International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET

A Review of Recent Cybersecurity Trends, Rapid Rise in Cybercrime and the Need for Effective Measures against it

Dheeraj Patil, Neeraj Tembare, Vedang Shinde, Calvin Suares, Shivam Shinde, Chandrakant Kokane

Nutan Maharashtra Institute of Engineering and Technology, Talegaon(D), Pune, Maharashtra, India

ARTICLEINFO

Article History :

Accepted: 10 Nov 2023
Published: 30 Nov 2023

Publication Issue :
Volume 10, Issue 6
November-December-2023
Page Number :
229-234

ABSTRACT

Cyber-security plays a very important role in the field of online communication and the internet. These days securing and protecting personal information is one of the biggest challenges. The internet and digitalization is spreading rapidly to all aspects of life, from supercomputers, artificial intelligence based applications to small scale devices, IoT, etc. The development of technology has provided a worldwide stage for anyone to access and perform various tasks. The internet is currently one of the major sources of information. As the technology is evolving at a rapid pace the rate of individuals or communities who aim to make unethical use of this evolution is also rising. When we delve into the realm of cyber security, the first thought that comes to mind is 'cybercrime,' a phenomenon that is escalating at an alarming rate. Governments and organizations are implementing a lot of measures and initiatives to combat these cyber threats.

Keywords : Cyber-Security, Cyber Threats

I. INTRODUCTION

In today's widely interconnected society, online-security has become a huge concern for individuals, businesses, and governments,etc. As our reliance on digital technologies continues to expand, so does the threat landscape, exposing our personal information, financial assets, and critical infrastructure to a growing range of cyberattacks. The ever-evolving nature of cyber threats, coupled with the increasing complexity of digital systems, necessitates a multifaceted approach to cybersecurity that encompasses both technical safeguards and user education.This review paper examines a novel web application that addresses the cybersecurity challenges of the modern digital age. The situation is alarming and requires immediate attention: Cybercrime has become a pervasive topic across all elements of the society. Over the past decade, cyberattacks have destroyed businesses, causing harm to both individual and national security.

This paper mainly focuses on the concept of cybersecurity and cybercrime, understanding the common methods used by attackers to exploit individuals and organizations. Trying to analyze the challenges faced by people while ensuring their safety

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

while using the internet and also looking towards the common mistakes made by the victim of a cybercrime, getting a better overview of the threat model. It also focuses on the recent development in cybercrime prevention methods and gives a detailed summary of some of the methods and their effectiveness while also pointing out gaps and flaws in the logic.

1.1 Common forms of cybercrime:

- Phishing
- Identity theft
- Hacking websites or computer networks;
- Spreading hate and inflammatory terrorism
- Violating copyright
- Selling illegal items
- Data and Media Piracy
- Cryptocurrency scams
- Online payment scams via QR codes
- Cyberbullying
- Data breaches
- Denial-of-service (DoS) attacks.

Phishing, credit card fraud, unlawful downloading, industrial espionage, child pornography, scams, cyberterrorism, and other offenses are all included in the category of computer crime. A minute part of online crimes are made public, while others are still unknown to many . Folks have been attempting to install virus protection software to safeguard their machines and address viral issues. The truth is that cybercriminals are hardly ever apprehended. Internet users must run antivirus software, create unique passwords, and antivirus programmes. The internet is the source of pornography, which is classified as obscenity and carries a penalty. Child internet crimes are a serious issue that warrants attention and has no simple fix. Although the internet is a fantastic tool and has assimilated into our existence, there are many things out on the internet that could cause serious issues and the users need to be wary of them and actively take measures to prevent being a victim to such dangers.

II. Objective

The main goal of this paper is to analyze the existing trends in cybersecurity and to spread the knowledge of the crimes or offenses that take place through the internet or cyberspace. It tries to identify the major issues and challenges present on the cyberspace and its potential to affect the users of cyberspace. It attempts to understand how an attacker is able to trap their victim and what are the common warning signs which an individual should be aware of. By analyzing various statistical data and reports the paper tries to analyze the relationship between intellectual property and cyberspace crime.

III. Literature Review

3.1 History of Cyber Crime

The word "Cybercrime" was initially proposed in 1995 by Sussman and Heuston. Cybercrime is best understood as a series of acts or conducts rather than something that can be defined in a single way. These actions are predicated on a material offense object that has an impact on computer systems or data.These are the unlawful activities in which a digital device or information system is either used as a tool, a target, or both. Cybercrime is sometimes referred to as e- crime, high-tech crime, information age crime, computer-related crimes, and other similar terms.Cybercrimes, to put it simply, are offenses or crimes committed using electronic communications or information systems. These kinds of crimes are essentially illicit actions involving computers and networks. The growth of the internet has also led to an increase in the volume of cybercrime since it is no longer necessary for the perpetrator to be physically present for the commission of the crime.

One peculiarity of cybercrime is that there's a chance that the perpetrator and the victim will never speak to one another.

In order to lessen the likelihood of being discovered and prosecuted, cybercriminals frequently choose to

operate out of nations with lax or nonexistent laws against cybercrime.

The idea that cybercrimes can only be perpetrated online or through cyberspace is a common misconception. Cybercrimes can actually be committed without a person's involvement in the internet; they don't always require the perpetrator to be online. One such example of privacy concerns is software privacy.

3.2 Evolution of Cyber Crime

Significant changes in technology and evolving criminal tactics have had a profound impact on the evolution of cybercrime over time. The below table shows how cybercrime has evolved and also lists out examples of major attacks of respective era.

Table-1: Evolution of Cyber Crime

Era	Characteristics
Early (1970s-80s)	Basic cybercrimes emerge.
1990s	Rise of malware and hacking.
2000s	Internet-driven crimes proliferate.
Mid-2000s	Cybercrime becomes sophisticated.
2010s	Surge in ransomware and state-sponsored attacks.
Current Trends	IoT threats and ongoing cyber espionage.
Future Risks	Anticipated impact of AI and deepfakes.

3.3 Statistical Analysis

According to research, nearly seven out of ten individuals are victims of cybercrime. Cybercrime, basically is the use of computers and other digital media to perpetrate criminal activity. There is an abundance of different types of cybercrimes that exist in the world today, including data theft, cyberterrorism, child pornography, phishing, and cyber extortion. Our review paper covers a few of them. India is becoming a major target for cyberattacks, which is why cybercrime is becoming a growing concern there. In 2021, the Indian Computer Emergency Response Team (CERT-In) reported that more than 156,000 cybercrime incidents had been reported in the country. Compared to the previous year, when there were over 115,000 reported cybercrime incidents, this indicates a significant increase.

3.3.1 Major cybercrime incidents

2020

· Ransomware attack: In May 2021, a ransomware attack targeted Fortis Healthcare, a significant Indian healthcare provider, interfering with patient care and data access.

· Data breach: In October 2021, over 20 million customers' personal information was compromised by a data breach at BigBasket, a well-known e-commerce platform in India.

· Phishing attack: In December 2021, employees of HDFC Bank, a well-known Indian bank, were the target of a phishing attempt that sought to obtain their login credentials.

2022

· Supply chain attack: SolarWinds, a software vendor with a large Indian customer base, was compromised in a supply chain attack in December 2021, allowing hackers to infiltrate the systems of numerous organizations, including the Indian government.

· Cryptocurrency scam: Numerous Indian investors were lured into cryptocurrency scams in 2022, losing millions of rupees due to fraudulent investment schemes promising high returns.

2023

· Malware attack: Government of India websites were subjected to malware attacks in early 2023, attempting to spread malicious software and compromise sensitive data.

· Data leak: Twitter, a social media platform with a large Indian user base, suffered a data leak in July 2023, exposing the personal information of over 500 million users, including Indian citizens.

· Identity theft: Cases of identity theft involving Indian citizens using online services were reported in 2023,

highlighting the growing risks associated with sharing personal information online.

IV. Detailed Analysis of Cyber Attacks

There are four main categories into which cybercrime falls.

a) Spamming: Also referred to as junk email, spam emails. It's an unsolicited email mass message. Since the middle of the 1990s, spam has grown in popularity, and most email users now deal with it. Spam bots are automated programs that search the internet for email addresses and gather the recipients' addresses. Spammers generate email distribution lists with the aid of spam bots. A spammer usually sends an email to millions of email addresses, hoping to get a small number of responses. Spam hinders users from effectively utilizing their time, storage space, and network bandwidth. The problem of unsolicited emails is growing annually and accounts for more than 77% of the total worldwide email volume. This leads to significant financial losses and the exposure of sensitive personal data such as passwords, Bank Verification Numbers (BVN), and credit card numbers. Users find themselves increasingly annoyed by the influx of spam emails, prompting them to look for a way to have these emails identified by a machine. This would alleviate their concerns about the authenticity of the emails. The prevalent solutions involve the utilization of diverse machine-learning models to recognize patterns in spam emails and mark them as such. These models analyze new emails in comparison to patterns identified in past spam emails. KNN classification and MLP are highly favored for their accuracy, recall, and precision.

b) Password Security and Memorability : Password-based authentication mechanism is the key to security, it is used to secure the accounts and other personal data from unauthorized access. Password authentication is the cheapest mechanism in order to authenticate a system. Passwords are the most vulnerable part of a system in a network. It majorly has 2 issues : strength and memorability.

According to the Verizon 2017 Data Breach Investigation Report, 81% of the data breaches in the systems are caused due to that hacker having stolen and/or the users used a weak password. Dictionary attacks attempt to defeat password protected systems by systematically entering each word in a dictionary as a password. Also passwords difficult to crack are very difficult to remember for humans. As there are multiple passwords with different characters.

So there is a need for passwords that are not easily crackable and easy to remember. A solution we found interesting is a password generator based on a keyword provided by the user. Using a python script taking an input from the user and creating a password based on the input adding necessary constraints to make it difficult to crack.

c) URL Phishing : Phishing is a prevalent form of social engineering utilized by cybercriminals to illicitly obtain personal information from internet users, including sensitive details like credit card information, usernames, and passwords.

Phishing is a common tactic employed by cybercriminals who send deceptive emails or messages containing links to fraudulent websites. These websites are designed to appear legitimate and often prompt users to disclose personal information, which is then exploited to gather data and pilfer passwords or sensitive financial details. Cybercriminals frequently conceal deceptive website links in emails (email phishing), text messages (smishing), or other messaging platforms such as social media apps. These links are designed to mimic well-known brands like Twitter, Google, Microsoft, Zoom, Amazon, or government agencies associated with health, finance, or social welfare.

Deep learning models are found to be the best to detect a phishing url. CNN models have an accuracy of 98% in detecting phishing urls.

d) File Encryption/Decryption : As the use of the Internet continues to grow, particularly for activities

like online banking and e-commerce, the need for secure file transfer mechanisms has become increasingly vital. The surge in internet- based communication and file transmission has amplified the necessity for secure transfer of sensitive information. Cryptography, which involves encrypting plain text and decrypting cipher text, is one of the methods used to ensure secure communication and file transfer over the internet. Some files have very personal or important confidential data that should not be transited on the internet or stored just as it is. If the data falls in wrong hands it could cause issues. So encrypting data is necessary, so only authorized users can access it. Encryption of data can be done by various ways such as AES, DES, RSA. RSA is found to be the most effective and secure for encrypting and also simple in decryption for authorized users.

V. Safety in cyberspace

Listed below are some points one should keep in mind while surfing the internet:

- If possible, always use a strong password and enable 2 steps or Two-step authentication in the webmail.
- Never share your password to anyone.
- Never send or share any personal information like bank account number, ATM pin, password etc over an unencrypted connection including unencrypted mail
- Websites that don't have the lock icon and https on the address bar of the browser are the unencrypted site. The “s” stands for secure and it indicates that the website is secure.
- Don’t sign to any social networking site until and unless one is not old enough.
- Don’t forget to update the operating system.
- Firewalls, anti- virus and anti-spyware software should be installed in ones PC and should be regularly updated.
- Visiting an untrusted website or following a link sent by an unknown or by an untrusted site should be avoided.
- Don’t respond to spam.
- Make sure while storing sensitive data in the cloud is encrypted.
- Try to avoid pop-ups: Pop-ups sometimes come with malicious software. When we accept or follow the popups a download is performed in the background and that downloaded file contains the malware or malicious software. This is called drive-by download. Ignore the pop-ups that offer site surveys on ecommerce sites or similar things as they may contain malicious code.

VI. Conclusion And Proposed Ideas

The web application's cybersecurity toolkit encompasses a range of essential tools that address common security vulnerabilities and safeguard users against various cyber threats. The password generator tool assists users in creating strong, unique passwords, a critical step in preventing unauthorized access to accounts and sensitive information. The phishing detection feature utilizes machine learning algorithms to identify and flag suspicious emails, protecting users from falling prey to phishing scams. The spam filtering tool effectively categorizes and eliminates unsolicited emails, reducing clutter and preventing exposure to malicious content. The file encryption tool enables users to safeguard their sensitive files by converting them into an unreadable format, preventing unauthorized access and data breaches.

Beyond its practical tools, the web application also provides a wealth of educational content designed to enhance users' cybersecurity awareness. The application's comprehensive library of articles and guides covers a wide spectrum of cybersecurity topics, ranging from basic security principles to advanced threat mitigation strategies. These resources empower users to gain a deeper understanding of cybersecurity risks, best practices, and incident response procedures.

Additionally, the application offers a curated collection of reference links, directing users to reputable sources of cybersecurity information and training.

VII. REFERENCES

[1]. https://www.researchgate.net/publication/367742804_A_Study_of_Cyber_Security_Threats_Challenges_in_Different_Fields_and_its_Prospective_Solutions_ A_Review

[2]. http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_ SOCIETY_and_CYBER_LAW

[3]. https://cybercrime.org.za/definition

[4]. http://vikaspedia.in/education/Digital%20Litercy/infation-security/cyber- laws

[5]. https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf

[6]. http://searchsecurity.techtarget.com/definition/emailspoofing

[7]. http://www.helplinelaw.com/employment-criminaland-labour/CDII/cyber- defamation-in-india.html

[8]. Suman Acharya, Sujata Joshi: Impact Of Cyber-Attacks On Banking Institutions In India: A Study Of Safety Mechanisms And Preventive Measures -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(6). ISSN 1567- 214x

[9]. http://ccasociety.com/what-is-irc-crime/

[10]. http://searchsecurity.techtarget.com/definition/denialof-service

[11]. EMERGING cybercrime Measures and challanges in cyberspace.pdf

[12]. http://www.cyberlawsindia.net/ cyber-india.html

[13]. https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

[14]. https://www.ijarcsse.com/docs/papers/Volume_5/8_August2015/V5I8- 0156.pdf

[15]. Kokane, Chandrakant D., and Sachin D. Babar. "Supervised word sense disambiguation with recurrent neural network model." Int. J. Eng. Adv. Technol.(IJEAT) 9.2 (2019).

[16]. Kokane, Chandrakant D., Sachin D. Babar, and Parikshit N. Mahalle. "Word Sense Disambiguation for Large Documents Using Neural Network Model." 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2021.

[17]. Chandrakant, et al. "Word Sense Disambiguation: A Supervised Semantic Similarity based Complex Network Approach." International Journal of Intelligent Systems and Applications in Engineering 10.1s (2022): 90-94.

[18]. Chandrakant D., et al. "Machine Learning Approach for Intelligent Transport System in IOV-Based Vehicular Network Traffic for Smart Cities." International Journal of Intelligent Systems and Applications in Engineering 11.11s (2023): 06-16.

[19]. Chandrakant D., et al. "Word Sense Disambiguation: Adaptive Word Embedding with Adaptive-Lexical Resource." International Conference on Data Analytics and Insights. Singapore: Springer Nature Singapore, 2023.

Cite this article as :

Dheeraj Patil, Neeraj Tembare, Vedang Shinde, Calvin Suares, Shivam Shinde, Chandrakant Kokane, "A Review of Recent Cybersecurity Trends, Rapid Rise in Cybercrime and the Need for Effective Measures against it", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 6, pp. 229-234, November-December 2023. Available at doi : https://doi.org/10.32628/IJSRSET2310616

Journal URL : https://ijsrset.com/IJSRSET2310616