2. "CYBER SECURITY AND CRIME"

Ms. Shraddha V. Kadu, Riya N. Thakare and Prof. Gauri S. Kalmegh*

ABSTRACT

Nowadays, cybercrime is one of the major crimes done by computer expert. In this paper, need of cyber security is mentioned and some of the impacts of the cybercrime. Being one of the most rapidly expanding sectors, internet has become one of the most vital part of our life from work to entertainment there's no other option now but it comes with a price of our privacy. Crimes are also on the rapid expansion causing our sensitive data to be used without our permission. Governments are aware of this matter doing everything they can to secure our networks but many say security is just an illusion. In this whole report we will analyses the strength of the people who are trying to spoil the cyber Ecosystem and the higher grounds where we can deceive them

Key words: Cyber Crime, Cyber security.

Introduction

Today man is able to send and receive any form of data may be an email 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 safety 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 we are unable to safeguard our private information in a very effective way and hence cyber days crimes are increasing day by day. Today more than 60 percent of total commercial transparent and best transaction. 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 need 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 infrastructure are essential to each nation's security and economic wellbeing. Making the Internet safer 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. Every individual must also be trained on this cyber security and save themselves from these increasing cyber-crimes.

TYPES OF CYBER CRIME

1. Online Scams

Online scams are basically scams that happen online.

Whether that's tricking you into giving out personal details online by an ad popping up telling you have won something and asking for your card details to pay for shipping. Sadly, you'll never receive anything but you'll start noticing weird transactions coming from your bank account.

3. Malware

Malware is the contraction of malicious software onto your system. It's a piece of software written with the intent of causing harm to data and devices. Malware is the overarching name for different types of viruses such as a 'Trojan' and 'spyware'. Malware is often done through a range of viruses that will get into your computer to cause havoc, by damaging your computer, tablet, phone; so the culprits can steal credit card details and other personal information.

4. Email Bombing

An email bomb is more a form of internet abuse. Email bombing is an overload of emails directed to one email address; this will cause the person receiving the emails server to become sluggish or even crash. They may not necessarily be stealing anything from you but having a sluggish server can be a real pain and hard work to fix.

5. Virus Dissemination

This is particularly sneaky form of cyber-crime. It not only gets a piece of malware (a virus of some sort) onto one part of the victim's system, but it spreads across other pieces of software.

Without a full and proper quarantine process and safe environment to test in (a sandbox), the next time you open a piece of undiagnosed-as-infected software, the process starts all over again.

6. Logic Bombs

Logic bombs act in the same way as a virus, but are small programs or sections of a program, which are triggered by an event. This event can be a certain date or time, a certain percentage of disk space filled the removal of a file and so on.

A program could then delete critical sections of code, rendering your software as useless. The people who implement logic bombs are most commonly installed by insiders who already had access to the system.

7. Theft

Internet theft is the broad term for any type of theft that happens over the internet, this can be done through many ways such as fake ads, fake emails, viruses and snooping. The aim of internet theft is to steal your personal information and use it to then steal money out of your bank account or make purchases using your details.

8. Social Media Hack & Spamming

Social media hacking is often done as a joke, like the attack by the people who hacked Burger King's twitter account. . Abd many celebrities that are hacked may end up following people they wouldn't usually or put random statuses. Even though for the average joe seeing a celebrity or brand post weird stuff can be amusing, it's an invasion of privacy.

However a hacker can also spread unwarranted content that can be distressing to people who view this content, it can also cause your account to be reported and shut down.

Social media spamming comes when a person makes a fake account and becomes friends or followed by the average person. This then gives the fake account the freedom to spam inboxes with bulk messaging; this can be done for spreading malware.

9. Electronic Money Laundering

Money generated in large volumes illegally must be laundered before it can be spent or invested. One way to launder money is to do it electronically through messages between banks which is known as a "wire transfer". It had previously seemed impossible to monitor or screen wire transfers as they occur due to the tremendous volume on transactions going through on a day to day basis, however banks are clamping down on the issue and filing away any suspicious activity.

10. Sales & Investment Fraud

By sourcing the contact details and available account information for savings or investment account holders, fraudsters can adopt the persona of an investment broker. They will then contact customers to entice them with easy and profitable opportunities, but they seem a lot more trustworthy because they talk about accounts you already own and real results.

IMPACT OF CYBERCRIME ON SOCIETY

Cyber-crime is any criminal act related to computers and networks which is called hacking, phishing, spamming or is used as a tool to commit an offence (child pornography and hate crimes) conducted through the Internet. It is a bigger risk now than ever before due to the sheer number of connected people and devices.

The impacts of a single, successful cyber-attack can have far-reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust. The overall monetary impact of cyber-crime on society and government is estimated to be billions of dollars a year. Criminals take advantage of technology in many different ways. The Internet, in particular, is a great tool for scammers and other miscreants, since it allows them to ply their trade while hiding behind a shield of digital anonymity.

Cyber-crime affects society in a number of different ways, both online and offline. Identity Theft: Becoming the victim of cyber-crime can have long-lasting effects on life. One common technique scammers employ is phishing, sending false emails purporting to come from a bank or other financial institution requesting personal information. If one hands over this information, it can allow the criminal to access one's bank and credit accounts, as well as open new accounts and destroy credit rating.

CYBERCRIME INCLUDES

- Illegal access
- Illegal interception system
- Interference data
- Interference misuse of devices fraud.

Advantages

- Peace of mind-With a smart home security system that you can readily access on your phone or computer, you can see what's going on anytime, anywhere. Alarms activate in the event of a security breach, fire or flooding, and then it's up to you to call the police and/or the fire department. If you're not home, your system alerts the police or a private security agency (or both).
- Easy to install.- Smart home security systems are typically simple to install and often require no additional hardware purchase. Sensors can be mounted with screws or placed with adhesive strips, so even renters can take advantage. Depending on the monitoring service you choose, you can either install the sensors yourself or hire a professional installer to do the work for you.
- Convenient and easily accessible.- As long as you have the code and are connected to the internet, you can arm or disarm your alarm systems remotely and view your security camera footage from anywhere.
- Scalable and movable.- If you're on a monthly plan with an

internet home security provider, you can upgrade (i.e., add more sensors) or downgrade your plan (i.e., discontinue professional monitoring) as necessary. Plus, if you need to move to a new home, you can bring your home security system with you.

Disadvantages

- Reliance on the internet. -One primary disadvantage is their reliance on the internet. The moment you lose connectivity (whether it's from equipment breakdown, ISP failure or a power outage), you lose real-time monitoring access to your home security system.

- Hacking susceptibility.- Because it's internet-based, a smart home security system is susceptible to hacking. It's necessary to adopt protective measures to keep your home security and other smart systems from hackers.

- Third-party access. -Some smart home security providers offer professional monitoring for a fee. Although these providers take proactive measures to secure their servers and maintain data confidentiality, it's worth noting that camera footage and data (such as when you leave or return home) pass through their servers.

CYBER SECURITY TECHNIQUES

- Authentication of data:

The documents that we received must always be authenticated be before downloading that is it should be checked if it has from a trusted and reliable source and that they are not altered. Authenticating of these documents is usually done by the anti-virus software present in the devices. Thus a good anti-virus software is also essential to protect the devices from viruses.

- Access control and password security:

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security

- Malware scanners:

This is software that usually scans all the files and documents presents in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are example of malicious software that are often groped together and referred to as malware.

- Firewalls:

A firewalls is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in cyber security.

- Anti-virus software:

Antivirus software is a computer program that detects, prevents and takes action to disarm or remove malicious software programs, such as virus and worms. Most anti-virus program include an auto-update feature that enable the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered, An anti-viruses software is a must and basic necessity for every system.

CONCLUSION

Cybercriminals are going to create jobs for security professional over the next few years. And they are going to do it at a remarkable rate.

Sadly there seems to be no end to hacker who wants to access your business and customer data and then use that information to their own malicious ends.

Each year brings with it savior hackers. This means that each year also brings new defense mechanism as well.

In the past years, AI to take a bit of the cyber security burden, to increase consumer vulnerability and block chain to transform cyber security efforts

So what do cybercriminals and cyber security have store. It's impossible to know for sure but this trend seems like a good place to start based on what's already happening today.

REFERENCE:

1. A Sophos Article 04.12v1.Dna,eight trends changing network security by James Lyne

2. Cyber Security: understanding Cyber Crimes- SunitBelapure Nina Godbole

3. www.JohnCyberManson.com

4. www.cybercellmumbai.com from Mumbai

5. www.usdoj.gov/criminal/cybercrime/index.html

Name of First Author: Ms. Shraddha V. Kadu
Designation of first author: Student, Prof. Ram Meghe Institute of Technology and Research Badnera, Amravati 444605, Maharashtra.
Email address of first author: shradhakadu30@gmail.com

Name of Second Author: Ms. Riya N. Thakare
Designation of Second author: Student, Prof. Ram Meghe Institute of Technology and Research Badnera, Amravati 444605, Maharashtra.
Email address of Second author: riyathakare99@gmail.com

Name of Third Author: Prof. Gauri S. Kalmegh
Designation of Third author: Assistant Professor, Department of Management Studies, Prof. Ram Meghe Institute of Technology and Research Badnera, Amravati 444605, Maharashtra.
Email address of Third author: gsdhale@mitra.ac.in

Cite this article:

Kadu, S. V., Thakare, R. N., Kalmegh, G. S., (2020). Cyber Security and Crime. *International Journal of Social & Scientific Research, 5*(IV), 5-12.