International Journal of Research (IJR)
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 03
March 2022

A Study on Awareness of Cyber Crime and Security

Junaid Hussain Wani
Teaching Assistant in Govt. Degree College (D. H. Pora)
Anantnag Jammu and Kashmir

Abstract:
This paper attempts to analyze the awareness of cyber-crime among internet users with different age groups and educational qualifications. Cyber-crime is the crime that is done using computer and network. Usage of internet has become a daily routine for majority of people for day-to-day transactions.

INTRODUCTION

The internet is growing rapidly. Nowadays it has given rise to new opportunities in the field of entertainment, business education, and many more. But The abuse of internet has given birth to new age crimes which are addressed by the Information Technology Act, 2000.As information around the globe has become more accessible, it has also become more vulnerable to misuse. People commit crimes due to the process of socialization that does not develop strong sense of what is right or wrong and due to the emerging opportunities, the enlarging desires that act as strong motivation for taking to crime to fulfill these desires.
Cyber-crime is any illegal activity which is committed using a computer network involves the breakdown of privacy, or damage to the computer system properties such as files, website pages or software.
There are many privacy concerns surrounding Cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. India records 50,035 cases of cybercrime in 2020, with a 11.8% surge in such offences over the previous year. The rate of cybercrime also increased from 3.3% in 2019 to3.7% in 2020 in the country, according to the National Crime Record Bureau (NCRB).

Total of 66, 01,285 cognizable crimes comprising 42, 54,356 Indian penal code (IPC) crimes 23, 46,929 special &local laws (SSL) crimes were registered in 2020.

• India is the third-most targeted country for Phishing attacks after the US and the UK
• The majority of cybercrimes are centered on forgery, fraud and Phishing
• Social networks as well as ecommerce sites are major targets

Common types of cybercrimes may be discussed under the following:-

1. Hacking - A hacker is an unauthorized user who attempts to or gains access to an information system.
Hacking is typically technical in nature (like creating advertising that deposits malware in a drive-by attack requiring no user interaction). But hackers can also use psychology to trick the user into clicking on a malicious attachment or providing personal data.
2.Spamming - the act of spreading unsolicited and unrelated content – has been observed in several different domains such as email, instant messaging, web pages, Internet Telephony, etc.

Spamming is sending of unsolicited bulk and commercial messages over the internet for the purpose of advertising for any prohibited purpose (especially the fraudulent purpose of phishing), or simply sending the same message over and over to the same user..

3. Cyber Pornography –

Women and children are victims of sexual exploitation through internet. Pedophiles use the internet to send photos of illegal child pornography to targeted children so as to attract children to such fun. Later they are sexually exploited for gains.

4. Phishing - Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.
5. Spoofing - It is the act of disguising one computer to electronically "look" like another compute, in order to gain access to a system that would be normally is restricted. Spoofing can take on many forms in the computer world, all of which involve some type false representation of information. There are a variety of methods And types of spoofing. Like IP, ARP, E-Mail, Web,nand DNS spoofing.

Categories of Cyber Crimes

1. **Crimes against Individuals:**
A crime against the individual refers to those criminal offences which are committed against the will of an individual to cause certain harm to them like physical or mental harm. For example assault, harassment, kidnapping, and stalking etc.
This is one of the directly affects any person or their properties. These crimes

care like – harassment via emails, cyber-stalking, cyber bullying, dissemination of obscene material, defamation, hacking, cracking, email spoofing.
Similarly, there are cybercrimes done to harm the property of an Individual or Organizations. They can be classified as – Intellectual property crimes, cybersquatting, cyber vandalism, hacking computer system, computer forgery, transmitting viruses & malicious software to damage information,

2. **Crimes against Property:**

Crime against property is any criminal act that destroys another's property, or that deprives an owner of property against the owner's will. There are cybercrimes done to destroy the property
Of an Individual. They can be classified as – Intellectual property crimes, cyber-squatting, cyber vandalism, hacking computer system, computer vandalism, computer forgery, transmitting viruses and malicious software to damage information, Trojan horses, cyber trespass, Internet time thefts, robbery or stealing money while money transfers ,etc.

3. **Crimes against Government /Firm /Company /Group of individuals:**
These types of crimes include cyber terrorism, possession of unauthorized information, distribution of pirated software, logic bombs, etc. this is one of the most common types of cybercrime today. When a company's online presence or any of its products are hacked, it becomes a serious problem that can result big loss of any organization.
There are certain cyber-crimes committed to threaten the international governments or organizations. These cybercrimes are mainly committed for the purpose of spreading terror among people of a particular country.
Following are the few examples of crime against Governments or Organizations:

1. Unauthorized access / control over computer system.
2. Cyber terrorism against the government or organization.
3. Possession of unauthorized information.
4. Distribution of Pirate software

.

4. Crime against humanity

Crime against humanity refers to specific crimes committed in the context of a large-scale attack target civilians, regardless of their nationality.
These crimes include murder, torture violence,
Persecution, enforced disappearance etc.

5. Crimes against Society:

Crimes against society, such as alcohol, drugs, and animal abuse charges, are crimes that negatively affect society, rather than individuals or property**.**
This one affects society as a whole. The main target of these types of crimes is public at large and societal interests. The cybercrimes against society include the following types of crimes:

1. Child pornography.
2. Indecent exposure of polluting the youth financial crimes.
3. Sale of illegal articles.
4. Trafficking.
5. Forgery.
6. Online gambling.
7. Web jacking

Cyber Security
A strong cyber security strategy has layers of protection to defend against cybercrime, including cyber-attacks that attempt to access, change, or destroy data; extort money from users or the organization; or aim to disrupt normal business operations.
Cyber security measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization

For strong cyber security system certain elements are needed

1**. Application security**
Testing security features within applications to prevent security vulnerabilities against threats
such as unauthorized access and modification. Application security includes all tasks that introduce a secure software development life cycle to development teams. Its final goal is to improve security practices and, through that, to find, fix and preferably prevent security issues within applications.

2. **Information security** – It is a process to protect digital data and other sensitive information from unauthorized access.
Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (CIA).
3. Storage security.

Data storage security involves protecting storage resources and the data stored on them.
Good data storage security minimizes the risk of an organization suffering data theft, unauthorized disclosure of data, data tampering, accidental corruption or destruction, and seeks to ensure accountability and authenticity of data as well as regulatory and legal compliance

4**. Network Security:**
Network security is a process to protect the underlying networking infrastructure from unauthorized access There is many people who attempt to damage our Internet-connected computers, violate our privacy and damage our system.
Network Security is vital in protecting client data and information, keeping shared data secure and ensuring reliable access and network performance as well as protection from cyber threats.

Cyber awareness

Internet has become one of the integral part of our daily life. It has transformed the way we communicate; make friends, share updates, play games, and shop. They are impacting most aspects of our day-to-day life.
Cyberspace connects us virtually with corers of online users across the globe. With increasing use of cyberspace, cybercrimes especially against women and children such as cyber stalking, cyber bullying, cyber harassment, child pornography, rape content, etc. are also increasing rapidly. To stay safe in the online world, it is important to follow some cyber safe practices which may help in making our online experience and productive:

1. Protect your child from Cyber Grooming: Grooming is a practice where someone builds an emotional bond with a child through social media or chat window with an objective of gaining their trust for sexual exploitation.
Children may remove privacy settings on social media to make more friends. Parents should discuss responsible use of social media. Also, they should educate and help them in selecting strong privacy settings.

2. Never click suspicious links or attachments: Never click on links or files received in e-mail, text message or social media from unknown person. This may be an attempt to infect computer with a malware.
3. Keep software updated: Keep your software and Operating system up-to-date. Hackers target software vulnerabilities to access private information and putting you at risk, so make sure to update all your software with the latest

security patches. Never install software, games, music and apps from trusted sources.

4. Set secure browser settings:

Always choose updated version of the browser and install safe browsing tools for protection yourself from hackers and malware

5. Do not use Smartphone for taking sensitive personal photographs and videos:

Do not use Smartphone for taking sensitive personal photographs and videos. Most of the smartphones are connected to internet and cloud storage. If a picture or video has been clicked/ recorded by using smartphone connected with the cloud, it may get saved automatically into the cloud. Even if users delete their photos or videos from their phone, the same photo or video can be recovered from the cloud account or any other device/ PC connected to the cloud using same account.

6. Beware of fake social media accounts- Not all the accounts are real and not all information provided on accounts are true.

7. Any content related to of Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material such as Rape/ Gang Rape (CP/RGR) content should be report to the concerned social media website(www.cybercrime.gov.in)

8. Enable your system firewall it will protect your system from the outer environment.

9. Use of different /Strong passwords is difficult to guess .More strong password you chose more will be the security.

10. Use antivirus and anti-malware software.

An antivirus software works by scanning incoming files or code that's being passed through your network traffic and also it will defend your system and data from malicious attacks.

11. Activate your email anti-spam blocking features will automatically block the spam messages from hackers.

Conclusion

Criminal behavior on the Internet, or cybercrime, presents as one of the Major challenges of the future to India and International law enforcement.

Number of internet users is continuously increasing and with this growth risk of several types of crimes is also amplified. There are various kinds of cyber-crimes which are happening in day-to-day life. But the people are not aware of all such types. The study shows that 48% of the respondents share their personal details with other persons even they don't know them closely.55% of respondents have agreed that their PCs are often damaged by viruses. It is the

duty of each one of us to be aware of the basic cyber security. Cyber security refers to the technologies and processes that are designed to protect computers, networks and data from unauthorized access and attacks delivered via the internet by cyber criminals. The people should be aware of the basic cyber securities such as they should:
Install a security suite, network threat protection etc. And File a complaint against the hackers in special cybercrime cells. This will definitely help to tackle the cyber-crimes.

REFERENCES:

1. Aggarwal, Gifty (2015), General Awareness on Cyber Crime. *International Journal of Advanced Research in Computer Science and Software Engineering*.

2 A comparative analysis of cybersecurity initiatives worldwide, international telecommunication union, Geneva

3. Barkha, Rama Mohan, U. (2011) Cyber Law and Crimes, IT Act 2000 & Computer Crime analysis. (3rd ed.), ISBN: 978-93-81113-23-3.

4. Cybercrime classification,[Online],Available: http:// shodhganga. inflibnet.ac.in/ bitstream /10603/7829/12/12_ chapter % 203.pdf [29 September 2013] 4. Cybercrime system requirements in India: Most necessary thing inIndia, [Online],Available: http://www.cyberlawsindia.net/ requires.

5.https://cybercrime.gov.in/Webform/Crime_OnlineSafetyTips.aspx

6.https://www.tutorialspoint.com/fundamentals_of_science_and_technology/cyber_crime_and_cyber_security.htm#:~:text=Cyber%20security%20is%20a%20potential,or%20exploitation%20or%20even%20theft.

7. Aparna and Chauhan, Meenal (2012), Preventing Cyber Crime: A Study Regarding Awareness of Cyber Crime in Tricity. *International Journal of Enterprise Computing and Business Systems*, January, Vol 2.