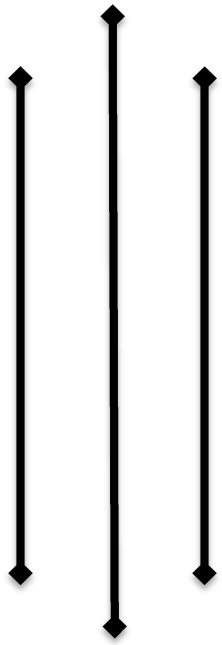
# Kathmandu Model College

**Bagbazzar, Kathmandu**

**Final Year Project Report 2022**

**Computer Science**



**A Report on the Topic**

# Cyber Law and Security

# Chapter 1 : Letter of Approval

This is to certify that this project is prepared by the joint and collective efforts of the members of the group and the topic "**Cyber Law and Security**" has been well studied. In our opinion the document is satisfactory in the scope and quality as a project for the required academic level.

| Submitted by | Submitted to |
|---|---|
| …… | …… |
| Aashrawat Shrestha<br>Kritan Khadka<br>Kritish Dhakal<br>Kushal Timsina<br><br>Branch: Science<br>Grade : 11 ' M11' | Hem Prasad Thapaliya ( HPT ),<br>Professor,<br>Department of Computer Science,<br>Kathmandu Model College ( KMC ),<br>Bagbazzar, Kathmandu. |

_____
Signature

Examined by :

Date :

# Chapter 2 : Acknowledgement

First and foremost, we would like to express our special thanks of gratitude to our teacher Mr. Hem Prasad Thapaliya for providing us this this golden opportunity to prepare this project report on the topic "**Cyber Law and Security**". This project helped to explore various topics like Cyber Law, Cyber Security, Cyber Crimes, Cyber Attacks etc. in a deeper basis which enhanced our knowledge in those fields.

Besides, we would like to thank all the teachers who helped us by giving us advice and providing the information which we required in order to prepare a proper report on the given topic.

Also I would like to thank my family and friends for their support. Without that support we couldn't have succeeded in completing this project and submitting it on time.

At last but not in least, we would like to thank everyone who helped and motivated us to work on this project.

# Chapter 3 : Preface

This document is prepared with the joint effort of every member of the group. The data for this document is collected from different websites and in variation. This document also contains data and statistics relating to Nepal and is a reader based document. Since there is a large scope of Cyber Security and Law collection of data was easier thing to do but filtering data was a tuff one. Also the data and stats were crossed checked to verify if the data found on the web were true and logical.

As said earlier the topic "**Cyber Security and Law**" has a larger scope of study; finding data in a single site was a harder job to perform. There were some limitations that we faced. Therefore our document is very useful in context of getting and finding all necessary data regarding the topic.

# Chapter 4 : Table of Contents


Chapter 1 : Letter of Approval ..... 1

Chapter 2 : Acknowledgement ..... 2

Chapter 3 : Preface ..... 3

Chapter 4 : Table of Contents ..... 4

Chapter 5 : Abstract ..... 5

Chapter 6 : Cyber Law and Security ..... 6

Unit 1: Cyber Security ..... 6

- Introduction to Cyber Security ..... 6
- Types of Cyber Security ..... 6
- Importance of Cyber Security ..... 7

Unit 2: Cyber Attacks and Vulnerabilities ..... 8

- Introduction to Cyber Attacks and Vulnerabilities ..... 8
- Types of Cyber Attacks ..... 8
- Ways to be protected from Cyber Attacks ..... 10

Unit 3: Cyber Law ..... 11

- Introduction to Cyber Law ..... 11
- Brief Information about Nepal's Cyber Law ..... 11
- Cyber Laws / Acts in Nepal ..... 12
- Importance of Cyber Law ..... 13
- Cyber Law Policies and Strategies by Government of Nepal ..... 14

Unit 4: Cyber Crime ..... 15

- Introduction to Cyber Crime ..... 15
- Categories of Cyber Crime ..... 16
- Types of Cyber Crime ..... 17
- Statistics of Cyber Crimes Cases in Nepal ..... 21
- History of Cyber Threats / Crimes in Nepal ..... 22

Unit 5: Cyber Security in Context of Nepal ..... 23

- Organizations working for Cyber Security in Nepal ..... 23
- Ranking of Nepal in the Global Cyber Security Index ..... 23

Chapter 7 : Index ..... 24

Chapter 8 : Bibliography ..... 26

# Chapter 5 : Abstract

Cyber Security and Cyber Law are one of the most trending topics in the current world as Cyber Space is constantly evolving and developing in the field of technology.

Cyber security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

Everyone should also play their part in the battle for cyber security as this problem will not be solved with only one side taking action. Furthermore, cyber security is a constantly evolving field and it will take all of us working together to keep the internet safe from malicious attacks.

Cyber law is the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, hardware and information systems (IS).

Cybercrime can be defined as any criminal activity which takes place on or over the medium of computers or internet.

# Chapter 6 : Cyber Law and Security

## Unit 1: Cyber Security

- ### Introduction to Cyber Security

Cyber security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The field is becoming increasingly significant due to the continuouslys expanding 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 (IoT).

Cyber security is also one of the significant challenges in the contemporary world, due to its complexity, both in terms of political usage and technology. Its primary goal is to ensure the system's dependability, integrity, and data privacy.

- ### Types of Cyber Security

Cyber security can be categorized into five distinct types:

- Critical infrastructure security
- Application security
- Network security
- Cloud security
- Internet of Things (IoT) security

- ## Importance of Cyber Security

Cyber security is important because it protects all categories of data from theft and damage. It is also important because it encompasses everything that relates to protecting our data from cyber attackers who want to steal this information and use it to cause harm. This can be sensitive data, governmental and industry information, personal information, personally identifiable information (PII), intellectual property, and protected health information (PHI).

If a cybercriminal was to gain access to various personal information and important data, they could cause a range of problems. They could share sensitive information, use passwords to steal funds, or even change data so that it benefits them in some way.

Without a cyber-security program, your organization cannot defend itself against data breach campaigns, which makes it an irresistible target for cybercriminals. Companies need cyber security to keep their data, finances, and intellectual property safe.

For individuals there is a higher risk of losing important files, such as family photos or a personal document.

In the case of public services or governmental organizations, cyber security helps ensure that the community can continue to rely on their services. Proper Cyber Security is most important to these organizations because of the data and information these organizations store and the uncertainty it can cause if those data are leaked.

# Unit 2: Cyber Attacks and Vulnerabilities

## • Introduction to Cyber Attacks and Vulnerabilities

Vulnerability is a weakness in design, implementation, operation, or internal control. A Cyber Attack is when an individual or an organization deliberately and maliciously attempts to breach the information system of another individual or organization. While there is usually an economic goal, some recent attacks show destruction of data as a goal.

## • Types of Cyber Attacks

To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of these categories below:

### 1. Backdoor

A backdoor in a computer system is any secret method of bypassing normal authentication or security controls.

### 2. Denial-of-service attack

Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

3. Direct-access attacks

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, key loggers, covert listening devices or using wireless microphones.

4. Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private computer conversation (communication), typically between hosts on a network.

5. Phishing

Phishing is the attempt of acquiring sensitive information such as usernames, passwords, and credit card details directly from users by deceiving the users. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

6. Social Engineering

Social engineering, in the context of computer security, aims to convince a user to disclose secrets such as passwords, card numbers, etc. or grant physical access.

7. Spoofing attack

A Spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, in order to gain access to information or resources that one is otherwise unauthorized to obtain and other illegitimate advantage.

8. Tampering

Data tampering is the act of deliberately modifying (destroying, manipulating, or editing) data through unauthorized channels. It can also be defined as a malicious modification or alteration of data.

9. Malware attack

Malware attack installs malicious software on a computer can leak personal information, can give control of the system to the attacker and can delete data permanently.

10. SQL Injection

A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

- Ways to be protected from Cyber Attacks

- Use online banking wisely.
- Mitigate cyber threats on mobile phone.
- Use online gaming safely.
- Have knowledge of Voice over Internet Protocol (VoIP).
- Update your computer software regularly.
- Back up Plug-ins.
- Use antivirus and antimalware software.
- Payment gateway security.
- Download VPN apps.
- Subscribe to computer security service.
- Be aware of phishing attacks.
- Use fire wall
- Use strong passwords.

# Unit 3: Cyber Law

## • Introduction to Cyber Law

Cyber law is the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, hardware and information systems (IS). Cyber law is also known as Internet Law. Cyber laws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices.

## • Brief Information about Nepal's Cyber Law

The country's cyber law progress has moved very slowly because email and computer transactions are not considered trustworthy by the government. The country does not utilize the same level of technology as other developed countries. The Nepal government believes that passwords can be easily guessed, thus leading to the hacking of user's accounts, which is largely due to outdated IT systems being used by high- profile government agencies. Part of the problem is that Nepal citizens tend to make easily-guessed passwords using numbers and information significant in their lives, including their first and last names, birthdays, phone numbers, and locations. The Nepal police department is working with the outdated Cyber Law Act of 2006/2007. Since the legislation (Electronic Media Act) was passed in 2006/2007, there has been little to no cyber law reform, which is crucial for staying up-to-date on information regarding changing technology. The Electronic Transaction Act 2008 does not address the changing dynamics and challenges of cyberspace. Hence, the Ministry of Communication and Information Technology has drafted a new policy draft named National Cyber Security Policy 2021 with the purpose to govern and address cyber security issues. Laws on cyber-matter should be updated frequently and regularly.

- Cyber Laws / Acts in Nepal

## 1. The Electronic Transactions Act, 2008

This was Nepal's first cyber law. Cybercrimes were dealt with under the Country's criminal code before this law came into force. Since the cases of cybercrime increased, it became necessary to enact a separate law.

As per defined by the Electronic Transaction Act, 2008 Cybercrime is a crime committed by using cyber means/computer technology. Cybercrime is also known as computer-related crime. All the illegal activities committed by using computer technology are considered cybercrime such as:

- Damage to the computer and computer system.
- Acts to gain illegal access to the computer.
- Use as a weapon to commit other crimes.
- Acts against the provision of cyber law.

Chapter 9 of the Act deals with offences relating to computers, the main highlights of which are as follows:

- Pirating or destroying any computer system intentionally without authority carries imprisonment for three years, or a fine of two hundred thousand rupees, or both.
- Accessing any computer system without authority results in imprisonment for three years, or a fine of two hundred thousand rupees, or both.
- Intentional damage to or deleting data from a computer system carries imprisonment for three years, or a fine of two hundred thousand rupees, or both.
- Publication of illegal material in electronic form carries imprisonment for 5 years, or a fine of one hundred thousand rupees, or both.
- Commission of a computer fraud carries imprisonment for two years, or a fine of one hundred thousand rupees, or both.

2. The Children's Act, 1992

The aim of this Act is to protect and uphold the rights of children. It also prohibits child pornography. Section 16(2) of the Act prohibits individuals from capturing any immoral picture of a child. Section 16(3) of the Act prohibits publication and distribution of any such photographs of children.

3. The Copyright Act, 2002

This act protects the copyright of ideas, including a computer program. It prohibits people from copying and modifying the original work of others, and using it for their own advantage or economic benefits.

4. The Individual Privacy Act, 2018

This act is the first legislation in Nepal to protect the right to privacy of its people, and define personal information. It protects the privacy of body, family life, residence, property, and communication. It puts the responsibility on public entities to protect the personal data of individuals. They cannot transfer such data to anyone without the consent of the owner. The Act prescribes a general punishment for violation of privacy as three years of imprisonment, or a fine of NPR 30,000, or both.

## • Importance of Cyber Law

In simple words, Cyber Law is important to control and minimize the crime related to the internet. Formulation of Cyber Law creates a boundary for safe use of the internet and regulates safe internet environment. In other words, Cyber Law is the guide book for safe use of Internet and surveillance for a better and safe internet space.

- Cyber Law Policies and Strategies by Government of Nepal

The new National Cyber Security Policy 2021 draft begins with background information on the need for cyber security policy, the need for the new law, challenges, objective, strategy, work plan and organizational structure. The draft has altogether 58 programs under 8 strategies. The strategies focus on framing laws for cyberspace, developing skilled human resources and organizing public awareness programs.

1. To Frame the laws and guidelines for secured and resilient cyberspace.

2. Develop institutional and organizational structure based on international guidelines to secure information and Information technology system.

3. Build infrastructure and technology to strengthen cyber security.

4. Develop skilled human resource in the cyber security sector.

5. To do public awareness campaigns on issues of cyber security.

6. To collaborate with public entities and the private sector for secure cyberspace.

7. Collaborate with international organizations for secured cyberspace.

8. To build a safe online space.

# Unit 4: Cyber Crime

- ## Introduction to Cyber Crime

Cybercrime can be defined as any criminal activity which takes place on or over the medium of computers or internet. Cybercrime is the most prevalent crime playing a devastating role in present world. Not only the criminals are causing enormous losses to the society and the government but are also able to conceal their identity to a great extent. There are number of illegal activities which are committed over the internet by technically skilled criminals. It can be said that, Cybercrime includes any illegal activity where computer or internet is either a tool or target or both.

Cybercrime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Whatsoever the good internet does to us, it has its dark side too.

Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber defamation etc. Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or Internet.

- ## Categories of Cyber Crime

There are three major categories that cybercrime falls into: individual, property and government. The types of methods used and difficulty levels vary depending on the category.

1. Property

This is similar to a real-life instance of a criminal illegally possessing an individual's bank or credit card details. The hacker steals a person's bank details to gain access to funds, make purchases online or run phishing scams to get people to give away their information. They could also use malicious software to gain access to a web page with confidential information.

2. Individual

This category of cybercrime involves one individual distributing malicious or illegal information online. This can include cyber stalking, distributing pornography and trafficking.

3. Government

This is the least common cybercrime, but is the most serious offense. A crime against the government is also known as cyber terrorism. Government cybercrime includes hacking government websites, military websites or distributing propaganda. These criminals are usually terrorists or enemy governments of other nations.

- Types of Cyber Crime

Cybercrime takes many different forms. Criminals who infiltrate computers and networks have developed a variety of malicious software and social engineering techniques used individually or in combination when use in committing different types of cybercrime. A few of the most common cybercrimes are described below.

1. Hacking

Criminal hacking is the act of gaining unauthorized access to data in a computer or network. Exploiting weaknesses in these systems, hackers steal data ranging from personal information and corporate secrets to government intelligence. Hackers also infiltrate networks to disrupt operations of companies and governments.

2. Malware

Malware, or malicious software, refers to any code designed to interfere with a computer's normal functioning or commit a cybercrime. Common types of malware include viruses, worms, Trojans, and various hybrid programs as well as adware, spyware, and ransomware.

3. Identity Theft

Identity theft occurs when someone unlawfully obtains another individual's personal information and uses it to commit theft or fraud. Not all identity thefts are a result of cyber-attacks, but malware such as Trojans and spyware are often used to steal personal information.

4. Social Engineering

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. Cyber criminals use social engineering to commit fraud online. Platforms such as online dating sites provide opportunities to initiate conversations with potential victims. Once the criminal establishes a relationship with the target and gains their trust, the criminal asks for money or information. Social engineering techniques are often combined with technology elements.

5. Software Piracy

Software piracy is unauthorized reproduction, distribution, and use of software. Pirated software takes the form of counterfeited commercial products and illegal downloads and reproductions, as well as violations of licensing agreements that limit the number of users who can access a program.

6. DDoS Attack

These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on user s' computers. The hacker then hacks into the system once the network is down.

7. Botnets

Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

8. Cyber Stalking

This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyber stalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyber stalker knows their victim and makes the person feel afraid or concerned for their safety.

9. PUPs

PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install antivirus software to avoid the malicious download.

10. Phishing

This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.

11. Online Scam

These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

12. Exploit Kits

Exploit kits need a vulnerability (bug in the code of a software) in order to gain control of a user's computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

13. Prohibited / Illegal Content

This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

14. Laundering

Money laundering is the illegal process of making large amounts of money generated by a criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source.

15. Extortion

Cyber extortion is an online crime in which hackers hold your data, website, computer systems, or other sensitive information hostage until you meet their demands for payment. It often takes the form of ransomware and distributed denial-of-service (DDoS) attacks, both of which could paralyze your business.

16. Sextortion

Sextortion is a form of online abuse, wherein the cybercriminal makes use of various channels like instant messaging apps, SMS, online dating apps, social media platforms, porn sites etc., to lure the users into intimate video/audio chats and makes them pose nude or obtains revealing pictures from them.

17. Cyber Bullying

Cyber bullying takes place when a teen or younger child uses a computing device to threaten, humiliate, or otherwise harass a peer. It may occur over a laptop, smartphone or tablet, and live within platforms such as text messages, emails, social media, online forums and chat rooms.

## • Statistics of Cyber Crimes Cases in Nepal

There are a total of 10.21 million people in Nepal who used the internet in 2020. The number of users increased by 315,000 between 2019 and 2020. Around 10 million people in Nepal use social media. It appears that the Nepali citizens have been reluctant to report cybercrime, with only 53 cases being registered in 2017. However, 2018 saw a sharp rise in the number of cases to 132. In 2018 and 2019, a total of 180 cases were registered. Out of these 180, 125 cases were from the capital city, Kathmandu and the rest from others. Most cybercrime cases are never reported. In the majority of cases, victims themselves are unaware that they have become victims.

## History of Cyber Threats / Crimes in Nepal

- In July 2013, a young woman fell victim to online swindling as she ended up transferring money for an online airline ticket booking. She got Rs. 15,000 back of the total Rs. 110,000 she transferred with the help of the district court.

- The first known case of cyber bullying was reported on October 7, 2014, in Kathmandu School of Law.

- Nepal Police caught an 18-year-old, for hacking government websites, including Nepal Telecom, National Tuberculosis Centre, in 2016.

- The official website of the Department of Passport got hacked on June 27, 2017 by a group of Turkish hackers and defaced with threatening note to reveal the government's data.

- On July 25, 2017, 58 government websites were reportedly hacked by a group called 'Paradox Cyber Ghost' making it one of the biggest breaches of all times in Nepal.

- On October, 2017, attackers hacked the SWIFT server of NIC Asia Bank initiating the transfer of $4.4 million from Kathmandu to other foreign countries. The bank was reported to have recovered $3.9 million, even though $580,000 had already been released to overseas bank account holders.

- On March 8, 2020, a hacker dumped data of 50,000 users of Foodmandu including names, mailing addresses, email addresses and phone numbers.

- On April 8, 2020, customer data of more than 160,000 customers of Vianet Communication were leaked. A hacker using the Twitter handle, Narpichas @paapi_kto_mah, made public data that included customers' emails, phone numbers, and addresses.

- ## Organizations working for Cyber Security in Nepal

As the Cyber Crimes in the country was increasing back in 2018, Nepal Police established a dedicated Cyber Bureau on June 10, 2018. The organization is known as Central Cyber Bureau and is located in Bohahity, Kathmandu with the pure intention to establish safe Cyber Space and to monitor any illegal activities happening in the internet.

There are also various private organizations working in Nepal to provide Cyber Security. Some of the organizations are named below:

- Eminence Ways
- Vairav Tech
- CryptoGen Nepal
- One Cover Pvt. Ltd.
- Reanda Biz Serve (IT)
- Cynical Technology
- ThreatNix
- Netfiniti

- ## Ranking of Nepal in the Global Cyber Security Index

Nepal has moved up to the 94th position in the Global Cyber security Index 2020 from the 106th slot in the 2018 edition, showing that its commitment to cyber security has increased, according to the International Telecommunication Union (ITU).

# Chapter 7 : Index

1. Internet of Things: the interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

2. Intellectual Property: intangible property that is the result of creativity, such as patents, copyrights, irresistible etc.

3. Irresistible: too powerful or convincing to be resisted.

4. Deliberately: consciously and intentionally.

5. Maliciously: in a manner characterized by malice or ill will; with intent to do harm.

6. Surreptitiously: in a way that attempts to avoid notice or attention.

7. Illegitimate: not authorized by the law.

8. Pirating: use or reproduce (another's work) for profit without permission, usually in contravention of patent or copyright.

9. Pornography: printed or visual material containing the explicit description or display of sexual organs or activity.

10. Legislation: laws, considered collectively.

11. Resilient: able to spring back into shape after being compressed or damaged.

12. Cyberspace: the notional environment in which communication over computer networks occurs.

13. Enormous: very large in size, quantity, or extent.

14. Exploiting: make use of (a situation) in a way considered unfair or underhand.

15. Infiltrate: enter or gain access to (an organization, place, etc.) surreptitiously and gradually, especially in order to acquire secret information.

16. Ransom ware: a type of malicious software designed to block access to a computer system until a sum of money is paid.

17. Counterfeited: imitate fraudulently.

18. Plethora: a large or excessive amount of something.

19. Dark Web: the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

20. Forums: a website or web page where users can post comments about a particular issue or topic and reply to other users' postings.

21. Advocating: publicly recommend or support.

22. Reluctant: unwilling and hesitant.

23. Swindling: obtain (money) fraudulently.

24. SWIFT: Society for Worldwide Interbank Financial Telecommunication.

# Chapter 8 : Bibliography

- ## Bibliography Part I

All these sites / links mentioned below were used for gathering information and data for the document. Beside these sites some of the information is mentioned on the basis of self-knowledge and from the help of seniors and guardians.


https://en.wikipedia.org/wiki/Computer_security

https://www.visma.com/cyber-security/why-is-cyber-security-important/

https://cyberblogindia.in/cyber-crime-and-laws-in-nepal-an-overview/

https://www.ratojob.com/electronic-transaction-act/

https://www.enepalese.com/2015/07/32099.html

https://online.norwich.edu/academic-programs/resources/types-of-cyber-crime

https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/

https://english.onlinekhabar.com/cybersecurity-in-nepal.html

https://shequalfoundation.org/cyber-security-in-nepal/

https://ictbyte.com/nepal/cybersecurity-organizations-and-companies-in-nepal/

- # Bibliography Part II

The below mentioned sources were used to build our website.

**Website Link: https://cybersecm11.netlify.app**


https://undraw.co

https://www.freecodecamp.org

https://www.w3schools.com

https://css-tricks.com

- # Bibliography Part III

The below mentioned software were used to build our website.

HTML (Hyper Text Markup Language):

➜ HTML was used to structure the website and add text, images and various other things to the website.

SCSS (Sassy Cascading Style Sheets):

➜ SCSS is a superpower version of CSS which allows developers to stylize their websites faster by providing a custom syntax that is easier to maintain. SCSS code is compiled/ converted to normal CSS automatically by an extension in VS Code, and the html of the website loads the CSS that was compiled by the extension. SCSS was used in this website to make the coding process faster.

JavaScript:

➜ JavaScript was used to add the functionality of switching the theme in website.

Git:

➜ Git was used to track all the changes made to the website so that if there was any major error we could revert back to an earlier state that was working properly.