



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

**Προς: Υπουργείο Ψηφιακής
Διακυβέρνησης**
Υπηρεσία Συντονισμού
Γραφείο Νομικών και
Κοινοβουλευτικών Θεμάτων

Κοιν: Γραφείο Υπουργού Ψηφιακής
Διακυβέρνησης

Θέμα: Απάντηση σε ερώτηση κοινοβουλευτικού ελέγχου

Σχετ.: α. Το υπ' αρ. πρωτ. 5152 ΕΞ 2026/10.02.2026 έγγραφο της Υπηρεσίας Συντονισμού

β. Η υπ' αρ. 2926/6.2.2026 Ερώτηση της βουλευτού κ. Φ. Αραμπατζή, με θέμα: «Λήψη μέτρων για την αντιμετώπιση της απάτης, μέσω ηλεκτρονικών μηνυμάτων και ηλεκτρονικού ταχυδρομείου, υπό την καταχρηστική και παράνομη ιδιοποίηση των διακριτικών των ΕΛΤΑ»

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), σύμφωνα με τον ν. 5086/2024 (Α'23), είναι υπεύθυνη για τον συντονισμό και την εφαρμογή στρατηγικών κυβερνοασφάλειας σε εθνικό επίπεδο, εστιάζοντας στην πρόληψη, τον εντοπισμό, την αποκατάσταση και την ανάκαμψη από κυβερνοεπιθέσεις ιδίως σε βασικές και σημαντικές οντότητες που εντάσσονται στο πεδίο εφαρμογής του ν. 5160/2024 (Α' 195). Ο ρόλος της επεκτείνεται στη διαχείριση περιστατικών σε κρίσιμες υποδομές, δημόσιες και ιδιωτικές, όπως ορίζονται νομοθετικά, την κανονιστική συμμόρφωση, τον επιχειρησιακό σχεδιασμό και την ανάπτυξη τεχνικών δυνατοτήτων, όπως τη λειτουργία Ομάδας απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών.

Στη σύγχρονη ψηφιακή εποχή, η απάτη μέσω phishing (μέσω email, ηλεκτρονικών μηνυμάτων, τηλεφωνικών κλήσεων, ψεύτικων ιστοσελίδων που μιμούνται νόμιμους οργανισμούς) αποτελεί μία από τις πιο διαδεδομένες και εξελισσόμενες απειλές, με τα κακόβουλα email να μιμούνται πειστικά νόμιμες επικοινωνίες τραπεζών, gov.gr ή άλλων οργανισμών (π.χ. ΕΛΤΑ), προκαλώντας οικονομικές ζημιές και απώλεια προσωπικών δεδομένων στους πολίτες καθημερινά. 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 phishing 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 2026-2030.

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.

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

Ο Διοικητής της Εθνικής Αρχής Κυβερνοασφάλειας

Μιχαήλ Μπλέτσας

Εσωτερική διανομή:

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