A Survey on Cybercrimes Awareness Knowledge in Bangladesh

Md. Mojibur Rahman Redoy Akanda¹, Mohammed Nadir Bin Ali², Masud Parvez³, Md Nazrul Islam⁴

¹²³⁴Daffodil International University, Dhaka, Bangladesh

Abstract— In the era of smart devices, Internet has become the part and parcel of our life. It has become the closest source of information. With the blessing of it, world has now become like a village. People can contact with the other part of the world within a second. Analogue communication medium has been override with this. In social media all the info remain together including educational, entertainment, news and other. To cope up with the situation of world, Bangladesh government has also introduced new slogan which is “Digital Bangladesh”. The Government is giving its best to make this slogan successful. As a result Internet has become much available to us. But every good thing has some bad parts. With the introduction of “Digital Bangladesh”, Digital crime is also introduced which is called cybercrime. Country like Bangladesh is facing more problem regarding this cybercrime issue because people here are not aware of using Internet properly. They are falling on various traps on the Internet which is set up by the cyber-criminals. In this study, it is deeply tried to find out some common mistakes of peoples which is driving us to be the victims of cybercrimes and also some crimes which we face most. The study finds normal people’s awareness level and other knowledge related to using the Internet which is not appeasement. That’s why lots of unexpected issues visible on the Internet which are actually cybercrimes. The Government is giving its best on digitalization, but not so much care about cybercrimes. The Government and other related organizations need to take proper care about this issue. It should be made mandatory to implement the cybercrime awareness study with the current education system. Then we can expect a healthy and safe cyber arena.

Keywords—Awareness study, Cyber threat, Digital Bangladesh, Survey on crimes, Victim of Cybercrimes.

I. INTRODUCTION

Digital Bangladesh has become a known slogan by the government these days in Bangladesh. Government is providing its full strength to successfully make Bangladesh a Digital Country. On the way to the Digital Bangladesh Internet for all is very much important thing. Because Internet has become the easiest medium of social, business and academic communication among the world and it has made the world like a global village.

It has also become the nearest source of knowledge and information. That’s why the government is ensuring high speed Internet to all, own satellite is launched and many more steps are being taken down to make the Internet more available. Sim Company also is giving lots of offers for Internet packages to its users. With all of these facilities Internet users in our country are growing tremendously.

According to Bangladesh Telecommunication Regulatory Commission (BTRC) total number of Internet subscribers has reached 91.348 Million at the end of December 2018 where mobile subscriber 85.552, WiMAX 0.061 and ISP+PSTN 5.735 Million [1]. Increasing number of Internet user is really a great news for us, but with the greatness a new crime is introduced named cybercrime. According to Council of Europe “Any criminal offence committed against or with the help of a computer network is identified as cybercrime”. So computer or computation related device is an essential for cybercrime perpetration and victimization [2]. Computer crime defined as criminal activities, involving information technology infrastructure, including illegal access of computer data from or within a computer [3]. A person, organization or country can lose money, important information and many more because of cybercrime. Bangladesh bank $81 Million heist is also one of the biggest examples of cybercrime in Bangladesh. Not only Bangladesh but also many countries are facing same problem following Russian bank $6 Million heist and India’s City Union Bank heist [4]. A new report from McAfee and the Center for Strategic and International Studies claims that cybercrime now costs the global economy $600 billion, up considerably from $445 billion in 2014 [5]. Nothing is immune in Internet. Most of the cybercrime activities occur because of unawareness. Every country, system and person are vulnerable but being aware can be reduced the rate of cybercrime.

BTRC indicates that overwhelming 80 percent Internet users of Bangladesh are on social networking website i.e. Facebook. State Minister for Information and Communications Technology, Zunaid Ahmed Palak made the disclosure saying, a new user of social networking site Facebook is being added in every 12 seconds in
Bangladesh which is more than the birth rate of the country. On the other hand, a report published by a national Bengali daily, citing Socialbakers (a social media analytic) the ratio of the age group of Facebook users in Bangladesh are 73% of 13-25 age, 20% of 26-34 age, 5% of 35-45 age 2% above of 45 age respectively [6].

With the above huge number of Internet users, cybercrime has become an alarming situation. Because most of them has no Internet literacy. Cyber criminals can drive those people in the wrong ways. If we think about some recent attacks like Brahmanbaria attack [7] and Ramu attack [8] are the proof of Internet illiteracy. People think Facebook posts authenticity is the same as newspaper because of illiteracy. Also, they are losing their personal information, affecting by malware, viruses, trojan and many cybercrime related issues. Security Intelligence Report of Microsoft 2017 showed that the encounter rate for the malware in Bangladesh in March was 26.6 percent which was highest in the world followed by Pakistan 26.2 percent on the same month. Encounter rate is the percentage of computers running Microsoft real-time security products that report a malware encounter, the report said [9]. So we can assume how problematic this scenario is.

Internet literacy includes one’s ability to indicate illegal and harmful contents on the Internet appropriately and the ability to protect one's privacy [10]. This study indicates some common cyber security issues faced by Bangladeshi Internet users and then took survey to know about their knowledge rate on cybercrimes. The survey shows the awareness rate of people, victimization rate and their prevention knowledge on cybercrimes.

II. ANALYSIS AND CYBERCRIME SELECTION

In this paper, researcher analyzed and read from various reports and papers to know the most happened cybercrimes in Bangladesh. Then selected those cybercrimes and based on those crimes made a list. By using this list, made a survey form to know the respondents knowledge about those crimes. Researcher selected total 16 cybercrime activities which is highly occurring and some faults which are done by Bangladeshi users.

A. The Selected Cybercrimes

In this section, all the selected crimes are listed which has been taken in consideration to do the study.

One Ring Scam: Getting miss call from different number from different countries. When call back to the number huge amount billed from the account.

Steganography: Hiding malware or message behind images or video then drive normal people to share this by using religious issues.

Cyber Defamation: Slagging someone on social media. We can see a celebrity or other person being slagged by other users on social media.

Man in the Middle Attack: Someone steals info from the middle of the network. We sometimes use insecure website and public Wi-Fi which can send plain text data to the network. This type of data can sniff from the network.

Email Bombing: Getting a bunch of scam emails on the mailbox and it’s flooding the inbox. As a result, legitimate emails are not easily findable among those scam emails.

Phishing: Getting mail with interesting link, software including offer or something which ask user to give info. This type of mail look like trusted sites, but they actually steal the data and credential. Phishing is one the most dangerous crimes which can be reduced only by increasing awareness.

Pretexting: Getting phone calls from someone who acts like a legitimate person and then asks for confidential information.

Conscious of Using Cloud: Smartphone has become part and parcel of our life these days. And all of its features are synced with cloud. Contact info, pictures we capture and all the files are synced with the cloud. But we do not care about the credential which is use to protect those info on the cloud.

Fake Job or Online Income Scam: As there are lots of unemployed persons available in our country, but Internet has become quite available so lot of us is trying to find jobs over the Internet. This makes them fall for fake jobs or online income scam.

Backdated Technology in Organization: Every time intruders try to make a new path to hack or destroy the system. On the other hand, tech giant industries or organizations are making new devices, patches, etc. to keep people safe from those attacks. To remain safe using updated technology can keep the users safe from the attack.

Giving Access of Info While Installing App: At the time of installing an app most of the time we don’t see which
kind of access it’s taking from our phone. There are some apps which can work like a RAT (Remote Access Trojan). It means, this can remotely access all your data including your camera and all the permissions has been taken from you at the time of installing it.

Games or Software Download from Unauthorized Source: We sometimes download games or software from unauthorized source which can be a trap of hacker. This kind of software or games also can act like a RAT.

Giving Info to Get Access or Download Something: There are some sites where if you want to get access of specific things it requires some info like credit card or other info, actually most of those websites are fake and a trap of hackers.

Sharing all personal info to the Internet: This is really a big problem in our country nowadays. We share all the information on the Internet which can be very much costly. Hacker’s first step to hack is information gathering and this can easily be done by checking your available information on the Internet.

Creating Email Account Subconsciously: Many people create email account and forget everything after doing specific works by using this. Then create new one when need other works to do.

Not Care about IoT Devices Security: IoT botnet attack is a dangerous attack in the world. This type of attacks can happen only because of IoT devices insecurity.

III. METHODOLOGY

In this section, prepared a list with the previously selected cybercrimes. This list is completed by searching recent reports and papers from the Internet. After listing those crimes, a survey titled “Awareness while using Internet in Bangladesh” is prepared to know the people’s actual knowledge rate, rate of them facing the crime and their prevention knowledge rate against those listed crimes. This survey also used to know some basic awareness knowledge of people. Researcher made a Google form and sent it to many university students, teachers, job holders and others to fill it up.

A. Configurations of the Survey and Tools

This survey form is divided into 5 sections. The first section has 10 queries asked about respondent’s information.

This including their daily Internet and social media uses, year since they use the Internet. Second section has 2 queries about respondent’s basic Yes/No knowledge on cybercrime. Another question is about their faced cybercrime knowledge.

In third section, listed all the cybercrimes which has been selected first by searching on recent reports and papers. List with all cybercrimes is presented to the respondent and ask them to select from the list if they have basic knowledge on them. They can choose multiple crimes from the list. This helped to know their basic knowledge on those crimes.

In fourth section, same list is given and asked to select from the list if they face any cybercrime among them. This helped to know the crimes face by the respondents most among the list.

Lastly also in section five, given same list and asked to select if they know to prevent them. This also helped to know the candidate’s knowledge on preventing those cybercrimes.

B. Selection Process of Respondents

The survey form is distributed into people from different sector. Link of the Google form is sent to the respondents through Facebook, email or other social media and told them to send the link to their friends also. Chain sampling, chain-referral sampling, referral sampling used to send the links to participants. Targeted candidates of the survey were minimum 16 years old. Because age above 16 should know about Cybercrime. This survey received total 290 responses. Among them, 51 sample responses are chosen which confidence level is high. This study chooses sample data to analysis the results correctly and clearly.

IV. CYBER CRIME AWARENESS ANALYSIS AND FINDINGS

This survey has 5 sections. All the analysis and findings had been divided on these 5 sections. Study also explained the sample data of total. Also explained every parts with appropriate graph.

A. Analysis on Respondents Demographics

The responses of the participants are come from different sector. Most of them are from Different Universities, Like: Daffodil International University, University of Asia Pacific, City University, University of Dhaka, Chittagong University, World University of Bangladesh and other. Some of them are college students, job holder at IT department, government job holder and other.
From the Fig. 1, we found that there are 68.6% male and 31.4% female response to this survey. According to a study by Grameenphone and Brac it is found that male and younger are dominating Internet [11]. Our study also proved their findings.

From the Fig. 2, it can be observed that, maximum respondent’s age is 16-25 which is 72.4%. This represents the young Internet user rate of Bangladesh according to this study.

From the Fig. 3, it is observed that 29.41% uses Internet 4-6 hours daily, 23.52% use 7-10 hours daily. So this also referred them as heavy Internet users.

From Fig. 4, it can be observed that participants daily social media usage duration rate is correspondly, 15.7% use 1-2 hours, 35.3% use 3-4 hours, 29.4% uses 5-6 hours and 19.6% use 7-10 hours.

And 64.7% of them use social media for education purpose, 70.6% use for chatting with friends and 56.9% use for just time passing.

**B. Cyber Security Knowledge and Victimization**

In 2nd section, first question is about participant’s basic knowledge on cybercrimes. If he/she select yes then he/she will go through rest of the section of the survey and fill up them. Either the survey will be submitted here with the given information.
In Fig. 5, it found that 68.6% of participants know about Cybercrime and rest of the 31.4% don't know about Cybercrime. They have no knowledge about Cybercrimes.

There is also a query asked and told to write the respondents if he/she experienced of facing any cybercrime in the past. Many respondents replied to this question and observed social media related problem they faced most. Such as hacking Facebook credential by phishing.

C. Analysis on Respondents knowledge about listed Cyber Crime

From the above section if respondents know about Cyber Security then she/he will go through this section.

In the Fig. 6, it has been observed that, 42.90% of them know about one ring scam, 17.10% know about steganography which is increasing day by day. 40% know about Cyber defamation rest 60% don't know about this crime. Nowadays on the social media we see lots of bad comments with slag words on celebrities social media posts or some other posts which represent the dangerous effect of cyber defamation.

Only 14.30% know about man in the middle attack, so rest of the respondents don't know about this and they use public Wi-Fi, browse and give personal info through insecure website which can make their personal info insecure. Email bombing is also a crime or attack by hackers to a business or normal people. We can see there 51.40% people know about this attack.

In section 2, we have seen some people shared that their accounts had been hacked by phishing. This show only 37.10% know about the phishing attack. Pretexting is used by hackers to collect information of targeted system which is the first step to hack a system. There only 17.10% know about pretexting.

Conscious of using cloud actually is not any kind of cybercrime title but this is a mistake which is happening by the users. People are using smart phones and synchronize its everything including photos and other personal info with cloud. But they are not careful about its security. The study find only 11.40% know about this problem which is really an alarming situation.

Fake job or online income scam has become a problem in Bangladesh but 82.90% people know about this issue. Only 20% people know that backdated technology use can be a problem for an organization or individuals. Cause hackers or intruders try to find new vulnerability. If someone want to prevent a system from attacks then it should keep updated.

In the era of smartphone, people use many apps to make their life easier and entertained. While installing apps they don’t check which kind of access its taking from the phone. On this way someone can spying on people's all activities. 54.30% people know about this crime.

Peoples also download games and software from unauthorized sources, which can also be a trap of an intruder. Study shows 48.60% people know about this problem. To browse or download a software, it sometimes need to give information, such as credit card details or other info which can be used in bad ways. 34.30% know about this that this is a way of crime.

Sharing every steps of real life on social media has become a trend in Bangladesh these days. By this, intruders can guess every attitude of people which can make them
vulnerable. Only 42.90% know about this serious problem. Creating email account unconsciously making cyber space fill up with wastage. 37.10% know that this is not a normal activity to create new email without using previous one.

On the mind of students or young researchers IoT devices become a hype but most of them are not careful about its security. IoT devices security is very much important either we can fall on a huge botnet attack. Study says 20% know about this issues.

D. Analysis on they facing Listed Crimes in Past

In Fig. 7, it is depicted that fake jobs and online income scam faced by 60% respondents and giving access while installing app 68.60% and 57.10% downloaded games or software from unauthorized sources. Giving info to get access or download something and sharing all information has the same 40% both.

Another surprising thing is only 5.70% know about man in the middle attack and they use insecure public Wi-Fi and websites. 20% know to prevent email bombing. Email bombing is nothing if someone know the prevention technique. If they doesn’t then it can be very much costly. Phishing has lots of variation, this study shows 31.40% know to defend it.

Only 8.60% can detect pretexting or know to prevent it. Another alarming thing is conscious of cloud usage which is securely used by only 2.90% people. Fake job or online income scam can be ignored by 45.70% people which is developing day by day as they are facing this most.

Study shows 8.60% people are concerned about backdated technology in organization or individuals which is really a risky situation. Giving access of info while installing apps is a serious mistake. Nowadays people are becoming accessible from anywhere in the world because of this issue.

E. Analysis on Respondents Prevention Knowledge

In Fig. 8, shows the prevention knowledge of respondents about listed cybercrimes. Before asking the question to the respondents, it made clear about those listed crimes to them by describing all of them in survey and asked to choose crimes they know to prevent. They can choose multiple answer. This study shows 17.10% people know to prevent one ring scam or they are careful about the crime. Only 11.40% people know to prevent steganography which is an alarming situation. 25.70% know to prevent Cyber defamation as a result people observe many shy things on social media.

Only 14.30% people care about access of software taking from phone or other devices at the time of installing it. 22.90% know to avoid games and software download from unauthorized source. Only 17.10% know to ignore fake websites which ask confidential info to access them or download something from them. 25.70% has knowledge that sharing personal info can make them vulnerable. 11.40% don’t create email account unconsciously. 34.30% are careful about IoT devices security.
V. CONCLUSION AND FUTURE WORK

This survey result completely shows us that cybercrimes related knowledge of Bangladeshi peoples is minimal. Government should take proper steps to increase the level of knowledge about cybercrimes. To make digital Bangladesh fully successful cybercrime knowledge is mandatory. Either attack like Bangladesh bank heist will make us suffer more in the future. Every related organization should be careful to enlarge the awareness level of our people. Hence, future work or research can make a proper education model where cybercrime awareness study can easily be implemented. And this will bring a healthy and secure cyber place for the people where everyone is safe.

References