Mastercard Cybersecurity Virtual Internship

Reference: https://www.theforage.com/simulations/mastercard/cybersecurity-t8ye

Tomás Villaseca C.

Tomas.villaseca.c@gmail.com

linkedin.com/in/tomasvc93/

Table of Contents

Task 1 - Design a Phishing Email Simulation

Task Overview:

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

Will learn:

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

Will do:

- Examine an obvious fake email and make it more believable.

Context

You are an analyst in the **Security Awareness Team**.

- **Security Awareness Team** = Group within an organization dedicated to educating employees about information security risks and promoting safe practices to protect the company's data and systems.

One of the most common threats organizations face today is **phishing**.

- **Phishing** = Social engineering attack that uses digital communications (usually email) to trick individuals into revealing sensitive data or deploying malicious software.
- **Phishing simulation campaign** = Controlled exercise conducted by an organization to test and improve employee's ability to recognize and response to phishing attempts by sending simulated phishing emails or messages that mimic real-world cyber threats.

Phishing Email Components

a) **Sender Address** = Often spoofed to appear legitimate, mimicking real companies or individuals.

- It may use slight misspellings or different domains to trick recipients.

b) **Subject Line** = Crafted to create urgency or curiosity, encouraging the recipient to open the email.

c) **Body Content** = The main text of the email, designed to seem authentic.

- Often includes a story or scenario to manipulate the recipient into taking action.

d) **Call to Action** = Specific request or instruction.

- Clicking a link, downloading an attachment, or providing information.

e) **Urgency and/or Threat** = Language that pressures the recipients to act quickly, often by suggesting negative consequences for inaction.

f) **Attachment** = May contain malware or lead to malicious websites.

- Often disguised as important documents or reports.

g) **Hyperlinks** = URLs that appear legitimate but actually lead to fake websites designed to steal information.

h) **Logos or Branding Elements** = Copied from legitimate organizations to increase the email's perceived authenticity.

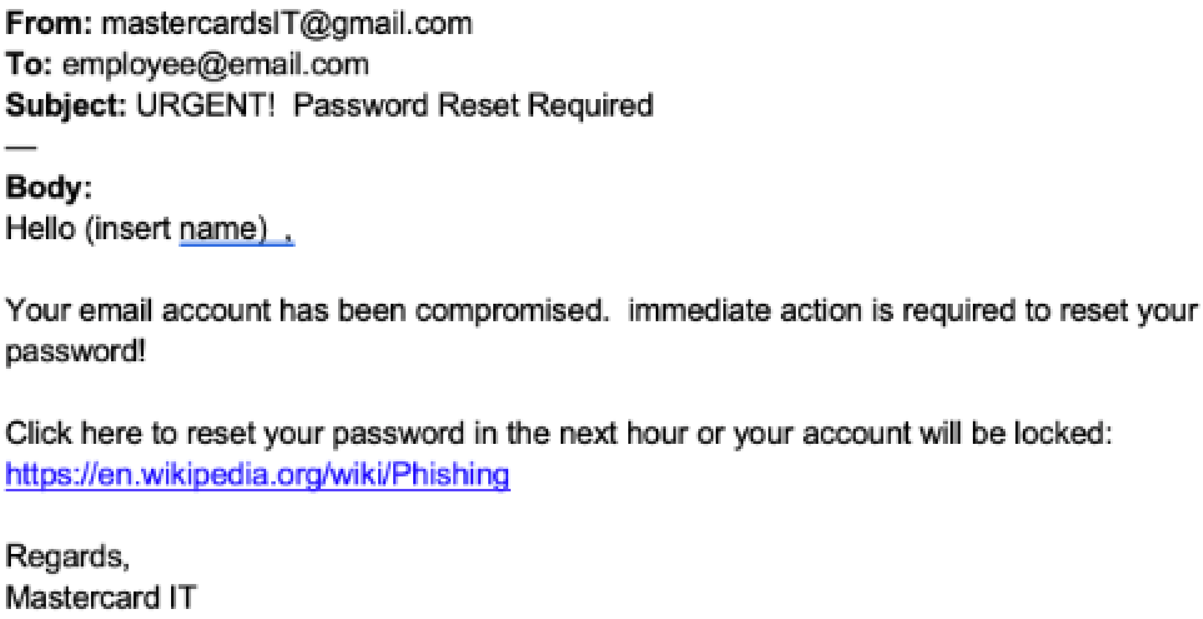
i) **Signature or Footer** = Often includes fake contact information or legal disclaimers to appear more official.

j) **Spelling or Grammatical Errors** = While some phishing emails are well-crafted, many contain errors that can serve as red flags.

- Some errors may be intentional to bypass spam filters or target less discerning individuals.

Phishing Email Example

Phishing Email Example:



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

Issues with the Phishing Email:

- **Suspicious looking source email address** → There is a typo in the source email address (mastercard**s** instead of mastercard)
- **Suspicious looking source email address** → You can also see that its coming from gmail, not Mastercard email.

Body of the phishing email could be more believable → Improve the spelling, grammar, and sloppy layout.

- In addition, the hyperlink could be masked in the plaintext.

Improve Phishing Email

Recreate and improve the obvious fake email to make it more believable.

- End goal is to encourage the user to click on the link.

To create a ‘good’ phishing email, you should:

- Add some context at the beginning - make it relevant to a Mastercard employee.
- Mask the hyperlink within text.
- Use correct spelling and grammar.
- Add points of legitimacy.

Student Attempt:

From: ITSupport@mastercard.com

To: employee@email.com

Subject: Important - Immediate Password Reset Required

Hello <name>,

We have detected unusual activity in your Mastercard email account and suspect it may have been compromised. To ensure the security of your account and prevent any unauthorized access, we require you to reset your password immediately.

Please click on the secure link below to reset your password within the next hour. Failure to do so may result in your account being temporarily locked.

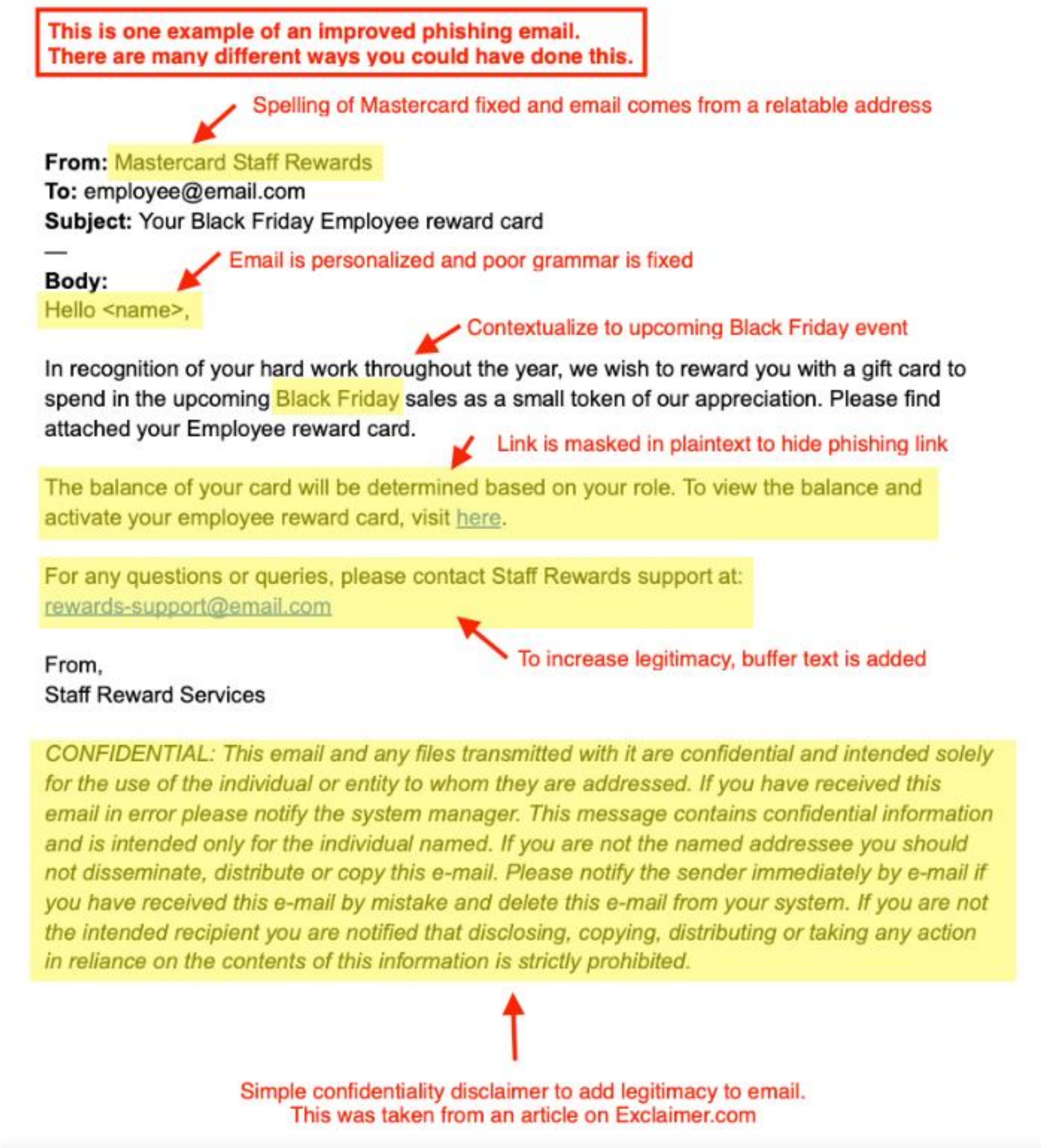
<a href="https://en.wikipedia.org/wiki/Phishing">Reset Your Password</a>

For your security, do not share this link with anyone. If you have any questions, please contact our IT support team at ITSupport@mastercard.com.

Thank you for your prompt attention to this matter.

Best regards,
Mastercard IT Support Team

Mastercard Improved Phishing Email Example:



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

Task 2 - Interpret Phishing Simulation Results

Task Overview:

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

Will learn:

- 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.

Will do:

- Create a short presentation to help teams improve security awareness.

Context

The phishing simulation designed in the first task was run last week.

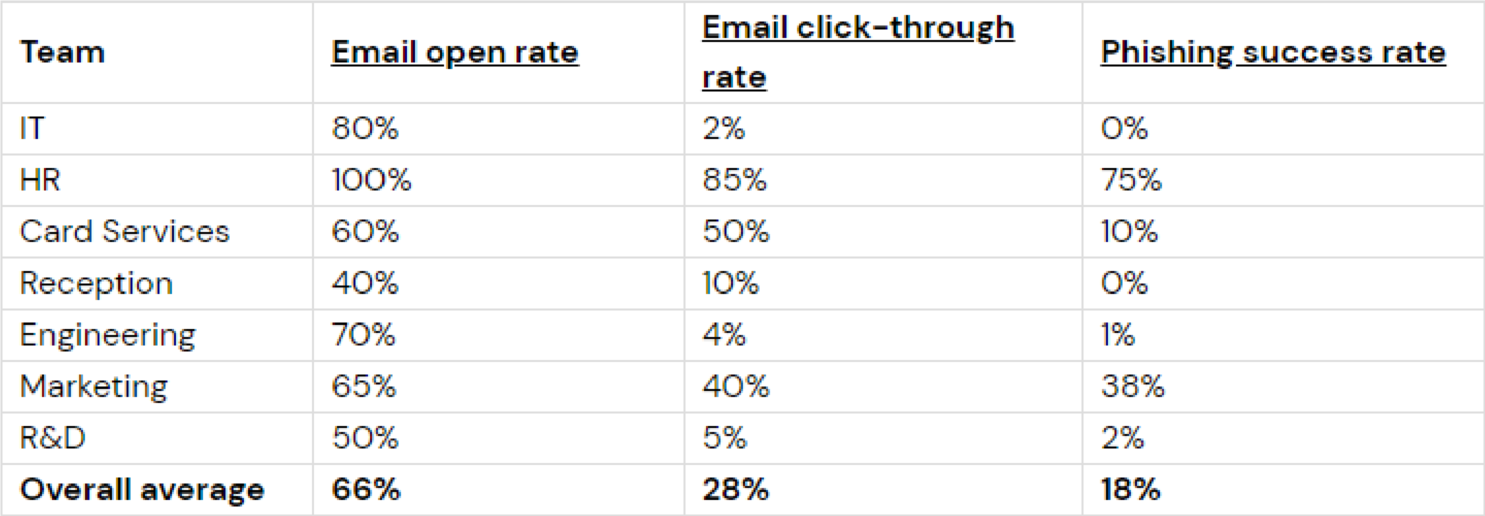
We've used some tools to analyze the results and we can see the failure rate of each department

- 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.
- **Design** and **implement** the appropriate **training** for those teams to lower our risk of an attack.

Phishing Simulation Results Interpretation

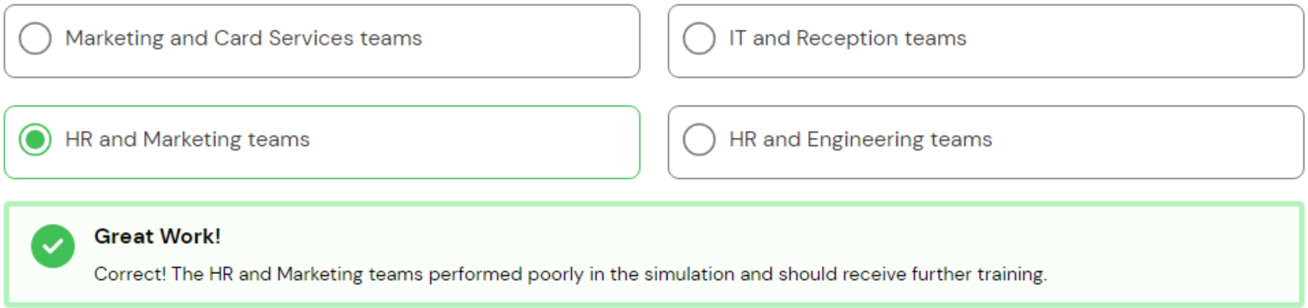


Team	Email open rate	Email click-through rate	Phishing success rate
IT	80%	2%	0%
HR	100%	85%	75%
Card Services	60%	50%	10%
Reception	40%	10%	0%
Engineering	70%	4%	1%
Marketing	65%	40%	38%
R&D	50%	5%	2%
Overall average	**66%**	**28%**	**18%**

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



○ Marketing and Card Services teams

○ IT and Reception teams

● HR and Marketing teams

○ HR and Engineering teams

✓ **Great Work!**

Correct! The HR and Marketing teams performed poorly in the simulation and should receive further training.

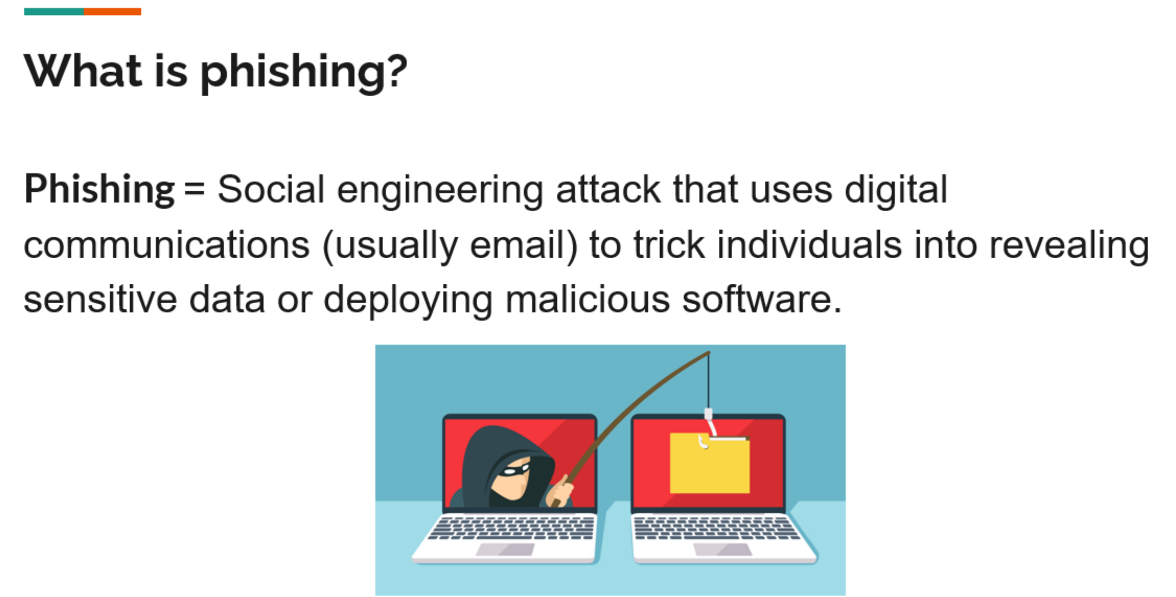
Create Phishing Awareness & Training Material

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!

Student Attempt:

Familiarize yourself with phishing attacks HR & Marketing Teams



What is phishing?

Phishing = Social engineering attack that uses digital communications (usually email) to trick individuals into revealing sensitive data or deploying malicious software.

Learn to spot phishing emails

Tactics Used in Phishing Emails:

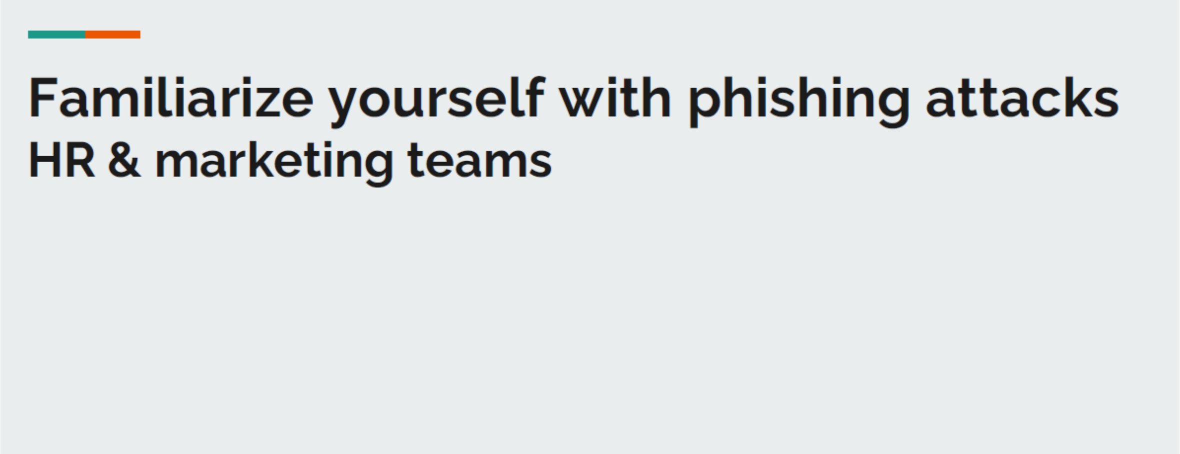
- **Urgency**: Messages often create a sense of urgency or fear (e.g., "Your account will be suspended if you don't respond immediately").
  - Example: An email claiming to be from a bank, stating that your account will be locked unless you verify your information.
- **Spoofed Email Addresses**: Attackers use email addresses that look similar to legitimate ones.
  - Example: support@yourbankk.com instead of support@yourbank.com.
- **Generic Greetings**: Phishing emails often use generic greetings like "Dear Customer" instead of your actual name.
  - Example: "Dear User, your account has been compromised."
- **Suspicious Links**: Emails contain links that, when hovered over, show a different URL than expected.
  - Example: A link text saying "Click here to reset your password" leading to a suspicious URL.
- **Attachments**: Unexpected attachments can contain malware.
  - Example: An invoice attachment from an unknown sender.

How do we stop getting phished?

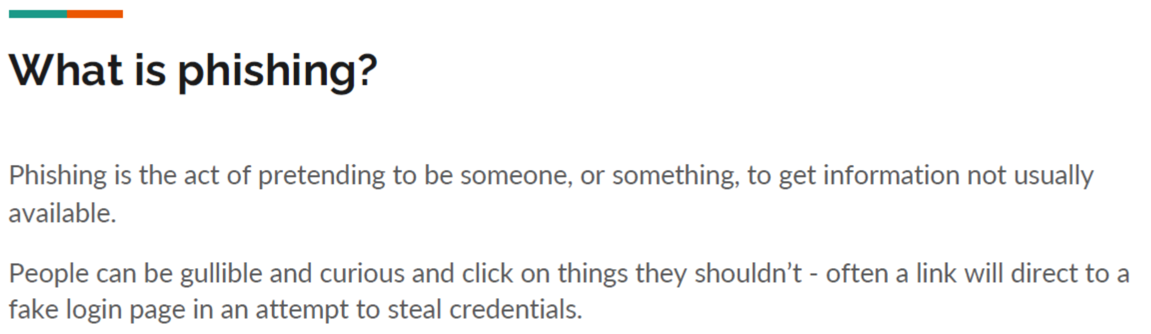
Helpful Tips and Hints:

- **Verify Sender Information**: Always check the sender's email address carefully.
- **Hover Over Links**: Hover over links to see where they lead before clicking.
- **Be Skeptical of Urgent Requests**: Don't fall for messages that create a sense of urgency or fear.
- **Look for Grammar and Spelling Mistakes**: Many phishing emails contain noticeable errors.
- **Use Security Software**: Ensure your devices have updated security software.
- **Educate Yourself and Others**: Regularly attend security awareness training and stay informed about the latest phishing tactics.
- **Report Suspicious Emails**: Immediately report any suspicious emails to your IT or security team.

Mastercard Phishing Awareness Presentation Example:



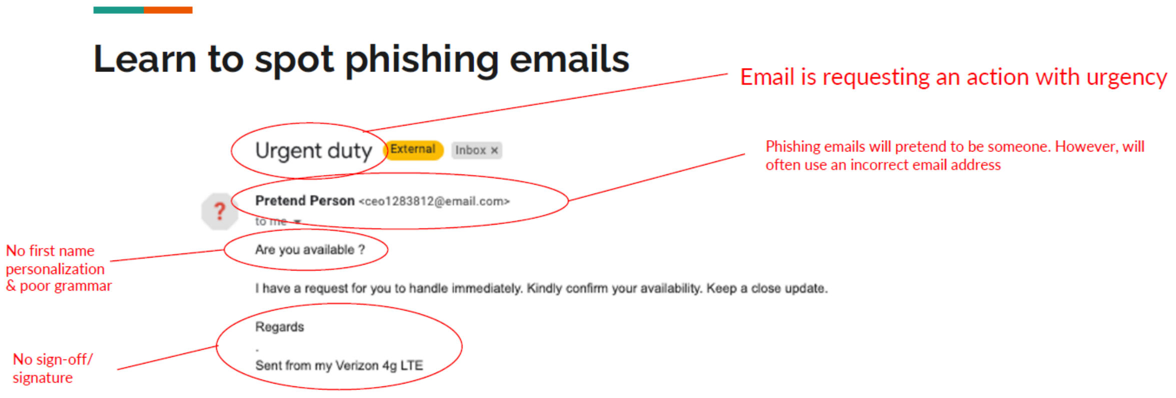
Familiarize yourself with phishing attacks
HR & marketing teams



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

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

Urgent duty External Inbox ×

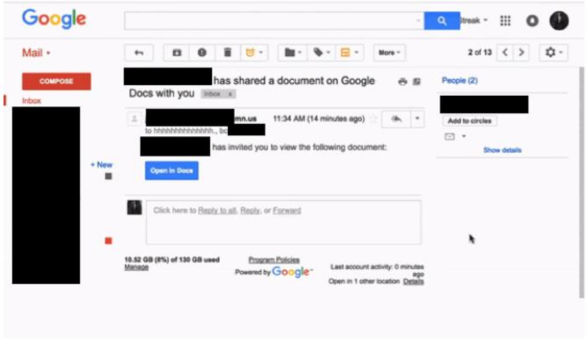
Pretend Person <ceo1283812@email.com>
to me

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

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



[redacted]

[redacted] has shared a document on Google Docs with you

[redacted]mn.us 11:34 AM (14 minutes ago)
to hhhhhhhhhhhhhh., bc[redacted]

[redacted] has invited you to view the following document:

[redacted]

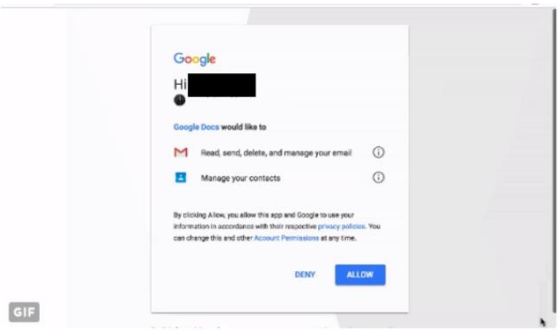
Open in Docs

Click here to Reply to all, Reply, or Forward

10.52 GB (8%) of 130 GB used
Manage

Program Policies
Powered by Google

Last account activity: 0 minutes ago
Open in 1 other location Details



Hi [redacted]

Google Docs would like to

Read, send, delete, and manage your email

Manage your contacts

By clicking Allow, you allow this app and Google to use your information in accordance with their respective privacy policies. You can change this and other Account Permissions at any time.

DENY ALLOW

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.

The main takeaway points from the example presentation include:

1. They use contextual & visual examples of how to spot phishing emails
2. The presentation is clear, concise & heavy on the visuals
3. They provide clear & concise action points