PHISHING:
WHAT YOU NEED TO KNOW

Scammers are after your money and everyone is a target.

A phishing scam often comes from a threat actor disguised as a reputable individual or organization who sends fraudulent emails. Their goal is to obtain sensitive data or infect a victim's system with destructive malware.

1 OUT OF 10 PEOPLE FALL VICTIM TO A PHISHING EMAIL

WHAT TO LOOK FOR

Step 1: Scammer spoofs or compromises an email account

Step 2: Scammer sends fraudulent emails from spoofed account

Step 3: Recipient shares sensitive information or installs malware on system

STAY ON GUARD FOR:

- Spelling & Grammar Errors
- Incorrect Sender Address
- Offers That are Too Good to Be True
- Request for Immediate Action

SLAM the Scams

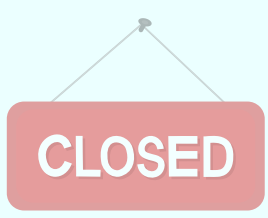
- S- veirfy the **SENDER**
- L- check for broken **LINKS**
- A- never open unsolicited **ATTACHMENTS**
- M- read the **MESSAGE** to look for spelling or other errors

Why are phishing emails bad?

Productivity Decreases

Personal Information Stolen

Money Loss



Business Shut Down

FIGHT THE PHISH

Catching a phishing email is critical to your business's security.
If you see 'something phishy', report it!
Beware of unsolicited messages - and always report a suspicious to email to your IT team!