Journal of Computer Science & Computational Mathematics, *Volume 13, Issue 1, March 2023*
DOI: 10.20967/jcscm.2023.01.004

Cybercrime Threats in Technology Era

Asmaa Al-Hakimi[1,*], Mohammed Nur[2]

[1]Faculty of Information Sciences and Engineering, Management and Science University, University Drive, Off Persiaran Olahraga, Section 13, 40100 Shah Alam, Selangor Darul Ehsan, Malaysia
[2]Kulliyyah of Economics Management Sciences (KENMS). International Islamic University Malaysia (Universiti Islam Antarabangsa Malaysia), Jalan Gombak, 53100, Selangor
[*]Corresponding author email: asmaa@msu.edu.my

***Abstract*:** The rapid advancement of technology has led to a complete erosion of privacy for users. Digital criminals have disregarded any privacy regulations and are engaged in various forms of digital crimes, including selling private information, online stalking, hacking personal devices, and blackmailing and abusing individuals by stealing their private information. This extends to online child abuse, kidnapping, human trafficking, and numerous other digital crimes. Users' private digital data is compromised without their consent, solely for the purpose of financial gain and personal benefit, regardless of how users feel about their data being used without permission. Hackers, spammers, and cybercriminals dominate the internet and exploit innocent users, subjecting them to abuse, blackmail, and trading of their information, often resulting in devastating consequences such as suicide due to severe abuse, manipulation, and fear. Users can no longer feel safe even within the confines of their homes, as they are being spied on through webcams and malicious files like malware. Cybercrime, social engineering, spyware, and malware are some of the negative outcomes of technology misuse, where users are manipulated to gain access to their private data. This article critically examines the revolution of cybersecurity in the age of technology and proposes technical guidelines to prevent cybercrime and safeguard users' data and privacy from unauthorized intrusion.

***Keywords*:** Cybercrime. cybersecurity. cyber planning. dark web. social engineering and digital privacy.

1. Introduction

Privacy refers to the state of being isolated and free from surveillance, where users can navigate the digital world and maintain a personal space without interference from external forces like hackers or commercial advertisements. It has become recognized as a fundamental human right, with users having the right to be left alone while using digital services. Personal information privacy involves individuals having control over their own information. However, the significant advancements in internet technology and various services and applications have greatly diminished user privacy in all aspects. Users no longer experience freedom while browsing as they must constantly defend themselves against various attacks from multiple sources. Internet users face numerous infringements on their privacy, with commercial companies and platforms utilizing and selling their information for business purposes without regard for privacy concerns [1]. Hackers and spammers stealthily steal users' private information to use as a weapon for blackmail, regardless of the potential harm it may cause. The U.S. Federal Trade Commission (FTC) reports that 85% of websites collect personal information from consumers, but only 14% have disclosed their privacy practices. Privacy concerns vary among countries and depend on factors such as culture, education, illegal digital practices, and government actions against technology misuse. Addressing these technology-related problems incurs substantial costs for users and governments seeking data protection and privacy. In 2018, according to the Society Online Trust Alliance (OTA), there were 2 million recorded cases of cybercrime, totaling $45 billion in financial losses, 1.3 million reported crypto-jacking attacks, and 60,000 total breaches. Legislative and regulatory actions worldwide have increased recently, aiming to enforce organizations' responsibility to adequately protect user data. Identity theft resources centers reported 1,244 private data breaches in 2018, exposing approximately 2 billion records. The number of breached sensitive records reached 447 million [2] [3]. Privacy rights clearinghouses reported 635 breaches and 1.4 billion exposed records in the same year. During the COVID-19 pandemic in 2020, cybercrime and malicious activities significantly rose, with personal information being stolen through network breaches and exploited for financial gain. Cybercriminals took advantage of mobile shopping and transactions, as mobile devices were often left unprotected. The pandemic heightened vulnerability, leading to an increase in targeted attacks. Criminals capitalized on the global spread of COVID-19 to conduct phishing scams and deceive unsuspecting victims. Malware, spyware, and Trojans were found embedded in interactive COVID-19 maps and websites. The following sections will delve into various topics, including the negative aspects of technology, cybersecurity issues stemming from technology misuse, internet crimes, the dark web, social engineering, and guidelines for cyber protection. Future developments will also be discussed [4][5] [6] .

2. Research Objectives

- To identify and analyze the different types of cybercrime threats that have emerged in the technology era.
- To identify and analyze the different types of cybercrime threats that have emerged in the technology era.
- To explore the methods and techniques employed by cybercriminals to carry out their criminal activities.

- To propose approaches and solutions for preventing and combating cybercrime.
- To raise awareness about the potential risks and dangers posed by cybercrime and promote digital knowledge and safe online practices.
- To provide recommendations for policymakers, organizations, and individuals on how to enhance cybersecurity and protect against cybercrime threats.

3. Internet Crimes

As technology continues to advance and the widespread availability of the internet, there has been a corresponding increase in harm and violations. Consequently, digital crimes are now occurring around the clock [7]. These digital crimes have resulted in users losing their privacy, finances, and, most significantly, their sense of self in various ways. The range of internet and computer crimes is extensive, including activities such as the dark web, spam, cybercrimes, spoofing, pornography, e-commerce fraud, malware, and social engineering. The subsequent section will provide a detailed examination of these internet crimes [8].

3.1 Dark Web the Dark E-Commerce

The Dark Web, also called Dark Net, is a web-based that contains all sorts of data that is related to anonymous users. Users data is protected in the web database via encryption, obfuscation, and forwarding. This specific web is encrypted. Access to this web is limited to dedicated software or specific proxying or authentication. This web is associated with criminal activity of many levels such as buying or selling drugs, pornography, and gambling [9]. There are many forms of the dark web that can be found on the net, these forms are:

- Tor (The Onion Router)
- Freenet
- peer-to-peer I2P
- Friend-to-Friend
- Riffle
- Freenet
- Tor2Web

The strong protection of anonymity has allowed the web to be the main channel to sell all types of banned and harmful items. This strong protection and the advantage of dealing behind the screen without being seen have created a great opportunity to harm innocent users via child abduction and abuse, human trafficking, and human abduction, and international humiliation of weak users who dont have the ability to free themselves from the abductor. In the dark web, a strong and smart user who has great power can reach almost any ordinary user surfing the net and they can harm them by taking advantage of their weakness. For those who get harmed via the dark web, there is almost no chance to escape. To access the dark web, there is a special browser such as the TOR browser, this browser provides more security and privacy. Most of the dark web sites benefit political dissenters and users who are trying to keep medical conditions private. The dark web has approximately 2.5 million daily visitors. This number of visitors has made the dark web a perfect sanctuary for criminal organizations and individuals and terrorist groups to communicate to sell and buy anything. Human abduction via the dark or deep web is very much possible. The criminal or the insane user on the dark net has the privilege of selecting any person of interest to be abducted for their pleasure or any other needs. There is a high chance that the victim does not even know about the dark net or why they have been abducted. This is how powerful the dark web is. The following sections present several crimes on the Dark Web [10].

3.1.1 Kidnapping for the Dark Web

Young girls are abducted for the purpose of the Dark Net's criminal activities. Chloe, for instance, was lured to Milan, Italy, under the fabrication of a modeling project. However, she was forcibly injected with the tranquilizer ketamine drug, placed inside a bag, and transported in the trunk of a car for approximately 120 miles to an isolated farmhouse. Throughout most of the journey, Chloe remained unconscious, having been gagged by her abductor. The horrifying revelation she received from the abductor was that she would be sold as a sex slave on the dark web, with a starting bid of 300,000 [11].

3.1.2 Child Sexual Abuse

Benjamin Faulkner, a Canadian individual, was involved in forbidden activities on the dark web, where he owned a disturbing website called "Child's Play." This dark-net child pornography website hosted over one million profiles and featured more than 100 pornography producers who had engaged in heinous acts of rape and brutality against children. These acts were documented in sadistic videos, intended to cater to the desires of pedophiles worldwide. Eventually, Benjamin Faulkner was apprehended, as authorities discovered an electronic device in his possession containing 47,000 images of child pornography and 2,900 videos. Additionally, his associate served as the administrator of another dark net child pornography site known as "The GiftBox Exchange," which was forcibly shut down in November 2016. Figure 1 presents some of the videos for users to access and watch kids being sexually abused [12].

Darknet is significant for vendors of child pornography, there are certain sites that provide this service such as (Hard Candy, Jailbait, Lolita City, PedoEmpire, Love Zone, The Family Album, and Kindergarten porn) that allow such users to communicate and share fantasies of child love practices. The group of users who get engaged with these sites are pedophiles. This group of users shares approaches and strategies for seducing and engaging in sexual acts with children. Figure 2 presents Childhub where female kids are sexually abused and being watched alive.

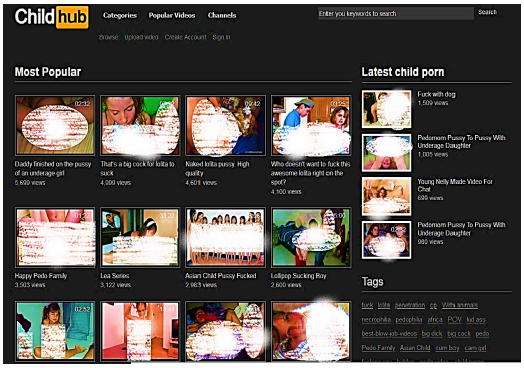

Figure 1. Child hub.

On the Dark Web, experts coach others on how to avoid law enforcement authorities and discuss encryption and anonymity techniques to prevent online detection. In the United States in the dark web around 200,000 children are trafficked for sex where each child coast from $150,000 to 200,000$. Several Darknet websites live streaming the rape and abuse of children. In Asia, Pedophiles direct rapists via video feed to coach them to reach the perfect fantasy. In one of the cases in the dark net, one had the privilege to order a group of eight men to rape eight-year-old girls alive to meet his fantasies for a sum of $100. To prevent traces of the cases images were only streamed instead of downloaded [13].

In some cases of child abuse and pornography in the dark net come from family members, in Germany, a couple operated a pedophile ring as a business has used their son for pornography, according to the police, the abusers had paid around č10,000 one of the times they abused their son. Videos of the son being sexually harassed have been sold on the dark net for the couples benefit. Moreover, the son was threatened by his mother to be sent to foster care if he reported the incident to the police. The couple was arrested and convicted of prostitution, rape, sexual and physical abuse, humiliation, and bondage for almost 60 separate identifies acts by the court [14].

It is crucial to address the following significant inquiries: What was the duration between the police's discovery and the arrest of the perpetrators? What is the current whereabouts of the child involved in these heinous acts? How can this child overcome the traumatic experiences and develop into a well-adjusted adult with a normal life? Is there a possibility for the child to regain the lost years of their childhood? Why hasn't the specific dark net platform been closed by authorities, and what factors contribute to its ability to remain operational and continue functioning? Furthermore, what about the fate of the other children who have fallen victim to the dark net's grasp?

The dark net showcases videos where adults engage in the exploitation of children, completely disregarding the children's right to safety. As a result, these children are reintegrated into society burdened with severe trauma, which unfortunately pushes some of them towards a path of relentless criminal behavior. In some cases, the proposed solution to halt their crimes is to condemn them to death, without considering the experiences and circumstances that led them to develop such a criminal mindset [15]. The question arises: Who can be held accountable for these disturbing circumstances?

Black Death is an Eastern European group operating on the Dark Web. This dark service deals with selling sex slaves to Saudi Arabia and provides virgin auctions for girls as young as fifteen. Users can see ads about the girls age, hair color, and other measurements. One of the victims is Laura, she is 15 years old and was booked for an auction with a starting price of č575,000. One of the latest sales in 2016 was 17 years old female who was born in the UK. The starting price of her auction started from č92,000. Apparently, the advertisement of these girls includes a note that says (the abductors do not sell girls who are ill, pregnant, young mothers, or have STDs). In the dark net, the abductors do not shy away to advertise they can kidnap specific targets for their desire with consideration of the high price that comes along with it. Figure 3 presents a list of videos to watch in the 365cp dark net market [16]. Figure 4 presents some of the abducted children being assaulted for pleasure. .

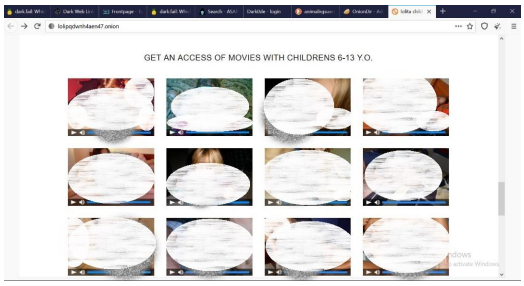

Figure 2. Lolita child porn dark net.

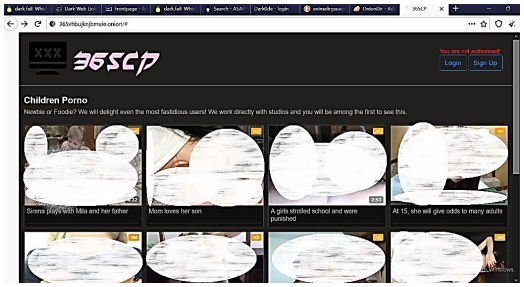

Figure 3. 365cp child porn dark net.

3.1.3 Girls on Sale and Auctions for the Dark Web

In certain cases, the individuals responsible for the kidnappings have been apprehended and sentenced to approximately 16 years or longer in prison. However, it appears that those who were arrested are typically the transporters rather than the masterminds who operate covertly in the background. They serve as expendable pawns to sustain the operations of the dark web enterprise. This method of compromising lower-level individuals is not limited to kidnapping but also

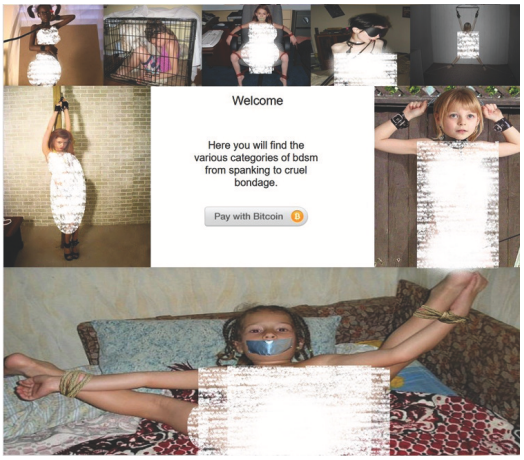

Figure 4. Kids are sexually abused for online pleasure.

applies to drug trafficking, where the main orchestrators manipulate lesser individuals to ensure the smooth functioning of their criminal business. The fate of innocent transporters being sentenced to death does not concern these higher-level criminals. Such actions from these "big heads" create an illusion for society that law enforcement is effectively tackling the situation by apprehending the culprits. One of the abductors, arrested in 2018, admitted to earning $17.7 million through the sale of girls on the dark web facilitated by the Black Death Group[17]. This kidnapper received a prison sentence. However, the pressing questions remain: Where are those girls? Have any of them been located? What good is it if one criminal is behind bars while the victims remain missing, and the original organization continues to perpetrate its crimes? Figure 5 presents videos of children being assaulted ready for download.

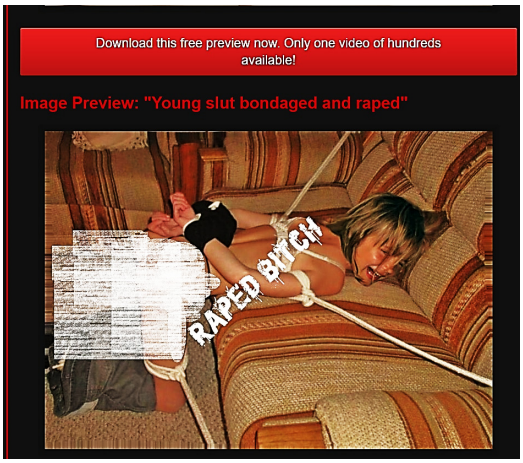

Figure 5. Children suffer the pain of torture.

3.1.4 Red Rooms. Face Death for Digital Pleasure

Red rooms are considered the pleasure rooms in the dark web. Offenders on the dark web will get the victim and open the opportunity for dark Webbers to request anything to be done to the victim, such as rape, torture, killing, and anything that can get into the viewers imagination. Victims have no say, no objections, or any control. They just must face death for digital pleasure. The victims of red rooms can be children or adults of different genders. Figure 6. presents red rooms on the dark web.

Figure 6. Red room access home page.

3.1.5 Human Organs Sold on the Dark Web

Without their consent, victims are abducted so that their organs can be sold on the dark web. The victims won't ever be found again after that. If a victim is discovered, they will either have an empty body or have been horribly disfigured. Figure .7 presents a home page for selling human organs on the dark web [17].

On the Dark Web, sellers have the ability to openly advertise hitman services. Users are given the option to hire these hitmen to eliminate a specific target, allowing them to even choose the preferred method of killing, whether it be a violent dog attack, a fatal gunshot, or a torturous approach. In these sinister corners of the internet, the sanctity of human life holds no significance; the sole determinant is the amount one is willing to pay to accomplish their sinister objective. Individuals seeking the elimination of a person of interest must locate the appropriate dark net platform that offers the desired method of killing or torture. Once a suitable service is found, the buyer is required to make the payment using Bitcoin. A well-known entity within the dark net for providing hitman services is Besa Mafia, where both buyers and sellers are able to maintain anonymity without revealing their true identities. Figure 8 and Figure 9. present samples of hitman pages on the dark web [18].

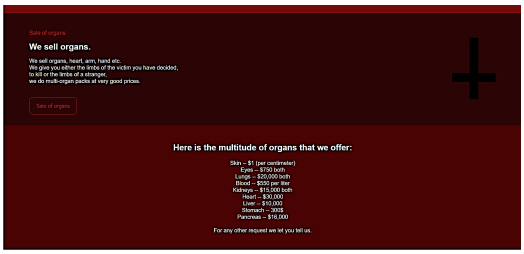

Figure 7. Red room access home page.

Summary

The dark web has accumulated many victims and users who derive pleasure from inflicting harm upon innocent individuals who are defenseless against violence. If any of these victims miraculously escape the clutches of the dark web, what kind of life awaits them afterward? This question holds true regardless of whether the victim is an adult or a child. Why are these victims blamed when they transform into terrifying

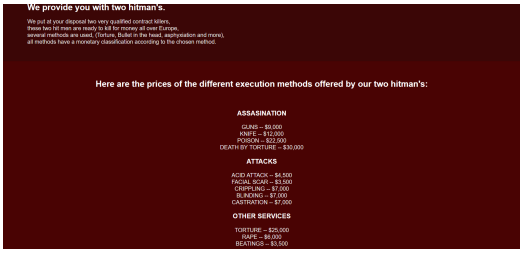

Figure 8. Hitman offers.

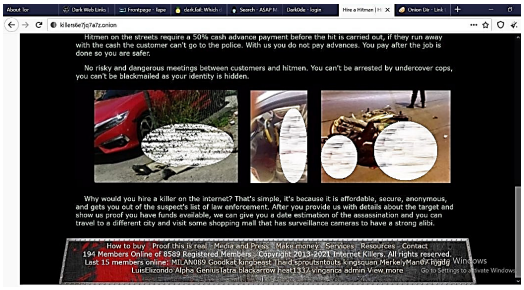

Figure 9. Hire Hit-Man dark net.

criminals seeking revenge against society? In one way or another, the dark web fosters a corrupt community that is solely concerned with digital crime [19]. The following are some links that were utilized to access the dark web to obtain the sample Figures featured in the paper.

Child promo

http://k3tmdmrtwm54qphakmklov5l5lf\
arpmrb4kv3s7clon2gqlkfkgbad.onion
http://24e5bzjwovkfkyyrtklo3lq2ebcclxy\
lfvxtecahl2lzzlq4s3ubepid.onion
http://trzqon6fvufqyx7gf7i7h7om42d2s4kd7\
z6zjzkxt4t6jlydzc54gid.onion
http://l5x7jah5q5k77a6uvbzqc4ddz2ekwz5o\
6ohnu6kregu7cmjkx5nmbad.onion

Evil

http://242iz66xzgqiwkahiheoiiftlaafn\
77mzpjycfiwdylchvrjtjqwgqd.onion/
http://juqkhpatrwkq4jklbb3rm6b32\
n53yqcbnle73pibyfzt3wk7ovtmgid.onion/

Red room

http://3ul3tviswa3nazyla57uayfc3d\
3shjrifwd2k4a36ybvgeaqk6pntad.onion/

Brutal

http://bellaxulobxgvg3zyxravw2tjin\
cpdterdepxlilscwexpahphroqad.onion/

Human organs

http://ta7yzyjv76vpcbygk4cflngnki7uxq\
a4mfjleooo7c2t3zabvmddjid.onion/

Rape

http://rapehero6iatzwl5bhbp7cmzi2mz\
ulkfdoo6vuke25voxhmere6qzyd.onion/ http:
//th7zig3ygl2k6dapobvkjhg2\vxhax3i2z2wt\
zrvwg7fm73fxpfavtad.onion/?product_cat=
heavy-weapons

Weapons

http://g2jxqyniqhqotqpr6u37g2zsddio3zdcamm\
ralourz3iri2txuy6xid.onion/index.php/
tmpl/component/view/productdeta\ils/
virtuemart_product_id/8/print/1

Hacking

http://ugdbp6mw65tljzmymg2u7xv3uhtmb\
cpgiiimtbsfqcv47kicisen7id.onion/

3.2 Social Engineering

The internet has introduced a brand-new virtual realm where users of various backgrounds, intelligence levels, and intentions can interact with one another. It was initially designed to facilitate easier, faster, and more convenient communication, which has indeed been achieved. Through the internet, users can communicate freely and anonymously, concealing personal details such as gender, age, nationality, and background. This anonymity has provided many users with a sense of freedom and security. Unfortunately, certain individuals such as hackers, scammers, and spammers have exploited these features, targeting vulnerable users in chat rooms, emails, websites, and other platforms. These internet criminals employ deceptive tactics to gain the trust of their victims and trick them into sharing personal information. Subsequently, they engage in activities such as blackmail, hacking, and theft. For the purpose of this paper, interviews were conducted with victims of internet crimes, ensuring their anonymity. The interviewees were assured that their private information was not required for the paper, and they were solely asked about their experiences as victims. The paper also highlights some notable cases related to internet crimes [20].

Victim 1

In 2009, a woman from Britain suffered a severe chemical attack by an individual who stalked her on Facebook, resulting in the loss of her facial features.

There was a beautiful woman who worked as a model and TV presenter and had a significant online presence, particularly on Facebook, where she had numerous followers and admirers. Among her admirers was a secret stalker who followed her every move. Unaware of being stalked, the victim continued her activities on Facebook, sharing updates about her life. The stalker used this information to approach her, expressing his love. Feeling threatened by his behavior, the victim reluctantly agreed to date him out of fear for her safety. After a few encounters, realizing that she wanted to end the relationship, the victim made the decision to break it off. In a disturbing turn of events, the toxic admirer hired a hitman to harm the woman, even threatening to disfigure her face. The hired assailant successfully attacked the model, resulting

in severe facial injuries. She was immediately rushed to the hospital, fighting for her life, and underwent surgery to salvage what could be saved. Fortunately, the police were able to apprehend both the stalker and the hired hitman. Although the victim survived the ordeal and eventually recovered, the scars left behind would serve as a lifelong reminder of the horrific incident.

Victim 2

In 2020, a woman from Egypt tragically took her own life because of experiencing relentless online harassment. The victim's personal photos were unlawfully obtained from her hacked phone and manipulated to create fake nude images. The criminal responsible for the fabricated pictures then began blackmailing her, threatening to expose the images on social media unless she complied with his sexual demands. Despite refusing to give in to his desires, the criminal followed through with his threat, causing the fake pictures to circulate widely on various social media platforms. As a result, the victim's family, friends, neighbors, and others were exposed to these manipulated images. This situation quickly turned into a nightmare, with the victim's family even contemplating harm towards her due to believing the pictures were genuine. Furthermore, another criminal discovered the fabricated pictures and began blackmailing her as well, continuing the cycle of threats and humiliation. Overwhelmed and devastated, the victim tragically decided to end her own life. Finally, the family realized the gravity of the situation and reported it to the police. Following an investigation, it was revealed that all the pictures were fabricated, and the victim was completely innocent.

Victim 3

In 2018, a woman from Dubai fell victim to blackmail by scammer on Snapchat. A married woman engages in conversations on Snapchat with random users, and one of them turns out to be a scammer who gains her trust through fake stories.
Despite initially refusing, she eventually sends him a picture, convinced that he won't misuse it. As the scammer asks for more pictures, he threatens to release them if she doesn't comply with his demands. Fearful, she agrees to meet him in person, where he convinces her that the pictures have been deleted. However, she is then approached by another man who threatens to share a video of her unless she gets into his car. Reluctantly, she complies and is taken to his house, where she is drugged, raped, and recorded without her consent. When she regains consciousness, he continues to blackmail her with the video. Desperate, she confides in her family, who report the incident to the police. With the help of a forensic investigator, the authorities locate and arrest the criminal. During the investigation, it is revealed that the victim's friend was the leader of the group involved in the harassment and blackmail. The entire group is subsequently apprehended by the police.

Victim 4

In 2002, a thirteen-year-old girl from Pittsburgh was abducted with the intention of being trafficked on the dark web. A 13-year-old female uses online chat rooms to converse with strangers. The thief saw her, approached her, and struck up a conversation, winning her over as a friend. For 9 months, they revealed every element of their lives. She was invited to go supper out by the criminal. She went out to meet him without alerting her family. The victim was then taken hostage and taken somewhere else. As they approach his residence, the criminal ties her up and informs her that she will be videotaped for pleasure and placed on the dark web. For several days, she was sexually assaulted for internet pleasure on the dark web. She was raped, beaten, and ridiculed for the enjoyment of internet spectators. Fortunately, the FBI and computer forensic specialists were able to[21].

3.3 Hacking

Hacking involves unauthorized access to someone's device with the intention of extracting valuable information for personal gain. It can lead to data manipulation, deletion, or destruction, resulting in severe legal or financial consequences for the data owner. Hackers possess extensive knowledge of information theft and employ various techniques, including psychological manipulation and technological expertise, to obtain the desired information[22][23]. No individual, company, industry, or network is immune to hacking. While security measures can offer high levels of protection, achieving absolute security is unattainable, with vulnerabilities persisting. Hacking is an ever-evolving threat, necessitating continuous advancements in technological security. Numerous incidents have surfaced involving hackers breaching personal devices and illicitly obtaining sensitive information. Such information is often exploited by hackers for blackmail, harassment, financial gain, sexual exploitation, or involvement in illicit markets. Many victims have shared their harrowing experiences, ranging from paying ransom demands and enduring sexual assault to even losing their businesses[24].
The motives behind hacking vary, and hackers often have no personal connection or concern for their victims. Some of the typical motivations for hacking include:

3.3.1 Personal data

Hackers attempt to gain unauthorized remote access to devices with the intention of stealing login credentials for social media accounts, bank accounts, and personal information such as photos or files. Once they obtain this information, they employ various tactics, such as impersonation or distributing the victim's details online through practices like porn revenge or doxing. In the context of cyberbullying, doxing is a method used to exert pressure, humiliate, shame, and insult the victim by making their personal information go viral on the internet. This practice often involves the involvement of online mobs, whose aim is to intimidate and instill fear in the victims, threatening their privacy and security. Perpetrators leverage the threat of exposing personal and private data to coerce their victims into complying with their

demands. The act of doxing can have severe consequences on the mental health of victims, leading to anxiety, depression, and even self-harm. Those who have experienced doxing often feel as though they are constantly being watched by the entire world, even if it may not be the reality. The fear they endure can make them feel trapped in their own imagination[25].

3.3.2 Revenge

Individuals with hacking skills, whether they are hackers, acquaintances, neighbors, or colleagues, have the ability to infiltrate someone's computer system. Their goal is to retrieve private and sensitive information in order to publicly expose and shame the victim. By sharing this information widely, they aim to cause detrimental effects such as damaging the victim's business, relationships, client base, and more.

3.3.3 Blackmail

Cybercriminals engage in hacking activities to gain unauthorized access to a targeted device, seeking valuable and confidential information that can be exploited for extortion or blackmail purposes. They manipulate victims by leveraging their fear of potential harm, using the stolen information as leverage to coerce them into fulfilling specific demands, providing services, or making monetary payments. Victims often succumb to these threats due to the fear of personal safety and the potential public exposure of their information on the internet. Hacking and cybercrime incidents occur daily, resulting in numerous victims falling prey to these malicious activities[26].

3.4 Scamming

Scamming causes a significant threat to innocent individuals who engage in online activities. It involves the victim losing money without any tangible evidence of the transaction. Victims are often enticed by attractive scam offers that create a desire to participate in hopes of receiving the promised financial benefits. For instance, job offers on platforms like Instagram and Facebook may claim that individuals can earn money from the comfort of their homes by working as data entry executives. However, once victims apply, they discover that they need to purchase specific products in order to receive the commission promised along with their initial payment. Despite their desperation, victims feel compelled to proceed [21]. Once they make an initial payment, they find themselves trapped in a continuous cycle of paying without receiving anything substantial in return. They cling to the hope of recouping their losses, but ultimately realize that no payment will ever materialize, leading them to eventually give up. Figure 10 and Figure 11 and Figure 12. present scam job offers and victims.

No matter one's gender, age, race, or background, anyone can be susceptible to becoming a victim. The victims lacked awareness of cyber security and displayed naivety by placing trust in unknown individuals online [22]. They were unaware of the existence of cybercrime and the potential risks associated with it [23]. Furthermore, none of the users took precautionary measures to prevent or protect themselves

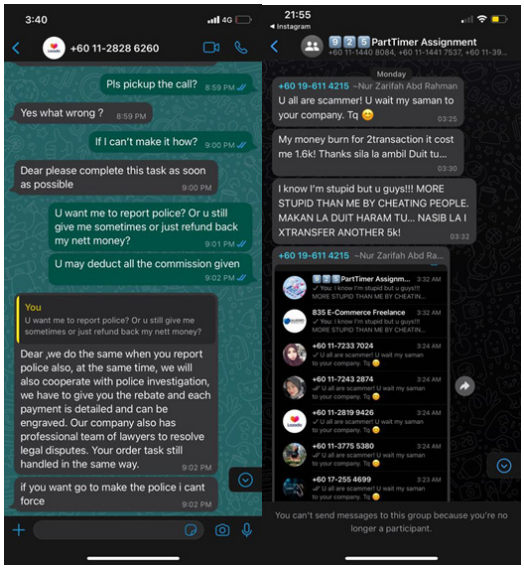

Figure 10. Scam victims conversation.

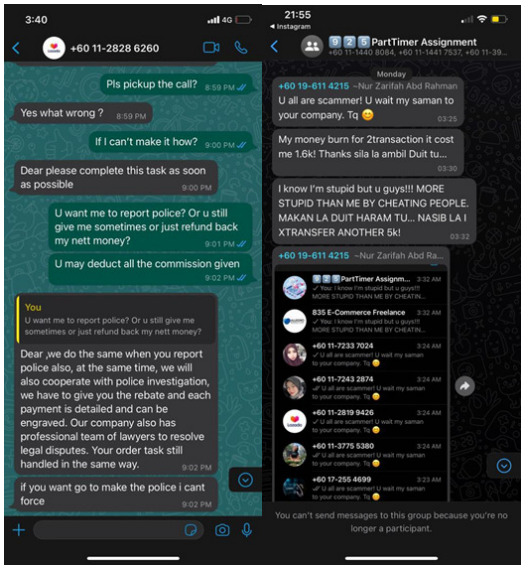

Figure 11. Scam victims.

from digital crimes. The absence of technological knowledge, computer skills, cyber self-defense, and protective measures resulted in these victims experiencing losses [24].

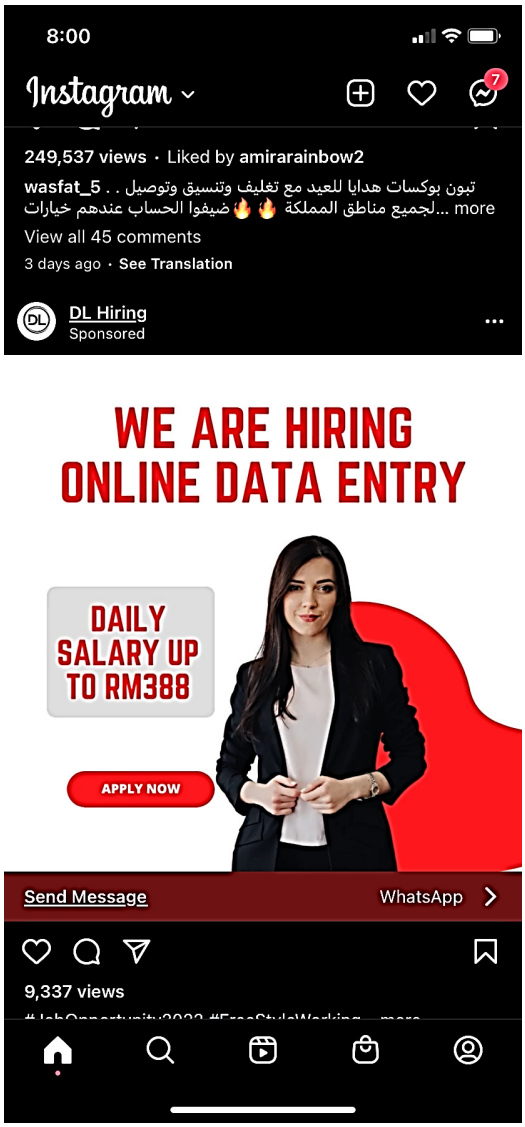

Figure 12. Fake job offer.

4. Cyber Protection

The Internet empire is populated with cyber criminals, posing a risk to any Internet user. It is virtually impossible for individuals, companies, or organizations to attain complete protection against these threats. No device can be safeguarded entirely. Nevertheless, adopting precautionary behaviors and taking appropriate actions can help to attain a certain level of protection [17].

To prioritize the safety of society, it is imperative for the Ministry of Education to revise the educational strategy by incorporating subjects on computing and cybersecurity, starting from an early age. It is crucial for students to comprehend that in this era of technology, they are exposed to digital risks, and they must be aware of the threats they may encounter while using technology and the internet. The cybersecurity curriculum should encompass practical and theoretical aspects that captivate students' attention and emphasize the dangers they may face. Proposed topics for the curriculum include real-life instances of digital crimes, digital child abuse, digital sexual harassment, digital human trafficking, the dark net and dark web, cyber-safety, preventing hacking and digital stalking, digital protection, phishing, scamming, malware, viruses, and methods to avoid and prevent them, steps to take if one is hacked or scammed, white (ethical) and black (unethical) hacking, cyberbullying, and spyware. This subject should be mandatory, ensuring that all students attend for their own safety. By educating students on cybersecurity from a young age, there is a higher likelihood of fostering a knowledgeable society proficient in computing and technology, with an intent focus on protection rather than attack and hacking.

Encryption is a reliable technique for concealing names and passwords. It offers a way to protect sensitive information using methods like Java programming and mathematical algorithms. By encrypting their names and passwords, users can enhance the security of their data. Table 1. provides several examples showcasing the transformation of names before and after encryption.

Table 1. Names before and after encryptio

Name	**Encryption**
Asma mahfoud	ÉÁijd džšď ÿţijÕ
Java hacker	\"vď Îď\"šď Íÿ ňÆ
Kesava	ÿÉď Îď
hi	şť
keep it real	ÿĆ ţË Æď ž
Nur	ÌÆ

The encrypted name can be linked to the email, ensuring that the sender's identity remains unreadable to others. This provides protection against stalkers attempting to track the user based on their name. Each time the encrypted name is copied or used for stalking purposes, it undergoes changes, making it even more difficult to track. Additionally, the encrypted name can serve as a secure password since it is highly improbable to guess. Figure 13 presents the name after encryption while it is being used.

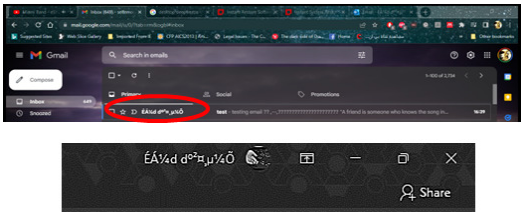

Figure 13. Name after being encrypted.

- While you are online surfing, enable (two-factor authentication) to make sure that no one else uses your

account from another device without your knowledge.

- Do not chat with strangers or share private information. Strangers you meet online are not real, you cannot trust them. If you must chat, then keep it simple, do not share files such as photos, and do not open links sent from them. Make sure the webcam is off and covered. Some users get kidnaped into the dark net business from online chatting with strangers.
- Check your friends list in your social media accounts and remove unknown users from your list.
- Disable location sharing in your device to prevent possible stalking.
- When you use a foreign device to log in to your email, make sure you remove your email from the device and remove the history and temporary files.
- Use complex passwords and do not use one password for all accounts. Change your passwords frequently to prevent hacking. Do not store your passwords digitally, keep them in a safe notebook where hackers cant reach them. Make sure that no one has access to this private notebook.
- Update your browser plug-in to keep your security on
- Make sure your firewall is on all the time.
- Make sure you do online shopping from trusted domains that have their own applications such as AMAZON, APPLE, LAZADA, ZALORA, SHEIN, UNIQLO, HM, etc. Do not shop from unknown websites and do not pay through these websites. You will be at a high risk of being robbed or hacked.
- Download software from trusted websites or purchase the original version.
- Keep a copy of your files in another external drive that no one has access to. Do not save critical or sensitive files in the cloud.
- Separate work email from personal to prevent possible hacking and data loss.
- While downloading free games or software that is supposed to be commercial do not use the key logger. Users are advised to buy the full version of the software. A key logger is an open gate for hackers to get into your device. Most websites that offer free applications are usually full of hackers.
- For extra safety, use the virtual machine if you are working on critical projects. The virtual machine is a desktop application that allows the user to run a different operating system within the main operating system. An example of a virtual machine application is a VMware workstation.
- Open-source operating systems are safer than commercial ones. Linux with all its versions is free to use, it performs like Windows. Hackers are always after popular sources and applications that are commercial. Users who care about security are advised to change to Linux.
- Secure all IoT gadgets from hacking.

5. Future work and conclusion

The availability of violent video games in digital markets has resulted in tragic incidents and severe consequences for many children. It is necessary to take preventive measures against these games. To promote societal improvement, an anti-social engineering game is being developed. This game aims to engage kids and teenagers in activities and competitions that encourage their participation in society. With multiple levels to complete, players must fulfill all requirements to earn rewards. The main objective of the game is to shift players' focus towards community building instead of violence and self-harm. The game will be developed using Python, Java, and Android programming languages, ensuring compatibility across all platforms. In future research, real-life cases of children and other users harmed by violent games will be presented alongside the introduction of this new proposed game.
Maintaining safety in the digital world is of utmost importance. The key factor for ensuring safety lies in adopting responsible and cautious behavior while using the internet. Engaging without care makes users vulnerable to various cybercrimes. Negligent users are at a higher risk of falling victim to digital crimes. Figure 14. provides an overview overview of the digital world in terms of vulnerabilities and safety when users are connected to the internet. This paper has explored the realm of cybercrime, the dark web, and the safety precautions that users should implement while engaging online.

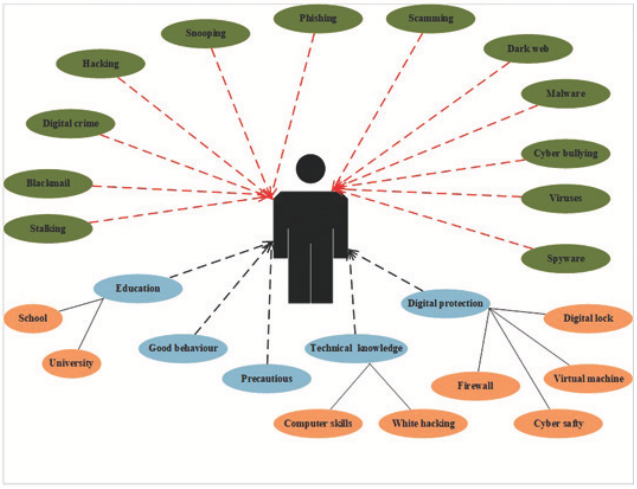

Figure 14. Users vulnerabilities vs safety precautions.

References

[1] S. Patil, V. Varadarajan, D. Walimbe, S. Gulechha, S. Shenoy, A. Raina, and K. Kotecha, "Improving the robustness of AI-based malware detection using adversarial machine learning," *Algorithms*, vol. 14, no. 10, p. 297, 2021.

[2] S. Brady and C. Heinl, "Cybercrime: Current threats and responses a review of the research literature," *Available: https://www.justice.ie/en/*, 2020.

[3] F. T. Commission *et al.*, "Ftc releases report on consumers online privacy," *Federal Trade Commission Press Release*, vol. 4, 1998.

[4] K. Olmstead, "Internet societys online trust alliance 2018 cyber incidents & breach trends report," *The Internet Society*, 2019.

[5] S. Raghavan, "Digital forensic research: current state of the art," *Csi Transactions on ICT*, vol. 1, pp. 91–114, 2013.

[6] "Internet society, 2018 cyber incident breach trends report," 2018.

[7] S. Cockcroft and P. Clutterbuck, "Attitudes towards information privacy," 2001.

[8] S. J. Milberg, S. J. Burke, H. J. Smith, and E. A. Kallman, "Values, personal information privacy, and regulatory approaches," *Communications of the ACM*, vol. 38, no. 12, pp. 65–74, 1995.

[9] U. UNCTAD, "Digital economy report 2019," 2019.

[10] R. Polanco, "The impact of digitalization on international investment law: Are investment treaties analogue or digital?" *German law journal*, vol. 24, no. 3, pp. 574–588, 2023.

[11] S. Affairs. British model chloe ayling kidnapped by black death group for auction in the dark web. [Online]. Available: https://securityaffairs.com/61786/cyber-crime/black-death-kidnapping-dark-web.html

[12] S. A. Nabavi, "Challenges of online marketing in kandahar city."

[13] J. R. Barnes and A. P. Davis, "National strategy for child exploitation prevention and interdiction," *National Strategy for Child Exploitation Prevention and Interdiction*, pp. 1–182, 2011.

[14] BBC News. German couple jailed for selling son to paedophiles on dark net. [Online]. Available: https://www.bbc.com/news/world-europe-45096183

[15] C. Jones and A. Seger. (2020, October) Guide for criminal justice statistics on cybercrime and electronic evidence. [Online]. Available: https://www.coe.int/cybercrime

[16] M. F. B. Rafiuddin, H. Minhas, and P. S. Dhubb, "A dark web story in-depth research and study conducted on the dark web based on forensic computing and security in malaysia," in *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*. IEEE, 2017, pp. 3049–3055.

[17] N. Anbalagan, R. A. A. Helmi, M. A. H. Ashour, and A. Jamal, "Trusted application using biometrics for android environment," in *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*. IEEE, 2020, pp. 7–12.

[18] M. Zimmerman. (2015, May) Darknet danger: Organs, murder, credit card info all for sale on internets underbelly. [Online]. Available: https://www.foxnews.com/tech/

[19] D. Rhumorbarbe, L. Staehli, J. Broséus, Q. Rossy, and P. Esseiva, "Buying drugs on a darknet market: A better deal? studying the online illicit drug market through the analysis of digital, physical and chemical data," *Forensic science international*, vol. 267, pp. 173–182, 2016.

[20] J. K. Aronson, R. E. Ferner, and G. C. Richards, "Deaths attributed to the use of medications purchased online," *BMJ Evidence-Based Medicine*, vol. 27, no. 1, pp. 60–64, 2022.

[21] K. Dashora, "Cyber crime in the society: Problems and preventions," *Journal of Alternative Perspectives in the social sciences*, vol. 3, no. 1, pp. 240–259, 2011.

[22] Z. Cekerevac, Z. Dvorak, L. Prigoda, and P. Cekerevac, "Hacking, protection and the consequences of hacking hacking, protection and the consequences of hacking," *Communications-Scientific letters of the University of Zilina*, vol. 20, no. 2, pp. 83–87, 2018.

[23] R. A. A. Helmi, C. S. Ren, A. Jamal, and M. I. Abdullah, "Email anti-phishing detection application," in *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*. IEEE, 2019, pp. 264–267.

[24] M. Bhardwaj and G. Singh, "Types of hacking attack and their countermeasure," *Int. J. Educ. Plann. Admin*, vol. 1, no. 1, pp. 43–53, 2011.