Cyberattacks Prevention Awareness in Bangladesh

Tahmim Jawad
United International University
011183091

Amit Hassan
United International University
011183081

Raj Shekhar Karmaker
United International University
011193149

Mohammed Mubin
United International University
011191275

***Abstract*—This paper is an exploratory study to inform or raise knowledge among Bangladeshis on how to avoid cyberattacks. This study explains how humans' personal information might be compromised due to their daily behaviors. It also discusses how to avoid Bangladesh's most typical cyberattacks. How will we deal with cyberattacks if this occurs? Furthermore, all of the methods used in this paper to prevent or deal with cyberattacks are taken from experts; additionally, the information provided here is research- and survey-based.**

I. Introduction

Bangladesh is one of the fastest-growing countries. It is growing and prospering every day. As the country develops, the Bangladeshi people get more acquainted with various things. The internet is one of the things that Bangladeshis are becoming accustomed to. The internet is growing in popularity, as are related job sectors and internet users. However, security and awareness of cyberattacks are not growing at the same rate as the internet and technology. Bangladesh's growth is being hampered by the terrible conditions produced by low cybersecurity. In February 2016, a large cyberattack occurred at Bangladesh Bank, intending to steal 101 million dollars but only obtaining 81 million dollars. This is a significant setback for Bangladesh. Furthermore, the entire world regards us as the least cyber-secure country. Not to mention that the people of Bangladesh are subjected to cyber attacks on a daily basis. Ransomware (16.5 percent), malware (22.9 percent), phishing (7.8 percent), cyberbullying (50.2 percent), and other (2.53 percent) are the most prevalent threats we receive. In those circumstances, 22 out of 100 victims attempted to file a complaint, and 55 percent were unsuccessful in obtaining justice from the police.

So from above, we understand the vulnerable position of Bangladesh. The primary goal of this paper is to educate individuals on how to prevent and protect against cyberattacks.

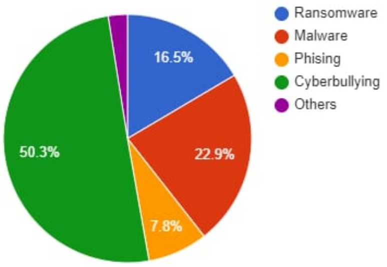

Fig. 1. Major Cyberattacks in Bangladesh

II. Background

The number of Internet users has grown dramatically in the last decade. It's happening all across the world. Every country, from underdeveloped to developing to developed, is today confronted with the benefits and drawbacks of technology. It is growing, and cyberattacks are becoming more sophisticated and complex as a result. Despite being a third-world country, Bangladesh has experienced a technological revolution. A Bangladeshi adolescent has easy access to computers and other electronic devices. As a result, they have ample opportunity to engage in hacking. In Bangladesh, hacking has already become a serious issue. Young people are becoming increasingly interested in hacking for the thrill it offers. Not only young individuals but also the mainstream media, are frequently involved in hacking and revealing private information. Bangladesh was subjected to its first cyberattack on September 19, 2007. The majority of Bangladesh's internet service providers (ISPs) were hit by a denial of service (DoS) attack. Following that, the Rapid Action Battalion (RAB) website was hacked in 2008. Shahee Mirza, the hacker, stated on the RAB website, "You have no idea what cyber security is or how to protect yourself." In 2010, a student filed the first cybercrime case in Dhaka. The case accuses two persons of uploading false information to a bogus account on Facebook, the major social networking website. The Mahmudur Rahman case is one of the most prominent cybercrime cases in Bangladesh, and it may be considered the country's first cybercrime case. In December 2012, Mahmudur Rahman, the creator of the Bangladeshi weekly Amar Desh, was sued in accordance with a High Court order for publishing reports on a Skype conversation between former International Crimes Tribunal chairman Justice Md. Nijamul Huq and an expatriate legal expert. On December 13, 2012, he and Amar Desh publisher Hashmat Ali were sued. On February 15, 2012, a group of purported Bangladeshi hackers known as the 'Black Hat Hackers' hacked over 250,000 Indian websites, including vital sites such as the Border Security Forces (BSF) website. In some cases, propaganda actions are also considered cybercrimes. Propaganda is biased and misleading information used to promote or advertise a specific political cause or philosophy. It causes tension and alarm among the general populace. For example, consider the Ramadan violence in Cox's Bazar in 2012. Someone using a bogus Facebook account posted a photo of the Holy Quran being desecrated on its wall. The bogus account was created in the name of a Buddhist man. This message infuriated the local Muslim community, and they attacked innocent Buddhist residents without first checking the veracity of the Facebook account. A large number of Buddhist temples, monasteries, and homes were destroyed. Also, 26 government institutions were hacked in 2012. In 2013, one government bank (Sonali Bank) was hacked, and the hackers made off with USD 250,000 with no fuss. Here are some examples. The threat of cyber intelligence, on the other hand, was primarily provoked by the 2016 Central Bank theft. In Bangladesh, it was one of the world's largest bank heists in cybercrime history. Through the SWIFT network, they were able to steal USD 101 million from the Bangladesh bank account at the Federal Reserve Bank of New York. Dridex (a banking Trojan) was later discovered to have been utilized in this theft. In 2014, the Bangladesh Cyber Security Strategy was launched. And its objective is to protect the cyber world from security threats, dangers, and national security difficulties. It follows the IMPACT (International Multilateral Pact Against Cyber Threats). The goal is to develop a vision for keeping the country secure in government, private, citizen, and international cyberspace. However, after such a large-scale heist, Bangladesh can easily assume the security state of our cyberspace.

III. Literature Review

On this paper [3], it talks about:

Massive cyberattacks A nationwide computer network in Estonia was crippled by a cyberattack in 2007 there. In 2017, a significant ransomware assault hit Eastern Europe. The malware specifically targeted national government agencies, banks, utilities, and other crucial infrastructure and businesses. The Georgian nation was the target of a significant cyberattack in October 2019. Over 15,000 websites were taken down by the attack. The websites included local newspapers, TV stations, banks, government offices, and courts. There was widespread terror across the nation.

U.S.A. prime target According to cyber-forensics company FireEye, America is the main target of foreign cyber-attacks. There were a number of significant cyberattacks in the United States in 2018. A former senior DHS cybersecurity officer said that the Russians had successfully gained access to hundreds of American utilities and power firms. A well-executed cyber-attack might bring down the electrical infrastructure, cut off electricity to a sizable portion of the nation, and compromise crucial financial or governmental information. Another cyber-attack in 2018 revealed a gas pipeline network's vulnerability. Due to a ransomware attack, the Atlanta municipal government stopped down in March 2018. Courts, city employees, and police officers were unable to access their computer information. A ransomware assault left Atlanta immobilized for more than a week. Atlanta paid USD 2.6 million to recover from a ransomware crisis that cost USD 52,000. Such a devastating cyber-terrorist strike may render the country helpless. People experience anxiety, dread, unease, and a crisis mood when they feel threatened. People may panic during a crisis and act selfishly or irrationally to flee due to a loss of functioning, control, and knowledge, as well as a lack of communication. Singer24 talks on the importance for disaster preparedness and training as well as how individuals react to and deal with tragedies. Long-term effects, reactions of the rescue and relief personnel, and psychological first aid are all possible. However, this discussion focuses on actual physical harm, including fatalities and injuries (such as earthquakes and building collapses). Typically, a cyber-attack only renders a program inoperable. Physical destruction is rare. A cyber-attack will cause a different kind of terror. The importance of awareness may be shown in the importance of authorities communicating clearly in order to prevent panic.

Education/awareness training Organizations are aware of the value of training and education in user security awareness. Education increases users' awareness of security issues and modifies their online behavior. However, ongoing awareness training gradually loses its effectiveness. Refresher training will be required to reduce optimistic bias and other forms of unrealistic thinking. Users need to be regularly reminded by organizations to be cautious about security. Users must be continuously kept vigilant and proactive by an instructional program, and they must develop good security practices. To deal with policy, processes, and tools, the majority of commercial organizations perform security awareness training. Protective conduct has been the subject of research relating to security awareness and education. The organizational system is the main topic of the training rather than a catastrophic national hack. However, there is no evidence in the literature that suggests that education and training reduce anxiety about a catastrophic national cyberattack. The Stimulus Organism-Response (S-O-R) theory, developed by Mehrabian, Russell, and Jacoby, will be modified to form the basis of the proposed theoretical framework. According to the "S-O-R" hypothesis, external stimuli will awaken or have an influence on an organism's emotional and cognitive state, which will cause a reaction. By demonstrating seven components inside the "S-O-R" framework, Jacoby expanded on this theory:

1) Environment (E) is the source of stimulus (S). The factor that awakens the person is known as the "stimulus." The stimulus is transformed into informative data. Some stimuli might not cause the organism to process information either consciously or unconsciously. The emotional and cognitive states of a person can be triggered by

environmental factors.

2) The unconscious processing of incoming inputs is known as automatic processing. More exposure can occasionally result in unconscious processing and learning.
3) An experimental repository of mental processes, emotions, and feelings is an organism (O). The term ”organism” itself refers to a person’s cognitive state and functions, including their long-term memory, past experiences, beliefs, and attitudes. Cognitive workspace, memory, awareness of motivations, emotions, perceptions, and cognition, and awareness of being aware are all components of consciousness.

In this paper [1] order to ensure that the most recent defenses are in place, assaults are immediately recognized, and countermeasures may be performed, humans have a role in maintaining and updating systems. This calls for policies to be in place and for people to be informed of what is necessary, as we know that user ignorance can lead to the introduction of additional vulnerabilities, such as the use of weak passwords, the installation of dubious software, and the use of insecure devices and applications. The public anticipates that the government will accept accountability, but if individuals do not also assume some responsibility, the steps governments implement may not be adequate. It is more challenging to effectively frame cybersecurity when there isn’t a clear antagonist. Giving the villain a face is the obvious conclusion to draw from this observation. Give specific instances of unambiguous bad guys, such as cyber gangs who undoubtedly commit extreme crimes. Describe their tactics in detail, including how they can wreck the lives of their victims. Of course, these villains do not represent the entire family of clear-cut and ambiguous antagonists, but this is not the problem. The difficulty is that framing cybersecurity will continue to be difficult without a distinct and unmistakable antagonist. There will be obvious victims if there is a clear villain. This makes it simpler for individuals to relate to the fight against cybercrime.

This paper [2], tells about society now facing a higher security risk in cyberspace than ever before as harmful cyberattacks develop in response to the volume and complexity growth of internet technology and mobile applications. Organizations have implemented sophisticated monitoring systems, such as password management, data leak prevention, and content monitoring technologies, as well as security technologies, such as firewalls for perimeter defense, to secure important organization data and information system assets. These products provide technical answers to the cybersecurity issue, but they fall short of offering complete security. Users may fail to follow the organization’s information security regulations completely. Internal dangers brought on by employees’ deliberate and unintentional disclosure of sensitive information are a severe problem.

IV. Aim and Objective

It is always emphasized that a problem usually comes with its own seeds of solution. This statement signifies the need for defining the objectives of the research. The main objective of the research is to create awareness among humans in Bangladesh about how they can prevent or deal with cyberattacks. In order to achieve this goal, the people of the country must be aware of the problem of cybercriminal activities. People must understand how the internet, as well as the cyber world, operates. So basically the goal is simple:

- To know how to make your website/profile/account secure.
- To know about the hacking methods.
- To find out the way to prevent hackers, if your account/profile/website got hacked.
- To know which website is not a trap.
- To know how to secure your device.

V. Researched Questions

We performed a poll to better understand the individuals and their lack of information. We obtained a sense of people’s understanding of cyberattacks and their reactions to them from it and the question was:

1) Do you know any of those cyberattacks from below?
   Malware
   Phishing
   Smishing
   Ransomware
2) Have you ever faced a situation where your or a familiar person’s account was hacked?
3) If it happened, what did you or they do to get their account back?
   Nothing like this happened to me
   Tried to recover their account by email
   Nothing
   I don’t know
4) Have you ever had the mistaken belief that your gadget had been hacked?
5) Have you ever tried or are you currently using antivirus to protect your device?
6) Do you think the police will give you justice if you report a cybercrime case?

VI. Data Collection and Method

We used both primary and secondary data collection. The methods are

- Primary

  Survey: We conduct a survey on different types of people.

  Focus Group: We also talked about it with a variety of folks.
- Secondary

  Internet: We browsed a lot and acquired as much information as we could.

  Research Paper: We also read a few papers in order to gain a better understanding of the issue.

VII. Methodology

A. Cyberattaks Method

Generally, Bangladeshis are subjected to four types of cyberattacks.

- Phishing
- Smishing
- Malware
- Ransomware

Phishing: Phishing is a method in which a hacker develops a website that looks identical to the original. Then they send the link via message, persuading people that it is genuine. The victim then inputs his private information, such as his credit card password, and so on.

Smishing: Smishing and phishing are as close as their names suggest. The only difference is that the hacker can use the URL to install harmful software on your device.

Maleware: Maleware is a type of software hacker that installs software on other people's computers without their knowledge. They can use the software to pull money and accomplish a variety of other things.

Ransomware: Hackers gain access to your device using this way via links or emails. The ransomware employs simple asymmetric encryption algorithms to encrypt a user's files, making them impossible to decrypt without the key.

B. Cyberattacks Prevention

Phishing & Smishing Prevention: There are some techniques to spot a phishing and smishing scam.

1) Learn to identify phishing scams
2) Do not click on any random link
3) Do not giveaway your password to any random site
4) Continuously change password
5) Use anti-phishing ad service
6) Always update your software
7) install the firewall

Malware Prevention: The most liked method to prevent such attacks is.

1) Always have anti-virus and anti-spyware.
2) Use authentication.
3) Always try to use a non-administrator account if it gets hacked it won't be able to access all information.
4) Never give more access than necessary to the application.
5) Keep your email from getting spam.
6) Always update your software.
7) Always try to notice any unauthorized activity.

Ransomeware Prevention: Tips that are followed to avoid such attacks are.

1) Always have anti-virus and anti-spyware.
2) Always have Backup data.
3) Network segmentation to avoid virus spread through the network.
4) Never give more access than necessary to the application.
5) Keep your email from getting spam.
6) Always update your software.
7) Limited user access.

C. Cyber Safe Protocols

To stay safe online, you must do the four things listed below.

1) Turn on multiple authentication.
2) Update Your software regular based
3) Think before clicking any links.
4) Try to use strong and diffrent pasword for every platform.

VIII. Result

We believe that if others read or use our way, they will first learn about how the hacker attacked us. Second, they will understand how to avoid being attacked. All of the information shown here was gathered from a number of organizations. If humans use this strategy, their chances of being attacked will be considerably reduced.

IX. Fututre Work

All we did here was share and collect all of the information and tips to avoid this attack. However, in the future, we want to work on how to handle it if you have already been attacked, how to get help from the law, what to do, and so on.

X. Conclusion

The major goal is to raise public awareness about this cyber attack. What they can do to avert such circumstances We decided that the most popular tips come from a variety of respectable sources. Its goal is to motivate individuals to become more involved in cybersecurity. It's a fantastic and vital field, however Bangladesh lags behind in this area. We hope that our report will encourage other people to work in this field to assist average people in dealing with such issues.

References

[1] Marijn Janssen Hans de Bruijn. Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1):1–7, 2017.

[2] Li Xu Ivan Ash Mohd Anwar Xiaohong Yuan Ling Li, Wu He. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45:13–24, 2019.

[3] Garry White. Generation z: Cyber-attack awareness training effectiveness. *Journal of Computer Information Systems*, 62(3):560–571, 2021.