Cyber Crime: A Real Threat And Mitigation Techniques

NIHAR VYAS, JINESH SHAH

Abstract— IN TODAY'S ERA OF ONLINE PROCESSING, THE MAJORITY OF INFORMATION IS STORED ONLINE AND IS VULNERABLE TO CYBER THREATS. THERE ARE A LARGE VARIETY OF CYBER RISKS, AND THEIR BEHAVIOR IS DIFFICULT TO PREDICT EARLY ON, MAKING IT TOUGH TO PREVENT CYBER-ATTACKS IN THEIR EARLY STAGES. CYBER-ATTACKS MAY HAVE A PURPOSE OR MAY BE HANDLED WITHOUT THE USER'S KNOWLEDGE. ATTACKS THAT ARE CARRIED OUT KNOWINGLY ARE CLASSIFIED AS CYBER-CRIME, AND THEY HAVE MAJOR RAMIFICATIONS FOR SOCIETY IN THE FORM OF ECONOMIC DISRUPTION, PSYCHOLOGICAL INSTABILITY, AND A THREAT TO NATIONAL SECURITY, AMONG OTHER THINGS. CYBERCRIME PREVENTION REQUIRES A THOROUGH EXAMINATION OF THEIR BEHAVIOR AS WELL AS AN AWARENESS OF THEIR EFFECTS AT MANY LEVELS OF SOCIETY. AS A RESULT, THE CURRENT MANUSCRIPT GIVES A KNOWLEDGE OF CYBERCRIME AND ITS EFFECTS ON SOCIETY, AS WELL AS PROSPECTIVE CYBERCRIME TRENDS.

Index Terms— CYBER ATTACKS, CYBER CRIMES, POTENTIAL ECONOMIC IMPACT, CONSUMER TRUST, NATIONAL SECURITY, ETHICAL HACKING, DATA THEFT.

1 INTRODUCTION

The current period is too rapid to take use of the time element to boost performance. It is only possible because of the Internet's use. The Internet is a collection of millions of computers connected by a network of electronic links. Millions of computers are connected to the internet. Everyone loves the usage of the Internet, but there is a flip side to the coin: cyber-crime committed through the use of the Internet. A cyber-crime is an act committed or omitted in violation of a law prohibiting or requiring it, for which a penalty is imposed upon conviction. In other terms, cyber-crime is defined as "criminal action directly related to the use of computers, specifically illegal intrusion into another's computer system or database, alteration or theft of stored or on-line data, or equipment and data vandalization." The Internet, often known as cyberspace, is rapidly expanding, as are cybercrime. Some of the different types of cyber-criminals are listed here.

2 TYPES OF CYBER CRIMINALS

2.1 CRACKERS

These people are out to cause harm for a variety of reasons, including antisocial motivations or simply for the sake of having fun. This category includes a lot of computer virus producers and distributors.

2.2 HACKERS

These individuals conduct research on other Individual's computer systems for the purposes of education, curiosity, or peer competitiveness. They could be aiming to acquire access to a more powerful computer, earn recognition from other hackers, establish a reputation, or gain acknowledgment as an expert without having completed formal education.

2.3 SCRIPT KIDDIES

These people use deception to deceive others. They usually do not seek to do any specific or long-term harm.

- *Nihar Vyas is currently pursuing Bachelor's degree program in computer science engineering with specialization in Cyber Security in Ganpat University, India, E-mail:nickvyas2312 @Gmail.com*
- *Jinesh Shah is currently pursuing Bachelor's degree program in computer science engineering with specialization inBig Data Analytics in Ganpat University, India, E-mail: sjinesh2001@Gmail.com*

2.4 BLACK-HAT HACKERS

Criminals, addicts, and irrational and incompetent people: Malcontents, addicts, and irrational and incompetent people: "These individuals range from the mentally ill to those who do not commit crimes on a daily routine. Some people work for a while, earn a little money, and then move on to another job to repeat the process. They may collaborate with others or work for organized gangs. Russian, Italian, and Asian organized crime gangs pose the biggest threat. According to the FBI, there were more than 30 Russian gangs operating in the United States in 1995. According to the FBI, "many of these malicious partnerships evade capture by employing advanced information technology and encrypted communications”.

2.5 CYBER TERRORISTS

Cyber terrorism can take various forms. Sometimes a clever hacker breaks into a government website, and other times a group of like-minded Internet users floods a website with traffic, causing it to fail. It is nevertheless prohibited for individuals hooked to drugs, alcohol, competition, or attention from others, as well as the criminally irresponsible, no matter how innocuous it may appear.

2.6 CYBER BULLIES

Any harassment that occurs through the internet is referred to as cyberbullying. Cyber bullying can take many forms, including threatening forum posts, name calling in chat rooms, creating bogus profiles on websites, and sending harsh or cruel email messages.

3. CYBER CRIMES CAN BE CATEGORIZED AS FOLLOWS

3.1 EMAIL SPOOFING

A spoofed E-Mail is one that pretends to come from one source but was actually received from a different one. Let's say Raj email address is nihar@gmail.com. Let's say her girlfriend Riya and he get into an argument. Riya then spoofs his E-Mail and sends obscene/vulgar messages to all of her acquaintances, having become his nemesis.

3.2 SPAMMING

Spammers are those who create electronic spam is the practice of sending unsolicited mass communications to anyone via electronic message systems (including most broadcast media and digital delivery methods). Although e-mail spam is pretty popular type of spam, the term is also applied to similar abuses in other forms of media. such as instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, file sharing network spam, video sharing site spam, and so on.

3.3 INTERNET TIME THEFT

When an unauthorized person utilizes Internet hours that have been paid for by another person, this is considered stealing. Internet time theft is classified as hacking because someone who obtains access to another person's ISP user ID and password, either by hacking or criminal means, uses it to use the Internet without the other person's knowledge. Even if one's personal use of the Internet isn't frequent, time theft can be detected if Internet time has to be recharged frequently. The problem of Internet time theft is linked to crimes involving "identity theft."

3.4 SALAMI ATTACK/SALAMI TECHNIQUE

These attacks are carried out in order to perpetrate financial crimes. The objective is to make the change so minor that it would go completely unreported in a single situation, such as when a bank employee uploads a software into the bank's servers that deducts a small amount of money from each customer's account. This illicit debit will most likely go unnoticed by the account user, but the bank staff will make a large monthly payment.

3.5 DATA DIDDLING

A data tampering attack involves altering raw data just before it is processed by a computer and then changing it to original after the processing is complete. Data tampering algorithms have been installed in India's electricity boards when private firms computerize their systems.

3.6 FORGERY

Using modern computers, printers, and scanners, counterfeit cash notes, postage and revenue stamps, mark sheets, and other documents can be created. Miscreants solicit the sale of falsified mark sheets or even degree certificates outside several colleges. Computers and high-quality scanners and printers are used to create these. In reality, giving big sums of money to student gangs in exchange for these phonies but genuine-looking credentials is becoming a flourishing business.

3.7 WEB JACKING

When someone takes control of a website by force, this is known as web jacking (by cracking the password and later changing it). As a result, “password sniffing” is the initial stage of this crime. The website's actual owner no longer has any influence over what appears on the site.

3.8 Usenet Newsgroup as the Source of Cybercrimes

Usenet is a popular way for people to share and distribute information on the Internet about specific topics or issues. Usenet is a network that allows people to share information with one another in a many-to-many basis. The newsgroups include a wide range of topics, totalling 3,00,00,30,000. It is theoretically feasible to prevent the distribution of some newsgroups. However, there is currently no technical means for managing the contents of any newsgroup. It's just a matter of self-control and net etiquette. Although it is possible to ban individual newsgroups, this should not be seen as a permanent solution to unlawful or harmful content. It is possible to put Usenet to illegal use in the following ways:

- Distribution/sale of pornographic material;
- Distribution/sale of pirated software packages
- Distribution of hacking software;
- Sale of stolen credit card numbers.
- Sale of stolen data/stolen property.

3.9 Password Sniffing

Password sniffers are programmers that watch and record network users' names and passwords when they log in, endangering a site's security. After installing the Sniffer, anyone can log in as an authorized user and access restricted documents. There are currently no laws in place to appropriately penalize someone who impersonates another person online. Hackers using Sniffer applications may be captured utilizing laws designed to restrict unauthorized access to information.

3.10 Identity Theft

Identity theft is a sort of fraud in which the identity of another person is utilized for mal intent. When a criminal exploits another person's identity for his or her own illegal reasons, this is known as impersonation. Phishing and identity theft are two crimes that are closely related. For example, acquiring credit in the victim's name, taking money from the victim's bank accounts, using the victim's credit card number, opening utility accounts, renting an apartment, or even filing bankruptcy in the victim's name are all examples. The cyber impersonation can take an endless amount of money under the victim's name without the victim knowing for months, if not years.

4. Impact Of Cyber Crimes

4.1 Impact of Cyber Crime over Youth

The newest way for society to interact is through cyber communication. Users may connect effectively and quickly with people all over the world through online social networking websites, text messages, and emails. Teens, in particular, spend a significant amount of time online each day, whether on computers or personal electronic devices.

4.2 The-Cost-Of-Protection

These individuals probe other people's computer systems for the purpose of education, curiosity, or competition with their peers. They could be aiming to acquire access to a more powerful computer, earn recognition from other hackers, establish a reputation, or gain acknowledgment as an expert without having completed formal education.

4.3 Sexual Solicitation

For kids who use forms of cyber communication, sexual solicitation is becoming a significant concern. It could happen in chat rooms or on social media platforms. When an adult or a peer attempts to engage in a sexual connection over the internet, this is known as sexual solicitation. A teen can be urged to reveal personal information, watch pornography, or talk about something sexual over the internet. Girls account for over 70% of those who are sexually solicited online. Teenagers should exercise extreme caution while sharing suggestive photos on the internet or conversing with strangers in chat rooms.

4.4 Lost-Sales

Cyber-crime is no longer just for criminals. In recent years, a new society has emerged: the cyber-activist. These are the versions of protesters who link themselves to buildings or trees over the internet. Their goal is to bring a company's online operations to a halt in order to send a statement about the company's business practices. Major organizations, such as PayPal and MasterCard, have been targeted in this way in the last several years. Hundreds of people claiming to be members of Anonymous assaulted the PayPal website in December 2010. In revenge for PayPal shutting off payment services to Wiki Leaks, they attempted to launch a denial-of-service attack. That crime resulted in the arrest of over a dozen hackers. While PayPal was spared a complete shutdown, many other businesses were not so fortunate. Customers are unable to access the company's online store as a result of a denial-of-service assault, which results in fewer sales. It may even result in lower long-term revenue if certain clients opt not to do business with a company that is prone to attack.

4.5 Impact of Cyber Crime over Consumer behavior

The information revolution, along with the strategic use of the Internet, has made a lot of generally open societies vulnerable to cybercriminal and cyber terrorist attacks, particularly in commercial business operations. This commercial dark side has been known as cybercrime, and it has taken on numerous forms that alter our impressions of how we shop online, thanks to the rise of e-commerce Corporations should recognize that these dangers to their online enterprises have strategic consequences for their long-term success, and take appropriate steps to eliminate or considerably decrease these threats so that consumer confidence in the Internet as a shopping alternative is maintained. These countermeasures, termed "cyber security," were created to protect consumer privacy and information while allowing for a worry-free shopping experience. There is a need for the creation of models that will allow businesses to evaluate the effects of cybercrime on online consumer confidence and respond by utilizing the benefits of recent cyber security advancements. With these two aspects of e-commerce having an impact on the online consumer, businesses must ensure that the security measures in place will ultimately win out, ensuring that customers will continue to use the Internet to meet their buying demands.

5. Mitigations against Cyber Crimes

5.1 Identify Risk

The newest way for society to interact is through cyber communication. Users may connect effectively and quickly with people all over the world through online social networking websites, text messages, and emails. Teens, in particular, spend a significant amount of time online each day, whether on computers or personal electronic devices.

5.2 Tripwire software

A tripwire is a piece of software that takes snapshots of essential system parameters and uses them to detect critical file changes. Since most intruding hackers make modifications when they instal backdoor entry points or change file system and directory attributes while hacking the system, tripwires provide evidence of electronic crimes.

5.3 Anomaly Detection

Unusual patterns of system activity are the focus of an anomaly detection system. Anomaly detection systems create and analyse user profiles, host and network activities, and system programmes to spot anomalies from expected behaviour.

5.3 Patch Operating System

One of the important eight mitigation tactics, in relation to the previously described patch applications, is to particularly patch/mitigate PCs (including network devices) with "extreme risk" vulnerabilities within 48 hours. It is recommended that you use the most recent version of your operating system and avoid using unsupported versions.

5.4 Use Strong Password

Use strong passwords that no one can guess and don't write them down anywhere. To make things easier, use a reliable password manager to generate strong passwords at random.

5.5 Beware of Spam Emails or untrusted Websites

Clicking on links in spam emails or other messages, or unknown websites, is another way for people to become victims of cybercrime. To keep safe online, avoid doing this.

5.6 Use of Anti-Virus Software and keep it updated

Using anti-virus software or a full internet security solution to safeguard your PC from threats is a good idea.

Anti-virus software scans, detects, and eliminates threats before they become a problem. This safeguard helps to protect your computer and data from cybercrime, offering you with sense of security.

If you use anti-virus software, make sure it's up to date so you can get the most out of it.

6. Conclusion

Between criminals and individual users, the future of the Internet is still up for grabs. Fears of a cyber-apocalypse persist, and the scope of damage that may be perpetrated by large-scale fraud is practically limitless. These fears should be rationally balanced by the knowledge that the issues are being addressed, perhaps not soon enough. The Internet's significance has been demonstrated in a several of ways, which should presumably be sufficient to prevent it from becoming a hotbed of criminal activity and a haven for the malevolent. Although the government has a vital role to play, the majority of fraud prevention must be done by private software producers and those with the ability to detect and prevent fraud. Consumer education campaigns will only help a small fraction of potential victims. Others must be automatically protected by non-stressing procedures that entail significant engagement. If it is to succeed, security must be simple and effective. In some ways, it's impossible to say if cybercrime will still be a relevant issue 10 years from now, but if the Internet is to continue to expand, it must be solved such that the reality of cybercrime are on par with, if not better than, real-world crimes.