Here is the background information on your task

You are an analyst in the Security Awareness Team. Our Chief Security Officer relies on our team to help our staff learn how to identify and report a security threat to Mastercard.

One of the most common threats organizations face today is phishing (the act of pretending to be someone/something to get information, in most cases, this is usually a password). Attackers may send links or attachments designed to infect the recipient's system with malicious software or lure them into providing financial information, system credentials or other sensitive data. You can find more information about what is phishing in the resources section below.

At Mastercard, one of the ways we mitigate phishing threats is by educating our people about the risks and how to identify them. One way we do this is with our phishing simulation campaigns. We test our staff every month by sending a phishing email that is made to look like something a bad actor would send. We use the results of the simulated test to help us design and implement future training.

Here is your task

The Mastercard Security Awareness team has been asked to think about potential vulnerabilities and how to improve security internally. It has been decided that the first step will be to run a phishing simulation email.

You are an analyst in the team and have been assigned the task to create the upcoming phishing email template for the simulation. Try to make it contextual and believable. The results will help us educate employees on how to identify this type of threat, and therefore prevent a bad actor from successfully launching a phishing campaign on the company.

A few months back - we detected a phishing email that was being used by an external bad actor on some of our employees - thankfully, it failed due to being an obvious fake. However, we know that phishing emails are now getting very sophisticated and a range of tactics are used. You’ve been asked to use this email as a starting point and improve on it to increase the likelihood of an employee clicking on the link.

You can use the following link as the placeholder in your email: https://en.wikipedia.org/wiki/Phishing

Please download the ‘Existing phishing template’ document in the Resources section below to view the email referred to above. Please update it to be more contextual and believable. There is also another resource below if you would like to learn more about phishing attacks.

NIST Guidance:

https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

Template:

From: mastercardsIT@gmail.com

To: employee@email.com

Subject: URGENT! Password Reset Required

—

Body:

Hello (insert 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

My Answer:

From: Mastercard Staff Rewards

To: employee@email.com

Subject: Your Black Friday Employee reward card

Hello Kunal ,

In recognition of your hard work throughout the year, we wish to reward you with a gift card to spend in the upcoming Black Friday sales as a small token of our appreciation. Please find attached your Employee reward card.

The balance of your card will be determined based on your role. To view the balance and activate your employee reward card, visit here.

For any questions or queries, please contact Staff Rewards support at:
rewards-support@email.com

From,

Staff Reward Services

CONFIDENTIAL: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

PART-2

Here is the background information on your task

The phishing simulation designed in the first task was run last week. We've used some tools to analyze the results. You can find the results in the Resources section below that shows the failure rate of each department - it is clear that some teams appear more likely to fall for a phishing email than others.

Now that we have these results, it is really important we use them to identify which areas of the business need more awareness about phishing, and then design and implement the appropriate training for those teams to ultimately lower our overall risk of an attack.

Here is your task

This task has two parts.

First, interpret the results of the phishing campaign, which can be found in the file called 'Phishing simulation results' in the Resources section below. The goal here is to understand which teams appear to be more likely to fall for a phishing email than others.

Second, and once you've analyzed the results, create a short presentation (3-5 slides) providing some awareness and training materials for the two teams that appear to be most susceptible. This will help us improve the security awareness of the teams that performed poorly in this campaign.

Remember that employees at times view training as boring - so try to make it clear, concise and easy to understand. Try to educate employees on what phishing is, as well as provide examples of tactics often used. Use any resources you choose, the more creative, the better!