**Gli studenti devono rispondere a 1 dei 2 casi presentati. Di seguito sono riportate le indicazioni relative alla lunghezza del saggio e ai**
**requisiti di formattazione. Gli studenti possono utilizzare qualsiasi risorsa fornita in classe o trovata online. Le risorse online devono essere basate su prove provenienti da fonti sottoposte a revisione paritaria.**

**Insieme all'esame dovrà essere consegnata anche una presentazione di 10 minuti sul processo di ricerca delle informazioni rilevanti per il saggio. La presentazione non è un riassunto del saggio, ma una riflessione su come sono state trovate le informazioni rilevanti e su come si è deciso di utilizzarle. La presentazione può essere realizzata in qualsiasi formato (ad esempio PowerPoint), ma deve essere consegnata come file video (.mp4).**

**Caso 1**

**Sviluppo di un'efficace formazione sul phishing per il personale sanitario in prima linea**

Gli attacchi di phishing nel settore sanitario rappresentano una minaccia significativa, poiché sfruttano le pressioni operative e le elevate esigenze cognitive degli operatori sanitari in prima linea. Infermieri, personale amministrativo e altro personale sono spesso bersagli critici a causa del loro accesso a dati e sistemi sensibili dei pazienti. Nonostante la diffusione di corsi di formazione annuali di sensibilizzazione e simulazioni di phishing integrate, alcuni studi (ad esempio Savage et al., 2025) evidenziano vulnerabilità persistenti e l'efficacia limitata degli approcci attuali. Sei un Chief Information Security Officer appena assunto da un'azienda e hai ricevuto l'incarico dalla tua organizzazione sanitaria di progettare un programma di sensibilizzazione e formazione sulla sicurezza informatica. La tua nuova organizzazione ha subito ripetuti incidenti di phishing che hanno portato all'esposizione dei dati dei pazienti e a interruzioni operative. I loro attuali metodi di formazione per le simulazioni di phishing si sono dimostrati inefficaci, con un basso coinvolgimento e un cambiamento minimo nel comportamento a lungo termine.

Il tuo compito è quello di progettare un programma di formazione sul phishing basato su fondamenti teorici e adattato al contesto sanitario. Il programma proposto deve affrontare in modo critico le sfide dell'attuale formazione sulla sicurezza informatica, esplorare approcci innovativi per migliorare i risultati dell'apprendimento e includere un quadro di valutazione per valutarne la potenziale efficacia. Includi una sintesi dei risultati di studi più recenti, concentrandoti sul motivo per cui i metodi di formazione sul phishing esistenti spesso falliscono in ambito sanitario. Includi una discussione sulle vulnerabilità specifiche del settore sanitario e un'analisi delle lacune di conoscenza, comportamento e competenze che contribuiscono alla suscettibilità al phishing tra il personale sanitario.

Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., ... & Voelker, G. M. (2024, novembre). Comprendere l'efficacia della formazione sul phishing nella pratica. In *2025 IEEE Symposium on sicurezza e privacy (SP)* (pp. 76-76). IEEE Computer Society.

**Caso 2:**

**Comprendere e sfruttare i rischi della competenza in un SOC**

I centri operativi di sicurezza (SOC) sono fondamentali per la difesa delle grandi organizzazioni multinazionali. Composti da professionisti della sicurezza informatica incaricati di identificare, analizzare e mitigare le minacce alla sicurezza, questi team sono fondamentali per proteggere i sistemi e i dati sensibili. Tuttavia, le competenze di questi professionisti possono anche comportare rischi quali pregiudizi cognitivi, eccessiva sicurezza e affidamento a modelli che possono portare a comportamenti prevedibili che potrebbero essere sfruttati da abili autori di minacce. Come evidenziato nello studio di de Wit, Pieters e van Gelder (2023), anche i professionisti della sicurezza più esperti sono inclini a pregiudizi sistematici e rumore nel processo decisionale. Sei un attore malintenzionato incaricato di prendere di mira un'organizzazione multinazionale sfruttando le vulnerabilità del suo team SOC. Il tuo obiettivo è capire in che modo i fattori umani delle caratteristiche di competenza creano opportunità di attacco attraverso l'ingegneria sociale e come questi possono essere utilizzati per manipolare i professionisti SOC e comprometterne l'efficacia.

Una multinazionale con un SOC all'avanguardia ha subito una serie di attacchi di phishing e malware falliti. Il tuo team, in qualità di attore avanzato, è stato assunto per eseguire un'infiltrazione di successo. Il SOC è composto da professionisti altamente qualificati che sono orgogliosi della loro capacità di rilevare e neutralizzare le minacce. Il tuo compito è quello di sviluppare un piano completo per raccogliere informazioni sul team SOC, identificare le vulnerabilità legate alla loro esperienza e progettare una campagna di ingegneria sociale per sfruttare queste debolezze. Includi una discussione sulle vulnerabilità distintive dei professionisti della sicurezza informatica e un'analisi delle lacune di conoscenza, comportamento e competenze che contribuiscono alle loro vulnerabilità.

de Wit, J., Pieters, W., & van Gelder, P. (2024). Pregiudizi e rumore nelle valutazioni dei rischi per la sicurezza, uno studio empirico sulla posizione informativa e la fiducia dei professionisti della sicurezza . *Security Journal*, *37*(1), 170-191.

**Formattazione del saggio**

Il saggio può contenere **3000 ± 10% parole** nel corpo principale (abstract e riferimenti non contano) in carattere Times New Roman 12. Il saggio deve essere digitato e scritto a doppia spaziatura su carta di formato standard (A4) con margini di 1" (standard in Word Document) su tutti i lati. Includere un'intestazione di pagina
intestazione (nota anche come "intestazione corrente") nella parte superiore di ogni pagina. L'intestazione corrente è una
versione abbreviata del titolo del documento e non può superare i 50 caratteri, spazi e punteggiatura inclusi. Il mancato rispetto di questo requisito può comportare un voto inferiore. Il conteggio delle parole non le immagini senza testo. Le tabelle saranno conteggiate nel conteggio finale delle parole. Se nelle tabelle vengono utilizzate immagini, queste saranno conteggiate come 500 parole. Il saggio dovrà avere una pagina del titolo con il titolo e il conteggio delle parole, un abstract, il corpo principale e i riferimenti.

**Per ulteriori informazioni, consultare https://taltech.ee/en/formatting-guidelines.**

**Per questo saggio, è necessario utilizzare lo stile APA 7th (vedi: https://apastyle.apa.org/style-grammar-guidelines/references/examples)**

**Altre risorse per l'APA 7th (io personalmente uso questa): https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_style_introduction.htm l**

**Valutazione**

Vedere https://taltech.ee/en/grading-system per la politica di valutazione di Taltech

**§ 14. Valutazione del rendimento accademico**
(1) I metodi e i criteri di valutazione definiti nel programma devono essere comunicati agli studenti prima dell'inizio degli studi e non devono essere modificati durante il semestre. I metodi di valutazione definiscono le modalità di attestazione dell'acquisizione di conoscenze e competenze (ad esempio, esame orale o scritto, valutazione di idoneità/non idoneità, saggio, relazione, lavoro di gruppo, questionario). Se per la valutazione dei risultati dell'apprendimento vengono utilizzati diversi metodi, la loro peso relativo nella determinazione del voto finale deve essere specificato nel programma. Un Il criterio di valutazione deve specificare il livello e l'ambito delle conoscenze attese che possono essere dimostrate dai metodi di valutazione.

(3) **In caso di valutazione graduata, il raggiungimento dei risultati di apprendimento è valutato in base alla seguente scala**:
A (5) – "eccellente" – raggiungimento eccezionale e particolarmente approfondito dei risultati di apprendimento, insieme a creatività e competenza consumata nell'applicazione delle abilità e delle conoscenze;
B (4) – "molto buono" – ottimo raggiungimento dei risultati di apprendimento, insieme a competenza nell'applicazione delle abilità e delle conoscenze in modo mirato e creativo. Alcuni dettagli delle conoscenze e delle abilità possono presentare errori che non sono né sostanziali né gravi;
C (3) – "buono" – buon raggiungimento dei risultati di apprendimento, insieme a competenza nell'applicazione delle abilità e delle conoscenze in modo pertinente. Una certa imprecisione e incertezza sono evidenti nella profondità e nei dettagli delle conoscenze e delle abilità;
D (2) – "soddisfacente" – raggiungimento sufficiente dei risultati di apprendimento, insieme all'applicazione delle conoscenze e delle competenze in modo tipico; in situazioni atipiche sono evidenti sia l'incertezza che la mancanza di conoscenze e competenze.
E (1) – "scarso" – raggiungimento minimo accettabile dei risultati di apprendimento più importanti, insieme a un'applicazione limitata delle conoscenze e delle competenze in situazioni tipiche; in situazioni atipiche situazioni atipiche sono evidenti sia una notevole incertezza che una mancanza di conoscenze e abilità; F (0) – "bocciato" – raggiungimento di conoscenze e abilità al di sotto dello standard minimo.