CyberSecurity Awareness for Students and Every Individual for Society:

(A Research Paper by Ehtisham Hyder, Pre-engineering student)

Introduction to Cybersecurity:

In simple words, “Cyber” means anything related to computers, the internet, and digital technology. While “Security” means protection from harm, danger, and unauthorized access. Cyber security refers to the protection of computers, mobile phones, and other digital devices from unauthorized access, attacks, and damage. In this modern era of technology, it becomes necessary for every person, even those with limited digital literacy, to acquire basic knowledge of cybersecurity. The basic knowledge includes how we save our digital devices from unauthorized access and malicious users. I chose this topic because I want to serve ordinary people and help them gain knowledge. I enjoy learning about important issues and sharing useful information with others. Cybersecurity is very important in today’s world, and by this research I want to teach students and every individual in society how to stay safe online. By sharing awareness, I hope to protect people from online threats and contribute positively to society.

• Importance for Society:

Mobile phones, computers, and the internet have become part of our lives. Digital devices have become essential tools for communication, education, and economic participation in modern society.

International Telecommunication Union, Geneva reported:

“In **2026**, there are approximately **5.78 billion users of smartphones worldwide**, representing **70% of the global population**.”

Students use smartphones and digital devices to do research, to increase their knowledge, to learn digital skills, and to browse and use Artificial Intelligence to enhance their academic performance. Despite increased internet penetration, digital literacy and cybersecurity awareness among students remain insufficient, making them vulnerable to phishing, identity theft, and online fraud.

• Cybercrime:

Cybercrime means any criminal activity that involves the use of digital devices or the internet. It includes a wide range of illegal actions such as hacking, identity theft, online fraud, cyberbullying (simply means to harass, threaten, or target someone), and the spread of malicious software.

Robert Mueller, Former Federal Bureau of Investigation Director once said:

“There are two types of companies in the world; those that have been hacked, and those who will be.”

Cybercrime is extremely costly — **global losses were estimated around $8.4 trillion in 2022** and projected to exceed **$11 trillion**, possibly reaching **$20 trillion by 2026** due to digital fraud, ransomware, and hacking

• Types of Cybercrime:

There are many types of cybercrimes:

Hacking: Unauthorized access to data or systems.

Phishing: Tricking users to reveal personal information.

Identity Theft: Stealing someone's identity for fraud.

Cyberbullying: Harassing others online.

Financial Fraud: Online monetary scams and banking fraud.

International Cybercrime Investigation Agency reports:

"Over **3.4 billion phishing emails** are sent daily in the world. Only in **Pakistan**, over **50+ million** phishing attacks were recorded in **2024-25.**"

• How do people become victims of Cybercrime?

It is the most common issue faced by people all around the world. One type in which criminals send fake SMS, WhatsApp, or emails pretending to be from banks, courier services, or the government. Example: "Your bank account is blocked. Click here to verify." When the user clicks, fake websites open, they enter their password and all the data from our device gets accessed by the malicious sender and maybe he misuses your data for illegal purposes. Sometimes, Users are deceived into revealing sensitive credentials, resulting in financial loss and identity misuse.

Another is fake job offers and investments, targeting students and job seekers. Example: We offer jobs of Rs. 1000/hour and investments to get daily bonuses. They demand to register now. When the victim fills the form, pays the application fee, in most cases the scammer may disappear.

Another is online shopping. Scammers make fake social media pages and list cheap products. Victims order products, pay advance payment and the seller blocks the number and sometimes, they threaten them.

Weak passwords are also a big cause of cybercrime. When we use weak passwords like 12345678 and name+date, hackers easily guess and hack accounts.

Between **July 1 and the end of October 2024**, the **Federal Investigation Agency's Cybercrime Wing (FIA-CCW), Islamabad, Pakistan** received 1426 complaints of hacked WhatsApp accounts including Facebook, but most of them were recovered. Cybercrime is also caused by downloading and using fake apps. When we download apps and give permissions, all of our data is transferred to them.

- **My Personal Experience When I Became a Victim of Cyber crime:**

Early in my digital experience, I became a victim of email hacking due to using a very weak password (1 to 8). This incident taught me the importance of cybersecurity. An unauthorized person gained access to my account, and I later discovered that it was being used on two different mobile devices without my permission, which led to the exposure of my personal data. When I realized the issue, I immediately changed my password and secured the account. This incident became a turning point in my understanding of cybersecurity, teaching me that negligence in digital security can have serious consequences. After this experience, I created strong and unique passwords for every email, website, and application using combinations of letters, numbers, and special characters. I also kept a secure offline record of my passwords, restricted unnecessary app permissions, and became more cautious about suspicious messages related to fake investments and job offers, which are common in Pakistan. This experience strengthened my interest in cybersecurity and motivated me to pursue computer science to better understand digital threats and develop secure technological solutions.

- **Prevention Techniques for Students and Every Individual in Society:**

To stay safe from cybercrime, every student and individual should be careful and think before they click, share, or download anything online. Do not open unknown links or messages, even if they look official, and always check the website before entering personal information. Use strong passwords and never share your OTP, CNIC, or bank details with anyone. Install apps only from trusted app stores, keep your phone and software updated, and avoid using public Wi-Fi for important accounts. Be cautious of fake job offers, prize messages, and strangers on social media who ask for money or private details. In simple words, staying alert, verifying information, and protecting personal data are the most important steps to stay safe in the digital world.

Federal Bureau of Investigation, Washington DC X-Director said:

"The cyber world is a double-edged sword_that connects us as well as exposes us."

While global cybersecurity reports suggest that many internet users lack basic security awareness and are vulnerable to online threats. To practically check this report, in the month of **April 2025**, I surveyed in my college among **65 FSc students** in my class about their cyber security. A survey showed that **90% of students** reused the same password across multiple accounts. At that time, I taught them about cyber crimes in the world. After 2 days, I again asked from them about passwords. **55 students** had changed and made different strong their passwords of email accounts, mobile apps, and mobile passwords.

According to global researches data shows that:

- **United States** has the highest number of cybercrime victims globally. In 2021 it had **466,501 victims**, more than any other country. Other highly affected countries include **United Kingdom, Canada, India, and Australia.** In developing economies like **India,** financial losses from cybercrime exceeded **22,842 crore in Indian rupees in 2024,** showing that both rich and developing nations are heavily affected by digital threats.

- **Practical Implementation Through Programming Projects:**

  As part of promoting cyber security awareness, I developed a simple Password Strength Checker using Python. I noticed that many students and people in our society were using weak and sequential passwords like “123456” or their name with date of birth, which makes accounts easy to hack. This tool checks password length, character variety, and detects weak sequential patterns. It provides feedback and a strength percentage to guide users. After testing it with my friends, many realized their passwords were weak and changed them to stronger ones. This project helped me improve my programming skills while practically spreading awareness about digital security.

- **Future Goal and Academic Motivation:**

My long-term academic goal is to pursue a Bachelor’s degree in Computer Science with specialization in fields such as Artificial Intelligence, Cyber Security and Cloud Computing. I aim to develop advanced technical expertise and contribute to creating secure and intelligent software systems. The self-learning certifications in cyber security fundamentals, artificial intelligence foundations, and communication and leadership skills have strengthened my academic motivation and prepared me for international scholarship opportunities. Through continuous learning, research, and practical projects, I plan to become a skilled computer scientist who can address modern digital security challenges and innovate useful technological solutions for society.

- **Conclusion:**

  Cyber security awareness is essential for students in the digital era. Awareness, law enforcement, and digital responsibility are the key to reducing its causes and protecting society from its severe impacts. As the use of the internet, mobile phones, and social media is increasing day by day, the risks of cyber attacks, online fraud, and data theft are also growing. By learning basic cyber safety rules such as using strong passwords, not sharing personal information, and being careful about unknown links and messages, people can protect themselves from online dangers. Students should especially be educated about cyber security because they are the most active internet users. Therefore, spreading cyber security awareness will help create a safe digital environment, reduce cyber crimes, and build a responsible and secure society for the future.

Github Link: https://github.com/Ehtishamhyder/Password-Strength-Checker.py