CYBERSECURITY UMBRELLA

2023

Phishing Campaign Summary

Version Table	
Date	19 Dec 2023
Version	23.12.19
Analyst	Minhaj Saiyed
Reviewed by	Sajid Saiyed

CYBERSECURITY UMBRELLA

Table of Contents

1. Phishing Campaign Summary

Phishing Simulation Summary

This report outlines the results of Flipp's phishing simulation Campaign, which took place on **November 16, 2023**. The simulation employed the Cybersecurity Umbrella Phishing platform to evaluate the susceptibility of in-scope users to phishing attacks. Phishing attacks involve deceiving email users into clicking on a malicious link with the intent of gaining unauthorized access to the network.

The simulation was carried out to measure Flipp's vulnerability to users falling victim to highly targeted impersonation attacks through parameters like click rates and click times as shown below. This report aims to enhance Flipp's understanding of their users' behaviour towards Phishing attacks and to promote a more secure and resilient workforce.

Simulation Details:

Date of First Group Simulation: **November 16, 2023**

Date of Second Group Simulation: **November 28, 2023**

Date of Third Group Simulation: **December 14, 2023**

Date of Fourth Group Simulation: **December 15, 2023**

Methodology:

The simulation aimed to replicate real-world phishing scenarios to assess the preparedness and awareness of employees in identifying and responding to potential threats.

Phishing Simulation Summary

1. The report provides a summary of phishing emails, indicating the **count of users** who clicked the phishing link.
2. The phishing training summary outlines the number of users who attempted, did not attempt, and successfully completed the training.
3. The report includes a breakdown of the click counts on the phishing link by users.

2. Overall Summary of Phishing Email Clicked by Users

The chart illustrates the number of users who clicked on the phishing link and those who did not.

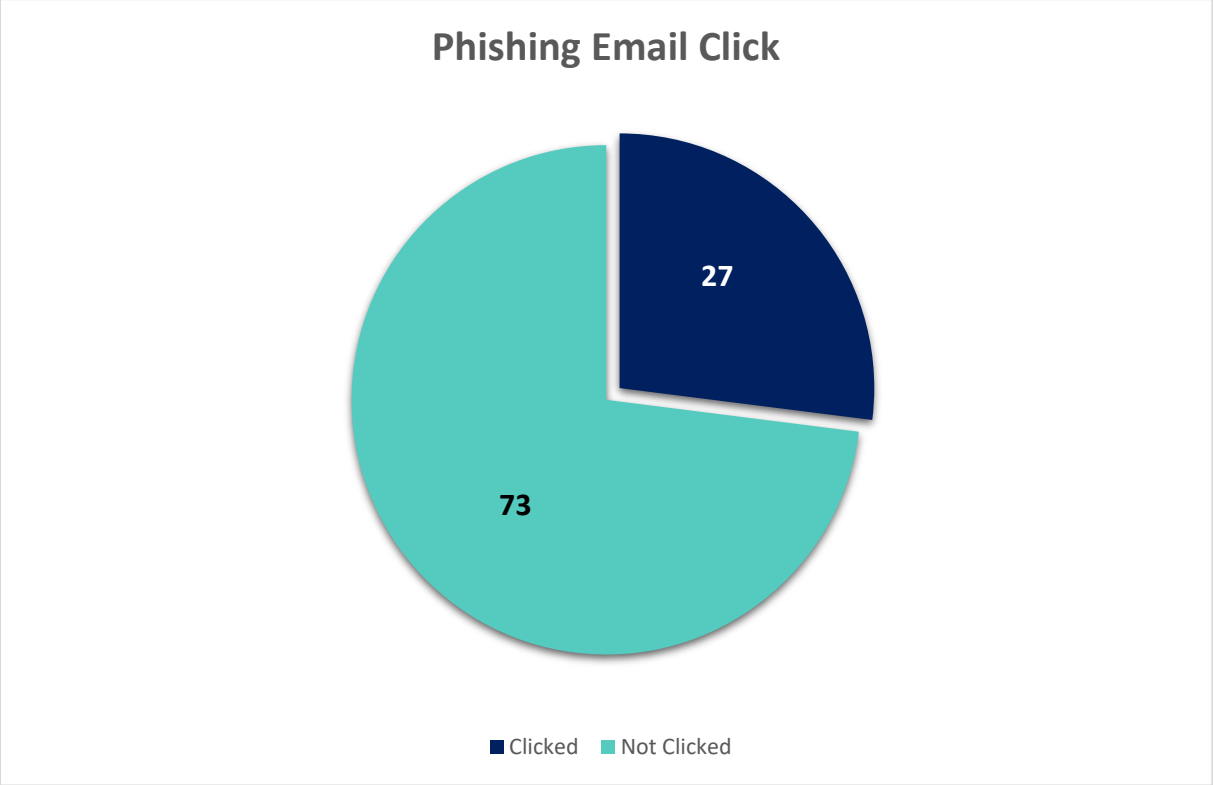


Figure 1 Phishing email click events.

- In the overall simulation encompassing all groups, a total of **100** users were participants.
- The data presented here is gathered from the combined results of the first three groups involved in the phishing campaign.
- Among the **100** participants, **27** individuals **(approximately 27%)** engaged with the phishing email by opening it and clicking the embedded link, subsequently falling victim to the simulated phishing attempt.
- Remarkably, the remaining **73** users **(73%)** exhibited a commendable level of resilience, demonstrating a cautious approach by refraining from interacting with the provided link. This reflects a robust awareness and preparedness against potential phishing attempts across all three groups.

3. Phishing Training Summary

The chart provides a visual breakdown of users who attempted and completed the phishing training, alongside those who did not participate at all.

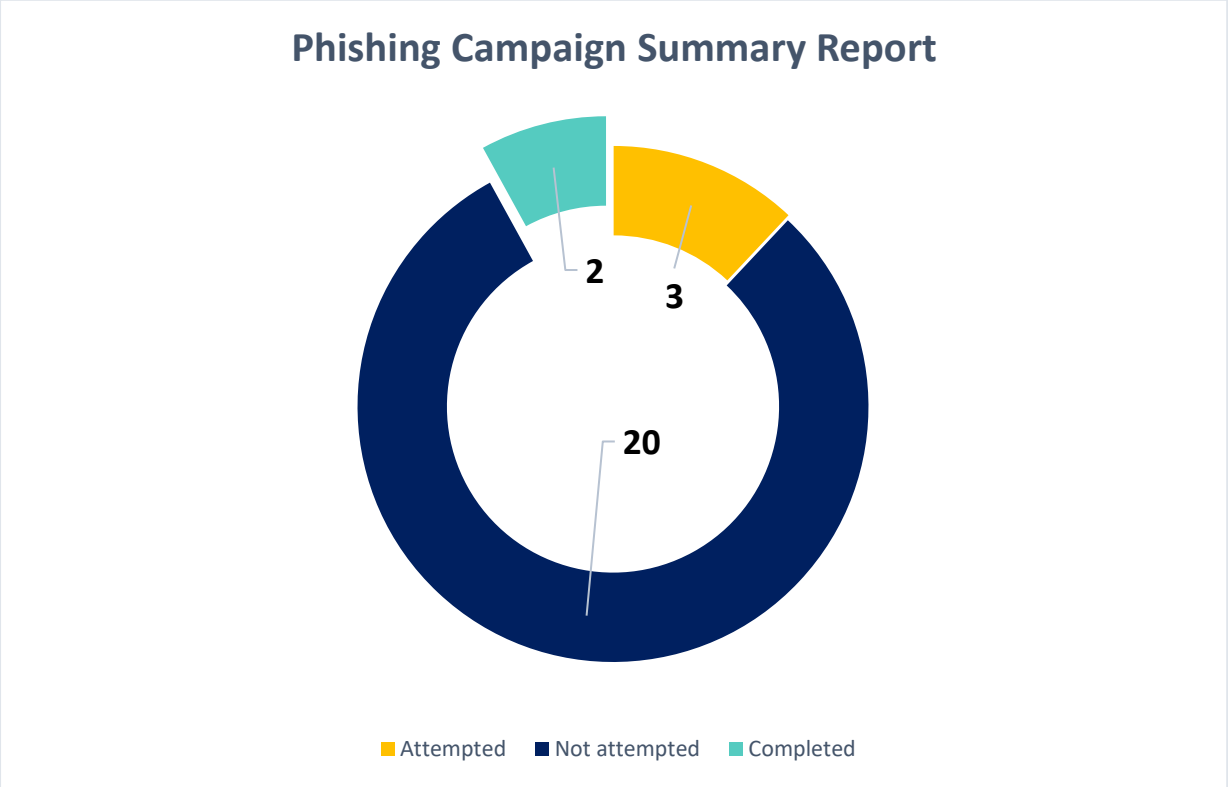


Figure 2 Phishing training attempts

- A total of **23** individuals have been identified as non-compliant users who clicked the phishing link in the email, leading to their enrolment in basic phishing training.
- Out of the users who initiated the training, a total of **3** individuals participated, with **2** successfully completing the entire training module.
- The remaining **27 users**, who were identified as defaulters, have yet to initiate any attempts to undergo the prescribed training.

I. Summary of Phishing training of according to user groups

The chart visually categorizes users based on their participation in the phishing training, distinguishing between those who attempted and completed the training, and those who did not participate at all, organized according to user groups.

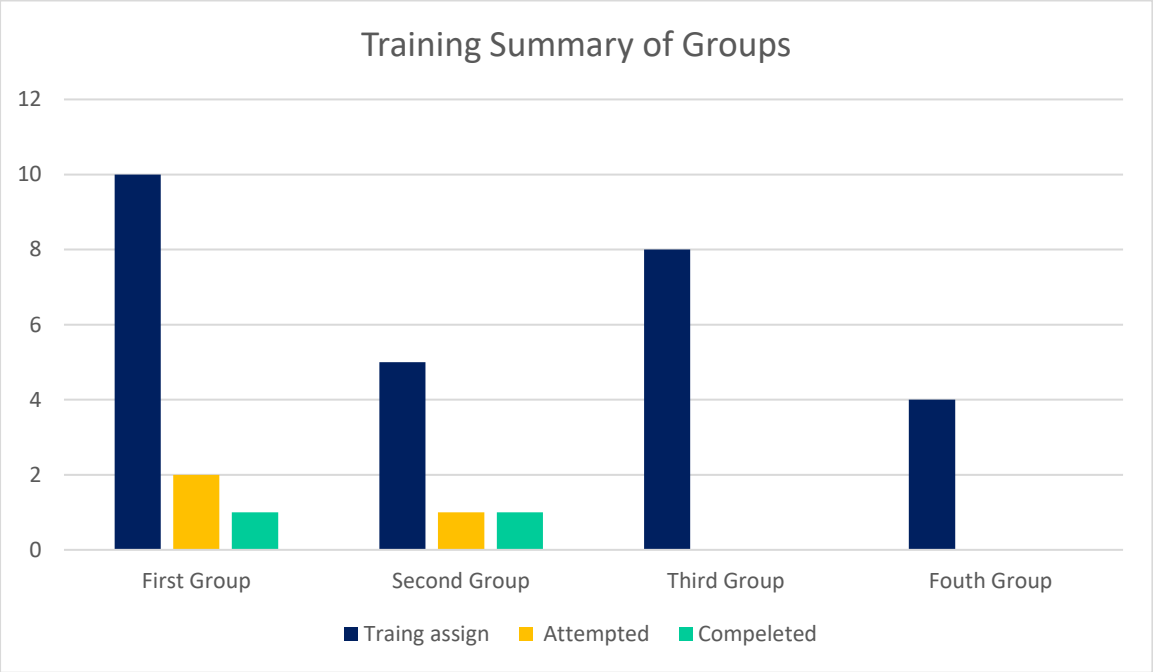


Figure 3 Training summary according to User groups

Name	Designation	Email	Training attempted/completed
Chanel Crawford	Sr. Team Lead, Operations	chanel.crawford@flipp.com	Completed
Cheyenne Jope	Team Lead, Operations	cheyenne.jope@wishabi.com	Completed
Adnela Fejzulovic	Sr. Digital Operations Coordinator	adnela.fejzulovic@flipp.com	Attempted

4. Phishing link Click Count by users.

The bar graph presented below visualizes the count of clicks attempted by users on the phishing link, categorized by groups.

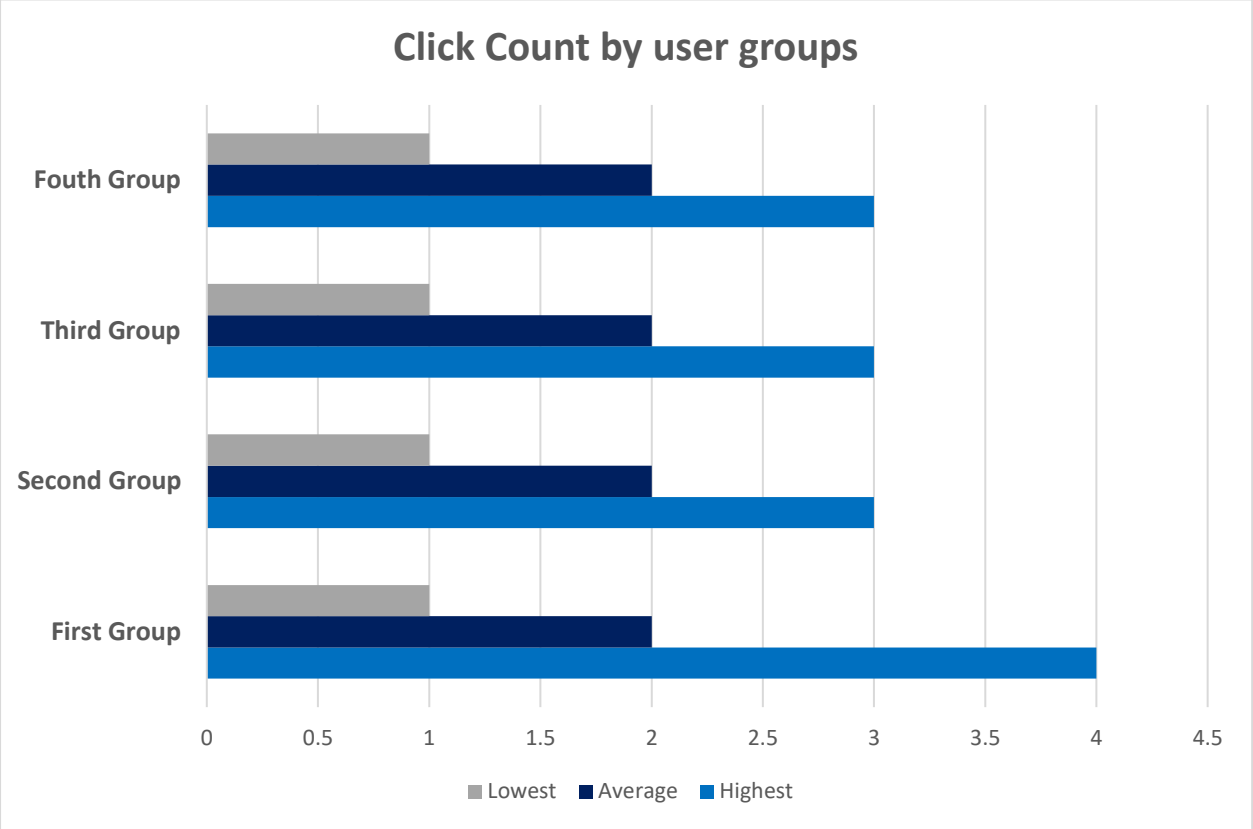


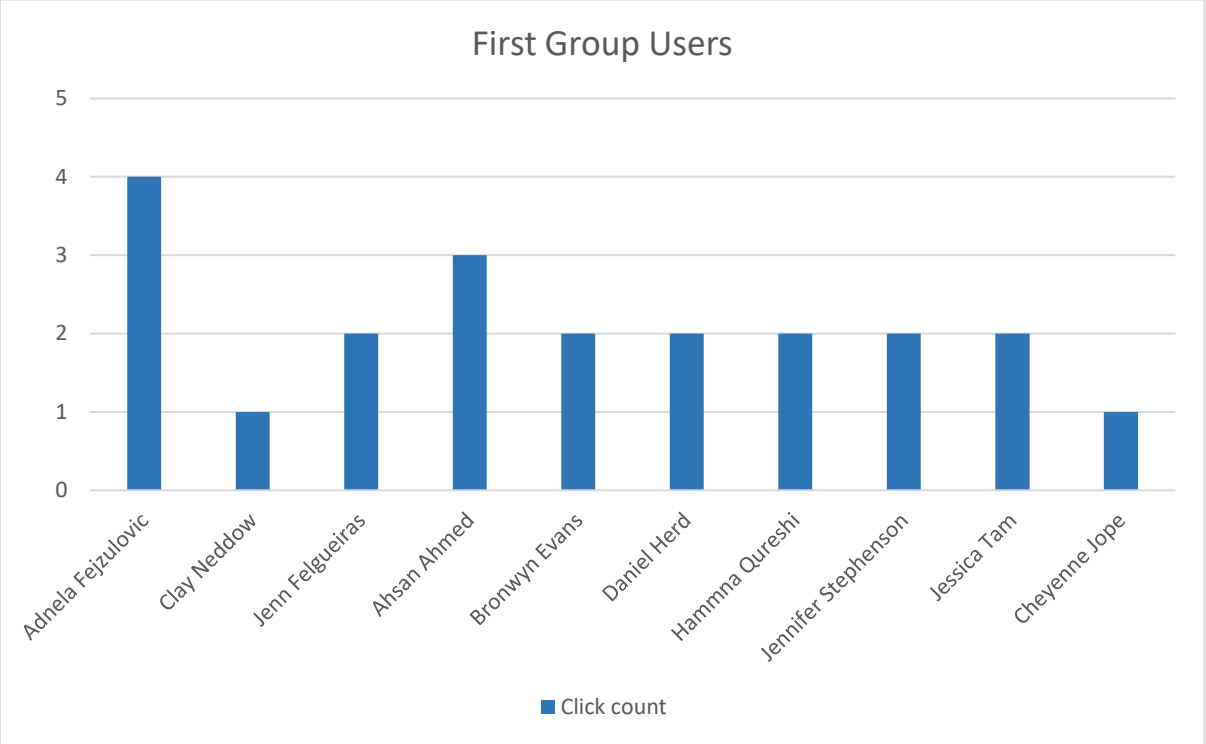
Figure 4 Click count by suers groups

- The data is organized into three groups for analysis.
- The first group shows a notable range with the **highest** click count at **4** and the **lowest** at **1**
- The other three groups exhibit a more consistent pattern, sharing similar **high (3)** and **low (1)** click counts.
- Despite these variations, all three groups present similar average and low click counts.
- For more detailed insights, refer to the table below, which includes usernames, emails, and designations associated with the respective click counts.

5. Users Group who clicked the link

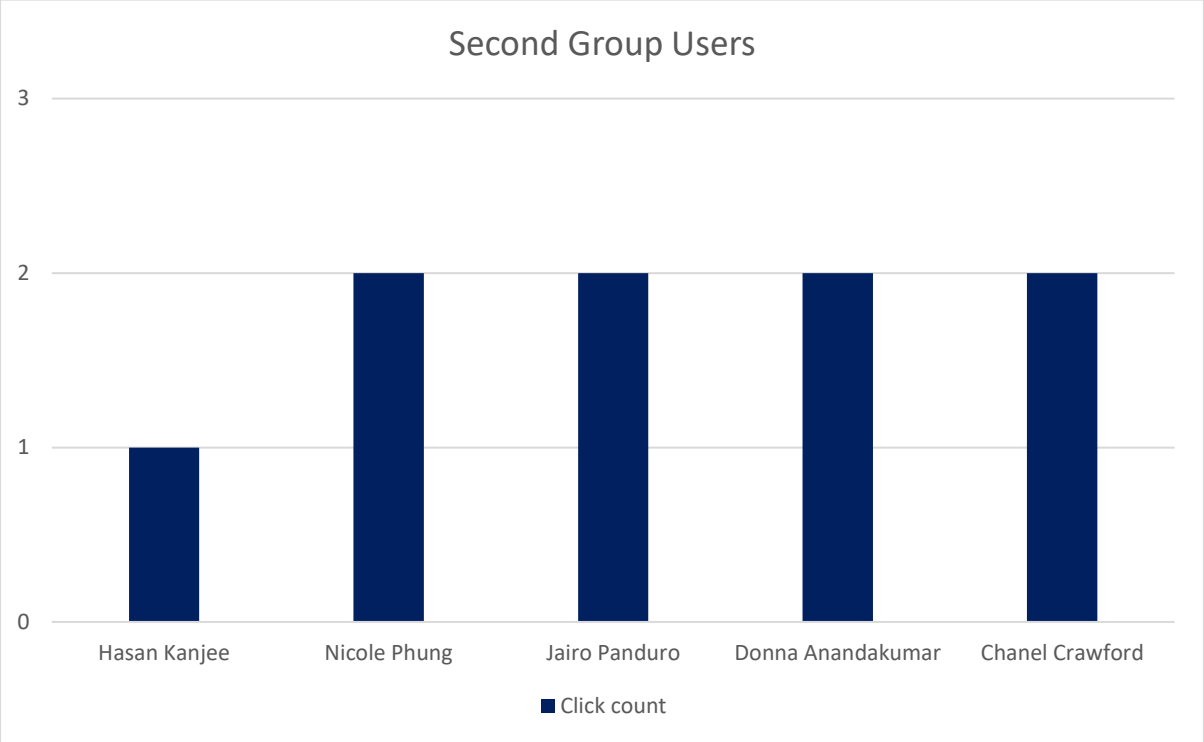
i. First Group Defaulters

- The displayed chart offers a visual depiction of user interaction within the **first group**, specifically emphasizing those who clicked on the phishing link.
- Notably, a total of **10 users** from the first group exhibited engagement by clicking on the provided link during the phishing simulation.
- This targeted phishing simulation was conducted within **Flyers Operation**, focusing on assessing the first group's susceptibility to such attacks.
- In summary, the data indicates that **10** out of **25** users in the first group clicked on the phishing link. This engagement rate provides insights into the group's awareness levels, showcasing areas for potential improvement.



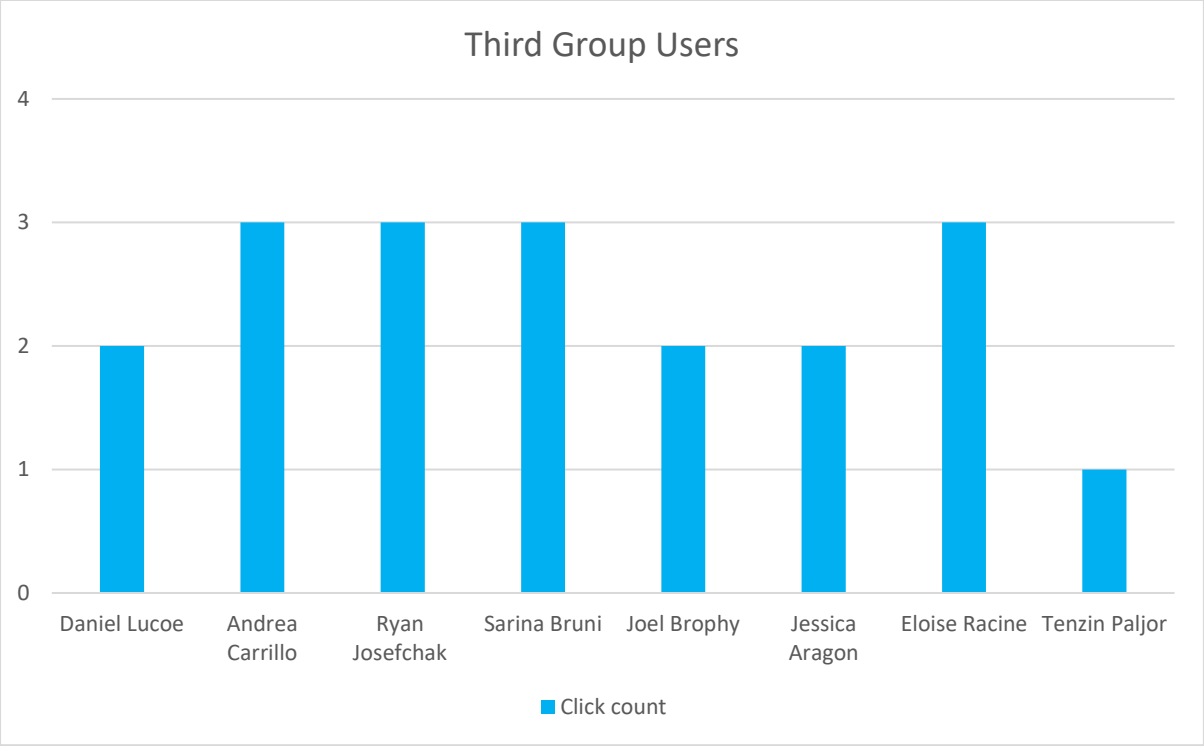
ii. Second Group Defaulters

- The presented chart provides a visual representation of user engagement within the **second group**, specifically highlighting those who clicked on the phishing link.
- Notably, a total of **5 users** from the second group demonstrated engagement by clicking on the provided link during the phishing simulation.
- This targeted phishing simulation was conducted within the **Engineering channel**, focusing on assessing the group's susceptibility to such attacks.
- In summary, the data indicates that only **5** out of **25 users** in the second group clicked on the phishing link. This low engagement rate is a positive outcome, showcasing a commendable level of awareness and resilience within the group**.**



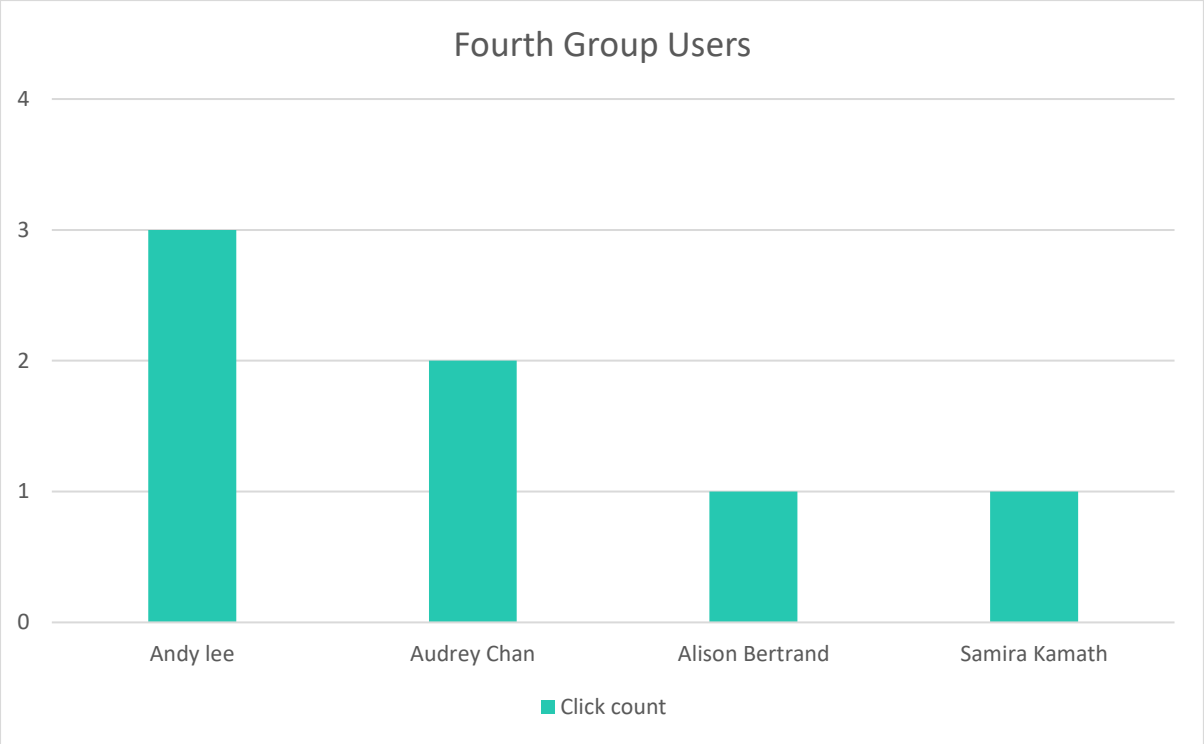
iii. Third Group Defaulters

- The presented chart visually illustrates user interactions within the **third group**, specifically highlighting those who engaged by clicking on the phishing link.
- Significantly, a total of **8 users** from the third group demonstrated engagement by clicking on the provided link during the phishing simulation.
- This targeted phishing simulation was conducted within the **Business Development Department**, focusing on assessing the first group's susceptibility to such attacks.
- In summary, the data indicates that **8 out of 25 users** in the first group clicked on the phishing link. This engagement rate sheds light on the group's awareness levels, revealing areas for potential improvement.



iv. Fourth Group Defaulters

- The presented chart visually illustrates user interactions within the **fourth group**, specifically highlighting those who engaged by clicking on the phishing link.
- Significantly, a total of **4 users** from the third group demonstrated engagement by clicking on the provided link during the phishing simulation.
- In summary, the data indicates that **4 out of 25 users** in the fourth group clicked on the phishing link. This engagement rate sheds light on the group's awareness levels, revealing areas for potential improvement.



6. List of Users with click counts

Employee Name	Designation	Employee Mail	Mail Clicked Count
Adnela Fejzulovic	Sr. Digital Operations Coordinator	adnela.fejzulovic@flipp.com	4
Clay Neddow	Digital Operations Lead	clay.neddow@flipp.com	1
Jenn Felgueiras	Team Lead, Operations	jenn.felgueiras@flipp.com	2
Ahsan Ahmed	Digital Operations Lead	ahsan.ahmed@flipp.com	3
Bronwyn Evans	Sr. Digital Operations Coordinator	bronwyn.evans@flipp.com	2
Daniel Herd	Data Quality Analyst	daniel.herd@flipp.com	2
Hammna Qureshi	Digital Operations Lead	hammna.qureshi@flipp.com	2
Jennifer Stephenson	Sr. Digital Operations Lead	jennifer.stephenson@flipp.com	2
Jessica Tam	Sr. Digital Operations Coordinator	jessica.tam@flipp.com	2
Cheyenne Jope	Team Lead, Operations	cheyenne.jope@wishabi.com	1
Hasan Kanjee	Sr. Software Engineer	hasan.kanjee@flipp.com	3
Nicole Phung	Software Engineer II	nicole.phung@flipp.com	1
Jairo Panduro	Sr. Software Engineer	v-jpanduro@flipp.com	2
Donna Anandakumar	Digital Operations Lead	donna.anandakumar@flipp.com	2
Chanel Crawford	Sr. Team Lead, Operations	chanel.crawford@flipp.com	2
Daniel Lucoe	Partner Account Lead	daniel.lucoe@flipp.com	2
Andrea Carrillo	Sr. Director, Partner Development	andrea.carrillo@flipp.com	3
Ryan Josefchak	Partner Account Lead	ryan.josefchak@flipp.com	3
Sarina Bruni	Sales Enablement Manager	sarina.bruni@flipp.com	3
Joel Brophy	Partner Account Lead	joel.brophy@flipp.com	2
Jessica Aragon	Business Development Lead	jessica.aragon@flipp.com	2
Eloise Racine	Sr. Partner Account Lead	eloise.racine@flipp.com	3
Tenzin Paljor	IT Support	tenzin.paljor@flipp.com	1
Audrey Chan	Sr. Partner Account Lead	audrey.chan@flipp.com	2
Andy Lee	Staff Software Engineer in Test	andy.lee@flipp.com	3
Samira Kamath	Digital Operations Lead	samira.kamath@flipp.com	1
Alison Bertrand	Software Engineer II	alison.bertrand@flipp.com	1

- The table displays how users interacted with the phishing link, showing a variety of click counts. The highest number of clicks was **4**, and the lowest was **1**. This diversity in responses highlights varying levels of susceptibility to the simulated phishing scenario. Analyzing these click counts provides insights for improving cybersecurity awareness and resilience among users.

THANK YOU FOR TAKING THE TIME TO REVIEW THIS REPORT

Your feedback is valuable to us,

In case you require more details regarding any topic please do not hesitate to reach out to us

support@cybersecurityumbrella.com

soc@cybersecurityumbrella.com