

ΤΙ ΕΙΝΑΙ Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ;

.....εργαλεία, πολιτικές, κατευθυντήριες γραμμές, προσεγγίσεις διαχείρισης κινδύνου, δράσεις κατάρτισης, βέλτιστες πρακτικές, εγγυήσεις και τεχνολογίες, οι οποίες μπορούν να χρησιμοποιηθούν για την προστασία της διαθεσιμότητας, της εμπιστευτικότητας των στοιχείων των συνδεδεμένων υποδομών κι αφορούν κυβερνήσεις, ιδιωτικούς οργανισμούς και πολίτες

Ορισμός κατά την Διεθνή Ένωση Τηλεπικοινωνιών

Πηγή: https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018 π.13

Η Κυβερνοασφάλεια συνδέεται με τις έννοιες Κυβερνοχώρος – Κυβερνοέγκλημα – Κυβερνοάμυνα



ΚΥΒΕΡΝΟΧΩΡΟΣ: ΤΙ ΔΥΝΑΤΟΤΗΤΕΣ ΜΑΣ ΠΑΡ'ΕΧΕΙ;

- ▶ Να συνδεόμαστε
- ▶ Να εκφραζόμαστε
- ▶ Να καινοτομούμε
- ▶ Να διαμοιράζουμε
- ▶ Να επιλέγουμε
- ▶ Να εμπιστευόμαστε



ΣΤΟΧΟΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

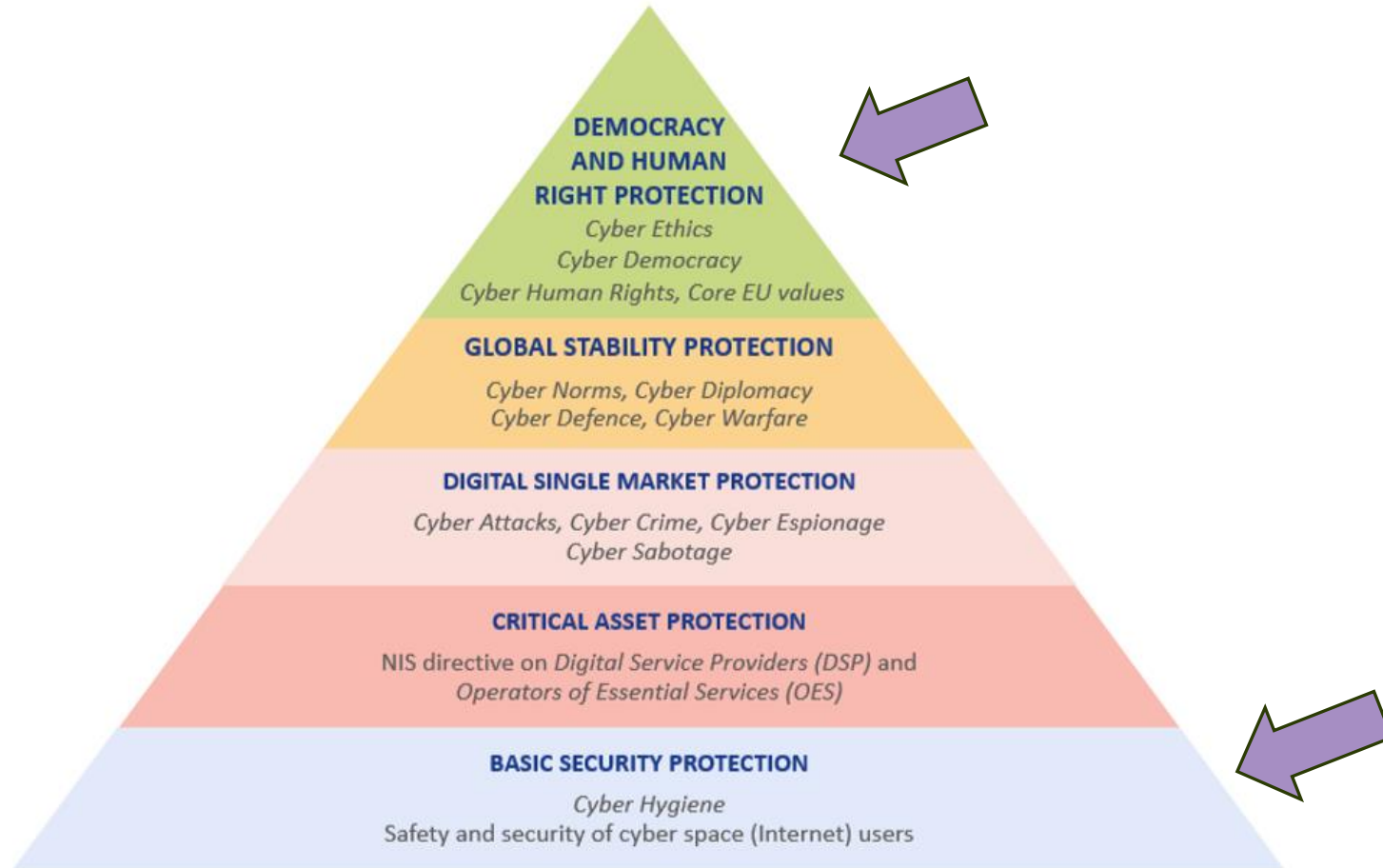
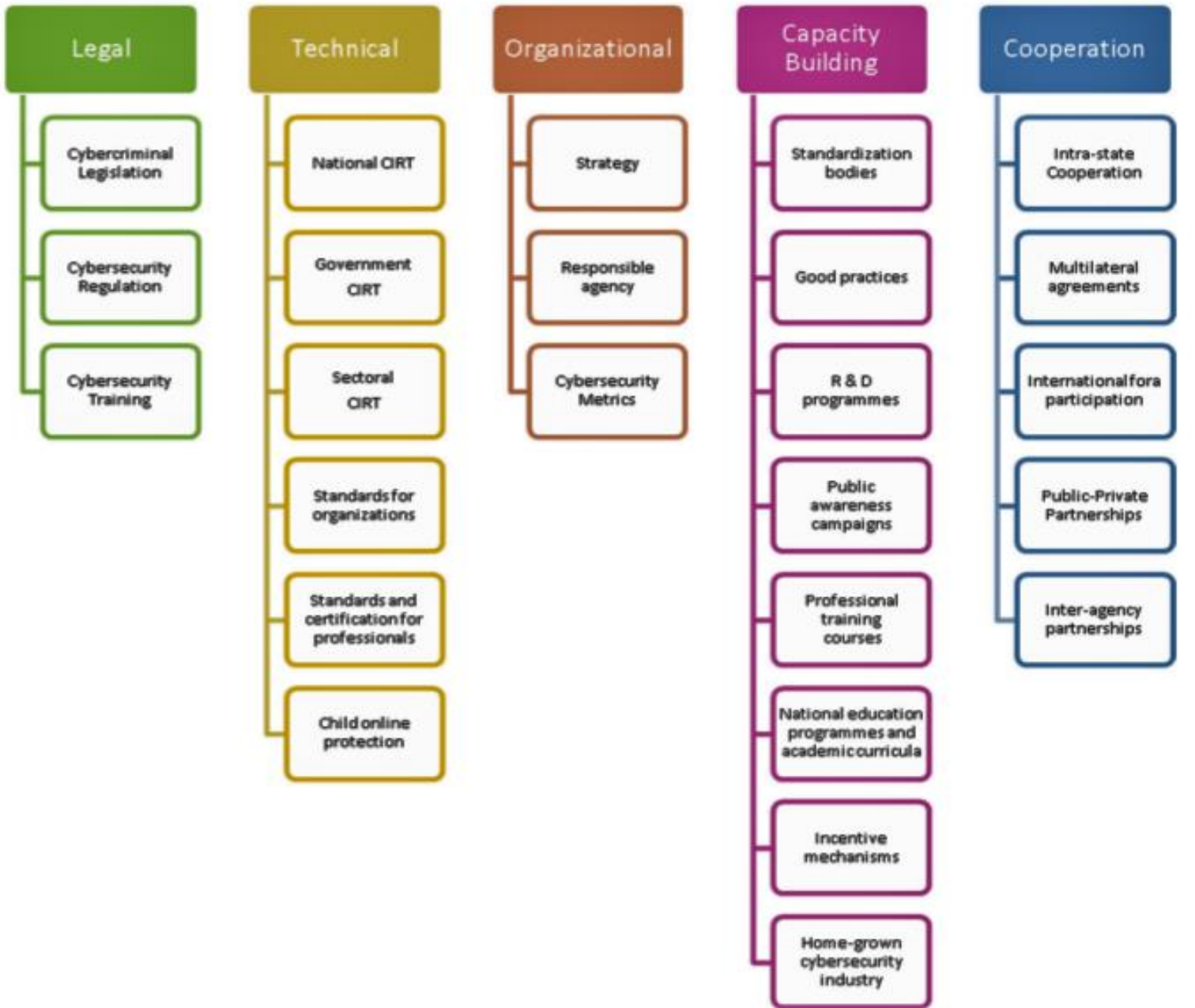


Figure 1. Layers of cybersecurity needs.

ΔΗΜΟΚΡΑΤΙΑ
ΚΑΙ
ΠΡΟΣΤΑΣΙΑ
ΑΝΘΡΩΠΙΝΩΝ
ΔΙΚΑΙΩΜΑΤΩΝ



ΜΕΤΡΑ ΣΕ ΝΟΜΙΚΟ, ΤΕΧΝΙΚΟ, ΟΡΓΑΝΩΤΙΚΟ, ΜΕΘΟΔΟΛΟΓΙΚΟ ΚΑΙ ΣΥΝΕΡΓΑΤΙΚΟ ΕΠΙΠΕΔΟ

ΦΟΡΕΙΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ - ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΟΥΣ ΦΟΡΕΙΣ

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

COVID19 TOPICS NEWS PUBLICATIO

ENISA Topics

- Cloud and Big Data
- COVID19
- Critical Infrastructures and Services
- CSIRT Services
- CSIRTs and communities
- CSIRTs in Europe
- Cyber Crisis Management
- Cyber Exercises
- Cybersecurity Education
- Data Protection
- Incident Reporting
- IoT and Smart Infrastructures

Latest news All news

Smart infrastructure during the COVID-19 pandemic

Αρμόδια Ομάδα Απόκρισης Κυβερνοπεριστατικών

ΚΕΝΤΡΙΚΗ ΔΗΜΟΣΙΕΥΣΕΙΣ ΕΙΔΟΠΟΙΗΣΕΙΣ - ΣΥΜΒΟΥΛΕΣ ΣΧΕΤΙΚΟ ΥΛΙΚΟ

Εθνικό Σύστημα Ευαισθητοποίησης στον Κυβερνοχώρο

Πέντε προϊόντα του Εθνικού Συστήματος Ευαισθητοποίησης στον Κυβερνοχώρο προσφέρουν ποικίλες πληροφορίες για χρήστες με ποικίλη τεχνική κατάρτιση. Εκείνοι με περισσότερο τεχνικό ενδιαφέρον μπορούν να διαβάσουν τις ειδοποιήσεις, τις αναφορές ανάλυσης, τις δραστηριότητες ή τα δελτία. Οι χρήστες που αναζητούν κομμάτια γενικότερου ενδιαφέροντος μπορούν να διαβάσουν τις Συμβουλές.

- Δραστηριότητες**
Παρέχει ενημερωμένες πληροφορίες σχετικά με τους τύπους δραστηριοτήτων ασφαλείας που επηρεάζουν την κοινότητα σε μεγάλο βαθμό
- Ειδοποιήσεις**
Έγκαιρη ενημέρωση σχετικά με τρέχοντα θέματα ασφαλείας, ευπάθειες και εκμεταλλεύσεις.
- Δελτία**
Εβδομαδιαίες περιλήψεις νέων ευπαθειών μαζί με πληροφορίες patch όταν είναι διαθέσιμες.
- Συμβουλές**
Συμβουλές και βέλτιστες πρακτικές σχετικά με τα κοινά θέματα ασφαλείας για το ευρύ κοινό.
- Αναφορές Ανάλυσης**
Ανάλυση σχετικά με νέες ή εξελισσόμενες απειλές στον κυβερνοχώρο.

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

Αρχική Το Υπουργείο Δραστηριότητες Γραφείο Τύπου Προκηρύξεις

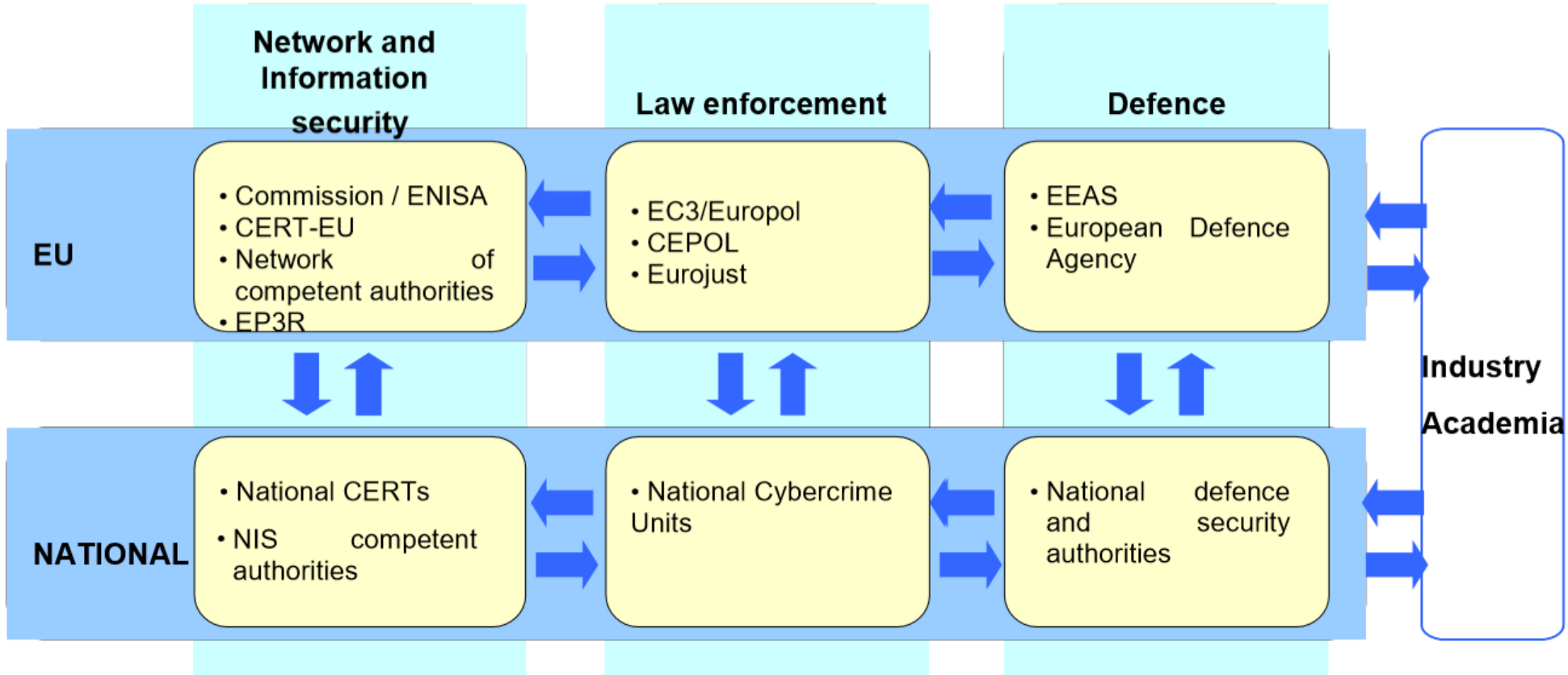
Κυβερνοασφάλεια

Η Γενική Διεύθυνση Κυβερνοασφάλειας υπάγεται στη Γενική Γραμματεία Τηλεπικοινωνιών & Ταχυδρομείων του υπουργείου Ψηφιακής Διακυβέρνησης και καταρτίζει την Εθνική Στρατηγική Κυβερνοασφάλειας, στην οποία καθορίζονται οι στρατηγικοί στόχοι, οι προτεραιότητες και τα μέτρα πολιτικής και κανονιστικής ρύθμισης, με σκοπό την εξασφάλιση υψηλού επιπέδου ασφαλείας για τα συστήματα τηλεπικοινωνιών και πληροφορικής σε εθνικό επίπεδο.

καλό είναι να επισκεφτούμε τους δικτυακούς τόπους και τα προφίλ τους στα Social Media

Πηγή:

<https://www.enisa.europa.eu/>
<https://csirt.cd.mil.gr/el/alerts-and-tips>
<https://mindigital.gr/kyvernoasfaleia>



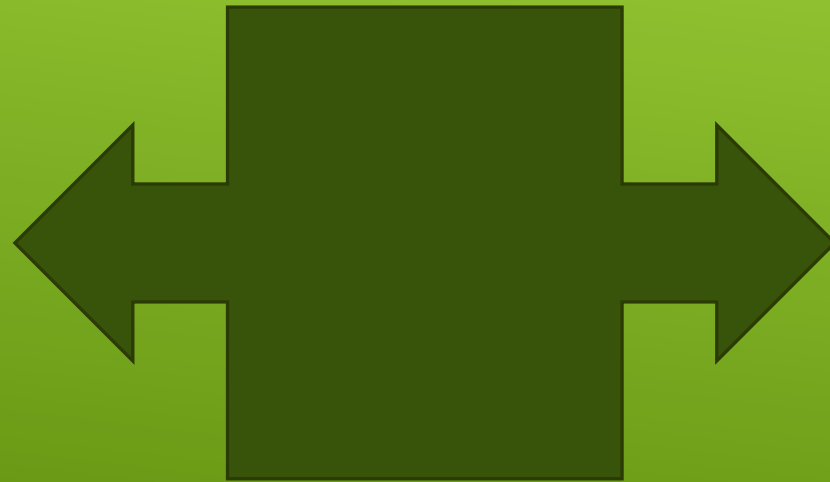
ΆΛΛΟΙ ΣΗΜΑΝΤΙΚΟΪ ΦΟΡΕΪΣ ΣΤΗΝ ΕΛΛΆΔΑ



- ▶ ΑΠΔΠΧ
- ▶ ΑΔΑΕ
- ▶ ΕΕΤΤ
- ▶ Συνήγορος του Καταναλωτή
- ▶ ΤτΕ
- ▶ Οργανισμός για την Πνευματική Ιδιοκτησία
- ▶ ΕΟΦ

ΟΙ ΔΥΟ ΒΑΣΙΚΟΙ ΠΥΛΩΝΕΣ ΠΟΥ ΔΙΑΜΟΡΦΩΝΟΥΝ ΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ;

Τεχνολογία



**Θεσμικό
πλαίσιο**

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΗ

- Η Στρατηγική Κυβερνοασφάλειας της ΕΕ (2013)
 - Η οδηγία NIS (2016) Ν. 4577/2018
 - Η Cybersecurity Act 2019
-
- Η Συνθήκη της Βουδαπέστης Ν. 4411/2016
 - Ο Γενικός Κανονισμός για τα Προσωπικά Δεδομένα ΕΕ 2016/679 και η Οδηγία ΕΕ 2016/680 Ν. 4624/2019



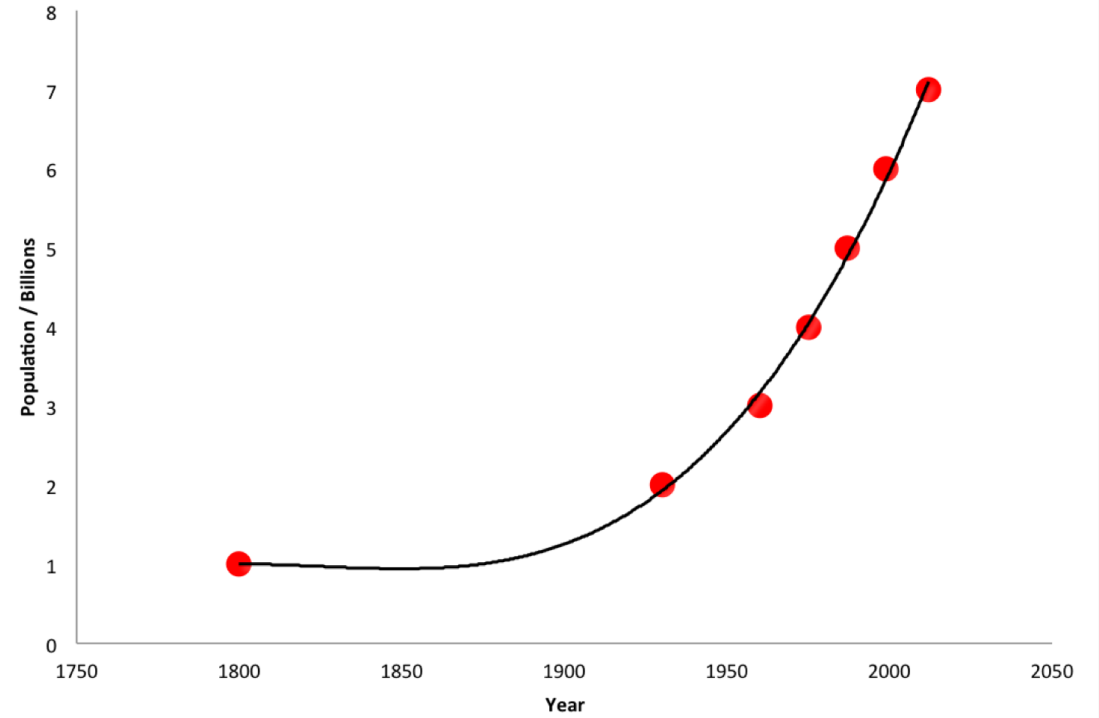
World Population

7,689,432,816

TOP 10 MOST POPULOUS COUNTRIES (July 1, 2020)

1. China	1,394,015,977	6. Nigeria	214,028,302
2. India	1,326,093,247	7. Brazil	211,715,973
3. United States	329,877,505	8. Bangladesh	162,650,853
4. Indonesia	267,026,366	9. Russia	141,722,205
5. Pakistan	233,500,636	10. Mexico	128,649,565

Human Population Growth

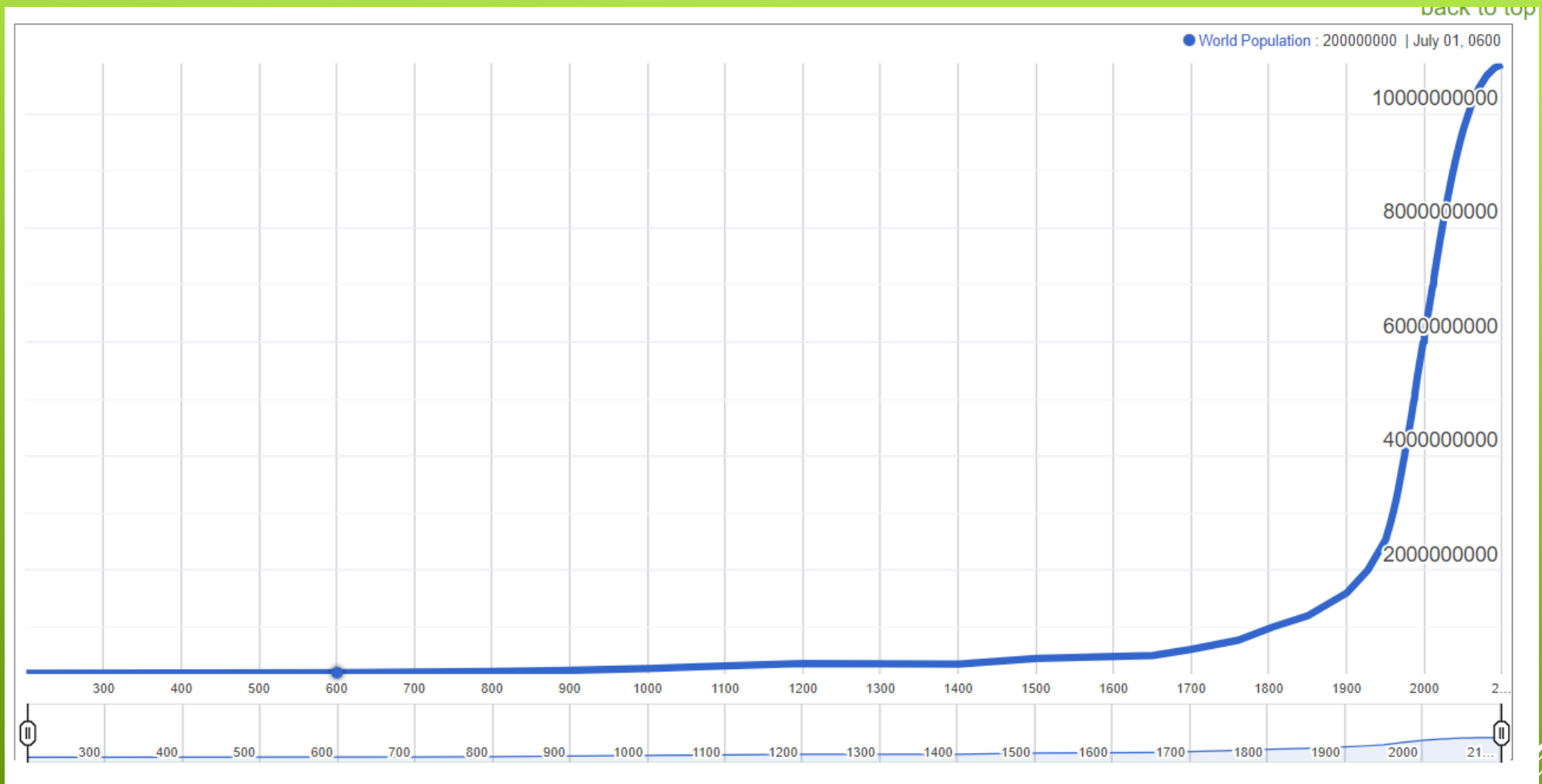


Πληθυσμιακή έκρηξη

ΠΑΓΚΟΣΜΙΟΣ ΠΛΗΘΥΣΜΟΣ

ΠΗΓΗ : [HTTPS://WWW.CENSUS.GOV/POPCLOCK/](https://www.census.gov/popclock/)

back to top

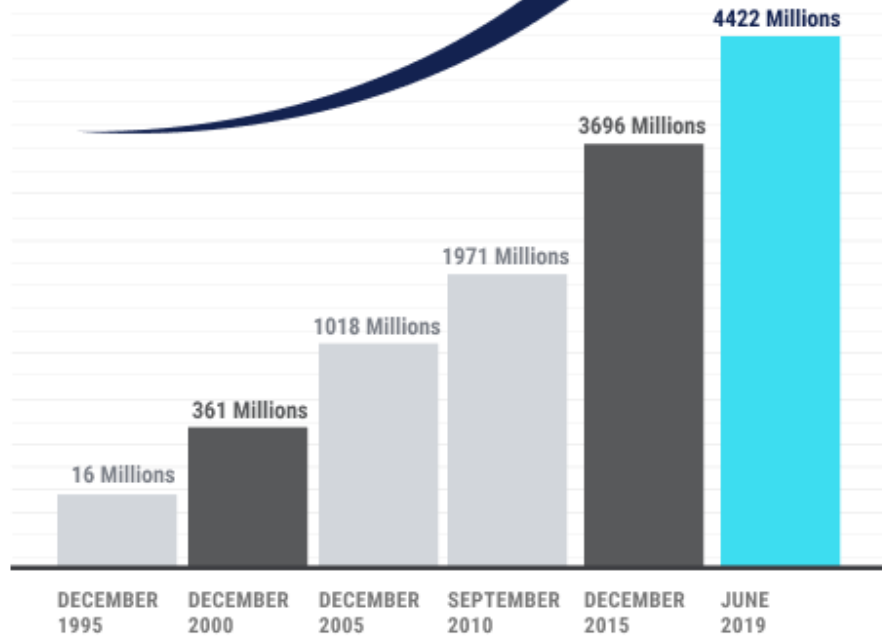


Πληθυσμιακή αποτύπωση στον χρόνο

ΠΗΓΗ : [HTTPS://WWW.WORLDOMETERS.INFO/WORLD-POPULATION/](https://www.worldometers.info/world-population/)

Internet Growth Statistics

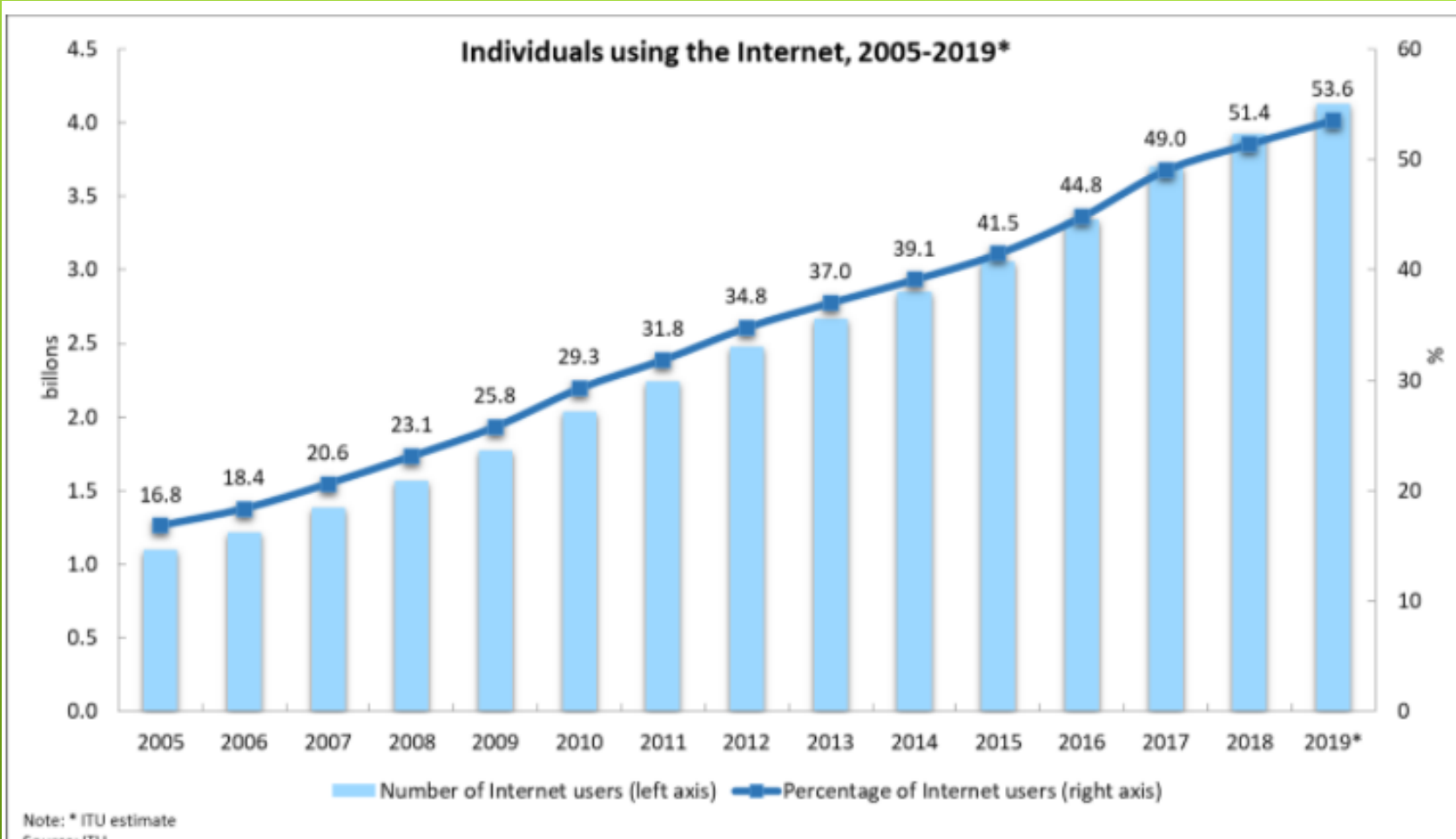
WORLD USERS (1995 TO 2019)



ΑΥΞΗΣΗ ΚΑΙ ΣΤΟΝ ΑΡΙΘΜΌ ΧΡΗΣΤΩΝ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ



Τεχνολογική ανισότητα



ΝΕΟΤΕΡΑ ΣΤΟΙΧΕΙΑ 53,6 %

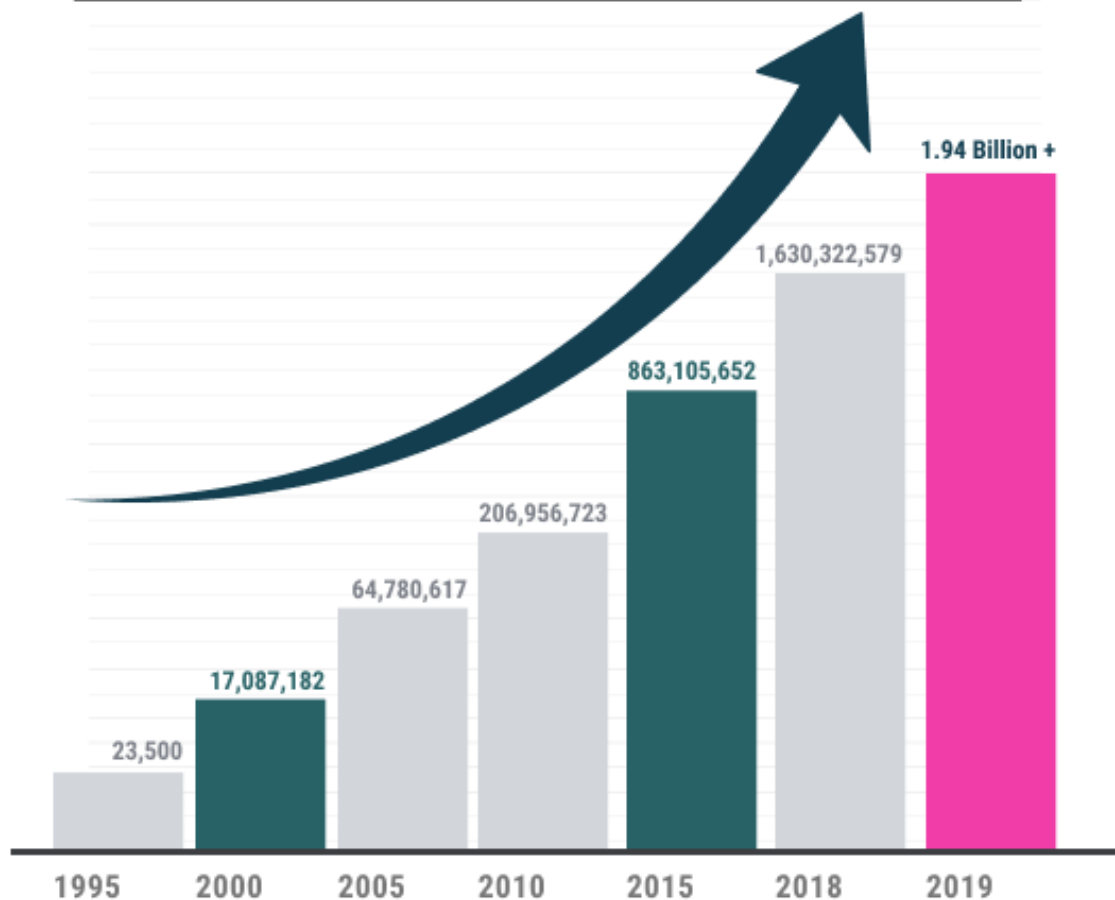


Χρήση κινητών συσκευών

Τεχνολογική ανισότητα ≤ κοινωνική ανισότητα

ΑΥΞΗΣΗ ΚΑΙ ΣΤΟΝ ΑΡΙΘΜΌ ΤΩΝ ΔΙΚΤΥΑΚΏΝ ΤΌΠΩΝ

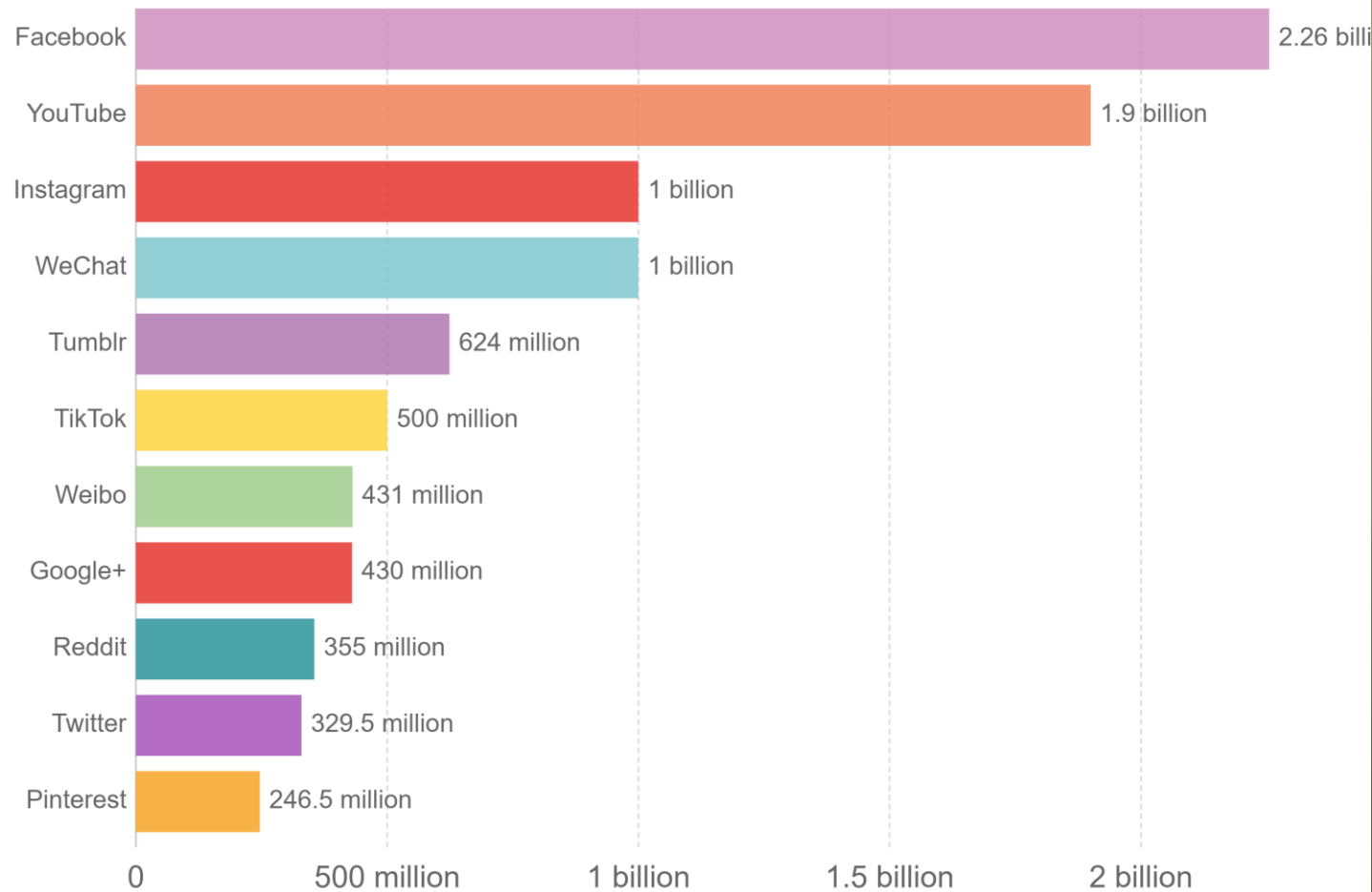
Total Number Of Websites (1995 to 2018)



Κάποιοι από τους
δικτυακούς τόπους
σχετίζονται με θέματα
παιδείας

Number of people using social media platforms, 2018

Estimates correspond to monthly active users (MAUs). Facebook, for example, measures MAUs as users that have logged in during the past 30 days. See source for more details.



Source: Statista and TNW (2019)

ΣΥΜΜΕΤΟΧΉ ΣΤΑ SOCIAL MEDIA

Πάνω από έξι (6)
εκατομμύρια χρήστες στο
Facebook μόνο στην
Ελλάδα
Και πάνω από 2,5 δις όλοι
οι χρήστες σήμερα

Πηγή:

<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

SURFACE WEB

Google
Bing Wikipedia

DEEP WEB

Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.

Academic Information
Medical Records
Legal Documents
Scientific Reports
Subscription Information
Social Media
(DARK WEB)

Multilingual Databases
Financial Records
Government Resources
Competitor Websites
Organization-specific Repositories

A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. Deep Web Technologies has zero involvement with the Dark Web.

Illegal Information
TOR-Encrypted sites
Political Protests
Drug Trafficking sites
Private Communications

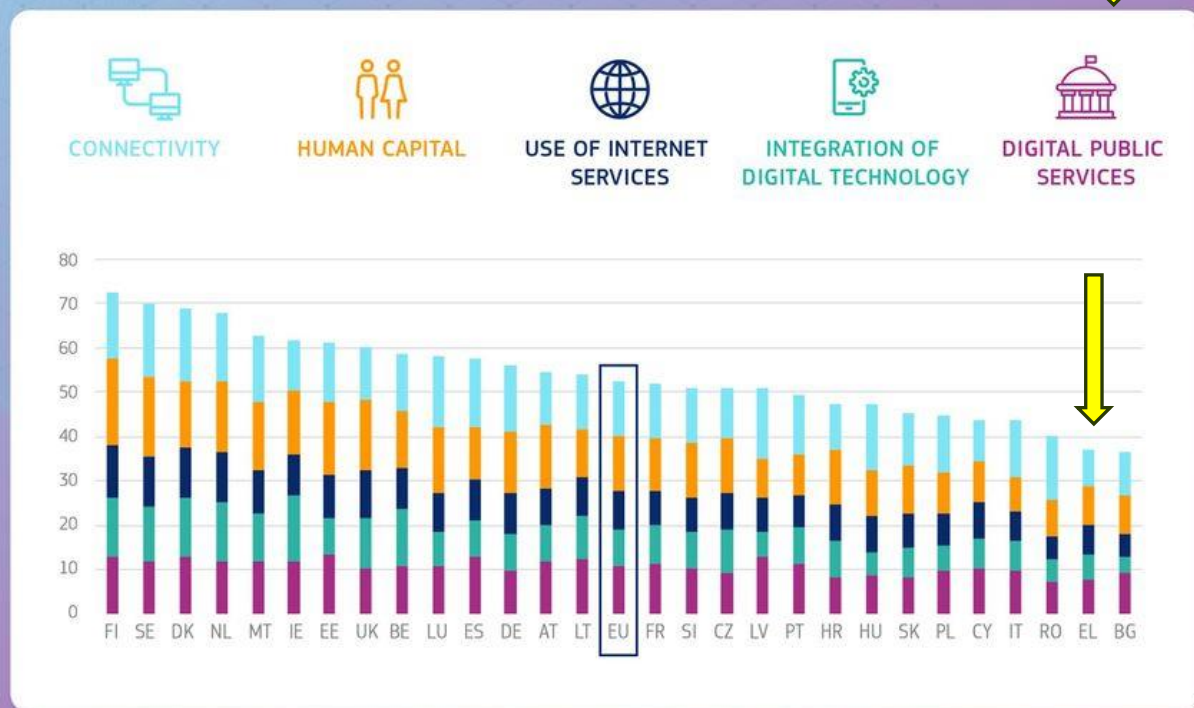
...!ΟΠΩΣ 'ΕΝΑ
ΠΑΓΟΒΟΥΝΟ!!!

Πηγη:

<http://www.thesydneyjournalist.com/wp-content/uploads/2017/08/Dark-Web-Infographic-by-Deep-Web-Tech.jpg>

DESI 2020

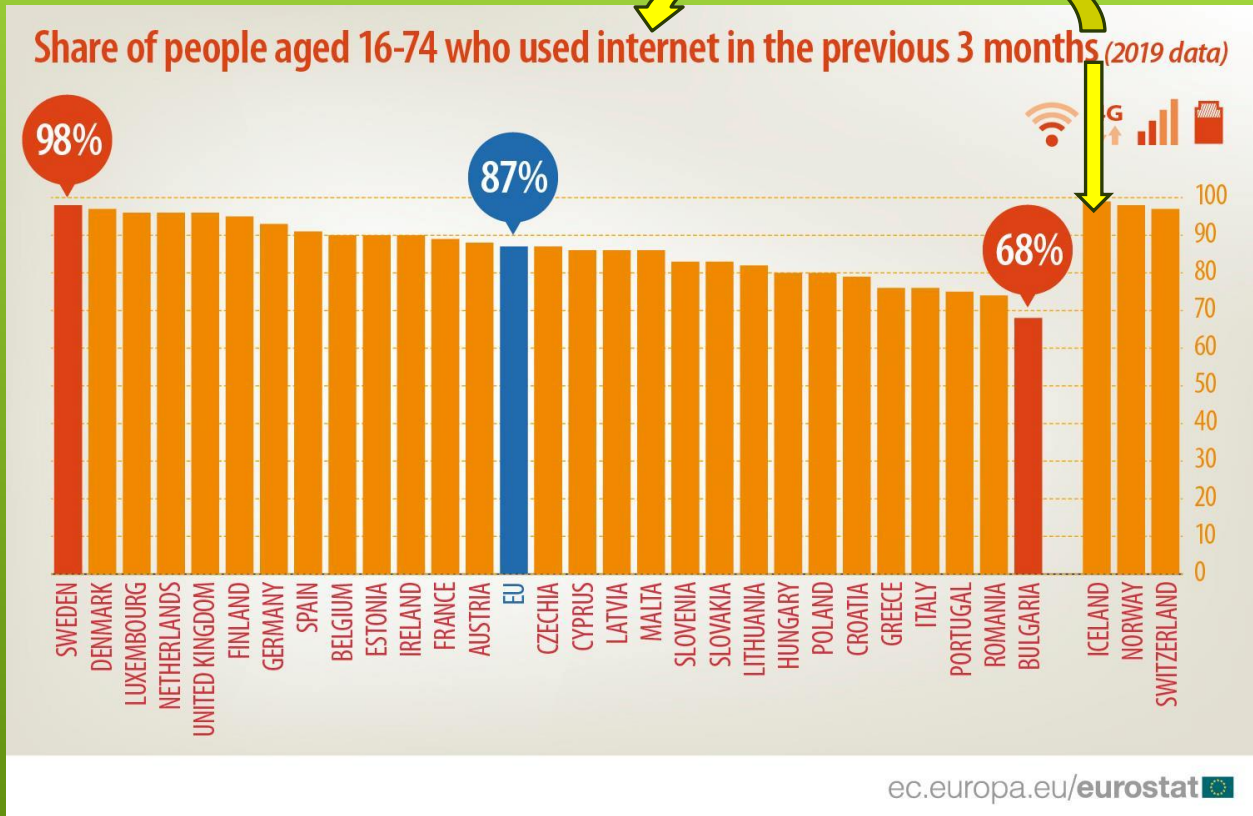
Digital Economy and Society Index



#DESleu #DigitalEU

ΨΗΦΙΑΚΗ ΣΥΓΚΛΙΣΗ Η ΑΠΟΚΛΙΣΗ

ΈΧΟΥΜΕ ΠΟΛΥ
ΔΡΟΜΟΜΠΡΟΣΤΑ ΜΑΣ ...
ΓΙΑ ΝΑ ΦΤΑΣΟΥΜΕ ΤΟΝ
ΜΕΣΟ ΟΡΟ

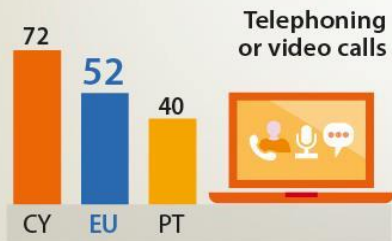
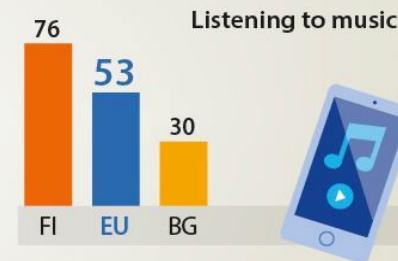
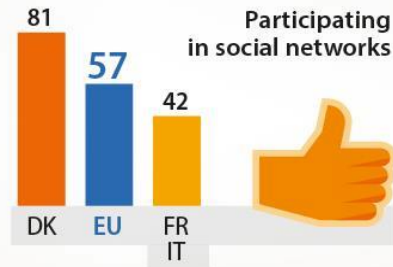
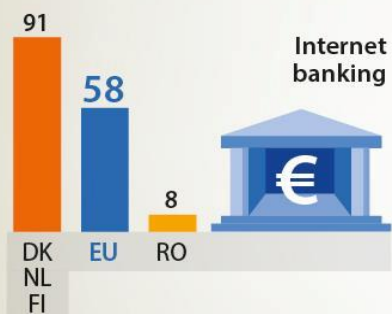
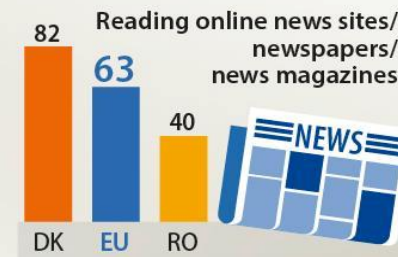
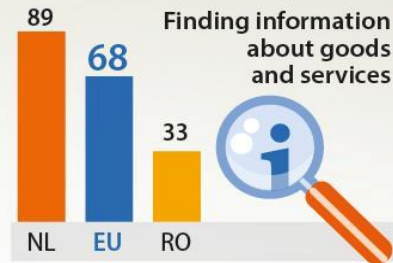
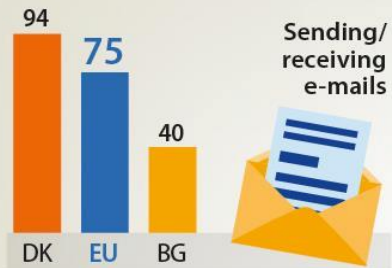


ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΣΕ ΕΠΊΠΕΔΟ ΕΕ

ΈΧΟΥΜΕ ΔΡΌΜΟ...
ΓΙΑ ΝΑ ΦΤΆΣΟΥΜΕ
ΤΟΝ Μ'ΕΣΟ ΌΡΟ

Η ΔΙΑΔΙΚΤΥΑΚΗ ΚΑΘΗΜΕΡΙΝΟΤΗΤΑ ΣΕ ΕΠΪΠΕΔΟ ΕΕ

Internet activities in the EU (% of people aged 16-74, 2019 data)



Annex B: Global ranking GCI 2018

The countries marked with an * are countries that did not participate in GCI 2018. They have neither submitted their answers to the questionnaire nor validated the data collected by the GCI team.

Member State	Score	Global Rank
United Kingdom	0.931	1
United States of America*	0.926	2
France	0.918	3
Lithuania	0.908	4
Estonia	0.905	5
Singapore	0.898	6
Spain	0.896	7
Malaysia	0.893	8
Canada*	0.892	9
Norway	0.892	9
Australia	0.890	10
Luxembourg	0.886	11
Netherlands	0.885	12
Saudi Arabia	0.881	13
Japan	0.880	14
Mauritius	0.880	14
Republic of Korea	0.873	15

GLOBAL CYBERSECURITY INDEX (GCI) 2018

ΠΗΓΗ: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf p.62

GLOBAL CYBERSECURITY INDEX (GCI) 2018

Member State	Score	Regional Rank	Global Rank
Israel*	0.783	24	39
Portugal	0.758	25	42
Monaco	0.751	26	43
Latvia	0.748	27	44
Slovakia	0.729	28	45
Bulgaria*	0.721	29	46
Slovenia*	0.701	30	48
Moldova	0.662	31	53
Ukraine	0.661	32	54
Cyprus*	0.652	33	56
Serbia	0.643	34	58
Montenegro	0.639	35	61
Albania	0.631	36	62
Czech Republic	0.569	37	71
Romania	0.568	38	72
Liechtenstein	0.543	39	75
Greece	0.527	40	77
Malta	0.479	41	82
Iceland	0.449	42	87
Bosnia and Herzegovina	0.204	43	118
Andorra	0.115	44	143
San Marino*	0.075	45	154

Στην 77^η θέση η
Ελλάδα

ΠΗΓΗ: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf p.64

ΑΛΛΑΓΕΣ ΣΤΗΝ ΚΑΘΗΜΕΡΙΝΟΤΗΤΑ ΜΑΣ ΚΑΙ ΣΤΟ ΠΑΡΑΓΩΓΙΚΟ ΜΟΝΤΕΛΟ

Τηλεργασία



Τηλεκπαίδευση

Περισσότερο διαθέσιμος χρόνος στο σπίτι

ΠΟΙΑ ΘΈΜΑΤΑ ΚΥΒΕΡΝΟΑΣΦΆΛΕΙΑΣ ΑΝΑΔΕΪΧΘΗΚΑΝ ΣΤΗΝ COVID 19 ΕΠΟΧΉ;

Ιδιωτικότητα

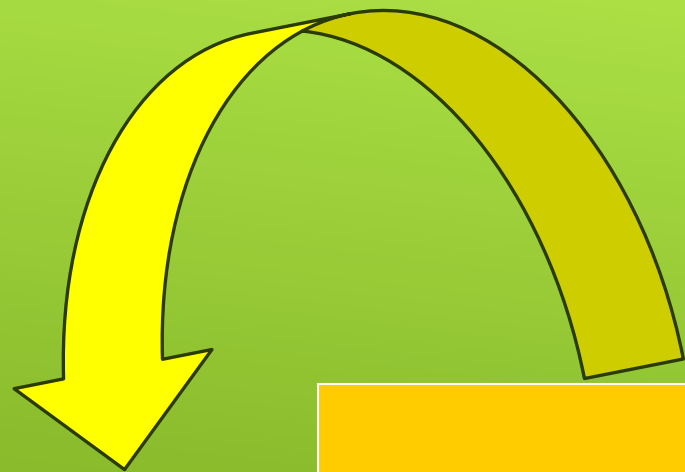
Κυβερνοεγκλήματα

**Fake news
Ρητορική Μίσους**

Προστασία κρίσιμων υποδομών

ΘΈΜΑΤΑ ΙΔΙΩΤΙΚΌΤΗΤΑΣ (PRIVACY)

- ▶ Τι είναι προσωπικά δεδομένα
- ▶ Τι είναι ευαίσθητα προσωπικά δεδομένα
- ▶ Γιατί τα προσωπικά δεδομένα είναι σημαντικά;



«ΌΤΙ ΕΙΝΑΙ ΔΙΚΟ ΜΟΥ»

Απάντηση μαθητή δημοτικού σε
ερώτηση του ομιλούντος
11/2/2020 σε εκδήλωση του
NOESIS

**Προσωπικά δεδομένα
(personal data)
είναι κάθε πληροφορία
που αναφέρεται και περιγράφει
ένα άτομο**



Ευαίσθητα δεδομένα (sensitive data)
είναι τα δεδομένα που αφορούν:

- φυλετική ή εθνική προέλευση,
- πολιτικά φρονήματα,
- θρησκευτικές ή φιλοσοφικές πεποιθήσεις,
- συμμετοχή σε ένωση,
- σωματείο και συνδικαλιστική οργάνωση,
- υγεία,
- κοινωνική πρόνοια,
- ερωτική ζωή,
- ποινικές διώξεις και καταδίκες

ΠΡΟΣΤΑΣΙΑ ΚΡΪΣΙΜΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



ΚΥΒΕΡΝΟ-ΕΓΚΛΗΜΑ ΚΡΙΜΑ-ΚΥΒΕΡΝΗΤΗΣ

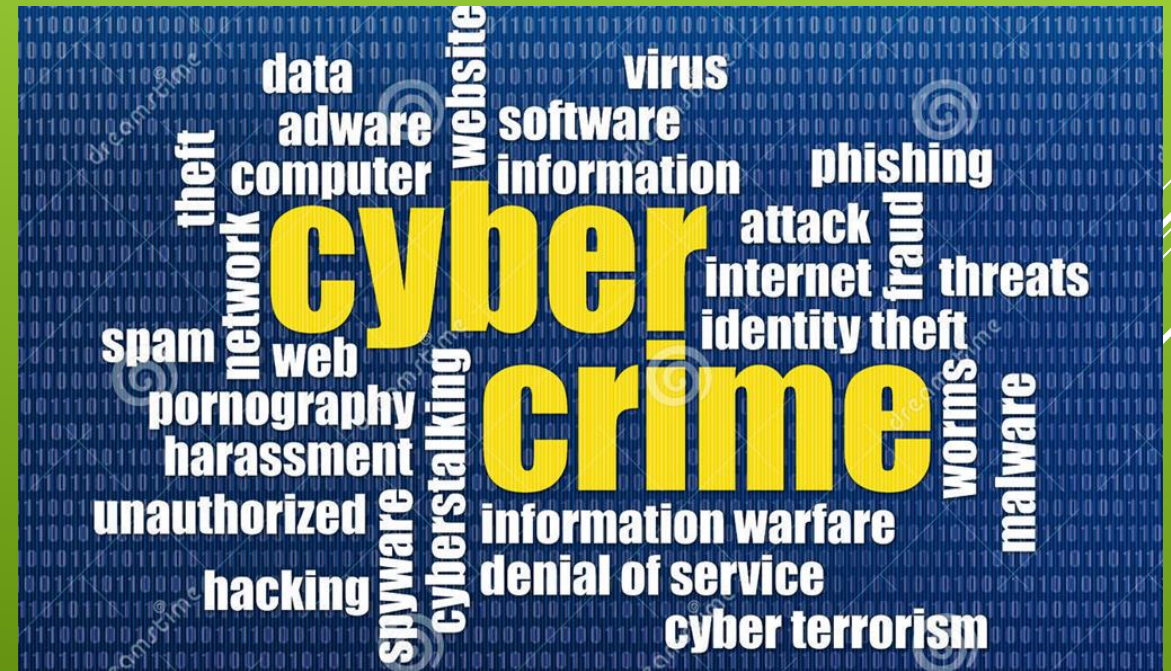
Κι όχι ηλεκτρονικό!!!!

Cybercrime (etymology)

116 Συνέκδικος Ἱερατικός.
τοῦ διαβόλου. Κρίμα σημαίνει τὸ αὐτὸ καὶ Κρίσις (judgement,) οἷον "Τα κρίματά σου ὡσεὶ ἄβυσσος πολλή" 1) "Κρίματα, ψῆφοι, δικαί" κατὰ τὸν Ἡσύχιον. Σημαίνει ἀκρίβη καὶ τὸ Κατάκριμα 2) ἡγουν τὴν Καταδίκην (condamnation) "Κρίμα, τὸ κατάκριμα καὶ ἡ καταδίκη, ὡς τὸ Κρίμα ἐαυτῶ ἐσθίει καὶ πίνει κ. τ. λ." 3) Λέγει καὶ ὁ Ἡσύχιος "Κρίμα, ἀνταπόδοσις Θεοῦ." Καὶ τρίτον, αὐτὸ τὸ κρινόμενον ἐγκλημα ἢ ἀμαρτήμα, λέγεται Κρίμα, ὅθεν οἱ Ῥωμαῖοι ἔλαβαν τὸ Crimen (crime,) ὀνομαζόντες οὕτως τὴν ἐγκληματικὴν τῶν πολιτικῶν νόμων παράβασιν, ὡς ἡμεῖς σήμερον ἰνομάζομεν (εἰς θρησκικὴν σημασίαν) Κρίμα (péché) τὴν παράβασιν τῶν ἐντολῶν τοῦ Θεοῦ, τὴν συνανύμην λεγομένην

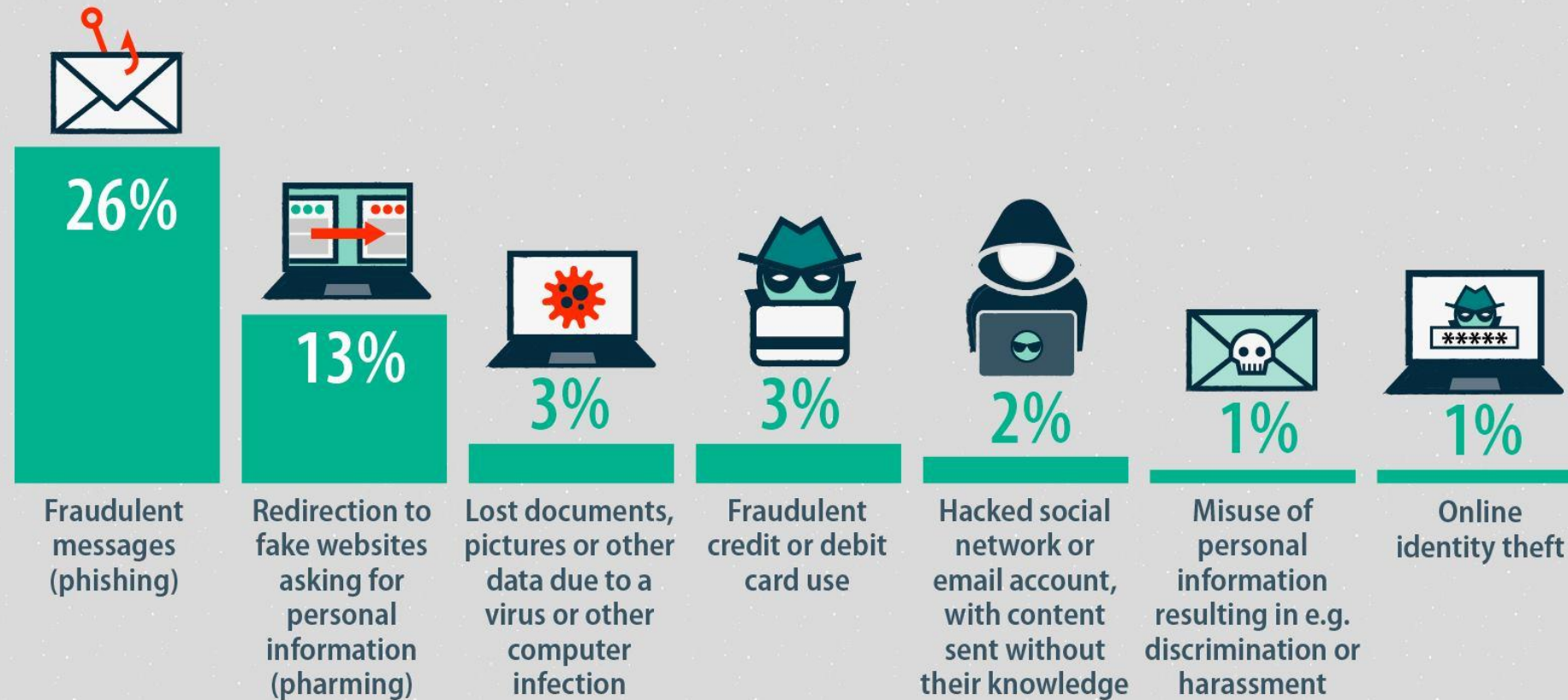


κυβερνήτης
kybernetes
governor of a ship (captain)



ΠΕΡΙΟΧΕΣ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Security related problems experienced through private internet use
in the last 12 months *(% of individuals aged 16 to 74, 2019)*



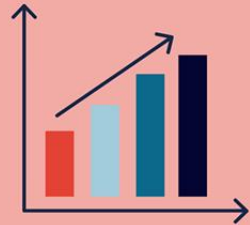
'ΕΓΚΥΡΗ ΠΛΗΡΟΦ'ΟΡΗΣΗ ΑΠΟΦΕΥΓΟΝΤΑΣ ΤΗΝ ΠΑΡΑΠΛΗΡΟΦ'ΟΡΗΣΗ

MISINFORMATION

[n.] /ˌmɪs.ɪn.fəˈmeɪ.ʃən/

false or inaccurate information, usually **not** created or shared with harmful intent

Example: Sharing a news story with inaccurate statistics or out-of-date information



DISINFORMATION

[n.] /ˌdɪs.ɪn.fəˈmeɪ.ʃən/

false or inaccurate information deliberately created and shared **to cause harm**

Example: Making up a quote from a public figure

MALINFORMATION

[n.] /ˌmæl.ɪn.fəˈmeɪ.ʃən/

true or accurate information (based in reality) shared or manipulated with the intent **to cause harm**

Example: Sharing private data, statistics, or images publicly



A E AMERICAN ENGLISH

FAKE NEWS

COVID-19 DISINFORMATION CAN ENDANGER PEOPLE'S LIVES



The infographic illustrates the cycle of fake news. It shows three people holding up signs that say "Fake products and services", "False mitigation and cures", and "Mistrust in official guidelines". A central banner says "BREAK THE CHAIN" with a red 'X' over it. Below this, three circular icons represent "SPOT THE FAKE" (with a magnifying glass over a document), "DO NOT ENGAGE" (with a red 'X' over a smartphone), and "REPORT IT" (with a speech bubble saying "FAKE NEWS"). At the bottom, a large exclamation mark is followed by the text "Share information from official sources only". The logo for "EUROPOL EC3 European Cybercrime Centre" is in the bottom right corner.

MAKE YOUR HOME A CYBER SAFE STRONGHOLD



Wi-Fi: always change the default router password



Install antivirus software on all devices connected to the internet



Review your apps' permissions and delete those you don't use



Choose strong and different passwords for your email and social media accounts



Back up your data and run regular software updates



Secure electronic devices with passwords, PIN or biometric information



Review the privacy settings of your social media accounts

Online shopping safety tips

Buy from **reliable** online vendors and check individual ratings

Think twice: if an offer sounds too good to be true, it probably is

Use **credit cards** when shopping online for stronger customer protection

Check your bank account often for **suspicious activity**



ΤΟ ΣΠΙΤΙ ΜΑΣ ΠΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΣ

ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΤΗΝ ΚΑΘΗΜΕΡΙΝΟΤΗΤΑ ΜΑΣ

CYBER SAFETY CHECKLIST


Back up online and offline files regularly and securely



Strengthen your home network


Use strong passwords


Keep your software updated


Manage social media profiles


Check privacy and security settings


Avoid opening and delete suspicious emails or attachments



INTERPOL

BE VIGILANT . BE SKEPTICAL . BE SAFE

ΛΙΣΤΑ
ΕΝΕΡΓΕΙΩΝ



Cyber safety with children

- Change the default factory **password** and keep software up-to-date
- Check the **security** and **privacy** settings of smart toys
- Use **parental controls** to safeguard your child's online activity
- Talk to your child about cyber safety. **Listen** to their online experiences and **explain** to them the importance of being just as safe online as offline

REMEMBER
Follow trusted sources for up-to-date factual information. If you become a victim of cybercrime, always report it to your national police.

ΜΕΝΟΥΜΕ
ΑΣΦΑΛΕΙΣ
ΔΕΝ ΜΕΝΟΥΜΕ
ΣΙΩΠΗΛΟΙ

ΕΧΕΙΣ
ΦΩΝΗ
ΕΙΜΑΣΤΕ
ΔΙΠΛΑ ΣΟΥ

#exeisfoni
#menoumeasfaleis

ΚΑΛΕΣΕ ή ΣΤΕΙΛΕ
SMS ΣΤΟ 100
www.yptp.gr
www.hellenicpolice.gr

Μάθε πώς να
προστατευτείς
εδώ



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη



Οδηγίες προς τους πολίτες για την προστασία ανηλίκων στο διαδίκτυο



✓ Δίνουμε το σωστό παράδειγμα με τη δική μας διαδικτυακή συμπεριφορά.



✓ Συζητάμε για τη διαδικτυακή ζωή και τα ενδιαφέροντα του παιδιού όπως κάνουμε και για την πραγματική.



✓ Ελέγχουμε μαζί τις ρυθμίσεις απορρήτου και ασφάλειας των λογαριασμών του (διπλός έλεγχος ταυτότητας / two step verification, σύνθετος κωδικός πρόσβασης)



✓ Κάνουμε μια ανασκόπηση της λίστας των φίλων του παιδιού στα μέσα κοινωνικής δικτύωσης, στα διαδικτυακά παιχνίδια και τις εφαρμογές.



✓ Συζητάμε με τα παιδιά για τους κινδύνους της έκθεσης των προσωπικών δεδομένων και φωτογραφιών (άσεων και μη) στο διαδίκτυο.



✓ Συμβουλεύουμε το παιδί να αποφεύγει το άνοιγμα οποιουδήποτε συνδέσμου (link) αγνώστου προελεύσεως.



✓ Εγκαθιστούμε εφαρμογή γονικού ελέγχου, που μπορεί να βοηθήσει τα παιδιά να πλοηγηθούν με ασφάλεια στο διαδίκτυο και τους γονείς να ελέγξουν το περιεχόμενο των ιστοσελίδων που επισκέπτονται.



✓ Αν αντιληφθούμε οποιοδήποτε πρόβλημα παραμένουμε ψύχραιμοι, ακούμε όλη την ιστορία χωρίς να διακόψουμε το παιδί, διαφυλάσσουμε τα όποια αποδεικτικά στοιχεία (screenshots φωτογραφιών / μηνυμάτων), αναφέρουμε το περιστατικό στις Αρχές και ζητάμε τη βοήθεια των ειδικών.

Ενημερωθείτε για θέματα ασφαλούς πλοήγησης στο διαδίκτυο και διαβάστε περισσότερες συμβουλές για γονείς και νέους στο www.cyberkid.gov.gr. Σε περίπτωση ανάγκης ή οποιασδήποτε παραβατικής συμπεριφοράς μέσω διαδικτύου, επικοινωνήστε με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στο 11188 ή στέλνοντας email στο ccu@cybercrimeunit.gov.gr

ΜΕΝΟΥΜΕ
ΑΣΦΑΛΕΙΣ
ΔΕΝ ΜΕΝΟΥΜΕ
ΣΙΩΠΗΛΟΙ

ΕΧΕΙΣ
ΦΩΝΗ
ΕΙΜΑΣΤΕ
ΔΙΠΛΑ ΣΟΥ

#exeisfoni
#menoumeasfaleis

ΚΑΛΕΣΕ ή ΣΤΕΙΛΕ
SMS ΣΤΟ 100
www.yptp.gr
www.hellenicpolice.gr

Μάθε πώς να
προστατευτείς
εδώ



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη



Οδηγίες προς ανηλίκους για την προστασία στο διαδίκτυο



✓ Τήρησε στο διαδίκτυο τους κανόνες που τηρείς και στην πραγματική ζωή.



✓ Μοιράσου τα διαδικτυακά ενδιαφέροντά σου με τους γονείς σου.



✓ Έλεγξε τις ρυθμίσεις απορρήτου και ασφάλειας των λογαριασμών σου (διπλός έλεγχος ταυτότητας / two step verification, σύνθετος κωδικός πρόσβασης).



✓ Απόφυγε την ανάρτηση ή αποστολή προσωπικών στοιχείων και φωτογραφιών στους λογαριασμούς σου όπως ονοματεπώνυμο, διεύθυνση, τηλέφωνο, σχολείο, φωτογραφίες δικές σου ή των συμμαθητών σου.



✓ Μην ανοίγεις μηνύματα/e-mail ή link από αγνώστους.



✓ Τσέκαρε ξανά τους φίλους που έχεις στους λογαριασμούς σου. Τους γνωρίζεις και στην πραγματική ζωή;



✓ Απόφυγε τις συνομιλίες με αγνώστους και μην ανοίγεις ποτέ την κάμερα. Οι κακόβουλοι χρήστες προσπαθούν να κερδίσουν την εμπιστοσύνη σου, δείχνοντας πάντα συμπαθητικοί και διαθέσιμοι.



✓ Ειδοποίησε αμέσως τους γονείς σου αν κάποιος χρήστης σε κάνει να αισθάνεσαι άβολα σε μια συνομιλία, καθώς και όταν σου ζητήσει να του στείλεις φωτογραφία σου ή να συναντηθείς μαζί του.



✓ Θυμήσου: αν σου συμβεί κάτι που σε φέρνει σε δύσκολη θέση στο διαδίκτυο πρέπει να το πεις και όχι να το υποστείς. Συζήτησέ το με κάποιον ενήλικο που εμπιστεύεσαι, δείχνοντας θάρρος και αποθήκευσε τα όποια αποδεικτικά στοιχεία έχεις στη διάθεσή σου (screenshot φωτογραφιών/ μηνυμάτων).

Μάθε περισσότερα για την ασφαλή πλοήγηση στο www.cyberkid.gov.gr ή κατεβάζοντας την εφαρμογή Cyberkid. Σε περίπτωση ανάγκης, επικοινωνήσε με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στο 11188 ή στέλνοντας email στο ccu@cybercrimeunit.gov.gr

safe@home

ΟΔΗΓΟΣ ΑΣΦΑΛΟΥΣ ΤΗΛΕΡΓΑΣΙΑΣ
από την Ε.Α.Δ. και την ΕΛ.ΑΣ. / ΔΙ.Δ.Η.Ε.

**Μένουμε σπίτι.
Εργαζόμαστε με ασφάλεια.**



Για εργαζόμενους

- Χρησιμοποιείτε τις προσωπικές σας συσκευές ή τις συσκευές που σας παρέχει η εταιρεία / ο φορέας σας. Σε κάθε περίπτωση, σιγουρευτείτε ότι το λειτουργικό σύστημα και οι εφαρμογές σας είναι ενημερωμένες, ότι έχετε εγκαταστήσει τα κατάλληλα αντικά προγράμματα και ότι η σύνδεση σας στο διαδίκτυο είναι ασφαλής.
- Αποφεύγετε να κάνετε προσωπική χρήση τυχόν εξοπλισμού που σας έχει παρασχεθεί από την εταιρεία / τον φορέα σας στο πλαίσιο της Τηλεργασίας.
- Στην περίπτωση που η εταιρεία / ο φορέας σας, σας έχει προμηθεύσει με σχετικό εξοπλισμό (π.χ. φορητό Η/Υ), μην αφήνετε τα μέλη της οικογένειάς σας να αποκτούν πρόσβαση σε αυτόν. Κλειδώνετε ή απενεργοποιείτε τον εξοπλισμό, όταν δεν είστε παρόντες και κρατάτε τον σε ασφαλή τοποθεσία για να αποτρέψετε τυχόν απώλεια, βλάβη από άσκοπη χρήση ή κλοπή.
- Χρησιμοποιείτε δυνατούς κωδικούς (αν είναι εφικτό password managers ή two-step verification).
- Πριν ξεκινήσετε να δουλεύετε μέσω Τηλεργασίας εξοικειωθείτε με τις εταιρικές / υπηρεσιακές διαδικασίες και πολιτικές.
- Στην περίπτωση που χρειαστεί να συνδεθείτε με το εταιρικό δίκτυο ή το εσωτερικό δίκτυο του φορέα σας να χρησιμοποιείτε, εφόσον υπάρχει τέτοια δυνατότητα, VPN, σύμφωνα με τις οδηγίες που θα σας παράσχει το εξειδικευμένο προσωπικό της εταιρείας / του φορέα σας.
- Εάν εντοπίσετε ασυνήθιστη ή ύποπτη δραστηριότητα σε οποιαδήποτε συσκευή χρησιμοποιείτε για την Τηλεργασία, επικοινωνήστε άμεσα με την εταιρεία / τον φορέα σας μέσω των ενδεδειγμένων καναλιών.
- Μείνετε σε επαγρύπνηση για οποιαδήποτε ύποπτη δραστηριότητα, ειδικά για αιτήματα που αφορούν οικονομικές συναλλαγές ακόμα και εάν φαίνονται να προέρχονται από άτομα που γνωρίζετε. Αυτό μπορεί να αποτελεί μία ακόμα περίπτωση κυβερνοαπάτης (cyberfraud). Επαληθεύετε και διασταυρώνετε οποιοδήποτε παρόμοιο μήνυμα / αίτημα.
- Μην ανοίγετε συνδέσμους ή επισυναπτόμενα αρχεία που λαμβάνετε από μηνύματα ηλεκτρονικού ταχυδρομείου από αποστολείς που δεν γνωρίζετε.
- Μην δίνετε προσωπικές πληροφορίες ή κωδικούς πρόσβασης, ακόμα και εάν φαίνεται με την πρώτη ματιά, να σας τα ζητούν νόμιμες εταιρείες / γνωστοί εθνικοί ή διεθνείς φορείς. Κανένας δημόσιος Οργανισμός (Ε.Ο.Δ.Υ., Υπουργείο Υγείας, Ο.Α.Ε.Δ., Παγκόσμιος Οργανισμός Υγείας κ.α.) ή ιδιωτικός φορέας (τράπεζες, τηλεπικοινωνιακοί πάροχοι κ.α.) δεν πρόκειται να σας ζητήσει ποτέ προσωπικούς κωδικούς πρόσβασης.
- Επαληθεύετε και διασταυρώνετε με οποιονδήποτε πρόσφορο τρόπο τη γνησιότητα των ηλεκτρονικών μηνυμάτων που λαμβάνετε και σας ζητούν να κλικάρετε ηλεκτρονικούς συνδέσμους (links) ή να μοιραστείτε κωδικούς πρόσβασης και άλλες προσωπικές σας πληροφορίες.
- Δημιουργήστε συγκεκριμένο πλάνο συνεργασίας με τα υπόλοιπα μέλη των ομάδων εργασίας για την περίοδο που θα δουλεύετε μέσω Τηλεργασίας, όπως τον τρόπο που θα ανατίθενται οι επιμέρους υποχρεώσεις για κάθε έργο / παραδοτέο, θα τηρούνται οι προθεσμίες, θα αξιολογείται η απόδοση και θα αξιολογούνται τα διαθέσιμα κανάλια επικοινωνίας.

ΚΑΘΗΜΕΡΙΝΟΤΗΤΑ ΕΡΓΑΖΟΜΕΝΩΝ

safe@home

ΟΔΗΓΟΣ ΑΣΦΑΛΟΥΣ ΤΗΛΕΡΓΑΣΙΑΣ
από την Ε.Α.Δ. και την ΕΛ.ΑΣ. / ΔΙ.Δ.Η.Ε.

Μένουμε σπίτι. Εργαζόμαστε με ασφάλεια.

Για εργοδότες

- Δημιουργήστε εσωτερικές πολιτικές και διαδικασίες και κάντε δοκιμές (tests) πριν τεθούν σε επιχειρησιακή λειτουργία. Είναι σημαντικό να έχετε ξεκάθαρες πολιτικές για την πρόσβαση σε εσωτερικές δομές / συστήματα καθώς και για το ποιος θα πρέπει να κληθεί σε περίπτωση προβλήματος. Δημιουργήστε ξεκάθαρες διαδικασίες για την αντιμετώπιση ενός περιστατικού ασφαλείας. Να λαμβάνετε επιπλέον μέτρα όταν πρόκειται για διαδικασία έγκρισης και υπογραφής εγγράφων από τη Διοίκηση.
- Λαμβάνετε περισσότερα μέτρα ασφαλείας, όπως ενδεικτικά, κρυπτογράφηση σκληρών δίσκων, αποσύνδεση ανενεργών χρηστών, προστασία ιδιωτικότητας οθόνης από τρίτους, ισχυρή αυθεντικοποίηση και έλεγχος των φορητών μέσων αποθήκευσης. Δημιουργήστε διαδικασίες εξ αποστάσεως απενεργοποίησης πρόσβασης σε συσκευές που χάθηκαν ή κλάπηκαν.
- Εφόσον τούτο είναι εφικτό, να επιτρέπετε στους εργαζόμενους σας να συνδέονται στο εσωτερικό δίκτυο μόνο μέσω του εταιρικού VPN με έλεγχο πολλαπλών παραγόντων. Βεβαιωθείτε ότι οι συνδέσεις με το εσωτερικό δίκτυο / συστήματα έχουν ρυθμιστεί και λήγουν αυτόματα μετά από μια περίοδο που ο χρήστης είναι ανενεργός, με απαίτηση νέας αυθεντικοποίησης για την εκ νέου σύνδεση.
- Διατηρείτε το λειτουργικό σύστημα και τις εφαρμογές των συσκευών ενημερωμένες μειώνοντας τις αδυναμίες των συστημάτων που θα μπορούσαν να εκμεταλλευτούν κακόβουλοι χρήστες.
- Ασφαλίστε τα κανάλια επικοινωνίας εφαρμόζοντας έλεγχο παραγόντων δύο σημείων για την είσοδο στους λογαριασμούς ηλεκτρονικού ταχυδρομείου των εργαζομένων σας.
- Εδραιώστε ασφαλείς επικοινωνίες μεταξύ των υπαλλήλων, αλλά και με εξωτερικούς συνεργάτες ή προμηθευτές.
- Ελέγχετε συχνά στο VPN για ασυνήθιστη δραστηριότητα χρηστών.
- Επικοινωνείτε τακτικά με το προσωπικό θέτοντας ρεαλιστικούς στόχους και χρονοδιαγράμματα, όπως και μηχανισμούς επιτήρησης αυτών, λαμβάνοντας υπόψη τις ιδιαίτερες καταστάσεις της εποχής.
- Ενημερώνετε - εκπαιδεύετε τους εργαζομένους σας για την πολιτική της Τηλεργασίας και τους κινδύνους από επιθέσεις στον κυβερνοχώρο και ειδικότερα για τη μέθοδο αλίευσης δεδομένων και κωδικών πρόσβασης τύπου "phishing", καθώς και για τη μέθοδο της κοινωνικής μηχανικής (social engineering).



ΚΑΘΗΜΕΡΙΝΟΤΗΤΑ ΕΡΓΟΔΟΤΩΝ

Να είστε σε επαγρύπνηση και μην:

⊗ Απαντάτε σε ύποπτα μηνύματα ή κλήσεις



⊗ Ανοίγεται συνδέσμους και συνημμένα σε ανεπιθύμητα μηνύματα



⊗ Μοιράζεστε τα τραπεζικά ή προσωπικά οικονομικά σας στοιχεία

⊗ Αγοράζετε από το διαδίκτυο πράγματα που φαίνεται να έχουν εξαντληθεί παντού



⊗ Μοιράζεστε ειδήσεις που δεν προέρχονται από επίσημες πηγές

⊗ Στέλνετε χρήματα προκαταβολικά σε κάποιον που δεν γνωρίζετε

⊗ Κάνετε δωρεές σε φιλανθρωπικές οργανώσεις χωρίς να ελέγχετε τη γνησιότητά τους



EURCPOL

ΚΑΘΗΜΕΡΙΝΟΤΗΤΑ ΚΑΤΑΝΑΛΩΤΩΝ

Συμβουλές ασφαλείας για διαδικτυακές αγορές

☰ Αγοράστε από **αξιόπιστους** πωλητές και ελέγξτε τις κριτικές

☰ Σκεφθείτε **διπλά**: αν μια προσφορά ακούγεται πολύ καλή για να είναι αληθινή, μάλλον είναι

☰ Χρησιμοποιήστε **πιστωτικές κάρτες** όταν κάνετε ηλεκτρονικές αγορές για μεγαλύτερη προστασία

☰ Να ελέγχετε συχνά τον τραπεζικό σας λογαριασμό για **ύποπτη δραστηριότητα**



YOU WON'T FIND A COVID-19 CURE ONLINE

EUROPOL

CRIMINALS ARE MAKING MONEY FROM THIS GLOBAL HEALTH CRISIS.

THOUSANDS OF WEBSITES CLAIM TO SELL COVID-19 CURES, TESTS OR VACCINES. **THEY ARE FAKE.**

UNAUTHORISED SELLERS ADVERTISE COUNTERFEIT FACE MASKS, VITAMINS AND DISINFECTANTS. **THEY ARE DANGEROUS.**

CRIMINALS PREY ON CONCERNED CITIZENS AND OFFER UNBRANDED MEDICAL PRODUCTS. **THEY ARE HARMFUL.**



ONLY RELY ON OFFICIAL GOVERNMENT SOURCES.



ONLY BUY FROM LICENSED SELLERS.



ONLY USE LEGITIMATE WEBSITES OFFERING SAFE PAYMENT OPTIONS.



ΚΑΘΗΜΕΡΙΝΟΤΗΤΑ ΚΑΤΑΝΑΛΩΤΩΝ

ΓΝΗΣΙΟΤΗΤΑ ΙΣΤΟΣΕΛΪΔΩΝ ΚΑΙ ΠΡΟΦΪΛ ΦΟΡΈΩΝ ΚΑΙ ΟΡΓΑΝΙΣΜΏΝ ΣΤΑ SOCIAL MEDIA



facebook



REMOTE ACCESS TROJANS (RAT)

EUROPOL
EC3
European Cybercrime Centre



A CYBERCRIME TOOL TO GAIN UNLIMITED ACCESS TO YOUR COMPUTER

Once installed, a RAT will allow cybercriminals to watch and listen through the camera and microphone, record all your on-screen activity, alter your personal files and use your device to distribute malware to other computers.



BE AWARE OF THE RAT – INFECTION SIGNS



Your internet connection is unusually slow



Unknown processes are running in your system (visible in the Task Manager, Processes tab)



Your files are modified or deleted without your permission



Unknown programs are installed on your device (visible in the Control Panel, Add or Remove Programs)

PROTECT YOURSELF



Ensure that your security software and operating system are up to date



Regularly back-up your data



Ensure that your device's firewall (if available) is active



Be wary while browsing the internet and do not click on suspicious links, pop ups or dialogue boxes



Only download apps and software from sources you can trust



Keep your web browser up to date and configured to alert you whenever a new window is opened or anything is downloaded



Cover your webcam when not in use



Do not click on links or attachments within unexpected or suspicious emails

INFECTED? WHAT TO DO NEXT



Disconnect your device from the network as soon as possible, in order to prevent additional malicious activity



Once you think that the infection has been removed, change the passwords for your online accounts and check your banking activity. Report anything unusual to your bank and, as needed, to your local law enforcement authorities



Install security software from a trustworthy source



Run a full scan of your device and remove the threats by using security software



Learn how to protect your computer from future infections and avoid data loss

Created by Europol

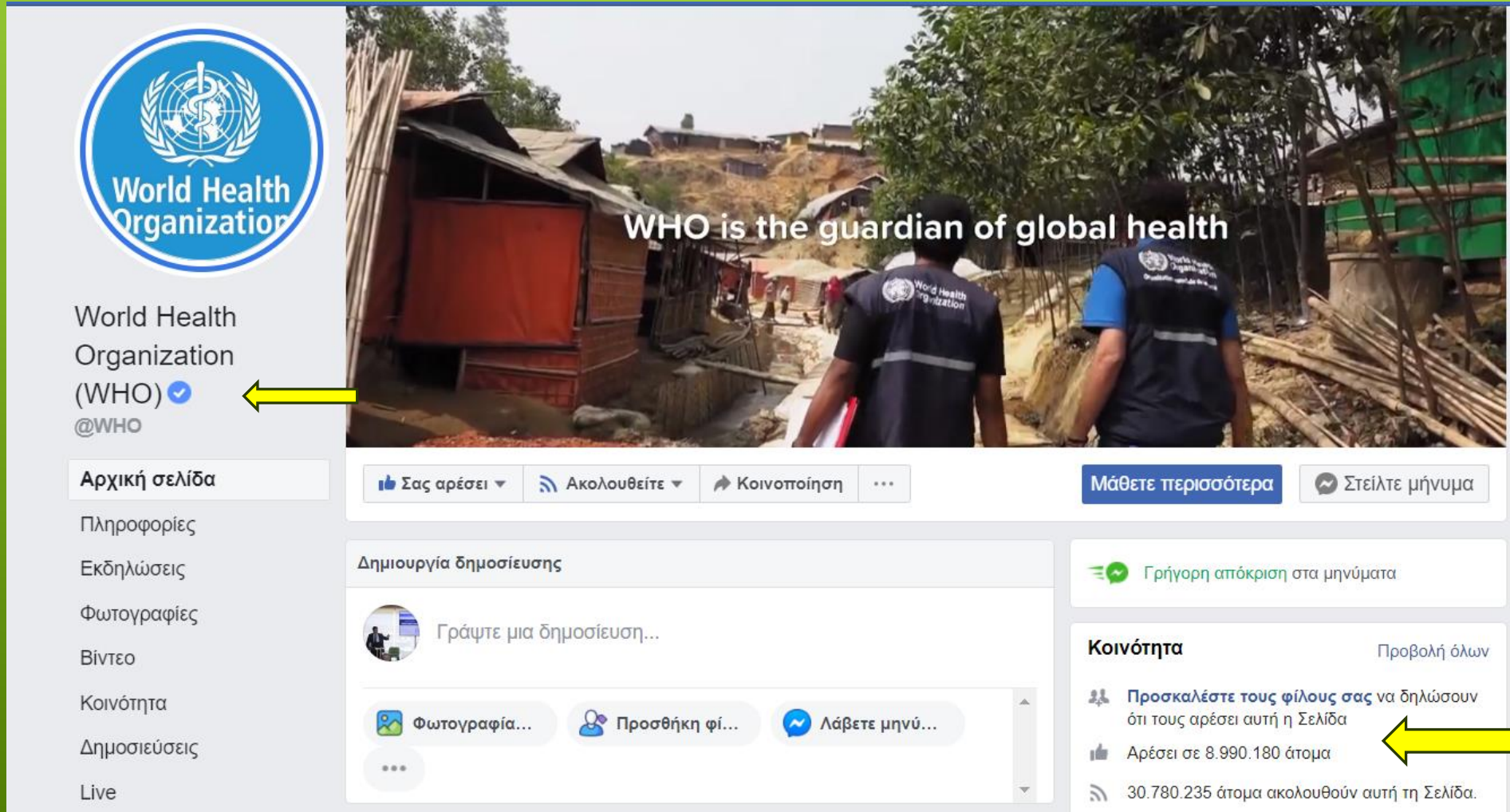
ΠΡΟΓΡΑΜΜΑΤΑ ΠΟΥ ΕΓΚΑΘΙΣΤΟΎΜΕ ΣΤΙΣ ΣΥΣΚΕΥΈΣ ΜΑΣ



NO MORE RANSOM!

www.nomoreransom.org

ΕΓΚΥΡΗ ΠΛΗΡΟΦΟΡΗΣΗ ΑΠΟΦΕΥΓΟΝΤΑΣ ΤΗΝ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗ



The image shows a screenshot of the World Health Organization's (WHO) Facebook page. The page header features the WHO logo and the text "World Health Organization (WHO) @WHO". A yellow arrow points to the page name. The main content is a post with a video thumbnail showing two WHO staff members in a rural setting, with the text "WHO is the guardian of global health". Below the post are interaction buttons for likes, follows, and shares. The right sidebar shows the page's community statistics, including a yellow arrow pointing to the follower count of 8,990,180.

World Health Organization (WHO) @WHO

Αρχική σελίδα

Πληροφορίες

Εκδηλώσεις

Φωτογραφίες

Βίντεο

Κοινότητα

Δημοσιεύσεις

Live

WHO is the guardian of global health

Σας αρέσει ▾ Ακολουθείτε ▾ Κοινοποίηση ...

Μάθετε περισσότερα Στείλτε μήνυμα

Γρήγορη απάντηση στα μηνύματα

Κοινότητα Προβολή όλων

Προσκαλέστε τους φίλους σας να δηλώσουν ότι τους αρέσει αυτή η Σελίδα

Αρέσει σε 8.990.180 άτομα

30.780.235 άτομα ακολουθούν αυτή τη Σελίδα.

ΔΙΚΑΙΩΜΑΤΑ ΜΑΣ ΚΑΙ ΑΝΕΞΑΡΤΗΤΕΣ ΑΡΧΕΣ



Αρχή

Ετήσιες Εκθέσεις

Επικαιρότητα

Νομοθεσία

Τα δικαιώματά μου

Οδηγίες για υπεύθυνους επεξεργασίας

Επικοινωνία

Hellenic Data Protection Authority

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Εγγραφή - Είσοδος μελών

Username:

Password:

εγγραφή login

Τα δικαιώματά μου>> Τα δικαιώματά μου στο πλαίσιο του ΓΚΠΔ

Αποφάσεις

Συχνές ερωτήσεις

Θεματικές ενότητες

Επιλογή Ενότητας

Σημαντικά αρχεία

Επιλογή Ενότητας

ΜΙΚΡΟΙ ΠΟΛΙΤΕΣ

ΑΣΦΑΛΕΙΑ

Τα δικαιώματα των πολιτών στο πλαίσιο του ΓΚΠΔ

Ο νέος Κανονισμός ενισχύει τα ήδη υφιστάμενα δικαιώματα των πολιτών (υποκειμένων των δεδομένων), ενώ παράλληλα κατοχυρώνει και νέα. Επιγραμματικά τα δικαιώματα αυτά είναι τα εξής (αναλύονται περαιτέρω στις αντίστοιχες ενότητες):

- **Δικαίωμα ενημέρωσης/Διαφάνεια:** Είναι το δικαίωμα να γνωρίζετε ποιος επεξεργάζεται τα δεδομένα σας, ποια είναι αυτά και για ποιον λόγο. Οι οργανισμοί που επεξεργάζονται δεδομένα σας πρέπει να σας παρέχουν σαφείς πληροφορίες σε απλή γλώσσα.
- **Δικαίωμα πρόσβασης:** Έχετε το δικαίωμα να ζητήσετε δωρεάν πρόσβαση στα προσωπικά σας δεδομένα που διαθέτει ένας οργανισμός.
- **Δικαίωμα διόρθωσης:** Έχετε το δικαίωμα να ζητήσετε τη διόρθωση ανακριβών προσωπικών δεδομένων και συμπλήρωσης ελλিপών στοιχείων.
- **Δικαίωμα διαγραφής («δικαίωμα στη λήθη»):** Έχετε το δικαίωμα να ζητήσετε τη διαγραφή προσωπικών σας δεδομένων, υπό ορισμένες προϋποθέσεις, όπως όταν τα δεδομένα δεν είναι πλέον απαραίτητα, έχετε ανακαλέσει τη συγκατάθεσή σας, τα δεδομένα έχουν υποβληθεί σε παράνομη επεξεργασία, κ.ο.κ.
- **Δικαίωμα περιορισμού της επεξεργασίας:** Έχετε το δικαίωμα να ζητήσετε τον περιορισμό της επεξεργασίας των προσωπικών σας δεδομένων όταν αμφισβητείται η ακρίβειά τους, η επεξεργασία είναι παράνομη, τα δεδομένα δεν χρειάζονται πλέον στον υπεύθυνο επεξεργασίας, έχετε αντιρρήσεις ως προς την αυτοματοποιημένη επεξεργασία.
- **Δικαίωμα στη φορητότητα των δεδομένων:** Έχετε το δικαίωμα να ζητήσετε τη μεταφορά των δεδομένων σας σε άλλον υπεύθυνο επεξεργασίας.
- **Δικαίωμα εναντίωσης:** Έχετε το δικαίωμα να εναντιωθείτε στην επεξεργασία προσωπικών σας δεδομένων από έναν οργανισμό, υπό την προϋπόθεση ότι δεν θίγεται το δημόσιο συμφέρον.
- **Δικαίωμα στην ανθρώπινη παρέμβαση:** Έχετε το δικαίωμα να προβάλλετε αντιρρήσεις όταν μια απόφαση που σας αφορά βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάταξης προφίλ, και η απόφαση αυτή παράγει έννομα αποτελέσματα ή σας επηρεάζει.

Αναζήτηση

Επιλογή κειμένου αναζήτησης

Επιλέξτε ενότητα

Αναζήτηση

ΥΠΗΡΕΣΙΕΣ ΠΡΟΣ ΠΟΛΙΤΕΣ

ΥΠΗΡΕΣΙΕΣ ΠΡΟΣ ΦΟΡΕΙΣ

DRD

ΔΙΚΑΙΩΜΑΤΑ ΜΑΣ ΚΑΙ ΑΝΕΞΑΡΤΗΤΕΣ ΑΡΧΕΣ

The screenshot shows the EETT website interface. At the top, there are navigation links for EN, GR, RSS, and menu items for Η ΕΕΤΤ, ΓΙΑ ΚΑΤΑΝΑΛΩΤΕΣ, ΓΙΑ ΠΑΡΟΧΟΥΣ, and ΓΙΑ ΜΜΕ & ΑΝΑΛΥΤΕΣ. The main header features the EETT logo, accessibility icons (A A A and ΑμεΑ), and a search bar. Below the header, there are four content boxes with icons and text:

- Σχετικά με τις Ηλεκτρονικές Επικοινωνίες** (Icon: globe and satellite) - [Δείτε περισσότερα](#)
- Σχετικά με τις Ταχυδρομικές Υπηρεσίες** (Icon: mail plane) - [Δείτε περισσότερα](#)
- Σχετικά με Κεραίες, Παρεμβολές και Ραδιοεξοπλισμό** (Icon: antenna tower) - [Δείτε περισσότερα](#)
- Σχετικά με την ποιότητα Υπηρεσιών Ηλεκτρονικών Επικοινωνιών** (Icon: magnifying glass over charts) - [Δείτε περισσότερα](#)

At the bottom, there are two red buttons: [Online Εφαρμογές για Καταναλωτές](#) and [Συχνές ερωτήσεις](#).

The screenshot shows the 'Submit Complaint' page on the EETT website. The header includes the EETT logo, accessibility icons (A A A and ΑμεΑ), and a search bar. The main content area features a red banner with the text **Υποβάλετε καταγγελία...**. Below the banner, there is a section titled **Για να υποβάλετε αίτημα/καταγγελία, παρακαλούμε συμπληρώστε την αντίστοιχη ηλεκτρονική φόρμα:** with a list of links:

- **Τηλεφωνία και Διαδίκτυο**
Για τα συγκεκριμένα θέματα, προτείνεται να επισκεφθείτε προηγουμένως τον «[Οδηγό Καταναλωτή για τηλεφωνία και Διαδίκτυο](#)».
- **Κατασκευές κεραιών κινητής τηλεφωνίας**
- **Θέματα παρεμβολών**
- **Θέματα ραδιοεξοπλισμού**
- **Ταχυδρομικές υπηρεσίες**

At the bottom, there is contact information: **Τομέας Εξυπηρέτησης Καταναλωτή: 210 615 1194** (καθημερινά 09:00-12:00) and a link: [Δήλωση περί Απορρήτου και Προστασίας Δεδομένων Προσωπικού Χαρακτήρα](#).

ΑΝ ΜΑΣ ΣΥΜΒΕΙ ΤΙ ΚΑΝΟΥΜΕ ΤΡΟΠΟΙ ΚΑΤΑΓΓΕΛΙΑΣ ΚΥΒΕΡΝΟ-ΕΓΚΛΗΜΑΤΟΣ

Εισαγγελία Πρωτοδικών

Αρχές Επιβολής του
Νόμου

Ανεξάρτητες Διοικητικές
Αρχές

Ειδικές Πλατφόρμες

Ηλεκτρονικό Ταχυδρομείο

Τηλεφωνικό Κέντρο 1188



www.gov.gr/ipiresies/polites-kai-kathemerinoteta

govgr BETA

Αναζητήστε εδώ ...

Αρχική > Πολίτης και καθημερινότητα

Γεωργία και κτηνοτροφία

Δικαιοσύνη

Εκπαίδευση

Επιχειρηματική δραστηριότητα

Εργασία και ασφάλιση

Οικογένεια

Περιουσία και φορολογία

Πολίτης και καθημερινότητα

Άσκηση εκλογικού δικαιώματος
Δείτε πού ψηφίζετε

Διεύθυνση κατοικίας και επικοινωνίας
Προμηθευτείτε τη βεβαίωση κατοικίας ειδικής χρήσης

Ενημέρωση και επικαιροποίηση στοιχείων πολίτη
Βρείτε τον ΑΜΚΑ σας, κάντε ηλεκτρονική εγγραφή στο Taxisnet κ.ά.

Εξ αποστάσεως εξυπηρέτηση πολιτών
Απόδοση κλειδαρίθμου με ψηφιακό ραντεβού, απομακρυσμένη υποβολή αγροτεμαχίων ενιαίας αίτησης ενίσχυσης κ.ά.

Καταγγελίες

1

4U

Πολίτης και καθημερινότητα

Άσκηση εκλογικού δικαιώματος
Δείτε πού ψηφίζετε

Διεύθυνση κατοικίας και επικοινωνίας
Προμηθευτείτε τη βεβαίωση κατοικίας ειδικής χρήσης

Ενημέρωση και επικαιροποίηση στοιχείων πολίτη
Βρείτε τον ΑΜΚΑ σας, κάντε ηλεκτρονική εγγραφή στο Taxisnet κ.ά.

Εξ αποστάσεως εξυπηρέτηση πολιτών
Απόδοση κλειδαρίθμου με ψηφιακό ραντεβού, απομακρυσμένη υποβολή αγροτεμαχίων ενιαίας αίτησης ενίσχυσης κ.ά.

Καταγγελίες
Προχωρήστε σε καταγγελία για το θέμα που σας αφορά

Μετακινήσεις
Προσωρινή άδεια οδήγησης, μεταφορικό ισοδύναμο, διέλευση

Καταγγελίες

Στη λίστα παρακάτω μπορείτε να δείτε τις υπηρεσίες που αφορούν την επιλεγμένη κατηγορία.

[Αντίγραφο Βιβλίου Αδικημάτων και Συμβάντων \(ΒΑΣ\)](#)

[Καταγγελία / παράπονα για θέματα παρεμβολών](#)

[Καταγγελία / παράπονα για κατασκευή κεραιάς κινητής τηλεφωνίας](#)

[Καταγγελία / παράπονα για ταχυδρομικές υπηρεσίες](#)

[Καταγγελία / παράπονα για τηλεφωνία - διαδίκτυο](#)

[Καταγγελία για αυτοκτονικό χρήστη του διαδικτύου](#)

[Καταγγελία για παιδόφιλο στο διαδίκτυο](#)

[Καταγγελία για υπόθεση σε βάρος του Ελληνικού Δημοσίου](#)

[Καταγγελία επιχειρήσεων για βιομηχανική κατασκοπεία](#)

[Καταγγελία επιχειρήσεων για παράνομη παροχή υπηρεσιών συνδρομητικής τηλεόρασης](#)

[Καταγγελία επιχειρήσεων για ψηφιακό βανδαλισμό πληροφοριακών συστημάτων](#)

2

www.gov.gr/ipiresies/polites-kai-kathemerinoteta/kataggelies/kataggelia-epikheirseon-gia-psephiako-bandalismo-plerophoriakon-sustematon

govgr BETA

Αναζητήστε εδώ ...

Αρχική > Πολίτης και καθημερινότητα > Καταγγελίες > Καταγγελία επιχειρήσεων για ψηφιακό βανδαλισμό πληροφοριακών συστημάτων

Καταγγελία επιχειρήσεων για ψηφιακό βανδαλισμό πληροφοριακών συστημάτων

Επιχειρήσεις μπορούν να υποβάλουν επώνυμη καταγγελία για ψηφιακό βανδαλισμό των πληροφοριακών τους συστημάτων (hacking).

Στη συνέχεια, μπορούν να παρακολουθούν ηλεκτρονικά την πορεία διεκπεραίωσης της καταγγελίας τους.

Είσοδος στην υπηρεσία

Χρήσιμοι σύνδεσμοι

- Πορεία διεκπεραίωσης καταγγελίας
- Επικοινωνία
- Οδηγίες διαδικασίας

3

ΚΥΒΕΡΝΗΣΗ ΑΣΤΟΝΙΑΣ
CYBER CRIME DIVISION
ΔΙΟΞΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΠΑΡΕΧΟΥΜΕ ΨΗΦΙΑΚΕΣ ΥΠΗΡΕΣΙΕΣ ΜΕ ΠΟΙΟΤΗΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΡΟΣΑΡΜΟΣΜΕΝΕΣ ΣΤΙΣ ΑΝΑΓΚΕΣ ΤΩΝ ΠΟΛΙΤΩΝ

Αρχική σελίδα Σχετικά με την ΔΙΔΗΕ Αρμόσεις Δελτία Τύπου Ηλεκτρονική βιβλιοθήκη Ηλεκτρονικά Αδικήματα Συχνές ερωτήσεις Επικοινωνία

Στη σελίδα αυτή μπορείτε να καταχωρήσετε μία νέα καταγγελία, ακολουθώντας τα βήματα του παρακάτω οδηγού. Στην περίπτωση που έχετε ήδη καταχωρίσει μία καταγγελία και θέλετε να ενημερωθείτε για την πορεία διεκπεραίωσης της πατήστε εδώ.

Επιλογή καταγγελίας Γενικά στοιχεία Ειδικά στοιχεία καταγγελίας Προεπισκόπηση και Καταχώρηση

Επιλέξτε από τα παρακάτω θέματα εκείνο για το οποίο επιθυμείτε να προχωρήσετε σε καταγγελία. Πληθύνονται σε κάποιες καταγγελίες, μπορείτε να δείτε διευκρινιστικές πληροφορίες, που θα σας βοηθήσουν στην τελική επιλογή σας.

- Θέμα καταγγελίας
- Καταγγελίες πολιτών και επιχειρήσεων για απατηλές διατραπεζικές συναλλαγές μέσω του διαδικτύου
- Καταγγελίες επιχειρήσεων για περιπτώσεις βιομηχανικής κατασκοπείας

4

OPERATION PANGEA I TO XI
Targeting counterfeit medicines



105 million
units seized



12.9 million
packages
inspected



1.1 million
packages seized



82,000
websites
shut down



3,000
arrests



153
participating
countries

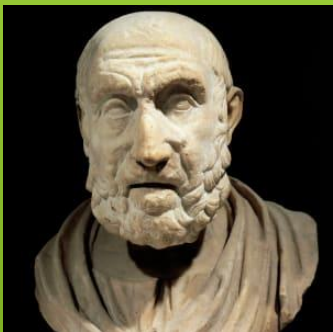


Η αναφορά και η καταγγελία για ένα κυβερνοέγκλημα οδηγεί στην διεξαγωγή επιχειρήσεων των Αρχών Επιβολής του Νόμου

PANGEA OPERATION



Η ΣΤΡΑΤΗΓΙΚΉ ΤΗΣ ΠΡΟΛΗΨΗΣ



Πατέρας της ιατρικής επιστήμης

Μη
αποτίμηση

Συγκριτικό
πλεονέκτημα


ΤΡΪΠΤΥΧΟ ΣΥΝΕΡΓΑΣΙΑΣ ΓΙΑ ΚΑΛΪΤΕΡΗ ΑΣΦΆΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΏΡΟ

Ακαδημαϊκή Κοινότητα

Δημόσιος Τομέας

Ιδιωτικός Τομέας

ΠΡΟΤΑΣΕΙΣ ΚΑΙ ΙΔΕΕΣ ΓΙΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

- ▶ Στρατηγική σε ατομικό και σε συλλογικό επίπεδο
 - ▶ Προτεραιότητα το παιδί - μαθητής
 - ▶ Δημιουργία κουλτούρας εμπιστοσύνης
 - ▶ Επένδυση στο humanware
 - ▶ Ενημέρωση - Εκπαίδευση – μετεκπαίδευση
 - ▶ Υιοθέτηση καλών πρακτικών
 - ▶ Πιστοποίηση
- 

ΠΡΟΤΑΣΕΙΣ ΣΕ ΕΠΙΠΕΔΟ ΠΟΛΙΤΕΙΑΣ ΓΙΑ ΚΑΛΥΤΕΡΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

- ▶ Ολιστική προσέγγιση
- ▶ Συνεργασία
- ▶ Θεσμική θωράκιση
- ▶ Μείωση του Κυβερνοεγκλήματος
- ▶ Έρευνα και Καινοτομία
- ▶ Κουλτούρα Βιοηθικής



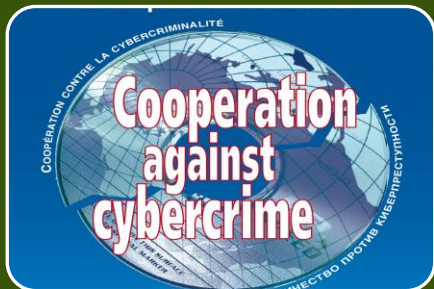
Αντί επι-λόγου



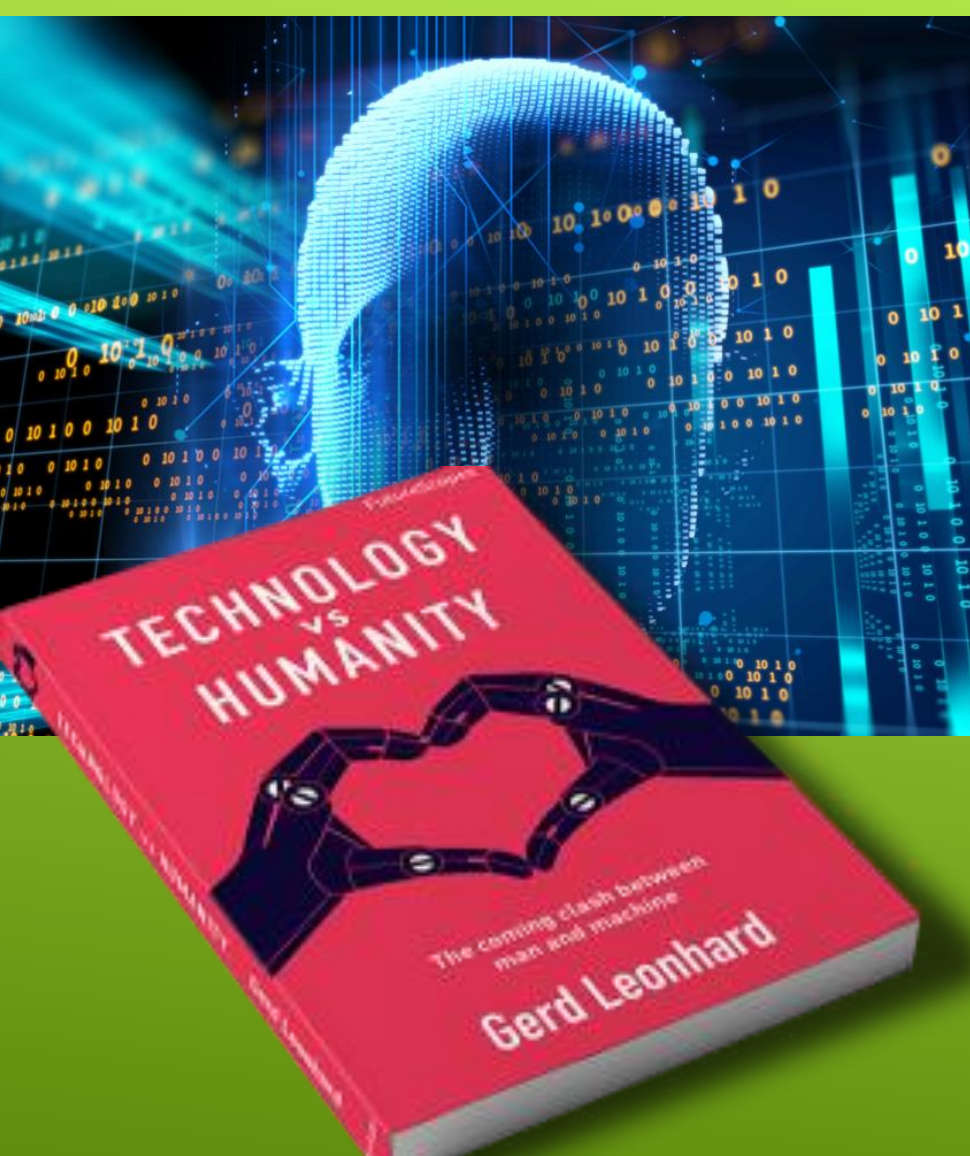
Η οργανωμένη κοινωνία μπορεί να αντιμετωπίσει τις **σύγχρονες προκλήσεις** (όπως η **Κυβερνοασφάλεια**) απέναντι στο σοβαρό και οργανωμένο έγκλημα, αξιοποιώντας κι ενισχύοντας την τεχνολογία



Η **θεσμική θωράκιση** αποτελεί προτεραιότητα (ενίσχυση κι εναρμόνιση νομικού πλαισίου αλλά και υποδομών για υλοποίηση) για μια ανοικτή, δημοκρατική και βιώσιμη κοινωνία



Η αξιοποίηση **ανθρωπίνων πόρων**, η βελτίωση του **θεσμικού πλαισίου**, η ενίσχυση της **διεθνούς συνεργασίας**, η επένδυση στην **καινοτομία** και την **εκπαίδευση** αποτελούν αναγκαία βήματα



Άνθρωπος

Τεχνολογία

Ευημερία

Η **Τεχνολογία** είναι **χρήσιμη** για όλους μας..... όταν **όλοι** μας φροντίζουμε για την **ανθρώπινη** διάστασή της!!!!.



Κι αυτό
είναι στο
χέρι μας...

ΕΥΧΑΡΙΣΤΩ ΠΟΛ'Υ ΓΙΑ ΤΗΝ ΠΡΟΣΟΧΉ ΣΑΣ ΣΤΗ ΔΙΑΘΕΣΗ ΣΑΣ ΓΙΑ ΕΡΩΤΗΣΕΙΣ

Γιώργος Παπαπροδρόμου

Υποστράτηγος ε.α. ΕΛ.ΑΣ.

Ειδικός σε θέματα αντιμετώπισης Κυβερνο-εγκλήματος

Πτυχιούχος Νομικής ΑΠΘ - Δικαστικός Γραφολόγος

pprodrom@gmail.com