Web Mastering Code:66667

JOHIR AHEMMOD CHOWDURI

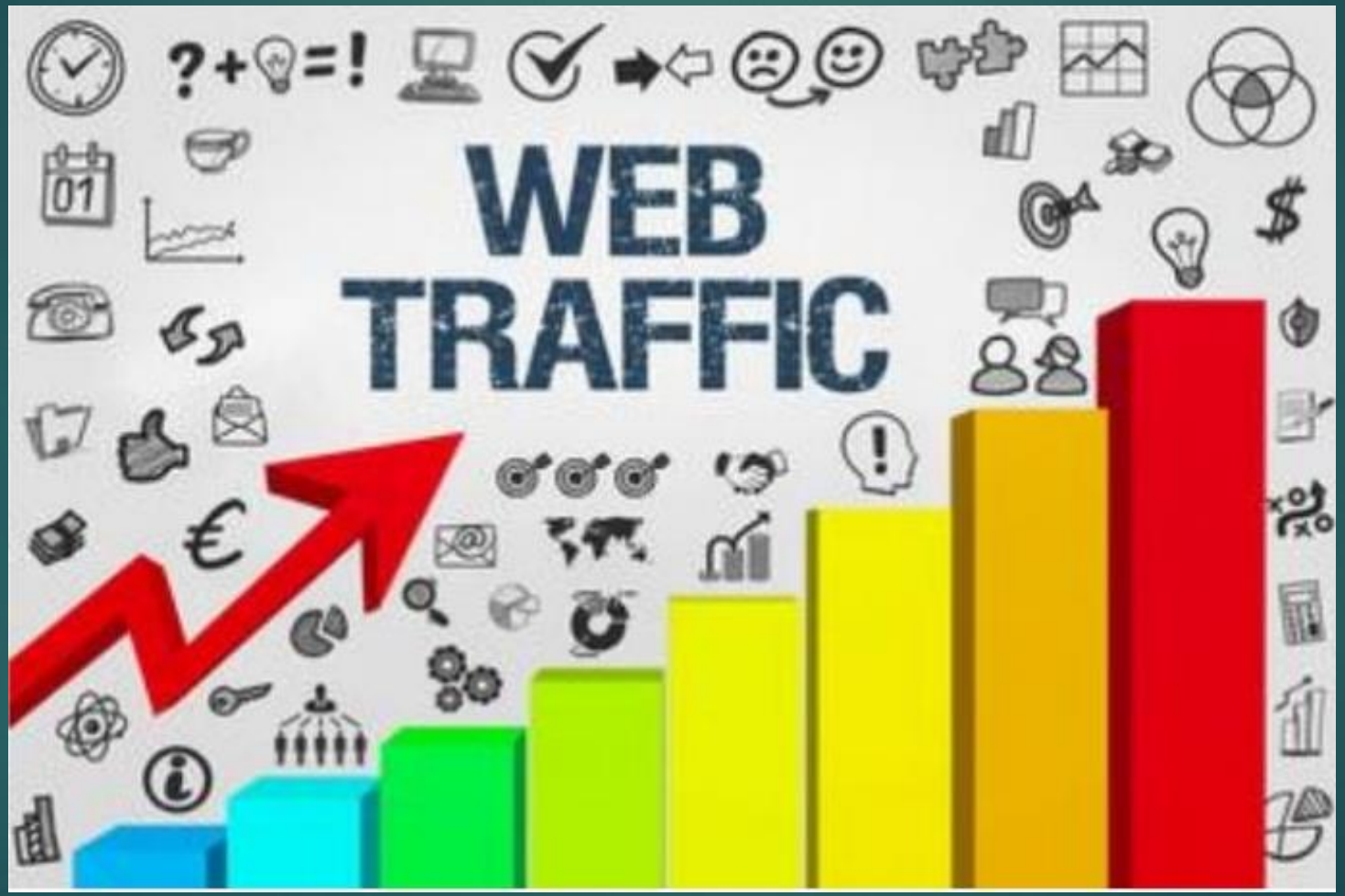
INSTRUCTOR

COMPUTER DEPARTMENT

অধ্যায় - ১১

ওয়েব নিরাপত্তা অনুধাবন

ওয়েব নিরাপত্তা অনুধাবন



আলোচ্য বিষয়ঃ

- ওয়েব নিরাপত্তা অনুধাবন
  - সাইট ট্রাফিক কি
  - ওয়েব ট্রাফিকের গুরুত্ব
  - পোর্ট ফরওয়ার্ডিং এর বর্ণনা
  - বিভিন্ন প্রকার সাইবার আক্রমণের বর্ণনা
  - ফায়ারওয়ালের কাজের বর্ণনা

Website Traffic

- Organic search traffic (SEO) – All visitors who find a website after using a search Engine like Google or Bing.
- Paid traffic – All visitors who go to a website after clicking on any form of paid promotion.
- Referral traffic – All visitors who come to a website after clicking a link on another website (with the exception of search engines and paid promotions) are labelled as referral traffic.
- Direct traffic – All visitors who can't be assigned to one of the previous sources are automatically assigned to "Direct traffic

Importance of site traffice

- The larger the **number** of visitors to your website the better!
- But you need to focus on increasing the **quality of your website traffic**, as not all traffic is good traffic. And in fact, bad traffic can bog your business down at some level.
- When you can increase your traffic along with the quality of the visitors, the better you will be able to **increase your website conversion** and get that traffic to become paying customers!

Port forwarding

- In computer networking, **port forwarding** or **port mapping** is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host

Cyber attack

- 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.
- A **cyberattack** is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent. Depending on context, cyberattacks can be part of cyberwarfare or cyberterrorism.
- A cyberattack can be employed by sovereign states, individuals, groups, society or organizations, and it may originate from an anonymous source.

Different type of cyber attack

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

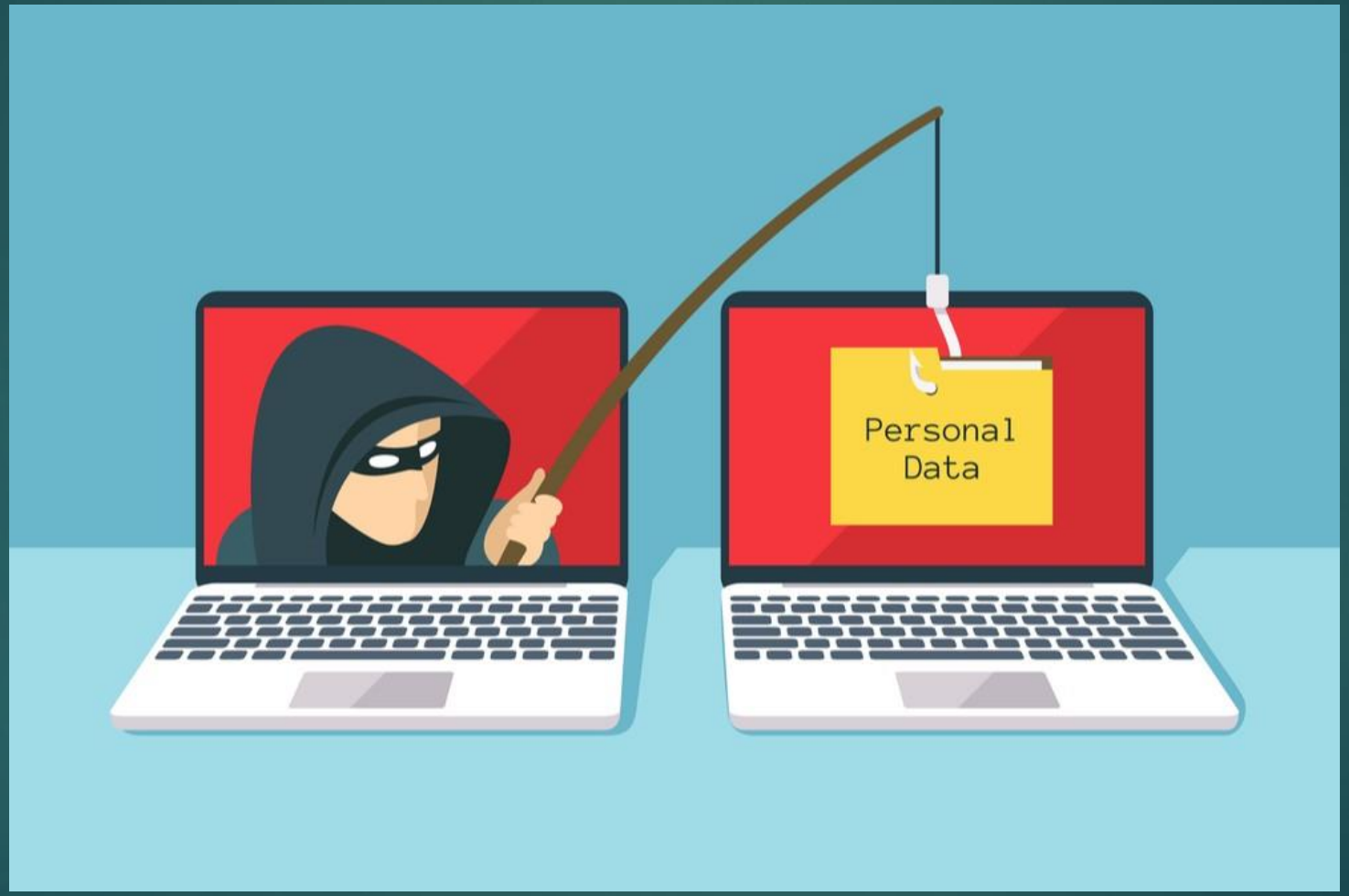
Distributed denial-of-service (DDoS) attacks

- A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up with highway, preventing regular traffic from arriving at its desired destination.

Phishing Attack

- Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.
- Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.
- Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators.

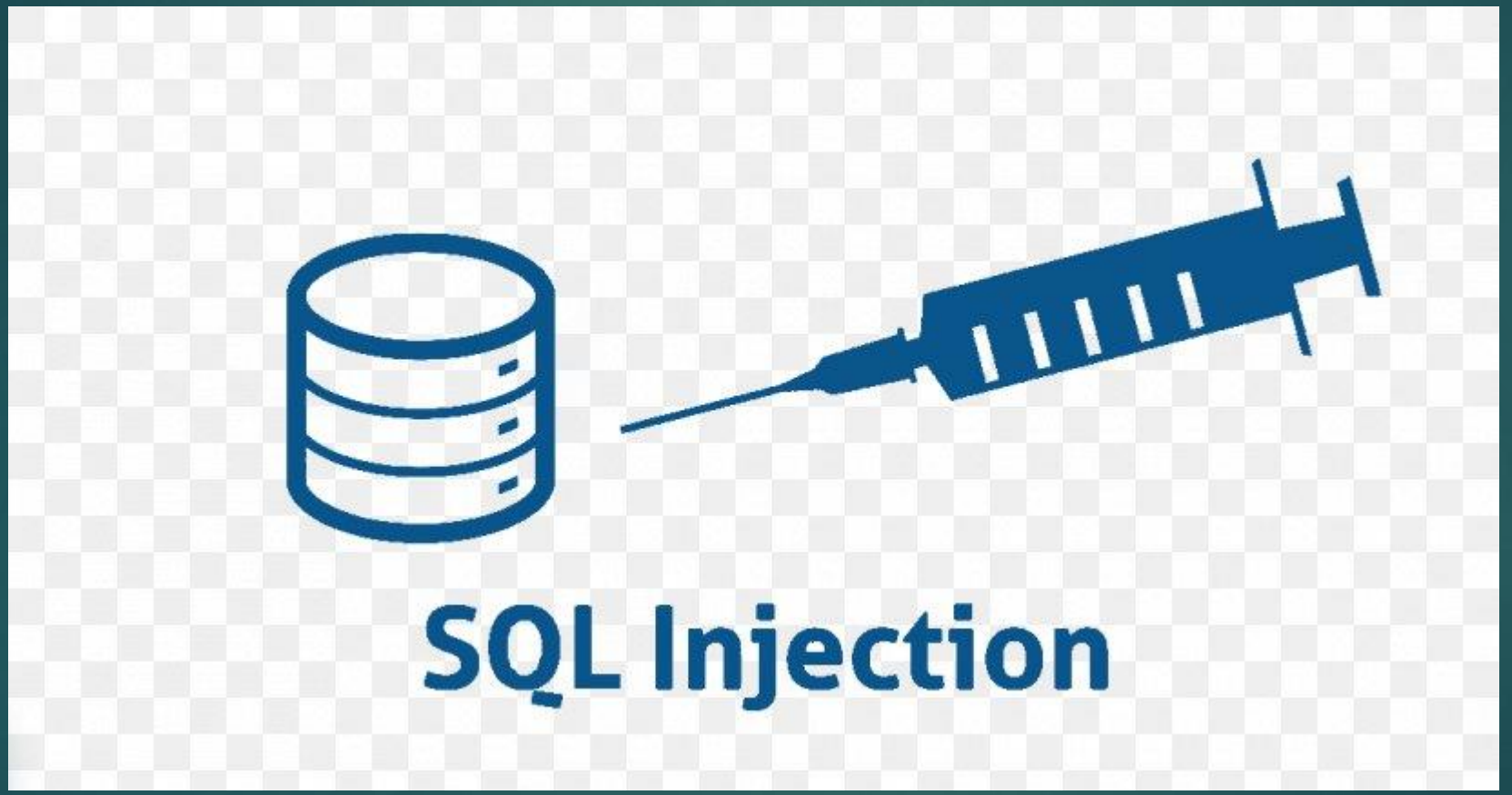
Phishing Attack



SQL injection attack

- SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for example, instead of the login or password) in order to run predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system.

SQL injection attack



Malware attack

- **Malware** (a portmanteau for **malicious software**) is any software intentionally designed to cause damage to a computer, server, client, or computer network(by contrast, software that causes *unintentional* harm due to some deficiency is typically described as a software bug).
- A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware.

Malware attack

কোন প্রশ্ন?

আগামী ক্লাসের আমরা যে বিষয়গুলো জানবো

- মার্কেটিং ও এসইও(সার্চ ইঞ্জিন অপটিমাইজেশন)
  - সার্চ ইঞ্জিন ও অন্যান্য ওয়েবসাইট ব্যবহার করে ওয়েবসাইটের মার্কেটিয়করণ
  - ওয়েবসাইটে এসইও কি
  - এসইও বন্ধুত্বসম্পন্ন ওয়েবসাইট
  - ওয়েবসাইটে এসইও ব্যবহারের পদ্ধতি

ধন্যবাদ সবাইকে