iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52481

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Analysis on Cyber Crimes and Preventive Measures

Asha Thomas
St. Albert's College (Autonomous)

Abstract: ***This paper is generally to analyse various cybercrimes and corresponding preventive measures. Cybercrimes refers to criminal activities carried out by means of computer systems or the internet. As Cybercrimes are considered as a great threat in today's world, to the security of nation, to someone's personal data and information, individual security, so there is the need of some basic awareness and security measures, by which people can safeguard themselves from such crime. Cybercrimes are considered as a major risk because they can have devastating effects like financial losses, breaches of sensitive data, failure of systems, and, it can affect an organization's reputation.***

In this paper, we will discuss more about cybercrimes, and how do they happen. Also, who are Cybercriminals and, the different types of cybercrimes and preventive measures.

I. INTRODUCTION

With the growth of the internet and proliferation of applications, products & services on it, citizens are being empowered and their lives transformed. However, with the growth of the internet, cybercrimes are also on the increase. Cybercrime can be defined as the illegal usage of any communication device to commit or facilitate in committing any illegal act. These crimes are committed using computers and computer networks. They can be targeting individuals, business groups, or even governments. Though law enforcement agencies are trying to tackle this problem, it is growing regularly and many people have become victims of identity theft, hacking, and malicious software. One of the best ways to stop these criminals and protect sensitive information is by making use of inscrutable security that uses a unified system of software and hardware to authenticate any information that is accessed over the Internet.

II. LITERATURE REVIEW

In this, we will see the two classifications of cybercrimes as below:

A. Targeting Computers

This type of cybercrimes includes every possible way that can lead to harm to computer devices for example malware or denial of service attacks.

B. Using Computers

This type includes the usage of computers to do all the computer crimes.
Cybercrimes in general can be classified into four categories:

1) *Individual Cyber Crimes:* This type is targeting individuals. It includes phishing, spoofing, spam, cyberstalking etc.
2) *Organisation Cyber Crimes:* The main target here is organizations. Usually, this type of crime is done by teams of criminals including malware attacks and denial of service attacks.
3) *Property Cybercrimes:* This type targets property like credit cards or even intellectual property rights.
4) *Society Cybercrimes:* This is the most dangerous form of cybercrime as it includes cyber-terrorism.

Next is the common types of cybercrimes, we come across with:

a) Phishing and Scam

Phishing is a type of social engineering attack that targets the user and tricks them by sending fake messages and emails to get sensitive information about the user or trying to download malicious software and exploit it on the target system.

©IJRASET: All Rights are Reserved

b) Identity Theft

Identity theft occurs when a cybercriminal uses another person's personal data like credit card numbers or personal pictures without their permission to commit a fraud or a crime.

c) Ransomware Attack

Ransomware attacks are a very common type of cybercrime. It is a type of malware that has the capability to prevent users from accessing all their personal data on the system by encrypting them and then asking for a ransom in order to give access to the encrypted data.

d) Hacking/Misusing Computer Networks

This term refers to the crime of unauthorized access to private computers or networks and misuse of it either by shutting it down or tampering with the data stored or other illegal approaches.

e) Internet Fraud

Internet fraud is a type of cybercrimes that makes use of the internet and it can be considered a general term that groups all the crimes that happen over the internet like spam, banking frauds, theft of service, etc.

f) Cyber Bullying

It is also known as online or internet bullying. It includes sending or sharing harmful and humiliating content about someone else which causes embarrassment and can be a reason for the occurrence of psychological problems. It became very common lately, especially among teenagers.

g) Cyber Stalking

Cyberstalking can be defined as unwanted persistent content from someone targeting other individuals online with the aim of controlling and intimidating like unwanted continued calls and messages.

h) Software Piracy

Software piracy is the illegal use or copy of paid software with violation of copyrights or license restrictions. Not only software can be pirated but also music, movies, or pictures.

i) Social Media Frauds

The use of social media fake accounts to perform any kind of harmful activities like impersonating other users or sending intimidating or threatening messages. And one of the easiest and most common social media frauds is Email spam.

j) Online Drug Trafficking

With the big rise of cryptocurrency technology, it became easy to transfer money in a secured private way and complete drug deals without drawing the attention of law enforcement. This led to a rise in drug marketing on the internet. Illegal drugs such as cocaine, heroin, or marijuana are commonly sold and traded online, especially on what is known as the "Dark Web".

k) Electronic Money Laundering

Also known as transaction laundering. It is based on unknown companies or online business that makes approvable payment methods and credit card transactions but with incomplete or inconsistent payment information for buying unknown products.

l) Cyber Extortion

Cyber extortion is the demand for money by cybercriminals to give back some important data they've stolen or stop doing malicious activities such as denial of service attacks.

m) Intellectual-property Infringements

It is the violation or breach of any protected intellectual-property rights such as copyrights and industrial design.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

n) Online Recruitment Fraud

One of the less common cybercrimes that are also growing to become more popular is the fake job opportunities released by fake companies for the purpose of obtaining a financial benefit from applicants or even making use of their personal data.

Who is a cybercriminal?

A cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities known as cybercrimes. They can be individuals or teams. Cybercriminals are widely available in what is called the "Dark Web" where they mostly provide their illegal services or products.

Not every hacker is a cybercriminal because hacking itself is not considered a crime as it can be used to reveal vulnerabilities to report and batch them which is called a "hacker". However, hacking is considered a cybercrime when it has a malicious purpose of conducting any harmful activities and we call this one "black hat hacker" or a cyber-criminal. It is not necessary for cybercriminals to have any hacking skills as not all cybercrimes include hacking.

Cybercriminals can be individuals who are trading in illegal online content or scammers or even drug dealers.

Some specific types of cybercrimes include the following:

- Cyberextortion: A crime involving an attack or threat of an attack coupled with a demand for money to stop the attack. One form of cyberextortion is the ransomware attack. Here, the attacker gains access to an organization's systems and encrypts its documents and files, making the data inaccessible until a ransom is paid. Usually, this is in some form of cryptocurrency, such as bitcoin.
- Cyber theft: An attack that occurs when an individual accesses a computer to glean a user's personal information, which they then use to steal that person's identity or access their valuable accounts, such as banking and credit cards. Cybercriminals buy and sell identity information on darknet markets, offering financial accounts, as well as other types of accounts, like video streaming services, webmail, video and audio streaming, online auctions and more. Personal health information is another frequent target for identity thieves.
- Credit card fraud: An attack that occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on darknet markets, where hacking groups that have stolen mass quantities of credit cards profit by selling to lower-level cybercriminals who profit through credit card fraud against individual accounts.
- Cyberespionage: A crime involving a cybercriminal who hacks into systems or networks to gain access to confidential information held by a government or other organization. Attacks may be motivated by profit or by ideology. Cyberespionage activities can include every type of cyberattack to gather, modify, or destroy data, as well as using network-connected devices, like webcams or closed-circuit TV (CCTV) cameras, to spy on a targeted individual or groups and monitoring communications, including emails, text messages and instant messages.
- Software piracy: An attack that involves the unlawful copying, distribution, and use of software programs with the intention of commercial or personal use. Trademark violations, copyright infringements and patent violations are often associated with this type of cybercrime.
- Exit scam: The dark web, not surprisingly, has given rise to the digital version of an old crime known as the *exit scam*. In today's form, dark web administrators divert virtual currency held in marketplace escrow accounts to their own accounts essentially, criminals stealing from other criminals.

Common examples of cybercrime

➢ *REvil and Kaseya Ransomware*

REvil is a Russian or Russian-speaking hacking group and it is known as a ransomware-as-a-service operation. The Kaseya incident took place in July - 2021.

The incident happened when one of the Kaseya's company's products was deploying the famous SODINOKIBI REvil ransomware to endpoints of Kaseya's customer network that attack surface was over 1000 Kaseya's customers worldwide.

A few hours later REvil took credit for the attack by posting on their Happy Blog website on the dark web and demanded a $70 million ransom to release a public decryptor that they claim can decrypt all the damaged devices.

The attack was so impactful that the United States government offered $10 million bounties to anyone that can give any information for arresting REvil members.

Yaroslav Vasinskyi, a 22 years Ukrainian, was charged with conducting the attack and unleashing the ransomware against Kaseya and other companies.

- *Stuxnet*

The Stuxnet incident is a famous incident that happened in 2010. Stuxnet is the name of a computer worm (type of malware) that targets SCADA (supervisory control and data acquisition) systems.

Stuxnet malware left devastating damage to Iran's nuclear power program. It was spreading through USB drives and affected mainly Microsoft Windows operating systems.

The malware functionality was to search for machines that are working as PLCs (programmable logic controllers) and if it was found the malware updates its code over the internet through the attackers.

- *Marriott Hotels*

In November 2018, Marriott hotels group suffered from a massive data breach that affected more than 500 million customers.

The compromise happened for the guest reservation database by an unknown party. The information that was leaked contained payment information, mailing addresses, passport numbers, and phone numbers for customers.

Marriott Group has immediately conducted incident investigations with a group of security experts plus setting up a website and a call centre.

They also sent emails to the affected customers and gave them free access to monitoring tools that monitor the internet and give an alert if any evidence of sharing personal information is found.

- *Rock You Data Breach*

Rock You is a company that works in the game field and was founded in 2005 by Lance Tokuda and Jia Shen. The company was working well until December 2009 when what is called "the biggest data breach of all time" happened.

The data breach exposed and leaked more than 32 million user account information from Rock You database.

The company was storing passwords in an unencrypted plain text format which made it easier for the hacker to have access to all passwords stored. The hacker used a very old and popular SQL vulnerability to leak all data from the database.

After this major breach, the total set of passwords that were leaked became a very helpful resource in penetration testing as hackers use this wordlist of passwords to test the security and password strength of accounts and products.

Effects of Cybercrimes on businesses

According to a 2018 report published by McAfee, the economic impact of cybercrimes is estimated to cost the global economy nearly $600 billion annually. Financial loss is one of the obvious effects of cybercrimes, and it can be quite significant. But cybercrimes also have several other disastrous consequences for businesses such as:

- Investor perception can become a huge problem after a security breach causing a drop in the value of businesses.
- Businesses may also face increased costs for borrowing, and raising more capital can be challenging as well after a security breach.
- Loss of sensitive customer data can result in penalties and fines for failing to protect customer data. Businesses may be sued over data breaches.
- Due to loss of reputation and damaged brand identity after a cyberattack, customers' trust in a business will decline. Businesses not only end up losing current customers but also find it difficult to gain new customers.
- Direct costs may also be incurred such as the cost of hiring cybersecurity companies for remediation, increased insurance premium costs, public relations (PR), and other services related to the attack.

Effects of cybercrime on national Défense

Cybercrimes may have public health and national security implications, making computer crime one of DOJ's top priorities. In the U.S., at the federal level, the Federal Bureau of Investigation's (FBI) Cyber Division is the agency within DOJ that is charged with combating cybercrime. The Department of Homeland Security (DHS) sees strengthening the security and resilience of cyberspace as an important homeland security mission. Agencies such as the U.S. Secret Service (USSS) and U.S. Immigration and Customs Enforcement (ICE) have special divisions dedicated to combating cybercrime.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

USSS's Electronic Crimes Task Force (ECTF) investigates cases that involve electronic crimes, particularly attacks on the nation's financial and critical infrastructures. USSS also runs the National Computer Forensics Institute (NCFI), which provides state and local law enforcement, judges and prosecutors with training in computer forensics.

The Internet Crime Complaint Centre (IC3), a partnership among the FBI, the National White Collar Crime Centre (NW3C) and the Bureau of Justice Assistance (BJA), accepts online complaints from victims of internet crimes or interested third parties.

III. METHODOLOGY

Cybercriminals take advantage of security holes and vulnerabilities found in systems and exploit them in order to take a foothold inside the targeted environment.

The security holes can be a form of using weak authentication methods and passwords, it can also happen for the lack of strict security models and policies. The world is constantly developing new technologies, so now, it has a big reliance on technology. Most smart devices are connected to the internet. There are benefits and there are also risks. The reasons why cybercrimes are increasing:

One of the risks is the big rise in the number of cybercrimes committed, there are not enough security measures and operations to help protect these technologies. Computer networks allow people in cyberspace to reach any connected part of the world in seconds. Cybercrimes can have different laws and regulations from one country to another, mentioning also that covering tracks is much easier when committing a cybercrime rather than real crimes.

Here is the list of certain reasons for the big increase in cybercrimes:

1) *Vulnerable devices:* As we mentioned before, the lack of efficient security measures and solutions introduces a wide range of vulnerable devices which is an easy target for cybercriminals.
2) *Personal motivation:* Cybercriminals sometimes commit cybercrimes as a kind of revenge against someone they hate or have any problem with.
3) *Financial Motivation:* The most common motivation of cybercriminals and hacker groups, most attacks nowadays are committed to profit from it.

A. How Cybercrime Works

Cybercrime attacks can begin wherever there is digital data, opportunity, and motive. Cybercriminals include everyone from the lone user engaged in cyberbullying to state-sponsored actors, like China's intelligence services.

Cybercrimes generally do not occur in a vacuum; they are, in many ways, distributed in nature. That is, cybercriminals typically rely on other actors to complete the crime. This is whether it's the creator of malware using the dark web to sell code, the distributor of illegal pharmaceuticals using cryptocurrency brokers to hold virtual money in escrow or state threat actors relying on technology subcontractors to steal intellectual property (IP).

Cybercriminals use various attack vectors to carry out their cyberattacks and are constantly seeking new methods and techniques for achieving their goals, while avoiding detection and arrest.

Cybercriminals often carry out their activities using malware and other types of software, but social engineering is often an important component for executing most types of cybercrime.

Phishing emails are another important component to many types of cybercrime but especially so for targeted attacks, like business email compromise (BEC), in which the attacker attempts to impersonate, via email, a business owner in order to convince employees to pay out bogus invoices.

B. Preventive Measures on Cyber Crimes

In this, we see the common mistakes made and their solutions.

1) Opening Emails from Unknown People

Email is the preferred form of business communication. With that many emails, it stands to reason that some are scams. Opening an unknown email, or an attachment inside an email, can release a virus that gives cybercriminals a backdoor into your company's digital home.

Solutions:

a) Advise employees not to open emails from people they don't know.
b) Advise employees to never open unknown attachments or links.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

2) Having Weak Login Credentials

81% of adults use the same password for everything. Repetitive passwords that use personal information, such as a nickname or street address, are a problem. Cybercriminals have programs that mine public profiles for potential password combinations and plug in possibilities until one hits. They also use dictionary attacks that automatically try different words until they find a match.

Solutions:

a) Require employees to use unique passwords
b) Add numbers and symbols to a password for increased security. For example, change "Switzerland" to "Sw1tzer!and"
c) Create rules that require employees to create unique, complex passwords of at least 12 characters; and change them if they ever have reason to believe that they have been compromised.
d) Use a password manager software to automatically generate strong individual passwords for multiple apps, websites, and devices.

3) Leaving Passwords on Sticky Notes

People tend to leave a sticky note on a screen with passwords written on it. This happens more often.

Solutions:

a) If employees must write down passwords, ask that the paper copies are kept inside locked drawers.

4) Having Access to Everything

In some cases, companies don't compartmentalize data. In other words, everyone from interns to board members can access the same company files. Giving everyone the same access to data increases the number of people who can leak, lose or mishandle information.

Solutions:

a) Set up tiered levels of access, giving permission only to those who need it on each level.
b) Limit the number of people who can change system configurations.
c) Don’t provide employees with admin privileges to their devices unless they really require such set up. Even employees with the admin rights should only use them as needed, not routinely.
d) Enforce dual sign-off before payments over a certain amount can be processed to combat CEO fraud.

5) Lacking Effective Employee Training

Research shows most companies do offer cybersecurity training. However, only 25% of business executives believe the training is effective.

Solutions:

Provide annual cybersecurity awareness training. Topics could include:

a) Reasons for and importance of cybersecurity training
b) Phishing and online scams
c) Locking computers
d) Password management
e) How to manage mobile devices
f) Relevant examples of situations

6) Not Updating Antivirus Software

The company should deploy antivirus software as a protective measure, but it should not be up to employees to update it. At some companies, employees are prompted to make updates and can decide whether or not the updates take place. Employees likely say no to updates when they are in the middle of a project, since many updates force them to close programs or restart computers. Antivirus updates are important, should be handled promptly and should not be left to employees.

Along with this, The Government has launched the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to enable public to report incidents pertaining to all types of cybercrimes, with a special focus on cybercrimes against women and children. A toll-free number 1930 has been operationalized to get assistance in lodging online cyber complaints. The Citizen Financial Cyber Fraud Reporting and Management System module has also been launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

IV. CONCLUSION

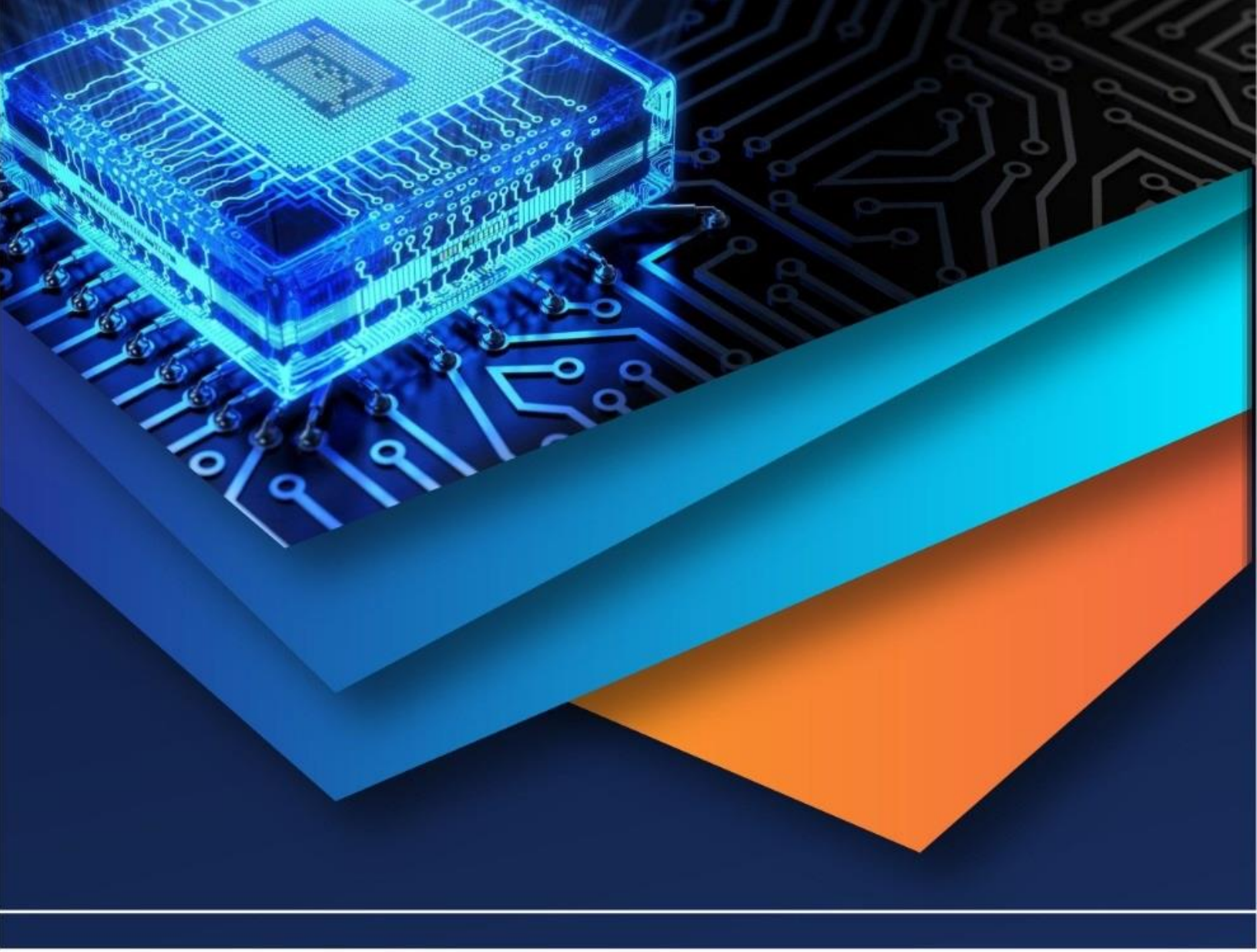
India is one of the countries with the highest number of cybercrimes in recent years, amounting to 4.5 million. Cybercrime refers to criminal behaviour committed by using a computer or other electronic device connected to the internet.

Cybercrime is the criminal behaviour of unauthorized access to computer systems. Cyber security provides a thorough understanding of how cyber-attacks can be controlled or recovered. There are a lot of websites and Online courses that provide advice on how cybercrimes and cybercrime hazards can be prevented, protected, and recovered. This paper is a glance into various cybercrimes, the various risks it poses and the strategies for prevention from the same.

REFERENCES

[1] Covid-19 Pandemic: A New Era of Cyber Security Threat and Holistic Approach to Overcome. Ahmed and Q. Tushar *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 2020, pp. 1-5, doi: 10.1109/CSDE50874.2020.9411533.
[2] Predicting and Preventing Cyber Attacks During COVID-19 Time Using Data Analysis and Proposed Secure IoT layered Model," L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider and G. Saldamli, *2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)*, 2020, pp. 113-118, doi: 10.1109/MCNA50957.2020.9264301.
[3] A Study on Various Cyber Attacks and A Proposed Intelligent System for Monitoring Such Attacks," A. S. Choudhary, P. P. Choudhary and S. Salve, 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 612-617, doi: 10.1109/ICICT43934.2018.9034445.
[4] Investigation and classification of cyber-crimes through IDS and SVM algorithm," H. Zolfi, H. Ghorbani and M. H. Ahmadzadegan, 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 180-187, doi: 10.1109/I-SMAC47947.2019.9032536.
[5] Thwarting Cyber Crime and Phishing Attacks with Machine Learning: A Study," M. Arshey and K. S. Angel Viji, 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 353-357, doi: 10.1109/ICACCS51430.2021.9441925.
[6] An Empirical Study of Cybercrime and Its Preventions," S. Batra, M. Gupta, J. Singh, D. Srivastava and I. Aggarwal, 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, pp. 42-46, doi: 10.1109/PDGC50313.2020.9315785
[7] A Technical Review Report on Cyber Crimes in India," P. Datta, S. N. Panda, S. Tanwar and R. K. Kaushal, 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), 2020, pp. 269-275, doi: 10.1109/ESCI48226.2020.9167567.
[8] Classification and Imapct of Cyber Threats in India: A review," S. Tanwar, T. Paul, K. Singh, M. Joshi and A. Rana, 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020, pp. 129-135, doi: 10.1109/ICRITO48877.2020.9198024.
[9] A Survey on Cyber Security Threats and Challenges in Modem Society," S. Z. Sajal, I. Jahan and K. E. Nygard, 2019 IEEE International Conference on Electro Information Technology (EIT), 2019, pp. 525-528, doi: 10.1109/EIT.2019.8833829.
[10] Cyber Crime in India: An Empirical Study Prof. Saquib Ahmad Khan International Journal of Scientific & Engineering Research Volume 11, Issue 5, May-2020 ISSN 2229-551
[11] Cyber Crimes in India: Trend and Preventions Sanjeev Kumar, Dr Anupam Manhas GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ) ISSN (E): 2347-6915 Vol. 9, Issue 5, May (2021)
[12] A Study on Cyber Crime and its Legal Framework in India APOORVA BHANGLA1 AND JAHANVI TULI Vol.no 4 2021. International Journal of Law Management & Humanities [ISSN 2581-5369
[13] CYBER CRIMES IN INDIA: TRENDS AND PREVENTION Ms. Riddhi Shah 2019 IJRAR March 2019, Volume 6, Issue 1
[14] RESEARCH PAPER ON CYBER SECURITY Mrs. Ashwini Sheth1, Mr. Sachin Bhosale2, Mr. Farish Kurupkar CONTEMPORARY RESEARCH IN INDIA (ISSN 2231-2137): SPECIAL ISSUE: APRIL, 2021.
[15] https://cltc.berkeley.edu/scenario-back-matter/
[16] https://www.bitdegree.org/tutorials/what-is-cyber-security/
[17] Research Paper on Cyber Security by Mrs. Ashwini Sheth, Mr. Sachin Bhosale, and Mr. Farish KurupkarIssues regarding cybersecurity in modern world by H. Geldiyev, M. Churiyev, and R. Mahmudov
[18] A Quick Guide to Cybersecurity Incidents and How to Avoid Them?
[19] Types of Cybersecurity Threats, and How to avoid them?
[20] Work From Home Cybersecurity, Tips, and Risks

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)