# Cyber Crime and Security

**Shivani Renuke, Soham Karalkar, Abhishek Mutkekar**
Computer science,
K.C. College of Engineering & Management Studies & Research, Kopri, Thane (East), Maharashtra 400603.

***Abstract*— A humongous development in E-Commerce market is seen in the entire world. Due to which Debit, Credit card and personal information security are the most important aspects for customers and banks. Cyber Crime is one the main concerns when it comes to internet. The world has become advanced in communication, especially after the internet was invented. A main problem facing today's society is the increase in cybercrimes or electronic. Hence cybercrime create threats to nations, committees and individuals across the globe. It has become common in the world that millions of people are victims of cybercrime. Stated the grave nature of cybercrime, its nature and implications, it is clear that there is a serious need for a common understanding of such crimes internationally to deal with it effectively. This research covers the definition, types, and causes and how to deal with cybercrime. It has also emphasized on the laws against cybercrime.**

***Keywords*— *Cybercrime, e-crime, cyber security, computers, internet, cyber laws.***

## I. INTRODUCTION

A computer network that links billions of devices together using the internet protocol which is connected by the internet. To this date, the Internet is one of the most important parts of our day-to-day life. The IT revolution has brought two main functions with internet. On one hand, it has given positive values. While, on the other hand, it has produced many issues that threaten the order of society and also produce a new wave of crime. The internet has different utilities depending on user requirements such as communication, research, education, financial transactions, threading, etc. The internet has become a domain, where the most lucrative and safest crimes are conducted. E-crimes are becoming more prevalent and harming individuals, businesses, governments, and society. Additionally, there are many things that can incite cybercriminals, such as the absence of legislation and punishment, financial gain, mental instability, and societal norms. E-crimes go by many names, including high-tech white-collar, cyberpunk, cracker, cyber espionage and hacking. Due to advancements in software and information technology, there is an annual increase in e-crimes. Therefore, e-crimes have spread through a variety of channels, such as malicious programs that are designed to break through personal computers or business systems in order to copy sensitive data or damage systems. The most renowned methods are Hacking, Stalking, Spamming, Phishing, Cyberstalking, Shoulder Surfing, Cyber defamation, Cyber terrorism, and Malware. Consequently, the first step is to protect the information and deny access to anyone in security programs. So many people and organizations have security software to protect their applications from hackers. Besides, many countries trying to impose e-crime laws pose threat to society and individuals. This is because of the spread and progress of information technology and the ease of acquisition of electronic appliances. The motive of this is to own a general survey regarding cybercrimes, cyber laws, and cyber security. It'll additionally explore the e-crimes component and therefore the leverage that creates e-crimes spreading in society. Specifically, it examines the subsequent points: Researching and reviewing the foremost common kinds of e-crimes, study the prevailing kinds of literature on the factors influencing e-crime, looking for the issues of the society in the mistreatment of the web, determine the factors influencing e-crime within the society. Especially, the influence of human ecology and technology over differing types of e-crimes, activity and analysis of perceptions, experiences, and attitudes toward e-crimes, determinant the link between social media and e-crimes.

Suggest the measures to scale back e-crime by the policy manufacturers and awareness programs so cyber security is formed sure. An Indian trading website named Upstox has admitted to a breach of the KYC (know your customer) data. The KYC information that money service companies collect to verify their customers' identities and prevent fraud or concealment may also be used by hackers to conduct fraud. On April 11, after receiving emails warning that contact information and KYC details in charge during a third-party information warehouse could be compromised, Upstox informed customers that it would reset their passwords and take other measures. Customers at Upstox were apologetic for the inconvenience and reassured that the company had reported the event to the appropriate authorities, tightened security, and expanded its bug bounty program to entice ethical hackers to stress-test its systems.

### *A. Cyber Crime*

Cybercrime has been outlined as against the law during which a laptop acts as an associate degree object of the crime (hacking, phishing, spamming) or is used as a tool to commit associate degree unlawful acts (child creative activity, hate crimes). Cybercriminals use engineering to access personal data, business trade confidential or use the web for exploitation or malicious functions. Criminals who perform these ill-gotten activities square measure typically called hackers. Kinds of cybercrime square measure DoS Attacks, Botnets, fraud, Cyberstalking, Phishing, Prohibited/Illegal Content, and online scams. A portion of the internet known as the "dark web" is not searched by search engines. You've probably heard that the "dark web" is a hub for criminal behavior, and that's true. Websites on the dark web resemble other websites in appearance, but there are significant variations. The naming system is the first. Dark web domains have an ending of .onion rather than .com or .co. It stands for a "special-use top-level domain suffix designating an anonymous hidden service accessible through the Tor network. Credit card numbers, various drugs, weapons, fake cash, stolen login information for Netflix, and software to break into other people's machines are all things that can be purchased. Purchase a "lifetime" Netflix premium account, fake money, prepaid debit cards, or registration information for a Bank of America account. You can pay hackers to break into devices on your behalf.

### *B. Types of Cyber Crime*

#### *1) Internet Fraud:*

Whenever an individual tries to get a product from the net, he/she is at excellent risk of being used by net fraud. So, an individual

needs to analyze and study the sources from which he/she is buying the merchandise. The e-commerce surroundings are packed with faux corporations and organizations United Nations agency distribute the worst quality product to the shoppers and are greatly concerned about stealing customers' checking account details.

*2) Trojans:*

Any malware that is usually concealed as trustworthy computer code can be referred to as a Trojan. Cybercriminals and hackers frequently use trojans in their quest to gain entry into users' systems. Typically, users are tricked into installing Trojans that carry the death sentence on their systems using some form of social engineering. Trojans help cybercriminals spy on others, steal their private data, and open backdoors into the system once they've been activated.

*3) Phishing:*

The cybercrimes are typically carried out by establishing phony social media profiles and rogue websites to entice users to them while posing as well-known and reputable brands. These websites often ask users to fill out personal information on forms before they can obtain any benefits, like discounts, and do so to evoke a sense of security. The most sophisticated of these websites may contain malicious scripts that collect this data directly from your computer without the use of forms.

*4) DoS Attack:*

A Denial of Service (DoS) attack is a malicious attempt to temporarily disrupt or halt the operations of a host connected to the internet to distract users from a server or other system resource. A specific computer, a port or administration on the targeted framework, a whole system, a section of a given system, or any component of a framework can all be targets of a Dos attack. Dos attacks may also target human-framework communications or human-reaction systems, such as by disrupting a vital expert's phone or pocket computer. The striking similarity between these examples is that, as a result of the successful DoS attack, the referred-to framework does not respond as recently, and administration is either denied or severely constrained.

*5) Cyberstalking:*

Cyberstalking is outlined as victimization of the net or alternative electronic suggests that with a read to harass or threaten any person, a cluster of people, or a company. It includes observation, false accusations, fraud, creating threats, injury to knowledge or instrumentality, the request of minors for sex, or gathering information that will be wont to threaten or harass.

## II. CAUSES OF CYBER CRIME

Cybercriminals forever select a straightforward thanks to build megabucks. They aim to make individuals or made organizations like banks, casinos, and monetary corporations wherever a large number of cash flows daily and hack sensitive information. Catching such criminals is tough. Hence, that will increase the activity of cyber-crimes across the world. Computers are vulnerable, therefore laws are needed to safeguard them against cyber criminals. List of subsequent reasons for the vulnerability of computers:

*A. Easy to access*

Because of the sophisticated technology, there are many ways that a system could be breached, which is why it is important to protect it from unauthorized access. Access codes, membrane images, advanced speech recorders, etc. That can easily trick biometric systems and bypass firewalls are stolen by hackers to get past multiple security systems.

*B. Capacity to store knowledge in a relatively tiny house*

The computer has the distinctive characteristic of storing data. This makes it plenty easier for individuals to steal data from other storage and use it for their profit.

*C. Complex*

The computers run on operative systems and these operative systems are programmed with ample codes. The human mind is imperfect so one will do mistakes at any stage. Cybercriminals cash in on those gaps.

*D. Negligence*

Negligence is one of the characteristics of human conduct. So, there is also a prospect to protect the pc system any negligence that provides cyber-criminal access and management over the pc system can be dangerous.

*E. Loss of proof*

The information associated with the crime is simply destroyed. So, loss of proof has become an awfully common and obvious drawback that paralyzes the system behind the investigation of cybercrime.

## III. HOW TO TACKLE CYBER CRIME

IT law has been described as "paper laws" for a "nature" and focuses primarily on computerized data (including data security and electronic commerce) viewpoints. Cyber law, also known as internet law, is a word that describes the legal problems associated with internet use. Due to its wide scope of law and regulation, it is less of a specialized topic of law than licensed innovation or contract law. Some of the heading topics include web access and use, security, the chance for expression, and purview. A third word, "machine law," has a propensity to refer to matters involving both internet law and the patent and copyright components of machine engineering and programming.

*A. Firewall*

In computing, a firewall is a system security framework that keeps an eye on both hostile and friendly system movement that is based on a connected principal set. The firewall acts as a barrier between an internal system that is acknowledged to be secure and reliable and an alternative system. Firewalls are both a type of merchandise arrangement and a piece of machinery.

*B. Antivirus*

Antivirus, or anti-virus software, is computer code that seeks out and removes malicious software. The purpose of antivirus software when it was first developed was to identify and remove computer infections. However, as more types of adware proliferated, antivirus software started to provide protection against other computer threats. Modern antivirus software can specifically protect against malicious Browser Helper Objects (BHOS), program hackers, ransomware, key loggers, backdoors, Trojan horses, worms, malignant LSPS, dialers, fraud tools, adware, and spyware.

*C. Sturdy Passwords*

Maintain totally different parole and username combos for every account and resist the temptation to put in writing them down. Weak passwords are often simply cracked victimization, bound offensive strategies like Brute force attack, Rainbow table attack, etc. The subsequent precautions are often taken to avoid your parole obtaining hacked. Using keyboard patterns for passwords. e.g. – qwerty. Using

straightforward combos. e.g. – Sam1995, Feb1995. Using default passwords. e.g. – Welcome1234, Sam1234. Keeping the parole identical because of the username. e.g. – Sam/Sam.

*D. Be social media savvy*

Take care to stay your social networking profiles (Facebook, Twitter, YouTube, etc.) area unit set to non-public. Take care to see your security settings. Take care of what information you post online. Once it's online, it will remain there indefinitely.

*E. Secure your Mobile Devices*

Many people do not appear to remember that their mobile devices are vulnerable to malicious code, like computer viruses and hackers. beware to transfer applications alone from certain sources. Just keep your code up-to-date. Beware to place an anti-virus code and to use a secure lock screen still. Otherwise, anyone can access all of your personal information on your phone if you misplace it or even set it down for a variety of moments.

*F. Protect your data*

Use encryption for your most crucial files, such as financial records and tax returns, to protect your data. By learning about internet fraud and hacking techniques, one may keep up to date. Fishing is a well-known hacking technique, however, one can avoid scams by learning about the most recent fishing attacks online. Thus, keep yourself secure and educate others about these scams by sharing your expertise.

*G. Online identity protection*

It is best to be overly careful when it comes to online identity protection. When disclosing personal information online, such as your name, address, phone number, and/or financial information, it is imperative that you exercise awareness and caution. When using social networking websites, you should enable your privacy settings.

*H. Protect your computer with security software*

For basic online security, a variety of security programs are required. Antivirus software and firewalls are examples of security software. The first line of defense for your computer is frequently a firewall. It regulates access to a computer. A firewall functions as a kind of "policeman" who keeps an eye on any data that is trying to pass through your computer on the internet. It allows communications that it recognizes as secure and safe while preventing "bad" traffic, such as attacks, from ever getting to your computer.

*I. Parental Control*

In the era of online technology, parents should strictly monitor all the activities of their children online. Giving ample privacy to children would be problematic. Parents need to be guarded and should gaze at browser history and email accounts periodically. A better way is by enabling parental control in mobile apps, browsers, and at the router level so that they can access only the secured sites. This will keep them safe from online fraud. Most apps like Netflix, Amazon Prime, and YouTube offer kids-only personalized content to safeguard children from malicious activity.

## IV. CONCLUSION

The use of technology has permeated every area of our daily life. Although technology provides many benefits, it also has certain drawbacks. It has become essential to exercise caution when utilizing any technology to avoid falling victim to cybercrime. Many nations still do not have clear laws governing cybercrimes. Many studies in the recent literature have concentrated on the demographic, sexual, economical, cultural, and political elements that influence cybercrime.

## REFERENCES


[1] Muhammad Hamza. CyberCrime and Security. December, 2017.
[2] Soumya Tiwari , Anshika Bhalla, Ritu Rawat CSE. Cyber Crimes and Security. June, 2022.
[3] Sunakshi Maghu, Siddharth Sehra, Avdesh Bhardawaj. Inside of Cyber Crimes and Information Security. ISSN 0974-2239 Volume 4, Number 8, (2014).
[4] Sajal, S. Z, Jahan, I, & Nygard KE. A Survey on Cyber Security Threats and Challenges in Modem Society. IEEE International Conference on Electro Information Technology (EIT), 2019.
[5] Vinit Kumar Gunjan. Present & Future Paradigms of Cyber Crime & Security Majors - Growth & Rising Trends. 4th International Conference on Artificial Intelligence with Applications in Engineering and Technology (ICAIET), 2014.
[6] Thierry Mbah Mbelli. Cyber Security, An approach to Network and application security. IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), 2016.
[7] Halder, Debarati, and K. Jaishankar. Cyber crime and the victimization of women: laws, rights and regulations. Information Science Reference, 2012.
[8] Zwicky, Elizabeth D., Simon Cooper, and D. Brent Chapman. Building internet firewalls. " O'Reilly Media, Inc.", 2000.
[9] Stolfo, Salvatore J., et al. Insider attack and cyber security: beyond the hacker. Vol. 39. Springer, 2008.
[10] Ralston, P. A. S., J. H. Graham, and J. L. Hieb. "Cyber security risk assessment for SCADA and DCS networks." ISA transactions 46.4 (2007).
[11] Byres, Eric, and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems." Proceedings of the VDE Kongress. Vol. 116. 2004.
[12] Fu, Kevin, and James Blum. "Controlling for cybersecurity risks of medical device software." Communications of the ACM 56, no. 10 (2013).
[13] Kshetri, Nir. "Pattern of global cyber war and crime: A conceptual framework."Journal of International Management 11.4 (2005).