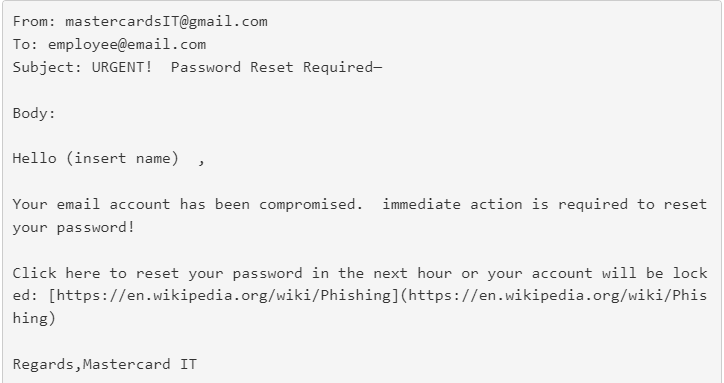
Phishing Email Simulation and Awareness Training

Summary

This is a phishing simulation test project report. Security team investigated a successful phishing email and created a benign phishing email based on the investigation for the employees of Mastercard to identify which departments are most vulnerable to phishing. Simulated email was created with a believable context and structure. Goal was to create an email that has the highest malicious link **click-through** rate and **successful phishing** rate. Analysis shows that the **HR** and **Marketing** department is most vulnerable to phishing attacks where the HR has the highest click-through rate and phishing success rate of 85% and 75% respectively. As a response, the security team created an awareness training for the employees to educate them on how to identify phishing emails and steps to follow to prevent future attacks.

Investigation

The security team received an alert on a successful phishing email targeted to the employees of Mastercard. The email impersonates Mastercard’s IT team and urges the users to click on a link to reset their account password. Below is the screenshot of the phishing email.



There are several identifiers in the email to label it as a phishing email.

* Sender’s address contains spelling error and sent from personal gmail address
* Does a poor job of adding proper context
* Uses urgency as the social engineering principle
* Malicious link is clearly visible pointing outside of the company domain

Phishing Simulation

By dissecting the phishing email our security team created a more convincing email to identify which employees are most susceptible to this type of attacks. Our crafted email hides the sender’s address in plaintext. Adds a proper subject line that is considered standard within the company. Personalizes the email by introducing who is contacting. Includes context about what has happened and what to do. Ensures users that they will be guided throughout the process. Finally, hide the malicious link within the text “here” and a disclaimer to make it more believable. This is a highly sophisticated phishing email and will paint a close to perfect picture of current phishing awareness in the company.

**Payload**:

From: mastercardIT

To: employee@mastercard.com

Subject: URGENT ACTION REQUIRED ! (Password Compromised)

Body:

Hello (insert name),

This is Michael from the Mastercard IT team. We have identified that your account has been **compromised** in our recent audit. This is a significant risk to our infrastructure!

Please reset your password now by clicking on the link below! Do not worry we will provide you step-by-step guidelines.

Click **here** to reset password.

Regards,

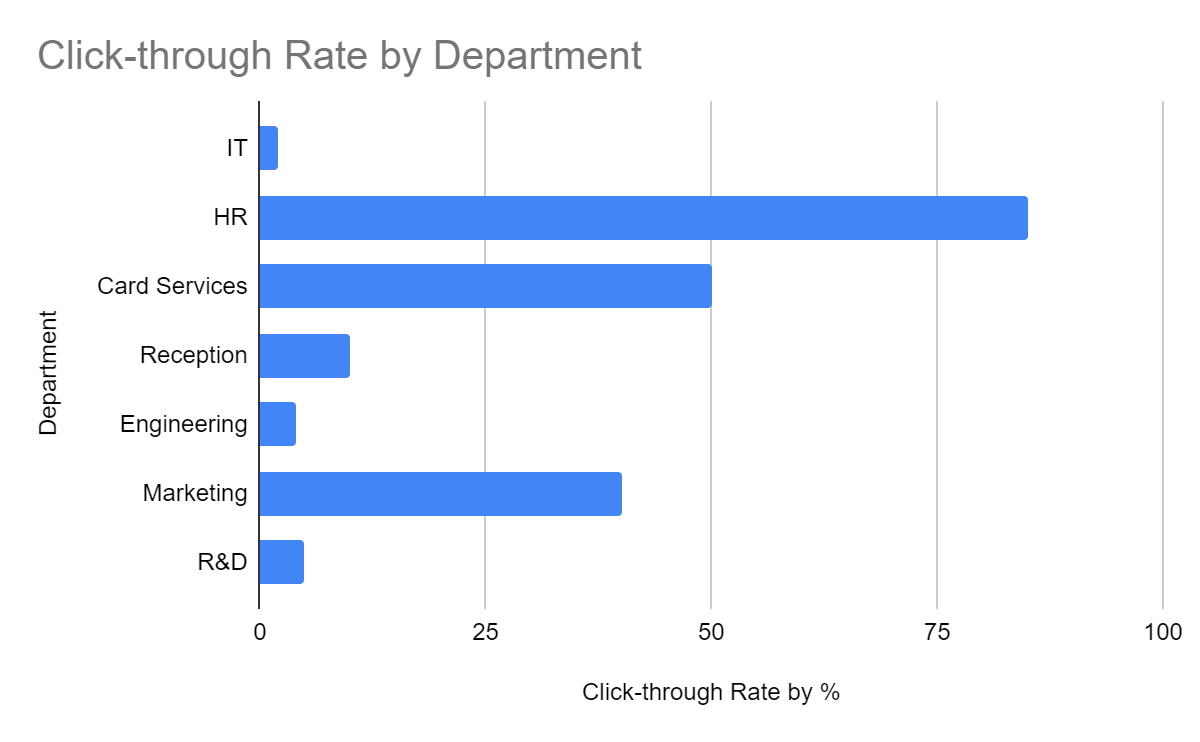
Mastercard IT

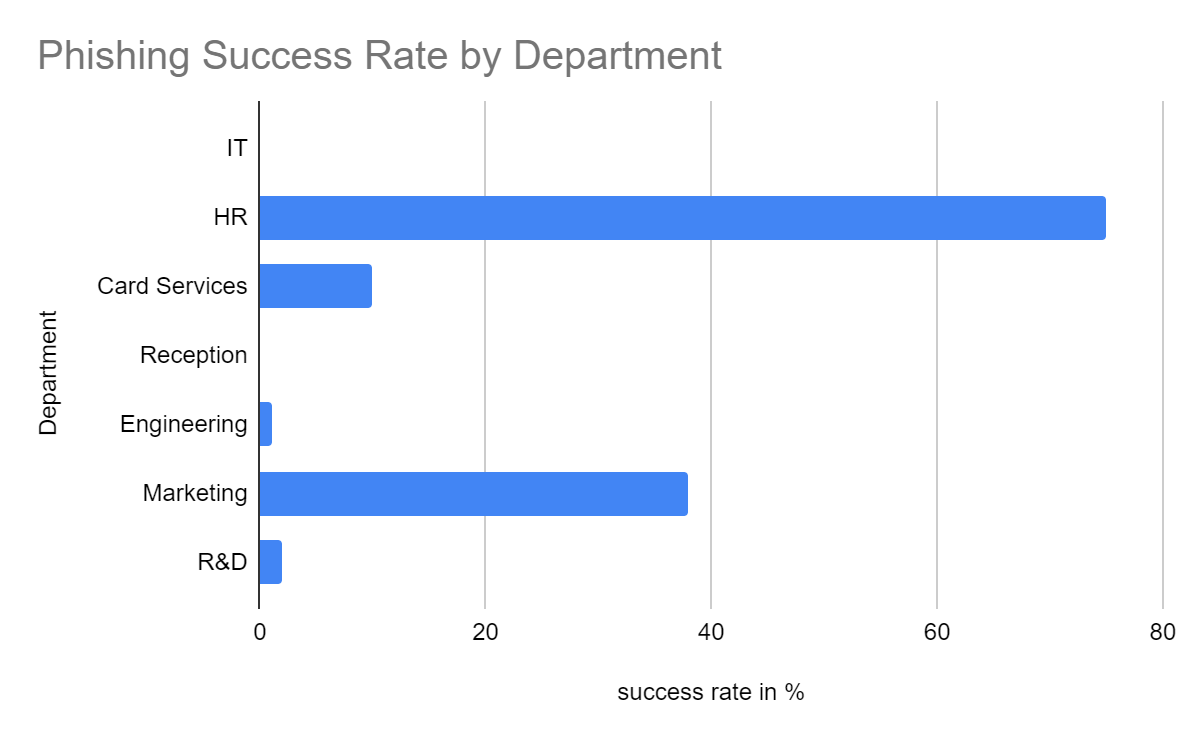
**disclaimer**:*The content of this email is intended for the person or entity to which it is addressed only. This email may contain confidential information. If you are not the person to whom this message is addressed, be aware that any use, reproduction, or distribution of this message is strictly prohibited. If you received this in error, please contact the sender and immediately delete this email and any attachments.*

Analysis

We ran our simulation test on all of the internal departments including the IT team. In total, seven departments were tested and two departments (HR and Marketing) showed the highest phishing success rate i.e they not only clicked but also provided credentials.

Analysis was done with two major attributes: email link click-through rate and successful phishing (credentials provided) rate. The HR, Card Services and Marketing department had the highest click-through rate. Even though 50% of the card services employees clicked on the link, their phishing success rate is only 10%. The HR department leads the chart with 85% click-through and 75% successful phishing. IT, Reception, Engineering and R&D users are the lowest in the graphs and indicate that they are better equipped with phishing attacks.





Response and Remediation

An awareness training is created to educate the employees of the HR, Marketing and Card Services department. This training includes information about how phishing works, how to identify a phishing email and how to best prevent this type of attack from happening again.

This training is short with simple effective contents that helps with user attention and maximizes the knowledge retention.

Security team is constantly monitoring for future phishing attacks and gathering metrics to identify if the current controls and procedures are effective against phishing.