Unit-4- E-Commerce Security and Fraud Issues and Protections

Basic EC Security Terminology, The Threats, Attacks, and Attackers
EC Security Requirements: Confidentiality, Integrity and Availability, Authentication, Authorization and Nonrepudiation; **Technical Malware attack:** Viruses, Worms, and Trojan Horses, Heartbleed, Distributed Denial of Service, Crypto blocker, Page hijacking, Botnets, Malvertising, ransom ware, sniffing, **Non-Technical malware attack:** Social Phishing, Pharming, Identity Theft and Identify Fraud, Spam Attacks; EC defines Strategy: access control(Authorization and Authentication, Biometric Systems), encryption and PKI (Symmetric Key Encryption, Asymmetric Key Encryption, Certificate Authority(CA), Secure Socket Layer(SSL). Securing e-commerce networks: Firewalls, Virtual Private Networks, Intrusion Detection Systems (IDS), intrusion prevention System (IPS). **[10 LH]**

E-Commerce Security: -

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised.

- Information security, or information systems security, refers to a variety of activities and methods that protect information systems, data, and procedures from any action designed to destroy, modify, or degrade the systems and their operations.
- Computer security in general refers to the risks and protection of data, networks, computer programs, computer power, and other elements of computerized information systems.
- It is a very broad field due to the many methods of attack as well as the many modes of defense.
- The attacks on and defenses for computers can affect individuals, organizations, countries, or the entire web.
- Computer security aims to prevent, repair, or at least minimize attacks.
- E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction

Following are the essential requirements for safe e-payments/transactions –

- **Confidentiality:** Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.
- **Integrity:** Information should not be altered during its transmission over the network.
- **Availability**: Information should be available wherever and whenever required within a time limit specified.
- **Authenticity**: There should be a mechanism to authenticate a user before giving him/her access to the required information.
- **Non- retraction:** It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of a message should not be able to deny the receipt.
- **Encryption:** Information should be encrypted and decrypted only by an authorized user.
- **Auditability:** Data should be recorded in such a way that it can be audited for integrity requirements.

EC Security Requirements

- **Authentication :** Authentication is a process used to verify (assure) the real identity of an EC entity, which could be an individual, software agent, computer program, or EC website. For electronic messages, authentication verifies that the sender/receiver of the message is who the person or organization claims to be (the ability to detect the identity of a person/entity with whom you are doing business).
- **Authorization:** Authorization is the provision of permission to an authenticated person to access systems and perform certain operations in those specific systems.
- **Auditing:** When a person or program accesses a website or queries a database, various pieces of information are recorded or logged into a file. The process of maintaining or revisiting the sequence of events during the transaction, when and by whom, is known as auditing.

- **Availability:** Assuring that systems and information are available to the user when needed and that the site continues to function. Appropriate hardware, software, and procedures ensure availability.
- **Nonrepudiation:** Closely associated with authentication is nonrepudiation, which is the assurance that online customers or trading partners will not be able to falsely deny (repudiate) their purchase, transaction, sale, other obligation. Nonrepudiation involves several assurances, including providing proof of delivery from the sender and proof of sender and recipient identities and the identity of the delivery company.
- **Confidentiality:** For sender, intended receiver should understand message contents using encryption and decryption. For sender, intended receiver should understand message contents.
- **Integrity:** sender and receiver want to make sure that the message are not altered without detection.

Threat, attack and attacker

- Anything potential to cause harm to the computer system or organization.
- A threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.
- A threat can be either "intentional" or "accidental" or otherwise a circumstance, capability, action, or event.
- Unintentional threats fall into three major categories: human error, environmental hazards, and malfunctions in the computer system.
- In computers and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset.
- An attacker is the individual or organization performing these malicious activities.

Intentional Attacks and Crimes

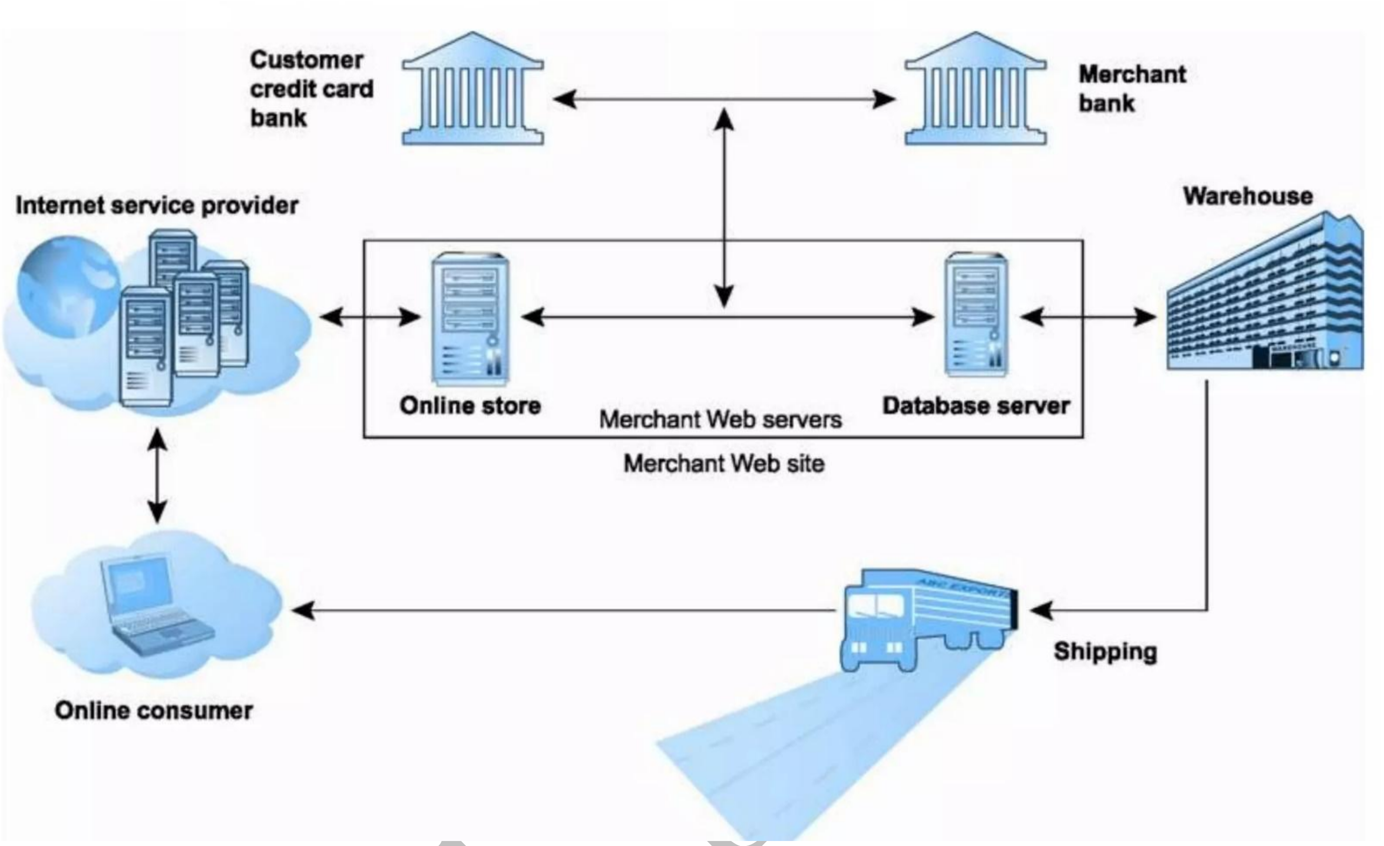
- Intentional attacks are committed by cybercriminals.
- Types of intentional attacks include theft of data, inappropriate use of data (e.g., changing it or presenting it for fraudulent purposes), theft of laptops and other devices and equipment, and/or inserting computer programs to steal data, vandalism or sabotage directed toward the computer or its information system damaging computer resources, losses from malware attacks, creating and distributing viruses and causing monetary losses due to Internet fraud.
- Intentional crimes carried out using computers and the Internet are called cybercrimes, which are done by cybercriminals (criminals for short) that include hackers and crackers. A hacker describes someone who gains unauthorized access to a computer system. A cracker (also known as a black hat hacker) is a malicious hacker with extensive computer experience who may be more damaging.

Basic EC Security Terminology

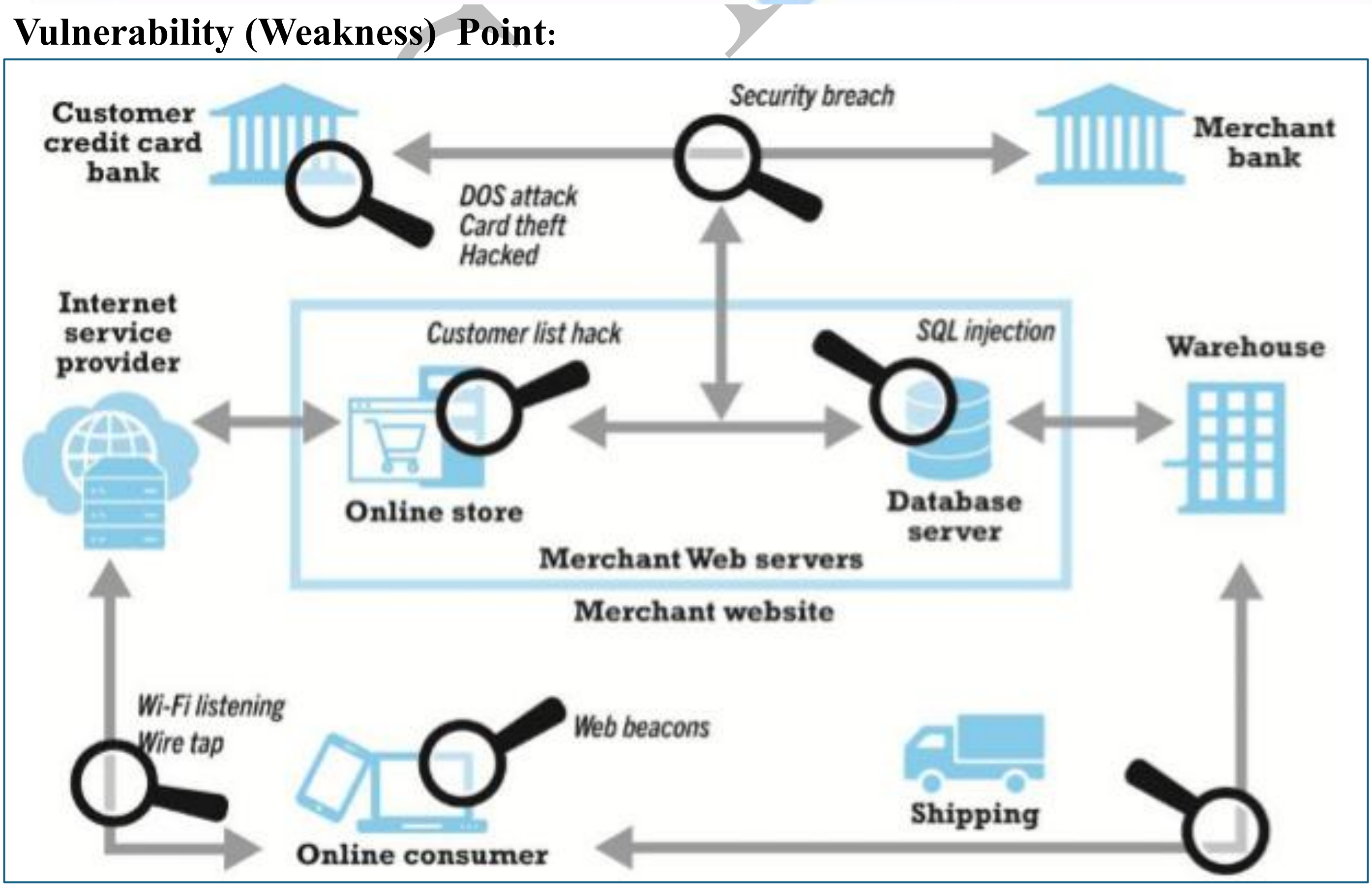
- **Business continuity plan:** A plan that keeps the business running after a disaster occurs. Each function the business should have a valid recovery capability plan.
- **Cybercrime:** Intentional crime carried out on by using the Internet.
- **Cybercriminal:** A person who intentionally carries out crimes over the internet.
- **Exposure:** An instance of being exposed to losses from an attack that exploits vulnerability (including estimate of damages).
- **Fraud:** Any business activity that uses deceitful practices or devices to deprive another of property or other rights.
- **Vulnerability:** Weakness or fault that can lead to exposure.
- **Malware:** malicious code such as viruses, worms, Trojan horses, bots, backdoors, spyware, adware, etc.
- **Cyber vandalism:** Intentionally disrupting, defacing or destroying a Web site.

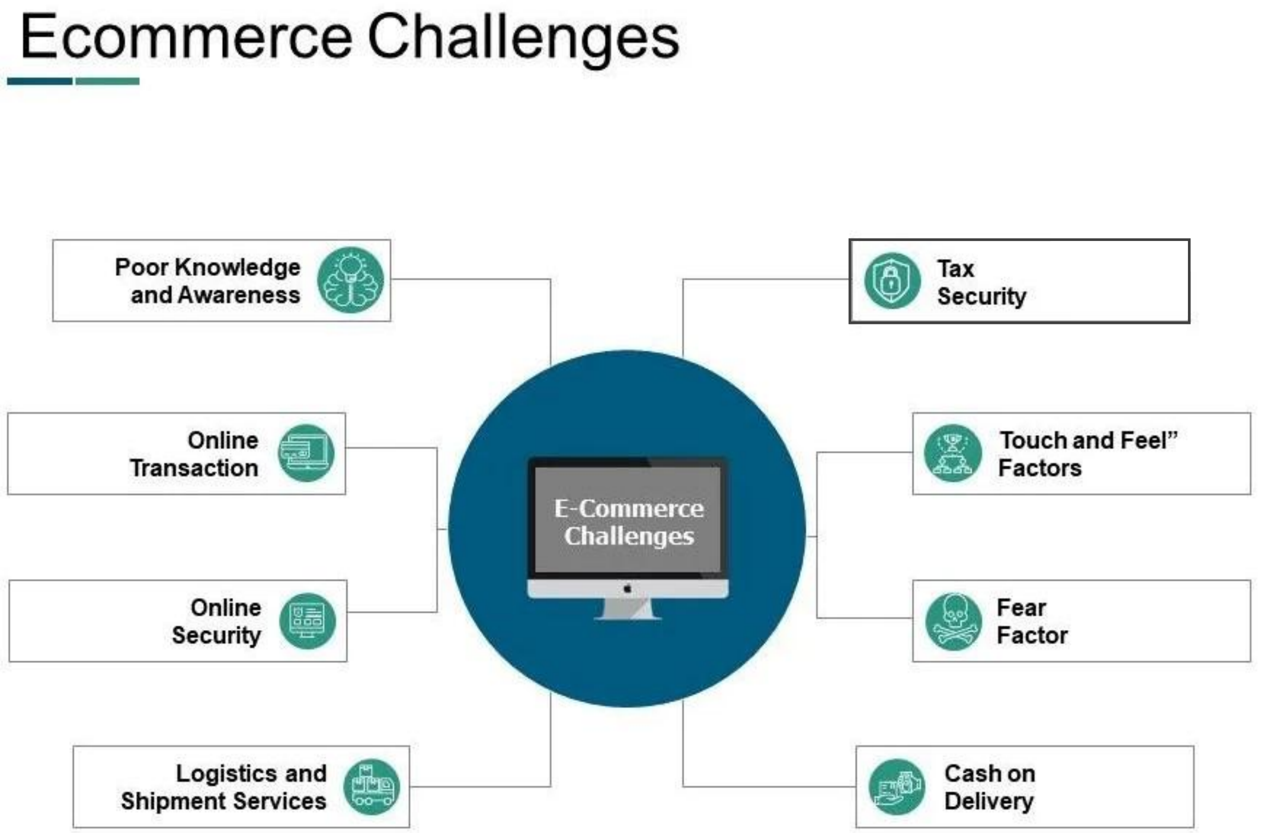
Typical E-commerce Transactions:

Payment gateways serve as the gateway for processing payments during e-commerce transactions. If these gateways are not adequately secured, they can become prime targets for cyber attackers seeking to steal sensitive financial information.



Vulnerability (Weakness) Point:



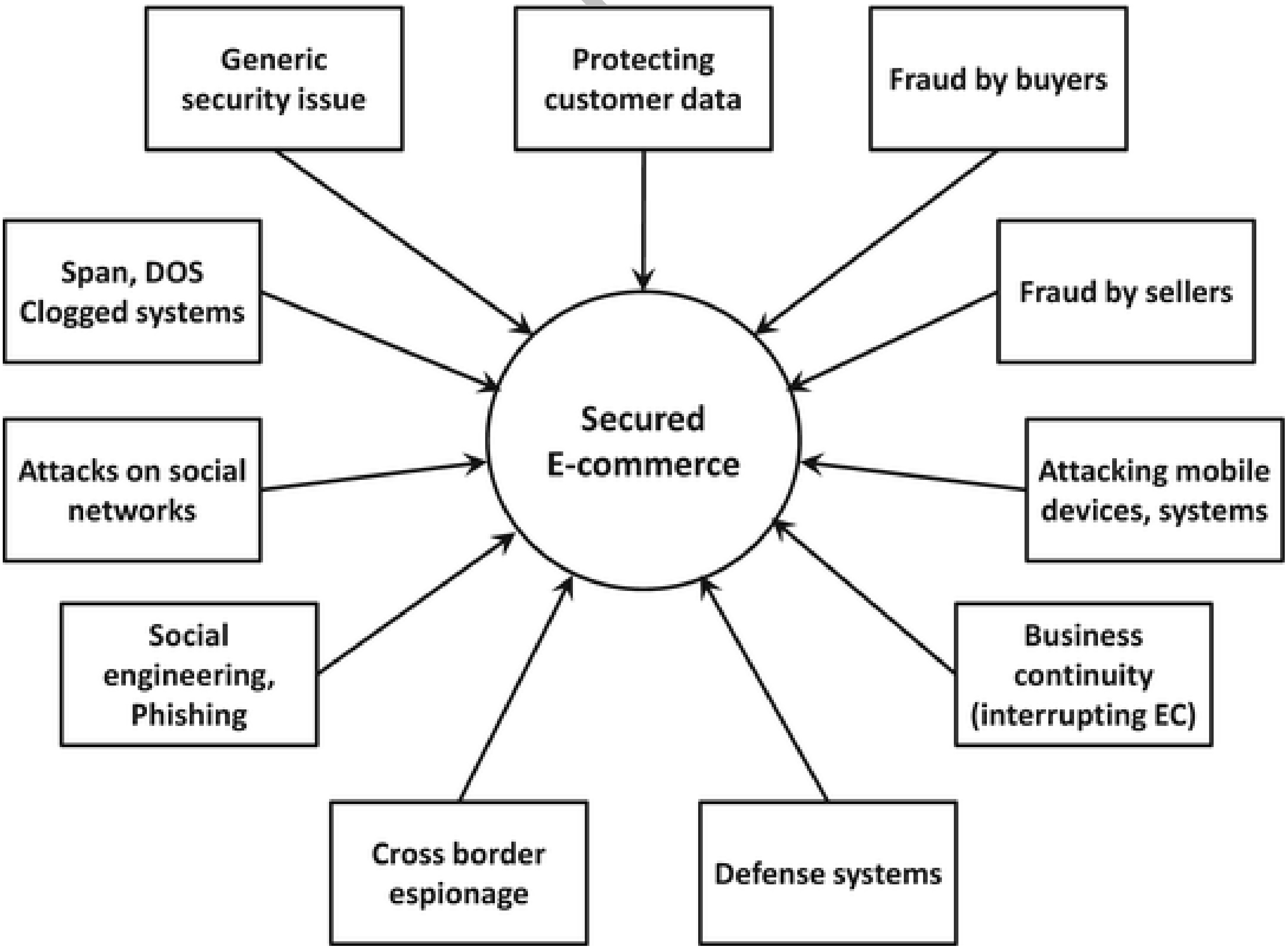


Ecommerce Challenges

E-Commerce Challenges

- Poor Knowledge and Awareness
- Online Transaction
- Online Security
- Logistics and Shipment Services
- Tax Security
- Touch and Feel" Factors
- Fear Factor
- Cash on Delivery

Major E-commerce Security Management Concerns:



Secured E-commerce

- Generic security issue
- Protecting customer data
- Fraud by buyers
- Fraud by sellers
- Attacking mobile devices, systems
- Business continuity (interrupting EC)
- Defense systems
- Cross border espionage
- Social engineering, Phishing
- Attacks on social networks
- Span, DOS Clogged systems

Technical Malware attack

Hackers often use several software tools (which unfortunately are readily and freely available over the Internet together with tutorials on how to use them) to learn about vulnerabilities as well as attack procedures.

Malware (Malicious Software): Viruses, Worms, and Trojan Horses:

- Malware is a software program that, when spread, is designed to infect, alter, damage, delete, or replace data or an information system without the owner's knowledge or consent.
- Malware is a comprehensive term that describes any malicious program or software (e.g., a virus is a "subset" of malware).
- Malware attacks are the most frequent security breaches.
- Computer systems infected by malware take orders from the criminals and do things such as send spam or steal the user's stored passwords. (key logger)

Viruses

- A virus is programmed software inserted by criminals into a computer to damage the system; running the infected host program activates the virus. A virus has two basic capabilities.
- First, it has a mechanism by which it spreads.
- Second, it can carry out damaging activities once it is activated.
- Sometimes a particular event triggers the virus's execution.
- The problem is that existing virus protection systems may not work against new viruses, and unfortunately, new viruses are created all the time.

Worms

Unlike a virus, a worm can replicate itself automatically (as a "stand-alone" without any host or human activation). Worms use networks to propagate and infect a computer or handheld device and can even spread via instant messages or e-mail. In addition, unlike viruses that generally are confined within a target computer, a worm can infect many devices in a network as well as degrade the network's performance.

Trojan horse

A Trojan horse is a program that seems to be harmless or even looks useful but contains a hidden malicious code. Users are tricked into executing an infected file, where it attacks the host, anywhere from inserting pop-up windows to damaging the host by deleting files, spreading malware, and so forth. e.g., Zeus, W32.

Heartbleed

- Heartbleed is a flaw in OpenSSL, the open-source encryption standard used by majority of websites that need to transmit the data that users want to keep secure. It basically gives you a secure line when you're sending an e- mail or chatting on IM."
- The potential damage may be large. In theory, any data kept in the active memory can be pulled out by the bug. Hackers can even steal encryption keys that enable them to read encrypted messages. About 650 million websites may be affected. The only advice provided by experts is to change the online passwords.

Crypto Locker

Discovered in September 2013, Crocker is a ransomware Trojan bug. This malware can come from many sources including e-mail attachments and can encrypt files on your computer, so that you cannot read these files. The malware owner then offers to decrypt the data in exchange for a Bitcoin or similar untraceable payment system.

- A **denial-of-service** (DoS) attack is "a malicious attempt to make a server or network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet."
- This causes the system to crash or become unable to respond in time, so the site is unavailable. One of the most popular types of DoS attacks occurs when a hacker "floods" the system by overloading the system with "useless traffic" so the user is prevented from accessing their e-mail, websites, etc.
- A DoS attack is a malicious attack caused by one computer and one Internet connection as opposed to a distributed denial-of-service (DDoS) attack, which involves many devices and multiple Internet

connections. For example, the attack on the Dyn(closing case) was done by thousands of computers taken hostage by the hackers.

Page hijacking or pagejacking:

Page hijacking or pagejacking is illegally copying website content so that a user can be misdirected to a different website. Social media accounts are sometimes hijacked for the purpose of stealing the accountholder's personal information. For example, Justin Bieber's 50 million followers fell victim to this method when Bieber's Twitter account was hijacked in March 2014.

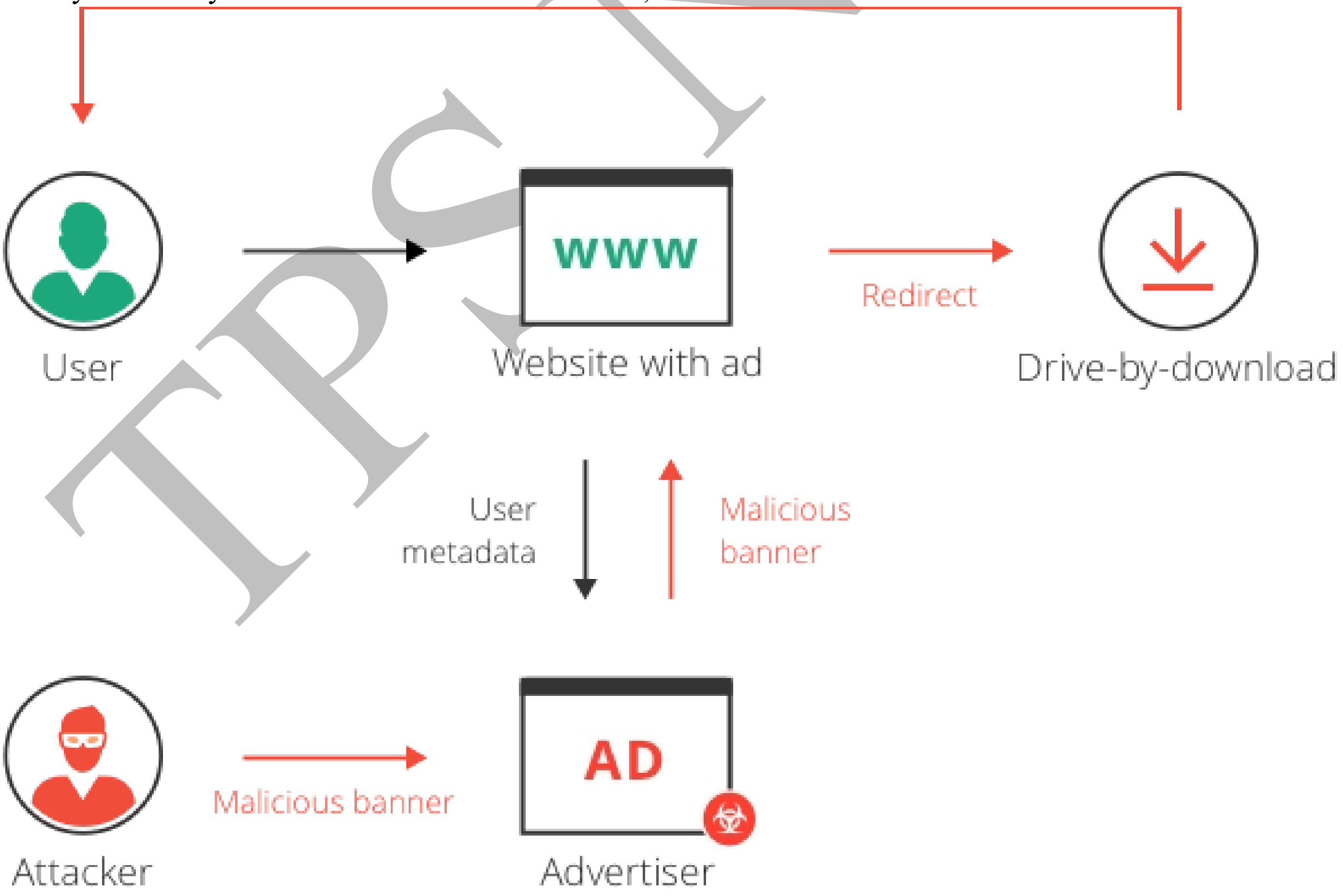
Botnets:

A botnet (short for "robot network") is a network of computers infected by malware that are under the control of a single attacking party, known as the "bot-herder." Each individual machine under the control of the bot-herder is known as a bot.

A **botnet** is malicious software that criminals distribute to infect many hijacked Internet-connected computers controlled by hackers. These infected computers then form a "botnet," causing the personal computer to "perform unauthorized attacks over the Internet" without the user's knowledge. Unauthorized tasks include sending spam and e- mail messages, attacking computers and servers, and committing other kinds of fraud, causing the user's computer to slow down. Each attacking computer is considered a computer robot.

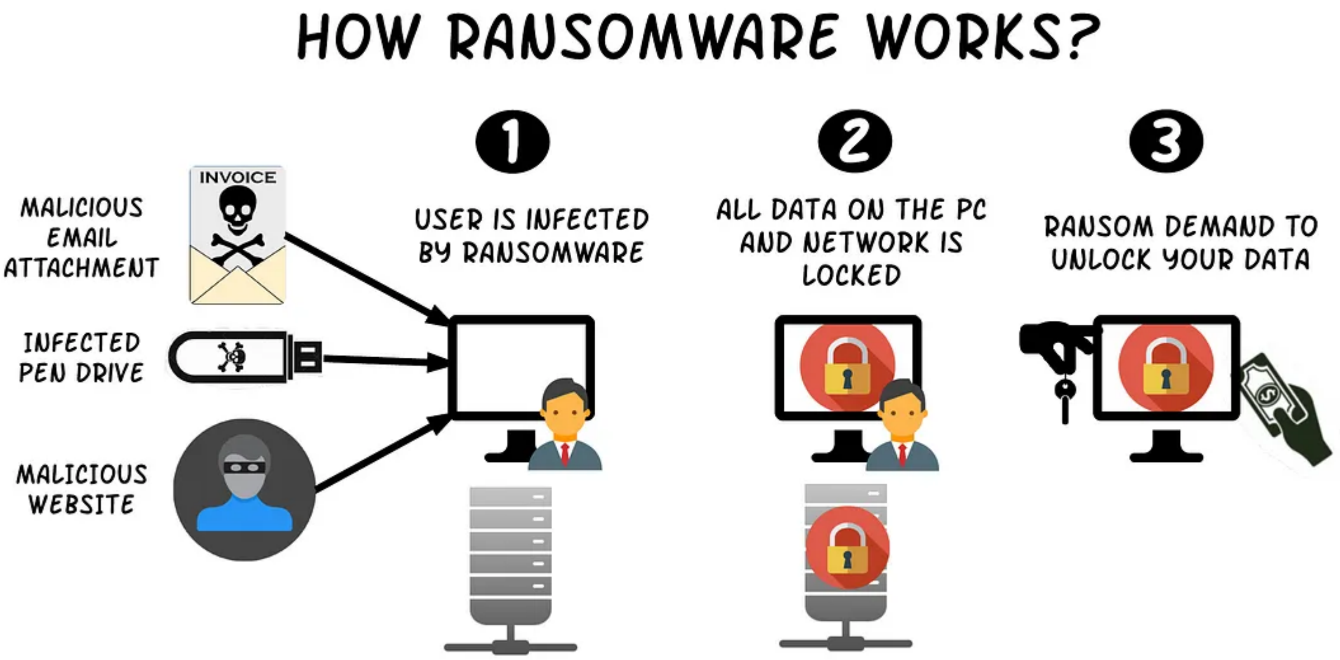
Malvertising:

Malvertising is a malicious attack that involves injecting harmful code into real online advertising networks. These misleading ads are then unknowingly displayed to users, leading them to unsafe destinations. Malvertising is a malicious form of Internet advertising used to spread malware. Malvertising is accomplished by hiding malicious code within relatively safe online advertisements. Note that hackers are targeting ads to hide malware at accelerating rates. For example, in 2013, Google disabled ads from over 400,000 sites that were hiding malware. A final word: If you get an e-mail that congratulates you on winning a large amount of money and asks you to "Please view the attachment," don't!



Ransomware:

Attacker converts and lock digital files by using malware and demands a restore before the system is unlocked it. A method of attack where the attacker encrypts files so the victim cannot open them unless they pay money.


HOW RANSOMWARE WORKS?
MALICIOUS EMAIL ATTACHMENT
INVOICE
INFECTED PEN DRIVE
MALICIOUS WEBSITE
1
USER IS INFECTED BY RANSOMWARE
2
ALL DATA ON THE PC AND NETWORK IS LOCKED
3
RANSOM DEMAND TO UNLOCK YOUR DATA

Sniffing:

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of tapping phone wires and getting to know about the conversation. It is also called wiretapping applied to the computer networks. A packet analyzer is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. Packet capture is the process of intercepting and logging traffic.

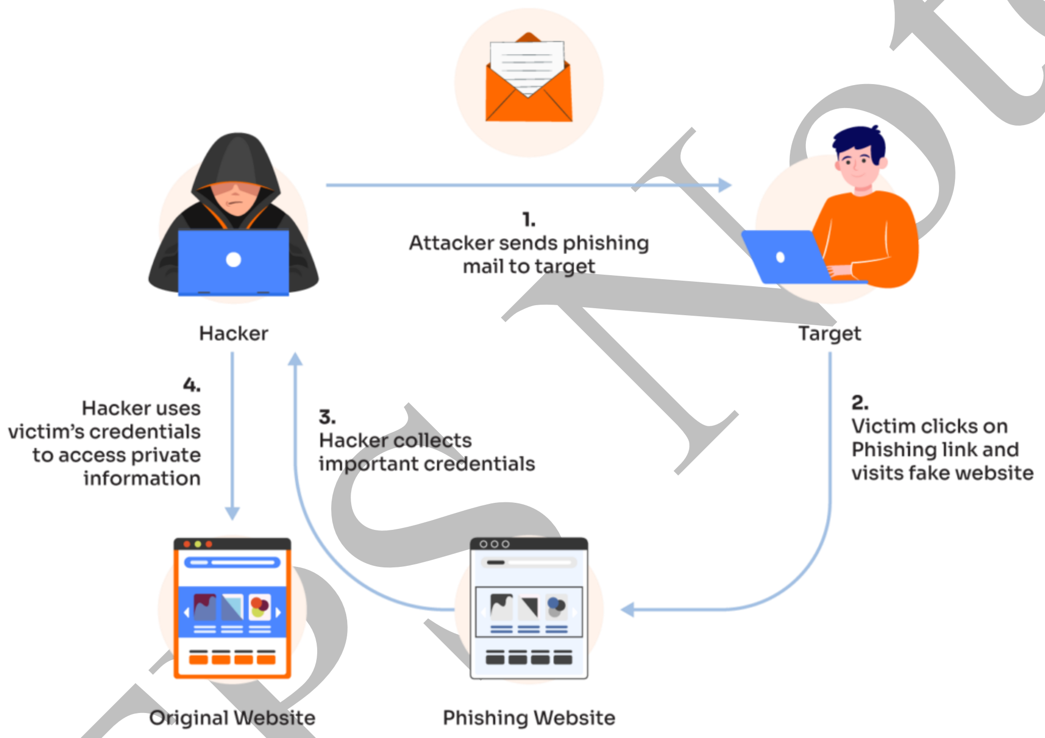
Non-Technical malware attack:

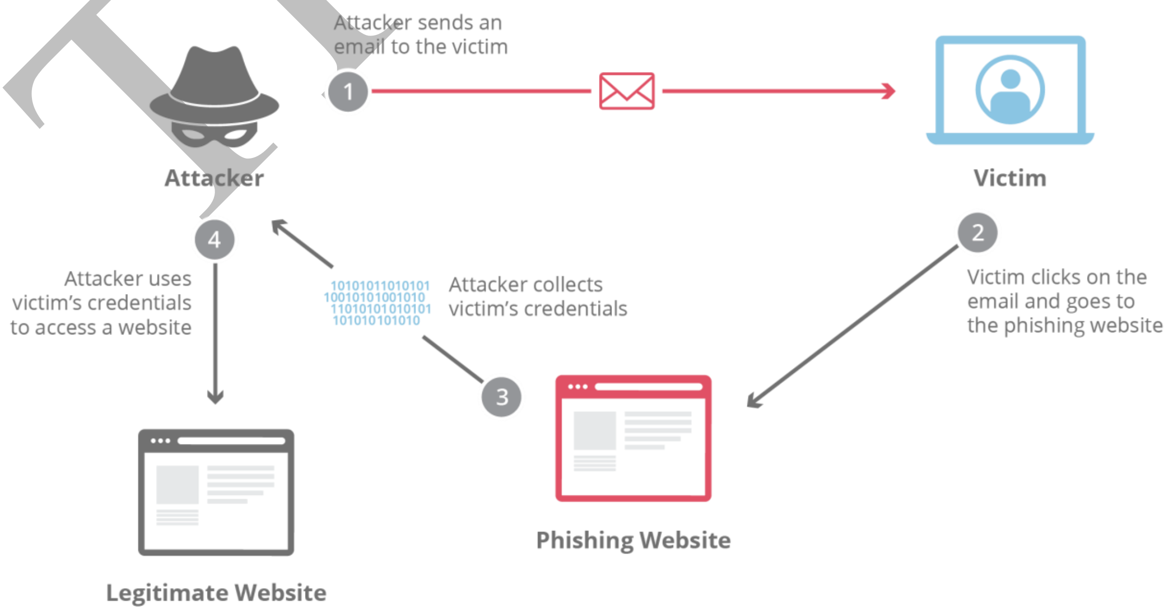
- Software and systems knowledge are used to perpetrate technical attacks. Insufficient use of antivirus and personal firewalls and unencrypted communication are the major reasons for technical vulnerabilities.
- Nontechnical organizational attacks are those where the security of a network or the computer is compromised (e.g., lack of proper security awareness training). We consider financial fraud, spam, social engineering, that includes phishing, and other fraud methods, as nontechnical.

- Many nontechnical methods also use some malware in their attacks. The goals of social engineering are to gain unauthorized access to systems or information by persuading unsuspected people to disclose personal information that is used by criminals to commit fraud and other crimes.

Social Engineering and Fraud

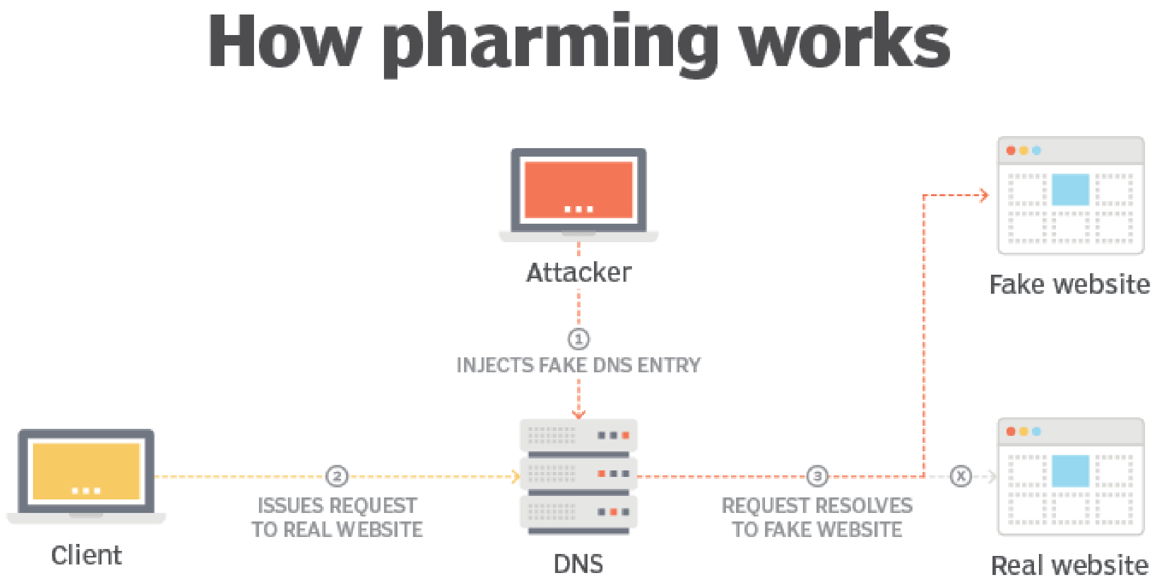
- **Social engineering** refers to a collection of methods where criminals use human psychology to persuade or manipulate people into revealing their confidential information, or their employment information, so they can collect information for illegal activities.
- The hacker may also attempt to get access to the user's computer in order to install malicious software that will give hackers control over the person's computer.
- **Social phishing** is a fraudulent process of acquiring confidential information, such as credit card or banking details, from unsuspecting computer users.
- A phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, well known, popular company, bank, school, or public institution.
- The user is instructed to enter a corrupt website, where he or she may be tricked into submitting confidential information (e.g., being asked to "update" information). Sometimes phishers install malware to facilitate the extraction of information.

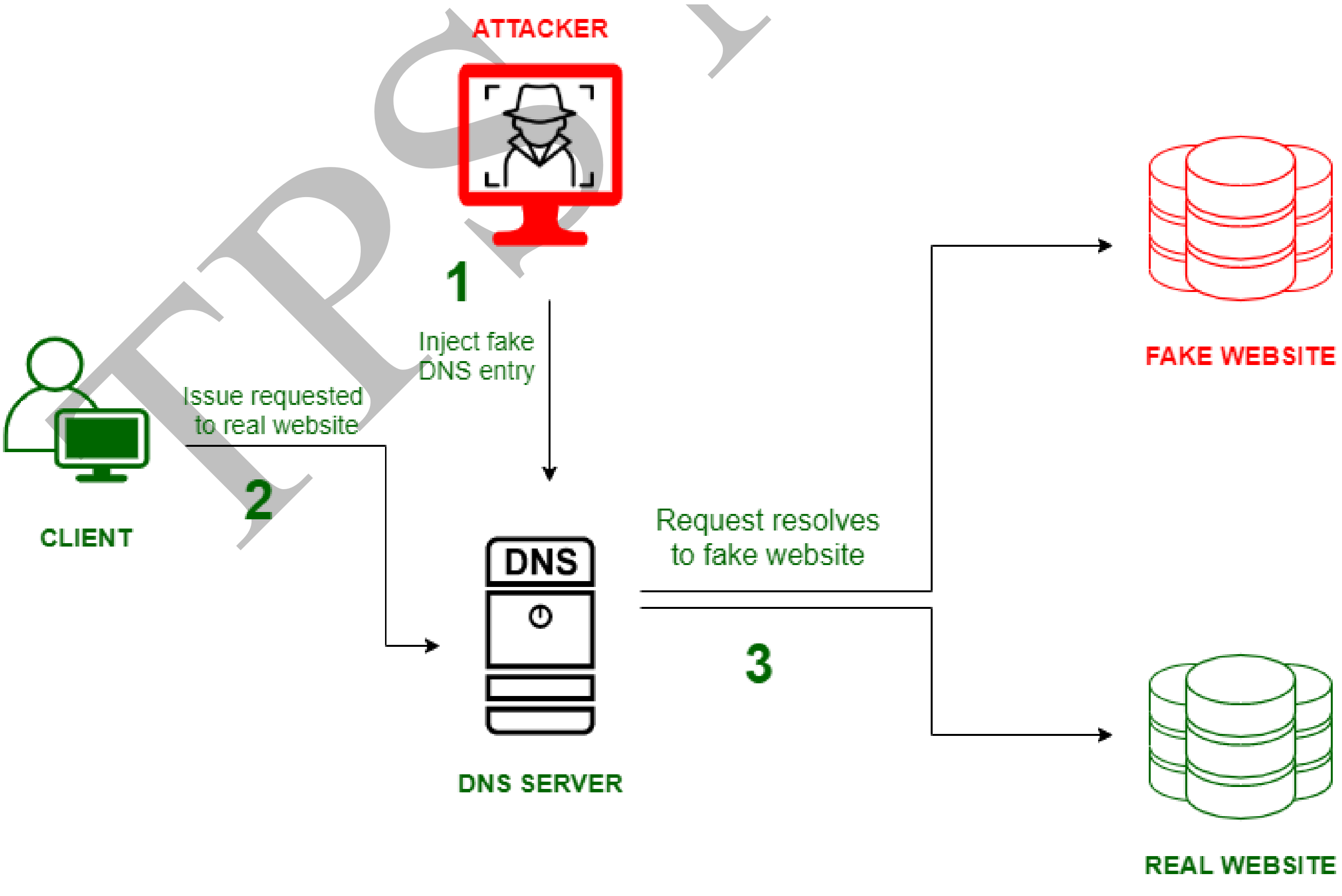

1.
Attacker sends phishing mail to target
Hacker
Target
4.
Hacker uses victim's credentials to access private information
3.
Hacker collects important credentials
2.
Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website


Attacker sends an email to the victim
1
Attacker
Victim
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
10101011010101
10010101001010
11010101010101
101010101010
2
Victim clicks on the email and goes to the phishing website
3
Phishing Website
Legitimate Website

Pharming:

- ➢ Like phishing, pharming is a scam where malicious code installed on a computer is used to redirect victims to bogus (fake) websites without the victims' knowledge or consent.
- ➢ Pharming can be more dangerous than phishing since users have no idea that they have been redirected to a fake website.
- ➢ Identity theft is a crime. It refers to wrongfully obtaining and using the identity of another person in some way to commit crimes that involve fraud or deception (e.g., for economic gain). Victims can suffer serious damages.


How pharming works
Attacker
① INJECTS FAKE DNS ENTRY
Fake website
Client
② ISSUES REQUEST TO REAL WEBSITE
DNS
③ REQUEST RESOLVES TO FAKE WEBSITE
Real website


ATTACKER
1
Inject fake DNS entry
CLIENT
Issue requested to real website
2
DNS
DNS SERVER
Request resolves to fake website
3
FAKE WEBSITE
REAL WEBSITE