**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ**

ΥΠΟΥΡΓΕΙΟ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΠΟΛΙΤΗ

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

# Απολογισμός Δραστηριοτήτων Διεύθυνσης Δίωξης Κυβερνοεγκλήματος Έτους 2025

ΔΙΕΥΘΥΝΣΗ
ΔΙΩΞΗΣ
ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

ΠΡΟΛΗΨΗ · ΕΡΕΥΝΑ · ΚΑΤΑΣΤΟΛΗ

# Περιεχόμενα

## 1. Εισαγωγή

**Η διάρθρωση της Διεύθυνσης Δίωξης Κυβερνοεγκλήματος με έδρα την Αθήνα προβλέφθηκε με το Π.Δ. 178/2014 και εν συνεχεία με το Νόμο 5187/2025.** Η Διεύθυνση Δίωξης Κυβερνοεγκλήματος είναι αυτοτελής κεντρική Υπηρεσία και υπάγεται απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας.

Η αποστολή της Διεύθυνσης Δίωξης Κυβερνοεγκλήματος συμπεριλαμβάνει τόσο την καταστολή όσο και την πρόληψη γνήσιων κυβερνοεγκλημάτων και εγκλημάτων που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.

Η Υπηρεσία μας χειρίζεται υποθέσεις αναφορικά με κυβερνοεγκλήματα, δηλαδή εγκλημάτων που τελούνται με τη χρήση διαδικτύου, κυρίως από άγνωστους δράστες και η διερεύνηση τους απαιτεί εξειδικευμένες γνώσεις, ενώ παρέχει συνδρομή σε Αστυνομικά Τμήματα και Τμήματα Ασφαλείας ανά την Επικράτεια.

**Το κυβερνοέγκλημα αποτελεί ένα πολύπλοκο οικονομικό και κοινωνικό φαινόμενο** που επηρεάζει τις λειτουργίες του κράτους, της οικονομίας και της καθημερινής ζωής. Η ανάγκη για αποτελεσματική κυβερνοασφάλεια και η συνεργασία τόσο σε εθνικό όσο και σε παγκόσμιο επίπεδο αποτελεί πλέον πρωταρχική προτεραιότητα.

Η Διεύθυνση Δίωξης Κυβερνοεγκλήματος κατά το έτος 2025 ανέπτυξε πλήθος δράσεων, όπως αναλυτικά περιγράφονται στο παρόν, αφενός στον τομέα της δίωξης των εγκλημάτων που διαπράττονται μέσω Διαδικτύου ή με τη χρήση αυτού κι αφετέρου στον τομέα της πρόληψης και ενημέρωσης των πολιτών για ζητήματα ασφαλούς πλοήγησης στο Διαδίκτυο.

## 2. Συνεργασίες

Η Υπηρεσία μας για την εκπλήρωση της αποστολής της, συνεργάζεται με άλλες, καθ' ύλην και κατά τόπο, αρμόδιες κεντρικές και περιφερειακές Υπηρεσίες της ΕΛ.ΑΣ., με Ανεξάρτητες Διοικητικές Αρχές, Υπηρεσίες και φορείς της Χώρας, καθώς και με αντίστοιχες υπηρεσίες, οργανισμούς και φορείς Ευρωπαϊκών και μη Χωρών, σύμφωνα με τις ισχύουσες διατάξεις και τις σχετικές διεθνείς συμφωνίες και συμβάσεις. Εξάλλου, για την επιτυχή πρόληψη, διερεύνηση και εξιχνίαση

υποθέσεων κυβερνοεγκλημάτων απαιτείται, μεταξύ άλλων, τάχιστη, στενή και αποτελεσματική συνεργασία μεταξύ των αρμόδιων Υπηρεσιών κάθε Κράτους, με δεδομένο ότι το κυβερνοέγκλημα δεν δύναται να περιοριστεί στα εδαφικά όρια μιας χώρας.

### 2.1. Συνεργασίες σε ευρωπαϊκό και διεθνές επίπεδο

Επισημαίνεται ότι, λόγω της διεθνούς διάστασης του κυβερνοεγκλήματος, η διερεύνηση δεν περιορίζεται στα εδαφικά όρια της Χώρας μας. Πραγματοποιείται ανταλλαγή δεδομένων και πληροφοριών με άλλες Χώρες μέσω θεσμοθετημένων διαύλων επικοινωνίας (μέσω της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας), διεξάγονται κοινές δράσεις και έρευνες (π.χ. μέσω της δημιουργίας Κοινών Ομάδων Έρευνας, στο πλαίσιο Ευρωπαϊκών Εντολών Έρευνας κ.λπ.) και πραγματοποιείται, στο πλαίσιο διαφόρων διεθνών συναντήσεων, ανταλλαγή βέλτιστων πρακτικών.

### 2.2 Διεθνής παρουσία & Leader σε Επιχειρησιακά Σχέδια Δράσης EMPACT

Κατά το έτος 2025 στέλεχη της Υπηρεσίας μας συμμετείχαν σε διάφορα εκπαιδευτικά σεμινάρια του Οργανισμού της Ε.Ε. για την Κατάρτιση στον Τομέα Επιβολής του Νόμου (CEPOL), της EUROPOL και της INTERPOL, όσο και σε συναντήσεις, συνέδρια, συνδιασκέψεις και εργαστήρια που διοργανώθηκαν από ευρωπαϊκούς και διεθνείς οργανισμούς, στην Ελλάδα και στο εξωτερικό (ENISA, Συμβούλιο της Ευρώπης, κ.ά.).

Επισημαίνεται ότι σε επίπεδο Ευρωπαϊκής Ένωσης, η Υπηρεσία μας συμμετέχει ενεργά με εκπροσώπους της στην υλοποίηση των προτεραιοτήτων **Cyber Attacks, Online Fraud Schemes, Online Child Sexual Exploitation, καθώς και Intellectual Property Crime, counterfeiting of goods and currencies (IPCCGC) του European Multidisciplinary Platform against Criminal Threats (EMPACT)**.

Η Υπηρεσία μας συμμετείχε σε δράση του EMPACT με όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, για τον περιορισμό του φαινόμενου της διακίνησης υλικού σεξουαλικής κακοποίησης ανηλίκων στα P2P δίκτυα. Γι' αυτό το σκοπό, η χώρα μας συμμετείχε σε εκπαίδευση χρήσης του προγράμματος **I.C.A.C.C.O.P.S.** και

κλήθηκε να αναγνωρίσει τουλάχιστον δέκα (10) στόχους εντός της επικράτειάς της με τη χρήση του προγράμματος I.C.A.C.C.O.P.S..

### 2.3 Συμμετοχή σε διεθνείς επιχειρήσεις

Κατά το έτος 2025 η Υπηρεσία μας συμμετείχε σε πλήθος επιχειρησιακών δράσεων σε συνεργασία με άλλες χώρες όπως αναλυτικά περιγράφονται παρακάτω:

#### 2.3.1. Επιχείρηση «Stream»

Η εν λόγω επιχείρηση πραγματοποιήθηκε υπό την αιγίδα των Γερμανικών Αρχών (State Criminal Police of Bavaria) και τον συντονισμό της Europol. Οδήγησε στην απενεργοποίηση της ευρέως γνωστής διαδικτυακής πλατφόρμας με την ονομασία Kidflix (η οποία λειτουργούσε αποκλειστικά και μόνον στο Dark Web και η οποία παρείχε υπηρεσίες θέασης και πρόσβασης σε σκληρότατο οπτικοακουστικό υλικό σεξουαλικής κακοποίησης ανηλίκων), στην ταυτοποίηση και κατά περίπτωση σύλληψη πλήθους εμπλεκόμενων διαδικτυακών χρηστών, αλλά και στην αναγνώριση-διάσωση πλήθους εμπλεκόμενων θυμάτων. Σχετικό Δελτίο Τύπου: https://www.astynomia.gr/2025/04/03/03-04-2025-i-elliniki-astynomia-symmeteiche-se-diethniki-epicheirisi-gia-tin-apenergopoiisi-tis-diadiktyakis-platformas-kidflix-pou-pareiche-prosvasi-se-yliko-sexoualikis-kakopoiisis-anilikon/

#### 2.3.2. Επιχείρηση «Helix»,

Η εν λόγω επιχείρηση πραγματοποιήθηκε υπό την αιγίδα των Σουηδικών Αρχών και τον συντονισμό της Europol. Διενεργήθηκε εκτεταμένη διαδικτυακή έρευνα σχετικά με χρήστες οι οποίοι συμμετείχαν σε ομαδικές βιντεοκλήσεις, μέσω πλατφόρμων επικοινωνίας, κατά τη διάρκεια των οποίων προέβαιναν σε πράξεις αυτοϊκανοποίησης ενώ έβλεπαν από κοινού βίντεο ιδιαίτερα σκληρής σεξουαλικής κακοποίησης ανηλίκων, ακόμα και βρεφών.

### 2.3.3. Πανευρωπαϊκή επιχειρησιακή δράση με κωδική ονομασία «Fever»,

Στη δράση αυτή πραγματοποιήθηκε για την καταπολέμηση του φαινομένου της πορνογραφίας ανηλίκων μέσω διαδικτύου. Πραγματοποιήθηκε το δίμηνο Μάρτιο-Απρίλιο 2025, υπό την αιγίδα των πολωνικών Αρχών και το συντονισμό της Europol, συμμετείχαν Αρχές επιβολής του νόμου συνολικά -12- χωρών, μεταξύ των οποίων και η Ελλάδα. Στο πλαίσιο της εν λόγω δράσης, συνολικά ταυτοποιήθηκαν -166- άτομα, εκ των οποίων τα -111- συνελήφθησαν, καθώς -κατά περίπτωση- κατείχαν ή διακινούσαν οπτικοακουστικό υλικό παιδικής σεξουαλικής κακοποίησης, διαχειρίζονταν ιστοσελίδες που υπήρχε αναρτημένο όμοιο υλικό, ή, ακόμα, κακοποιούσαν σεξουαλικά ανήλικους. Στη χώρα μας, μετά από ενδελεχή και εμπεριστατωμένη έρευνα, ψηφιακή ανάλυση και αξιοποίηση πληροφοριών και δεδομένων, εντοπίστηκαν -4- διαδικτυακοί χρήστες οι οποίοι, κάνοντας χρήση συγκεκριμένων ηλεκτρονικών ιχνών, απέκτησαν πρόσβαση σε ιστότοπους και εφαρμογές και κατείχαν πλήθος αρχείων με υλικό σεξουαλικής κακοποίησης ανηλίκων, πρόσφορο προς διαμοιρασμό. Σχετικό Δελτίο Τύπου: https://www.astynomia.gr/2025/04/11/11-04-2025-i-elliniki-astynomia-symmeteiche-stin-panevropaiki-epicheirisi-fever-gia-tin-katapolemisi-tis-pornografias-anilikon/

### 2.3.4. Επιχείρηση Victim Identification Taskforce (VIDTF)

Αποτελεί διεθνή δράση συνεργασίας ειδικών για τον εντοπισμό και τη διάσωση παιδιών-θυμάτων σε υλικό σεξουαλικής κακοποίησης. Η δράση πραγματοποιήθηκε τον Μάιο και τον Σεπτέμβριο του 2025. Σχετικό Δελτίο Τύπου: https://www.europol.europa.eu/media-press/newsroom/news/three-children-safeguarded-following-vidtf-16

### 2.3.5. Επιχείρηση «Endgame»

Η δράση αυτή είχε ως αποτέλεσμα τη σύλληψη στη χώρα μας βασικού υπόπτου για τη δημιουργία και πώληση κακόβουλου λογισμικού τύπου RAT (Remote Access Trojan). Η επιχείρηση υλοποιήθηκε υπό το συντονισμό της Europol και της Eurojust, ενώ σε αυτή συμμετείχαν επίσης αστυνομικές και δικαστικές Αρχές της Αυστραλίας, του Βελγίου, του Καναδά, της Δανίας, της Γαλλίας, της

Γερμανίας, της Ελλάδας, της Λιθουανίας, των Κάτω Χωρών, του Ηνωμένου Βασιλείου και των Ηνωμένων Πολιτειών, με την υποστήριξη πάνω από 30 εθνικών και διεθνών δημόσιων και ιδιωτικών φορέων. Σκοπός ήταν ο τερματισμός της λειτουργίας υποδομών που ευθύνονται για τη μόλυνση χιλιάδων υπολογιστών με κακόβουλο λογισμικό. Στο πλαίσιο αυτό, η Διεύθυνση Δίωξης Κυβερνοεγκλήματος, μετά από κατάλληλη αξιοποίηση πληροφοριακών στοιχείων σε συνεργασία με αλλοδαπές Αρχές, προχώρησε στη συλλογή δεδομένων για την εν λόγω εγκληματική δραστηριότητα από χρήστη του διαδικτύου στην Ελλάδα. Σημειώνεται ότι, κατά τη Διεθνή Επιχείρηση «Operation Endgame», πραγματοποιήθηκαν ακόμη -10- έρευνες, από τις οποίες -9- στην Ολλανδία και -1- στη Γερμανία, διακόπηκε η πρόσβαση σε 1.025 εξυπηρετητές (servers) διεθνώς και κατασχέθηκαν -20- ιστοσελίδες (domains). Σχετικό Δελτίο Τύπου: https://www.astynomia.gr/2025/11/13/13-11-2025-i-elliniki-astynomia-stin-operation-endgame-gia-ton-termatismo-leitourgias-ypodomon-pou-diefkolynoun-to-kyvernoegklima/


**Εικόνα 1. Operation Endgame**


**Εικόνα 2. Κατασχεμένα κατόπιν έρευνας της ΔΙ.ΔΙ.Κ.**

### 2.3.6. Επιχείρηση «Talent»

Η δράση αυτή είχε ως στόχο τη διακοπή λειτουργίας δύο εκ των μεγαλύτερων διαδικτυακών πλατφορμών στον κόσμο, για το έγκλημα στον κυβερνοχώρο. Υλοποιήθηκε με την υποστήριξη και υπό το συντονισμό της Europol, το διάστημα από 28 έως 30 Ιανουαρίου 2025. Στην επιχείρηση συμμετείχαν Αρχές επιβολής του Νόμου από -8- Χώρες (Γερμανία, Ηνωμένες Πολιτείες της Αμερικής, Ελλάδα, Ισπανία, Γαλλία, Ρουμανία, Ιταλία και Αυστραλία), με κύριο στόχο τον εντοπισμό των διαχειριστών και των τεχνικών υποδομών των πλατφορμών, οι οποίες ήταν ενεργές για μεγάλο χρονικό διάστημα με πλήθος παράνομου περιεχομένου, ενώ παράλληλα προσφέρονταν προς πώληση σε αυτές, παράνομα αποκτηθέντα δεδομένα, κακόβουλο λογισμικό και υπηρεσίες φιλοξενίας διαφημίσεων ή άλλες υπηρεσίες. Σχετικό Δελτίο Τύπου: https://www.astynomia.gr/2025/01/30/30-1-2025-i-elliniki-astynomia-symmeteiche-se-diethnous-klimakas-astynomiki-epicheirisi-gia-ti-diakopi-leitourgias-dyo-ek-ton-megalyteron-diadiktyakon-platformon-ston-kosmo-gia-to-egklima-ston-kyvern/


**Εικόνα 3. Operation Talent**

### 2.3.7. Επιχειρησιακή δράση για την καταπολέμηση του φαινομένου της «ψηφιακής κλοπής δεδομένων» (Digital Skimming action).

Η Ελληνική Αστυνομία, μέσω της Διεύθυνσης Δίωξης Κυβερνοεγκλήματος, συντόνισε το 2025 ως επικεφαλής (Leader), από κοινού με την Europol (co-Leader), Η εν λόγω επιχειρησιακή δράση έλαβε χώρα κατά το χρονικό διάστημα από την 1η Νοεμβρίου 2025 έως 7η Νοεμβρίου 2025, με την υποστήριξη της EUROPOL και του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA). Στην επιχειρησιακή αυτή δράση συμμετείχαν Αστυνομικές Αρχές και Ομάδες Απόκρισης σε Συμβάντα Ασφάλειας Υπολογιστών (CSIRTs) σε παγκόσμιο επίπεδο. Συγκεκριμένα, συμμετείχαν:

α) Ιδιωτικός Τομέας: οι εταιρείες κυβερνοασφάλειας Group-IB και SANSEC.

β) Σχήματα Καρτών / Δίκτυα Καρτών Πληρωμών: Visa, Mastercard και American Express.

γ) Χώρες εκπροσωπούμενες από Αρχές Επιβολής του Νόμου (LEAs) ή/και CSIRTs: Βέλγιο (BE), Ισπανία (ES), Φινλανδία (FI), Γεωργία (GE), Ελλάδα (EL), Κροατία (HR), Κάτω Χώρες (NL), Πολωνία (PL), Πορτογαλία (PT), Ισλανδία (IS), Μολδαβία (MD) και Σλοβακία (SK).

Κύριος στόχος της επιχειρησιακής δράσης ήταν, μέσω συντονισμένων ενεργειών μεταξύ των Αρχών Επιβολής του Νόμου και των CSIRTs:

α) ο προσδιορισμός της έκτασης του φαινομένου, μέσω του εντοπισμού ιστοσελίδων που έφεραν κακόβουλο λογισμικό,

β) η ενίσχυση της συνεργασίας μεταξύ των LEAs και των CSIRTs, με τη βελτίωση της ανταλλαγής, ανάλυσης και διάδοσης πληροφοριών (criminal intelligence

sharing), με σκοπό την πρόβλεψη, πρόληψη και παρακολούθηση της εγκληματικής δραστηριότητας,

γ) η ενίσχυση της συνεργασίας μεταξύ αξιόπιστων εταιρειών του ιδιωτικού τομέα και των CSIRTs,

δ) η χαρτογράφηση βασικών υπόπτων, υποδομών και διαδικασιών διευκόλυνσης που διαδραματίζουν πρωταγωνιστικό ρόλο στο εξελισσόμενο επιχειρηματικό μοντέλο του Digital Skimming και

ε) η έναρξη κοινών επιχειρησιακών δραστηριοτήτων με σκοπό τη διακοπή της εγκληματικής δραστηριότητας, των παραγόντων απειλής πίσω από τις επιθέσεις, καθώς και της σχετικής εγκληματικής υποδομής.

Σε εθνικό επίπεδο, στο πλαίσιο ελέγχου διαδικτυακών καταστημάτων για πιθανή παρουσία κακόβουλου λογισμικού, πραγματοποιήθηκε επικοινωνία με 19 επιχειρήσεις των οποίων οι ιστοσελίδες παρουσίαζαν ενδείξεις μόλυνσης.

Από τα αποτελέσματα της δράσης αυτής προέκυψε ότι πάνω από τις μισές επιχειρήσεις που ανταποκρίθηκαν (54,5%) είχαν πραγματικό πρόβλημα ασφάλειας, γεγονός που επιβεβαιώνει τη σημασία της έγκαιρης επικοινωνίας και του τεχνικού ελέγχου. Η μη ανταπόκριση δεν επιτρέπει την εξαγωγή συμπερασμάτων και για τον λόγο αυτό εξαιρείται πλήρως από την αξιολόγηση ασφάλειας.

### 2.3.8. Παγκόσμια δράση για την καταπολέμηση της «επενδυτικής απάτης» (Investment fraud action)

Η επενδυτική απάτη είναι μια μορφή απάτης που βρίσκεται σε έξαρση από την περίοδο της εμφάνισης του Covid μέχρι και σήμερα. Η δράση πραγματοποιήθηκε στο πλαίσιο του “European Multidisciplinary Platform Against Criminal Threats” (EMPACT) κατά το χρονικό διάστημα από την 20η Οκτωβρίου 2025 έως και την 22η Οκτωβρίου 2025.

### 2.3.9. Διεθνής επιχειρησιακή δράση της INTERPOL με κωδική ονομασία “Nebula”.

Η δράση έχει ως στόχο την αντιμετώπιση των απατών ηλεκτρονικού ψαρέματος (phishing) σε παγκόσμιο επίπεδο. Στο πλαίσιο της εν λόγω επιχείρησης διερευνήθηκε, εντοπίστηκε και εξαρθρώθηκε πλατφόρμα phishing-as-a-service

(PhaaS) με την ονομασία Darcula, απενεργοποιήθηκαν διακομιστές που χρησιμοποιούνταν για παράνομες δραστηριότητες phishing και ελήφθησαν μέτρα για την αποτροπή περαιτέρω ζημιών σε βάρος των θυμάτων. Οι Επιχειρησιακές Εβδομάδες Δράσης πραγματοποιήθηκαν από τις 15 Οκτωβρίου 2025 έως και τις 15 Ιανουαρίου 2026 και κατά τη διάρκεια αυτών γνωστοποιήθηκαν προς επεξεργασία και αξιοποίηση στοιχεία πιθανών Ελλήνων θυμάτων. Στόχοι της επιχείρησης αποτέλεσαν i) ο προληπτικός εντοπισμός πιθανών θυμάτων και ii) ο περιορισμός οικονομικών απωλειών μέσω ενημέρωσης και υποστήριξης από τις αρμόδιες αρχές, η συλλογή και αξιοποίηση πληροφοριών για τον συντονισμό ενεργειών κατά των δραστών, η ενίσχυση της πολυεθνικής και πολυδικαιοδοτικής συνεργασίας των Αρχών Επιβολής του Νόμου, καθώς και η περαιτέρω εδραίωση της συνεργασίας μεταξύ της INTERPOL και των εθνικών αρχών, θέτοντας τις βάσεις για μελλοντικές κοινές επιχειρησιακές δράσεις και αναβάθμιση δεξιοτήτων.

### 2.3.10. Επιχειρησιακή δράση κατά του Phishing.

Η δράση αυτή ξεκίνησε εντός του 2025 σε συνεργασία με τις συναρμόδιες Αρχές της Ρουμανίας και της EUROPOL και αφορούσε παραβιάσεις λογαριασμών ηλεκτρονικής τραπεζικής με τη μέθοδο Phishing κατά το χρονικό διάστημα από 15 Ιουνίου 2021 έως και 14 Σεπτεμβρίου 2022. Οι παραβιάσεις πραγματοποιούνταν από ομάδα τουλάχιστον 80 ταυτοποιηθέντων δραστών ρουμανικής υπηκοότητας και διαμένοντες στη Ρουμανία, οι οποίοι έδρασαν με οργανωμένη δομή, με αποτέλεσμα την εξαπάτηση 537 Ελλήνων πολιτών – πελατών της Εθνικής Τράπεζας. Υπολογίζεται ότι το συνολικό παράνομο περιουσιακό όφελος που έχουν αποκομίσει οι δράστες ανέρχεται στα 534.000 Ευρώ. Κατόπιν αιτήματος των Αρχών της Ρουμανίας σχηματίστηκε από την Υπηρεσία μας αυτοτελής δικογραφία για παράβαση των άρθρων 187, 370Β, 386Α του Π.Κ. «Εγκληματική οργάνωση με σκοπό την τέλεση του κακουργήματος της απάτης με σκοπούμενο όφελος άνω των 120.000 Ευρώ, Παράνομη πρόσβαση σε πληροφοριακά συστήματα, Απάτη με υπολογιστή», καθώς και του Ν. 4557/2018 «Πρόληψη και καταπολέμηση της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες». Στο πλαίσιο αυτής πραγματοποιήθηκε αλληλογραφία με ημεδαπά τραπεζικά ιδρύματα για τη χορήγηση στοιχείων ταυτοποίησης Ελλήνων

θυμάτων για την περαιτέρω διερεύνηση της υπόθεσης. Η υπόθεση βρίσκεται σε εξέλιξη και για το έτος 2026.

## 3. Κέντρο Επιχειρήσεων και Γραμμή Επικοινωνίας Πολιτών "Cyber Alert"

Ιδιαίτερη μνεία πρέπει να γίνει στην επιτυχημένη λειτουργία του Κέντρου Διαχείρισης Διαδικτυακού Κινδύνου **"Cyber Alert",** το οποίο λειτουργεί σε **24ωρη βάση**, όπου εξειδικευμένοι αστυνομικοί της Υπηρεσίας διαχειρίζονται τις καταγγελίες των πολιτών. Οι εν λόγω πληροφορίες και καταγγελίες περιέρχονται στην Υπηρεσία μας μέσω του πενταψήφιου τηλεφωνικού αριθμού **11188**, μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου στη θυρίδα ccu@cybercrimeunit.gov.gr, μέσω της ηλεκτρονικής πλατφόρμας υποβολής καταγγελιών GOV.GR, όπου πολίτες, επιχειρήσεις και φορείς έχουν τη δυνατότητα να υποβάλουν καταγγελίες - αιτήσεις Κυβερνοεγκλήματος (e-crime) προς την Υπηρεσία μας. Σημειώνεται ότι με δωρεάν κλήση στο 11188 δίνεται η δυνατότητα στον καλούντα να συνομιλήσει απευθείας με εξειδικευμένο αστυνομικό της ΔΙ.ΔΙ.Κ. ή της Υ.ΔΙ.Κ.Β.Ε., ανάλογα με τη γεωγραφική του θέση με στόχο την άμεση εξυπηρέτηση και ενημέρωση των πολιτών.

**Από 01/01/2025 έως και τις 31/12/2025 στο τηλεφωνικό κέντρο της Υπηρεσίας μας εισήχθησαν 37.969 κλήσεις.**

Εξάλλου, το εν λόγω Κέντρο έχει οριστεί για τη Χώρα μας ως σημείο επαφής για την εκπλήρωση των σκοπών του άρθρου 35 της Σύμβασης του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο «Δίκτυο 24/7» (Ν. 4411/2016 (ΦΕΚ Α-142)) και του άρθρου 13 παράγραφος 1 της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις Επιθέσεις κατά Συστημάτων Πληροφοριών, υπό την εποπτεία Εισαγγελέα Εφετών.

## 4. Διωκτικό έργο

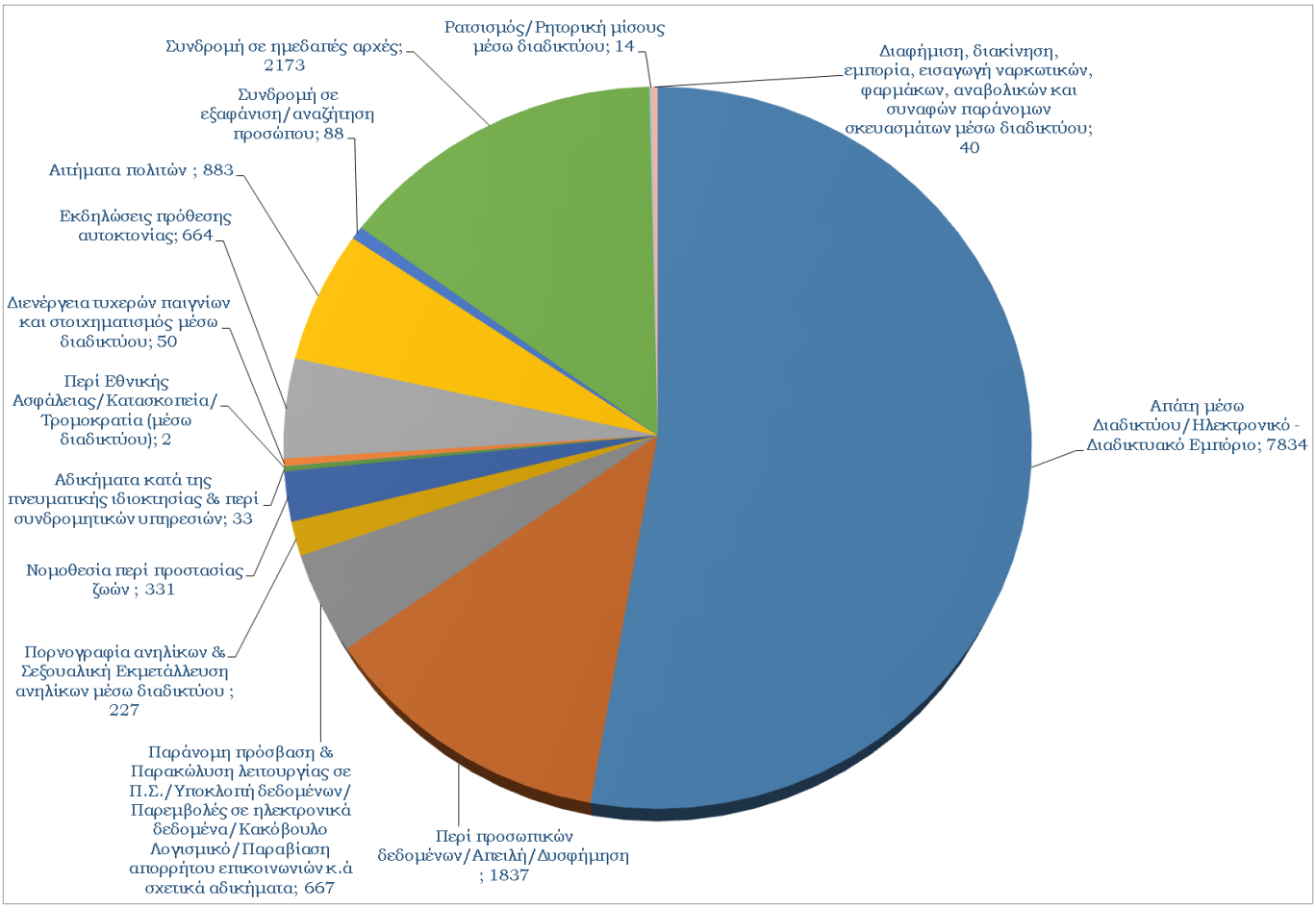
### 4.1 Σύνολο υποθέσεων

Ο συνολικός αριθμός νέων υποθέσεων που χειρίστηκε συνολικά η ΔΙ.ΔΙ.Κ. κατά το έτος 2025 ανήλθε σε **δέκα τέσσερις χιλιάδες οχτακόσια σαράντα εννιά (14.849)**, εκ των οποίων η ΔΙ.ΔΙ.Κ. χειρίστηκε **δέκα χιλιάδες εννιακόσια**

**ενενήντα δύο (10.992)** κι η Υ.ΔΙ.Κ.Β.Ε. **τρείς χιλιάδες οκτακόσια πενήντα επτά (3.857)**.

Στις ανωτέρω υποθέσεις περιλαμβάνονται οι καταγγελίες που δέχθηκε η ΔΙ.ΔΙ.Κ. και η Υ.ΔΙ.Κ.Β.Ε. μέσω ηλεκτρονικού ταχυδρομείου και της διαδικτυακής πύλης GOV.GR, οι οποίες ανήλθαν σε **έντεκα χιλιάδες εκατόν εξήντα οκτώ (11.168). Ειδικότερα, στον παρακάτω πίνακα αναγράφεται ο συνολικός αριθμός νέων υποθέσεων ανά κατηγορία/αδίκημα** (*Ο αριθμός αυτός αναφέρεται στα νέα πρωτόκολλα που εκδόθηκαν, είτε επρόκειτο για νέα εισαγγελική παραγγελία, είτε για προανακριτικό υλικό, εγκλήσεις πολιτών κ.λπ.*).

| ΚΑΤΗΓΟΡΙΑ | ΔΙ.ΔΙ.Κ. | Υ.ΔΙ.Κ.Β.Ε. | ΣΥΝΟΛΟ |
|---|---|---|---|
| Απάτη μέσω Διαδικτύου/Ηλεκτρονικό - Διαδικτυακό Εμπόριο | 5705 | 2129 | 7834 |
| Περί προσωπικών δεδομένων/Απειλή/Δυσφήμηση | 1294 | 543 | 1837 |
| Παράνομη πρόσβαση & Παρακώλυση λειτουργίας σε Π.Σ./Υποκλοπή δεδομένων/ Παρεμβολές σε ηλεκτρονικά δεδομένα/Κακόβουλο Λογισμικό/Παραβίαση απορρήτου επικοινωνιών κ.ά σχετικά αδικήματα | 529 | 138 | 667 |
| Πορνογραφία ανηλίκων & Σεξουαλική Εκμετάλλευση ανηλίκων μέσω διαδικτύου | 184 | 43 | 227 |
| Νομοθεσία περί προστασίας ζωών | 315 | 16 | 331 |
| Αδικήματα κατά της πνευματικής ιδιοκτησίας & περί συνδρομητικών υπηρεσιών | 27 | 6 | 33 |
| Περί Εθνικής Ασφάλειας/Κατασκοπεία/ Τρομοκρατία (μέσω διαδικτύου) | 8 | 0 | 2 |
| Διενέργεια τυχερών παιγνίων και στοιχηματισμός μέσω διαδικτύου | 49 | 1 | 50 |
| Εκδηλώσεις πρόθεσης αυτοκτονίας | 644 | 20 | 664 |
| Αιτήματα πολιτών | 816 | 67 | 883 |
| Συνδρομή σε εξαφάνιση/αναζήτηση προσώπου | 79 | 9 | 88 |
| Συνδρομή σε ημεδαπές αρχές | 1290 | 883 | 2173 |
| Ρατσισμός/Ρητορική μίσους μέσω διαδικτύου | 12 | 2 | 14 |
| Διαφήμιση, διακίνηση, εμπορία, εισαγωγή ναρκωτικών, φαρμάκων, αναβολικών και συναφών παράνομων σκευασμάτων μέσω διαδικτύου | 40 | 0 | 40 |




**Εικόνα 4. Νέες υποθέσεις που χειρίστηκε η ΔΙ.ΔΙ.Κ. κατά το έτος 2025**

## 4.2 Σύνολο Εισαγγελικών Παραγγελιών

Κατά το έτος 2025, διαβιβάσθηκαν προς εκτέλεση στην Διεύθυνση Δίωξης Κυβερνοεγκλήματος **δύο χιλιάδες τετρακόσιες ενενήντα επτά (2.497) Εισαγγελικές Παραγγελίες** για Προκαταρκτική Εξέταση ή Προανάκριση από όλες τις Εισαγγελίες Πρωτοδικών της Χώρας, εκ των οποίων οι **τριακόσιες πενήντα οχτώ (358)** διαβιβάστηκαν στην Υποδιεύθυνση Δίωξης Κυβερνοεγκλήματος Βορείου Ελλάδος.

Ειδικότερα, οι Εισαγγελικές Παραγγελίες που διαβιβάσθηκαν στη ΔΙ.ΔΙ.Κ. και την Υ.ΔΙ.Κ.Β.Ε. ανά μήνα:

| Εισαγγελικές Παραγγελίες | |
|---|---|
| **Μήνας** | **Πλήθος** |
| Ιανουάριος | 202 |
| Φεβρουάριος | 194 |
| Μάρτιος | 248 |
| Απρίλιος | 190 |
| Μάιος | 191 |
| Ιούνιος | 139 |
| Ιούλιος | 257 |
| Αύγουστος | 171 |
| Σεπτέμβριος | 289 |
| Οκτώβριος | 275 |
| Νοέμβριος | 156 |
| Δεκέμβριος | 185 |
| **ΣΥΝΟΛΟ** | **2497** |

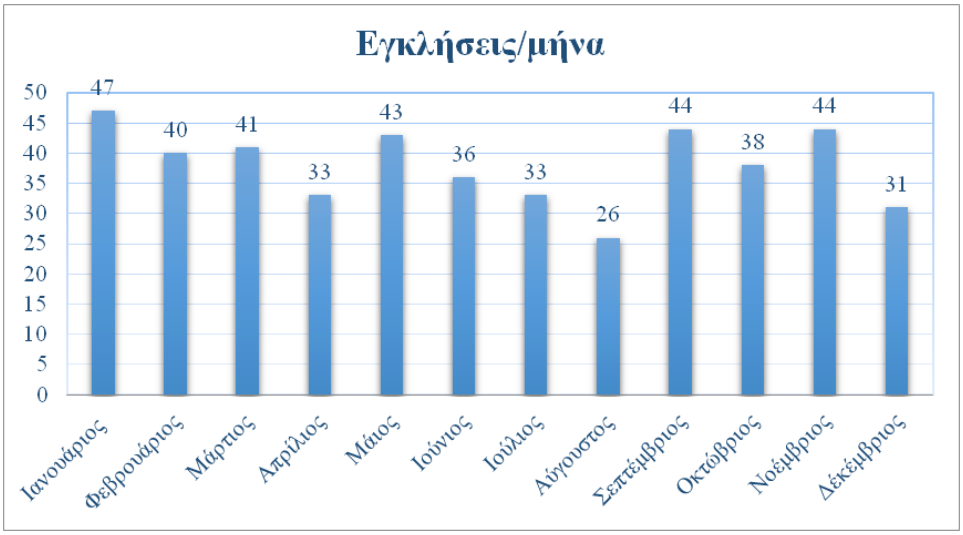

Στον παρακάτω πίνακα αναγράφονται τα συνηθέστερα αδικήματα για τα οποία εκδόθηκαν Εισαγγελικές Παραγγελίες στην ΔΙ.ΔΙ.Κ. και Υ.ΔΙ.Κ.Β.Ε.:

| ΚΑΤΗΓΟΡΙΑ | ΠΛΗΘΟΣ |
|---|---|
| Απάτη μέσω Διαδικτύου/Ηλεκτρονικό - Διαδικτυακό Εμπόριο | 892 |
| Περί προσωπικών δεδομένων/Απειλή/Δυσφήμηση | 693 |
| Παράνομη πρόσβαση & Παρακώλυση λειτουργίας Π.Σ./Υποκλοπή δεδομένων/Παραβίαση απορρήτου επικοινωνιών κ.ά. σχετικά αδικήματα/Περί Πνευματικής Ιδιοκτησίας | 204 |
| Πορνογραφία ανηλίκων & Σεξουαλική Εκμετάλλευση ανηλίκων μέσω Διαδικτύου | 144 |
| Νομοθεσία περί προστασίας ζώων | 49 |

### 4.3. Σύνολο εγκλήσεων

Ο συνολικός αριθμός νέων εγκλήσεων που χειρίστηκε συνολικά η ΔΙ.ΔΙ.Κ. κατά το έτος 2025 ανήλθε σε **τετρακόσιες πενήντα έξι (456).**

| Εγκλήσεις | |
|---|---|
| **Μήνας** | **Πλήθος** |
| Ιανουάριος | 47 |
| Φεβρουάριος | 40 |
| Μάρτιος | 41 |
| Απρίλιος | 33 |
| Μάιος | 43 |
| Ιούνιος | 36 |
| Ιούλιος | 33 |
| Αύγουστος | 26 |
| Σεπτέμβριος | 44 |
| Οκτώβριος | 38 |
| Νοέμβριος | 44 |
| Δεκέμβριος | 31 |
| **ΣΥΝΟΛΟ** | **456** |



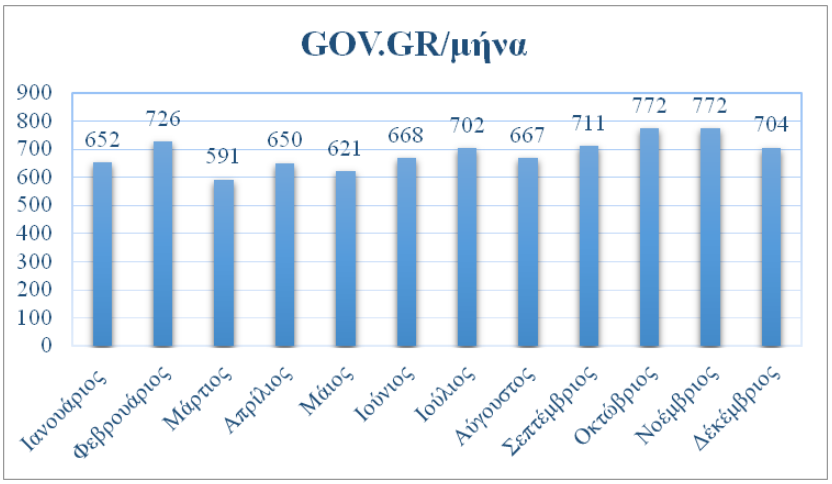

Στον παρακάτω πίνακα αναγράφονται τα συνηθέστερα αδικήματα για τα οποία υπεβλήθησαν εγκλήσεις στην ΔΙ.ΔΙ.Κ. και Υ.ΔΙ.Κ.Β.Ε.:

| ΚΑΤΗΓΟΡΙΑ | ΠΛΗΘΟΣ |
|---|---|
| Απάτη μέσω Διαδικτύου/Ηλεκτρονικό - Διαδικτυακό Εμπόριο | 243 |
| Περί προσωπικών δεδομένων/Απειλή/Δυσφήμηση | 148 |
| Παράνομη πρόσβαση & Παρακώλυση λειτουργίας Π.Σ./Υποκλοπή δεδομένων/Παραβίαση απορρήτου επικοινωνιών κ.ά. σχετικά αδικήματα/Περί Πνευματικής Ιδιοκτησίας | 42 |
| Πορνογραφία ανηλίκων & Σεξουαλική Εκμετάλλευση ανηλίκων μέσω Διαδικτύου | 19 |

### 4.4. Σύνολο καταγγελιών μέσω της διαδικτυακής πύλης GOV.GR

Ο συνολικός αριθμός καταγγελιών μέσω της διαδικτυακής πύλης GOV.GR που χειρίστηκε συνολικά η ΔΙ.ΔΙ.Κ. κατά το έτος 2025 ανήλθε σε **οκτώ χιλιάδες διακόσια τριάντα έξι (8.236).**

| GOV.GR | |
|---|---|
| **Μήνας** | **Πλήθος** |
| Ιανουάριος | 652 |
| Φεβρουάριος | 726 |
| Μάρτιος | 591 |
| Απρίλιος | 650 |
| Μάιος | 621 |
| Ιούνιος | 668 |
| Ιούλιος | 702 |
| Αύγουστος | 667 |
| Σεπτέμβριος | 711 |
| Οκτώβριος | 772 |
| Νοέμβριος | 772 |
| Δεκέμβριος | 704 |
| **ΣΥΝΟΛΟ** | **8236** |




Στον παρακάτω πίνακα αναγράφονται τα συνηθέστερα αδικήματα για τα οποία υπεβλήθησαν καταγγελίες μέσω της διαδικτυακής πύλης GOV.GR:

| ΚΑΤΗΓΟΡΙΑ | ΠΛΗΘΟΣ |
|---|---|
| Απάτη μέσω Διαδικτύου/Ηλεκτρονικό - Διαδικτυακό Εμπόριο | 6232 |
| Περί προσωπικών δεδομένων/Απειλή/Δυσφήμηση | 1102 |
| Παράνομη πρόσβαση & Παρακώλυση λειτουργίας Π.Σ./Υποκλοπή δεδομένων/Παραβίαση απορρήτου επικοινωνιών κ.ά. σχετικά αδικήματα/Περί Πνευματικής Ιδιοκτησίας | 524 |
| Πορνογραφία ανηλίκων & Σεξουαλική Εκμετάλλευση ανηλίκων μέσω Διαδικτύου | 24 |
| Διενέργεια τυχερών παιγνίων | 19 |

### 4.5. Σύνολο καταγγελιών μέσω ηλεκτρονικού ταχυδρομείου

Ο συνολικός αριθμός καταγγελιών μέσω ηλεκτρονικού ταχυδρομείου που χειρίστηκε συνολικά η ΔΙ.ΔΙ.Κ. κατά το έτος 2025 ανήλθε σε **δύο χιλιάδες εννιακόσια τριάντα δύο (2.932).**

| Καταγγελία με Ηλεκτρονικό Ταχυδρομείο | |
|---|---|
| **Μήνας** | **Πλήθος** |
| Ιανουάριος | 234 |
| Φεβρουάριος | 261 |
| Μάρτιος | 235 |
| Απρίλιος | 318 |
| Μάιος | 297 |
| Ιούνιος | 184 |
| Ιούλιος | 218 |
| Αύγουστος | 210 |
| Σεπτέμβριος | 277 |
| Οκτώβριος | 257 |
| Νοέμβριος | 241 |
| Δεκέμβριος | 200 |
| **ΣΥΝΟΛΟ** | **2932** |


Στον παρακάτω πίνακα αναγράφονται τα συνηθέστερα αδικήματα για τα οποία υπεβλήθησαν καταγγελίες μέσω ηλεκτρονικού ταχυδρομείου:

| ΚΑΤΗΓΟΡΙΑ | ΠΛΗΘΟΣ |
|---|---|
| Απάτη μέσω Διαδικτύου/Ηλεκτρονικό - Διαδικτυακό Εμπόριο | 1241 |
| Περί προσωπικών δεδομένων/Απειλή/Δυσφήμηση | 370 |
| Νομοθεσία περί προστασίας ζώων | 327 |
| Παράνομη πρόσβαση & Παρακώλυση λειτουργίας Π.Σ./Υποκλοπή δεδομένων/Παραβίαση απορρήτου επικοινωνιών κ.ά. σχετικά αδικήματα/Περί Πνευματικής Ιδιοκτησίας | 105 |
| Πορνογραφία ανηλίκων & Σεξουαλική Εκμετάλλευση ανηλίκων μέσω Διαδικτύου | 87 |
| Διενέργεια τυχερών παιγνίων | 27 |

### 4.6. Σύνολο αιτημάτων διεθνούς αστυνομικής συνεργασίας

Στο πλαίσιο της διεθνούς αστυνομικής συνεργασίας (Interpol, Europol, SIRENE), η ΔΙ.ΔΙ.Κ. και η Υ.ΔΙ.Κ.Β.Ε. διαχειρίστηκε **χίλια τριακόσια πενήντα επτά (1.357)** αιτήματα συνεργασίας.

Τα αιτήματα αφορούν περιπτώσεις διακρατικών αστυνομικών ερευνών, που είχαν ως αντικείμενο κακουργηματικού χαρακτήρα ηλεκτρονικά εγκλήματα και αφορούσαν σε συνδρομή σε εξαφάνιση/αναζήτηση προσώπου, αιτήματα ημεδαπών αρχών για αδικήματα που έχουν τελεσθεί στο διαδίκτυο, αιτήματα αλλοδαπών αρχών για αδικήματα που έχουν τελεσθεί στο διαδίκτυο (μέσω Europol-Interpol), αιτήματα για συνδρομή στην Europol' s European Union Internet Referral Unit (EUIRU), αιτήματα για συνδρομές σε δικαστικές-αστυνομικές αρχές για θέματα τρομοκρατίας.

### 4.7 Δεσμεύσεις χρηματικών ποσών ως προϊόντων εγκληματικής δραστηριότητας

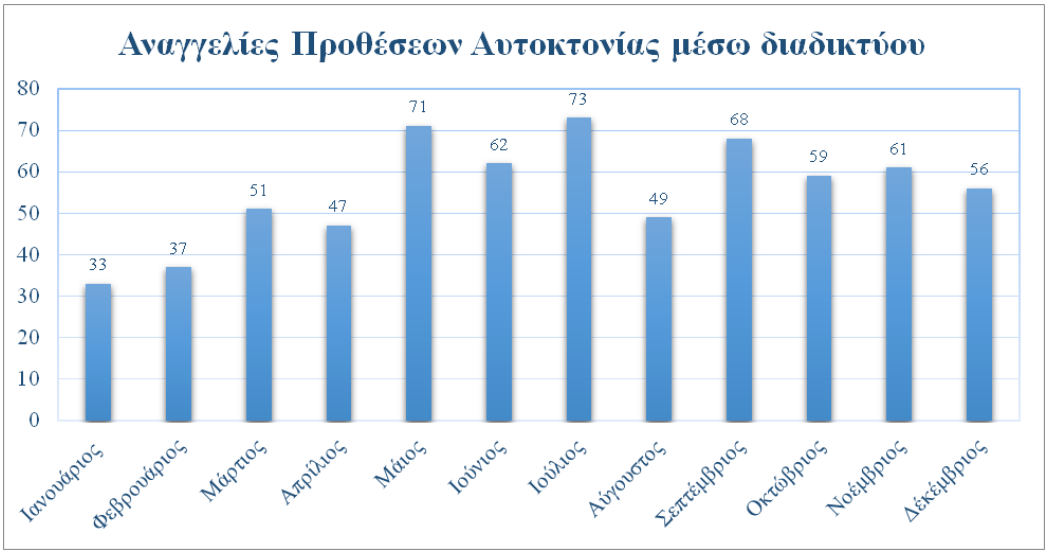
Η Διεύθυνση Δίωξης Κυβερνοεγκλήματος στο πλαίσιο διερεύνησης υποθέσεων απατών στον κυβερνοχώρο κατάφερε να δεσμεύσει εντός του 2025 σε συνεργασία με χρηματοπιστωτικά ιδρύματα και ψηφιακά ανταλλακτήρια της αλλοδαπής μέσω της Αρχής Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματική Δραστηριότητα, ως προϊόντα εγκληματικής δραστηριότητας, χρηματικά ποσά που ανέρχονται συνολικά περί τα €4.860.000 και 56.000 USDT (ισόποσα των 56.000 δολαρίων ΗΠΑ). Κατέστη δε εφικτό, ποσό €4.212.000 να επιστραφεί στους πραγματικούς δικαιούχους του και τα υπόλοιπα ποσά βρίσκονται σε διαδικασία επιστροφής.

### 4.8. Αναγγελία προθέσεων αυτοκτονίας μέσω Διαδικτύου

Από την Υπηρεσία μας, κατά το έτος 2025, διερευνήθηκαν **εξακόσια εξήντα επτά (667) περιπτώσεις πρόθεσης αυτοκτονίας που εκδηλώθηκαν μέσω Διαδικτύου, ενώ σε εκατόν εξήντα έξι (166) από αυτές καταγράφηκε η εμπλοκή ανήλικου, οι εκατόν είκοσι μία (121) περιπτώσεις εξετάσθηκαν από γιατρό και οι τριάντα τέσσερις (34) οδηγήθηκαν σε νοσηλεία.**

Το σύνολο των περιπτώσεων ανά μήνα αποτυπώνονται στο ακόλουθο διάγραμμα:

| Υποθέσεις πρόθεσης αυτοκτονίας που εκδηλώθηκαν μέσω Διαδικτύου | |
|---|---|
| **Μήνας** | **Πλήθος** |
| Ιανουάριος | 33 |
| Φεβρουάριος | 37 |
| Μάρτιος | 51 |
| Απρίλιος | 47 |
| Μάιος | 71 |
| Ιούνιος | 62 |
| Ιούλιος | 73 |
| Αύγουστος | 49 |
| Σεπτέμβριος | 68 |
| Οκτώβριος | 59 |
| Νοέμβριος | 61 |
| Δεκέμβριος | 56 |
| **ΣΥΝΟΛΟ** | **667** |




### 4.9. Έρευνες - Συλλήψεις – Απόδοση κατηγοριών

Από τη ΔΙ.ΔΙ.Κ. πραγματοποιήθηκαν **ογδόντα έξι (86)** κατ' οίκον έρευνες, ενώ συνελήφθησαν συνολικά **εκατόν είκοσι οχτώ (128)** άτομα στο πλαίσιο του αυτοφώρου για τα ακόλουθα αδικήματα:

| Αδίκημα | Κατ' οίκον έρευνες | Συλληφθέντες |
|---|---|---|
| Απάτη | 3 | 104 |
| Απειλή, εξύβριση, συκοφαντική δυσφήμηση | - | 1 |
| Διέγερση σε διάπραξη εγκλημάτων, βιαιοπραγίες ή διχόνοια | 5 | 3 |
| Πορνογραφία ανηλίκων | 61 | 9 |
| Εκδικητική πορνογραφία | 3 | 2 |
| Πνευματική Ιδιοκτησία | 9 | 4 |
| Παράνομη πρόσβαση (370Α, Β κ.λπ.) | 3 | 1 |
| Εκβίαση (απόπειρα) | 1 | 1 |
| Παραμέληση εποπτείας ανηλίκου | - | 2 |
| Συμμετοχή σε αυτοκτονία (απόπειρα) | - | 1 |
| Παράνομο εμπόριο κροτίδων/βεγγαλικών | 1 | - |
| ΣΥΝΟΛΟ | 86 | 128 |

Ειδικότερα, από τη Διεύθυνση Δίωξης Κυβερνοεγκλήματος πραγματοποιήθηκε αστυνομική επιχείρηση στην έδρα δύο (2) νομικών προσώπων, κατόπιν καταγγελίας για λειτουργία εντός αυτών τηλεφωνικών κέντρων (Call Centers) που διέπρατταν επενδυτικές απάτες. Στο πλαίσιο αυτής επιβεβαιώθηκαν τα καταγγελλόμενα, συνελήφθησαν εκατόν τέσσερα (104) άτομα - ημεδαποί και αλλοδαποί - και κατασχέθηκε πλήθος πειστηρίων (φηφιακά και έγχαρτα) προς περαιτέρω εξέταση, καθώς και χρηματικά ποσά, τα οποία παραδόθηκαν στο Ταμείο Παρακαταθηκών και Δανείων.

Γίνεται μνεία, ότι σε ορισμένους εκ των ανωτέρω συλληφθέντων αποδόθηκαν επιπλέον κατηγορίες (*λ.χ. σύσταση εγκληματικής οργάνωσης, εκβίαση, παραβίαση προσωπικών δεδομένων).*

## 5. Δράσεις Πρόληψης και Ενημέρωσης πολιτών

Το Αρχηγείο της Ελληνικής Αστυνομίας και η Διεύθυνση Δίωξης Κυβερνοεγκλήματος **έχουν αναπτύξει σύνολο καινοτόμων δράσεων**. Οι δράσεις αυτές όπως αναλυτικά περιγράφονται παρακάτω αποτελούν σημαντικούς πυλώνες στην πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, ενισχύοντας την εξωστρέφεια της Ελληνικής Αστυνομίας με στόχο τη διείσδυση στην κοινωνία και την οικογένεια.

Η Υπηρεσία μας εφαρμόζει ολοκληρωμένη επικοινωνιακή στρατηγική με στόχευση ανά κοινό, μέσο και θεματολογία. Οι τακτικές δράσεις περιλαμβάνουν:

- Θεματικές εβδομαδιαίες καμπάνιες (π.χ. απάτες στα μέσα κοινωνικής δικτύωσης, ηλεκτρονικό ψάρεμα, κοινωνική μηχανική κ.λπ.).
- Άμεση αξιοποίηση της επικαιρότητας για τη δημιουργία awareness content (π.χ. ψευδείς διαγωνισμοί, phishing μηνύματα).
- Μηνιαία θεματικά αφιερώματα (με έμφαση σε επίκαιρα ή εποχικά θέματα).
- Ημερίδες, ομιλίες και τηλεδιασκέψεις σε σχολεία, φορείς και επιχειρήσεις.
- Συμμετοχή σε παγκόσμιες ημέρες και θεματικές περιόδους όπως:
  - Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου
  - Cybersecurity Awareness Month
  - Ευρωπαϊκή Ημέρα Προστασίας Προσωπικών Δεδομένων
  - Ενημερωτικά σποτ & video reels με αφορμή πρόσφατες υποθέσεις

### 5.1 Ημερίδες Ασφαλούς Πλοήγησης

Το Αρχηγείο της Ελληνικής Αστυνομίας, μέσω της Διεύθυνσης Δίωξης Κυβερνοεγκλήματος, διοργανώνει ή συμμετέχει σε ημερίδες και διαλέξεις σε όλη την Ελληνική Επικράτεια, έχοντας ως στόχο την **ενημέρωση μαθητών, γονέων, εκπαιδευτικών, καταναλωτών, εμπόρων και επιχειρηματιών** για την πρόληψη και την αντιμετώπιση των κινδύνων που σχετίζονται με τις νέες τεχνολογίες, τις διαδικτυακές αγορές, τα φαινόμενα διαδικτυακής βίας, τους κινδύνους που ελλοχεύουν στις ιστοσελίδες κοινωνικής δικτύωσης, κ.ά..
Οι θεματολογίες αναπτύσσονται βασιζόμενες σε πραγματικές υποθέσεις που έχει χειριστεί η Υπηρεσία μας είναι οι ακόλουθες:

- φαινόμενο διαδικτυακού εξαναγκασμού και εκφοβισμού
- φαινόμενο διαδικτυακής παραπλάνησης μέσα από λογαριασμούς μέσων κοινωνικής δικτύωσης αλλά και διαδικτυακών παιχνιδιών
- ψεύτικοι διαδικτυακοί λογαριασμοί
- φαινόμενο προκλήσεων μέσω διαδικτύου
- φαινόμενο εκδικητικής πορνογραφίας και στοχοποίησης θυμάτων στον πραγματικό κόσμο
- εκφοβισμός μέσω διαδικτύου
- διαδικτυακά παιχνίδια και χρόνος παραμονής σε αυτά
- διαδικτυακές απάτες
- τεχνητή νοημοσύνη

Χαρακτηριστικά αναφέρεται ότι κατά το έτος 2025 διοργανώθηκαν **τετρακόσιες ενενήντα οχτώ (498) ενημερωτικές εκδηλώσεις και διαλέξεις δια ζώσης ή εξ αποστάσεως σε όλη την Ελλάδα και στο εξωτερικό, ενημερώνοντας περί τους 90.000 πολίτες,**, ικανοποιώντας αιτήματα από διάφορους φορείς (κρατικούς φορείς, *ΟΤΑ, συλλόγους Γονέων και Κηδεμόνων, σχολεία, δημόσιους και ιδιωτικούς φορείς, Πανεπιστημιακά ιδρύματα κ.λπ.*), γεγονός που καταδεικνύει τόσο το έντονο ενδιαφέρον των πολιτών για ενημέρωση σε θέματα διαδικτυακών κινδύνων, όσο και την εξωστρεφή δράση της Υπηρεσίας μας και του Αρχηγείου της Ελληνικής Αστυνομίας.

Ειδικότερα, πραγματοποιήθηκαν ενημερωτικές δράσεις σε όλη την Ελλάδα και αξίζει ιδιαίτερης αναφοράς σε αυτές που πραγματοποιήθηκαν στην Περιφέρεια Κρήτης και σε απομακρυσμένες περιοχές όπως στους Φούρνους, στην Πάτμο και στη Νίσυρο.

Επιπρόσθετα πραγματοποιήθηκαν κατόπιν πρόσκλησης εκπροσώπων του απόδημου ελληνισμού στην Νυρεμβέργη ενημερωτικές δράσεις σε μαθητές, γονείς, εκπαιδευτικούς της Νυρεμβέργης και του Μονάχου από στελέχη της Υπηρεσία μας.

Στις ανωτέρω ενημερωτικές εκδηλώσεις διαμοιράστηκαν χιλιάδες αντίτυπα του παραμυθιού με τίτλο «Ο Σίφης ο Ποντικός & το Διαδίκτυο» το οποίο συνέγραψε η κ. Κάρμεν Ρουγγέρη σε συνεργασία με την ΔΙ.ΔΙ.Κ., καθώς και αντίτυπα του βιβλίο δραστηριοτήτων για την ασφαλή πλοήγηση που δημιουργήθηκε σε συνεργασία με την εταιρεία "PLAYMOBIL HELLAS".

**Εικόνα 5. Ημερίδα ΔΙ.ΔΙ.Κ.**

### 5.2. «Ψηφιακή Ακαδημία»

Στο πλαίσιο των καινοτόμων δράσεων που αναπτύσσει η Υπηρεσία μας με στόχο την ευαισθητοποίηση του κοινού αναφορικά με επισφαλείς διαδικτυακές συμπεριφορές στον κυβερνοχώρο δημιουργήθηκε η «Ψηφιακή Ακαδημία» σε συνεργασία με το Θεσμοθετημένο Εργαστήριο ΑΕΤΜΑ Lab και του ΙΜΤ Msc του Τμήματος Πληροφορικής του Δημοκρίτειου Πανεπιστημίου Θράκης. Ειδικότερα, δημιουργήθηκαν δύο παιχνίδια για ανήλικους:

- ηλικίας 8-12 ετών: Ανάπτυξη παιχνιδιού απτών διεπαφών με ενσωμάτωση Επαυξημένης Πραγματικότητας (Augmented Reality). https://www.cyberkid.gov.gr/ar-game/


- ηλικίας 13-18 ετών: Ανάπτυξη παιχνιδιού εμβύθισης μέσω του Metaverse (με χρήση Εικονικής Πραγματικότητας - VR & WebGL ). https://www.cyberkid.gov.gr/vr-game/


Μέσα από τη χρήση αυτών των εφαρμογών τα οποία παρουσιάζονται με την μορφή παιχνιδιού, οι μαθητές δύναται να μεταφερθούν, να περιηγηθούν και να αλληλοεπιδράσουν σε τρισδιάστατους χώρους ή να συνδυάσουν την προβολή του φυσικού κόσμου του οποίου η πραγματικότητα είναι επαυξημένη, με ψηφιακές πληροφορίες (κείμενο, ήχους, video), λαμβάνοντας κατάλληλα ερεθίσματα σχετικά με τους κινδύνους στο διαδίκτυο και να ενημερωθούν παίζοντας.

Η «Ψηφιακή Ακαδημία» παρουσιάστηκε στο πλαίσιο της 87ης Διεθνούς Έκθεσης Θεσσαλονίκης, όπου μικροί και μεγάλοι είχαν την ευκαιρία να ζήσουν από κοντά αυτή την μοναδική εμπειρία Επιπρόσθετα **απέσπασε το Silver Award στο Education Leader Awards 2024**, ενώ βραβεύτηκε στο **EC3 Cyber Innovation Forum 2024**, όπου διακρίθηκαν καινοτόμες προτάσεις που έχουν αντίκτυπο στην πρόληψη και την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο, αξιοποιώντας τη χρήση νέων τεχνολογιών.

**Εικόνα 6. VR Game**

### 5.3 Καινοτόμος και εκπαιδευτικός προσομοιωτής κυβερνοεπιθέσεων με τίτλο “CYBERTRAP”

Σκοπός του “CYBERTRAP” είναι η ενίσχυση της ψηφιακής εγρήγορσης των “παικτών», μέσω μίας διαδραστικής εμπειρίας 10 δωματίων – 10 μορφών ψηφιακής απάτης και υποκλοπής προσωπικών δεδομένων, εμπνευσμένων από πραγματικά περιστατικά. Στο CYBERTRAP ο χρήστης θα καλείται να εντοπίσει τις παγίδες σε κάθε δωμάτιο, οι οποίες όμως βασίζονται σε πραγματικές υποθέσεις και τρόπους δράσης και να ξεκλειδώσει τον επόμενο γρίφο. Η καινοτομία αυτού του διαδικτυακού escape room είναι ότι ο χρήστης για να επιλύσει τον γρίφο ακούει διαλόγους που βασίζονται σε πραγματικές υποθέσεις και ρεαλιστικά σενάρια βασισμένα σε σύγχρονες απάτες ή βλέπει πραγματικά μηνύματα που έλαβαν οι χρήστες που εξαπατήθηκαν. **Το “CYBERTRAP” παρουσιάστηκε για πρώτη φορά στην 89η Διεθνή Έκθεση Θεσσαλονίκης.**


**Εικόνα 7. Προσομοιωτής CYBERTRAP**

### 5.4 Συνεργασία με το Ίδρυμα «Θεοτόκος»

Το Ίδρυμα Θεοτόκος είναι Πρότυπο Προνοιακό Κέντρο και από τη σύστασή του το 1963, προσφέρει υπηρεσίες πρόληψης, ολιστικής παρέμβασης και αποκατάστασης σε άτομα με Νοητικές Αναπτυξιακές Διαταραχές & Διαταραχές του Αυτιστικού Φάσματος, από την πρώιμη παιδική ηλικία έως την νεαρή ενήλικη ζωή. Στο πλαίσιο συνεργασίας με το Ίδρυμα, έχουν πραγματοποιηθεί ήδη ενημερωτικές ημερίδες για την ασφαλή χρήση του διαδικτύου σε ωφελούμενους και εκπαιδευτές του Ιδρύματος. Ενώ, μέσα από τη συνεργασία μας δημιουργήθηκε εκπαιδευτικό υλικό για εκπαιδευτές και γονείς ατόμων με Νοητικές Αναπτυξιακές Διαταραχές & Διαταραχές του Αυτιστικού Φάσματος προς ενημέρωση των πολιτών. **Σημειώνεται ότι η συνεργασία αυτή διακρίθηκε με το 2ο Βραβείο στο EPR (European Platform for Rehabilitation) – Study and Prize 2025. Η διάκριση αυτή είναι εξαιρετικά σημαντική, καθώς το αναφερόμενο έργο θα ενταχθεί στη μελέτη του EPR για την αυτόνομη διαβίωση, ενώ στη συνέχεια θα προωθηθεί στα αρμόδια ευρωπαϊκά όργανα για πιθανή ένταξή του στην Στρατηγική της Ευρωπαϊκής Ένωσης για την Αναπηρία.**


**Εικόνα 8. Εκπαιδευτικό υλικό για άτομα με Νοητικές Αναπτυξιακές Διαταραχές & Διαταραχές του Αυτιστικού Φάσματος**

### 5.5 Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης στο Διαδίκτυο

Η Διεύθυνση Δίωξης Κυβερνοεγκλήματος του Αρχηγείου της Ελληνικής Αστυνομίας, στο πλαίσιο της Παγκόσμιας Ημέρας Ασφαλούς Πλοήγησης στο Διαδίκτυο διοργανώνει παράλληλες δράσεις ενημέρωσης σε εκπαιδευτικές μονάδες και φορείς.

**Η Διεύθυνση Δίωξης Κυβερνοεγκλήματος του Αρχηγείου της Ελληνικής Αστυνομίας διοργάνωσε εβδομάδα εορταστικών εκδηλώσεων σε Αθήνα και Θεσσαλονίκη από τις 5 έως τις 11 Φεβρουαρίου 2025 με θέμα «Ένας κόσμος συνδεδεμένος - ένας κόσμος προστατευμένος»**

Στόχος ήταν η ενημέρωση μαθητών, γονέων, εκπαιδευτικών, ειδικών ψυχικής υγείας και επαγγελματιών για τις σύγχρονες τάσεις του Κυβερνοεγκλήματος που σχετίζονται με ανηλίκους και τις σύγχρονες μορφές απατών που πραγματοποιούνται στον κυβερνοχώρο.

Στην εβδομάδα αυτή ενημερώθηκαν περισσότεροι από 45.000 πολίτες. Ειδικότερα, την Τρίτη 11 Φεβρουαρίου 2025, στο αμφιθέατρο του Ιδρύματος Βασίλη και Ελίζας Γουλανδρή, πραγματοποιήθηκε ενημερωτική εκδήλωση σε συνδιοργάνωση με το Πανελλήνιο Σχολικό Δίκτυο. Παράλληλα, με απόλυτη επιτυχία και ευρεία συμμετοχή πραγματοποιήθηκαν οι διαδικτυακές εκδηλώσεις εορτασμού της Παγκόσμιας Ημέρας Ασφαλούς Πλοήγησης στο Διαδίκτυο 2025, που συνδιοργανώθηκαν από τη Διεύθυνση Δίωξης Κυβερνοεγκλήματος της Ελληνικής Αστυνομίας και το Πανελλήνιο Σχολικό Δίκτυο του Υπουργείου Παιδείας, Θρησκευμάτων και Αθλητισμού.

Παράλληλα, την Τρίτη 11 Φεβρουαρίου, στη Θεσσαλονίκη και συγκεκριμένα στο Αμφιθέατρο «Σταύρος Κουγιουμτζής» στο Δημαρχείο Πυλαίας-Χορτιάτη, πραγματοποιήθηκε, από την Υποδιεύθυνση Δίωξης Κυβερνοεγκλήματος Βορείου Ελλάδος, ενημερωτική εκδήλωση, με το κοινό να αποτελείται κυρίως από εκπαιδευτικούς της Δευτεροβάθμιας Εκπαίδευσης καθώς και εκπροσώπους της Περιφέρειας Κεντρικής Μακεδονίας, του Βιοτεχνικού Επιμελητηρίου και του Εμπορικού Επιμελητηρίου Θεσσαλονίκης.

https://www.astynomia.gr/2025/02/13/13-02-2025-enas-kosmos-syndedemenos-enas-kosmos-prostatevmenos-draseis-tis-diefthynsis-dioxis-ilektronikou-egklimatos-gia-tin-pagkosmia-imera-asfalous-ploigisis-sto-diadiktyo/

**Εικόνα 9. Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης στο Διαδίκτυο 2025**

### 5.6 Ενημερωτικοί ιστότοποι cyberkid.gr και cyberalert.gr

Κατά το έτος 2024 πραγματοποιήθηκε ανακατασκευή του ιστότοπου www.cyberalert.gr ενώ πραγματοποιήθηκε και ανανέωση του ιστότοπου www.cyberkid.gr. Στον ιστότοπο **www.cyberkid.gr** παρέχονται χρήσιμες πληροφορίες και συμβουλές σχετικά με το πως μπορεί να εκμεταλλευτεί **όλη η οικογένεια** αλλά και οι εκπαιδευτικοί τα θετικά των σύγχρονων τεχνολογιών που μας περιβάλλουν και φυσικά του διαδικτύου, ενώ στον ιστότοπο **www.cyberalert.gr** παρουσιάζεται η συστηματική και επιστημονική μελέτη των θεμάτων και προβλημάτων που προκύπτουν για το εμπόριο και τους καταναλωτές από τις ηλεκτρονικές συναλλαγές, με σκοπό την ενημέρωση επιχειρηματιών, εμπόρων και καταναλωτών για τους διαδικτυακούς κινδύνους και την ασφαλή χρήση του διαδικτύου στις.

Αναλυτικά στοιχεία σχετικά με τον αριθμό των χρηστών και των προβολών των ανωτέρω ιστοτόπων:

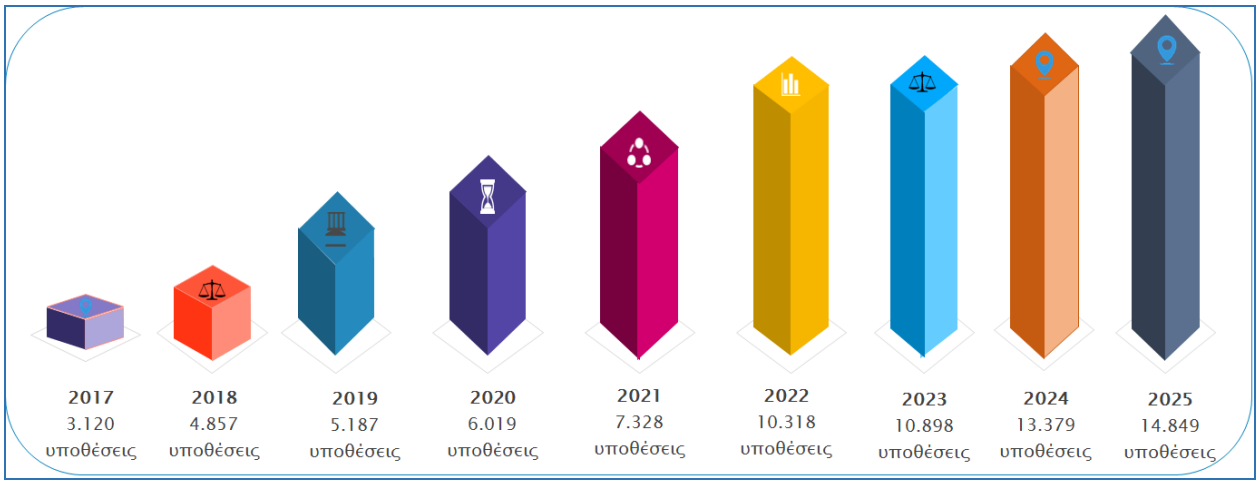
| | **www.cyberkid.gr** | **www.cyberalert.gr** |
|---|---|---|
| **Χρήστες που επισκέφτηκαν τον ιστότοπο (users)** | 27.180 | 149.947 |
| **Προβολές ιστοτόπου (page views)** | 249.112 | 216.026 |

### 5.7 Παρουσία ΔΙ.ΔΙ.Κ. στα Μέσα Κοινωνικής Δικτύωσης

**Η Διεύθυνση Δίωξης Κυβερνοεγκλήματος διαθέτει πιστοποιημένη παρουσία στα δημοφιλέστερα Μέσα Κοινωνικής Δικτύωσης** έχοντας δημιουργήσει πιστοποιημένους λογαριασμένους με στόχο την άμεση και σε πραγματικό χρόνο (real time) ενημέρωση των πολιτών για νέους κινδύνους αλλά και για τάσεις στον τομέα του κυβερνοεγκλήματος που ανακύπτουν καθημερινά στο διαδίκτυο. Αναλυτικότερα:

| | **Χρήστες που έχουν ήδη δηλώσει ότι τους «αρέσει» (like) και «ακολουθούν» τη δραστηριότητα** |
|---|---|
| **Cyberkid** στο **Facebook** | 16.360 |
| **Cyberalert** στο **Facebook** | 32.962 |
| **Cyberalert** στο **X (πρώην Twitter)** | 12.349 |
| **Cyberalert** στο **Instagram** | 24.937 |
| **Cyberalert** στο **Youtube** | 2.126 εγγεγραμμένοι χρήστες /36.263 προβολές |

# 6. Συμπεράσματα




**Κυρίαρχες τάσεις για το 2025**

Το 2025 η κυβερνοαπάτη εξελίχθηκε σε μία από τις σοβαρότερες ψηφιακές απειλές παγκοσμίως, με κύριο καταλύτη την **εκτεταμένη χρήση της τεχνητής νοημοσύνης από εγκληματικά δίκτυα**. Οι απατεώνες αξιοποίησαν **εργαλεία generative AI** για τη δημιουργία ιδιαίτερα πειστικών phishing μηνυμάτων, καθώς και deepfakes (φωνής και βίντεο), τα οποία χρησιμοποιήθηκαν για πλαστοπροσωπία γνωστών στο ευρύ κοινό προσώπων (πολιτικών, γιατρών, προσώπων του θεάματος), στελεχών επιχειρήσεων, τραπεζικών υπαλλήλων ή ακόμη και συγγενικών προσώπων. Η κοινωνική μηχανική ενισχύθηκε σημαντικά, με επιθέσεις που βασίζονται περισσότερο στην ψυχολογική χειραγώγηση παρά σε τεχνικά κενά ασφαλείας.

Παράλληλα, παρατηρήθηκε έντονη αύξηση απατών μέσω κοινωνικών δικτύων και εφαρμογών ανταλλαγής μηνυμάτων, όπου οι δράστες προσποιούνται αξιόπιστους οργανισμούς ή γνωστά brands. Οι επιθέσεις “takeover” λογαριασμών και η κατάχρηση-κλοπή ταυτότητας παρέμειναν βασικές μέθοδοι. Ιδιαίτερα αυξημένες ήταν και οι οικονομικές απάτες, με τα κρυπτονομίσματα να αποτελούν βασικό στόχο, οδηγώντας σε τεράστιες οικονομικές απώλειες μέσω ψεύτικων επενδυτικών σχημάτων και πλαστοπροσωπίας.

Παρότι η τεχνολογία εξελίχθηκε, οι παραδοσιακές μορφές απάτης δεν εξαφανίστηκαν, αλλά προσαρμόστηκαν. Η απάτη στην εφοδιαστική αλυσίδα, η κατάχρηση τρίτων συνεργατών συνέχισαν να εμφανίζονται όπου κρίνονταν αποτελεσματικές (Man-in-the-Middle). Για τις επιχειρήσεις, η κυβερνοαπάτη το 2025 αναδείχθηκε σε κορυφαίο στρατηγικό κίνδυνο, συχνά πιο ανησυχητικό ακόμη και από το ransomware, ενώ οι μικρότερες εταιρείες επηρεάστηκαν δυσανάλογα λόγω περιορισμένων πόρων ασφάλειας.

**Συνολικά, το 2025 κατέστη σαφές ότι η κυβερνοαπάτη δεν αποτελεί πλέον μεμονωμένο τεχνικό πρόβλημα, αλλά ένα διαρκώς εξελισσόμενο επιχειρηματικό και κοινωνικό φαινόμενο που απαιτεί συνδυασμό τεχνολογικών, οργανωτικών και εκπαιδευτικών μέτρων.**

Ειδικότερα:

1. Κυρίαρχη τάση για το 2025 στις απάτες με μέσο τέλεσης τα ηλεκτρονικά μέσα εν γένει και το διαδίκτυο ειδικότερα εξακολουθούν να συνιστούν οι **επενδυτικές απάτες** (investment scams) με χρήση **κρυπτονομισμάτων.** Οι δράστες προτρέπουν τα θύματα να δημιουργήσουν ψηφιακά πορτοφόλια και μέσω αυτών να πραγματοποιήσουν απατηλές συναλλαγές. Κοινός τόπος επίσης, είναι η χρήση άλλων κρυπτονομισμάτων (altercoins) πλην των Bitcoin (BTC), τα οποία βασίζονται σε αλυσίδες συστοιχιών (blockchains) που σε αρκετές περιπτώσεις δυσχεραίνουν το έργο των Αρχών Επιβολής του Νόμου, λόγω της με αργούς ρυθμούς τεχνολογικής εξέλιξης των σχετικών λογισμικών ανάλυσης συναλλαγών σε κρυπτονομίσματα σε σχέση με τους γοργούς ρυθμούς εμφάνισης νέων μορφών εγκληματικότητας. Σημειώνεται, ότι η εν λόγω τάση είναι διεθνής σύμφωνα την «Έκθεση Εκτίμησης Κινδύνου για το Οργανωμένο Έγκλημα» της Europol - Internet Organised Crime Threat Assessment (IOCTA).
2. Συχνό φαινόμενο συνιστούν και οι **παραβιάσεις ψηφιακών πορτοφολιών** με σκοπό την κλοπή κρυπτονομισμάτων και τη μεταφορά τους σε έτερα ίδιου νομίσματος είτε άλλου κατόπιν μετατροπής τους τόσο μέσω ανταλλακτηρίων κρυπτονομισμάτων όσο και μέσω αποκεντροποιημένων υπηρεσιών δωρεάν διατιθέμενων στο διαδίκτυο (Decentralized Swap Services) με πιο διαδεδομένες τις PancakeSwap, UniSwap, SushiSwap και Gemini.

3. Εντός του 2025 οι **ρομαντικές απάτες** (romance scams), ομοίως με προτροπή του θύματος από τους δράστες να επενδύσουν εν τέλει σε κρυπτονομίσματα (pig butchering), καθώς και οι **απάτες με τη μέθοδο του ενδιάμεσου** (Man-in-the-Middle scams) συνήθως κατόπιν παραβίασης των πληροφοριακών συστημάτων και ειδικότερα του ηλεκτρονικού ταχυδρομείου ενός νομικού προσώπου (Business Email Compromise-BEC) διαθέτουν μερίδιο στην πίτα των απατών και για το 2025. Η χρήση κρυπτονομισμάτων συναντάται περισσότερο στις ρομαντικές απάτες συγκριτικά με τις απάτες με τη μέθοδο του ενδιάμεσου.
4. Καταγράφηκαν αρκετά περιστατικά **τηλεφωνικών απατών με τη χρήση του spoofing**, ήτοι τηλεφωνικών απατών όπου για παράδειγμα οι δράστες καλούσαν τα θύματα προσποιούμενοι τους λογιστές τους και πείθοντάς τους ότι δήθεν εκκρεμεί στο ΑΦΜ τους επιστροφή φόρου ή ασφαλιστικής εισφοράς, τους έστελναν το IBAN του λογαριασμού τους για να πιστωθεί το ποσό της επιστροφής. Ακολούθως, οι δράστες δημιουργούσαν ένα διαδικτυακό περιβάλλον, το οποίο προσομοίαζε με το περιβάλλον της ηλεκτρονικής τραπεζικής της Τράπεζας συνεργασίας του υποψήφιου θύματος και του το έστελναν με υπερσύνδεσμο (Hyper Link) προκειμένου να εισέλθει δηλώνοντας τα διαπιστευτήρια εισόδου του και να αποδεχτεί την πίστωση. Με αυτό τον τρόπο οι δράστες αλίευαν τα διαπιστευτήρια εισόδου του υποψήφιου θύματος και αποκτούσαν πρόσβαση στο λογαριασμό ηλεκτρονικής τραπεζικής του προκειμένου να υφαρπάξουν οποιοδήποτε διαθέσιμο ποσό.
5. Επίσης καταγράφηκαν αρκετά περιστατικά απατών τύπου **Phishing ή Smishing** (SMS Phishing). Πιο δημοφιλής τρόπος δράσης (modus operandi) είναι αυτός, όπου οι δράστες προσποιούνταν νόμιμες οντότητες προκειμένου να υποκλέψουν προσωπικούς κωδικούς των υποψήφιων θυμάτων με σκοπό να υφαρπάξουν είτε χρήματα από τους τραπεζικούς τους λογαριασμούς είτε ψηφιακά νομίσματα από τα ψηφιακά τους πορτοφόλια. Οι νόμιμες οντότητες που χρησιμοποιούνται από τους δράστες ως επίφαση για να προσεγγίσουν τα θύματα δεν περιορίζονται στα χρηματοπιστωτικά ιδρύματα, αλλά χρησιμοποιούνται πλέον τα ονόματα ανταλλακτηρίων κρυπτονομισμάτων, ιστοτόπων αγοραπωλησιών προϊόντων, υπηρεσιών ροής δεδομένων (Streaming Services), υπηρεσιών ταχυμεταφοράς - Courier, όταν για παράδειγμα κάποιος

θέλει να πουλήσει κάτι μέσω online πλατφόρμας, οι δράστες τον προσεγγίζουν και τον πείθουν να αποστείλει το προϊόν μέσω υπηρεσιών ταχυμεταφοράς στέλνοντάς του ταυτόχρονα υπερσύνδεσμο αλίευσης που θα οδηγεί εν τέλει σε παραπλανητικό περιβάλλον ηλεκτρονικής τραπεζικής με σκοπό την αλίευση των προσωπικών του κωδικών.

6. Η ραγδαία εξέλιξη στον τομέα της τεχνητής νοημοσύνης οδήγησε εντός του 2025 τους εγκληματίες να αξιοποιήσουν τις νέες τεχνολογίες για να βελτιώσουν τις μεθόδους εξαπάτησης. Ένας σχετικός τρόπος δράσης είναι τα γνωστά **"Deepfake Scams"**, όπου οι δράστες κάνουν χρήση «deepfake» οπτικοακουστικού υλικού για πλαστογράφηση φωνών και προσώπων (συνήθως αναγνωρίσιμων στο ευρύ κοινό) με στόχο για παράδειγμα να πείσουν τα υποψήφια θύματα να προβούν σε δήθεν αποδοτικές επενδύσεις.

**Αναφορικά με τις κυβερνοεπιθέσεις:**

1. Κατά το έτος 2025 οι υποθέσεις που αφορούσαν κυβερνοεπιθέσεις **παρουσίασαν αυξημένη επιχειρησιακή σημασία**, με τις έρευνες να επικεντρώνονται κυρίως σε περιστατικά παράνομης πρόσβασης σε πληροφοριακά συστήματα, υποκλοπής δεδομένων και διάδοσης κακόβουλου λογισμικού. Σε σημαντικό αριθμό περιπτώσεων διαπιστώθηκε η αξιοποίηση υποδομών και υπηρεσιών εκτός της ελληνικής επικράτειας, γεγονός που ανέδειξε την ανάγκη στενής συνεργασίας με αλλοδαπές Αρχές και διεθνείς οργανισμούς για τη διερεύνηση και την αντιμετώπιση των σχετικών αδικημάτων.
2. Παράλληλα, τα αδικήματα **κατά της πνευματικής ιδιοκτησίας στον κυβερνοχώρο διερευνήθηκαν στο πλαίσιο στοχευμένων επιχειρησιακών ενεργειών**, τόσο σε εθνικό όσο και σε διεθνές επίπεδο. Σε ορισμένες από τις υποθέσεις αυτές, οι παράνομες διαδικτυακές πλατφόρμες που αποτέλεσαν αντικείμενο έρευνας δεν περιορίστηκαν αποκλειστικά στην παράνομη διάθεση ψηφιακού περιεχομένου, αλλά συνδέθηκαν και με ευρύτερες κυβερνοεγκληματικές δραστηριότητες, στοιχείο που επιβεβαιώνει τη σημασία της αντιμετώπισης των σχετικών αδικημάτων στο πλαίσιο της συνολικής ασφάλειας στον κυβερνοχώρο.

**Αναφορικά με την διαδικτυακή προστασία των ανηλίκων:**

1. Το 2025 καταγράφεται σαφής **αναβάθμιση της επιχειρησιακής ικανότητας προστασίας ανηλίκων**, ενώ ταυτόχρονα οι απειλές γίνονται πιο σύνθετες λόγω της ευρείας χρήσης γενετικής τεχνητής νοημοσύνης και deepfakes, που επιτρέπουν σε δράστες να παράγουν ή να αλλοιώνουν υλικό σεξουαλικής κακοποίησης και να προσεγγίζουν ανήλικους με ρεαλιστικές ψηφιακές ταυτότητες.
2. Σε σχέση με το 2024, όπου καταγράφηκε έντονη δραστηριοποίηση αλλά με κυρίαρχα πιο «παραδοσιακά» μοτίβα προσέγγισης, το 2025 παρατηρείται **μετατόπιση προς αυτοματοποιημένα οικοσυστήματα εξαπάτησης (phishing as a service, smishing, spoofing)** και ευρεία αξιοποίηση AI για κλιμάκωση του grooming και της σεξουαλικής εκβίασης (sextortion).
3. Την ίδια στιγμή, οι δείκτες υπόθεσης στοχευμένων εγκλημάτων σε βάρος ανηλίκων παραμένουν υψηλοί, με νέες δικογραφίες, εισαγγελικές παραγγελίες και διασυνοριακές συνεργασίες να αποτυπώνουν αυξημένη ροή πληροφοριών και ταχύτερη επιχειρησιακή απόκριση.
4. **Η διεθνής συνεργασία ενισχύθηκε καθοριστικά** για την απενεργοποίηση υποδομών διάχυσης υλικού κακοποίησης, την ταυτοποίηση θυμάτων και των συλλήψεων. Με την συμμετοχή σε επιχειρήσεις - δράσεις όπως οι Stream, Helix και Fever, Victim Identification Taskforce (VIDTF), επιβεβαιώνει ότι οι συντονισμένες ενέργειες μας με την Europol και την Interpol πολλαπλασιάζουν το αποτύπωμα προστασίας πέρα από τα εθνικά σύνορα. Σε αντιπαραβολή με το 2024, όπου οι συνεργασίες ήταν σημαντικές αλλά λιγότερο εκτεταμένες, το 2025 καταγράφεται ποσοτική και ποιοτική διεύρυνση των κοινών επιχειρήσεων και των μηχανισμών αναγνώρισης θυμάτων, στοιχείο που ανεβάζει τον πήχη της διακρατικής ανταπόκρισης.
5. Τεχνολογικά **ενισχύθηκε η ανίχνευση, ιεράρχηση και συσχέτιση υλικού CSAM, καθώς και ο εντοπισμός deepfake και ψευδών ταυτοτήτων.**

## 7. Αναδυόμενες Τάσεις

1. **Το 2026 η κυβερνοαπάτη αναμένεται να εξελιχθεί** σε μία ακόμη πιο διαδεδομένη και συστημική απειλή. Η κυβερνοαπάτη δεν αποτελεί πλέον μια περιφερειακή μορφή κυβερνοεγκλήματος, αλλά έναν από τους κυρίαρχους κινδύνους για επιχειρήσεις, οργανισμούς και ιδιώτες.
2. Καθοριστικό ρόλο σε αυτή την εξέλιξη θα διαδραματίσει η **τεχνητή νοημοσύνη**, η οποία θα επιτρέψει την πλήρη αυτοματοποίηση των επιθέσεων απάτης. Η εμφάνιση αυτόνομων συστημάτων τεχνητής νοημοσύνης, ικανών να σχεδιάζουν και να εκτελούν επιθέσεις χωρίς άμεση ανθρώπινη παρέμβαση, θα καταστήσει την απάτη πιο μαζική, προσαρμοστική και δύσκολα ανιχνεύσιμη. Παράλληλα, **η ευρεία χρήση συνθετικών φωνών, εικόνων και βίντεο** (Deepfakes), θα ενισχύσει την αξιοπιστία των επιθέσεων πλαστοπροσωπίας, ιδίως σε περιπτώσεις υψηλής οικονομικής αξίας, όπως η εξαπάτηση επιχειρηματικών στελεχών ή η εκμετάλλευση προσωπικών σχέσεων.
3. Ιδιαίτερη ανησυχία προκαλεί και **η ανάπτυξη συνθετικών ψηφιακών ταυτοτήτων**, οι οποίες δημιουργούνται με τη βοήθεια τεχνητής νοημοσύνης και μπορούν να παρακάμπτουν παραδοσιακούς ελέγχους ταυτοποίησης, κυρίως στον χρηματοπιστωτικό τομέα.
4. Ταυτόχρονα, **οι πλατφόρμες ηλεκτρονικού εμπορίου και τα συστήματα άμεσων πληρωμών** αναμένεται να αποτελέσουν **βασικούς στόχους** απατεώνων, καθώς οι συναλλαγές πραγματοποιούνται με μεγάλη ταχύτητα και συχνά χωρίς δυνατότητα αναστροφής, γεγονός που περιορίζει τον χρόνο αντίδρασης των θυμάτων και των οργανισμών.
5. Παράλληλα, η **κοινωνική μηχανική θα εξελιχθεί περαιτέρω**, συνδυάζοντας ανθρώπινη κρίση και τεχνητή νοημοσύνη, ώστε οι επιθέσεις να είναι βαθιά προσωποποιημένες και ψυχολογικά στοχευμένες.
6. Επιπλέον, η **κλοπή διαπιστευτηρίων, η παράκαμψη μηχανισμών πολυπαραγοντικής αυθεντικοποίησης και η πλαστογράφηση ταυτότητας** θα αποτελέσουν βασικά εργαλεία των απατεώνων.
7. Το τοπίο των κυβερνοεπιθέσεων στην Ελλάδα για το επόμενο έτος διαμορφώνεται από μια κρίσιμη μετάβαση, καθώς όλες οι Αρχές Επιβολής του Νόμου καλούνται να αντιμετωπίσουν την ωρίμανση του «εγκλήματος ως υπηρεσία» **(Cybercrime-as-a-Service)** σε ένα περιβάλλον έντονης γεωπολιτικής

πίεσης. Σύμφωνα με την Εθνική Αρχή Κυβερνοασφάλειας, η εφαρμογή της νέας στρατηγικής 2026-2030 σηματοδοτεί τη μετατροπή των ελεγκτικών μηχανισμών από απλούς παρατηρητές σε ενεργούς επιχειρησιακούς κόμβους, με κύριο στόχο την προστασία των κρίσιμων υποδομών.

8. Η μεγαλύτερη πρόκληση για τις Αρχές θα είναι η αντιμετώπιση επιθέσεων που ενισχύονται από την Τεχνητή Νοημοσύνη, **καθώς τα εργαλεία Agentic AI επιτρέπουν στους δράστες να αυτοματοποιούν σύνθετες παραβιάσεις και να εκτελούν εκστρατείες κοινωνικής μηχανικής με τρομακτική ακρίβεια.** Ιδιαίτερη έμφαση δίνεται στη θωράκιση του δημόσιου τομέα μετά τις πρόσφατες αυξήσεις σε περιστατικά ransomware. Η πλήρης ενσωμάτωση της οδηγίας NIS 2 παρέχει πλέον το νομικό οπλοστάσιο για αυστηρότερη λογοδοσία και υποχρεωτική αναφορά περιστατικών.
9. Τα ζητήματα πνευματικής ιδιοκτησίας στο διαδίκτυο μετατοπίζονται από την **παραδοσιακή καταστολή της πειρατείας περιεχομένου στην αντιμετώπιση σύνθετων δικτύων που εκμεταλλεύονται την Τεχνητή Νοημοσύνη** και τις τεχνολογίες ανωνυμοποίησης.
10. Στόχος θα είναι η στη δίωξη οργανωμένων ομάδων που χρησιμοποιούν παράνομες πλατφόρμες streaming και "πειρατικά" λογισμικά ως δούρειους ίππους για την εγκατάσταση κακόβουλου λογισμικού (malware), συνδέοντας άμεσα την προστασία των δικαιωμάτων δημιουργού με την ευρύτερη κυβερνοασφάλεια των πολιτών. Παράλληλα, **η ανάδυση του Generative AI δημιουργεί ένα νέο πεδίο δράσης για τις Αρχές,** καθώς καλούνται να διαχειριστούν υποθέσεις όπου η πνευματική ιδιοκτησία παραβιάζεται κατά την εκπαίδευση μοντέλων τεχνητής νοημοσύνης ή μέσω της δημιουργίας εξελιγμένων deepfakes. Η πρόκληση για την Ελληνική Αστυνομία έγκειται στην ιχνηλάτηση εσόδων από τέτοιες δραστηριότητες, τα οποία συχνά ξεπλένονται μέσω κρυπτονομισμάτων, καθιστώντας απαραίτητη τη διεθνή συνεργασία μέσω της Europol για την εξάρθρωση των οικονομικών υποδομών των παραβατών.
11. Η αυστηροποίηση του πλαισίου εντός του 2026 αναμένεται να επικεντρωθεί στη **διαφάνεια των αλγορίθμων και στην προστασία των δημιουργών** από την ανεξέλεγκτη ψηφιακή αναπαραγωγή, με τις Αρχές να αναλαμβάνουν ρόλο εγγυητή της νομιμότητας σε μια ολοένα και πιο αυτοματοποιημένη αγορά.

Τέλος, στο πλαίσιο του EMPACT η Ελληνική Αστυνομία μέσω της Διεύθυνσης Δίωξης Κυβερνοεγκλήματος θα συμμετέχει στη δράση για την καταπολέμηση του φαινομένου **“SMS Blaster”,** που συνιστά επίσης διαφαινόμενη τάση για το 2026. Συγκεκριμένα, **η επίθεση SMS Blaster συνιστά μια εξειδικευμένη μορφή κακόβουλης δραστηριότητας στον χώρο των κινητών επικοινωνιών, κατά την οποία οι επιτιθέμενοι αξιοποιούν τεχνολογίες λογισμικού-καθοριζόμενης ραδιοσυχνότητας (Software-Defined Radio – SDR) και ψευδείς σταθμούς βάσης κινητής τηλεφωνίας (fake base stations / IMSI catchers).** Στόχος της επίθεσης είναι η παραπλάνηση των κινητών συσκευών, η υποκλοπή αναγνωριστικών δεδομένων και η αποστολή παραπλανητικών μηνυμάτων SMS. Η λειτουργία της επίθεσης βασίζεται στην εκμετάλλευση εγγενών αδυναμιών του πρωτοκόλλου 2G (GSM), το οποίο, παρά τον παρωχημένο χαρακτήρα του, εξακολουθεί να υποστηρίζεται από μεγάλο αριθμό σύγχρονων συσκευών για λόγους οπισθοσυμβατότητας. Η επίθεση εξελίσσεται συνήθως στα ακόλουθα στάδια:

1. **Δημιουργία ψευδών σταθμών βάσης**: Ο επιτιθέμενος εγκαθιστά δύο ψευδείς σταθμούς βάσης. Ο πρώτος προσομοιώνει νόμιμο δίκτυο 4G/LTE, με σκοπό να προσελκύσει τη συσκευή-στόχο, ενώ ο δεύτερος λειτουργεί ως δίκτυο 2G, μέσω του οποίου πραγματοποιείται η κακόβουλη δραστηριότητα.
2. **Εξαναγκασμός υποβάθμισης σύνδεσης (downgrade attack)**: Η κινητή συσκευή εξαναγκάζεται να υποβαθμίσει τη σύνδεσή της από 4G σε 2G, μέσω τεχνικών όπως το RRC Redirection ή το Cell Reselection, εκμεταλλευόμενη το ισχυρότερο σήμα που εκπέμπει ο ψευδής σταθμός βάσης.
3. **Απόκτηση αναγνωριστικών συσκευής**: Μετά τη σύνδεση στο δίκτυο 2G, ο επιτιθέμενος αποκτά πρόσβαση σε κρίσιμα αναγνωριστικά της συσκευής, όπως το IMSI (International Mobile Subscriber Identity) και το IMEI (International Mobile Equipment Identity), χωρίς να απαιτείται διαδικασία αμοιβαίας αυθεντικοποίησης, λόγω των ελλείψεων ασφαλείας του πρωτοκόλλου GSM.
4. **Αποστολή παραπλανητικών SMS (Smishing)**: Μέσω της ψευδούς βάσης, αποστέλλονται SMS με πλαστογραφημένη ταυτότητα αποστολέα (SMS spoofing), τα οποία εμφανίζονται ως προερχόμενα από επίσημους φορείς, δημόσιες υπηρεσίες ή τραπεζικά ιδρύματα και περιέχουν συνδέσμους phishing ή άλλο κακόβουλο περιεχόμενο.

5. **Επανασύνδεση στο νόμιμο δίκτυο**: Μετά την ολοκλήρωση της επίθεσης, η συσκευή επανασυνδέεται στο νόμιμο δίκτυο κινητής τηλεφωνίας, χωρίς εμφανή ίχνη της κακόβουλης παρέμβασης, γεγονός που καθιστά τον εντοπισμό και τη διερεύνηση της επίθεσης ιδιαίτερα δυσχερή.