Journal of Advanced Multidisciplinary Research Studies and Development

ISSN : 2583-6404
Mar - Apr 2023

CYBER LAW AND CYBER SECURITY

Bageshree Deo
Faculty, Department of BBA (CA), Brihan Maharashtra College of Commerce (Autonomous), Pune.

Abstract
It is the 'Digital Age' today. Because of technological advancements, life has become easy and convenient for a common man. Thanks to Internet which has brought the world closer. It has provided multiple ways to gain knowledge, interact with people through email, social networking site that enable to reunite with old friends, transact online and many more utilities. Man is now dependent on the internet for all of his requirements. Social networking, online shopping, online schooling, online jobs, online banking can be done over the internet. But Internet is a blessing in disguise. If used cautiously and carefully, it is a boon. But wrong usage can create a disaster. Many cyber crimes have proliferated. It has become a major problem. As technology continues to advance, so do the threats and risks associated with it. It is imperative for individuals and organizations to be vigilant in protecting themselves against cyber attacks. To control it, one has to abide by the Cyber Security norms. One has to know and implement the security features while working online. Cyber security is supported by Cyber Law.
This paper aims to understand the different cyber crimes and and its causes. The main motive is to make the internet user aware of the security features and throw light on the safeguarding cyber laws.
Keywords: Internet, Cybercrime, Cyber security, Cyber Law.

► *Corresponding Author: Bageshree Deo*

Introduction

Cybersecurity refers to the practice of protecting computer systems, networks, and digital devices from unauthorized access, use, theft, or damage. Cybersecurity is essential in today's digital age because cyber attacks can have devastating consequences, such as financial loss, reputational damage, and even physical harm.
Cyber Law refers to the legal framework that administers the use of internet, computers and other digital device. Cyber crimes can be controlled and the cyber criminals can be legally charged by the cyber law.
"*Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet.*"[1]
Cybercrime is distinct from other types of crime that occur in society. The reason for this is that it has no territorial limits, and cyber criminals are unknown. It affects all parties, from government to business to citizens. With the rising use of information and Communication technology (ICT), cybercrime is on the rise in India.
So the concern is why the cyber crimes are increasing in numbers?
The Covid epidemic transformed cyber fraud into a business, wherein all regular offline practices were done online, right from schooling to business to banking.

[1] https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf

ISSN : 2583-6404
Mar - Apr 2023

Conceptual Framework:

According to the National Crime Records Bureau (NCRB) report for 2020, cybercrime increased by 12% across the country, but other crimes such as murder, theft, and cheating decreased owing to national and regional lockdowns.

"*India reported 11.8% rise in cyber crime in 2020; 578 incidents of 'fake news on social media*"[2]

Employees working from home, among other factors, have increased the number of cyber-attacks across the country.

(https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece)

"*Among States, the maximum cyber crime cases were reported in Uttar Pradesh followed by Karnataka, Maharashtra, Telangana and Assam, the NCRB (National Crime Records Bureau) data showed*"[3]

Karnataka has the largest amount of identity thefts and personation frauds utilising computer resources. Bihar has the greatest number of reported credit/debit card and ATM scams. Telangana reported the highest amount of online banking frauds, OTP frauds, cyber blackmailing or threatening, and social media fake news.

While Maharashtra had the biggest number of cheating cases (under Section 420),

Jharkhand had the highest number of internet gambling offences.

Today, the most common types of cyber attacks are malware, social engineering, hacking, credential compromise, web attacks, and DDoS (Distributed Denial of Service) attacks.

The main cause of Cyber crime is the weakness in the organisation's information system. This makes the system vulnerable for hackers to gain unauthorized access to system and data and cause significant harm.

Some examples of vulnerability include

- A flaw in a firewall that allows malicious hackers to gain access to a computer network.
- Inadequate security cameras
- Opening mails from unknown senders
- Clicking on invalid links
- Falling prey to suspicious requests

[2] https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece

[3] https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece

ISSN : 2583-6404
Mar - Apr 2023

Cybercrime is a continuous process. In this scenario, how to keep oneself safe and secure. One should follow some simple safeguarding techniques like:
Using a full-service internet security suite.
Using strong passwords and changing it frequently.
Keep your software updated.
Manage your social media settings.
Strengthen your home network.
Keep up to date on major security breaches.
Knowing some simple measures and knowing whom to call if you experience or witness others engaging in criminal activity online is necessary. As stated in The National Cyber Crime Reporting Portal (https://cybercrime.gov.in/) "*This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints.*"
One of the most common cyber threats is phishing, where attackers attempt to gain sensitive information such as passwords and financial data by posing as a trustworthy entity, like a bank or popular website. Phishing attacks are often carried out through emails or text messages that contain links to fake websites designed to look like the legitimate ones. To avoid falling victim to phishing attacks, it is important to always verify the legitimacy of any requests for sensitive information before providing them. This can be done by independently contacting the organization through a known and verified method of communication, such as calling their official customer service line.
"*Spear phishing" is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents.*"[4]
Another cyber threat that has become increasingly prevalent is ransomware. Ransomware is a type of malware that encrypts the victim's files or systems, making them inaccessible until a ransom is paid. To avoid falling victim to ransomware attacks, it's important to regularly back up your data and keep your operating systems and antivirus software up to date as well as to avoid opening suspicious emails or downloading files from untrusted sources.
"*Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files."*[5]
Another cyber crime is the Dark web which is not known to many. What crimes are on the dark web?
Some of the more prevalent illegal activities include arms trafficking, drug dealing, and the sharing of exploitative content—often involving children—such as pornography and images of violence and other types of abuse.

[4] https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf
[5] https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/#:~:text=Continuous%20data%20backups%3A%20Ransomware's%20definition,and%20without%20paying%20a%20ransom.

ISSN : 2583-6404
Mar - Apr 2023

As stated by https://www.cisa.gov/stopransomware/dark-web-and-cyber-crime, the Dark web requires Tor Browser and all Tor urls end in .onion.

Tor was created by the U.S. Naval Research Lab in 1995. The Tor Project (nonprofit) created in 2006. It mainly deals with internet browsing and site hosting. It routes traffic through multiple nodes and encrypt at every step on the way. There are layers of encryption as compared to an onion, hence the name 'The Onion Router' and the top level domain is .onion

With the development of technology, the first step to prevent from unauthorized access to any computer, is the password. It is mandatory. Since every operating system requires password to log in. In fact, strong and complicated passwords not just protect us from attackers to gain access but it also slows down the process of illegal entry and consumes more time to crack the password. Hence it is recommended to use random passwords and a combination of numbers, symbols and text. Such passwords are best to use as it takes long time to guess. With many complex passwords for your many different accounts, how can you keep it all straight? Surprisingly, different passwords for different accounts are less risky than using the same password on multiple sites, re-using old passwords, using easy-to-guess passwords, letting your software remember your passwords, or not frequently changing your passwords.

In addition, it is important to use strong and unique passwords for each account and enable two-factor authentication whenever possible. Two-factor authentication adds an extra layer of security by requiring users to provide additional verification, such as a code sent to their phone or email, before accessing their account. It is important to educate yourself and stay informed about the latest cyber threats and security best practices.

Inspite of taking all these security measures, there are chances of cyber attacks. Destructive minds are always at work, inventing new ways of cracking into the system, stealing data and creating a crime and adding to the crime pile.

But there is always an antidote written by the constructive minds. Be it an antivirus, firewall or cryptography.

Antiviruses is a security option that protects networks from these malwares. Multiple Antivirus packages are available in the market today, like Norton, Quick Heal, Seqrite, McAfee etc. An organization can rely on Firewall too. Firewall can be hardware, software or combination of both which will inspect network traffic passing through it and either accept the message or reject the message based on set of rules. Firewall policies allow all type of traffic but block some services like Telnet/SNMP, and port numbers those are used by an attacker. If network administrator forgets to block something then it might be exploited after sometime by the attacker without your knowledge and permission. For mobile users, firewall allows access in to the private network with the help of secure login procedure and it authenticates the certificates. Henceforth for public Wi-Fi users it is concern to always check whether the firewall is on for public networks. Next generation firewalls are focused on blocking malware and suspicious activities with Intrusion Detection and Prevention systems. IDS monitors the suspicious events happening in network any case any intrusion occurs IDS provide some alert warning across the entire network. Among different types of firewalls such as:

- Packet Filter firewall
- Application Gateway (Proxy) Firewall
- Web Application Firewall (WAF)
- Next-Gen Firewall

Organizations use combination of 2-3 types of firewalls together for the better security.

Also the cyber law is always at one's beck and call. In her research paper, Pallavi Kapila has mentioned,"*In order to stop and punish the cyber criminals, "Cyber Law" was introduced. Cyber Law can be defined as law of the web, i.e., it is a part of the legal systems that deals with the Internet, Cyberspace and with other legal issues like online security or online privacy.*[6]

Several laws have been introduced in order to stop crimes related to the Internet and punish the criminal. These are laws that govern the Cyberspace cybercrimes, digital and electronic signatures, data protections and privacy.

The Cyber Law in India[7] gives us a list of Cyber laws in India. To name a few we have:

Sl.No Offences Section Under IT Act

1. Tampering with computer source Documents Sec.65
2. Hacking with computer systems, Data Alteration Sec.66
3. Sending offensive messages through communication service, etc Sec.66A
4. Dishonestly receiving stolen computer resource or communication device Sec.66B
5. Identity theft Sec.66C
6. Cheating by personation by using computer resource Sec.66D
7. Violation of privacy Sec.66E
8. Cyber terrorism Sec.66F
9. Publishing or transmitting obscene material in electronic form Sec .67
10. Un-authorized access to protected system Sec.70
11. Penalty for misrepresentation Sec.71
12. Breach of confidentiality and privacy Sec.72
13. Publishing False digital signature certificates Sec.73
14. Publication for fraudulent purpose Sec.74

Research Methodology

This is a descriptive research that is empirical, or primary data based where most of the data collected is qualitative in nature. A questionnaire in the form of Google Form was circulated amongst the students, working professionals, non-working professionals and non-professionals from Pune of varied age groups. This form was prepared to collect information regarding their awareness of cyber security and cyber law. Through this form, the experiences of people were understood.

The questions were multiple choice based objective questions. Online Google Form was preferred than physical form, as more people can be reached. Also, people are more comfortable with filling the online form. They are assumed to be technology literate people.

The key questions in the form had mainly focused on:

1) The age of person
2) Use of Internet for
3) Are you aware of Cyber Threats
4) Were you ever been a victim of cyber threat?
5) Which threat did you come across?
6) What security measures are adopted?

Sample size collected was 51.

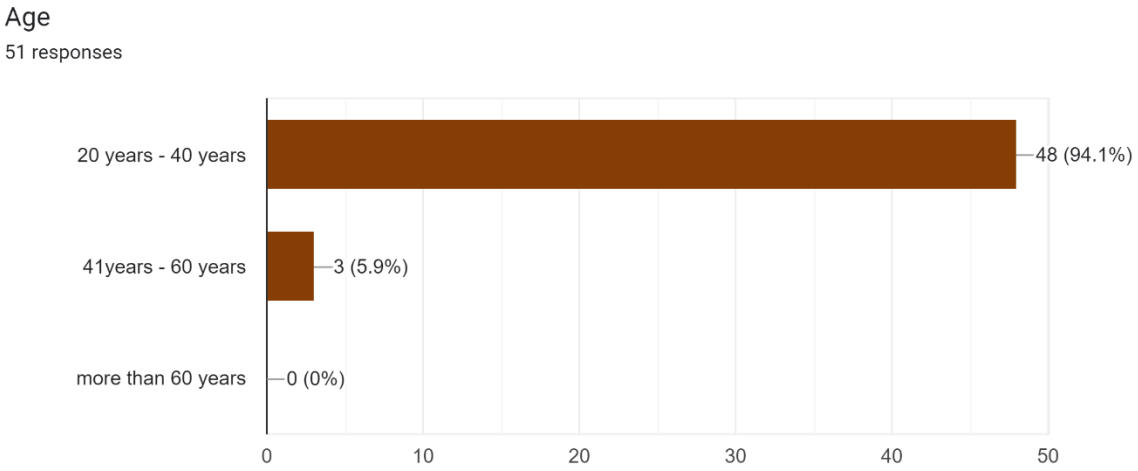
[6] https://www.researchgate.net/publication/350107577_Cyber_Crimes_and_Cyber_Laws_in_India_An_Overview

[7] https://cyberpolicebangalore.nic.in/pdf/Cyber%20law%20IPC.pdf

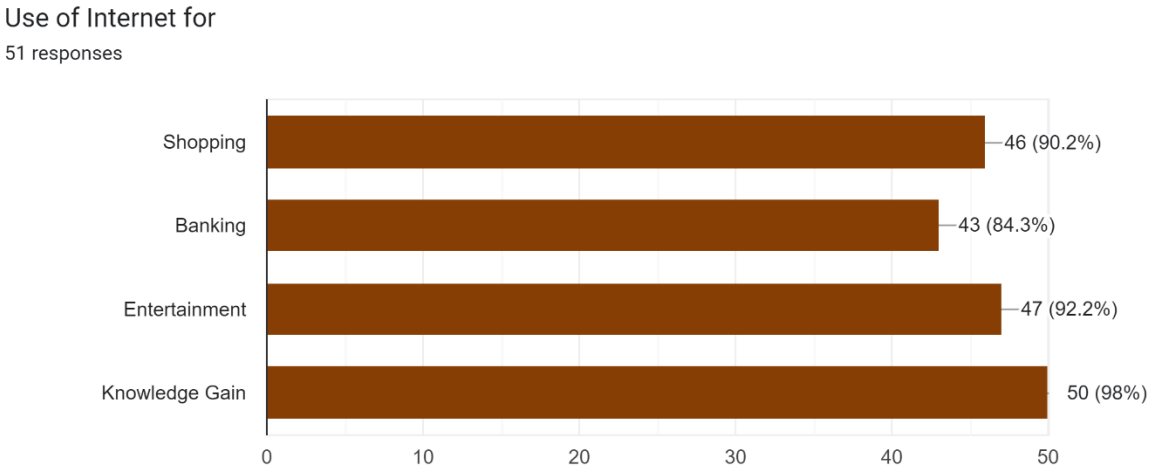
ISSN : 2583-6404
Mar - Apr 2023

Data analysis and findings

The data collected has revealed some very interesting facts.

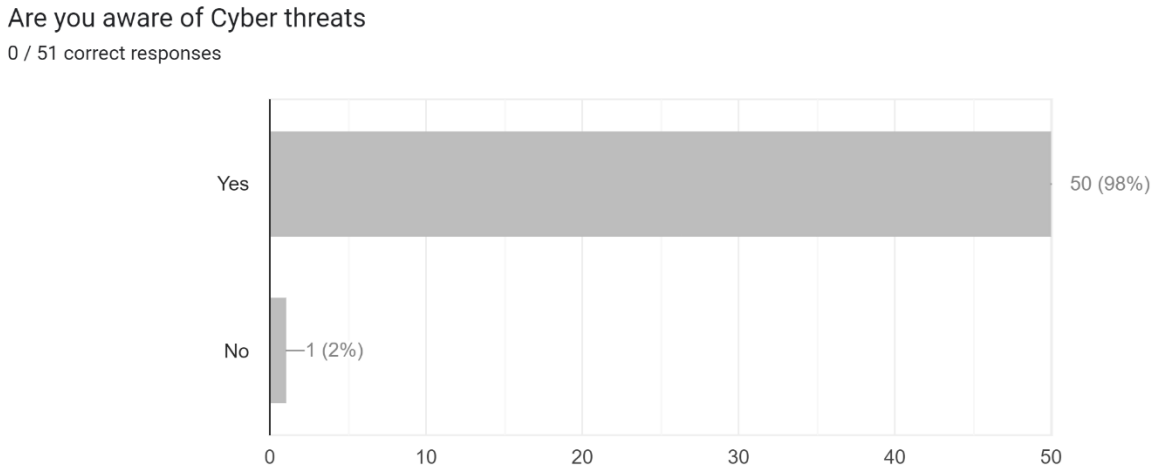


The average age of the respondents is between 20 to 40 years of age since the highest number of respondents, that is 94.1%, fall in this age group. This indicates that the maximum use of Internet is done by the young crowd.

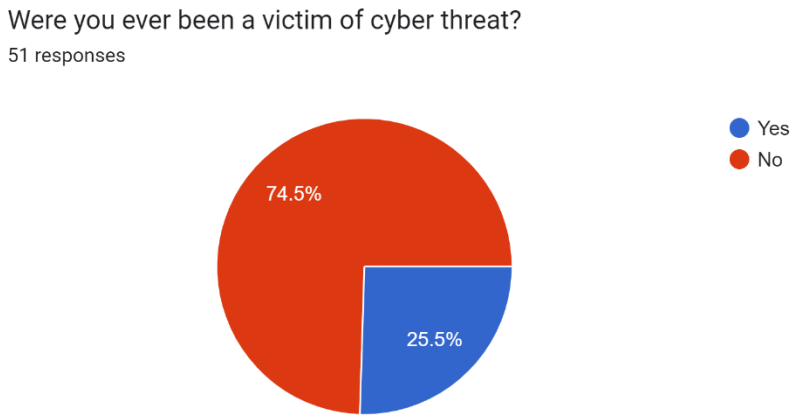


The use of Internet is varied in all the respondents. According to the graph, it is 98% for knowledge gain where there is a possibility of downloading certain suspicious data or any doubtful open source. 92.2% for Entertainment which can carry any Trojans or virus and social engineering alongwith it. Most vulnerable is Banking(84.3%) and Shopping(90.2%). Covid 19 and the growth of technology together have encouraged digital Banking, where there are maximum chances of phishing, ransomware, spoofing.

ISSN : 2583-6404
Mar - Apr 2023

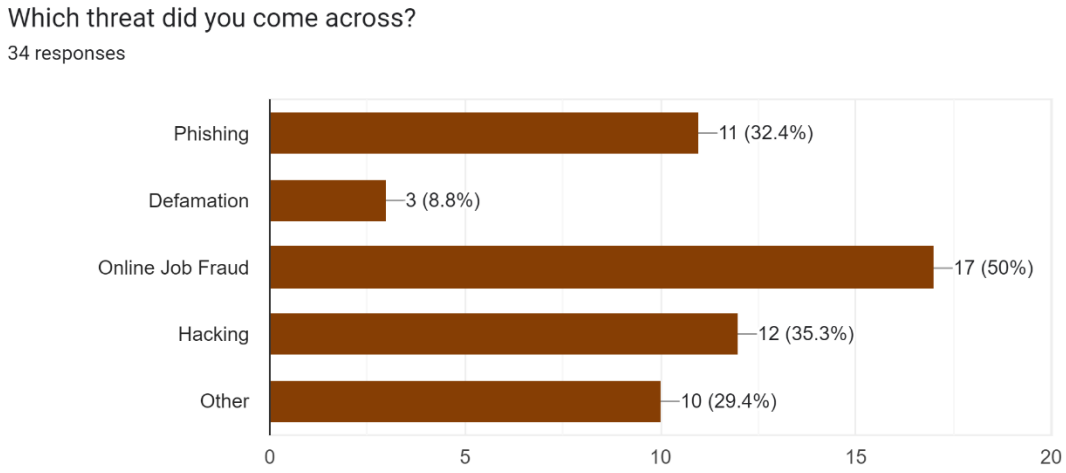


According to the graph, almost 98% of the respondents are mindful of the cyber threats and only 2% are not. Inspite of knowing the threats, people today are using Internet and are dependent on it for some functions as it seems to be convenient.

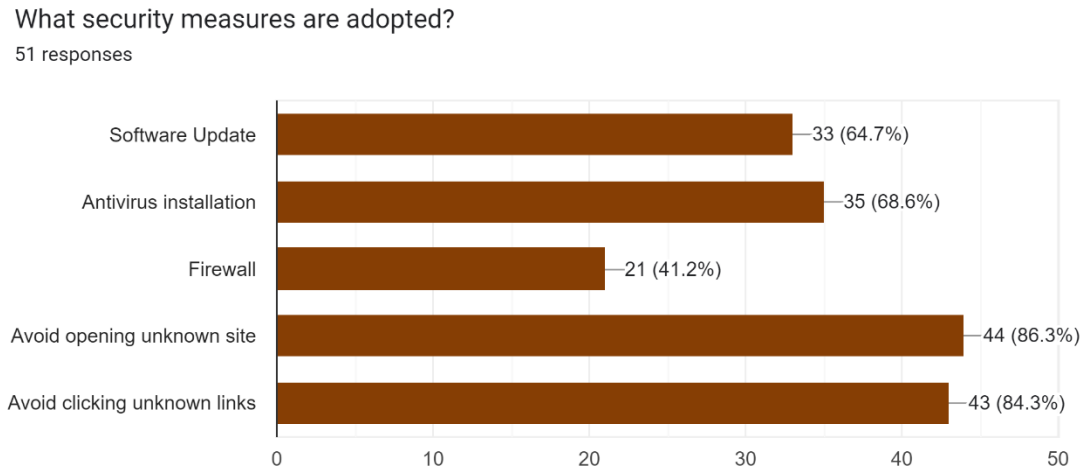


Unknowingly, 25.5% of respondents are victims of cyber threat even after taking the necessary precautions. Everyday some or the other threat creeps in.

ISSN : 2583-6404
Mar - Apr 2023



Some threats were added in the form. Out of which online job fraud seems to be the highest (50%). People do have come across the phishing threat and hacking.



Respondents have taken the necessary care while dealing with Internet. The graph shows that people are now more alert and careful while carrying out tasks over Internet.

Conclusion

Cyber threats continue to evolve and become more sophisticated. As such, it is important to remain vigilant and take proactive measures to protect yourself and your organization from potential attacks. Remember, prevention is key when it comes to cybersecurity. Always be cautious and suspicious of unsolicited emails or messages, especially those requesting sensitive information. By following these best practices and staying informed, you can help ensure that your personal and professional information remains secure in today's digital age. Remember, cybersecurity is a shared responsibility. It is important to not only protect yourself but also to encourage others around you to do the same. Everyone should attend cybersecurity training course, and play an

ISSN : 2583-6404
Mar - Apr 2023

important role in promoting cyber awareness and safety in our daily lives. Stay safe and Stay informed!

References

1. https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf
2. https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece
3. https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece
4. https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf
5. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/#:~:text=Continuous%20data%20backups%3A%20Ransomware's%20definition,and%20without%20paying%20a%20ransom.
6. https://www.researchgate.net/publication/350107577_Cyber_Crimes_and_Cyber_Laws_in_India_An_Overview
7. https://cyberpolicebangalore.nic.in/pdf/Cyber%20law%20IPC.pdf