Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 10, October: 2022

Exploring Cybercrime: Unveiling its influence on Today's Youth

Tasleem Bano
Assistant Professor
Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur, Rajasthan

Shyama Yadav
Assistant Professor
Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur, Rajasthan

Vidhan Singh
Science Student
Eklavya Educational Complex, Patna, Bihar

Devendra Kumawat
Science Student
Diamond Academy senior secondary school, Jaipur, Rajasthan

Abstract

Cybercrime it's not be a stranger word for the today's world. Cybercrime is a type of crime that committed on internet and by a computer lot his papers are write for describe the cyber crime and study the how Today's youth are trapped in this web. Cybercrime is not only committed by the young; it is done by people of all ages. Sometimes, a person may not even know that they are engaging in cybercrime.

Keywords

Cybercrime, computer, internet, crime, Cyber-attack, laws, virus, attacker

I. INTRODUCTION

Digitization is a great success for humans. Computers and the online world have changed the lifestyle of the entire world because they make things very easy. However, today when we use computers and the online world, it is not completely safe for users. The online world has a positive impact as it connects the whole world, allowing users to communicate with anyone. It is very useful for sharing knowledge and representing ourselves globally. But some users engage in criminal activities and exploit the online world

http://doi.org/10.36893/IEJ.2022.V51I10.094-093

for personal gain. Due to a lack of awareness, some users misuse computers and the internet, which can lead to criminal activities.

Nowadays, 80% of people are aware of cybercrime, but many lack knowledge about its dangers. Some may mistakenly believe that the term "cybercrime" doesn't harm people, but in reality, it poses serious threats to innocent users. It's crucial to educate and raise awareness about Cyber security to ensure the safety of individuals online.

Cybercriminals target online businesses because they have a lot of user data. They demand money, but this attack affects every single user because their personal information is exposed to others. This data contains personal information of users like full name, mobile number, address, debit card details, email, and government documents, etc.

To reduce cybercrime, we need to educate and make people aware. Many cybercriminals take advantage of the lack of awareness and information to target innocent users and harm them financially or breach their data. By spreading awareness and providing proper education, we can protect the cyber world.

EXPLANATION ON CYBERCRIME

Cyber crime is a type of crime that are conduct by computer or internet lack of knowledge and awareness it’s affect the financial, mentally and reputational well-being. It covers a wide range of offenses, including the dissemination of dangerous software, online fraud, identity theft, and hacking.

II. TYPES OF CYBERCRIME THAT AFFECT YOUTH

Young people can be impacted by a variety of cybercrimes; some typical instances are..Cyberbuilyuing Cyberbullying is the term used to describe the act of harassing someone online, usually through the transmission of threatening or frightening communications. This negative conduct might appear on mobile devices, social media, messaging apps, and gaming websites. Its repeated nature and intention to instill fear, wrath, or shame in those it targets are what define it..

Here are a few instances of cyberbullying:

- Sending mean, threatening, or embarrassing texts, emails, or direct messages.
- Sharing compromising or humiliating photos or videos of someone on the internet.
- Impersonating someone online and sending mean or embarrassing messages on their behalf.
- Isolating someone from online communities or activities.

http://doi.org/10.36893/IEJ.2022.V51I10.081-103

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 10, October: 2022

The effects of cyberbullying can be catastrophic for victims. They could feel a variety of unfavorable feelings, such as embarrassment, fear, anxiety, and melancholy. In addition, social isolation, subpar academic achievement, and even death can result from cyberbullying.

Sexual abuse

The use of technology for a child's sexual exploitation or abuse is known as online sexual abuse. This can contain content related to child sexual abuse, sexting, and grooming. The physical and mental well-being of victims of online sexual assault may suffer long-term consequences.

The process through which an adult establishes a rapport with a youngster in order to win their trust and take advantage of them sexually is known as grooming. To get in touch with kids, groomers can utilize social media, gaming platforms, and messaging apps. To win the trust of the youngster, they could assume phony identities, act younger than they actually are, or present presents or other incentives. The groomer may begin sending the child sexually suggestive texts or pictures or attempt to get them to have sex once they have earned their trust..

Sending or receiving sexually provocative texts or photographs is known as sexting. Consensual sexting is possible, but it can also be used to mistreat or exploit minors. A groomer might, for instance, coerce a youngster into sending them sexts or threaten to reveal the child's private communications to others if the child disobeys their requests..

Any visual representation of a child participating in sexual behavior is considered child sexual abuse material. This can apply to pictures, movies, and content that is live-streamed. It is forbidden to own or disseminate materials that depict child sexual assault.

Victims of online sexual abuse may suffer terrible consequences. They could feel a variety of unfavorable feelings, such as embarrassment, fear, anxiety, and melancholy. Substance misuse, food disorders, and post-traumatic stress disorder (PTSD) can all result from online sexual assault. Extreme instances of sexual abuse online can result in suicide.

There are a number of things that can be done to prevent and address online sexual abuse. Parents and educators can play a vital role in educating youth about online sexual abuse and teaching them how to stay safe online. It is also important to create a safe and supportive environment for young people to talk about their online experiences.

Here are some tips for preventing and addressing online sexual abuse:

* Talk to youth about online sexual abuse and the different types of online sexual abuse that can occur.

http://doi.org/10.36893/IEJ.2022.V51I10.081-103

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 10, October: 2022

* Teach youth to be careful about what information they share online and who they communicate with.

* Monitor youth's online activity and use parental controls to block access to inappropriate websites.

* Make sure that youth use strong passwords for all of their online accounts and that they enable two-factor authentication whenever possible.

* Install security software on all of the youth's devices and keep it up to date.

* Create a safe and supportive environment for youth to talk about their online experiences. If a young person tells you that they have been a victim of online sexual abuse, take their concerns seriously and offer them support. You can also help them to report the crime to the appropriate authorities.

It's critical to realize that you are not alone in experiencing online sexual assault and that support is accessible. Ask for help from a responsible adult, such as a parent, teacher, or counselor. Additionally, think about reporting the abuse to the platform or website that is hosting it.

Extra advice for handling sexual assault on the internet:

• Refrain from answering the abuser. It will only inspire them if you reply.

• Preserve the abuse's proof. Screenshots of emails, texts, or posts on social media may be included in this.

• Prevent the abuser from reaching out to you.

· Talk about the situation and discuss your experiences with a trustworthy adult.

• Make self-care a priority by making sure you get enough sleep, eat a healthy diet, and work out frequently.

Although it is a severe issue, it is vital to keep in mind that you have options for self-defense and coping with online sexual abuse.

Online scams

Online scams are like digital traps set by cunning individuals to trick unsuspecting victims and steal their money or personal information. These scams can range from fake lottery winnings to phishing emails that mimic trusted organizations. It's important to stay vigilant, educate ourselves about common scam tactics, and never share sensitive information with unknown sources online. Remember, staying informed is the key to protecting ourselves from online scams

Phishing scams:

http://doi.org/10.36893/IEJ.2022.V51I10.081-103

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 10, October: 2022

Phishing scams are like digital traps set by cunning individuals to deceive people into revealing sensitive information. These scams can be as sneaky as an email that looks like it's from your bank, asking you to urgently verify your account details on a fake website. It's important to stay cautious and double-check the authenticity of any requests before sharing personal information online. Stay vigilant and keep your data safe!

Picture this you admit a dispatch that appears to be from a well- known online retailer. The dispatch claims that there's an issue with your recent purchase and urges you to click on a link to resolve it. still, that link leads you to a fraudulent website designed to steal your particular information and fiscal details. By falling victim to this fiddle, the cybercriminals gain unauthorized access to your sensitive data, putting you at threat of identity theft and fiscal loss. Phishing swindles frequently exploit trust and produce a sense of urgency to trick individualities into discovering their nonpublic information. It's pivotal to remain watchful and corroborate the authenticity of any requests before participating particular details online. licit associations will know ask for sensitive information through relaxed channels or unanticipated dispatches Flash back, being apprehensive and conservative is vital in securing yourself against phishing swindles and other forms of cybercrime. Stay informed and stay safe

Honey trap

A "honey trap" is a type of cybercrime that occurs internationally. It often targets army soldiers. In this scheme, a person, whether a man or a woman, contacts someone and builds a sympathetic connection. After prolonged conversations, they attempt to gather personal information. The purpose of a honey trap is to cause physical and financial harm. It's crucial to be cautious when strangers show sympathy and try to form emotional bonds. Avoid sharing any personal information and don't get overly excited when talking to people of different genders. Remember, once they have your information, they may resort to blackmail. Stay safe and stay alert!

Loan fraud

During the COVID-19 pandemic, many people lost their jobs and businesses suffered. Criminals take advantage of this situation by creating fraudulent loan applications and advertising them on various platforms. Innocent people apply for loans, but the criminals demand high interest rates and resort to abuse and blackmail when they can't repay. Be cautious and apply for loans through legal banks.

Technical support scams

http://doi.org/10.36893/IEJ.2022.V51I10.081-103

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 10, October: 2022

Technical support scams involve scammers pretending to be legitimate tech support representatives to deceive and defraud people. They use tactics like cold-calling, pop-up ads, and phishing emails to trick victims. Be cautious and seek support from trusted sources to avoid falling victim these scams. Spread awareness to help others stay safe online.

Gaming scams

Nowadays, children are more into video gaming and may unknowingly install gaming apps that can be used for cyber fraud and crime. Cyber attackers upload malicious apps on the Play Store, which can infect your device and give them remote access. Before installing any app, check for positive ratings and ensure it won't harm your system. Spread awareness among children about these risks.

Identify

Identity theft is a serious crime where someone steals your personal information, such as your name, Social Security number, or credit card details, and uses it without your permission. This can lead to various fraud activities, like opening new accounts, making unauthorized purchases, or even committing crimes in your name. It's essential to be cautious and take preventive measures to protect yourself from identity theft. This includes safeguarding your personal information, using strong passwords, being wary of phishing attempts, and regularly monitoring your financial statements.

Data breaches

Due to the use of different computer applications and web pages for connecting to social media, data breaches are increasing. We share our data on social media, such as bios, photos, videos, etc., to represent ourselves. Some applications request permission to use your device's camera, microphone, and storage. Users often overlook reading and accepting these permissions. These apps and social media platforms can potentially breach your data and share it with business companies. It's important to be cautious and avoid sharing suspicious or important information on social media. Always read the permission list that appears after logging in and avoid accepting unwanted permissions for apps.

Parcel delivery fraud or OTP theft

Parcel delivery fraud is a new way for criminals to financially harm people. In this fraud, a delivery person comes to your home and gives you a parcel that you didn't order. When you inform them that the parcel wasn't ordered by you, the delivery person asks for an OTP to cancel or return the order. If you provide the OTP, they can steal your banking and social media account information and carry out cyber attacks against you. If you encounter this situation, remember not to share any OTP or personal

http://doi.org/10.36893/IEJ.2022.V51I10.081-103

information and refuse to accept the parcel. Also, make sure to file a complaint at the police station. If you have lost money, call 1930 immediately.

a. Social account

On social media platforms, anyone can have an account, including attackers who monitor your activity. Therefore, it's important to connect with legitimate and verified users. Additionally, remember to change your social media account password regularly. Be cautious and never open links sent by strangers. Protect your account with a strong password and avoid sharing private images and videos on social media platforms

Malicious software

Malicious software, also known as malware, refers to any software designed to harm or exploit computer systems. It can include viruses, worms, ransomware, and spyware. One unique aspect of malware is its ability to disguise itself and spread through various channels, such as email attachments or infected websites. It may result in financial loss, data breaches, and compromised personal information security. Therefore, to safeguard yourself from malware attacks, it's essential to have up-to-date antivirus software and adopt safe browsing practices.

Worms:

Worms and viruses are both dangerous programs, however worms don't require a host file to propagate. They have the ability to propagate throughout networks and duplicate themselves, harming computer systems. Worms can infect other devices through a variety of techniques and by taking advantage of software flaws. To defend against worms, it's critical to maintain current software and implement robust security measures

Trojans: Trojan horses are cunning pieces of malware that pose as safe software. Once on your computer, they have the ability to corrupt data, steal personal information, and even take over. Having robust antivirus software is essential, and you should exercise caution while downloading files or clicking on strange URLs.

Ransomware:A dangerous kind of software called ransomware encrypts your files and requests a fee to unlock them. Via phishing emails, malware downloads, or hacked websites, it can infiltrate your machine. You should periodically backup your files, keep your antivirus software up to date, and exercise caution when opening email attachments and clicking on dubious links in order to protect yourself**.**

http://doi.org/10.36893/IEJ.2022.V51I10.081-103

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 10, October: 2022

Spyware: Malicious software known as spyware gathers data from your device covertly and without your awareness. It has the ability to log your keystrokes, monitor your online activity, and even record your chats. Make sure you have dependable antivirus software and stay away from downloading files from untrusted sites to protect yourself from spyware. Remain alert and safeguard your gadgets.

III. IMPACT OF CYBERCRIME ON YOUTH

In the current digital era, youth cybercrime is a major worry. Cybercrime is the term used to describe illegal actions committed online, including identity theft, hacking, online frauds, and cyberbullying. Young people who participate in these activities may suffer negative social and personal consequences.
The theft of private information is one of the main effects of cybercrime on young people. Young people are using social media and online platforms more and more, and they frequently post personal information and interact online. Sadly, fraudsters may use this data for nefarious intent, which could result in financial fraud and identity theft.

In addition, the problem of cyberbullying has become widespread among youth. Bullies can target their victims using online messaging services and social media, which can lead to mental anguish, anxiety, depression, or self-harm. Bullies can harass their victims more easily on the internet since they can do so anonymously and without worrying about repercussions.
Cybercrime affects young people in ways that go beyond immediate repercussions. It may also have an effect on their careers and academic pursuits. For example, becoming a victim of phishing or other internet scams can lead to reputational harm and financial loss. Furthermore, engaging in illicit online activity may result in legal ramifications that could negatively impact one's opportunities going forward.
It is imperative to increase awareness and offer education on internet safety in order to mitigate the negative effects of cybercrime on young people. Communities, parents, and schools should collaborate to educate children about the dangers of the internet and self-defense techniques. Stricter laws and regulations against cybercrime can also serve as a deterrent and give young people a safer online environment.

IV. CONCLUSION

As my study thesis on cybercrime and its effects on today's kids comes to a close, it is evident that this is a problem that has to be addressed. Cybercrime has a significant impact on youth, influencing their opportunities for the future, education, well-being, and privacy. It's critical to create stronger legislation, educate our children about internet safety, and increase public awareness in order to address this. By

http://doi.org/10.36893/IEJ.2022.V51I10.081-103

working together, we can make the internet a safer place for the next generation. Let's arm kids with the information and tools they need to safely traverse the internet. Continue your fantastic work of bringing attention to this crucial subject!

REFERENCE:

[1] 1. Twenge, J. M., & Campbell, W. K. (2018). "The narcissism epidemic: Living in the age of entitlement." Atria Books.

[2] 2. Anderson, C. A., & Dill, K. E. (2000). "Video games and aggressive thoughts, feelings, and behavior in the laboratory and in life." Journal of personality and social psychology, 78(4), 772.

[3] 3. Arnett, J. J. (2000). "Emerging adulthood: A theory of development from the late teens through the twenties." American psychologist, 55(5), 469.

[4] 4. Kuss, D. J., & Griffiths, M. D. (2012). "Internet gaming addiction: A systematic review of empirical research." International journal of mental health and addiction, 10(2), 278-296.

[5] 5. Subrahmanyam, K., & Greenfield, P. (2008). "Online communication and adolescent relationships." The Future of children, 18(1), 119-146.

[6] 6. Prensky, M. (2001). "Digital natives, digital immigrants part 1." On the horizon, 9(5), 1-6.

[7] 7. Lenhart, A., & Madden, M. (2007). "Teens, privacy, & online social networks: How teens manage their online identities and personal information in the age of MySpace." Pew Internet & American Life Project.

[8] 8. Boyd, D. (2014). "It's complicated: The social lives of networked teens." Yale University Press.

[9] 9. Moreno, M. A., & Uhls, Y. T. (2019). "New media, old dilemmas: The challenges of balancing online social and academic lives." Pediatric annals, 48(1), e3-e8.

[10] 10. O'Reilly, T. (2005). "What is web 2.0: Design patterns and business models for the next generation of software." Communications & strategies, 65(1), 17-37.

[11] 11. Subrahmanyam, K., & Smahel, D. (2011). "Digital youth: The role of media in development." Springer Science & Business Media.

[12] 12. Rideout, V. (2015). "The common sense census: Media use by tweens and teens." Common Sense Media Research.

[13] 13. Brown, J. D., & Bobkowski, P. S. (2011). "Old media and the internet: Competing or complementing?." Journal of communication, 61(3), 498-516.

[14] 14. Heath, C., & Luff, P. (2000). "Technology in action." Cambridge University Press.

[15] 15. Livingstone, S., & Helsper, E. J. (2007). "Gradations in digital inclusion: Children, young people and the digital divide." New media & society, 9(4), 671-696.

http://doi.org/10.36893/IEJ.2022.V51I10.081-103

[16] Kaushik, M. and Kumar, G. (2015) “Markovian Reliability Analysis for Software using Error Generation and Imperfect Debugging” , International Multi Conference of Engineers and Computer Scientists 2015, vol. 1, pp. 507-510.

[17] R. Sharma and G. Kumar, "Working vacation queue with K-phases essential service and vacation interruptions," International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, India, 2014, pp. 1-5, doi: 10.1109/ICRAIE.2014.6909261.

http://doi.org/10.36893/IEJ.2022.V51I10.081-103