501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC

PHISHING TESTING AND TRAINING PROGRAM BEST PRACTICES

1. Planning Your Campaign

Define Clear Objectives: Establish what you aim to achieve, such as improving threat detection skills or reducing susceptibility to phishing attacks.

Segment Your Audience: Differentiate simulations for various groups within the organization based on their role, department, or past performance in phishing simulations.

2. Setting Up the Campaign

Customize Email Templates: Employ a variety of phishing templates that reflect real-world threats, ensuring they are relevant and diverse in style to avoid predictability.

Utilize Smart Groups: Segment users based on their interaction with past phishing tests (e.g., clicked once, twice, or three times or more in the last 12 months), with special attention to the "High Risk" group who clicked three times or more.

Decide on Training Content: Select or design training modules tailored to different user groups, with unique, more intensive training for the High Risk group.

Schedule Campaigns Wisely: Distribute the sending of phishing simulations over at least one week to prevent pattern recognition and ensure a more natural distribution.

3. Executing the Campaign

Perform a Technical Check: Confirm that your email and network setup allows the phishing emails to be delivered effectively.

Launch a Pilot Test: Conduct a preliminary test on a small group to ensure all elements of the campaign work as planned.

Communicate with Stakeholders: Notify IT, management, and other relevant parties about the campaign to secure their support and avoid misunderstandings.

4. Enhancing Engagement and Accountability

Copy Managers on Notifications: When users fail a phishing test and are assigned training, automatically notify their managers to increase accountability.

Collaborate with Leadership: Work with executive sponsors or leadership to share phishing statistics and campaign results at regular company meetings, fostering a culture of transparency and collective responsibility.

Create and Communicate a Goal: Work with executive sponsors to identify a company-wide phishing success goal, such as 98% no-failures. Track and share statistics against this goal at company meetings.

501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC

PHISHING TESTING AND TRAINING PROGRAM BEST PRACTICES

5. Post-Campaign Analysis

Review the Results: Analyze campaign data to identify trends, vulnerabilities, and overall training effectiveness.

Provide Constructive Feedback: Share individual and group results in a way that encourages learning and improvement, not punishment.

Adjust Training and Campaigns Based on Insights: Use the insights gained to refine future phishing simulations and training content.

6. Continuous Improvement

Iterate on Content and Techniques: Regularly update your phishing scenarios and training materials to keep pace with evolving threats.

Foster a Security Culture: Promote an environment where reporting phishing attempts is encouraged and supported.

Track Long-term Progress: Monitor behavioral changes and the organization's phishing resilience over time to gauge the effectiveness of your training program.

7. Legal and Ethical Considerations

Ensure Privacy Compliance: Adhere to all relevant privacy laws and regulations in your phishing campaigns.

Be Ethical in Your Approach: Avoid using distressing or overly personal content in phishing simulations to prevent undue stress.

By integrating these practices, you not only tailor the training to the unique needs and risks of different user groups within your organization but also enhance overall engagement with cybersecurity initiatives, ensuring a more secure and informed workplace.

For more info, contact: **info@501ciso.com**

501CISO
501C CYBERSECURITY LEADERSHIP