# FAMILIARIZE YOURSELF WITH PHISHING ATTACKS

After we conducted our email phising campaign in various department to know the team that are likely to fall for a phising email scam, we indentified HR TEAM as the most vulnerable team to malicious attack. Recording the highest email click-through rate among other staff members. Below are the interpretation of our results.

Email open rate: 100%
Email click-through rate: 85%
Phishing success rate: 75%

**BABATUNDE QODRI**
**INFORMATION SECURITY ANALYST**

# WHAT IS PHISHING?

Phishing is an act of sending fradulent  information via text or email which appear to emanate from reliable source. the intent of the malicious actor is to gain access to your sensitive data, login details and steal money from your bank. The nefarious actor can also embed malware on user's device.

# TYPES OF PHISHING ATTACKS

Malicious actor deploys different tactics to deceive users to gain access to sensitive data and phishing attack can sometimes appears in different form, Here are the few types of phishing attack you should be aware of:

- EMAIL PHISHING
- SPEAR PHISHING
- LINK MANIPULATION
- WHALING (CEO FRAUD)
- MALWARE
- VISHING


## LEARN HOW TO SPOT PHISHING EMAILS

There are several ways to spot phishing emails to avoid getting hacked by malicious actor, although emails phishing has become the most commonly used route for malicious actor according to the recent research, if you are spot any suspicious message in your inbox, this is what you should consider first.  Before we delve in, Let create a scenario on how malicious actor operate....

## PHISHING SCAM SCENARIO

In the early cold morning, you received a cold email from the company you are currently working at, in the message, you are beautifully praised for the dedication and hardwork that you've displayed in the time of working because it is just a few week to start the new year, the sweet message come with a phishing link to register your personal details to claim the new compensation offers and an additonal pay of $50,000 for your digilence at work. Infoming you that they need you to register before 24hours. without hesitant, you rush to fill the form without verifying the veracity of the message. The next thing you hear is your acccount has been debited!!! This is a true picture of how phishing email are, and understanding how to recognize and  prevent being phished go a long way in protecting your valuable data.

## HOW DO WE STOP GETTING PHISHED?

There are several ways to recognized and prevent getting phished agaist cybercriminals. These are some few ways and best practice to protect yourself are:

## HELPFUL TIPS TO STAY VIGILANT ABOUT PHISHING

1. Use security software to protect your data
2. Activate multi-factor authentication on your device
3. Back up your data regularly
4. Avoid public Wi-fi
5. Use strong or longer password