Thinking Securely in a Digital World

Kavinga Yapa Abeywardena

Sr. Lecturer - Computer Systems Engineering Department

Faculty of Computing - SLIIT

Why Should *Every Student* Think About Cybersecurity?

YOUR **SOCIAL MEDIA ACCOUNTS**

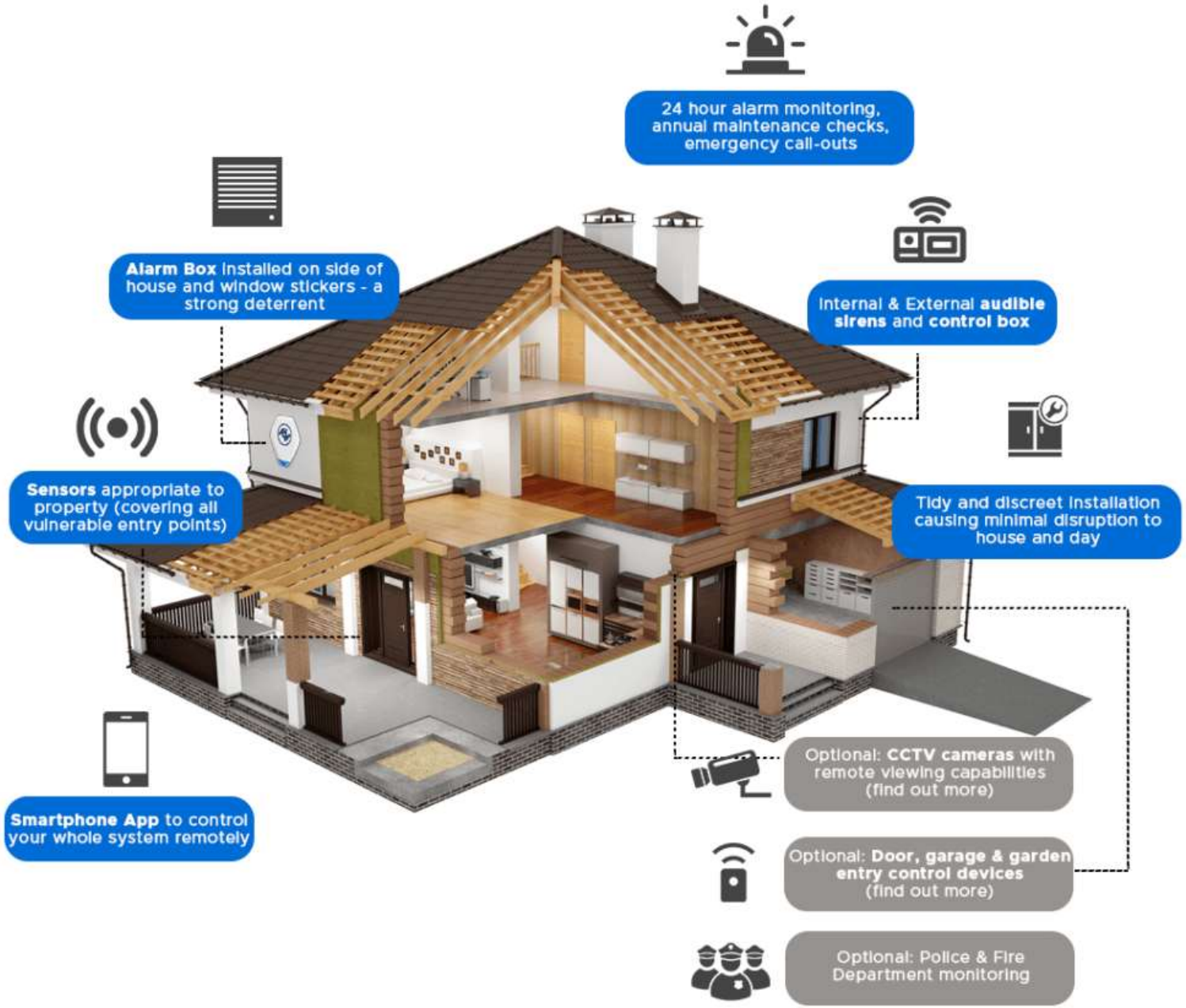
YOUR **BANKING / PAYMENT APPS**

YOUR **UNIVERSITY LMS ACCOUNT**

YOUR **PERSONAL PHOTOS AND DOCUMENTS**

YOUR **FUTURE WORKPLACE SYSTEMS**

- Cybersecurity is not only an IT problem.
- It is a **daily decision-making skill** for every digital user.


24 hour alarm monitoring, annual maintenance checks, emergency call-outs
Alarm Box installed on side of house and window stickers - a strong deterrent
Internal & External audible sirens and control box
Sensors appropriate to property (covering all vulnerable entry points)
Tidy and discreet installation causing minimal disruption to house and day
Smartphone App to control your whole system remotely
Optional: CCTV cameras with remote viewing capabilities (find out more)
Optional: Door, garage & garden entry control devices (find out more)
Optional: Police & Fire Department monitoring

Information is an **asset** which like other important business asset, has **value** to an organization and consequently needs to be suitably **protected**.

Information Security

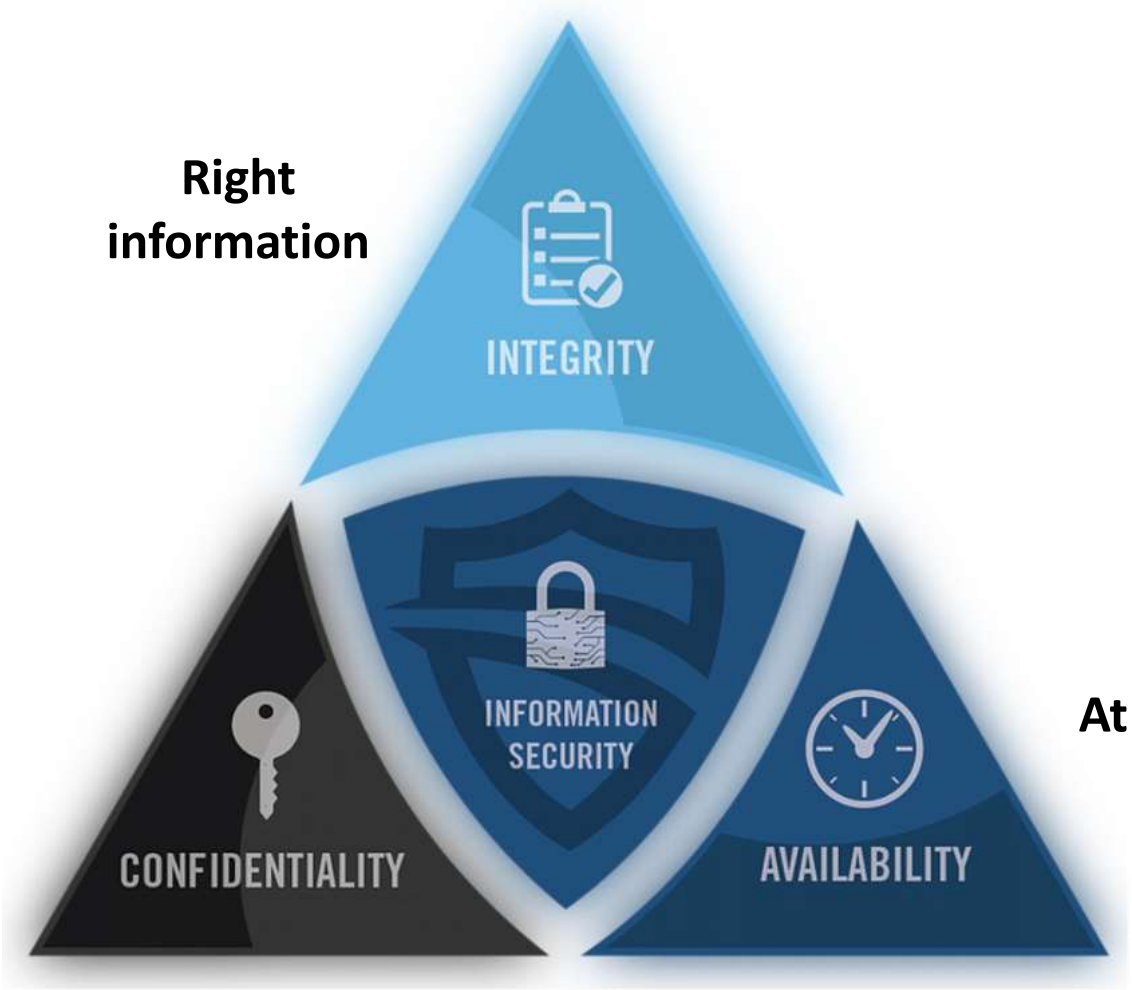
The **protection** of information and its elements including systems and hardware that use, store and transmit that information.

Primary Goals of IS (CIA)

Right information

To the right person

At the right time



Confidentiality

- Ensuring that the information is accessible only to those authorized to have access
- Achieved by,
  - Password
  - Two-factor authentication
  - Biometric verification
  - Encryption

Integrity

- Safeguarding the accuracy and completeness of information and processing method
- Achieved by
  - Version control
  - Backups and recovery procedures
  - Checksums & digital signature
  - Encryption

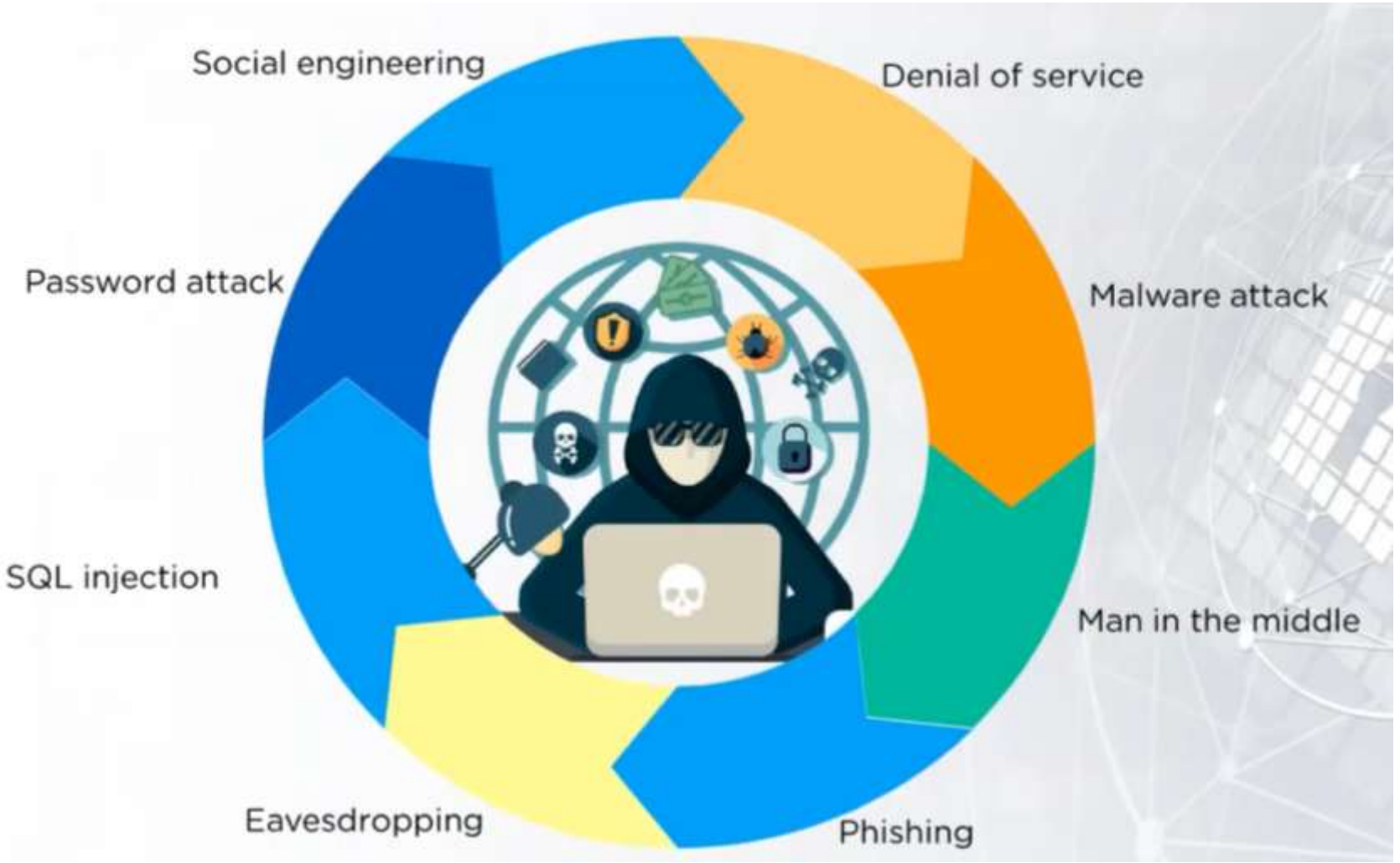
Availability

- Ensuring that authorized users have access to information when required
- Achieved by
  - Offsite-backup
  - Redundancy
  - Disaster recovery
  - Proper monitoring
  - Failover

Security breaches leads to

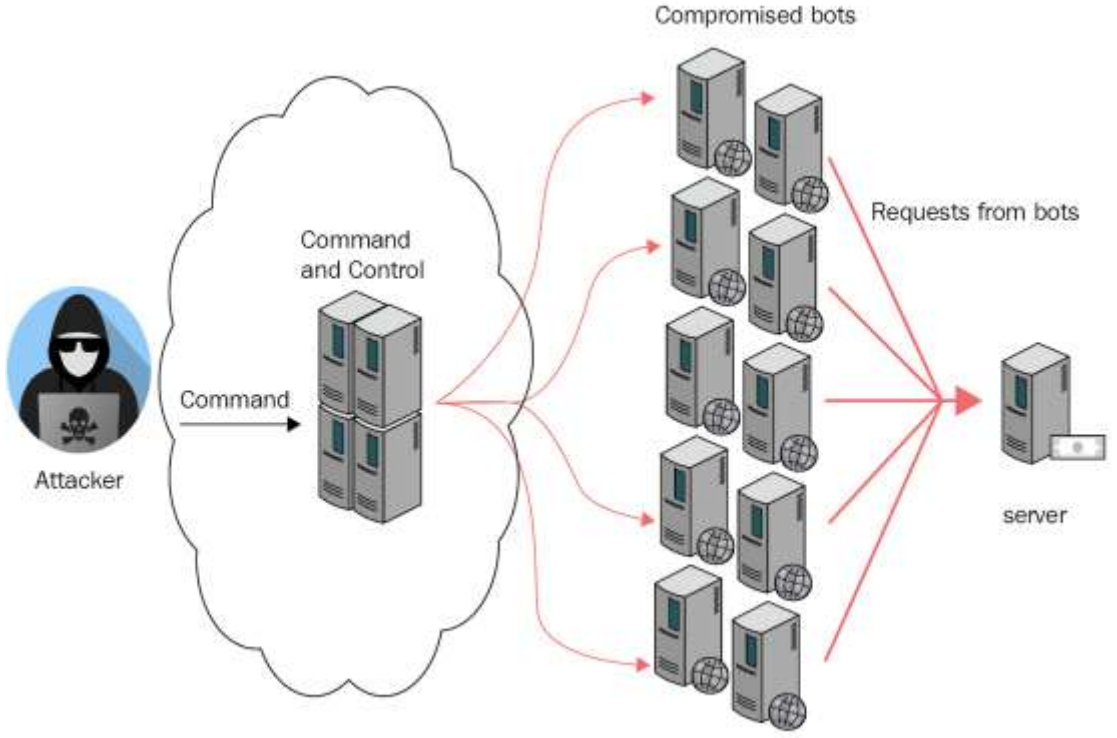
- Reputation loss
- Financial loss
- Intellectual property loss
- Loss of customer confidence
- Business interruption cost

Types of Attacks



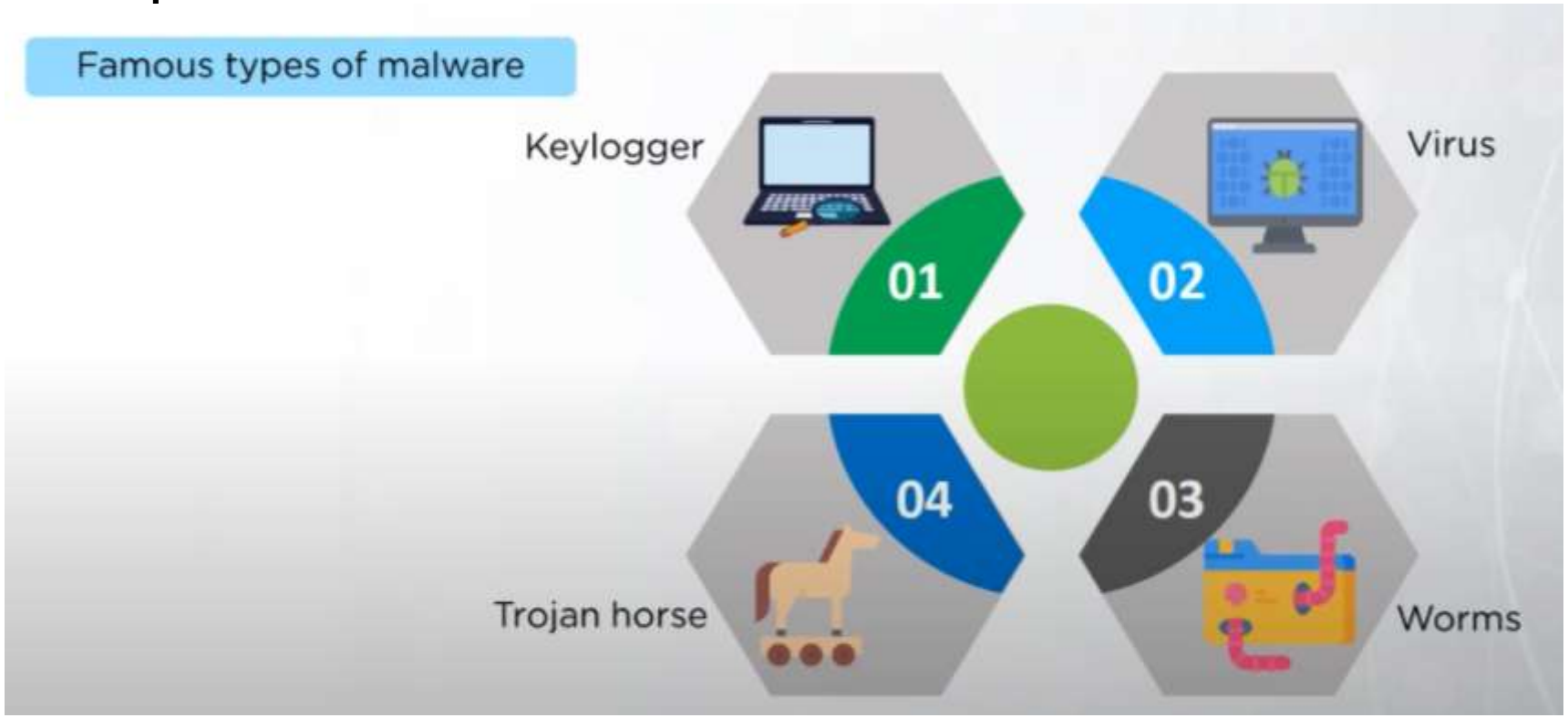
1. Denial of Service (DOS Attack)

- Make an **online resource or service unavailable** to its intended users by temporarily or indefinitely by disrupting a host connected to the Internet.



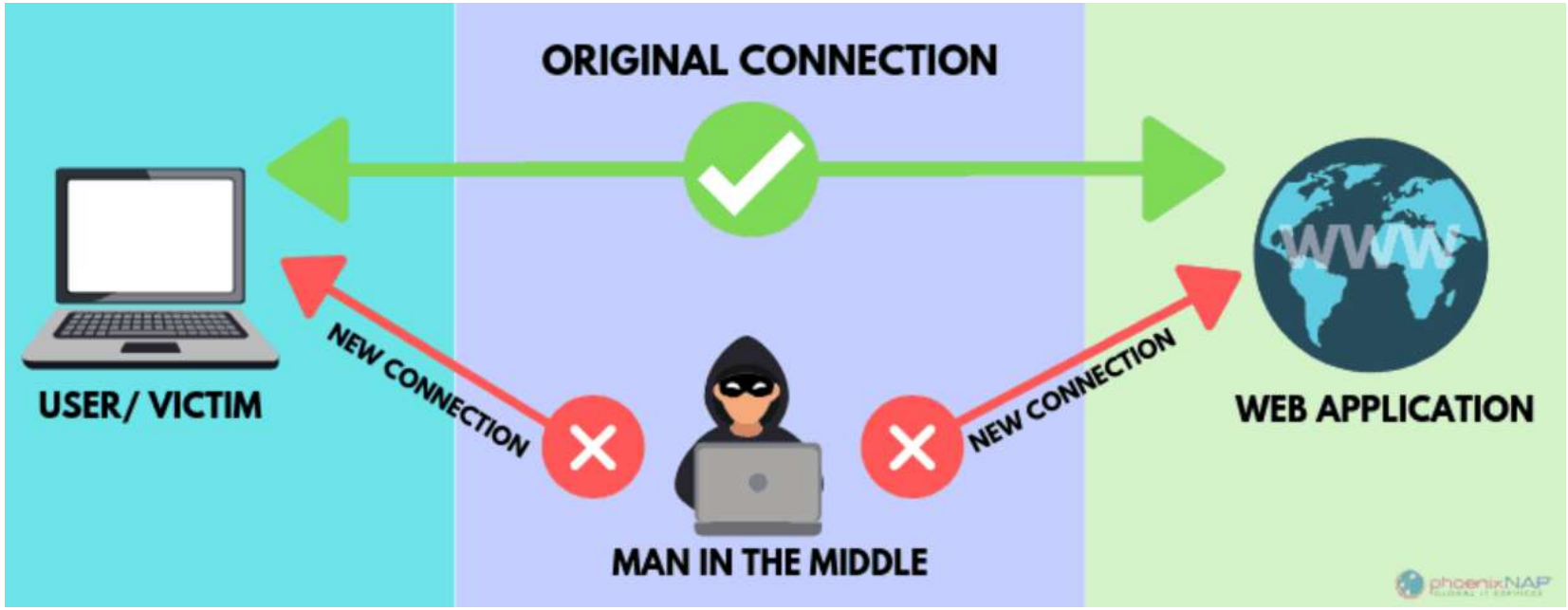
2. Malware

- It is a **malicious program** or software that disrupts or damages the computer



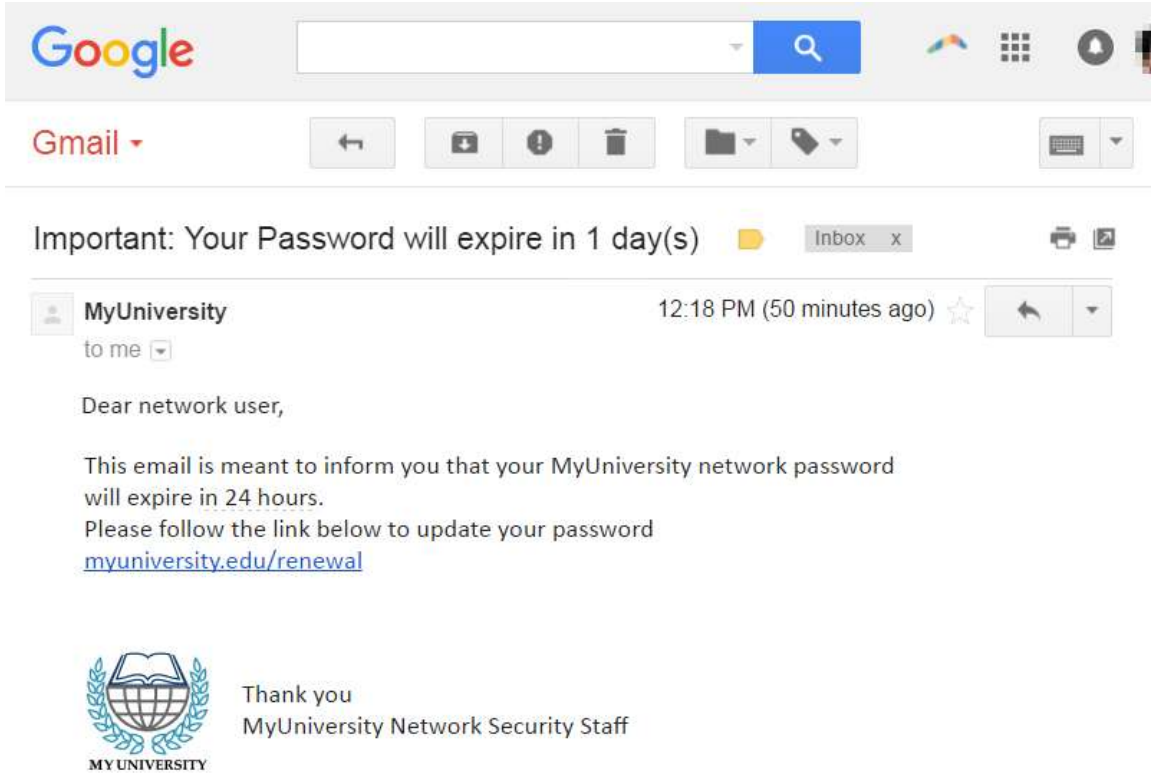
3. Man in the Middle

- Network-based attack whether the **attacker intercept the communication** or the data flow between victim and the end-point



4. Phishing Attack

- Practice of **sending fraudulent communications** that appear to come from a reputable source often in a form of email



E.g. Email claiming to be from:

- Bank
- University
- PayPal
- Facebook

Purpose:

- steal passwords
- steal credit card info

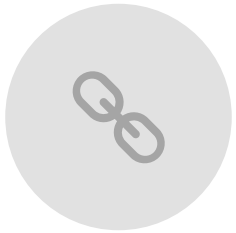
Threat Decomposition - Phishing Attacks

At which step can we stop the attack?

Pattern Recognition - Phishing Attacks

URGENT LANGUAGE

UNKNOWN SENDER



SUSPICIOUS LINKS

REQUESTS FOR PASSWORDS

“YOU WON A PRIZE”

You should learn to **recognize patterns**, not memorize attacks!

Algorithmic Thinking - Prevention Phishing Attacks

SAFE EMAIL DECISION ALGORITHM

CHECK SENDER ADDRESS

CHECK URGENCY

HOVER OVER LINK

VERIFY FROM OFFICIAL WEBSITE

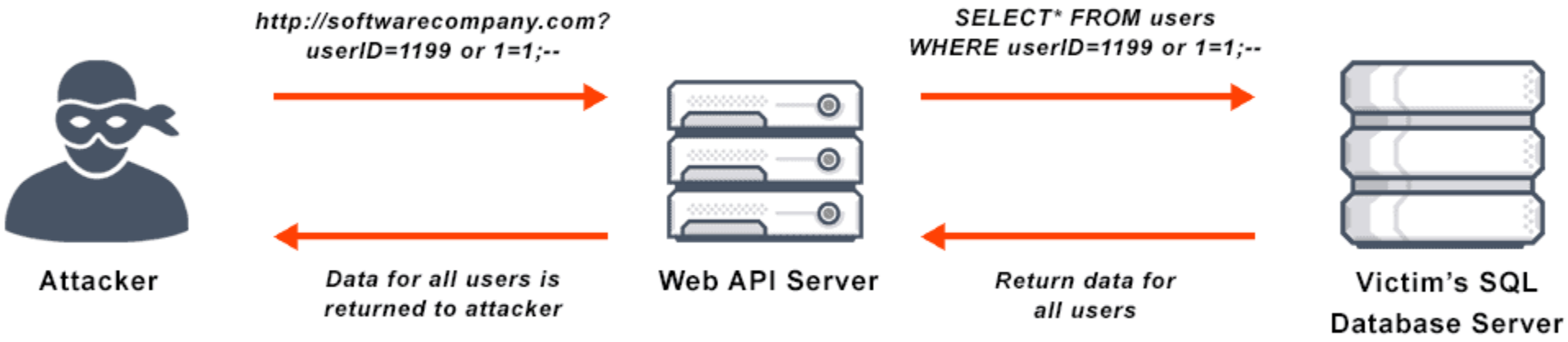
IF SUSPICIOUS → DO NOT CLICK

5. Eavesdropping

- Attacker **observe the network traffic** in your system
- Example

6. SQL Injection

- Attacker **inject malicious input into an SQL statement** retrieve information from a database



7. Password Attack

- **Crack or get the password** for user account
- E.g.

Dictionary attack

We use every password that is possible through the dictionary

Brute force

It is a trial and error method used to decode the password or data

Keylogger

keylogger records all the hits on the keyboard

Shoulder surfing

attackers observe the user's keyboard by looking over the user's shoulder

8. Social Engineering

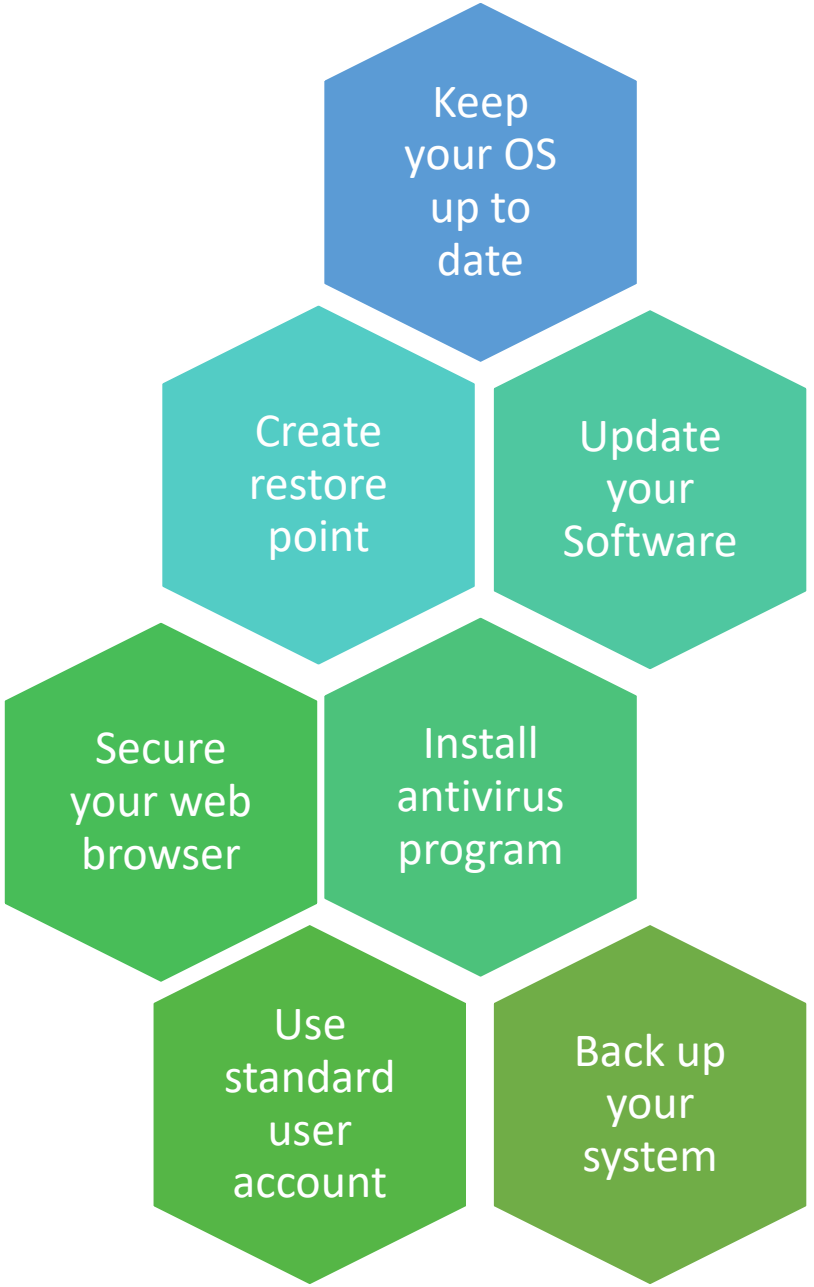
- Attackers **create social situations that encourage you to share confidential information**
- Phishing is an example for social engineering attack

How to secure?

Basic computer security checklist

- [x] User is **password** protected
- [x] **OS** is updated
- [x] Download software from reputable sources
- [x] **Antivirus** or antimalware is installed
- [x] Terminate unusual services running that consumes resources
- [x] **Firewall** is on
- [x] Clear private data from web browsers
- [x] Backup regularly

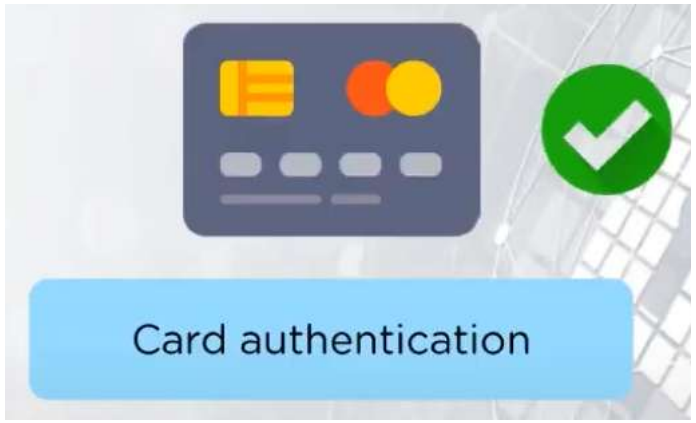
Secure your OS

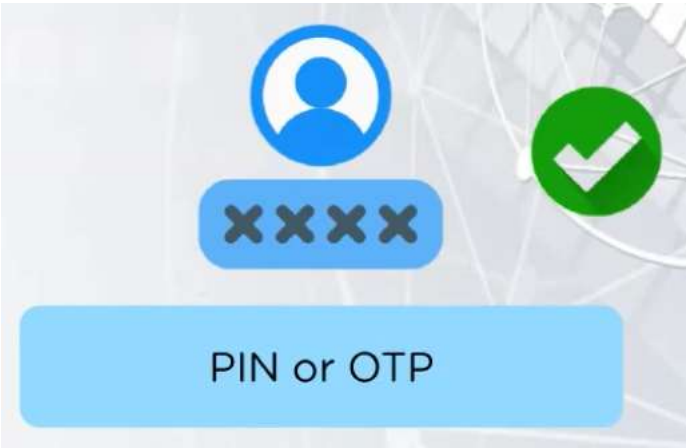


2-factor authentication

- Adds **layer of security to the authentication process** by making it harder for attacker to gain access to a person's device or online accounts

For example: When you do online payment





Secure Password

- Create strong passwords so that no one will be able to remember/crack
- A good password should
  - not contain your basic details (name, birthdate, mobile number etc)
  - Contain at least 8 characters
  - Be combination of upper and lower case
  - Contain numbers and special characters
  - Be randomized

Antivirus

- Computer program that **prevent**, **detection** and **remove malware**
- Install an Antivirus and keep it up to date

Firewall

- A firewall is software or firmware that **prevents unauthorized access to a network**
- The barrier that sits between a private internal network and the public Internet
- The main purpose is to **allow non-threatening traffic in and to keep dangerous traffic out**

Thank You!