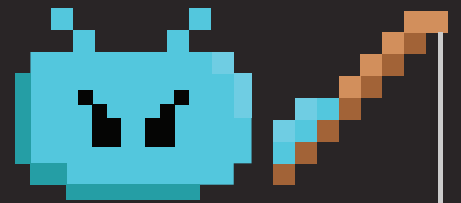# PHISHING: INBOX INVADERS

Learn how to spot phishing emails …
and defeat these inbox invaders.

WHAT IS PHISHING?

A phish is a deceptive email or message that looks legitimate and encourages you to take actions that could compromise your computer or network, or reveal sensitive information.

Scammers use phishing attacks to steal valuable information and gain illegal access to systems.

LIKELY LURES, BELIEVABLE BAIT!

Phishing emails (called "lures") try to manipulate people by stirring strong emotions:
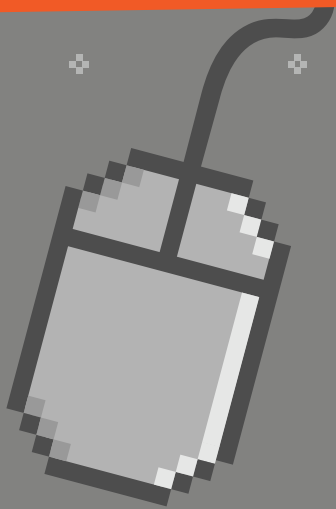
- Fear   - Curiosity   - Empathy   - Greed
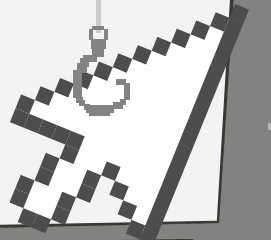
IT'S NO GAME!

A single employee falling for a phish has been known to trigger serious data breaches that expose everything from business secrets to the confidential data of millions of people.

In your personal life, phishing can lead to identify theft, stolen data, and other long-term consequences.

ANYONE CAN BE A VICTIM!

EXECUTIVES · SYSTEMS ADMINISTRATORS · CUSTOMER SERVICE REPRESENTATIVES · HUMAN RESOURCES STAFF · INTERNS · ACCOUNTING STAFF … EVEN YOU!

LET'S ALL LEVEL UP!

HOW YOU CAN HELP DEFEAT PHISHING:

- Don't blindly trust anything that comes into your inbox. Always verify an email's authenticity before you click any links or open attachments.
- Be suspicious of messages that are vague, generic, or impersonal, or that stir strong emotions, such as fear, empathy, urgency, or anger.
- Never trust an email that asks for personal or sensitive information, such as your username or password.
- Check the "From:" field closely but be aware that this information can be spoofed.
- Phishing websites may look legitimate by imitating company logos and using domain names that might be close misspellings or lookalikes.

SOMETHING'S NOT QUITE RIGHT?

If you suspect you've received a phish—even if you're not quite sure—report it to your IT security group right away!