PHISHING SIMULATION FINDINGS

[Payment Processing Company] December 2023 Presented by Nathan Tendido

01 PHISHING

The Cybersecurity team performed a phishing simulation, which included all 7 departments.

- Research and Analyst teams have both identified a recent increase in email phishing campaigns targeted at [Payment Processing Company] and its employees.

What is Phishing?

- Phishing is a cyber attack in which attackers use deceptive emails, messages, or websites to trick individuals into divulging sensitive information, such as login credentials, passwords, credit card numbers, or other personal information.

- The goal of phishing is usually to gain unauthorized access to accounts, steal money, or commit identity theft.

What is Phishing?

- Phishing attacks typically involve sending emails or messages that appear to be from a legitimate source, such as a bank, government agency, or internal staff members.

- These messages often contain **urgent or alarming language**, prompting the recipient to act quickly without thinking on an extremely short notice deadline.

- The emails may include links to fake websites that closely mimic the appearance of legitimate sites, where users are then prompted to enter their sensitive information.

02 RESULTS

The phishing simulation included a single email sent to all departments.

- The HR and Marketing teams were found to be the most susceptible to email phishing attacks.

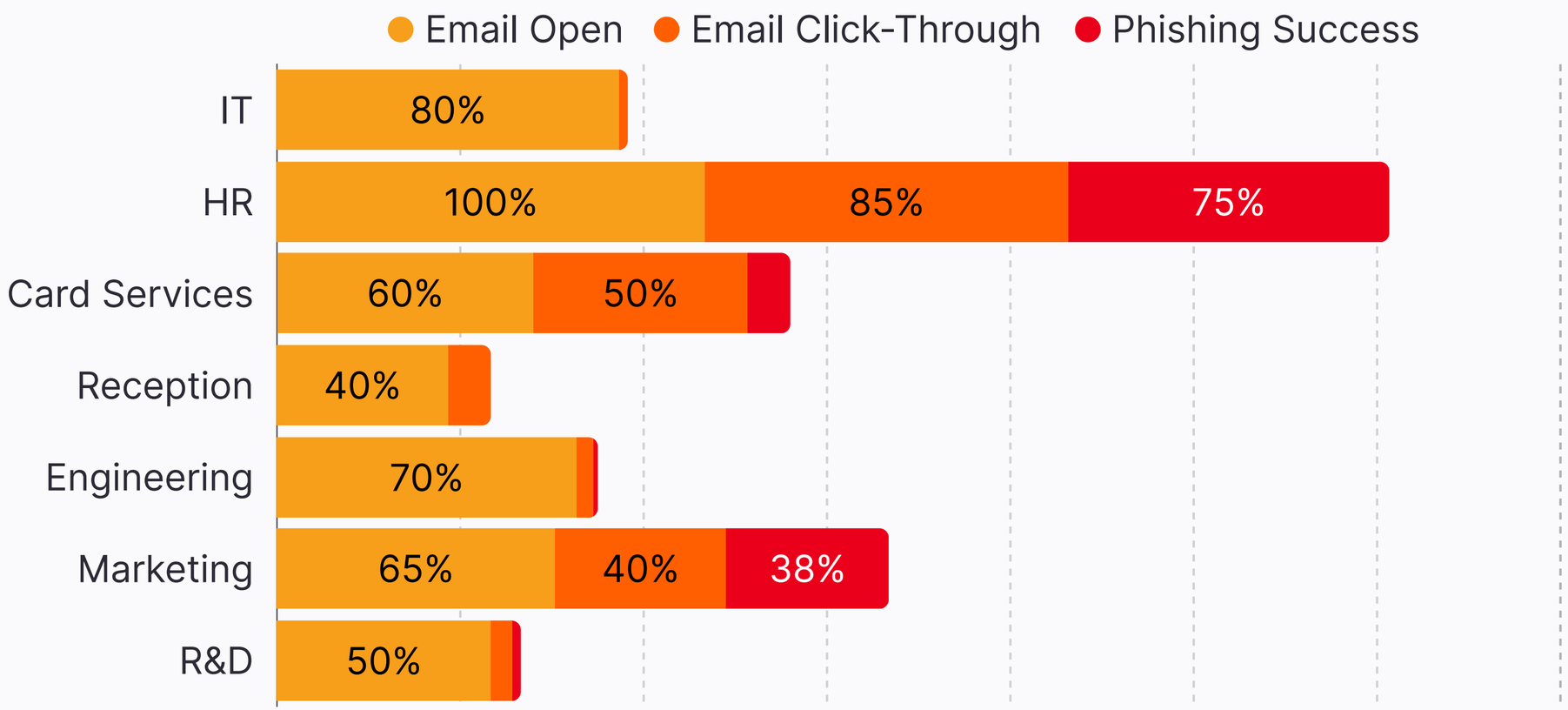
Email Open
→ 66%

Email Click-Through
→ 28%

Phishing Success
→ 18%

Reports
→ 0%

Email Open vs Email Click-Through vs Phishing Success



03 RISK

The simulation identified alarming rates of click-through and phishing success.

- Awareness and preventative action is required in order to ensure the safety and security of all team members as well as all cardholders.

Risk: Human Resources

- Unauthorized access to view and edit sensitive employee information, including social security numbers, addresses, and direct deposit bank information.
- Unauthorized access to view confidential legal records
- Compromised access to higher privileged user accounts and workstations

Risk: Marketing

- Unauthorized access to sensitive financial and marketing projects
- Unauthorized access to confidential personal information from marketing survey and research
- Unauthorized access to email campaign lists
- Compromised access to marketing user accounts and workstations

Risk: Unreported Incidents

- In the phishing simulation, 66% of team members opened the email but did not report the email to management or to the security team.

- Reporting suspicious emails will help the security team analyze specific emails in greater scrutiny and be able to block and report any suspicious emails to the rest of the company.

04 IDENTIFY

Phishing emails often have mistakes that can be caught if scrutinized.

- We will look over the simulation email and review red flags in the email.

From: [Payment Processing Company] Human Resources
To: jane_doe@[Payment Processing Company].com
Subject: Urgent: Action Required - ADP Account Access Reset

Dear Jane,
I hope this email finds you well. Upon review of employee accounts, we have found that your ADP employee account is in non-compliance of [Payment Processing Company] password safety standards. In order to ensure the security of [Payment Processing Company] employee information, regular password resets for ADP employee accounts are required. As a a precautionary measure, we have temporarily suspended your account access and require you to reset your ADP account credentials in order to regain access.
To initiate the account reset process, please click on the following link:

Click here to reset your ADP Employee Account access.

It is crucial that you complete this process at your earliest convenience to ensure the security of your account and the sensitive information it contains. We understand that unexpected requests can be concerning, but please be assured that this is a precautionary measure to maintain the integrity of our systems. Delays in resetting access may result in delays to payroll disbursements and errors in tax reporting for 2023.
If you encounter any difficulties or have concerns about the legitimacy of this email, please contact our support team immediately at 650-101-6501. We are here to assist you and address any questions or concerns you may have.
Please treat this matter with the urgency it deserves, and thank you for your prompt attention to this important issue.

Best regards,
[Payment Processing Company] Human Resources

reviewing the alt text shows that this email was a gmail account and not an org email

From: [Payment Processing Company] Human Resources
To: jane_doe@[Payment Processing Company].com
Subject: Urgent: Action Required - ADP Account Access Reset

sense of urgency

Dear Jane,

I hope this email finds you well. Upon review of employee accounts, we have found that your ADP employee account is in non-compliance of [Payment Processing Company] password safety standards. In order to ensure the security of [Payment Processing Company] employee information, regular password resets for ADP employee accounts are required. As a a precautionary measure, we have temporarily suspended your account access and require you to reset your ADP account credentials in order to regain access.

additional sense of urgency

To initiate the account reset process, please click on the following link:

Click here to reset your ADP Employee Account access.

link provided in email - all reset links should be initiated by you directly from ADP portal

It is crucial that you complete this process at your earliest convenience to ensure the security of your account and the sensitive information it contains. We understand that unexpected requests can be concerning, but please be assured that this is a precautionary measure to maintain the integrity of our systems. Delays in resetting access may result in delays to payroll disbursements and errors in tax reporting for 2023. *"OR ELSE!" statement*

If you encounter any difficulties or have concerns about the legitimacy of this email, please contact our support team immediately at 650-101-6501. We are here to assist you and address any questions or concerns you may have.

this is a disconnected phone number

Please treat this matter with the urgency it deserves, and thank you for your prompt attention to this important issue.

Best regards,
[Payment Processing Company] Human Resources

No individual sign off, individual title, or contact information

QUESTIONS?