LAB- HOW: Establishing an Enterprise Simulated Phishing Program

The purpose of this lab is to document how you will create, and embed, a successful simulated phishing program.

Background

1. How many employees work at your organization?

☐ 0-999

☐ 1,000-4,999

☐ 5,000-24,999

☐ 25,000-49,999

☐ 50,000+

2. What industry does your enterprise belong to?

3. What has the impact of phishing been on your organization to date?

☐ Loss of Data

☐ Malware Infection

☐ Compromised Accounts

☐ Disruption of Employee Activities

□ Other

4. Which of the following technologies are currently employed by your organization to reduce the risk from phishing?

□ Email/Spam Filters

□ Outbound Proxy Protection

□ Advanced Malware Analysis

□ URL Wrapping

□ Other:

5. Is your enterprise currently running a simulated phishing program?

□ Yes

□ No

6. Which of the following activities does your enterprise currently use to train end users on how to identify and report phishing messages?

□ Annual security awareness training sessions

□ Monthly notifications or newsletters

□ Phishing simulation exercises

□ Other:

Goals & Objectives

7. Define your phishing program goals?

At a high level, what do you want this program to achieve?

8. Outline a high level business case.

What will the benefits of the program be to the enterprise and how will it contribute towards the business meeting its objectives?

Sponsorship & Governance

9. Who will sponsor the program

What department/function will fund and sponsor the initiative?

10. Who will manage the program end-to-end?

Who is responsible for the whole thing?

11. Who are your key stakeholders and are there interdependencies?

Stakeholders can effect success or failure and may be directly impacted by this program. Who are you top priorities? Which stakeholders will play a vital role in helping you implement the program?

Change Impact & Risk Assessment

12. What business processes will be impacted by this change?

Category	Impacts	High / Medium / Low
People		
Process		
Technology		

13. What are the key risks facing the program?

Consider risks associated with the implementation process and throughout the program lifecycle.

Communication

14. How will you communicate to the enterprise without impacting your program?

Communication is key, but you how much is too much?

15. Are there any Works Councils or Unions to be engaged with in advance of any program activity?

Remember, Works Councils consensus is essential.

16. What does success look like?

Success Criteria & KPIs: These could range from project to business-as-unusual transition to reporting key performance indicators to senior management.

17. How often should senior management receive program updates?

Management should be updated on key trends and KPIs; enterprise and functional susceptibility; behavioral shifts; and action items that require top-down sponsorship.

Whitelisting & Administration

18. Who will you work with to ensure timely inbound email delivery and how will you test it?

Rigorous testing will be required to ensure inbound delivery of emails and access to education.

19. Additional administration support may be required from Operational and IT teams throughout each simulation start and end date. Why and how can this be reduced?

Each simulation will result in a significant increase in emails being reported. What can you do to help manage the impact on teams/resources, particularly which a response is required, and ensure end users are reporting appropriately?

Simulated Phishing

20. Big bang versus phased approach?

Which approach is right for your enterprise and how will you gain a true baseline or susceptibility/awareness/reporting?

21. Who will you target?

What employee groups are in scope, and why?

23. A simulated phish has been sent. What happens if an employee clicks a link or opens an attachment?

Remember we want to reinforce positive behavior change directly related to the goals previously outlined.

24. 0% susceptibility shouldn't necessarily be a program goal. Why?

Remember, awareness is about reducing risk.

25. How will you handle repeat offenders?

You will have users who consistently fail simulated phishing tests, even after completing training modules. What should you do next to for users that represent a high risk?

Phishing Awareness

26. List five top tips you could regularly share via your awareness program to help end users avoid being the victim of spear phishing attacks?

1	
2	
3	
4	
5	

27. In your opinion, how do simulated attacks improve security awareness training?

It’s important to train employees to recognize and resist phishing tactics directed at them. How do simulated phishing programs achieve this?