Digital Marketing (Module 1 Assignment)

Que. 1) Please break down the URLs listed below. (list-out Protocol, Domain, TLD)

- **. https://www.flipkart.com/**
- **https://www.irctc.co.in/**
- **https://www.allegro.pl/**
- **https://www.johnlewispartnership.co.uk/**
- **https://www.uidai.gov.in/**

Answer:-

Here are the breakdowns of the provided URLs:

URL: https://www.flipkart.com/

Protocol: https

Domain: flipkart

TLD (Top-Level Domain): com

URL: https://www.irctc.co.in/

Protocol: https

Domain: irctc

TLD (Top-Level Domain): co.in

URL: https://www.allegro.pl/

Protocol: https

Domain: allegro

TLD (Top-Level Domain): pl

URL: https://www.johnlewispartnership.co.uk/

Protocol: https

Domain: johnlewispartnership

TLD (Top-Level Domain): co.uk

URL: https://www.uidai.gov.in/

Protocol: https

Domain: uidai

TLD (Top-Level Domain): gov.in

Que.2) What is HTTPS/SSL update?

Answer:-

HTTPS (Hypertext Transfer Protocol Secure) and SSL (Secure Sockets Layer)

updates refer to improvements and changes in the protocols and technologies

that secure communications over the internet. Here’s a breakdown of these

terms and their updates:

HTTPS: This is an extension of HTTP (Hypertext Transfer Protocol) used for

secure communication over a computer network. HTTPS ensures data integrity

and privacy by encrypting the data exchanged between a user’s browser and

the web server. It uses SSL/TLS protocols to encrypt the communication.

SSL/TLS: SSL (Secure Sockets Layer) and its successor TLS (Transport Layer

Security) are cryptographic protocols designed to provide secure communication over a computer network. SSL is now considered deprecated,

and TLS is the modern standard.

Key Aspects of HTTPS/SSL Updates:

Protocol Upgrades:

TLS 1.3: Released in 2018, TLS 1.3 is the latest version of the TLS protocol. It

offers improved security and performance compared to its predecessors (TLS

1.0, 1.1, 1.2). Notable improvements include the elimination of outdated

cryptographic algorithms and a simplified handshake process, reducing

latency.

Deprecation of Older Protocols: As part of improving security, older protocols

such as SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 are being phased out in favor of

newer, more secure versions like TLS 1.2 and TLS 1.3.

Certificate Enhancements:

Shorter Certificate Lifespans: Certificate authorities (CAs) now issue SSL/TLS

certificates with shorter lifespans (typically one year) to enhance security and

reduce the impact of compromised certificates.

Stricter Validation Processes: CAs have implemented stricter validation processes for issuing certificates to ensure the authenticity of websites and

prevent fraudulent certificates.

Security Practices:

HSTS (HTTP Strict Transport Security): This is a web security policy mechanism

that helps to protect websites against man-in-the-middle attacks by ensuring

browsers only interact with the website using HTTPS.

Certificate Transparency: A security measure that involves maintaining a public

log of all certificates issued by CAs, making it easier to detect and respond to

fraudulent certificates.

Improved Browser Support:

Modern web browsers are updated to support the latest TLS versions and

enforce stricter security measures, such as warning users when they

encounter websites using outdated or insecure protocols.

Encryption Standards:

Elliptic Curve Cryptography (ECC): Adoption of more secure and efficient

cryptographic algorithms, such as ECC, which offers higher security with

shorter key lengths compared to traditional RSA encryption.

These updates collectively enhance the security, performance, and reliability

of HTTPS communications, making the internet safer for users and businesses.

Que. 3) List out 10 famous browsers used worldwide.

Answer :-

Here are ten famous browsers used worldwide:

➢ Google Chrome

➢ Mozilla Firefox

➢ Microsoft Edge

➢ Apple Safari

➢ Opera

➢ Brave

➢ Vivaldi

➢ Samsung Internet

➢ UC Browser

➢ Tor Browser