist international rules primarily based on people's concerns that help them protect their information and data from many unauthentic users. Cyber law in Vietnam is not a distinct body of legislation. Contract, intellectual property, data protection, and privacy regulations are involved. With computers and the internet dominating every part of our lives, there was a need for robust cyber legislation. Cyber laws regulate the digital transmission of information, software, information security, e-commerce, and financial activities.

## References

1. Anderson R, Barton C, Böhme R, Clayton R, Van Eeten MJ, Levi M, *et al*. Measuring the cost of cybercrime. In The economics of information security and privacy, 2013, p265-300.
2. Broadhurst R. Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management, 2006.
3. Broadhurst R, Grabosky P, Alazab M, Bouhours B, Chon S. An analysis of the nature of groups engaged in cyber crime. An analysis of the nature of groups engaged in cyber crime, International Journal of Cyber Criminology. 2014;8(1):1-20.
4. Gordon S, Ford R. On the definition and classification of cybercrime. Journal in computer virology. 2006;2(1):13-20.
5. Saini H, Rao YS, Panda TC. Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications. 2012;2(2):202-209.
6. Weissbrodt D. Cyber-conflict, cyber-crime, and cyber-espionage. Minn. J. Int'l L. 2013;22:347.