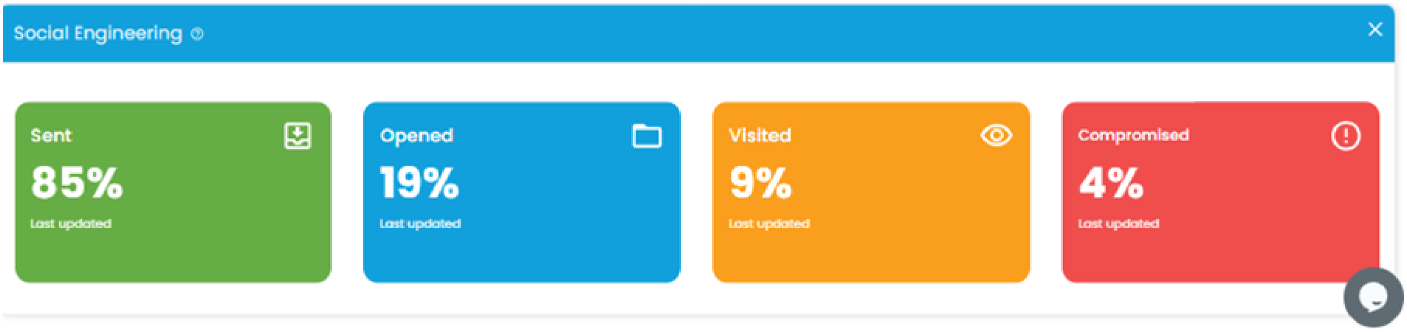
Social Engineering

This section offers a comprehensive overview of your organization's resilience against social engineering attacks, particularly simulated phishing campaigns. Here's what you can expect:

- **User Engagement Metrics**: Gain insights into user behavior during simulated phishing campaigns, including the percentage of users who have opened, visited, and compromised by interacting with simulated phishing emails.
- **Quantitative Analysis**: Track the effectiveness of your organization's security awareness training and phishing simulation programs by analyzing user engagement metrics, allowing you to measure progress over time and identify areas for improvement.
- **Risk Assessment**: Assess the susceptibility of your workforce to social engineering attacks and prioritize training efforts based on the percentage of compromised users, ultimately strengthening your organization's defenses against real-world threats.
- **Educational Opportunities**: Use the data provided to tailor targeted training initiatives, educate users about the dangers of phishing, and promote a culture of cyber security awareness and vigilance across your organization.



Sent
85%
Last updated

Opened
19%
Last updated

Visited
9%
Last updated

Compromised
4%
Last updated

By leveraging this section, you can proactively address vulnerabilities related to social engineering, empower users to recognize and report phishing attempts, and bolster your organization's overall resilience to cyber threats. Explore the insights provided to refine your security awareness training programs and enhance your organization's security posture.

Revision #1
Created 19 April 2024 03:16:29
Updated 19 June 2024 06:53:45