Mastercard Cybersecurity Job Simulation

Task 2: Phishing Campaign Results & Targeted Awareness Strategy

Author: Temple Nnanna Idam-Nkama
Role: Cybersecurity Analyst – Security Awareness Team
Date: January 2025

Objective

This task was focused on analyzing the outcome of a phishing simulation campaign. The goal was to pinpoint which departments were most vulnerable to phishing attacks and then develop a custom training strategy to strengthen their cybersecurity awareness.

Key Metrics Explained

To properly evaluate the results, we tracked the following three metrics:

1. **Email Open Rate** – This shows the percentage of recipients in a department who opened the phishing email. It helps us understand how engaging or urgent the subject line appeared.
2. **Click-Through Rate (CTR)** – This is the percentage of recipients who clicked on the malicious link inside the phishing email after opening it. A high CTR usually indicates a lower level of caution.
3. **Phishing Success Rate** – This is the percentage of recipients who not only clicked the link but also took the bait (e.g., entered sensitive information). It's the most critical metric, showing real susceptibility to phishing attacks.

Phishing Simulation Results

Here's how the departments performed:

Team	Email Open Rate	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 Avg.	66%	28%	18%

Insights

- **HR** was the most vulnerable department with a **75% success rate**. That means most of the team not only opened and clicked the email but also followed through with risky actions.
- **Marketing** was next in line with **38% success**, showing a high click-through rate and a worrying number of users falling for the bait.
- **IT, Engineering, and Reception** showed excellent phishing resistance, with 0–1% success rates.

Awareness Strategy for Vulnerable Teams

Given the results, focused training was developed for the HR and Marketing departments. Key activities included:

- Scenario-based micro-learning videos using HR and Marketing email examples.
- Quick reference posters with “Red Flags” to spot suspicious emails.
- A 5-minute phishing checklist exercise to encourage slow, critical reading.
- Team-based phishing drills followed by review sessions to discuss what went wrong.

These resources were designed to be practical, team-specific, and easy to apply in daily work situations.

Next Steps

This training is not a one-time fix. Follow-up phishing simulations will be run quarterly to test progress, and monthly awareness emails will be sent to all departments.

By identifying the weak points and targeting them with the right content, we’re actively reducing the company’s risk of a real-world phishing breach.