Research Paper E-ISSN NO : 2455-295X | VOLUME : 7 | ISSUE : 8 | AUGUST 2021

IMPACT OF CYBERCRIME ON MENTAL HEALTH

MRS. RENUKA POLLY DASS [1] | MRS. PREETI BAHUGUNA [2]

[1,2] ASSISTANT PROFESSOR, ROHILKHAND COLLEGE OF NURSING, BIU, BAREILLY, U.P.

ABSTRACT:

Cybercrime refers to criminal activities that are committed using internet technology. Cybercrime occurs through personal websites, blogs, e-mail, Texting, social networking sites, chat rooms, message boards, instant messaging and photographs. Victims who are targeted via cyberbullying report increased depressive affect, anxiety, loneliness, suicidal behavior, and somatic symptoms. There is nothing more calming than spending quality time with another human being who makes you feel safe and understood. In fact, face-to-face interaction triggers a cascade of hormones that counteracts the body's defensive "fight-or-flight" response.

KEYWORDS:

IMPACT, CYBERCRIME, MENTAL HEALTH.

INTRODUCTION

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Cybercrime, especially involving the Internet, represents an extension of existing criminal behavior alongside some novel illegal activities.[1]

The internet has only been in widespread use by the general public for a few decades (a 'start date' could be considered to be the launch of the World Wide Web on the 6 August 1991), but online activity has already become ubiquitous in the developed world and is becoming progressively more common in much of the developing world as well (Naught on, 2016).[2]

Cybercrime also called **Computer crime**, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.[1]

In the 12 months to June 2020, incidents of fraud and computer misuse in England and Wales rose from 4.84m incidents to 5.94m year-on-year, according to the Office for National Statistics. For every 1,000 people, there were 94 victims of fraud and 35 of computer misuse, up from 82 and 21 respectively in the previous 12-month period.[3]

In February 2021—nearly one year from the start of the pandemic—there were 377.5 million brute-force attacks—a far cry from the 93.1 million witnessed at the beginning of 2020. India alone witnessed 9.04 million attacks in February 2021. The total number of attacks recorded in India during Jan & Feb 2021 was around 15 million.[4]

"As per the data maintained, since its inception 3,17,439 cybercrime incidents and 5,771 FIRs have been registered up to February 28, 2021 in the country which includes, 21,562 cybercrime incidents and 87 FIRs in Karnataka and 50,806 cybercrime incidents and 534 FIRs in Maharashtra.[5]

TYPES OF CYBERCRIME

As mentioned above, there are many different types of cybercrime; most cybercrimes are carried out with the expectation of financial gain by the attackers, though the ways cybercriminals aim to get paid can vary. Some specific types of cybercrimes include the following:

- **Cyber extortion:** A crime involving an attack or threat of an attack coupled with a demand for money to stop the attack. One form of cyber extortion is the ransom ware attack. Here, the attacker gains access to an organization's systems and encrypts its documents and files -- anything of potential value -- making the data inaccessible until a ransom is paid.
- **Identity theft:** An attack that occurs when an individual accesses a computer to glean a user's personal information, which they then use to steal that person's identity or access their valuable accounts, such as banking and credit cards. Cybercriminals buy and sell identity information on dark net markets, offering financial accounts, as well as other types of accounts, like video streaming services, webmail, video and audio streaming, online auctions and more. Personal health information is another frequent target for identity thieves.
- **Cyber bullying:** Cyber bullying is that the use

of the web and related technologies to harm people during a deliberate, repeated, and hostile manner. i.e. by posting unwanted photos, Sending inappropriate text messages, giving negative comments, Blackmailing with certain demands, Threats of violence or death.

- **Credit card fraud:** An attack that occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on dark net markets, where hacking groups that have stolen mass quantities of credit cards profit by selling to lower-level cybercriminals who profit through credit card fraud against individual accounts.
- **Cyber Grooming:** It is a practice where someone builds an emotional bond with children through social media or messaging platforms with an objective of gaining their trust for sexually abusing or exploiting them.
- **Exit scam:** The dark web, not surprisingly, has given rise to the digital version of an old crime known as the *exit scam*. In today's form, dark web administrators divert virtual currency held in marketplace escrow accounts to their own accounts -- essentially, criminals stealing from other criminals.[6]

HOW CYBERCRIME WORKS

Cybercrime attacks can begin wherever there is digital data, opportunity and motive. Cybercriminals use various attack vectors to carry out their cyber attacks and are constantly seeking new methods and techniques for achieving their goals, while avoiding detection and arrest.[6]

Cybercrime occurs through personal websites, blogs, e-mail, Texting, social networking sites, chat rooms, message boards, instant messaging and photographs.

Many cyber attacks begin when someone clicks on what appears to be an innocent link. This click can lead to a:

✓ Virus that infects software and reproduces copies of itself when the software is opened.

✓ Worm that infects software and spreads copies without the user taking action.

✓ Trojan that appears to be safe software but contains malware that acts when downloaded and opened.

✓ Ransom ware is malware that keeps users from accessing their system or device or encrypts files until a fee (ransom) has been paid.

✓ Root kits hide malware from antivirus detection and removal programs.

✓ Losing access to medical records and lifesaving medical devices, such as when a ransom ware virus holds them hostage, will deter your ability to effectively care for your patients.

✓ Hackers' access to private patient data not only opens the door for them to steal the information, but also to either intentionally or unintentionally alter the data, which could lead to serious effects on patient health and outcomes.

IMPACT OF CYBERCRIME ON MENTAL HEALTH

Exposure to the fraudsters and misinformation are creating a mental turbulence and is one of the biggest hindrances in our daily chores.

It is causing victims to experience emotional, physical and financial trauma. People are experiencing more panic and depression. It is becoming increasingly difficult for people to trust others online. After suffering a traumatic experience they feel guilty and complain of insomnia and eating disorders.

The experience of helplessness makes them feel annoyed and angry. The victim explains " I was unprepared. I never thought I would be a victim of such a crime. I feel I am violated."

The emotional impact is more long lasting in instances where the data of the victim are breached. They wrestle with their feeling of failure and vulnerability, disruption in sleep and low energy levels and find alcohol and drugs as the best thing to confine themselves and free from thoughts.

After-effects can be severe for some with the symptoms of depression, anxiety, eating disorders, feeling of humiliated, exposed, shame & angry, guilty, self-harm, feeling disinteresting in activities, feeling overwhelmed, feeling isolated from society, sexually transmitting infections, relationship problems with family, friends & partners, difficulty coping with stress and even post-traumatic stress disorder (PTSD) and suicidal thoughts.[7]

One of the biggest contributing factors to victims' distress is the feeling of hackers violating them. Some victims have even described the feeling as being similar to that of a sexual attack. Nearly 70% of Victims find themselves unwilling to trust those around them, impacting their personal relationships heavily.

Even famous victims cannot avoid the psychological fallout of cyber attacks. After the celebrity phone-hacking scandal, victims and their families described themselves as suffering from long-term paranoia and distress.

HOW TO PREVENT CYBERCRIME

While it may not be possible to completely eradicate cybercrime and ensure complete internet security, businesses can reduce their exposure to it by maintaining an effective cyber security strategy using a defense-in-depth approach to securing systems, networks and data.

Cybercrime risks can be reduced with the following steps:

✓ develop clear policies and procedures for the business and employees;

- create cyber security incident response management plans to support these policies and procedures; and use two-factor authentication (2FA) apps or physical security keys;
- outline the security measures that are in place about how to protect systems and corporate data;
- carefully scrutinize all email requests for transfer of funds to determine if the requests are out of the ordinary;
- continually train employees on cyber security policies and procedures and what to do in the event of security breaches;
- keep websites, endpoint devices and systems current with all software release updates or patches; and
- back up data and information regularly to reduce the damage in case of a ransom ware attack or data breach.
- Never share your passwords, private photos, or personal data online, not even with friends. Try to limit your identity.
- Privacy settings on social media to select those who can access your posts online. Restrict access of your profile only to your friends.
- Think before you post. When you're sad, angry or depressed wait to post or respond.
- Never -install unwanted Software and Apps like dating apps, online games, etc. from unknown sources.[6]

HOW TO DEAL WITH CYBERCRIME

- Report the incident and block the user.
- Seek help: Reach out to family and friends - they will provide you with emotional support and can also help you find the courage to file a complaint.
- Avoid retaliating or responding: This may be easier said than done, but try not responding to someone who is being unreasonable and offensive. A response or reaction from you may be exactly what the abuser wants. Don't give them attention or satisfaction or the situation could snowball into something uglier.
- Don't delete the evidence: Under provisions of the IT Act, you can file a written complaint to the cyber police, or even file an FIR about the incident. Take screenshots of the abuse so you can use it to strengthen your case.
- Don't post identifying information online: This is extremely important. Don't ever share personal information with strangers or on public forums - and this includes geo-tagging your posts with your location. Cyber bullying is bad enough, but if your harassers know where you live or hang out, things can become dangerous fast. Report it. Still you can report it though the content is not targeting you.[8]

HOW TO REDUCE MENTAL STRESS

- Communicate with your parents/elders/friends immediately.
- Help them to minimize the chance of repeat victimization.
- Listen to how they feel, and don't be judgmental.
- Stop the activity, report the crime, repair the damage and prepare for re-victimization.[9]
- Avoid people who stress you out.
- **Take control of your environment:** If the evening news makes you anxious, turn off the TV. If going to the market is an unpleasant chore, do your grocery shopping online.
- **Express your feelings instead of bottling them up:** If something or someone is bothering you, be more assertive and communicate your concerns in an open and respectful way. If you've got an exam to study for and your chatty roommate just got home, say up front that you only have five minutes to talk.
- **Look at the big picture.** Take perspective of the stressful situation. Ask yourself how important it will be in the long run. Will it matter in a month? A year? Is it really worth getting upset over? If the answer is no, focus your time and energy.
- **Practice gratitude.** When stress is getting you down, take a moment to reflect on all the things you appreciate in your life, including your own positive qualities and gifts. This simple strategy can help you keep things in perspective.
- **Don't try to control the uncontrollable.** Many things in life are beyond our control, particularly the behaviour of other people. Rather than stressing out over them, focus on the things you can control such as the way you choose to react to problems.
- **Look for the upside.** When facing major challenges, try to look at them as opportunities for personal growth. If your own poor choices contributed to a stressful situation, reflect on them and learn from your mistakes.
- **Share your feelings.** Expressing what you're going through can be very cathartic, even if there's nothing you can do to alter the stressful situation. Talk to a trusted friend or make an appointment with a therapist.
- **Get moving-** When you're stressed, the last thing you probably feel like doing is getting up and exercising.
- There is nothing more calming than spending quality time with another human being who makes you feel safe and understood. In fact, face-to-face interaction triggers a cascade of hormones that counteracts the body's defensive **"fight-or-flight" response**. Its nature's natural stress reliever (as an added bonus, it also helps

stave off depression and anxiety). So make it a point to connect regularly—and in person—with family and friends.

- ✓ **Eat a healthy diet.** Well-nourished bodies are better prepared to cope with stress, so be mindful of what you eat. Start your day right with breakfast, and keep your energy up and your mind clear with balanced, nutritious meals throughout the day.
- ✓ **Reduce caffeine and sugar.** The temporary “highs” caffeine and sugar provide often end with a crash in mood and energy. By reducing the amount of coffee, soft drinks, chocolate, and sugar snacks in your diet, you’ll feel more relaxed and you’ll sleep better.
- ✓ **Avoid alcohol, cigarettes, and drugs.** Self-medicating with alcohol or drugs may provide an easy escape from stress, but the relief is only temporary. Don’t avoid or mask the issue at hand; deal with problems head on and with a clear mind.
- ✓ **Get enough sleep.** Adequate sleep fuels your mind, as well as your body. Feeling tired will increase your stress because it may cause you to think irrationally.[10]
- ✓ **Avoid making major life decisions.** Doing things like switching jobs or careers can already be stressful and are even harder to adjust to directly after a disaster.[11]

CONCLUSION

As online threats and cyber-attacks continue to permeate the Internet, it is essential that we as a community develop a better understanding of these issues and how they can impact our lives. This review took a significant step towards that goal by exploring how members of the public perceive and engage with risk and how they can be impacted after a cyber-attack has taken place. We focused on the social and psychological impacts of attacks as these are often overlooked in research and practice. These are, however, crucial factors in enhancing our understanding the broader side of attack impacts.

REFERENCES

1. Michael Aaron Dennis. Cybercrime. Encyclopaedia Britannica. July 2021. Available at: https://www.britannica.com/topic/cybercrime

2. https://www.open.edu/openlearn/health–sports–psychology/psychology/the–psychology– cybercrime /content-section-3.1

3. Cyber trauma’ leaves online victims with psychological scars. Antonia Cundy. 26 Jan 2021. Available at: https://www.ft.com/content/1bb6e777-b615-461e-a4f5-3f89927e5ad6

4. https://www.business-standard.com/article/technology/india–becomes–favourite–destination–for–cyber–criminals–amid–covid–19-121040501218_1.html

5. The Hindu. Mar 2021. Available at: https://www.thehindu.com/sci-tech/technology/317-lakhs-cybercrimes-in-india-in-just-18-months-says-govt/article34027225.ece

6. Kate Brush. Cybercrime. Dec 2020. Available at: https://searchsecurity.techtarget.com/definition/cybercrime

7. https://www.linkedin.com/pulse/effect-cyber-crime-mental-health-sripriya-v

8. https://www.firstpost.com/health/the–impact-of-cyberbullying-on-mental-health-and-how-to-deal-with-online-abuse 7951381.html#:~:text=Health%20risks%20associated%20with%20cyberbullying,(PTSD)%20in%20predisposed%20adolescents.

9. Eleanor dallaway. Cybercrime victims. 2021. Available at: https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/?__cf_chl_jschl_tk__=pmd_b6e3a8a34dffdeeef0604c55388cee8259eda6c8-1626787129-0-gqNtZGzNAfijcnBszQri

10. Lawrence Robinson, Melinda Smith, M.A., and Robert Segal. M.A. stress management. Help guide. Sep 2020. Available at: https://www.helpguide.org/articles/stress/stress-management.htm

11. Coping Tips for Traumatic Events and Disasters. May, 2021. Available at: https://www.samhsa.gov/find-help/disaster-distress-helpline/coping-tips