

Awareness on Cyber Crimes among College Students with Special Reference to Arts & Science Colleges in Alappuzha District of Kerala, India

Discipline: Cyber Law and Security

Promod Gopal

Assistant Professor, Department of Commerce, NSS College Pandalam, Kerala, India

Email: promodgopal1@gmail.com

Neeraj S.

Milad -E-Sherief Memorial College, Kayamkulam, Kerala, India

Email: neerajs7592@gmail.com

Received: 26.09.2024 | Revised Submission: 27.04.2025 | Accepted: 05.05.2025 | Available Online: 07.05.2025

Abstract

This paper aims to examine the level of awareness regarding cybercrimes among college students. As the utilization of cyber space rises, so does the occurrence of cybercrimes. Therefore, the purpose of this study is to examine the level of awareness of various cybercrimes among college students, analyze their reactions to cybercrimes they have encountered, and evaluate the safety measures they have implemented to protect themselves from cybercrimes. The results of the study showed that several students do not have a clear idea about cybercrimes like trojan horse and web jacking, and there are students who are not following legal measures to fight against cybercrimes. It is highly essential to increase awareness about cybercrimes among college students.

Keywords: Cybercrimes, cyber space, awareness

Introduction

India is one of the largest countries in the world in the context of internet usage. Internet is the widely used medium for teaching and learning. Increase in the use of internet by way of smart phones, tablets, computers and other devices in day-to-day lives has led to an increase in cybercrimes. Students use the internet to access social networking sites and post videos, online banking, book tickets etc. which saves energy and time. In some situations, students are exposed to cybercrimes while doing virtual transactions or visiting social media platforms. Cybercrimes occur due to lack of knowledge about cybercrimes and cyber laws. Therefore, it is now necessary to understand cybercrime in order to protect current and future generations. Government has to develop effective strategies to educate students to avoid cybercrimes.

Statement of the Problem

The primary objective of university education is to equip students with the necessary skills and knowledge for their future endeavours. As students nurture their talents and skills, they contribute to the growth and development of the nation. At present, students highly depend on the internet to increase their knowledge and advance their skills. Thus, internet has become a vital aspect of the day-to-day life of students. The increase in the usage of internet will result in the occurrence of various types of cyber criminals. This is a growing concern in the virtual world as people are becoming highly connected to the internet. The incidence of cybercrimes is rising rapidly, and more and more people are vulnerable to its risks. It is necessary to conduct detailed investigations into the issues of cybercrime because there has been a considerable increase in cases of identity theft, online fraud, malware, and hacker attacks. As technology is advancing faster, students should be offered with safe and secure free from cybercrimes. All colleges are required to raise awareness about cybercrimes. The purpose of this study is to give an insight on the level of awareness among college students regarding cybercrimes.

Relevance of the Study

The research on understanding and recognizing cybercrimes and cyber laws is of great importance in our current society. Students are the primary users of information obtained from the internet. Consequently, it's crucial for students to gain knowledge about cyber threats and the potential repercussions they can have. This research holds significant importance in incorporating cyber awareness programs into the daily curriculum of all universities and branches of education.

Objectives

1. To access the level of awareness on different types of cybercrimes among college students.
2. To understand the different types of cybercrimes encountered by college students.
3. Analyse college student's response to cybercrimes in cyber space.
4. To access the influence of gender on choice of safety measures against cybercrimes.
5. To understand the safety measures adopted by college students against cybercrimes

Methodology

The present study is descriptive in nature and the data was collected from 100 students randomly selected from the arts and science colleges in Alappuzha district,

Kerala, India. The primary data were collected through service and systematically collected google forms. Convenient sampling method is used to collect data. The study period was between September and October 2024.

Review of Literature

- **Vinaya Chaturvedi (2018)** conducted a study on the impact of cybercrime technology on digital banking in India. The objective of this study is to examine the level of awareness among individuals regarding the utilization of internet banking as a means of accessing bank accounts and obtaining necessary information conveniently. The study also analysed the reasons why some customers do not prefer electronic banking. It further aims to understand different cybercrimes related to digital banking operations. The survey results indicate that individuals in the age group of 30 to 40 are not choosing digital banking because they lack awareness about its benefits. The individuals who engage in digital banking are well-informed about cybercrimes and they are actively implementing various preventive measures to safeguard themselves from cybercrimes while utilizing the internet, thereby minimizing the risk of falling victim to cybercrime.
- **Shikha Panwar (2018)** conducted a study on cyber security awareness and challenges in India, as information security is crucial in today's internet-driven world. The primary objective of the research is to understand the significance of information security for organizations, institutions, and companies, and to investigate the reasons behind its necessity. Additionally, the study aims to explore how individuals and other internet users can safeguard their information. They examined the different forms of cybercrimes and how they impact organizations, as well as the challenges faced by these organizations. They concluded that raising awareness about cyber security is crucial for organizations to minimize cybercrime in the future. They should ensure the safety of their organizational data by utilizing the most advanced security measures available. The organizations are aware of the importance of information security, but the employees who utilize it are not particularly concerned about it, so the organizations should make an effort to educate the users about its significance.

Cyber Crime

Cybercrime poses a significant problem to both companies as well as individuals, making it a dangerous attack that must be addressed seriously. There are multitudinous cases where the attack has resulted in significant fiscal loss for both the company and individuals due to the data breach. In today's technology-driven world,

computers have come the primary source for penetrating and participating information. Cybercrime refers to a crime committed against computers and other digital bias. Teessider-attacks can pose a significant trouble not only to the association but also to the entire nation. To this day, there have been multitudinous cases of digital attacks in India and worldwide, egging the need for enhanced security measures. These attacks are also impacting the frugality of the country if not addressed in the early stages. Cybercrime encompasses a range of offenses committed online, exercising the internet via computers, laptops, tablets, internet-enabled boxes, and smartphones. Acts that are against the law and involve computers can either be used as a tool or a target, leading to cybercrime. It is also appertained to as electronic crimes-crime, high technology crime, information age crime etc. These types of crimes involve illegal conditioning that use computers and networks. As the internet has advanced, the number of cybercrime conditioning has also grown.

Preventive Measures

- **Maintain your applications up to date:** -This is an essential requirement for anycomputer system and application. It is crucial to regularly update your operating system, services, and applications to ensure that you have the most recent bug fixesand security patches. This also applies to smartphones, tablets, local computers, notebooks, online services, and all the applications they run internally.
- **Enable the network firewall:** -The majority of operating systems come with a pre-configured firewall that safeguards against harmful packets originating from both internal and external sources. A system firewall serves as the initial digital barrier whenever an individual attempts to transmit a malicious packet to any accessible ports.
- **Create unique and complex passwords:** -Avoid using the same password for multiple websites, and ensure that it includes a combination of letters, special characters, and numbers. Create robust passwords for every website and simultaneously store them in an encrypted database.
- **Install and update antivirus and anti-malware software:** -This is a highly effective measure for both individuals using desktops and corporate users. It is always advisable to ensure that antivirus and antimalware software are regularly updated and perform scans on local storage data. Although free antivirus and antimalware solutions can be beneficial, they are typically trial software and do not provide comprehensive protection against the majority of common virus malware and other network threats.

- **Enable the email spam filtering option:** -Unsolicited emails often serve as a breeding ground for computer hacking, as they frequently contain malicious links or attachments. To activate the anti-spam function in your email client, ensure that it is enabled. Additionally, it is crucial to refrain from opening links or attachments from unknown senders. This will help protect against phishing attempts and prevent the installation of harmful software.
- **Enforce two-step verification for all online services:** -In today's digital landscape, many online services and products provide an additional layer of security through two-factor authentication. These security measures provide an additional layer of authentication, ensuring that even if an attacker manages to obtain the username and password, they will still be unable to gain access. The hackers will be unable to access online accounts because they do not possess the two-factor authentication generated or created by computers.
- **Secure the local hard disk:** -Digital crime doesn't only happen online – imagine someone breaking into a house and stealing a notebook, so it is crucial to safeguard data on the hard drive. In the event that criminals attempt to access the drive's content, they will be unable to determine the correct key to unlock it.
- **Only purchase from reputable and trustworthy online retailers:** - All SSL-certified websites are actually secure. To safeguard yourself from becoming a target of theft or fraud, make sure that the website you are using is secure with https encryption and only shop on reputable online platforms like Amazon, eBay, or Walmart.
- **Make use of VPN services:** - The operation of VPN services is on the rise annually, and it's completely normal to use one to help third- party companies from covering online exertion. One of the reasons to use a VPN is to pierce a secured network from a remote position.
- **Secure the e-mail:** -By utilizing a reliable privacy key, one can guarantee that their email is only accessible to the intended recipient. Pgp is a tool that helps to sign, encrypt, and decrypt various forms of digital communication, such as texts, emails, and files, thereby enhancing the security of your online correspondence.
- **Track the children's internet use:** - Occasionally, local network breaches do not originate from an individual's personal computer, but rather from children's tablets, phones, or notebooks. Teach children about online safety and take measures to protect them from falling prey to cyber criminals.

Discussion and Interpretation

Findings

1. Majority of the students are only slightly aware about trojan horse and web jacking.
2. Majority of the students are aware about cyber crimes through academic learnings and newspapers.
3. A majority of the students encountered online fraud, which is currently the most prevalent cyber crime in the present world.
4. Only a small portion of respondents react to the cyber crime by informing police.
5. Majority of students use passwords as safety measures against cyber crimes.
6. Only a few students use VPN as a safety measure against cyber crimes.

Conclusion

Scholars must have a good understanding of cyberspace as it's a pivotal source of information for their academic hobbies. still, the way pupil communities use cyberspace poses a significant challenge for parents and educational institutions, as cyberspace access has come more accessible and affordable than ever ahead. In India, the proportion of cybercrimes is adding, as there's a lack of mindfulness about these crimes and how to combat them through cyber law. The maturity of the repliers has concurred that online fraud is the primary issue they encountered while exercising the internet. utmost of the scholars is familiar with cybercrime through their academic studies and reading journals. It's apparent that a significant number of repliers are still lacking mindfulness regarding certain cybercrimes. Some individualities are ignorant of the necessary preventives to guard their information in moment's world, where identity theft has come a current crime. thus, it's pivotal for them to take applicable measures to cover their data. They should take advantage of the benefits of using a VPN to enhance their protection against cybercrimes. A significant number of the actors are not taking advantage of the advantages offered by a virtual private network (VPN). multitudinous scholars are impacted by cybercrimes, yet they are not prepared to report these incidents to law enforcement. This has to be altered. It's pivotal to address all the issues in cyberspace through legal means. numerous individualities calculate on watchwords as a security measure, but they ensure that they don't use the same word for multiple websites. Also insure the regular changing of watchwords. The act of downloading pictures, games, and other digital content is considered a form of cybercrime. To avoid falling victim to cybercrime, it's pivotal to apply preventative measures and preventives while navigating the online world, in order to help unborn incident.

References

1. Vinaya Chaturvedi (2018) Cybercrime Technological Blight in Digital banking in India. *Journal of Business and Management*. pp 55-62
2. Shikha Panwar (2018) Cyber security Awareness challenges in India. *International Research Journal of Engineering and technology*. Vol.5 issue - 1, pp 1258 - 1259.