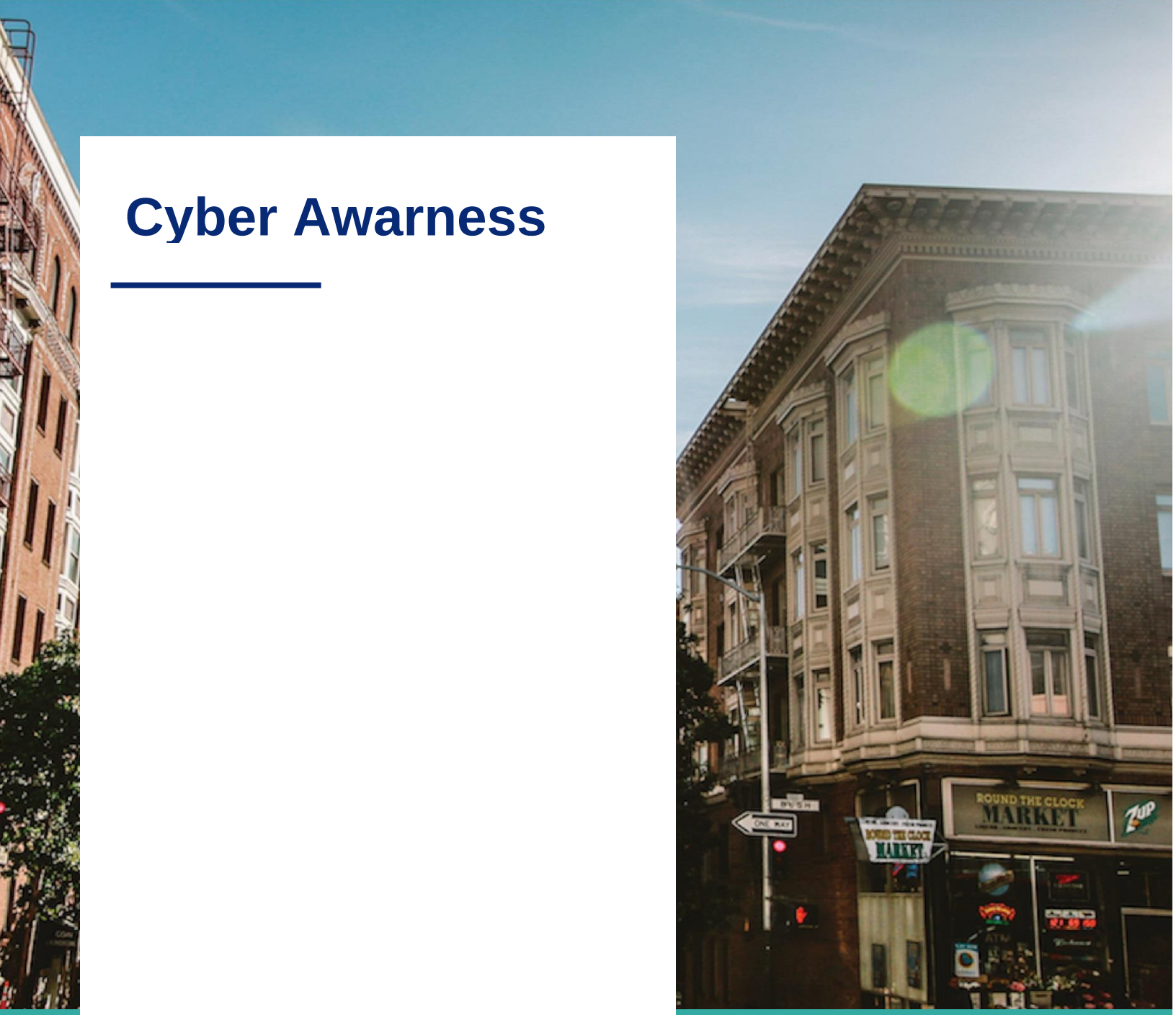


Cyber Awarness

NOVEMBER 23

TITLE: Cyber Awarness

NAME: Harsh Baheti

DIV: A

ROLL NO: SECOA112

GUIDED BY: Mrs. Anagha Chaudhari

Abstract

When an enterprise's employees are cyber security aware, it means they understand what cyber threats are, the potential impact a cyber-attack will have on their business and the steps required to reduce risk and prevent.

“One of the main cyber-risks is to think they don't exist."

During These Lockdown Period there is 72.56% increase in cyber attacks.There should be awareness in people about cyber security. As a web security company, over the past weeks, we have been witnessing an increased amount of website exploitation attempts. Unfortunately, many threat actors have started to abuse the panic and discomfort of the COVID-19 pandemic to conduct special crafted malware and phishing attacks worldwide. As an increased amount of work now happens online, this page serves the purpose of making it easier to spread awareness.

Table Of Content

What Are Cyber Threats?

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general or use a breached computer as a launch point for other attacks.

Cyber Threats:-

1. Malware
2. Phishing
3. Password Attacks
4. DDoS
5. Man In Middle
6. Drive By Download
7. Maladvertising
8. Rogue Software

Malware

Malware is the collective name for a number of malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network.

Types:-

- Spyware.
- Adware.
- Trojan.
- Worms.
- Virus.
- Rootkits

Phishing 

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Types:-

- **Email phishing**
- **Spear phishing**
- **Smishing and vishing**
- **Angler phishing**

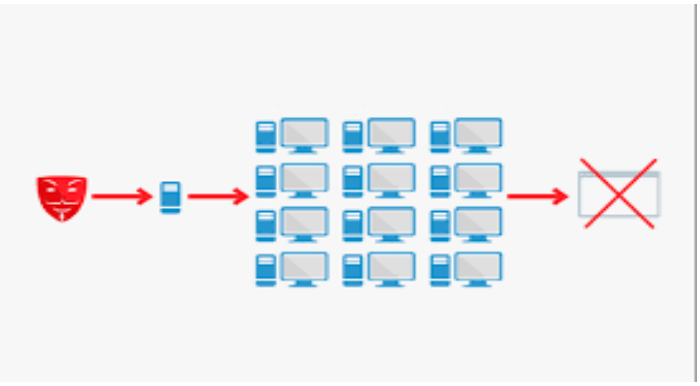
Password Attacks

In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system in scrambled form

Types of attacks:

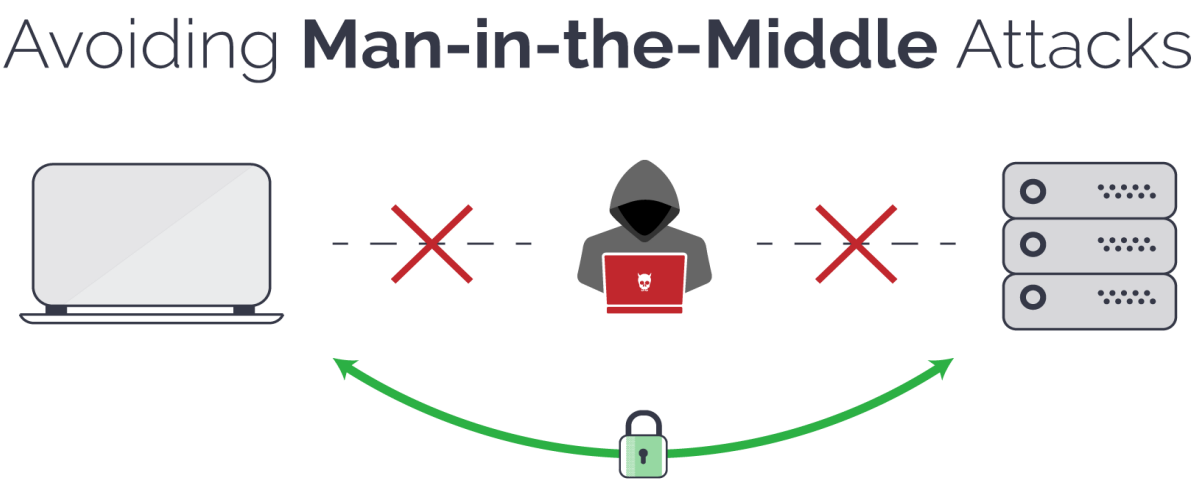
- **Brute Force Attack**
- **Dictionary Attack**
- **Rainbow Table Attack**
- **Credential Stuffing**
- **Password Spraying**
- **Keylogger Attack**

DDoS



In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Man In Middle

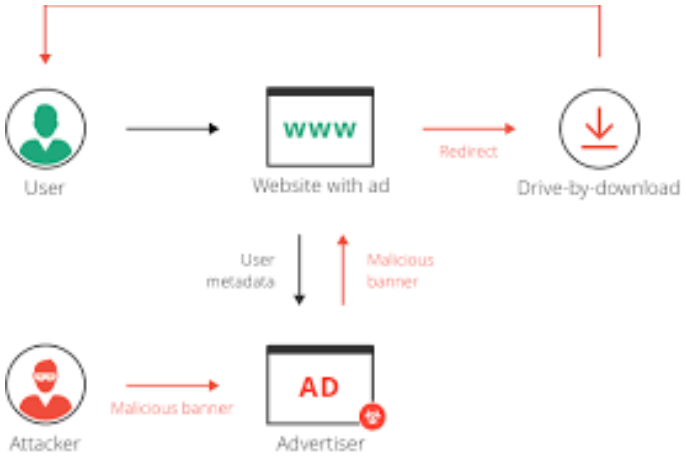


In cryptography and computer security, a man-in-the-middle, monster-in-the-middle, machine-in-the-middle, monkey-in-the-middle or person-in-the-middle (PITM) attack is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Drive By Download

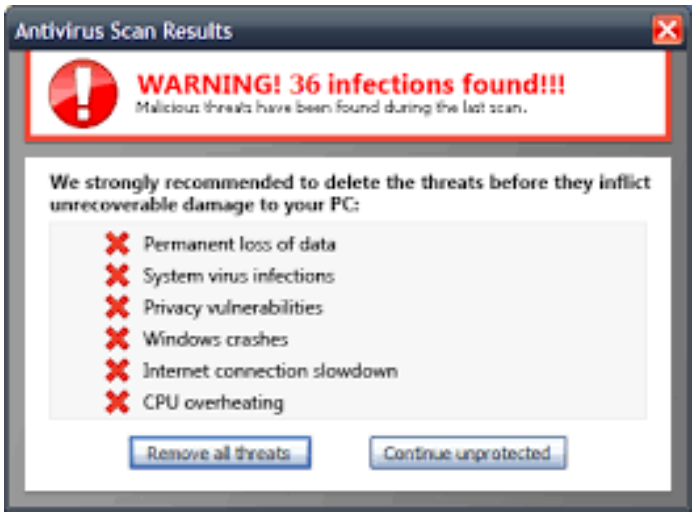
Drive-by download means two things, each concerning the unintended download of computer software from the Internet: Downloads which a person has authorized but without understanding the consequences. Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.

Maladvertising



Malvertising is the use of online advertising to spread malware. It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages

Rogue Software



Rogue security software is a form of malicious software and internet fraud that misleads users into believing there is a virus on their computer and aims to convince them to pay for a fake malware removal tool that actually installs malware on their computer.

Conclusion

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The vulnerability management life cycle is designed to counter the efforts made by the attackers in the quickest and most effective way. This chapter has discussed the vulnerability management life cycle in terms of the vulnerability management strategy. It has gone through the steps of asset inventory creation, the management of information flow, the assessment of risks, assessment of vulnerabilities, reporting and remediation, and finally the planning of the appropriate responses. It has explained the importance of each step in the vulnerability management phase and how each should be carried out.