Κυβερνοέγκλημα
Τρέχουσες απειλές, τάσεις και προκλήσεις στην Ελλάδα

Βασίλειος Ε. Παπακώστας
Αστυνομικός Διευθυντής
Διευθυντής Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος/Α.Ε.Α.

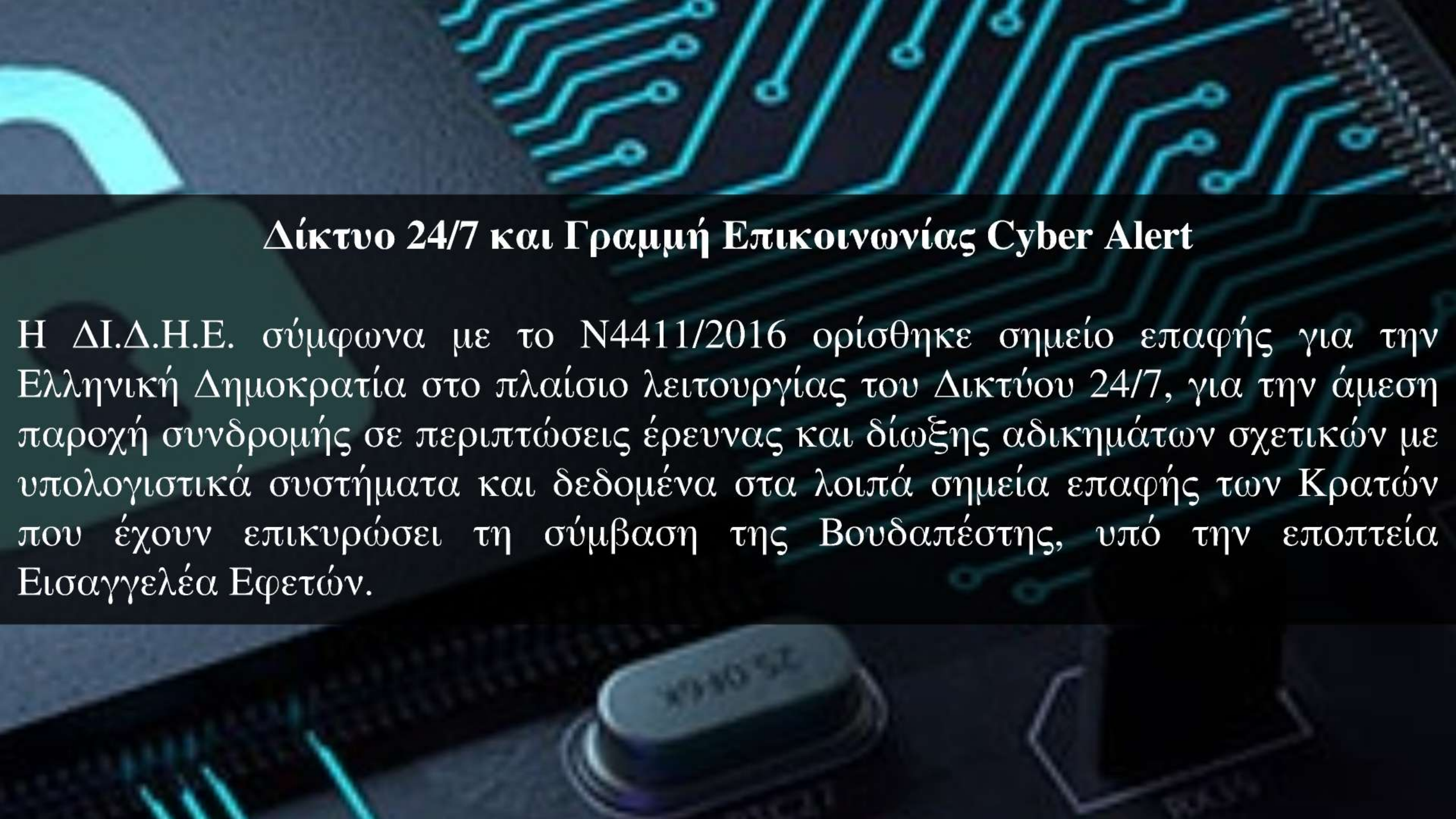
CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

14/03/2015: Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

01/09/2015: Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδος

- **Τμήμα Διοικητικής Υποστήριξης & Διαχείρισης Πληροφοριών**
- **Τμήμα Καινοτόμων Δράσεων και Στρατηγικής**
- **Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών & Προστασίας Λογισμικού & Πνευματικών Δικαιωμάτων**
- **Τμήμα Διαδικτυακής Προστασίας Ανηλίκων & Ψηφιακής Διερεύνησης**
- **Τμήμα Ειδικών Υποθέσεων & Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων**

❗ Πανελλαδικά:Περιφερειακοί Αστυνομικοί Σύνδεσμοι



Δίκτυο 24/7 και Γραμμή Επικοινωνίας Cyber Alert

Η ΔΙ.Δ.Η.Ε. σύμφωνα με το Ν4411/2016 ορίσθηκε σημείο επαφής για την Ελληνική Δημοκρατία στο πλαίσιο λειτουργίας του Δικτύου 24/7, για την άμεση παροχή συνδρομής σε περιπτώσεις έρευνας και δίωξης αδικημάτων σχετικών με υπολογιστικά συστήματα και δεδομένα στα λοιπά σημεία επαφής των Κρατών που έχουν επικυρώσει τη σύμβαση της Βουδαπέστης, υπό την εποπτεία Εισαγγελέα Εφετών.

Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο

- Το έγκλημα στον κυβερνοχώρο είναι γρήγορο και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- Μπορεί να διαπραχθεί χωρίς την μετακίνηση του δράστη.
- Είναι έγκλημα «χωρίς πατρίδα» και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.
- Τα ίχνη που αφήνει είναι ψηφιακά.
- Για την τέλεσή του απαιτούνται εξειδικευμένες γνώσεις.
- Είναι εύκολο στην διάπραξή του, για όσους είτε γνωρίζουν σχετικά είτε τους παρέχεται ως υπηρεσία (Crime as a Service).
- Δίνει τη δυνατότητα ομαδικής επικοινωνίας, συντονισμού και οργάνωσης, σε άτομα με ίδια εγκληματολογικά ενδιαφέροντα.
- Η αστυνομική διερεύνησή του απαιτεί εξειδικευμένες γνώσεις.

Δυσχέρειες στην διερεύνηση και την διαλεύκανση Κυβερνοεγκλήματος:

- **Διασυνοριακός – Διεθνοποιημένος χαρακτήρας του Κυβερνοεγκλήματος**
- **Εμπλοκή περισσοτέρων από μια Χώρων για την χορήγηση ηλεκτρονικών ιχνών**
- **Δυσκολίες ανίχνευσης – απόδειξης**
- **Για την χορήγηση ηλ. στοιχείων συχνά ζητείται επίσημο αίτημα δικαστικής συνδρομής**

Στη φετινή έκθεση, ο αντίκτυπος της πανδημίας COVID-19 παραμένει ορατός. Η επιταχυνόμενη ψηφιοποίηση που σχετίζεται με την πανδημία έχει επηρεάσει σημαντικά την ανάπτυξη μιας σειράς απειλών στον κυβερνοχώρο, όπως:

- Τα προγράμματα τύπου ransomware επιτρέπουν σε μια μεγαλύτερη ομάδα εγκληματιών να επιτίθενται σε μεγάλες εταιρείες και δημόσιους οργανισμούς απειλώντας τους με πολυεπίπεδες μεθόδους εκβιασμού, όπως επιθέσεις DDoS.

- Το κακόβουλο λογισμικό για κινητά εξελίσσεται με τους εγκληματίες να προσπαθούν να παρακάμψουν πρόσθετα μέτρα ασφαλείας, όπως ο έλεγχος ταυτότητας δύο παραγόντων.

- Οι ηλεκτρονικές αγορές έχουν οδηγήσει σε απότομη αύξηση της διαδικτυακής απάτης.

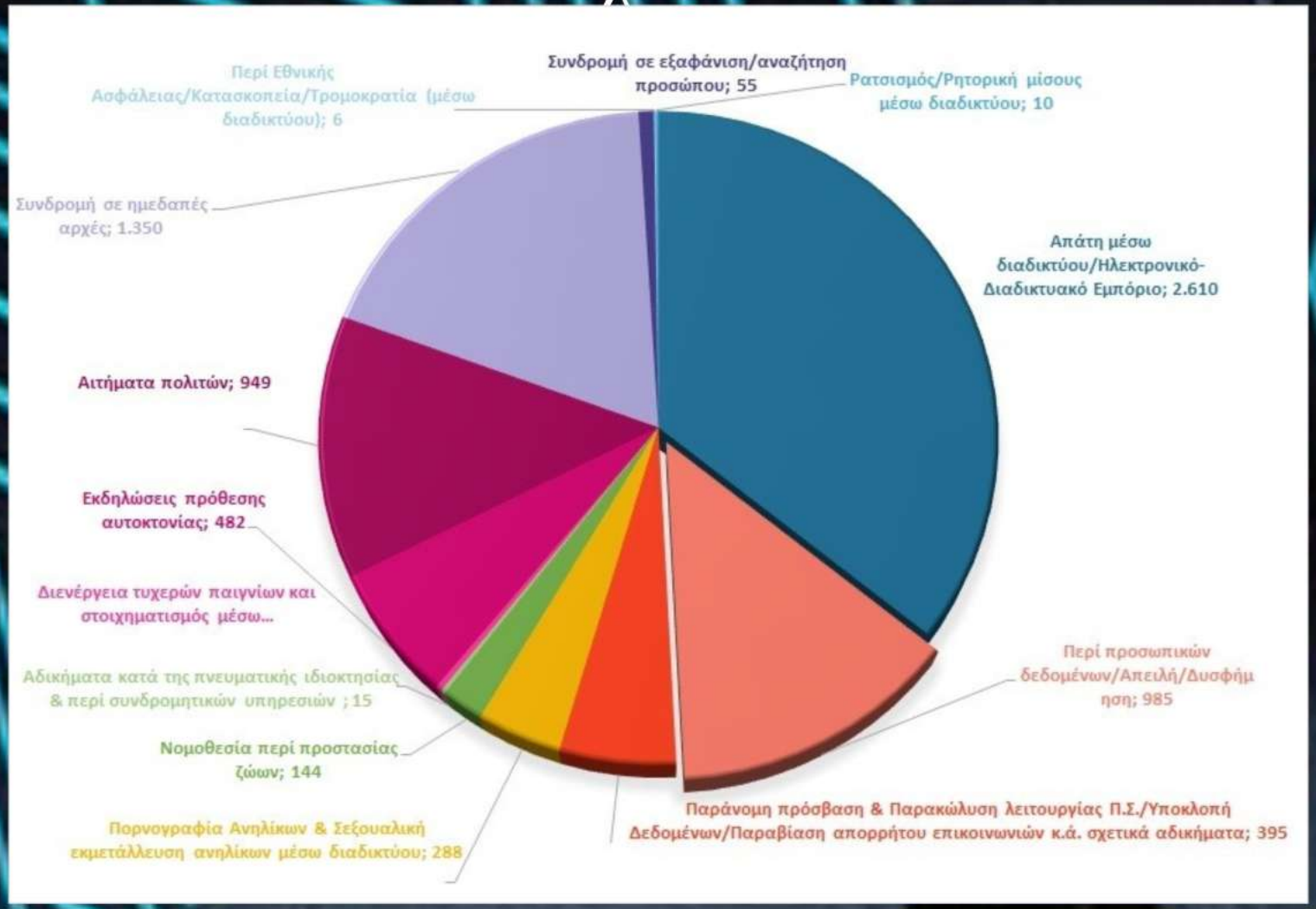
- Το υλικό σεξουαλικού περιεχομένου που δημιουργείται για προσωπική χρήση προκαλεί αυξανόμενη ανησυχία και διανέμεται επίσης για κέρδος.

- Οι εγκληματίες συνεχίζουν να καταχρώνται υπηρεσίες όπως VPN, κρυπτογραφημένες υπηρεσίες επικοινωνίας και κρυπτονομίσματα.

ENISA Threat Landscape 2021

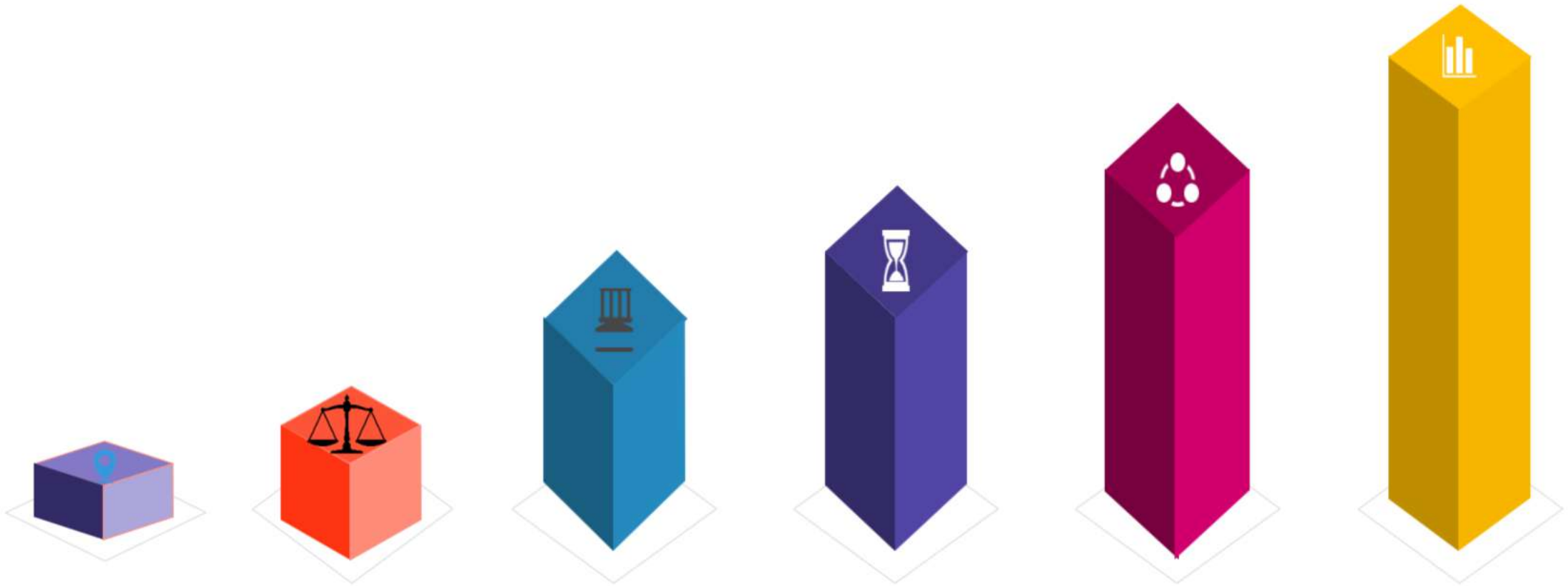
- Το 2020 και το 2021, καταγράφηκαν πολλά περιστατικά που οφειλόταν σε ανθρώπινα λάθη.
- Υπήρξε αύξηση στις παραβιάσεις δεδομένων που σχετίζονται με τον τομέα της υγείας.
- Το Ransomware έχει χαρακτηριστεί ως η κύρια απειλή για το 2020-2021.
- Οικονομική επιβράβευση των εγκλημ
ατιών παραμένει το κύριο κίνητρο. Τα κρυπτονομίσματα είναι η πιο κοινή μέθοδος πληρωμής.
- Οι απάτες με τη μέθοδο του ενδιάμεσου (Business Email Compromise- BEC) αυξήθηκαν, εξελίχθηκαν σε πολυπλοκότητα και έγιναν περισσότερο στοχευμένες.
- Ο αριθμός των μολύνσεων cryptojacking έφθασε σε ιστορικό υψηλό το Α΄ τρίμηνο του 2021, σε σύγκριση με τα τελευταία χρόνια.

Στατιστικά στοιχεία ΔΙΔΗΕ 2021



- Το 2021 υπήρξε αύξηση 21,7% στο σύνολο των νέων υποθέσεων που χειρίστηκε η ΔΙ.Δ.Η.Ε.
- Οι απάτες που πραγματοποιήθηκαν μέσω διαδικτύου εμφάνισαν αύξηση 27%
- Στο τηλεφωνικό κέντρο της Υπηρεσίας εισήχθησαν 89.390 κλήσεις.

Συνολικός αριθμός νέων υποθέσεων που χειρίστηκε η ΔΙ.Δ.Η.Ε.



2016
2.751 υποθέσεις

2017
3.120 υποθέσεις

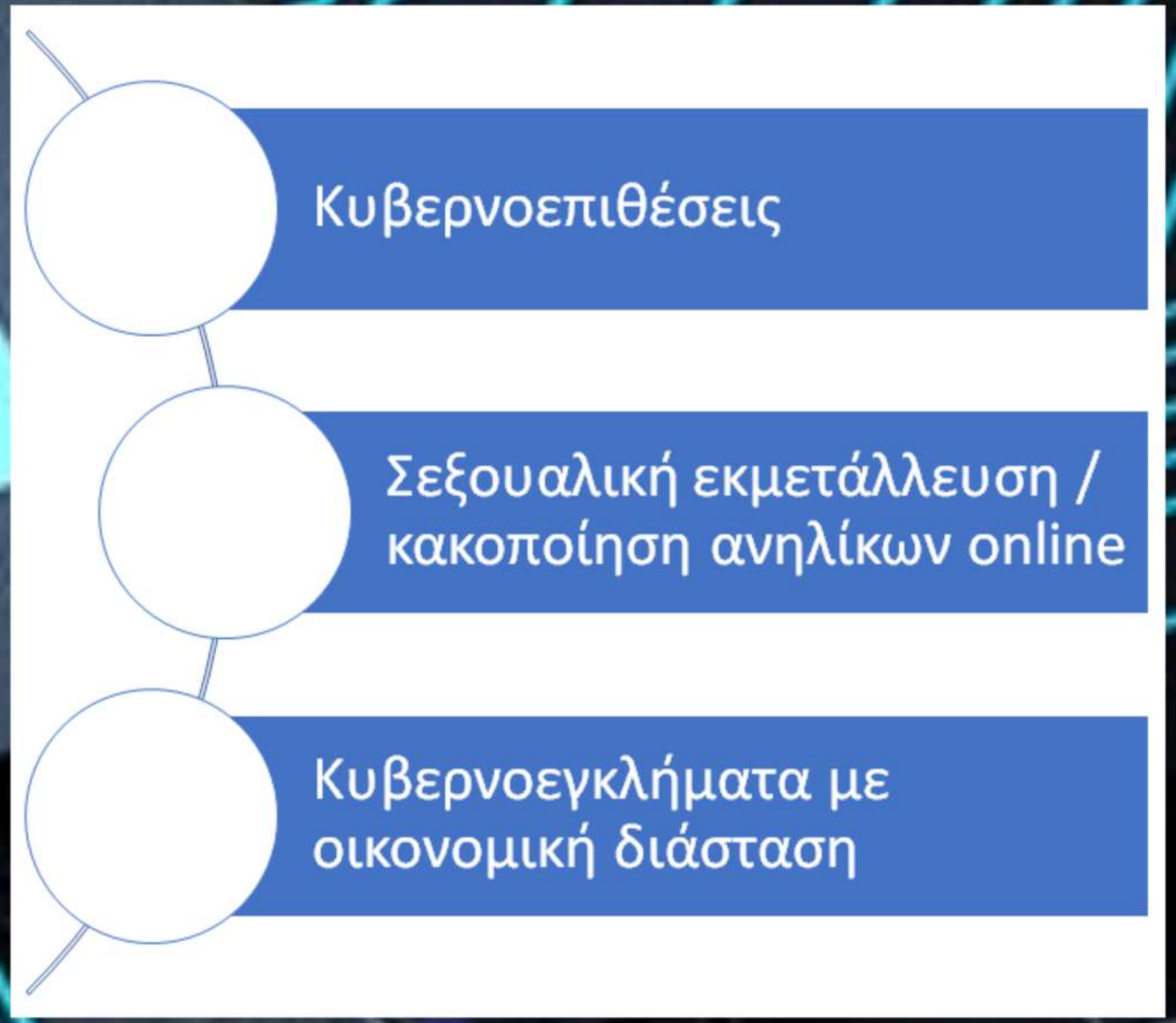
2018
4.857 υποθέσεις

2019
5.187 υποθέσεις

2020
6.019 υποθέσεις

2021
7.328 υποθέσεις

Κατηγορίες γνήσιων κυβερνοεγκλημάτων



Συνέργειες


ΕΕΤΤ
ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ


ΔΙΕΥΘΥΝΣΗ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
11012
ΓΡΑΜΜΗ ΚΑΤΑΓΓΕΛΙΩΝ


ΔΔΠ
Διεύθυνση Διαχείρισης & Ανάλυσης Πληροφοριών


ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ


EUROPOL


ΑΔΑΕ


enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY


Southeast European Law Enforcement Center
SELEC


OIPC ICPO
INTERPOL
INTERPOL


ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

EUROJUST

European Union Agency for Criminal Justice Cooperation

Home | About us | Judicial cooperation | Crime types and cases | States and partners | Publications

New action against online criminal network defrauding users of popular consumer sites

08 July 2021 | PRESS RELEASE

Eurojust has coordinated a follow-up action against a Romanian criminal network involved in extensive online fraud against users of popular consumer sites such as Amazon and eBay. During an action day, the Romanian and Greek authorities arrested eight members of an organised crime group (OCG). The criminal network used phishing scams to defraud online customers of at least EUR 2 million as they tried to buy prestigious cars and a range of other products, or to book accommodations. In total 30 places were searched and EUR 220 000 in cash, mobile phones and travel documents were seized.

Last month, Eurojust supported another operation against other members of the same OCG, who committed online fraud in the Dutch housing market, leading to two arrests.

The OCG managed to get hold of bank account numbers and other data of customers using phishing techniques, the sending of fraudulent messages to victims. Unaware that their devices had been infected by malware, customers provided personal financial data, credit card or bank account numbers, and login details.

This happened when they booked accommodations on websites such as Airbnb, for instance, or purchased goods via Amazon. Customers subsequently lost the money that was taken from their credit cards or bank accounts for the purchase of products or services, which they never received. Regarding the accommodations, the scammers pretended certain places were their properties and made victims believe the transactions were taking place via Airbnb.

The data of victims were shared with other participants in the scheme. The criminal network set up at least 300 bank accounts in Hungary, Spain, Poland, Germany and the Netherlands, using forged identity documents, to hide their profits.

The online scammers also pretended to sell equipment and cars on eBay by posting fictitious advertisements and transferring the profits to their own accounts. For this purpose, they used the names of non-existent transport and payment companies, which were similar to legally operating enterprises, thus misleading victims.

Hellenic Police, Cybercrime Division

EUROJUST

Massive trans-European pay-TV fraud disrupted

Crackdown on a criminal network illegally selling audiovisual material, by Italian, Bulgarian, German, Greek, French and Dutch authorities with the support of Eurojust

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

OPENBAAR MINISTERIE

POLITIE

18/09/2019 JOINT ACTION DAY Parallel actions carried out by judicial and law enforcement authorities throughout Europe to shut down hundreds of illegal servers. Real-time coordination of the national authorities provided through a coordination centre set up at Eurojust. European Investigation Orders and freezing orders swiftly executed across Europe to seize and secure evidence.

CASE REFERRED TO EUROJUST A case is opened at Eurojust, after detecting cross-border links to a parallel investigation into the same criminal network by the Public Prosecutor Office of Rome as well as to another five Member States. Eurojust helps to advance the investigations through quick information exchange and centralised coordination of the national authorities.

LAUNCH OF ITALIAN INVESTIGATIONS The Public Prosecutor Office of Naples starts a complex investigation into a criminal network illegally re-broadcasting and selling pay-per-view products and services.

< 200 servers taken offline

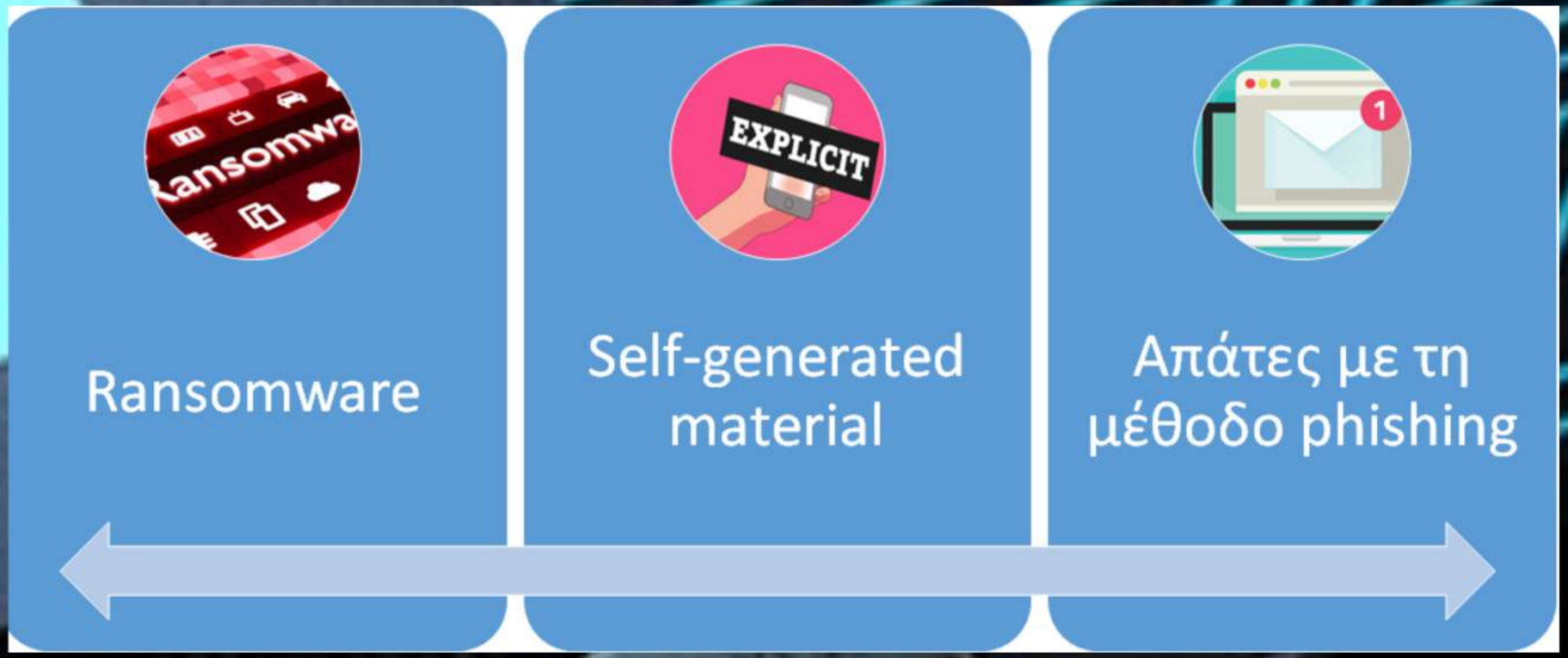
< 150 *PayPal* accounts blocked

22 suspects identified

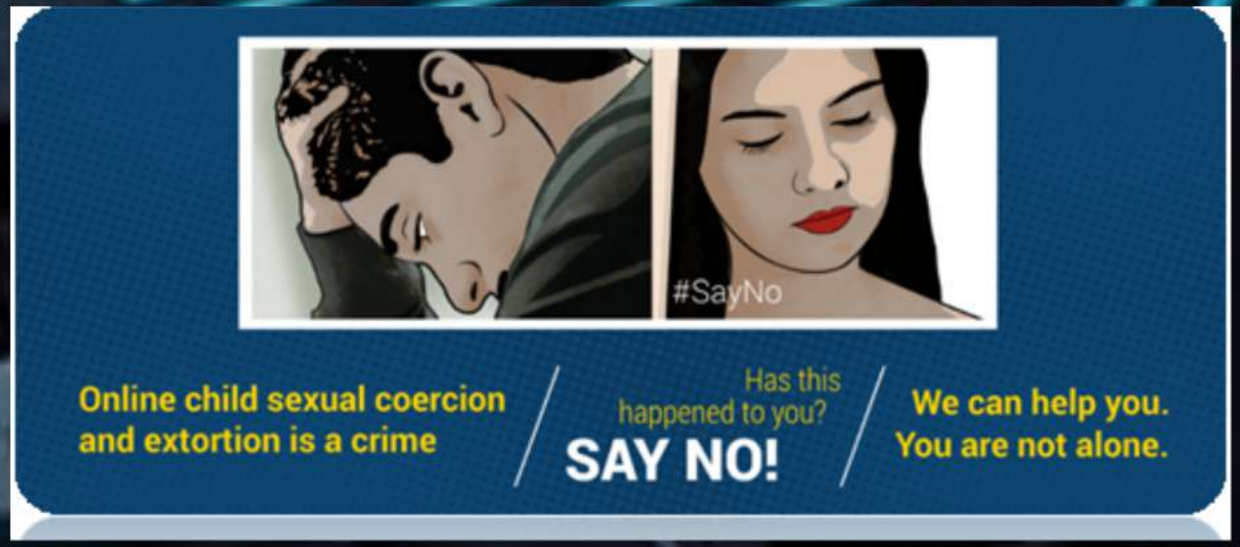
Evidence seized:
servers, digital equipment, payment instruments, record sheets

www.eurojust.europa.eu

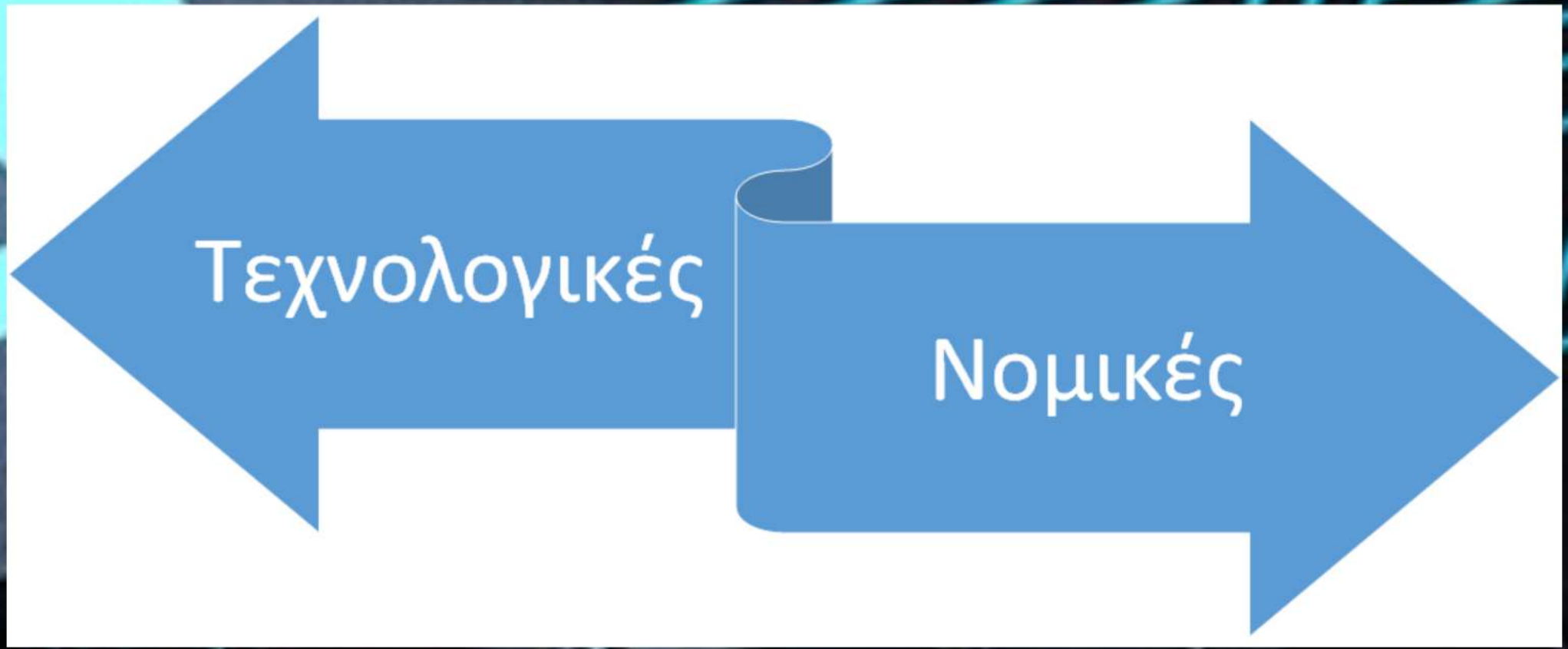
Τρέχουσα κατάσταση – Τάσεις



Τρέχουσα κατάσταση – Τάσεις



Προκλήσεις



Τεχνολογικές προκλήσεις

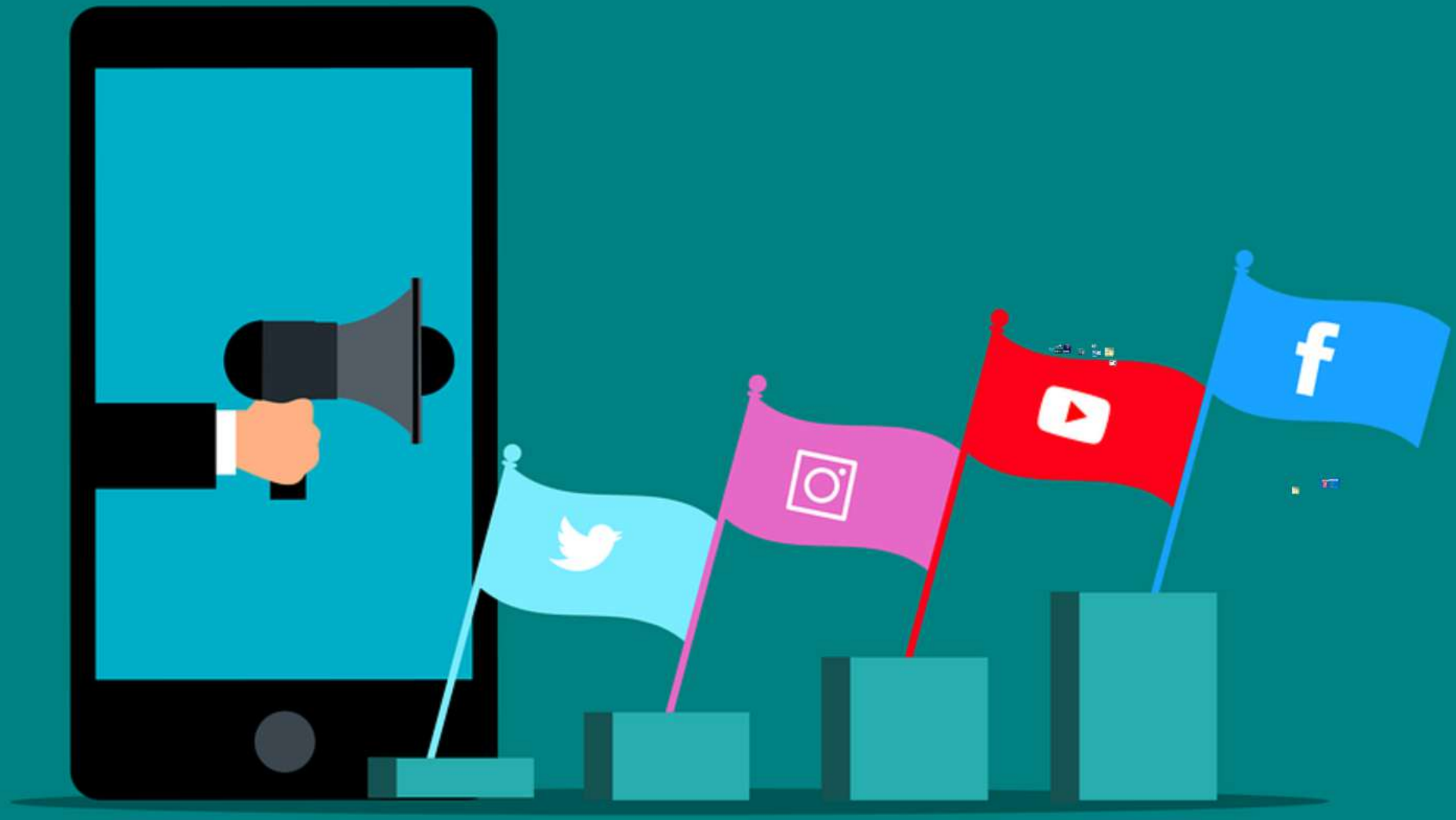
Νομικές προκλήσεις

- Προσωπικά δεδομένα vs Απόρρητο επικοινωνιών vs Ασφάλεια
- Διατήρηση δεδομένων
- Διασυνοριακή πρόσβαση σε δεδομένα
- Παραδεκτό
- Ζητήμα "νέφους" (cloud) (Άρθρο 265 - Κ.Π.Δ. (Νόμος 4620/2019 Κατάσχεση ψηφιακών δεδομένων)
- Κρυπτονομίσματα (Νόμος 4734/2020 τροποποίηση του ν. 4557/2018)
  - Κατάσχεση
  - Λειτουργία tumblers / mixers

Σύνοψη - Επίλογος

- Οι εγκληματίες εκμεταλλεύονται τις τεχνολογικές εξελίξεις.
- Η τεχνολογία εξελίσσεται ταχύτερα από τη νομοθεσία.
- Απαιτείται η λήψη μέτρων ασφάλειας για εταιρικό και προσωπικό ψηφιακό εξοπλισμό και θέσπιση πολιτικών ασφαλείας από οργανισμούς και επιχειρήσεις.
- Ο κόσμος αλλάζει & η προσαρμογή (εκπαίδευση - ενημέρωση & ευαισθητοποίηση) όλων μας στα νέα δεδομένα είναι επιβεβλημένη.

Δράσεις Ενημέρωσης



Ενημερωτικά Φυλλάδια

Συμμετοχή στο περίπτερο ΕΛ.ΑΣ στην Διεθνή Έκθεση Θεσσαλονίκης

Τηλεοπτικά & Ραδιοφωνικά μηνύματα ΔΙ.Δ.Η.Ε.

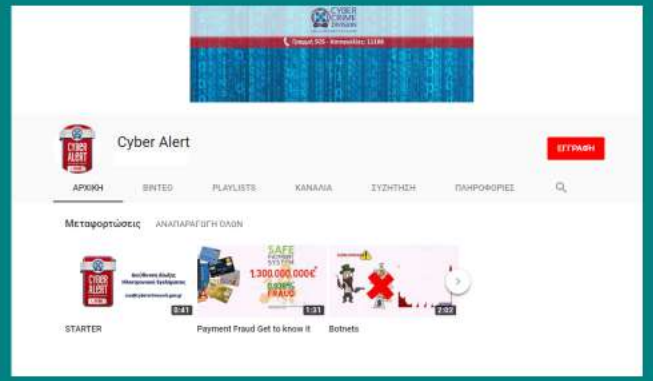

https://cyberalert.gr/
11188 ccu@cybercrimeunit.gov.gr Λεωφ. Αλεξάνδρας 173, Τ.Κ. 11522 - Αθήνα
CYBER ALERT
ΑΡΧΙΚΗ CYBERALERT FEELSAFE ΕΠΙΚΟΙΝΩΝΙΑ
CYBER ALERT
από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος
MOBILE MALWARE
ΜΑΘΕΤΕ ΠΩΣ ΘΑ ΘΩΡΑΚΙΣΤΕΙΤΕ
16 09 2015 Τηλεοπτικό μην...


Ασφαλώς.. με κάρτα!
FEELSAFE
@ e-commerce
Γραμμή FEELSAFE
Ενημερώσου!
Νέα
FEEL EXPERT
Ελάτε στο περίπτερο της Ελληνικής Αστυνομίας στην 80η ΔΕΘ
5-13 Σεπτεμβρίου, και ενημερωθείτε από τη
Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος


Not secure https://www.cyberkid.gov.gr/
Cyberkid
ccu@cybercrimeunit.gov.gr
11188
6-10 ΕΤΩΝ 11-14 ΕΤΩΝ 15-18 ΕΤΩΝ ΓΟΝΕΙΣ ΨΗΦΙΑΚΟΣ ΠΑΙΔΟΤΟΠΟΣ ΔΙΑΔΙΚΤΥΟ APPLICATION CYBERKID ΕΠΙΚΟΙΝΩΝΙΑ
ΝΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ!
www.cyberkid.gr
ΑΛΛΑ ΜΕ ΑΣΦΑΛΕΙΑ


CYBERKID
ΓΡΑΜΜΗ SOS
ΦΙΛΙΚΕΣ ΣΥΜΒΑΣΕΙΣ
Εσύ υπέγραψες ?
eLEARNING
Αρχίζει το μάθημα
ΣΥΜΒΟΥΛΕΣ - ΝΕΑ
Για όλες τις ηλικίες
ΨΗΦΙΑΚΗ ΑΛΑΝΑ


CyberKid
@cyberkid.gov.gr
Αρχική σελίδα
Πληροφορίες
Φωτογραφίες
Εκδηλώσεις
Σε επείγον περιστατικό καλέστε το 11188.
Cyberkid
Σας αρέσει
Ακολουθείτε
Κοινοποίηση
Επικοινωνήστε μαζί μας


Cyber Alert
ΕΓΓΡΑΦΗ
ΑΡΧΙΚΗ
ΒΙΝΤΕΟ
PLAYLISTS
ΚΑΝΑΛΙΑ
ΣΥΖΗΤΗΣΗ
ΠΛΗΡΟΦΟΡΙΕΣ
Μεταφορτώσεις
ΑΝΑΠΑΡΑΓΩΓΗ ΟΛΩΝ
STARTER
Payment Fraud Get to know it
Botnets


CYBER ALERT
@CyberAlertGR
Αρχική σελίδα
Πληροφορίες
Φωτογραφίες
Εκδηλώσεις
Σε επείγον περιστατικό καλέστε το 11188.
Σας αρέσει
Ακολουθείτε
Κοινοποίηση
Επικοινωνήστε μαζί μας


cyberalert.gr
Ακολουθείτε
242 δημοσιεύσεις
19.2k ακόλουθοι
Ακολουθείτε 22 χρήστες
CyberAlert
Το επίσημο Instagram της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας
cyberalert.gr
διαδικτυο
ransomware
ransomware
Money mul...


cyberalert
Cyber Crime Division - Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος - Ελληνική Αστυνομία
Tweet
Tweet & απαντήσεις
Πολυμέσα
Η δραστηριότητα Tweet σας

govgr

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος του Αρχηγείου της Ελληνικής Αστυνομίας σύμμαχος στην ασφάλεια των πολιτών στον Κυβερνοχώρο!

@CyberAlertGR
@cyberkid.gov.gr
@hellenicpolice

@CyberAlertGR
@hellenicpolice

cyberalert.gr

Cyber Alert
Ελληνική Αστυνομία - Hellenic Police