



# Security Awareness Training: Phishing

By: Lauren Anderson



# What is Phishing?

**According to Google, phishing is an attempt to steal personal information or break into online accounts using deceptive emails, messages, ads, or sites that look similar to sites you already use.**

# An Example of Phishing

**Attention! Your PayPal account will close soon!**

Dear Member,

We have faced some problems with your account Please update the account .If you do not update will be Closed.

To Update your account, just confirm your informations.(It only takes a minute.)

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

**Relog in your account now**

# Ways to Recognize Phishing

- 1. Being asked for your personal or financial information**
- 2. Being asked to click links or download software**
- 3. An email that appears to be from a reputable organization, social media site, coworker or a family member**

# How to Avoid Phishing Messages

- 1. Never click a link in a suspicious email.**
- 2. Check for incorrect grammar and spelling in email address and in the content of email.**
- 3. Never respond to requests for personal information.**

# What to Do When You Suspect Phishing

**Contact the Information Technology HelpDesk at your organization**