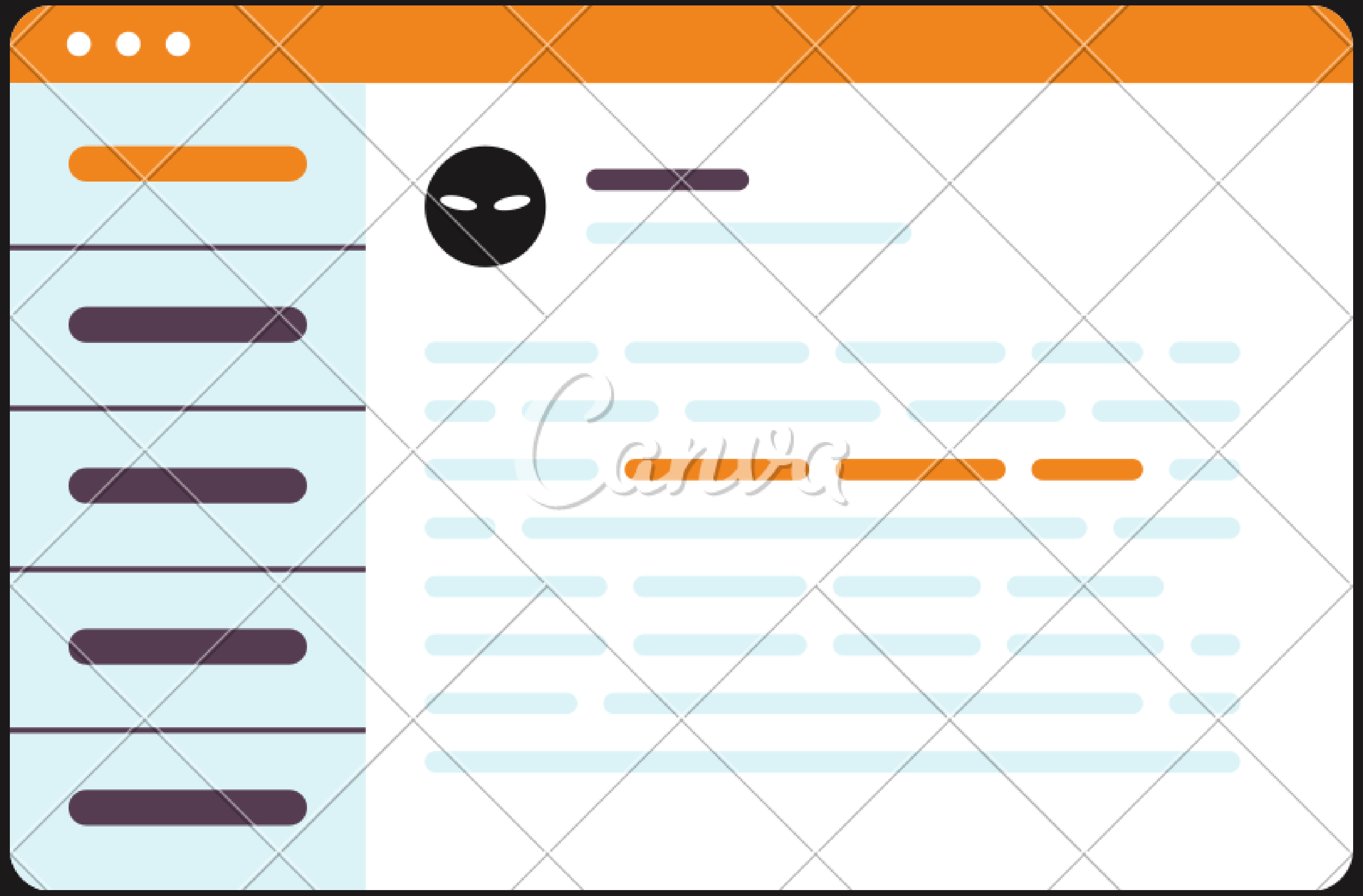
PHISHING

Think Before You Click!

INTRODUCTION

Welcome! This training will equip you with the knowledge and skills to identify and avoid phishing attempts. Phishing is a cybercrime where attackers try to trick you into revealing sensitive information, like passwords or credit card details, by disguising themselves as a trusted source. By understanding phishing tactics, we can all work together to protect our company data and personal information.



COMMON TECHNIQUES

01 URGENCY AND SCARCITY

- Phishing emails often create a sense of urgency or pressure to act quickly, such as by claiming your account will be suspended if you don't click a link.

02 GENERIC GREETINGS

- Phishing emails often lack personalization and use generic greetings like “Dear Customer” instead of your name.

03 SUSPICIOUS LINKS AND ATTACHMENTS

- Don’t Click on links or open attachments from unknowns senders. Hover over the link to see the actual URL before clicking.

04 THREATS

- Phishing emails may threaten negative consquences if you don’t comply with their demands.

05 GRAMMAR AND SPELLING ERRORS

- Phishing emails may contain typos or grammatical mistakes.

HOW TO SPOT A PHISHING ATTACK

1

Be cautious of unsolicited emails, call or texts, even if they appear to be from a fimiliar source.

2

Verify the sende’s address. Don’t rely solely on the display name.

3

Do not click on suspicious links or open unknown attachments.

4

Be wary of emails requesting urgent action or personal infromation.

5

Check for grammatical errors or inconsistencies in the message.

DO IF SUSPECT A PHISHING ATTACK

1

Do not respond to the message.

2

Do not click on any links or open attachments.

3

Report the phishing attempt to your IT department.

4

Forward the Suspicious email to IT Department as an attachment.(do not forward directly).