MWAIS 2023 Proceedings

Midwest (MWAIS)

2023

A Practical and Real-world Discussion of Safety Risks to Children in Cyberspace

Darrell Norman Burrell

Calvin Nobles

A Practical and Real-world Discussion of Safety Risks to Children in Cyberspace

Darrell Norman Burrell
Marymount University
dburrell2@thechicagoschool.edu

Calvin Nobles
Illinois Institute of Technology
cnobles1@iit.edu

ABSTRACT

Ninety-five percent of American teenagers have access to the Internet, and 45% are online almost constantly (Anderson & Jiang, 2018). With the rise of technology, cyber crimes against teenagers are increasing, and keeping them safe online is becoming increasingly difficult. Cybercrimes against teenagers can be in different forms, such as cyberbullying, identity theft, hacking, phishing, exploitation, and online scams (Bozzola et al., 2022). This paper provides an overview of the current trends and statistics of cybercrimes against teenagers and recommends the best approaches to keep teenagers safe online from criminals.

Keywords
Child safety, Cyberbullying, Online Identity Theft, cybercrime, Online cyber risks, Phishing, Online Scams, Online predators, Teenagers

INTRODUCTION

In today's world, technology has become an essential part of teenagers' lives, with many spending most of their time online. While this has brought many benefits, it has also exposed them to cybersecurity risks and cybercrime. This paper explores the nature of those risks and looks for viable solutions. In the digital age, social media platforms have become a daily part of life for many people. As parents, we understand the risk of exposing our children to such platforms and the need to understand their psychological risks and dangers better.

The use of social media in children is a growing concern due to its potential risks and dangers. The American Academy of Pediatrics (AAP) recommends that parents limit their children's use of social media and be aware of potential cyber-psychological risks and cybersecurity dangers that can arise from using these platforms (Bozzola et al., 2022). Cyber-psychological risks and cybersecurity dangers include cyberbullying, online predators, and the potential of exposing children toed to inappropriate content (Bozzola et al., 2022).

Various motivations drive criminals to use the Internet and social media to commit crimes (Crisp, 2021). One of the most common motivations is to gain access to victims' personal information, such as banking or credit card details. Criminals can use this information to commit fraud or steal identities (Crisp, 2021). Additionally, criminals may use the Internet and social media to groom children for sexual exploitation. They use social media to build relationships with children and gain their trust before exploiting them for sexual purposes (Crisp, 2021). Another motivation is to commit cyber crimes, such as hacking into computer systems or websites (Bozzola et al., 2022).

These types of crimes are becoming increasingly common, and they pose a severe threat to the safety and security of children online. Finally, criminals may use the Internet and social media to commit other forms of abuse, such as cyberbullying or harassment (Bozzola et al., 2022). The National Center for Missing and Exploited Children received a record-breaking number of complaints of suspected child sexual exploitation in 2020: over 21.7 million. This number is a new high. This makes the total number of reports obtained in a single year the greatest it has ever been. (National Center for Missing & Exploited Children, 2021). Additionally, a study conducted by the Pew Research Center found that 59% of teens have been the target of some online harassment, and 16% of teens have been the target of severe forms of harassment, such as physical threats or sustained harassment (Anderson & Jiang, 2018). These statistics demonstrate the prevalence of Internet and social media-related crimes, highlighting the need for further research and prevention strategies to combat the problem.

PROBLEM STATEMENT

Ninety-five percent of American teenagers have access to the Internet, and 45% are online almost constantly (Anderson & Jiang, 2018). With the rise of technology, cyber crimes against teenagers are increasing, and keeping them safe online is becoming increasingly difficult. Cybercrimes against teenagers can be in different forms, such as cyberbullying, identity theft, hacking, phishing, exploitation, and online scams (Bozzola et al., 2022). This paper provides an overview of the current trends and statistics of cybercrimes against teenagers and recommends the best approaches to keep teenagers safe online from criminals.

METHOD

The method used included a narrative review of the literature to influence the world of practice and educate parents, children, and researchers on best practices for keeping children safe in cyberspace. A narrative review of the literature is a proven and highly accepted approach to identifying the current trends and debates surrounding a research problem and the various methods and real-world and not theoretical strategies for solving it (Creswell, 2021). The approach to the literature review provided an invaluable tool for both academic and professional research as it consolidates and synthesizes the findings of a wide variety of dispersed and disbanded discussions on the topic into one relevant and comprehensive discussion that can be a valuable guide for others with limited knowledge on this topic (Creswell, 2021).

CURRENT TRENDS AND STATISTICS OF CYBERCRIMES AGAINST TEENAGERS

Cyberbullying

Cyberbullying is a form of online harassment involving electronic devices to spread harmful content about an individual or group. Cyberbullying is a growing concern for teenagers and is prevalent on social media platforms such as Twitter, Facebook, and Instagram (Sonthalia,2021). Cyberbullying has far-reaching consequences on teenagers' mental health, such as anxiety, depression, and suicide (Bozzola et al., 2022).

Inappropriate Material

Children can be exposed to inappropriate content on social media platforms (Sonthalia, 2021). Children on various social media platforms will likely encounter offensive, inappropriate, or illegal content (Sonthalia, 2021). Parents should be aware of the content their children are exposed to and take steps to ensure that their children are not viewing inappropriate material (Bozzola et al., 2022). Additionally, parents should be aware of any potential addiction or obsession their children may have with social media platforms, which can lead to psychological issues such as depression and anxiety (Sonthalia, 2021).

Identity Theft

Identity theft is a cybercrime that involves stealing someone's personal information, such as social security numbers, credit card information, and bank details to commit fraud. Identity theft can have profound financial implications for teenagers and their families, leading to ruined credit scores and debt (Bozzola et al., 2022). Phishing emails frequently target children intending to commit identity theft or otherwise unauthorized use of children's personal information to get money or credit fraudulently. More than one million minors (those younger than 17 years old) in the United States were victims of identity theft in 2017, and the estimated costs associated with these crimes totaled $2.6 billion (Nicholson et al., 2020).

Hacking

Hacking is a cybercrime involving unauthorized access to computer systems or networks. Hackers can steal sensitive information, install malware, or perform other malicious activities. Hacking is the leading cause of data breaches

(Karunakaran et al., 2018). Teenagers are at risk of hacking because they often use weak passwords and share their login details with friends (Bozzola et al., 2022).

Phishing

Phishing is a cybercrime that involves tricking people into revealing their personal information, such as login details or financial information, by posing as a trustworthy source (Bozzola et al., 2022). Phishing scams can have profound financial implications for teenagers and their families. Phishing scams are becoming an increasingly popular attack vector among cybercriminals. While the Department of Defense and the Pentagon report getting as many as 10 million phishing assaults each day, the Anti-Phishing Workgroup typically finds upwards of 40,000 distinct phishing sites each month (Harrison et al., 2016). These sites target approximately 500 distinct brands. However, there is no guarantee that a phishing assault will be successful. According to Harrison, Svetieva, and Vishwanath (2016), only 30–60 percent of all phishing attacks result in a victim being deceived. According to Harrison, Svetieva, and Vishwanath (2016), many attacks are effective, but some are not. This may be due to particular characteristics of the attacks themselves, or it may be due to the characteristics of the individuals who are being attacked. Consequently, it is plausible that characteristics exist within individuals or the content of the phishing message, enabling some attacks to result in higher degrees of victimization than others (Harrison et al., 2016).

Online Scams

Online scams are fraudulent activities that involve tricking people into sending money or personal information. Online scams include fake lotteries, prize draws, and job offers (Bozzola et al., 2022). The Internet is a useful way to reach a mass audience without spending much time or money. A website, online message, or social media can reach large numbers with minimum effort. It is easy for fraudsters to make their messages look real and credible sometimes (Bozzola et al., 2022). Online scams can have profound financial implications for teenagers and their families.

Online Predators

While social media can be a great way to communicate with friends and make new connections, it can also be a dangerous place. Online predators are a severe risk to the safety of children who use social media. Online predators are adults who use the Internet to target and exploit children, often for sexual purposes (Hong et al., 2022). These predators often use social media platforms to form relationships with children, intending to meet them in real life. Naïve children are easily lured into dangerous conversations with these predators and asked to share personal information, photos, or videos (Hong et al., 2022). Without adequate safeguards, children can be at risk of being manipulated by these predators or even meeting them in person, leading to severe physical and psychological harm (Hong et al., 2022).

Online predators, which use the Internet to target and groom children, are a real and present danger to all children using social media (Hong et al., 2022). These predators can use the Internet to contact children, learn about them, and groom them for future exploitation (Dorasamy et al., 2021). They can also use the anonymity of the Internet to disguise themselves and hide their true identity, making them harder to identify (Dorasamy et al., 2021).

The trends in online predator behavior have also changed in recent years (Dorasamy et al., 2021; Hong et al., 2022). Predators are increasingly targeting children through social media platforms such as Facebook, Instagram, and Snapchat (Dorasamy et al., 2021; Hong et al., 2022). Additionally, they use less overt methods of grooming and manipulation, such as compliments and flattery (Dorasamy et al., 2021; Hong et al., 2022).

As such, parents, educators, and other adults must be aware of these trends and take steps to protect children from online predators.

Psychological Theories

Several psychological theories can explain teenagers' vulnerability to cybersecurity risks and cybercrime. The self-control theory suggests that teenagers are more vulnerable to cybercrime because they lack self-control and are impulsive, making them more likely to engage in risky online behaviors (Lyngs et al., 2019).

The social learning theory suggests that teenagers are vulnerable to cybercrime because they learn from their peers and are more likely to engage in risky online behaviors if they see their peers doing so (Bandura, 1977). The routine activity theory suggests that teenagers are vulnerable to cybercrime because they are more likely to engage in online activities, making them more likely to encounter cybercriminals (Cohen & Felson, 1979).

The strain theory suggests that teenagers are more vulnerable to cybercrime because they experience strain and stress, which can lead to deviant online behaviors (Merton, 1938).

Risk Factors for Cybercrimes Against Teenagers

Several risk factors contribute to cybercrimes against teenagers. These risk factors include poor parental monitoring, low self-esteem, impulsivity, lack of cyber awareness, and poor digital literacy (Dorasamy et al., 2021; Hong et al., 2022). Parents play a critical role in protecting their teenagers from cybercrimes by monitoring their online activities and educating them on online safety (Dorasamy et al., 2021; Hong et al., 2022). Moreover, impulsivity is a risk factor for cyberbullying victimization and perpetration among teenagers (Dorasamy et al., 2021; Hong et al., 2022). Digital literacy and cyber awareness can also protect teenagers from cybercrimes by enabling them to recognize and avoid cyber threats (Dorasamy et al., 2021; Hong et al., 2022).

EVIDENCE-BASED PRACTICES TO PROTECT TEENAGERS FROM CYBERCRIMES

Parental Monitoring

Parental monitoring is a critical practice to protect teenagers from cybercrimes. Research has shown that parental monitoring is associated with lower cyberbullying victimization and perpetration among teenagers (Dorasamy et al., 2021; Hong et al., 2022). Parents can monitor their teenagers' online activities using parental control software, restricting their access to specific websites and monitoring their social media accounts (Dorasamy et al., 2021; Hong et al., 2022).

Education and Awareness

Education and awareness programs can protect teenagers from cybercrimes by increasing their knowledge and skills in online safety. Schools, parents, and guardians can provide education and awareness programs to teenagers on online safety, cyberbullying, and the dangers of sharing personal information online (Dorasamy et al., 2021; Hong et al., 2022). Such programs can also teach teenagers to use strong passwords, avoid clicking on suspicious links and report cyber threats to authorities (Dorasamy et al., 2021; Hong et al., 2022).

Digital Literacy

Digital literacy uses technology and information to solve problems, communicate, and create content (Talib, 2018). Digital literacy can protect teenagers from cybercrimes by enabling them to recognize and avoid cyber threats (Talib, 2018). Parents and educators can promote digital literacy among teenagers by providing opportunities to practice digital skills and teaching them critical thinking and media literacy skills (Talib, 2018).

Cyberbullying Prevention and Intervention Programs

Cyberbullying prevention and intervention programs can protect teenagers from the harmful effects of cyberbullying. These programs promote positive relationships, teach social-emotional skills, and support victims and perpetrators of cyberbullying (Alim, 2016). Research has shown that such programs effectively reduce cyberbullying perpetration and victimization among teenagers (Alim, 2016).

EFFECTIVENESS OF TECHNOLOGY-BASED INTERVENTIONS IN PROTECTING TEENAGERS FROM CYBERCRIME

Several studies have examined the effectiveness of technology-based interventions in protecting teenagers from cybercrime. Mobile applications designed to prevent cyberbullying effectively increased teenagers' awareness of safe online practices and reduced the incidence of cyberbullying (Alim, 2016). Online safety programs effectively increase teenagers' knowledge of safe online practices and reduce the risk of cyberbullying (Alim, 2016). Parental controls have also effectively protected teenagers from cybercrime risks (Bozzola et al., 2022).

Parental controls effectively reduce teenagers' exposure to online pornography and violent content (Dorasamy et al., 2021; Hong et al., 2022). Internet filtering has also been effective in protecting teenagers from cybercrime risks. Internet filtering effectively reduces teenagers' exposure to inappropriate content and protects them from phishing scams (Dorasamy et al., 2021; Hong et al., 2022).

Privacy Settings

Modifying some fundamental settings can make it much more difficult for cybercriminals to target you or family members. Several safeguards are available, but not everyone will require or want them all.

Make social media private: Make sure that the privacy settings on your Facebook, Twitter, and any other social media profiles are turned on. Remove anything from your profile that could be seen by the public, such as your location and contact details, if you require such a profile.
Facebook allows users to restrict who can view their friend lists and who can find their profiles. Creating a phony profile of a real person you know and then texting you to get financial assistance is a popular tactic used in online scams. Go to Facebook's Settings and Privacy, Followers, and Public Content, and pick "Who can see the people, pages, and lists you follow?" from the drop-down menu. Choose between My Friends or Just Me.
Tap your profile picture in Messenger, then go to Settings and select Privacy > Message Delivery. Click on Others on Facebook, then select Do not Receive Request from the drop-down menu that appears under Other People. Perform the actions mentioned above for other Instagram users. In the Potential Connections area, change the settings so that you either Do not. Receive Requests or Message Requests will be sent to you. This will restrict the number of potential connections that can message you directly.

You may choose who can add you to groups and who can see your status and personal information by going to the Settings menu on WhatsApp, selecting Account, and selecting the Privacy option.

Phone contacts: Ensure that recognized contacts are entered into the phone's address books to make it simpler to disregard unknown numbers. The next step is to divert calls from unknown numbers to voice mail. They will leave a message if it is significant to them. To silence calls from unknown numbers on an iPhone, navigate to Settings > Phone > Silence Unknown Callers. This will direct everyone you have never previously communicated directly to your voicemail. To access the Phone settings on an Android smartphone, launch the Phone app, navigate to the menu button (it looks like three dots), and then hit that button. The choices for blocking numbers and protecting against spam and caller ID are often found on most mobile devices, even though they go by various names. (If you are screening calls with voice mail, double-check that the outgoing message is recorded and that your inbox needs to be completely filled.)

Enhance the level of privacy you enjoy: You should generally enable the privacy settings on all your devices and apps. Be aware of the most recent cons. Swindlers prefer to take advantage of current events, such as the pandemic or the need for relief in Ukraine. For instance, the Federal Trade Commission warned about student loan scams less than one day after Vice President Biden announced a proposal to cancel some student loans. President Biden announced the initiative.

If you are aware of the most recent cons that are going around, you will be better able to recognize dishonest behavior immediately. You may receive up-to-date information about the most recent scams by visiting websites such as Fraud.org. The Federal Trade Commission (FTC) and the American Association of Retired Persons (AARP) maintain extremely resource-rich websites for combating fraud.

Always operate with the assumption that individuals or businesses are not who they claim to be.
It is easy to imitate a real person or organization. Your initial inclination should be to question whether or not the person is who they say they are. Proceed to the following step, even if you have the slightest bit of uncertainty.

Confirm everything by utilizing a different communication channel. Instead, you should find the most effective means to get in touch with the firm all on your own, such as by visiting the company's website and locating an official customer service number there. If you need clarification on something, you should consult a friend or member of your family.

Please do not respond to messages, do not click on links, and do not pick up the phone when it rings. Avoid becoming involved in any probable scams, even if there is a fascination. This includes refraining from clicking on links sent by contacts that need to be more familiar. Received a text message purporting to be from UPS and relating to a package? Instead, check the official UPS website.

Look for the sender's telephone number, email address, or website URL. Investigate the message for any telltale signs that it is a hoax, and if there is doubt, look it up on Google. When using social networking or messaging apps, verify the authenticity of the user by clicking through to their profile and determining whether or not it was made recently.

REFERENCES

1. Alim, S. (2016) Cyberbullying in the world of teenagers and social media: A literature review, *International Journal of Cyber Behavior, Psychology, and Learning (IJCBPL)*, *6*(2), 68–95.
2. Anderson, M., & Jiang, J. (2018) Teens, social media & Technology 2018, Pew Research Center, https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/
3. Bandura, A. (1977) Social learning theory, Englewood Cliffs, NJ: Prentice Hall.
4. Bozzola, E., Spina, G., Agostiniani, R., Barni, S., Russo, R., Scarpato, E., Di Mauro, A., Di Stefano, A.V., Caruso, C., Corsello, G. & Staiano, A. (2022) The use of social media in children and adolescents: Scoping review on the potential risks, *International Journal of Environmental Research and Public Health*, *19*(16), p.9960, doi: 10.3390/ijerph19169960, PMID: 36011593; PMCID: PMC9407706.
5. Crisp, J. H. (2021) Use and abuse of social media in human trafficking, *Journal of the American Academy of Child & Adolescent Psychiatry*.
6. Cohen, L. E., & Felson, M. (1979) Social change and crime rate trends: a routine activity approach, *American Sociological Review*, *44*(4), 588–608, https://doi.org/10.2307/2094589.
7. Creswell, J. W. (2021) *A concise introduction to mixed methods research*, SAGE publications.
8. Dorasamy, M., Kaliannan, M., Jambulingam, M., Ramadhan, I., & Sivaji, A. (2021) Parents' awareness on online predators: Cyber grooming deterrence, *The Qualitative Report*, *26*(11), 3683-3723.
9. Harrison, B., Svetieva, E., & Vishwanath, A. (2016) Individual processing of phishing emails: How attention and elaboration protect against phishing, *Online Information Review*, *40*(2), 265–281.
10. Hong, S., Lu, N., Wu, D., Jimenez, D. E., & Milanaik, R. L. (2020) Digital sextortion: Internet predators and pediatric interventions, *Current Opinion in Pediatrics*, *32*(1), 192-197.
11. Karunakaran, S., Thomas, K., Bursztein, E., & Comanescu, O. (2018, June) Data breaches: User comprehension, expectations, and concerns with handling exposed data, In *SOUPS@ USENIX Security Symposium* (pp. 217-234).
12. Lyngs, U., Lukoff, K., Slovak, P., Binns, R., Slack, A., Inzlicht, M., Van Kleek, M. and Shadbolt, N. (2019, May) Self-control in cyberspace: Applying dual systems theory to a review of digital self-control tools, In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-18).
13. Merton, R. K. (1938) Social structure and anomie, *American Sociological Review*, *3*(5), 672–682.
14. National Center for Missing & Exploited Children (2021) Online enticement. https://www.missingkids.org/blog/2021/rise-in-online-enticement-and-other-trends--ncmec-releases-2020-
15. Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O. D., & Anderson, P. (2020, September) Investigating teenagers' ability to detect phishing messages, In *2020 IEEE European Symposium on Security and Privacy Workshops* (pp. 140–149), IEEE.
16. Sonthalia, S. (2021) Evolution of cyber bullying and its consequences on teenagers, *International Journal of Law Management & Humanities*, *4*(3),3211.
17. Talib, S. (2018) Social media pedagogy: Applying an interdisciplinary approach to teach multimodal critical digital literacy, *E-learning and Digital Media*, *15*(2), pp.55-66.