

Student Name -Swastik Airee

Student ID - 224389999

Business Intelligence and Database Individual Practical Assignment

MIS781

Contents

[Introduction 3](#_Toc166871458)

[Objectives of the BI Dashboards 3](#_Toc166871459)

[Phishing Campaign Manager Dashboard: 3](#_Toc166871460)

[User Dashboard: 3](#_Toc166871461)

[HR Manager Dashboard: 4](#_Toc166871462)

[Benefits/Advantages of Your BI Dashboards 4](#_Toc166871463)

[Phishing Campaign Manager Dashboard: 4](#_Toc166871464)

[User Dashboard: 5](#_Toc166871465)

[HR Manager Dashboard: 5](#_Toc166871466)

[Assumptions 6](#_Toc166871467)

[Phishing Campaign Manager: 6](#_Toc166871468)

[User: 6](#_Toc166871469)

[HR Manager Dashboard: 6](#_Toc166871470)

[Description of Business Rules and Variables Used 7](#_Toc166871471)

[Phishing Campaign Manager Dataset: 7](#_Toc166871472)

[User Dataset: 8](#_Toc166871473)

[HR Manager Dataset: 9](#_Toc166871474)

[Dashboard 1: For Phishing Campaign Manager 11](#_Toc166871475)

[Chart 1 – Distribution of Campaign Budget 12](#_Toc166871476)

[Chart 2 - Distribution of Emails Sent and Emails Opened by Campaign 12](#_Toc166871477)

[Chart 3 – Average Click Rate Pre and Post Training Follow-Up 13](#_Toc166871478)

[Chart 4 – Success Rates of Phishing Campaigns Across Different Departments 14](#_Toc166871479)

[Chart 5 – Comparison of Success Rate and Budget of Campaign by Department 14](#_Toc166871480)

[Dashboard 2: For Individual User Performance 15](#_Toc166871481)

[Chart 1 – No. of Phishing Emails Clicked by Name and Department 16](#_Toc166871482)

[Chart 2 – Average of Score by Name and Department 16](#_Toc166871483)

[Chart 3 – Email Click Rate of Employees 17](#_Toc166871484)

[Chart 4 – Relation between Training Scores and Phishing Emails Clicked 18](#_Toc166871485)

[Chart 5 – Relationship between Tenure and Phishing Emails Clicked 18](#_Toc166871486)

[Dashboard 3: HR Manager Insights Dashboard 19](#_Toc166871487)

[Chart 1 – Distribution of Departments by Training Completion 20](#_Toc166871488)

[Chart 2 – Correlation of Attendance Rate with Training Score 21](#_Toc166871489)

[Chart 3 – Distribution of Avg. Training Score by Department 22](#_Toc166871490)

[Chart 4 – Effect of Age and Tenure on Risk Level 22](#_Toc166871491)

[Recommendations 23](#_Toc166871492)

[Recommendations - Phishing Campaign Manager 23](#_Toc166871493)

[Recommendations - Individual User Performance 23](#_Toc166871494)

[Recommendations - HR Manager Insights 24](#_Toc166871495)

[Reference 25](#_Toc166871496)

[Appendix 26](#_Toc166871497)

# Introduction

# The purpose of this report is to present the development and analysis of business intelligence (BI) solutions using Microsoft Power BI, focusing on simulated phishing campaign dashboards. These dashboards are designed to enhance skills in researching, understanding, applying, evaluating, and presenting business intelligence tools, which are critical for BI professionals. The Dashboards created in this report are used to help support organizations in developing protective measures such as cultivating training programs and modules to educate employees on best practices and contribute to better information security but it is rarely enough to rely on them alone (Baillon et al., 2019). The dashboards provide comprehensive insights into phishing campaign performance, individual user engagement, and training effectiveness, allowing for data-driven decision-making and targeted interventions to improve cybersecurity posture across the organization.

# Objectives of the BI Dashboards

## Phishing Campaign Manager Dashboard:

**Monitor Campaign Performance:** Track the performance metrics of various phishing campaigns over time, including open rates, click rates, and report rates.

**Identify Trends and Patterns:** Analyse trends in user engagement and response to phishing attempts, identifying peak periods and common phishing tactics that either succeed or fail.

**Assess Campaign Effectiveness:** Evaluate the effectiveness of different phishing campaign strategies and tactics, understanding which ones lead to higher engagement or awareness.

**Resource Allocation**: Optimize resource allocation by identifying which campaigns require more focus or a different approach based on user response data.

## User Dashboard:

**Provide Individual Feedback:** Offer detailed insights and feedback to individual users on their interactions with phishing emails, including their response times and actions taken.

**Highlight Areas for Improvement**: Identify specific areas where users can improve their awareness and response to phishing attempts, providing targeted recommendations.

**Track Personal Progress:** Allow users to track their progress over time in terms of recognizing and responding to phishing attempts, helping them see improvements or identify persistent challenges.

**Encourage Proactive Behaviour:** Motivate users to engage more proactively with phishing training and awareness programs by showing their performance and comparison with peers.

## HR Manager Dashboard:

**Assess Overall Susceptibility:** Provide an overview of the entire organization’s susceptibility to phishing attacks, highlighting which departments or groups are most at risk.

**Evaluate Training Effectiveness:** Measure the effectiveness of existing phishing awareness and training programs, identifying areas where the training has succeeded or needs improvement.

**Departmental Comparisons:** Compare the performance of different departments or teams in recognizing and responding to phishing attempts, helping to identify best practices and areas needing more attention.

**Inform Policy and Training Decisions:** Use data-driven insights to inform decisions regarding new policies or training programs aimed at reducing the organization’s overall risk to phishing attacks.

# Benefits/Advantages of Your BI Dashboards

We now detail the specific benefits and advantages the dashboards offer to their respective stakeholders.

## Phishing Campaign Manager Dashboard:

**Enhanced Decision-Making:**

Provides comprehensive insights into the effectiveness of phishing campaigns, enabling data-driven decisions to improve campaign strategies.

**Real-Time Monitoring:**

Allows for real-time tracking of phishing campaign performance, helping to quickly identify and respond to emerging threats or trends.

**Resource Optimization:**

Helps in the optimal allocation of resources by identifying which campaigns need more attention or adjustments.

**Increased Accountability:**

Provides clear metrics and KPIs that can be used to measure the performance of different phishing campaigns and the team's response to them.

## User Dashboard:

**Personalized Insights:**

Offers individualized feedback on user interactions with phishing emails, helping users understand their strengths and weaknesses.

**Motivation and Engagement:**

Encourages users to engage more proactively with phishing awareness training by showing their progress and performance relative to peers.

**Behavioural Improvement:**

Identifies specific areas for improvement, enabling users to better recognize and respond to phishing attempts.

**Empowerment:**

Empowers users with knowledge and tools to protect themselves against phishing attacks, fostering a culture of security awareness.

## HR Manager Dashboard:

**Comprehensive Risk Assessment:**

Provides an overall view of the organization’s susceptibility to phishing attacks, highlighting high-risk areas and departments.

**Training Effectiveness Evaluation:**

Measures the impact of phishing awareness and training programs, helping to identify successful strategies and areas needing improvement.

**Targeted Interventions:**

Enables the HR manager to implement targeted training and security measures based on the specific needs and vulnerabilities of different departments.

**Policy Development:**

Informs the development of new policies and procedures aimed at reducing phishing risks and enhancing organizational security.

# Assumptions

## Phishing Campaign Manager:

**Completeness:** The dataset includes all relevant phishing campaign data conducted within the specified period.

**Response Data:** The fields Emails\_Opened, Links\_Clicked, and Successful\_Attacks accurately capture user interactions with phishing emails.

**Department Targeting:** Each phishing campaign targets only one department, but a department can be targeted by multiple campaigns.

**Manager Identification:** Campaign Managers and their IDs are distinct and not linked to their Employee IDs in other datasets.

## User:

**Completeness:** The dataset includes all relevant user performance data related to phishing simulations conducted within the specified period.

**Score Calculation:** The Score field represents the user's performance score based on their interaction with phishing emails during the simulation.

**Phishing Campaign Exposure:** Each employee can receive multiple phishing emails from different campaigns.

**Training Completeness:** Not all employees have completed the phishing awareness training prior to the phishing simulations.

**Exposure:** Eachemployee was part of the same no. of simulations and received same no. of phishing emails.

## HR Manager Dashboard:

**Risk Level Calculation:** The Risk\_Level field represents the risk level assigned to each employee based on their behavior and training completion.

**Certification Level:** The Certification\_Level field accurately reflects whether the employee has achieved certification in phishing awareness training.

**Score Calculation:** The Avg\_Training\_Score and Last\_Performance\_Review\_Score fields represent the employee's performance in training and the most recent performance review, respectively.

# Description of Business Rules and Variables Used

## Phishing Campaign Manager Dataset:

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Description** | **Business Rule** |
| Campaign\_ID | Integer | Unique identifier for each phishing campaign | Unique value,  Not nullable |
| Start\_Date | Date | Start date of the phishing campaign | Not nullable,  Format: YYYY-MM-DD |
| End\_Date | Date | End date of the phishing campaign | Not nullable,  Format: YYYY-MM-DD |
| Emails\_Sent | Integer | Total number of phishing emails sent during the campaign | Not nullable,  Non-negative integer |
| Emails\_Opened | Integer | Total number of phishing emails opened by recipients | Can be Null  Non-negative integer |
| Links\_Clicked | Integer | Total number of phishing email links clicked by recipients | Can be Null,  Non-negative integer |
| Successful\_Attacks | Integer | Total number of successful phishing attacks (where user fell for the phishing attempt) | Can be Null  Non-negative integer |
| Department | String | Department targeted by the phishing campaign | Not nullable |
| Campaign\_Type | String | Type of phishing campaign conducted | Not nullable, Valid values: Spear Phishing, Whaling, Clone Phishing, Business Email Compromise, Email Spoofing |
| Budget | Float | Budget allocated for the phishing campaign | Not nullable, Non-negative |
| Success\_Rate | Float | Success rate of the phishing campaign, calculated as Successful\_Attacks / Emails\_Sent | Not nullable, Range: 0-1 |
| Awareness\_Score | Integer | Score indicating the awareness level of the targeted department | Not nullable, Range: 0-100 |
| Training\_Follow\_Up | String | Indicates whether follow-up training was conducted post-campaign (Yes/No) | Not nullable, Values: "Yes", "No" |
| Department\_ID | String | Unique identifier for the department | Not nullable, Unique value |
| Department\_Size | Integer | Total number of employees in the department | Not nullable, Non-negative integer |
| Campaign\_Manager\_ID | String | Unique identifier for the campaign manager | Not nullable, Unique value |
| Manager\_Name | String | Name of the campaign manager | Not nullable |
| Manager\_Email | String | Email address of the campaign manager | Not nullable, |
| Budget\_Percentage | Float | Percentage of the total security budget allocated to the campaign | Not nullable, Range: 0-1 |
| Campaign\_Name | String | Name of the phishing campaign | Not nullable |

## 

## User Dataset:

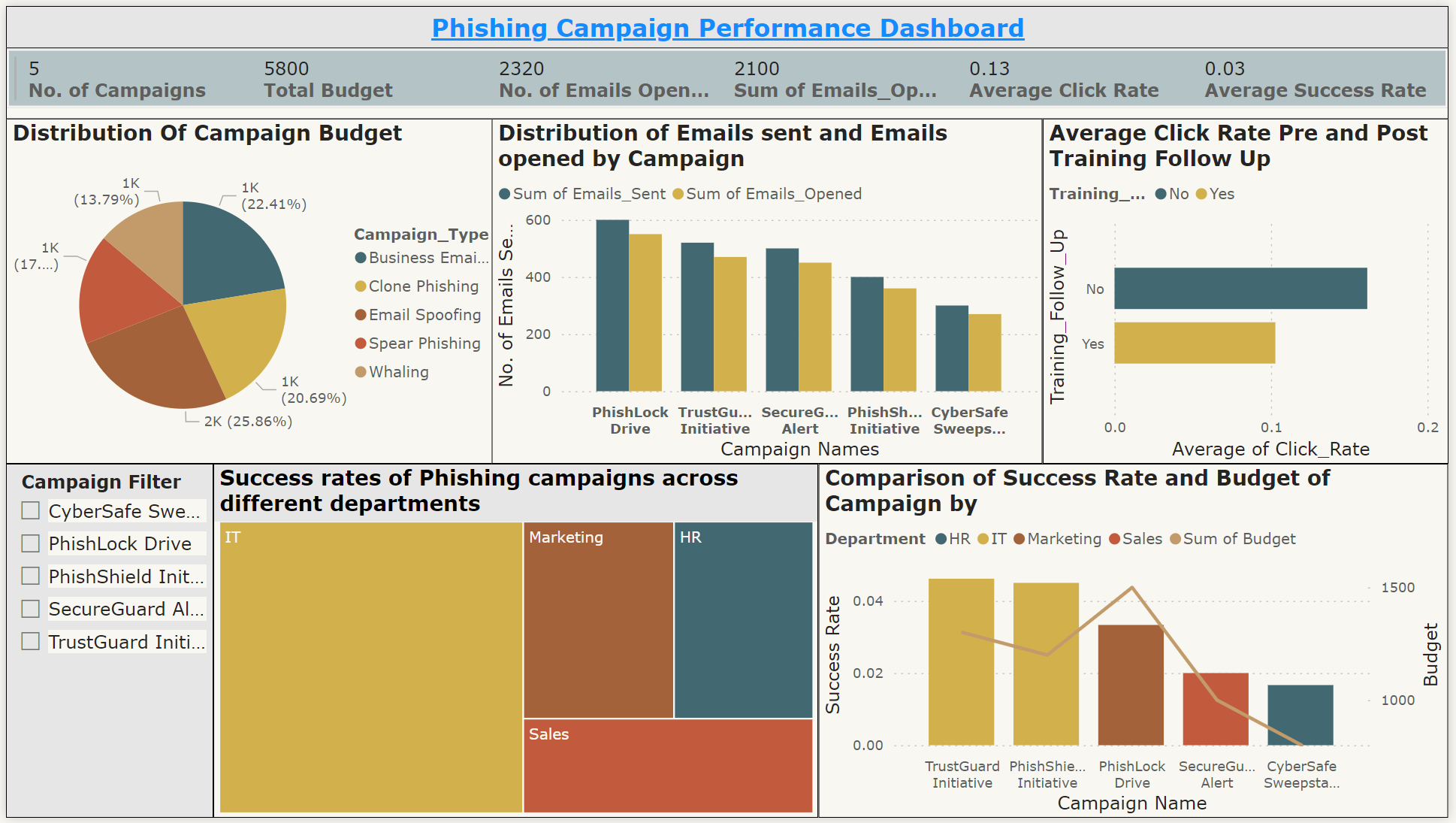
|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Description** | **Business Rule** |
| User\_ID | String | Unique identifier for each user | Unique value, Not nullable |
| Name | String | Name of the user | Not nullable |
| Department | String | Department where the user works | Not nullable |
| Training\_Completed | String | Indicates if the user has completed phishing awareness training (Yes/No) | Not nullable, Values: "Yes", "No" |
| Phishing\_Emails\_Clicked | Integer | Number of phishing emails the user clicked on during simulations | Can be Null, Non-negative integer |
| Last\_Training\_Date | Date | Date of the last phishing awareness training the user attended | Not nullable, Format: YYYY-MM-DD |
| Phishing\_Simulation\_Date | Date | Date when the phishing simulation was conducted | Not nullable, Format: YYYY-MM-DD |
| Score | Float | User's performance score in the phishing simulation | Can be Null, Range: 0-100 |
| Role | String | User's role in the organization | Not nullable |
| Email\_Click\_Rate | Float | Ratio of phishing emails clicked to phishing emails received | Can be Null, Range: 0-1 |
| Avg\_Response\_Time (Min) | Integer | Average time in minutes taken by the user to respond to phishing emails | Can be Null, Non-negative integer |
| Number\_Of\_Simulations | Integer | Total number of phishing simulations conducted for the user | Not nullable, Non-negative integer |
| Phishing\_Emails\_Received | Integer | Total number of phishing emails received by the user during simulations | Not nullable, Non-negative integer |
| Employee\_ID | String | Internal identifier for the employee | Not nullable, Unique value |
| Job\_Title | String | User's job title | Not nullable |
| Tenure | Integer | Number of years the user has been with the organization | Not nullable, Non-negative integer |

## HR Manager Dataset:

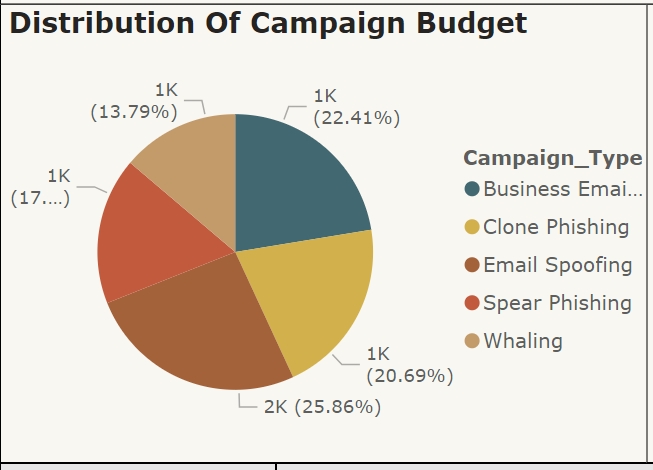
|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Description** | **Business Rule** |
| User\_ID | String | Unique identifier for each employee | Unique value, Not nullable |
| Name | String | Name of the employee | Not nullable |
| Department | String | Department where the employee works | Not nullable |
| Training\_Completed | String | Indicates if the employee has completed phishing awareness training (Yes/No) | Not nullable, Values: "Yes", "No" |
| Risk\_Level | String | Assigned risk level of the employee based on training and behavior | Not nullable, Values: "Low", "Medium", "High" |
| Last\_Training\_Date | Date | Date of the last phishing awareness training the employee attended | Not nullable, Format: YYYY-MM-DD |
| Tenure | Integer | Number of years the employee has been with the organization | Not nullable, Non-negative integer |
| Age | Integer | Age of the employee | Not nullable, Non-negative integer |
| Gender | String | Gender of the employee | Not nullable, Values: "M", "F", "Other" |
| Avg\_Training\_Score | Float | Average score of the employee in phishing awareness training | Nullable, Range: 0-100 |
| Last\_Performance\_Review\_Score | Integer | Score from the employee's most recent performance review | Not nullable, Range: 0-100 |
| Attendance\_Rate | Float | Attendance rate of the employee for phishing awareness training sessions | Nullable, Range: 0-100 |
| Certification\_Level | String | Certification level achieved by the employee in phishing awareness training | Not nullable, Values: "Certified", "Not Certified" |
| Risk\_Level\_Score | Integer | Score representing the employee’s risk level, with lower scores indicating lower risk | Not nullable, Range: 1-3 |
| Number\_of\_Trainings\_Completed | Integer | Total number of phishing awareness training sessions completed by the employee | Not nullable, Non-negative integer |

Dashboard 1: For Phishing Campaign Manager

The BI solutions provided by this dashboard offer a holistic view of phishing campaign performance, enabling stakeholders to make data-driven decisions. Each chart is strategically placed to address specific insights: the top metrics and overview summarize key performance indicators, providing a quick snapshot of overall campaign activity; the budget distribution chart gives immediate insight into resource allocation, essential for strategic planning. Central charts on email engagement and training effectiveness highlight user interaction and the impact of training, critical for assessing engagement and training outcomes. Visualizations on the bottom left focus on departmental susceptibility and performance, crucial for targeted interventions, while the bottom right chart correlates budget with success rates, guiding efficient resource allocation. From this dashboard, stakeholders such as the Phishing Campaign Manager, IT Security Team, HR Department, and Executive Management can gain insights into budget effectiveness, employee engagement, training impacts, and departmental vulnerabilities. By laying out these attributes in a logical flow, the dashboard ensures that stakeholders can easily navigate and extract meaningful insights, ultimately enhancing the organization's phishing defence strategies.

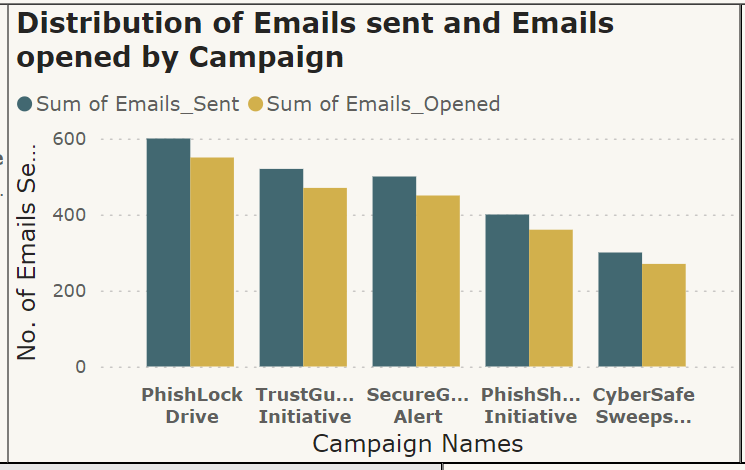


## Chart 1 – Distribution of Campaign Budget



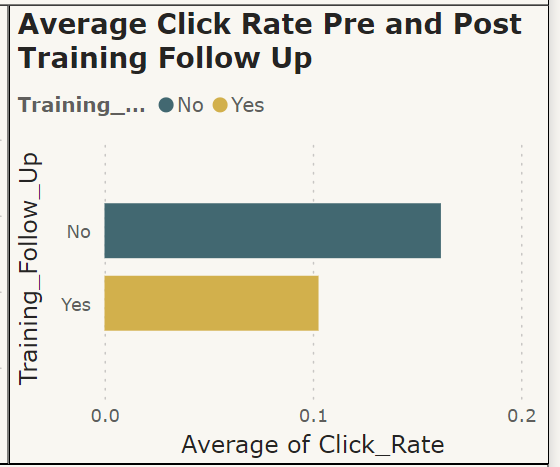
This pie chart illustrates the percentage distribution of the total budget across various phishing campaign types: Business Email Compromise, Clone Phishing, Email Spoofing, Spear Phishing, and Whaling. The chart effectively visualizes the proportional allocation, with Whaling and Business Email Compromise receiving the highest budgets. This helps in understanding resource distribution and strategic focus areas. The dominant budget allocation to Whaling (25.86%) and Business Email Compromise (22.41%) suggests these campaigns are prioritized, likely due to their higher perceived impact or success rate. This visualization aids in evaluating financial planning and resource management.

## Chart 2 - Distribution of Emails Sent and Emails Opened by Campaign



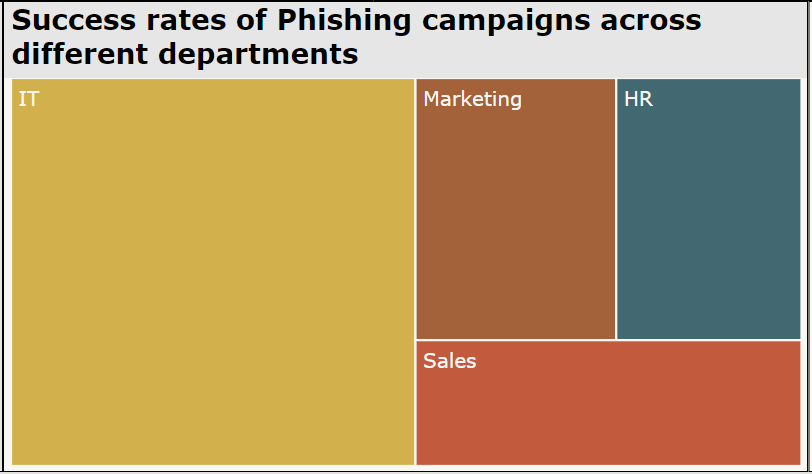
This bar chart compares the number of emails sent and opened for each phishing campaign, including PhishLock Drive, TrustGuard Initiative, SecureGuard Alert, PhishShield Initiative, and CyberSafe Sweepstakes. Bar charts are used for their effectiveness in comparing multiple metrics across categories. The chart reveals that while the number of emails opened is consistently lower than the number sent, PhishLock Drive had the highest engagement, and CyberSafe Sweepstakes had the lowest. This insight helps evaluate campaign effectiveness in capturing user attention, guiding future strategies.

## Chart 3 – Average Click Rate Pre and Post Training Follow-Up



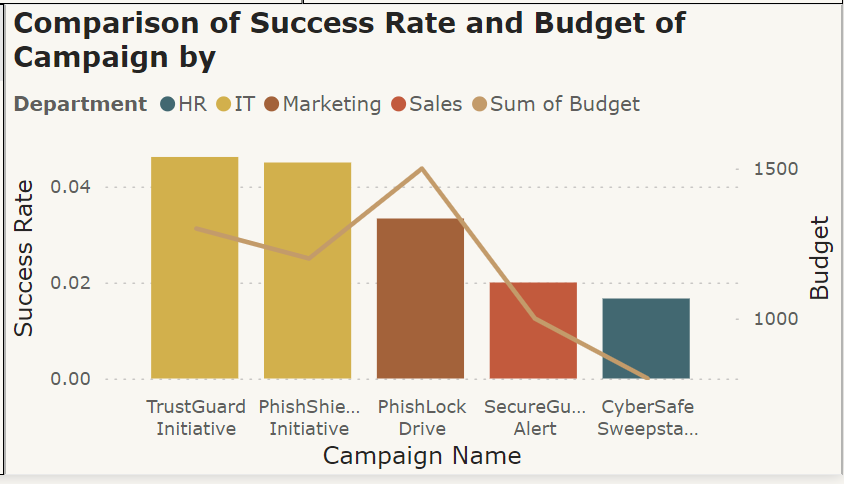
This bar chart compares the average click rates on phishing emails before and after training follow-ups. Two bars represent employees who did not receive follow-up training ("No") and those who did ("Yes"). Bar charts are effective for this comparison, highlighting the impact of training on employee behavior. The chart shows a lower average click rate for employees who received follow-up training, indicating the effectiveness of continuous training in reducing phishing susceptibility. This insight underscores the importance of regular training to improve cybersecurity awareness and defenses.

## Chart 4 – Success Rates of Phishing Campaigns Across Different Departments



This treemap visualizes the success rates of phishing campaigns across various departments, including IT, Marketing, HR, and Sales. Each department's block size indicates its relative success rate. Treemaps effectively compare departments by showing variations in susceptibility. The chart reveals that the IT department has the highest success rate for phishing campaigns, followed by Marketing, HR, and Sales. This insight suggests a need for more focused training or enhanced security measures in the IT department. Identifying high-susceptibility departments enables targeted interventions to reduce phishing success rates.

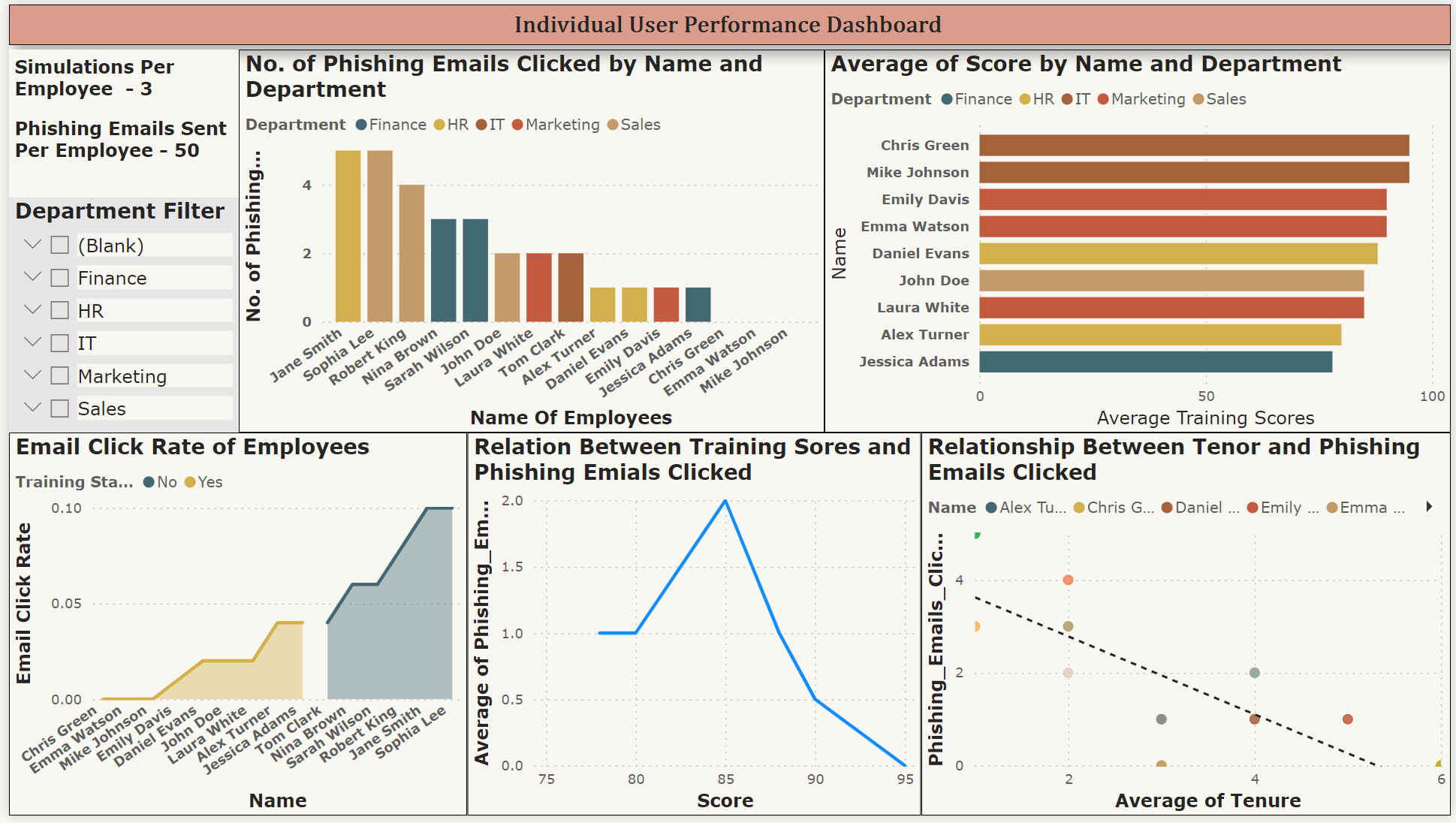
## Chart 5 – Comparison of Success Rate and Budget of Campaign by Department



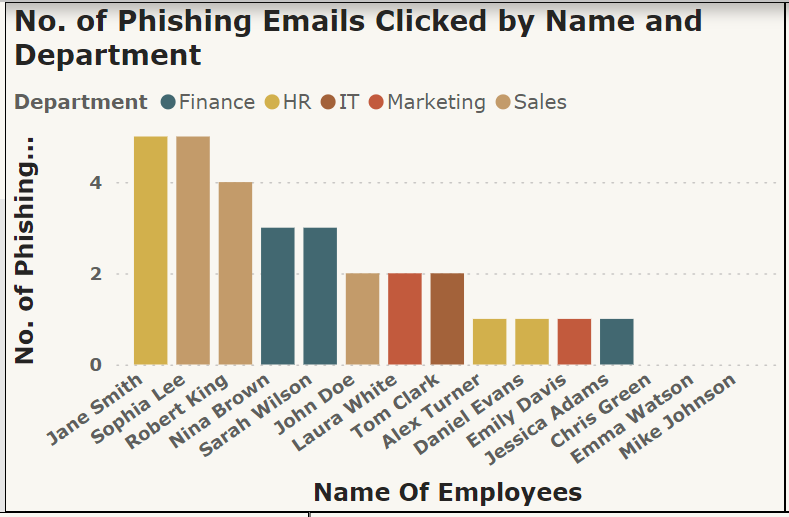
This combined bar and line chart compares the success rate and budget of phishing campaigns across departments like HR, IT, Marketing, and Sales. Bars represent success rates, while the line shows the sum of the budget allocated to each campaign. This format highlights the relationship between financial investment and campaign effectiveness. The chart reveals that higher budgets do not always correlate with higher success rates. For instance, TrustGuard Initiative and PhishShield Initiative have similar success rates but different budgets. This insight helps optimize future budget allocations for improved campaign performance.

# Dashboard 2: For Individual User Performance

The Individual User Performance Dashboard is designed to provide a comprehensive view of phishing simulation engagement and training effectiveness, enabling stakeholders to make data-driven decisions. Phishers try to either steal the digital credentials of their victims to harm them directly, use stolen credentials to carry out attacks on others, or install malware on victim’s system that can be used to steal other information and extort payments to have the information restored (Volkamer et al., 2020). The summary metrics at the top offer a quick snapshot of overall phishing exposure and training status, while the department filter enhances interactivity by allowing users to focus on specific departments. Central charts highlight individual performance, comparing phishing email clicks and average training scores, which is crucial for assessing the impact of training and identifying areas needing improvement. Bottom charts emphasize behavioral trends, such as the correlation between tenure and phishing email clicks and the relationship between training scores and phishing susceptibility. This logical arrangement ensures stakeholders—including employees, team leaders, IT security, HR, and executive management—can easily navigate and extract meaningful insights, facilitating the development of targeted training and support initiatives to enhance the organization’s cybersecurity posture.

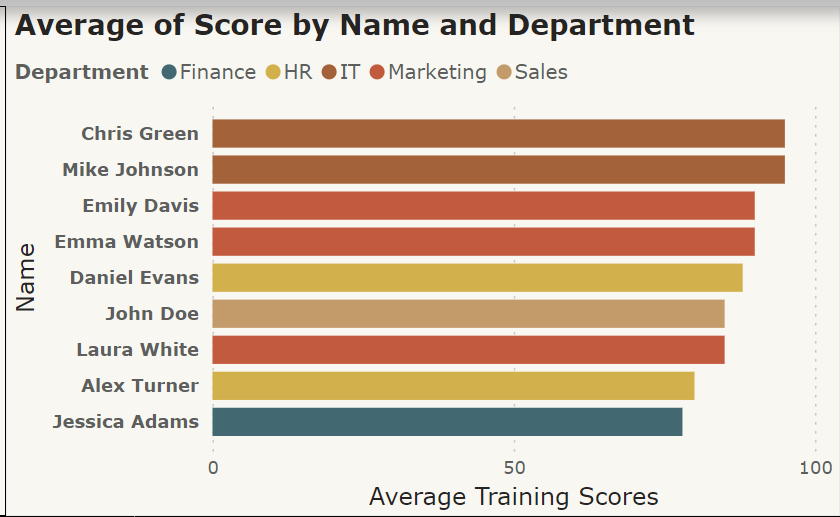


## Chart 1 – No. of Phishing Emails Clicked by Name and Department



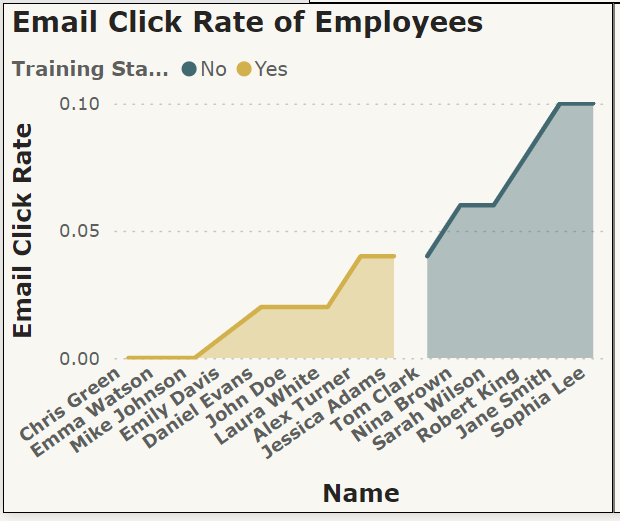
This bar chart shows the number of phishing emails clicked by individual employees, categorized by departments (Finance, HR, IT, Marketing, Sales). Bar charts effectively compare individual susceptibility to phishing emails. The chart reveals that Jane Smith, Sophia Lee, and Robert King from the Finance department have the highest number of clicks, suggesting a need for additional training and awareness programs in this department. Employees like Mike Johnson and Emma Watson have fewer clicks, indicating better phishing recognition skills. Identifying individuals with higher click rates enables targeted interventions to reduce phishing risks.

## Chart 2 – Average of Score by Name and Department



This bar chart shows the average training scores of individual employees, categorized by departments (Finance, HR, IT, Marketing, Sales). Bar charts effectively compare individual training performance. Chris Green, Mike Johnson, and Emily Davis have the highest average scores, indicating strong understanding and retention of training material. In contrast, Jessica Adams has the lowest average score, suggesting a need for further training. This insight helps tailor training programs to ensure all employees achieve satisfactory cybersecurity awareness levels. Identifying employees with varying scores enables targeted follow-up and support, enhancing overall training effectiveness.

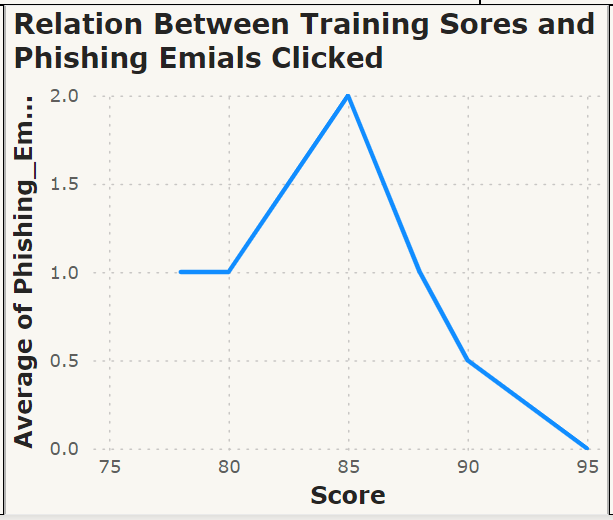
## Chart 3 – Email Click Rate of Employees



This line chart shows the email click rates of individual employees, segmented by training status ("Yes" for those trained and "No" for those untrained). Line charts effectively highlight differences between trained and untrained employees. The chart reveals that trained employees generally have lower click rates, while untrained employees like Jane Smith and Sophia Lee have the highest rates. This suggests that training significantly reduces phishing email clicks. Identifying these patterns helps evaluate training effectiveness and pinpoint employees needing additional support to improve cybersecurity awareness.

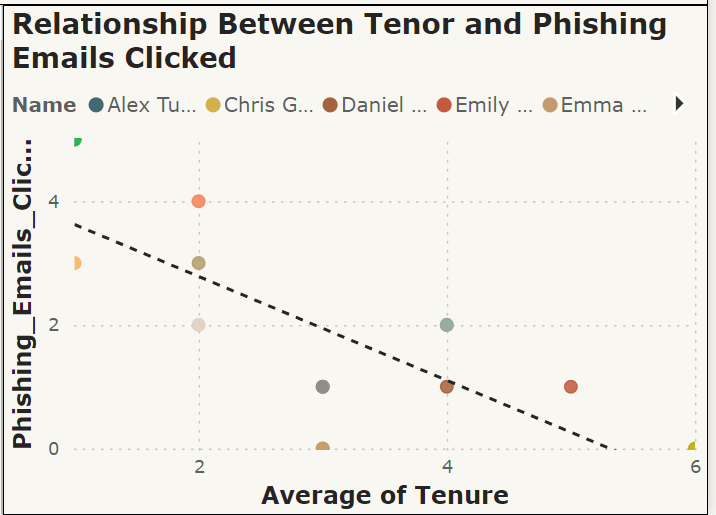
## 

## Chart 4 – Relation between Training Scores and Phishing Emails Clicked



This line chart depicts the relationship between employees' training scores and the average number of phishing emails they clicked. Line charts effectively highlight trends between training performance and phishing susceptibility. The chart shows that employees with higher training scores generally click fewer phishing emails, particularly those scoring above 90. However, there is a peak around a score of 85, where the average number of clicks is highest. This suggests that while higher scores correlate with better phishing recognition, mid-range scores may require additional attention. This insight aids in refining training programs to address specific vulnerabilities.

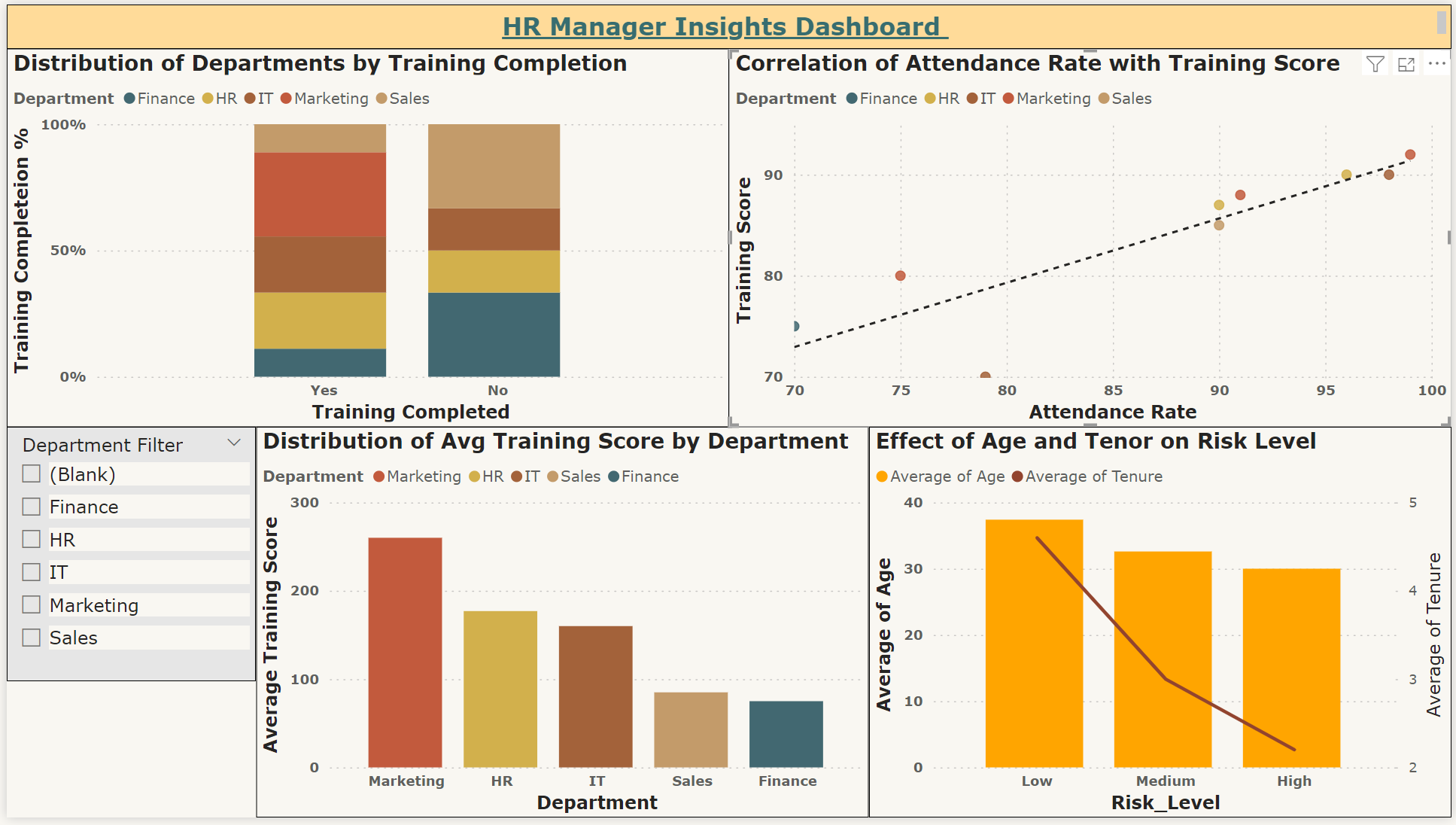
## Chart 5 – Relationship between Tenure and Phishing Emails Clicked



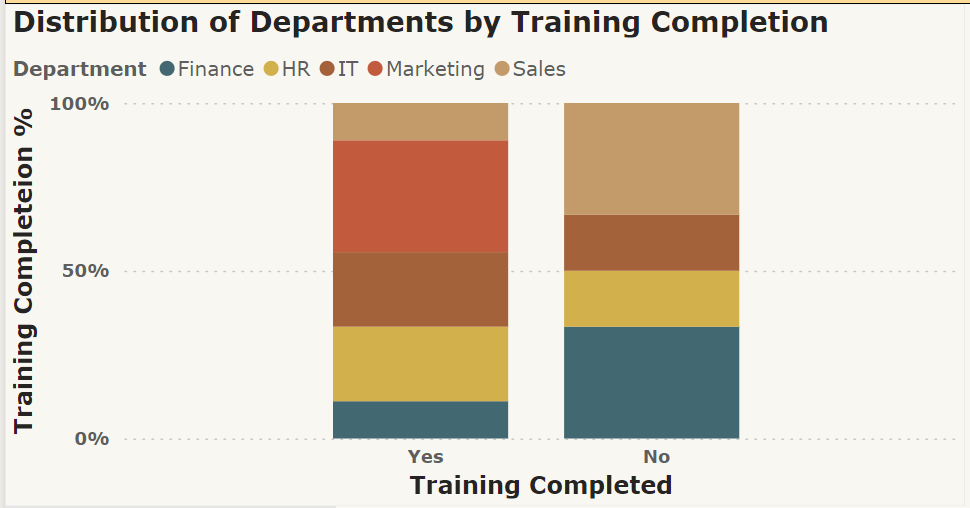
This scatter plot shows the relationship between the average tenure of employees and the number of phishing emails they clicked. Each dot represents an employee, with the x-axis showing tenure and the y-axis showing the number of clicks. The trend line reveals a negative correlation, indicating that employees with longer tenures tend to click fewer phishing emails. This suggests that more experienced employees may have better phishing recognition skills due to greater exposure to training and awareness programs. This insight helps tailor training programs to enhance phishing recognition skills among newer employees.

# Dashboard 3: HR Manager Insights Dashboard

The HR Manager Insights Dashboard is designed to provide a comprehensive view of training performance and its impact on cybersecurity awareness, enabling stakeholders to make informed decisions. The summary metrics at the top offer a quick snapshot of overall training completion and effectiveness. Central charts highlight the distribution of training completion across departments and the positive correlation between attendance rates and training scores, essential for identifying areas needing improvement. Charts at the bottom focus on average training scores by department and the effect of age and tenure on risk levels, helping to pinpoint which departments and employee demographics require targeted training. The interactive department filter allows users to focus on specific departments, making the dashboard adaptable to various stakeholder needs. Increasing phishing awareness is becoming increasing urgent (Yeoh et al., 2021) and this logical layout ensures stakeholders can easily navigate and extract meaningful insights, facilitating the development of targeted training and support initiatives to enhance the organization’s overall cybersecurity posture

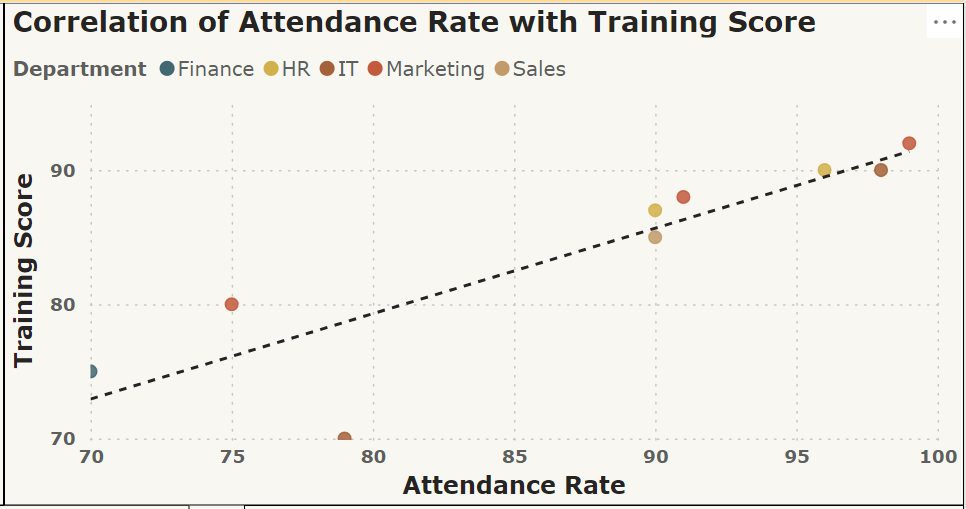
****

## Chart 1 – Distribution of Departments by Training Completion



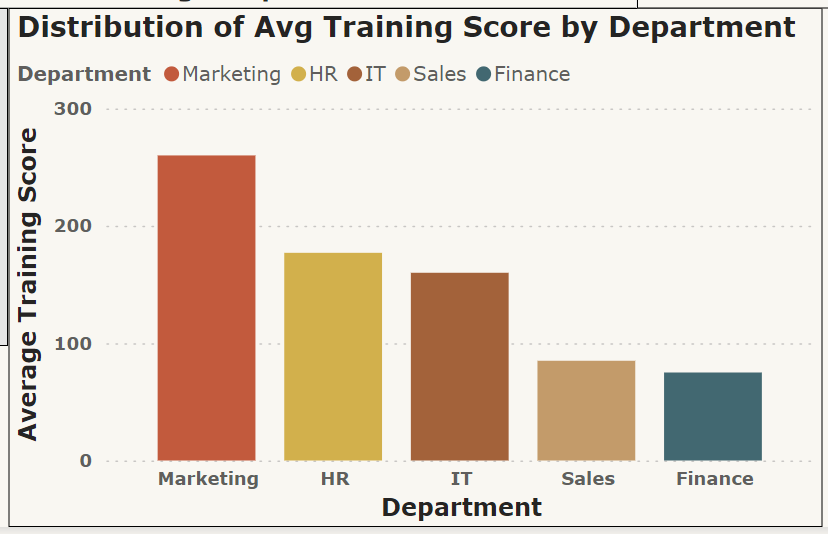
This stacked bar chart compares training completion across departments (Finance, HR, IT, Marketing, Sales), showing the proportions of employees who have completed the training ("Yes") versus those who have not ("No"). Stacked bar charts effectively visualize these proportions within each group. The chart reveals that the IT and Finance departments have higher training completion rates, while the Sales department has a significant portion of untrained employees. This suggests a need for targeted efforts to increase training completion, especially in the Sales department, to ensure consistent cybersecurity awareness across the organization.

## Chart 2 – Correlation of Attendance Rate with Training Score



This scatter plot shows the correlation between training attendance rates and training scores across departments (Finance, HR, IT, Marketing, Sales). Each dot represents an employee, with the x-axis showing attendance rates and the y-axis showing training scores. The trend line indicates a positive correlation, suggesting that higher attendance rates generally lead to higher training scores. This visualization highlights the importance of regular training attendance in achieving better training outcomes. Departments and employees with lower attendance and scores may need additional support to improve participation and performance, ensuring consistent cybersecurity awareness across the organization.

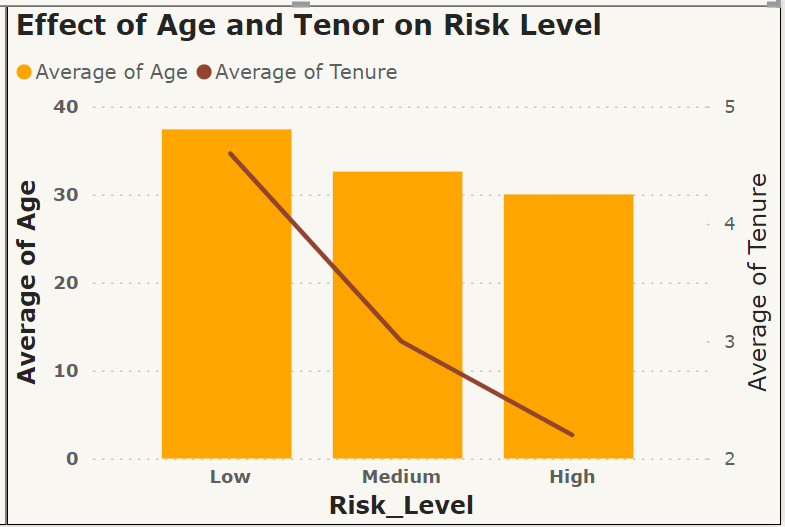
## Chart 3 – Distribution of Avg. Training Score by Department



This bar chart compares average training scores across departments (Marketing, HR, IT, Sales, Finance). Bar charts effectively highlight performance differences. The chart shows that the Marketing department has the highest average training score, followed by HR and IT, while the Sales and Finance departments have lower scores. This suggests that while some departments excel in training, others, particularly Sales and Finance, may need additional support to improve outcomes. Identifying these disparities helps direct resources and efforts where they are most needed to ensure uniform cybersecurity awareness and competency across the organization.

## 

## Chart 4 – Effect of Age and Tenure on Risk Level



This combined bar and line chart shows the effect of age and tenure on risk levels (Low, Medium, High). The bars represent average age, while the line represents average tenure. The chart reveals that employees with lower risk levels tend to be older and have longer tenures, while those with higher risk levels are younger and have shorter tenures. This suggests that experience and age contribute to lower susceptibility to risks. Targeted training for younger and less experienced employees is recommended to reduce their risk levels and enhance overall cybersecurity.

# Recommendations

The following recommendations are based on the insights derived from the HR Manager Insights Dashboard, Individual User Performance Dashboard, and Phishing Campaign Manager Dashboard. These strategies aim to enhance overall cybersecurity awareness, training effectiveness, and resource optimization across the organization.

## Recommendations - Phishing Campaign Manager

To enhance the overall effectiveness of phishing campaigns, the following recommendations are proposed:

* Shift budgets from less effective campaigns like CyberSafe Sweepstakes to more engaging ones such as PhishLock Drive.
* Tailor programs to address specific phishing tactics employees are most susceptible to, improving resilience across all departments.
* Target the IT department with specific training and additional security measures due to its higher susceptibility.
* Use insights from successful campaigns like PhishLock Drive and TrustGuard Initiative to ensure efficient resource use.
* Continuously monitor campaign performance and adjust strategies based on real-time data to maintain and improve the organization's security posture.

## Recommendations - Individual User Performance

To enhance phishing awareness and reduce risks, the following actions are recommended:

* Focus on employees with mid-range scores to address specific vulnerabilities.
* Target high-risk individuals and departments, such as Finance, with personalized sessions and regular follow-ups.
* Use experienced employees as mentors, sharing best practices and conducting peer-led training sessions.
* Track performance and provide real-time feedback, reinforcing training with periodic refresher courses.
* Tailor training to address the unique needs of each department.
* Promote continuous learning, encourage the reporting of phishing attempts, and make cybersecurity a shared responsibility.

## Recommendations - HR Manager Insights

Based on the insights from the HR Manager Insights Dashboard, the following recommendations are proposed:

* Focus on departments with lower training completion rates, particularly the Sales department, to ensure consistent cybersecurity awareness.
* Highlight the importance of regular attendance, as higher attendance rates correlate with better training scores.
* Offer extra support to departments like Sales and Finance, which have lower average training scores, to enhance their performance.
* Implement targeted interventions for younger and less tenured employees, who are at higher risk levels, to reduce their susceptibility to phishing attacks.
* Utilize experienced employees as mentors to improve overall cybersecurity awareness across the organization.

# References

Volkamer, M., Sasse, M. A., & Boehm, F. (2020). Analysing Simulated Phishing Campaigns for Staff. *Computer Security*, *12580*, 312–328. <https://doi.org/10.1007/978-3-030-66504-3_19>

Yeoh, W., Huang, H., Lee, W.-S., Al Jafari, F., & Mansson, R. (2021). Simulated Phishing Attack and Embedded Training Campaign. *Journal of Computer Information Systems*, *62*(4), 1–20. <https://doi.org/10.1080/08874417.2021.1919941>

Baillon, A., de Bruin, J., Emirmahmutoglu, A., van de Veer, E., & van Dijk, B. (2019).

*PLOS ONE*, *14*(12), e0224216. <https://doi.org/10.1371/journal.pone.0224216>

Chris, Richa, Denise, & Ratul. (2024, March 15). *Simulate a phishing attack with Attack simulation training - Office 365*. Learn.microsoft.com. <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-simulations?view=o365-worldwide>

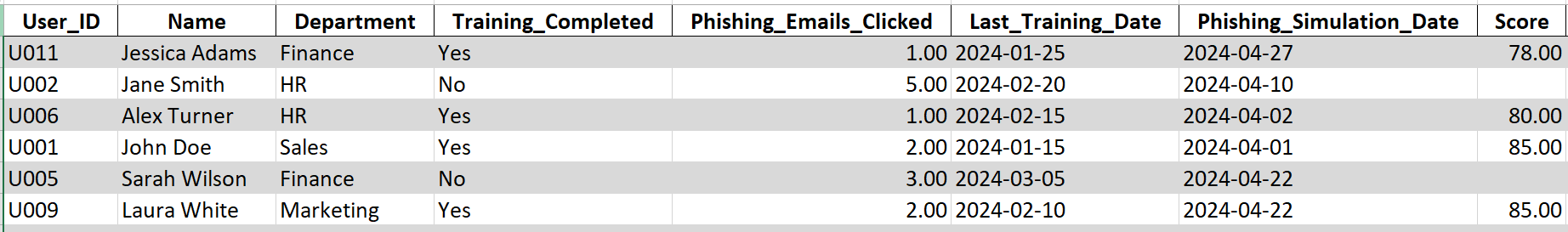
# Appendix

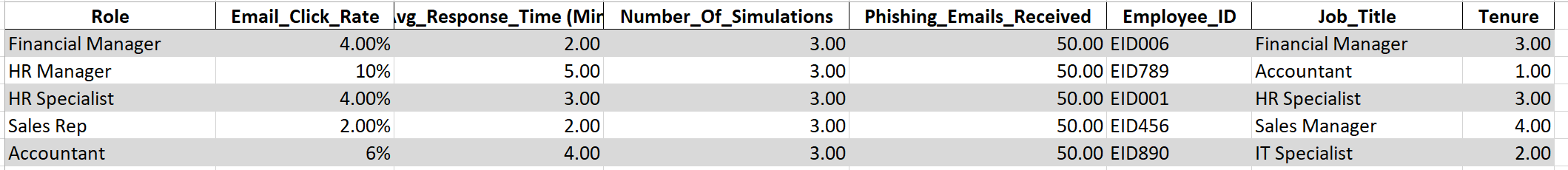
**A) Power BI Essential Training LinkedIn Course**



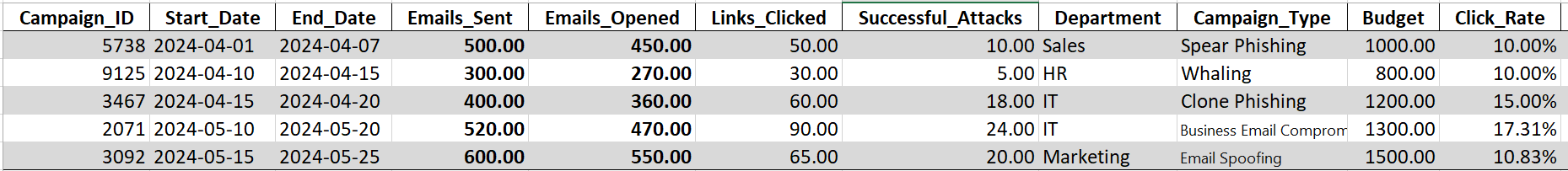
B) Dataset used to build the dashboards

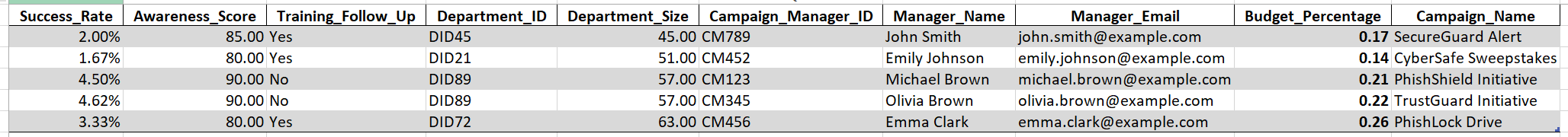
1. Individual User Performance





1. Phishing Campaign Manager





1. HR Manager Insights

