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

Ψηφιακή Ασφάλεια στην Καθημερινότητα και Προστασία Δεδομένων στη Σύγχρονη Εποχή του AI

Β.2 Περιγραφή προδιαγραφής

Το σεμιναριο αυτό εχει ως σκοπό την ανάπτυξη βασικών γνώσεων, δεξιοτήτων και στάσεων στον τομέα της ψηφιακής ασφάλειας, ώστε οι καταρτιζόμενοι να αναγνωρίζουν κινδύνους, να διαχειρίζονται αποτελεσματικά περιστατικά ασφάλειας και να εφαρμόζουν ασφαλείς πρακτικές κατά τη χρήση διαδικτύου, εφαρμογών και κοινωνικών δικτύων, προστατεύοντας τα προσωπικά και επαγγελματικά τους δεδομένα

Β.3 Ανάγκη κατάρτισης

Η επαγγελματική καθημερινότητα των πολιτών και επιχειρήσεων βασίζεται ολο και περισσότερο πλέον σε ψηφιακές υπηρεσίες όπως ηλεκτρονικές συναλλαγές, e-banking, social media, εργασία από απόσταση, έξυπνες συσκευές IoT και χρήση AI. Λόγω αυτής της εξάρτησης/αναγκαιότητας αυξάνονται σημαντικά τα περιστατικά ηλεκτρονικής απάτης, υποκλοπής δεδομένων και κακόβουλων επιθέσεων.

Παρατηρείται έλλειψη βασικών γνώσεων ψηφιακής ασφάλειας, γεγονός που οδηγεί σε οικονομικές απώλειες, κινδύνους παραβιάσεων προσωπικών δεδομένων σε οργανισμούς και επιχειρήσεις.

Το σεμινάριο στοχεύει στην ενίσχυση και απόκτησης πρακτικών των ψηφιακών δεξιοτήτων,

ψηφιακής συνείδησης καθώς και στην ικανότητα προστασίας του εαυτού, του σπιτιού και του χώρου εργασίας μας.

Β.4 Στόχοι κατάρτισης

Οι συμμετέχοντες, με το πέρας του προγράμματος θα πρέπει να είναι ικανοί σε επίπεδο:

➢ Γνώσεως να:

• Ταξινομουν τα πεντε βήματα προς ανάκτηση παραβιασμένου λογαριαμου

• Περιγράφουν τουλάχιστον τρία βασικά κριτήρια αναγνώρισης ασφαλών ιστοσελίδων

• Αναγνωρίζουν τουλάχιστον τρεις κινδύνους που σχετίζονται με τη διαχείριση αδειών εφαρμογών και προσωπικών δεδομένων.

• Εξηγούν τουλάχιστον δύο βασικές έννοιες προστασίας ιδιωτικότητας στα κοινωνικά δίκτυα

• Περιγράφουν τουλάχιστον τρεις βασικές λειτουργίες εργαλείων ασφάλειας όπως antivirus και firewall.

• Ονομάζουν τουλάχιστον τέσσερα βασικά μέτρα προστασίας προσωπικών δεδομένων κατά τη χρήση διαδικτύου.

• Περιγράφουν δυο μέτρα ασφαλούς τηλεργασίας

➢ Δεξιοτήτων να:

• Διαχειρίζονται τις ενημερώσεις ασφαλείας σε συσκευές και εφαρμογές για την προστασία δεδομένων.

• Εφαρμόζουν τη διαδικασία αναφορας περιστατικου

• Εφαρμόζουν τουλάχιστον δύο εργαλεία για έλεγχο ασφάλειας ιστοσελίδων.

• Διορθώνουν τουλάχιστον 2 social media posts για αποφυγή παραχώρησης προσωπικών δεδομένων.

• Επιλέγουν ασφαλείς πρακτικές πλοήγησης σε δημόσια δίκτυα εφαρμόζοντας τουλάχιστον δύο μέτρα προστασίας πρόσβασης για την προστασία λογαριασμών.

• Εφαρμόζουν τουλάχιστον δυο κανονισμούς και νομοθεσίες σχετικα με την προστασια της επιχείρησης

• Αναγνώριση (μέσα από πρακτικό εργαλείο αξιολόγησης - Penetration Tests) ευάλωτων σημείων σε κυβερνοεπιθέσεις ανα οργανισμό

➢ Στάσεων να:

• Αντιμετωπίζουν με υπευθυνότητα μια κυβερνοεπιθεση

• Υιοθετούν υπεύθυνη στάση ως προς τη διαχείριση προσωπικών δεδομένων στο διαδίκτυο.

• Εκτιμούν τη σημασία της προληπτικής προστασίας κατά τη χρήση ψηφιακών υπηρεσιών.

• Αναπτύσσουν συνειδητή στάση απέναντι στους κινδύνους παραπληροφόρησης και ψηφιακής εξαπάτησης.

• Υποστηρίζουν την εφαρμογή ασφαλών πρακτικών χρήσης ψηφιακών συσκευών.

• Εκτιμούν τη σημαντικότητα του Backup τόσο στην προσωπική οσο και επαγγελματική ζωή.

• Αμφισβητούν την εφαρμογή εσωτερικών πρακτικών σε περίπτωση που δεν είναι εναρμονισμένοι με τους βασικούς κανόνες ψηφιακής ασφάλειας

Β.5 Περιγραφή υποψηφίου για συμμετοχή

Το πρόγραμμα απευθύνεται σε εργαζόμενους δημόσιου και ιδιωτικού τομέα, αυτοαπασχολούμενους και στελέχη ΜΜΕ των οποίων τα επαγγελματικά καθήκοντα περιλαμβάνουν καθημερινή χρήση ψηφιακών εργαλείων και πληροφοριακών συστημάτων. Ενδεικτικά, αφορά θέσεις διοικητικής και γραμματειακής υποστήριξης, οικονομικών υπηρεσιών και λογιστηρίου, επικοινωνίας και μάρκετινγκ, εξυπηρέτησης πελατών, καθώς και εργαζόμενους σε καθεστώς τηλεργασίας που συνδέονται εξ αποστάσεως σε εταιρικά δίκτυα. Δεν απαιτείται εξειδικευμένο τεχνικό υπόβαθρο· προαπαιτούμενο αποτελεί η βασική γνώση χρήσης υπολογιστή και διαδικτύου στο εργασιακό περιβάλλον.

Β.6 Καθαρή διάρκεια

11:00

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

Στοιχεία ΠΕΠ:

Β.8 Δομή Προγράμματος

Ενότητα	Ανάλυση περιεχομένου	Διάρκεια	Πρακτικό
Εναρκτήρια ενότητα	Γνωριμία συμμετεχόντων – παγοθραύστης • Παρουσίαση σκοπού & στόχων σεμιναρίου • Συμβόλαιο δέσμευσης	00:30	Όχι
Ψηφιακή ασφάλεια και Τύποι Κυβερνοεπιθεσεων	● Κυβερνοασφάλεια και κυβερνοεπίθεση ● Τι είναι τα δεδομένα και γιατί έχουν αξία ● Hackers, τύποι και κίνητρα ● Κακόβουλα λογισμικα (Malwares) ● Επιθέσεις σε επίπεδο Δικτύου (Network Attacks) ● Τα 3 πιο γνωστά Malware στην ιστορία ● Παραδείγματα πραγματικών επιθέσεων (Κυπρος)	01:30	Όχι
Επιθέσεις μέσω Κοινωνικής τεχνικής (Social Engineering)	• Phishing (email) • Vishing και Smishing • Tailgating και Baiting	01:00	Όχι

Διαχείριση Περιστατικών & Πρακτική Εφαρμογή	• Τι κάνουμε αν πατήσουμε phishing link και παραβιαστεί ο λογαριασμός μας; • Βασικά βήματα ανάκτησης • Διαδικασία αναφοράς περιστατικών	01:30	Όχι
Ασφαλής Χρήση Διαδικτύου και Διαχείριση Ψηφιακού Αποτυπώματος	• Πώς αναγνωρίζουμε ασφαλείς ιστοσελίδες ,ελεγχος URL ,terms and policies • Αδειες χρήσης εφαρμογών • Αγορές online με ασφάλεια • Αποθήκευση κωδίκων στο Browser • Δημόσια WiFi και τι να προσέχω • Χρήση VPN και Tor • Social Media και ιδιωτικότητα ΤΕΛΟΣ 1ΗΣ ΜΕΡΑΣ	02:30	Όχι
• Πώς αναγνωρίζουμε ασφαλείς ιστοσελίδες ,ελεγχος URL ,terms and policies • Αδειες χρήσης εφαρμογών • Αγορές online με ασφάλεια • Αποθήκευση κωδίκων στο Browser • Δημόσια WiFi και τι να προσέχω • Χρήση VPN και Tor • Social Media και ιδιωτικότητα	• Τι είναι το IOT (Internet of Things) • Mobile Privacy και εύρεση συσκευών στον Δίκτυο μου • Κίνδυνοι - Less Is More • Χρήση Firewall και Antivirus • Γιατί είναι σημαντικά τα Updates • Παράδειγμα επίθεσης Mirai (2016)	01:00	Όχι
Προστασία δεδομένων και κρυπτογράφηση	• Clean Desk, Clean Screen Policies, secure USB ports	01:30	Όχι

	• Ισχυροί κωδικοί πρόσβασης (password policies) • Δημιουργία Κρυπτογραφημένου αρχείου - Χρήση Password Managers • Μέθοδοι προστασίας λογαριασμών • ENIGMA - Η πιο διάσημη μηχανή κρυπτογράφησης • Σε τι χρησιμεύει το Backup (external drive,cloud,NAS)		
Προστασια της επιχείρησης και πρότυπα	• Κανονισμοί & Νομοθεσία (GDPR, NIS2,DORA) • Πρότυπα Ασφάλειας (ISO 27001, NIST) • Cybersecurity policies • Penetration Tests • Ασφαλής Τηλεργασία • Εκπαίδευση προσωπικού	01:00	Όχι
Καταληκτική ενότητα	• Ανακεφαλαίωση • Απολογιστική Αξιολόγηση • Συμπεράσματα	00:30	Όχι

Ημερομηνία υποβολής: 15/05/2026