International Scholars Journals

International Journal of Law and Legal Studies ISSN 2736-1608, Vol. 10 (4), pp. 001, December, 2022.
Available Online at http://www.internationalscholarsjournals.com/ © International Scholars Journals

Author(s) retain the copyright of this article.

Perspective

An overview on cybercrime classifications

John Blad[*]

Department of Political Science, University of Bologn, Bologna, Italy.

Received: 22-Nov-2022, Manuscript No. IJLLS-22-87494; Editor assigned: 24-Nov-2022, Pre QC No: IJLLS-22-87494 (PQ); Reviewed: 09-Dec-2022, QC No: IJLLS-22-87494; Revised: 16-Dec-2022, Manuscript No: IJLLS-22-87494 (R); Published: 23-Dec-2022

ABOUT THE STUDY

A crime committed through a computer or computer network is referred to as a cybercrime. Either the computer was the intended target or it was used in the crime. Someone's security or finances may be compromised through cybercrime. When private information is intercepted or made public, whether legally or illegally, there are various privacy issues concerning cybercrime. International cybercrimes, such as financial theft, espionage, and other cross-border crimes, are committed by both state-sponsored and non-state actors. Cyberwarfare is the term sometimes used to describe cybercrimes that take place beyond national boundaries and include at least one nation-state. Cybercrime, according to Warren Buffett, is the "number one concern with mankind" and "poses genuine risks to humanity."

Classifications

Computer fraud, financial crimes, con games, and cybersex trafficking are just a few of the many acts that fall under the umbrella of computer crime (Gámez-Guadix, 2016).

Computer fraud: The use of a computer to steal, modify, or obtain unauthorized access to a computer system or network is known as computer fraud. Internet fraud may be used to describe computer fraud that uses the Internet (Kross, 2021). Depending on the jurisdiction, computer fraud is defined legally in a variety of ways, but often entails unauthorised access to a computer. Hacking into computers to change data, disseminating dangerous software like computer viruses or worms, installing malware or spyware to steal data, phishing, and advance-fee scams are all examples of computer fraud. Computer systems may also be used to aid other types of fraud, such as bank fraud, carding, identity theft, extortion, and theft of sensitive information. These crimes frequently result in the loss of financial or personal information (Kuss, 2017).

Cyberterrorism: Generally speaking, cyberterrorism is an act of terrorism carried out *via* computer or cyberspace resources. Cyberterrorism can take the form of planned, widespread disruption of computer networks, particularly those of personal computers connected to the Internet, using tools such computer viruses, computer worms, phishing, malicious software, hardware techniques, or programming scripts. Since the beginning of 2001, Internet issues and server frauds have significantly increased, according to government officials and information technology security experts. Government organizations in the United States, including the Federal Bureau of Investigation and the Central Intelligence Agency, are becoming increasingly concerned that such intrusions are a part of a planned effort by cyberterrorist foreign intelligence services or other groups to map potential security gaps in crucial systems (Leinsalu, 2020).

Cyberextortion: Cyberextortion is a sort of extortion that happens when a website, email server, or computer system is attacked by malevolent hackers, such as through denial-of-service attacks, or is threatened with such an attack (Martínez-Ferrer, 2018). Cyberextortionists demand money in exchange for a guarantee that the assaults will stop and that they would provide "protection". The Federal Bureau of Investigation claims that cybercriminals who engage in extortion are increasingly targeting corporate websites and networks, impairing their functionality, and demanding money to resume service. Each month, the FBI receives more than 20 reports of crimes, many of which are not filed because the victim's identity should not be made public. Usually, attackers employ a distributed denial-of-service attack. However, there are additional forms of cyberextortion, including doxing, extortion, and bug poaching (Meerkerk, 2009).

Cybersex trafficking: Cybersex trafficking involves the transportation of victims followed by the webcam live streaming of rape or coercive sexual activity (Meshi, 2020). The victims are taken to "cybersex dens" after being threatened, tricked, or kidnapped. Wherever the cybersex traffickers have access to a computer, tablet, or phone with an internet connection is where the dens may be found (Wheatley, 2019). The perpetrators make advantage of videoconferences, dating websites, chat rooms on the internet, applications, dark web sites, and other platforms. To conceal their identities, they make use of digital currency and online payment methods. Authorities get millions of reports of its occurrence each year. To combat this kind of cybercrime, new laws and police protocols are required.

REFERENCES

1. Gámez-Guadix M, Borrajo E, Almendros C (2016). Risky online behaviors among adolescents: Longitudinal relations among problematic Internet

[*] **Corresponding author:** John Blad, Email: bladdjho123@gmail.com

use, cyberbullying perpetration, and meeting strangers online. J Behav Addict. 5:100-107.

2. Kross E, Verduyn P, Sheppes G, Costello CK, Jonides J, Ybarra O (2021). Social media and well-being: Pitfalls, progress, and next steps. Trends Cogn Sci. 25:55-66.

3. Kuss D, Griffiths M (2017). Social networking sites and addiction: Ten lessons learned. Int J Environ Res Public Health. 14:311.

4. Leinsalu M, Baburin A, Jasilionis D, Krumins J, Martikainen P, Stickley A (2020). Economic fluctuations and urban-rural differences in educational inequalities in mortality in the Baltic countries and Finland in 2000–2015: A register-based study. Int J Equity Health. 19:223.

5. Martínez-Ferrer B, Moreno D, Musitu G (2018). Are adolescents engaged in the problematic use of social networking sites more involved in peer aggression and victimization? Front Psychol. 29:801.

6. Meerkerk GJ, van Den Eijnden RJJM, Vermulst AA, Garretsen HFL (2009). The Compulsive Internet Use Scale (CIUS): Some psychometric properties. Cyberpsychol Behav. 12:1-6.

7. Meshi D, Cotten SR, Bender AR (2020). Problematic social media use and perceived social isolation in older adults: A cross-sectional study. Gerontology. 66:160-168.

8. Wheatley D, Buglass SL (2019). Social network engagement and subjective well-being: A life-course perspective. Br J of Sociol. 70:1971-1995.