

Cybercrime and Safety: Emerging Trends

Mr. M. Soma Sekar

Assistant Professor, Department of ECE
PERI Institute of Technology
Chennai, India.

Abstract: Cyber security is critical in the information technology industry. In today's world, information security is a major concern. When we think of cyber security, the first thing that comes to mind is cybercrime, which is growing at an alarming rate. Numerous governments and companies are using a variety of steps to combat cybercrime. Despite several attempts, cyber security continues to be a major issue for a large number of people. This article discusses the difficulties that contemporary cyber security faces. Additionally, it contains the most current information on cyber security methods, ethics, and the trends redefining the sector.

Keywords — Cyber security, cybercrime, cybernetics, social media, cyberstalking, cloud computing, and Android applications are some of the terms used in this article.

1. INTRODUCTION

With the push of a button, today's man may send and receive any kind of data, whether it's an e-mail, an audio or video clip, but has he ever thought how securely his data is transported or delivered to the other person without any information being leaked? The answer is cyber security. The Internet is the fastest-growing infrastructure in today's globe. In today's modern environment, many new technologies are changing the face of mankind. However, we are unable to secure our personal information as effectively as we would want as a consequence of this new technology, and as a result, cybercrime is on the increase. Because over 60% of all commercial transactions are now handled online, this industry required a high degree of security to guarantee that transactions are transparent and efficient. As a consequence, cyber security is a big concern these days. Cyber security encompasses a wide range of disciplines, including cyberspace, in addition to securing information in the IT industry. Cloud computing, mobile computing, e-commerce, online banking, and other cutting-edge technologies all need a high level of protection. The security of these technologies has become a priority since they hold sensitive information about a person. Enhancing cyber security and protecting critical information infrastructures are critical to every country's security and economic well-being. Making the Internet safer (and ensuring the safety of Internet users) has been a major focus of both new service development and government regulation. A more comprehensive and secure approach is required to combat cybercrime. Provided that technology safeguards alone cannot prevent each crime, law enforcement officials must be

given the resources they need to adequately investigate and punish cybercrime. To avert the loss of sensitive data, several nations and governments are increasingly establishing stringent cyber security laws. To defend themselves from the rising number of cybercrimes, everyone should be informed on cyber security. In the world of technology, cyber security is crucial, and data security has become one of the most serious challenges today. When it comes to combating cybercrime, which is on the increase, the government and numerous organisations are trying a range of approaches. As a consequence of a number of circumstances, cybercrime is on the increase again. The difficulties that cyber security confronts as a consequence of new technical breakthroughs and innovations are briefly explored in this study, but the focus of the article is on existing cyber security practises, trends, and other ethics in the cyber security industry.

2. STALKING ON THE INTERNET

Cyber stalking is the practise of following someone via the Internet or other technical means. Many people use the words "online harassment" and "online abuse" interchangeably. Stalking is characterised as persistently annoying or threatening behaviour, such as following someone, showing up at their home or workplace, making harassing phone calls, leaving written messages or goods, or vandalising their property.

Cyber stalking is a technologically-based "attack" on a single person for the sake of revenge, dominance, or wrath. Stalking via the internet may take many forms, including harassment, embarrassment, and humiliation of the victim, enticing bank accounts, or other types of economic control, such as ruining the

victim's credit score in order to isolate the victim by nagging family, friends, and employers.

A "traditional" stalker is one who uses technology to follow and locate their target and their movements (e.g. using Facebook notifications to know what party they are attending). A true cyber stalker's purpose is to do harm to their chosen target by taking advantage of technology's anonymity and untraceable distance. Despite the fact that the perpetrator has completely turned their life upside down, many victims never discover the identity of the internet stalkers who have damaged them.

3. COMPUTER HACKING

Hacking is a crime that entails hacking into computer systems and gaining unauthorised access to the information they hold. The number of people who have been hacked has increased by 37% this year. A case of purported web site hacking and obtaining home addresses from city residents' e-mail accounts has been reported.

Crackers are those who seek to get unauthorised access to computers. Installing a 'backdoor' programme on your computer is generally how this is done. Many crackers try to obtain access to resources by employing password cracking software, which checks billions of passwords in order to find the one that works best for gaining access to a computer. Obviously, changing passwords on a regular basis is a wonderful strategy to prevent this.

Any technical effort to change the normal behaviour of network connections and related systems in computer networking is referred to as hacking. A hacker is a person who participates in the act of hacking [9]. Historically, the term "hacking" was used to describe helpful, clever technical labour that was not necessarily related to computers. On the other hand, hacking and hackers are now most often associated with harmful programming attacks on the Internet and other networks.

3.1 CYBERCRIME AND SECURITY

Illegal behaviour using or involving the use of a computer, a computer network, or a networked device is referred to as cybercrime. Profit-driven cybercriminals or hackers are responsible for the majority of cybercrime, although not all. Cybercrime may be committed by individuals or organisations. .

3.2 THE MOST UP-TO-DATE INFORMATION ON CYBER SECURITY ISSUES

The most important security risks for corporations will be privacy and data theft. We now live in a world where all data is digitally stored. On social networking

sites, users may interact with friends and family in a safe setting. Cybercriminals will continue to attack social networking sites in order to gain personal information from ordinary people. New attacks against Android-based devices will be launched, although not on a large scale. Because tablets and smartphones share the same operating system, they will be infected with the same malware. Malware specimens for Macs will continue to increase, albeit at a far slower pace than for PCs. Users will be able to write programmes for almost any Windows-based device (PCs, tablets, and smartphones) with Windows 8, making it possible to construct malicious software comparable to that seen on Android devices.

4. RECENT CYBER SECURITY TRENDS SURVEY ISSUES

The following list was compiled as a result of cyber security research and polling.

4.1 Apps and Mobile Devices

The number of security vulnerabilities rises in lockstep with the number of mobile devices. Every new smartphone, tablet, or other mobile device provides another vulnerable access point to networks, allowing a cyberattack to take place. Criminals are fully aware of this nasty dynamic, and they are ready to strike with highly targeted malware and mobile app attacks. Similarly, the problem of lost and stolen devices will grow to include new and old technologies that cyber security planners were previously unaware of.

4.2 Networking on Social Media

The number of security vulnerabilities increases as the number of mobile devices rises. Every new smartphone, tablet, or other mobile device provides another vulnerable access point to networks, allowing a cyber attack to take place. Criminals are fully aware of this nasty dynamic, and they're ready to strike with highly targeted malware and mobile app attacks. Similarly, the problem of lost and stolen devices will expand to include new and old technologies that cyber security planners previously overlooked.

4.3 Computing on the Cloud

Businesses will increasingly adopt cloud computing. Businesses are shifting to the cloud because of the significant cost savings and efficiency it provides. Organizations with a well-designed architecture and operational security plan will be able to properly handle the dangers of cloud computing. Unfortunately, current studies and research suggest that when screening these providers, organisations underestimate the need of security due diligence. As the number of individuals who use the cloud expands in 2012, more breaches will highlight the challenges that these services confront when it comes to forensic

Social Media's Role in Cybersecurity: In today's world, interactive organisations must devise innovative methods for safeguarding personal information in an increasingly hostile environment. In terms of cyber security and personal cyber-attacks, social media is crucial.

Cyber-attacks against cyberspace may grow as a result of new techniques. Cybercriminals will continually change current malware signatures to take advantage of developing technology weaknesses. In other circumstances, they are truly interested in finding unique elements of new technology in order to find malware insertion holes. Cyber criminals are using contemporary Internet technologies and millions or billions of active users to get quick and simple access to a big number of people.

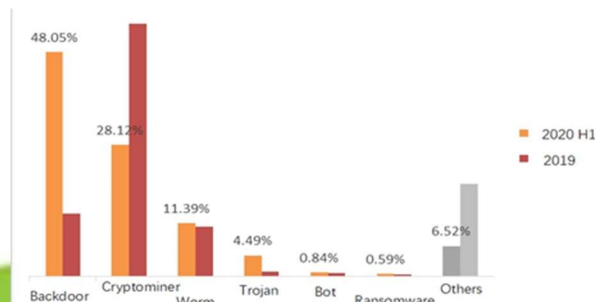
Keeping sensitive information safe with a login and password is a simple way to ensure privacy. This way of offering security is one of the most essential cyber security efforts.

It must be shown that the data comes from a trustworthy source that has not been tampered with before it is disseminated. A gift from a computer's anti-virus antivirus software is often used to verify these documents. It is more vital to protect equipment from viruses using publicly opposed virus software.

A software programme that scans all of a computer's files and papers for malicious code or viruses. Viruses, worms, and Trojan horses categorise and label examples of harmful software systems in this domain as malware.

A firewall is a piece of software or hardware that stops hackers, viruses, and worms from infiltrating your computer over the internet. .

The Role of Social Media in Cybersecurity: In today's world, interactive organisations must come up with new ways to protect personal information in a more difficult environment. Social media is critical in terms of cyber security and personal cyber-attacks.

[illegible]

Antivirus software and internet security programmes may help protect a programmable device against assault by identifying and deleting viruses. Although antivirus software was prevalent in the early days of the internet, as technology advanced, a range of free protection programmes were accessible.

n.d.) n.d.) n.d.) n.d.) n.d.) n.d.) n.d.) n.d.) n.d.) n.d.)
n.d.) n.d.) n.d. A password manager is a piece of software that organises and manages your passwords. Password managers often encrypt passwords and require the user to generate a master password. A master password is a single, preferably extremely strong password that grants access to the user's full password database.

Protective Suits:- Firewalls, anti-virus, anti-spyware, and other security utilities are included in security suites. Additionally, they provide complimentary theft prevention, safety checks of portable storage devices, private internet surfing, and other security-related services.

Certain online firms allow customers to use a six-digit security token that changes every 30-60 seconds. The keys on the token have performed calculations and adjusted numbers depending on the embedded time. This implies that every thirty seconds, there is only one potential sequence of digits that will allow you to access your online account.

7 FINAL REMARKS

Cybercrime has evolved into a significant, ubiquitous, aggressive, rapidly expanding, and more sophisticated threat to national and economic security. Numerous sectors, organisations, governments, and private-sector firms (especially those involved in essential infrastructure) face grave threats. For enterprises and governments alike, establishing a consistent cyber security posture will be critical for future development, innovation, and competitive advantage. By collaborating across public and private sector partnerships and advancing security measures, businesses can work toward a future environment that is both open and secure, as well as prosperous, particularly for mission-critical systems, processes, and applications that are connected to cyberspace.

REFERENCES

- [1] Derek Manky, Five Emerging Trends in Cyber Crime, December 4, 2018.
- [2] Sunit Belapure's Cyber Security: Understanding Cyber Crimes Nina Godbole is a model and actress.
- [3] Audrie Krause's Computer Security Practices in Nonprofit Organizations - A NetAction Report.
- [4] Md Liakat, Kutub Thakur, Md Liakat, Md Liakat, Md Liakat, Md Liakat, Md Liakat, Md Liakat, Md Liakat, Md Liakat, Md Liakat, Md Liakat
- [5] Cyber Security Challenges and Emerging Trends on Cutting-Edge Technologies- Dr.Prof. Rajasekharaiah K.M, Chhaya S Dule, Sudarshan, ICRAEM 2020Is Cyber Security Enough- A Study on Big Data Security Breaches in Financial Institutions
- [6] Nikita TresaCyriacLipsaSadath 2019 GLA University, Mathura, Uttar Pradesh, India, hosted the 4th International Conference on Information Systems and Computer Networks (ISCON). The dates are November 21-22, 2019.
- [7] An Overview Study on Internet Cybercrime- Journal of Information Engineering and Applications

Vol 2, No. 1, 2012 ISSN 2224-5782 (print) ISSN 2225-0506 (online)

[8] Ravi Sharma (nine) Ravi Sharma (nine) Ravi Sharma (n Examining the Most Recent Emerging Trends in Cyber Security and the Challenges They Pose to Society Volume 3, Issue 6, June 2012 ISSN 2229-5518 International Journal of Scientific and Engineering Research

[9] SuryakantYadav, VeenooUpadhyay Cyber Security Challenges and Emerging Trends: Current Technologies is a study of cyber security challenges and emerging trends. Volume 05, Issue 07, July 2018, International Journal of Engineering Research and Management (IJERM) ISSN: 2349-2058

[10] J. Li. Multi-firewall technology research and application in business network security. 9(5):153–162 in International Journal of Security and Its Applications, 2015.