

Ενημέρωση Α' Τάξης από την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος



[1]

Ο Οκτώβριος είναι παραδοσιακά αφιερωμένος στον **Ευρωπαϊκό Μήνα Κυβερνοασφάλειας (European Cybersecurity Month - ECSM)**, την ετήσια εκστρατεία της Ευρωπαϊκής Ένωσης που ξεκίνησε το 2012 και έχει στόχο την ευαισθητοποίηση των πολιτών και οργανισμών γύρω από ζητήματα ψηφιακής ασφάλειας. Η πρωτοβουλία διοργανώνεται από την **Ευρωπαϊκή Επιτροπή** και τον **Ευρωπαϊκό Οργανισμό για την Κυβερνοασφάλεια (ENISA)**, με την υποστήριξη κρατών-μελών και ιδιωτικών φορέων σε όλη την Ευρώπη.

Στόχος του είναι να προωθήσει τη σημασία της κυβερνοασφάλειας μέσω διάφορων σεμιναρίων, δράσεων και παρουσιάσεων.



[2]

Μέσα σε αυτό το κλίμα οι καθηγητές πληροφορικής του σχολείου μας, Γαϊτανίδης Δ., Δασκαλάκης Γ., Καλαϊτζίδου Δ., Κατσάρης Χ., διοργάνωσαν την ενημέρωση από την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδος. Η ενημέρωση πραγματοποιήθηκε την Τρίτη 21 Οκτωβρίου 2025 και την παρακολούθησαν μαθητές της Α'. Οι μαθητές μας ενημερώθηκαν για την

ασφαλή χρήση του διαδικτύου, τους κινδύνους που υπάρχουν, την προστασία του ψηφιακού τους αποτυπώματος, την προστασία του εαυτού τους από την επικίνδυνη έκθεσή τους στα κοινωνικά δίκτυα, τον διαδικτυακό εκφοβισμό, τα ποινικά αδικήματα στα οποία μπορούν να υποπέσουν οι θύτες, από την μη ορθή χρήση του διαδικτύου και το μη σεβασμό της προσωπικότητας και των ιδιαίτερων χαρακτηριστικών των συνομηλτών τους. Επιπλέον έγινε ιδιαίτερη αναφορά στις νέες απειλές που έχουν παρουσιασθεί με εργαλεία τεχνητής νοημοσύνης.



[3]

Η ενημέρωση ήταν εναρμονισμένη με το μήνυμα της εκστρατείας για τον **Ευρωπαϊκό Μήνα Κυβερνοασφάλειας 2025**. Το βασικό μήνυμα της φετινής εκστρατείας είναι «**Thinkbeforeyouclick**», δηλαδή «**Σκέψου πριν κάνεις κλικ**». Επικεντρώνεται στην ανάγκη να αντιμετωπιστεί η έλλειψη δεξιοτήτων στην κυβερνοασφάλεια και να ενισχυθεί η ευαισθητοποίηση μέσα από καινοτόμες στρατηγικές όπως η χρήση παιχνιδοποίησης (gamification), ώστε να γίνει η ασφάλεια στο διαδίκτυο μέρος της καθημερινής κουλτούρας για όλους.



[4]

Για το 2025, το επίκεντρο της καμπάνιας είναι το **phishing**, η πιο συνηθισμένη μέθοδος για την έναρξη κυβερνοεπιθέσεων. Σύμφωνα με τα στοιχεία της ENISA, περίπου **60% των περιστατικών κυβερνοεπιθέσεων ξεκινούν με phishing**, που μπορεί να λάβει πολλές μορφές:

- **Email phishing** - κλασικά παραπλανητικά μηνύματα.
- **Quishing** - χρήση QR codes για παγίδευση του χρήστη.
- **Smishing** - επιθέσεις μέσω SMS.
- **Vishing** - τηλεφωνικές απάτες με φωνητικές κλήσεις.
- **Spear phishing** - στοχευμένες επιθέσεις σε συγκεκριμένα άτομα.
- **Whaling** - επιθέσεις σε ηγετικά στελέχη.
- **BEC (Business Email Compromise)** - πλαστογράφηση εταιρικών email.
- **Deep fakes & AI-based scams** - απάτες που αξιοποιούν τεχνητή νοημοσύνη.

Ιδιαίτερα ανησυχητική είναι η νέα τάση του **“phishing-as-a-service”**, όπου εγκληματίες προσφέρουν έτοιμα «πακέτα» επιθέσεων με κλωνοποιημένες σελίδες γνωστών brands. Παράλληλα, η χρήση **μεγάλων γλωσσικών μοντέλων (LLMs)** έχει κάνει τα phishing emails πιο πειστικά· μάλιστα, μέχρι τις αρχές του 2025, **πάνω από το 80% των περιστατικών κοινωνικής μηχανικής παγκοσμίως** σχετίζονταν με καμπάνιες που βασίζονταν σε AI.



[5]



[6]

Η δράση αυτή αποτελεί μέρος της συνολικής προσπάθειας που γίνεται από τους καθηγητές πληροφορικής για την ορθή χρήση του διαδικτύου. Το διαδίκτυο έχει αλλάξει τη ζωή των ανθρώπων και προσφέρει πολλά χρήσιμα και διασκεδαστικά μέσα, αλλά ελλοχεύει και κινδύνους, που έχουν πάρει άλλη μορφή και διάσταση και με τα εργαλεία τεχνητής νοημοσύνης. Οι μαθητές μας χρειάζεται να αποκτήσουν γνώση και να καλλιεργήσουν κριτική ματιά για να χρησιμοποιούν το διαδίκτυο με ασφάλεια. Πρόθεση και επιθυμία μας να είμαστε δίπλα τους και να τους υπενθυμίζουμε **«Σκέψου πριν κάνεις κλικ»!**

by Despina on Τετ, 22/10/2025 - 22:59

Source

URL:

<http://2gymevosm.mysch.gr/drupal7/?q=el/content/%CE%B5%CE%BD%CE%B7%CE%BC%CE%AD%CF%81%CF%89%CF%83%CF%B7-%CE%B1%CF%84%CF%AC%CE%BE%CE%B7%CF%82-%CE%B1%CF%80%CF%8C-%CF%84%CE%B7%CE%BD-%CE%B4%CE%B9%CE%B5%CF%8D%CE%B8%CF%85%CE%BD%CF%83%CE%B7-%CE%B4%CE%AF%CF%89%CE%BE%CE%B7%CF%82-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CF%BF%CE%BD%CE%B9%CE%BA%CE%BF%CF%8D-%CE%B5%CE%B3%CE%BA%CE%BB%CE%AE%CE%BC%CE%B1%CF%84%CE%BF%CF%82>

Σύνδεσμοι

[1] https://drive.google.com/file/d/1tUvhY9a_hYMPsL_z3Oc5kNHu8pa4P5Dx/view?usp=sharing [2] <https://drive.google.com/file/d/1pc5aXwoThGz0SXu0dk0a47rC7J1DiE5m/view?usp=sharing> [3] https://drive.google.com/file/d/1ShxjQ_fOIHpD9GVRnRzhrY_dvtEjS2ej/view?usp=sharing [4] <https://drive.google.com/file/d/1ggDCGtTLjSnGXFT8EtZWMB4VKUNV3kgx/view?usp=sharing> [5] <https://drive.google.com/file/d/14bXFcP1zovAXEXe4PeryJ3H4M1SKfpAB/view?usp=sharing> [6] https://drive.google.com/file/d/1ZqihBuxP7bsa_PzGsAPz0zOvpCSzBrqA/view?usp=sharing