International Journal of Cyber Behavior, Psychology and Learning
Volume 13 • Issue 1

Varieties and Skills of Cybercrime

Tansif Ur Rehman, University of Karachi, Pakistan*
https://orcid.org/0000-0002-5454-2150

Sajida Parveen, Karachi Institute of Economics and Technology, Pakistan

Mehmood Ahmed Usmani, University of Karachi, Pakistan

Muhammad Ahad Yar Khan, University of Karachi, Pakistan

ABSTRACT

Several thousand organized groups, as well as gangs, are dedicated to cybercrime. The potential rewards for cybercrime can be immense, even for relatively simple crimes. The rapid advancement of technology means that cybercrime is constantly evolving, making it difficult to define and predict. While some may believe cybercrime to be the work of individual lone actors, the reality is quite different. Today, there are thousands of groups dedicated to cybercrime, attracted by its potential rewards. The pace of cybercrime globally is increasing rapidly, and resolving cybercrime is often more challenging than traditional crimes. Authorities worldwide receive thousands of complaints daily, and cybercriminals are becoming increasingly innovative, organized, and sophisticated. They work hard to uncover new vulnerabilities and avoid detection while consumers remain unaware of the risks. With the rapid expansion of ICTs, cybercriminals have unique opportunities to exploit, and the full extent of the dangers is still largely unknown.

KEYWORDS

Cybercrime, Hacking, Malware, Pharming, Phishing, Skills, Spyware

INTRODUCTION

Cybercrime refers to criminal activities that are conducted using electronic devices and the internet. It encompasses a wide range of illegal activities that involve the use of technology, such as hacking, phishing, identity theft, ransomware attacks, and malware distribution (Clancy, 2023; Hamerton & Webber, 2023). The emergence of the internet and other digital technologies has created new opportunities for criminals to engage in illegal activities. Cybercrime is a growing problem worldwide, affecting individuals, businesses, and governments. It is estimated that cybercrime costs the global economy billions of dollars every year (Dhaya & Kanthavel, 2023).

Cybercriminals use a variety of tactics to carry out their illegal activities, including social engineering, malware distribution, and network intrusion (Roy & Tripathy, 2023). They often target

DOI: 10.4018/IJCBPL.324091

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

individuals and organizations with weak security measures, seeking to exploit vulnerabilities in software and computer systems (Alsmadi, 2023; Lorenzo-Dus, 2023). The fight against cybercrime is an ongoing challenge for law enforcement agencies, cybersecurity experts, and individuals alike (Lehto & Neittaanmaki, 2023). It requires a multi-faceted approach that includes education, awareness, and robust security measures to protect against cyber threats.

Cybercrime is a worldwide threat to individuals, businesses, and governments, as more activities are conducted online (Allum & Gilmour, 2023; Bancroft, 2019; Hamerton & Webber, 2023). Cybercriminals use various techniques and tools to carry out their illicit activities (Johansen, 2020; Troia, 2020), such as stealing personal information (Leukfeldt & Holt, 2019), hacking into systems (Steinberg, 2019; Troia, 2020), and disrupting critical infrastructure (Clancy, 2023; Lorenzo-Dus, 2023).

To effectively combat cybercrime, it is essential to understand the different varieties and skills involved (Dhaya & Kanthavel, 2023). The varieties of cybercrime refer to the various types of cyber-attacks that can occur, including phishing, ransomware, and distributed denial of service (DDoS) attacks (Roy & Tripathy, 2023). Each type of cybercrime requires different skills and techniques, such as social engineering, malware development, and network analysis (Alsmadi, 2023; Lehto & Neittaanmaki, 2023).

Understanding the skills involved in cybercrime is crucial to developing effective countermeasures (Sikos & Haskell-Dowland, 2023). Cybercriminals often possess high technical expertise and may use sophisticated tools and methods to evade detection and carry out their activities (Kumar et al., 2023; Scanlan, 2023). Some common skills cybercriminals use include programming, encryption, and network analysis (Hubbard & Seiersen, 2023; Shires et al., 2023).

Overall, studying the varieties and skills of cybercrime is essential to developing effective prevention and response strategies and protecting individuals, businesses, and governments from the damaging effects of cyberattacks. This paper will explore the different types of cybercrime and the skills required to carry them out to improve our understanding of this complex and evolving threat.

JUSTIFICATION OF THE RESEARCH

The study of the varieties and skills of cybercrime is essential for several reasons.

Firstly, cybercrime has become increasingly prevalent in recent years, with more individuals and organizations becoming targets of cyberattacks. Understanding the different types of cybercrime and the skills required to carry them out is crucial for developing effective prevention and response strategies.

Secondly, cybercrime is constantly evolving, with new techniques and tools being developed by cybercriminals all the time. By studying the different varieties and skills of cybercrime, researchers can stay current with the latest trends and technologies and help organizations and law enforcement agencies keep pace with these developments.

Thirdly, cybercrime often has severe consequences for its victims, both in terms of financial losses and damage to reputation. By understanding the varieties and skills of cybercrime, researchers can help to identify the most effective ways to mitigate these risks and protect individuals and organizations from cyber threats.

Overall, studying the varieties and skills of cybercrime is essential for developing effective strategies to prevent, detect, and respond to cyberattacks and protect the safety and security of individuals and organizations online.

FOCUS OF THE RESEARCH

Respective work focuses on 11 varieties and skills involved in cybercrime. Cybercrime statistics and the top 10 countries facing cybercrime are also highlighted. Cybercrime is a multifaceted problem requiring a comprehensive approach as the subject matter is far more complex to comprehend.

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/varieties-and-skills-of-cybercrime/324091

Related Content

A Socio-Technical Perspective
(2021). *Real-Time and Retrospective Analyses of Cyber Security (pp. 202-233).*
www.irma-international.org/chapter/a-socio-technical-perspective/260536

Improving Moral Behaviour in the Business Use of ICT: The Potential of Positive Psychology
Candace T. Grantand Kenneth A. Grant (2016). *International Journal of Cyber Ethics in Education (pp. 1-21).*
www.irma-international.org/article/improving-moral-behaviour-in-the-business-use-of-ict/166624

A Cyberbullying Portfolio for School Social Educators
Gilberto Marzanoand Joanna Lizut (2022). *Research Anthology on Combating Cyber-Aggression and Online Negativity (pp. 243-262).*
www.irma-international.org/chapter/a-cyberbullying-portfolio-for-school-social-educators/301638

Towards a Cyberfeminist Framework for Addressing Gender-Based Violence in Social Media: An Introduction
Subhajit Panda (2023). *Cyberfeminism and Gender Violence in Social Media (pp. 108-138).*
www.irma-international.org/chapter/towards-a-cyberfeminist-framework-for-addressing-gender-based-violence-in-social-media/331901

Support for Cyberbullying Victims and Actors: A Content Analysis of Facebook Groups Fighting Against Cyberbullying
Sophia Alimand Shehla Khalid (2022). *Research Anthology on Combating Cyber-Aggression and Online Negativity (pp. 1616-1639).*
www.irma-international.org/chapter/support-for-cyberbullying-victims-and-actors/301710