ΠΟΛΥΕΠΙΧΕΙΡΗΣΙΑΚΑ ΠΡΟΓΡΑΜΜΑΤΑ ΚΑΤΑΡΤΙΣΗΣ ΣΥΝΗΘΗ ΥΠΟΒΟΛΗ ΝΕΑΣ΄Η ΣΑΝ ΝΕΑΣ΄Η ΟΠΩΣ ΕΙΝΑΙ ΠΡΟΔΙΑΓΡΑΦΗΣ

Α. Στοιχεία ΚΕΚ

Αριθμός ΑνΑΔ:	5046
Επωνυμία:	C.I.P. CITIZENS IN POWER

Β. Στοιχεία προδιαγραφής

Β.1 Τίτλος προδιαγραφής

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

Β.2 Περιγραφή προδιαγραφής

Πρόγραμμα μαζικής κατάρτισης 7 ωρών για μη τεχνικό προσωπικό, εστιασμένο στον «ανθρώπινο παράγοντα» — την #1 αιτία κυβερνοεπιθέσεων. Περιλαμβάνει αναγνώριση phishing, δημιουργία ισχυρών κωδικών, ασφαλή υβριδική εργασία, βασικά GDPR/NIS2 και αντίδραση σε περιστατικά, μέσω live demos, phishing simulations και hands-on ασκήσεων. Βασισμένο σε δεδομένα της Αρχής Ψηφιακής Ασφάλειας Κύπρου (53% των επιχειρήσεων δέχθηκαν επίθεση το 2025).

Β.3 Ανάγκη κατάρτισης

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

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(I)/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.

Β.4 Στόχοι κατάρτισης

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.

Β.5 Περιγραφή υποψηφίου για συμμετοχή

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).

Β.6 Καθαρή διάρκεια

07:00

Β.7 <u>Σύνδεση με Πρότυπα Επαγγελματικών Προσόντων (ΠΕΠ)</u>

Στοιχεία ΠΕΠ:

Β.8 Δομή Προγράμματος

Ενότητα	Ανάλυση περιεχομένου	Διάρκεια	Πρακτικό
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)	01:15	Όχι
Phishing: Η #1 Απειλή — Αναγνώρισε, Αποφύγισε, Ανέφερε	• Ανατομία ενός phishing email: τα 10 σημάδια αναγνώρισης	01:30	Όχι

	• 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		
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	01:15	Όχι

	MFA, εγκαθιστά password manager		
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 • 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	01:00	Όχι
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)	01:00	Όχι

	• Προσομοίωση: «Η επιχείρηση δέχεται επίθεση» — ομαδική αντίδραση		
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	01:00	Όχι

Ημερομηνία υποβολής: 14/04/2026