Cyber Security & it's Emerging Trends & Techniques

Sanjivani Bhumiraj Raut

Student, M.Sc IT, Keraleeya Samajam (Regd.) Dombivli's Model College, Maharashtra, India

Abstract – Cyber Security plays an important role in data technology .Securing data is becoming a challenging task. We have a tendency to expect relating to the cyber security the first issue that involves our mind is 'cyber crimes' that are increasing immensely day by day. Varied Governments and companies are taking many measures thus on stop these cyber crimes. Besides varied measures cyber security continues to be a awfully large concern to many. The topic of cyber security is one that ought to be talked concerning a lot of usually in today's society. This paper tells the importance of cyber security and spreads the awareness amongst everyone. This paper primarily focuses on challenges faced by cyber security on the foremost recent technologies .It along focuses on latest about the cyber security techniques, ethics and to boot additionally the trends dynamic the face of cyber security.

Key Words: Cyber Security, Cyber Crime, Cyber ethics

1. INTRODUCTION

Today, because of the fashionable life individuals have joined technology life. At the same time, safeguarding of data has become progressively troublesome. Additionally, the heavy use and growth of social media, on-line crime or law-breaking has enhanced. Within the world of information technology, knowledge security plays a big role. The data security has become one in every of today's main challenges. Whenever we predict of cyber security, we tend to initial of all think of 'cybercrimes,' that expand enormously on a daily basis. Completely different government and businesses take varied steps to avoid this manner of law-breaking. Additionally to varied cyber protection initiatives, many folks also are terribly upset concerning it.

Today man is in a position to send associated with variety of information could also send an e-mail or an audio or video simply by the press of a single button but did he ever assume however firmly his information is being transmitted or sent to the opposite person safely ? The solution lies in cyber security. Nowadays web is that the quickest growing infrastructure in a day life. However because of these rising technologies we are unable to safeguard our non-public info in an exceedingly very effective means and thus currently cyber crimes are increasing day by day. Nowadays quite sixty percent of total business transactions are done on-line; therefore this field needed a prime quality of security for clear and best transactions. The scope of cyber security isn't simply restricted to securing the data in IT business however to varied alternative fields [5] .

2. WHT IS CYBER CRIME?

Cybercrime is any criminal activity that involves a pc, networked device or a network. While most cybercrimes area unit disbursed so as to get profit for the cybercriminals, some cybercrimes area unit disbursed against computers or devices on to injury or disables them. Others use computers or networks to unfold malware, unlawful data, pictures or different materials. Some cybercrimes do each -- i.e., target computers to infect them with a worm, that is then unfold to different machines and, sometimes, entire networks [1].

Most crime is Associate in an attack on data concerning people, firms, or governments. though the attacks don't present itself on a figure, they are doing present itself on the private or company virtual body, that is that the set of informational attributes that outline folks and establishments on the net. In alternative words, within the digital age our virtual identities are essential parts of everyday life: we have a tendency to be a bundle of numbers and identifiers in multiple laptop databases closely-held by governments and firms. Crime highlights the spatial relation of networked computers in our lives, moreover because the fragility of such on the face of it solid facts as individual identity [2].

3. VARIOUS TYPES OF CYBER CRIMES

1) Cyber Extortion

A crime involving a requirement for cash to prevent the attack. One sort of cyber extortion is that the ransomware attack. Here, the assaulter gains access to organization's systems and encrypts its documents and files, something of potential price, creating the information inaccessible till a ransom is paid. Usually, this can be in some sort of crypto currency, like bit coin.

2) CryptoJacking

An attack that uses scripts to mine crypto currencies inside browsers whiles not the user's consent. Crypto jacking attacks could involve loading crypto currency mining software package to the victim's system. However, several attacks rely on JavaScript code that will in-browser mining if the user's browser encompasses a tab or window open on the malicious website. No malware must be put in as loading the affected page executes the in-browser mining code [1].

3) Identity Theft

An attack that happens once a private accesses a laptop to reap a user's personal info, which they then use to steal that person's identity or access their valuable accounts, like banking and credit cards. Cybercriminals get and sell identity info on dark net markets, giving monetary accounts, likewise as different varieties of accounts, like video streaming services, webmail, video and audio streaming, on-line auctions and additional. Personal health info is another frequent target for identity thieves [3].

4) Frauds

An attack that happens once hackers infiltrate retailers' systems to urge the credit cards or banking information of their customers. Taken payment cards are often bought and sold in bulk on dark net markets, wherever hacking teams that have taken mass quantities of MasterCard profit by marketing to lower-level cybercriminals

5) Software Piracy

An attack that involves the unlawful repeating, distribution and use of package programs with the intention of business or personal use. Trademark violations, copyright infringements and patent violations square measure usually related to this kind of crime.

4. WHAT IS CYBER SECURITY?

Cyber security is the method of defending computers, devices, electronic systems, networks, and information from malicious attacks. These cyber attacks sometimes geared toward accessing, changing, or destroying sensitive information; extorting cash from users; or interrupting traditional business processes [3].

Implementing effective cyber security measures is especially difficult these days as a result of, a lot of devices than folks, and attackers are getting a lot of innovative. The term applies in an exceedingly type of contexts, from business to mobile computing, and might be divided into many common classes.

- Network security is securing an electronic network from intruders, whether or not targeted attackers or opportunist malware.

- Application security focuses on keeping code and devices freed from threats. A compromised application might offer access to the info it's designed to safeguard. Triple-crown security begins within the style stage, well before a program or device is deployed.

- Data security protects the integrity and privacy of information, each in storage and in transit.

- Operational security includes the processes and choices for handling and protective information assets. Information could also be keeping or shared all represent this umbrella.

- Disaster recovery and business continuity outline however a corporation responds to a cyber-security incident or the other event that causes the loss of operations or information. Disaster recovery policies dictate however the organization restores its operations and data to come to constant operative capability as before the event. Business continuity is that the set up the organization falls back on whereas attempting to control while not bound resources.

- End-user education - Addresses the foremost unpredictable cyber-security factor: folks. Anyone will accidentally introduce a plague to associate otherwise secure system by failing to follow smart security practices. Teaching users to delete suspicious email attachments not infix unidentified USB drives, and varied alternative necessary lessons is significant for the safety of any organization.

5. AWARENESS

Most individuals don't realize all of those scams happening to them .Thanks to this, individuals don't acumen to shield themselves and the way to prevent being a target. It's necessary that we tend to, as a nation; specialize in creating these people attentive to the potential risks related to the net. Cyber security must be additional general knowledge and education must be additional without delay accessible. It's necessary for us to assist educate people on what they will do to prevent and forestall potential cyber security attacks.

We log into our email account, checking account, or social media account and that we don't even suppose the method. These area unit the categories of activities that hacker's create a living off of. The bulk of individuals aren't solely unaware that cyber threats area unit real, however also are unaware of what to try to concerning them. Most of the people simply hope or assume that fraud and phishing attacks aren't about to happen to them. But, creating society aware that even the tiniest tasks will create potential threats is crucial for his or her safety.

Awareness is that the commencement in reducing the quantity of identity thefts and private info threats. The bulk of people perceive that by having their personal info on-line that they're taking a risk of that info being compromised. However, they are doing not possess the data to understand the way to shield themselves. These folks conjointly

Understand that they must not embrace terribly sensitive info on-line, like their social insurance numbers. Yet, they are doing not notice that even accessing your email might be even as harmful to their safety.

Individuals believe that if they need a singular positive identification then they're protective themselves enough that they are doing not have to be compelled to worry concerning cyber security threats. Whereas this can be an honest commencement, and it's powerfully suggested to form distinctive passwords, it still merely isn't enough to stay info personal. Most hackers have the technology and data to understand the way to decode these passwords or bypass them fully. Day by day that our technology is up is another day that hackers area unit determining the way to crack that technology.

Likewise, a lot of the population believes that putting in virus protection or spy package onto their computers is enough. They suppose that this package goes to avoid wasting them from ever being hacked or having their data purloined this can be conjointly merely not true. We want to vary this fashion of thinking by serving to society acknowledge the signs of the potential threats and risks. We tend to then got to hand them the knowledge that they have to stay themselves safe and guarded. A number of the signs that users got to remember of that typically indicate a phishing try are: words being misspelled, an exact degree of urgency or "deadlines", pretend names and net links, and missive of invitation for private data.

6. TRENDS CHANGING CYBER SECURITY

Over the last 20 years, organizations have doubled down on cyber security investments and it's no marvel why: From pricey knowledge breaches to paralyzing malicious attacks, businesses area unit sport to stay pace with the evolving complexness and class of cyber threats. In addition to new technology, organizations additionally face new cyber security challenges within the face of the COVID-19 pandemic. per Cisco's way forward for Secure Remote Work Report, sixty one % of survey respondents according that their organizations veteran a rise in cyber threats of over twenty five % .

Below are the seven raising trends within the cyber security field to remember.

1) New Technologies and Devices :

One issue is that the increase in new technologies and new devices. By 2027, Business executive predicts that quite forty one billion web of Things (IoT) devices are going to be on-line and connected. The IoT business has become a major target for cybercriminals and has sent device manufacturers scrambling to safeguard their sensible plugs, wearable fitness devices, and baby monitors from attacks.

2) Increasing Ransom ware Attacks

Monetization is another key issue causative to the increase in cyber attacks. Within the past, it had been tough for cybercriminals to make the most of attacks, however that has since modified. Now, cybercriminals have progressively turned to ransomware attacks, or those during which attackers gain access to and cipher a victim's knowledge and demand a ransom.

Crypto currencies and therefore the emergence of ransomware have created it easier for somebody to commit against the law and obtain away with it as a result of they'll get paid in untraceable ways.

This trend has impelled attackers to commit cybercrimes in pursuit of financial gain whereas at the same time creating it tougher to trace and determine these criminals.

3) Attacks on Cloud Services

In recent years, several businesses have adopted cloud-based computing services that alter users to access code applications, information storage, and alternative services via a web affiliation instead of counting on physical infrastructure. Hold this technology comes with several advantages like reduced operational prices and exaggerated potency.

Although choosing such systems will be extremely helpful to organizations, they need additionally become the target of cyber threats. If these systems aren't properly designed or maintained, attackers are additional possible to be ready to exploit vulnerabilities within the systems' security and gain access to sensitive data. This can be significantly vital, seeing that several of today's organizations have faith in cloud services as workers work remotely.

4) Outdated and inefficient Systems

Businesses increase the danger of attack or breach by connecting inheritance systems. Once IT implements patchwork solutions to resolve operational problems, security vulnerabilities will be created unwittingly.

As cyber attacks have become more and more, these superannuated and inefficient systems become simple targets.

This fast evolution of cyber security threats suggests that professionals within the field and those desirous to be part of them need to be up-to-date on the most recent skills, strategies, and job opportunities so as to stay competitive.

5) Remote Work Risks

The COVID-19 pandemic has lead to an enormous increase in remote staff worldwide, and remote work is here. Sadly, this contributes to associate hyperbolic risk of cyber threats for several organizations.

In the age of remote work, cybercriminals are taking advantage of misconfigured cloud security measures and insecure home devices and networks. Remote staffs are typically the target of phishing makes an attempt by email, voice, text, and third-party applications.

Because of these threats, there's associate increasing demand for cyber security professionals.

6) Continued Use of Multifactor Authentication

Many firms have combined the employment of passwords with multi-factor authentication (MFA) as an extra layer of protection against information breaches and alternative cyber attacks. Multifactor authentication, users ought to use 2 or a lot of devices to verify their identities.

While Master of Fine Arts may be an extremely effective thanks to secure accounts and forestall attacks, cybercriminals can be able to bypass sure forms of authentication.

7) Increased Interest in data Privacy

There are increasing considerations concerning information privacy within the world of cyber security, each within the context of shopper and company data. There square measure numerous federal, state-level, and international information privacy laws that today's organizations ought to go with, and customers are turning into a lot of involved with however their information is being employed.

Data breaches and cyber attacks expose sensitive personal data and place customers and firms in danger. Today's organizations ought to take into account things like encryption, secret protection, and network security to strengthen their information privacy. It's additionally necessary that companies have a team of extremely adept cyber security professionals operating to secure their information and shield against probably devastating information breaches.

7. CYBER SECURITY TECHNIQUES

1) Keep Your Software Up to date

As we have seen the increase in number of ransomware attacks, ransomware attacks were a significant attack vector for each businesses and customers. One in every of the foremost necessary cyber security tips to mitigate ransomware is fix out-of-date code, each software, and applications. This helps take away important vulnerabilities that hackers use to access your devices. Here are a couple of fast tips to urge you started [6].

- Turn on automatic system updates for your device
- Make sure your desktop applications program uses automatic security updates
- Keep your applications program plugging like Flash, Java, etc. updated

2) Use Antivirus Protection

Anti-virus (AV) protection package has been the foremost current answer to fight malicious attacks. Av package blocks malware and different malicious viruses from coming into your device and compromising your knowledge. Use anti-virus package from sure vendors and solely run one Av tool on your device.

Using a firewall is additionally vital once defensive your knowledge against malicious attacks. A firewall helps sort hackers, viruses, and different malicious activity that happens over the net and determines what traffic is allowed to enter your device. Windows and raincoat OS X comes with their individual firewalls, capably named Windows Firewall and raincoat Firewall. Your router ought to even have a firewall in-built to forestall attacks on your network.

3) Use Strong Password

You've in all probability detected that sturdy passwords are vital to on-line security. The reality is countersigns are vital to keep hackers out of your data! Consistent with the National Institute of Standards and Technology's (NIST) 2017 new password policy framework, you must consider:

Dropping the crazy, advanced mixture of character letters, symbols, and numbers. Instead, take one thing a lot of easy however with a minimum of eight characters and a most length of sixty four characters.

- Don't use a similar countersign double.
- The countersign ought to contain a minimum of one minuscule letter, one uppercase letter, one number, and 4 symbols however not the subsequent &%#@_.

  Choose one thing that's simple to recollect and ne'er leave a countersign hint go in the open or create it in public out there for hackers to visualize.
- Reset your countersign after you forget it. But, modification it once each year as a general refresh.

4) Use Multi Factor Authentication Method

Two-factor or multi-factor authentication is a service that adds additional layers of security like a personal identification code, another password or even a fingerprint. With multi-factor authentication, you will be prompted to enter more than two additional authentication methods after entering your username and password.

5) Learn about Phishing Scams – be very suspicious of emails, phone calls, and flyers

During a phishing attempt, the attacker pretends to be someone or something that the sender should not deceive into disclosing their credentials, clicking on a malicious link, or opening an attachment that infects user's system with malware, Trojans or zero day vulnerability exploit. Often leads to a ransomware attack. In fact, 90% of ransomware attacks come from phishing attempts.

Here are some important cyber security tips to remember about phishing scams:

- Don't open emails from people you don't know
- Know which links are safe and which aren't: Skip it mouse over a link to see where it goes to.
- Beware of emails sent to you in general: see where they are coming from and if there are any grammatical errors
  Malicious links can also come from friends who have been infected. So, be very careful!

6) Protect Your Sensitive Personal Identifiable Information (PII)

Personal data (PII) is any information that may be utilized by a cybercriminal to spot or find an individual. PII embraces information appreciate name, address, phone numbers, information of birth, social insurance Number, information processing address, location details, or the other physical or digital identity data. Your master card information should be protected.

Within the new “always-on” world of social media, you ought to be terribly cautious regarding the knowledge you include online. It’s counseled that you simply solely show the very minimum about yourself on social media. Contemplate reviewing your privacy settings across all of your social media accounts, particularly Facebook. Hackers use this information to their advantage!

7) Use Your Mobile Devices Securely

According to McAfee Labs, your mobile device is currently a target to quite 1.5 million new incidents of mobile malware. Here are some fast tips for mobile device security:

- produce a troublesome Mobile Pass code – Not Your Birth date or Bank PIN
- Install Apps from trusty Sources
- Keep Your Device Updated – Hackers Use Vulnerabilities in Unpatched Older operative Systems
- Avoid causing PII or sensitive info over text message or email.

8. CYBER ETHICS

Internet morals imply satisfactory conduct for utilizing Web. The term "cyber morals" alludes to a set of ethical rules or a code of conduct connected to the online environment. As a dependable netizen, you ought to watch these rules to assist make the internet a secure put [5].

1. We ought to be genuine, regard the rights and property of others on the Internet.
2. Do not utilize a computer to hurt other people.
3. Do not meddle with other people's computer work.
4. Do not snoop around in other people's computer files.
5. Do not utilize a computer to steal.
6. Do not utilize a computer to bear untrue witness.
7. Do not duplicate or utilize exclusive computer program for which you have got not paid (without permission).
8. Do not utilize other people's computer assets without authorization or legitimate compensation.
9. Do not fitting other people's mental output.
10. Do not think around the social results of the program you're composing or the framework you're designing.
11. Do not continuously utilize a computer in ways that guarantee thought and regard for other people.

9. CONCLUSION

Computer security may be a endless theme that's getting to be more critical since the world is getting to be exceedingly interconnected, with systems being utilized to carry out basic exchanges. Cyber wrongdoing proceeds to wander down distinctive ways with each Unused Year that passes and so does the security of the data. The most recent and troublesome advances, in conjunction with the modern cyber apparatuses and dangers that come to light each day, are challenging organizations with not as it were how they secure their foundation, but how they require unused stages and intelligence to do so. There's no culminate arrangement for cyber violations but we ought to attempt our level best to play down them in arrange to have a secure and secure future in cyber space.

Cyber security awareness is more important presently than it has ever been some time recently. Dangers to individual data are expanding and personalities are getting stolen each day. Making people mindful of usually the primary step. The moment step is giving people the apparatuses and information that they need to protect themselves.

10. ACKNOWLEDGEMENT

I am over helmed all told humbleness and thankfulness to acknowledge my depth to any or all those that have helped me to place these concepts, well on top of the amount of simplicity and into one thing concrete.

I would like to express my special thanks of gratitude to Asst.Prof.Jyoti Samel who gave me the golden opportunity to do this wonderful research on the topic "Cyber security and its emerging trends and techniques", which also helped me in doing a lot of Research and I came to know about so many new things. I am really thankful to her. I express my deepest gratitude towards our research paper guide for her valuable and timely advice during the phases in research. I would like to thank her for providing all the facilities and support as the co-coordinator.

Any try at any level can't be satisfactorily completed while not the support and steering of my oldsters and friends helped me in gathering totally different info, aggregation information and guiding me from time to time in making this

11. REFERENCES

[1] Cybercrime by Kate Brush
[2] Cybercrime law by Michael Aaron Dennis
[3] What is Cyber Security? By "Wikipedia"
[4] Emerging trends in Cyber Security by Kristen Burnham
[5] A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies by Nikhita Reddy Gade and Ugander G J Reddy Article February 2014
[6] Cyber security techniques, by Cipher