Scholastic Research Publications, SRP Group®
International Journal of Humanities Science Innovations and Management Studies
Volume 2 Issue 1, Pg. No. 24-33, January-February, 2025
IJHSIMS-V2I1P105, Doi: https://doi.org/10.64137/30508509/IJHSIMS-V2I1P105

Review Article

Cyber Crime and its Effects on Society in Our Digital Era

[1]Dr. Sreeja Vinayadas, [2]Sayed Ali Moosa Alaswami, [3]Layla Ashraf Mohamed, [4]Ruaa Mohamed Kayani, [5]Al Hanoof Abdul Karim

[1]*Assistant Professor, Department of English Literature, University of Bharain, Bharain.*
[2,3,4,5] *Student, Department of English Literature, University of Bharain, Bharain.*

Received Date: 16th December 2024 Revised Date: 11th January 2025 Accepted Date: 26th January 2025 Published Date: 09th February 2025

Abstract - Cybercrimes are a type of computer and internet crime that targets cyber security systems that protect information and contacts to harm piracy, violation of property rights, extortion, or fraud. These crimes cause much damage to institutions and individuals. Thus, this report will discuss how deep cyberattacks can have impacts on various levels. Also, how can this type of crime be prevented and stopped by awareness and protection methods applied by individuals and institutions, and steps were taken by the government to prohibit such crime.

Keywords - Awareness, Crime, Exploitation of Technical Rights.

1. Introduction to Cybercrime

The first recorded electronic crime occurred in 1820! This is hardly surprising considering that the abacus—thought to be the earliest computer—has been around in China, Japan, and India since 3500 BC. [1]. The growing dependence on technology in modern life has given rise to cybercrime, a wicked act. In a time when computers control anything from nuclear power plants to microwave ovens and refrigerators, cybercrime has grown to hazardous proportions. Cybercrime can be described as a criminal act involving using a computer system to commit illegal activities or as a crime involving computing against a digital target, which results in several consequences to people, organizations, and sometimes countries. In our time, with advanced developments, electronic crimes must stop and solve this problem; the levels of solution move according to scientists and government fields because our time depends on technology.

2. Cybercrime

2.1 Definition of Cybercrime

Illegal activity employing a computer, a network of computers, or a networked device is known as cybercrime. Profit-driven hackers and cybercriminals commit criminality to varying degrees. People or organizations can commit cybercrime. Certain cybercriminals possess a great degree of technical proficiency, employ sophisticated tactics, and are well-organized. Some are not experienced hackers. Seldom is cybercrime used to damage computers for purposes other than financial gain. These could be of a private or political nature.

2.2 Types of Cybercrime

As claimed by Adv. Prashant Mali [2] cybercrimes can be classified into four major categories as the following: first, cybercrime against individuals; second, cybercrime against property; third, cybercrime against organizations; and last, cybercrime against society. In addition, each of these categories has many examples of cybercrime, as presented below:

2.2.1 Cybercrime against Individuals

(i) Email Spoofing: An email that has undergone spoofing is when the email header is changed to make it look as though it was sent from one source when, in fact, it came from another.

(ii) Spamming: Delivering several copies of unsolicited mail or bulk emails, like chain letters, is known as spamming.

(iii) Cyber Defamation: This happens when someone defames someone using a computer or the internet. For instance, somebody may send malicious emails or post false information regarding someone on a website.

(iv) Harassment & Cyberstalking: Cyberstalking is the practice of monitoring someone's online behavior. Numerous protocols, including email, chat rooms, and user net groups, can assist with it.

2.2.2. Cybercrime against Property

(i) Credit Card Fraud: This type of fraud involves using a credit card, as the name implies. Usually, this occurs when a card gets stolen, or somebody finds out the card number.

(ii) Intellectual Property Crimes: These include

-Software piracy: Dissemination of software copies and unauthorized program copying.

-Copyright Infringement: Use content protected by copyright without authorization.

-Trademark Violations: Utilizing copyrights and related rights without the rightful owner's consent.

-Theft of Computer Source Code: Stealing, damaging, or abusing a computer's source code.

(iii) Internet Time Theft: This occurs when someone is not allowed to use internet time that is really paid for by someone else.

2.2.3. Cybercrime against Organizations

(i) Unauthorized Accessing of Computer: using the network or computer without the owner's consent. It comes in two varieties:

a) Data alteration or deletion: Unauthorized data alteration.

b) Computer voyeur: The offender reads or copies proprietary or confidential data without altering or erasing it.

(ii) Computer Contamination / Virus Attack: A computer virus is a computer program capable of infiltrating other programs by altering them to contain a copy of itself, which may have evolved over time. Files that damage or contaminate the computer's boot section are considered viruses. Unlike viruses, worms can attach themself to a host without one.

(iii) Email Bombing: Delivering a lot of emails to a person, business, or mail server, which finally causes it to crash.

(iv) Trojan Horse: This is an unapproved program that runs from within what appears to be an approved program, hiding its true purpose.

2.2.4. Cybercrime against Society

(i) Forgery: Computers, along with good scanners and printers, can be used to fabricate currency notes, revenue stamps, mark sheets, and other documents.

(ii) Cyber Terrorism: Using technology to commit acts of terrorism and frighten or force others.

(iii) Web Jacking: Hackers can take over and obtain access to another website, even if they alter its content to further their political goals or make money.

3. The Impacts of Cybercrime

Cybercrime has a tremendous influence on society, both online and offline. These impacts affect people of all ages, producing psychological problems and institutions from all disciplines, causing economic disruption and affecting important societal components by jeopardizing national security.

3.1. Impact on the Level of the Individual

A cybercrime attacker's consequences might be numerous at once, especially if the victim is a person. Identity theft is said to have become the most widespread type of cybercrime, with victims facing grave consequences. Phishing, for example, occurs when a victim receives a fraudulent email claiming to be from a financial institution and asking for personal information, prompting the victim to give personal information. It gives the criminal access to all financial accounts and lets him drain all of the funds for his purposes, leaving the victim bereft and total loss. Another kind of identity theft is when a cybercriminal attempts to hack a victim's device and obtains all information (such as images, account passwords, and other personal information), then uses it against the victims by extortion and threatening them. These cases are brought forward with the goal of vengeance, resulting in the victim suffering from mental illnesses and depression, which may lead to suicide.

Moreover, the majority of cyber attackers prioritize children and teenagers as the individual category. Sumanjit Das and Tapaswini Nayak [3:148] argued that cyberbullying the worst fear in teenagers' eyes is. A person experiences dread from cyberbullying when they are subjected to threats, disparaging remarks, or offensive images or language from another individual. Causes teenagers severe mental anguish, depression, and humiliation, and if a person is bullied online, he or she may be depressed up to the level of self-harm. In addition, according to Majid Yar and Kevin F. Steinmetz [4:175], child phonography claims to have high and direct harm to children, often entailed in producing such material. Cyber pornography means the use of the internet to spread child and adult pornography, and this has dangerous effects on society that can include addiction, isolation, increased aggression, negative feelings about themselves, and neglecting other areas of their lives (Maltz & Maltz, 2006; Manning, 2006).

3.2. Impact on the Level of the Institution

Cybercrime may pose a danger to organizations, governments, and even international relations, among other things. It jeopardizes a state's and government's sovereignty, as well as national security and critical infrastructure. Cybercrime negatively influences earnings, but it may also harm a company's brand and capacity to thrive eventually. A cyberattack causes a company's operations to be disrupted, costly, and time-consuming. Businesses should additionally invest in repairing and upgrading their systems, retraining their workers, and controlling reputational impact. A large-scale hack can seriously harm a company's reputation, despite the fact that many firms may experience one at some point throughout their operations. Consequently, the business loses business and clientele, and it has to put in a lot of effort to repair its reputation.

In addition, governments at all levels are growing increasingly reliant on these technologies to provide basic services. This dependency has the disadvantage of increasing the danger of cyber interactions and data breaches. Personally Identifiable Information (PII) of any resident whose name, date of birth, and social security number are stored on a local government system might be compromised as a result of these breaches. Data breaches caused by phishing, hacking, and insider threats are on the rise, resulting in significant financial losses as a result of the expenses of repairing the breach and addressing the potential harm to people whose PII has been exposed [5].

3.3. Damage to Society

Hence, cybercrime tactics span from an individual device to a nation's database; the reasons for such assaults have several negative effects on society and may wreak a great deal of devastation in everyday life.

Researchers from the computer science department at the University of Oxford set out to characterize and record the various ways that today's cyber incidents are causing harm. They also assessed the potential for these effects, or harms, to propagate over time. The hope is that this will help people comprehend the various issues cyberattacks can bring about for the public, the government, and academic institutions [6]. The damage generated by cybercrime attempters has been identified at five key levels, which are physical/digital, economic,

psychological, reputational, and cultural. Each category has unique results that demonstrate the seriousness of cyber-attacks. For example, in the physical/digital category, there is the risk of loss of life or infrastructure damage. Still, in the economical category, there is the prospect of a drop in stock price, regulatory fines, or lower earnings. According to the psychological theme, individuals may become unhappy, humiliated, ashamed, or bewildered, whereas reputational repercussions may include the loss of key personnel, ruined consumer relationships, and severe media scrutiny. Ultimately, there is a risk of social and/or societal disruption to day-to-day life, including effects on vital services, a negative perception of technology, or a decline in internal morale in firms impacted by a high-profile incident.

4. How to Avoid Exposure to Cybercrime

4.1. Methods of Protection from Cybercrime

4.1.1. Using the Firewall

A firewall is responsible for Defending Against Inbound Threats. While firewalls can be installed in various locations within a company's network, the network perimeter is the most typical. Installing a firewall at the network perimeter establishes and maintains the boundary between the trustworthy public internet and the protected internal network. A network firewall placed at the network perimeter may also benefit from the fact that all network traffic that enters and leaves the corporate network passes through a single point of communication between it and the open internet. By installing a firewall in this position, it will be able to get total visibility into data flows beyond the network's perimeter. Threat prevention features in a next-generation firewall can detect and block attempted assaults before they enter the corporate network. This significantly lowers the risk of cyberattacks that the organization and its employees confront and the potential harm that these attacks could do [7].

4.1.2. Encryption

Encryption jumbles up communication or file information to make it secure. A message cannot be decrypted without the correct key and cannot be encrypted without it. With the sender and recipient owning the key to decode data, it is the most efficient way to hide communication utilizing encoded data. The notion is similar to youngsters inventing secret code words and other discrete ways of communicating in which only they can understand the message. Encryption is similar to conveying secret communications between parties; if someone attempts to pry without the appropriate keys, they will be unable to comprehend the message. When it comes to your data, the primary goal of encrypting the information saved on your computer and devices is to safeguard your privacy, data, and intellectual property. This is also known as endpoint encryption, and it adds an extra layer of security to private data saved on your devices, as well as data stored on portable media and particular files and folders [8].

4.1.3. Digital Signature

According to Eliza Paul [9], the digital signature is a mathematical system for proving the genuineness of digital messages or documents. It is a digital fingerprint that is unique to a person and may be used to identify signers and protect data in digital documents. It is a type of electronic signature that complies with legal requirements by confirming the legitimacy and legitimacy of an electronic record and the signer's identity. A digital document's source, date, identity, and status can all be verified via digital signatures. A signature attests to the fact that the data came from the signer and was not changed while in transit. Authenticity and security are top priorities when it comes to signatures. The chance of a document being duplicated or altered is reduced with digital signatures. Signatures are checked, authenticated, and legitimated using digital signatures.

4.1.4. Using Intrusion Detection Systems

Tony states [10] that adversaries are constantly developing new attack techniques and exploits to circumvent your defenses. Many attacks involve extra software or social engineering to obtain login information that allows them access to your network and data. Network security requires a network intrusion detection

system to detect and react to malicious traffic. An intrusion detection system's primary advantage is that it notifies IT specialists in the event that an attack or network incursion is suspected. A network intrusion detection system monitors data moving between machines and incoming and outgoing network traffic. Intrusion detection systems for networks analyze network traffic and give out alerts when unusual activity or recognized threats are detected. This allows IT staff to investigate the matter further and take the required precautions to stop or avoid an attack.

5. Steps Taken by the Government to Prevent Cybercrime

According to Amer [11], The Kingdom of Bahrain, led by His Majesty King Hamad Bin Isa Al Khalifa and guided by His Excellency Lieutenant General Shaikh Rashid bin Abdullah Al Khalifa, Minister of Interior, established a Cyber Crime Directorate in accordance with Royal Decree number 109 of 2011. The directorate went about its business, attempting to train its employees so that they would be competent and well-informed on the most up-to-date means of countering cybercrime. In this context, the directorate sponsored conferences and seminars for various sectors to raise public awareness about coping with this type of crime. His Majesty issued Decree Number 60 of 2014 concerning information technology crimes law in the context of his belief in the need to establish overall security and address all attempts to disrupt it, as well as a qualitative shift in the area of combating information technology crimes. The decree includes a number of legislative provisions that penalize cybercriminals and regulate the jobs entrusted to legal agencies. Because of the rise in electronic dangers worldwide, as stated by the Cyber Crime Directorate in past years, it has also become important to implement a national cyber security policy. Because all modern communications rely on information technology and the internet, such a plan has become one of Bahrain's primary issues. The strategy's ultimate goal is to provide a secure cyberspace environment while preserving the country and its information technology infrastructure's accomplishments.

6. Methodology

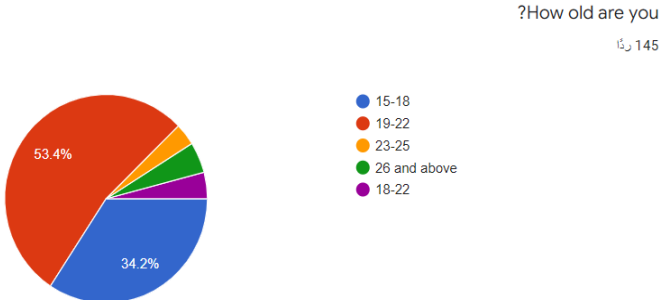
For research, a quantitative approach is applied to conduct this research. A survey was conducted through social networking sites to find out the purpose and aim of the research. The survey aims to determine how much people know and understand about cybercrime and whether or not they know how to protect themselves from cybercrime. Also, to find out if they have encountered cybercrime.

The questionnaire consisted of ten questions in total, one of which obtained information on the age of the respondent and nine of them to obtain the data required for the report. The survey link has been published using WhatsApp for different types of people, and we have collected more than 70 answers.

7. Findings and Discussion

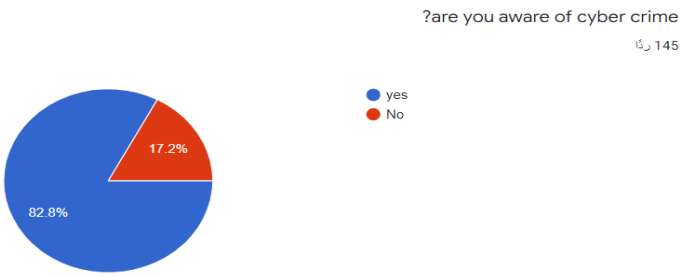
We wanted to know the extent of people's awareness of cybercrime, its types, and ways to protect against it, so we conducted a questionnaire containing 10 questions and published it to our colleagues in the College of Information Technology and on social media. We collected the results and converted them into percentages.

1.



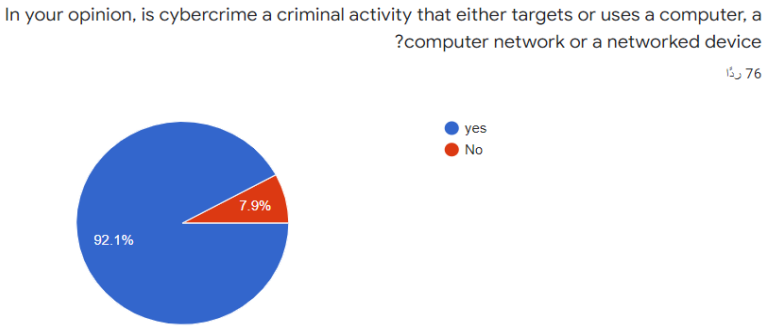
The first question was about age, and we got 145 answers, from which we concluded that the majority of the respondents were from the age group 19-22. This means that the respondents are more aware and mature.

2.



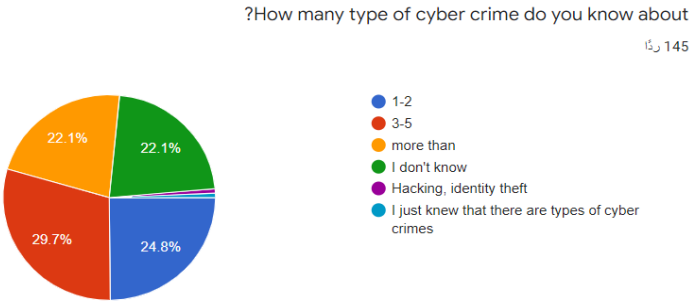
The objective of the second question is to measure the extent to which users are interested in the problem of cybercrime, and we obtained 145 answers, from which we concluded that most users are interested in the problem of cybercrime, as the yes vote was 82%.

3.



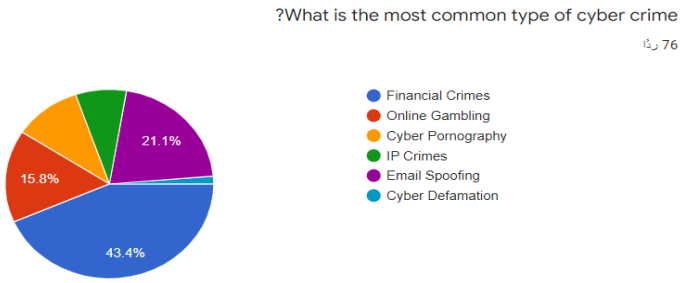
In the third question, we wanted to know if users had actual knowledge of the meaning of cybercrime and the difference between it and viruses. We got 76 people answering, and most of them agreed with the definition we know about cybercrime, with 92 percent.

4.



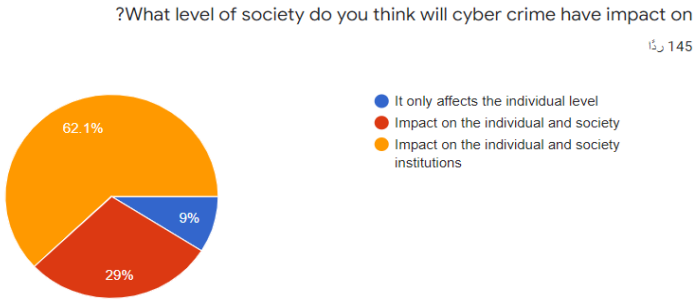
In the fourth question, we wanted to know the number of types of cybercrime that users know. We got 145 answers from which we concluded that users know about 3-5 types of cybercrime, and only a few of them know that there are types of cybercrime where the selection rate is 29%. They represent the highest percentage of choices, but the lowest choice was that they didn't know what kind of cybercrime.

5.



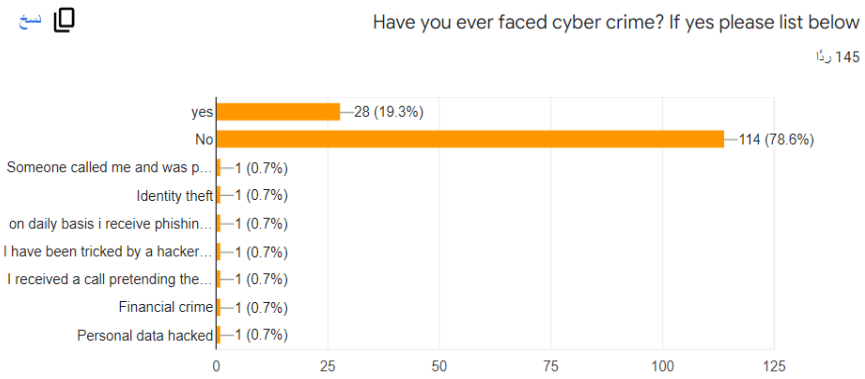
In the fifth question, we wanted to measure the most famous and common type among people and got 76 answers. We concluded that the most prevalent type of cybercrime among people is financial crimes, where the vote on the option of financial crimes was equal. It equals 43.4%, which represents the highest percentage.

6.



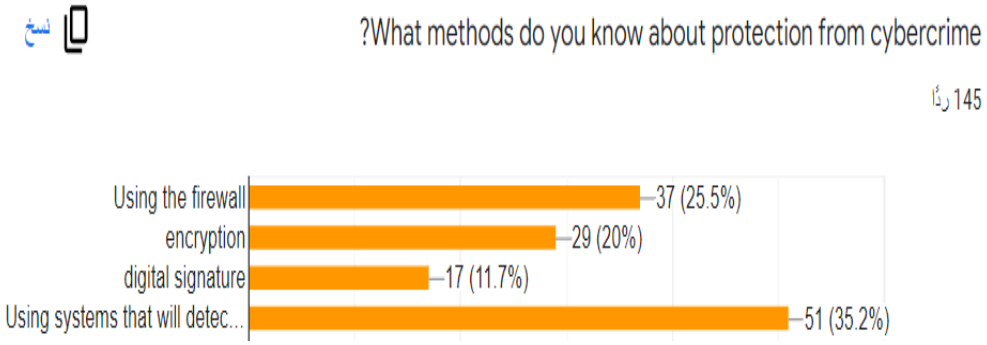
In this sixth question, we wanted to measure what people think about the impact of cybercrime if it only affects the individual level or on the individual, society, and institutions; we got the answer from 145 people, from which we concluded that most opinions confirm that cybercrime affects the individual, society, and institutions as the vote for this option was 62.1%, which was the highest percentage.

7.



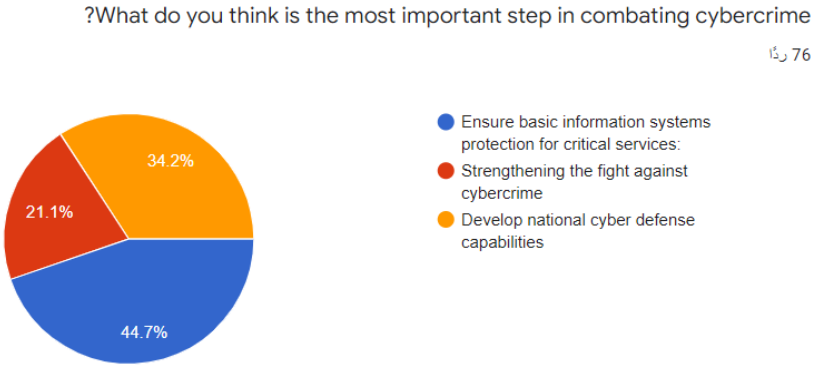
In the seventh question, we wanted to measure whether users were directly exposed to cybercrime or not. We got the answer from 145 people and concluded from it that most of the users were not directly exposed to cybercrime, where the vote for no was more than yes. Those who were exposed to cybercrime were They mentioned different types of crimes they were subjected to as shown in the previous figure.

8.



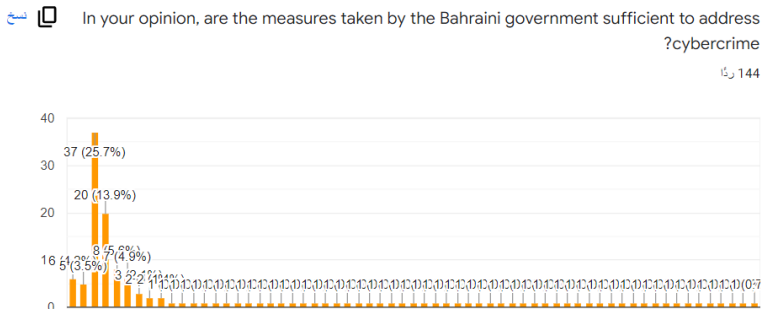
In the eighth question, we wanted to measure the ways that people think are the best ways to protect against cybercrime. We collected 145 answers to this question, and we will conclude that the majority of users believe that using systems that will detect all intrusions is the best way to protect against cybercrime, as voting on this option was equivalent to 35.2, which represents the highest percentage.

9.



In the ninth question, we wanted to know what is the step that people think is the most important step in the fight against cybercrime. We got an answer of 75, and we will conclude that the step of ensuring the protection of essential information systems for vital services is the most important step in the fight against cybercrime, as it got 44.7%, which is the highest percentage.

10.



In the last question, we wanted to measure people's satisfaction with the measures taken by the Kingdom of Bahrain in combating cybercrime, and we got 144 answers. We concluded that users believe the measures introduced by the Kingdom of Bahrain to combat cybercrime must be developed, but they are not low-level measures. Users were satisfied with 4/5.

8. Conclusion

The impact of cybercrime on important societal components has been fully documented in this paper. The paper defined cybercrime and the many varieties of cybercrime by categorizing it into four key categories: crime against individuals, property, organizations, and society. It also explains the various repercussions that cyberattacks may have on individuals, institutions, and society. It also explains how to prevent being a victim of cybercrime and how to protect yourself from it. Also, the government's efforts to combat cybercrime are discussed.

References

[1] Introduction to Cybercrime, 2011. [Online]: Available: https://www.studymode.com/essays/Introduction-To-Cyber-Crime-550163.html

[2] Adv. Prashant Mali, What are Types of Cybercrime? 2009. [Online]: Available: https://www.lawyersclubindia.com/articles/classification-of-cybercrimes--1484.asp

[3] Sumanjit Das, and Tapaswini Nayak, "Impact of Cyber Crime: Issues and Challenges" *International Journal of Engineering Sciences and Emerging Technologies*, vol. 6, no. 2, pp. 142-453, 2013. |Google Scholar| Publisher Site|

[4] Majid Yar, and Kevin F. Steinmetz, *Cybercrime and Society, London: SAGE Publications, 2019.* | Publisher Site|

[5] Gerald Cliff, Growing Impact of Cybercrime in Local Government, 2017. [Online]: Available: https://icma.org/articles/pm-magazine/growing-impact-cybercrime-local-government

[6] Researchers Identify Negative Impacts of Cyber Attacks, 2018. [Online]: Available: https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks

[7] Why a Firewall is the First Line of Defense Against Cyber Attacks? [Online]: Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/why-a-firewall-is-the-first-line-of-defense-against-cyber-attacks/

[8] Encryption 101: What It Is, How It Works, and Why We Need It, 2015. [Online]: Available: https://www.trendmicro.com/vinfo/us/security/news/online-privacy/encryption-101-what-it-is-how-it-works

[9] Eliza Paul, What is Digital Signature: How it Works, Benefits, Objectives, Concepts, 2017. [Online]: Available: https://www.emptrust.com/blog/benefits-of-using-digital-signatures/

[10] Tony Bradley, What is an IDS and Why Do You Need It? 2018. [Online]: Available: https://www.alertlogic.com/blog/what-is-a-network-ids-and-why-do-you-need-it/

[11] Amer S. Mustafa, Combating Cyber Crime in The Kingdom of Bahrain, 2015. [Online]: Available: https://unipath-magazine.com/combating-cyber-crime-in-the-kingdom-of-bahrain/

Appendix

Questions that were used in the survey

1. How old are you?
   - 15-18
   - 19-22
   - 23-25
   - 26 and above

2. Are you aware of cybercrime?
   - Yes
   - No

3. In your opinion, is cybercrime a criminal activity that either targets or uses a computer, a computer network, or a networked device?
   - Yes
   - No

4. How many types of cybercrime do you know about?
- 1-2
- 3-5
- more than
- I don't know

5. What is the most common type of cybercrime?
- Financial Crimes
- Online Gambling
- Cyber Pornography
- IP Crimes
- Email Spoofing
- Cyber Defamation

6. What level of society do you think will cybercrime have an impact on?
- It only affects the individual level
- Impact on the individual and society
- Impact on the individual and societal institutions

7. Have you ever faced cybercrime? If yes, please list it below.
- Yes
- No

Free writing space

8. What methods do you know about protection from cybercrime? (You can choose more than one option)
- Using the firewall
- Encryption
- digital signature
- Using systems that will detect all intrusions, with the importance of focusing on developing solutions to security vulnerabilities.

9. What do you think is the most important step in combating cybercrime?
- Ensure basic information systems protection for critical services:
- Strengthening the fight against cybercrime
- Develop national cyber defense capabilities

10. In your opinion, are the measures taken by the Bahraini government sufficient to address cybercrime?
- 1
- 2
- 3
- 4
- 5

Survey link: https://cutt.us/11QOE