Αθήνα, 14/04/2026
Α. Π.: 13348 ΕΞ 2026
Απάντηση στο έγγραφο: 12004
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. 12004 ΕΞ 2026/01-04-2026 έγγραφο της Υπηρεσίας Συντονισμού

β. Η υπ' αρ. 4290/31.3.2026 Ερώτηση του βουλευτή κ. Γ. Μανούσου με θέμα: «Έξαρση SMS απάτης (smishing) – Τι κάνει η Πολιτεία και οι εταιρείες τηλεφωνίας για την προστασία των πολιτών;»

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 Αρχή, στο πλαίσιο των αρμοδιοτήτων της για την προστασία κρίσιμων ψηφιακών υποδομών και υπηρεσιών, παρακολουθεί και αξιολογεί συστηματικά κινδύνους που ενδέχεται να επηρεάσουν τη διαθεσιμότητα δικτύων και συστημάτων που υποστηρίζουν βασικές κοινωνικές και οικονομικές λειτουργίες. Στο πλαίσιο εφαρμογής της ενωσιακής και εθνικής νομοθεσίας για την κυβερνοασφάλεια, και ιδίως της Οδηγίας NIS2, όπως ενσωματώθηκε με τον ν. 5160/2024, οντότητες που εμπίπτουν στο πεδίο εφαρμογής του νόμου, υποχρεούνται να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα διαχείρισης των κινδύνων κυβερνοασφάλειας, καθώς και διαδικασίες αντιμετώπισης περιστατικών κυβερνοασφάλειας και επιχειρησιακής συνέχειας. Οι ως άνω απαιτήσεις έχουν εξειδικευθεί στην κ.υ.α. 1689/2025 (Β' 2186), η οποία καθορίζει το Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και

Σημαντικών Οντοτήτων του ν.5160/2024, και δεσμεύουν και τους παρόχους τηλεπικοινωνιακών υπηρεσιών και δικτύων.

Στη σύγχρονη ψηφιακή εποχή, η εξαπάτηση χρηστών για κλοπή δεδομένων μέσω email / SMS αποτελεί μία από τις πιο διαδεδομένες και εξελισσόμενες απειλές, με τα κακόβουλα μηνύματα να μιμούνται πειστικά νόμιμες επικοινωνίες τραπεζών, δημόσιων οργανισμών ή άλλων φορέων, προκαλώντας, διαταραχή της επιχειρησιακής συνέχειας των πληττόμενων οργανισμών, οικονομικές ζημίες και διαρροή προσωπικών δεδομένων των πολιτών. Ιδιαίτερη πρόκληση συνιστά το γεγονός ότι τα κακόβουλα μηνύματα καθίστανται ολοένα και πιο δύσκολο να διακριθούν από τις νόμιμες επικοινωνίες. Για τον μέσο χρήστη, ο εντοπισμός στοιχείων που αποκαλύπτουν την απάτη είναι συχνά εξαιρετικά περίπλοκος, καθώς τα μηνύματα αυτά μιμούνται με αυξανόμενη ακρίβεια τη μορφή, το ύφος και τα τεχνικά χαρακτηριστικά αξιόπιστων οργανισμών ή προσώπων.

Παράλληλα, η κεντρική και άμεση αντιμετώπιση τέτοιων φαινομένων κατά την χρονική στιγμή της εκδήλωσής τους, παρουσιάζει δυσχέρειες. Τα τεχνικά μέτρα που μπορούν να ληφθούν για τον περιορισμό ή την αποτροπή παρόμοιων επιθέσεων μπορούν να έχουν αυξημένη αποτελεσματικότητα, ωστόσο, αναπόφευκτα εφαρμόζονται «εκ των υστέρων», δηλαδή αφού το περιστατικό έχει ήδη εκδηλωθεί. Κατά το χρονικό αυτό διάστημα, ενδέχεται να έχει ήδη επηρεαστεί σημαντικός αριθμός χρηστών, γεγονός που καταδεικνύει τα όρια της αποκλειστικά τεχνικής προσέγγισης στην αντιμετώπιση των ηλεκτρονικών απατών αυτής της κατηγορίας.

Περαιτέρω, η απάτη μέσω «ηλεκτρονικού ψαρέματος» (phishing, μέσω ηλεκτρονικού ταχυδρομείου) ή "smishing" (μέσω μηνυμάτων κινητού τηλεφώνου) εντάσσεται στις επιθέσεις κοινωνικής μηχανικής (social engineering), δηλαδή επιθέσεις που εκμεταλλεύονται την ανθρώπινη συμπεριφορά και όχι απαραίτητα κάποια τεχνικά κενά ασφαλείας. Για τον λόγο αυτό, η συστηματική ευαισθητοποίηση και ενημέρωση των πολιτών καθίσταται κρίσιμος πυλώνας πρόληψης. Η ενίσχυση της γνώσης σχετικά με τις συνηθέστερες μορφές απάτης και τις τεχνικές κοινωνικής μηχανικής που χρησιμοποιούνται, επιτρέπει στον μέσο χρήστη να διενεργεί βασικούς ελέγχους πριν ανταποκριθεί σε αιτήματα που διατυπώνονται μέσω ηλεκτρονικής αλληλογραφίας, γραπτών μηνυμάτων ή άλλων καναλιών ψηφιακής επικοινωνίας. Στο πλαίσιο αυτό, η ΕΑΚ έχει ήδη αναλάβει σχετικές δράσεις ενημέρωσης και πρόληψης και υφίσταται ήδη προγραμματισμός οι σχετικές παρεμβάσεις της να ενισχυθούν περαιτέρω στο πλαίσιο της υλοποίησης της νέας Εθνικής Στρατηγικής Κυβερνοασφάλειας (ΕΣΚ) 2026-2030. Ειδικότερα, μέσω του Ειδικού Στόχου 1.Δ, προβλέπεται η διαμόρφωση και υλοποίηση ενός ενιαίου Εθνικού Σχεδίου Επικοινωνίας και Ευαισθητοποίησης για την κυβερνοασφάλεια, με στόχο την ενημέρωση πολιτών, επιχειρήσεων και δημόσιων φορέων σχετικά με τις απειλές και τις βέλτιστες πρακτικές ασφάλειας. Το σχέδιο θα περιλαμβάνει εκστρατείες ενημέρωσης, εκπαιδευτικό υλικό και συντονισμένες δράσεις με τα μέσα ενημέρωσης και τους αρμόδιους φορείς.

Επιπλέον, η ΕΑΚ αξιοποιεί συστηματικά τους διαθέσιμους διαύλους επικοινωνίας της, προκειμένου να ενημερώνει μέσω ανακοινώσεων της έγκαιρα το ευρύ κοινό για εκτενή περιστατικά απάτης στον κυβερνοχώρο, καθώς και για τους συναφείς κινδύνους. Η ταχεία και στοχευμένη δημοσιοποίηση σχετικών προειδοποιήσεων και παροχής συστάσεων προς τους πολίτες μέσω της ιστοσελίδας της Αρχής (https://cyber.gov.gr/antimetopisi-apeilon/systaseis-pros-polites/) δύναται να

συμβάλλει ουσιαστικά στον περιορισμό της έκτασης των επιπτώσεων και στην ανάπτυξη της ενημέρωσης και της ευαισθητοποίησης του ευρύτερου πληθυσμού σε θέματα κυβερνοασφάλειας.

Συνολικά, αν και η καταπολέμηση των απατών μέσω SMS και η προστασία προσωπικών δεδομένων, δεν αποτελούν κατεξοχήν αρμοδιότητες της ΕΑΚ, η ίδια μέσω της εκπλήρωσης του ρόλου της, ενισχύει συστηματικά το επίπεδο κυβερνοανθεκτικότητας της χώρας μέσω κανονιστικών παρεμβάσεων, εποπτικών μηχανισμών, έκδοσης οδηγιών, κατευθύνσεων ή και ανακοινώσεων, καθώς και στοχευμένης υποστήριξης των βασικών και σημαντικών οντοτήτων.

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