Open Pharma

Deployment plan for enhancing information security at OpenPharma

LUIS CRUZ GRC ANALYST FEB 2025

Open Pharma

- Developing a comprehensive deployment plan for the User Charter is essential to ensure all OpenPharma employees are informed, understand, and commit to the organization's information security policies. This plan aligns with OpenPharma's culture of scientific excellence, formal communication, and meticulous documentation, as outlined in the company culture brief.

1. Communication strategy

Formal Announcement via Email:

- Distribute the User Charter to all employees through the company's Gmail system.
- The email will include a brief overview of the charter's importance and a direct link to the document stored in Notion.

Integration into Notion:

- Upload the User Charter to Notion, ensuring it is accessible to all employees.
- Notion serves as the central repository for company policies and procedures, aligning with our commitment to meticulous documentation.

All-Hands Meeting:

- Schedule a company-wide meeting via Google Calendar, utilizing Zoom or Google Meet for virtual attendance.
- During this meeting, leadership will present the User Charter, emphasizing its significance and addressing any questions.

Open Pharma

2. Confirmation of agreement

Open Pharma

- Electronic Acknowledgment:
  - Utilize DocuSign to facilitate electronic signatures from employees, confirming their agreement to abide by the User Charter.
  - This method ensures secure and verifiable acknowledgment, consistent with our formal communication practices.

3. Tracking and documentation

- Monitoring Compliance:
- Track the distribution and acknowledgment process using Asana, our project management tool. The email will include a brief overview of the charter's importance and a direct link to the document stored in Notion.
- Asana will help monitor which employees have received, read, and signed the User Charter, ensuring comprehensive compliance

- Handling Non-Compliance:
- For employees who have not acknowledged the User Charter within the specified timeframe, send reminder emails via Gmail.
- If non-compliance persists, escalate the issue to the respective department heads for further action.

Open Pharma

4. Collaboration with departments

- **Human Resources (HR):**
- Work closely with HR to integrate the User Charter acknowledgment into the onboarding process for new hires.
- Ensure that the User Charter is part of the mandatory training modules.

- **Information technology (IT):**
- Coordinate with the IT department to manage the distribution of the User Charter and monitor electronic acknowledgments.
- Ensure that all digital platforms used in this process are secure and functioning correctly.

Open Pharma

Ensuring Comprehensive Compliance

Regular Updates:

- Periodically review and update the User Charter to reflect any changes in policies or regulations
- Communicate updates to all employees through the established channels and require re-acknowledgment if necessary.

Feedback Mechanism:

- Encourage employees to provide feedback on the User Charter and its implementation.
- Use SurveyMonkey to collect feedback and make improvements as needed.

Tools and Channels Utilized

- **Gmail:** For formal communication and distribution of the User Charter.
- **Notion:** To store and provide access to the User Charter and related documentation.
- **Google Calendar:** To schedule the all-hands meeting for the User Charter presentation.
- **Zoom/Google Meet:** For virtual meetings to discuss the User Charter.
- **DocuSign:** To obtain and store electronic signatures from employees.
- **Asana:** To track the acknowledgment process and ensure compliance.

By following this deployment plan, OpenPharma ensures that all employees are informed, understand, & commit to the User Charter, thereby strengthening the organizations security posture.

Phishing Awareness Communication Plan

This plan aims to inform and educate employees who interacted with the simulated phishing email, reinforcing the importance of cybersecurity awareness and adherence to best practices

Open Pharma

Summary of the Recent Phishing Campaign

To evaluate and strengthen OpenPharma's defenses against phishing threats, our security team conducted a simulated phishing exercise.

An email masquerading as a Zoom notification, promoting new features, was sent to all employees.

Key Objectives:

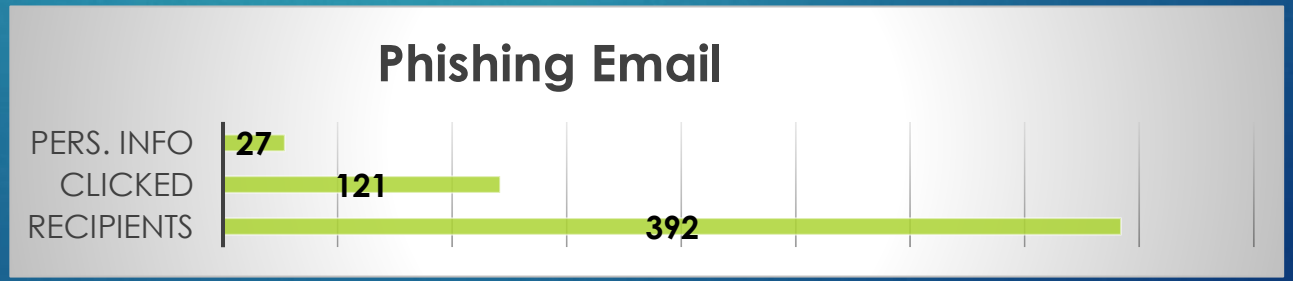
- Assess employees' ability to identify phishing attempts.
- Pinpoint areas needing enhancement in our cybersecurity training.

Findings:

- A considerable number of employees clicked the link in the deceptive email.
- Several individuals entered personal details on the fake website.

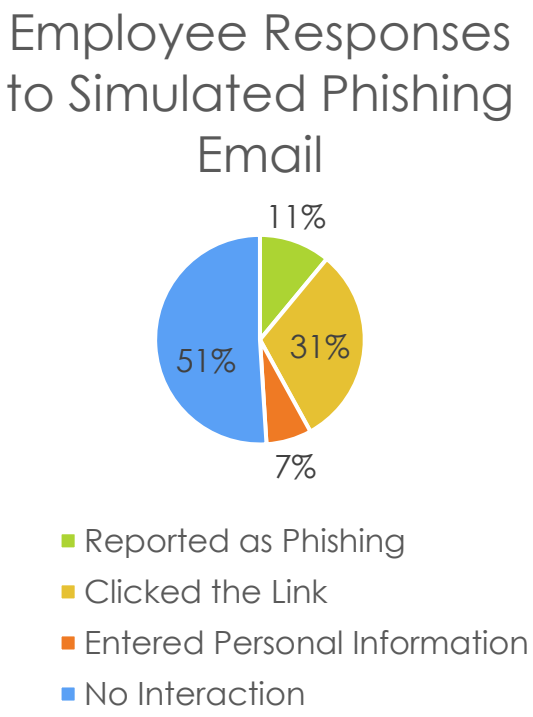
Potential Risks:

- In real-world scenarios, such actions could lead to unauthorized access to sensitive company information, financial losses, and damage to our reputation.



Open Pharma

Analysis of Campaign Results



The data collected from the simulation provides insight into the organization's current cybersecurity posture:

Reporting Rate: A portion of employees recognized the email as suspicious and reported it to the security team.

Click Rate: A notable percentage of employees clicked on the link within the email, indicating susceptibility to phishing tactics.

Submission Rate: A subset of those who clicked further compromised security by submitting their credentials.

This analysis highlights the need for targeted educational initiatives to bolster employees' ability to detect and appropriately respond to phishing attempts.

Open Pharma

Communication Strategy & Channels

•**Personalized Notifications:** Send individualized emails to employees who engaged with the phishing simulation, detailing their actions and potential security implications.

•**Educational Workshops:** Organize mandatory training sessions focusing on phishing identification, prevention strategies, and proper reporting procedures.

•**Resource Distribution:** Provide quick reference guides and access to online modules to reinforce learning and support continuous improvement.

•**Communication Channels:**
•*Email Correspondence:* Utilize company email for official communications and personalized feedback.
•*Intranet Portal:* Host resources, training schedules, and reporting tools on a dedicated section of the company's intranet.
•*Virtual Meetings:* Conduct interactive workshops and Q&A sessions through the company's preferred virtual meeting platforms.

Open Pharma

Corrective Actions for Involved Employees

Immediate Feedback: Inform employees promptly upon failing a phishing simulation, providing clear explanations of what was missed to facilitate immediate learning.

Remedial Training: Assign specialized cybersecurity courses designed to enhance phishing detection skills, ensuring the content differs from previous training to maintain engagement and effectiveness.

Escalation Process for Repeat Failures:

- **Second Failure:** Require additional training and a meeting with the employee's manager to discuss the risks associated with phishing and strategies for improvement.
- **Third Failure:** Involve Human Resources to implement further actions, which may include more intensive training or other appropriate measures.

Follow-Up Assessments: Conduct subsequent phishing simulations to evaluate progress, reinforce learning outcomes, and identify any persistent vulnerabilities.

Open Pharma

Recommendations for Prevention

Strategies to Prevent Phishing Attacks

For Individual Users:

Maintain Vigilance: Be cautious with unsolicited communications, especially those urging immediate action or requesting sensitive information.

Verify Sender Identities: Double-check email addresses and avoid clicking on links or downloading attachments from unknown or suspicious sources.

Utilize Available Resources: Stay informed about emerging threats by participating in regular training sessions and consulting the company's cybersecurity guidelines.

For the Security Team:

Regularly Update Training Materials: Ensure that educational content reflects the latest phishing techniques and incorporates real-world examples to enhance relevance.

Conduct Periodic Simulations: Implement regular phishing simulations to assess and improve organizational resilience, adapting strategies based on the outcomes.

Enhance Email Filtering Systems: Implement advanced email filtering solutions to detect and block potential phishing attempts before they reach employees' inboxes

Thank You

By implementing this communication plan, OpenPharma aims to foster a culture of cybersecurity awareness, ensuring all employees are equipped to recognize and thwart phishing attempts effectively.

Open Pharma