Cyber Security, The Digital Antidote Of Cyber Crime

Md Shabir Khan Akash
Roll: 1603108

Md Shohanoor Rahman
Roll: 1603112
Department of Computer Science & Engineering
Rajshahi University of Engineering & Technology

***Abstract*—The topic that we are interested to discuss and focus on our technical writing is involved with the term "Cyber Security". This term is quite familiar in the era of this digital world and modern technology. Cyber Security is the protection or shield against the term 'Cybercrime' that is defined as a crime in which a computer is the object of the crime (unethical hacking, phishing, spamming) or is used as a tool to commit an offense (cyber bullying, hate crimes). Cyber Security can possess the potential of removing cyber crime from the cyber world, but sometimes cyber security also lags behind from taking necessary steps against cyber crime. Unfortunately, there's no 100% guarantee that even with the best precautions some of these cyber crimes won't happen to you, but there are steps that can be taken to minimize the chances.**

I. Introduction

In the most basic sense, cybersecurity refers to practices, policies, and technologies that are designed to protect computers, servers, networks and connected devices from unauthorized access, while also mitigating the risk of damage in the event of an intrusion [1]. Cybersecurity includes both physical preventive measures as well as digital.So as example,

- Physical forms of cybersecurity: Locked doors and video surveillance systems, Security Sensor Vaults etc.
- Digital forms of cybersecurity: Antivirus softwares, Network monitoring services, data encryption, Cryptography etc.

The field is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Due to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world [2]. Cyber security is the name for the safeguards taken to avoid or reduce any disruption from an attack on data, computers or mobile devices. Cyber security covers not only safeguarding confidentiality and privacy, but also the availability and integrity of data, both of which are vital for the quality and safety of care. Security breaches can occur when we use paper records, send information using fax machines and even verbally. However, the consequences of security breaches with digital information are potentially far more severe, as information can be distributed more easily and to a far wider audience.

Cybercrime generally occurs with that internet user who doesn't really concern or care about cyber security. As from the cybercrime perspective, Hackers are one of the real culprits of this notorious activities. From the cyberbullying to unethical hacking, Online Money theft each and every cybercrimes of the day to day modern life are quite interrelated.Cybercrimes are classified into some types by their activity and consequences.Computer or cybercrime encompasses a broad range of activities [3]. These are-

- Financial fraud crimes
- Cyberterrorism
- Cyberextortion
- Cyberwarfare
- Online harassment
- Drug trafficking
- Spreading Offensive content

Though there are enormous number of cybercrimes up there on the web but proper learning about web, some precautions made by the internet user can certainly make the bad things disappeared right away.

II. Methodology

Cyber security is a constantly changing area and moreover often it may seem quite confusing. However, there are quite many effective and relatively simple steps that can be taken to protect information and protect a user and his/her organization.By Taking some simple and effective actions and practicing safe behaviors will reduce online threats as well as cybercrimes.

Some effectively important steps to improve cyber security are the following:

A. MOVING AWAY FROM USING UNSUPPORTED SOFTWARE

This is when software e.g. operating systems,apps,web browsers etc. are no longer updated by the supplier. Although the software will continue to operate, it will no longer protect against online threats through updates or patching (a software update, often relates to improving security). If a security weakness

is discovered, software can be compromised and become vulnerable to a cyber-attack. For benefits to be gained from up-to-date security measures, such as improved speed and efficiency, only use supported software on your systems and devices. If unsupported software is being used, ensure that properly manage the risk by having a strong firewall and up-to-date anti-virus and/or anti-malware software.

B. MANAGING SECURITY RELATIONSHIPS WITH SUPPLIERS AND PARTNERS

As organisation grows and works with more suppliers and partners,there become a link in one or more complex supply chains.It is important to observe good practice (and in many cases, compliance) because vulnerabilities will place not only own organisation at risk, but also others within the supply chain. If use third-party managed IT services, contracts and service level agreements should be checked, and ensure that whoever handles systems and data has security controls in place.

C. BACKING UP OWN DATA

Safeguard of most important data by backing up to a secure external hard drive or storage system based in the Cloud. There also ensure regularly test backups and, if confidential data off-site e.g. the Cloud be saved,all appropriate data protection measures and government standards and guidance that relate to health and social care organisations must be followed.

D. USING STRONG PASSWORDS

Passwords should be easy to remember and difficult to guess.Numbers and symbols can still be used but using three random words is the key to creating a strong password.Using a strong, separate password for email and other important accounts is a good practice.For most important accounts, if it's available, there should use Two-Factor Authentication. This means involving a second step after entering your password e.g. providing a fingerprint, answering a security question, or entering a unique code sent to users device.

E. RUNNING UP-TO-DATE ANTI-VIRUS SOFTWARE

Computers, tablets and smartphones can easily become infected by small pieces of software known as malware. Common types include viruses or spyware and ransomware. To help prevent infection, install internet security software, like anti-virus and/or anti-malware on devices and keep it up to date.

F. TRAINING STAFFS OR FRIENDS TO BE CYBER AWARE

Make sure staff are trained to know the benefits of operating digitally, but are also aware of cyber security threats and how to deal with them. Due to the rapid development and changes in digital technology it is a good idea to add cyber security to annual training plans/ matrix.

G. DELETEING SUSPICIOUS EMAILS AND AVOID CLICKING ON UNKNOWN ATTACHMENTS OR LINKS

Email is an excellent communication tool but is frequently used to deliver unwanted or unwelcome material, often referred to as 'spam' or 'junk' email. Avoiding respond to such 'phishing' emails even if they seem to come from a company or person may be known, because doing so can confirm the address is legitimate to the sender.

H. ALWAYS DOWNLOADING AND INSTALLING THE LATEST SOFTWARE AND APP UPDATES

Software updates are designed to fix weaknesses in software and apps which could be used by hackers to attack on device. Installing them as soon as possible helps to keep the device secure.

REFERENCES

[1] https://www.tw-security.com/introduction-to-cyber-security

[2] Stevens, Tim (11 June 2018). "Global Cybersecurity: New Directions in Theory and Methods". Politics and Governance. 6 (2): 1–4. doi:10.17645/pag.v6i2.1569.

[3] Gordon, Sarah (25 July 2006). "On the definition and classification of cybercrime" (PDF). Retrieved 14 January 2018.