Cyber Security

Application of Information & Communication Technology

About us:

JAHAN ZAIB
SIBGHA ZAMEER
WALEED AHMAD
FIZA TAHIR

Cyber Security

- **Introduction:**

Cybersecurity is the practice of protecting internet-connected systems such as hardware, software and data from cyber threats.

- **Types:**

There are many types of Cyber Securities like Application Security, Data Security, Cloud Security, Mobile Security, Network Security.

Cyber Security

THREATS:

Attack types	Description
Malware	Software designed to harm or gain unauthorized access.
Phishing	Deceptive techniques to trick users into revealing info.
DoS and DDoS Attacks	Overwhelm systems with excessive traffic.
Data breaches	Unauthorized access to sensitive data.
Insider threats	Threats from within an organization.
Spyware	Software that Secretly gathers information about a person or organization without their consent or knowledge.
Ransomeware	Software that encrypts files or locks a device, demanding payment for their release.

PASSWORD AUTHORIZER

What is Password Authorizer:

Password authorizer is a tool that takes password form user and tell whether the password is weak or strong .It is used to evaluate the effectiveness of password by analyzing various aspects of a password, such as length, complexity, and randomness, to determine how resistant it is to hacking attempts.

Why do we use Password Authorizer:

We use password authorizer for following purposes:

- **Security:**

Passwords are the first line of defense against unauthorized access to accounts or systems so we use it to increase the security of our account

- **Education and Awareness**:

Password Authorizer not only evaluate passwords but also educate users on the principles of strong password creation

- **Risk Mitigation**:

It is used to reduce risk against various attacks of hackers

Functionality of Password Authorizer

- **It consist up of password input box where user can enter and check the strength of password**
- **When user enter a strong password containing upper case letter , lower case letter , special character,8 or more letters etc then it shows that password is strong**
- **When user enters a weak password it shows the password is weak**
- **It also tells what is missing in password that makes it a weak password**

Working of Password Authorizer:

Weak Password: Indicates that the password is very easy to guess or crack.

Feedback: "Your password is weak."

Medium Password: Indicates that the password has some level of security but could be improved.

Feedback: "Your password is medium strength."

Strong Password: Indicates that the password is sufficiently secure and resistant to common attacks.

Feedback: "Your password is strong."

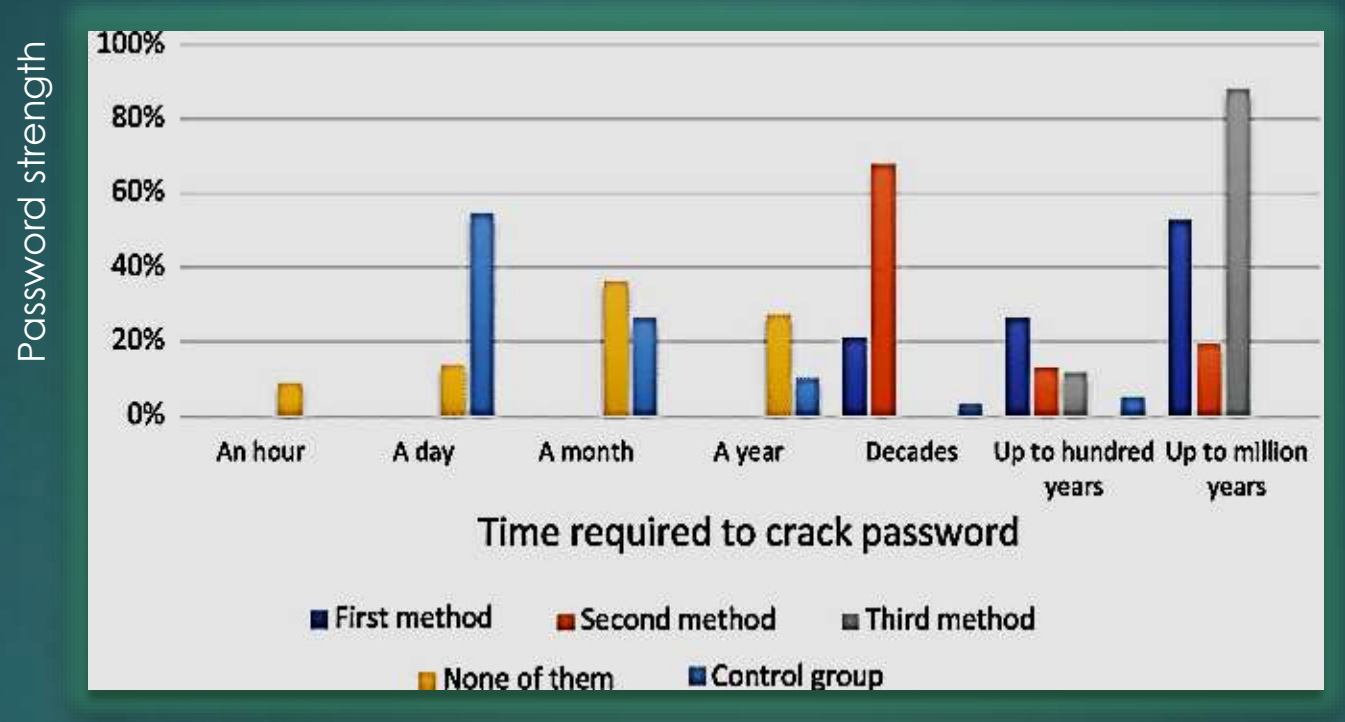
Password Length: Emphasizes the importance of having a long password.

Feedback: "Your password should be at least [8] characters long for better security."

Character Diversity: Encourages the use of a mixture of character types (uppercase letters, lowercase letters, numbers, and special characters).

FLOW CHART:

This chart shows how the strength of password affect the time required to crack the password.



Some common password authorizer:

- Kaspersky Password Checker.
- PasswordMeter.com.
- How Secure Is My Password.
- Norton Password Generator.

PHISHING WEBSITE

- **Definition:** A fraudulent website designed to mimic legitimate websites, aiming to trick users into providing sensitive information.
- **Characteristics:** Often look identical to real websites, including logos, design, and URL.
- **Intent:** To steal personal data such as login credentials, credit card information, or other sensitive data.

➢ **WORKING:**

- **Email or Message:** Users receive emails or messages directing them to the phishing website, often posing as trusted sources like banks, social media platforms, or online retailers.
- **Deceptive Tactics:** Phishing websites employ various tactics such as urgency (e.g., claiming an account will be suspended), fear (e.g., threat of legal action), or incentives (e.g., fake promotions) to prompt users to input their information.
- **Data Collection:** Once users enter their information on the phishing website, it is collected by the perpetrators for malicious purposes.

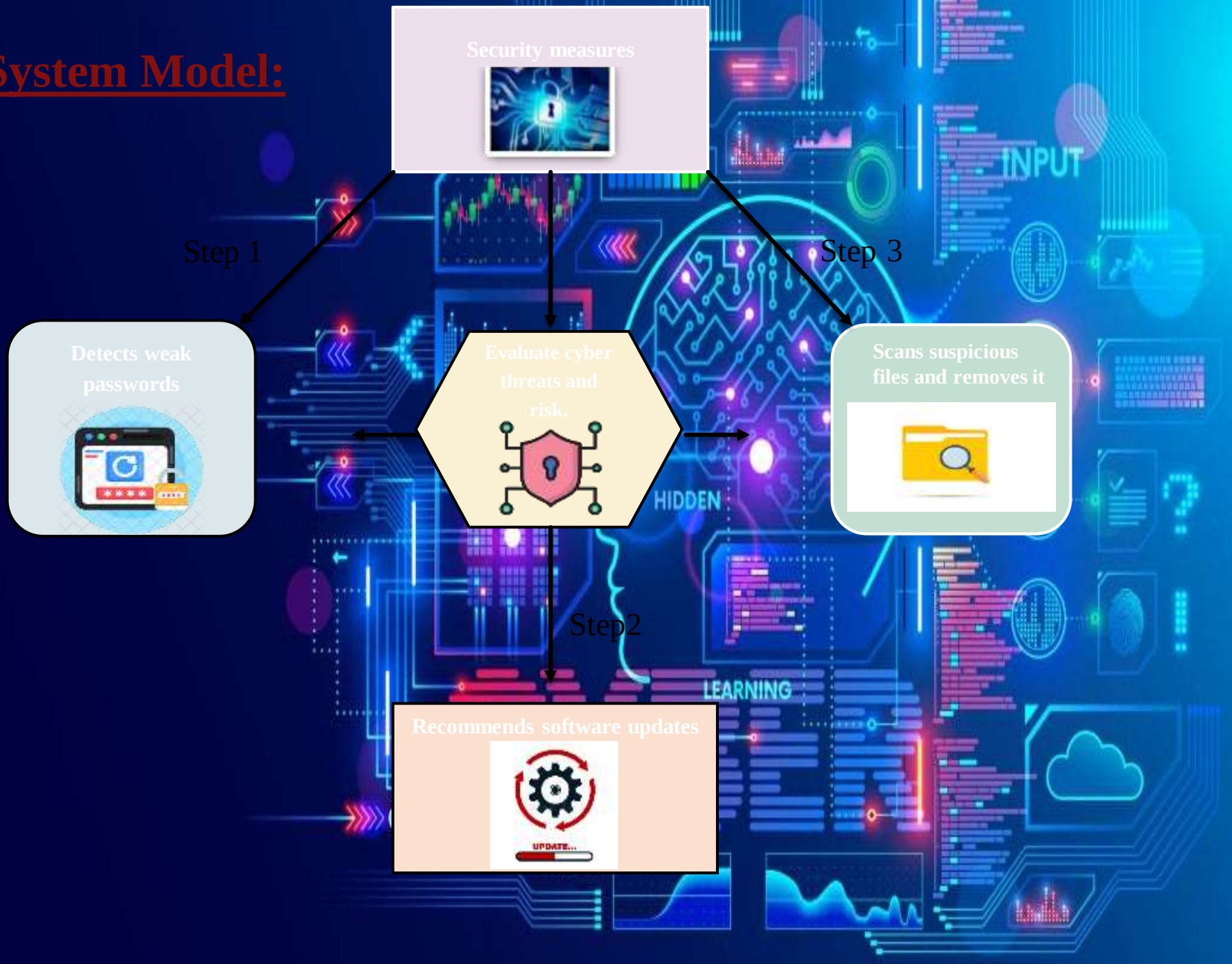
IMPACTS ON USERS:

- **Financial Loss:** Users may suffer financial loss if their banking or credit card information is compromised.
- **Identity Theft:** Personal information obtained through phishing can lead to identity theft, affecting users' credit scores and reputation.
- **Trust Erosion:** Incidents of phishing erode trust in online platforms and services, impacting users' confidence in conducting online transactions

CAUSES

- **Lack of Awareness:**
  . Many users are unaware of the existence and tactics of phishing websites, making them more susceptible to falling into the trap
- **Trust in Familiarity:**
  Users often trust familiar-looking websites or emails without verifying their authenticity, making it easier for phishing websites to deceive them.
- **Emotional Triggers:**
  Phishing emails often evoke emotions such as fear or excitement to prompt impulsive actions without careful consideration.
- **Poor Security Practices:**
  Users who fail to implement security measures such as multi-factor authentication or anti-phishing software are at a higher risk of falling victim to phishing attacks.

➢ System Model:



Virus Checker

- A virus checker, correctly called an antivirus, is a software program that automatically search a computer file for known viruses.

- Detect and prevent malicious software and viruses on your computer or laptop. An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software from your computer or laptop.

How it works?

Antivirus software usually works on one of **two principles**:

1. **Either it scans programs and files as they enter your device and compares them to known viruses.**
2. **It scans programs already on your device, looking for any suspicious behavior.**

Viruses

Some types of viruses are:

1. **Spyware**
2. **Trojan Horse**
3. **Worm Virus**
4. **DDOS Attack**

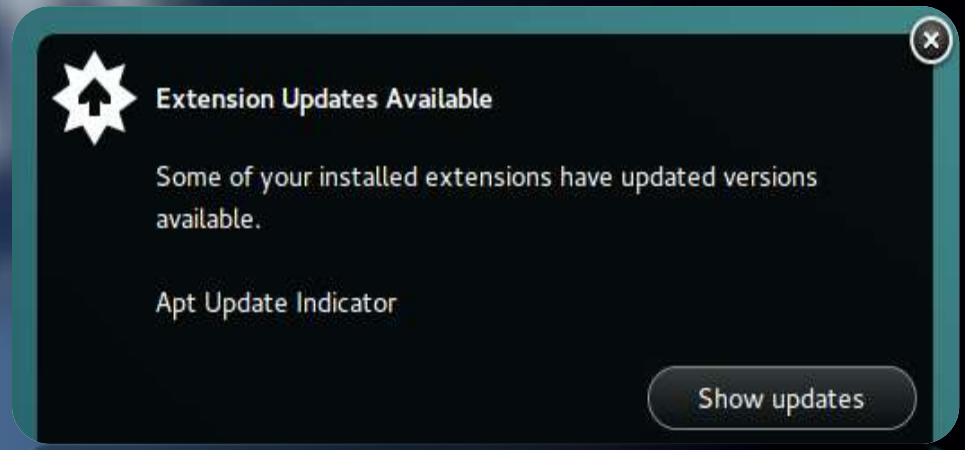
Antiviruses

Some types of Antiviruses are:

1. **Avast**
2. **Windows Defender**
3. **McAfee**
4. **Norton**

Update Notifier

- An **update notifier** is a tool or feature within software applications or systems that alerts users when updates are available for the software.
- It serves to inform users about new versions, patches, bug fixes, security updates, or feature enhancements.



Update Notifier

Importance:

- Windows Updates are often irritating to us, but they come with important **security updates** that are essential for the safety of it's users.
- If we don't update our operating system with time, it becomes obsolete and redundant to **malware attacks**.
- **Hackers** often exploit known vulnerabilities in outdated software to gain unauthorized access, or steal sensitive information.

Thank You!

Made with love for Sir Ahsan Arif...