International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Need of Media Information Literacy in Cyber Crime

Dr. Sewa Singh Bajwa

Professor, Department of Journalism and Mass Communication, Chaudhary Devi Lal University, Sirsa, India

Abstract: ***This paper explores the increasing prevalence of cybercrime in India and the urgent need for digital literacy to mitigate its risks. The digital world, while offering numerous benefits, has also given rise to new forms of criminal activity. Cybercrime, including hacking, identity theft, phishing, malware attacks, and more, poses a significant threat to individuals and businesses. The situation in India is particularly concerning, with a sharp rise in cyber-attacks in recent years. The paper emphasizes the role of digital literacy in combating cybercrime, highlighting its importance in identifying potential threats, protecting personal information, and responding appropriately to cyber-attacks. It also discusses the challenges to achieving digital literacy in India, such as lack of access to technology, inadequate infrastructure, and a lack of awareness and training. The paper concludes by suggesting ways to promote digital literacy, including providing access to technology, creating digital resources, offering training and education, encouraging digital citizenship, fostering a culture of learning, and conducting public awareness campaigns.***

Keywords: Cybercrime in India, Digital Literacy, Cyber security, Digital Infrastructure, Public Awareness Campaigns

1. Introduction

The digital world refers to the realm of digital technology and the internet, where information is stored, processed, and transmitted electronically. With the rapid advancement of technology, the digital world has become an integral part of our daily life and influences the way we communicate, work, learn, and entertain ourselves. The internet is the backbone of the digital world, connecting billions of people across the globe. It provides access to a wealth of information and resources, including websites, online databases, and digital libraries. Social media platforms, such as Twitter, Facebook and Instagram, allow individuals to connect and communicate with each other on a global scale.

However, the digital world has also raised concerns about privacy and security. With the vast amount of personal information shared online, there is a risk of identity cyber bullying, theft and online fraud. As such, individuals and businesses need to take steps to protect their online security and privacy. The digital world has transformed how we live, work, and communicate. It has provided us with countless opportunities and resources that were once unimaginable, but it also requires us to be mindful of the potential risks and challenges that come with it. The digital world has brought about significant advancements in technology and communication, but it has also given rise to new forms of criminal activity.

Cybercrime is a growing problem in the digital world, with criminals using the internet and digital technologies to commit various types of fraud and illegal activities. Cybercrime can take many forms, including hacking, identity theft, phishing, malware attacks, ransomware, and distributed denial-of-service (DDoS) attacks. Hackers use their knowledge of computer systems to gain unauthorized access to networks, stealing sensitive and private information such as credit card numbers, passwords, and other personal data.

There are several types of cyber Crime:

- **Identity theft:** When a person's information, such as their name, address etc., is stolen and used to commit fraud or other crimes.
- **Hacking:** The unauthorized access to a computer or computer system to steal data, modify or destroy data, or cause other damage is called hacking.
- **Malware:** Malicious software that is designed to infect a computer system or network, often to steal data or cause damage.
- **Phishing:** The use of fraudulent emails, text messages, or other communications to trick people into providing sensitive information or downloading malware.
- **Cyberbullying:** Using the internet, social media, or other digital technologies to harass, intimidate, or threaten others.
- **Online scams:** Fraudulent schemes designed to trick people into giving away money or personal information, such as lottery scams, phishing scams, and investment scams.
- **Cyberstalking:** The use of the internet or other digital technologies to harass, intimidate, or stalk someone.
- **Ransomware:** Malware that encrypts a victim's data and demands payment in exchange for the decryption key.
- **Distributed Denial of Service (DDoS) attacks:** When a network is overwhelmed with traffic from multiple sources, causing it to crash or become unavailable to users it is called as Distributed Denial of Service.
- **Cyber espionage:** The use of computer networks to gain unauthorized access to confidential information or trade secrets, often for industrial or political espionage.

Cyber Crime in India

India has been a victim of cybercrime since the early 2000s when the country began to experience an increasing number of cyber-attacks. Cybercrime refers to any criminal activity involving computer networks or digital technologies and can include a wide range of offences, such as hacking, cyber espionage, identity theft, and online fraud.

The history of cybercrime in India can be traced back to the early 2000s when the country began to see an increase in cyber-attacks. At the time, India did not have a strong legal

framework to address cybercrime, and law enforcement agencies were ill-equipped to deal with this new form of crime. As a result, cybercriminals were able to operate with relative impunity, and the number of cyber-attacks continued to rise. In 2000, the Indian government passed the Information Technology Act, which provided a legal framework for dealing with cybercrime. The Act criminalized a wide range of cyber offences, including hacking, identity theft, and online fraud, and provided for penalties that included imprisonment and fines. Despite the passage of the Information Technology Act, cybercrime continued to be a major problem in India. In 2005, the country experienced one of its most high-profile cyber-attacks, when a group of hackers targeted the Indian Parliament's website. The attack, which was allegedly carried out by a group of Pakistani hackers, resulted on the website being shut down for several days.

Over the years, cybercrime has continued to be a major problem in India. In 2016, the country experienced one of its largest data breaches when a group of hackers targeted the databases of several major banks. The hackers were able to gain access to sensitive customer data, including account numbers and personal information. In recent years; the Indian government has taken steps to combat cybercrime. In 2018, the government established the National Cyber Security Coordinator, which is responsible for overseeing the country's cybersecurity efforts. The government has also taken steps to increase awareness about cybercrime and provide training to law enforcement agencies. Despite these efforts; cybercrime continues to be a major problem in India. In 2020, the country saw a sharp increase in cyber-attacks, as criminals took advantage of the COVID-19 pandemic to launch phishing attacks and other scams.

The statistics of the National Crime Records Bureau (NCRB) related to cybercrime are also very shocking. According to the final report released by NCRB in the year 2021, the number of cases of broadcasting sexual content is 12 per cent of the total cybercrime across the country and the worrying situation is that such cases have increased 3 times in the last 5 years. UP, Assam, Odisha, Karnataka, and Kerala are among the top 5 states in this matter.

Cyber-crime doubled in the last 5 years in the country:

Year	Cyber Crime Cases	Cyber Crime Rate
2021	52974	3.9
2020	50035	3.3
2019	44735	3.7
2018	27248	2.1
2017	21796	1.7

Top 5 States in Cyber Crime:

As per the NCRB 2021 Report top five states in terms of cyber crime incidents are as under:

State	Cyber Crime Incidents
Telangana	7003
Maharashtra	1678
Bihar	1373
Odisha	1205
Andhra Pradesh	952

Cyber Crime and Digital Literacy

Cybercrime is a growing concern in the digital age, as more and more people are relying on technology to conduct their daily lives. The increasing use of technology has led to a rise in cyber attacks and digital crimes, and it is becoming increasingly important for individuals to be digitally literate to protect themselves and their information from potential cyber threats. Cybercrime refers to any illegal activity that involves the use of digital technology. This can include hacking, identity theft, online harassment, and cyber-stalking. Cybercriminals often use a range of techniques to gain access to personal information, including phishing scams, malware, and social engineering tactics. These attacks can cause significant harm to individuals and organizations, including financial loss, reputational damage, and even physical harm.

Digital literacy, on the other hand, refers to the ability to effectively use and understand digital technology. This includes the ability to navigate digital platforms, use software and hardware, and understand the potential risks associated with using technology. Digital literacy is essential in today's society, as it allows individuals to participate fully in the digital world and protect themselves from cyber threats. There are several ways in which digital literacy can help individuals protect themselves from cybercrime. First, it can help individuals identify potential threats and take appropriate action to prevent them. For example, a digitally literate individual may be able to recognize a phishing email and avoid clicking on any links or providing personal information. Similarly, they may be able to identify suspicious behavior on their social media accounts and take steps to secure their accounts.

Second, digital literacy can help individuals protect their personal information online. This includes using strong passwords, regularly updating software and security settings, and avoiding sharing sensitive information on public platforms. A digitally literate individual is more likely to be aware of the potential risks associated with sharing personal information online and take steps to protect their data.

Third, digital literacy can help individuals respond appropriately in the event of a cyber-attack. This includes knowing whom to contact and what steps to take to report the incident and minimize the damage. A digitally literate individual may also be able to help others who have been affected by a cyber-attack by sharing information and resources.

To promote digital literacy and combat cybercrime, individuals need to be educated about the potential risks associated with using technology. This can include providing training and resources to individuals and organizations, as well as promoting awareness of the importance of digital literacy in schools and other educational settings.

In addition, governments and organizations can take steps to promote cybersecurity and combat cybercrime. This can include investing in cybersecurity infrastructure, providing support and resources to victims of cybercrime, and working

with law enforcement to identify and prosecute cybercriminals.

Cybercrime is a growing concern in the digital age, and it is becoming increasingly important for individuals to be digitally literate to protect themselves and their information from potential cyber threats. Digital literacy can help individuals identify potential threats, protect their personal information, and respond appropriately in the event of a cyber-attack. By promoting digital literacy and investing in cybersecurity infrastructure, we can work together to combat cybercrime and create a safer digital world for all.

Problems in the Way of Digital Literacy

Digital literacy is becoming increasingly important in today's world, as technology continues to play an important role in our daily lives. However, in India, there are several challenges to achieving digital literacy, including lack of access to technology, inadequate infrastructure, and a lack of awareness and training.

One of the biggest challenges to achieving digital literacy in India is the lack of access to technology. While internet penetration in India has grown significantly over the past decade, there are still many people who do not have access to the internet or other digital technologies. This is particularly true in rural areas, where internet connectivity and other digital infrastructure are often lacking.

Another challenge is inadequate infrastructure. In many parts of the country, internet speeds are slow, and there are frequent power outages that can disrupt connectivity. This can make it difficult for people to access digital resources and can hinder their ability to learn and develop digital skills.

A lack of awareness and training is another major challenge to achieving digital literacy in India. Many people are simply not aware of the benefits of digital technologies, or they may not understand how to use them effectively. This can be particularly true for older generations, who may not have grown up with digital technologies and may be more resistant to adopting them.

There are several ways in which India can address these challenges and promote digital literacy. One approach is to invest in digital infrastructure, including high-speed internet connectivity and reliable power sources. This can help to ensure that people in even the most remote areas of the country have access to the internet and other digital resources.

Another approach is to provide training and education on digital technologies. This can include formal training programs for students, as well as community-based programs that are designed to reach people who may not have access to formal education. These programs can help to promote awareness of digital technologies and teach people how to use them effectively.

In addition, India can promote the development of digital resources that are accessible and affordable for people at all income levels. This can include initiatives such as providing low-cost smartphones or tablets, as well as creating digital resources that are available in local languages and that are designed to meet the specific needs of different communities.

Source: https://reciprocity.com/resources/what-are-cybersecurity-threats/

Finally, India can work to promote digital literacy through public awareness campaigns and other outreach efforts. By highlighting the benefits of digital technologies and educating people about how to use them effectively, these campaigns can help to promote a culture of digital literacy throughout the country.

Achieving digital literacy targets in India is a complex challenge that requires a multifaceted approach. By investing in digital infrastructure, providing training and education, promoting accessible digital resources, and raising awareness of the benefits of digital technologies, India can work to overcome these challenges and promote

digital literacy throughout the country. By doing so, India can help to ensure that all of its citizens are able to participate fully in the digital world and to reap the many benefits that digital technologies have to offer.

How to Promote Digital Literacy

Promoting digital literacy is crucial in today's world, where technology plays a significant role in our daily lives. Digital literacy enables individuals to use technology to access information, communicate effectively, and solve problems efficiently. Here are some ways to promote digital literacy:

Provide access to technology: The first step in promoting digital literacy is to provide access to technology. This includes providing affordable access to computers, tablets, and smartphones, as well as access to high-speed internet connectivity. Schools, libraries, and community centres can be excellent resources for providing access to technology.

Create digital resources: Developing digital resources that are easy to use and accessible is an effective way to promote digital literacy. These resources can include instructional videos, interactive tutorials, and online learning platforms. Additionally, creating digital resources in local languages can help to reach more people and improve accessibility.

Offer training and education: Providing training and education on digital technologies is an essential component of promoting digital literacy. Schools, colleges, and universities can offer courses and workshops that teach digital skills, such as how to use productivity software, create digital content, and navigate the internet. Community centres can also offer digital literacy programs, especially for seniors or people who cannot afford expensive training.

Encourage digital citizenship: Digital literacy includes responsible and ethical behaviour online. Promoting digital citizenship can help people use technology effectively while also being mindful of privacy and security concerns. This includes educating people on how to protect their personal information online, avoid cyberbullying, and recognize fake news.

Foster a culture of learning: Encouraging a culture of learning and exploration can promote digital literacy. Emphasizing the importance of lifelong learning and providing access to online resources, such as ebooks, audiobooks, and podcasts, can help people develop their digital skills.

Public awareness campaigns: Public awareness campaigns can raise awareness of the importance of digital literacy and help to dispel misconceptions about technology. These campaigns can be conducted through social media, billboards, or other media outlets.

2. Conclusion

To conclude, cybercrime has become a significant issue in India, with a growing number of individuals and organizations falling victim to various types of cyber-attacks. Cybercrime can result in significant financial losses, reputational damage, and even physical harm. It is, therefore, crucial to promoting digital literacy in India to minimize the risks of cybercrime.Digital literacy can help individuals and organizations to use digital technologies safely and effectively, reducing the likelihood of falling victim to cybercrime. By promoting digital literacy, people can learn how to protect their personal information, recognize phishing emails, and secure their online accounts. This, in turn, can help to minimize the risk of cyber-attacks and other forms of online fraud.

To promote digital literacy in India, there needs to be a concerted effort by the government, educational institutions, and the private sector to provide access to digital resources and offer training and education on digital technologies. Additionally, raising public awareness about the risks of cybercrime and promoting responsible behaviours online can help to create a culture of digital literacy in India.

In conclusion, the increasing prevalence of cybercrime in India highlights the urgent need for digital literacy. By promoting digital literacy, individuals and organizations can reduce the risks of cybercrime and maximize the benefits of digital technologies. It is essential to take steps to ensure that all individuals in India have access to the tools and resources they need to use technology safely and effectively, both now and in the future.

References

[1] Agarwal, N., & Tiwari, R. (2021). Digital Media Literacy in India: A Study of Awareness, Attitudes, and Practices. Journal of Media Literacy Education, 13(1), 56-71. https://doi.org/10.23860/JMLE-2021-13-1-5

[2] Anand, V., & Krishnamurthy, S. (2019). Digital Media Literacy and Its Role in Education: An Indian Perspective. Journal of Education and Practice, 10(10), 124-131. https://www.iiste.org/Journals/index.php/JEP/article/view/49608

[3] Datta, S., & Jain, S. (2020). Digital Media Literacy in India: A Study of Awareness, Usage, and Attitudes. Journal of Information Science Theory and Practice, 8(4), 13-29. https://doi.org/10.1633/JISTaP.2020.8.4.2

[4] Kumar, A., & Kumar, N. (2021). Digital Literacy in India: Challenges and Opportunities. International Journal of Information Management, 57, 102302. https://doi.org/10.1016/j.ijinfomgt.2021.102302

[5] Singh, S., & Bhatia, S. (2019). Digital Literacy and Cyber Security Awareness: Imperatives for India. In M. Gupta, P. Sharma, & A. Tiwari (Eds.), Human Development and Interaction in the Age of Ubiquitous Technology (pp. 203-214). IGI Global. https://doi.org/10.4018/978-1-5225-9815-7.ch012

[6] https://reciprocity.com/resources/what-are-cybersecurity-threats/