ΓΙΑ ΥΠΗΡΕΣΙΑΚΗ ΧΡΗΣΗ

Κωδικός Προδιαγραφής Προγράμματος Κατάρτισης:

ΠΟΛΥΕΠΙΧΕΙΡΗΣΙΑΚΑ ΠΡΟΓΡΑΜΜΑΤΑ ΚΑΤΑΡΤΙΣΗΣ - ΣΥΝΗΘΗ

ΑΙΤΗΣΗ ΚΕΝΤΡΟΥ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΚΑΤΑΡΤΙΣΗΣ

ΓΙΑ ΕΓΚΡΙΣΗ ΠΡΟΔΙΑΓΡΑΦΗΣ ΠΡΟΓΡΑΜΜΑΤΟΣ ΚΑΤΑΡΤΙΣΗΣ

Επωνυμία Κέντρου Επαγγελματικής Κατάρτισης:

Αριθμός Πιστοποιητικού Κέντρου Επαγγελματικής Κατάρτισης (ΚΕΚ):

ΣΤΟΙΧΕΙΑ ΠΡΟΔΙΑΓΡΑΦΗΣ ΠΡΟΓΡΑΜΜΑΤΟΣ ΚΑΤΑΡΤΙΣΗΣ

Σημ: Αναφέρατε αναλυτικά όλα τα στοιχεία της Προδιαγραφής σύμφωνα με τις Κατευθυντήριες Γραμμές που περιλαμβάνονται στο Παράρτημα ΙΙ του Οδηγού Πολιτικής και Διαδικασιών του Σχεδίου.

1. Τίτλος προδιαγραφής προγράμματος κατάρτισης (μέχρι 70 χαρακτήρες):

Κυβερνοασφάλεια & Ψηφιακή Υγιεινή: Τεχνικές Ασφαλούς Συμπεριφοράς για Όλους τους Εργαζόμενους

2. Διάρκεια κατάρτισης (ώρες): 7

3. Ανάγκη κατάρτισης (σαφής, σύντομη, περιεκτική):

Α. Η Κυπριακή Επιχείρηση στο Στόχαστρο

Τα στοιχεία είναι αδιαμφισβήτητα: σύμφωνα με τις εθνικές έρευνες της Αρχής Ψηφιακής Ασφάλειας Κύπρου (2025), το 53% των κυπριακών επιχειρήσεων υπέστη τουλάχιστον μία κυβερνοεπίθεση τον τελευταίο χρόνο — δηλαδή κατά μέσο όρο μία επίθεση κάθε 8 ημέρες. Από τις επιχειρήσεις που δέχθηκαν επίθεση, το 51% υπέστη οικονομική ζημία, με μέσο κόστος €12.000 ανά περιστατικό.

Η κυρίαρχη απειλή παραμένει το phishing — τα δόλια ηλεκτρονικά μηνύματα που μιμούνται αξιόπιστες πηγές. Το phishing αντιπροσωπεύει το 44% όλων των κυβερνοεπιθέσεων στις κυπριακές επιχειρήσεις και αποτελεί την πιο πρόσφατη μορφή επίθεσης στο 75% των περιπτώσεων. Παράλληλα, σε παγκόσμιο επίπεδο, πάνω από το 35% των παραβιάσεων ασφαλείας ξεκινούν από ανθρώπινο λάθος — εργαζόμενοι που κλικάρουν σε κακόβουλο σύνδεσμο, χρησιμοποιούν αδύναμους κωδικούς, ή αποθηκεύουν δεδομένα σε μη ασφαλή μέσα.

Β. Το Χάσμα Κατάρτισης

Το πιο ανησυχητικό εύρημα δεν είναι ο αριθμός των επιθέσεων αλλά η απουσία ετοιμότητας. Σύμφωνα με τις ίδιες έρευνες:

• Σχεδόν 1 στις 4 επιχειρήσεις δεν έχει δημιουργήσει, ενημερώσει ή αναθεωρήσει τις πολιτικές κυβερνοασφάλειάς της εδώ και πάνω από ένα χρόνο.

• Το 43% των επιχειρήσεων δηλώνει ότι δεν γνωρίζει καν ότι υπάρχουν σεμινάρια κυβερνοασφάλειας.

• Μόνο το 22% των επιχειρήσεων συμμετείχε σε κάποια εκπαιδευτική δράση κυβερνοασφάλειας.

• Στους πολίτες, το 74% δεν γνωρίζει ότι υπάρχουν σεμινάρια και μόνο το 15% έχει παρακολουθήσει κάποιο.

• Το 48% των επιχειρήσεων που δεν δέχθηκαν επίθεση πιστεύει πως «δεν αποτελεί στόχο» — ψευδαίσθηση που αυξάνεται κάθε χρόνο.

Γ. Η Υβριδική Εργασία Πολλαπλασιάζει τους Κινδύνους

Η υιοθέτηση υβριδικής εργασίας στην Κύπρο μετά την πανδημία δημιούργησε νέα κενά ασφάλειας: εργαζόμενοι συνδέονται από μη ασφαλή δίκτυα Wi-Fi, χρησιμοποιούν προσωπικές συσκευές για εταιρικά δεδομένα, αποθηκεύουν κωδικούς σε post-it ή σημειωματάρια, και μοιράζονται αρχεία μέσω μη εγκεκριμένων εφαρμογών. Η περίμετρος ασφαλείας δεν είναι πλέον το γραφείο — είναι ο κάθε εργαζόμενος.

Δ. Το Κανονιστικό Πλαίσιο Αυξάνει τις Απαιτήσεις

Η ενσωμάτωση της Ευρωπαϊκής Οδηγίας NIS2 στο κυπριακό δίκαιο (Νόμος 60(Ι)/2025) επεκτείνει σημαντικά τον κύκλο των ρυθμιζόμενων οντοτήτων και επιβάλλει αυστηρότερες υποχρεώσεις κυβερνοασφάλειας — συμπεριλαμβανομένης της εκπαίδευσης προσωπικού. Ταυτόχρονα, ο ΓΚΠΔ (GDPR) απαιτεί γνωστοποίηση παραβίασης εντός 72 ωρών, ενώ οι ρυθμιστικές αρχές εξετάζουν αν η επιχείρηση διέθετε κατάλληλες πολιτικές, κατάρτιση και μέτρα ασφάλειας πριν το συμβάν. Η μη συμμόρφωση μπορεί να επιφέρει πρόστιμα έως 4% του παγκόσμιου τζίρου.

Αυτό το πρόγραμμα δεν απευθύνεται σε τεχνικούς IT. Απευθύνεται στον κάθε εργαζόμενο — τον πραγματικό πρώτο τοίχο άμυνας κάθε επιχείρησης. Στόχος είναι να μετατρέψει κάθε συμμετέχοντα σε ενεργό παράγοντα προστασίας, εξοπλίζοντάς τον με πρακτικές γνώσεις, εργαλεία και αντανακλαστικά. Ευθυγραμμίζεται πλήρως με τις κατευθύνσεις της Αρχής Ψηφιακής Ασφάλειας Κύπρου, τις απαιτήσεις NIS2/GDPR, και τις προτεραιότητες της ΑνΑΔ για ψηφιακές δεξιότητες.

4. Στόχοι (διατυπώνονται ως μαθησιακά αποτελέσματα):

Μετά την ολοκλήρωση του προγράμματος οι καταρτιζόμενοι θα είναι σε θέση να:

Σε επίπεδο γνώσεων

1. Αναγνωρίζουν τις κύριες κυβερνοαπειλές που αντιμετωπίζουν οι κυπριακές επιχειρήσεις (phishing, ransomware, social engineering, κακόβουλο λογισμικό, εσωτερικές απειλές).

2. Περιγράφουν τα χαρακτηριστικά ενός phishing email/μηνύματος και τα σημάδια αναγνώρισής τους.

3. Εξηγούν τις βασικές αρχές «ψηφιακής υγιεινής» (cyber-hygiene): ισχυροί κωδικοί, ασφαλής σύνδεση, ενημερώσεις, αντίγραφα ασφαλείας.

4. Αναφέρουν τις βασικές υποχρεώσεις που απορρέουν από τον ΓΚΠΔ (GDPR) και τον Νόμο NIS2 σε σχέση με την προστασία δεδομένων.

5. Κατηγοριοποιούν τα ρίσκα ασφάλειας που σχετίζονται με υβριδική/απομακρυσμένη εργασία, χρήση προσωπικών συσκευών και δημόσιων δικτύων.

Σε επίπεδο δεξιοτήτων

1. Εντοπίζουν και αποφεύγουν phishing emails, ύποπτους συνδέσμους και social engineering τεχνικές σε πραγματικά σενάρια.

2. Δημιουργούν και διαχειρίζονται ισχυρούς κωδικούς πρόσβασης χρησιμοποιώντας password managers και πολυπαραγοντική αυθεντικοποίηση (MFA).

3. Εφαρμόζουν πρακτικές ασφαλούς απομακρυσμένης εργασίας (VPN, ασφαλές Wi-Fi, κρυπτογράφηση, clean desk policy).

4. Αντιδρούν σωστά σε περιστατικό ασφαλείας: ποιον ενημερώνω, τι κάνω, τι δεν κάνω.

5. Εφαρμόζουν βασικές πρακτικές προστασίας δεδομένων στην καθημερινή εργασία (κοινή χρήση αρχείων, αποθήκευση, απόρριψη).

6. Αναπτύσσουν Προσωπικό Σχέδιο Ψηφιακής Υγιεινής για εφαρμογή στον χώρο εργασίας τους.

Σε επίπεδο στάσεων

1. Αντιμετωπίζουν την κυβερνοασφάλεια ως ευθύνη κάθε εργαζομένου και όχι ως αποκλειστικό θέμα IT.

2. Υιοθετούν στάση επαγρύπνησης: «σκέψου πριν κάνεις κλικ» ως αντανακλαστικό.

3. Αναγνωρίζουν ότι η αναφορά ενός ύποπτου συμβάντος δεν αποτελεί ντροπή αλλά καθήκον.

4. Εκτιμούν τη σημασία της συνεχούς ενημέρωσης σε ένα τοπίο απειλών που εξελίσσεται ραγδαία.

5. Δεσμεύονται για τη δημιουργία κουλτούρας κυβερνοασφάλειας στον οργανισμό τους.

5. Περιγραφή υποψηφίων για συμμετοχή (θέσεις εργασίας / επάγγελμα):

Το πρόγραμμα απευθύνεται σε όλους τους εργαζόμενους ανεξαρτήτως θέσης, τμήματος ή τεχνολογικού υπόβαθρου. Δεν αποτελεί τεχνικό σεμινάριο IT — είναι πρόγραμμα μαζικής κατάρτισης για τον «ανθρώπινο παράγοντα» της κυβερνοασφάλειας. Συγκεκριμένα:

• Διοικητικούς υπαλλήλους και γραμματείς
• Στελέχη λογιστηρίου και οικονομικών τμημάτων
• Υπαλλήλους εξυπηρέτησης πελατών
• Στελέχη πωλήσεων και μάρκετινγκ
• Στελέχη ανθρώπινου δυναμικού
• Διευθυντές τμημάτων, team leaders, supervisors
• Προσωπικό υποδοχής και frontline υπαλλήλους
• Οποιονδήποτε εργαζόμενο χρησιμοποιεί υπολογιστή, email ή κινητή συσκευή στην εργασία του

Ιδιαίτερα κατάλληλο για επιχειρήσεις που εφαρμόζουν υβριδικό μοντέλο εργασίας, διαχειρίζονται ευαίσθητα δεδομένα πελατών ή υπόκεινται σε ρυθμιστικές υποχρεώσεις (GDPR, NIS2).

5Α. Περιγραφή εκπαιδευτή (προσόντα/πείρα):

Μάριος Κουντουρής - Computer Expert, IT Project Manager και Εκπαιδευτής Ενηλίκων

Ο Μάριος Κουντουρής σπούδασε Μηχανικός Υπολογιστών και Πληροφορική (BSc) καθώς και Data Science and Engineering (MSc) στο Τεχνολογικό Πανεπιστήμιο Κύπρου. Εργάζεται ως IT/Senior Project Manager στο Citizens In Power, όπου συντονίζει ευρωπαϊκά ερευνητικά προγράμματα (Horizon/Erasmus+) και διαχειρίζεται την ψηφιακή υποδομή του οργανισμού.

Διαθέτει εκτεταμένη τεχνική εμπειρία σε θέματα ασφάλειας πληροφοριακών συστημάτων, διαχείρισης δικτύων, προστασίας δεδομένων και εφαρμογής πολιτικών κυβερνοασφάλειας σε οργανισμούς. Η εμπειρία του καλύπτει τον πλήρη κύκλο ψηφιακής ασφάλειας: από τον σχεδιασμό πολιτικών και διαδικασιών, μέχρι την τεχνική υλοποίηση μέτρων προστασίας, την εκπαίδευση προσωπικού και τη διαχείριση περιστατικών. Έχει εργαστεί εκτεταμένα με πολλαπλές τεχνολογίες (web development, server management, database administration) και κατανοεί σε βάθος τόσο τις τεχνικές όσο και τις ανθρώπινες πτυχές της κυβερνοασφάλειας.

Ως εκπαιδευτής ενηλίκων, έχει σχεδιάσει και υλοποιήσει εκπαιδευτικά προγράμματα σε θέματα ψηφιακών δεξιοτήτων, κυβερνοασφάλειας και ψηφιακού μετασχηματισμού. Η εκπαιδευτική του προσέγγιση βασίζεται στην πρακτική εφαρμογή, τη χρήση ρεαλιστικών σεναρίων και live demonstrations, καθιστώντας σύνθετα τεχνικά θέματα προσβάσιμα σε μη τεχνικό κοινό. Πιστεύει ότι η κυβερνοασφάλεια δεν είναι θέμα τεχνολογίας αλλά κουλτούρας — και η κατάρτιση κάθε εργαζομένου αποτελεί την πιο αποτελεσματική επένδυση προστασίας.

Για περισσότερες πληροφορίες μπορείτε να διαβάσετε και το βιογραφικό σημείωμα που επισυνάπτεται.

6. Σύνδεση με Πρότυπα Επαγγελματικών Προσόντων της ΑνΑΔ:

Δεν ισχύει

7. Μέθοδοι και τεχνικές κατάρτισης:

Μέθοδοι κατάρτισης

Η μέθοδος που θα χρησιμοποιηθεί είναι η κατά πρόσωπο εκπαίδευση. Η επιλογή αυτή ενδείκνυται ιδιαίτερα για πρόγραμμα κυβερνοασφάλειας που απευθύνεται σε μη τεχνικό προσωπικό, καθώς:

• Επιτρέπει live demonstrations που δείχνουν σε πραγματικό χρόνο πώς λειτουργεί μια επίθεση phishing, πώς χακάρεται ένας αδύναμος κωδικός, πώς μοιάζει ένα ψεύτικο website — δημιουργώντας άμεση αίσθηση κινδύνου.

• Η κατά πρόσωπο αλληλεπίδραση ενισχύει τη δέσμευση εργαζομένων που συχνά θεωρούν την κυβερνοασφάλεια «βαρετό θέμα IT».

• Ο εκπαιδευτής μπορεί να προσαρμόσει τα σενάρια στη συγκεκριμένη πραγματικότητα κάθε ομάδας.

• Δημιουργεί κλίμα εμπιστοσύνης όπου οι συμμετέχοντες μπορούν να παραδεχτούν λάθη ή αδυναμίες χωρίς φόβο.

Τεχνικές Κατάρτισης

1. Τεχνική της Επίδειξης (Live Demo)

Κεντρικός πυλώνας. Ο εκπαιδευτής επιδεικνύει σε πραγματικό χρόνο: πώς δημιουργείται ένα phishing email, πώς σπάει ένας αδύναμος κωδικός σε δευτερόλεπτα, πώς μοιάζει ένα ψεύτικο site, τι βλέπει ο hacker. Τα live demos δημιουργούν «wow moment» που μετατρέπει αφηρημένους κινδύνους σε χειροπιαστή πραγματικότητα.

2. Τεχνική της Προσομοίωσης

Οι συμμετέχοντες λαμβάνουν «ψεύτικα» phishing emails κατά τη διάρκεια του σεμιναρίου και πρέπει να αποφασίσουν: κλικάρω ή όχι; Αναφέρω ή αγνοώ; Η τεχνική αυτή μετατρέπει τη θεωρία σε αντανακλαστικό. Επίσης: προσομοίωση αντίδρασης σε περιστατικό ασφαλείας.

3. Πρακτική Άσκηση

Δομημένες ασκήσεις: δημιουργία ισχυρού κωδικού, εγκατάσταση password manager, ρύθμιση MFA σε πραγματικό λογαριασμό, αναγνώριση 10 phishing emails (ποια είναι αληθινά;), έλεγχος αν τα δικά τους credentials έχουν διαρρεύσει.

4. Τεχνική της Μελέτης Περίπτωσης (Case Study)

Πραγματικά σενάρια από την Κύπρο: η παραβίαση Thalis (Cyprus Post), επιθέσεις σε τράπεζες, ransomware σε λογιστικά γραφεία, phishing σε τουριστικές επιχειρήσεις. Ανάλυση: τι πήγε στραβά, ποιος ήταν ο ανθρώπινος παράγοντας, πώς θα μπορούσε να αποφευχθεί.

5. Τεχνική της Διάλεξης – Εισήγησης

Συνοπτικές εισηγήσεις για το θεωρητικό πλαίσιο: τύποι απειλών, αρχές κυβερνοασφάλειας, βασικά GDPR/NIS2, τι σημαίνει «ψηφιακή υγιεινή». Σύντομες και εστιασμένες, αφήνοντας τον κύριο χρόνο στην πράξη.

6. Βιωματικό Εργαστήριο

«Phishing Quiz»: οι συμμετέχοντες βλέπουν 15 emails/μηνύματα και αποφασίζουν ποια είναι κακόβουλα. «Password Cracking Challenge»: πόσο γρήγορα θα σπάσει ο κωδικός σου; «Spot the Fake»: αναγνώριση ψεύτικων ιστοσελίδων, SMS, QR codes.

7. Εργασία σε Ομάδες

Ομάδες σχεδιάζουν βασική πολιτική κυβερνοασφάλειας για τον οργανισμό τους, αναπτύσσουν «Do's and Don'ts» λίστα, δημιουργούν incident response checklist.

8. Τεχνική του Καταιγισμού Ιδεών (Brainstorming)

Ανάδειξη τρωτών σημείων στις καθημερινές πρακτικές κάθε ομάδας. «Πού είμαστε ευάλωτοι;» — οι ίδιοι οι συμμετέχοντες εντοπίζουν κενά.

9. Τεχνική Ερωτήσεων – Απαντήσεων

Διαρκής αλληλεπίδραση, αποσαφήνιση αποριών, σύνδεση με πραγματικές εμπειρίες.

7Α. Διαρρύθμιση χώρου κατάρτισης:

Η διαρρύθμιση του χώρου θα είναι σε «Εργαστηριακή Διάταξη με Ομαδική Συνεργασία», όπου κάθε καταρτιζόμενος διαθέτει πρόσβαση σε υπολογιστή ή φορητή συσκευή με σύνδεση στο διαδίκτυο — απαραίτητο για τις ζωντανές επιδείξεις, τα phishing quizzes και τις πρακτικές ασκήσεις. Οι σταθμοί εργασίας θα επιτρέπουν εύκολη εναλλαγή μεταξύ ατομικής εργασίας και ομαδικών δραστηριοτήτων. Ο εκπαιδευτής χρησιμοποιεί projector για τα live demos ενώ μετακινείται στον χώρο για εξατομικευμένη καθοδήγηση.

8. Μέσα και υλικά κατάρτισης:

Μέσα Κατάρτισης:

• Υπολογιστής εκπαιδευτή και προβολικό σύστημα (projector) για live demonstrations
• Εργαστήριο υπολογιστών ή/και φορητών συσκευών με πρόσβαση στο διαδίκτυο
• Διαφάνειες παρουσίασης (PowerPoint)
• Demo περιβάλλον: δείγματα phishing emails, fake websites, password cracking tools (εκπαιδευτικά)
• Πλατφόρμα Kahoot/Mentimeter

Υλικά Κατάρτισης:

• Εγχειρίδιο κατάρτισης «Κυβερνοασφάλεια για Όλους» με πρακτικές οδηγίες
• Φάκελος 15 δειγμάτων phishing emails/μηνυμάτων (Phishing Quiz Pack)
• Quick Reference Card: «Τα 10 Σημάδια ενός Phishing Email»
• Quick Reference Card: «Πώς Δημιουργώ Ισχυρό Κωδικό»
• Quick Reference Card: «Τι Κάνω αν Πέσω Θύμα — Βήματα Αντίδρασης»
• Checklist: Ψηφιακή Υγιεινή για Υβριδική Εργασία
• Φύλλα εργασίας: Cyber Risk Self-Assessment, Incident Response Plan template
• Αφίσα «Do's & Don'ts» για εκτύπωση στο γραφείο

• Λίστα δωρεάν εργαλείων κυβερνοασφάλειας (password managers, MFA apps, breach checkers)

9. Σύστημα τήρησης στοιχείων:

Πιστή τήρηση Παρουσιολογίου

10. Σύστημα αξιολόγησης:

Τύποι Αξιολόγησης

Θα αξιοποιηθούν διαμορφωτική και απολογιστική/τελική αξιολόγηση, συνδυάζοντας ποιοτικές και ποσοτικές μεθόδους.

Κατά τη διάρκεια: Kahoot quiz (αναγνώριση phishing, σωστές πρακτικές κωδικών, γνώσεις GDPR), Mentimeter polls (αυτοαξιολόγηση συνηθειών), phishing simulation scoring, παρατήρηση κατά τις πρακτικές ασκήσεις.

Στο τέλος: Ηλεκτρονικό ερωτηματολόγιο αξιολόγησης.

Άξονες Αξιολόγησης

Εκπαιδευτής: τεχνική γνώση, ικανότητα απλοποίησης σύνθετων θεμάτων, ποιότητα live demos, εξατομικευμένη καθοδήγηση.

Καταρτιζόμενοι: συμμετοχή, απόδοση στο phishing quiz (πριν/μετά), εφαρμογή πρακτικών, ποιότητα ομαδικών παραδοτέων.

Περιεχόμενο: πρακτική εφαρμοσιμότητα, ρεαλιστικότητα σεναρίων, σύνδεση με κυπριακή πραγματικότητα, κάλυψη NIS2/GDPR.

Συνθήκες: τεχνολογική υποδομή, πρόσβαση στο internet, δυνατότητα live demos.

Οργάνωση: ροή ενοτήτων, αναλογία θεωρίας/πράξης (στόχος 25%-75%), τήρηση χρόνων.

Εργαλεία Αξιολόγησης

Διαμορφωτική: Kahoot, Mentimeter, phishing simulation scoring.

Απολογιστική: Google Forms ερωτηματολόγιο + σύγκριση phishing quiz score πριν/μετά.

Τεχνικές Αξιολόγησης: Ερωτηματολόγια, phishing quiz (pre/post), παρατήρηση, αξιολόγηση ομαδικών παραδοτέων (πολιτική ασφάλειας), peer feedback.

Τύποι Ερωτήσεων: Κλειστές (Likert 1-5, πολλαπλής επιλογής), ανοικτές, ερωτήσεις σεναρίων.

Κλίμακες: Τακτική/Ιεραρχική (Likert 1-5). Αναλογική (1-100) πριν/μετά.

Αποδέκτες: ΚΕΚ, εκπαιδευτής, καταρτιζόμενοι.

Τρόποι Κοινοποίησης: Γραπτή Έκθεση, Προφορική Παρουσίαση, Περίληψη αποτελεσμάτων.

11. Πιστοποίηση της κατάρτισης:

Το ΚΕΚ δεσμεύεται για απονομή Πιστοποιητικού Κατάρτισης σε όσους από τους συμμετέχοντες θα ολοκληρώσουν με επιτυχία το πρόγραμμα. Στο Πιστοποιητικό Κατάρτισης, στο κάτω μέρος, θα πρέπει να αναφέρεται: «Το πρόγραμμα εγκρίθηκε από την Αρχή Ανάπτυξης Ανθρώπινου Δυναμικού».

12. Περιεχόμενο κατάρτισης:

Α/Α	ΑΝΑΛΥΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ ΕΝΟΤΗΤΩΝ	ΔΙΑΡΚΕΙΑ (ΩΡΕΣ)
1	**Τα Θεμέλια: Το Τοπίο Κυβερνοαπειλών στην Κύπρο** • Γιατί η κυβερνοασφάλεια αφορά τον καθένα — όχι μόνο το τμήμα IT • Αριθμοί που μιλούν: 53% των κυπριακών επιχειρήσεων δέχθηκαν επίθεση • Τι είναι phishing, ransomware, social engineering, malware — εξήγηση χωρίς τεχνική ορολογία • Ο ανθρώπινος παράγοντας: γιατί εσύ είσαι ο πρώτος τοίχος άμυνας • Κανονιστικό πλαίσιο: GDPR, NIS2 — τι σημαίνει για εσένα • Self-assessment: «Πόσο ασφαλής είμαι;» (ερωτηματολόγιο baseline) *Διάλεξη/Εισήγηση, Επίδειξη, Συζήτηση, Ερωτήσεις-απαντήσεις*	0,75
2	**Phishing: Η #1 Απειλή — Αναγνώρισε, Αποφύγισε, Ανέφερε** • Ανατομία ενός phishing email: τα 10 σημάδια αναγνώρισης • Spear phishing, smishing (SMS), vishing (τηλέφωνο), QR code phishing • Live demo: Πώς δημιουργεί ένας hacker ένα πειστικό phishing email σε 2 λεπτά • AI-powered phishing: πώς η τεχνητή νοημοσύνη κάνει τις επιθέσεις πιο πειστικές • Phishing Quiz: 15 emails — ποια είναι αληθινά, ποια κακόβουλα; • Τι κάνω αν κλίκαρα: βήματα άμεσης αντίδρασης *Επίδειξη, Προσομοίωση, Βιωματικό εργαστήριο, Πρακτική άσκηση, Ερωτήσεις-απαντήσεις*	1,5
	ΔΙΑΛΕΙΜΜΑ	**0,25**
3	**Κωδικοί, Αυθεντικοποίηση & Ψηφιακή Ταυτότητα** • Live demo: Πόσο γρήγορα σπάει ο κωδικός σου; (password cracking σε πραγματικό χρόνο) • Πώς δημιουργώ κωδικό που δεν σπάει — πρακτικές τεχνικές • Password managers: τι είναι, πώς δουλεύουν, πρακτική εγκατάσταση • Πολυπαραγοντική αυθεντικοποίηση (MFA): η ασπίδα που πρέπει να ενεργοποιήσεις • Έλεγχος: Έχουν διαρρεύσει τα στοιχεία μου; (haveibeenpwned.com demo) • Πρακτική: Κάθε συμμετέχων αλλάζει κωδικούς, ρυθμίζει MFA, εγκαθιστά password manager *Επίδειξη, Πρακτική άσκηση, Βιωματικό εργαστήριο, Ερωτήσεις-απαντήσεις*	1,25
4	**Ασφαλής Υβριδική Εργασία & Προστασία Δεδομένων** • Κίνδυνοι εκτός γραφείου: δημόσια Wi-Fi, προσωπικές συσκευές, USB, εκτυπωτές • VPN: τι είναι, γιατί το χρειάζομαι, πώς το χρησιμοποιώ • Ασφαλής κοινή χρήση αρχείων: cloud storage, email attachments, εξωτερικά media	1,25

	• Clean desk & clean screen policy • GDPR στην πράξη: τι δεν στέλνω ποτέ σε email, πώς διαγράφω σωστά • Case study: Κυπριακή εταιρεία χάνει δεδομένα λόγω ανθρώπινου λάθους *Διάλεξη/Εισήγηση, Επίδειξη, Μελέτη περίπτωσης, Πρακτική άσκηση, Εργασία σε ομάδες*	
	ΔΙΑΛΕΙΜΜΑ	**0,25**
5	**Social Engineering, Ransomware & Αντίδραση σε Περιστατικά** • Social engineering: πώς σε χειραγωγούν (pretexting, baiting, tailgating) • Ransomware: τι γίνεται όταν «κλειδώνουν» τα δεδομένα — πραγματικά παραδείγματα • Deepfakes & AI scams: η νέα γενιά απάτης • Incident Response: τα 5 βήματα αν πέσεις θύμα (αποσύνδεσε, ενημέρωσε, μην πληρώσεις, τεκμηρίωσε, μάθε) • Προσομοίωση: «Η επιχείρηση δέχεται επίθεση» — ομαδική αντίδραση *Επίδειξη, Προσομοίωση, Μελέτη περίπτωσης, Εργασία σε ομάδες, Συζήτηση*	1
6	**Κουλτούρα Κυβερνοασφάλειας & Προσωπικό Σχέδιο Δράσης** • Δημιουργία κουλτούρας: πώς κάνουμε την ασφάλεια «κανονικότητα» και όχι βάρος • Ομαδική άσκηση: σχεδιασμός «Do's & Don'ts» πολιτικής για τον οργανισμό • Προσωπικό Σχέδιο Ψηφιακής Υγιεινής: τι αλλάζω από αύριο • Phishing Quiz 2.0: επανάληψη quiz — σύγκριση βελτίωσης (πριν vs μετά) • Αξιολόγηση προγράμματος • Q&A και κλείσιμο *Πρακτική άσκηση, Εργασία σε ομάδες, Καταιγισμός ιδεών, Ερωτήσεις-απαντήσεις*	0,75
	ΣΥΝΟΛΟ	**7 ώρες**

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Η υποβολή της αίτησης προϋποθέτει ότι, το Κέντρο Επαγγελματικής Κατάρτισης έχει ενημερωθεί για τις πρόνοιες του Οδηγού Πολιτικής και Διαδικασιών που διέπουν τη συνεργασία του με την ΑνΑΔ για την εφαρμογή Πολυεπιχειρησιακών Προγραμμάτων Κατάρτισης - Συνήθων, τις αποδέχεται και δεσμεύεται για την πιστή τήρησή τους.

Ημερομηνία _____ Ονοματεπώνυμο Διευθυντή ή Υπογραφή και Σφραγίδα Εξουσιοδοτημένου Αντιπροσώπου Κέντρου Επαγγελματικής Κατάρτισης