Dri reno

11-5-23

Teresa Duvall

Article review 1

The IJCIC aims to publish theoretical and empirical studies that contribute to a better understanding of the causes, patterns, and trends of crime, deviance, and security in cyberspace, as well as countermeasures for broader implications. Here are some key points about the scope of the IJCIC: Focus areas: Origins, patterns, causes, motivations, and trends of cybersecurity and cybercrime in the contemporary era. New methods and approaches to existing issues within the field. Theoretical and empirical research on cybercrime and cybersecurity. Policy and legal aspects of cybercrime and cybersecurity. Social and economic impacts of cybercrime and cybersecurity. Target audience: Researchers in criminology, social sciences, computer science, and other related fields. Cybersecurity practitioners, members of police agencies, and policymakers. Academic researchers are interested in cybercrime and cybersecurity. Types of articles published: Original research articles Review articles Case studies Book reviews Examples of topics covered in the IJCIC: Cybercrime: Dark web activities, cyberstalking, cyberbullying, online fraud, hacking, data breaches, cyberterrorism, ransomware attacks, cryptocurrency-related crimes. Cybersecurity: Security vulnerabilities, malware analysis, intrusion detection and prevention systems, network security, data encryption, digital forensics, incident response, cybersecurity education and awareness. Cyberintelligence: Cyber threat intelligence, dark web monitoring, cybercrime investigations, social media intelligence, open-source intelligence. Cyberlaw and policy: Cybercrime legislation, international cooperation on cybersecurity, data privacy regulations, ethical considerations of cyber warfare. Social and economic impacts of cybercrime and cybersecurity: Economic costs of cybercrime, the impact of cybercrime on individuals and organizations, social and cultural implications of technology and cybersecurity. Overall, the IJCIC provides a platform for researchers and practitioners to share their knowledge and insights on a wide range of cybercrime and cybersecurity issues. The scope of the journal is broad and encompasses various disciplines, making it a valuable resource for anyone interested in staying up-to-date on the latest developments in this rapidly evolving field.

This research article investigates the complex interplay between cyberattacks, the cyber threat landscape, and public perceptions of cybersecurity policies. It delves into the following key areas: Cyber ​​attacks: Definition: Deliberate attempts to exploit vulnerabilities in computer systems and networks. Impact: Data breaches, financial losses, disruption of critical infrastructure, and physical damage. Examples: malware attacks, phishing scams, zero-day exploits, and DDoS attacks. Views regarding Cybersecurity Regulations: Different viewpoints:

Strong government intervention: Supporting more stringent laws, even if they violate people's rights, to maintain public safety and security.

Minimal government involvement: Promoting private sector solutions for cybersecurity while placing a high priority on individual rights and privacy.

Factors that influence: Firsthand knowledge of cyberattacks: Those who are directly impacted are more likely to favor robust government action. Stronger support for governmental actions is correlated with higher perceived knowledge of cyber dangers.

Trust in government institutions: Support for intervention is influenced by one's perception of the government's ability and transparency. Extra Things to Think About:

Wide-ranging effects of cyberattacks: In addition to causing costs to people and businesses, cyberattacks can jeopardize vital infrastructure and national security.

A multifaceted approach to cybersecurity: To be effective, plans must include public education, legal frameworks, and technological advancements.

International cooperation: Information sharing and cooperation between nations are necessary to combat global cyber threats.

Privacy and individual liberty concerns: People who respect their privacy could be reluctant to accept laws that impose restrictions.

Reference:

*IJCIC*. Cybercrime Analytics. (2020, September 10). <https://www.cybercrimeanalytics.com/affiliations-and-memberships/ijcic/>

Academic.oup.com. (n.d.). <https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745?searchresult=1>