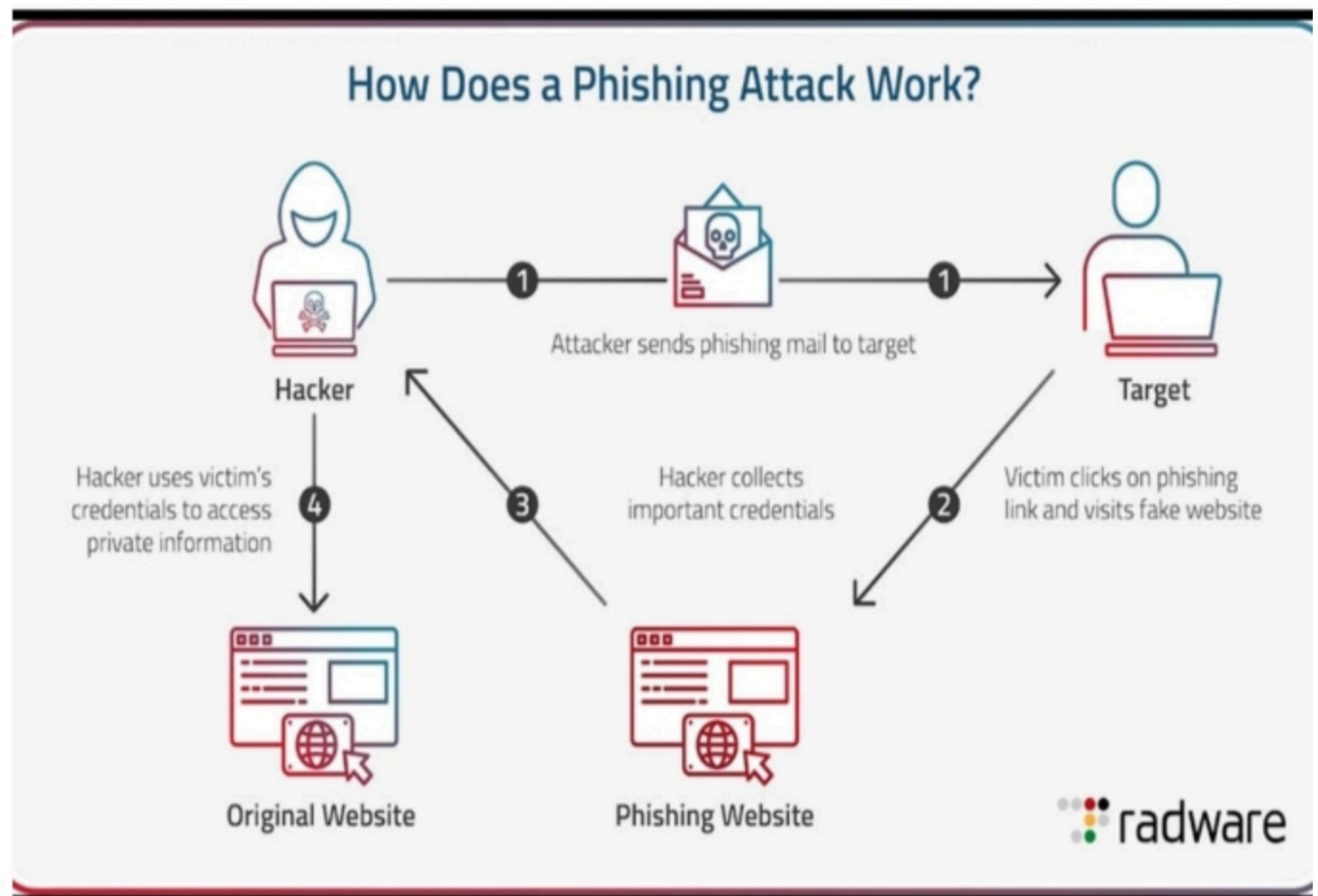


3. the offer came through unknown / unofficial source (because they haven't mentioned Email or contact no.)



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.

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.

Identify one real phishing email : A final-year student, Aman, receives a LinkedIn message saying "You are shortlisted for a Remote Software Developer role at Google.

Salary: ₹18 LPA.

Pay ₹2,499 as verification fee.

Limited seats. Pay now to confirm."

ANSWER THE QUESTIONS :-

a) What type of cybercrime is happening here?

ANS- Job scam .

b) List 3 red flags that show it is a scam?

ANS- 1. Asking for verification fee .

2. Saying for limited seats .