Students are to answer 1 of the 2 cases presented. See below for essay length and formatting requirements. Students can use any resource given in class or found online. Online resources should be evidence based from peer reviewed sources.

A 10-minute presentation of your process of finding relevant information for your essay will also be delivered with your exam. The presentation is not a summary of your paper, but a reflection on how you found relevant information and decided how to use it. The presentation can use any form of presentation (e.g. powerpoint) but needs to be delivered as a video file (.mp4).

Case 1

Developing Effective Phishing Education for Healthcare Frontline Personnel

Phishing attacks in healthcare pose significant threats, exploiting the operational pressures and high cognitive demands on frontline healthcare workers. Nurses, administrative staff, and other personnel often serve as critical targets due to their access to sensitive patient data and systems. Despite the prevalence of annual awareness training and embedded phishing simulations, studies (e.g., Savage et al., 2025) highlight persistent vulnerabilities and the limited effectiveness of current approaches. You are a newly employed Chief Information Security Officer to a company and have been instructed by your healthcare organization to design a cybersecurity awareness and training program. Your new organisation has experienced repeated phishing incidents resulting in the exposure of patient data and operational disruptions. Their current training methods for phishing simulations have proven ineffective, with low engagement and minimal long-term behaviour change.

Your task is to design a theoretically grounded phishing education program tailored to the healthcare context. The proposed program must critically address the challenges of current cybersecurity training, explore innovative approaches to enhance learning outcomes, and include an evaluation framework to assess its potential effectiveness. Include a summary from findings from more recent studies with a focus on why existing phishing training methods often fail in healthcare settings. Include a discussion of the distinct vulnerabilities in healthcare and analysis of the knowledge, behavioural, and skill deficits that contribute to phishing susceptibility among healthcare personnel.

Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., ... & Voelker, G. M. (2024, November). Understanding the Efficacy of Phishing Training in Practice. In *2025 IEEE Symposium on Security and Privacy (SP)* (pp. 76-76). IEEE Computer Society.

Case 2:

Understanding and Exploiting the Risks of Expertise in a SOC

Security Operations Centres (SOCs) are vital to the defence of large multinational organizations. Staffed by cybersecurity professionals tasked with identifying, analysing, and mitigating security threats, these teams are critical to protecting sensitive systems and data. However, the expertise of these professionals can also introduce risks such as cognitive biases, overconfidence, and reliance on patterns can lead to predictable behaviours that skilled threat actors might exploit. As highlighted in the study by de Wit, Pieters, and van Gelder (2023), even experienced security professionals are prone to systematic biases and noise in decision-making. You are a threat actor tasked with targeting a multinational organization by exploiting vulnerabilities in its SOC team. Your goal is to understand how the human factors of characteristics of expertise create attack opportunities through social engineering and how these can be used to manipulate SOC professionals to compromise their effectiveness.

A multinational corporation with a state-of-the-art SOC has been experiencing a series of failed phishing and malware attacks. Your team, as advanced threat actors, has been hired to execute a successful infiltration. The SOC comprises highly trained professionals who pride themselves on their ability to detect and neutralize threats. Your task is to develop a comprehensive plan for gathering intelligence on the SOC team, identifying vulnerabilities tied to their expertise, and designing a social engineering campaign to exploit these weaknesses. Include a discussion of the distinct vulnerabilities of cybersecurity professionals and an analysis of the knowledge, behavioural, and skill deficits that contribute to their vulnerabilities.

de Wit, J., Pieters, W., & van Gelder, P. (2024). Bias and noise in security risk assessments, an empirical study on the information position and confidence of security professionals. *Security Journal*, *37*(1), 170-191.

Formatting of Essay

The essay can be **3000 ± 10% words** in main body (abstract and references do not count) in 12-point Times New Roman font. Your essay should be typed and double-spaced on standard-sized paper (A4) with 1" margins (standard in Word Document) on all sides. Include a page header (also known as the "running head") at the top of every page. The running head is a shortened version of your paper's title and cannot exceed 50 characters including spacing and punctuation. Not meeting this requirement can result in a lower grade. Word count does not include pictures with no text. Tables will count towards the final word count. If pictures are used for tables, they will count as 500 words. The essay shall have a title page with Title and word count listed, abstract, main body, and references.

See https://taltech.ee/en/formatting-guidelines for more information

For this essay, APA 7th is to be used (see: https://apastyle.apa.org/style-grammar-guidelines/references/examples)

Other resources for APA 7th (I personally use this one):
https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_style_introduction.html

Grading

See https://taltech.ee/en/grading-system for Taltech Grading policy

§ 14. Assessment of academic performance
(1) The methods and criteria of assessment defined in syllabus shall be available to students before the commencement of studies and they must not be changed during a semester. The assessment methods define the manner of attesting the acquisition of knowledge and skills (e.g. an oral or written examination, pass/fail assessment, an essay, a report, group work, a questionnaire). If various methods are used for the assessment of learning outcomes, their relevant weights in determining the final grade shall be specified in the syllabus. An assessment criterion shall specify the expected level and scope of knowledge which can be proved by the assessment methods.

(3) **In case of graded assessment, the achievement of learning outcomes is assessed based on the following scale**:
A (5) – "excellent" – outstanding and particularly profound achievement of learning outcomes, along with creativity and consummate proficiency in applying skills and knowledge;
B (4) – "very good" – very good achievement of learning outcomes, along with proficiency in applying skills and knowledge in a targeted and creative manner. Some details of knowledge and skills may exhibit errors which are neither substantive nor serious;
C (3) – "good" – good achievement of learning outcomes, along with proficiency in applying skills and knowledge in a relevant manner. A certain imprecision and uncertainty are apparent in the depth and detail of knowledge and skills;
D (2) – "satisfactory" – sufficient achievement of learning outcomes, along with application of knowledge and skills in a typical manner; in atypical situations both, uncertainty as well as lack of knowledge and skills are apparent.
E (1) – "poor" – minimum acceptable achievement of the most important learning outcomes along with limited application of knowledge and skills in typical situations; in atypical situations both, considerable uncertainty as well as lack of knowledge and skills are apparent;
F (0) – "failed" – achievement in knowledge and skills below the minimum standard.