

Αθήνα, 05/08/2026

Α. Π.: 29323 ΕΞ 2026

Απάντηση στο έγγραφο: 28052

ΕΞ 2026



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΠΙΤΕΛΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΤΜΗΜΑ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ
Δ/νση: Χανδρή 1 & Θεσσαλονίκης
Τ.Κ.: 18346, Μοσχάτο Αττικής
Πληροφορίες: Ι. Βοζώρης
Τηλ.: 210 480 2040
E-mail: i.vozoris@cyber.gov.gr

Προς: 1. Υπηρεσία Συντονισμού
2. Γραφείο Νομικών και
Κοινοβουλευτικών Θεμάτων

Κοιν: Γραφείο Υπουργού

Θέμα: Απάντηση σε Ερώτηση στο πλαίσιο κοινοβουλευτικού ελέγχου

Σχετ.: α. Το υπ' αρ. πρωτ. 28052 ΕΞ 2026/28-07-2026 έγγραφο της Υπηρεσίας Συντονισμού

β. Η υπ' αρ. 7336/27.7.2026 Ερώτηση της βουλευτού κ. Ε. Λιακούλη με θέμα: «Άμεση ανάγκη ευρείας ενημερωτικής καμπάνιας για την αντιμετώπιση τηλεφωνικών απατών και ληστειών με τη χρήση Τεχνητής Νοημοσύνης (AI Voice Cloning)»

Σε απάντηση του α' σχετικού, με το οποίο διαβιβάστηκε στην Υπηρεσία μας το ως άνω β' σχετικό, και στο πλαίσιο των αρμοδιοτήτων μας, σας ενημερώνουμε για τα εξής:

Η Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ), δυνάμει του ν. 5086/2024 (Α' 23), αποτελεί την αρμόδια εθνική αρχή για τη διαμόρφωση, παρακολούθηση υλοποίησης και τον συντονισμό εφαρμογής της εθνικής στρατηγικής κυβερνοασφάλειας. Σύμφωνα με το ν. 5160/2024 (Α' 195), ασκεί αρμοδιότητες ρυθμιστικές, εποπτείας και επιχειρησιακού συντονισμού αναφορικά με την πρόληψη, ανίχνευση, αντιμετώπιση και αποκατάσταση περιστατικών κυβερνοασφάλειας που επηρεάζουν βασικές και σημαντικές οντότητες. Οι αρμοδιότητές της περιλαμβάνουν, ιδίως, τη διαχείριση σημαντικών περιστατικών σε κρίσιμες υποδομές του δημόσιου και ιδιωτικού τομέα, τη διασφάλιση της κανονιστικής συμμόρφωσης, τον επιχειρησιακό σχεδιασμό και την ανάπτυξη τεχνικών δυνατοτήτων, συμπεριλαμβανομένης της λειτουργίας Ομάδας Απόκρισης για Συμβάντα Ασφάλειας Υπολογιστών (CSIRT).

Η αξιοποίηση τεχνολογιών τεχνητής νοημοσύνης (Artificial Intelligence – AI), συμπεριλαμβανομένων εφαρμογών σύνθεσης ή αναπαραγωγής φωνής (voice cloning) και δημιουργίας ψευδούς οπτικοακουστικού περιεχομένου (deepfakes), διευρύνει σημαντικά τις δυνατότητες των δραστών να εξαπατούν πολίτες μέσω επιθέσεων κοινωνικής μηχανικής (social engineering), εκμεταλλευόμενοι την εμπιστοσύνη, την ψυχολογική πίεση και τη συναισθηματική τους φόρτιση.

Οι πρακτικές αυτές αναδεικνύουν μια ιδιαίτερα ανησυχητική και διαρκώς εξελισσόμενη μορφή κακόβουλης αξιοποίησης των ψηφιακών τεχνολογιών, όπου οι δυνατότητες της τεχνητής νοημοσύνης χρησιμοποιούνται για την παραπλάνηση και εξαπάτηση των πολιτών μέσω χειραγώγησης της ανθρώπινης συμπεριφοράς, καθιστώντας τις επιθέσεις ολοένα πιο πειστικές και δυσχερώς ανιχνεύσιμες. Αντίστοιχα φαινόμενα παρατηρούνται ήδη σε επιθέσεις ηλεκτρονικού «ψαρέματος» (phishing) μέσω ηλεκτρονικού ταχυδρομείου και «smishing» μέσω γραπτών μηνυμάτων κινητής τηλεφωνίας, των οποίων τα χαρακτηριστικά καθίστανται ολοένα και πιο πειστικά, δυσχεραίνοντας την αναγνώρισή τους από τον μέσο χρήστη.

Σε απάντηση του πρώτου ερωτήματος, η Εθνική Αρχή Κυβερνοασφάλειας στο πλαίσιο των αρμοδιοτήτων της, υλοποιεί δράσεις ενημέρωσης και ευαισθητοποίησης για την ασφαλή χρήση των ψηφιακών υπηρεσιών και την αναγνώριση των συνηθέστερων μορφών ηλεκτρονικής απάτης συμπεριλαμβανομένων των deepfake. Παράλληλα, αξιοποιεί συστηματικά τους διαθέσιμους διαύλους επικοινωνίας της για την έγκαιρη δημοσιοποίηση ανακοινώσεων και συστάσεων προς τους πολίτες σχετικά με εκτεταμένες εκστρατείες απάτης στον κυβερνοχώρο, καθώς και για την παροχή πρακτικών οδηγιών προστασίας μέσω της ειδικής ενότητας συστάσεων προς τους πολίτες στην ιστοσελίδα της.

Επιπλέον, η νέα Εθνική Στρατηγική Κυβερνοασφάλειας 2026–2030 αναγνωρίζει ότι η κακόβουλη αξιοποίηση τεχνολογιών τεχνητής νοημοσύνης και “deepfakes” συνιστά αναδυόμενη απειλή, με δυνητικές επιπτώσεις όχι μόνο στην κυβερνοασφάλεια αλλά και στην εμπιστοσύνη των πολιτών. Για τον λόγο αυτό, προβλέπει την περαιτέρω ενίσχυση της εθνικής κυβερνοανθεκτικότητας μέσω δράσεων πρόληψης, έγκαιρης ανίχνευσης και αντιμετώπισης κυβερνοαπειλών, την ανάπτυξη μηχανισμών συνεργασίας και ανταλλαγής πληροφοριών σε εθνικό και ευρωπαϊκό επίπεδο, την ενίσχυση των δυνατοτήτων αντιμετώπισης του κυβερνοεγκλήματος, καθώς και την ενίσχυση της ενημέρωσης και ευαισθητοποίησης των πολιτών έναντι τεχνικών κοινωνικής μηχανικής, ψευδούς ψηφιακού περιεχομένου και εκστρατειών παραπλάνησης.

- Ειδικότερα, σε απάντηση του δεύτερου και του τρίτου ερωτήματος, μέσω του Ειδικού Στόχου 1.Δ.1 και του 2.Α.4 της Εθνικής Στρατηγικής Κυβερνοασφάλειας που απευθύνονται και στους πολίτες, προβλέπονται σε συνεργασία των ΕΑΚ, ΥΨΗΔ, ΓΓ Επικοινωνίας & Ενημέρωσης, η διαμόρφωση και υλοποίηση ενός ενιαίου Εθνικού Σχεδίου Επικοινωνίας και Ευαισθητοποίησης για την Κυβερνοασφάλεια, το οποίο περιλαμβάνει συντονισμένες εκστρατείες ενημέρωσης, εκπαιδευτικό υλικό και δράσεις ευαισθητοποίησης πολιτών, επιχειρήσεων και δημόσιων φορέων σχετικά με τις σύγχρονες κυβερνοαπειλές και τις βέλτιστες πρακτικές προστασίας,
- σε συνεργασία των ΥΨΗΔ, ΕΑΚ, ΕΛ.ΑΣ, η διαμόρφωση και υλοποίηση ενός ενιαίου Εθνικού Σχεδίου Δράσης για την αντιμετώπιση κακόβουλων deepfakes, το οποίο περιλαμβάνει τον προσδιορισμό απαιτήσεων για τεχνολογίες ανίχνευσης παραποιημένου περιεχομένου, την ανάπτυξη πρωτοκόλλων συνεργασίας μεταξύ αρμόδιων φορέων, καθώς και την καλλιέργεια ικανοτήτων έγκαιρης αναγνώρισης και διαχείρισης σχετικών περιστατικών. Παράλληλα, προωθεί την ευθυγράμμιση με ευρωπαϊκές κατευθύνσεις και διεθνείς βέλτιστες πρακτικές, συμβάλλοντας στην περαιτέρω θωράκιση του θεσμικού πλαισίου και στη διασφάλιση της εμπιστοσύνης στην ψηφιακή επικοινωνία και ενημέρωση.

Τέλος, η ΕΑΚ βρίσκεται πάντα σε συστηματική και γόνιμη συνεργασία με όλους τους συναρμόδιους φορείς για το συντονισμό υλοποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας και την επίτευξη των εθνικών στρατηγικών στόχων.

Κατά τα λοιπά, αρμόδιο να απαντήσει επί των τιθέμενων ζητημάτων είναι το συνενωτώμενο Υπουργείο Προστασίας του Πολίτη.

Θέτουμε υπόψη σας τα παραπάνω και παραμένουμε στη διάθεσή σας για κάθε σχετικό θέμα.

Ο Διοικητής

Μιχαήλ Μπλέτσας

Εσωτερική διανομή:

1. Γραφείο Διοικητή Εθνικής Αρχής Κυβερνοασφάλειας
2. Γενική Διεύθυνση Επιτελικού Σχεδιασμού
3. Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας
4. Διεύθυνση Συντονισμού Φορέων