CYBERCRIME AND SECURITY

Yashwanth A S[1]

INTRODUCTION

Computer or Cyber Crime, which includes or any crime involves that a computer or any network. The pc may be utilized against the law, or it will be going to be targeted. Cyber-crime has emerged as new segregation of crimes, which is rapidly increasing because of extensive use of the web and technology services. Maximum of the Cyber-crime cases are finding of 46%, which were associated with cyber pornography and followed by the hacking of different set of online transactions which takes place in the laptops or the mobiles. In such cases, 60% of offenders are aged between 18 to 30 years of age group.

The term ‘Cyber Security’ is also defined as “to the practice of protecting the pc systems, networks, and programs from digital, virtual, or any varieties of attacks.” The cyber-attacks will tend to access, change, or perhaps destroy sensitive or personal information to the extent of doing away with money from users of a computer, laptop, or any device like mobiles.

It is necessary to adopt the effective cybersecurity measures by a person or by the group or any institutions or the offices and management, etc. considering that the innovations the cyber-attacks, and therefore the upward graph of technology and its tools today. Internet usage in India these days has grown rapidly and relentlessly. It has been given new opportunities for those in every field who seeking fraudulence in every field like entertainment, business, sports, or education.

The coin has two faces in it. The Internet is also having its disadvantages as cybercrime or criminality committing day by day through the internet. It found that the kinds of domains most ordinarily impersonated for malicious purposes relate to the foremost profitable companies worldwide, like search engines which are in the mainstream and the social media, usage of financial transactions, shopping online, and paying through banking or online payment websites. The first purpose is to launch phishing attacks and scams on users to steal credentials or money.

[1] LLB (3 YEARS), DR. RML COLLEGE OF LAW, BANGALORE.

Cyber-squatting is when domain names are registered that try and trick users into believing they're associated with existing brands, typically by intentionally misspelling variants of their names.

Whilst not always finished malicious intent, many of those domains pose a cyber-risk to visitors, and also the practice is illegitimate within the US. Internet protection has a much greater domain for concern not only for American people but for other governments also.

The sabotage of the Internet can be taken as an example. It is a reprehension for many officials who work for the public and also for of the experts in cybersecurity as they are facing likely threatening, for several deskbound office workers, it might be a little bit of a day's excitement. Popular resistance on a greater front is the participation of government in cybersecurity shows the indistinguishable tension that is there within the real world.

In India, Cyber awareness yet to be created in huge to the public, especially for the students and the persons[2] who are using the internet service for daily use from any devices like computer, laptop, or mobile for different purposes like internet banking, paying off the fees, and using the same for different perspectives which are in the possible ways have to be secured and thoroughly knowledge use of the internet.

DIFFERENT CYBER CRIMES

- Denial of Service attack
- Hacking
- Virus Dissemination
- Computer Vandalism
- Cyber Terrorism
- Software Piracy
- Denial of Service Attack: It is an attack that leads to the bandwidth of a victim's network. It is like depriving a victim of using their e-mail by filling it with spam mail and thus disrupting his service.
- Hacking: It refers to an illegal disruption in any particular computer and/or in any network that is being used by any individuals, groups, or by different departments.

[2] Cyber Sabotage means and can be deliberated as an act which can be result in a malicious disruption of particular processes and functions has been damaged of an equipment or information.

- Virus Dissemination: The software which attaches is called Malicious and it is causing other software by downloading any attachments received by mail (Virus, worms, bug, web hacking, e-mail booming, etc.)
- Computer Vandalism: It is like damaging or destroying the data which particularly to the concerned victim rather than stealing and transmitting the virus.
- Cyber Terrorism: It is like an Internet-based attack in which terrorists have been done for their activities.
- Software Privacy: Theft of a particular software through unanimous copying or illegal usage of genuine software programs that are not available for free.

CYBER CRIMINALS

- Hackers
- Crackers.
- Insiders
- Virus Writers.
- Cyber Terrorism.
- Hackers: Persons who intend to attain unauthorized access to a particular automatic data processing system or any Social Media Accounts like Facebook, Instagram, etc.
- Crackers: A Hacker with a Criminal intent who sabotage computers, steal information located on secure machines, and cause disruption.
- Insiders: A disgruntled insider of an Organisation who unauthorizedly reveals the info to the outsiders of a company.
- Virus Writers: those that code virus programs and distribute them via the internet causing malicious damage to host systems.
- Cyber Terrorism: The one nation which is politically motivated to use internet technology that is causing severe disruptions during a society or particularly against a country.

FURTHER INTERFERENCE

The system which is called critical infrastructure is by the executive level which is involving and enlisting the private and public companies who run the nation's business-like energy sector, transport and courier service, communication, and medical services to assist improve the safety of a system on which all the sectors can depend upon. The services provided by them are very decisive, as the supposition goes because they are not only important for the economy but also for the defence of our nation.

Therefore, there are high chances of them being seen as targets due to interconnections, and the security of internet users is very low which can be easily disrupted by terrorists or by fed-up employees, and even by spies. This threat which can lead to so many problems has not been yet materialized in such a way which is on raising the public alarm and indicate by the warning given by the Government.

Attacks the last February that finishes off e-commerce sites such as Yahoo, eBay, and many other famous websites showed the vulnerability of our systems which shows that there exists economic harm to a much greater extent than security. After arresting some it is seen like well-recognized quiet attackers, and a teenage hacker phenome in his house basement will be liable for taking down a minimum of one among the sites.

The threat that the governing body is worried about, disabling the same or hampering any particular serious service information, is nevertheless appearing as a distant thing. The information which might lead to any harm appears yet again to possess calmed to the public as fears.

However, hacking is becoming malicious as and intent within the 1970s as a phenome as to be referred phreaking, is the technology loop for people who sought to subvert as they have early access to computerized phone systems.

Law enforcement is facing a difficulty like the above mentioned criminal activity, is partially facing legislation by the lack to help as action at law, the skilled investigators are very shortage within the cyber development which is being lacked. All these types of events are making it transparent that the structure is being hospitable to the criminal activity because it became more and more sophisticated, crime is being made easy.

CYBERSECURITY AND SOCIAL MEDIA

Social media connects us with our friends and families, associates, etc. What we put upon it may end up getting circulated. Despite the security provisions made by various social media platforms, people who want to breach our social handles often find a way to do the same.

Losing our private and vital information to someone who is a stranger can prove to be as damaging as losing our bank account details, and that is why it is important to fully understand cybersecurity for social media. Social media is now an integral part of our everyday living. We use it to keep in touch with our friends and family, share photos and videos of all those things happening in our lives.

It has replaced phone calls, messages, emails, etc. for a lot of us. But, as with anything else online, all of us need to be aware of the risks. The prevalence of social media platforms and the anonymity of their users have paved a way for hackers and other people who want to get unauthorized access to our private accounts, commit cyber-crimes. The internet provides us with access to everything, but it is important to remember that it also provides everyone accesses to us. Therefore, it is necessary to protect oneself from the malicious activities that happen on the web.

THE CYBERCRIME STATE TODAY

In a recent survey which has been made in the US State of Cybercrime, 3 out of the 4 respondents have been detecting in a security event everyday life during last 12 months, yet at the different identical time and different level, still the organizations are reporting that they are stricken off by technology debt and the estimated budget to approximately exceed 1 trillion dollars. It is like the businesses are efficiently using their budget on technology as they are making innovations and they are providing Information Technology as an infrastructure to the new age without any desuetude but they are not able to provide effective security measures.

Common lackings of security are found in an organization and mostly these lead to cybercrimes such as:

- Spending on cybersecurity by an organization without planning.
- Third-Party providers need not give any assessments of their safety capabilities.
- There is a very low capacity of understanding and an assessment of the supply-chain taking risks which are offered through phishing emails.
- Inadequate or non-existent management of the mobile device and its security.
- The threat by an insider and the risk has not been adequately looked upon.

- Thorough knowledge is a lack of employee awareness and security, the training has to be given at every level of an organization.

Cybercrime is today's world is not only limited to computer systems or laptops only; Mobile devices have to face problems like virus attacks, malware of the software, and phishing scams. Thanks to the wide arena for Android phone users which have become home for the spread of a particular type of malware.

In a study which was done recently, among the OS apps 72% were thought to be suspicious, unnecessarily present, or benevolent, with Trojans leading to the bulk of threats.

SAFETY MEASURES

- Change the Passwords every 15 days.
- Don't keep one password to several apps, use different passwords.
- Keep changing Debit/Credit Passwords regularly.
- Activate the two Factor Verification within the email, WhatsApp, and the other apps which allow you to activate the identical.
- Don't share the OTP, ATM Pins, and Email Passwords with anyone.
- Do not share any personal photos on any Social Media Platforms, it has been causing a new way of Cyber-crime and harassing people.
- Do not post personal details within the Social Media, if needed, anybody can give the main points within the Messenger app if you do not have the Email or telephone number of someone.
- Use the Faraday Bag or Faraday Wallets to avoid the probabilities for a cyber-crime.
- Avoid the usage of Public Wi-Fi to avoid Cyber Crimes. It should easily cause crime because not a secured one and might take any details from the mobile especially the Banking Apps within the mobile, User ID, and Password of the other apps.

CONCLUSION

Therefore it is necessary to want care of one's security on the web. it's going to be done through following certain precautions and techniques like reviewing the browser setting and confirming that it is not storing and sharing user's direction, using incognito browsing to shield oneself from harmful web data and cache, employing a verified and authentic program, not storing the financial information on any online unverified online platform, not using malicious websites, using VPN to safeguard the privacy of the user, employing a vigorous firewall to shield oneself against viruses and malware, and consulting appropriate authorities when anything suspicious happens online. The internet provides us with access to everything, but it is important to remember that it also provides everyone accesses to us.

Therefore, it is necessary to safeguard oneself from malicious activities that happen online. All the issues which have been discussed above are put together under one roof of protection for privacy. But, when cases related to cyber-crime are referred, really care must be taken to achieve privacy protection. To ensure effective personal privacy for every commercial use which is done online can bring more and better use of identical software technologies which leads to the creation of threat within the primary stage more than on laws formed by Governments newly.

Further, what we call is calling as the threat, in reality, is Internet monitoring or powers which created have risen due to some of the provisions in different cases of cyber-crime which might be thought as good due to the advancement in technology and it also protects e-privacy.

MSPs must confirm the right backup and systems that recover are in the same place and servers at the endpoints of the user should not even be thought of to be reached if there is any kind of cyber-attack also. In downline, it can wipe out a particular institution and can cause harm to its reputation still because the client of MSP, thus systems must be prepared for security which can easily be backed up in any case if a user by mistake gets into trap.

SMBs have been increasingly looking into the MSPs these days as a tool for fighting cybercrime for which it will be targetted while the business way forward. The cybercrime field showing research while growing and scholars are exploring new innovative methods, and new research are making a big impact on the safer side. So, it is hopefully an indicator that is showing that the arena and research of cybercrime have arrived, and we are moving way ahead.

Cybersecurity is taken into account to form guidelines and take the required actions focused to prevent cybercrime, but cybersecurity is not restricted there only. These two varieties of problems are considered as taking into account what happens and who the survivor of the crime is, moreover because of their tutorial areas required to be studied. Thus, the two, cybersecurity and cyber-crimes, must always be thought of as two distinct issues, with various safeguards made to handle the varied privacy of the victims and security reasons with each. Each kind of information related to the personal front, government-oriented, or corporate world related need to be highly secured.

Variety levels of data, which belong to the government, related to research and development work, banking sector, institutes of defence, etc. these might be a very high level of confidentiality to be maintained if a little bit of negligence made, it may cause the damage up to different level and complete national security or society at large, and hence there is a need to be taken care of data security as an extremely high level.

Hence, cybersecurity looks all about giving protection to government, various organizations, and many businesses, aspiring to form it in a way that hackers can't hunt out the lackings threaten the organizations based on that lacking. While Cybercrime focuses greater on individuals and families online. It is the utmost requirement that the best people of a company or government must invest in cybersecurity measures to create it strong and inaccessible.

The chief problem of cybercrime which is lied modus operandi and the persistence of cybercriminal. The legal enforcement departments like police, judiciary, and agencies like investigative have to stay with them in web-based applications latest developments and so that can quickly identify the actual perpetrator.

Cybercrime and cybersecurity are different words but interlinked very much and different levels of crime are happening day to day online which targeted all types of people like not only the educated and highly qualified persons in the different fields are facing cybercrime by one or the other way.

So, the main solution is not only educating the people by the Government departments or increasing the specialists in the field, but people have to come forward to fight against cybercrime. It is not possible to solve only by the government or the legal departments, also it's the duty of the people of a country or the states, have to be educated themselves and maintain secrecy through online transactions, in social media, and anything which related to the computer or mobile by directly or indirectly.

Finally, it is better than cure if we all are taking care before the fraudulence happing in the online world, have to be educated every person in the family or society or a company or anywhere else in the country. The Government part is that they have to educate by doing awareness camps and programs at each different level and should be increased the specialists in the field of cybercrime to be fought against the same.