Phishing Campaign Report

Table of content

1. Introduction

Phishing is an example of a highly effective form of cybercrime that enables criminals to deceive users and steal important data. (Zainab Alkhalil, 2021) To combat this growing issue, organizations must employ comprehensive and effective strategies. Attacks are reported each year, and a reduction in the number of such attacks is unlikely to occur in the near future. (Jampen, 2020) Simulated phishing campaigns are a powerful tool to assess and enhance an organization's resilience to these threats. This report introduces three specialized BI dashboards designed to provide valuable insights into simulated phishing campaigns, targeting distinct user groups: Phishing Campaign Managers, Individual Users, and HR Managers.

These dashboards offer a detailed analysis of campaign performance, user behaviour, and employee susceptibility, enabling stakeholders to identify weaknesses, tailor training programs, and implement targeted interventions. By leveraging these insights, organizations can significantly strengthen their cybersecurity defences and foster a culture of awareness and vigilance.

1.1 Objectives

Campaign Manager

- Gain a comprehensive understanding of campaign effectiveness by analysing user behaviour and key metrics.
- Identify trends and vulnerabilities in user behaviour to optimize future campaign design and training strategies.
- Evaluate the performance of different email templates, attachment types, and campaign themes to refine future campaigns for maximum impact.

User

- Raise individual awareness and understanding of phishing tactics through data visualization of user behaviour and campaign results.
- Identify areas for personal improvement in recognizing and reporting phishing attempts.
- Encourage a culture of cybersecurity vigilance within the organization.

HR Manager

- Pinpoint high-risk departments and employee groups most susceptible to phishing attacks based on various factors.
- Develop targeted phishing awareness training programs to address specific departmental and individual needs.
- Inform data-driven decisions regarding disciplinary actions and interventions for phishing incidents.

1.2 Benefits/Advantages

1. Comprehensive Analysis:

- Benefit: Provides a holistic view of phishing campaign performance and user behaviour.
- Advantage: Enables stakeholders to make informed decisions based on detailed and actionable insights.

2. Targeted Training Programs:

- Benefit: Identifies specific vulnerabilities and risk factors among different user groups.
- Advantage: Allows for the development of customized training programs that address the unique needs and weaknesses of each group, enhancing overall effectiveness.

3. Improved Cybersecurity Posture:

- Benefit: Helps reduce the success rate of phishing attacks through continuous monitoring and improvement.
- Advantage: Strengthens the organization's cybersecurity defences, protecting sensitive information and reducing the risk of data breaches.

4. Enhanced Reporting and Accountability:

- Benefit: Tracks and reports on key metrics such as attachment click rates, email template performance, and regional susceptibility.
- Advantage: Facilitates accountability and transparency in cybersecurity efforts, allowing for more effective management and oversight.

5. Proactive Risk Management:

- Benefit: Assesses and categorizes employee risk levels based on their behaviour and history.
- Advantage: Enables HR Managers to proactively address high-risk areas through targeted interventions, reducing the likelihood of successful phishing attacks.

6. Encourages a Culture of Vigilance:

- Benefit: Promotes awareness and education among all employees about the dangers of phishing.
- Advantage: Fosters a workplace culture where employees are more vigilant and proactive in reporting and responding to phishing attempts.

1.3 Assumptions

Campaign Manager

1: Each campaign is uniquely identified by the Campaign ID and all IDs are unique and non-nullable.
2: The Email Template field will only contain one of the following values: "Template A", "Template B", "Template C", "Template D", "Template E".
3: The Landing Page field will only contain one of the following values: "Landing Page 1", "Landing Page 2", "Landing Page 3", "Landing Page 4", "Landing Page 5".
4: The Attachment Type field will only contain one of the following values: "PDF", "Word Doc", "None", "Excel File", "Redirect Link".
5: Start Date and End Date will follow the DD-MM-YYYY format and be non-nullable.
6: Numerical fields such as Sent Emails, Opened Emails, Links Clicked, Reported Emails, and Successful Logins are non-nullable and represent integer values.

Table 2 Assumptions (Campaign Manager)

User

1: Each User ID is a unique integer that uniquely identifies a user.
2: The full name of the user is provided in a standard format.
3: The age groups are categorized into four fixed ranges: 20-30, 30-40, 40-50, and 50-60.
4: Gender is recorded as either "Male" or "Female".
5: Boolean fields such as Email Opened, Link Clicked, Credentials Entered, Reported Phishing, and Training Completed will only contain "Yes" or "No".
6: All fields are non-nullable, ensuring complete data for each user.
7: The risk score has been accurately calculated based on the phishing campaign performance.

Table 2 Assumptions (User)

HR Manager

1: Each employee is uniquely identified by the Employee ID and all IDs are unique and non-nullable.
2: The Employment Status field will only contain the values "Active" or "Terminated".
3: The Hire Date and Termination Date fields (if applicable) follow the DD-MM-YYYY format.
4: The Employment Type field will only contain the values "Full-Time" and "Part-Time"
5: The Education Level field will only contain one of the following values: "Associate's", "Bachelor's", "Master's".
6: The Risk Level field will only contain the values "Low", "Moderate", or "High".
7: The Training Status field will only contain the values "Completed" or "Not Completed".
8: The Disciplinary Action field will only contain the values "None", "Verbal Warning", or "Written Warning".
9: The Remedial Training and Follow-up Review fields can be nullable and will contain the values "Assigned" or "None" for Remedial Training, and "Scheduled" or "None" for Follow-up Review.

Table 3 Assumptions (HR Manager)

1.4 Description of business rules and variables

Campaign Manager

Attribute	Data Type	Description	Business Rule
Campaign ID	Integer	Unique identifier for each phishing campaign	- Unique value - Not nullable
Campaign Name	String	Name or title of the phishing campaign	- Not nullable
Target Industry	String	Industry sector targeted by the campaign	- Not nullable
Target Region	String	Geographic region targeted by the campaign	- Not nullable
Start Date	Date	Start date of the phishing campaign	- Not nullable - Date format: DD-MM-YYYY
End Date	Date	End date of the phishing campaign	- Not nullable - Date format: DD-MM-YYYY
Email Template	String	Template used for the phishing email. Template A – Renew Subscription Template B – Security Alert Template C – Account Update Template D – Promotional Offer Template E – Shipment Update	- Not Nullable - Value options: Email Template 1, Email Template 2, Email Template 3, Email Template 4, Email Template 5

Landing Page	String	Identifier of the phishing landing page corresponding to the template	- Not Nullable - Value options: Landing Page 1, Landing Page 2, Landing Page 3, Landing Page 4, Landing Page 5
Attachment Type	String	Type of file attachment used in the phishing email	- Not Nullable - Value options: PDF, Word Doc, None, Excel File, Redirect Link
Sent Emails	Integer	Total number of phishing emails sent in a campaign	- Not nullable
Opened Emails	Integer	Number of phishing emails opened by recipients in a campaign	- Not nullable
Links Clicked	Integer	Number of recipients who clicked the link in the phishing email in a campaign	- Not nullable
Reported Emails	Integer	Number of phishing emails reported by recipients in a campaign	- Not nullable
Successful Logins	Integer	Number of recipients who entered valid credentials on the phishing page in a campaign	- Not nullable

User

Attribute	Data Type	Description	Business Rule
User ID	Integer	Unique identifier for each user	- Unique value - Not nullable
Name	String	Full name of the user	- Not nullable
Age Group	String	Age ranges the user falls into	- Not nullable - Value options:

			20-30, 30-40, 40-50, 50-60
Gender	String	Gender of the user	- Not nullable - Value options: Male, Female
Email	String	Email address of the user	- Not nullable - Unique value
City	String	City where the user is located	- Not nullable
State	String	State where the user is located	- Not nullable
Email Opened	Boolean	Indicates if the user opened the phishing email	- Not nullable - Value options: Yes, No
Link Clicked	Boolean	Indicates if the user clicked the link in the phishing email	- Not nullable - Value options: Yes, No
Credentials Entered	Boolean	Indicates if the user entered their credentials on the phishing page	- Not nullable - Value options: Yes, No
Reported Phishing	Boolean	Indicates if the user reported the phishing attempt	- Not nullable - Value options: Yes, No
Training Completed	Boolean	Indicates if the user completed the phishing awareness training	- Not nullable - Value options: Yes, No
Previous Incidents	Integer	Number of previous phishing incidents the user was involved in	- Not nullable
Risk Score	Integer	Risk score assigned to the user based on their behaviour and history. Low risk score is desired.	- Not nullable

HR Manager

Attribute	Data Type	Description	Business Rule
Employee ID	Integer	Unique identifier for each employee	- Unique value - Not nullable
Hire Date	Date	Date when the employee was hired.	- Not nullable - Date format: DD-MM-YYYY
Termination Date	Date	Date when the employee's employment was terminated.	- Nullable - Date format: DD-MM-YYYY
Employment Status	String	Current employment status of the employee	- Not nullable - Value options: Active, Terminated
Job Level	String	Level or position of the employee's job role	- Not nullable
Department	String	Department or division the employee belongs to	- Not nullable
Salary	Decimal	Annual salary of the employee	- Not nullable
Employment Type	String	Type of employment contract	- Not nullable - Value options: Full-Time, Part-Time, Contract.
Years of Experience	Integer	Total years of work experience of the employee	- Not nullable
Education Level	String	Highest level of education attained by the employee	- Not nullable - Value options: Associate’s, Bachelor's, Master's
Training Status	String	Indicates if the employee has completed required training	- Not nullable - Value options: Completed, Not Completed

Previous Incidents	Integer	Number of previous incidents or violations by the employee	- Not nullable
Risk Level	String	Assessed risk level associated with the employee. Lower risk level is desired.	- Not nullable - Value options: Low, Medium, High
Disciplinary Action	String	Any disciplinary action taken against the employee	- Not nullable - Value options: None, Verbal Warning, Written Warning
Remedial Training	String	Indicates if remedial training is required for the employee	- Nullable - Value options: Assigned, None
Follow-up Review	String	Indicates if a follow-up review is scheduled for the employee	- Nullable - Value options: Scheduled, None

2. BI Dashboards

2.1 Campaign Manager

Figure 1 allows the manager to analyse the effectiveness of recent simulated phishing campaigns. This dashboard offers a centralized view of key metrics.

1. Attachment Click Rates: Identify which attachment types are most likely to be clicked by users. This information can be used to tailor future campaigns and user training to address specific attachment risks.
2. Campaign Reporting: Analyse which campaigns generated the highest number of reported phishing attempts. This allows for closer examination of these campaigns and potential adjustments to content or tactics to minimize the likelihood of users falling victim in real-world phishing attempts.
3. Dissecting Email Template Performance: Analyse which email templates are most likely to result in user clicks. This data can inform future template design and messaging strategies to minimize user vulnerability.
4. Overall Campaign Performance: Evaluate the overall effectiveness of your campaign, from the total number of emails sent to successful login attempts on phishing pages.
5. Regional Performance: Compare the success rates of phishing campaigns across different regions within your organization. This can help identify areas requiring more targeted training or awareness initiatives.

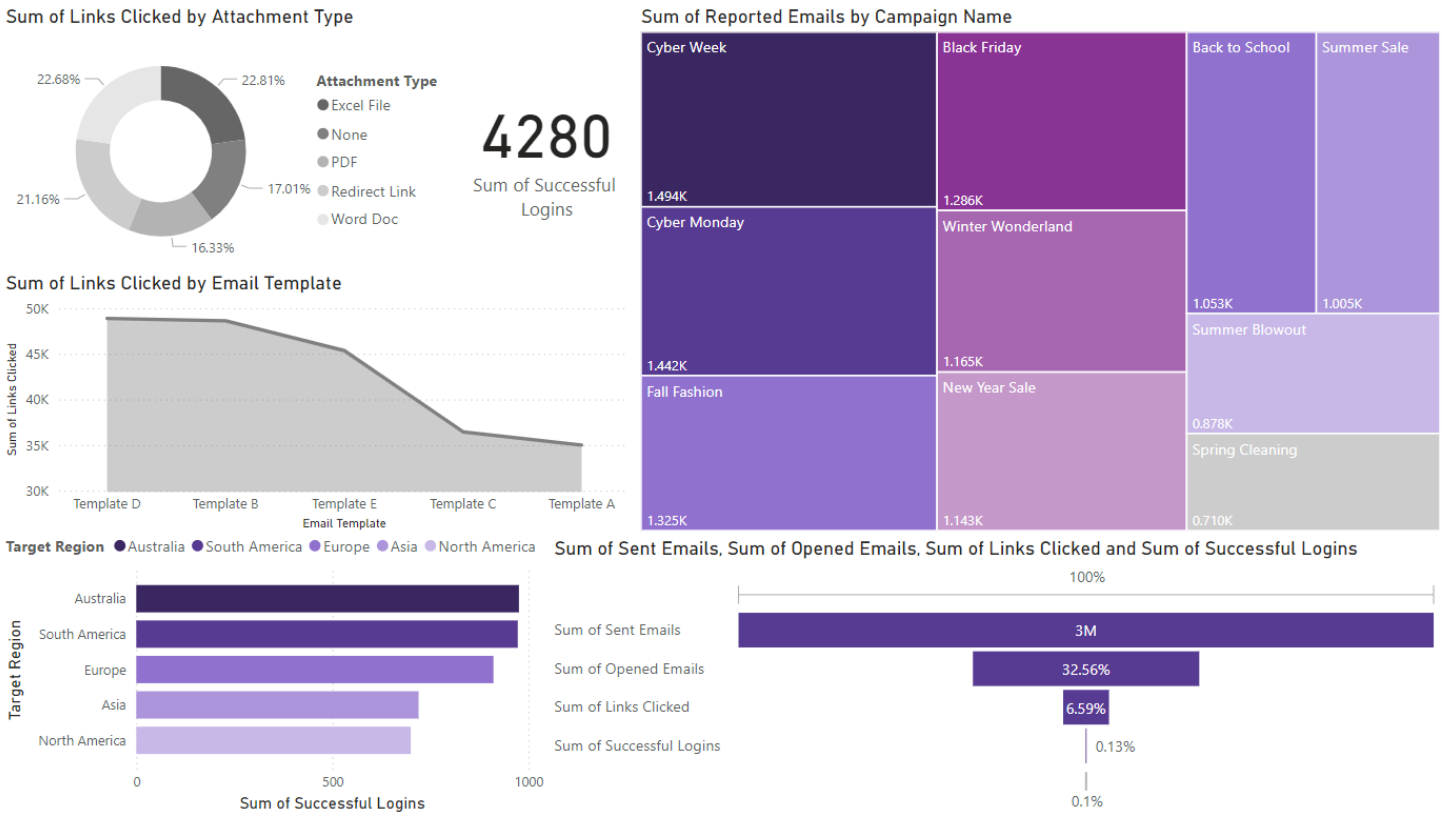

Figure 1 Campaign Manager Dashboard

Chart 1

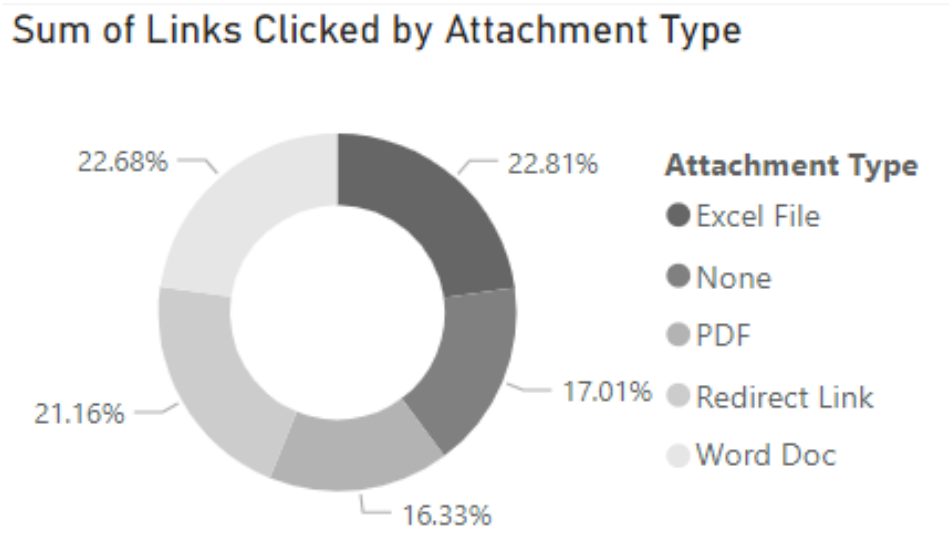

Figure 2 Links Clicked by Attachment Type

Figure 2 shows the percentage of links clicked for different attachment types. Based on this chart, Excel Files and Word Doc attachments have the highest percentage of links clicked (around 22% each). This suggests that users are more likely to click on emails with these attachment types. This might be due to trust in familiar file types: Excel files and word files are a common file type used in many workplaces, so users might be less suspicious of an email containing one.

Chart 2

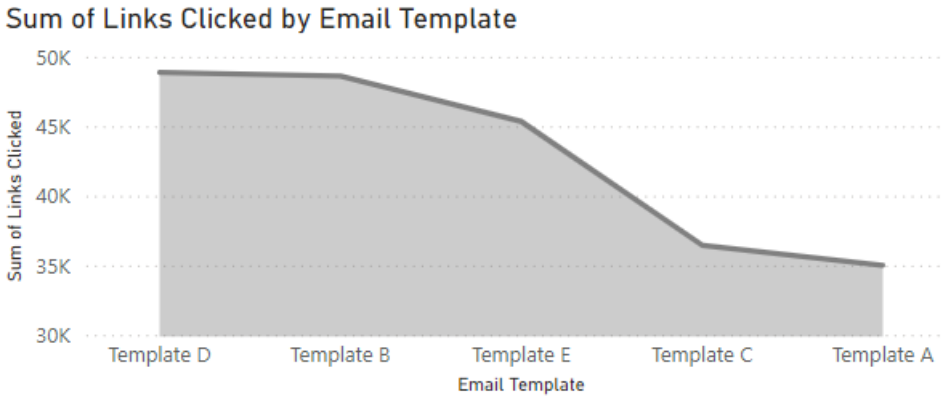

Figure 3 Links Clicked by Emal Template

Figure 3 shows the number of links clicked by email template. It shows that Promotional offer has the highest number of links clicked, followed by Security Alert, Shipment update, Account update and Renew Subscription.

Here are some explanations for this finding:

- Promotional Offers: People are generally receptive to promotions and discounts, so they might be more likely to click on a link to learn more.
- Security Alerts: Security alerts can be alarming, and users might click on a link out of concern or fear of negative consequences if they don't.
- Shipment updates: Emails with shipment updates might be expected by users, so they might be more likely to click on links to track their packages.
- Account Update: Emails providing account information updates might be less likely to contain attention-grabbing elements or calls to action, resulting in fewer clicks.
- Subscription renewals: Subscription renewal emails might be seen as routine by users, making them less likely to click on links.

Chart 3

Figure 4 Successful Logins by Target Region

Figure 4 compares the number if successful logins across five different regions: Australia, South America, Europe, Asia, and North America. Australia has the highest number of successful logins. This suggests that users in Australia may be more susceptible to phishing attacks compared to other regions and need more training. North

America has the lowest value in the metric. This indicates that users in North America are less likely to fall victim to phishing attacks.

Possible explanations for the trends:

- Regional Spam Filters: Some regions might have stricter spam filters that prevented some phishing emails from reaching users' inboxes.
- User Awareness: Users in some regions might be more aware of phishing scams and thus less likely to click on links or enter credentials.

Chart 4

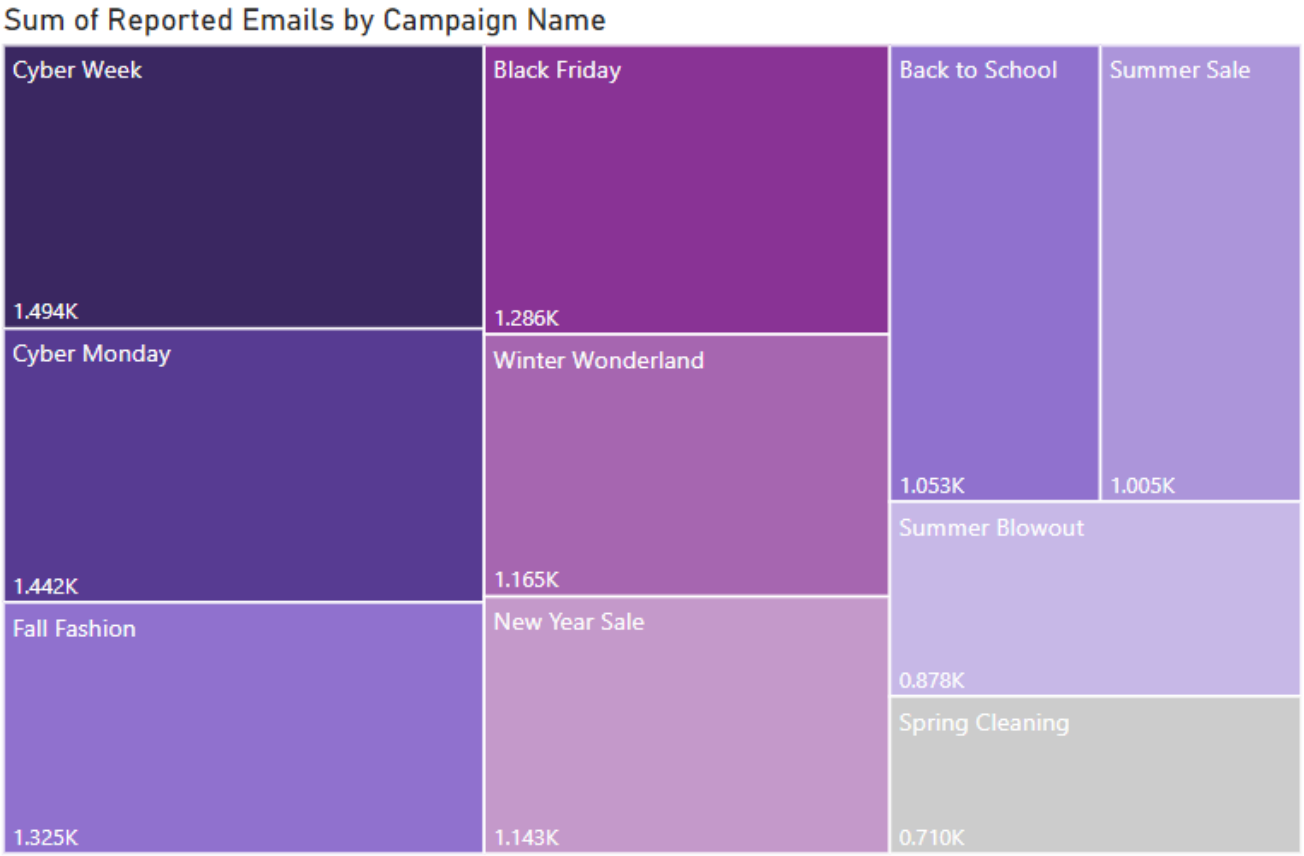

Figure 5 Reported Emails by Campaign Name

Figure 5 shows the number of emails reported as phishing attempts for various campaigns. Cyber week has the greatest number of reported emails followed by Cyber Monday, Fall Fashion and Black Friday. Spring Cleaning has the least number of reported emails followed by Summer Blowout and Summer Sale.

This might be due to the following reasons.

- User Awareness: Users might be more familiar with common phishing tactics associated with certain sales periods, like Black Friday or Cyber Monday.
- Campaign Timing: Campaigns sent closer to holidays or shopping seasons (like Cyber Week or Black Friday) might have grabbed more attention. People are more likely to be on the lookout for phishing scams during these times because they expect a higher volume of legitimate emails from retailers.
- Lower Attention: Spring Cleaning and Summer promotions might be less attention-grabbing compared to campaigns like Cyber Week, Black Friday, or Fall Fashion.

2.2 For User

Figure 6 provides insights into the results of simulated phishing campaigns conducted across the United States. This dashboard offers a centralized view of key metrics:

1. Process of Phishing outlines the phishing attack stages, showing a significant portion of users falling for the scam, underlining the urgency for enhanced training.
2. Average Risk Score by Demographic highlights states with varying levels of phishing awareness, with states.
3. Counts of Links Clicked by Age Group reveals that which age group is most likely to click phishing links.
4. Percentage of Links Clicked by Gender provide insights into gender-based differences in phishing susceptibility.
5. Key Influencers for Reporting Phishing demonstrates the effectiveness of anti-phishing training.
6. Average Previous Incidents by Reported Phishing indicates that users who do not or do not report phishing have a higher or low number of previous incidents.

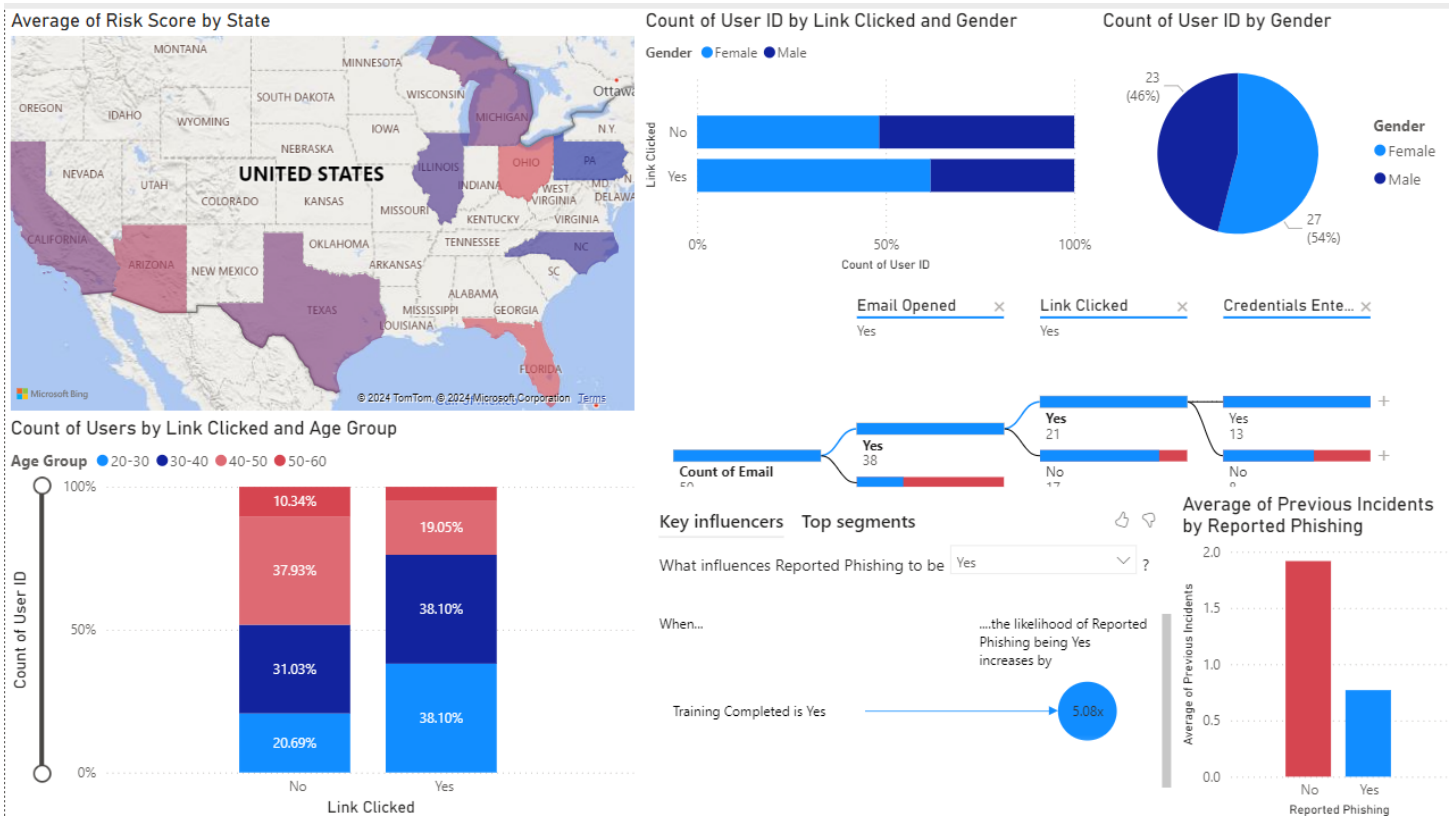

Figure 6 Individual User Dashboard

Chart 1

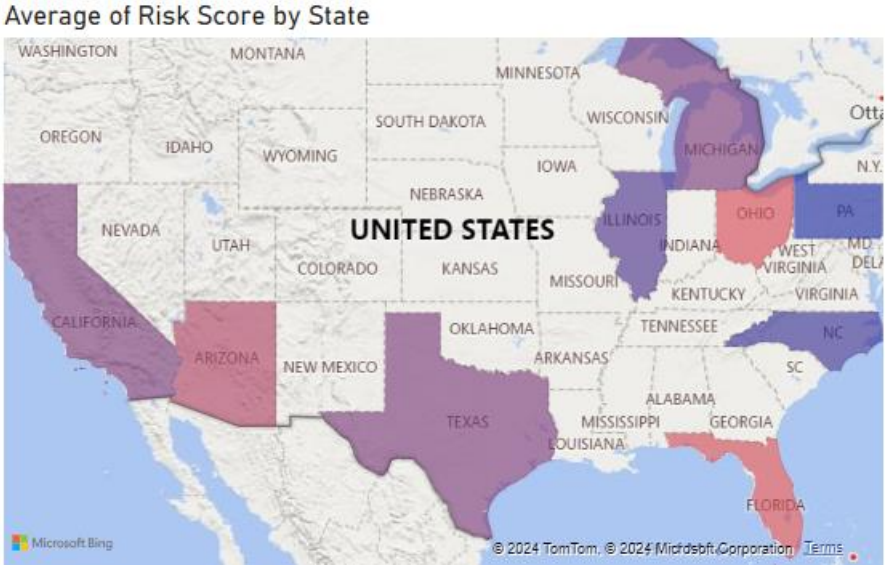

Figure 7 Average Risk Score by Demographic

Figure 7 shows the average risk score by state in the US. States shaded in blue have a lower average risk score than the states shaded in red. Florida, Ohio and Arizona have a higher average risk score. North Carolina, Pennsylvania and Illinois have a lower risk score. This indicates in offices in states like Florida, Ohio and Arizona, employees are less aware of the dangers of phishing attacks may have a higher risk score. There should be more focused training in these states.

Chart 2

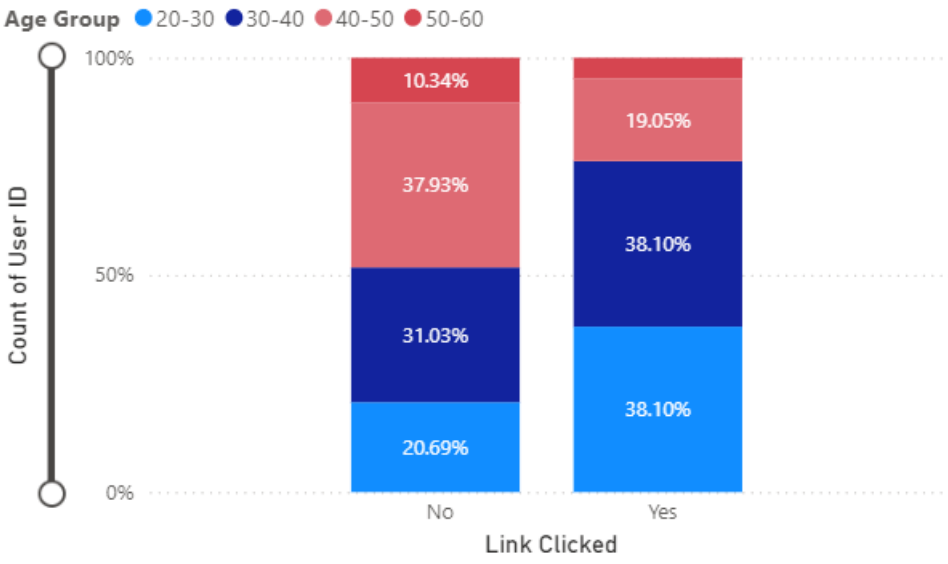

Figure 8 Counts of links clicked by age group.

Figure 8 shows the percentage of users who clicked on a link or not, broken down by age group. Users in the 20-30 age group are most likely to click the link. Users in the 50-60 age group are least likely to click the link for a phishing attempt.

There are a few reasons why younger users might be more likely to click on links in phishing emails.

- Less familiarity with phishing scams: Younger users may be less familiar with phishing scams and may be more trusting of emails that appear to be legitimate.
- More tech-savvy: Younger users may be more tech-savvy and may be more likely to click on links without thinking about the potential risks.

Chart 3

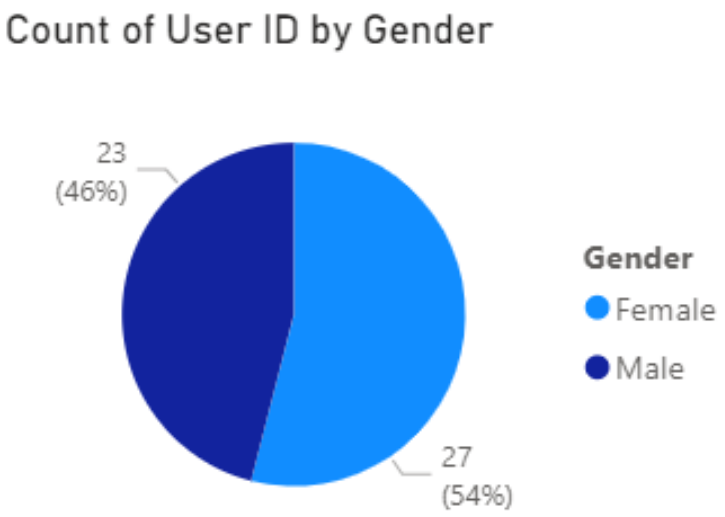

Figure 9 Percentage of Users by gender

Figure 9 shows the distribution of users by gender who participated in the campaign. There are slightly more males (54%) than females (46%) users.

Chart 4

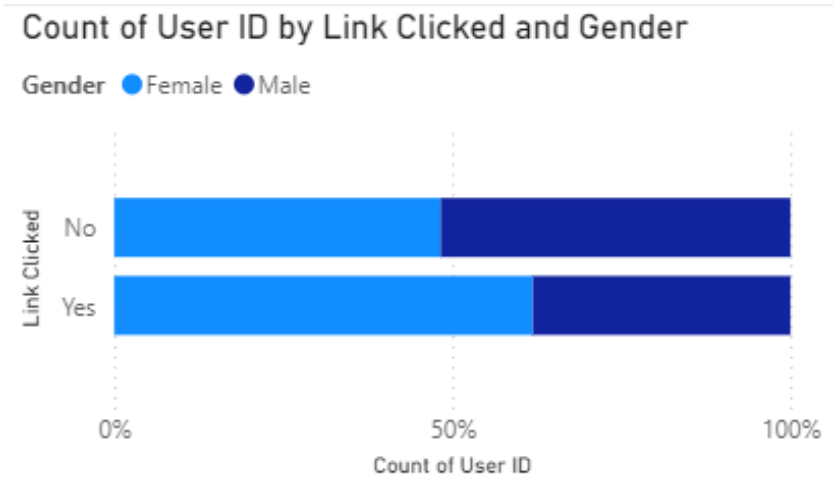

Figure 10 Percentage of links clicked by gender.

Figure 10 shows the percentage of users who clicked the link or not by gender. Females are much more likely to click on the link even though men have a larger overall sample size as seen in Figure 9. There are several possible reasons for this, such as:

- Women may be more likely to click on links in emails, especially if the email appears to be from a legitimate source.

- Phishing emails often use social engineering tactics to trick users into clicking on links. These tactics may be more effective on women than men.

Chart 5

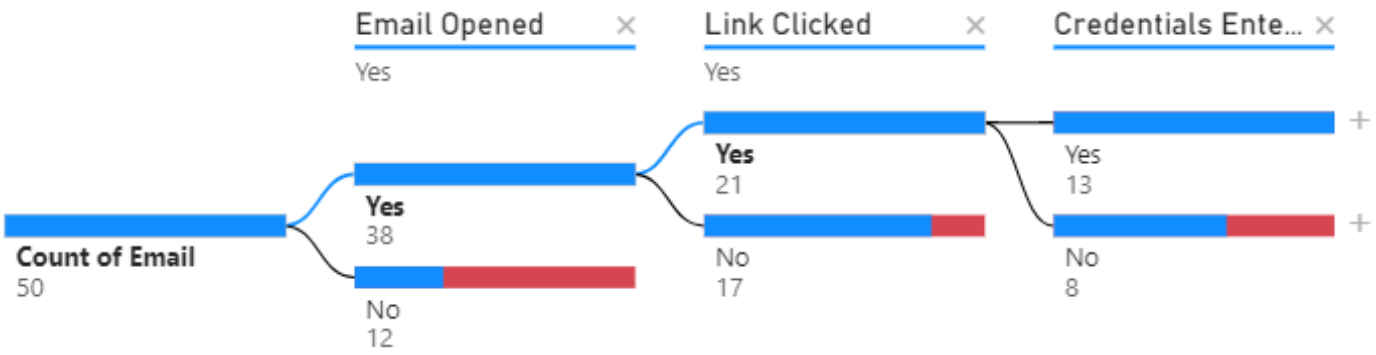

Figure 11 Process of Phishing

Figure 11 gives an overview of the process of phishing attacks.

1. Email Opened: 38 employees opened the email.
2. Link Clicked: 21 people clicked on the link that takes the victim to a fake website.
3. Credentials Entered: 13 people entered their details credentials (username and password).

The campaign was able to get the credential of 26% of participants in the campaign which is an alarming situation.

Chart 6

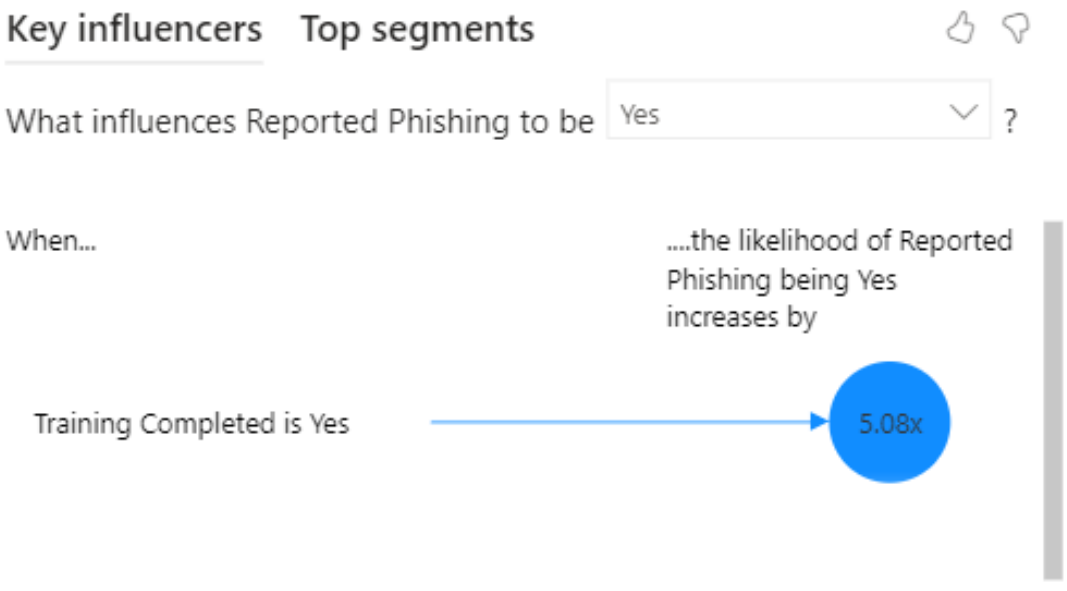

Figure 12 Key Influencer for Reporting Phishing

Figure 12 suggests that users who have completed the anti-phishing training are 5.08 times more likely to report a phishing attempt compared to users who haven't completed the training. Anti-phishing materials could be improved but they are surprisingly effective when users actually read them. (Lorrie Cranor, 2010)

Chart 7

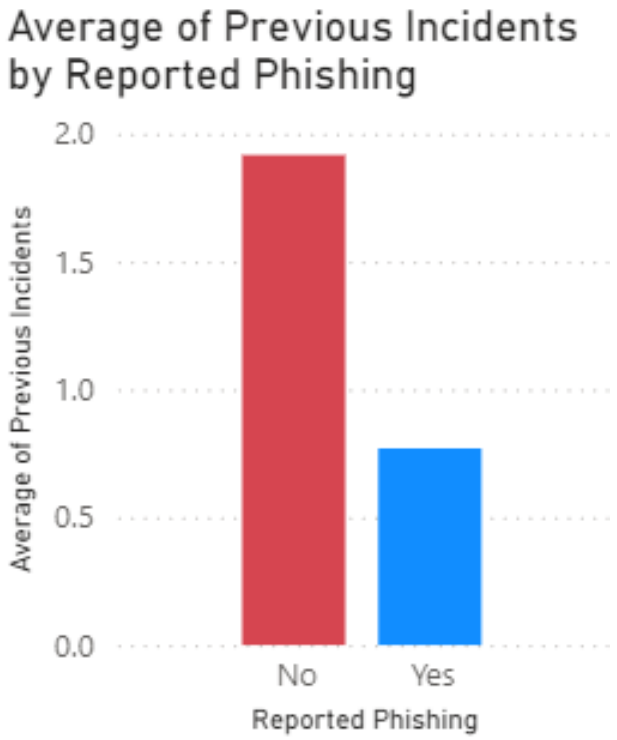

Figure 13 Average Pervious Incidents by reported phishing.

Figure 13 displays the average number of previous phishing incidents users have been involved in, broken down by whether they reported the current phishing attempt. This indicate that users who did not report have a higher average number of previous phishing incidents as well. Users who have been involved in more phishing incidents are still not aware of the tactics used by phishers and are unable to spot them repeatedly.

2.3 Dashboard 3: For HR Manager

This HR dashboard provides insights that can be used to identify high-risk departments and employees, allowing for targeted training and interventions to strengthen the organization's cybersecurity posture. This dashboard offers a centralized view of key metrics.

- **Employee Risk Level:** The dashboard segments employees by risk level (High, Moderate, Low) based on a combination of factors including department, previous incidents, and training completion. **Disciplinary Actions:** The dashboard shows the distribution of disciplinary actions taken in response to phishing incidents (None, Verbal Warning, Written Warning).
- **Department Risk:** The dashboard allows you to see the number of employees by department and risk level.
- **Training Completion:** The dashboard allows to determine what influences anti-phishing training completion rate.

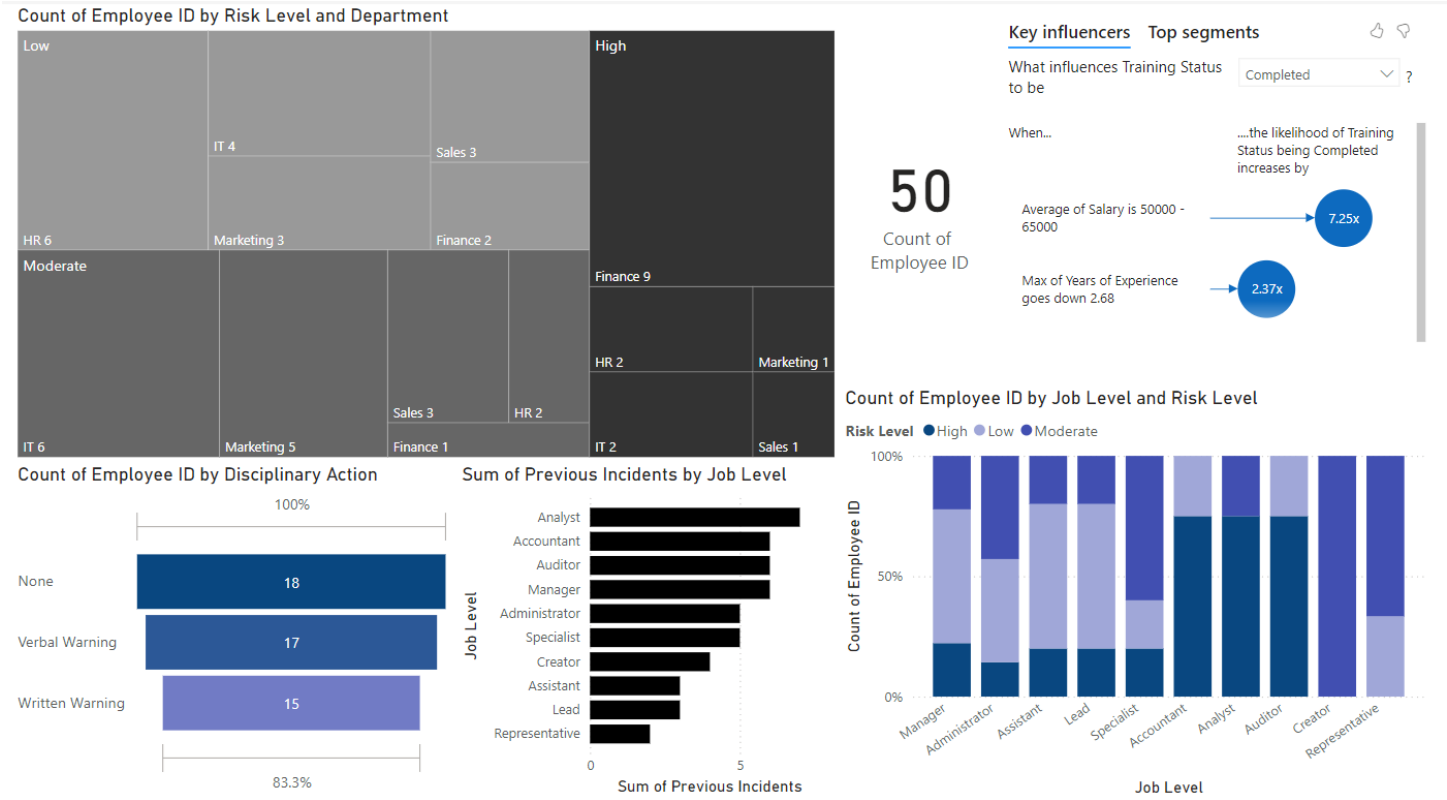

Figure 13 HR Manager Dashboard

Chart 1

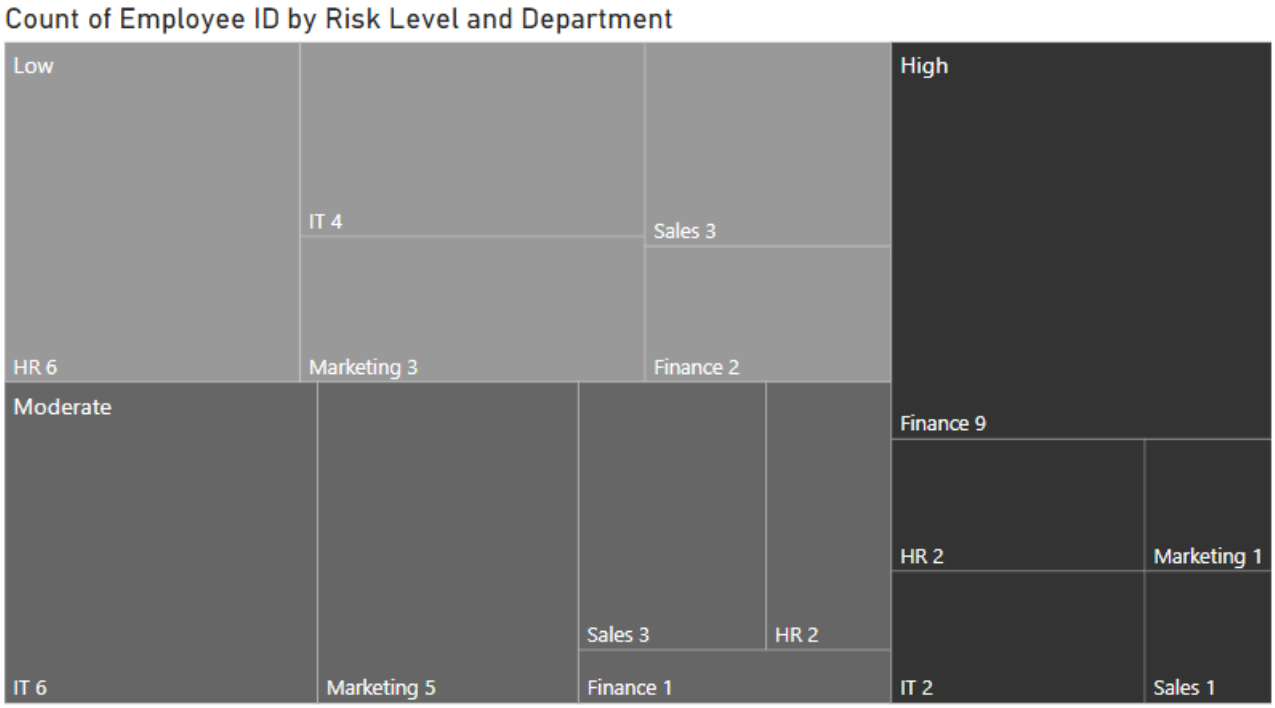

Figure 14 Number of Employees by risk level and department

Figure 12 shows the number of employees in each department categorized by their risk level. The department with the most employees overall is Finance (12 employees), but also has the most high-risk employees (9). IT

has the second most employees (12) with a more even distribution across risk levels (4 low risk, 6 moderate risks, and 2 high risk). Here are some additional insights you can glean from the data:

- Employees in Finance are more likely to be categorized as high risk.
- There are more employees in low-risk categories than moderate or high-risk categories.

Chart 2

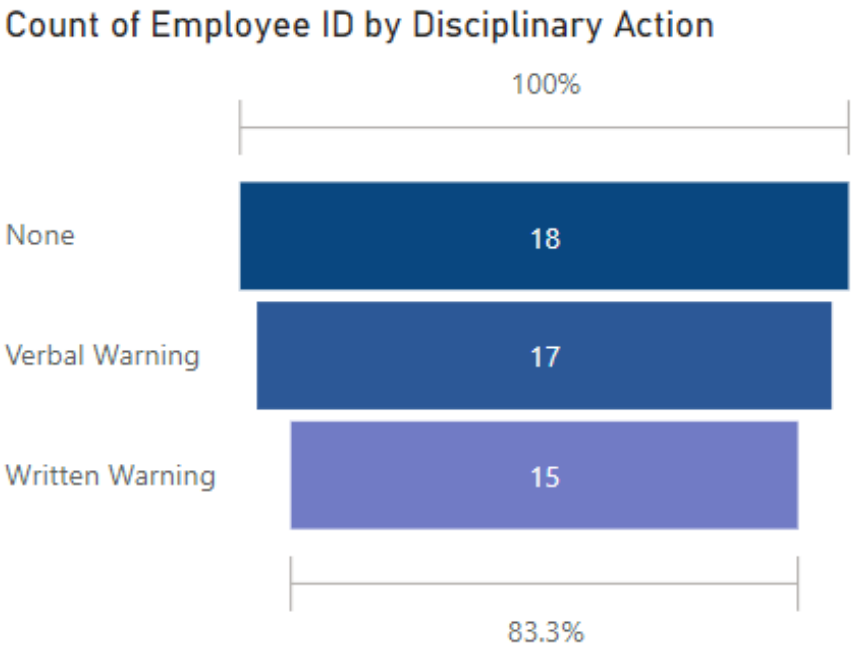

Figure 15 Number of Employees by Disciplinary Action

Figure 15 shows the number of employees by disciplinary action after successful phishing. No action has been taken for most employees for failing the training. Action should be me made mandatory for all employees so that there is higher attention to phishing emails.

Chart 3

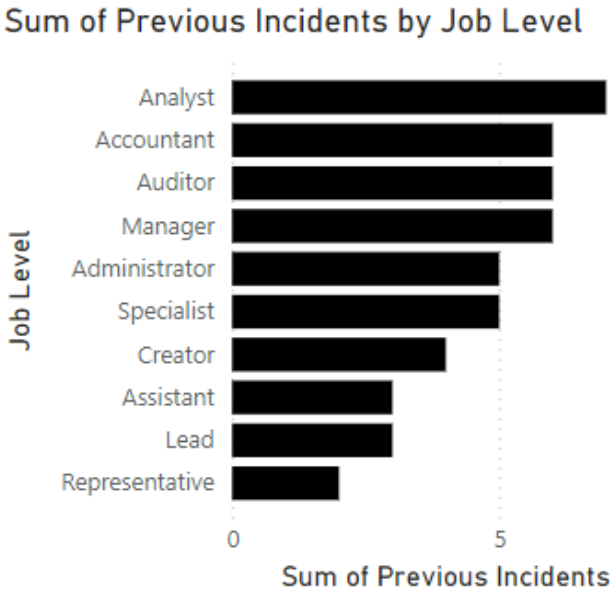

Figure 16 – Sum of previous incidents by job level

Figure 16 shows the total number of previous incidents for all employees in that job level. Analysts have the highest number of previous incidents followed by accountants, auditors and managers. More focus should be put on these job levels as they are more prone to fall for phishing emails. Managers have more responsibility for training others about cybersecurity best practices, so they may be held to a higher standard.

Chart 4

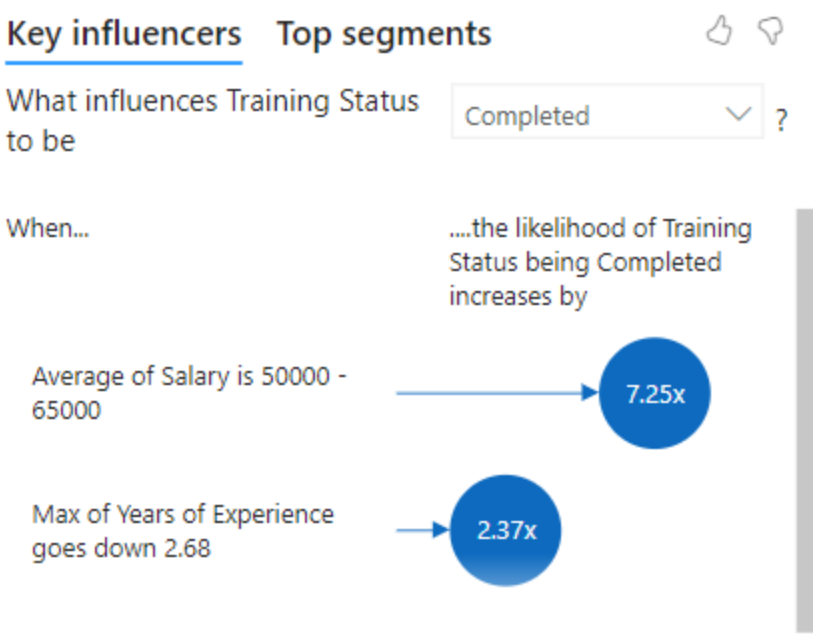

Figure 17 Key Influencers – Risk Level

Figure 17 is showing two of the biggest factors that contribute to an employee completing the training. The factors are:

- Average Salary: Employees with a salary in the range of 50,000 to 65,000 are 7.25 times more likely to have completed the training.
- Years of Experience: Employees with a lower maximum number of years of experience (less than 2.68) are 2.37 times more likely to have completed the training.

Training completion should be made mandatory.

Chart 5

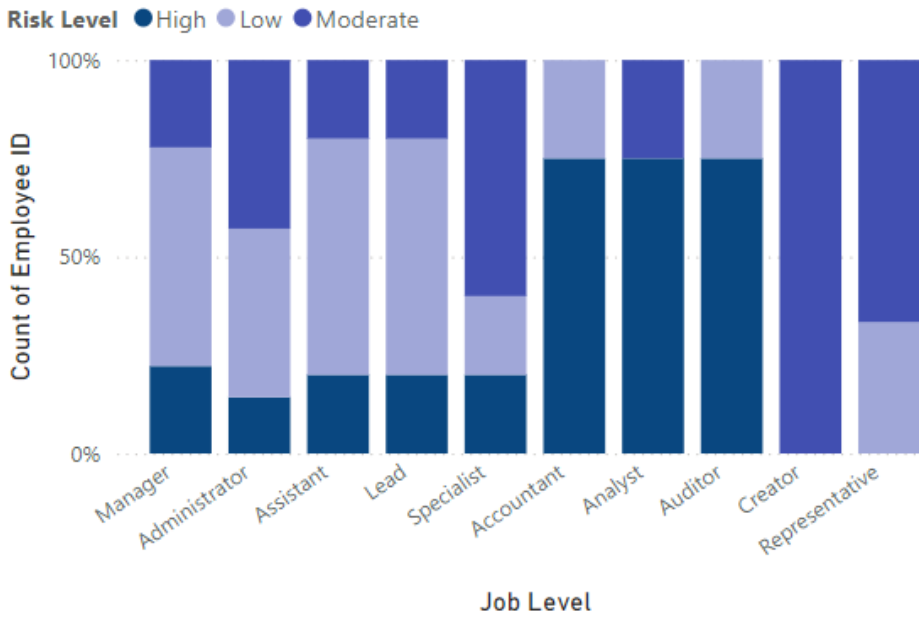

Figure 18 Risk Level by Job Level

Figure 18 shows the distribution of risk levels across different job titles. The chart shows that Accountants, Auditors, and Analysts are all categorized as having majority high risk employees in this phishing campaign. These roles might involve working with external parties or opening attachments more frequently, increasing the likelihood of encountering phishing attempts. Privileged users are one of the top targets for spear phishing attacks because of their access to sensitive information. (Anand, 2024)

3. Recommendations

Campaign Manager

1. Improve Training on High-Risk Attachments
   Issue: The dashboard shows that Excel files and Word documents have the highest link-click rates.
   Recommendation: Implement targeted training programs focusing on the dangers of opening attachments, particularly Excel and Word files, within phishing emails. Provide examples and simulations to help users recognize suspicious attachments. (Verizon, 2024)

2. Customize Campaigns Based on Template Performance
   Issue: Promotional offers and security alerts have the highest number of link clicks.
   Recommendation: Design and deploy additional training that includes mock phishing emails using these templates. Emphasize the tactics often used in these types of emails and educate users on how to spot red flags.

3. Enhance Regional Training Initiatives
   Issue: Australia has the highest number of successful logins, indicating higher susceptibility.
   Recommendation: Conduct region-specific training sessions, particularly in regions with higher phishing success rates. Tailor content to address regional behaviours and common phishing tactics relevant to that area.

User

1. Focus Training on High-Risk Age Groups
   Issue: Users in the 20-30 age group are most likely to click phishing links.
   Recommendation: Develop age-specific training programs that address the unique online behaviours and susceptibilities of younger users. Incorporate interactive and engaging methods to ensure better retention of information.

2. Address Gender-Specific Susceptibility
   Issue: Females are more likely to click on phishing links compared to males.
   Recommendation: Create awareness campaigns that consider gender-specific factors. Use data to inform training content and focus on scenarios where women might be more targeted.

3. Implement Continuous Awareness Programs
   Issue: Users who have completed anti-phishing training are significantly more likely to report phishing attempts.
   Recommendation: Make anti-phishing training mandatory and recurring. Ensure all employees undergo regular refresher courses to stay updated on the latest phishing tactics and best practices for avoiding them.

4. Reinforce Reporting Mechanisms
   Issue: Users with a higher number of previous incidents are less likely to report phishing.
   Recommendation: Simplify and promote the process of reporting phishing emails. Encourage a culture of vigilance and reward users who consistently report phishing attempts to improve overall awareness and responsiveness.

HR Manager

1. Target High-Risk Departments with Intensive Training
   Issue: Finance and IT departments have a higher number of high-risk employees.
   Recommendation: Implement focused training programs for high-risk departments, emphasizing the specific phishing threats relevant to their roles. Some visual deception attacks can fool even the most sophisticated users. (Dhamija, 2006)

2. Enforce Disciplinary Actions and Remedial Training
   Issue: Not all employees receive disciplinary actions for falling for phishing attempts.
   Recommendation: Establish a clear policy for disciplinary actions and ensure it is consistently enforced. Mandate remedial training for employees who fall victim to phishing to reduce future risk.

3. Address Key Influencers of Risk
   Issue: Higher salaries and more years of experience are linked to increased phishing risk.
   Recommendation: Investigate the reasons behind this correlation. Consider integrating phishing awareness and cybersecurity training into the onboarding process for new hires and regular training sessions for all employees, regardless of tenure or salary.

4. Monitor and Review Training Effectiveness
   Issue: Employees with fewer years of experience are more likely to complete training.

Recommendation: Regularly review and update training materials to ensure they are engaging and effective for all employees.

5. Reference

Anand, S. (2024). *Don't Be The Weakest Link In The Ongoing Battle Against Phishing Attacks.* KBI Media. Retrieved from https://kbi.media/dont-be-the-weakest-link-in-the-ongoing-battle-against-phishing-attacks/

Dhamija, R. T. (2006). *Why phishing works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* Retrieved from https://doi.org/10.1145/1124772.1124861

Jampen, D. G. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. Human-Centric Computing and Information Sciences. *SpringerOpen*. Retrieved from https://hcis-journal.springeropen.com/articles/10.1186/s13673-020-00237-7

Lorrie Cranor, P. K. (2010). *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions.* Retrieved from https://www.researchgate.net/publication/221514257_Who_falls_for_phish_A_demographic_analysis_of_phishing_susceptibility_and_effectiveness_of_interventions

Verizon. (2024). *Data Breach Investigations Report.* Verizon. Retrieved from https://www.verizon.com/business/en-au/resources/reports/dbir/?cmp=knc:ggl:ves_international:gm:awareness_ds_cid=71700000097472489_ds_agid=58700007917919528&utm_medium=&utm_source=google&utm_campaign=GGL_NB_AU_Nonbranded_Limited&utm_content=AU_Security_DB

Zainab Alkhalil, I. K. (2021). *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy.* Cardiff, United Kingdom: Cardiff Metropolitan University. Retrieved from https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full