Journal of Science, Computing and Engineering Research (JSCER)
Volume-3, Issue- 2, Mar - April 2022.
DOI: https://doi.org/10.46379/jscer.2022.030201

Emerging Trends in Cyber Crime and Safety

R.Shanthi prabha
Assistant Professor, Department Of Computer Science, Sri Adi Chunchanagiri Women's College, Cumbum, Tamilnadu.

Article Information

Received : February 10 2022
Revised : March 5 2022
Accepted : March 15 2022
Published : April 02 2022

Corresponding Author:
Amirhossein Jahromi
Email: amirhossein1121@gmail.com

Abstract— Cyber Security plays an important role in the field of information technology. In the present day to securing the information is biggest issue. Whenever we think about the cyber security the first thing that comes to our mind is cyber crimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: ***cyber security; cybercrime; cyber ethics; social media; cyber stalking; cloud computing; android apps.***

Citation: R.Shanthi prabha "Emerging Trends in Cyber Crime and Safety", Journal of Science, Computing and Engineering Research, 3(2),237-240, 2022.

I. INTRODUCTION

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes. In the field of technology, cyber security has a significant role, and the security data become one between the most critical problems faced in today's world. When there is discussion regarding the cyber-crimes which are increasing very rapidly, the government and many corporations are having many measures so as for stopping these kinds of crimes. Inspire of many different steps, cybercrime is still increasing day by day. In this study, there is brief coverage over the challenges faced by the cyber security from new technology advancement and innovations and in addition to this, the paper also has its main focus on the latest cyber security techniques, trends and other ethics involved in the sector of cyber security.

Figure 1: Cyber Crime

II. CYBER STALKING

Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person,

appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

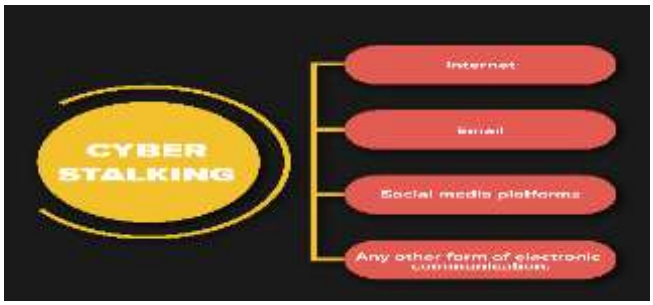

Figure 2: Cyber Stalking

Cyber stalking is a technologically-based "attack" on one person who has been targeted specifically for that attack for reasons of anger, revenge or control. Cyber stalking can take many forms, including:

- harassment, embarrassment and humiliation of the victim
- emptying bank accounts or other economic control such as ruining the victim's credit score
- harassing family, friends and employers to isolate the victim

The term can also apply to a "traditional" stalker who uses technology to trace and locate their victim and their movements more easily (e.g. using Facebook notifications to know what party they are attending). A true cyber stalker's intent is to harm their intended victim using the anonymity and untraceable distance of technology. In many situations, the victims never discover the identity of the cyber stalkers who hurt them, despite their lives being completely upended by the perpetrator.

A. Hacking

"Hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37 per cent increase this year. A case of suspected hacking of certain web portals and obtaining the residential addresses from the e-mail accounts of city residents had recently come to light. Crackers are people who try to gain unauthorised access to computers. This is normally done through the use of a 'backdoor' program installed on your machine. A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer. Obviously, a good protection from this is to change passwords regularly.

In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking [9]. The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on the Internet and other networks.

B. Cyber Crime And Security

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

C. Latest On Cyber Security Issues

Privacy and data theft will be the top security issues that organizations need to focus. We live in a world where all information is in digital form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. There will be new attacks on Android operating system based devices, but it will not be on a massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android.

III. RECENT SURVEY ISSUES ON CYBER SECURITY TRENDS

The following list was developed from cyber security research and survey.

A. Mobile Devices and Apps

The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber attack, as each creates another vulnerable access point to networks. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning.

B. Social Media Networking

Growing use of social media will contribute to personal cyber threats. Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

C. Cloud Computing

More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

D. Protect systems rather Information

The emphasis will be on protecting information, not just systems. As consumers and businesses are like move to store more and more of their important information online, the requirements for security will go beyond simply managing systems to protecting the data these systems house. Rather than focusing on developing processes for protecting the systems that house information, more granular control will be demanded - by users and by companies - to protect the data stored therein.

E. New Platforms and Devices

New platforms and new devices will create new opportunities for cybercriminals. Security threats have long been associated with personal computers running Windows. But the proliferation of new platforms and new devices - the iPhone, the iPad, Android, for example - will likely create new threats. The Android phone saw its first Trojan this summer, and reports continue with malicious apps and spyware, and not just on Android.

F. Everything Physical can be Digital

The written notes on a piece of paper, the report binder and even the pictures on the wall can be copied in digital format and gleaned for the tools to allow a activist-type of security violation, and increasingly this will be a problem.

IV. SPECIFIC CYBER SECURITY TECHNOLOGIES

Cyber-attacks on cyberspace can grow by capitalizing on new techniques. Cybercriminals will most frequently change the current malware signatures to take advantage of new technical faults. In other instances, they actually search for special features of emerging technology to detect weaknesses in malware injection. Cyber criminals are taking advantage of emerging Internet technology and millions and billions of active users to access a huge amount of people easily and effectively using these new technologies.

Access Control and Password Security: Security provided by the means of username and password is a simple way of providing security for the private information to preserve privacy. This means of providing security is one of the most critical cyber security initiatives.

Authentication of Data: Until the transmitted information need to be attested that it has come from a reputable supply that was not changed. These documents are often authenticated using a gift from the opposing virus software package inside computers. An honestly opposed virus software package is more essential to protect devices from viruses.

Malware Scanners: A software system which sometimes scans all files and documents for malicious code or harmful viruses inside the system. The samples of malicious software systems in this field are generally sorting and noted as malware by viruses, worms, and the Trojan horses.

Firewall: Firewall is a software or hardware package which helps separate hackers, viruses and worms trying to access your PC through the web .The firewall checks all messages that come in and blocks those that fail to meet the security requirements compatible with all messages .Firewalls plays a very vital role in malware detection.

Role of Social Media in Cyber Security: In recent modern world, there is a need of interactive businesses which needs to find new ways to secure personal information in more entangled environment. Social media has important role to play in cyber security and in personal cyber-attacks. Adoption of social media among employees is growing and threat of attack is therefore increasing since most of them nearly use social media or social networking sites everyday it is now a massive forum for cyber criminals to hack private information ICRAEM 2020 IOP Conf. Series: Materials Science and Engineering 981 (2020) 022062 IOP Publishing doi:10.1088/1757-899X/981/2/022062 5 and steal valued information. In recent days, it's very easy to share personal information easily and businesses must make sure that recognise, react in real time and prevent breaches of any kind as quickly as possible. These social media has easily make people to share their private information and hackers can use these information. Therefore, people have to take reasonable steps to avoid misuse and loss of their information through these social media.

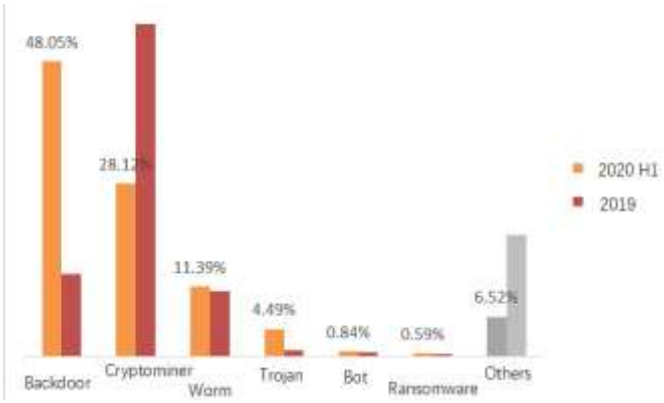

Figure 3: Cyber Security issues in Social Media

V. INTERNET SECURITY PRODUCTS

a) Antivirus

Antivirus software and internet security programs are able to project a programmable device from attack by detecting and eliminating the viruses. Antivirus software was used in the early years of internet but now with the development several free security applications are available on internet.

b) Password Managers

The password managers is a software application that is used to store and organize the passwords. Password managers usually store passwords encrypted, requiring the person to create a master password; a single, ideally a very strong password which allows the user access to their entire password database.

c) Security Suits

The security suits contains the suits of firewalls, anti-virus, anti-spyware and many more. They also gives the theft protection, portable storage device safety check, private internet browsing or make security related decisions and are free of charge.

d) Security Tokens

Some online sites offers the users the ability to use the six digit code which randomly changes after every 30-60 seconds on a security token. The keys on the token have built computations and manipulated numbers based on the current time built into the device. This means that after every thirty

seconds there is only a certain sequence of numbers possible which would be correct to access to the online account.

VI. CONCLUSION

Cyber crime is now serious, widespread, aggressive, growing, and increasingly sophisticated, and poses major implications for national and economic security. Many industries, institutions, public- and private-sector organizations (particularly those within the critical infrastructure) are at significant risk. For businesses and governments alike, getting the Cyber Security posture right across all its elements will be vital for future growth, innovation and competitive advantage. There is no single answer for success, but by working across public and private sector partnerships and by advancing security measures particularly with regard to mission-critical systems, processes and applications that are connected into cyberspace, businesses will be able to work towards a future environment that is both open and secure and prosperous.

REFERENCES

[1]. Five Emerging trends in Cyber Crime- Derek Manky, December 4, 2018.
[2]. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole.
[3]. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
[4]. Challenges of Cyber security and the Emerging Trends-Md Liakat, Kutub Thakur, July 02, 2019.
[5]. Cyber Security Challenges and its Emerging Trends on Latest Technologies- Dr.Prof. Rajasekharaiah K.M , Chhaya S Dule ,Sudarshan , ICRAEM 2020.
[6]. Nikita TresaCyriacLipsaSadath Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions 2019 4th International Conference on Information Systems and Computer Networks (ISCON) GLA University, Mathura, UP, India. Nov 21-22, 2019.
[7]. An Overview Study on Cyber crimes in Internet- Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.1, 2012.
[8]. Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.
[9]. VeenooUpadhyay, SuryakantYadav Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018.
[10]. J. Li. The research and application of multi-firewall technology in enterprise network security. Int'l J. of Security and Its Applications, 9(5):153–162,2015.