https://doi.org/10.56815/IJMRR.V1.I4.2022/22-29
International Journal of Multidisciplinary Research & Reviews
ISSN:2945-3135
Vol 1, No. 04, 2022

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH & REVIEWS
journal homepage: www.ijmrr.online/index.php/home

DIGITAL ERA IN CYBER CRIME AND SECURITY

Dr Chethana Sridhar[1] , Disha.R .Pandey[2], Ranjitha .B.A[3], Harshini.S[4] , Sushmitha .R[5]

[1]Asst.Professor, Dept of Computer Applications, Sivananda Sarma Memorial RV College
[2]1st year BCA, Sivananada Sarma Memorial RV college
[3]1st year BCA,Sivananda Sarma Memorial RV College
[4]1st year BCA,Sivananda Memorial RV College
[5]1st year BCA,Sivananda Sarma Memorial RV college

How to Cite the Article: Sridhar C., P. R. Disha, B.A Ranjitha, S. Harshini, R. Sushmitha (2022). DIGITAL ERA IN CYBER CRIME AND SECURITY. International Journal of Multidisciplinary Research & Reviews , 1(4), 22-29.

Keyword

Crime, Cyber Crime, Cyber Crime security Fraudsters, Hacking , Phishing, Mobile Networks, Social Media, Cyber Security, Identity Theft.

Abstract

Cyber Security is a potential activity by which information and other communication and other communication system are protected from or defended against the unauthorized use or modification or exploitation or even theft .The types of cybercrime are Identity theft, Psychological tricks ,Social media frauds and mobile application frauds ,the most frequently heard in banking frauds . There are many causes of cyber crimes like cyber hoaxes, negligence, revenge or motivation, poor law enforcing bodies and cyber crime committed from publicity or recognition , social media player important role in cyber security. There are many act on Cyber Security like IT Act 2000(Cyber Stalking) and many more.

1. INTRODUCTION

Information and other communication systems may be safeguarded from or defended against the illegal use, alteration, exploitation, or even theft through the use of cyber security. Identity theft, psychological ploys, social media fraud, mobile application fraud, and banking fraud are the four main categories of cybercrime. Cybercrimes can be caused by a variety of factors, including negligence, retaliation or other motivations, ineffective law enforcement, and crimes done for fame or recognition. Social media plays a crucial part in cyber security. Acts regarding cyber security abound, including the IT Act 2000 (Cyber Stalking) and several more. Let's first define what cybercrime is before delving deeper into cybercrime security. Basically, cybercrime is any crime that contains computer or a network using technology A cybercrime is an act that is carried out via electronic communication tools. The crime rate is rapidly increasing in India. Cybercrime used to be mostly perpetrated by lone people or small groups, but today's cybercriminals come in many forms, including professional and organized hacking gangs. between the ages of 6 and 18; kids and teenagers. Today's man may send and receive any type of data, including audio, video, and emails, with the press of a button, but has he ever considered how securely his data is being transported and given to the other person without any information being leaked? Cyber security has the solution. Cybersecurity protects all internet-connected systems, including data, software, and hardware, from cyber attacks.It is a group of techniques, policies, and tools used to protect computers, software, networks, and data from damage, theft, and unauthorized access.

https://doi.org/10.56815/IJMRR.V1.I4.2022/22-29
International Journal of Multidisciplinary Research & Reviews
ISSN:2945-3135
Vol 1, No. 04, 2022

Why Is Cyber security So Vital?

Since it protects against data theft and destruction, cyber security is essential. Private data, sensitive data, business information systems, etc. are all covered by this.The company cannot defend itself against data breach operations without a cyber security programed, making it an easy target for hackers.

2.CATEGORIES OF CYBER CRIME

The principal types of cybercrime based on their impact and goal, fall into one of the following four categories:

1. Crimes against Persons:
   These types of crimes are committed to hurt specific people. These include cyber bullying, cyber stalking, email harassment, defamation, Other examples include phishing, carding, child pornography, assault by threat, denial-of-service attacks, forgeries, and SMS spoofing.
2. Violations of Property:
   There are cybercrimes committed to damage a person's property. Intellectual property crimes, cyber-squatting, cyber-vandalism, computer hacking, computer forgeries, spreading viruses and malicious software to harm data, Trojan horses, and other similar offences can all be characterized as such cyber trespass, internet time thefts ,robbery or stealing money while money transfers etc.
3. Crimes against Government/ Firm / Company /Group of individuals:
   These types of crimes include cyber terrorism, possession of unauthorized information, distribution of pirated software ,web jacking ,salami attacks ,logic bombs etc.
4. Crimes against Society:
   All the above mentioned crimes have their direct or indirect influence on the society at large. Therefore, all such crimes are included in this such as pornography ,online gambling ,forgery, sale of illegal articles, phishing, cyber terrorism ,etc.

3. What's the link between cookies and cyber security?

Browser "Cookies" are a crucial tool used today on the internet. They first appeared in 1994, and arguments around cookie consent have been going on for more than ten years at this point. Even today, many ardent internet users do not fully comprehend the benefits of using cookies, when to enable them, and when to categorically refuse to accept them. We explore all cookies in this guest blog and how they relate to online security and data privacy. To make sure you utilize cookies correctly, you must have a thorough grasp of them. The security of your sensitive data and personal information can significantly improve if you use Cookies effectively. However, acting carelessly Cookies enabled may have the exact opposite effect. Accepting cookies on every website you visit might put your sensitive information at risk for being kept and shared website you visit. You will often notice a pop-up message providing an acceptance to use Cookies on that website when you visit it. Technically speaking, the technology is meant to enhance your website viewing experience. For instance, the website will recall your username, password, and activity choices that you often use. In essence, the website will always remember who you are so you won't have to repeatedly submit the same information. These days, browser "cookies" are a crucial tool on the internet. Their emergence began in 1994, when there was negative conversation

4. TYPES OF CYBERCRIME [1]

A cyber crime is a crime committed using networks and computers. This covers a wide variety of behaviors, including stealing money from online bank accounts to downloading music files unlawfully.

4.1Identity Theft I

It involves collecting someone's personal information against their will and without authorization. The fraudster can access your bank accounts by using stolen personal information and identity documents. . Use a false name

https://doi.org/10.56815/IJMRR.V1.I4.2022/22-29
International Journal of Multidisciplinary Research & Reviews
ISSN:2945-3135
Vol 1, No. 04, 2022

on social media When the cops are making an arrest, give them your name. Hacking into social media accounts or acquiring access to them are a few instances of identity theft. Using photocopies of identity documents incorrectly. Skimming of credit/debit cards.

4.2 Tricks of the Mind

Attackers utilize them to manipulate users' thoughts in order to lure them in with tempting promises. Once the victim is in their grasp, the assailants might take advantage of them by taking their property, their confidential information, or inflicting other types of harm. This type of assault is designed from the ground up to trick the victim into falling into their trap by sending phony emails, calls, and SMS. Phishing, Vishing, and Smishing are all attempts to defraud the victim of their money or inflict other harm to the victim.

Here are a few instances of Tricks of mind:

- Credit/debit card fraud
- Lottery scams
- Workplace fraud

4.3 Social Media Frauds

It is become an essential component of our life. It is a new method of telling others about the happenings in our life and of connecting with them about them. Through their social media profile, one may learn about a person's whole history and even make predictions about the future based on trends seen in the past. An individual is put in danger since unauthorized access to social media profiles can result in information loss, public shaming, or even worse outcomes like physical attack or robbery. Therefore, it is crucial to preserve and use social media profiles appropriately.

Several instances of social media fraud include:

- Compassion fraud
- Relationship fraud
- Cyber bullying
- Cyber stalking

4.4 Mobile Application Fraud

The usage of mobile apps has expanded in tandem with the use of smart phones, raising the related security threats. Since there are now four times as many mobile transactions as there were two or three years ago, cybercriminals are now specifically targeting mobile consumers to steal their data and money. These application scammers are more vulnerable to cyber attacks as a result. The user must be aware of these assaults on frequently used mobile applications including digital payment applications and gaming applications. Cyber attacks employing infected mobile applications are one type of mobile application fraud.

4.5 .ONLINE BANKING FRAUDS[6]

What are scams in internet banking?

All banking services are now offered online. Online services include getting account statements, transferring money to other accounts, getting a cheque book, creating demand draughts, and many more. The majority of these services don't need going to the bank in person; they may be completed from home. Cyber frauds involving banking are growing as more services are moving to internet platforms. Our online bank accounts need to be secured with strong passwords, just like the jewelry-filled locker we lock up with a lock and key. The valuables will also be stolen if the key is taken. The money in the bank accounts will also be taken Thus, protecting bank accounts with complex passwords becomes crucial. Attacks connected to Digital Payments Applications are

one type of online banking fraud. Bank account hacking due to a weak password Multiple account hacking due to the use of the same password

4.6. Virus Attack On Personal Computer

In our daily lives, laptops and personal computers are indispensable. We save important information in the computer, including bank account data, business documents, and private files like images, music, and movies. Protection of all of this data is therefore absolutely necessary. It is just as crucial to safeguard our sensitive data from viruses and other dangerous software that might harm it as it is to keep a physical eye on our safe deposit boxes.

Some examples on how our personal computer can get affected by virus:

- Virus attack through external devices
- Virus attack by downloading files from un-trusted websites
- Virus assault using the download of harmful software

5.CAUSES OF CYBER CRIMES[7]

The difficulty in protecting a computer system from unauthorized access stems from the ease of entry. Access codes, recorders, pins, retinal pictures, and other items may be stolen and used to trick biometric systems, circumvent firewalls, and get past several security systems.

5.2 Cyber hoaxes - Cybercrimes might be carried out solely to put someone in danger or harm their reputation. The riskiest of all causes is this one. The parties engaged are committed to fighting for their cause and want to see their cause and objective realized. They are referred to as cyber terrorists.

5.3 Negligence- It is possible to neglect to take precautions to protect the system. Due to this carelessness, thieves have the ability to harm the computer.

5.4 Motivation for retaliation-The desire to learn a complicated system with the intention of harming the victim financially. This includes children or people who manipulate data for e-commerce, e-banking, or fraudulent transactions out of a desire to make quick money.

5.5 Weak Law Enforcement- Because many nations do not have cybercrime legislation, many offenders escape punishment.

5.6 Cybercrime done for attention or recognition-Typically, young people who desire nothing more than to stand out from the crowd without offending anyone.

6. CYBER SECURITY TECHNIQUES[9,10]

The idea of a login and password has been a key method of information protection. This might be the first step towards implementing cyber security.

6.2 Data authentication: Before downloading, the papers we get must always be certified, meaning its provenance from a trustworthy and dependable source and their authenticity from tampering must be verified. The anti-virus software installed on the devices is often responsible for authenticating these documents. Consequently, having strong antivirus software is equally crucial for shielding the gadgets from malware.

6.3 Malware Scanning Tools : This programme typically checks all of the system's files and papers for hazardous viruses and malicious code. Malicious software is generally referred to as malware and includes items like viruses, worms, and Trojan horses.

6.1 Access control and password security

The concept of username and password has been fundamental way of protecting our information .This may be one of the first measures regarding cyber security

6.2 Authentication of data

The documents that we receive must always authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these

documents is usually done by the anti-virus software present in the devices .Thus a good anti-virus software is also essential to protect the devices from viruses

6.3 Malware Scanners

This is software that usually scans all the files and documents present in the system for malicious code of harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

6.4 FireWalls

A firewall is a piece of hardware or software that prevents hackers, viruses, and worms from trying to access your computer through the internet.The firewall that is in place examines each message as it enters or exits the internet, blocking those that do not adhere to the set security requirements. Therefore, firewalls are crucial for identifying malware..

6.5 Anti-Virus Software

Computer application known as antivirus software works to identify, stop, and take action against dangerous software programmes like viruses and worms.

7 TRENDS CHANGING CYBER SECURITY[9]

7.1 Web Servers

The legal web servers that cybercriminals have compromised are used to transmit their malicious code. Data-stealing assaults, many of which draw media attention, are a significant hazard as Protecting web servers and web applications must now receive more attention.

7.2 Cloud Computing And Its Services

Cloud services are currently being slowly adopted by all small, medium, and large businesses. To put it another way, the earth is gradually advancing into the clouds. As traffic can bypass conventional ports of inspection, the most recent trend poses a significant problem for cyber security. In addition, as the number of cloud-based apps increases, policy controls for online applications and cloud services will also need to change and have an automatic update capability that allows them to obtain virus profiles

7.3 APT'S And Targeted Attacks

A new class of cybercrime software is called a "APT" (advanced persistent threat). Over time, network such targeted assaults have largely been identified thanks to security features like web filtering and intrusion prevention systems (IPS) (mostly after the initial compromise).

7.4 Mobile Networks

We can communicate with anyone, anywhere in the world, today. Security, however, is a very serious worry for these mobile networks. As more people use gadgets like tablets and phones, firewalls and other security protections are becoming leaky.

7.5 Encryption Of The Code

The act of encoding communications (or information) so that hackers or eavesdroppers cannot read them is known as encryption. An encryption algorithm is used in an encryption technique to transform the message or information into an unintelligible cipher text. An encryption key, which determines how the message is to be encoded, is typically used for this data privacy is protected at the very early stages of encryption .Thus, the aforementioned are some of the developments that are altering the global landscape of cyber security.

8 INDIA'S CYBERCRIME RATE[6]

The number of cybercrimes in the nation has surged by a factor of 4, or 306 percent, over the past four years. 12,317 incidences of cybercrime were reported in 2016, while 50,035 cases were reported in 2020. India's cybercrime rate, or the number of crimes committed online per 100,000 people, increased by 270 percent in just four years from 1 in 2016 to 3.7 in 2020. According to NCRB data, at the conclusion of each year, 65.81 percent

https://doi.org/10.56815/IJMRR.V1.I4.2022/22-29
International Journal of Multidisciplinary Research & Reviews
ISSN:2945-3135
Vol 1, No. 04, 2022

of cases were still open for investigation. Additionally, cases from past years that were not investigated carry over to the current year. An average of 45.57 percent of the cases opened for inquiry in a given year were still being looked at from the year before.

.

REF: An Overview Study on Cyber Crimes In Internet

The threats of attacks on web application to extract data or to distribute malicious code persists.

9 Cyber Security And The Right To Privacy

IT ACT 2000

Crime: Cyber stalking

Definition: Following a person covertly and monitoring his online communication

Mechanism: By electronic means, such as e-mail, instant messaging (IM), posts to a website, or messages sent through a discussion forum.

Amendments to Section: 43, 66 (Compensation and punishment of three years with fine)

Technical measures to stop cyber stalking include keeping personal information private when using the internet, chat, instant messaging, and other electronic communication channels.

Crime: Theft of Intellectual Property

Source code tampering is defined as.

Mechanism: Getting a hold of source code or other relevant data, then stealing, changing, etc. the code.

Sections and Amendments:43,65,66

(Compensation and punishments of three years with fine)

Technical Measures: Technical safeguards and strong authentication are used to prevent data eakage

Crime: E-mail bombing

Definition : Flooding your email account with an excessive amount of emails can sometimes make it difficult to notice essential messages.

Mechanism: Bulk email production utilizing automated techniques to target a certain address

Sections and amendments :43,66

(Compensation and punishment of three years)

Technical Measures: Putting anti-spam filters in place.

Crime: Phishing

Definition: A bank Financial Crime in Online Banking

Mechanism: Identity theft is carried out through means of social engineering

Sections and amendments: 43,66, 66C

(Compensation and punishments of three years with fine)

- Technical Measures: Removal of fraudulent websites right away
- Users should be wary of phishing attacks and have a strong authentication system for financial and electronic banking.
- Maintaining the security of the computer systems used to conduct business with financial institutions and banks

Crime: Identity Theft

Definition : Stealing an individual's online identification information Mechanism : Phishing scams or hacking of personal identifying information

Sections and amendments:43

(Compensation and punishments of three years with fine)

Technical Measures: Protecting individual identification information, safeguarding computer systems, spreading knowledge of identity theft prevention, and using safe online practices

Crime: Spoofing

Definition: Spoofing is a crime that is defined as utilizing familiar and amiable people to steal credentials

Mechanism: . Using tools and other manipulation methods, GUI's work

Sections and Amendments:43,66

(Compensation and punishments of three years with fine)

Technical Measures: . Using tools and other manipulation methods, GUI's work safeguarding the credentials and implementing anti-spoofing measures

CONCLUSION

Since networks are used to conduct crucial transactions, cyber security is a large topic that is getting more significant as the globe becomes more connected. Organizations are facing challenges with how they safeguard their infrastructure and how they need to develop new platforms and intelligence to do so as a result of the newest and most disruptive technology as well as the new cyber tools and threats that surface every day. Only those who are unaware that they are part of the same process as the cosmos can use technology in a destructive way. The Federal Government are making every effort to raise awareness among the populace. so that consumers can secure their data from cybercrime and stay safe. Therefore, the country's cybercrime can be decreased with sufficient knowledge and information.

REFERENCES

1. Cyber Security-Awareness for Citizens:
   -Issued by the Maharashtra Cyber, Home Department, and Special Inspector General of Police State of Maharashtra government.

2. India's experience with cyber crime ,Cyber Security, and Cyber Rights
   -Sent by Ms. Jyothi Lakhani, Head, Computer Science Department Maharaja Ganga Singh College in Bikaner.
3. Shilpa Yadav, Tana Shree, and Yashika Arora delivered a research paper on "Cyber Crime and Security.
4. Concerning cybercrime and security: by the information science department of Kuwait University's College of Computing Sciences and Engineering, Kuwait

5. A study by Anupreet Kaur Mokha, Assistant Professor at SGTB Khalsa College, University of Delhi, on Cybercrime Awareness and Security
6. An outline of a study on cybercrime on the internet by V. Karam Chand Gandhi, assistant professor at Thanjavur University of Technology in Tamil Nadu, Department of Computer Science and Management, Thanjavur, Tamil Nadu
7. Inside of Cyber crimes and information Security: Threats and Solutions
   -By Sunakshi maghu,Siddhart Sehra and Avdesh Bhardawaj, Department of EECE, ITM university, Gurgaon, Haryana, India
8. Introduction to Cyber Security:
   -By Arvin Kumar ,Department of computer science and engineering ,Galgotial University ,Uttar Pradesh
9. An analysis of the latest technologies' impact on cyber security challenges. Osmania University, G.J. Ugander Reddy, and Peridot Technologies Hyderabad
10. Internet safety: Malla Reddy College of Engineering and Technology, Telangana, Department of Information