**Title: Embedding Human-Centric Cybersecurity in Start-Up Environments: Socio-Technical and Ethical Solutions**

# Purpose of the Presentation

This presentation offers socio-technical and ethically responsible solutions to the three key human factors identified in my Unit 3 essay:  
1. Social engineering susceptibility  
2. Insider threats  
3. Inadequate security awareness and culture  
  
The proposed solutions are framed within behavioural theories, mental models, and ethical frameworks, including principles from the Menlo Report. The presentation also includes a reflection on new challenges introduced by generative AI.

# Outline of Slides and Structure

## Slide 1 – Introduction

Recap of Unit 3 focus areas  
Purpose and scope of the presentation

## Slide 2 – Overview of Proposed Solutions

Socio-technical approach  
Ethical considerations and behavioural framing

## Slide 3–4 – Reducing Social Engineering Susceptibility

Phishing simulations and mental models (Wash, 2010)  
Menlo Report principles (Respect for Persons, Beneficence)

## Slide 5–6 – Managing Insider Threats

Role-based access (NIST SP 800-53)  
Psychosocial indicators (Greitzer & Frincke, 2010)  
Monitoring ethics (Reeves et al., 2021)

## Slide 7–8 – Improving Security Awareness and Culture

Gamification, leadership, shared values (Schlienger & Teufel, 2003)  
Inclusive training (Bailey et al., 2012, Menlo Report – Justice)

## Slide 9 – Generative AI Risks

AI in phishing and impersonation  
Policy updates and NIST AI RMF (2023)

## Slide 10 – Conclusion

Reaffirming the need for ethical, usable, and behaviour-focused security

## Slide 11 – References

Full Harvard-style reference list on slides and transcript