

Mastercard Cybersecurity Virtual Experience Program

Program Overview:

As the world of electronic payments grows, so do we. And we want you to grow with us. Mastercard is part of the NY CEO Jobs Council - a consortium of 30 large NYC employers who are committed to employing 100,000 youth from underserved communities over the next decade. The CEOs of these companies have made a personal pledge to the initiative.

In this virtual experience, you will have the opportunity to build skills and learn what it's like to work as a Security Analyst at Mastercard. Specifically, you'll help design a phishing email simulation for the Security Awareness team. You will learn that cyber threats come in many different forms and that you don't need a technical background to help keep a company and its employees safe from threats.

We hope this program provides a great resource for you to up-skill and strengthen your resume as you explore career options and a potential career in cybersecurity!

Scenario:

Review the scenario below. Then complete the program and activities

You are an analyst in our Security Awareness Team.

Our Chief Security Officer (CSO) relies on our team to help our staff learn how to identify and report security threats to Mastercard.

One of the most common threats organizations face today is phishing. So, what is phishing?

- Phishing is 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.
- Successful phishing attempts can cost companies like Mastercard millions of dollars and put our employees at risk. So it's very important that we keep the business and our staff safe from harm.

At Mastercard, one of the ways we mitigate phishing threats is by educating our people about the risks and how to identify them. An effective way to build awareness is through phishing simulation campaigns:

- We test our staff every month by sending a fake 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.

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.

Start the quick quiz to learn what an ‘obvious fake’ might look like.

Follow the instructions and complete the quiz before moving on to the next part of the activity.

Your manager wants you to lead Mastercard’s next phishing simulation campaign. This is an awesome opportunity for you to step up and show what you can do.

The first step is to create the fake phishing email to use in the simulation.

In the quiz, you just saw what an ‘obvious fake’ looks like, so it’s important to make yours contextual and believable to increase the likelihood of an employee clicking on the phishing link.

Follow the instructions to complete the next part of the activity.

Improved Phishing Email Activity:

From: it-support@mastercard.com

To: employee@email.com

Subject: Action Required: Update Your Password for Security Compliance

Body:

Hello [Insert Name]!

As part of our ongoing efforts to enhance security within our organization, we have detected unusual activity associated with your email account. To ensure the safety of your personal information and maintain compliance with our security protocols, we need you to update your password immediately.

Please click the link below to securely update your password within the next 24 hours:

[Update Your Password](#)

If you do not update your password within the given timeframe, your account may be temporarily suspended as a precautionary measure.

If you have any questions or need further assistance, please contact the IT Support Team directly at it-support@mastercard.com.

Thank you for your prompt attention to this matter.

Best regards,
Mastercard IT Support Team

Confidentiality Notice: This email and any attachments 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 us immediately and delete it from your system. Unauthorized use, disclosure, or distribution of this communication is prohibited.

The phishing simulation designed in the first task was run last week. So, what’s next?

We’ve used some tools to analyze the results and we can see 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, we need to:

- identify which areas of the business need more awareness about phishing, and
- design and implement the appropriate training for those teams to lower our risk of an attack.


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.

<u>Team</u>	<u>Email Open Rate</u>	<u>Email Click-Through Rate</u>	<u>Phishing Success Rate</u>
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%

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.

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!

My Presentation:  Intro to Phishing Presentation

https://docs.google.com/presentation/d/1hl2W_rsNWerrgZYCB_RfRUIUbR9tR8Z6foBCCNPHjak/edit#slide=id.p