Mastercard Cybersecurity virtual experience program on Forage - April 2025

- **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**

“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.

Splunk project

Chart 1

Count by Category

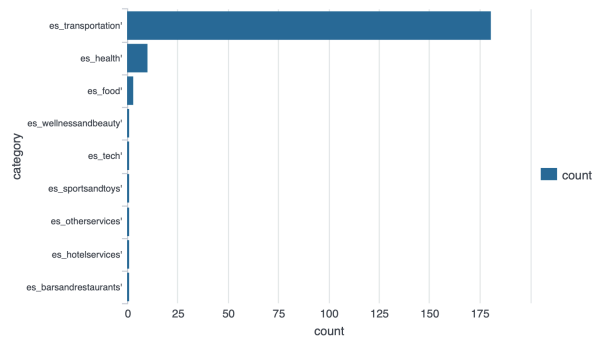


Chart 2

Count of Fraudulent Payments

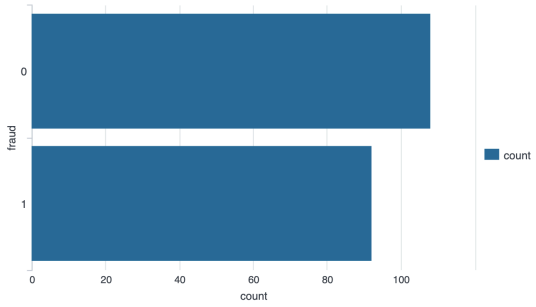


Chart 3

Count by Age

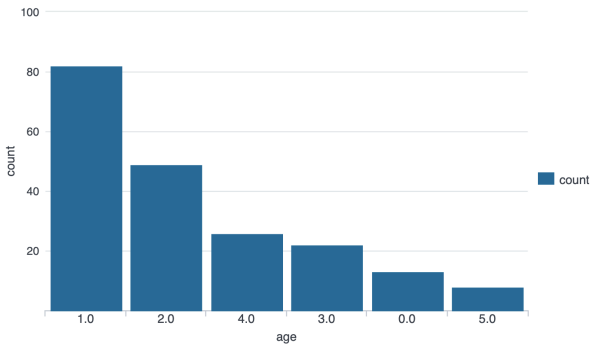


Chart 4

Count by Merchant

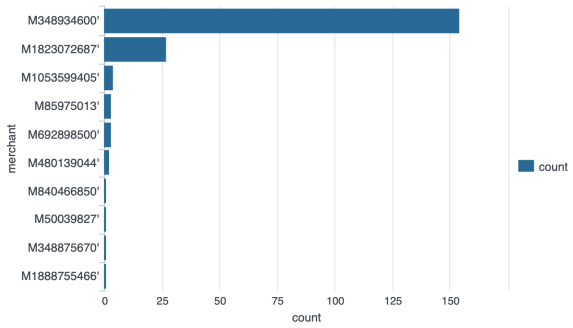


Chart 5

Fraudulent Transactions by Age (Table)

Age	Fraud	count
0.0	0	5
	1	8
1.0	0	44
	1	38
2.0	0	25
	1	24
3.0	0	14
	1	8
4.0	0	14
	1	12
5.0	0	6
	1	2

Chart 6

Fraudulent Transactions by Age (Chart)

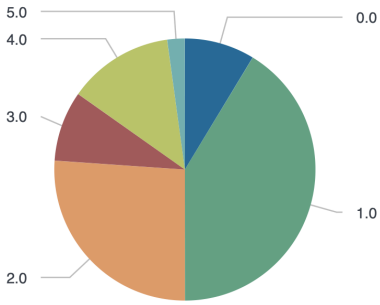


Chart 7

Fraudulent Transactions by Category

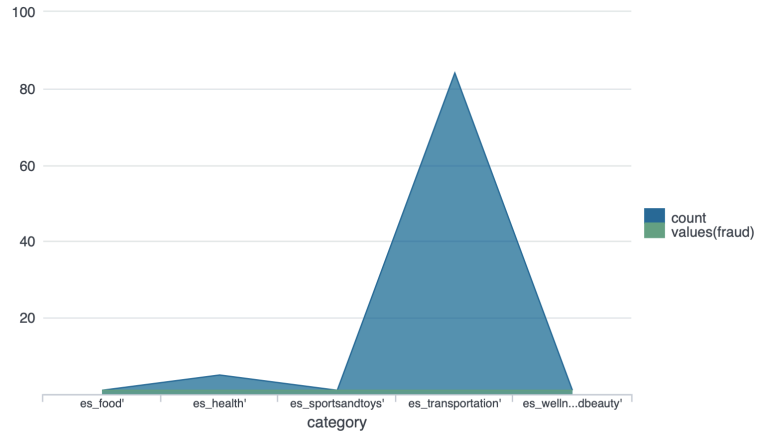


Chart 8

Fraudulent Transactions by Step (Month)

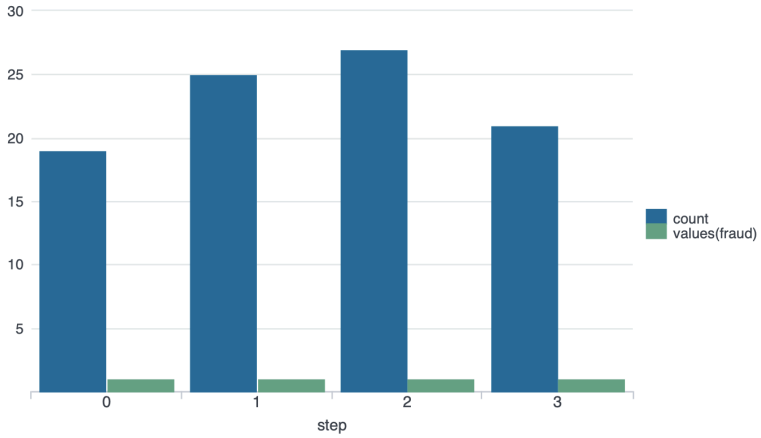


Chart 9

Fraudulent Transactions by Gender

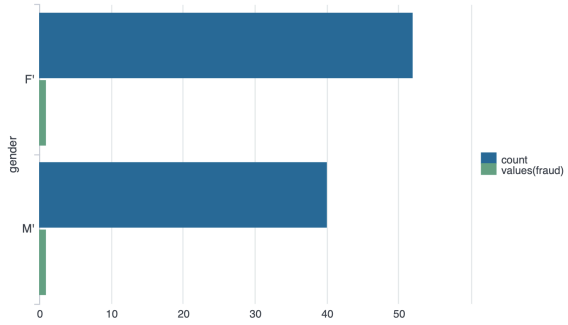


Chart 10

Gender with the most fraudulent activity (female) by Category

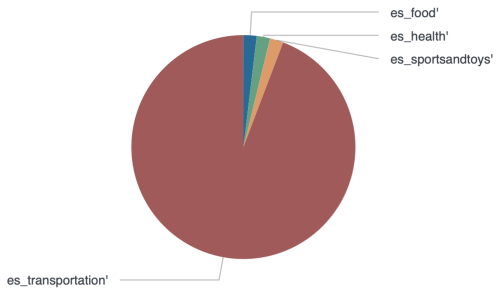
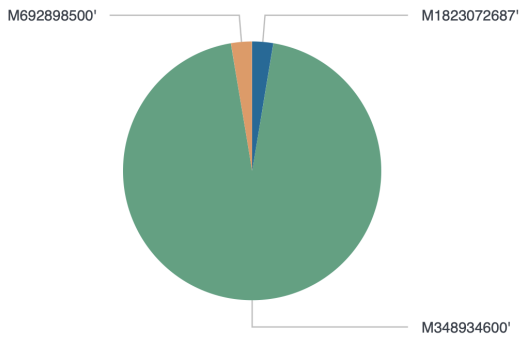


Chart 11

Age group with the most fraudulent activity (1.0 = 19 - 25) by Merchant

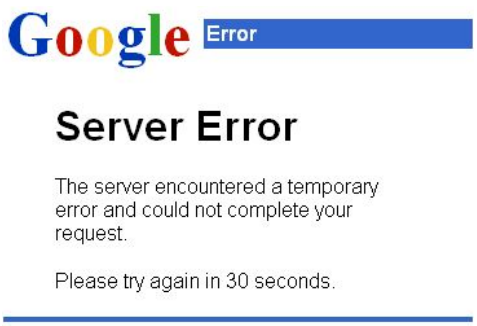


1. What kind of attack has happened and why do you think so?
2. As a cyber security analyst, what are the next steps to take? List all that apply.
3. How would you contain, resolve and recover from this incident? List all answers that apply.
4. What activities should be performed post-incident?

As a member of the cyber security division, your team must handle this incident and the team lead has assigned the issue to you. Below is the timeline of events:

- 10:30 a.m. – The IT Service Desk receives a report from one of your colleagues at the bank that they have received an email from HR telling all employees to update their timesheets in the company's support portal so the timesheets can be approved on time by their line managers against the next pay day. The colleague clicked the link in the email that opened what looked like the portal.

However, following the employee's input of the user credentials, an unfamiliar error page appeared like the one below.



- 2:00 p.m. – Eight more reports of emails similar to the one reported earlier are received by the IT Service Desk. Upon further investigation, it was found that 62 colleagues across the Risk Department received the same email over the course of two days. The emails directed the users to a fake website to steal their usernames and passwords and download a harmful program.
- 3:50 p.m. – The IT Service Desk receives calls and emails from more colleagues that the file-shares are not opening and they receive an error when trying to open a Word document they have always been able to open.

1. What kind of attack has happened, and why do you think so?
    - In a **phishing** attack, the perpetrator pretends to be a reputable entity or person via email to obtain sensitive information like login credentials. In this case, the attacker disguised as the company's HR by asking employees to update their timesheets.
    - **Malware** is intrusive software designed to harm or exploit computers. In this case, the user executed a phishing attack payload that may have installed malware onto their system. As users cannot open a Word document that they have always been able to open, this could be ransomware or a virus.
2. As a cyber security analyst, what are the next steps to take? List all that apply.
    - Begin documenting the investigation.
    - Prioritise handling the incident based on factors such as functional impact, information impact and recoverability effort.
    - Advise users to change and strengthen all logins, passwords and security questions.
3. How would you contain, resolve and recover from this incident? List all answers that apply.
    - Identify and mitigate all exploited vulnerabilities.
    - Attempt to remove malware from all hosts affected.
    - Return affected systems to an operationally ready state.
    - Confirm that the affected systems are functioning normally.
    - Stay alert and continue to monitor for any similar future activity.
4. What activities should be performed post-incident?
    - Follow-up report detailing everything that occurred.
    - Hold a lesson-learnt meeting.
    - Educate: Create a cyber awareness program for employees. Such programs help employees identify future phishing emails.