Humanities Report
"Impact of Cyber Financial crime on mental health"

UHU005 - Humanities for Engineers
Sixth-Semester

Submitted by:

Sukirat Singh Monga (102165014)
Aman Aggarwal (102165010)
Pranav Prakash (102165011)
BE Third Year, ENC [3NC5]

Submitted To:
Ms. Rishita Goyal

School of Humanities & Social Sciences Thapar Institute of Engineering & Technology, Patiala May 2024

COPYRIGHT NOTICE

LETTER OF TRANSMITTAL

Date: 4 May, 2024

Respected Madam,

This is to inform you that we have prepared a report on the topic “Impact of Cyber Financial crime on mental health” and now we are submitting the same to you.

Our analysis includes knowledge people have regarding this topic, whether they have ever faced any such issues in their lives, their course of action in such cases, and their awareness regarding cyber laws, cyberbullying, and its mental impact. We concluded that people are highly unaware of this and are curious about this topic and also how we can educate and spread knowledge about this. We have provided an outline of the complete survey and the solution in the attached report for your review.

Through this report and survey conducted, we tried to get an insight to people’s point of view in context to Cyber security,Cyber financial crimes and its impact on mental health.

Thank you for trusting us to complete this research for you. We appreciate your time and look forward to your review. Please review the official report and respond with your thoughts.

Lastly, we would be thankful if you could please give your judicious advice on our effort.

Yours Sincerely,

Sukirat Singh Monga (102165014)
Aman Aggarwal(102165010)
Pranav Prakash(102165011)

CERTIFICATE

This is to certify that the Report titled "Impact of Cyber Financial crime on mental health" embodies the original work done by students of Thapar Institute of Engineering and Technology, Batch 3NC5:

Sukirat Singh Monga (102165014)
Aman Aggarwal(102165010)
Pranav Prakash(102165011)

Under the Supervision of Ms. Rishita Goyal

Date: 04 May,2024

ACKNOWLEDGEMENTS

We want to express our sincere gratitude and profound veneration to our research supervisorMs. Rishita Goyal for providing her invaluable guidance, comments and suggestions throughout the course of the report. She has been of great help in our venture, and an indispensable resource of technical knowledge. She is truly a fantastic mentor to have.

We are also thankful to our friends who devoted their valuable time and helped us in all possible ways towards successfully completing this report. We thank all those who have contributed either directly or indirectly towards this report.

Above all, we would also like to thank the almighty and our families for their unyielding loveand encouragement. They always wanted the best for us and we admire their determination and sacrifice.

ABSTRACT

This report investigates the burgeoning threat of cyber financial crime within the broader context of cybersecurity's paramount importance in contemporary national security discourse. Commencing with an elucidation of foundational technical concepts, the report navigates through the intricate terrain of specialized viruses and worms before delving into the nexus between cybersecurity, cybercrime, and cyber espionage.

The genesis of this report stems from a pervasive dearth of awareness surrounding cybersecurity among individuals, leaving them perilously exposed in the digital milieu. It underscores the alarming ease with which malicious actors can perpetrate financial crimes, leveraging digital channels to orchestrate fraud, theft, and money laundering, thereby exacerbating vulnerabilities in financial systems worldwide.

The evolution of cyber-financial crime reflects the rapid advancement of technology and the expanding attack surface presented by interconnected digital networks. Criminals exploit weaknesses in cybersecurity defenses, exploit loopholes in financial software, and exploit human vulnerabilities through social engineering tactics to perpetrate their illicit schemes.

Mitigating the risks posed by cyber-financial crime requires a multifaceted approach encompassing technological innovation, regulatory enforcement, and public awareness initiatives. Financial institutions must invest in robust cybersecurity measures, including encryption protocols, anomaly detection systems, and comprehensive employee training programs to mitigate the threat of cyber attacks..

People nowadays face cyber thefts, fraud, and other forms of online issues that affect their mental health. After surveying, we learned that people are unaware of this, continuously suffer, and sometimes cannot cope.

We also considered and surveyed about the current state of cyberbullying nowadays and its impact on mental health.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

Cyber-Financial Crime

Cyberfinancial crime poses an increasingly significant threat in today's interconnected digital landscape, challenging traditional notions of security within financial systems. As technology continues to advance and financial transactions increasingly migrate online, criminals are exploiting vulnerabilities to perpetrate a wide array of illicit activities, ranging from fraud and identity theft to money laundering and extortion. As organizational assets are made up of multiple disparate systems, an effective and efficient cyber security posture requires coordinated efforts across all its information systems. Therefore, cyber-financial crime is made up of the following sub-domains:

Fredrick Chang (2012), former Director of Research at the National Security Agency in the United States, discusses the interdisciplinary nature of cybersecurity:

> ***"A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the required traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed."***

In attempting to arrive at a more broadly acceptable definition aligned with the genuinely interdisciplinary nature of cyberfinancial crime, we reviewed relevant literature to identify the range of meanings, discern dominant themes, and distinguish different aspects. This research was augmented by multiple engagements with a multidisciplinary group of cybersecurity practitioners, academics, and graduate students who could not cope up mentally with these ongoing cyber frauds. Together, these two activities resulted in a new, more inclusive, and unifying cyber-financial definition that will hopefully enable an enhanced and enriched focus on interdisciplinary cybersecurity. This report reflects the process used to develop a more holistic definition that better situates cybersecurity as a multidisciplinary activity, consciously stepping back from the predominant technical view by integrating multiple perspectives.

1.1 What are some of the cyber-financial crime sub-domains?

Payment Card Fraud: This involves unauthorized use of credit or debit card information for fraudulent transactions, including card skimming, card-not-present fraud, and identity theft related to payment cards.

Phishing and Spoofing: Cybercriminals send deceptive emails or messages impersonating legitimate entities to trick individuals into disclosing sensitive financial information, such as login credentials or account details.

Ransomware Attacks: Malicious software encrypts victims' files or systems, demanding payment (often in cryptocurrency) for decryption or to prevent data leaks, thereby disrupting operations and extorting funds from businesses and individuals.

Insider Threats: Employees or insiders with privileged access may misuse their authority to commit financial crimes, such as embezzlement, insider trading, or data theft for financial gain.

ATM Skimming: Criminals install devices on automated teller machines (ATMs) to capture card details and personal identification numbers (PINs), enabling them to withdraw funds fraudulently or clone cards for unauthorized transactions.

Stock Market Manipulation: Cybercriminals may engage in activities such as pump-and-dump schemes, where they artificially inflate the price of stocks through false information dissemination, then sell off their holdings for profit.

Cryptojacking: Malicious actors hijack victims' computing resources to mine cryptocurrencies without consent, draining computing power and energy resources while profiting from the generated digital currencies.

Business Email Compromise (BEC): Cybercriminals compromise email accounts of executives or employees to orchestrate fraudulent financial transactions, such as wire transfers or invoice manipulation, often resulting in substantial financial losses for organizations.

1.2 The importance and challenges of cyber-financial crime

Given the rapidly evolving technological landscape and the fact that the adoption of software is ever-increasing across various sectors, including finance, government, military, retail, hospitals, education, and energy, to name a few, more and more information is becoming digital and accessible through wireless and wired digital communication networks and across the omnipresent internet. All this highly sensitive information is of great value to criminals and evil-doers, which is why it is important to protect it using strong cyber security measures and processes.
The importance of good cyber financial crime strategies is evident in the recent high-profile security breaches of organizations such as Equifax, Yahoo, and the U.S. Securities and Exchange Commission (SEC), who lost extremely sensitive user information that caused irreparable damage to both their finances and reputation. And as the trend suggests, the rate of cyber-attacks show no sign of slowing down. Companies, both large and small, are targeted everyday by attackers to obtain sensitive information or cause disruption of services.

The same evolving technological landscape also challenges implementing effective cyber security strategies. Software constantly changes when its updated and modified which introduces new issues and vulnerabilities and opens it up for various cyber-attacks. Furthermore, IT infrastructure evolves as well with many of the companies already migrating their on-premise systems to the cloud which introduces a whole new set of design and implementation issues resulting in a new category of vulnerabilities. Companies are unaware of the various risks within their IT infrastructure and hence fail to have any cyber security countermeasures in place until it's far too late.

1.3 Cyber bullying.

Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behavior, aimed at scaring, angering or shaming those who are targeted.

Examples include:

- spreading lies about or posting embarrassing photos or videos of someone on social media.
- sending hurtful, abusive or threatening messages, images or videos via messaging platforms.
- impersonating someone and sending mean messages to others on their behalf or through fake accounts.

CHAPTER 2

LITERATURE REVIEW

Our literature review spanned a wide scope of sources, including a broad range of academic disciplines including: computer science, engineering, psychology, security studies, health.

Deconstructing the term cyberfinancial helps to situate the discussion within both domains of "cyber" and "financial" and reveals some of the legacy issues. “Cyber” is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality. It evolved from the term "cybernetics", which referred to the “field of control and communication theory, whether in machine or in the animal”. The term "cyberspace" was popularized by William Gibson’s 1984 novel, *Neuromancer,* in which he describes his vision of a three-dimensional space of pure information, moving between computer and computer clusters where people are generators and users of the information. What we now know as cyberspace was intended and designed as an information environment, and there is an expanded appreciation of cyberspace today. For example, Public Safety Canada (2010) defines cyberspace as “the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where… people are linked together to exchange ideas, services and friendship.” Cyberspace is not static; it is a dynamic, evolving, multilevel ecosystem of physical infrastructure, software, regulations, ideas, innovations, and interactions influenced by an expanding population of contributors, who represent the range of human intentions.

As for the term "financial security", in the literature we reviewed, there appeared to be no broadly accepted concept, and the term has been notoriously hard to define in the general sense. According to Buzan, Wæver, and Wilde (1998), discourses in security necessarily include and seek to understand who securitizes, on what issues (threats), for whom, why, with what results, and under what conditions. Although there are more concrete forms of security, the term takes on meaning based on one’s perspective and what one values. It remains a contested term, but a central tenet of security is being free from danger or threat. Further, although we have indicated that security is a contested topic, Baldwin (1997) states that one cannot use this designation as “an excuse for not formulating one’s own conception of security as clearly and precisely as possible.”

TYPES OF CYBER-FINANCIAL CRIMES

There is no proper legislation for cybercrimes in many countries/states. A comprehensive technique for the prevention of cybercrimes is needed.

- **Unauthorized access to data** : Information stored in computer may be personal records, corporate marketing plans or the detailed technical description of a new product. These types of data are sensitive as well as secret. Only authorized access to data should be possible otherwise the use of technology will be lost. The snooping of data is possible because of frequent need for access to computer-based data, and the routine use of telephone lines for data transfer.

- **Physical security :** Physical security can be ensured by locking disk files, hard disks, and removable storage media. Physical security can be achieved through limited access to computer rooms.

- **Passwords or other forms of identification :** Passwords or other codes are required to access computers or networks. Optical imaging is used in advanced systems to identify the unique network of blood vessels on the retinas of users. This technique is used in highly secure computer networks. Biometric security devices such as "eyeball scanners" and voice recognition units are very expensive and not available to most organizations.

- **Data encryption methods :** Data encryption is a technique used to turn information into unreadable form. This is done by authorized users by using soft wares and hard wares. There are many data encryption techniques. These may be unique to an individual organization or peculiar to its products. The Data Encryption Standard (DES) of the National Bureau of Standards is also a well-known technique. DES is used especially in banks.

- **Screen blanking :** Screen blanking is not a sophisticated method. In this technique, video monitors go blank after a period of nonuse. Because of this data entry stations cannot be viewed by unauthorized persons.

- **Wilful destruction of data :** Hackers and others people can destroy data. They are tempted to try their skill/knowledge and experience at invading protected systems which are assumed highly secure

- **Data manipulation :** Data manipulation is the most serious type of cybercrimes. If a person can do an unauthorized entry in a system, he/she can also be able to modify the data they contain. Employees who access organization's administrative computers in order to change records of their salaries are one examples of data manipulation.

CHAPTER 3

OBJECTIVES & RESEARCH METHODOLOGY

3.1 OBJECTIVES:

1. To identify how much people are aware of cyber-financial crime
2. To study how it tends to affect their mental health..
3. To find whether and how people face cyberbullying in daily life.
4. To find whether it is affecting their daily lives and what can be done to prevent cybercrime,
5. To increase awareness about cyber-financial crime and help people cope up in such situations.

3.2 RESEARCH DESIGN

The research was conducted in India, including respondents from TIET, Patiala, and some other places. The study was conducted in 2024 with the help of a self-designed questionnaire consisting of relevant questions. The focus of the study was on the impact of cyber-financial crimes on mental health.

The targeted population for the research study is individuals with smartphones and might have faced.

3.3 SAMPLE DESIGN

Convenience sampling has been used for the research. Questionnaires are provided to individuals based on researchers' convenience. The sample size for the research has been 200+ respondents.

3.4 TOOLS USED FOR DATA COLLECTION

Primary data used in the research is obtained through questionnaires and direct observations. The tool used in this research for data collection is Google form questionnaire and the response was collected in excel sheet.

3.5 TOOLS USED FOR DATA ANALYSIS

The tool used in this research for data analysis is pie chart and bar graph. These tools have been used to analyze and draw interpretations out of the data collected.

CHAPTER 4

RESULTS AND DISCUSSIONS

For this report, we conducted a survey on Google Form with a sample size of around 150+ including students, young adults and aged adults.

Q1. Gender

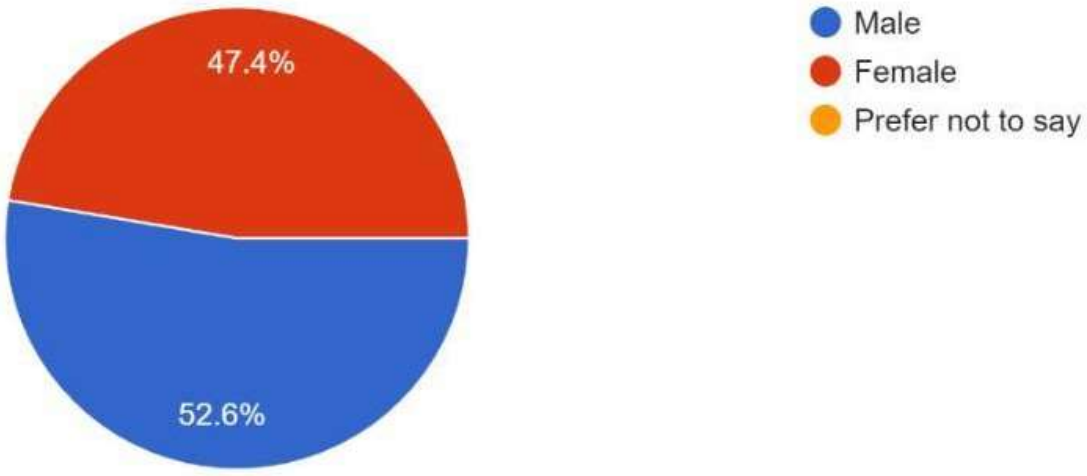


Fig1. Pie chart gender of the people participating in the survey

The pie chart shows that out of total 52.6% respondents are Male and 47.4% of the respondents are Female.

Q2. Variety of Age Groups participating in the survey.

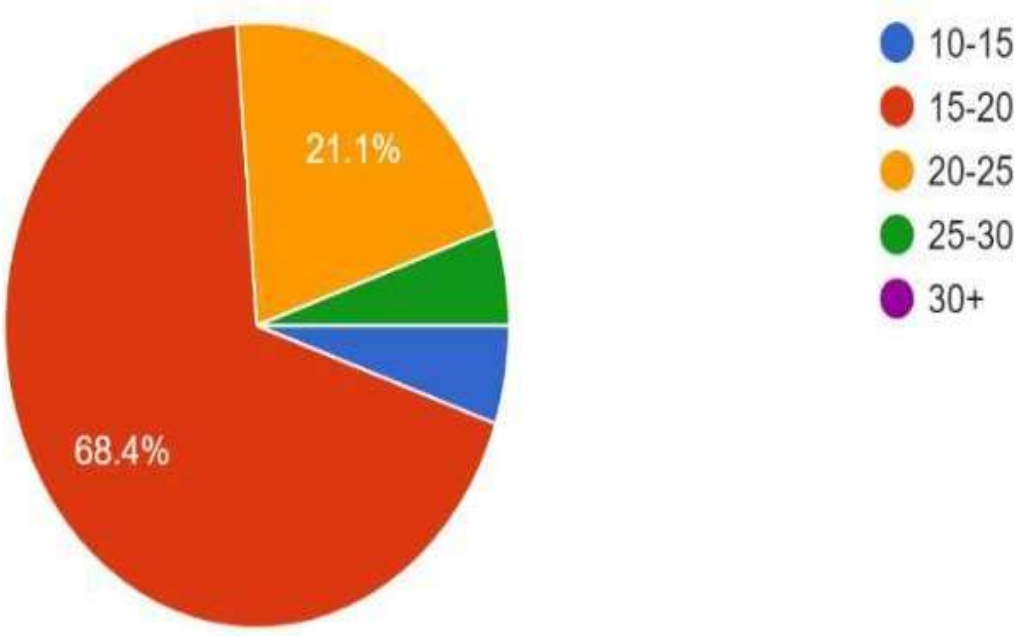


Fig 2. Age group of the people participating in the survey

The pie chart shows that out of total 68.4% respondents belonged to 15-20 age and 21.2% of the respondents belong to 20-25 age and rest belong to other age groups.

Q3. Then we wanted to ask them if they knew about cyber financial crime or even if they had a simple hint about the topic or not

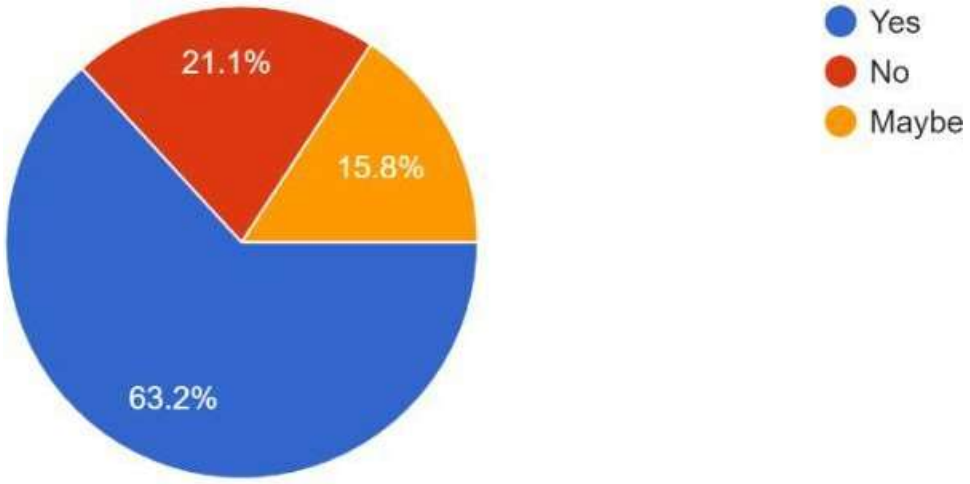


Fig 3. Do you know or have some idea about cyberfinancial crime?

After studying about the chart we saw that gender had no role in awareness and everyone of each gender were equally aware of the term cyber-security but then when we studied about the age group we saw a great dip in awareness about cybersecurity in young adults and as well as aged adults.

Whereas young adults, students and even young teenagers had some idea about cyber security. So age does play a role as a deciding factor regarding cyber crime as well its mental impact on people.

Q4. Do you regularly check your bank statements for unauthorized transations?

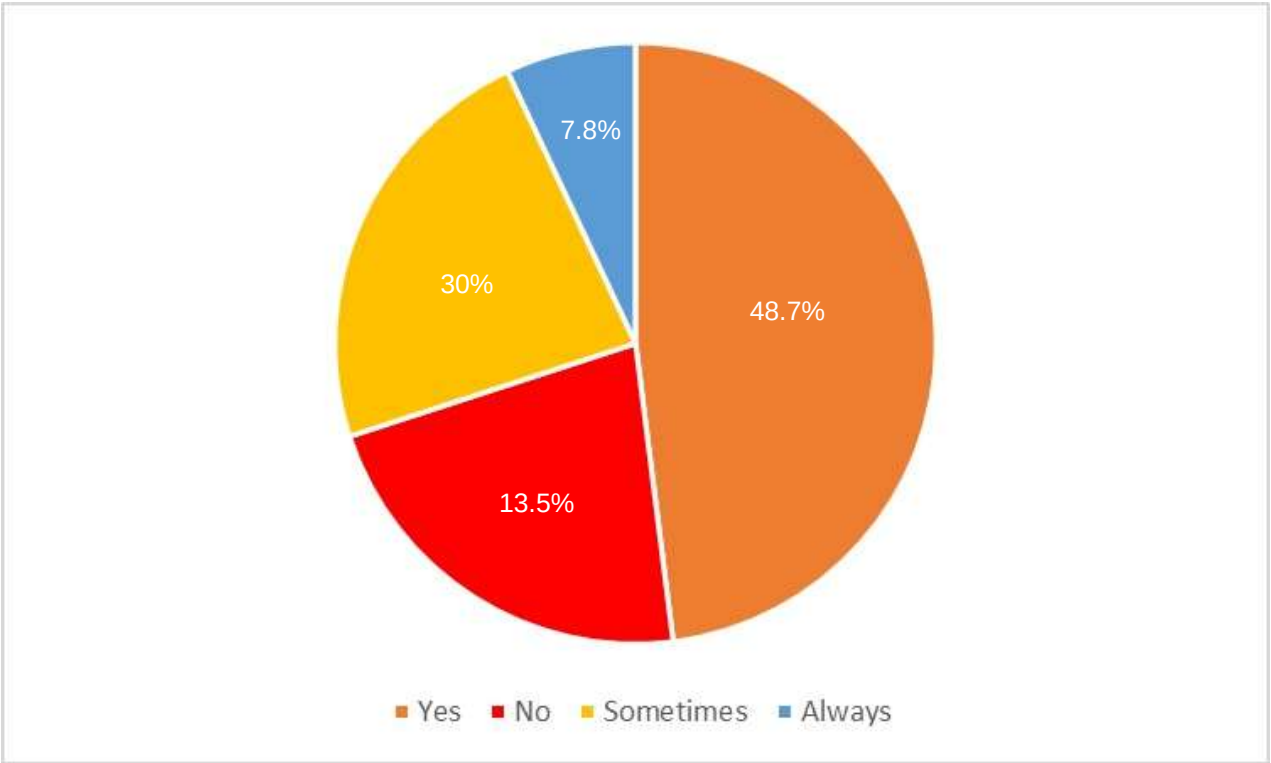


Fig:4

There is a significant portion of respondents activity monitoring their bank statements for any unauthorized transaction, demonstrating a proactive approach to managing their financial security.

Q5. But, as most of them are aware of cyber financial crime we wanted to know if they feel secure while using their device or surfing the internet.

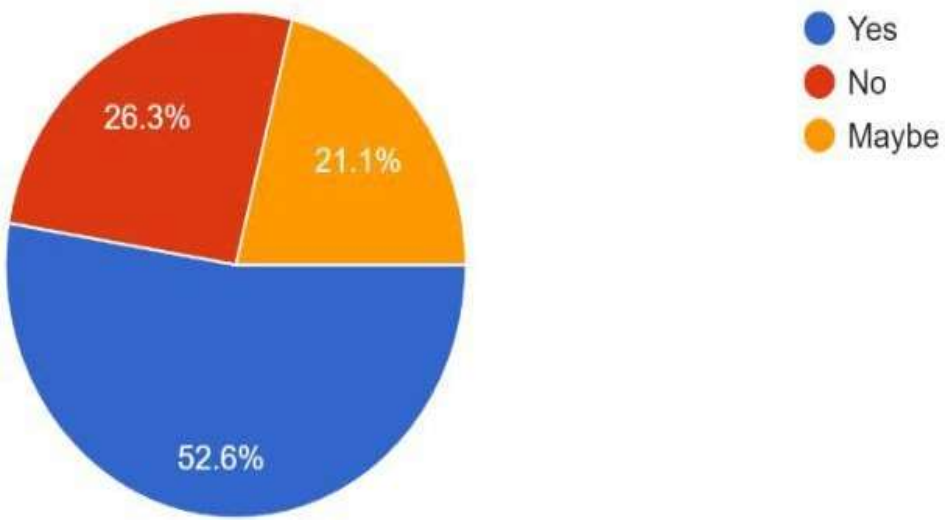


Fig 5. Have you ever felt that your electronic device may be exposed to some external threat due to the internet?

52.6% agreed to the survey that they feel like their data is constantly under threat and on the verge of being misused, most probably in some cybercrime, whereas 26.3% of the people feel their data is completely secure and believe they are completely safe. Whereas 21.1% people are still unaware if they pose any risk or not.

Q6. The previous data lead us to the next question of whether having their data exposed to the internet caused any impact on their mental health, are people in complete peace of mind or is this bothering them to such an extent that it might lead to further issues.

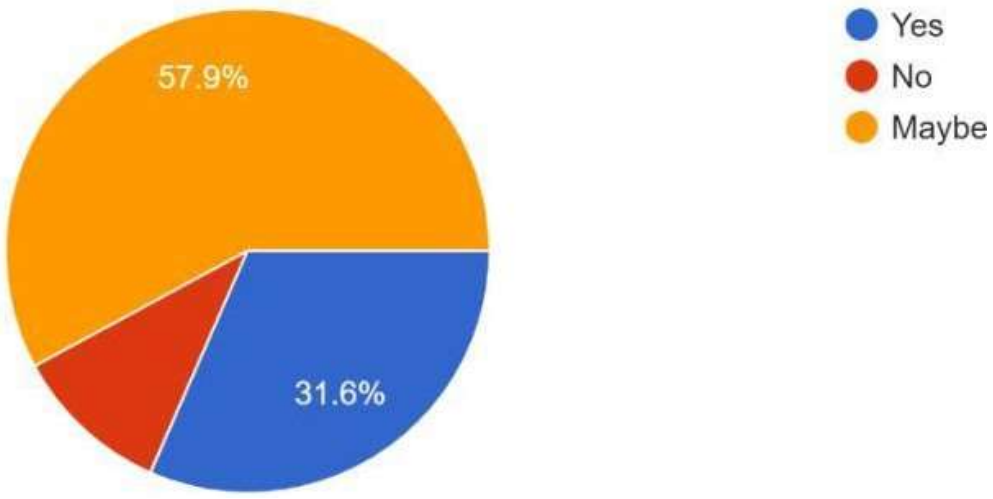


Fig 6. Do you think vulnerability to cyber-financial crime affects your mental health

This question leads us to the answer yes if people know about the threat they are facing regarding their data is disturbing them enough to affect their mental peace. As only a marginally low amount of people 10.5% amount of the people who participated in the survey had no affect on their mental health.

Q7. Have you ever been a victim of cyberbullying or know someone who has been a victim?

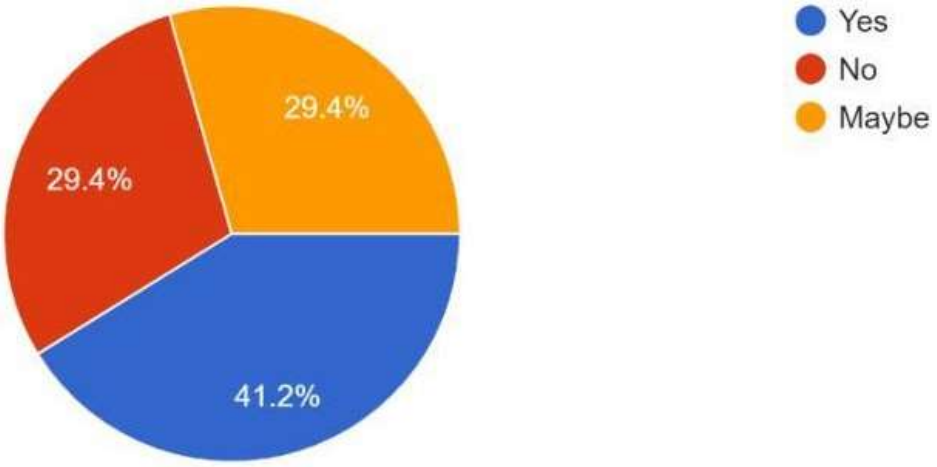
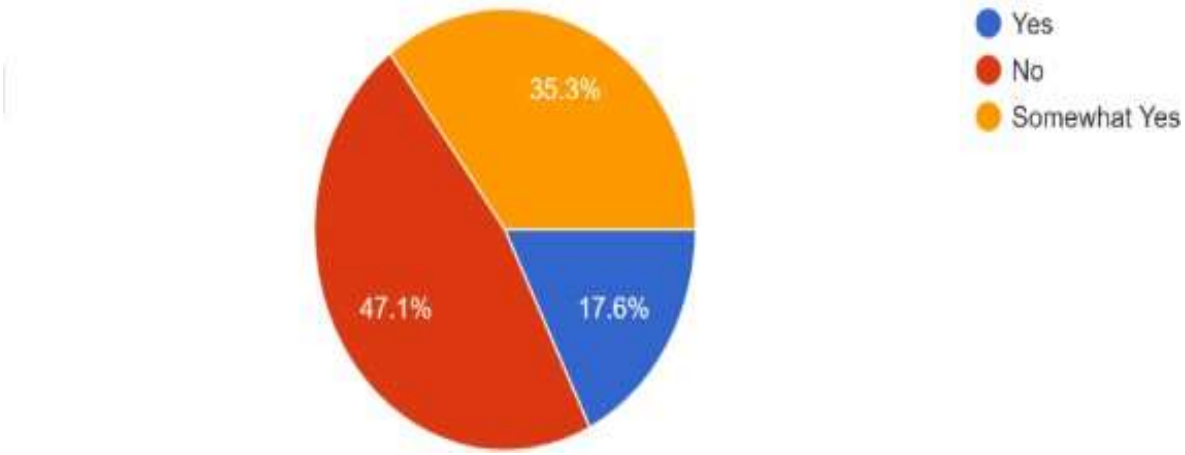


Fig 7. Have you ever been a victim of cyberbullying or know someone who has been a victim?

The following question also showed us the trend compared to 2010-2015. People are being bullied in the cyber world quite a lot, with just 29.4% of people saying they never saw any cyberbullying, which shows how common this shameful and illegal act is nowadays.

Q8. Further we wanted to know how much people already know about cyber laws and about the precautions one must take to prevent it. If told how to protect themselves, are they willing to take precautions against all kinds of cyber crimes?



This above pie chart shows that majority of respondents are not aware of cyber laws, only 17.6% of respondents were sure of knowing cyber laws.

Q9.

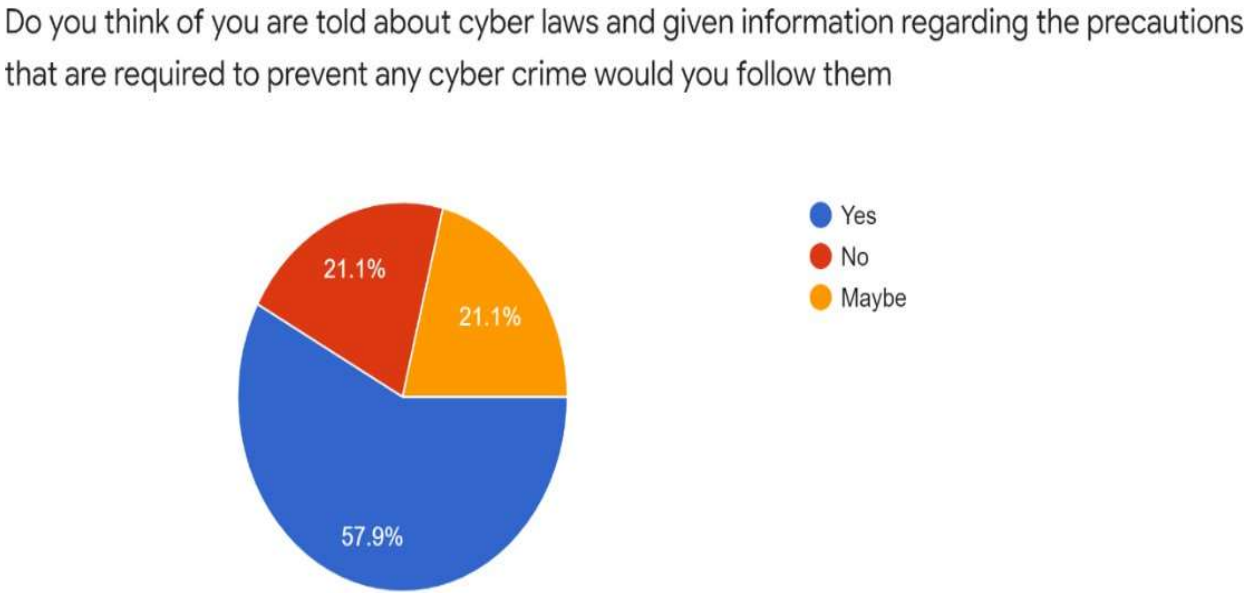


Fig 9. Do you think information regarding cyber financial crime is necessary?

This led us to result that people are willing to receive information about cyber laws and are willing to take necessary actions to prevent cyber-financial crime / cyberbullying.

4.2 Discussions.

4.2.1. THE MAIN CAUSE OF CYBER- FINANCIAL CRIME: MENTAL ILLNESS

Sin is not an individual matter but it has the genesis of criminal behavior. If a person feels guilty of his sin then he can develop positive changes by not doing crime again, on the other hand if a person has done a sinful act and realizes that he did a great job and will continue it can be very destructive. This sense of right and wrong is developed and becomes strong in childhood. Parents and elders are role models for youngsters so if the parents don't give any importance to moral values and are mentally sick then children may have the risk of developing antisocial behavior.

"Children should not grow up with a set of models of parents, teachers etc. who are abusive. There is absolutely no argument with that. It is known that the abused tend to be abusers, in turn. The major objective is never to hurt or uncontrollably release anger, but rather to curb unacceptable behavior and teach methods of altering it''. Most of our learning is through modeling and imitation. A child's mind is like a blank sheet, it is the environment which teaches the child and modifies his behavior. Abusing children may have long term effects on children.

These effects may be emotional, psychological and social. It also depends on the temperament of the child for example if a child is abused in a class he may have symptoms of withdrawal, shyness, low self-esteem, childhood depression and anxiety. On the other hand if a student in the same class is abused the same as the previous one he may have symptoms like aggression, bullying, a sense of revenge, hatred, envy etc so childhood is very important as these types of behaviors developed through society can lead toward destructive behavior in future. Suppressed thoughts also leads toward destructive behavior because of suppressed thoughts a person reacts emotionally. According to Wegner & Zanakos (1994) "Thought suppression is the serious issue as it can decrease mental health and can increase mental illness, and most common form is obsessive thinking, depression and emotional reactions". When a person thinks about an event which disturbed his life, the symptoms starts to appear again until the thought is end. According to Roemer and Borkovec (1993), "the reappearance of the banished thoughts may signal the onset of depression, aggression, fear and anxiety". Mostly people do cyber-financial crimes to get fun but they may not continue for a life time.

4.2.2 BASIC STEPS THAT CAN BE TAKEN TO IMPROVE YOUR CYBER SECURITY

1. Change Your Passwords

Changing your passwords is the simplest thing you can do to up your security and rest easy at night knowing your data is safe. If you haven't already, you should run your key emails and usernames through Troy Hunt's HaveIBeenPwned tool, which runs your information through any personal account data that has been illegally accessed and then released into the public domain. As Troy puts it, "Data breaches are rampant and many people don't appreciate the scale or frequency with which they occur." It's important to keep in mind that this is only publicly released information, so it's entirely possible (and in fact quite likely) that there are other breaches we haven't yet heard about.
At the same time, it's best to avoid changing login information so frequently that your users suffer password fatigue and settle for variations on the same theme.

2. Use a Password Manager

If you really want to get serious about passwords, you'll want to use a password manager tool like LastPass, Dashlane, or Sticky Password to keep track of everything for you. These tools help you use unique, secure passwords for every site you need while keeping track of them for you. That way, you get the security benefits of changing your password, without having to worry about making things hard on your employees. Even better, if you need someone on your team to log into any of your accounts you can share password sets so they can update your website, post to your social media accounts, and much more.

3. Delete Any Unused Accounts

An easy way for an attacker to gain access to your network is to use old credentials that have fallen by the wayside. you can end up with several old accounts if you don't have a good offboarding plan in place. When you're looking at ways to up your security on a budget, doing some housekeeping on your old accounts is a great place to start.

4. Enable Two-Factor Authentication

If you haven't already, you need to think about enabling two-factor authentication to add some extra security to your logins. Generally, it's as simple as registering a phone number or installing an app, but it adds that extra layer of security that makes it harder for an attacker to get into your accounts.

5. Keep Your Software Up to Date

Software updates always seem to pop up at the most inconvenient time, and so it becomes easy to dismiss them and save it for a later date. The thing is, the reason that you're being bugged to update your software is because it's, well, bugged. Equifax, one of the biggest data breaches in recent memory, happened because of an unpatched software vulnerability.
As with passwords, the thing to understand here is that once these vulnerabilities become public, hackers go looking for people running that specific software who could be vulnerable. If you've been meaning to get around to installing an update, take the time to do it. Even if it pops up at an inconvenient time, it'll almost certainly cost you less time to install an update than it will to deal with an actual data breach.

6. Training to Identify Phishing and Spear Phishing Attacks

One of the most popular and effective ways for hackers to attack a particular target is through phishing and spear phishing attacks. Phishing attacks are more generalized, but spear-phishing is personalized to each target and can often be extremely convincing. The only way to be sure that you will be safe is through training. You need to understand everything that is possible in a spear phishing attack, and what details they can be on the lookout for in order to be ready if you are targeted.

7. Keep yourself updated with cyber laws

Develop a keen interest in reading about cyber laws and that's all you need to be aware of your rights and the course of action if you feel something is going in the wrong direction.

4.2.3 THINGS THAT CAN BE DONE TO REDUCE CYBER-FINANCIAL CRIME / CYBERBULLYING

- In practical life people who are mentally ill face many difficulties in changing their thinking processes. There is a need to change the maladaptive behavior and negative thinking into positive thinking.

- Mental health professionals can change the thinking patterns of mentally ill people by different techniques like psychotherapy, behavioral training and cognitive therapy. The people who are not flexible and stick to their negative behavior create many difficulties for themselves and for society at large.

- Mental health problems can be treated by psychotherapy. Psychotherapy is very effective in preventing anxious behavior and stress. It can be done individually or in group settings depending on the severity.

- Mentally ill people can be treated through contact with the organizations. To contact the organizations the main role is of families. The families of mental ill people should be aware of the negative consequences of mental illness and should contact the organizations and social services for help.

- Awareness should be created among people about the moral values including reporting the crime when observed.

- The people who are committing cyber crimes just for enjoyment should be given awareness of the harm it brings to the innocent people.

- Optimistic approach changes the perception and approach of a person's view about life. It is the positive attitude which leads to continued success. Positive approach leads to success. The person who has positive thinking feels content and is never jealous. He never blames to anyone for his failure but tries to have better position in society and if he fails in doing so he never give up.

CONCLUSION

Cyber-financial issues are also challenging for students and academics more generally. Experts of all sorts widely disagree how likely future cyber-doom scenarios are—and all of their claims are based on (educated) guesses. While there is at least proof and experience of cyber-crime, cyber-espionage or other lesser forms of cyber-incidents on a daily basis, cyber-incidents of bigger proportions (cyber-terror or cyber-war) exist solely in the form of stories or narratives. The way we imagine them influences our judgment of their likelihood; and there are an infinite number of ways in how we could imagine them. Therefore, there is no way to study the 'actual' level of cyber-risk in any sound way because it only exists in and through the representations of various actors in the political domain. As a consequence, the focus of research necessarily shifts to contexts and conditions that determine the process by which key actors subjectively arrive at a shared understanding of how to conceptualize and ultimately respond to a security threat.

Cyber crimes cannot be eliminated from society but it is quite possible to check them. Mental illness leads toward deviant behavior which is associated with psychological, emotional and biological factors. Mental health is enhanced by policies and programmes in government and business sectors. Employment, education, justice, a peaceful environment, housing and welfare on the one hand, and specific activities in the health field related to the treatment of mental illness on the other are also included in this concern.

Appendix

Survey form and Questionnaire:

Impact of Cyber Financial Crime on Mental Health

Greetings!! It would be a pleasure if you could spare not more than 3 minutes to fill out the following survey related to "Impact of Cyber Financial Crime on Mental Health."

NOTE: Your participation in this survey is completely voluntary. Your responses will be kept confidential, and the data from this research will be reported ONLY in the aggregate.

Q1) Gender

- *Male*
- *Female*
- *Prefer Not to say*

Q2) Variet of Age Groups Participating in the survey

- *10-15*
- *15-20*
- *20-25*
- *25-30*
- *30+*

Q3) Do you know or have some idea about cyberfinancial crime?

- *Yes*
- *No*
- *Maybe*

Q4) Do you regularly check your bank statements for unauthorized transations?

- *Yes*
- *No*
- *Sometimes*
- *Never*

Q5) Have you ever felt that your electronic device may be exposed to some external threat due to the internet?

- *Yes*
- *No*

- *Maybe*

Q6) Do you think vulnerability to cyber-financial crime affects your mental health

- *Yes*
- *No*
- *Maybe*

Q7) Have you ever been a victim of cyberbullying or know someone who has been a victim

- *Yes*
- *No*
- *Maybe*

Q8) Have you noticed any changes in your behavior or emotions related to online financial activities since the surge in cybercrime incidents?

- *Yes*
- *No*
- *Maybe*

Q9) Have you sought support or counseling to cope with the stress or trauma resulting from cyber financial fraud?

- *Yes and it helped*
- *No but considering it*
- *No,haven't felt the need*

Q10) Do you use strong and unique passwords for your online banking accounts?

- *Yes*
- *No*
- *Many times*

Q11) Have you ever shared your banking credentials with anyone online?

*

- *Yes*
- *No*
- *Many times*

Q12) Do you believe financial institutions are doing enough to protect their customers from cyber financial crime?

*

- *Yes*
- *No*
- *Not aware*

Q13) Have you ever encountered fraudulent transactions on your credit card?

*

- *Yes*
- *No*
- *Many times*

Q14) Do you think education and awareness about cyber financial crime are essential for preventing it?

*

- *Yes*
- *No*
- *Sometimes*

Q15) The following questions have to be answered on a rating of three.

- *1)Not Concerned at all.*
- *2)Slightly Concerned.*
- *3) Strongly Concerned.*

*

Date

Q16) How concerned are you about the threat of cyber financial crime?

*

- *Concerned*
- *Slightly concerned*
- *Strongly Concerned*
- *Other:*

Q17) How often do you update your antivirus and security software?

*

- *Once a year*
- *Once a month*
- *Every week*
- *Other:*

Q18) To what extent do you think government regulations can help prevent cyber financial crime?

*

- *Massive help*

- *Minimal help*
- *No help*
- *Other:*

Q19) How frequently do you check the security certificates of websites before entering sensitive financial information?

*

- *Never*
- *Sometimes*
- *Always*
- *Other:*

Q20) How confident are you in recognizing phishing attempts or fraudulent websites?

*

- *Not Sure at all*
- *Very Sure*
- *Don't know*
- *Other:*

Q21) To what extent do you think encryption technology can safeguard financial transactions?

*

- *Very Significantly*
- *Partially*
- *Not at all*
- *Other:*

Q22) How often do you review the privacy settings of your social media accounts to minimize the risk of cyber financial crime?

*

- *Never*
- *Rarely*
- *Everyday*
- *Other:*

Q23) How well do you think financial institutions communicate security measures and risks to their customers?

*

- *Effectively*
- *Rarely*
- *Never*
- *Other:*

Q24) How proactive do you consider yourself in reporting suspicious activities related to cyber financial crime?

*

- *Very Proactive*

- *Not proactive at all*
- *Sometimes proactive*
- *Other:*

Q25) How likely are you to invest time and resources in educating yourself further about cyber financial crime prevention?

*

- *Very likely*
- *Unlikely*
- *Never*
- *Other:*

REFERENCES

- Gandhi, R., et al. (2011). "The social and psychological impact of cyberattacks." ScienceDirect.
- Dallaway, E. (2016). "Cyber risk and cybersecurity: a systematic review of data." Springer.
- Modic, D., & Anderson, R. (2015). "Impact of cyber-attacks on financial institutions." ScienceDirect.
- Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). "The psychological impact on the lives of cyber-attack victims." Painted Brain.
- Symantec Corporation (2010). "Cybercrime victim survey results." Painted Brain.
- Kwong, A. S. F., et al. (2020). "COVID-19, economic impact, mental health, and coping strategies." Frontiers.
- Pettinicchio, D., et al. (2021). "Mental health outcomes during COVID-19 lockdowns." PLOS ONE.
- McKee-Ryan, F., et al. (2005). "Mental health and unemployment: A systematic review." ScienceDirect.
- Paul, K. I., & Moser, K. (2009). "Youth unemployment and mental health impacts." ScienceDirect.
- Strandh, M., et al. (2014). "Economic recessions and mental health outcomes." BMC Public Health.
- Auerbach, R. P., et al. (2018). "Impact of relationship issues on student mental health." Springer.
- Oxford Academic (2017). "Cyber-bullying and its impact on mental health." European Journal of Public Health.
- Nature (2020). "Scrutinizing the effects of digital technology on mental health." Nature.
- OpenLearn (2020). "Psychological and emotional impact of cybercrime." Open University.
- BMC Public Health (2020). "A scoping review on the current mental health status." BMC Public Health.

- ScienceDirect (2020). "Link between mental health, crime, and violence." ScienceDirect.

- European Public Health Association (2017). "Mental health and mental disorder research collection." Oxford Academic.

- Gandhi, R., et al. (2011). "The psychological impact of cyberattacks." ScienceDirect.

- Painted Brain (2020). "The psychological impact on the lives of cyber-attack victims." Painted Brain.

- PLOS ONE (2020). "Impact of COVID-19 pandemic on mental health: An international study." PLOS ONE.