Scenario: SecureBank

Business Intelligence Solution Report

Assessment 2: Individual

Himanshi Sachdeva (224850909)

MIS781 Business Intelligence and Database

Table of content

Contents

1. Introduction

In the digital age, cyberattacks such as phishing remain one of the most prevalent and damaging threats to organizational security. Phishing attacks exploit human vulnerabilities, making employee behavior a critical component in any cybersecurity strategy. To address this challenge, **SecureBank**, a major financial institution, initiated simulated phishing campaigns across its workforce. The aim was to assess employee awareness, gauge training effectiveness, and track IT response actions in order to proactively strengthen its security posture.

This business intelligence (BI) report outlines a data-driven solution designed to support three key stakeholders within SecureBank: the **Phishing Campaign Manager**, the **Human Resources (HR) Manager**, and the **IT Security Team**. Each stakeholder plays a distinct role in managing phishing risk—whether it's monitoring simulation results, enforcing training compliance, or coordinating timely incident responses.

1.1 Objectives of the BI Dashboards

This BI solution comprises three tailored dashboards designed to address the distinct needs of SecureBank's operational stakeholders. Each dashboard transforms complex phishing simulation data into actionable insights, with the ultimate goal of minimizing human vulnerabilities and enhancing security responsiveness.

Phishing Campaign Manager Dashboard
The objective of the Phishing Campaign Manager dashboard is to provide a comprehensive overview of employee engagement with simulated phishing campaigns. This dashboard helps the campaign manager to:

- Track overall exposure by monitoring who clicked phishing links and entered credentials
- Evaluate the effectiveness of each campaign over time
- Identify departments that are consistently at higher risk
- Understand employee reporting behavior to assess awareness and responsiveness
- Use behavioral patterns to design more targeted and realistic future simulations

By doing so, the dashboard supports the development of smarter, data-driven phishing campaigns that improve training relevance and reduce successful phishing attempts.

HR Manager Dashboard
The HR Manager dashboard is designed to monitor employee readiness, compliance with security training, and behavioral risk across departments and job roles. The key objectives of this dashboard are to:

- Evaluate phishing awareness training completion rates across teams
- Identify job titles and departments with higher risk based on click and credential entry behavior
- Detect repeat offenders to enable focused retraining or intervention
- Assess whether training completion correlates with safer behavior in phishing simulations

This dashboard empowers HR to take a proactive role in shaping a security-conscious workforce by aligning training strategy with observed behaviours and risks.

IT Security Team Dashboard
The IT Security Team dashboard focuses on managing and monitoring responses to phishing incidents. It provides visibility into how the security team reacts to threats, enabling operational efficiency and accountability. Its objectives include:

- Track the volume and timing of IT responses to phishing incidents (e.g., password resets, training enforcement)
- Analyse action trends by type and by IT administrator
- Monitor the time lag between phishing email delivery and IT action
- Provide a detailed incident log for investigation, reporting, or audits
- Enable filtering and deep dives by date, department, action type, or admin

Through this dashboard, the IT team can optimize its response workflow, ensure timely intervention, and maintain high standards in phishing incident management.

1.2 Benefits/Advantages of the BI Dashboards

The business intelligence solution developed for SecureBank offers several critical advantages by enabling stakeholders to access meaningful insights that guide proactive security decision-making. The following are the four most impactful benefits of the dashboards:

Stakeholder-Specific Insights for Targeted Action
Each dashboard is custom-designed to meet the information needs of a specific role—Phishing Campaign Manager, HR Manager, and IT Security Team. This ensures that each stakeholder receives relevant, role-appropriate insights that can directly inform policy, training, or incident response strategies.

Proactive Identification of High-Risk Behavior
By tracking metrics such as click-throughs, credential entries, and repeat offenders, the dashboards help identify individuals, job roles, or departments that exhibit risky behavior. This enables timely intervention, targeted training, and resource allocation before vulnerabilities escalate into actual breaches.

Clear Linkage Between Training and Behavioral Outcomes
The dashboards integrate training completion data with phishing simulation responses, enabling HR to evaluate whether training translates into safer behavior. This supports continuous improvement of training programs and ensures they are data-informed rather than assumption-driven.

Enhanced IT Response Monitoring and Accountability
The IT Security Team dashboard enables real-time monitoring of responses to phishing incidents, including time-to-response, action types, and admin workload. This enhances operational oversight, supports resource balancing, and strengthens compliance with security protocols.

1.3 Assumptions

The dashboards and analyses presented in this report are based on a synthetic dataset generated to reflect realistic phishing simulation scenarios within a financial institution. To ensure consistency, usability, and analytical relevance, the following assumptions were made during the design and development of the BI solution:

- Each Employee belongs to one Department and has one Job Title
- Each Phishing Simulation is Independent
- Training Status is Updated Per Simulation
- Security actions are logged only for simulations where users interacted with phishing emails.
- Dataset Reflects a Three-Month Simulation Window
- Each employee participates in multiple phishing simulations

1.4 Description of business rules and variables used in this report

Attribute	Data Type	Description	Business Rule
EmployeeID	Integer	Unique identifier for each employee	• Unique value • Not null
EmployeeName	String	Full name of the employee	• Used for display only • Not used in join relationships • Not null
Department	String	Department to which the employee belongs	• Must match controlled list of departments • Not null
JobTitle	String	Role of the employee	• Must match job title catalogue • Not null
Email	String	Work email address of the employee	• Must be valid and unique • Not null
Salary	Integer	Annual salary of the employee	• Must be a positive integer • May be used for HR segmentation or salary-risk trends • Not null

DepartmentHead	String	Name of the person managing the department	• Used for HR reporting only • optional in visualisations • Not null
PhishingID	Integer	Unique ID for each phishing simulation event	• Must be unique and linkable to EmployeeID • Not null
EmailSentDate	Date	Date phishing email was sent	• Must be within simulation period • Not null
ClickedLink	Boolean	Whether the employee clicked the phishing link	• TRUE/FALSE only • Not null
EnteredCredentials	Boolean	Whether the employee entered login credentials	• TRUE/FALSE only • TRUE only if ClickedLink = TRUE • Not null
ReportedPhishing	Boolean	Whether the employee reported the phishing email	• TRUE/FALSE only • Can occur independently • Not null
TrainingStatus	String	Training completion status at time of simulation	• Values must be either “Completed” or “Pending” • Not null
SecurityActionID	Integer	Unique ID for IT security action	• Must be unique • Not null
ActionTaken	String	Type of IT action taken	• Must be one of: “Password Reset”, “Security Training”, “No Action” • Not null
ActionDate	Date	Date on which the IT action was taken	• Must be ≥ EmailSentDate • Not null
ITAdmin	String	Name of the IT administrator performing the action	• Must match predefined list of IT admins • Not null

2. BI Dashboards (Screenshots from Power BI; 3 BI Dashboards are required)

2.1 Dashboard 1: For Phishing Campaign Manager

This dashboard is designed to support the Phishing Campaign Manager in monitoring employee engagement with simulated phishing attacks and evaluating the effectiveness of awareness efforts. By visualizing phishing behavior across departments and over time, the dashboard provides valuable insights to design smarter, more targeted campaigns that reduce organizational exposure to phishing threats.

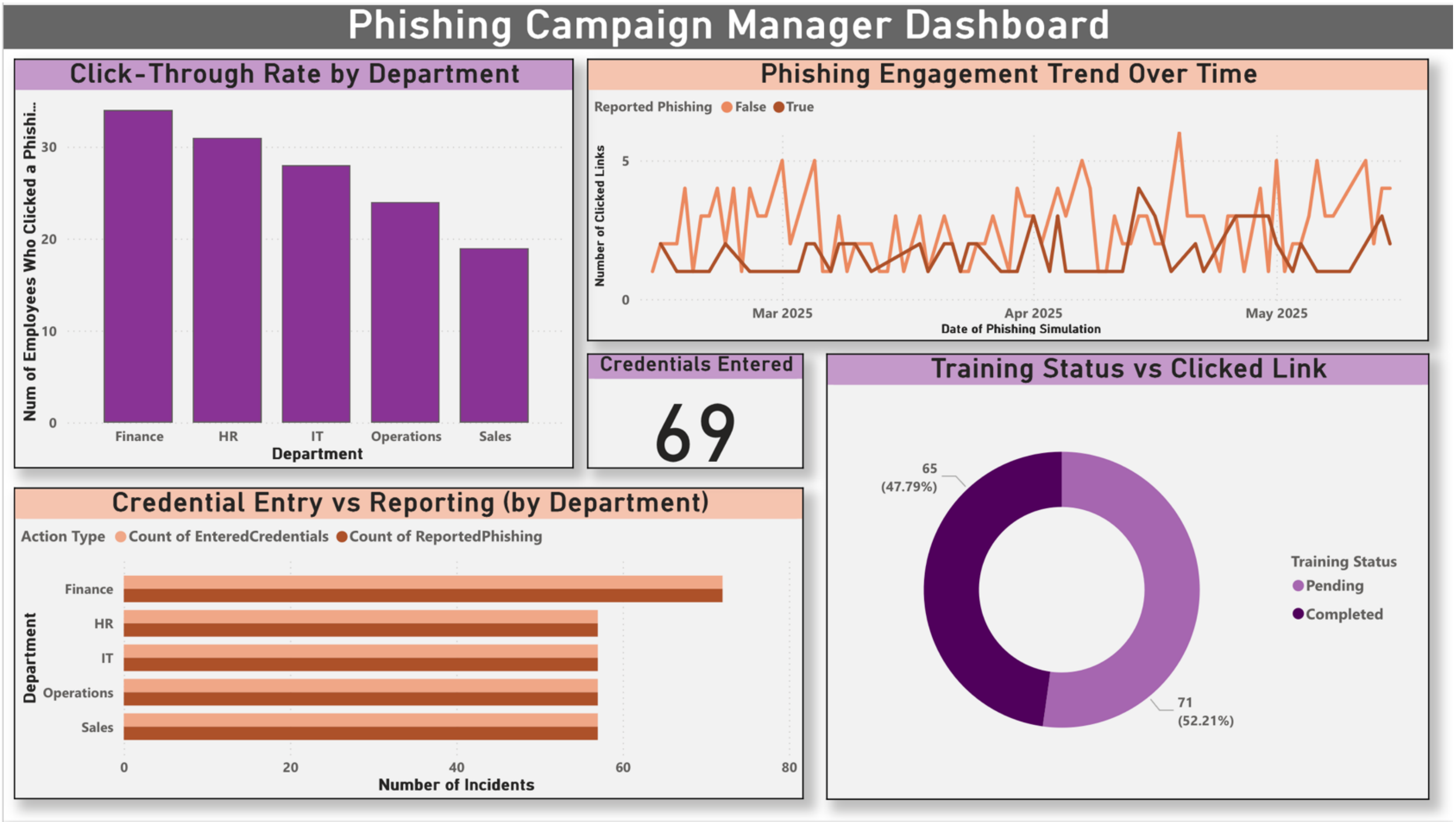

Phishing Campaign Manager Dashboard
Click-Through Rate by Department
Num of Employees Who Clicked a Phishi...
0
10
20
30
Finance
HR
IT
Operations
Sales
Department
Phishing Engagement Trend Over Time
Reported Phishing ● False ● True
Number of Clicked Links
0
5
Mar 2025
Apr 2025
May 2025
Date of Phishing Simulation
Credentials Entered
69
Training Status vs Clicked Link
65
(47.79%)
71
(52.21%)
Training Status
● Pending
● Completed
Credential Entry vs Reporting (by Department)
Action Type ● Count of EnteredCredentials ● Count of ReportedPhishing
Department
Finance
HR
IT
Operations
Sales
0
20
40
60
80
Number of Incidents

Figure 1. Phishing Campaign Manager Dashboard

Key Visualizations and Insights

1. Click-Through Rate by Department (Bar Chart)

This visual highlights which departments have the highest number of employees clicking phishing links. Finance and HR lead in click volume, suggesting a need for targeted training in those teams. The chart helps identify high-risk groups, making it easier for the campaign manager to prioritize interventions and fine-tune phishing scenarios to department specific contexts.

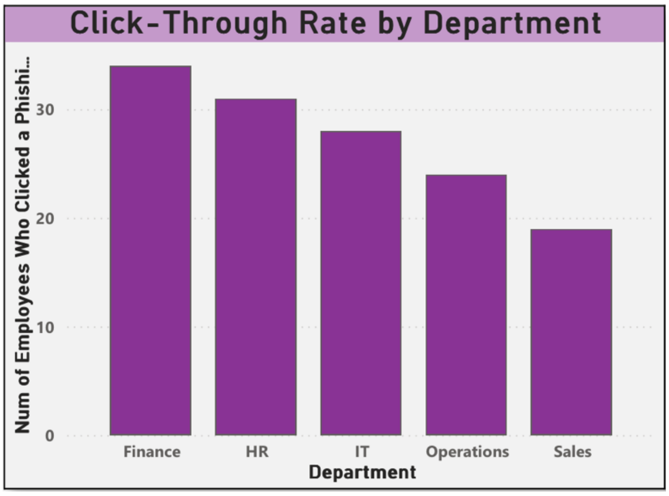
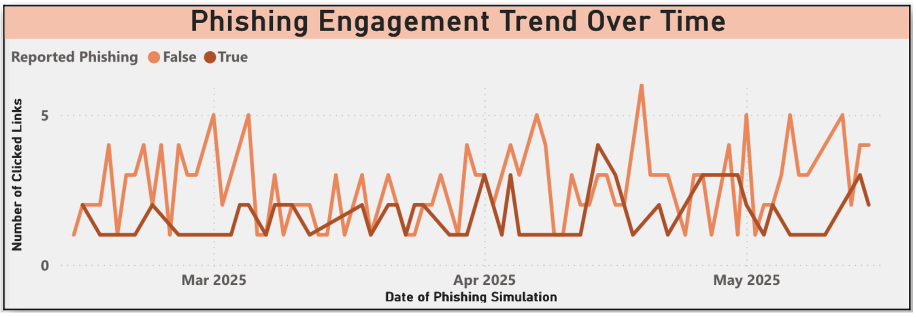


Figure 1 HR Manager Dashboard)

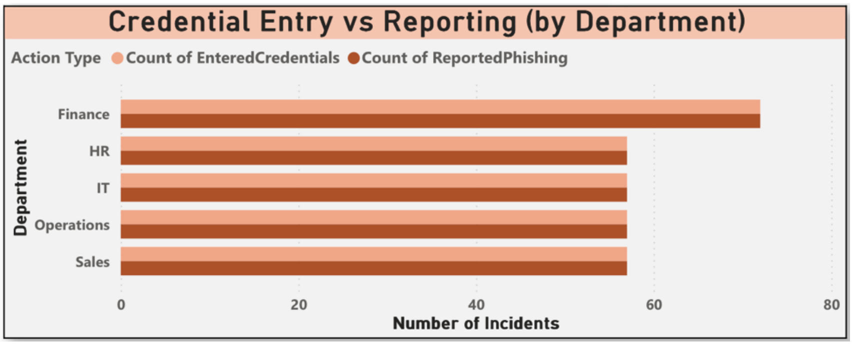
2. Phishing Engagement Trend Over Time (Line Chart)

This time series tracks the volume of phishing link clicks across the simulation period. Peaks in engagement indicate periods when specific phishing emails were more effective, or employee vigilance was lower. This allows campaign managers to review and refine the timing, messaging, and content of future phishing simulations.



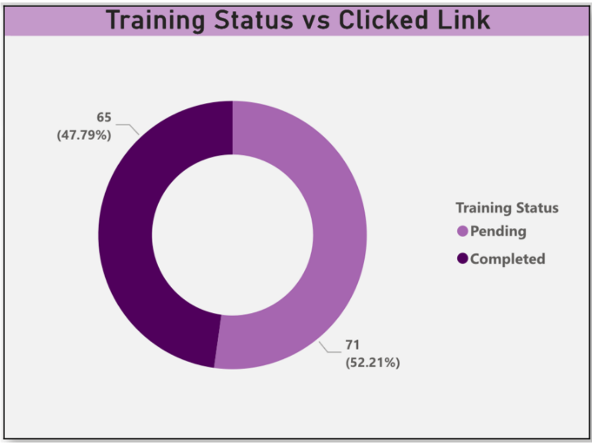
3. Credential Entry vs Reporting by Department (Stacked Bar Chart)

This comparison shows, for each department, how many employees entered credentials versus how many reported the phishing attempt. A high number of credential entries paired with low reporting (as seen in Finance) highlights a behavioral risk that requires immediate corrective action. The manager can use this to assess both the awareness level and the willingness of employees to report threats.



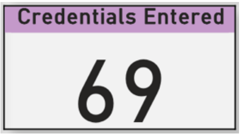
4. Training Status vs Clicked Link (Donut Chart)

This chart evaluates the relationship between training completion and phishing link clicks. The relatively even split between clicks from 'Completed' and 'Pending' training status suggests that training, while present, may not be sufficiently effective or recent. This could inform follow-up micro-training or gamified reinforcement campaigns.



5. KPI Card: Credentials Entered

The KPI card shows a total of 69 credential entries across simulations. This is a critical risk indicator as these entries represent the highest level of potential damage in real-world phishing scenarios. Campaign managers can use this number to track reductions over time as training and simulations mature.



Credentials Entered

69

Summary of Usefulness

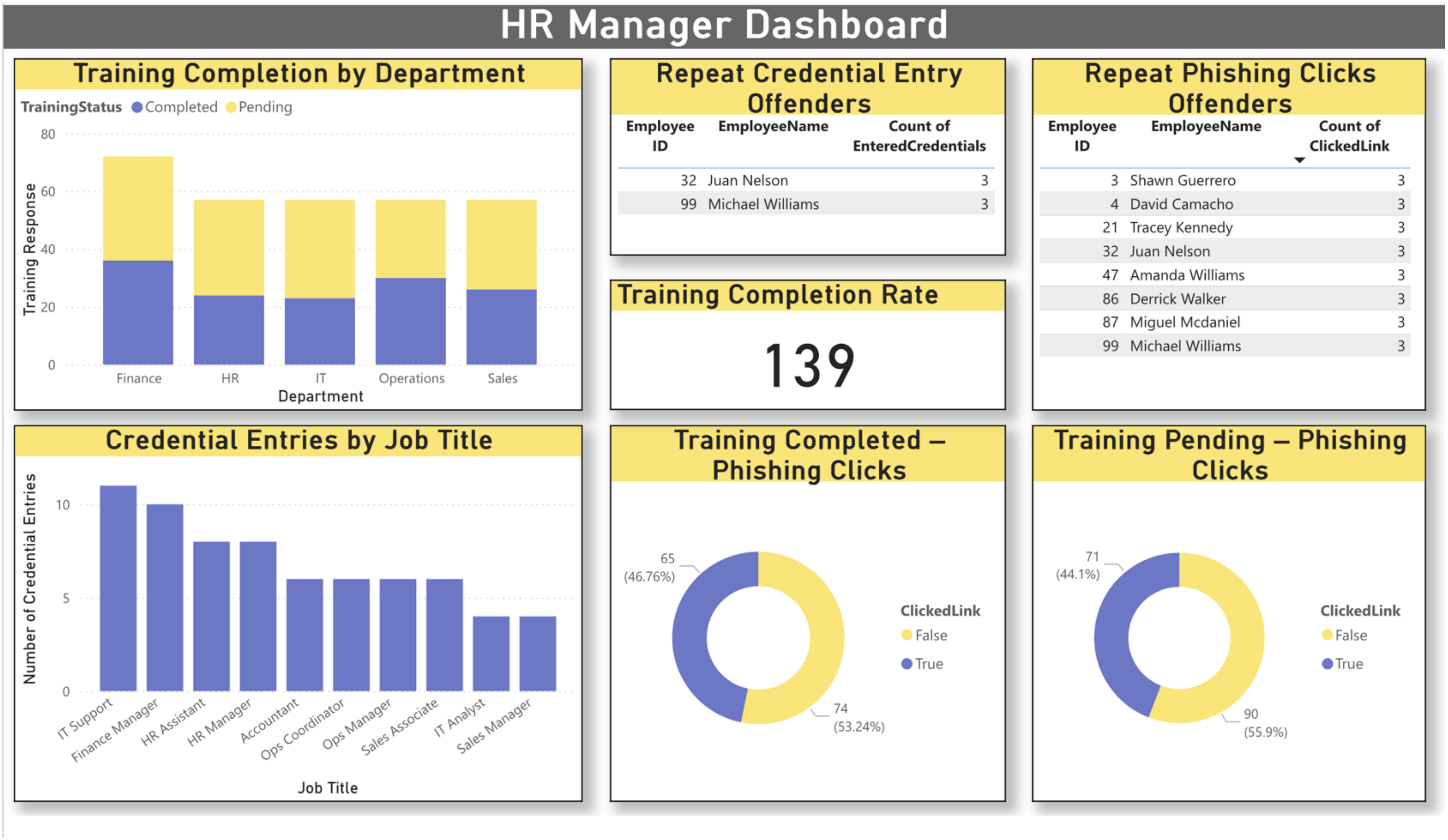
This dashboard allows the Phishing Campaign Manager to:

- Measure employee susceptibility across departments
- Track simulation performance over time
- Correlate engagement with training outcomes
- Identify critical risk areas requiring focused attention

By leveraging these insights, the campaign manager can tailor future phishing emails, improve the design of training materials, and reduce successful phishing interactions across SecureBank.

2.2 Dashboard 2: For HR Manager

The HR Manager dashboard is designed to assess employee readiness, compliance with security training, and behavioral risk across departments and job roles. It provides comprehensive visibility into how employee actions align with their training status, enabling HR to make informed decisions about awareness programs and targeted interventions.



HR Manager Dashboard

Training Completion by Department

Repeat Credential Entry Offenders

Employee ID	EmployeeName	Count of EnteredCredentials
32	Juan Nelson	3
99	Michael Williams	3

Repeat Phishing Clicks Offenders

Employee ID	EmployeeName	Count of ClickedLink
3	Shawn Guerrero	3
4	David Camacho	3
21	Tracey Kennedy	3
32	Juan Nelson	3
47	Amanda Williams	3
86	Derrick Walker	3
87	Miguel Mcdaniel	3
99	Michael Williams	3

Training Completion Rate

139

Credential Entries by Job Title

Training Completed – Phishing Clicks

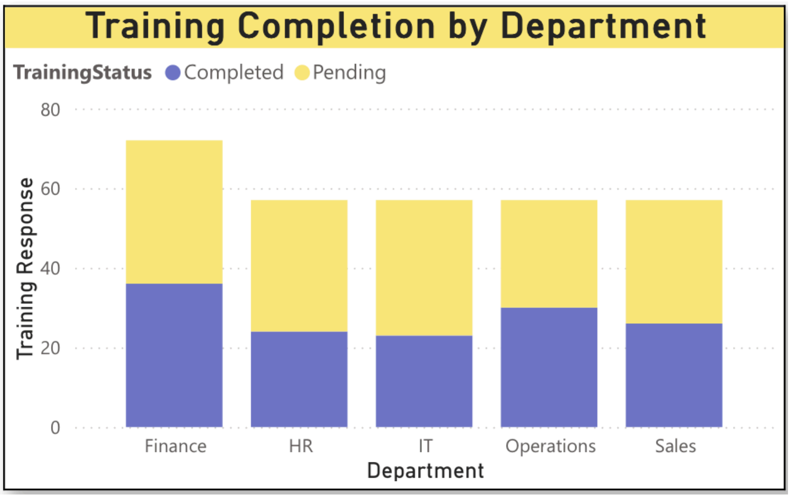
Training Pending – Phishing Clicks

Figure 2. HR Manager Dashboard

Key Visualizations and Insights

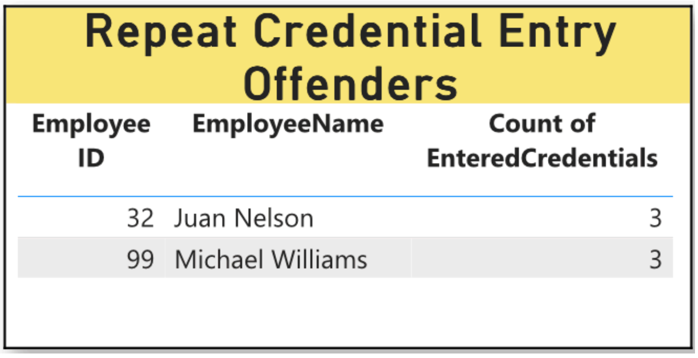
1. Training Completion by Department (Stacked Column Chart)

This chart displays the number of employees who have completed or are pending phishing awareness training, segmented by department. Finance shows relatively higher completion, while other departments exhibit a larger proportion of pending statuses. This helps HR prioritize follow-up actions in specific teams where training uptake is lower.



2. Repeat Credential Entry Offenders (Table)

This table highlights employees who entered credentials in phishing simulations more than once. Repeat offenses by the same individuals flag potential behavioral risks and provide a clear basis for individual-level coaching, retraining, or disciplinary follow-up.

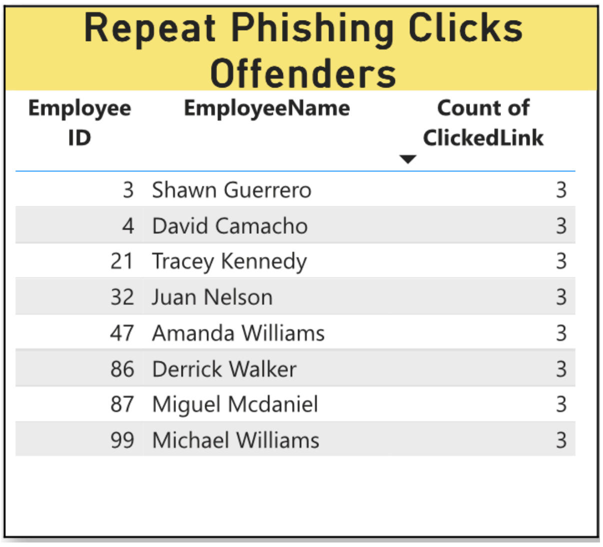


Repeat Credential Entry Offenders

Employee ID	EmployeeName	Count of EnteredCredentials
32	Juan Nelson	3
99	Michael Williams	3

3. Repeat Phishing Click Offenders (Table)

Similar to the previous visual, this table identifies employees who repeatedly clicked phishing links. These individuals are at elevated risk and may not fully grasp the training content or be actively engaged, making them ideal candidates for refresher training or personalized security guidance.

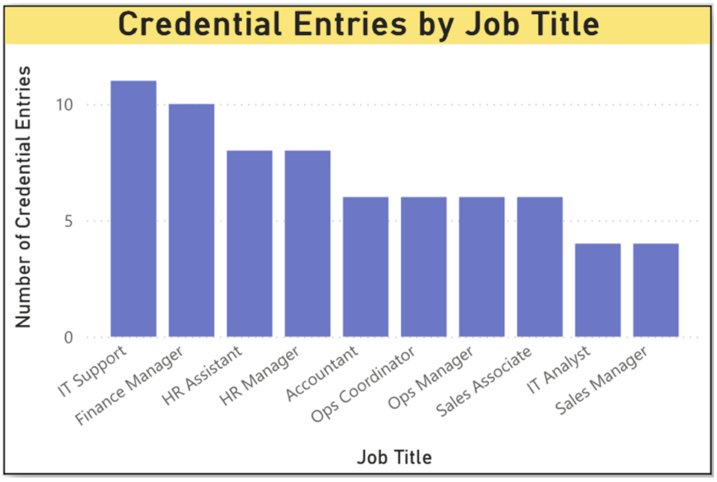


Repeat Phishing Clicks Offenders

Employee ID	EmployeeName	Count of ClickedLink
3	Shawn Guerrero	3
4	David Camacho	3
21	Tracey Kennedy	3
32	Juan Nelson	3
47	Amanda Williams	3
86	Derrick Walker	3
87	Miguel Mcdaniel	3
99	Michael Williams	3

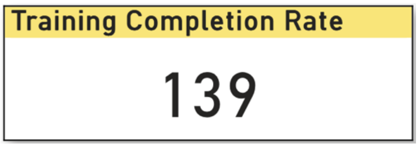
4. Credential Entries by Job Title (Bar Chart)

This chart allows HR to identify job roles most likely to submit credentials during phishing attempts. Roles like IT Support, HR Assistant, and Finance Manager show a higher frequency of credential entry. These insights inform role-specific training design, especially for positions with elevated access or sensitive data responsibilities.



5. Training Completion (KPI Card)

This KPI displays the total number of training responses (completed and pending), serving as a quick benchmark of overall training engagement. When tracked over time, it can help HR measure campaign reach and training compliance across the organization.

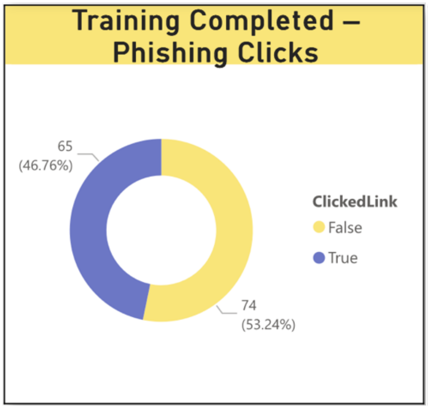


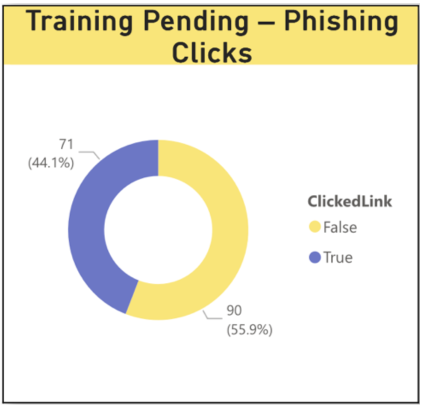
Training Completion Rate

139

6. Phishing Clicks by Training Status (Donut Charts)

These side-by-side donut charts compare click behavior among employees who have completed training versus those who have not. While both groups show significant click activity, the pending group has a higher percentage of phishing link clicks, reinforcing the importance of timely training delivery and completion tracking.





Summary of Usefulness

The HR Manager dashboard supports the following actions:

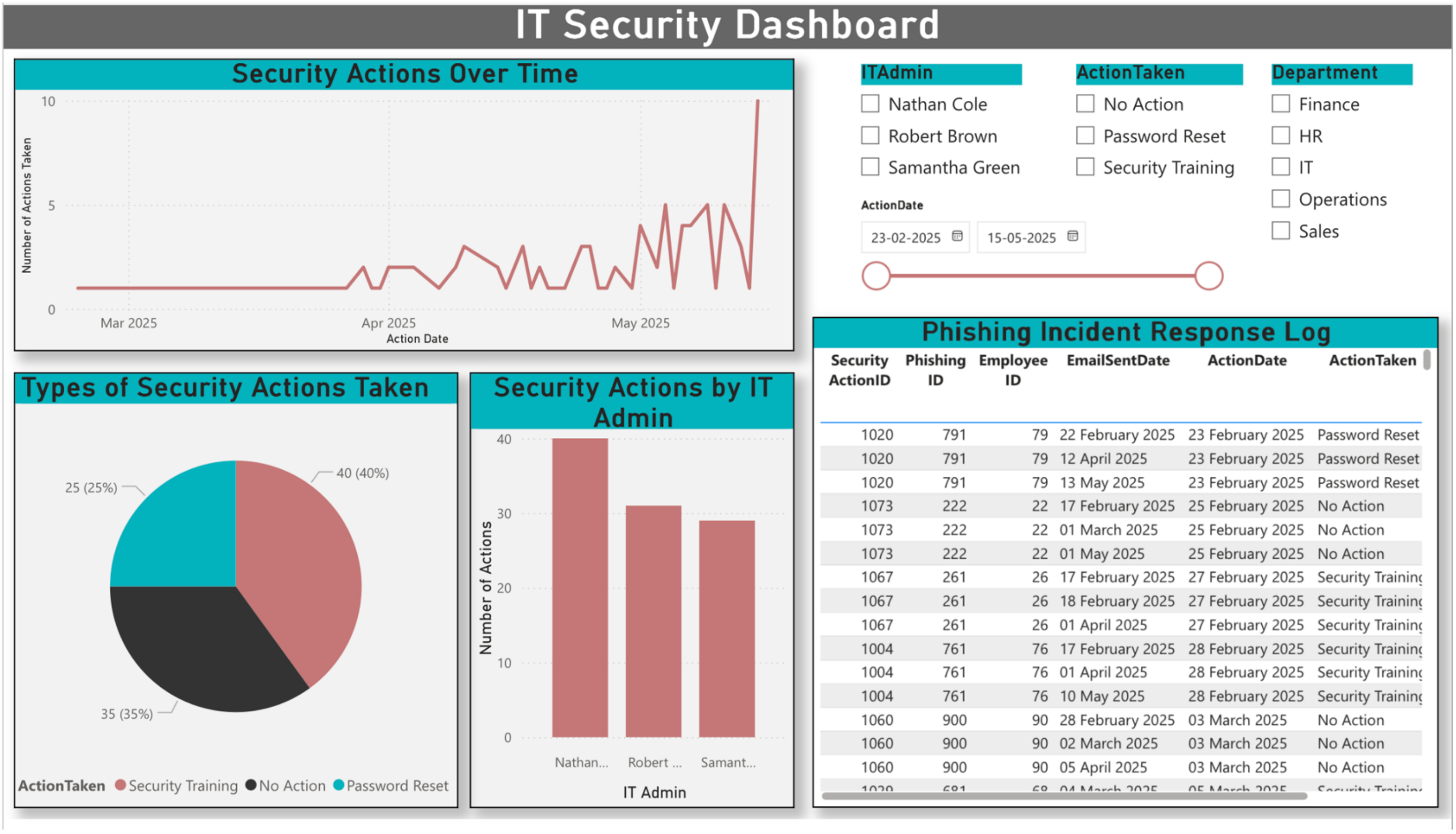
- Monitor and improve phishing training participation
- Identify individuals and job roles at greatest behavioral risk
- Correlate training outcomes with real behavior in simulations
- Tailor awareness campaigns by department or job function

Ultimately, this dashboard empowers HR to take a proactive, evidence-based approach to building a more cyber-aware workforce, enhancing SecureBank's human-layer security posture.

2.3 Dashboard 3: For IT Security Manager

The IT Security Team dashboard is designed to support operational efficiency and accountability in response to phishing incidents. It provides real-time visibility into the volume, type, and timeliness of IT actions taken after employee interactions with phishing simulations. With a focus on responsiveness and workload distribution, this dashboard allows

IT leadership to improve coordination, reduce response time, and ensure that high-risk incidents are promptly addressed.



ActionDate: 23-02-2025 – 15-05-2025

Phishing Incident Response Log

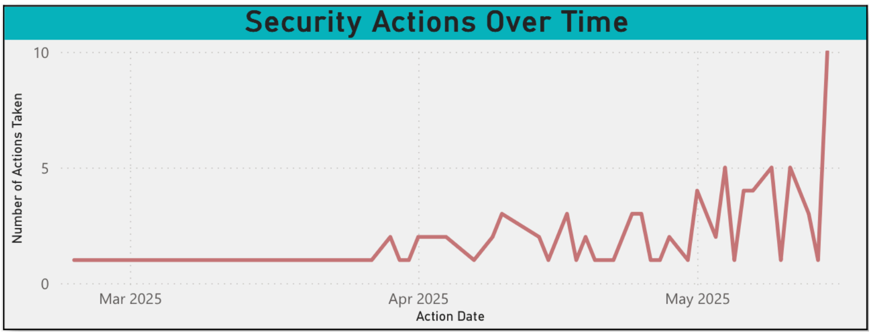
Security ActionID	Phishing ID	Employee ID	EmailSentDate	ActionDate	ActionTaken
1020	791	79	22 February 2025	23 February 2025	Password Reset
1020	791	79	12 April 2025	23 February 2025	Password Reset
1020	791	79	13 May 2025	23 February 2025	Password Reset
1073	222	22	17 February 2025	25 February 2025	No Action
1073	222	22	01 March 2025	25 February 2025	No Action
1073	222	22	01 May 2025	25 February 2025	No Action
1067	261	26	17 February 2025	27 February 2025	Security Training
1067	261	26	18 February 2025	27 February 2025	Security Training
1067	261	26	01 April 2025	27 February 2025	Security Training
1004	761	76	17 February 2025	28 February 2025	Security Training
1004	761	76	01 April 2025	28 February 2025	Security Training
1004	761	76	10 May 2025	28 February 2025	Security Training
1060	900	90	28 February 2025	03 March 2025	No Action
1060	900	90	02 March 2025	03 March 2025	No Action
1060	900	90	05 April 2025	03 March 2025	No Action
1029	681	68	04 March 2025	05 March 2025	Security Training

Figure 3. IT Security Team Dashboard

Key Visualizations and Insights

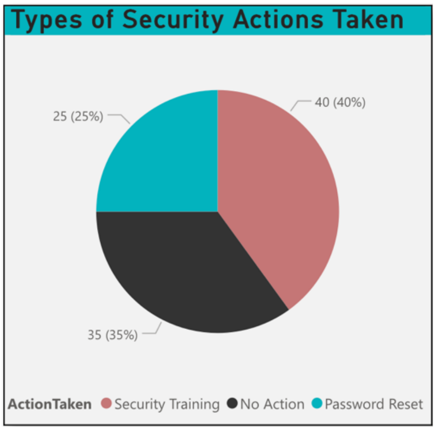
1. Security Actions Over Time (Line Chart)

This chart shows how IT interventions have varied over the simulation period. The upward trend reflects either an increase in phishing events or more active response efforts by the IT team. Spikes may correlate with periods of high phishing engagement, helping the team plan for resource allocation and evaluate if automation or escalated response protocols are needed.



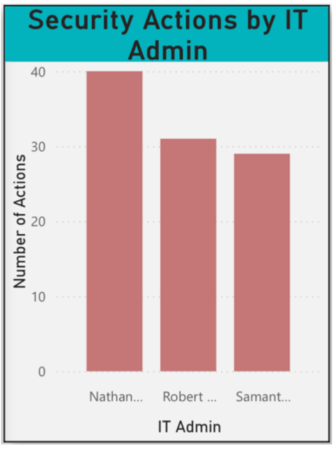
2. Types of Security Actions Taken (Pie Chart)

This visual shows the distribution of IT actions: Password Resets, Security Training, and No Action. The dominance of Password Resets and Training suggests that IT is actively mitigating threats. However, the portion of No Action indicates opportunities for improving trigger rules or follow-up mechanisms. It also helps assess policy consistency.



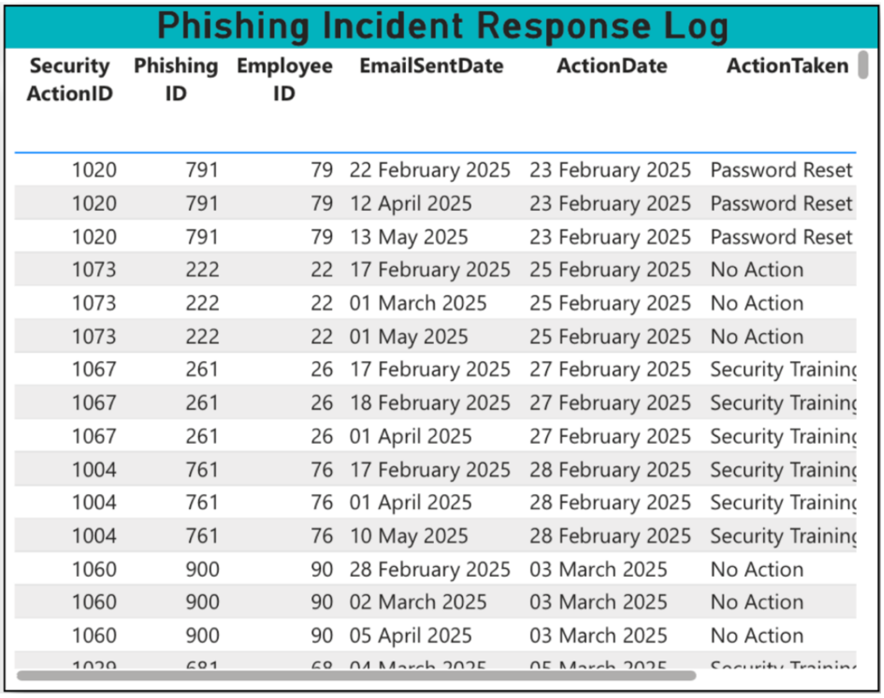
3. Security Actions by IT Admin (Bar Chart)

This chart displays the number of actions performed by each IT administrator. Nathan Cole leads in intervention volume, followed by Robert Brown and Samantha Green. This helps identify workload distribution, potential bottlenecks, and training needs across the IT support team.



4. Phishing Incident Response Log (Table)

The table provides a detailed record of each phishing incident and the corresponding IT response. It includes fields such as PhishingID, EmailSentDate, ActionTaken, and ActionDate, allowing for audit, traceability, and performance evaluation. Combined with slicers, it enables dynamic filtering by IT Admin, Department, Action Type, and Date.

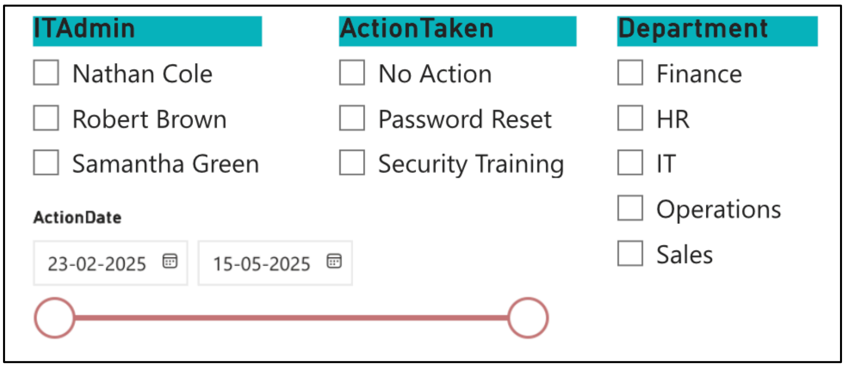


Phishing Incident Response Log

Security ActionID	Phishing ID	Employee ID	EmailSentDate	ActionDate	ActionTaken
1020	791	79	22 February 2025	23 February 2025	Password Reset
1020	791	79	12 April 2025	23 February 2025	Password Reset
1020	791	79	13 May 2025	23 February 2025	Password Reset
1073	222	22	17 February 2025	25 February 2025	No Action
1073	222	22	01 March 2025	25 February 2025	No Action
1073	222	22	01 May 2025	25 February 2025	No Action
1067	261	26	17 February 2025	27 February 2025	Security Training
1067	261	26	18 February 2025	27 February 2025	Security Training
1067	261	26	01 April 2025	27 February 2025	Security Training
1004	761	76	17 February 2025	28 February 2025	Security Training
1004	761	76	01 April 2025	28 February 2025	Security Training
1004	761	76	10 May 2025	28 February 2025	Security Training
1060	900	90	28 February 2025	03 March 2025	No Action
1060	900	90	02 March 2025	03 March 2025	No Action
1060	900	90	05 April 2025	03 March 2025	No Action
1029	681	68	04 March 2025	05 March 2025	Security Training

5. Slicers for Interactive Analysis

The inclusion of slicers enhances interactivity and allows the user to explore incident trends by specific IT Admins, departments, action types, or simulation dates. This makes the dashboard more versatile and user-driven, supporting both high-level summaries and detailed reviews.



ITAdmin
□ Nathan Cole
□ Robert Brown
□ Samantha Green

ActionTaken
□ No Action
□ Password Reset
□ Security Training

Department
□ Finance
□ HR
□ IT
□ Operations
□ Sales

ActionDate
23-02-2025 15-05-2025

Summary of Usefulness

This dashboard enables the IT Security Team to:

- Monitor operational performance in phishing incident response
- Ensure timely mitigation of credential risks or unreported phishing clicks
- Balance workloads across IT personnel
- Maintain an auditable trail of actions taken for future compliance or investigation

By using this dashboard, SecureBank's IT team can not only detect but also respond to phishing threats with speed, precision, and accountability, contributing to a more resilient cybersecurity framework.

3. Recommendations (at least 3 recommendations for 3 BI Dashboards)

Based on the findings from the three BI dashboards developed for SecureBank, the following recommendations are proposed to improve phishing awareness, training effectiveness, and IT response capability across the organization.

Recommendation 1: Launch Department-Specific Refresher Campaigns (Phishing Campaign Manager Dashboard)

The Phishing Campaign Manager dashboard revealed that departments such as **Finance and HR** exhibit higher click-through and credential entry rates, paired with lower phishing reporting behaviour.

Action:
Launch tailored phishing awareness refreshers for these high-risk departments. Customize phishing scenarios to resemble actual business processes relevant to their roles (e.g., payroll alerts for Finance).

Justification:
Generic training may not resonate with contextual threats. Department-specific simulations will improve realism and effectiveness, thereby reducing susceptibility and enhancing reporting behaviour.

Recommendation 2: Prioritize Role-Based Micro-Training for High-Risk Job Titles (HR Manager Dashboard)

The HR dashboard identified job roles like **IT Support, Finance Manager, and HR Assistant** as more likely to enter credentials during phishing simulations, even among those who completed training.

Action:
Design and deploy short, role-specific micro-learning modules that highlight real-world phishing risks tailored to each job function. Reinforce these with brief, interactive quizzes or simulation follow-ups.

Justification:
One-size-fits-all training isn't sufficient. High-risk roles require more nuanced, engaging content that reflects the specific threats they are likely to encounter in their workflow.

Recommendation 3: Improve Incident Response SLA Tracking and IT Resource Balancing (IT Security Team Dashboard)

The IT Security dashboard indicates variable response times and uneven distribution of actions among IT administrators, with one admin (e.g., Nathan Cole) handling a significantly higher volume.

Action:
Implement SLA targets for phishing response time and automate alerts for delayed actions. Evaluate team workloads and consider redistributing tasks or cross-training admins to ensure balanced intervention capacity.

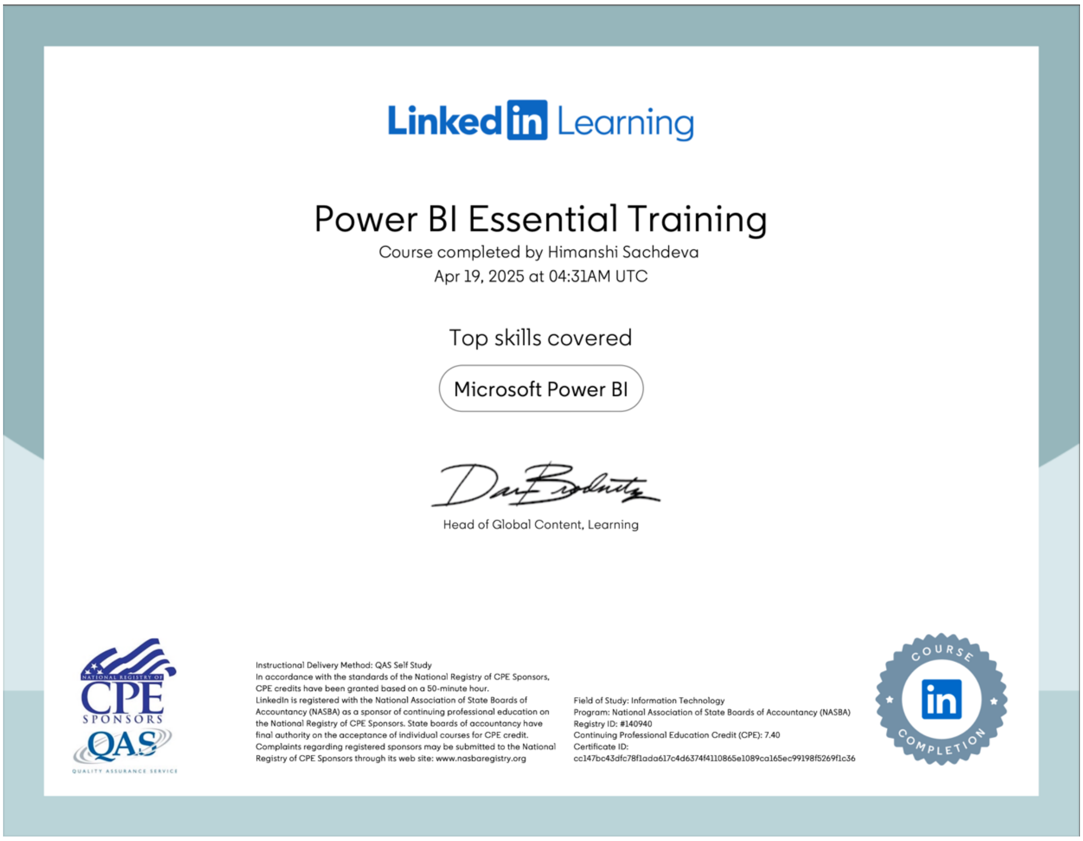
Justification:
Consistent and timely responses to phishing threats are critical to minimize risk. Establishing clear performance benchmarks and balancing workloads will improve both speed and accountability in the IT security function.

4. References

- OpenAI. (2025). *Synthetic dataset generated using ChatGPT for phishing simulation analysis*.
- Microsoft. (n.d.). *Dashboard design tips*. Microsoft Learn. https://learn.microsoft.com/en-us/power-bi/create-reports/service-dashboards-design-tips
- Yeoh, W., Talburt, J. R., & Zhou, Y. (2014). *Information quality and governance for business intelligence*. IGI Global.
- Power, D. J. (2007). *DSS 2.0: Supporting decision making with new technologies* (1st ed.). IGI Global.

5. Appendix (& Dataset)

Appendix A: Certificate of Completion for Power BI



Linked in Learning

Power BI Essential Training

Course completed by Himanshi Sachdeva

Apr 19, 2025 at 04:31AM UTC

Top skills covered

Microsoft Power BI

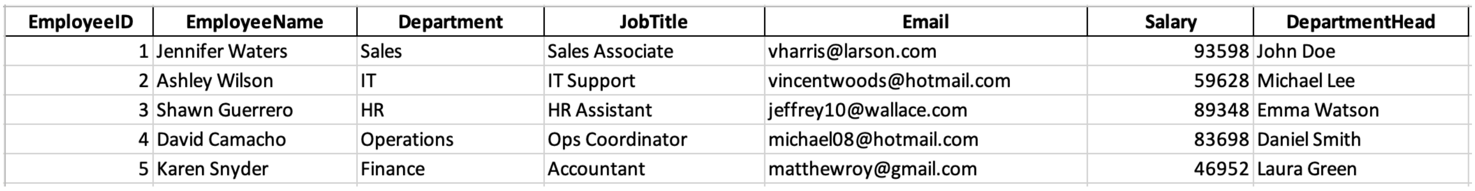
Head of Global Content, Learning

Instructional Delivery Method: QAS Self Study
In accordance with the standards of the National Registry of CPE Sponsors, CPE credits have been granted based on a 50-minute hour.
LinkedIn is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Field of Study: Information Technology
Program: National Association of State Boards of Accountancy (NASBA)
Registry ID: #140940
Continuing Professional Education Credit (CPE): 7.40
Certificate ID:
cc147bc43dfc78f1ada617c4d6374f4110865e1089ca165ec99198f5269f1c36

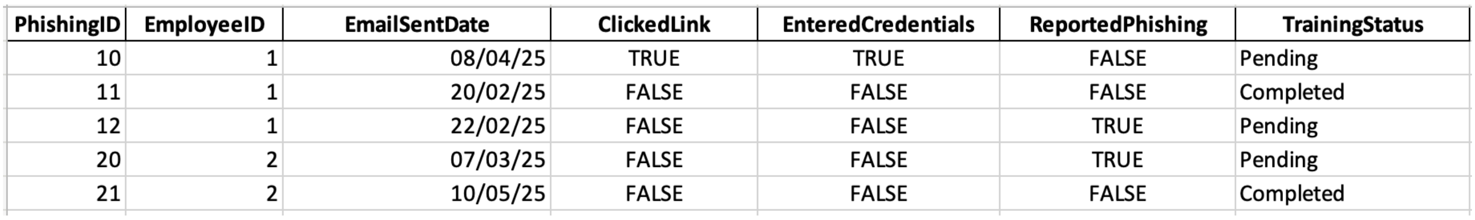
Figure 4. Power BI Essential Training - Course Completion Certificate

Appendix B: Dataset Sample showing first 5 rows



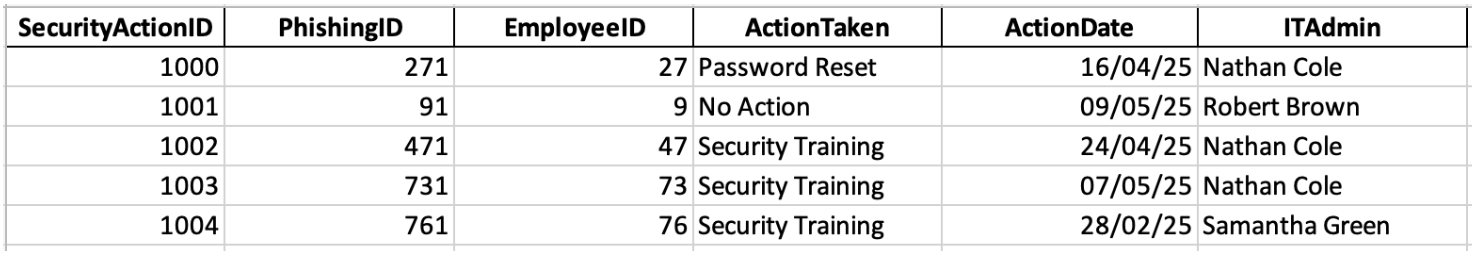
EmployeeID	EmployeeName	Department	JobTitle	Email	Salary	DepartmentHead
1	Jennifer Waters	Sales	Sales Associate	vharris@larson.com	93598	John Doe
2	Ashley Wilson	IT	IT Support	vincentwoods@hotmail.com	59628	Michael Lee
3	Shawn Guerrero	HR	HR Assistant	jeffrey10@wallace.com	89348	Emma Watson
4	David Camacho	Operations	Ops Coordinator	michael08@hotmail.com	83698	Daniel Smith
5	Karen Snyder	Finance	Accountant	matthewroy@gmail.com	46952	Laura Green

Figure 5. HR Manager Dataset



PhishingID	EmployeeID	EmailSentDate	ClickedLink	EnteredCredentials	ReportedPhishing	TrainingStatus
10	1	08/04/25	TRUE	TRUE	FALSE	Pending
11	1	20/02/25	FALSE	FALSE	FALSE	Completed
12	1	22/02/25	FALSE	FALSE	TRUE	Pending
20	2	07/03/25	FALSE	FALSE	TRUE	Pending
21	2	10/05/25	FALSE	FALSE	FALSE	Completed

Figure 6. Phishing Campaign Dataset



SecurityActionID	PhishingID	EmployeeID	ActionTaken	ActionDate	ITAdmin
1000	271	27	Password Reset	16/04/25	Nathan Cole
1001	91	9	No Action	09/05/25	Robert Brown
1002	471	47	Security Training	24/04/25	Nathan Cole
1003	731	73	Security Training	07/05/25	Nathan Cole
1004	761	76	Security Training	28/02/25	Samantha Green

Figure 7. IT Security Dataset