Cybercrime an emerging challenge for internet users: An overview

N. I. Ali, S. Samsuri, M. S. A. Seman, I. A. Brohi, A. Shah

Department of Information Systems, International Islamic University Malaysia

Received 10th June 2018 and Revised 15th September 2018

1. INTRODUCTION

Internet users are growing rapidly since the last four decades. Nearly four billion peoples around the globe are online, which shows that half of the world using the internet nowadays, out of which half of the individuals started using it since 2017 (“internet world Stats,” 2018). World statistics show the dramatic increase in the users of the internet. (Fig. 1) shows the penetration of internet users around the globe. Whilst, statistics revealed that 95% Americans are using the internet in their routine activities, whereas, in total 49% of the population using the internet in Asia, the number of internet users increased rapidly from 2017 to 2018 (“internet world Stats,” 2018).

As the popularity of the internet is increasing day by day, along with providing many benefits such as ease of use, time-saving, and convenience, it also invites the criminals to perform the cybercrimes very easily. Crime means something illegally done. Cybercrime refers to the execution of unlawful activity by using cyberspace as the source of crime. Cyber security refers to “a measure for protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction” (Gallaher, Link and Rowe, 2008). In the recent years, the world has witnessed the swift rise in the cybercrimes due to the increase in use of internet. Internet has connected the computers of world, it has became easier for cybercriminals to conduct the cybercrime. Unlike the physical crimes, the virtual crimes can be done remotely without geographical boundaries and sometimes it becomes very hard to trace them and collect the digital evidence (Hui, and Wang, 2017).

2. BACKGROUND

The existence of cybercrime can be traced before the presence of Microsoft, personal computer, internet and windows (Thomas.2008). First Cybercrime was conducted in 1820 in a fabric company of France, when the Joseph-Marie Jacquard produce the looms for repetitive use in weaving the clothes. This caused insecurities among other employees and they managed to stop him from further use of the new technology and modifying the loom patterns (Dalla and Geeta, 2013; Mohiuddin, 2006; Nagpal, 2008; Rajput, n.d.). The traces of cybercrime is available since 1960's when the internet was not yet invented but the cybercriminals were already existed inside the organization, who were harmful to their organizations (Dineshbhai and Patel, 2017). The traces of cyber crime is available since 1960’s when the internet was not yet invented but the cybercriminals were already existed inside the organization, who were harmful to their organizations (Dineshbhai and Patel, 2017). First, officially registered cybercrime was conducted in 1964 by the young student of Massachusetts Institute of Technology (MIT), the pattern of crime was to unofficially access the long-
distance calls by inhabiting the ringing tone (Thomas, 2008). In 1986 another more serious cybercrime was reported where the systems administrator at the ‘Lawrence Berkeley National Laboratory’, Clifford Stoll, noted certain irregularities in accounting data, where the cybercriminals stolen the army data and passed it to enemies, Stoll takes the measure and the criminals were arrested and send to prison (Tech, n.d.). After that, many cybercrimes were reported around the world. The one of the major cybercrime reported in 2012 at the South Carolina Department of Revenue’, when cyber criminals broke the system and steal 3.6 million Security numbers and 387,000 credit/debit card numbers (Dineshbhai and Patel, 2017).

2.1 Classification of Cybercrimes.

Carter David divides the cybercrime in four broad categories. (David. 1995)

a) Computer as the Target: The crime in which computer is target to steal the personal information related to individuals or marketing companies and that steal data can be used for blackmailing purpose.
b) Computer as the Instrumentality of the Crime: The category of cybercrimes in which computer or its processes used to conduct the crime but not directly the data that is available to computer.
c) Computer Is Incidental to Other Crimes: In this category computer is not essential device to conduct the crime but its related technologies can be use to faster the crime process and also make it difficult to analyse the crime laundering and unlawful ban transactions are its example.
d) Crimes Associated with the Prevalence of Computers: The crimes which are the result of innovations of computer technology, especially with the introduction of microcomputers, which can be one of the reasons for dispersion of more cybercrime activities.

Cybercrime can be classified in two types

1. Crimes that directly target the computer networks or devices, for example hacking, malware, computer virus, Daniel-of-Service (DoS).

- **Hacking**- it is attempt by the cybercriminals also called hackers in this case to access your computer without permission. Some hackers do this just to get the popularity whereas others do this to give harm to their enemies and other institutions. ‘Black Hats’ and Crackers are also the Hackers. Hackers are usually the high-level programmer. Some companies hire the Hackers called ‘White Hackers’ to investigate their system flaws and fix them before the attack of the Hacker’s
- **Malware**- This is the short form of malicious software. The malware is a virus, which attach itself with computer program and can circulate over the network. Malware, virus or worm can be used interchangeably. The malware is capable of occupying and destroying the computer memory and can be a cause of loss.

- **Daniel-Of-Service(DOS)**- It is an attempt by criminals to deny the service requested by the users. The cybercriminals send the unlimited requests to the server, which cause the overloading of the server and the user cannot receive their required services from the server. DOS usually attacks the high-profile websites, including institution.

2. Crimes that uses computer or internet to conduct the crime, for example Fraud, identity theft, cyberstalking, Phishing, Email spoofing, Password sniffing

- **Fraud**- Often called credit card fraud can happened by using your credit card details. Do not forget to receive your receipt after by the credit card. Be careful when doing online buying. Never save your credit card number with the online website. This type of crime usually happened when you drop your pre-pin debit/ credit card, the criminals take the opportunity to shop until the card is blocked.
- **Identity theft**- when someone else theft your identity and pretend as you is called identity theft. The cybercriminals used the identity of the victim to access their accounts, and other activities. Many time the cybercriminals use the lost documents or inbox to take the loan.
- **Cyberstalking**- Cyberstalking can be done through cyber stalker by virtually follow their victim through the internet. They cannot harm their victims physically but can give them mentally torture. Cyberstalker, usually keep an eye on the internet activities of victim and can blackmail him/ her. Victim for cyberstalking are usually women and the kids who are not familiar with the security measures of internet usage.
- **Phishing**- It means to extract the confidential data such as debit/credit card information. Accounts username and password combination. This can be done through e-mail spoofing and password sniffing. The phisher sends the victim the spoof emails pretend to be from their institutions. If the victim access that email than phisher malware software can attack your system and get the sensitive data i.e. password of accounts, which can be used to access your data.

2.2 Who can be cybercriminals?

The cybercriminal are divided into three categories.

a) Cybercriminals who done the cybercrimes only to seek the recognition, this types of criminals are usually youngster and want to be famous that’s why conduct the cybercrimes.(Bhat and Khan, 2015)

b) Cybercriminals, who wants to make quick. They are usually involved in the online crimes, transactions and
frauds. Their main aim is to commit fraud and transfer amount of the victims into their accounts (Bhat and Khan, 2015)
c) Third and most dangerous category is the one who commit cybercrimes, just to harm the state or any
country, their main aim is to just fight a cause so they did not care to whom they are giving the destruction.
They are called cyber-terrorist (Bhat and Khan, 2015)

3. MATERIALS AND METHODS

In this section, we discuss the concepts, tools and methods utilized in the preparation of this paper.

3.1 Recent report on cybercrime by Internet Crime Complaint Centre (IC3)

The (IC3) was established by USA in 2000, the main purpose of this organization is to receive and investigate cyber crime cases around the world. There have been 4,063,933 crimes reported. According to report released by IC3 in 2017 approximately 284,000 complaints are reported each year. The loss of $1.42 billion by victims was reported in 2017 (IC3, 2017) as shown by (Fig. 2).

![Fig 2. Cybercrime complaints from all over the world to IC3 (IC3, 2017)](image)

(Table 1) shows the age wise victims and loss reported during 2017, there were total loss of $1,095,255,921 in 2017 (IC3, 2017). We can notice from table 1, as the age increases, the number of victims and volume of loss also increased.

<table>
<thead>
<tr>
<th>Age Range</th>
<th>Total Count</th>
<th>Total Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 20</td>
<td>9,053</td>
<td>$8,271,311</td>
</tr>
<tr>
<td>20 - 29</td>
<td>41,132</td>
<td>$67,981,630</td>
</tr>
<tr>
<td>30 - 39</td>
<td>45,458</td>
<td>$156,287,698</td>
</tr>
<tr>
<td>40 - 49</td>
<td>44,878</td>
<td>$244,561,364</td>
</tr>
<tr>
<td>50 - 59</td>
<td>43,764</td>
<td>$275,621,946</td>
</tr>
<tr>
<td>Over 60</td>
<td>49,523</td>
<td>$342,531,972</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>233,808</strong></td>
<td><strong>$1,095,255,921</strong></td>
</tr>
</tbody>
</table>

IC3 is very active in generating reports every year regarding to the cyber-attacks around the globe. It provides detailed and complete information in order to increase awareness among people regarding types of crimes, total losses and other related information. IC3 is preparing the reports related to cybercrime every year and with the collaboration of FBI. Similarly these reports are distributed across the world, whereas, other developed countries such as United Kingdom and Canada are also trying to establish similar type of centres (Abubakar, et al., 2015).

(Table 2) shows the top 20 countries by victims who reported to IC3 except America for which separate table was given with state wise reported numbers. Most cases were registered in California State, with 41,974 victims. Table 2 demonstrates that highest cases in 2017 were registered from Canada i.e. 3,164 whereas lowest cases were registered from Afghanistan i.e. 238 (IC3, 2017). With the efficient measures taken by the government of each country, these crimes can be reduced. Every country should impose the cyber law in order to prevent their people being the victim of cybercrime. (Fig. 3) shows the types of cybercrime with victims count in 2017. Most crimes happen under the category of Non-payment/ Non-Delivery with 84079 victims whereas least cases reported under the Hacktivist category with 158 victims. (IC3, 2017)
As the internet connects the computer of all over the world together, it also invites the criminal minds to access and attack the once privacy without the geographical boundary. Cybercrime has become one of the emerging challenges for the internet users around the globe. As the number of internet users have increased, it also provides the cybercriminals to access their activities. The cybercriminals can attack the individuals or organizations to fulfill their dirty needs. The internet users must take measures to keep safe their selves from cybercriminal attacks.

- Keep data secure like your username and password. Do not share this information with anyone.
- Always use the strong password.
- Always deals with the trusted websites for online transactions.
- Always install the strong antivirus on your smart devices and computer.
- Do not open the unknown emails.
- Do not response to any email, which is asking for your username and password of your accounts, because these institutes never request this type of information online.
- Most importantly, if anyone face cybercrime activity, he or she should report it.

5. CONCLUSION

In this paper, authors discussed the challenges faced by the internet users in the form of cybercrimes. It was observed that the cybercrime was there before the invention of internet. Different types of cybercrimes and cybercriminals also discussed in this paper. The recent report issued by the IC3, one of the largest organization to report and solve the cybercrimes around the globe was also discussed. In last the possible prevention from the cybercrimes were discussed.

REFERENCES:


