A. For Employees (Training Participants)

Part 1: Current Experiences & Perceptions of Phishing

1. To start, could you tell me a bit about your general experience with emails and messages you receive at work? Do you often encounter anything that looks suspicious or out of the ordinary?

2. When you receive an email that seems suspicious, what's your initial reaction or thought process? What steps do you typically take?

3. How would you describe your current knowledge about phishing, and on a scale of 1 to 5 (where 1 is not confident at all and 5 is extremely confident), how confident do you feel in your ability to identify a phishing email or a social engineering attempt today?

4. What are some of the most common "red flags" or cues you look for when trying to spot a phishing attempt? What makes them stand out to you?

5. Have you ever clicked on something you later realized was phishing, or nearly did? Could you describe what happened and what made you realize it might be a threat?

6. How comfortable do you feel asking colleagues or your manager if you're unsure about an email? Why or why not?

7. If you suspected an email was a phishing attempt, how would you typically report it within the organization?

Part 2: Training Experiences & Future Preferences

1. Thinking back to any previous cybersecurity or phishing awareness training you've received, what aspects do you remember most clearly? What parts were particularly helpful or memorable, and what parts were less useful or difficult to apply?

2. Have you seen or heard discussions about phishing or security in team meetings, internal newsletters, conferences, or on platforms like SharePoint?

3. What specific knowledge or practical skills would make you feel truly confident spotting phishing attempts in your inbox?

4. When it comes to learning about cybersecurity threats like phishing, what format do you find most engaging? For example, would you prefer interactive modules, short videos, real-life examples, or something else?

5. How long would you ideally be willing to spend in a single training session? Would you prefer shorter, more frequent modules or one longer workshop?

6. The thesis mentions that "incomplete training and the role of folk models in phishing susceptibility" can be an issue (Wash & Cooper, 2018). Do you feel there are any common gaps in understanding, or misconceptions among colleagues, that new training could address?

7. What kinds of follow-up reminders or refreshers (e.g., posters, SharePoint articles, short emails, brief training sessions) would you prefer to help maintain awareness over time?

8. Are there any specific phishing scenarios or examples you'd like the training to cover, perhaps ones you've actually received or heard about?

B. For IT

Part 1: Current Program & Challenges

1. Could you describe the current philosophy or strategic approach behind your organization's phishing awareness training program? What are the primary objectives you aim to achieve?

2. What specific types of training programs or tools are you currently utilizing (e.g., simulated phishing drills, embedded training, a "Report Phishing" button as mentioned in the thesis)?

3. How will you measure the effectiveness of your phishing awareness training? Will you be tracking metrics like click-through rates from simulations, or will you be utilizing alternative ways to measure effectiveness?

4. In our thesis, we highlight that "phishing remains as the most prevalent social engineering threat, thriving even where sophisticated technical controls are in place." What are the biggest challenges you face in mitigating the human element of phishing attacks within our organization?

5. What are the most prevalent and concerning phishing threats you are observing right now? Are you seeing an increase in spear phishing, whaling, or perhaps newer techniques involving AI-generated media or QR codes?

6. What technical defenses (e.g., automated email warnings, attachment sandboxing) are currently in place, and how do they work alongside the people-centric training?

Part 2: Future Development & Strategic Thinking

1. Based on your observations and data, where do you believe the current training program will succeed, and where do you see the most significant areas for improvement?

2. During our thesis we have noted that improvements from training can "erode within a few months if training is not reinforced" (Wash & Cooper, 2018). How do you plan to incorporate reinforcement mechanisms to ensure long-term retention of knowledge and behavioral change?

3. What are your thoughts on personalizing training content, considering some sources have seen that "message personalization sharply increases success rates of attackers" (Hillman et al., 2023; Quinkert et al., 2021)?

4. Will you be segmenting users by role (e.g., finance, HR, executives) when crafting phishing scenarios, and would drive that decision?

5. How do you stay updated on evolving phishing techniques and incorporate new threat intelligence into your training modules?

6. Given that "phishing often serves as the initial point of attack that then enables further cyberattacks such as malware infections, ransomware attacks, and other attacks and fraud schemes," how would the training program address the broader implications of a successful phishing attack?

7. What organizational barriers like budget, time, executive sponsorship, etc., shape how you will design and roll out training?

8. How will you ensure that training remains engaging and relevant, preventing it from becoming a "checkbox exercise"? Will you collect and incorporate employee feedback after each campaign?

9. Looking ahead, what are your strategic priorities for evolving the phishing awareness training program in the coming years? Are there any new technologies or methodologies you are considering implementing?