



FORAGE VIRTUAL INTERNSHIP

MASTERCARD

Mikhail Amzar

5/28/2024

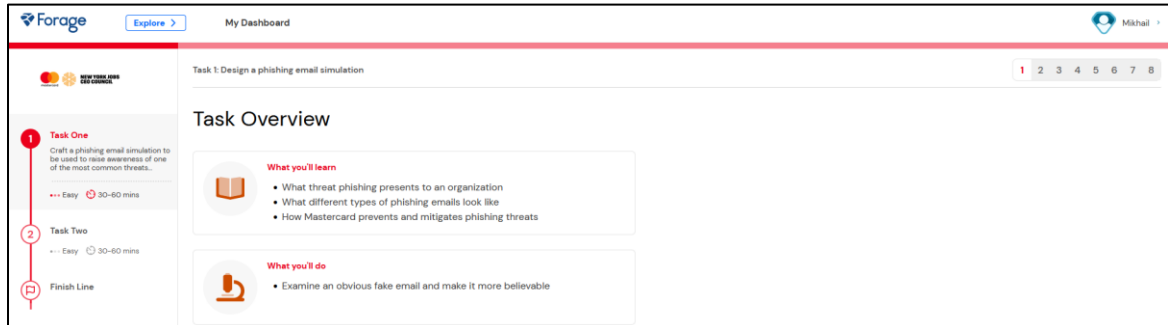
Virtual Internship with
Mastercard.

CONTENTS

Task 1	2
1.Introduction	2
Objectives	2
Activities	2
2.Context	2
Who are you and what do you do?	2
What is phishing?	2
How do we mitigate phishing threats?	3
How does a phishing email look like?	3
3.Spot the phishing email	3
The email	3
Improvement to be made to make it appear more legitimate:	4
TASK 2	6
1.Overview	6
Objectives	6
2.Context	6
What did you do?	6
Presentation	7
3.What they must know	7
What is phishing?	7
What is spear phishing?	7
What is clone phishing?	7
What is Whaling?	7
What is advanced fee scam?	8
What is Account deactivation scam?	8
Website forgery scam	8
Bonus from Cloudflare to check out:	8
Presentation slides and information from Forage example:	9
Resume Snippet	11
Interview Tip- "Why are you interested in this role?"	11

TASK 1

1. INTRODUCTION



This is the landing page of the virtual internship. On a first overview, it seems to be focused on topic of email phishing.

The first task describes that I must craft a phishing email simulation to be used to raise awareness of this common threat.

Objectives

1. Learn to recognize how a phishing email looks like.
2. Understand the types of phishing emails.
3. See how Mastercard prevents and mitigates phishing threats.

Activities

Examine an obvious phishing email, make it more believable.

2. CONTEXT

Who are you and what do you do?

You are an analyst in the Security Awareness Team.

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.

How do we mitigate phishing threats?

We need to **educate** our personnel about the risks and how to identify the threats. For example, simulate a phishing campaign:

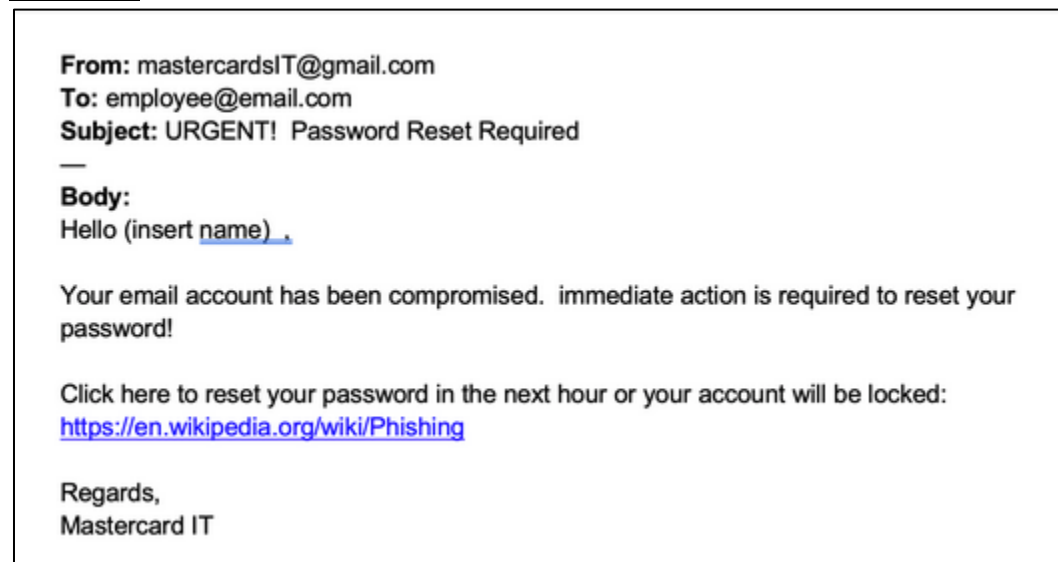
- Test our staff every month by sending a fake phishing email to them, craft something to look like it came from a real threat actor.
- Use test results to acquire insight to design and implement training to counter this threat.

How does a phishing email look like?

Some can be obvious that it's a phishing email. But some can be sophisticated and appear legitimate.

3.SPOT THE PHISHING EMAIL

The email



- Suspicious source email address. Why would an IT department use Gmail instead of Mastercard's own domain?
- Some errors in the sentence, like 'immediate' with a small letter.
- Seemingly non-related URL to the subject being addressed in the email?

This is a phishing email, obviously.



Great Work!

Correct! First of all, there is a typo in the email address. You can also see that it is coming from gmail, not a Mastercard email.

Improvement to be made to make it appear more legitimate:

Attacker can fix the grammar, spelling, & layout. Also masking the URL in text that is more believable to be a password reset link.



Your task is to create a believable phishing email

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.

You've just seen 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.

My attempt:

B *I* U |  

From: staffsupport@mastercards.com
To: employee@email.com
Subject: **Password Reset Required**

Body:

Hello (insert name),

Your email account has been compromised.
Please take immediate action to reset your password.

Navigate to this link to reset your password:
[https://ad.mastercard/account/password-reset](https://en.wikipedia.org/wiki/Phishing)

How would a believable phishing email look like?

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

—

Body:
Hello <name>,

Email is personalized and poor grammar is fixed

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

- Confidentiality disclaimer + buffer text for inquiries at the bottom of the email.
- Mask link in plaintext.
- Include context and relate to real world events.

TASK 2

1.OVERVIEW

Objectives

- Learn how to identify which area in your organization needs awareness on phishing threats.
- Learn what you need to do to design an effective training program for the teams to counter and lower the risk of attacks.

2.CONTEXT

What did you do?

Let's say the simulation program was conducted a week before. You have the results and observe the failure rates of each department to phishing threats.

Using those results you (again):

- Identify which area in your organization needs awareness of phishing threats.
- Decide what you need to do to design an effective training program for the teams to counter and lower the risk of attacks.

Example of results:

Team	<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%

HR, Marketing, Card services, Engineering, R&D.

Presentation

Presentation can be by using slides to display the necessary information related to phishing, common strategies, real-life examples based on known attacks, and strategies to identify phishing attempts.

Employees must be taught what phishing is and the impact it can cause if employees fall victim to it.

3.WHAT THEY MUST KNOW

What is phishing?

Phishing is a form of attack where an attempt is made to steal sensitive information by masquerading/disguising as a legitimate entity to the victim.

Example of **sensitive information**?

- Credentials for any platform (username, password).
- Secret authentication codes (one-time keys).
- Credit card numbers.
- Bank account information.

Or could just be any other kind of information/data that's important to the user.

What is spear phishing?

It is like regular phishing, only that **it is targeted and specific to one individual**.

The attacker could have gathered details and information about the target which allows the phishing attempt to be more personalized and dangerous.

What is clone phishing?

Clone phishing is about mimicking a previously legitimate email that was delivered to the target. The new identical email will have its previous attachment and links (if it had any) replaced by a malicious substitute that still retains original detail like filename or spoofed URL to trick the target.

The clone email will be sent using spoofed email address that appears to come from original sender.

What is Whaling?

Whaling is used to describe attacks that are directed at senior executives or privileged users within business. Contents in this attack typically look like something that likely require attention of the target (containing legal subpoenas, executive issues etc).

Another vector of attack related to whaling is targeted at lower-level employees instead. The attacker will send a request that appears to come from the employees' higher up/executive.

What is advanced fee scam?

Ever heard of the Nigerian prince scam? Yea.

What is Account deactivation scam?

Attacker's persuasion tactics in the phishing message/email will focus on how the [victims account \(bank, work, etc\) are compromised or will be deactivated, and unless the victim acts quickly their account will be gone](#). This is a lie of course; the attackers rely on the sense of urgency they put on the victim so that the victim would panic and not think twice.

Here's an example: the attacker sends an email that appears to come from an important institution like a bank, and they claim the victim's bank account will be deactivated if they do not take action quickly.

The attacker will then request the login and password to the victim's bank account in order to prevent the deactivation. In a clever version of the attack, once the information is entered, the victim will be directed to the legitimate bank website so that nothing looks out of place.

Website forgery scam

This type of scam is commonly paired with other scams such as the account deactivation scam.

In this attack, [the attacker creates a website that is virtually identical to the legitimate website of a business the victim uses, such as a bank](#).

When the user visits the page through whatever means, be it an email phishing attempt, a hyperlink inside a forum, or via a search engine, the victim reaches a website which they believe to be the legitimate site instead of a fraudulent copy. All information entered by the victim is collected for sale or other malicious use.

Bonus from Cloudflare to check out:

"The most common examples of phishing are used to support other malicious actions, such as [on-path attack](#) and [cross-site scripting](#) attacks.

These attacks typically occur via email or instant message, and can be broken down into a few general categories. It's useful to become familiar with a few of these different vectors of phishing attacks to spot them in the wild."

Links:

[Cloudflare Phishing.](#)

There are more examples and types of phishing attack strategy:

<https://www.terranovasecurity.com/blog/top-examples-of-phishing-emails>

Presentation slides and information from Forage example:

What is phishing?

Phishing is the act of pretending to be someone, or something, to get information not usually available.

People can be gullible and curious and click on things they shouldn't - often a link will direct to a fake login page in an attempt to steal credentials.

Learn to spot phishing emails

Urgent duty External Inbox x

Pretend Person <ceo1283812@email.com>
to me

Are you available ?

I have a request for you to handle immediately. Kindly confirm your availability. Keep a close update.

Regards
Sent from my Verizon 4g LTE

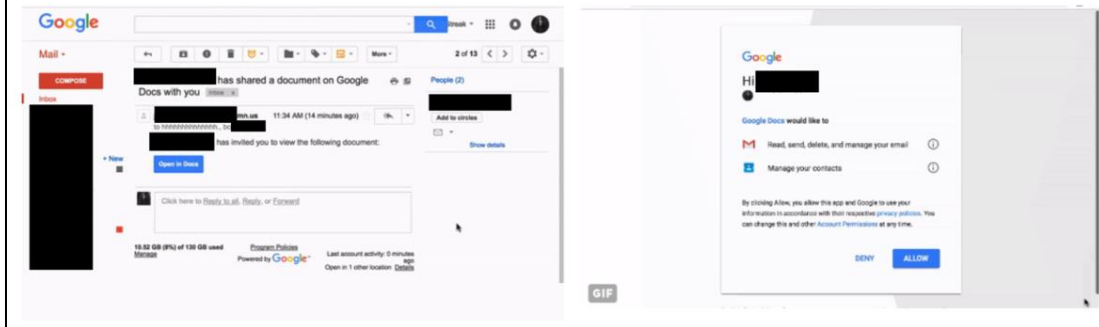
Email is requesting an action with urgency

Phishing emails will pretend to be someone. However, will often use an incorrect email address

No first name personalization & poor grammar

No sign-off/signature

Always be cautious - they can be as sophisticated as this...



How do we stop getting phished?

If it's too good to be true it probably is.

Always be suspicious. Better safe than sorry.

Double check with other employees on a separate communication channel.

For example, in the rewards card phishing email, you could confirm by calling Rewards Services about the employee card being sent out before clicking on the email.

Remember to always:

Check the URL of the website is correct.

Always be suspicious of any email requesting personal information.

Use a password manager to securely store unique passwords for each website.

Use a secondary/side channel to double check when someone requests you to do something.

RESUME SNIPPET

Mastercard Cybersecurity virtual experience program on Forage - May 2024

- Completed a job simulation where I served as an analyst on Mastercard's Security Awareness Team.
- Helped identify and report security threats such as phishing.
- Analyzed and identified which areas of the business needed more robust security training and implemented training courses and procedures for those teams.

INTERVIEW TIP- "WHY ARE YOU INTERESTED IN THIS ROLE?"

I recently participated in Mastercard's job simulation on the Forage platform, and it was incredibly useful to understand what it might be like to participate on a Security Awareness team at Mastercard.

I worked on a project to identify phishing emails and design security awareness training courses. Through this job simulation, I built my skills in problem-solving, data analysis, and data presentation and practiced them in a real-world context.

Doing this program confirmed that I really enjoy working in cybersecurity and I'm excited to apply these skills on a Security Awareness team at a company like Mastercard.