Seminar session 1: The Human Factor – Introductions

Overview:

- Ground rules for seminars
- Module structure
- Assessment structure
- Further information
- Q&A

Seminar Dos and Don'ts:

Do:

- Engage with the content and do the reading!
- Contribute to discussions, everyone's experiences are useful
- Mute your microphone when not talking
- Use the chat for general questions
- Respect other student's opinion
- Ask questions, there are not stupid questions!

Don't:

- Talk over the top of each other
- Be afraid to ask for help
- Think you can do it all in isolation

Learning Outcomes:

- Review the concepts and principles of human behaviour within the context of cyber security.
- Develop an in-depth understanding of the elements of risk in a socio-technical system.
- Critically examine effective strategies to promote and manage the human factor in cyber security.
- Critically evaluate the social and ethical considerations in developing and applying usable security.

Module Structure:

- Unit 1: Human Factors and Cyber Security
- Unit 2: Fitting the Task to the Human
- Unit 3: Mental Models and Accessibility Issues
- Unit 4: Usable Security Design
- Unit 5: Ethical, Societal and Organisational Issues
- Unit 6: Mental Models and Risk Communication

Assessment Structure:

- Human Factors of cyber security outline of the viewpoint of the Queens Medical Centre ASMIS.
- Essay identifying issues
- Presentation to mitigate those issues in an ethical and social context