PHISHING

Mastercard Cybersecurity Job simulation

From: IT Support support@mastercard.com

To: Tom@mastercard.com

Subject: Immediate Password Reset Required - Action Needed

Dear Tom,

We have detected unusual activity on your Mastercard email account that may indicate unauthorized access. As part of our security protocol, we require you to reset your password to protect your account.

Please follow the secure link below to reset your password within the next hour. Failure to do so may result in a temporary lockout of your account.

Reset Your Password

If you have any concerns or need further assistance, please contact the IT Support team immediately.

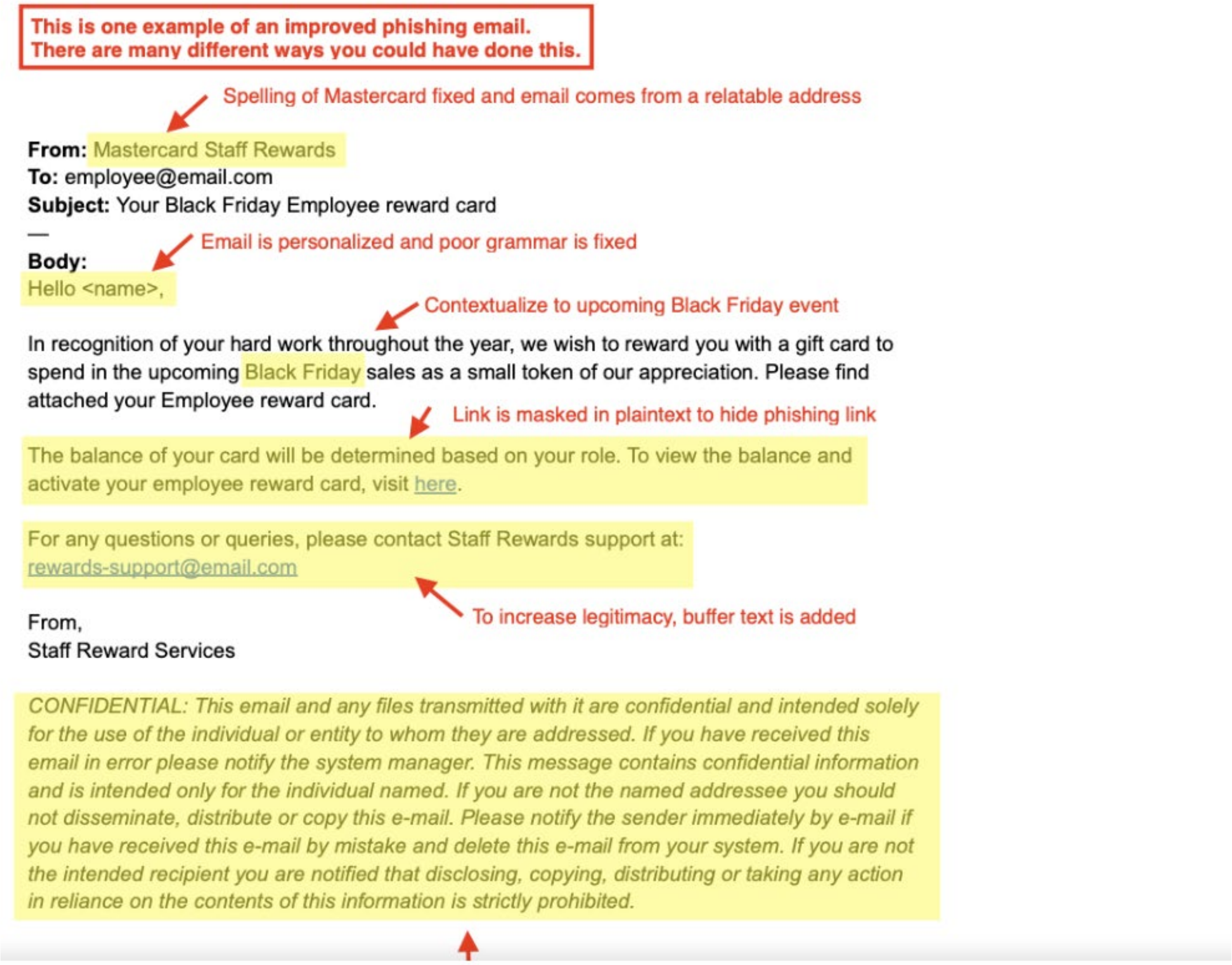
Thank you for your prompt attention to this matter.

Best regards,

Mastercard IT Support

Phone: 1-800-123-4567

Email: support@mastercard.com



This is one example of an improved phishing email.
There are many different ways you could have done this.

Spelling of Mastercard fixed and email comes from a relatable address

From: Mastercard Staff Rewards
To: employee@email.com
Subject: Your Black Friday Employee reward card
—

Email is personalized and poor grammar is fixed

Body:
Hello <name>,

Contextualize to upcoming Black Friday event

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.

Link is masked in plaintext to hide phishing link

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

To increase legitimacy, buffer text is added

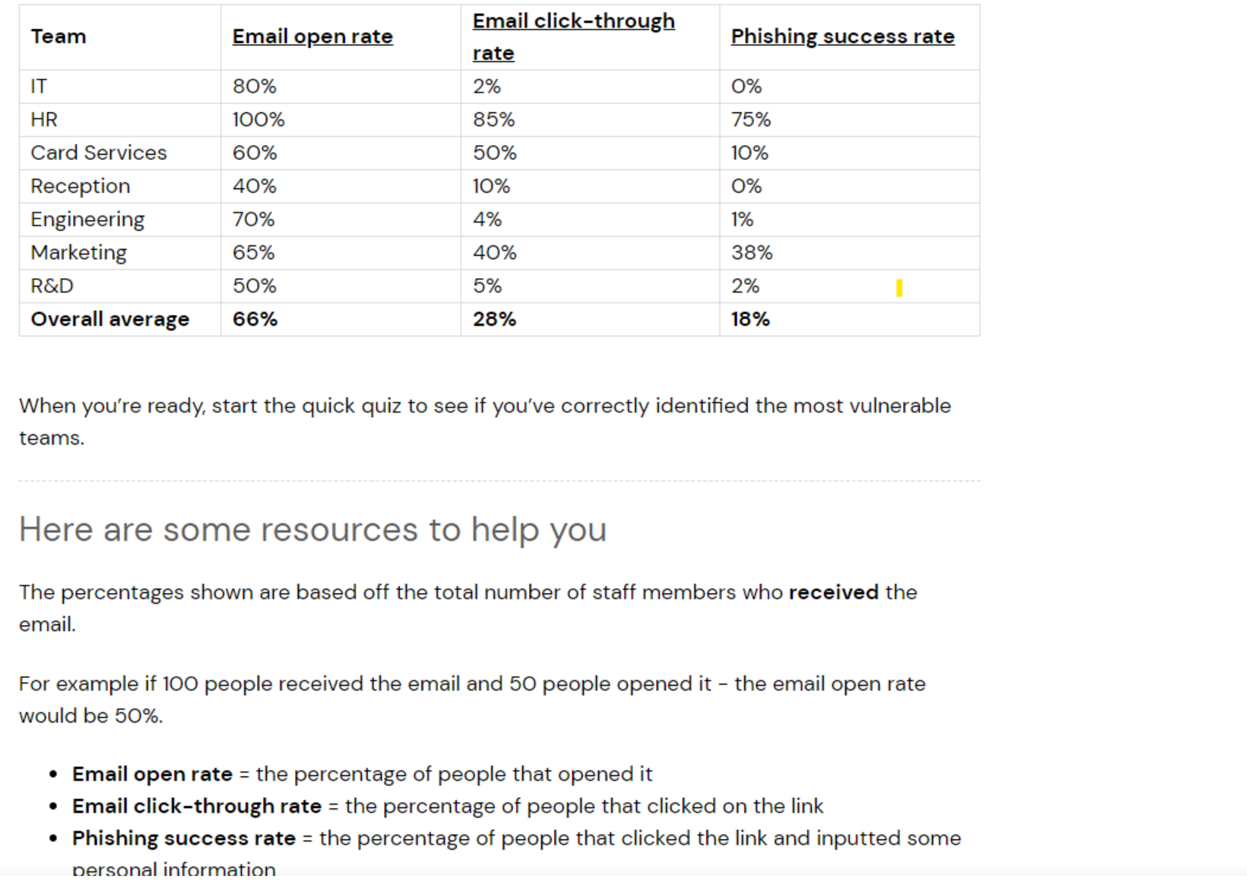
From,
Staff Reward Services

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.

Interpret the results

First, let’s have a look at the results of the phishing campaign.

This table helps you to identify which teams appear to be **more likely** to fall for a phishing email than others.



Team	**Email open rate**	**Email click-through rate**	**Phishing success rate**
IT	80%	2%	0%
HR	100%	85%	75%
Card Services	60%	50%	10%
Reception	40%	10%	0%
Engineering	70%	4%	1%
Marketing	65%	40%	38%
R&D	50%	5%	2%
Overall average	**66%**	**28%**	**18%**

When you’re ready, start the quick quiz to see if you’ve correctly identified the most vulnerable teams.

Here are some resources to help you

The percentages shown are based off the total number of staff members who **received** the email.

For example if 100 people received the email and 50 people opened it - the email open rate would be 50%.

- **Email open rate** = the percentage of people that opened it
- **Email click-through rate** = the percentage of people that clicked on the link
- **Phishing success rate** = the percentage of people that clicked the link and inputted some personal information

Create a short presentation

Now that you've analyzed the results, it's time to 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.

To help prepare your presentation slides, you can use the template provided below:

Remember that employees at times view training as boring - so try to make the presentation 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!