Practical 8: **Identify Phishing Attack**

Aim:

To identify phishing attempts through digital messages.

Objectives:

- To detect cybercrime
- To recognize scam elements

Materials Required:

- Provided phishing example

Procedure:

Read message text

Carefully go through the entire message to understand its content and intent.
Make note of any unusual requests or unfamiliar senders.

Identify suspicious elements

Look for spelling errors, urgent demands, unknown links, or too-good-to-be-true offers.
These signs often indicate potential scams or malicious intent.

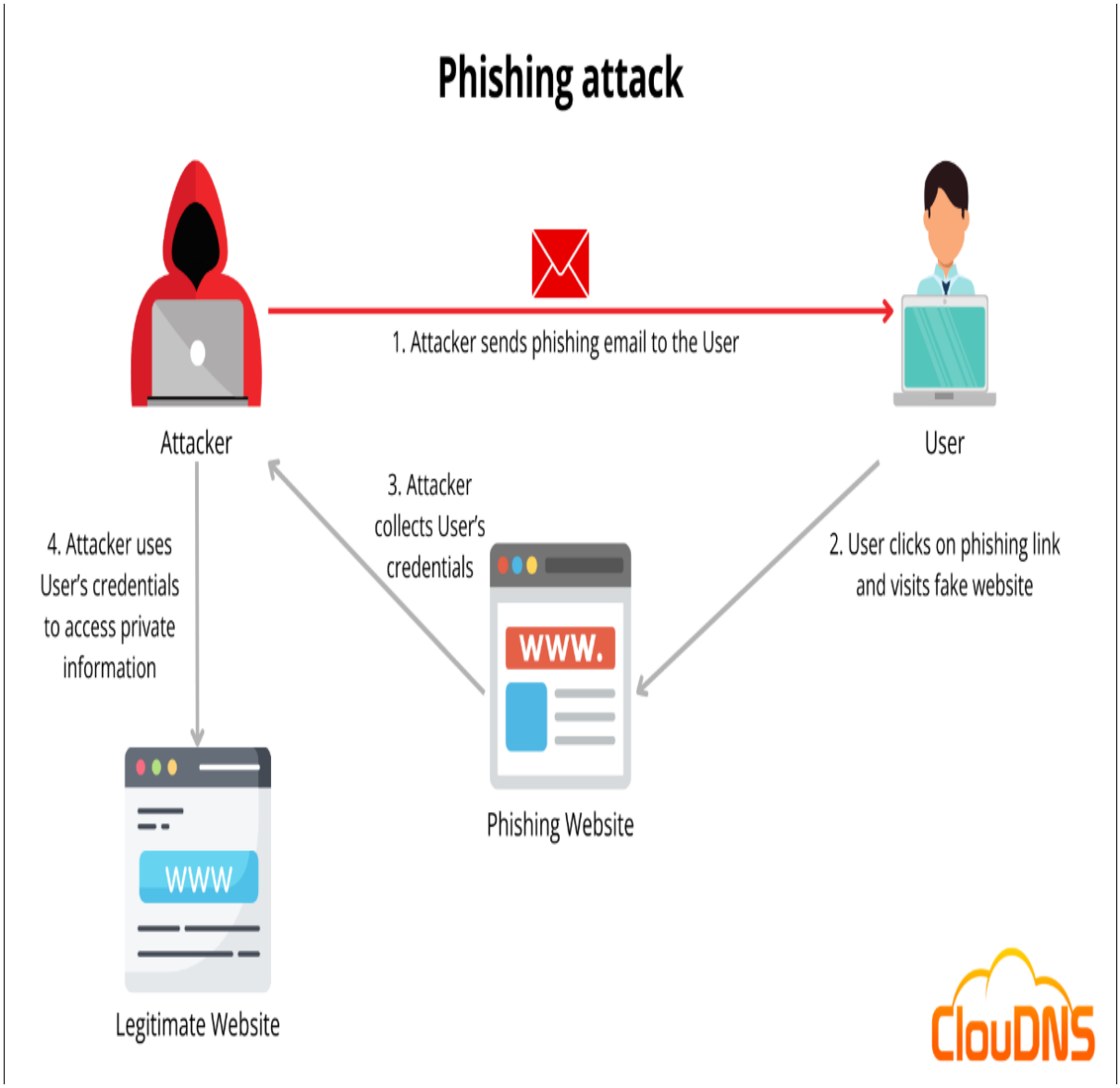
List cybercrime type

Based on the suspicious elements, categorize the message as phishing, fraud, malware attempt, etc.
This helps in understanding the nature and threat level of the cybercrime.

Write verification steps

Suggest ways to confirm authenticity, such as checking the sender's email, contacting the official source, or scanning links.
These steps help prevent falling victim to cyberattacks.

Output:-


Phishing attack
1. Attacker sends phishing email to the User
Attacker
User
3. Attacker collects User's credentials
4. Attacker uses User's credentials to access private information
2. User clicks on phishing link and visits fake website
WWW.
WWW
Phishing Website
Legitimate Website
ClouDNS