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

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.

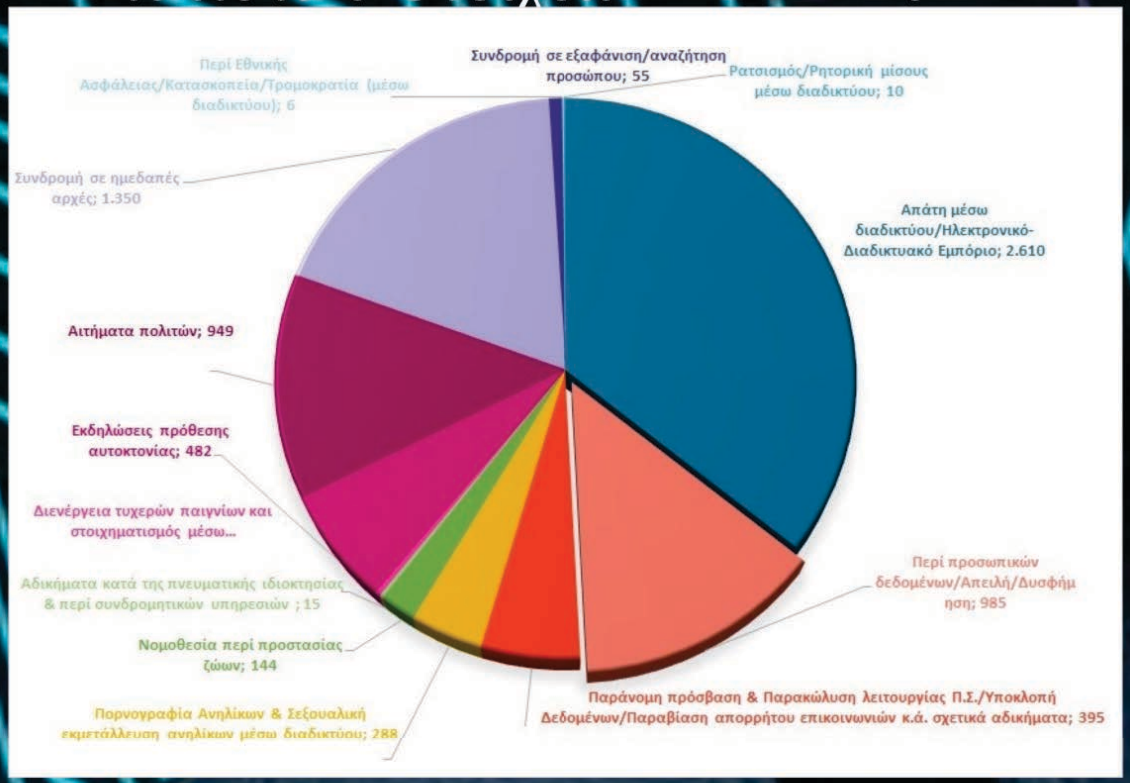
- Το υλικό σεξουαλικού περιεχομένου που δημιουργείται για προσωπική χρήση προκαλεί αυξανόμενη ανησυχία και διανέμεται επίσης για κέρδος.

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

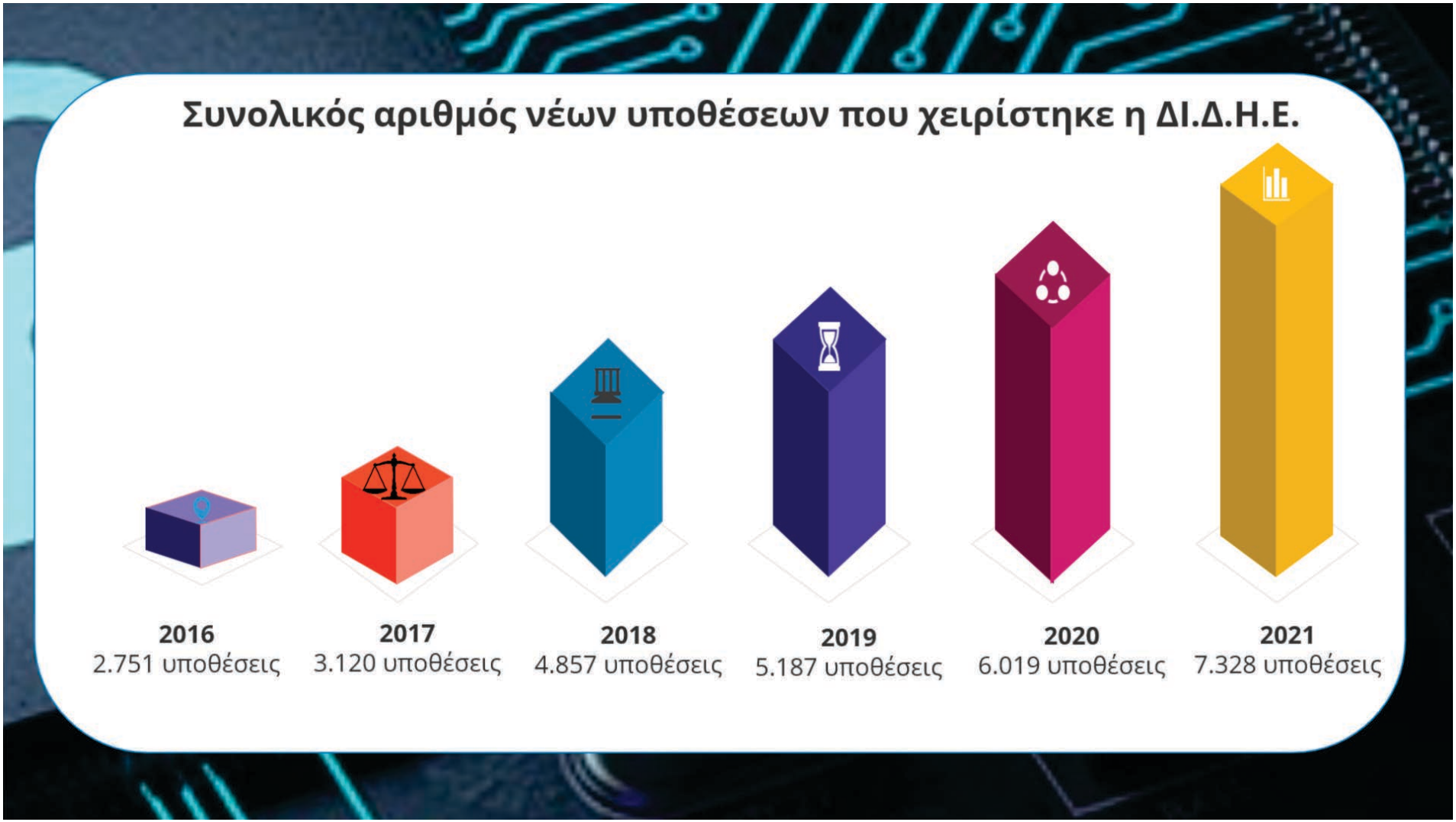
ENISA Threat Landscape 2021

- 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 εγκληματιών 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.

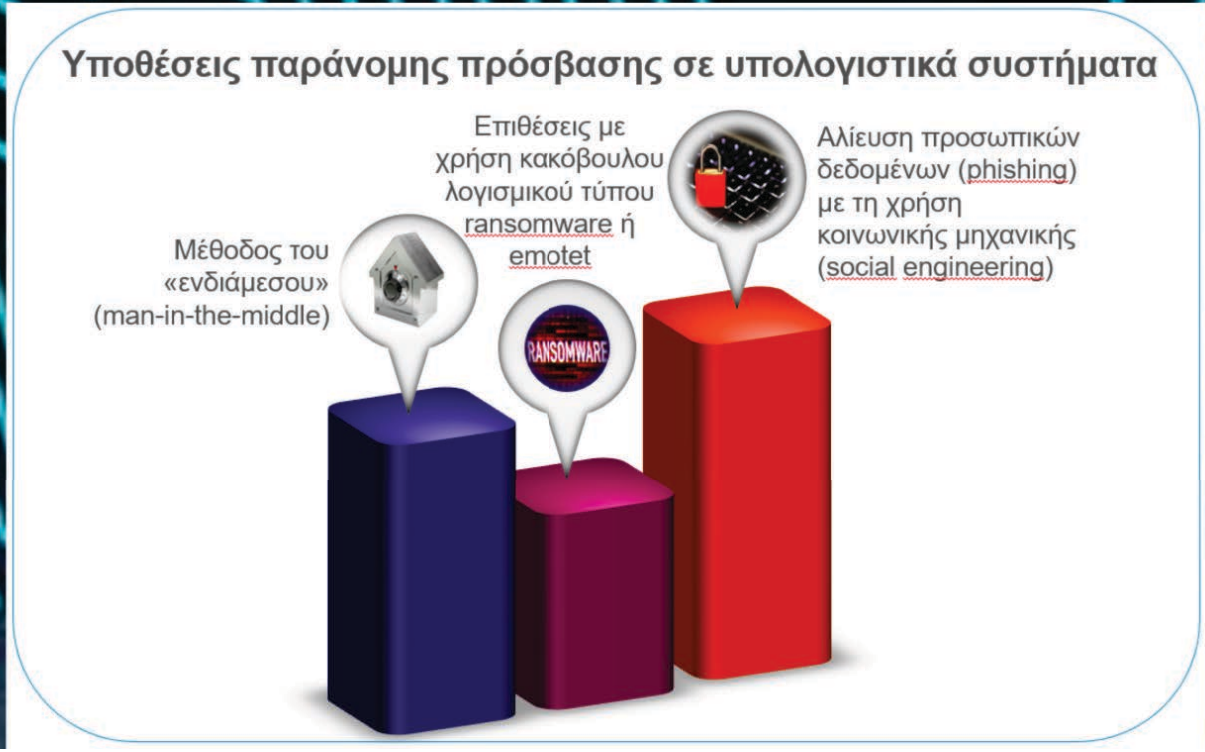

Συνολικός αριθμός νέων υποθέσεων που χειρίστηκε η ΔΙ.Δ.Η.Ε.
2016
2.751 υποθέσεις
2017
3.120 υποθέσεις
2018
4.857 υποθέσεις
2019
5.187 υποθέσεις
2020
6.019 υποθέσεις
2021
7.328 υποθέσεις

Εγκλήματα με οικονομική διάσταση στο ψηφιακό εταιρικό περιβάλλον

- Επιθέσεις Phishing
- Ransomware & Cryptoware
- Απάτη CEO
- Επιθέσεις Man-in-the-middle
- Εκβίαση με επίθεση DDoS

Οι απάτες που πραγματοποιήθηκαν μέσω διαδικτύου εμφάνισαν αύξηση 27% εκ των οποίων οι σημαντικότεροι τρόποι δράσης πραγματοποιήθηκαν με μεταφορές χρημάτων μέσω τραπεζικών συστημάτων και οι απάτες που σχετίζονταν με απατηλή χρήση τραπεζικής κάρτας.
Το μεγαλύτερο ποσοστό αύξησης παρουσίασαν οι μεταφορές χρημάτων σε απατηλούς λογαριασμούς μέσω τραπεζικών συστημάτων (354%) και οι απάτες με την υπόσχεση παροχής επενδυτικών υπηρεσιών (307%).

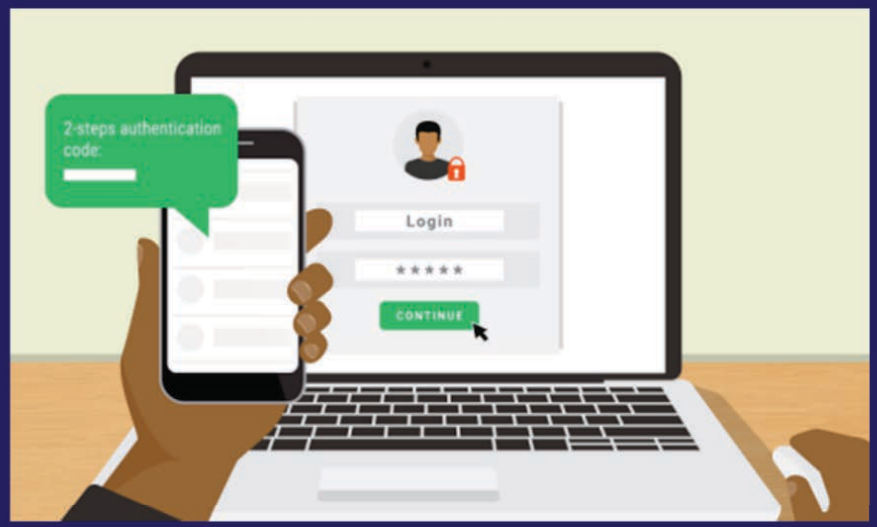
Οι συνηθέστεροι τρόποι δράσης παραμένουν η αλίευση προσωπικών δεδομένων (phishing) με τη χρήση κοινωνικής μηχανικής (social engineering) και η μέθοδος του «ενδιάμεσου» (man-in-the-middle). Επίσης οι επιθέσεις με κακόβουλο λογισμικό τύπου ransomware ή emotet εμφάνισαν σημαντικό ποσοστό αύξησης της τάξης του 110% .



Λογισμικό

- Χρήση προγραμμάτων προστασίας από κακόβουλο λογισμικό, τόσο στον υπολογιστή, όσο και στις φορητές συσκευές (smartphones, tablets) και τακτική ενημέρωσή τους
- Εγκατάσταση διαθέσιμων αναβαθμίσεων και ενημερώσεων / διορθώσεων ασφαλείας του λειτουργικού συστήματος και των λοιπών προγραμμάτων και εφαρμογών
- Αποφυγή εγκατάστασης προγραμμάτων και εφαρμογών από μη ασφαλείς πηγές

Κωδικοί πρόσβασης



- Τακτική αλλαγή **κωδικών πρόσβασης** στο ηλεκτρονικό ταχυδρομείο & τις λοιπές online υπηρεσίες
- Χρήση τεχνικών **αυθεντικοποίησης δύο βημάτων** (2-steps authentication)

Χρήστες

- Δεν ανταποκρινόμαστε σε μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνήματα όπου ζητείται η αποκάλυψη στοιχείων πρόσβασης σε ηλεκτρονικούς λογαριασμούς & υπηρεσίες
- Δεν επιλέγουμε σε συνδέσμους (links) που εμπεριέχονται σε e-mails από αγνώστους, καθώς οι σύνδεσμοι αυτοί ενδέχεται να παραπέμπουν σε κακόβουλες ιστοσελίδες ή/και να προκαλούν την εγκατάσταση κακόβουλου λογισμικού
- Επανελέγχουμε τηλεφωνικά «ύποπτα» αιτήματα που αφορούν π.χ. καταβολή χρημάτων σε διαφορετικό τραπεζικό λογαριασμό, αποκάλυψη κωδικών πρόσβασης κ.λπ.

Ο ρόλος της εταιρείας
& των CISO (chief Information Security Officer) - ISM (Information Security Manager)

Ενημέρωση / εκπαίδευση του προσωπικού

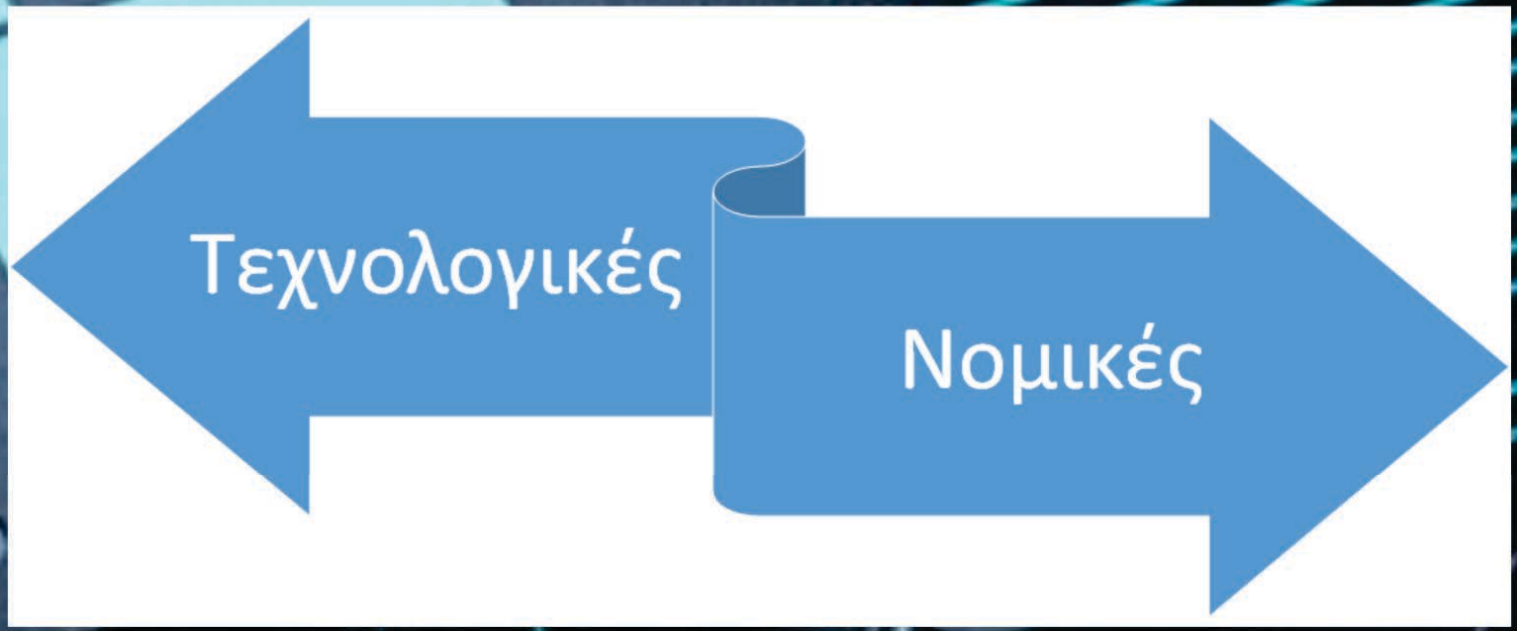
Παρά τα μέτρα ασφαλείας
ο αδύναμος κρίκος παραμένει ο άνθρωπος!

Ο ρόλος της εταιρείας & των CISO - ISM

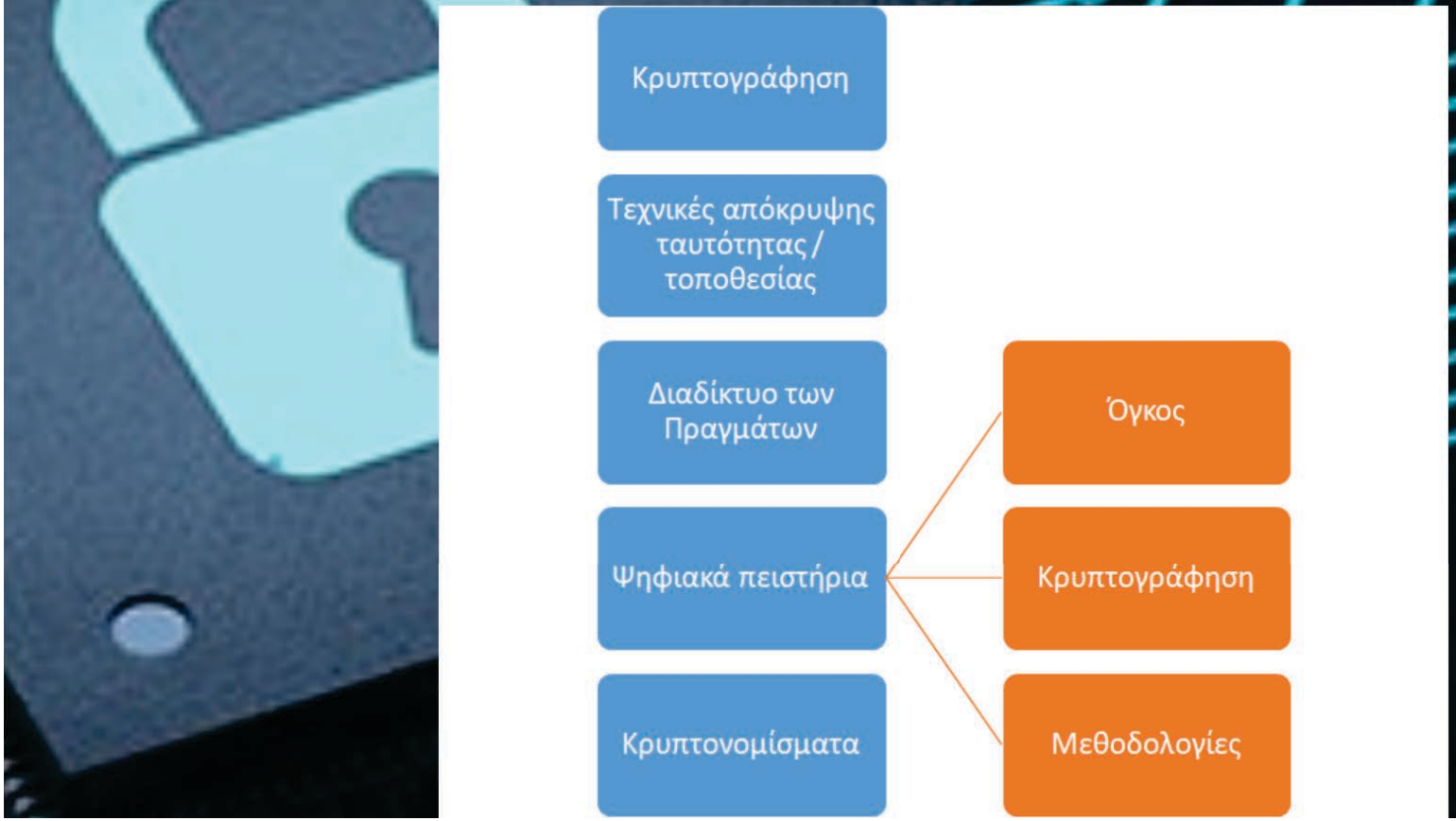
- Φυσική ασφάλεια
- Πολιτικές ασφάλειας κατά τη χρήση των ψηφιακών, υπολογιστικών συστημάτων και Διαδικτύου (policies, standards, procedures)
  - USB sticks, Cloud κ.λπ.
  - VPN, Bring your own Device (BYOD)
  - Δικαιώματα πρόσβασης
  - Τήρηση αρχείων καταγραφής
  - Τήρηση αντιγράφων ασφαλείας (back up)
- Εφαρμογή μεθόδων κρυπτογράφησης - αποθήκευση δεδομένων και κλειδιών κρυπτογράφησης
- Ασφαλή κανάλια επικοινωνίας

Προσοχή στην πρόσβαση σε εταιρικά δεδομένα από δημόσια WiFi δίκτυα!

Προκλήσεις



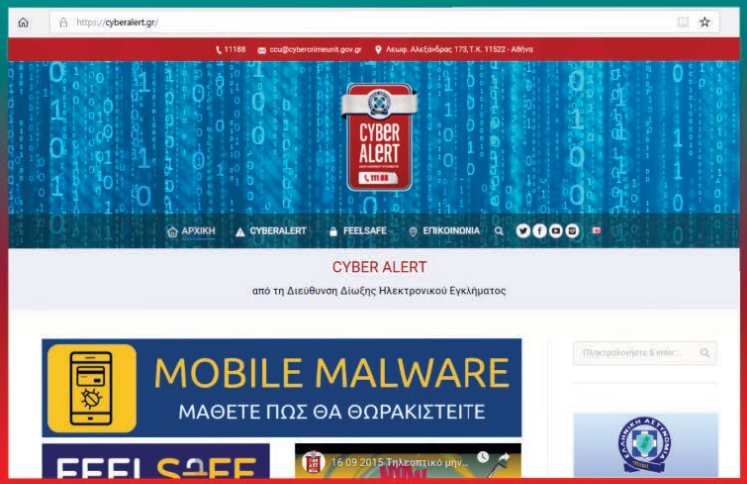
Τεχνολογικές προκλήσεις

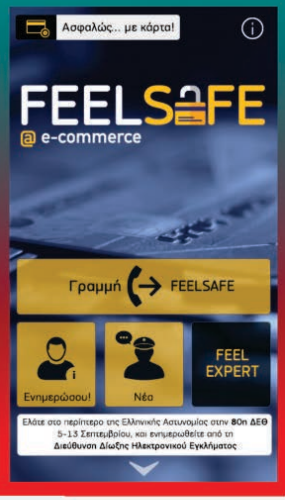


Νομικές προκλήσεις

- 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

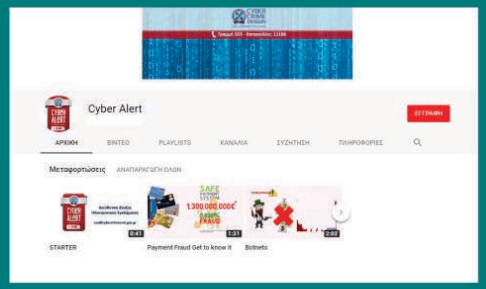
Δράσεις Ενημέρωσης

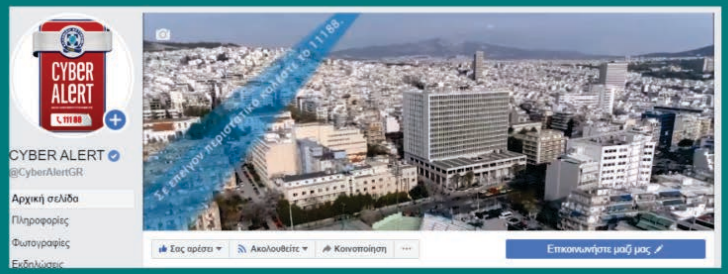

https://cyberalert.gr/
CYBER ALERT
ΑΡΧΙΚΗ
CYBERALERT
FEELSAFE
ΕΠΙΚΟΙΝΩΝΙΑ
CYBER ALERT
από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος
MOBILE MALWARE
ΜΑΘΕΤΕ ΠΩΣ ΘΑ ΘΩΡΑΚΙΣΤΕΙΤΕ

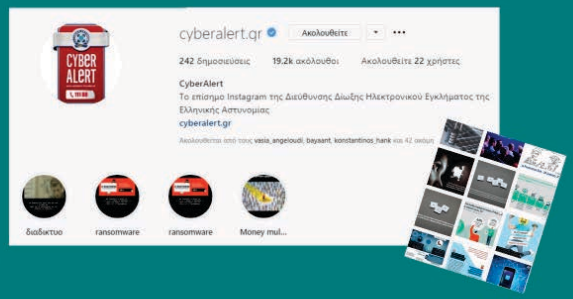

Ασφαλώς... με κάρτα!
FEELSAFE
@ e-commerce
Γραμμή
FEELSAFE
Ενημερώσου!
Νέα
FEEL EXPERT


Not secure https://www.cyberkid.gov.gr/
Cyberkid
11188
ΝΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ!
www.cyberkid.gr
ΑΛΛΑ ΜΕ ΑΣΦΑΛΕΙΑ

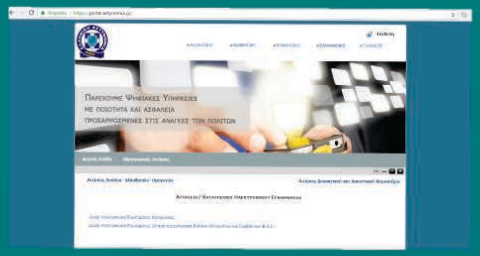

CYBERKID
ΓΡΑΜΜΗ SOS
ΦΙΛΙΚΕΣ ΣΥΜΒΑΣΕΙΣ
Εσύ υπέγραψες ?
eLEARNING
Αρχίζει το μάθημα
ΣΥΜΒΟΥΛΕΣ - ΝΕΑ
Για όλες τις ηλικίες
ΨΗΦΙΑΚΗ ΑΛΑΝΑ







Διαδικτυακή Πύλη ΕΛ.ΑΣ




ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ
CYBER ALERT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ
111 88
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