# Phishing: Conversation Guide

Phishing: A crime in which a target or organization is contacted by email, phone, or text in order to steal sensitive information.

**What: Phishing emails are being clicked at WSECU. We want your feedback and support to identify why.**

**Why: Phishing attacks are common and increasing.**

In 2019, a DBIR study found that 22% of investigated security breaches in the United States involve phishing attacks. Further, the study found that 74% of organizations in the United States experienced a successful phishing attack (2020, DBIR). Early reports from 2020 and 2021 show that the rate of attempts are likely to increase by nearly 9% quarter over quarter.

**Instructions:**

To complete this activity, meet with your employee and follow the below steps. This activity will unlock a conversation and provide us with feedback as to why employees are unable to recognize phishing attempts. Don't forget to submit your answers, this is how you will receive credit for completion.

## Step 1

With your employee, review the types of phishing emails on the back side of this form.

Share the phishing email your employee clicked.

## Step 2

Engage in a conversation, answering the following (Asked to the employee. Be sure to take notes):

- Why do you think phishing emails at WSECU are being clicked?
- What will you do differently to prevent clicking on future phishing emails?
- What additional support do you need to prevent clicking on phishing emails in the future?

## Step 3

Email the employee's responses to jhamm@wsecu.org, within 1 business day of having the conversation.

# 10 Common Traits of Phishing Emails

Phishing: A crime in which a target or organization are contacted by email, phone, or text in order to steal sensitive information.

## 1 Poor Spelling and Grammar

Phishing emails often include poor spelling or grammar. If there is an added period in Goog.le, beware!

## 2 You did not Initiate the Action

Receive an Amazon order that you did not place? Don't click it, it's a phish!

## 3 Generic Greetings

"Hello Sir/Madam" may be cause for alarm, and is one of the top ten common traits of a phishing email.

## 4 You're Asked to Send Money

Asking for money over text, email or social media is a prime example of phishing and cyber fraud.

## 5 Asking for Personal Information

NEVER give out your personal information online to an unverified source.

## 6 Too Good to be True

Phishing emails often include poor spelling or grammar. Notice the name of the company, it is not "Bank of American**s**," it's Bank of America.

## 7 Suspicious Attachments

See an attachment you don't recognize? Don't click! The attachment might be an attack.

## 8 From a Government Agency

Receive an IRS or FBI email? Watch out! This may be a fear-tactic to get you to click on a phishing attack.

## 9 Unrealistic Threats

Threats of jail time, wage garnishments, or worse, can be another fear-tactic to get you to click on an attack.

## 10 Inconsistencies in Links

Be sure to **hover** over each link to check it for accuracy. For example: www.Google.com should read www.google.com when you hover over it.