ejpmr, 2023,10(3), 346-353

SJIF Impact Factor 6.222

EUROPEAN JOURNAL OF PHARMACEUTICAL AND MEDICAL RESEARCH

www.ejpmr.com

Review Article

ISSN 2394-3211

EJPMR

ELECTRONIC DEVICE FOR MAKING CRIME FROM CLOSED CHAMBER TO OPENED WORLDWIDE PLATFORM

Soumya Chakraborty, Soumyajit Mondal* and Dhrubo Jyoti Sen

School of Pharmacy, Techno India University, Salt Lake City, Sector-V, EM-4/1, Kolkata-700091, West Bengal, India.

***Corresponding Author: Soumyajit Mondal**

School of Pharmacy, Techno India University, Salt Lake City, Sector-V, EM-4/1, Kolkata-700091, West Bengal, India.

Article Received on 17/02/2023 **Article Revised on 08/03/2023** **Article Accepted on 28/03/2023**

ABSTRACT

Cybercrime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic wracking to denial of service attacks. It is a general term that covers crimes like phishing, Credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and or distribution of viruses, spam and so on. It also covers that traditional crimes in which computers or networks are used to enable the illicit activity. Cyber-crime is increasing day by day, nowadays it has become a new fashion to earn money by fraud calls or to take revenge through hacking other accounts.

KEYWORDS: Computer fraud, Cyber terrorism, Cyber extortion, Ransom ware, Cyber warfare, Financial crimes, scams, Cybersex Trafficking and Ad fraud.

INTRODUCTION

A scam is a deceptive scheme or trick used to cheat someone out of something, especially money. Scam is also a verb meaning to cheat someone in such a way. Example: Banks will never call you asking for your credit card number or social security number over the phone.[1-5] A scam is an illegal trick. Scams usually try to get money illegally from people. A scam is a type of fraud. A fraud is deceit, trickery. Deceit: intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right. Trickery: was accused of credit card fraud an act of deceiving or misrepresenting. A crime is an illegal action or activity for which a person can be punished by law.[6]

The cybercrime is a crime involving a computer or computer network. The computer may have been used in committing the crime, or it may be the target. Cybercrime may harm someone's security or finances.

There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, legally or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as cyberwarfare. Warren Buffett describes cybercrime as the "number one problem with mankind" and said that it "poses real risks to humanity." In India, one of the very first cases of cyber-crime was that of Yahoo V. Akash Arora. This case occurred in 1999. In this case, the defendant Akash Arora was accused of using the trademark or domain name 'yahooindia.com' and a decree of permanent injunction was sought.

1962. The modern history of cybercrime began when Allen Scherr launched a cyber-attack against the MIT computer networks, stealing passwords from their database via punch card. Allan L. Scherr (born November 18, 1940) is an American computer scientist notable for his work in time-sharing operating systems and leading the original development of the IBM MVS operating system, used on IBM mainframe computers.[7]

Figure-1: Inventor of cyber crime.

Classifications: Computer crime encompasses a broad range of activities, including computer fraud, cyber terrorism, cyber extortion, ransom ware, cyber warfare, financial crimes, scams, cybersex trafficking, and ad fraud.

Computer fraud: It is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system. If computer fraud involves the use of the Internet, it can be considered Internet fraud. The legal definition of computer fraud varies by jurisdiction, but typically involves accessing a computer without permission or authorisation.[8]

Figure 2: Computer fraud.

Cyber terrorism: It is in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources. Acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by means such as computer viruses, computer worms, phishing, malicious software, hardware methods, or programming scripts can all be forms of cyberterrorism.[9]

Figure 3: Cyber terrorism.

Cyber extortion: It is a type of extortion that occurs when a website, e-mail server, or computer system is subjected to or threatened with attacks by malicious hackers, such as denial-of-service attacks. Cyber extortionists demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cybercrime extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate, and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack. However, other cyberextortion techniques exist, such as doxing, extortion, and bug poaching. An example of cyber extortion was the Sony Hack of 2014.[10]

Figure 4: Cyber extortion.

Ransom ware: It is a type of malware used in cyberextortion to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid. The Kaspersky Lab 2016 Security Bulletin report estimated that a business falls victim to ransomware every 40 minutes, and predicted that the time would decrease to 11 minutes by 2021. With ransomware remaining one of the fastest-growing cybercrimes in the world, global damage caused by it is predicted to cost up to $20 billion in 2021.[11]

Figure 5: Ransom ware.

Cybersex trafficking: It is the transportation of victims and then the live streaming of coerced sexual acts or rape on webcam. Victims are abducted, threatened, or deceived and transferred to "cybersex dens". The dens can be in any location where the cybersex traffickers have a computer, tablet, or phone with an internet connection. Perpetrators use social media networks, video conferences, dating pages, online chat rooms, apps, dark web sites, and other platforms. They use online payment systems and cryptocurrencies to hide their identities. Millions of reports of its occurrence are sent to authorities annually. New legislation and police procedures are needed to combat this type of cybercrime.[12]

Figure 6: Cybersex trafficking.

Cyber warfare: The U.S. Department of Defence notes that cyberspace has emerged as a national-level concern through several recent events of geostrategic importance, including the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become normalized in future warfare among nation-states, the military commanders intend to adapt the concept of cyberspace operations impact in the future.[13]

Figure 7: Cyber warfare.

Computer as a tool: When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the like existed before the development of computers and the internet. The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.

COMPUTER AND INTERNET FRAUD

Computer fraud is defined the use of a computer to help execute a illegal activity or the targeting of a computer with the intent to alter, damage, or disable it.

Figure 8: Cyber warfare.

Obscene or offensive content: The content of websites and other electronic communications may be distasteful, obscene, or offensive for a variety of reasons. In some instances, these communications may be illegal.

Ad-fraud: These are particularly popular among cybercriminals, as such frauds are lucrative and less likely to be prosecuted. Jean-Loup Richet, a professor at the Sorbonne Business School, classified the large variety of ad-fraud committed by cybercriminals into three categories: identity fraud, attribution fraud, and ad-fraud services.[14]

Figure 9: Obscene.

Online harassment: The examples and perspective in this section may not represent a worldwide view of the subject. You may improve this section, discuss the issue on the talk page, or create a new section, as appropriate. (March 2016) (Learn how and when to remove this template message). Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing, for example, on gender, race, religion, nationality, or sexual orientation.

Figure 10: Online harassment.

Drug trafficking: Darknet markets are used to buy and sell recreational drugs online. Some drug traffickers use encrypted messaging tools to communicate with drug mules or potential customers. The dark web site Silk Road was the first major online marketplace for drugs, starting operation in 2011. It was permanently shut down in 2014 by the FBI and Europol. After Silk Road 2.0 went down, Silk Road 3 Reloaded emerged. However, it was just an older marketplace named Diabolus Market that used the name for more exposure from the brand's previous success.[15]

Phishing: It is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransom ware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2020, it is the most common type of cybercrime, with the FBI's Internet Crime Complaint Centre reporting more incidents of phishing than any other type of computer crime. The term "phishing" was first recorded in 1995 in the cracking toolkit AOHell, but may have been used earlier in the hacker magazine 2600. It is a variation of fishing and refers to the use of lures to "fish" for sensitive information.

Figure 11: Drug trafficking.

Measures to prevent or reduce the impact of phishing attacks include legislation, user education, public awareness, and technical security measures. The importance of phishing awareness has increased in both personal and professional settings, with phishing attacks among businesses rising from 72% to 86% from 2017 to 2020.

Types

Email phishing: Phishing attacks, often delivered via email spam, attempt to trick individuals into giving away sensitive information or login credentials. Most attacks are "bulk attacks" that are not targeted and are instead sent in bulk to a wide audience. The goal of the attacker can vary, with common targets including financial institutions, email and cloud productivity providers, and streaming services. The stolen information or access may be used to steal money, install malware, or spear phish others within the target organization. Compromised streaming service accounts may also be sold on darknet markets.

Spear phishing: Spear phishing is a targeted phishing attack that uses personalized emails to trick a specific individual or organization into believing they are legitimate. It often utilizes personal information about the target to increase the chances of success. These attacks often target executives or those in financial departments with access to sensitive financial data and services. Accountancy and audit firms are particularly vulnerable to spear phishing due to the value of the information their employees have access to.

Threat Group-4127 (Fancy Bear) targeted Hillary Clinton's campaign with spear phishing attacks on over 1,800 Google accounts, using the accounts-google.com domain to threaten targeted users. A study on spear phishing susceptibility among different age groups found that 43% of 100 young and 58 older users clicked on simulated phishing links in daily emails over 21 days. Older women had the highest susceptibility, while susceptibility in young users declined over the study, but remained stable in older users.

Figure 12: Phishing.

Whaling and CEO fraud: Whaling attacks use spear phishing techniques to target senior executives and other high-profile individuals with customized content, often related to a subpoena or customer complaint. CEO fraud involves sending fake emails from senior executives to trick employees into sending money to an offshore account. It has a low success rate, but can result in organizations losing large sums of money.

Clone phishing: Clone phishing is a type of attack where a legitimate email with an attachment or link is copied and modified to contain malicious content. The modified email is then sent from a fake address made to look like it's from the original sender. The attack may appear to be a resend or update of the original email. It often relies on the sender or recipient being previously hacked so the attacker can access the legitimate email.[16]

Voice phishing: Voice over IP (VoIP) is used in phishing or voice phishing attacks, where attackers make automated phone calls to large numbers of people, often using text-to-speech synthesizers, claiming fraudulent activity on their accounts. The attackers spoof the calling phone number to appear as if it is coming from a legitimate bank or institution. The victim is then prompted to enter sensitive information or connected to a live person who uses social engineering tactics to obtain information. Phishing takes advantage of the public's lower awareness and trust in voice telephony compared to email phishing.

SMS phishing: SMS phishing or smishing is a type of phishing attack that uses text messages from a cell phone or smartphone to deliver a bait message. The victim is usually asked to click a link, call a phone number, or contact an email address provided by the attacker. They may then be asked to provide private information, such as login credentials for other websites. The difficulty in identifying illegitimate links can be compounded on mobile devices due to the limited display of URLs in mobile browsers. Smishing can be just as effective as email phishing, as many smartphones have fast internet connectivity. Smishing messages may also come from unusual phone numbers.

Page hijacking: It involves redirecting users to malicious websites or exploit kits through the compromise of legitimate web pages, often using cross site scripting. Hackers may insert exploit kits such as MPack into compromised websites to exploit legitimate users visiting the server. Page hijacking can also involve the insertion of malicious inline frames, allowing exploit kits to load. This tactic is often used in conjunction with watering hole attacks on corporate targets.

Calendar phishing: This involves sending fake calendar invitations with phishing links. These invitations often mimic common event requests and can easily be added to calendars automatically. To protect against this form of fraud, former Google click fraud czar Shuman Ghosemajumder recommends changing calendar settings to not automatically add new invitations.[17]

Link manipulation: Phishing attacks often involve creating fake links that appear to be from a legitimate organization. These links may use misspelled URLs or subdomains to deceive the user. In the following example URL, http://www.yourbank.example.com/, it can appear to the untrained eye as though the URL will take the user to the example section of the yourbank website; actually this URL points to the "yourbank" (i.e. phishing) section of the example website. Another tactic is to make the displayed text for a link appear trustworthy, while the actual link goes to the phisher's site. To check the destination of a link, many email clients and web browsers will show the URL in the status bar when the mouse is hovering over it. However, some phishers may be able to bypass this security measure. Internationalized domain names (IDNs) can be exploited via IDN spoofing or homograph attacks to allow attackers to create fake websites with visually identical addresses to legitimate ones. These attacks have been used by phishers to disguise malicious URLs using open URL redirectors on trusted websites. Even digital certificates, such as SSL, may not protect against these attacks as phishers can purchase valid certificates and alter content to mimic genuine websites or host phishing sites without SSL.

Filter evasion: Phishers have sometimes used images instead of text to make it harder for anti-phishing filters to detect the text commonly used in phishing emails. In response, more sophisticated anti-phishing filters are able to recover hidden text in images using optical character recognition (OCR).

Social engineering: Phishing often uses social engineering techniques to trick users into performing actions such as clicking a link or opening an attachment, or revealing sensitive information. It often involves pretending to be a trusted entity and creating a sense of urgency, like threatening to close or seize a victim's bank or insurance account. An alternative technique to impersonation-based phishing is the use of fake news articles to trick victims into clicking on a malicious link. These links often lead to fake websites that appear legitimate, but are actually run by attackers who may try to install malware or present fake "virus" notifications to the victim.

Prevention: The Department of Homeland Security also instituted the Continuous Diagnostics and Mitigation (CDM) Program. The CDM Program monitors and secures government networks by tracking and prioritizing network risks, and informing system personnel so that they can take action. In an attempt to catch intrusions before the damage is done, the DHS created the Enhanced Cybersecurity Services (ECS) to protect public and private sectors in the United States. The Cyber Security and Infrastructure Security Agency approves private partners that provide intrusion detection and prevention services through the ECS. An example of one of these services offered is DNS sink holing.[18]

Legislation: Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries such as the Philippines, laws against cybercrime are weak or sometimes non-existent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise.

Penalties: Penalties for computer-related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanour such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison.

Awareness: As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals increasingly attempt to steal that information. Cybercrime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information continues to grow in importance. According to the FBI's Internet Crime Complaint Center in 2014, there were 269,422 complaints filed. With all the claims combined there was a reported total loss of $800,492,073. But cybercrime does not yet seem to be on the average person's radar. There are 1.5 million cyber-attacks annually, which means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute, with studies showing that only 16% of victims had asked the people who were carrying out the attacks to stop. Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is being protected while online.[19]

Figure 13: Cybercrime intelligence squad.

Intelligence: As cybercrime has proliferated, a professional ecosystem has evolved to support individuals and groups seeking to profit from cybercriminal activities. The ecosystem has become quite specialized, including malware developers, botnet operators, professional cybercrime groups, groups specializing in the sale of stolen content, and so forth. A few of the leading cybersecurity companies have the skills, resources and visibility to follow the activities of these individuals and groups. A wide variety of information is available from these sources which can be used for defensive purposes, including technical indicators such as hashes of infected files or malicious IPs/URLs, as well as strategic information profiling the goals, techniques and campaigns of the profiled groups. Some of it is freely published, but consistent, ongoing access typically requires subscribing to an adversary intelligence subscription service. At the level of an individual threat actor, threat intelligence is often referred to as that actor's "TTP" or "tactics, techniques, and procedures", as the infrastructure, tools, and other technical indicators are often trivial for attackers to change. Corporate sectors are considering crucial role of artificial intelligence cybersecurity.

Diffusion of cybercrime: The broad diffusion of cybercriminal activities is an issue in computer crime detection and prosecution. Hacking has become less complex as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have contributed substantially to information sharing as beginners can benefit from older hackers' knowledge and advice.[20]

CONCLUSION

We are living in a digital age and cyberspace is not limited to one's boundaries, rather it covers an entire world. As a result cybercrime is increasing day by day in all the countries including India. The biggest challenge relates to cybercrime being its dynamic nature because of the ongoing evolution of digital technology. As a result new cybercrime methods and techniques come into practice. Therefore cybercrime should be given as much importance as other crime happening in our society be it theft, rape, murder etc.

REFERENCES

1. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. 392.
2. Bossler, Adam M.; Berenblum, Tamar "Introduction: new directions in cybercrime research". Journal of Crime and Justice, 2019; 42 (5): 495–499.
3. Gordon, Sarah "On the definition and classification of cybercrime". Journal in Computer Virology, 2006; 2: 13–20.
4. Richet, Jean-Loup. "How cybercriminal communities grow and change: An investigation of ad-fraud communities". Technological Forecasting and Social Change, 2022; 174 (121282): 121282.
5. Laqueur, Walter; C., Smith; Spector, Michael. Cyberterrorism. Facts on File, 2002; 52–53.
6. Carback, Joshua T. "Cybersex Trafficking: Toward a More Effective Prosecutorial Response". Criminal Law Bulletin, 2018; 54 (1): 64–183, 64.
7. Wilbur, Kenneth C.; Zhu, Yi. "Click Fraud". Marketing Science, 2008; 28 (2): 293–308.
8. Richet, Jean-Loup. "From Young Hackers to Crackers". International Journal of Technology and Human Interaction, 2013; 9 (3): 53–62.
9. Canetti, Daphna; Gross, Michael; Waismel-Manor, Israel; Levanon, Asaf; Cohen, Hagit (1 February). "How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks". Cyberpsychology, Behavior, and Social Networking, 2017; 20 (2): 72–77.
10. Gross, Michael. "The psychological effects of cyber terrorism". The Bulletin of the Atomic Scientists. National Institutes of Health, 2016; 72 (5): 284–291.
11. Min, Donghyun; Ko, Yungwoo; Walker, Ryan; Lee, Junghee; Kim, Youngjae. "A Content-Based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense". IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022; 41 (7): 2038–2051.
12. Young, Adam. "Cryptoviral Extortion Using Microsoft's Crypto API: Can Crypto APIs Help the Enemy?". International Journal of Information Security, 2006; 5 (2): 67–76.
13. Chibba, Michael. "Contemporary issues on human trafficking, migration and exploitation". Migration and Development, 2014; 3 (2): 163–173.
14. Humphreys, Krystal; Le Clair, Brian & Hicks, Janet. "Intersections between Pornography and Human Trafficking: Training Ideas and Implications". Journal of Counselor Practice, 2019; 10 (1): 19–39.
15. Smith, Troy E. "Cyber Warfare: A Misrepresentation of the True Cyber Threat". American Intelligence Journal, 2013; 31 (1): 82–85.
16. Baker, Emiley; Wade Baker; John Tedesco. "Organizations Respond to Phishing: Exploring the Public Relations Tackle Box". Communication Research Reports, 2007; 24 (4): 327.
17. Arachchilage, Nalin; Love, Steve; Scott, Michael. "Designing a Mobile Game to Teach Conceptual Knowledge of Avoiding 'Phishing Attacks'". International Journal for E-Learning Security, 2012; 2 (1): 127–132.
18. Perrault, Evan K. "Using an Interactive Online Quiz to Recalibrate College Students' Attitudes and Behavioral Intentions About Phishing". Journal of Educational Computing Research, 2017; 55 (8): 1154–1167.
19. Patchin, J. W.; Hinduja, S. "Bullies move beyond the schoolyard: A preliminary look at cyberbullying". Youth Violence and Juvenile Justice, 2006; 4 (2): 148–169.
20. Broadhurst, R., and Chang, Lennon Y.C. "Cybercrime in Asia: trends and challenges", in B. Hebenton, SY Shou, & J. Liu (eds), Asian Handbook of Criminology. New York: Springer, 2013; 49–64