****

**MIS781 – Business Intelligence and Database – Trimester 1 2024Assessment Task 2 – Individual Assignment: Business Intelligence Solution Development and Report**

2024



**Anagha PRASHANTH RAJE URS**

**S223709844**

# Table of content

[Introduction­­­­­­­­­­­­­­­ ……………………………………………………………………………………………………2](#_bookmark0)

[Objectives of your BI Dashboards …………………………………………………………………………2](#_bookmark1)

[Benefits/Advantages of your BI Dashboards .………………………………………………………. 2](#_bookmark2)

[Assumptions](#_bookmark3) ……………………………………………………………………………………………………………… 3

[Description of business rules and of variables used in this report .………………………](#_bookmark4).. 5

[Dashboard 1](#_bookmark6), Chart 1.1 …………………………………………………………………………………………………6

Chart 1.2, Chart 1.3 …………………………………………………………………………………………………………7

Chart 1.4, Chart 1.5 …………………………………………………………………………………………………………8

[Dashboard 2](#_bookmark10), Chart 2.1 ………………………………………………………………………………………………….9

Chart 2.2, Chart 2.3 …………………………………………………………………………………………………………10

Chart 2.4, [Dashboard 3](#_bookmark12) ………………………………………………………………………………………………….11

Chart 3.1, Chart 3.2 …………………………………………………………………………………………………………12

Chart 3.3, Chart 3.4 …………………………………………………………………………………………………………13

Chart 3.5, [Recommendations …………………………………………………………………………………14](#_bookmark14)

[Reference](#_bookmark15) ……………………………………………………………………………………………………………………16

Appendix (Certificate and Datasets) …………………………………………………………………………….17

Introduction

This report presents the analysis of simulated phishing campaigns conducted across Victoria, Australia, targeting campaign managers, HR personnel, and individual users. Utilizing MS Power BI, the report showcases various dashboards that visualize user interactions and responses to these phishing attempts. The insights derived from these dashboards aim to enhance understanding of phishing vulnerability among different user groups and inform strategies to improve cybersecurity measures. The visualizations and subsequent analyses offer valuable perspectives on user behaviour, facilitating informed decision-making in cybersecurity practices

## Objectives of your BI Dashboards

**Objective 1 (for Phishing Campaign Manager):** The objective of analysing the campaign manager dataset is to evaluate the effectiveness of various phishing campaigns conducted across different departments. This includes measuring key metrics such as emails sent, emails opened, links clicked, attachments downloaded, reported phishing incidents, and compromised accounts. By understanding these metrics, we aim to identify trends, departmental vulnerabilities, and the overall impact of each campaign on employee behaviour and security awareness.

**Objective 2 (for User):** The objective of analysing the HR dataset is to assess the interaction of employees with phishing emails in terms of their opening rates, link clicking behaviour, credential submission, and reporting of phishing attempts. This dataset will help in understanding the susceptibility of employees across different departments and positions, as well as the effectiveness of completed training programs. The analysis will provide insights into areas requiring additional training and support to enhance cybersecurity resilience.

**Objective 3 (for HR Manager):** The objective of analysing the individual user dataset is to gain a detailed understanding of individual behaviours and responses to phishing campaigns. This includes tracking specific user actions such as link clicks, credential submissions, and phishing report rates. The dataset also captures training completion status and associated risk scores, which will help in identifying high-risk individuals and tailoring personalized training interventions to reduce the likelihood of successful phishing attacks

## Benefits/Advantages of your BI Dashboards

**Campaign Manager**: The Campaign Manager Dashboard provides comprehensive insights into the effectiveness of phishing campaigns across different departments. By visualizing key metrics such as emails sent, opened, links clicked, and compromised accounts, it helps identify departmental vulnerabilities and the impact of phishing attempts. The geographic distribution of link clicks aids in understanding regional risks, while the breakdown of reported phishing incidents and compromised accounts supports targeted training and prevention strategies. This dashboard is crucial for optimizing cybersecurity efforts and enhancing overall organizational resilience against phishing attacks

**Individual User:** provides a detailed analysis of user behaviour in response to phishing attempts. By visualizing training completion, reported phishing incidents, and risk scores by department, it helps identify the effectiveness of training programs and pinpoint high-risk areas. The dashboard also highlights link-clicking behaviour and employee tenure, offering insights into the correlation between experience and phishing susceptibility. These insights are crucial for tailoring training programs, improving user awareness, and enhancing overall organizational cybersecurity posture.

**HR:** It provides crucial insights into employee interactions with phishing emails, focusing on link clicks, training completion, and phishing reports by department and position. It helps HR identify departments and roles with higher susceptibility to phishing attacks, allowing for targeted training and intervention. The geographic visualization of link clicks highlights regional vulnerabilities. By analysing the effectiveness of training programs, the dashboard aids in enhancing cybersecurity awareness and reducing risk, ultimately strengthening the organization’s overall defence against phishing threats.

Assumptions

## Campaign manager:

1. **CampaignID:** Unique identifier for each phishing campaign. Assumed to be auto incremented and unique.
2. **CampaignName**: Descriptive name of the campaign. Assumed to reflect the targeted department or nature of the phishing attempt.
3. Department: The department targeted by the phishing campaign. Assumed to be correctly recorded and essential for analysis of departmental susceptibility.
4. **EmailSent**: Total number of phishing emails sent during the campaign. Assumed to be accurate and verified by the campaign manager.
5. **EmailsOpened**: Number of emails opened by recipients. Assumed to be tracked via read receipts or similar mechanisms.
6. **LinksClicked**: Number of times recipients clicked on links within the phishing emails. Assumed to be tracked by the campaign's embedded URL tracking system.
7. **AttachmentsDownloaded**: Number of times attachments in phishing emails were downloaded. Assumed to be monitored through email server logs.
8. **ReportedPhish**: Number of recipients who reported the phishing attempt. Assumed to be collected through internal reporting mechanisms.
9. **CompromisedAccounts**: Number of accounts compromised as a result of the phishing campaign. Assumed to be determined through security incident reports.
10. **CampaignDurationDays**: Duration of the campaign in days. Assumed to be accurately recorded from the campaign's start to end date.
11. **EmployeeID**: Unique identifier for each employee targeted by the campaign. Assumed to be unique and mapped correctly to employee records.
12. **City**: Location of the targeted employees. Assumed to be relevant for geographical analysis of phishing susceptibility.

Individual User

1. **User ID:** Unique identifier for each user. Assumed to be auto incremented and unique for each participant.
2. **Name**: The full name of the user. Assumed to be accurately recorded for identification and reporting purposes.
3. **Department**: The department in which the user works. Assumed to be correct and important for analysing departmental vulnerability to phishing.
4. **City**: The city where the user is located. Assumed to be accurate and relevant for geographic analysis of phishing susceptibility.
5. **Campaign ID:** Unique identifier for each phishing campaign. Assumed to be auto incremented and unique for each campaign.
6. **Campaign Name:** The name of the phishing campaign. Assumed to reflect the nature of the phishing attempt.
7. **Phishing Email Type:** The type of phishing email sent. Assumed to be correctly categorized to understand different phishing techniques.
8. **Employee Tenure**: The number of years the user has been employed. Assumed to be accurate and relevant for analysing susceptibility based on experience.
9. **Clicked Link**: Indicates whether the user clicked on a phishing link (1 for yes, 0 for no). Assumed to be accurately tracked.
10. **Submitted Credentials**: Indicates whether the user submitted their credentials (1 for yes, 0 for no). Assumed to be accurately tracked.
11. **Report Phishing:** Indicates whether the user reported the phishing attempt (1 for yes, 0 for no). Assumed to be collected through internal reporting mechanisms.
12. **Training Completed:** Indicates whether the user completed phishing awareness training (1 for yes, 0 for no). Assumed to be accurately recorded.
13. **Risk Score**: A numerical score representing the user's susceptibility to phishing. Assumed to be calculated based on user actions and other risk factors.

HR Manager:

1. **EmployeeID**: Unique identifier for each HR manager. Assumed to be auto incremented and unique for each participant.
2. **FullName**: The full name of the HR manager. Assumed to be accurately recorded for identification and reporting purposes.
3. **Department**: The department in which the HR manager works. Assumed to be correct and important for departmental analysis.
4. **Position**: The job position of the HR manager. Assumed to be accurately recorded to understand susceptibility based on job roles.
5. **City**: The city where the HR manager is located. Assumed to be accurate and relevant for geographic analysis.
6. **EmailSentDate**: The date when the phishing email was sent. Assumed to be accurately recorded to track the timeline of the campaign.
7. **EmailOpenedDate**: The date when the phishing email was opened. Assumed to be accurately tracked via email server logs.
8. **LinkClicked**: Indicates whether the HR manager clicked on a phishing link (1 for yes, 0 for no). Assumed to be accurately tracked.
9. **CredentialsEntered**: Indicates whether the HR manager submitted their credentials (1 for yes, 0 for no). Assumed to be accurately tracked.
10. **ReportPhishing**: Indicates whether the HR manager reported the phishing attempt (1 for yes, 0 for no). Assumed to be collected through internal reporting mechanisms.
11. **TrainingCompleted**: Indicates whether the HR manager completed phishing awareness training (1 for yes, 0 for no). Assumed to be accurately recorded.
12. **PhishingEmailType**: The type of phishing email used in the campaign. Assumed to be correctly categorized to analyse different phishing techniques.

Description of business rules and variables used in this report.

**1.Campaign manager:** A screenshot of a computer

Description automatically generated

**2. Individual UserA screenshot of a computer

Description automatically generated**

**3.HR**

**A screenshot of a computer

Description automatically generated**

**Dashboards**

**Dashboard 1: For Phishing Campaign Manager**

This dashboard offers a detailed analysis of phishing campaigns managed by the campaign team. The bar chart highlights departmental engagement by comparing emails sent and opened. The map visualizes the geographical spread of clicked links, pinpointing areas of higher susceptibility. The pie chart breaks down the interactions, comparing links clicked, attachments downloaded, and phishing reports. The line chart provides insights into departmental awareness and vulnerability by contrasting reported phishing incidents with compromised accounts. The tree map offers a comprehensive view of reporting behaviour and departmental size, showing the number of phishing reports and employee counts. Overall, this dashboard helps identify trends, pinpoint vulnerabilities, and enhance phishing awareness and response strategies.

A screenshot of a computer

Description automatically generated

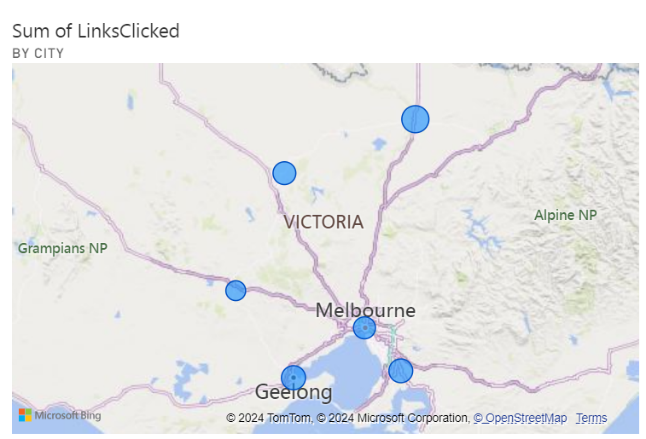
**Chart 1.1: Cluster Bar chart - Analysis of Emails sent and Emails opened with Department.**

A graph of blue bars

Description automatically generated

This bar chart shows the phishing campaign results by department, comparing the number of emails sent and opened. The Finance department received around 6,000 emails, with 4,000 opened. Marketing had 5,500 sent and 3,800 opened. Sales saw 5,000 emails sent and 3,500 opened. IT had 4,500 sent and 3,000 opened. HR had the lowest engagement with 3,000 emails sent and 2,000 opened. Finance and Marketing departments show the highest engagement, with a large proportion of emails being opened, indicating a higher risk of phishing threats. Sales and IT also have significant engagement but slightly lower than Finance and Marketing. The HR department shows the least engagement, suggesting lower exposure but also potentially lower awareness. This chart helps identify departments that need targeted phishing awareness and training programs.

**Chart 1.12: Map – Engagement between Links clicked in different cities of Victoria**

****

This map shows the highest engagement with phishing links in Melbourne and Geelong, indicating these cities are at higher risk for successful phishing attacks. Other cities in Victoria show moderate to low engagement. Insights suggest focusing phishing awareness and training efforts in Melbourne and Geelong, while monitoring other cities for potential increases in activity. This geographical analysis helps in deploying targeted cybersecurity measures and educational campaigns.

**Chart 1.3: Pie chart – Analysis of Links clicked, attachments downloaded and Reported phishing**

**A blue circle with a red line

Description automatically generated**

This pie chart visualizes the engagement with phishing emails, showing that the majority of actions are link clicks (68.31%, 6K), followed by attachment downloads (30.67%, 3K), with phishing reports being minimal (1.01%, 0K). The high link clicks rates indicate significant engagement with phishing content, posing a considerable risk. The notable amount of attachment downloads further heightens the potential threat. The very low rate of phishing reports suggests a pressing need for improved awareness and training among employees to encourage reporting and mitigate risks effectively.

**Chart 1.4: Line chart - Reported phishing incidents and compromised accounts by department**

**A graph with a line

Description automatically generated**

This line chart compares reported phishing incidents and compromised accounts by department. Finance has the highest reported phish (25) and compromised accounts (15), indicating high vulnerability despite awareness. Marketing and Sales show moderate reporting and compromises, suggesting balanced engagement and risk. IT has a sharp rise in compromised accounts (20) with fewer reports, highlighting a critical vulnerability. HR shows the least engagement with low reports and compromises. This phishing campaign analysis reveals departments needing targeted training, particularly IT, to improve awareness and reduce vulnerability. Understanding these dynamics allows for tailored training programs and security measures to be implemented where they are needed most, enhancing overall organizational security.

**Chart 1.5: Tree map**

**A screenshot of a computer

Description automatically generated**

This tree map compares reported phishing incidents and employee counts by department. Finance and Sales have the highest employee counts and reported phishing incidents, indicating higher engagement and awareness. Marketing and IT show moderate engagement, while HR has the lowest counts, suggesting lower exposure and awareness. To increase reporting, targeted training programs can be implemented, especially in HR and IT. Regular phishing simulations and awareness campaigns can also help improve vigilance and reporting rates across all departments. This comparison helps guide efforts to enhance phishing awareness and response strategies.

**Dashboard 2: For Individual Users**

This dashboard provides a comprehensive analysis of phishing susceptibility and training effectiveness across various departments. It includes visualizations such as a bar chart comparing training completion and reported phishing incidents, highlighting the impact of training programs. Another bar chart shows the sum of risk scores by department, identifying high-risk areas. A line chart compares employee tenure with risk scores to determine if experience correlates with better phishing awareness. Additionally, a pie chart displays the distribution of clicked phishing links across departments, pinpointing those most at risk. Overall, this dashboard aids in evaluating training effectiveness, identifying high-risk departments, and informing targeted security measures to improve cybersecurity.

A screenshot of a graph

Description automatically generated

**Chart 2.1: Cluster Bar chart**

**A graph of blue rectangular bars

Description automatically generated with medium confidence**

This chart compares training completions (light blue) and phishing reports (dark blue) across departments. The Operations department shows high training (12) and reporting (15), indicating effective training programs. Finance has balanced training (9) and reporting (9) numbers, while IT has high reporting (18) despite moderate training (11), suggesting high vigilance. HR shows fewer training completions (7) but significant reporting (10), indicating high awareness. Marketing has low training (5) and reporting (8), pointing to a need for more training efforts. Sales exhibits moderate training (8) and balanced reporting (9) numbers. Overall, higher training completions generally correlate with increased phishing reports, demonstrating the effectiveness of training programs, particularly in IT and Operations.

**Chart 2.2: Cluster column chart**

**A blue bar graph with white text

Description automatically generated**

This bar chart displays the sum of risk scores by department. The Finance department has the highest risk score (around 1050), followed by Operations (1000), Marketing (850), HR (800), Sales (700), and IT (650). Finance's high-risk score suggests significant vulnerability, requiring targeted interventions. Operations and Marketing also show elevated risk, indicating areas needing enhanced training and security measures. The relatively lower risk score in IT (650) may reflect better awareness and practices, possibly due to the technical nature of their roles. Overall, this chart highlights departments that need focused efforts to mitigate phishing risks.

**Chart 2.3: Pie chart**

**A colorful pie chart with numbers

Description automatically generated**

This pie chart shows the distribution of clicked phishing links by department. Marketing leads with 12 clicks (27.27%), followed by Finance with 10 clicks (22.73%), Sales with 9 clicks (20.45%), HR with 8 clicks (18.18%), IT with 3 clicks (6.82%), and Operations with 2 clicks (4.55%). The high click rates in Marketing, Finance, and Sales suggest these departments are more susceptible to phishing attacks, indicating a need for targeted awareness training and increased vigilance. Conversely, IT and Operations have the lowest click rates, reflecting better phishing awareness or more effective training programs. This chart highlights the need for additional training and vigilance in Marketing, Finance, and Sales departments to reduce phishing risks.

**Chart 2.4: Line graph**

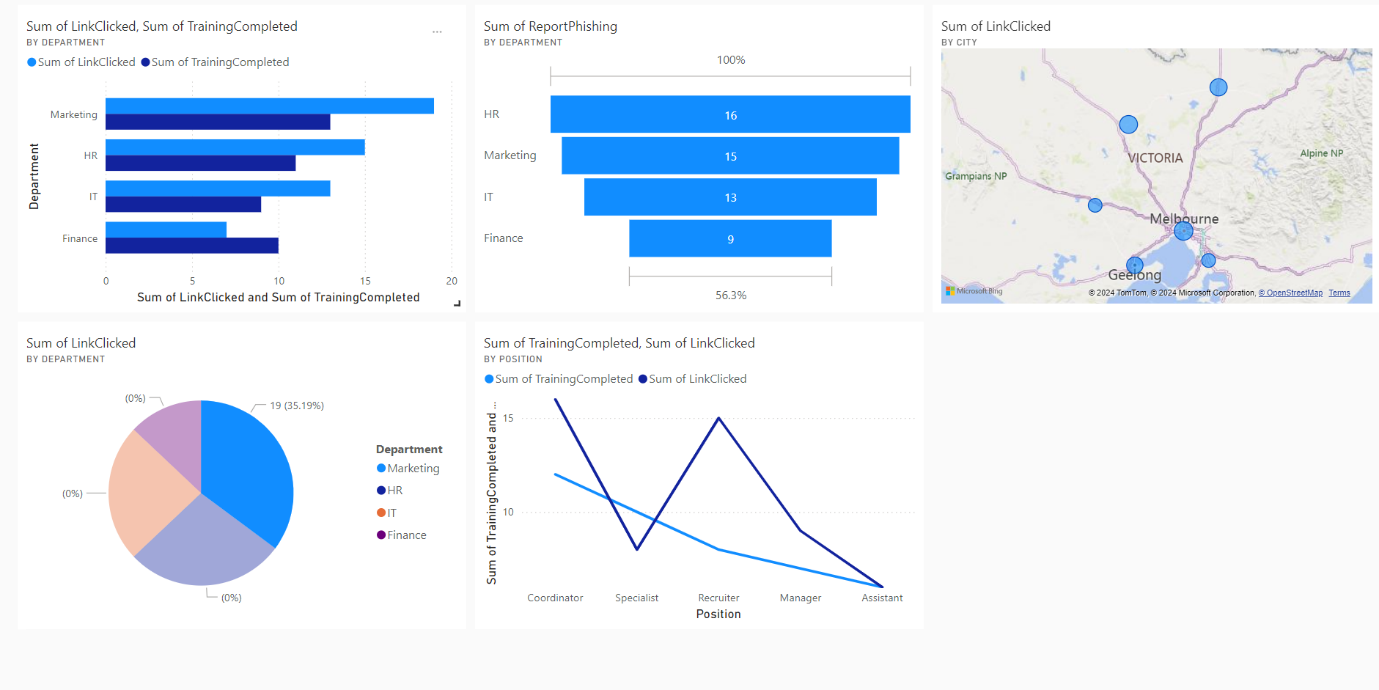
**A graph showing the number of employees

Description automatically generated with medium confidence**

The chart compares the sum of employee tenure and the sum of risk scores by department. Finance has the highest risk score (1000) and longest employee tenure, suggesting potential complacency despite experience. Operations also shows high risk (around 950) and tenure, indicating a similar issue. Marketing and HR have moderate risk scores (800 and 700 respectively) with lower tenure, reflecting a balanced but concerning risk level. IT has the lowest risk score (around 500) but also the lowest tenure, suggesting new hires might be better trained or more vigilant. This comparison helps identify departments where additional training and vigilance are necessary to reduce phishing risks, particularly in Finance and Operations.

**Dashboard 3: For HR manager**

This phishing campaign dashboard provides a comprehensive analysis of phishing susceptibility and training effectiveness across various departments. It includes visualizations such as a bar chart comparing training completion and link clicked, highlighting the impact of training programs. Another bar chart shows the sum of reported phishing incidents by department, identifying areas with better awareness. A line chart compares positions with link clicked and training completion, evaluating the training's impact on different roles. Additionally, a pie chart displays the distribution of clicked phishing links across departments, pinpointing high-risk areas. Overall, this dashboard aids in evaluating training effectiveness, identifying high-risk departments, and informing targeted security measures to improve cybersecurity.

****

**Chart 3.1: Clustered Bar chart**

**A graph with blue bars

Description automatically generated**

This chart compares the sum of link clicks and training completions across departments. Marketing has the highest link clicks (18) and training completions (16), indicating a need for enhanced training despite high completion rates. HR has 15 clicks and 10 completions, suggesting effective training reduced clicks. IT shows 14 clicks and 7 completions, requiring more targeted training. Finance has 8 clicks and 9 completions, indicating training effectiveness. The chart highlights the need for continuous, department-specific training in Marketing, IT, and HR to reduce phishing link clicks.

**Chart 3.2: Funnel chart**

**A graph with blue rectangular bars

Description automatically generated with medium confidence**

This funnel chart visualizes the number of reported phishing incidents by department. HR leads with 16 reports, indicating strong awareness and response, while Marketing follows closely with 15. IT has 13 reports, showing moderate awareness, and Finance lags with only 9 reports, highlighting a significant gap. To improve overall cybersecurity, Finance requires targeted training to enhance phishing awareness and reporting. IT should also receive additional training to boost their reporting rates. Marketing and HR should maintain their current training programs and explore ways to sustain high performance. Continuous improvement of training content and department-specific interventions are recommended to address emerging phishing tactics and ensure comprehensive coverage and effectiveness across the organization.

**Chart 3.3: Map**

A map with blue dots

Description automatically generated

This map chart visualizes the sum of phishing link clicks across various cities in Victoria, Australia. Melbourne has the highest number of clicks (20), followed by Geelong (15), Ballarat (10), and Bendigo (8). Other cities like Cranbourne and Shepperton also show significant clicks (7 and 6 respectively). This chart highlights the need for targeted phishing awareness and training programs in Melbourne and Geelong to reduce click rates. Smaller cities should not be neglected, as their click rates indicate vulnerability. By focusing on these geographic areas, the organization can implement more effective, location-specific training to mitigate phishing risks.

**Chart 3.4:**

**A pie chart with numbers and a few different colored circles

Description automatically generated with medium confidence**

This pie chart visualizes the sum of phishing link clicks by department. Marketing has the highest number of clicks (19, 35.19%), followed by HR (15, 27.78%), IT (13, 24.07%), and Finance (7, 12.96%). The chart highlights Marketing and HR as the most susceptible to phishing attacks, indicating a need for intensive, tailored training sessions for these departments. IT also requires additional training to boost awareness and resilience. While Finance has the fewest clicks, continuous monitoring and ongoing training are essential to maintain and improve their performance. Targeted training efforts across all departments will help reduce phishing link clicks and enhance overall cybersecurity.

**Chart 3.5:**

A graph with blue lines

Description automatically generated

This line chart compares the sum of training completions and link clicks across different positions. Coordinators have the highest link clicks (16) despite 12 training completions, highlighting the need for more effective, position-specific training. Specialists show 11 clicks and 10 completions, indicating relatively good training effectiveness with room for improvement. Recruiters have 15 clicks and only 9 completions, suggesting significant training gaps. Managers have balanced figures with 8 clicks and 8 completions, showing moderate training effectiveness. Assistants have the fewest clicks (6) and 7 completions, indicating successful training outcomes. The chart emphasizes the need for targeted, enhanced training programs, especially for high-risk positions like coordinators and recruiters, to reduce phishing susceptibility.

**Recommendations**

Dashboard 1

1: Implement Comprehensive Phishing Awareness Training

**Justification:** The bar chart shows high engagement with phishing emails in Finance and Marketing, indicating higher risk. The tree map reveals low engagement and reporting rates in HR.

**Action:** Conduct department-specific training sessions to improve phishing awareness and reduce risk, involving department heads and the IT Security Team.

2: Develop and Promote Enhanced Phishing Reporting Tools

**Justification:** The pie chart shows a low rate of reported phishing incidents, suggesting unawareness of reporting mechanisms.

**Action:** Introduce user-friendly reporting tools and encourage prompt phishing incident reporting can enhance early detection and mitigation, involving the IT Security Team and all employees.

3: Targeted Geographical and Department Training

**Justification:** The map indicates high engagement with phishing links in Melbourne and Geelong, while the line chart shows critical vulnerabilities in IT. Localized and department-specific training can address these risks.

**Action:** Implement targeted training in high-risk locations and conduct regular phishing simulations in critical departments, involving regional managers and the IT Department Head.

Dashboard 2

1.Implement Refresher Training for Long-Tenured Employees

**Justification**: The line chart shows high risk scores despite long tenure in Finance and Operations.

**Action**: Conduct regular refresher training sessions for long-tenured employees that will help maintain high awareness levels, involving department heads and the HR Training Team.

2. Prioritize Phishing Awareness Training in High-Risk Departments

**Justification**: The pie chart indicates high click rates in Marketing, Finance, and Sales. Using real-world phishing examples can make the training more relevant and impactful.

**Action**: Prioritize phishing awareness training in these high-risk departments, department heads and the IT Security Team.

3. Enhance Employee Engagement with Reporting Mechanisms

**Justification**: The low rate of reported phishing incidents in the pie chart suggests unawareness of reporting mechanisms. Improved reporting tools and awareness campaigns can enhance early detection and mitigation.

**Action**: Introduce user-friendly reporting tools and encourage prompt phishing incident reporting, involving the IT Security Team and all employees.

Dashboard 3

1.Implement Interactive Training Modules for Coordinators and Recruiters

Justification: The line chart shows high link click rates among coordinators (16 clicks) and recruiters (15 clicks), despite significant training completions (12 and 9, respectively). This indicates a need for more effective, engaging training methods.

Action: Develop interactive, position-specific training modules for coordinators and recruiters. These modules should include realistic phishing simulations and scenario-based learning. Involve department heads and the HR Training Team to ensure training is relevant and impactful.

2. Conduct Regular Refresher Courses for Specialists

Justification: Specialists have a moderate number of link clicks (11) and training completions (10), indicating a relatively good but improvable training effectiveness.

Action: Implement periodic refresher courses for specialists to reinforce phishing awareness. Use advanced phishing simulations to keep the training challenging and engaging. Collaborate with the HR Training Team and IT Security Team to maintain high training standards.

3. Targeted Phishing Awareness Campaigns for Marketing and HR

Justification: The pie chart indicates high click rates in Marketing (19 clicks, 35.19%) and HR (15 clicks, 27.78%), highlighting these departments as high-risk areas.

Action: Prioritize phishing awareness campaigns in Marketing and HR departments. Utilize real-world phishing examples and department-specific scenarios to enhance relevance. Involve department heads and the IT Security Team to tailor the campaigns effectively.

Reference:

Mimecast. (n.d.). *Customer community*. https://community.mimecast.com/s/article/awareness-training-managin Mimecast. (n.d.). Customer community. <https://community.mimecast.com/s/article/awareness-training-managing-campaignsg-campaigns>

Phishing Awareness Training for employees: Best Practices | ProofPoint AU. (2024, May 17). Proofpoint. <https://www.proofpoint.com/au/blog/security-awareness-training/phishing-awareness-training-best-practices-your-employees>

Top nine phishing simulators | Infosec. (n.d.). <https://www.infosecinstitute.com/resources/phishing/top-9-free-phishing-simulators/>

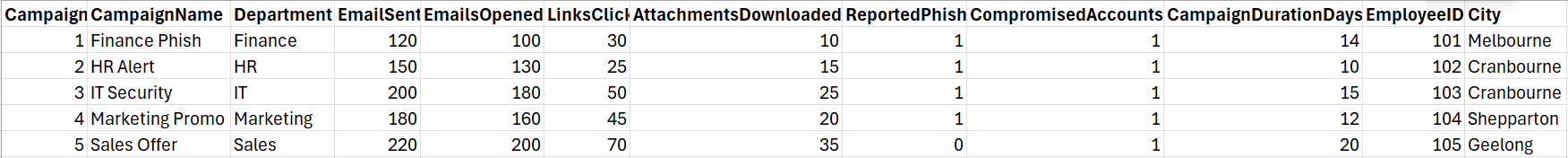
Phishing Awareness Training: Simulating Phishing Attacks. (n.d.). Rapid7. <https://www.rapid7.com/solutions/phishing-awareness-training/>

Appendix: Certificate and datasets

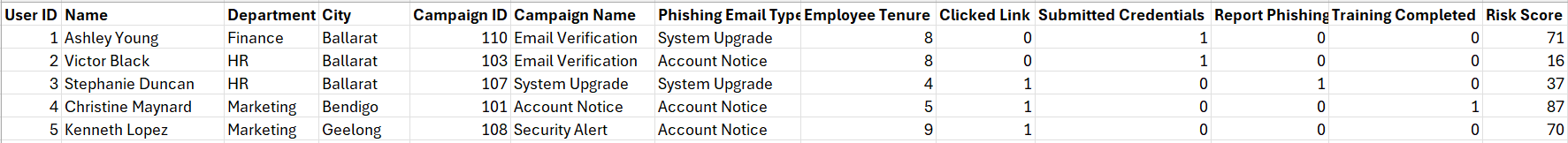
A screenshot of a certificate

Description automatically generated

Dataset 1: Campaign Manager



Dataset 2: Individual User



Dataset 3: HR manager

