PHISHING QUICK REFERENCE GUIDE

WHAT IS PHISHING?

Phishing is a cyber attack where attackers impersonate legitimate organizations or individuals through email, text messages, or phone calls to deceive individuals into providing sensitive information such as usernames, passwords, or financial details.

IF YOU HAVE CLICKED A PHISHING LINK:

Immediately disconnect from the internet.

Contact the IT or Security Department for assistance.

Monitor your accounts for any unauthorized activity.

COMMOM INDICATORS OF PHISHING ATTEMPTS

- Urgent or Threatening Language: Messages that create a sense of urgency or fear, pressuring you to act immediately.
- Unfamiliar Sender Addresses: Emails from unknown senders or addresses that closely resemble legitimate ones but with slight misspellings.
- Requests for Sensitive Information: Any unsolicited request for personal or financial information.
- Generic Greetings: Use of non-personalized greetings like "Dear Customer" instead of your name.
- Unexpected Attachments or Links: Emails containing attachments or links that you were not expecting or contain grammatical errors.

PREVENTIVE MEASURES

- VERIFY SENDER'S IDENTITY: ALWAYS CHECK THE SENDER'S EMAIL ADDRESS CAREFULLY.
- HOVER OVER LINKS: BEFORE CLICKING, HOVER OVER LINKS TO SEE THE ACTUAL URL.
- AVOID UNTRUSTED ATTACHMENTS: DO NOT OPEN ATTACHMENTS FROM UNKNOWN OR UNTRUSTED SOURCES.
- ENABLE MULTI-FACTOR AUTHENTICATION (MFA): ADDS AN EXTRA LAYER OF SECURITY TO YOUR ACCOUNTS.
- REGULARLY UPDATE PASSWORDS: USE STRONG, UNIQUE PASSWORDS AND CHANGE THEM PERIODICALLY.

Open Pharma

IF YOU SUSPECT PHISHING

- Do not click on any links or download attachments
- Report the email immediately to the IT or Security Department by forwarding it to security-team@openpharma.com.