

# Mastercard Cybersecurity Job Simulation

## Task 1: Phishing Simulation Campaign

**Project Lead:** Temple Nnanna Idam-Nkama

**Date:** January 2025

### Task Overview

As part of the Mastercard Cybersecurity Job Simulation, I served on the Security Awareness Team, where I was given the opportunity to lead the next phishing simulation campaign. This was a chance to take initiative and demonstrate practical cybersecurity skills in a simulated corporate environment.

My first task involved working with a phishing email that had previously been sent by an external bad actor to some Mastercard employees. Fortunately, the phishing attempt failed because the email was clearly fake and easily spotted.

I was asked to improve on that failed phishing email and redesign it to be more realistic and convincing. The goal was to use the improved version in an internal phishing simulation to test employee awareness and response under pressure.

## Original Phishing Email (Used as Reference)

*From: [mastercardsIT@gmail.com](mailto:mastercardsIT@gmail.com)*

*To: [employee@email.com](mailto:employee@email.com)*

*Subject: URGENT! Password Reset Required*

*Body:*

*Hello [Employee Name],*

*Your email account has been compromised. Immediate action is required to reset your password!*

*Click here to reset your password in the next hour or your account will be locked:*

*<https://en.wikipedia.org/wiki/Phishing>*

*Regards,*

*Mastercard IT*

## Why This Matters

Phishing emails are getting more clever and harder to spot. This simulation was designed to prepare employees for real threats by exposing them to a more advanced version of a real phishing attempt.

Even though the original email failed, it showed how real the danger is—and how easy it would be for a slightly more polished attempt to succeed. As part of the Security Awareness Team, my job was to make the fake email more believable so we could better train and evaluate employee readiness.

## Key Skills Demonstrated

- Phishing recognition and social engineering awareness
- Simulation design for internal cybersecurity drills
- Communication strategy within a security framework
- Leadership and initiative as part of the Security Awareness Team

## **Improved Phishing Email (Used for the Simulation)**

*From: [IT.Support@mastercard.com](mailto:IT.Support@mastercard.com)*

*To: [employee@email.com](mailto:employee@email.com)*

*Subject: URGENT: Security Alert - Password Reset Required*

*Body:*

*Hello [Employee Name],*

*We have detected unusual activity in your email account, which may indicate unauthorized access. For your safety and to protect company data, immediate action is required.*

*To resolve this issue, please reset your password within the next hour. Failure to do so will result in temporary account suspension to safeguard your information.*

*Click the secure link below to reset your password:*

***Reset Password Now***

*If you have any concerns or need further assistance, please contact the IT Helpdesk at [helpdesk@mastercard.com](mailto:helpdesk@mastercard.com) or call us at 1-800-MC-SECURE.*

*Thank you for your prompt attention to this matter.*

*Best regards,*

*Mastercard IT Security Team*

*[www.mastercard.com](http://www.mastercard.com)*

## **Repository Info**

This file documents my first task in the Mastercard Cybersecurity Job Simulation. More updates and breakdowns of additional tasks are documented in the subsequent files.

*Temple Nnanna Idam-Nkama*

*Cybersecurity Analyst*

*Security Awareness Team*