Mastercard

Cybersecurity Virtual Experience Program

Forage Job Simulation

Contents:

The program consists of two tasks, namely:

Task One: Design a phishing email simulation

Craft a phishing email simulation to be used to raise awareness of one of the most common threats organizations today face.

What I learnt:

- What threat phishing presents to an organization
- What different types of phishing emails look like
- How Mastercard prevents and mitigates phishing threats

What I did:

- Examine an obvious fake email and make it more believable

Task Two: Interpret phishing simulation results

Interpret the performance of the phishing email simulation to deliver phishing prevention training to the affected teams.

What I learnt:

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

What I did:

- Create a short presentation to help teams improve security awareness

Task One:

Task one started with a brief introductory video and points on what is phishing, and what Mastercard does to mitigate phishing - they send dummy phishing emails themselves to train their employees. Mastercard's security team performs phishing simulations by sending a fake phishing email every month and tests their staff. The results of these tests help Mastercard in future training campaigns.

Mastercard gave me a fake email to improve up on, here is that email:

Obvious Fake:

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 Draft 1:

From: IT@mastercard.com

To: employee@email.com

Subject: URGENT: Password Reset Required.

Body:

Dear employee,

Your email account has been compromised. We request you to reset your password at the earliest to recover your account.

Please follow the link below to reset your password:

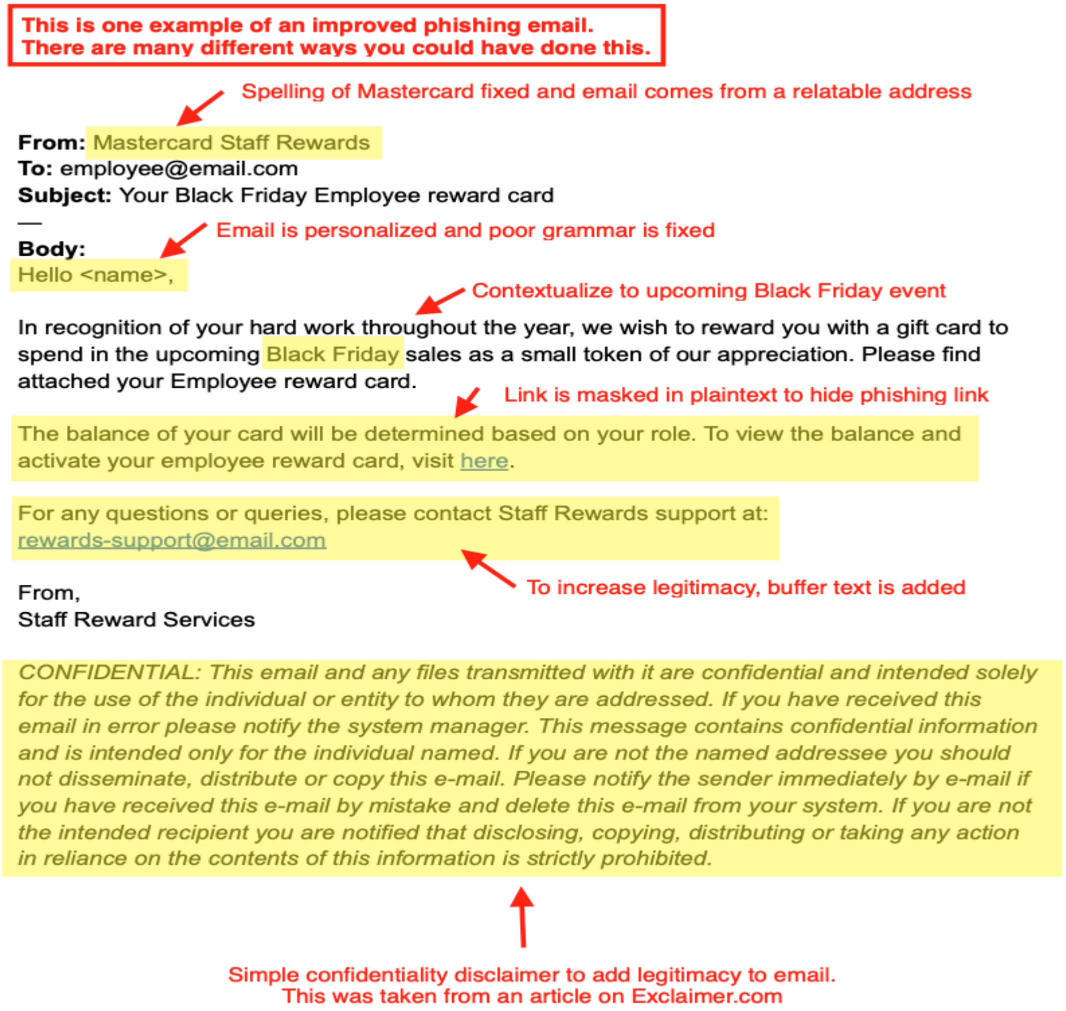
https://en.wikipedia.org/wiki/Phishing

Regards,

Mastercard IT

After seeing Mastercard's version of improvement to the obvious fake (which is shown below), I made a second draft and improved my first attempt:

Mastercard's version:



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.

Simple confidentiality disclaimer to add legitimacy to email.
This was taken from an article on Exclaimer.com

My Draft 2:

From: IT@mastercard.com

To: employee@email.com

Subject: URGENT: Password Reset Required.

Body:

Dear (employee name),

The security team had received suspicious activity from your account and upon further investigation it was found that your email account had been compromised. We request you to reset your password at the earliest and recover your account.

Please follow the link below to reset your password:

[Password Reset](https://en.wikipedia.org/wiki/Phishing)

To stay safe online, we advise you to go through our training on how to keep your account safe which can be found [here](https://en.wikipedia.org/wiki/Phishing).

Regards,

Mastercard IT

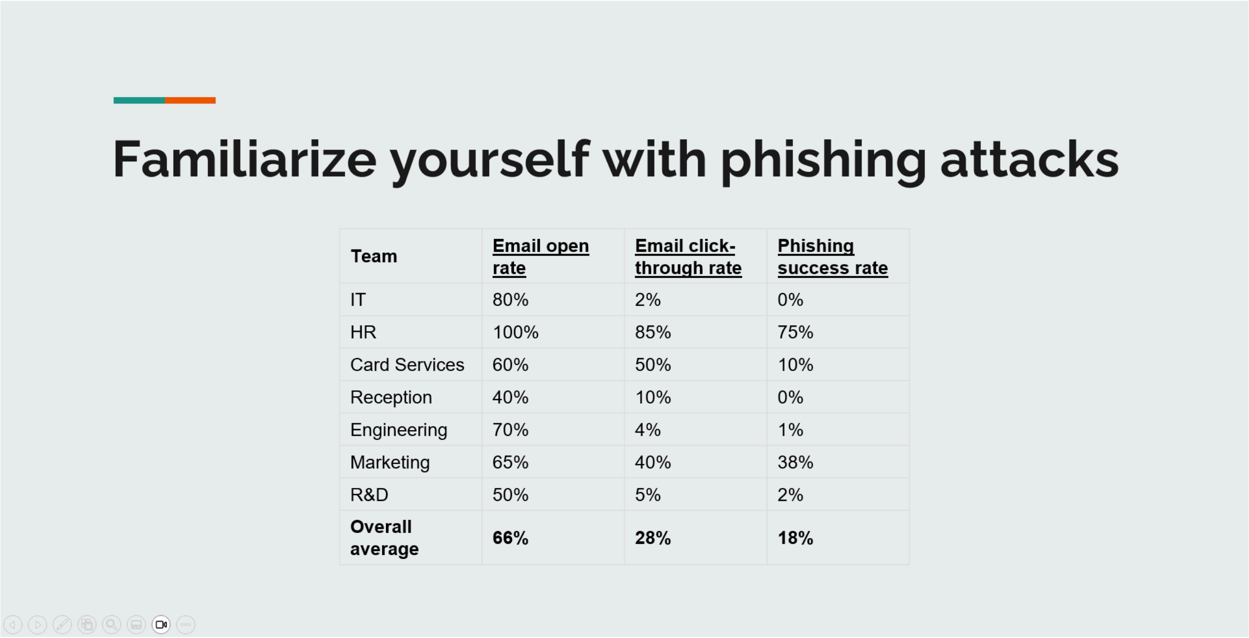
DO NOT CLICK ON EXTERNAL EMAIL LINKS! - NO HAGA CLIC EN ENLACES DE CORREO ELECTRÓNICO EXTERNOS! - NE CLIQUEZ PAS SUR LES LIENS D'EMAILS EXTERNES !

Task Two:

In task two, I was asked to make a presentation based on the results of the phishing simulation in Mastercard.

Here are the screenshots of the presentation and a link to it: https://github.com/PaarthPandey10/forage-job-simulation-portfolio/blob/main/mastercard-cybersecurity/mastercard-cybersecurity-task2-forage.pdf

Presentation:



Familiarize yourself with phishing attacks

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%**

What is phishing?

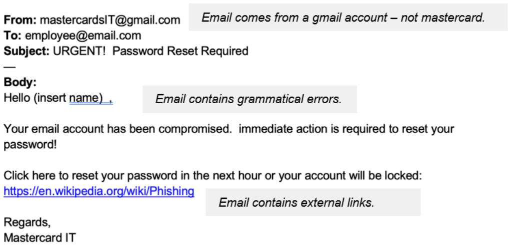
Phishing is a cyber scam where attackers trick you into clicking, sharing sensitive info (like passwords or card numbers), or downloading malware.

They often pretend to be someone you trust—like IT, HR, or even your bank—via emails, texts, or fake websites.

Goal? To steal your data or infect your device.

Think before you click. If it feels off, it probably is.

Learn to spot phishing emails



From: mastercardsIT@gmail.com *Email comes from a gmail account – not mastercard.*
To: employee@email.com
Subject: URGENT! Password Reset Required
—
Body:
Hello (insert name) . *Email contains grammatical errors.*

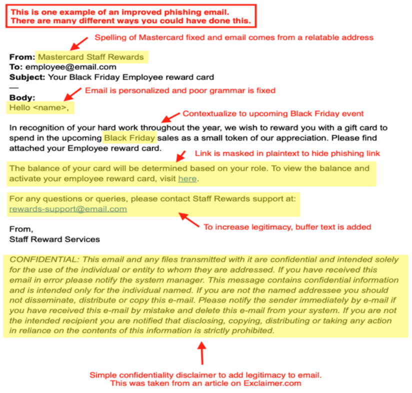
Your email account has been compromised. immediate action is required to reset your password!

Click here to reset your password in the next hour or your account will be locked:
https://en.wikipedia.org/wiki/Phishing *Email contains external links.*

Regards,
Mastercard IT

Obvious Fake Phishing Email

Improved Phishing Email



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.

Simple confidentiality disclaimer to add legitimacy to email.
This was taken from an article on Exclaimer.com

How do we stop getting phished?

Watch for Red Flags:

- Urgent or threatening tone (“Your account will be locked!”)
- Misspelled email addresses or domains
- Unexpected attachments or links
- Requests for passwords or sensitive info

Stay Sharp:

- Hover, don’t click: Hover over links to preview the real URL
- Verify with the source: Call or message the person directly if unsure
- Don’t share credentials via email—no legit service asks for them
- Use MFA (Multi-Factor Authentication) wherever possible

When in doubt: Report suspicious emails to your IT/security team. Better safe than sorry.