

Οι φοιτητές καλούνται να απαντήσουν σε μία από τις δύο περιπτώσεις που παρουσιάζονται. Δείτε παρακάτω τις απαιτήσεις για το μέγεθος και τη μορφοποίηση της έκθεσης. Μπορείτε να χρησιμοποιήσετε οποιαδήποτε πηγή δόθηκε στην τάξη ή βρείτε διαδικτυακά, αρκεί οι διαδικτυακές πηγές να βασίζονται σε αποδεικτικά στοιχεία από επιστημονικά ανασκοπημένες δημοσιεύσεις.

Θα παραδώσετε επίσης μια παρουσίαση διάρκειας 10 λεπτών σχετικά με τη διαδικασία που ακολουθήσατε για να βρείτε τις κατάλληλες πληροφορίες για την εργασία σας, μαζί με το διαγώνισμά σας. Η παρουσίαση δεν αποτελεί περίληψη της εργασίας, αλλά αντανάκλαση του τρόπου με τον οποίο εντοπίσατε τις σχετικές πληροφορίες και αποφασίσατε πώς θα τις αξιοποιήσετε. Η παρουσίαση μπορεί να γίνει με όποιο μέσο επιθυμείτε (π.χ. powerpoint), αλλά πρέπει να παραδοθεί ως αρχείο βίντεο (.mp4).

Περίπτωση 1

### Αποτελεσματική Εκπαίδευση για Αποφυγή Phishing στους Εργαζόμενους της Υγείας στην Πρώτη Γραμμή

Οι επιθέσεις phishing στον χώρο της υγείας αποτελούν σοβαρή απειλή, αξιοποιώντας τις αυξημένες απαιτήσεις και τα υψηλά επίπεδα πίεσης στους εργαζόμενους της πρώτης γραμμής. Νοσηλευτές, διοικητικό προσωπικό και άλλοι υπάλληλοι συχνά γίνονται βασικοί στόχοι λόγω της πρόσβασης που έχουν σε ευαίσθητα δεδομένα ασθενών και συστήματα. Παρά την ύπαρξη ετήσιων εκπαιδύσεων και δοκιμών phishing, μελέτες (π.χ. Savage et al., 2025) αναδεικνύουν συνεχιζόμενες αδυναμίες και χαμηλή αποτελεσματικότητα των υπάρχουσων μεθόδων. Έχετε μόλις αναλάβει τη θέση του Chief Information Security Officer και σας έχει ανατεθεί από τον οργανισμό υγείας να σχεδιάσετε πρόγραμμα ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια. Ο νέος σας οργανισμός έχει αντιμετωπίσει επαναλαμβανόμενα περιστατικά phishing με αποτέλεσμα την έκθεση δεδομένων ασθενών και λειτουργικές διαταραχές. Οι τρέχουσες εκπαιδύσεις για προσομοιώσεις phishing δεν έχουν φέρει τα επιθυμητά αποτελέσματα, με χαμηλή συμμετοχή και ελάχιστη αλλαγή στη συμπεριφορά μακροπρόθεσμα.

Η αποστολή σας είναι να δημιουργήσετε ένα εκπαιδευτικό πρόγραμμα για phishing με θεωρητική βάση, ειδικά σχεδιασμένο για το περιβάλλον της υγείας. Το πρόγραμμα πρέπει να αντιμετωπίζει κριτικά τις προκλήσεις της υπάρχουσας εκπαίδευσης στην κυβερνοασφάλεια, να προτείνει καινοτόμες μεθόδους για καλύτερα μαθησιακά αποτελέσματα και να περιλαμβάνει πλαίσιο αξιολόγησης της αποτελεσματικότητάς του. Συμπεριλάβετε περίληψη από σύγχρονες μελέτες που εξηγούν γιατί οι τρέχουσες μέθοδοι εκπαίδευσης για phishing αποτυγχάνουν συχνά στον χώρο της υγείας. Συζητήστε τις ιδιαίτερες αδυναμίες του κλάδου, καθώς και την ανάλυση των ελλείψεων γνώσης, συμπεριφοράς και δεξιοτήτων που συμβάλλουν στην ευαλωτότητα των εργαζομένων στην υγεία απέναντι στις επιθέσεις phishing.

Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., ... & Voelker, G. M. (Νοέμβριος 2024). Αξιολόγηση της αποτελεσματικότητας της εκπαίδευσης κατά του phishing στην πράξη. Στα *2025 IEEE Symposium on Security and Privacy (SP)* (σελ. 76-76). IEEE Computer Society.

## Κατανόηση και Αξιοποίηση των Κινδύνων της Εξειδίκευσης σε ένα SOC

Τα Κέντρα Επιχειρήσεων Ασφαλείας (SOC) αποτελούν τη ραχοκοκαλιά της άμυνας μεγάλων πολυεθνικών εταιρειών. Στελεχωμένα με ειδικούς στην κυβερνοασφάλεια που έχουν ως αποστολή την ανίχνευση, ανάλυση και αντιμετώπιση απειλών, αυτές οι ομάδες παίζουν καθοριστικό ρόλο στην προστασία ευαίσθητων συστημάτων και δεδομένων. Ωστόσο, η εξειδίκευση των επαγγελματιών μπορεί να κρύβει κινδύνους, όπως γνωστικές προκαταλήψεις, υπερβολική αυτοπεποίθηση και επαναλαμβανόμενα μοτίβα συμπεριφοράς, τα οποία έμπειροι κυβερνοεγκληματίες θα μπορούσαν να εκμεταλλευτούν. Όπως αναδεικνύει η μελέτη των de Wit, Pieters και van Gelder (2023), ακόμη και οι πιο έμπειροι ειδικοί της ασφάλειας πέφτουν συχνά θύματα συστηματικών προκαταλήψεων και θορύβου στη λήψη αποφάσεων. Ο ρόλος σας είναι να αναλύσετε πώς τα ανθρώπινα χαρακτηριστικά της εξειδίκευσης δημιουργούν ευκαιρίες επιθέσεων μέσω κοινωνικής μηχανικής και πώς αυτά τα στοιχεία μπορούν να χρησιμοποιηθούν για να επηρεάσουν την αποτελεσματικότητα των επαγγελματιών SOC.

Μια πολυεθνική εταιρεία με ένα υπερέγχρονο SOC έχει αντιμετωπίσει μια σειρά αποτυχημένων επιθέσεων με phishing και κακόβουλο λογισμικό. Η ομάδα σας, ως έμπειροι κυβερνοπειρατές, καλείται να σχεδιάσει μια επιτυχημένη διείσδυση. Το SOC στελεχώνεται από άριστα εκπαιδευμένους επαγγελματίες που βασίζονται στην ικανότητά τους να εντοπίζουν και να εξουδετερώνουν απειλές. Η αποστολή σας περιλαμβάνει τη δημιουργία ενός ολοκληρωμένου σχεδίου συλλογής πληροφοριών για την ομάδα SOC, τον εντοπισμό αδυναμιών που σχετίζονται με την εξειδίκευσή τους και το σχεδιασμό μιας καμπάνιας κοινωνικής μηχανικής για την αξιοποίηση αυτών των κενών. Προσθέστε συζήτηση για τα ιδιαίτερα τρωτά σημεία των επαγγελματιών της κυβερνοασφάλειας και ανάλυση των γνωστικών, συμπεριφορικών και δεξιοτήτων ελλείψεων που ενισχύουν τις ευπάθειές τους.

de Wit, J., Pieters, W., & van Gelder, P. (2024). Προκαταλήψεις και θόρυβος στις αξιολογήσεις κινδύνου ασφάλειας: Μια εμπειρική μελέτη για τη θέση πληροφόρησης και την αυτοπεποίθηση των επαγγελματιών ασφάλειας. *Security Journal*, 37(1), 170-191.

## Λιαμόρφωση της έκθεσης

Η έκθεση μπορεί να έχει **3000 ± 10% λέξεις** στο κυρίως σώμα (η περίληψη και οι αναφορές δεν υπολογίζονται). Γράψτε το κείμενο σε γραμματοσειρά Times New Roman, μέγεθος 12pt, δακτυλογραφημένο και με διπλό διάστημα, σε χαρτί μεγέθους A4 με περιθώρια 1" (όπως είναι στάνταρ σε Word). Σε κάθε σελίδα τοποθετήστε κεφαλίδα (γνωστή και ως “running head”) που είναι μια σύντομη εκδοχή του τίτλου σας και δεν πρέπει να ξεπερνά τους 50 χαρακτήρες συμπεριλαμβανομένων των κενών και της στίξης. Η μη τήρηση αυτών των οδηγιών μπορεί να οδηγήσει σε χαμηλότερη βαθμολογία. Οι εικόνες χωρίς κείμενο δεν προσμετρούνται στην καταμέτρηση λέξεων. Οι πίνακες προσμετρούνται στο σύνολο των λέξεων. Αν χρησιμοποιηθούν εικόνες ως πίνακες, μετράνε ως 500 λέξεις. Η έκθεση πρέπει να έχει σελίδα τίτλου με τον τίτλο και τον αριθμό λέξεων, περίληψη, κυρίως σώμα και αναφορές.

Λείτε <https://taltech.ee/en/formatting-guidelines> για περισσότερες πληροφορίες

Για το συγκεκριμένο δοκίμιο, απαιτείται η χρήση του APA 7η έκδοση (**δείτε:** <https://apastyle.apa.org/style-grammar-guidelines/references/examples>)

Άλλα εργαλεία για το APA 7η έκδοση (Προσωπικά χρησιμοποιώ το παρακάτω):

[https://owl.purdue.edu/owl/research\\_and\\_citation/apa\\_style/apa\\_style\\_introduction.htm](https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_style_introduction.htm)  
1

Δείτε <https://taltech.ee/en/grading-system> για την πολιτική βαθμολόγησης του Taltech

#### § 14. Αξιολόγηση ακαδημαϊκής επίδοσης

(1) Οι μέθοδοι και τα κριτήρια αξιολόγησης που ορίζονται στο πρόγραμμα σπουδών πρέπει να είναι διαθέσιμα στους φοιτητές πριν την έναρξη των μαθημάτων και δεν επιτρέπεται να αλλάξουν κατά τη διάρκεια του εξαμήνου. Οι μέθοδοι αξιολόγησης προσδιορίζουν τον τρόπο πιστοποίησης της απόκτησης γνώσεων και δεξιοτήτων (π.χ. προφορική ή γραπτή εξέταση, αξιολόγηση με βάση την επιτυχία ή αποτυχία, δοκίμιο, αναφορά, ομαδική εργασία, ερωτηματολόγιο). Εάν χρησιμοποιούνται διάφορες μέθοδοι για την αξιολόγηση των μαθησιακών αποτελεσμάτων, τα αντίστοιχα ποσοστά βαρύτητας για τον τελικό βαθμό πρέπει να αναφέρονται στο πρόγραμμα. Τα κριτήρια αξιολόγησης ορίζουν το αναμενόμενο επίπεδο και εύρος γνώσεων που μπορούν να αποδειχθούν μέσω των μεθόδων αξιολόγησης.

#### (3) Σε περίπτωση αξιολόγησης με βαθμολογία, η επίτευξη των μαθησιακών αποτελεσμάτων αξιολογείται με βάση την ακόλουθη κλίμακα:

- A (5) – "άριστα" – εξαιρετική και βαθιά κατανόηση των μαθησιακών στόχων, σε συνδυασμό με δημιουργικότητα και άριστη εφαρμογή δεξιοτήτων και γνώσεων.
- B (4) – "πολύ καλά" – πολύ καλή επίτευξη των στόχων, με ικανότητα εφαρμογής γνώσεων και δεξιοτήτων με στόχευση και δημιουργικότητα. Μικρές ασάφειες ή λάθη μπορεί να υπάρχουν, χωρίς να είναι σημαντικά.
- C (3) – "καλά" – καλή επίτευξη στόχων, με σχετική ικανότητα εφαρμογής δεξιοτήτων και γνώσεων. Υπάρχει κάποια ασάφεια ή αβεβαιότητα στη λεπτομέρεια και το βάθος της γνώσης.
- D (2) – "ικανοποιητικά" – επαρκής επίτευξη των μαθησιακών αποτελεσμάτων, με τυπική εφαρμογή γνώσεων και δεξιοτήτων. Σε μη συνηθισμένες καταστάσεις, εμφανίζονται αμφιβολίες ή ελλείψεις.
- E (1) – "ανεπαρκώς" – ελάχιστη αποδεκτή επίτευξη των βασικών μαθησιακών στόχων με περιορισμένη εφαρμογή γνώσεων και δεξιοτήτων σε συνηθισμένες περιπτώσεις. Σε ασυνήθιστες καταστάσεις, παρατηρούνται έντονη αβεβαιότητα και ελλείψεις. F (0) – "αποτυχία" – η επίδοση σε γνώσεις και δεξιότητες είναι κάτω από το ελάχιστο αποδεκτό επίπεδο.