EFFAT UNIVERSITY
COLLEGE OF ENGINEERING
COMPUTER SCIENCE DEPARTMENT
COURSE TERM PAPER FALL 2022

Deema Hamidah	Shumokh Abdullah	Nada Khalefa	Hadeel Balahmar
S20106517	S21107192	S21107101	S20106481
dehamidah@effat.edu.sa	shaabdullah@effat.edu.sa	Naakhalefa@effat.edu.sa	Habalahmar@effat.edu.sa

Cyberstalking

Abstract:

Cyberstalking is a dangerous predatory conduct that results from the drive for control that evolved as humans searched for riches and reputation. Stalking used to refer to non-electronic techniques of infiltration that entailed behavioral invasion. Obsessive relational intrusion (ORI), a phenomenon linked to stalking and intended to foster closeness [1]. A person who repeatedly invades their feeling of physical or symbolic seclusion is said to have ORI, which is an undesirable craving for closeness. As more people use the Internet, there is an increasing risk of online harm, including cyberstalking. However, the Internet has figuratively turned into a breeding ground for a brand-new and distinct category of criminal offender known as the cyber stalker, who employs sophisticated stalking techniques to prey upon, harass, threaten, and instill a great deal of fear in their victims.

Introduction:

In the current online environment, Cyberstalking is a common occurrence. According to Mariam Webster, cyberstalking is "the use of electronic communication to harass or threaten someone with physical harm". It may seem at first that physical stalking is more dangerous than cyberstalking. In reality, both can be as terrifying and possibly have the same danger. In this research, we'll go into detail about this area of the internet and talk about how one can deal with or completely avoid

cyberstalking, which is now recognized as a serious crime. The problem of cyberstalking is getting worse. Online harassment has been a problem for 40% of Americans, according to the Pew Research Center. While women are the majority of cyberstalking victims, 20 to 40% of victims are men. Though preventing cyberstalking can be very challenging, this research will list some effective ways in which we can reach maximum security and limit exposure to cyberstalking [2].

Literature review:

The author of this paper [3] described cyberstalking as a fast-moving, high-tech crime committed in the field of information technology. The term "cyberstalking" describes stalking or harassment that takes place online through channels like email, forums, and social media. Cyberstalking comes in a wide variety of aspects. It is very upsetting when such communications come from different accounts that the same person controls. Cyberstalking does not require direct communication, and some victims might not even be aware that they are being tracked online. Cyberstalkers of various types used the Internet in various ways, according to an analysis of specific cyberstalking behaviors. It's possible that the victim is being managed or intimidated, or that information is being gathered for offline stalking or identity theft. DeKeseredy et al. (2019) report that 35% of respondents have been the victim of stalking made possible by technology. Only 10% of respondents, according to Fansher and Randa (2019), reported having been stalked by someone they had met online. These studies show a glaring lack of consensus regarding how frequently cyberstalking occurs. This discrepancy could be explained by several things, such as

methodological differences, variations in people's willingness to report such incidents, or even a lack of understanding of what constitutes cyberstalking. It's crucial to be aware of cyberstalking

and the preventative steps you can take to secure yourself because, if you are not careful, it can lead to several negative outcomes. It's probably a good idea to let the website's administrators and law enforcement know about this.

The author of this article [4] contrasts the outcomes between online stalking victims and those who had previously been victimized offline. They hypothesized that victims of cyberstalking experienced increased emotional and physical symptoms as well as depression and anxiety. 229 Italian students were sent a questionnaire to investigate the effects of cyberstalking. 107 members (46.7%) reported having been the target of online harassment. Of these, 72 (67.3%) had experienced both online and offline victimization in their lifetime. Overall, our findings showed that cyberstalking was more common in our sample than in earlier research. compared to pure victims of cyberstalking and non-victims, experienced more stress and trait anxiety symptoms in their daily lives. It highlights how crucial it is to offer assistance.

In this article [5], the author discusses the harm done to victims of cyberstalking, which is a problem that doesn't always go away after the stalking has stopped. According to research, people who are the targets of cyberstalking may suffer from various negative effects. As a result of their experiences, some cyberstalking victims experience psychological side effects like depression, sleep problems, increased attention span, post-traumatic stress disorder, and anxiety (Worsley et

al. 2017). The fact that perpetrators can contact victims at any time via a variety of technologies is one factor contributing to these psychological effects. Because the behavior is written or visual in nature, cyberstalking also has a persistence separate from face-to-face communication. For instance, if the email is read several times, the person might look back and remember being a victim (Fissel 2019).

This article's author discusses the various ways stalking can take place [6]. As an illustration: Consistently monitoring someone's photos, places they have been with friends, and other private information. Spyware data collection: Stalkers use spyware to keep an eye on what their target is doing on his phone at all times. Taking control of online accounts: Hacking into the victim's online accounts to retrieve personal information and images. using the GPS on the victim's phone to track their location. Threats: Threats made by a stalker are similar to those made during cyberbullying, with the exception that they are not meant to devalue the victim but rather to cause alarm and distress in order to pressure the victim into doing something they don't want to. Reputational damage: Some stalkers resort to this tactic when they are unable to obtain what they want from their targets. Encouragement of others to harass the victim: Many online stalkers will recruit third parties to help them in their harassment campaign. This type of harassment is common, and victims frequently report receiving hundreds of phone calls and text messages.

In this article [7], the author discusses possible explanations for the recent rise in cyberstalking. Our dependence on technology to communicate with people, wherever they might be in the world,

increased during the pandemic years. Technology gives us a lot of good things, especially as a social lifeline. However, it can also be abused by people who want more access to our lives. Over

the past two years, there has been an increase in cyberstalking incidents, according to the authorities. Police received 98,863 reports of stalking between 2020 and 2021, a 300% increase from the prior year. At the moment, all stalking incidents reported to the Suzy Lamplugh Trust are 100%. (a charity working to protect and help victims of stalking). This is up from 80% before the pandemic in 2019. While there are many factors contributing to this rise, boredom and loneliness during the pandemic years are undoubtedly important ones. Given these factors and the widespread use of social media, it is not surprising that, as of the beginning of 2020, 82% of victims reported that social networking sites had been used in cyberstalking incidents.

The researcher in this study [8] explains the dangers of cyberstalking on victims. For instance, the first risk is the victim's physical safety at risk due to digital footprints, as cyber stalkers may use these footprints to determine the victim's current location and carry out physical harm or even murder. Second, there is the possibility that the cyberstalker will discover the victim's home, family, or even friends' contact information. Thirdly, by gathering data, the cyberstalker could learn more about the victim and use social engineering to deceive them. Similar to this, it is stated that cyber stalkers may always gather their information in order to quickly access personal information about the victims by using people who are close to the victim. Fourthly, the online stalker might assemble enough data about the victim to steal their identity. Finally, a cyber stalker

could access the victim's account and use it to harass them directly or financially, for example, by breaking into their bank account and sending a false email. The use of spyware, which is widely

available today and can be downloaded for a low cost or even for free from the Internet, has made it possible for stalkers to locate their victims and gather information about them.

The unethical practice of cyberstalking is growing and evolving in a variety of ways. In an effort to close this knowledge gap, this article [9] develops a model to understand and assess the prevalence of cyberstalking victimization. Cyberstalking is a subset of cybercrime that makes use of other tools or computer networks to further its own ends. There are some guidelines to follow even though cyberstalking has no official definition. ICTs are used in cyberstalking to track down victims and survey, harass, or take advantage of them to spread fear, panic, or alarm. It is the scene of violations and potential victimization. According to Gnasigamoney and Sidhu, the lack of statistics and a lack of a scientific definition are to blame for the lack of understanding of this novel phenomenon. This study came to the conclusion that it is impossible to persuade students to drastically reduce their Internet usage because it is frequently necessary for many aspects of everyday life. In conclusion, this study provides an in-depth analysis of the factors and connections that influence cyberstalking victimization.

Findings:

1) according to the statistic of WHOA (working to halting online abuse) conveyed that 74% of the victims were female, and only 21% were males. Fig:1 [10]

2) based on age: most of victims were 31 years old and older, 27% were between 18 – 30 years old. Fig:2 [11]

3) Approximately 1 in 4 stalking victims reported some form of cyberstalking such as e-mail (83%) or instant messaging (35%). Fig:3 [12]

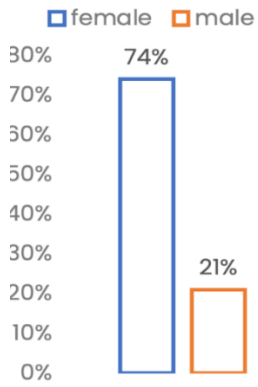

Figure: 1

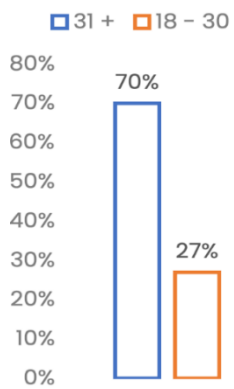

Figure: 2

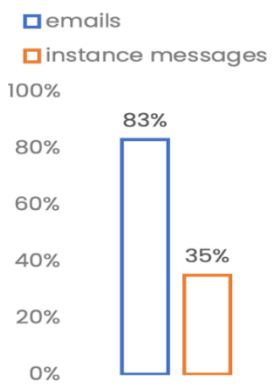

Figure: 3

Discussion:

The three main components of technology are commodities and services, human activities that produce these items, and technological skills. The factors are connected and reinforce one another.

Research, development, and manufacturing activities provide consumer products and services as well as information and skills that support the development of technical capability. Demand for goods and services drives technical development, and some of the outcomes are invested back into infrastructure, education, and research to advance technology. As a result, technology advances due to the "supply push" and "demand pull," impacted at each stage by a wide range of variables such as available resources, the state of the economy, and customer preferences.

Common attacks and threat actor's examples:

EMAIL: [13] Some victims receive a deluge of threat-filled, specifically crafted emails. But even non-threatening emails can be considered harassment; receiving unsolicited mail with offensive jokes, links, or images can be a bad experience.

How simple it is for a stalker to compile information about their target is another terrifying feature of social media stalking. They can look through posts from family and friends to find out more about a person, use the location data in images, and keep track of any excursions or meets that the victim puts online. However, meta data for images can be deleted.

SOCIAL MEDIA: [13] social media: These applications (Instagram, Facebook, Twitter, etc.) are used to share days and a lot of information about the person. This is a vulnerability that a cyberstalker can take advantage of to learn more about his victim and to threaten him.

TEXT AND IMS: [13] A cyberstalker who has access to their victim's phone number or instant messaging credentials might send dozens, if not hundreds, of messages per day. Sending voice

clips, voicemails, photos, and URLs is now also possible. Texting is frequently the most direct way to communicate with a victim, whether they want to threaten them or demand their attention.

It's important to keep in mind that these communications do not have to contain explicit threats or acts of violence in order to qualify as cyber-stalking. Even if someone texts you several times each day, it can still feel intrusive and disturbing, especially if the messages contain discriminating language or unwelcome approaches or requests.

COMPUTER SECURITY: [14] is the most hazardous method used, here the cyberstalker seizi control of a victim's computer through hacking

• This requires advanced computer skills, although online instructions are available.

• Whenever the victim's computer is linked to the internet, the invader has control over its behavior.

To protect our physical and digital wellbeing, people must be proactive and avoid needless internet exposure [3]. Examples include: Reviewing and resetting the passwords for all of their online accounts every three months, using stringent privacy controls on social networking networks, limiting the information you share online with those who aren't your close friends or relatives, removing location services metadata before publishing images online since the stalker could be able to track you down, and stop providing strangers you meet online, in chat rooms, social media,

or gaming platforms your full name, phone number, home location, or place of employment if you don't have to.

A security tool can help you defend against threats and network eavesdropping. You can use Bitdefender's Digital Identity Protection tool to keep an eye on the digital footprint you leave behind when you visit the web. You can receive notifications regarding attempts that commit identity fraud, including information disclosure, account takeovers, and media platforms impersonations.

A constantly growing attack surface that spans the entire planet has been created through increased Internet and gadget connectivity. As a result, the world's most active danger domain is now the internet. Today's cybersecurity risks necessitate the participation of every sector of society,

including the public, the corporate sector, and law enforcement, in order to deter cyberstalkers and strengthen defenses. Knowing about cybersecurity can help you to regain your security, privacy, and online safety. To regain your security and privacy, you must take away any access that the stalker may have. In other words, limiting access and keeping information private can help you to be more secure from being cyberstalked.

If a person is constantly threatening, harassing, and intimidating you online, you may have a cyberstalker on your hands. Cyberstalkers are individuals who just won't leave you alone and might even make you fear for your life. Unfortunately, when you have an online stalker, you are not alone. As many as 8% of Americans record being stalked online at some point in their life. In many cases, it is possible to get rid of the person on your own by locking down your social media and different accounts. if you are replying to their messages, you are encouraging them to continue.

Although it could be extremely hard to ignore repeated messages, it might provoke the person to leave you alone. Go to every social media platform where you have a presence and block the cyberstalker's account. Once you have blocked the person, they may be not able to see your posts or your account. Usually, they cannot even see your comments on different people's posts. In addition, make screenshots of every message you get from your cyberstalker, as well as all comments, blog posts, or other online content that's related to you. Record the dates and times in your log. Go to your local police department and inform them that you want to file a police report. Bring copies of all the emails, messages, comments, and different content from your cyberstalker with you and show them to the officer who takes your report. Although many stalking victims are reluctant to tell others of what they are going through, it is important that those around the victim know what is happening. This includes family, friends, work colleagues, and even neighbors.

Conclusion:

In conclusion, we have made an effort to discuss all facets of cyberstalking. Cyberstalking, harassment, and threatening behavior are serious problems that can seriously harm the people who are the targets. It is critical to take precautions for your safety and to seek assistance if you exhibit these behaviors. This may entail logging the behavior, blocking the offender, and filing a complaint. It might also involve asking for assistance if you feel unsafe or are in danger right away, getting support from professionals in the field, and thinking about taking legal action if the behavior is serious or continuous.

References:

[1] J. Sammons and M. Cross, "Cyberstalking - an overview | ScienceDirect Topics," *Sciencedirect.com*, 2017. https://www.sciencedirect.com/topics/computer-science/cyberstalking

[2] A. A. Says: "What is cyberstalking? - differences, types, examples, laws," *Intellipaat Blog*, 13-Dec-2022. [Online]. Available: https://intellipaat.com/blog/what-is-cyberstalking/.

[3] P. Kaur, A. Dhir, A. Tandon, E. A. Alzeiby, and A. A. Abohassan, "A systematic literature review on cyberstalking. An analysis of past achievements and future promises," *Technological Forecasting and Social Change*, vol. 163, p. 120426, Dec. 2020, doi: 10.1016/j.techfore.2020.120426.

[4] daniela acquadro maran and tatiana begotti, "Prevalence of Cyberstalking and Previous Offline Victimization in a Sample of Italian University Students," Social Sciences, vol. 8, no. 1, p. 30, Jan. 2019, doi: 10.3390/socsci8010030.

[5] B. W. Reyns and E. R. Fissel, "Cyberstalking," The Palgrave Handbook of International Cybercrime and Cyberdeviance, pp. 1283–1306, 2020, doi: 10.1007/978-3-319-78440-3_57.

[6] Y. Kamin, "Cyber harassment prevention through user behavior analysis online in kingdom of Saudi Arabia (KSA)," Journal of theoretical and applied information technology, Jan. 2018, Accessed: Dec. 09, 2022. [Online]. Available: https://www.academia.edu/es/72097769/Cyber_harassment_prevention_through_user_behavior_analysis_online_in_kingdom_of_Saudi_Arabia_KSA_.

[7] "Why cyberstalking is on the rise and how to stop it," Schillings. https://www.schillingspartners.com/learn/why-cyberstalking-is-on-the-rise-and-how-to-stop-it/

[8] Z. Hamin, W. Rosalili, and W. Rosli, "Hamin & Rosli -Cloaked by Cyber Space: The Risks of Cyber Stalking in Malaysia a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License Cloaked By Cyber Space: A Legal Response to the Risks of Cyber Stalking in Malaysia," vol. 12, no. 1, pp. 316–332, 2018, doi: 10.5281/zenodo.1467931.

[9] W. Abu-Ulbeh, M. Altalhi, L. Abualigah, A. A. Almazroi, P. Sumari, and A. H. Gandomi, "Cyberstalking Victimization Model Using Criminological Theory: A Systematic Literature Review, Taxonomies, Applications, Tools, and Validations," Electronics, vol. 10, no. 14, p. 1670, Jul. 2021, doi: 10.3390/electronics10141670.

[10] Ms. Sonali Yadav and Ms. Ankita Srivastava, "Cyber Stalking: A Nuisance to the Information Technology," researchgate, Lucknow, 2014.

[11] Rohini Chahal, Lovish Kumar, Shivam Jindal and Poonam Rawat, "Cyber Stalking: Technological Form of Sexual Harassment," researchgate, Uttarakhand, 2019.

[12]
K. Baum, S. Catalano, M. Rand, and K. Rose, "Special Report Stalking Victimization in the United States," 2009. [Online]. Available: https://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf

[13]
River Hart "How to Prevent Cyberstalking via Email, Text, & More," *ProPrivacy.com*. https://proprivacy.com/guides/prevent-cyberstalking

[14] *Types of cyber stalking - online risk: The cyberstalker, Google Sites: Sign-in*. Available at: https://sites.google.com/site/onlineriskthecyberstalker/types-of-cyberstalking