Cybersecurity

Cybersecurity

- The practice of protecting systems, networks, and programs from digital attacks
- Information Security: Protecting confidentiality, integrity, and availability of information
- Network Security: Safeguarding networks from unauthorized access and malicious attacks
- Application Security: Securing software applications from vulnerabilities that could be exploited
- Data Security: Protecting data from unauthorized access, theft, or corruption
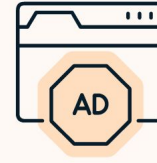
Cyber Threats

Malware

Phishing

1. Attacker sends phishing mail to target

Hacker

Target

3. Hacker collects important credentials

4. Hacker uses victim's credentials to access private information

2. Victim clicks on Phishing link and visits fake website

Original Website

Phishing Website
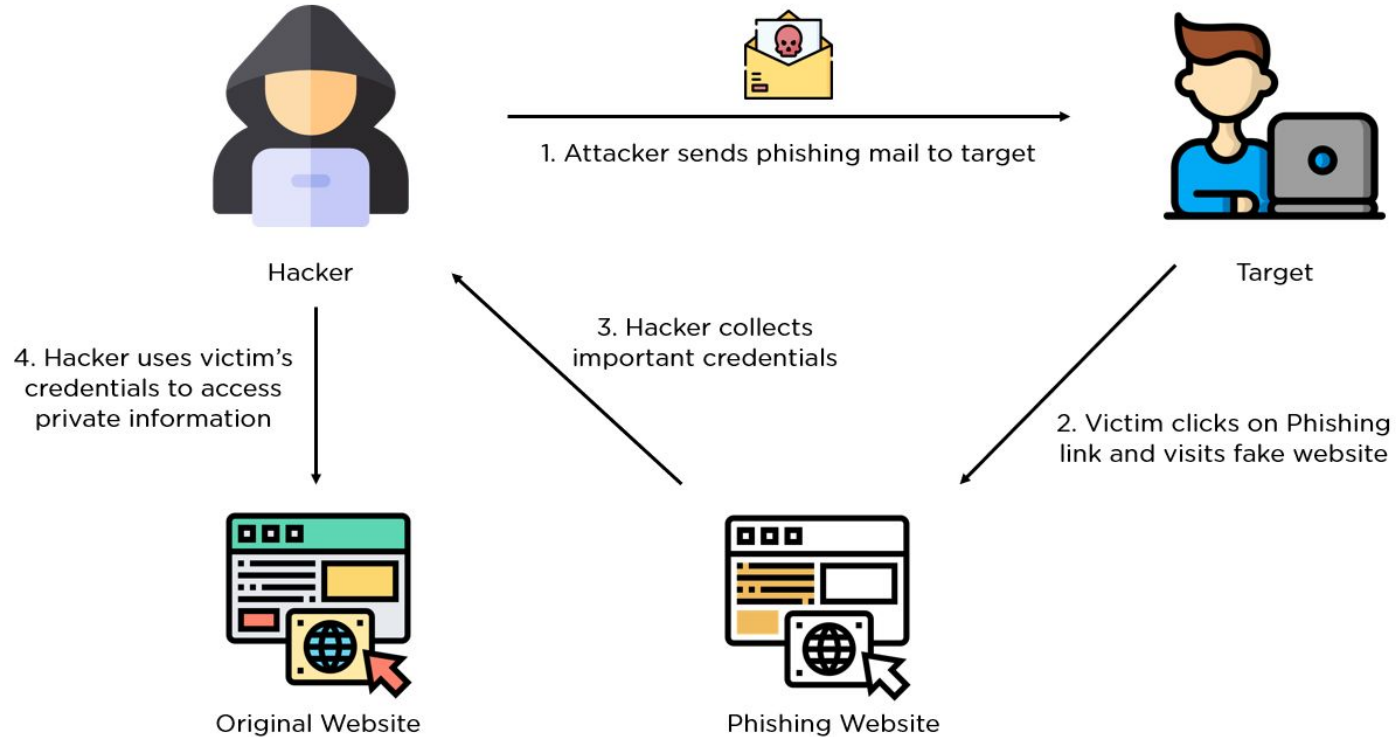
Social Engineering

Social Engineering Tactics to Watch For

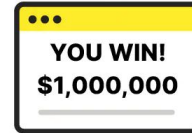Knowing the red flags can help you avoid becoming a victim.
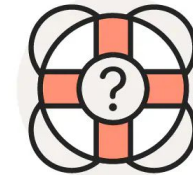
Your 'friend' sends you a strange message.

Your emotions are heightened.

The request is urgent.

YOU WIN! $1,000,000

The offer feels too good to be true.

You're receiving help you didn't ask for.

The sender can't prove their identity.

Man-in-the-middle

And much more...

Cyber Defense (Individual)

As individual person

- Change default password
- Strong password
- Software up-to-date
- Don't click link from unknown sender
- MFA (Multi-factor authentication)
- Avoid public Wi-Fi
- Backup data (Mostly to the cloud)

Homework

- The important of cybersecurity
- [Research] Finding the news about data breach and understand how much impact
- [Research] Finding the method to handling phishing or scammer
  - Keyword: Cybersecurity Awareness

End of presentation