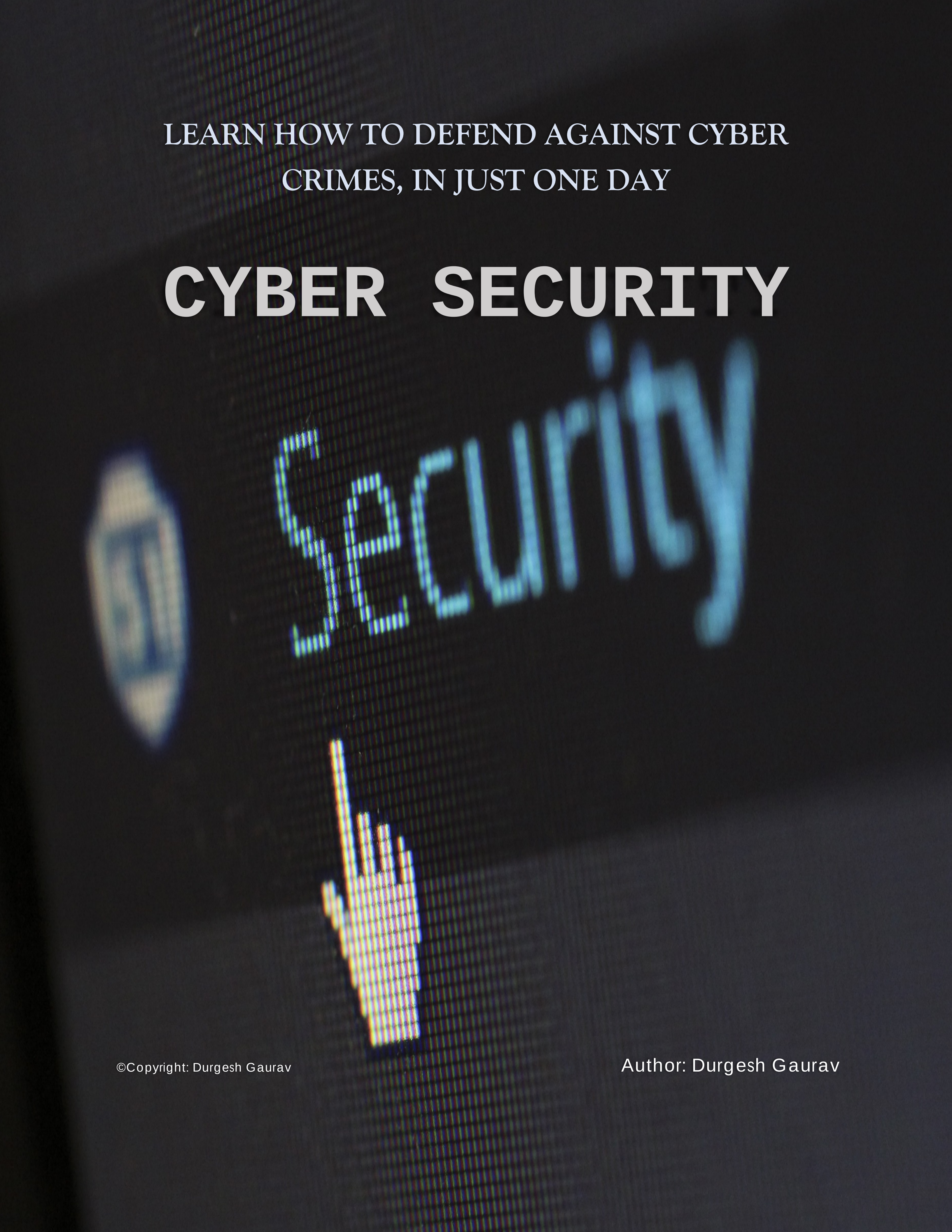
LEARN HOW TO DEFEND AGAINST CYBER CRIMES, IN JUST ONE DAY

CYBER SECURITY



Author: Durgesh Gaurav

Learn How to Defend Against Cyber Crimes, In Just One Day

Learn about cyber security in no time, understand the cyber-security concepts and defend against growing cyber-crimes.

Cover-page image credits: Pixabay

A book by Durgesh Gaurav to every enthusiast.

Learn How to Defend Against Cyber Crimes, In Just One Day by Durgesh Gaurav

www.DurgeshGaurav.com

For permissions contact:

Info@DurgeshGaurav.com

PREFACE

The purpose of the book is to educate and spread awareness about cyber-security and its necessity in our lives. Knowing some basic cyber-security tools would be helpful to protect ourselves from major and minor cyber-crimes. The book focuses on the cyber-security building blocks and defensive concepts along with cyber-threats protection. The regular advancements in technology are also creating a mandate for us to be alerted to ensure the safety of self and people around us. Keeping every technical device secure is virtually impossible for any organization, government or any group of cyber-security professionals. Mass awareness is required to keep every individual secured against the cyber-threats, vulnerabilities and their consequences.

ABOUT THE AUTHOR

Durgesh Gaurav is dedicated to creating and maintaining safe cyber-space for organizations and individuals. While working in the software engineering industry, he developed a strong passion for cyber-security. For fun, he actively engages in analysis of security breaches in the industry and creates solutions to both prevent and combat such threats. He has been also performing analysis and investigation in digital forensic as one of his passions.

Durgesh holds a Bachelor of Engineering in Electronics and Instrumentation and is currently pursuing his Master of Science in Cyber Security. If you have questions or concerns, write at info@durgeshgaurav.com.

TABLE OF CONTENTS

CHAPTER 1: CYBER TECHNOLOGY

1.1 THE TECHNOLOGICAL ERA

The ongoing growth and development of technology and its widespread adaptation among us has transformed our society. Our lifestyle continues to be affected and transformed. Many facilities are just a click away. Whether you need a flight ticket or you want to do shopping, everything can be attained digitally. Although this digital transformation is beneficial however there stand opportunities for its misuse.

Some uses of technology are in the form of technical devices such as smartphones, laptop computers, PDAs and other electronic devices. These devices are connected to the Internet which is known as the network of networks. However, the big question is how secure these devices are? Moreover, how secure we and our families are on the Internet?

We are connected to the Internet through billion of devices located throughout the world. Some of the devices and their master users (who are connected to the same Internet) can very easily track and harm our online activity. They are known as “hackers”. It is highly possible that we can become a victim of a cyber-crime.

Let’s understand first about cyber-threats and their classifications. A cyber-threat is any threat that happens digitally, whether it is the computer or smartphone they all comes under cyber-technology. A cyber-technology covers all digital hardware and software, whereas information technology only holds the software part.

Technology is available to everyone and people use it in both good and bad manner. We can assume it as electricity, it goes to every house, but it then depends what someone want to do with the electricity. Some may want to use it to power their household items like bulbs and kitchen electrical appliances, but a few may use it to perform dangerous experiments.

1.2 IMPORTANCE OF CYBER-SECURITY

Our involvement in technology has not only grown but it has also been integrated. We use computers, smartphones, PDAs or any other digital devices to fulfil our daily tasks. A majority of the digital devices are connected to the Internet. Whenever we use the Internet through our devices, our information flows from the device to several networks through the internet.

When our information travels from one place to another, the information can be viewed or stolen by someone during transaction. The information intercepted by the third person can be used to hack the bank accounts or perform any malicious activity using the hacked information worldwide.

1.3 BENEFITS OF CYBER-SECURITY

A computer is composed of several hardware and software. The hardware and software contains several components within. A single error within any component is known as bug which can produce high security risks to the overall system. A computer or any device may contain several bugs which produces vulnerabilities and other threats. A single vulnerability can cause serious blows to the digital security.

Cyber-security provides an assurance that the data is secure and it cannot be accessed or exposed without your permission. It prevents unauthorized access to the networks and the connected computers. It provides protection against virus, trojans, and all types of malware and prevents data theft to ensure privacy and safety.

Hacking is on the rise and if we are not alert then our computers and devices are open to threats from many sources. The threats are increasing in numbers and dealing with them requires some understanding of cyber-security. Cyber-security provides us ways to appropriately configure and manage the computers and other devices to an optimum level of security. Configuration management, security tools, prevention techniques and regular monitoring plays an important role to keep up a safe space for self and family.

CHAPTER 2: CYBER-CRIMES AND CYBER-THREATS

2.1 CYBER-CRIMES

The cyber-crimes are several and can be classified into various categories such as financial cyber-crimes, cyber-frauds, identity theft, privacy violation, intellectual property theft, and cyber-bullying. In simple words, any crime which is performed using a computer or any digital device is a cyber-crime. It is not only about the cyber-crimes, the Internet is also a threat to your privacy. Your Internet service provider known as ISP and other connected third parties tracks your online data.

Whenever you go online, your data gets tracked. There are various techniques through which hackers can track data. We will discuss about them later in this book. Hackers can steal information such as social security number, bank details, friends contact list, medical history or any other personal details. Once the attackers have the details, then the attacker can create a fake identity and can impersonate the victim on the Internet and commit numerous crimes under victim’s name.

2.1.1 FINANCIAL CYBER-CRIMES

Financial assets are confidential for everyone. Someone can get into a bank account and steal all available financial assets and that is common in the cyber world. We all are vulnerable to cyber-threats; especially children are more vulnerable if they are not technical enough to handle cyber-security issues themselves. The cyber-criminals always look out for ways to steal financial assets, personal information and the social identity. It also includes several other harmful crimes such as performing data breaches where computer and network securities are broken, spoofing using phishing or spear phishing, account hack, use of malware and ransomware.

A cyber-criminal can access required information by hacking into an account using the gathered information or by attacking the servers. By using hacking tools and techniques it is highly possible that hacker may get access to anyone's financial accounts. A hacker can run a few commands or install a few tools onto a person's computer, smartphones and any other digital device and gains control over it.

The hackers may create a bridge to command and control any computer or network to get access to the financial or any other information. The scope of the book is limited however, we will cover some of the information on how the cyber-attacks happens in chapter 3 and 4. We will be discussing some monitoring tools and techniques to prevent such attacks in chapter 5.

2.1.2 CYBER-FRAUDS

Cyber-fraud is common in the digital world. Several false promises are made online or false offers are provided. Any false commitment made over internet to someone is known as cyber-fraud. Many malicious websites and hackers make pseudo advertisements and offers. People fall prey to these advertisements or offers or contents and provide their sensitive information without thinking twice. Once the information is provided, the cyber-criminal uses it for criminal activities or may use it directly to fetch the financial assets. Identification of such malicious content is essential for security.

A presence of a good antivirus and its add-on on your web-browser will provide malware protection and can help preventing such type of attacks. If a computer or any similar device gets exposed to the malicious website, emails and false advertisement then hackers get a chance to install more malicious tools into the device to perform future attacks easily.

However, precaution and alertness is the key to stay secure against any type of fraud. Website and companies have digital certificates which can be viewed easily and should be checked for validity and security.

2.1.3 IDENTITY THEFT

Internet browsing is common. Whichever website we visit may or may not require login credentials. Some of the websites may need our personal details such as name, contact details, social security number, health insurance details, credit card number or other financial particulars. Numerous crimes can be performed easily with the stolen identities.

Hackers are using other people's identity to hack and steal information from private and government resources. These resources could be from minor information to top secret government information. It is important to protect both personal and official information from all unknown sources. Revealing information may lead to serious cyber-crimes.

2.1.4 PRIVACY VIOLATION

In the cyber-space, many hackers work to gain information to invade into someone's privacy. They may look to steal or break social media accounts and bank accounts. Once a hacker gets the information they may look forward to accessing the accounts. Stalking social media, anonymously texting, emailing, stalking, etc. falls in this category.

2.1.5 INTELLECTUAL PROPERTY THEFT

Innovation is the key to development and growth. Technology is growing and generating new products and services to simplify our daily requirements. The growth of the Internet has simplified banking and other services. Many technologies are being used to perform such services. They were developed and released for public use. For example, a new car design which runs on electricity was an innovation. The owner can claim for the ownership rights of invented product by filing for a patent.

To develop a product, innovation, creativity, time and research are required. The value of product design information is high, for an example, the secret recipe of Coca Cola or Pepsi is everything for their business and if the recipe gets stolen then it would be a huge loss for their business. A hacker can attack a company and steal the sensitive information. The hacker could sell it or alter it to make an alternate product and get it patented. In this case the original owner loses the credibility and suffers a huge monetary and brand value loss.

2.1.6 CYBER-BULLYING

Social networking is quite common today. Social websites such as Facebook, Twitter and other applications like emails or online chatting applications are popular among us. Social media can be misused by someone to spread negative against anyone. These are accessible to everyone and can be spread at a high rate. Someone may easily become a victim of cyber-crime.

Cyber-bullying is one of the major cyber-issues all over the world among young people, especially within high-school children. Cyber-bullying is a crime which may give birth to threat, embarrassment and humiliation to the victim. Anything which is posted online against someone that leads humiliation, threat or any kind of embarrassment to that person so that it may result suffering in psychological, social or any mental form is known as cyber-bullying.

Cyber-bullying is not only a one-time threat or a crime. It becomes recurring once initiated. It is often noted that people, especially children, suffering from cyber-bullying do not report because they either feel ashamed or threatened to report such crimes. It may result in negative behavioral changes within themselves. Cyber-threats are difficult to be avoided and need to be reported to the appropriate authorities. In a case study, Hannah Smith[1] a schoolgirl aged 14, committed suicide in her room due to being bullied though comments about her body weight and a family death on Ask.fm which is a social question answer website.

Cyber-bullying also attracts more people who force the victim to live a miserable life with depression, anxiety, and abstract self-confidence[2]. This may lead to a fear or embarrassment in the victim's mind and they do not discuss life related issues to anyone. It can happen any time to anyone.

It has been often noted that the depression leads to loss of appetite followed by weight loss or increased appetite followed by weight gain, improper sleep, loss of energy, and loss of interest in healthy activities[3]. It indirectly leads to a poor academic and life performance. It is necessary to take precautions to protect our families. We will be discussing the four kind of cyber-bullying which are common in practice.

2.1.6.1 CYBER-STALKING

Another type of cyber-bullying is known as cyber-stalking. This is common in teenage life. Financial information, social activities, text message, emails, voice calls, etc. and misuses it to defame the victim or for any other obscure activity. It is a form of cyber-bullying in other terms. An easy access to technology has unfortunately evolved this crime.

The problem with the Internet is that it gives anonymity which makes the criminal difficult to track and identify. The criminal may also monitor the victim's activity. It may also result in child exploitation which is a very serious crime and should not be neglected at all.

[1] Puresight.com. (n.d.). Hannah Smith | PureSight | Real Life Stories. [online] Available at: http://www.puresight.com/Real-Life-Stories/hannah-smith.html [Accessed 4 Aug. 2017].

[2] Kidshealth (n.d.). Cyberbullying. [online] Kidshealth.org. Available at: http://kidshealth.org/en/parents/cyberbullying.html# [Accessed 11 Jul. 2017].

[3] Dualdiagnosis (n.d.). Depression and Addiction | Dual Diagnosis. [online] Dual Diagnosis. Available at: http://www.dualdiagnosis.org/depression-and-addiction/ [Accessed 11 Jul. 2017].

A cyber-stalker can use computers, smartphone applications, phone calls, messaging services and even other communication devices or applications to perform a stalking. Cyber-stalking can impact self-confidence, career, isolation from friends and family due to humiliation and embarrassment. We will discuss how to prevent such crime against the innocent people later in this book.

2.1.6.2 FLAMING

It is another form of cyber-bullying which focuses on online forums, chat services, gaming streams and other communication platforms to defame the victim by posting negative, abusive, and aggressive comments against the victim. The purpose of the cyber-bully is to embarrass and break the self-confidence of the victim.

2.1.6.3 POSING

If someone impersonates the victim and post written, verbal/audio or video materials to ruin the reputation of the victim then it is known as 'Posing'. In a scenario, someone hacks into a victim's Facebook profile and posted something embarrassing, threatening, abusive, or blackmailing content. Unaware of the hack, the victim's friends and family believes that the post came or originated from the victim. This is becoming a serious concern as hacking is growing along with technology.

2.1.6.4 TRICKERY

Often the victims get tricked into revealing the information when tricked by a cyber-criminal. When victims do not possess sufficient understanding of the system and process, it is easy to trick them into a trap. Hackers use this technique to misuse the revealed information to exploit the entire system. It is an easy way to extract information rather than performing actual hacking to infiltrate the home or enterprise system.

2.2 CYBER-THREATS

Another important subdivision of cyber-security is malware which is one of the biggest threats to cyber-security. It is a malicious software that can be defined as a computer application or software written with specific codes, designed to disrupt or destroy the functionality of a computer. A hacker can install a virus in a computer and make it infected. The hacker then can perform various operations to steal information or execute commands on the same computer.

Often seen ransomware is a problem because of malware. A hacker may gain access to a computer and encrypt the data. Once the data is encrypted the hacker may call for a ransomware. You might have heard about 'WannaCry' ransomware in the news lately.

The hacker may also delete data or do whatever they want with the help of malwares. Stealing information and using it to execute any crime can be done easily. These threats are present everywhere and hackers can exploit any vulnerability present in the computer system.

Hackers always look for victims to make a mistake. They lure users and infect their computer with multiple techniques. They send offers in email attachment that contains embedded applications in the form of games, audio, images, video or documents. These are malware and they are very common. Once a user clicks on any one of these files, the embedded software is downloaded secretly into the computer. Many times, people fall prey to malwares as they are not aware of such traps.

A technique called phishing and spear phishing is common for email hack process which is again executed by sending infected attachment in emails. Once the attackers gain access to the computer, they can also gain access to the computer network. Hence, computer and the network becomes their slave. That means entire families could be at risk. We will discuss later in detail, how to deal with issues we have discussed so far in the book. In order to proceed further we need to first understand some basics of computer and Internet.

CHAPTER 3: COMPUTER NETWORK

3.1 NETWORKS AND THE INTERNET

The Internet is the largest network, with approximately 7,519,028,970[4] number of computers connected to it. An enterprise may have a small office network which is connected to the Internet service provider (ISP). The ISPs provides Internet to offices and to homes and connects them to internet.

We can think of the Internet as a large spider web where a thread is connected to the other threads, similarly a computer is connected to other computers. Similar to how we have addresses for our houses, the digital devices also have addresses. They are known as Internet Protocol (IP) addresses. We can identify a person's details such as location, name and user's other details using the IP address very easily.

We have one more address that is the hardware number of your device which is known as Media Access Control (MAC) address. We can easily identify any device using MAC address and its geographic location using the IP address. We need to know this to understand the problem and take necessary actions whenever needed. Since a computer is connected to an ISP, the ISP can track the data, so does a hacker.

All digital devices are connected to home router which is directly or indirectly connected to

4. Internetworldstats.com. (n.d.). World Internet Users Statistics and 2017 World Population Stats. [online] Available at: http://www.Internetworldstats.com/stats.htm [Accessed 12 Jul. 2017].

a modem. Modem is responsible for the conversion and separation of digital connection signals from ISP into an Internet data packet or an Internet connection in simple terms. In harmful contents. However, it cannot block all of them. Therefore, the user has to be responsible for all the security activities happening over the Internet.

Every connected device in home has a unique IP address and they all are connected to the router. The router is responsible for providing connection to the modem and the modem connects user to the ISP. But, we only hear of only one IP address which is the home IP address and not the device IP addresses. So, what is happening here?

Actually, when any of the devices makes a connection to the router, the router then maps an IP address to the device. For example, when we go to a restaurant with family, a waiter takes our order for food and notes it down in a notebook. The waiter remembers the seating positions and manages everyone's order flawlessly. The waiter transfers the order to the chef who cooks the food and again the waiter brings the food once it is ready and serves it in the same order.

Similarly, the router takes everyone's order whosoever have access to the router. Once it takes everyone's order, like the waiter it transforms everyone's IP address into one IP address using Network Address Translator (NAT) and remembers each address in its memory. This is known as mapping, this prevents the device from being discovered by anyone on the internet.

Another important aspect of Internet communication is port numbers. Computers have special doors within called ports. The applications like web browsers such as Google Chrome, Firefox and Internet Explorer, Microsoft Office 365, antiviruses, etc. that we use on our computers has port numbers. They run on particular ports for each application.

We can assume our area’s postal code or zip code is the IP address and house is the port number. While delivering a mail a zip code is required to know the area zone. Once the area is identified, the mail will be delivered to the zip code area office first. From the post office, the mails move and is delivered in the home using the house number and the street name.

Similarly, when data packets from the Internet or any server arrive at home, it gets delivered to the router first. Then from there it checks the table and performs the address translation to see where to send the data. Then the router sends the data to the respective authorized device. These ports are sensitive and hackers scan them to exploit the computers.

Now we have some information about how each device is working at our homes. We now know how data is travelling from router or modem to various servers such as Google, Microsoft, Yahoo or Facebook. The interesting thing is all the websites like Google.com or Facebook.com are not actually Google.com or Facebook.com instead they are in numbers.

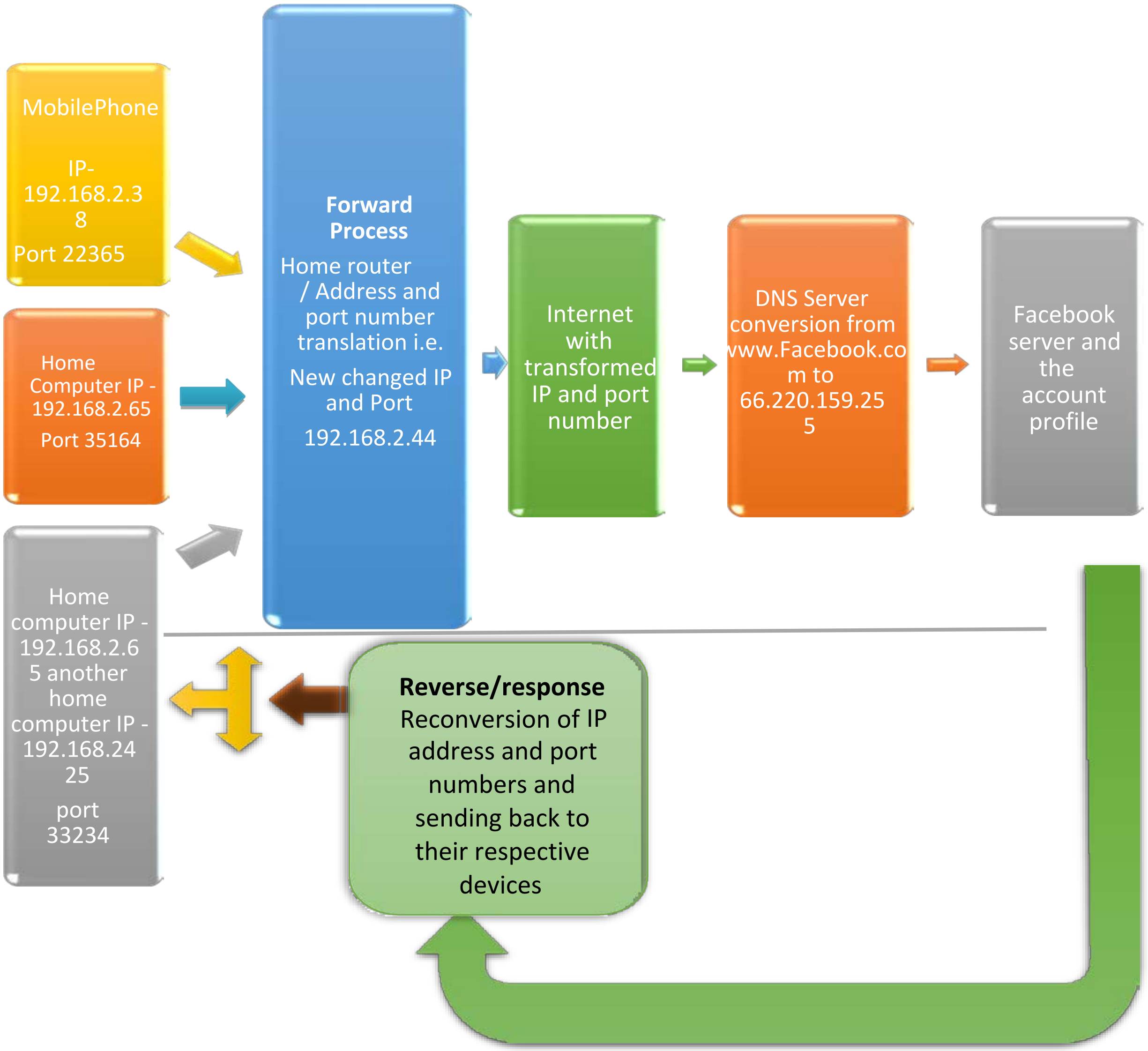
These websites are always in numbers, i.e. IP addresses 66.220.159.255, obtained from Google search is one of the Facebook servers and there are many. But the interesting point is that we do not use the IP addresses to locate our desired websites in our web browsers such as Google Chrome, Firefox, Safari or Microsoft Edge.

When we type www.facebook.com from our phone or computer, the device generates and sends a request to the router device. The router then changes the device’s IP address using NAT into a unique private IP address. The IP address later gets converted into a public IP address by ISP. The Internet packet generated during this request travels from the computer to the Facebook server with the help of the Domain Name System server (DNS). Now, let’s look further into the DNS server.

When we enter a website’s name in the web browser’s address bar, then the web browser sends the name to the DNS server. The DNS server then translates the name, i.e. www.facebook.com to the actual Facebook’s server address, i.e. 66.220.159.255. The process is shown in the Figure 1. It is a cycle and once the server responds, the process takes the exact reverse process to respond back and serve with the necessary actions.

The router receives the requested packets from the Facebook server and it checks who

Figure 1. Internet Flow with DNS Conversion


MobilePhone
IP- 192.168.2.38
Port 22365
Home Computer IP - 192.168.2.65
Port 35164
Home computer IP - 192.168.2.65 another home computer IP - 192.168.2425
port 33234
Forward Process
Home router / Address and port number translation i.e.
New changed IP and Port
192.168.2.44
Internet with transformed IP and port number
DNS Server conversion from www.Facebook.com to 66.220.159.255
Facebook server and the account profile
Reverse/response
Reconversion of IP address and port numbers and sending back to their respective devices

requested these packets. The router checks the table for the device IP address and the application's port number. It transfers the packets to the particular device and the application and then we can view our Facebook account. That's how it works, it automatically does the translation and it is lightning fast.

When a website is trying to open a malicious web page with some tricks (which will be covered in later books) we will be able to make out whether the website is genuine or it's a malicious one. In the next section, we will discuss how vulnerable we are to the cyber-attacks because of the networks and computer vulnerabilities.

3.2 ASSOCIATED VULNERABILITIES

We can now discuss what kinds of devices are connected to the networks and connection properties with some protocols. We need to understand a few protocols to know our network and the Internet connection better. We use wireless connection to connect devices to the Internet.

A Wi-Fi connection can be set up on the home or office router with different security settings. These securities parameters could be less or high, i.e. Wired Equivalent Privacy (WEP) 64 bit is less secure as compared to Wi-Fi Protected Access (WPA) and WPA2 256 bit. The more the number of bits, the more secure it is.

Now we can discuss about the issues with the Wi-Fi settings and their consequences. Many times, people do not set their Wi-Fi security. By default, the router comes with a factory password and SSID (Service Set Identifier) or we can say a user name and the password is printed on your router.

If the router security password has not been modified along with the Wi-Fi password, then anyone can access the router. The Internet connection which is registered in a person's name can be used maliciously by a cyber-criminal to commit crimes and frauds. The routers usually come with factory user names and passwords. It is not a difficult to figure out how to access them with default router settings by a hacker.

Anyone can easily invade in router's security and have access to Internet connection which could be dangerous because the Internet system then would become slave to the invader. The hacker will then be able to do any cyber-crime using the owner's name. To avoid this situation, we can set a difficult password for the router access for better security. We should always go for a WPA2 password as it most secure. In the next section, we will discuss computer network protocols and ports.

3.3 PROTOCOLS AND PORTS

We will discuss a few protocols required to understand security concept. For Internet, a computer connected to groups of networks follows protocols. Protocols are nothing but a set of rules defined to interact with other computers and devices. Our interaction with the digital devices may be performed in different modes such as information transfer, email reading, media transfer such as image, audio, or video, Internet browsing and more. We cannot discuss all the protocols as they are too many however, we will discuss the essential ones in this book.

It is important to understand how things are working in computer and how we can control them. The Transmission Control Protocol/Internet Protocol (TCP/IP) is responsible for communication over the Internet. The TCP protocol breaks a message into smaller pieces and these pieces get assembled at the receiving end.

The IP protocol is responsible for correct communication using the address verification like the postal deliver. It reads the address and verifies it to check whether it was delivered and received correctly. We have another protocol that is known as FTP (File Transfer Protocol). The FTP protocol is responsible for data transfer or we can simply say downloading a file.

Another important part is the 'port'. A computer has several ports in it. They are similar to doors to reach room in a hotel with its own unique number. A computer has its 'own rooms' and they can be opened or accessed using the room number, i.e. the port number. A visitor in that case knows your room number and comes directly in the hotel room after the reception and security checks, if any. Similarly, in computers all applications run on port numbers.

If any external application or service either from internally or externally needs to access any application on computer, it needs to know the port number on which the application is running. For an example, when we browse the Internet it may follow a few protocols. A simple HTML page, i.e. a web page runs on port 80 and when we send a normal email it follows port 25 and that protocol is known as Simple Mail Transfer Protocol (SMTP).

There are several ports in a computer and each application uses different ports for their individual operations. The Internet data packets arrives through different ports such as SMTP port though which emails (email clients i.e. Microsoft Outlook, Mozilla Thunderbird, etc.) comes from using port number 25 as said earlier.

The secure email technology uses a secure connection called Secure Socket Layer (SSL) that comes from port 465 and Transport Later Security (TLS) from port 587. Similarly, the normal web browsing comes into port 80 through Hyper Text Transfer Protocol (HTTP) and the secure version comes from port 443 Hyper Text Transfer Protocol Secure (HTTPS).

There are 65535 ports available in series from 0 and each port is assigned to only one application protocol. However, we use secure ports for the communication over the Internet such as use of HTTPS and SSL/TLS. These ports are highly secure and reliable as compared to normal ports.

These ports are like doors to a computer and cannot be closed because the computer uses them to communicate with the outer world. From 0 to 1024 ports are reserved for system use. That means any external or personal application apart from system applications cannot use the port range from 0 to 1024, only system application can use these reserved ports.

3.4 ISSUES

If you are using as secure port that means your data is encrypted and it cannot be seen in a simple readable or a plain text format. It is still very difficult to break the secure connection with secure ports. Hackers perform port scanning to find vulnerabilities in the computer or any other device. When they find an open door i.e. open port, they try to get into the system using that door. The knowledge of ports and related technical details is therefore necessary.

The computer network works on the identification and verification of the data packets and is similar to the school identification (ID) or office ID card. If anyone has the ID card the security guard will let the person in similarly, the computer reads the information and checks for the valid identification tags. If the information is found to be valid the computer assumes the person is an authorized and legit person.

It is possible that a hacker may easily fake the data or disarm the application security which is protecting us from the attacks. The devices are firewalls and IDPS (Intrusion Detection and Prevention System). If security is disabled, it gets very easy to access a computer and will become highly difficult to stop any intrusions if performed. Now, let’s discuss more about the firewalls. IDPS will be covered in upcoming book series.

3.5 FIREWALL

A firewall acts as the security guard. Firewall acts as a big wall in between intruder and the computer. A firewall takes care of the security by performing the necessary actions for the safety of computer. The firewall is similar to the security guard which inspects and blocks any malicious content.

A good and advance firewall must have three components. Firstly, an inbuilt traditional firewall for blocking malicious contents and allowing authentic contents. Secondly, an Intrusion Detection and Prevention System (IDPS) to detect and prevent malicious activity from the network before it strikes the computer. Lastly, the access controls to the computer and related services. Access control is responsible for preventing unauthorized person to access the computer.

When we browse the Internet, an attacker may intercept, steal and modify data using a sniffer or data packet capturing tools. In this case, a computer may get vulnerable or even worst an attacker may fake data and try to gain the access control of the computer. In this process, the first thing the attacker is going to face is the firewall. A firewall can be installed on the router, computer or any digital device containing operating system software.

When server sends the data packets to the computer, the firewall checks for the authenticity of packets. If the data packets are not authentic then the firewall blocks them to ensure safety.

3.6 CONNECTED DEVICES

With the development in technology, the computing devices are getting smaller and smarter. They are getting integrated in several household devices such as our refrigerators, smartphones, and thermostats and in almost all the devices we use daily. This interconnection of the devices to the networks is known as the Internet of Things (IoT). Since they all are interconnected. If one device is compromised then others may also get infected.

All the data may get stolen and misused. The IoT devices contain several subsystems or sub devices. More the number of systems are present in a device; more is the probability of having a missing or a wrong piece of computer codes. This is known as vulnerability in computer. Single vulnerability is more than enough to let the computer get into compromised state. The hackers always look seeks to exploit these vulnerabilities to gain access. We will be discussing how these technologies are targeted to make victims of cyber-crime in the next chapter.

CHAPTER 4: CYBER-CRIME VICTIMS

4.1 THE THINGS YOU SHOULD BE AWARE OF

This section is the most crucial in this book. We will be discussing about the viruses and similar harmful threats and how they affect the computers. The prime purpose of cyber-security is to maintain confidentiality, integrity and availability (CIA) of the data. Hackers always try to affect the CIA of the data or to gain the control access. There are many ways a hacker can perform such activities.

A hacker can use a number of tools to infect a digital device. The hacker will first collect information about the computer and network devices and based on the information gathered he will plan to infect the machine with most suitable malware or by any other technique. The purpose of the hacker is to exploit the vulnerability or the weakness to make a passage to intrude in.

A vulnerability may be present in software, configuration settings or maybe even in the hardware. Identification of vulnerability will help the hacker to select the malware and an appropriate technique to exploit a weak spot and gain access to the device.

4.2 MALWARES

There are several types malware that can be used to exploit a computer or a network. A malware could be defined as the application which performs malicious activity or shows malicious intent. It is a virus which infects the computer and malfunction them. A Trojan is a type of malware. Trojan resembles to the Trojan horse story where an army hid in the giant wooden horse and trickily invaded inside the castle of the city of Troy.

In that story, after ten-years of unsuccessful attempts to win the war against the Trojans, the Greeks decided to play a trick. They constructed a huge wooden horse to hide. They hid some of their bravest men inside the wooden horse and the rest moved to a nearby place. After leaving the wooden horse in front of the gate, the Greeks pretended to sail away.

The Trojans later brought the horse into their city after considering it as a victory trophy. In the night, the hidden Greek force inside the horse came out of the horse. They silently opened the gates for the rest of the Greek army to attack the Trojans and won the war.

A computer program that contains hidden malicious content that tricks the users to execute the program is known as a 'Trojan horse' or 'Trojan' similar to the story.

Next is the 'downloader' malware. It is small in size and downloads the actual malware later on once executed. It is a bit difficult to catch because it does nothing but downloading the malware.

Next in the line is a 'blastware'. It modifies your computer Master Boot Records (MBR) which is responsible to load an operating system on the computer. A blastware modifies the computer booting sequence that starts when you power on the computer. A blastware can hide itself very well.

Next is a 'botnet'. It can give hidden controls of a computer to the hacker and turn the computer into a hostile computer exactly like a zombie.

Next is the 'spyware'. A spyware does the work like its name, i.e. spying on people. It can track whatever anyone is doing or typing on the computer including the credit card numbers, user names and passwords and all other details.

4.3 CYBER TROUBLES

Assume a scenario where someone installs a malware into your computer and execute a cyber-attack in your name after gaining access to your computers. It is very common in these days to have such malware in the computers. In this case, possibly the police may enquire you for the cyber-attack which was performed by somebody else.

It is difficult to track a hacker. A smart hacker can hide the identity. Hacker can change the IP address which makes difficult to track them. The MAC address can also be altered by the hacker which is the hardware number through which a computer can be identified.
The Internet is a way more powerful and resourceful than we think. It is basically divided into three parts. First part, we know and we use it every day like Google, Outlook,

Facebook and the others which are open to all. Second part, there is a deep web which is hidden to the public on the internet and is being used by the big corporates to hide their communications from other organization as well as from the hackers. The last part, on the Internet is a dark web which is completely illegal and where serious illegal activities happen.

On the Internet, several markets are available. Some are legal and some are illegal. These illegal markets are known as the dark web markets or the black market. Numerous ways are available for a hacker to divert someone towards wrong things. They may get drugs, gun and even commit severe adultery case on the dark market if computer is infected and is in control of the hacker.

People may get weapons illegally from the dark market on the Internet. People could get involved in other criminal activities such as illegal trading or start working for a hacker. A majority of times people do not possess enough knowledge to understand what is right and what is wrong in the cyber world. You should be responsible for your security.

4.4 WHAT ATTACKERS DO?

It is important to understand that what hackers do to exploit networks and devices. The Internet is a resourceful thing, from research information to entertainment; all is in the scope of the Internet. We depend on the Internet for our daily tasks. Internet has become a basic necessity. The Internet connection has been serving as the backbone and the building blocks for our critical infrastructures departments like the energy sector, financial sector, defense sector as well as our educational and research sectors. Everything is interrelated and highly dependent on the use of computers.

When we use Internet then it is not only connected to one network but to several other networks. It is difficult to identify a hacker as discussed previously. Also, it is not easy to find someone from a huge collection of network. A hacker may be from one network amongst a hundred thousand. They stay anonymous and collect information about how to exploit network devices.

A hacker may use a phishing method in which a fake attractive email is sent to lure the victim. It is a method of trapping through which a person can hook a victim into a scam or a cyber-attack. Once trapped, the attack could happen and the computer will be compromised.

A hacker can send an infected email containing a malware to the victim to perform exploitation or information gathering. Once the victim opens the email and executes the attachment then the computer gets infected. Sometimes we download an image and the computer gets compromised due to a technique called ‘steganography’.

‘Shell’ is a command line language like command prompt (CMD) in the Microsoft Windows operating system or a Linux system. Using shell, a hacker can create a backdoor entry or exploit the computer easily. A shell can be embedded, i.e. attached to a Microsoft Word document, PowerPoint, Excel, PDF, and even picture and video, etc. This means any file from an unknown source can infect your computer.

An antivirus may be not sufficient enough to handle difficult scenarios and will not be able to protect all the time against strong threats. People can be easily be targeted using phishing attack or more technical methods such as configuration setting exploitation (improper computer settings) and system unpatched vulnerability (software related problem). A hacker may install a key logger which stores a copy of everything user types on your computer. It tracks all the written information.

Tracking the digital currency known as 'Bitcoin' is complicated. It is difficult to track the amount transferred to the hacker since they have been using bitcoins as a payment method which is anonymous. A bitcoin is a digital currency system which is not maintained by the government and the banks. Instead, it is maintained by some random volunteers all over the world.

The hacker can also access the routers using various techniques. They can divert the network traffic or connect with anyone's computer or with any other device. Most of the time an attack happens by falling into a trap of a hacker. Monitoring is essential in cyber-security; non-monitored devices are comparatively easy to exploit and a majority of the time we do not monitor our background process activities.

A technique known as 'social engineering' is popular for hacking in which a hacker communicates with the victim directly or indirectly. In a simple terminology, we can say a hacker uses social skills to find out a way to find and exploit the vulnerability present in the entire system.

Mostly, people use a simple password that contains any name, date of birth, place of birth, favorite sports or sports player name or favorite destination. It is not very difficult for a hacker to figure out the login credentials or find another workaround to gain access to the computer.

You must also be concerned about the phishing trick used by the hackers. A hacker could create a pseudo website which appears similar to a known website. The website may look like a genuine website. Thus, it will be hard to distinguish it from a real website except for its domain name i.e. website name. Having this advantage, a hacker could trick user to click on one of a malicious link or an object.

Once the click happens, the computer may get infected by a malware and hacker can gain access into the computer devices and network. We have discussed about the DNS servers, when we enter a website's name it gets converted into the real address i.e. server name in numbers which is an IP address. A number of times, an attacker may target a DNS server. To perform an attack, a hacker can change the IP address of the server user requested and causes misdirection.

When we browse internet, computer generates cookies which stores our information and is used by the website. Cookies make work easy for the website developers, therefore they prefer to create cookies and store the information in it to give the best web browsing experience. However, the stored cookies have the user's information in it. A Hacker can use these cookies to hack the account. It is a good practice to keep deleting cookies and web browsing history.

CHAPTER 5: FAMLIY TARGETED FOR CYBER-CRIMES

5.1 KEEPING FAMILY SAFE

The big question is how to keep our children and the other family members safe? Monitoring is important in cyber-security. There are several tools in the market which can be used to monitor and control intrusions up to a significant level. However, alertness towards intrusions is going to be the most crucial in the entire protection process.

The first thing is to keep information secure, do not spread information with social society or strangers. Also, we can educate the family members and people around us not to spread any sensitive information to anyone especially on a social media. The social network is responsible many times for most of the information leaks.

We can restrict anyone's activity on the Internet using parental control tools to avoid any information leaks. Often, firewalls have these settings. Open computer's or router's firewall settings and block all the unwanted websites or the unwanted categories of websites.

5.2 MONITORING & CONTROL TOOLS

It is recommended to use 'Microsoft Enhanced Mitigation Emergency Toolkit' for Windows based operating system. It provides an extra layer of security and protection against malicious activity. It is compatible with the pre-installed anti-malware and firewalls. There are several third party parental control applications available which can be used to perform the same functionality.

Popular software called 'ContentWatch Net Nanny 7' is capable of performing parental control over the Internet. 'Symantec Norton' also provides Family Premier parental control app. After installing the application, we may go to the settings page and apply the Internet restriction for children and other family members as required.

The other factor is which is extremely important is hard disk drive (HDD) encryption. Data is sensitive and if a hacker gains access to encrypted data, it will be of no use for him as it cannot be read in a plain text or textual format. For example, if 'hello' is written as '51JkL', no one will be able to know what it is, this is called encryption.

Some freeware tools called 'DiskCryptor' and 'VeraCrypt' are available which can encrypt entire hard drive or separate hard drive partitions. It is similar to putting a password on the computer storage. The data will not be visible to anyone without password. It will keep the information safe. We can install the software on the computer to get protection from information leaks.

Prevent illegal downloading and harmful content browsing. Install best antivirus possible to restrict the malicious contents to be downloaded or executed. 'Bitdefender', 'Symantec', 'Malwarebytes' and 'McAfee' are some good names in antimalware applications business. An antimalware application should be updated and run regularly to avoid any present malware.

Set limits for the Internet usage either by limiting the data or by time. We can do it using special applications. 'NetBalancer' is a popular application to limit the Internet download and upload. We also can turn wireless Internet connection down during nights to avoid excess Internet usage. Spend some time with children and teach them about safety. Also, we should check with our children's school about their policy against cyber-crime and its active implementation.

Protect router configuration and set a strong password. Never leave router password and SSID default. Always select WPA2 password for wireless and change the SSID for the network. We can also increase security for the family by adding everyone's computer hardware number (MAC address) in the allowed list. The router will not grant access to anyone else apart from the allowed list. We can also make router connection hidden using the router settings.

Generate a guest Wi-Fi password for the guest with another password. Therefore, no one will be able to access or attack the network directly. Keep track of the network configurations and settings and update the passwords regularly.

Use a strong password everywhere and we can ask our family members to prefer using a lengthy password of at least ten characters which includes symbols, numbers and alphabets

in both upper and lower-case characters. If the password is a combination of numbers, symbols, and characters which includes upper and lower cases then it would be highly difficult to break.

Network monitoring is highly important and should be considered as one of the most crucial part. Through network monitoring we can have a track of network statistics and controls. ‘Splunk’ is a tool for network monitoring and data collection and we can perform analysis on the collected data from event logs and other network traffic data. But we have to be careful of legal restrictions (if applicable) to perform such operations.

With an ‘Angry IP scanner’ we can perform network scanning. Not only to know the network usage by children but by any unauthorized access as well. It will display information about the MAC address, active ports and along with other essential information. A tool called ‘Total Network Monitor’ can perform such several operations and send alerts with a detailed report in case of any abnormal event are experienced by the tool.

Another tool can be used is called ‘Wireshark’ which is light in operation and highly efficient freeware. It can be used to monitor network activity and packet sniffing. The packets can be analyzed to see the presence of any malicious activity in the network. The only problem with network monitoring is that more storage is required to capture the network data. But we can delete the old data according to our requirements.

In the case of computer infection, a computer may start hiding some important information as programed by the hackers. The background process may be hidden such that no one will be able to know that the computer is infected. They are known as ‘rootkits’ and ‘bootkits’. They infect the computer and hide information about the running applications in the background. ‘Process Explorer’ and ‘Process Hacker’ are the tools that can help in this situation and they will let user know what is going on in the background.

A computer records everything like in a register we do. Computer registers all application and tool when installed into its ‘registry’. Windows registry and computer file system are highly important and if they are infected, it could result in serious troubles. Tools such as ‘Process Monitor with ProcDOT’ will help in this situation. The malware tries to embed itself into the

system and hence they can hide certain important information. Through these tools, we will be able to identify and extract actual information. I would also advise to use ‘Regshot’ which can tell the exact details about the infection.

Identification and cure for all types of malware requires good understanding of some related technologies and skills. A website called ‘www.virustotal.com’ is useful to check for malicious content in a document online for malware.

5.3 PROTECTION AGAINST CYBER-BULLYING

The tool ‘Splunk’ can be used to know about the network activity. Any unusual activity in the network can be traced by Splunk. The data can be then submitted to the police for legal action against the criminal. Keeping the cookies and cache memory clear of the web browser will help reducing the risk in many ways. The hacker will not be able to steal important account information from cookies. Using a strong 256bit AES encrypted user defined password for the router is recommended to ensure the network security.

Stay active towards children’s social activity and monitor them, teach children and other family members about awareness and safety. Keep checking for any unusual activity over the network or devices. Often, cyber-stalker makes use of the computer’s data to bully a victim.

We should never leave any session open when we walk out of the room. Do logout from all the accounts and computer before leaving the room. Prefer to use multi authentication factor i.e. which requires two or more stages to grant access to the account. Always prefer and make everyone’s habit of using private browsing, deleting cache and cookies every time they close the browser.

Update the software and operating system whenever an update is available. This will eliminate the vulnerabilities present in the computer. Always take a backup for the important data. ‘Norton Ghost’ is an online cloud based backup system capable of backing up the hard drive. Teach family to not to respond to any Cyber-bullying messages and ask them to avoid posting sensitive or personal information online.

Keep track of your online activity, check last login details for any unknown login. Gmail provides this feature at the bottom of the email account. Any unknown message should be avoided and considered serious. Immediately

report it to the cyber-crime department or to the local police especially when repeated. Gather as much as proofs as possible, take screenshots and save emails or text messages.

CHAPTER 6: SUMMARY

6.1 SUMMARY

Technology is complex and growing at a rapid rate. Innovation and development have been creating new ways to solve our problems to live a better life. However, the technology itself is just a facilitator and may be misused. Cyber-crime is rising due to the misuse of the technology by the hackers. A hacker can steal the finances. It is also possible for a hacker to steal someone's information and commit crimes in his name. It is not only about hackers and information related to us; it is also about cyber-stalking and cyber-bullying.

They are common in school and children can be a victim of such cyber-crime. It is advisable to consult with the school about the cyber-crime policy for such incidents. Also, securing the computer and network, monitoring malicious activity with the tools and techniques discussed and teaching children and other family members about safety and security can prevent any harm to them from any kind of possible cyber-crimes. Precaution is the best cure.

The implementation of cyber-security tools is a good way to prevent cyber-crimes. The techniques of implementation and monitoring of the tools plays an important role in the overall efficiency of cyber-security.

However, implementation of legal processes is essential, i.e. we may need other people's consent whose are connected to our network and whose data we may want to monitor. When implemented, the tools will be able to monitor the activities to identify the malicious content or activities. Once any malicious activity is identified it should be reported to cyber-crime department (FBI). The cyber-crime can also be reported at www.justice.gov.