WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Impact of Cybercrime and Hacking Films on Young Generation

Ghorad Naresh Sambhaji

Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra

ABSTRACT

This research paper is to describe the impact on the young generation who watch cybercrime/hacking movies. Films with stories that include aspects of cybercrime/hacking are being made more and more frequently and inclusively, these films are shaping the young generation's view of cybercrimes. This study is to find out if there are any recurring themes in how these movies are portrayed to make an impact on this generation. Using the technique of qualitative data analysis, rules are constructed to identify films that really have the ability to influence public perception. This generation is more likely to be inspired to act in movies. Instead of passively waiting for things to go our way, they give us motivation and ideas to choose the good from it. Some of them are affected in a positive way, but some choose to derive illegal benefits from it. This generation can better distinguish between good and evil through movies.

KEYWORDS: Cybercrime, Hacking, Young generation, Impact, Influence, Cybersecurity.

I. INTRODUCTION

The film industry is notorious for its inaccurate portrayal of cybercrime and hacking movies. What do these movies get right about hacking and digital security? Movies about cybercrime and hackers have romanticized the world of compromised digital security. The level of realism in each film production varies, but they all choose excitement over reality. A cynical person at a keyboard for a few seconds and exclaiming, "I'm in" is a trope prevalent enough in cybercrime movies to serve as its own running gag. Movies often portray hacking as a crime, but in reality it is only about data or the importance of storing data that is important to people's personal information. Watching movies is part of students' daily life. Today, movies are widely available in a variety of formats that can easily be played every day. This makes students more obsessed with watching such crime movies. Sometimes this is also done through an educational announcement. The choice of hacking as a career option has also increased in many ways. In the future, mental health can be seen to be affected through such films. Several current cyber-attacks combine a number of techniques such as social engineering attacks. To illustrate, phishing emails and phone scams use several social psychology theories to get visitors to click on a link, creating a sense of scarcity. In movies and on television, computer professionals work at keyboards at speeds that are hard for most of us to match. However, hacker movies often feature active and exciting cybercrime cases, which makes them more interesting to watch.

II. WHAT IS CYBERCRIME AND HACKING

Criminal activity that uses or targets a computer network or network devices is known as cybercrime. Most cybercrime is committed by hackers or cybercriminals who are badly affected by improper knowledge acquisition. However, there are times when cybercriminals seek to damage systems or networks for personal, financial, or political purposes. Cybercrime can be committed by individuals or groups of online criminals who are well organized, use cutting-edge methods and have extensive technical skills. Some hackers are novices.

The 5 most common types of cybercrime:

- Phishing scams
- Internet fraud
- Online infringement of intellectual property rights
- Identity theft
- Online harassment and cyberstalking

Hacking is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal organized data. Although hacking is not always malicious, the phrase has a bad reputation due to its association with online crime.

III. WHAT ARE CYBERCRIME AND HACKING FILMS

In 1983, War-Games was one of the first hacker films. The protagonist of the story is David, an indifferent high school student who also happens to be a computer prodigy. He stumbles upon a system that doesn't identify itself, but allows him to play games while trying to break into a computer gaming company. Cybercrime, which is on the rise, seems to have affected many film productions. Aiming to raise awareness of these otherwise lesser-known crimes, these films present different types of cases that can happen to anyone. Most cybersecurity movies or shows are based on a true story, which makes watching them exciting and educational at the same time.

Some of the best cyber movies are:

- Live Free or Die Hard (2007)
- Cam (2018)
- Swordfish (2001)
- Bad Samaritan (2018)
- Intelligence (2020)
- Hacker (2016)
- Deep Web (2015)
- Cyber Secrets (2013)

IV. CONSEQUENCES OF COMPUTER CRIME/HACKING MOVIES

With the urgent demand for professionals in the cyber security sector, it is essential to understand the reality of hacking. While movies can make hacking look exciting and glamorous, the reality is that many hacking techniques have harmful effects on user tracking.

A. TEENAGE HACKERS:

According to a crime study, young individuals are more likely to engage in cybercrimes/hacking. Teenage hackers are motivated by idealism and impressing their friends rather than being aware of fraud. Most are influenced in such a way that they are unlikely to engage in theft, fraud or harassment. Teenage hackers find such films more entertaining, instead seeing hacking as a "moral crusade". Others are motivated by the desire to solve technical problems and show off to friends. Young hackers could profit from their skills if they avoided cybercrime.

With a reasonable effort at realism, the movie Blackhat (2015) tried to show how email phishing could be used to get someone's password, but it's unlikely that someone working at the National Security Agency (NSA) would come across such a scam.

Yet, when this type of social engineering is accurately portrayed in movies or on television, it can increase the threat of further fraud by teenagers.

B. EXPECTATIONS VERSUS REALITY:

Most often, hacking is portrayed as a frenetic activity with frenetic stress-inducing music and flashing boxes on the screen.

However, in one episode of the fantasy series ARROW, the heroes can continue to "hack" despite not being able to see their screens, and eventually this hacking war turns into a tennis match, with both hackers sending energy blasts and so on until the opponent's computer is blown up.

However, the capabilities of movies often do not match the features or applications of real hacking systems. Dealing with people's expectations of computing and their understanding of hacking runs particularly common hacks that non-technical people are prone to can be problematic in addressing people's expectations of computer use and hacking.

V. INFLUENCE ON THE YOUNG GENERATION

In fact, hacking is a long boring process of collecting data piece by piece and using that small data to abuse into someone's rights or system, for example: access to the target account.

Some effects on watching movies among the younger generation:

Mental Health:

Films can be used in a variety of ways to provoke a certain kind of provocation feelings and moods that are beneficial for human development and well-being. The young generation watches such hacking movies for entertainment or even as a learning tool that promotes brain development. depending on the program one is watching, different genres of cybercrime/hacking movies produce different highs and lows. Depending on a person's history, interests and personality, certain films may have a different impact on them than others. The physical and mental state of young people is greatly affected by

movies; adverse consequences and destructive behaviour, while benefits include productivity on mental health. The numerous types of cybercrime that young children may observe will influence how they behave as they begin to grow into adulthood. According to a psychological study, watching hacking movies can make young minds less sensitive to the pain, suffering of others, more fearful of the world around them, and more prone to aggressive or harmful behaviour towards each other.

Exposed To Violence:

Today's young generation can access media both on conventional devices such as television and on mobile devices such as laptops and tablets. This makes them more likely to be exposed to violent content such as online hacking or a simple form of cybercrime due to increased access, resulting in harming or injuring people in real life. The violence depicted in such films can lead to the growth of young minds to commit more crime. They start comparing the real world as part of the movie character, which encourages them to hack for evil purposes.

Data Security In Education;

A major risk for universities is the widespread use of the Internet on and off campus. Students, faculty, and staff use extensive Wi-Fi and LAN networks that extend across and between campuses. Hundreds or thousands of people use networks to access the Internet on a range of devices from desktop computers, laptops, tablets and mobile phones. Students use the Internet extensively to research projects, communicate with friends, send e-mails, and enjoy visiting sites that are often, if not always, dubious. The risk of someone becoming a victim of web-borne threats by clicking on the wrong link in their email, or malicious advertising, malicious links or accidental downloads on websites increases with the number of users and the wide and intensive use of the Internet. Hackers occasionally target educational institutions by posting links to student-friendly websites or sending phishing emails to university email accounts. These kinds of criminal aspects have proliferated from the young generation to cheat during papers or to get valuable information from others and use it to blackmail others to complete their work or for fun.

Increase In Crime:

According to published government data, India reported 50,000 cases of hacking crimes in 2020. That's an 11% increase over the previous year, including more than 500 cases of fake news across all media. According to the research, the cyber-crime rate has climbed from 3% in 2019 to 3.7% in 2020. The number of reported cyberattacks, however, fell in 2022, down from 14.02 Lakhs in 2021. As per government figures, 2.08 Lakh incidents were reported in 2018, 3.94 Lakh attacks were recorded in 2018 and 11.58 Lakh cybersecurity incidents were reported to CERT-In in 2020.

Advantages And Disadvantages

The movies show hacking as a quick operation (with a monitor full of running green text). Watching cyber crime and hacking movies doesn't always have a negative effect, but it also has positive effects. The young generation should know the importance of the knowledge shown in movies versus the actual process or work done in real life. Hacking is not only about blackmailing or secretly sharing personal information, but sometimes hacking can be more than that.

Some of the major benefits that the young generation can get through movies are scouting, scanning, gaining access, maintaining access, cleaning tracks, reporting crimes in case of emergency. Film motivated students can take up ethical hacking as their career options as there is an increasing need for employment in various sectors to maintain or save their companies' data from criminal hackers. Hacking by legal means should also be of prime importance to students as movies pretend its illegal way to describe it to the younger generation. Hacking legally can help in the fight against cyber terrorism or prevent any loss of secrets or private information from hackers. Even in the field of banking, the security of a large amount of data can be prevented. The young generation should know that technological security is not always perfect, there are always loop holes.

Although there are some disadvantages that the young generation can influence the movies more on the young generation because they are more influenced in a bad way. Such a bad influence can lead to an increase in terrorism. They can increase cybercrime without having to worry about getting caught. Cybercrimes like malicious attack on someone's private system which is completely illegal. Inspiration for such half knowledge from movies can lead the young generation into trouble. Such activities can cause changes in their behaviour, actions and can change their outlook on everything, they cannot differentiate between reel life and real life. Such films encourage them to take revenge, which leads them to become harassers.

VI. CONCLUSION

The field of cyber security is often portrayed inaccurately in movies. However, by recognizing deviations from reality, we gain a greater understanding of the necessity and value of cyber security solutions as a whole, especially in today's era of rapid technological advancement. While working in cybersecurity, whether as a systems expert or a white hat, can result in a high salary, hacking and cybersecurity aren't nearly as glamorous as they make them out to be in the movies. And a world that is safer for the people you love and know, that fact is better than any movie.

In general, the study supports the possibility of a beneficial effect, as in the case of changing the attitudes of graduate students, but also emphasizes the need to take into account the individual characteristics of the viewer in order to achieve the desired effects. In particular, variations in pre-film moods are likely to be the main reasons for variations in the effectiveness of film impact. The film may have had a negative impact on the students because of their initial hostile attitude towards others. The findings serve as a foundation for further study and raise the following critical questions: elucidating the role that individual differences play in impact effectiveness, predicting how films will positively affect different demographic groups, and identifying the mechanisms underlying sustainability.

BIBBLOGRAPHY

[1] McAlaney, J., Thackray, H. and Taylor, J. The social psychology of cybersecurity. The Psychologist, Vol.29, no.9, 2016, pp. 686

[2] Rogers, M. K., The psyche of cybercriminals: A psycho-social perspective. In G. Ghosh and E. Turrini (Eds.) Cybercrimes: A Multidisciplinary Analysis, 2010.

[3] Leyden, J., Top 10 best hacking films of all time https://portswigger.net/daily-swig/top10-best-hacking-films-of-all-time. 23 April 20

[4] Barrasso, N., 7 Best Movies about Cybersecurity and Hacking. https://www.cybereason.com/blog/moviesabout-cyber-security-hacking-crime, Apr. 18, 2018.

[5] Cybersecurityventures: https://cybersecurityventures.com/movies-about-cybersecurity-andhacking. Accessed June 22, 2020.

[6] Johnson, M. (2013). Cybercrime : security and digital intellience. U.S.A: Gower publishing LTD.

[7] Moon B., Mccluskey J., Mccluskey C. (2010). A general theory of crime and computer crime: An empirical test. Journal of Criminal Justice, 38(4), 767-772.

[8] Schaeff B,Chan H. and Ogulnick S. (2009). Cyber Crime and Cyber Security. A wite paper for Franchisors licensors, and others, p.1-15.

[9] Kirsh SJ. Cartoon violence and aggression in youth. *Aggression and Violent Behavior*. 2006;11:547-557 (2004) (DEC2020BOD)