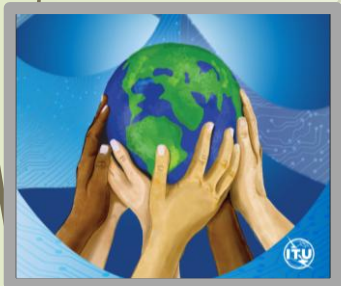
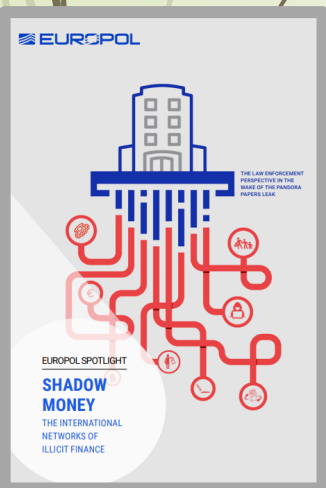


Η οικονομική διάσταση του Κυβερνοεγκλήματος



Κατερίνη, 01/12/2025



Εισηγητής:
Γιώργος Παπαπροδρόμου
Αντιστράτηγος ε.α. (ΕΛ.ΑΣ.)
Πτυχιούχος Νομικής ΑΠΘ – Δικαστικός Γραφολόγος
Πρώην Διευθυντής Δ/σης Δίωξης Ηλεκτρονικού Εγκλήματος
Αρχηγείου Ελληνικής Αστυνομίας

Βασικά σημεία της σημερινής παρουσίασης



1. Τι γνωρίζουμε για το οικοσύστημα του **Κυβερνοχώρου**;
2. Πως διαμορφώνεται το τοπίο της Κυβερνοασφάλειας;
3. Πως προσδιορίζεται η **οικονομική διάσταση** του **κυβερνοεγκλήματος**;
4. Ποιο είναι το σημερινό **διακύβευμα** για άτομα, οικογένειες και κοινωνίες;
5. Ποιες δεξιότητες χρειάζεται να διαθέτουμε στον 21^ο αιώνα;
6. Η **σημαντικότητα** των κοινωνικών θεσμών (**οικογένεια, σχολείο,**)

Πρόσφατα περιστατικά Κυβερνοεγκλημάτων

Profit - Κέρδος



16.6 million packages of fake and harmful toys taken off EU markets



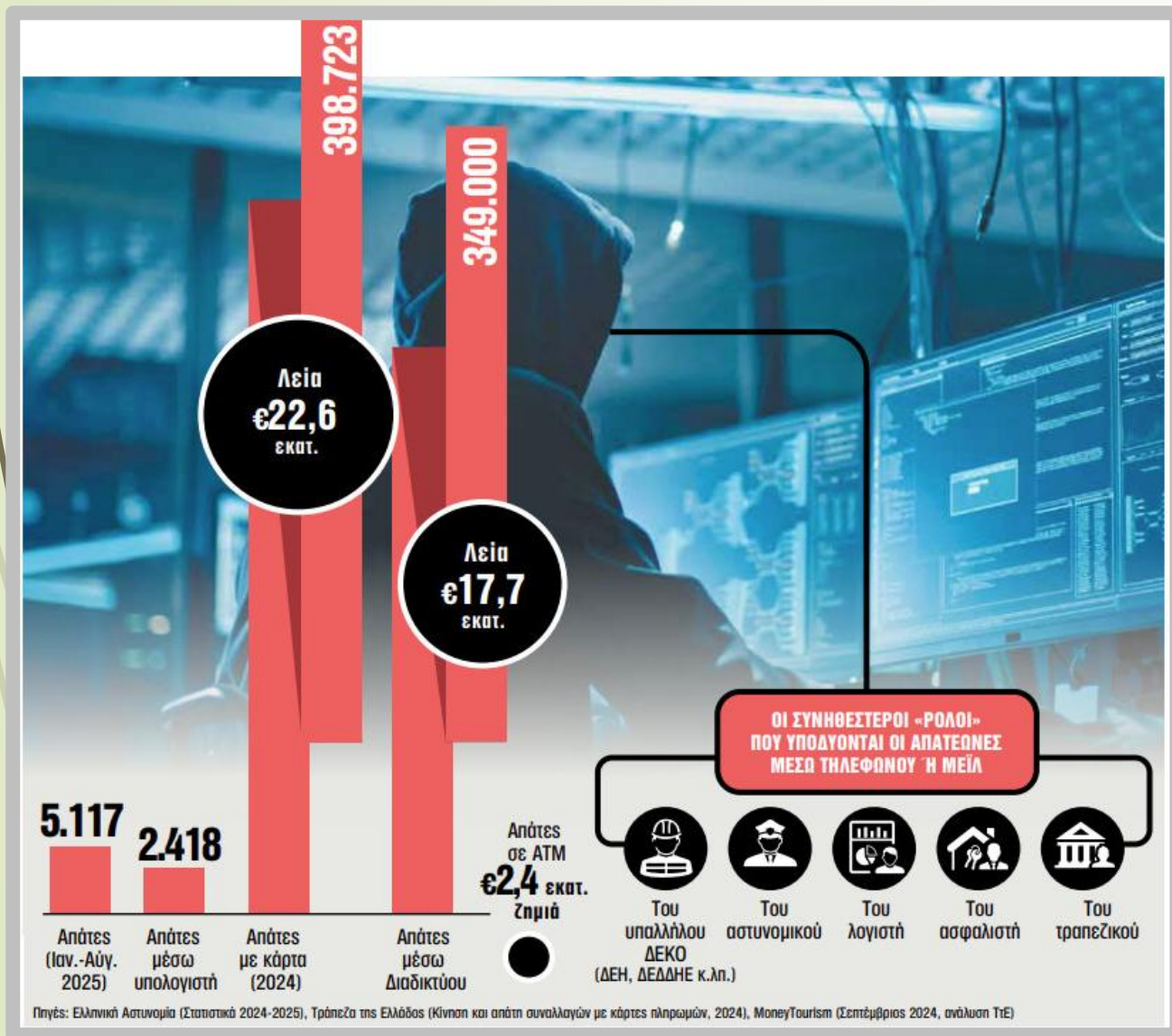
EUR 47 million in crypto traced to disrupt digital piracy services



Πηγές

1. <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/>
2. <https://www.europol.europa.eu/media-press/newsroom>

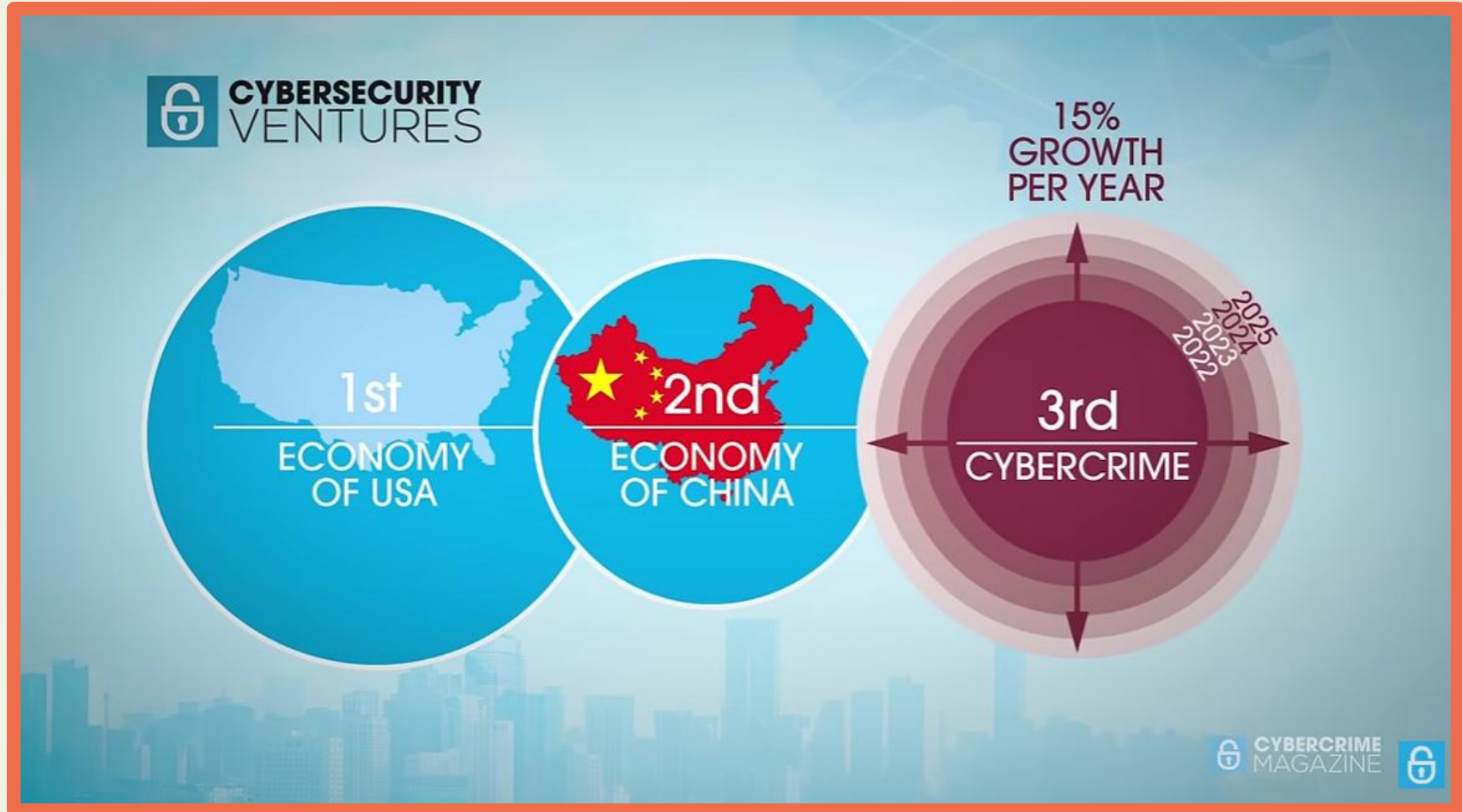
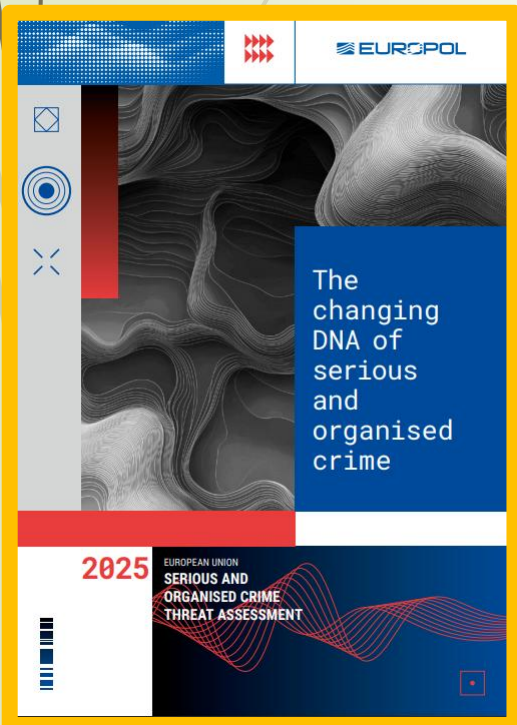
Απάτες στην Ελλάδα



Πηγές

<https://www.tanea.gr/print/2025/10/20/greece/ekriksi-stis-psifiakes-apates/>

Η **τρίτη** σε μέγεθος Οικονομία παγκοσμίως



Πηγές

1. <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52025DC0148> [σελ. 1](#)
2. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>
3. <https://deepstrike.io/blog/cybersecurity-statistics-2025-threats-trends-challenges>
4. <https://cybersecurityventures.com/official-cybercrime-report-2025/>

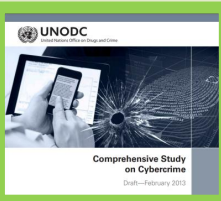
Η **τρίτη** σε μέγεθος Οικονομία



Πηγές

1. <https://www.cia.gov/the-world-factbook/field/real-gdp-purchasing-power-parity/country-comparison/>
2. <https://www.worldometers.info/gdp/gdp-by-country/>

Rank	Country		Date of Information
1	<u>China</u>	\$33,598,000,000,000	2024 est.
2	<u>United States</u>	\$25,676,000,000,000	2024 est.
3	<u>India</u>	\$14,244,000,000,000	2024 est.
4	<u>Russia</u>	\$6,089,000,000,000	2024 est.
5	<u>Japan</u>	\$5,715,000,000,000	2024 est.
6	<u>Germany</u>	\$5,247,000,000,000	2024 est.
7	<u>Brazil</u>	\$4,165,000,000,000	2024 est.
8	<u>Indonesia</u>	\$4,102,000,000,000	2024 est.
9	<u>France</u>	\$3,732,000,000,000	2024 est.
10	<u>United Kingdom</u>	\$3,636,000,000,000	2024 est.



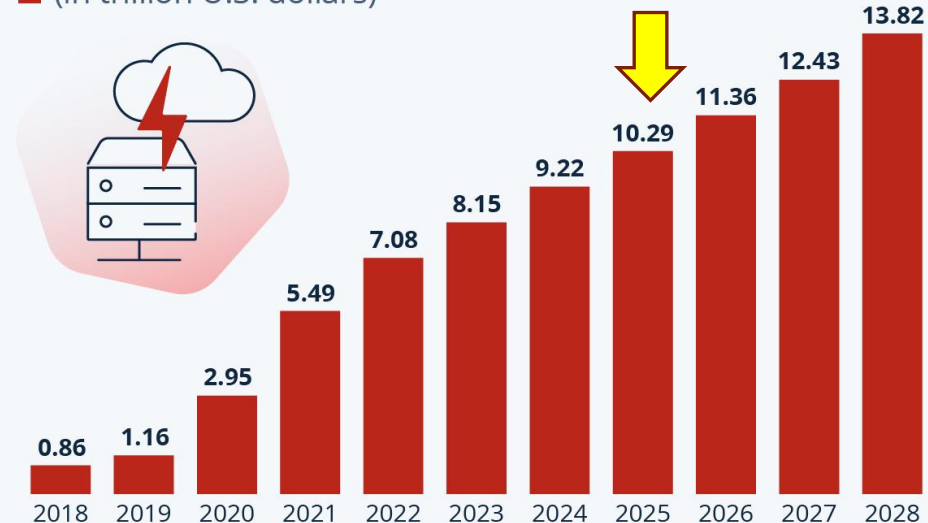
Αντίκτυπος του Κυβερνοεγκλήματος

Impact of different cybercrimes

Cyber crime type	Average loss	Victims	Loss	
Investment fraud	\$108,479	30.5k	\$3.3B	
Tech support scam	\$24,788	32.5k	\$806.6M	
Confidence or romance fraud	\$38,688	19k	\$735.9M	
Online payment fraud	\$6,134	62.9k	\$386.1M	
Credit card fraud	\$11,492	23k	\$264.1M	
Government impersonation	\$20,820	11.6k	\$240.6M	
Identity theft	\$6,776	27.9k	\$189.2M	
Spoofing	\$5,227	20.6k	\$107.9M	
Lottery scam	\$14,797	5.7k	\$83.6M	
SIM swapping	\$35,860	2k	\$72.7M	
Extortion	\$1,379	39.4k	\$54.3M	
Phishing	\$173	300.5k	\$52.1M	
Ransomware attack	\$14,404	2.4k	\$34.4M	
Denial of service attack	\$30,105	568	\$17.1M	
Online harassment	\$757	14k	\$10.6M	
Malware attack	\$12,239	762	\$9.3M	

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.

Source: Statista Market Insights



statista

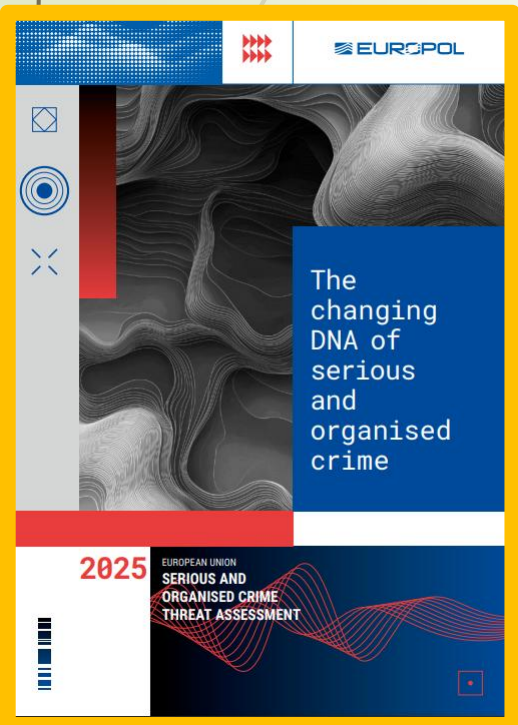
Πηγές:

- <https://www.itsecuritypro.gr/kyvernoasfaleia-kai-mikromesaies-epicheiriseis/>
- <https://elisme.gr/to-pragmatiko-timima-toy-kyvernoegkl/>
- https://surfshark.com/research/data-breach-impact/statistics?fbclid=IwAR0AQp4OOnT3_hyJPbUEcf2d8SZelUUcwy_NSrPFa2-rwyg4KKNj-aw_Cfw
- <https://www.facebook.com/photo/?fbid=711019361235436&set=a.561580072846033>

Περιγραφή της κατάστασης



Ισχυρά δίκτυα οργανωμένου εγκλήματος
πολλαπλασιάζονται στην Ευρώπη,
αντλώντας δύναμη από το **διαδίκτυο**,
δεισδύουν στην **οικονομία** και επιδρούν
αρνητικά στην κοινωνία μας,
όπως επισημαίνεται στην αξιολόγηση απειλών όσον αφορά το σοβαρό και
οργανωμένο έγκλημα στην ΕΕ



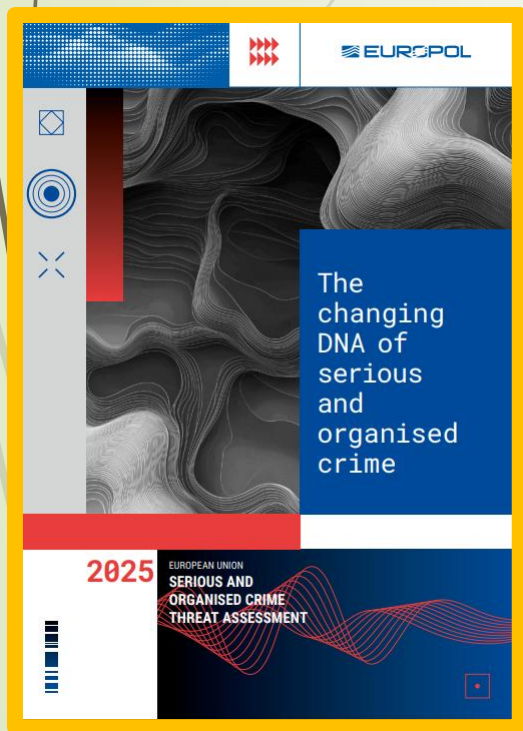
Πηγές

1. <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52025DC0148> **σελ. 1**
2. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>



Περιγραφή της κατάστασης

Μόλις το οργανωμένο έγκλημα εδραιωθεί σε μια κοινότητα ή έναν οικονομικό τομέα, η **εξάλειψή** του καθίσταται εξαιρετικά **δύσκολη**:
το ένα τρίτο των πλέον απειλητικών εγκληματικών δικτύων δραστηριοποιείται για περισσότερα από δέκα έτη.



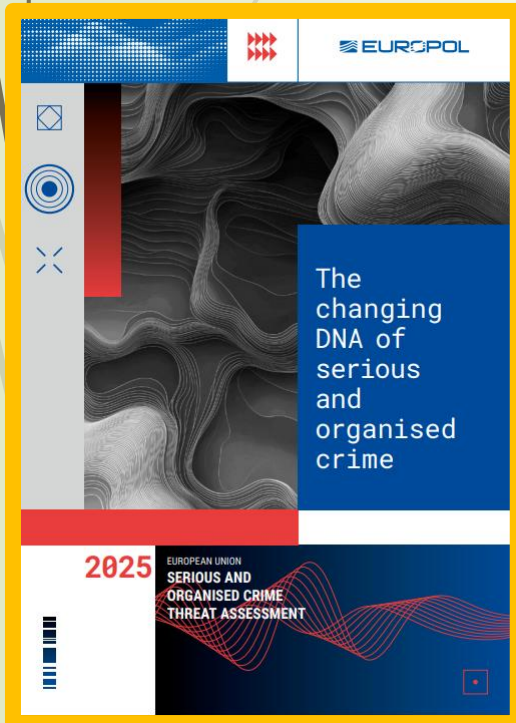
Πηγές

1. <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52025DC0148> [σελ. 1](#)
2. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>

Περιγραφή της κατάστασης

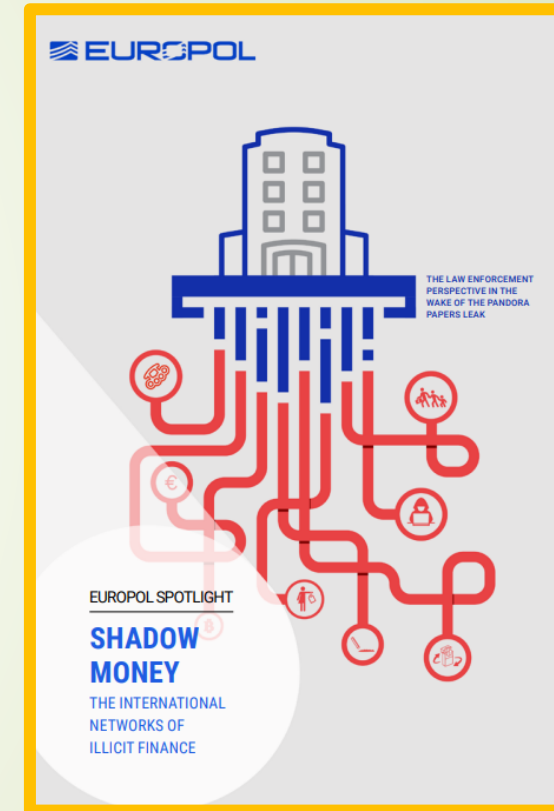


Τα κρυπτονομίσματα και τα παράλληλα χρηματοπιστωτικά συστήματα **βοηθούν** τα δίκτυα του οργανωμένου εγκλήματος να **νομιμοποιούν** και να **αποκρύπτουν** τα έσοδά τους από εγκληματικές δραστηριότητες.



Πηγές

1. <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52025DC0148> σελ. 1
2. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>
3. https://www.europol.europa.eu/cms/sites/default/files/documents/Shadow%20money%20%E2%80%93%20the%20international%20networks%20of%20illicit%20finance_PUBLIC_0.pdf
4. <https://chateurope.eu/en/offshore-companies-at-the-heart-of-pandora-papers/>



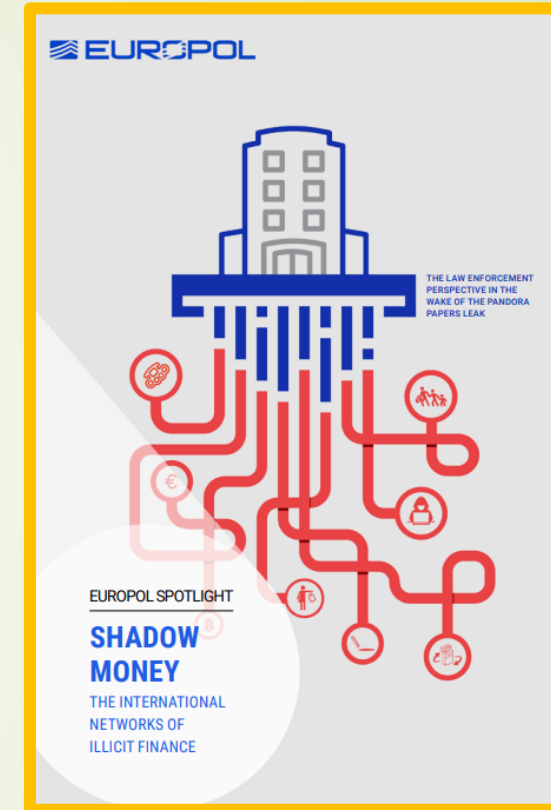
Οικονομικές απώλειες από το κυβερνοέγκλημα

❑ Άμεσες Οικονομικές Απώλειες

(πχ. Καταβολή λύτρων Λυτρισμικού, καταβολή χρημάτων σε απάτες, απατηλές διαδικτυακές αγορές, διαδικτυακός τζόγος, **αγορά ναρκωτικών – ψυχοτρόπων ουσιών και παράνομων φαρμάκων**, αγορά υλικού σεξουαλικής εκμετάλλευσης ανηλίκων, συνδρομές σε πειρατικά κανάλια, κα)

❑ Έμμεσες Οικονομικές Απώλειες

(πχ. διακοπή λειτουργίας επιχειρήσεων και οργανισμών, Ζημιά Φήμης, Αυξημένα Ασφάλιστρα,, επαναφορά λειτουργίας πληροφοριακών συστημάτων)



Πηγές

1. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52025DC0148_σελ.1
2. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>
3. https://www.europol.europa.eu/cms/sites/default/files/documents/Shadow%20money%20%E2%80%93%20the%20international%20networks%20of%20illicit%20finance_PUBLIC_0.pdf
4. <https://chateurope.eu/en/offshore-companies-at-the-heart-of-pandora-papers/>
5. <https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919fee4079180e81701969ad0a18.pdf>



Αδυναμία καταγραφής του συνολικού κόστους

- ❑ Αναξιόπιστα Συστήματα Αναφοράς Κυβερνοεγκλημάτων
- ❑ Απουσία εναρμονισμένου νομικού πλαισίου
- ❑ Μη ολιστική χρήση των ΤΠΕ στο σύστημα απονομής δικαιοσύνης
- ❑ Ελλιπής ενημέρωση των ευάλωτων ατόμων
- ❑ Μειωμένο ενδιαφέρον των συναρμόδιων φορέων (πανεπιστήμια, ερευνητικά κέντρα, επιμελητήρια)



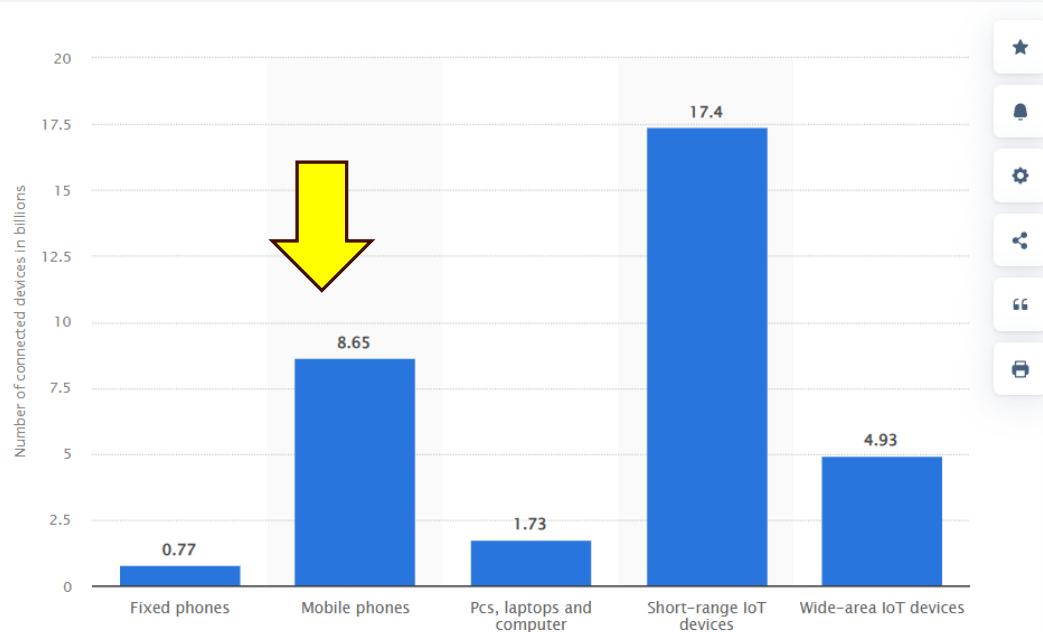
Πηγές

1. <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52025DC0148> σελ. 1
2. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>
3. https://www.europol.europa.eu/cms/sites/default/files/documents/Shadow%20money%20%E2%80%93%20the%20international%20networks%20of%20illicit%20finance_PUBLIC_0.pdf
4. <https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919fee4079180e81701969ad0a18.pdf>
5. <https://www.gov.gr/ipiresies/polites-kai-kathemerinoteta/kataggelies>

Κυβερνοχώρος & Τεχνολογίες αιχμής- ΤΝ – Κβαντικές Τεχνολογίες



Number of connected devices worldwide as of February 2025

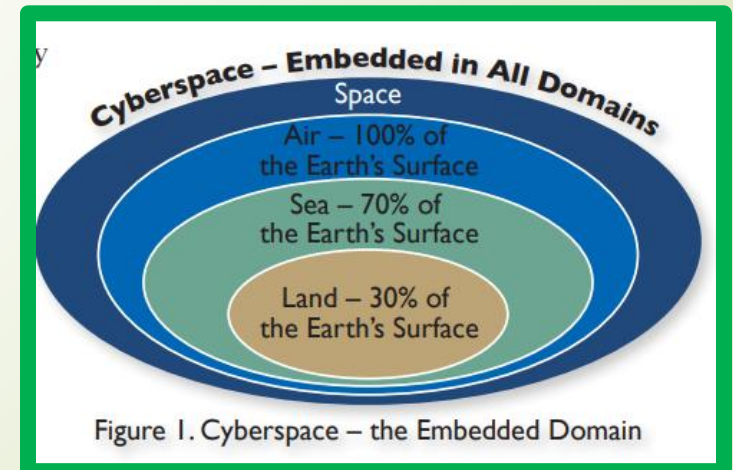


Δισεκατομμύρια
άνθρωποι
και συσκευές

A **global domain** within the **information environment** consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers .

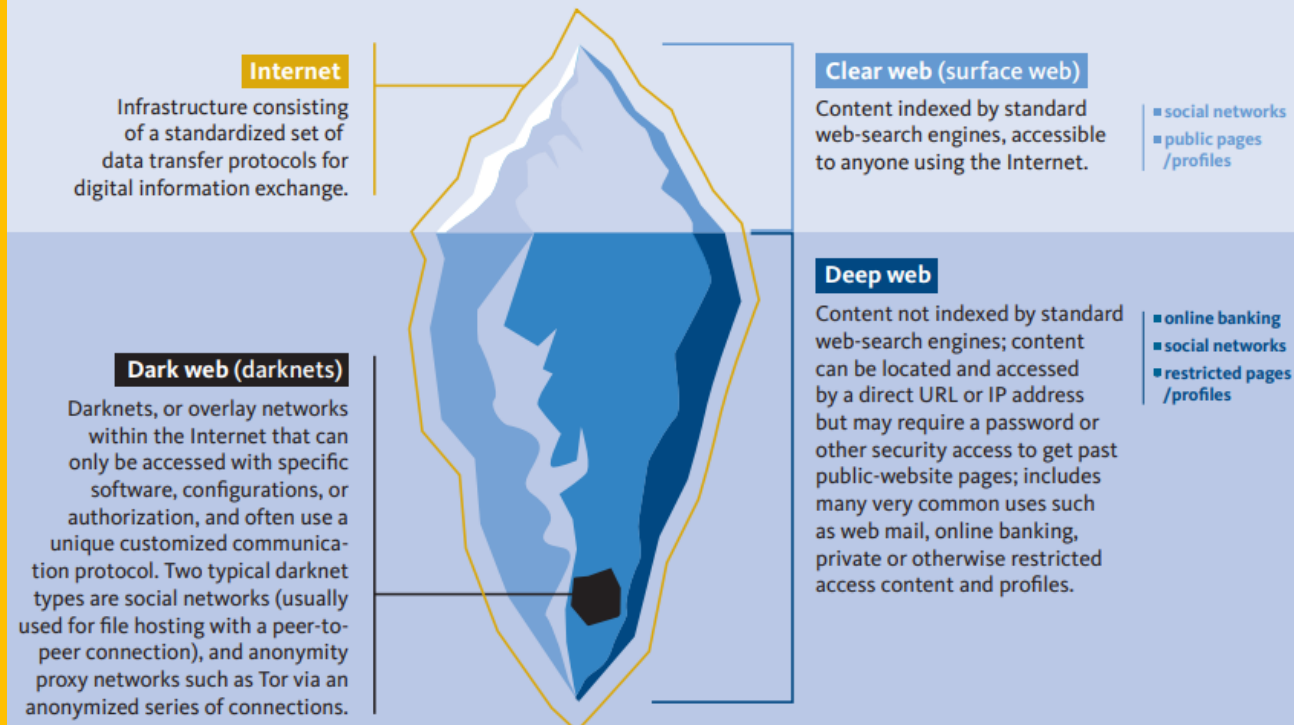
Πηγές

1. (JP 3-12) DoD Dictionary of Military and Associated Terms 2021 p. 55
2. Eric Schmidt, Jared Cohen, Η Νέα Ψηφιακή Εποχή, 2014, Εκδόσεις Δίαυλος, σελ. 127, 152,
3. <https://www.statista.com/statistics/1559435/connected-devices-worldwide/>



Η κατανόηση του Κυβερνοοικοσυστήματος

THE INTERNET: CLEAR WEB, DEEP WEB AND DARK WEB



Πολύπλοκο - σύνθετο περιβάλλον
Με αβεβαιότητες



Πηγές:

1. <http://www.thesydneyjournalist.com/wp-content/uploads/2017/08/Dark-Web-Infographic-by-Deep-Web-Tech.jpg>
2. <https://reliefweb.int/report/world/unodc-world-drug-report-2022> BOOKLET 2 DRUG DEMAND DRUG SUPPLY P. 57
3. <https://op.europa.eu/el/publication-detail/-/publication/ddf757c8-53ea-11ec-91ac-01aa75ed71a1>

Τι απειλεί σήμερα τον Κυβερνοχώρο;



1. **Ransomware**
2. **Malware**
3. Social Engineering threats
4. **Threats against data**
5. Threats against availability: **Denial of Service**
6. Threats against availability: **Internet threats**
7. **Disinformation – misinformation**
8. **Supply-chain attacks**

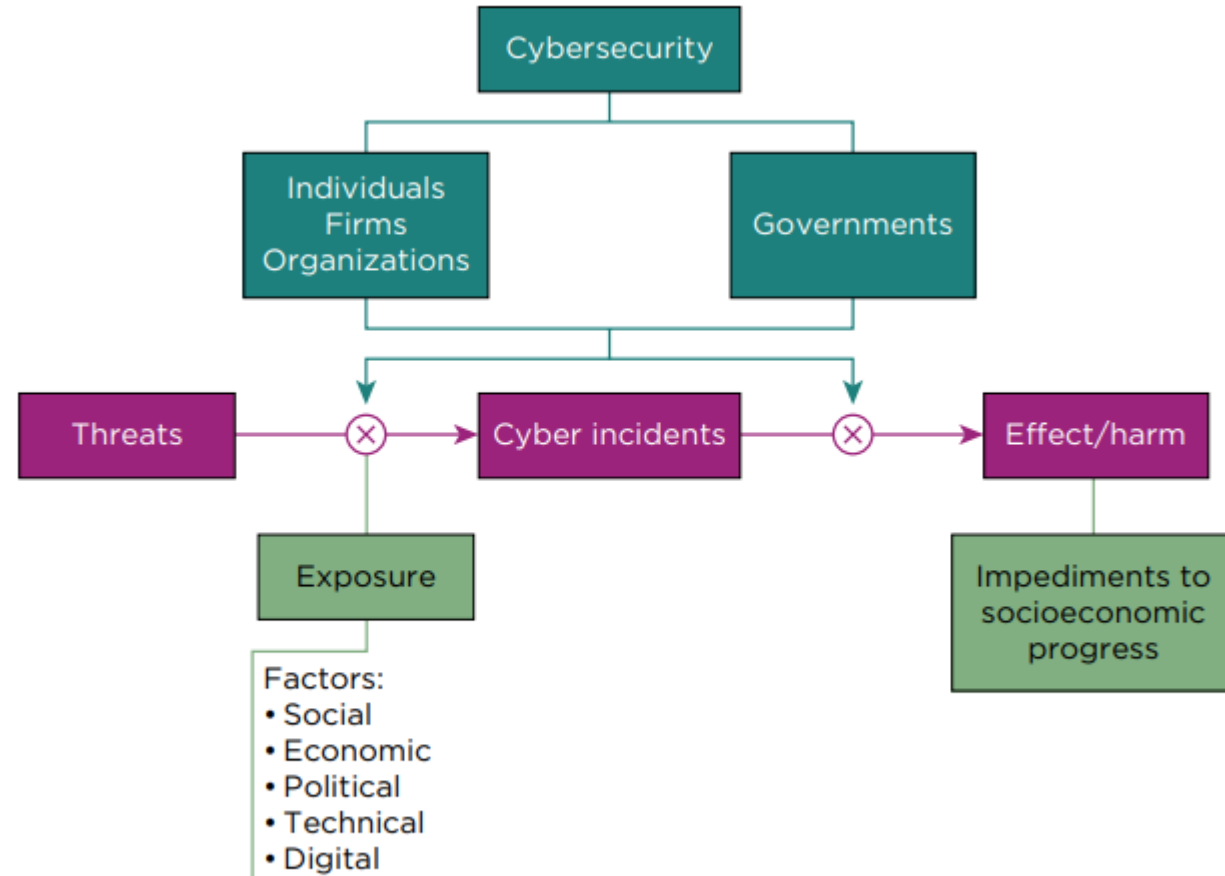
Φορείς απειλών χρησιμοποιούν την τεχνητή νοημοσύνη σε μια ποικιλία κακόβουλων δραστηριοτήτων

Δημοσιεύθηκε **01/10/2025**

Πηγές:

1. https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf
2. <https://www.enisa.europa.eu/media/media-press-kits/logos>
3. <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>
4. https://www.europarl.europa.eu/news/el/headlines/society/20220120STO21428/oi-megaluteres-apeiles-ston-tomea-tis-kubernasfaleias?fbclid=IwAR1jJnQz2hSpnHq93o9jqimHIFDgecBHcEcb-WTFojtP1kwKz_qxnmMJgMs
5. <https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection/?tab=publications>
6. <https://id4d.worldbank.org/guide/cybercrime-and-cybersecurity>
7. <https://www.enisa.europa.eu/search?keys=artificial+intelligence#contentlist>

Ποιους αγγίζει η Κυβερνοασφάλεια



Source: Original figure for this book, based on Woods and Böhme 2021.

❑ Άτομα
❑ Εταιρείες
❑ Οργανισμοί
❑ Κυβερνήσεις

Πηγές:

1. https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en
2. <https://openknowledge.worldbank.org/server/api/core/bitstreams/692c6149-748f-40dc-b9e6-8e09ba3e47bf/content> p. 3
3. <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf> p. 15-25

Συνοπτικά οι μορφές του Κυβερνοεγκλήματος

Προσωπικά Δεδομένα

Ιδιωτικότητα

Σεξουαλική
Εκμετάλλευση
Ανηλίκων

Απάτες

Κυβερνοεπιθέσεις

Παραπληροφόρηση

Ρητορική Μίσους

Κυβερνοέγκλημα

**Fake news – Hate Speech-
Deepfakes- Cyber-bullying**

Ναρκωτικά
και
Φάρμακα

Διανοητική
Ιδιοκτησία

Διάφορα αδικήματα
Πχ διαδικτυακός τζόγος,
ΤΗΒ, Τρομοκρατία

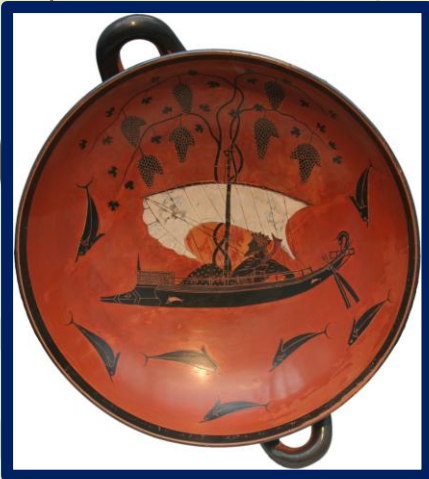
Κυβερνοεπιθέσεις

Εκφοβισμός στον
Κυβερνοχώρο

Προστασία κρίσιμων υποδομών

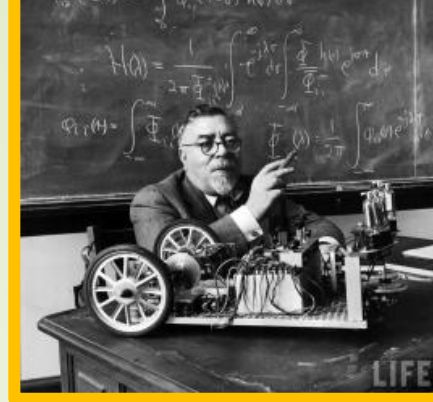
Cybercrime(etymology)

=**Κάθε** έγκλημα στον Κυβερνοχώρο



Κυβερνήτης
kybernetes
governor of a ship
(captain)

Norbert Wiener 1894-1964
“Cybernetics”, 1948



116 Συνέκδικος Ἱερατικός.
τοῦ διαβόλου. Κρίμα σημαίνει τὸ αὐτὸ καὶ Κρίσεις
(judgement,) οἷον “Τα κρίματά σου ὡσεὶ ἄβυσσος
πολλή.” 1) “Κρίματα, ψῆφοι, δικαί” κατὰ τὸν
Ἡσύχιον. Σημαίνει ἀκρίμη καὶ τὸ Κατάκριμα 2)
ἔχουν τὴν Καταδίκην (condamnation) “Κρίμα,
τὸ κατάκριμα καὶ ἡ καταδίκη, ὡς τὸ Κρίμα ἑαυτῷ
ἐσθίει καὶ πίνει κ. τ. λ.” 3) Λέγει καὶ ὁ Ἡσύχιος
“Κρίμα, ἀνταπόδοσις Θεοῦ.” Καὶ τρίτον, αὐτὸ τὸ
κρινόμενον ἔγκλημα ἢ ἀμαρτήμα, λέγεται Κρίμα,
ὅθεν οἱ Ῥωμαῖοι ἔλαβαν τὸ Crimen (crime,) ὀνο-
μάζοντες οὕτως τὴν ἐγκληματικὴν τῶν πολιτικῶν νό-
μων παράβασιν, ὡς ἡμεῖς σήμερον ἐνομάζομεν (εἰς θρη-
σκικὴν σημασίαν) Κρίμα (péchē) τὴν παράβασιν
τῶν ἐντολῶν τοῦ Θεοῦ, τὴν συνωνύμως λεγομένην

Crimen
Κρίμα



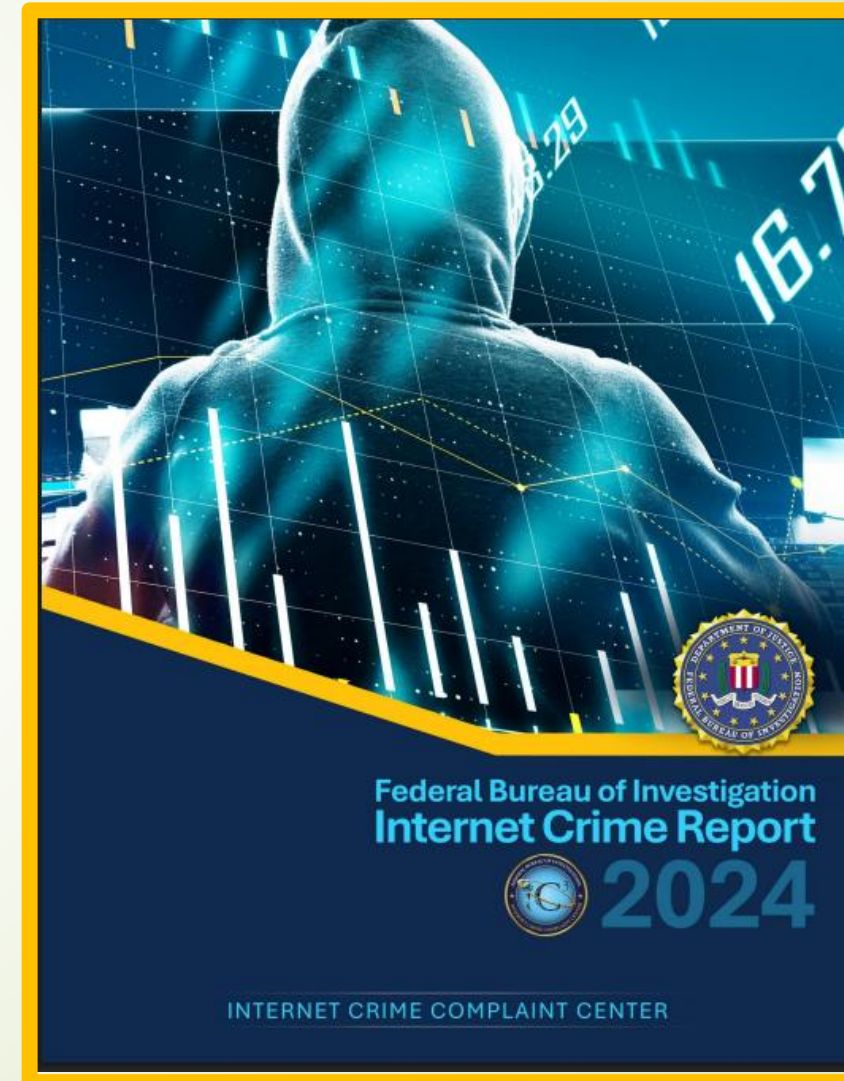
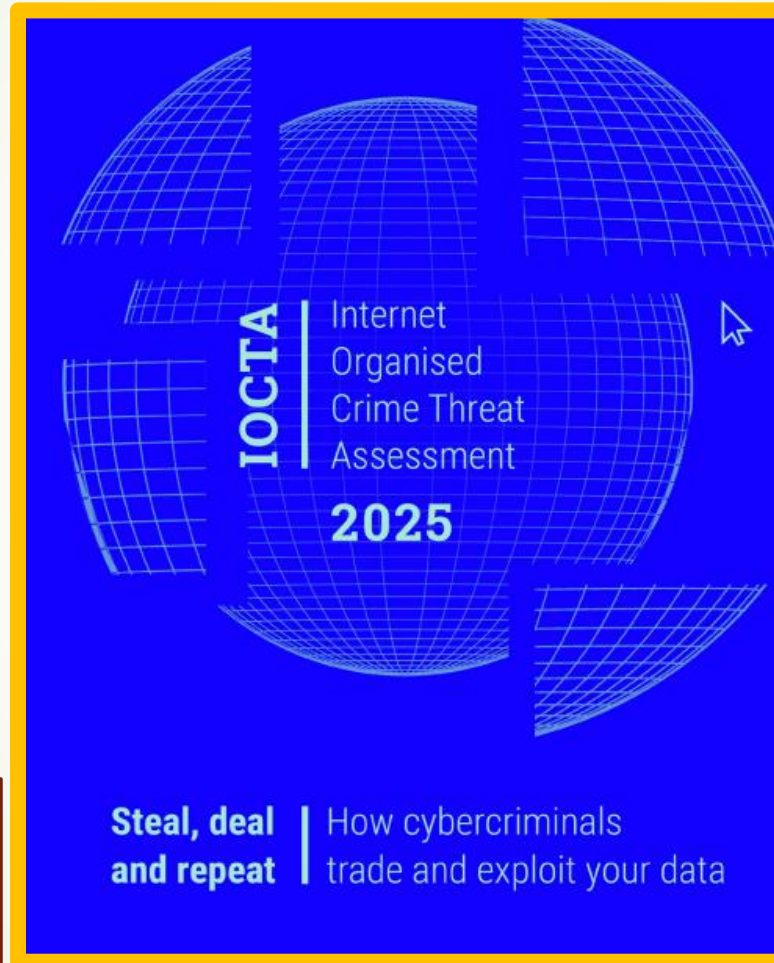
William Gibson 1948-
“Neuromancer”
Cyberspace”, 1984



Πηγές:

1. Stuart Russel, Peter Norvig, Τεχνητή Νοημοσύνη, Μια σύγχρονη προσέγγιση, εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ. Σελ.46
2. James Gleick, The Information, 2011, εκδόσεις Τραυλός, σελ. 16, 329-330,352
3. Ian F. McNeely, Lisa Wolverton, Επανεφεύρεση της Γνώσης, ΕΝΑΛΙΟΣ, 2017, σελ. 344-345
4. Robin Mansell, Το Διαδίκτυο στη Φαντασία, 2018, εκδόσεις Ροπή, σελ. 81
5. Armand Marie Leroi, Η Λιμνοθάλασσα, πως ο Αριστοτέλης επινόησε την επιστήμη, 2018, εκδόσεις Ροπή, σελ. 198
6. Φίλιππος Τσιμπόγλου, Συνεργασίες Βιβλιοθηκών, 2008, εκδόσεις Παπασωτηρίου, σελ.37
7. https://www.allthescience.org/what-is-cybernetics.htm?fbclid=IwAR1a3OvyGvUzIrN6zSd_fQybbT9RZ0GlzSwr7B4n0-MKU3g6rmnsiRkMHxc#imagePopurp
8. Νικόλαος Γ. Ιντζεσίλογλου, Κοινωνία και Νέα Τεχνολογία, 2014, Εκδόσεις ΣΑΚΚΟΥΛΑ, σελ. 565-570
9. Εισαγωγή στις Ψηφιακές Σπουδές, Συλλογικό έργο, 2020, Εκδόσεις Ροπή, σελ. 11, 85-87, 104, 115, 259-262,
10. Μανώλης Ανδριωτάκης, Τεχνητή Νοημοσύνη για όλους, 2022, Εκδόσεις Ψυχογιός, σελ. 99, 167
11. Eric Schmidt, Jared Cohen, Η Νέα Ψηφιακή Εποχή, 2014, Εκδόσεις Δίαυλος, σελ. 127, 145, 152, 153, 162, 168, 229, 356, 363

Το Κυβερνοέγκλημα **αυξάνεται** & **αλλάζει**



Δημοσιεύθηκαν **11/06/2025** & **04/4/2025**

Πηγές:

1. https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf
2. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
3. <https://id4d.worldbank.org/guide/cybercrime-and-cybersecurity>
4. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>



Σύμβαση για το **Κυβερνοέγκλημα** του ΟΗΕ

Η πρώτη Παγκόσμια Σύμβαση

Hanoi 25/10/2025



Πηγές:

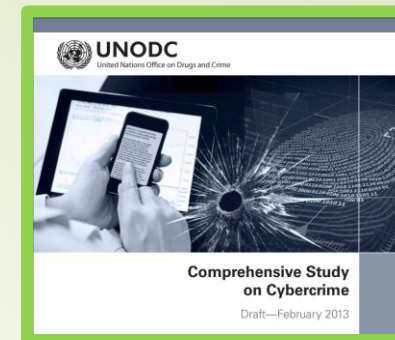
1. <https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html>
2. <https://blogs.worldbank.org/en/digital-development/combating-cybercrime-in-budapest-and-hanoi>
3. https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=en
4. https://www.unodc.org/documents/Cybercrime/publications/un_cyber_policy_processes_links_add_the_links_to_the_web_page.pdf?v=3.6
5. <https://www.eurojust.europa.eu/sites/default/files/assets/files/united-nations-convention-against-cybercrime-sirius-factsheet.pdf>

72 κράτη την έχουν υπογράψει
Στοιχεία της 01/12/2025

Σύμβαση για το Κυβερνοέγκλημα

Το πρώτο διεθνές κείμενο

Budapest 23/11/2001- CETS No 185



Antigua and Barbuda
and Malaysia have
been invited to accede
to the Convention on
Cybercrime

STRASBOURG, FRANCE | 24 SEPTEMBER 2025

On 24 September 2025, following the 1538th
Meeting of the Ministers' Deputies', Antigua and...



Πηγές:

1. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
2. https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf
3. <https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan-2023-public-v1/1680a99137>
4. <https://www.coe.int/en/web/cybercrime/-/greece-becomes-31st-state-to-sign-the-second-additional-protocol-to-the-convention-on-cybercrime>
5. <https://www.coe.int/en/web/cybercrime/-/antigua-and-barbuda-and-malaysia-have-been-invited-to-accede-to-the%C2%A0convention-on-cybercrime>
6. <https://ministryofjustice.gr/wp-content/uploads/2019/08/12aNomos4411-1.pdf>

97 κράτη είναι πλέον είτε συμβαλλόμενα μέρη **(81)**,
είτε την έχουν υπογράψει είτε έχουν προσκληθεί να
προσχωρήσουν **(16)**

Στοιχεία της 01/12/2025

N. 4411/2016 (ΦΕΚ Α142/3-8-2016) επικύρωση από Ελλάδα
20/1/2023 η Ελλάδα υπογράφει και το 2° ΣΠ

Δημοκρατία & Ανθρώπινα Δικαιώματα

Το πραγματικό διακύβευμα

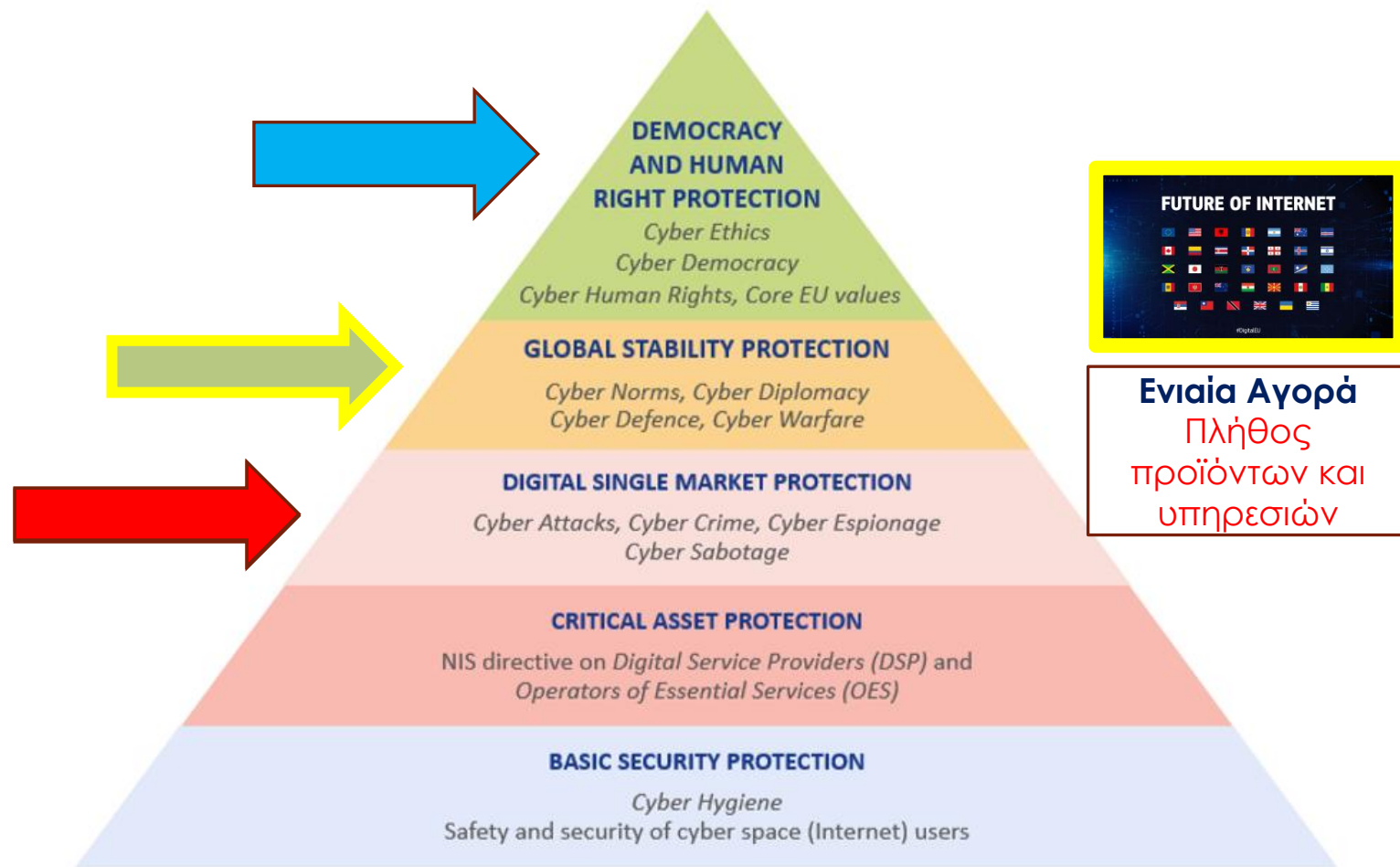
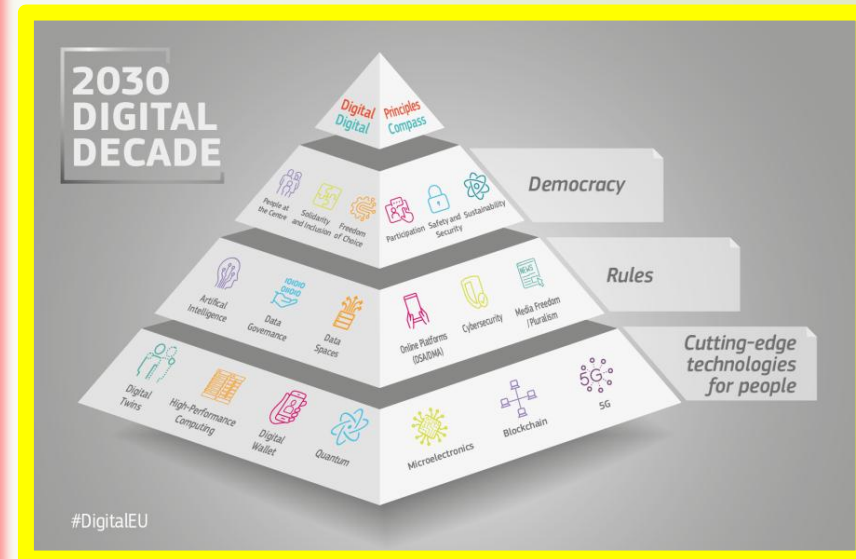


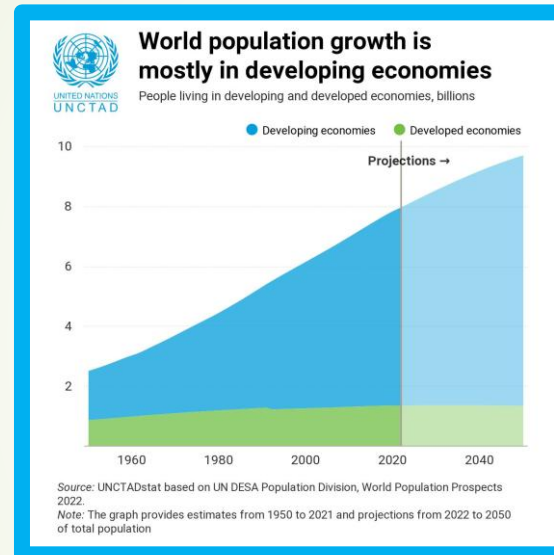
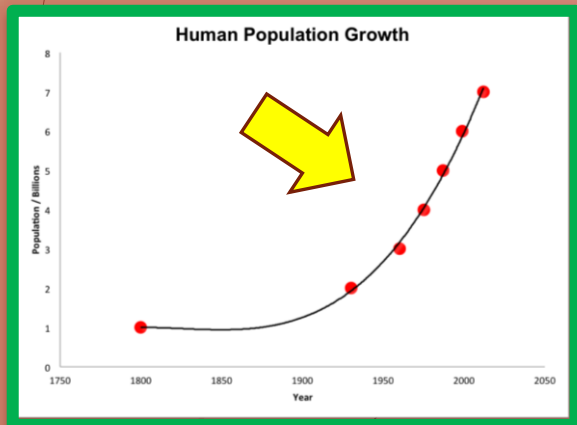
Figure 1. Layers of cybersecurity needs.



Πηγές:

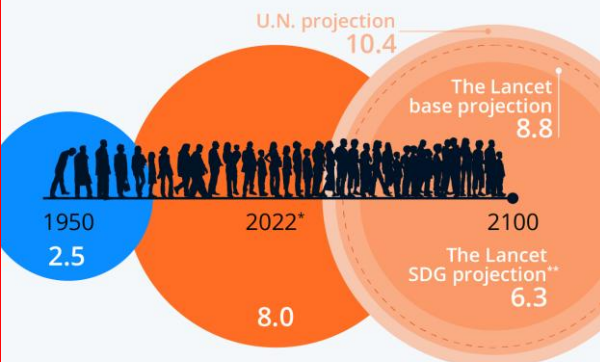
- <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-input-to-the-css-review-b-p.7>
- https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2695
- https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210622_Hybrid_CoE_Paper_7_Geopolitics_and_strategies_in_cyberspace_WEB.pdf
- <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>

Πόσοι είναι οι χρήστες των νέων τεχνολογιών;



Population Boom and Bust?

Global population (in billion people)



* as of Nov 15 ** given the attainment of developmental goals

Sources: U.N. Population Division, The Lancet



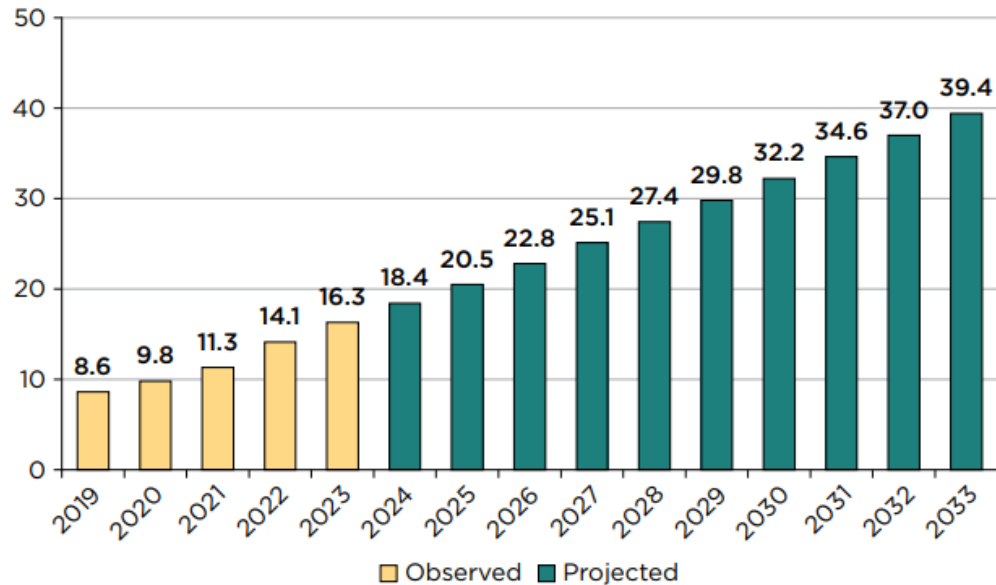
statista

Πηγές

- <https://www.census.gov/popclock/>
- <https://www.worldometers.info/world-population/>
- <https://www.facebook.com/photo?fbid=509355941231664&set=A.298981855602408>
- <https://www.facebook.com/Statista.lnc/photos/pcb.5553912264721206/5553912154721217>
- J. Bradford Delong, Στον δρόμο προς την ουτοπία, 2023, Μεταίχμιο, σελ. 25-26, 36-40, 42

Περισσότερα τα κινητά από τους ανθρώπους

Number of Internet of Things connected devices (billions)

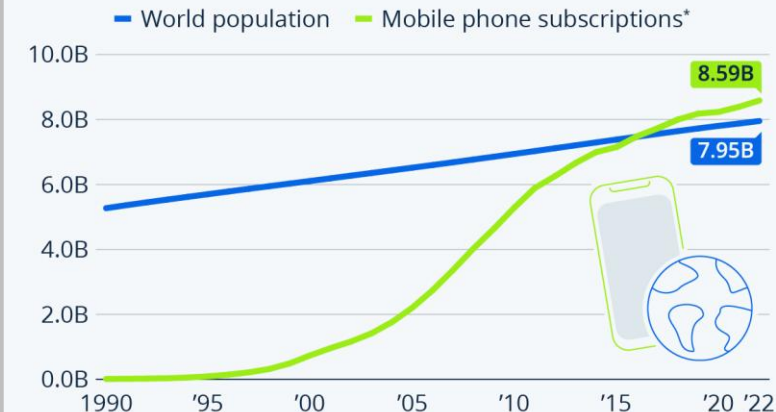


Source: Original figure for this book, based on data from Transforma Insights 2024.



More Phones Than People

Estimated number of mobile-cellular phone subscriptions vs. world population estimates



* includes postpaid and active prepaid subscriptions that offer voice communications; excludes subscriptions via data cards or USB modems, radio paging and telemetry services

Sources: ITU, World Bank, UN Population Division

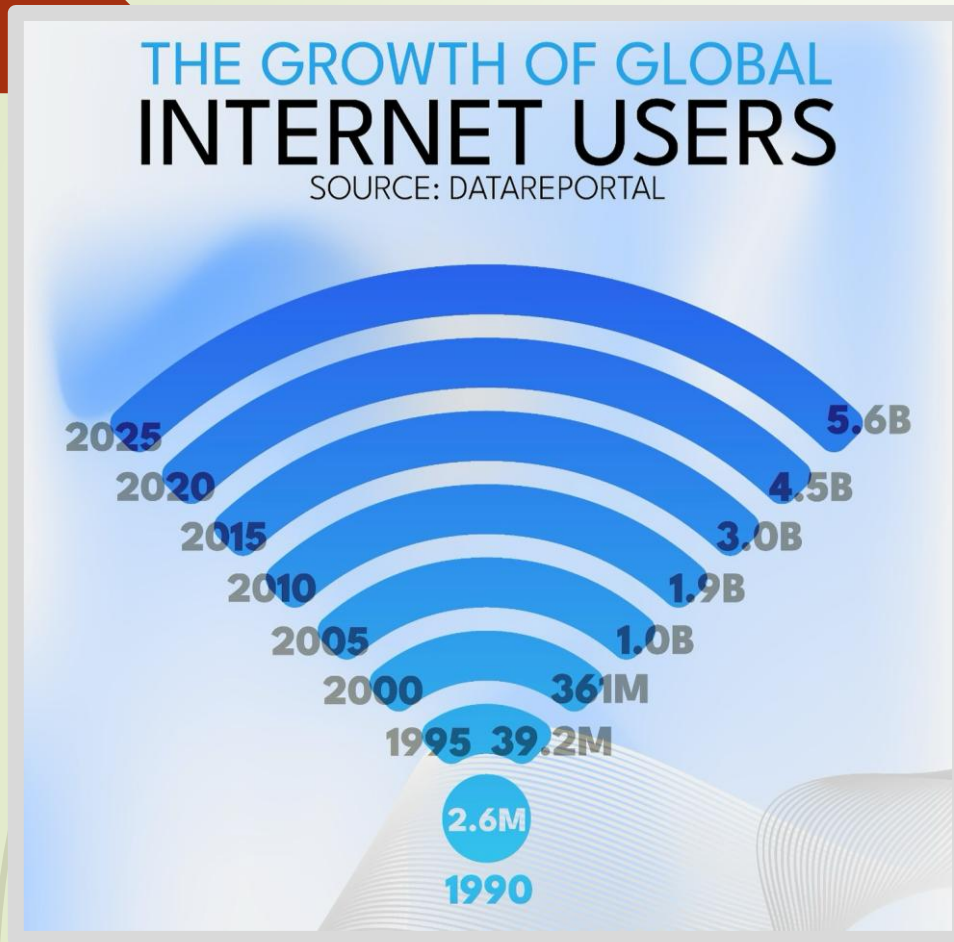


statista

Πηγές:

- <https://www.weforum.org/stories/2023/04/charted-there-are-more-phones-than-people-in-the-world/>
- <https://openknowledge.worldbank.org/server/api/core/bitstreams/692c6149-748f-40dc-b9e6-8e09ba3e47bf/content>

Η τεχνολογική ανισότητα μέρος της συνολικής ανισότητας



2,2 δισεκατομμύρια
συνάνθρωποι μας
Μη Συνδεδεμένοι



Πηγές:

1. <https://www.facebook.com/photo/?fbid=1128585352642440&set=a.224950713005913>
2. https://www.itu.int/hub/publication/D-IND-ICT_MDD.GCR-2025-4/ p.22-23
3. <https://www.facebook.com/photo/?fbid=122210232734146486&set=a.122121627272146486>

Μη συνδεδεμένη “Ανισότητα”

Figure 2.1: Individuals using the Internet

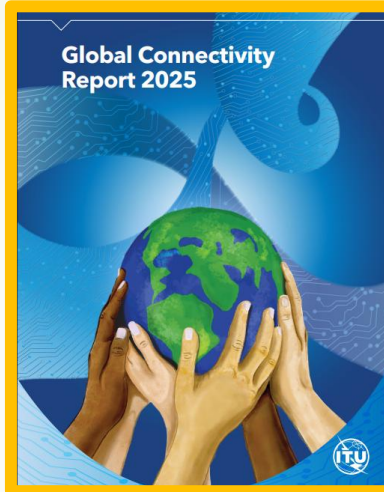
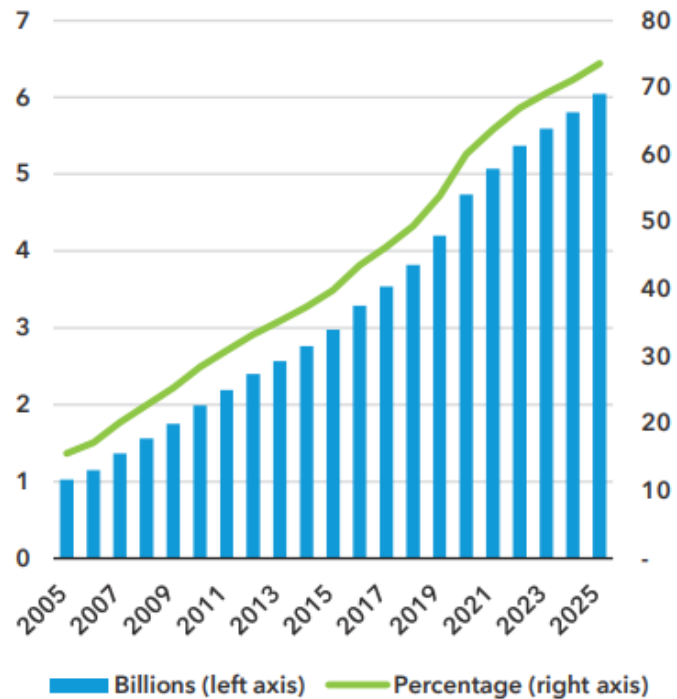
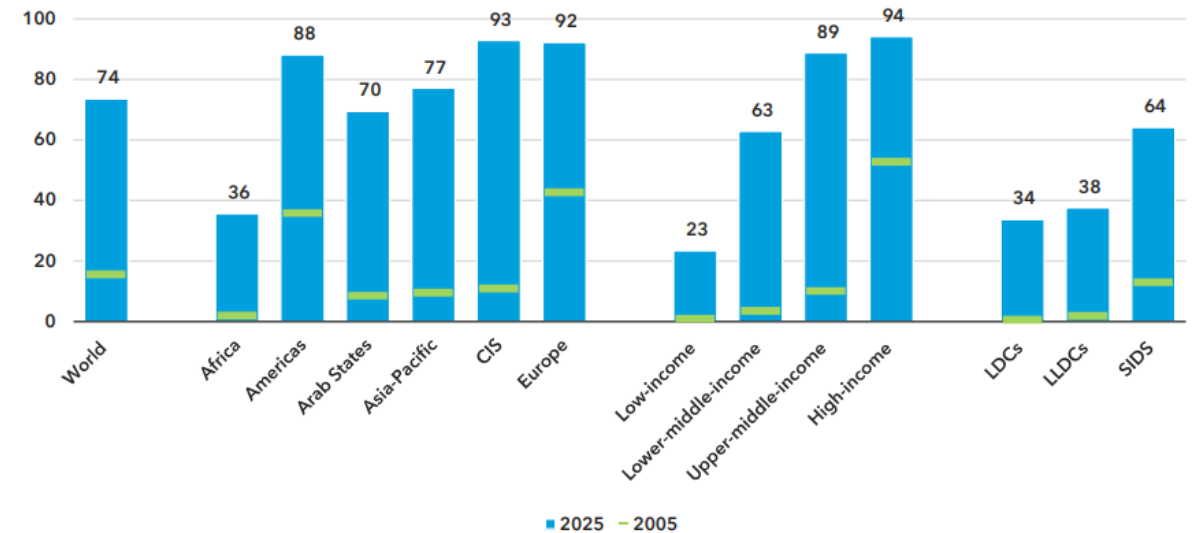


Figure 2.2: Percentage of individuals using the Internet by region and special groups 2005 and 2025



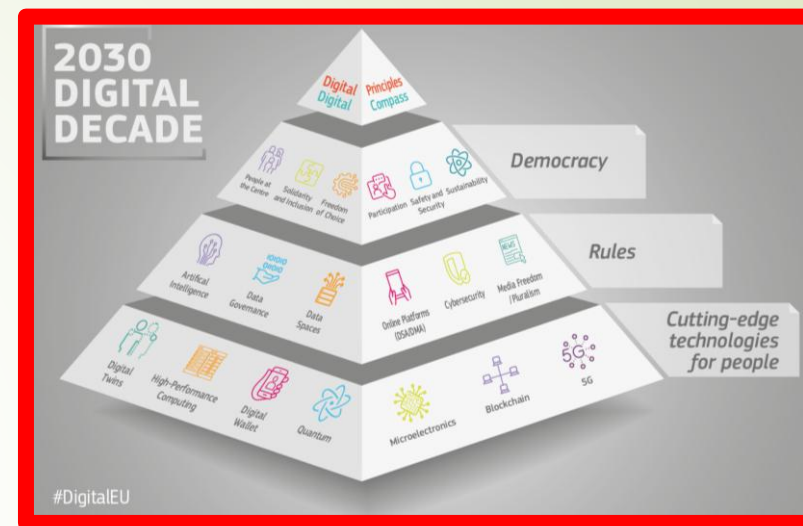
Συνδεδεμένοι 73,17 %
Μη Συνδεδεμένοι 26,83 %

Πηγές:

1. <https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx>
2. https://www.itu.int/hub/publication/D-IND-ICT_MDD.GCR-2025-4/ p.22-23



Στρατηγική Ασφάλειας ΕΕ



- Ένα ασφαλές για το μέλλον περιβάλλον
- Αντιμετώπιση εξελισσόμενων απειλών
- Προστασία από την τρομοκρατία και το οργανωμένο έγκλημα
- Ένα ισχυρό ευρωπαϊκό οικοσύστημα ασφάλειας

Πηγές:

1. https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en
2. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379
3. <https://digital-strategy.ec.europa.eu/el/policies/europes-digital-decade>
4. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package?fbclid=IwAR2IWdrlQMiWv3aBNlJzkdDZVsxj12o6gn7ZK_2edWPuWVlIbhf9Gat_cltM_aem_Abz5czPFhGStxvQmG_U2oaUUIGQD7ogwR0M9948FzcRnZepyGCJv7Uutp6nsyoe1lgGzgPryCwt_wRuLiozYdJW9
5. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0148>

- **Η Στρατηγική Κυβερνοασφάλειας της ΕΕ (2013)**
- **Η οδηγία NIS (2016)** ΚΑΤΑΡΓΗΘΗΚΕ ΜΕ ΟΔΗΓΙΑ **NIS.2 2022/2555/EU (Δεκέμβριος 2022)**
- **N. 4577/2018 φεκ Α-199** Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις.
- **Η Cybersecurity Act 2019 (ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2019/881)**
- **N. 4927/2019 φεκ Α-143** Κύρωση της Συμφωνίας Έδρας μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και του Ευρωπαϊκού Οργανισμού Ασφάλειας Δικτύων και Πληροφοριών (ENISA), «Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA)».
- **N. 4727/2020 ΦΕΚ Α-184** Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις **Κυβερνοασφάλειας της ΕΕ**
- **N. 4961/2022 φεκ Α-146** Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις.
- **N. 5002/2022 φεκ Α-228** Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών
- **N. 5086/2024 φεκ Α-23** Εθνική Αρχή Κυβερνοασφάλειας και λοιπές διατάξεις
- **N. 5099/2024 φεκ Α-48** σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών (Κανονισμός ΕΕ 2022/2065)
- **N. 5160/2024 φεκ Α-195** σχετικά με την ενσωμάτωση της NIS2 (Οδηγίας ΕΕ 2022/2555)
- **N. 5188/2025 φεκ Α-49** Πράξη για την Διακυβέρνηση των Δεδομένων (Κανονισμός ΕΕ/2022/868)

Βασικές Υποδομές & Δίκτυα

Οδηγία NIS (2016/1148/ΕΕ)- NIS2 (2022/2555/ΕΕ)



**Ανάπτυξη στοχευμένων
προσεγγίσεων για
High Value Targets HVTs**



NIS 2

Expanded scope to include more sectors and services as either essential or important entities.



PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR SERVICES



DIGITAL SERVICES SUCH AS SOCIAL NETWORKING SERVICES PLATFORMS AND DATA CENTRE SERVICES



WASTE WATER AND WASTE MANAGEMENT



SPACE



MANUFACTURING OF CERTAIN CRITICAL PRODUCTS (SUCH AS PHARMACEUTICALS, MEDICAL DEVICES, CHEMICALS)



POSTAL AND COURIER SERVICES



FOOD

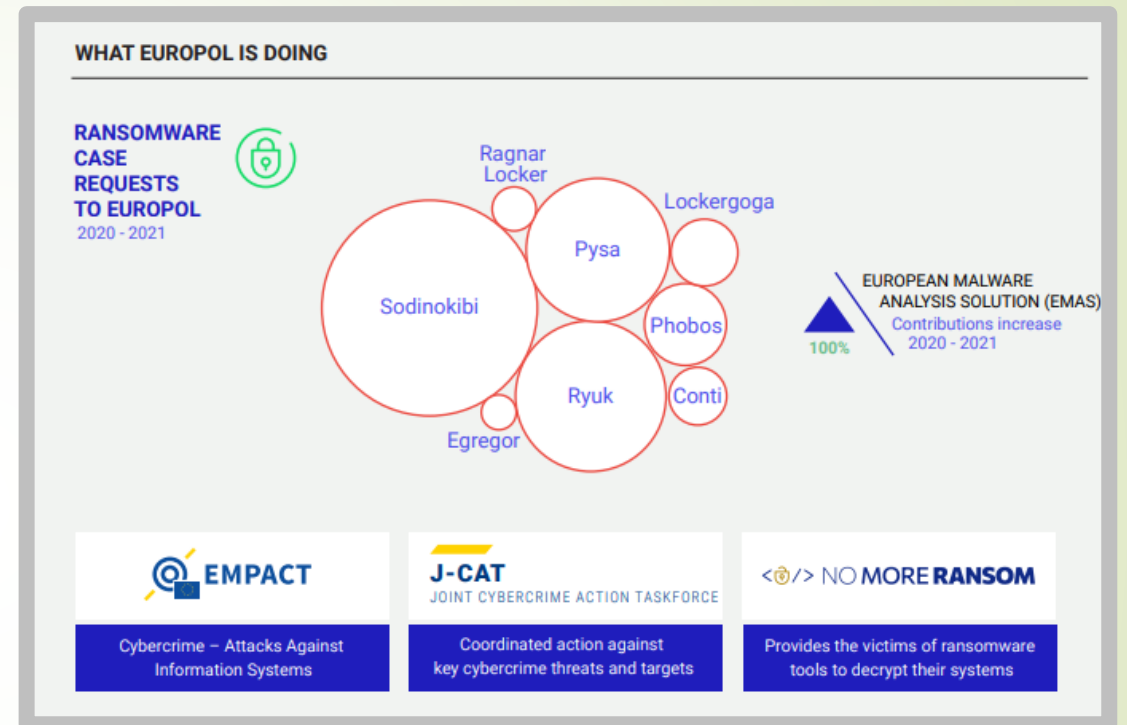


PUBLIC ADMINISTRATION

Πηγές:

1. <https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2>
2. <https://eur-lex.europa.eu/eli/dir/2022/2555>
3. <https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive#ecl-inpage-nis2-directive>
4. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
5. <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>
6. <https://cyber.gov.gr/odigia-nis2/>

Ransomware- Λυτρισμικό



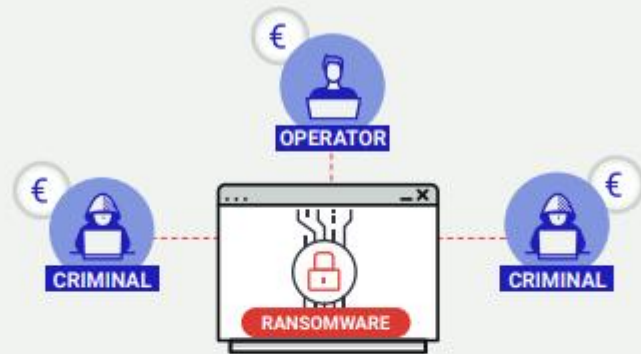
Προσοχή!!!
Δεν δίνουμε ποτέ λύτρα (χρήματα)!!!!

Πηγές:

1. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf p. 14
2. <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>
3. <https://www.bbc.com/news/articles/cqjeej85452o>

Ransomware- Λυτρισμικό

The fight against ransomware



RANSOMWARE AFFILIATE PROGRAMS

MULTI-LAYERED EXTORTION METHODS

Calling clients,
employees, business
partners and/or
journalists to
pressure victim

Threatening
DDoS attack
against victim

Exfiltrating data and threatening publication/action

ένα είδος επίθεσης, όπου οι δράστες αναλαμβάνουν τον έλεγχο των περιουσιακών στοιχείων ενός στόχου και απαιτούν λύτρα σε αντάλλαγμα για την επιστροφή της διαθεσιμότητας των περιουσιακών στοιχείων ή σε αντάλλαγμα για τη δημόσια αποκάλυψη των δεδομένων του στόχου

Πηγές:

1. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf p. 14
2. <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>

Κυβερνοεπιθέσεις - DDOS επιθέσεις

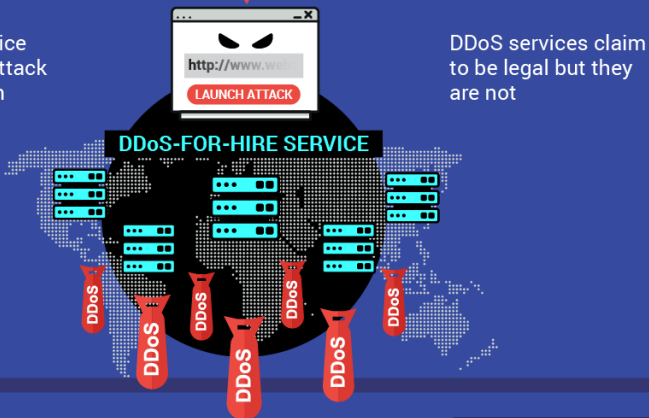
How can DDoS attacks paralyse the internet

1 The criminal hires a DDoS attack service on the internet



Paid via popular online payment services and cryptocurrencies

2 The DDoS service launches the attack using their own attacking infrastructure



DDoS services claim to be legal but they are not

3 The DDoS attack overloads the servers of essential internet services and makes them inaccessible for regular users



INTERNET USERS



EUROPOL

www.europol.europa.eu



Κατανεμημένες επιθέσεις άρνησης
παροχής Υπηρεσιών
Τεχνητή αύξηση του όγκου της
δικτυακής κίνησης στους διακομιστές
του Οργανισμού, διακόπτοντας τις
παρεχόμενες υπηρεσίες στους
νόμιμους χρήστες

Πηγή:

<https://www.europol.europa.eu/publications-documents/how-can-ddos-attacks-paralyse-internet>

Προσωπικά δεδομένα (personal data)

Τι είναι και ποιος τα κατέχει;



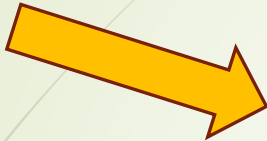
Cloud storage

«Ό,τι είναι δικό μου»

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

Κοινό Σημείο ενδιαφέροντος για
παιδιά, γονείς κι εκπαιδευτικούς

Τα Μαζικά Δεδομένα στο «Νέο Περιβάλλον»



Το κόστος
των
διαρροών



MORE SENSITIVE			LESS SENSITIVE	
SECRET	PERSONAL	PUBLIC	ANONYMIZED	NONPERSONAL
Passwords	Name	Username	What I Click	Weather or Temperature
Passport Number	Home Address	Language	What Websites I Visit	Energy Consumption
Health Data	Email Address	Device Type	What I Search For	
GPS Coordinates	Home Telephone	Cookie Preferences		
Religion	Gender Identity			
Political Affiliation	Date of Birth (in some circumstances)			

Πηγές:

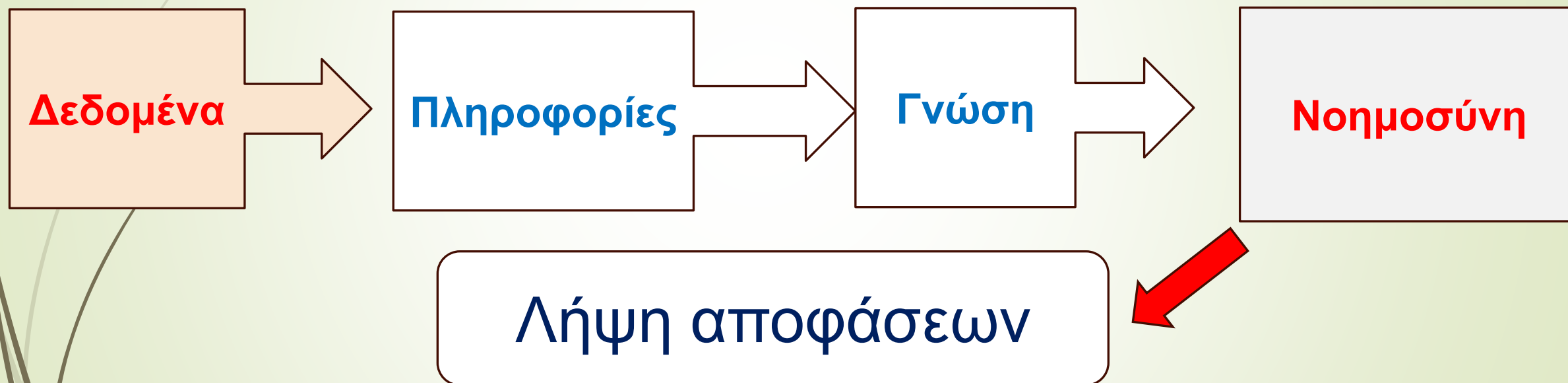
1. <https://cyber.gov.gr/antimetopisi-apeilon/systaseis-pros-polites/>
2. <https://www.cima.ned.org/publication/big-data-not-big-brother>
3. <https://www.dpa.gr/el/polites/gkpd>
4. <https://www.coe.int/en/web/data-protection>
5. https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf
6. <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>
7. <https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection/?tab=publications>
8. https://edps.europa.eu/data-protection/data-protection_en
9. <https://www.facebook.com/photo/?fbid=122202984878146486&set=a.122121627272146486>
10. <https://www.ibm.com/reports/data-breach>



Η αξία των δεδομένων

DIKI or DIKW model

Data -Information- Knowledge -Intelligence/Wisdom



Πηγές:

1. <https://www.systems-thinking.org/dikw/dikw.htm>
2. http://ioc.unesco.org/Oceanteacher/OceanTeacher2/02_InfTchSciCmm/DIKWchain.pdf

Κατανόηση κάποιων κανόνων δικαίου



Άρθρο 21 ΝΟΜΟΣ 4624/2019 Συγκατάθεση ανηλίκου

1. Όταν εφαρμόζεται το άρθρο 6 παράγραφος 1 στοιχείο α) του ΓΚΠΔ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα ανηλίκου, κατά την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών απευθείας σε αυτόν, είναι σύννομη, εφόσον ο ανήλικος έχει συμπληρώσει το 15ο έτος της ηλικίας του και παρέχει τη συγκατάθεσή του.
2. Εάν ο ανήλικος είναι κάτω των 15 ετών η επεξεργασία της παραγράφου 1 είναι σύννομη μόνο μετά την παροχή συγκατάθεσης του νομίμου αντιπροσώπου του.

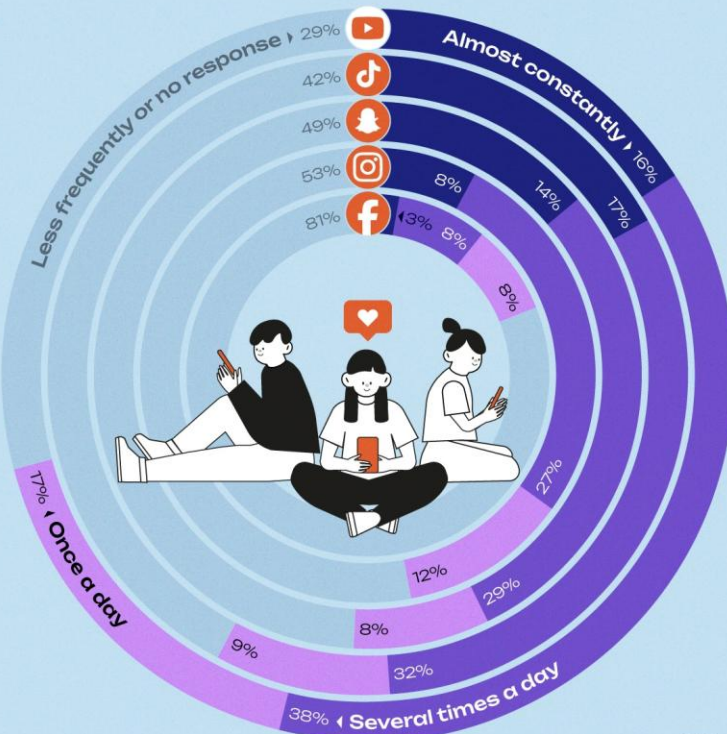
Πηγή:

<https://www.dpa.gr/el/polites/prostasia>

Πλατφόρμες Μέσων Κοινωνικής Δικτύωσης

SOCIAL PLATFORM USAGE AMONG U.S. TEENS

% of U.S. teens (13-17) who say they visit or use the following apps...



Source: Pew Research Center (2023)

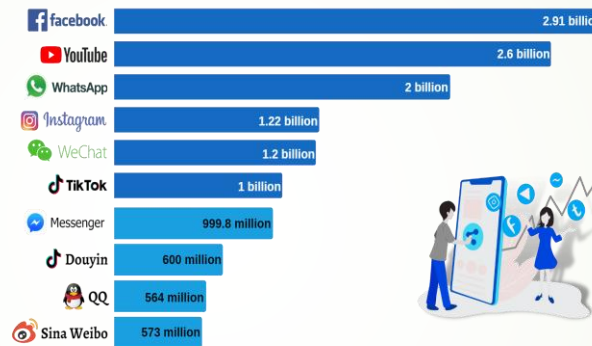
voronoi
BY VISUAL CAPITALIST

Where Data Tells the Story

Download on the
App Store

GET IT ON
Google Play

Most Popular Social Platforms



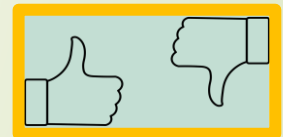
Number of monthly active users

Broadband Search



Source: localiq.com

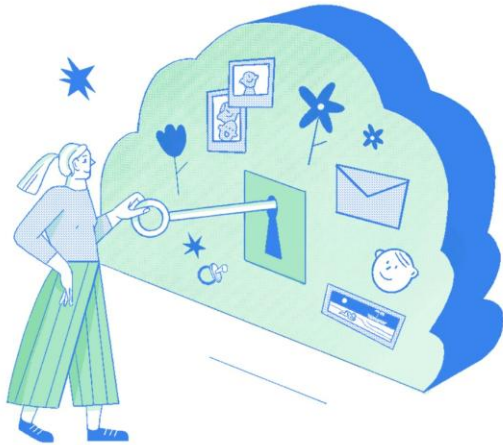
09/02/2009



Πηγές:

- <https://ec.europa.eu/newsroom/rtd/items/713444/en>
- https://techcrunch.com/2009/02/09/facebook-activates-like-button-friendfeed-tires-of-sincere-flattery/?guce_referrer=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAHjAogdfUs5MX2xkxydv8nAaSxh1gYdVW2la_YpxBQnv3X5hYg5TL7pe9boB--joVG9yXiGNvWqKKd44nVm3qUYc-olMwfHj4pyYDd50Ay9O2Z7CBdRoDUiQzyJ1UJG6DoYhHAMxyh6C7OvdF1XTdBupwUD3FN8GTel07yTbr9a
- <https://www.broadbandsearch.net/blog/internet-statistics#post-navigation-0>
- <https://x.com/tutorialspoint/status/1818904743663878399/photo/1>
- <https://www.facebook.com/photo/?fbid=798586115633146&set=a.479638654194562>

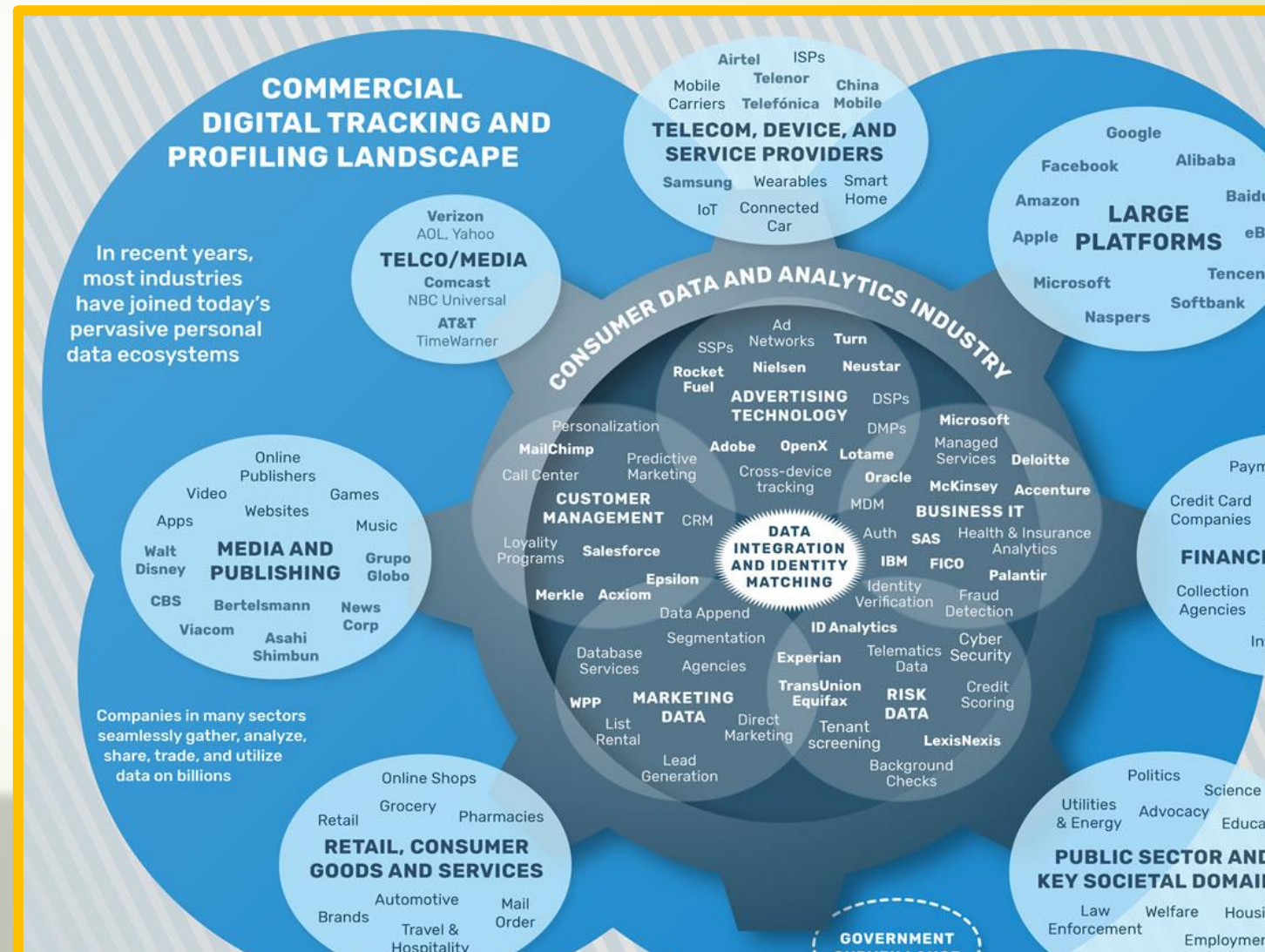
Τα δεδομένα μας στο νέο ψηφιακό περιβάλλον



Cloud storage

Πηγές

1. <https://crackedlabs.org/en/corporate-surveillance/#6>
2. <https://crackedlabs.org/en/corporate-surveillance/#7>
3. https://www.globalencryption.org/parents-guide-to-encryption/?fbclid=IwAR2SiOsZPE_UezZcqykzKCDmold9_0vZOS3j13i0PKzWDUeMW1UFvEzwvvg#parents

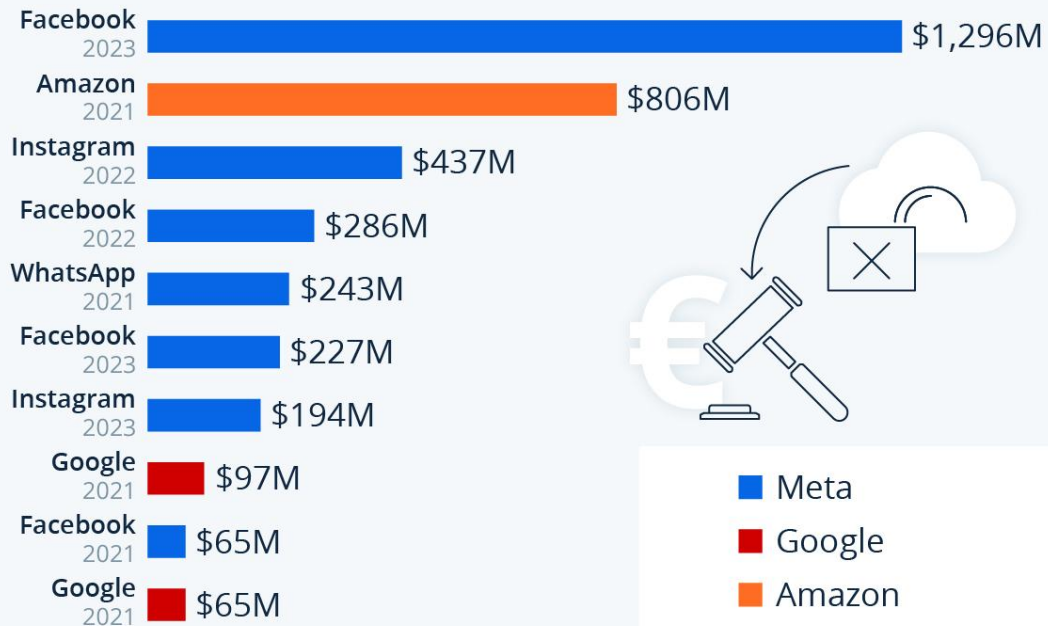


Πρακτικές συνέπειες- Νέα Οικονομία

Πρόστιμα σε Millions – Έσοδα σε Billions

Big Tech, Big Fines

Largest fines for breaching one or more articles of the General Data Protection Regulation in the EU



Converted from euros on May 23, 2023

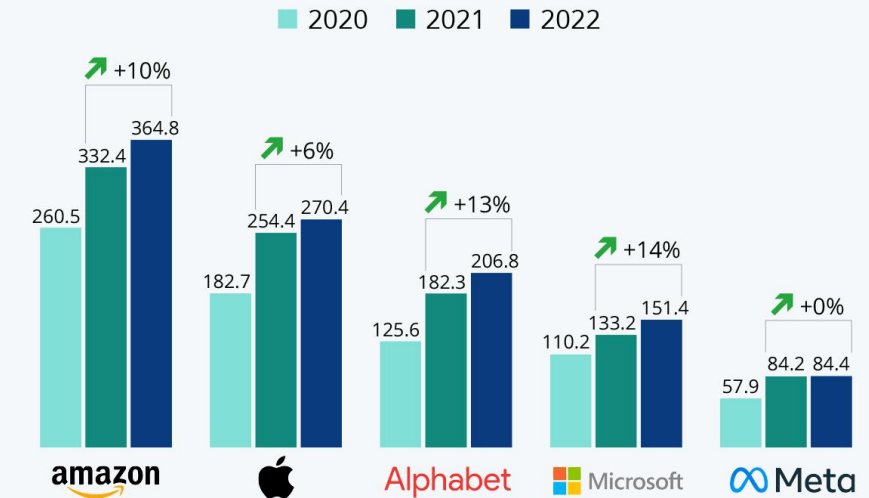
Sources: CMS GDPR Enforcement Tracker, European Data Protection Board



statista

Is Big Tech Growth Losing Steam?

GAMAM revenue in the first nine months of the following years (in billion U.S. dollars)



Source: Company filings



statista

Πηγές:

- <https://www.facebook.com/Statista.Inc/photos/a.168793176566502/5540151162763983/>
- <https://www.statista.com/chart/25691/highest-fines-for-gdpr-breaches/>

ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (PHISHING)

Ο όρος "phishing" αναφέρεται στα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου, που σκοπό έχουν να εξαπατηθούν οι παραλήπτες τους και να γνωστοποιήσουν στους απατεώνες προσωπικές και οικονομικές τους ροφορίες ή κωδικούς ασφαλείας τους.

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ;

Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου:

μπορεί να μοιάζουν πάρα πολύ με τα μηνύματα που στέλνουν στους πελάτες τους οι τράπεζες.

αντιγράφουν το λογότυπο, τα χαρακτηριστικά και το ύφος των πραγματικών μηνυμάτων ηλεκτρονικού ταχυδρομείου.



ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

➤ Διατηρείτε το λογισμικό ενημερωμένο, περιλαμβανομένου του φυλλομετρητή ιστοσελίδων (browser), του αντικού προγραμμάτος (antivirus) και του λειτουργικού συστήματος.

➤ Να είστε ιδιαίτερα προσεκτικοί εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου "τράπεζας" σας ζητά ευαίσθητες πληροφορίες (π.χ. τον κωδικό πρόσβασης του τραπεζικού σας λογαριασμού μέσω internet banking).

➤ Ελέγξτε προσεκτικά το μήνυμα ηλεκτρονικού ταχυδρομείου: συγκρίνετε τη διεύθυνση με τα προηγούμενα πραγματικά μηνύματα από την τράπεζα συνεργασίας σας. Ελέγξτε για ορθογραφικά λάθη και λάθη γραμματικής ή σύνταξης.

➤ Μην απαντάτε σε ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου, αντίθετα προωθήστε το στην τράπεζα συνεργασίας σας, πληκτρολογώντας την ηλεκτρονική της διεύθυνση μόνοι σας.

➤ Μην κάνετε απευθείας κλικ στον ηλεκτρονικό σύνδεσμο (link) και μην πραγματοποιείτε λήψη (download) του επισυναπτόμενου αρχείου, αντίθετα πληκτρολογήστε τη διεύθυνση του ηλεκτρονικού συνδέσμου στον φυλλομετρητή ιστοσελίδων (browser) που χρησιμοποιείτε.

➤ Σε περίπτωση οποιασδήποτε αμφιβολίας, ελέγξτε την ιστοσελίδα ή τηλεφωνήστε στην τράπεζα συνεργασίας σας.

Αλίευση Δεδομένων Phishing



Το πακέτο σας φτάνει στα ΕΛΤΑ αύριο

Θα θέλαμε να σας ενημερώσουμε ότι λάβαμε τα στοιχεία αποστολής σας για το πακέτο UPS UPS#659183201 και θα παραδοθεί στα Ελληνικά Ταχυδρομεία στην Αθήνα για εθνική παράδοση αύριο.

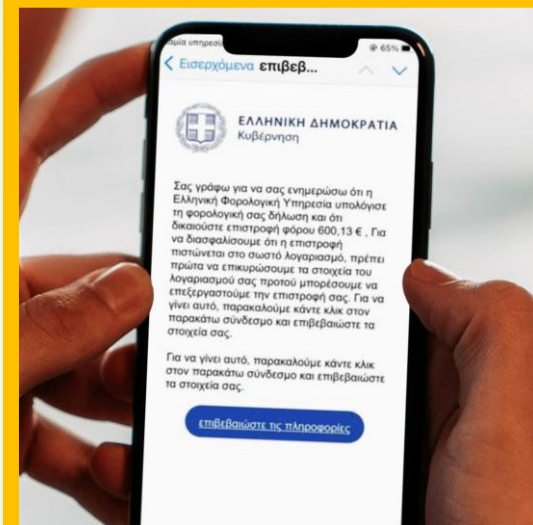
Το πακέτο σας θα αποθηκευτεί στο ΚΕΝΤΡΟ ΔΙΑΛΟΓΗΣ ΑΘΗΝΩΝ μέχρι να επιβεβαιώσετε τα στοιχεία σας:

Λεπτομέρειες

Με εκτίμηση,

ΕΛΤΑ.

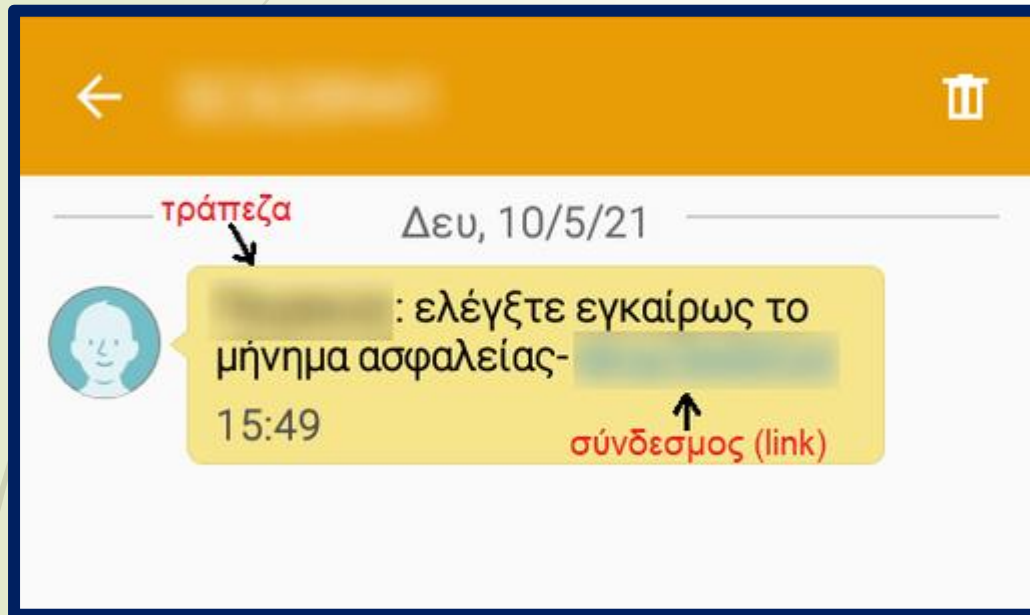
Unsubscribe



Πηγές:

1. <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/e-commerce-tips-and-advice-to-avoid-becoming-fraud-victim>
2. https://www.europol.europa.eu/sites/default/files/documents/report_on_phishing_-_a_law_enforcement_perspective.pdf
3. <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/e-commerce-tips-and-advice-to-avoid-becoming-fraud-victim>
4. <https://www.politica.gr/politica-89-8/g-papaprodromou-diarkis-epikairopoiisi-tis-atzentas-kubernoasfaleias-na-axiopoiithoun-oi-neoi-epistimonες/>
5. <https://www.facebook.com/hellenicpolice/posts/pfbid02btGBuuZe7nx7HTnSsWT8fNtZHfnpu4YAoqK74beG9Ys8rBwFFn7DgPfxkFogcHudl>

Αλίευση Δεδομένων -Smishing



BANK SMISHING SMSs

Smishing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message.



HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account. But...the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

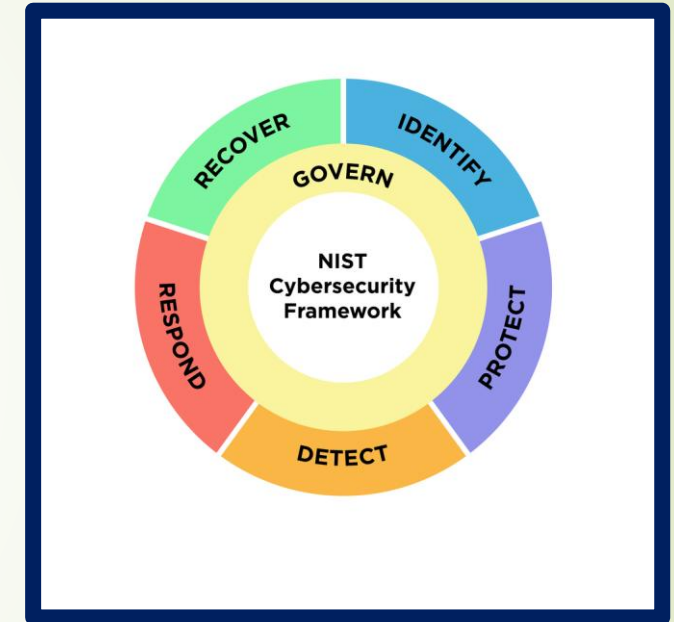
EUROPOL
EC3 | European Cybercrime
Centre

#CyberScams

Πηγές:

1. https://www.europol.europa.eu/sites/default/files/documents/3_phishing_vishing_sms.pdf
2. <https://www.astynomia.gr/odigos-tou-politi/chrisimes-symvoules/symvoules-gia-asfali-prosvasi-sto-diadiktyo/>

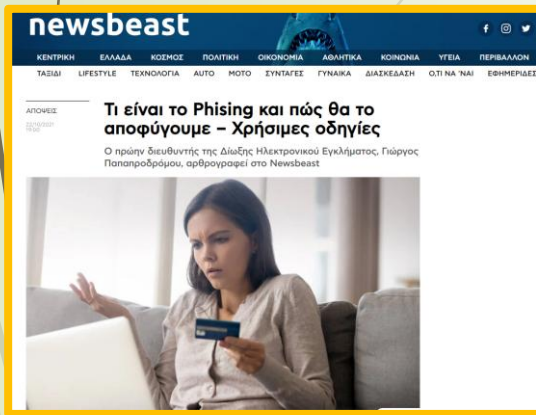
Κακόβουλο Λογισμικό & Αλίευση Δεδομένων



Πηγές:

1. https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf p. 17
2. <https://encyclopedia.kaspersky.com/glossary/trojan-droppers/>
3. <https://www.nist.gov/image/nist-cybersecurity-framework-20-draft>
4. https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf p. 12

Τι είναι το Phishing και πως θα το αποφύγουμε;

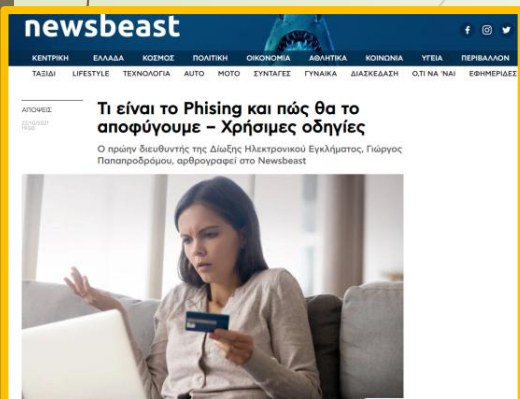


- **Δεν δίνουμε** ποτέ το όνομα χρήστη και τους κωδικούς πρόσβασης από λογαριασμούς (τραπεζικούς κλπ)
- **Δεν ακολουθούμε** συνδέσμους και δεν ανοίγουμε συνημμένα αρχεία από άγνωστους αποστολείς μηνυμάτων (ηλεκτρονικού ταχυδρομείου, sms)
- **Χρησιμοποιούμε** ασφαλέστερους κωδικούς (*συνδυασμός γραμμάτων, αριθμών, συμβόλων*)
- **Αποφεύγουμε** τον ίδιο κωδικό για κάθε λογαριασμό μας
- **Αλλάζουμε** τον κωδικό σε τακτά χρονικά διαστήματα
- **Δεν δίνουμε** τον αριθμό κινητού τηλεφώνου μας στα μέσα κοινωνικής δικτύωσης
- **Επισκεπτόμαστε** ασφαλείς δικτυακούς τόπους οργανισμών

Πηγή:

<https://www.newsbeast.gr/apopseis/arthro/7933191/ti-einai-to-phising-kai-pos-tha-to-apofygoume-chrisimes-odigies>

Τι είναι το Phishing και πως θα το αποφύγουμε;



- **Προσέχουμε** για συντακτικά και ορθογραφικά λάθη στα μηνύματα μας
- Οι συσκευές μας να διαθέτουν **επικαιροποιημένο λογισμικό**
- **Παρακολουθούμε** συχνά την **κίνηση του λογαριασμού** μας
- **Παρακολουθούμε** την **λειτουργία του κινητού** μας
- **Αναφέρουμε** οπωσδήποτε οποιαδήποτε απόπειρα απάτης
- **Γνωρίζουμε** την **διαδικασία αμφισβήτησης συναλλαγής** που ακολουθεί η τράπεζα μας αλλά και τα δικαιώματά μας ως καταναλωτές-
(προσοχή το πρώτο εικοσιτετράωρο)
- **Συζητούμε** το θέμα με το άμεσο περιβάλλον μας και αναζητούμε βοήθεια *(Η σιωπή βοηθά και ενθαρρύνει τους απατεώνες του Κυβερνοχώρου)*
- **Επισκεπτόμαστε** τον **επίσημο** δικτυακό τόπο των φορέων και οργανισμών

Πηγή:

<https://www.newsbeast.gr/apopseis/arthro/7933191/ti-einai-to-phising-kai-pos-tha-to-apofygoume-chrisimes-odigies>

Τα παιδιά προτεραιότητα των κοινωνιών



Janus
Korczak
6/8/1942

- ❑ Σύνταγμα 1975/1986/2001/2008/2019 **άρθρο 21**
- ❑ The United Nations Convention on the Rights of the Child (UNCRC) **20/11/1989**
- ❑ ΕΣΔΑ **άρθρο 14**
- ❑ Χάρτης Θεμελιωδών Δικαιωμάτων **άρθρο 13, 14, 34**
- ❑ Ν. 2101/1992 ΦΕΚ Α 192 **Κύρωση της Διεθνούς Σύμβασης για τα Δικαιώματα του Παιδιού**

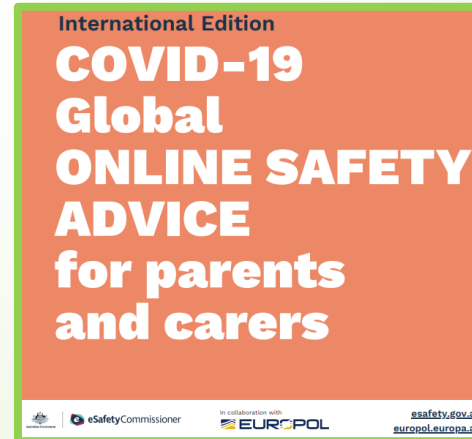
Παιδιά θύματα κυβερνοεγκλημάτων

Connected baby monitor



Πηγές:

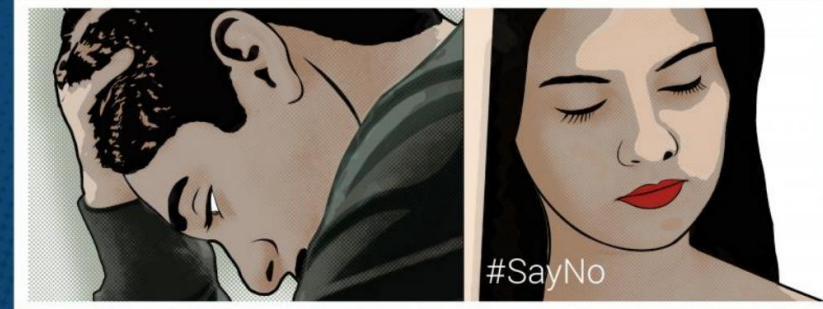
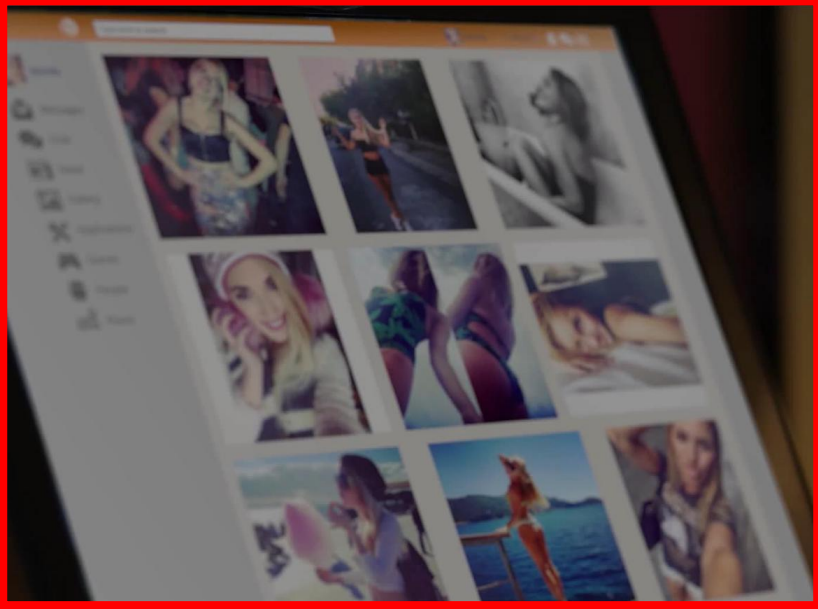
1. <https://www.europol.europa.eu/publications-documents/covid-19-global-online-safety-advice-for-parents-and-carers>
2. <https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik>
3. <https://op.europa.eu/el/publication-detail/-/publication/ddf757c8-53ea-11ec-91ac-01aa75ed71a1>
4. https://www.globalencryption.org/parents-guide-to-encryption/?fbclid=IwAR2SiOsZPE_UezZcqykzkCdmold9_0vZOS3j13i0PKzWDUeMW1UFvEzwvvg#parents
5. <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse>





STOP CHILD ABUSE
TRACE an OBJECT

Καμπάνια της Europol – Say No



**Online child sexual coercion
and extortion is a crime**

Has this
happened to you?
SAY NO!

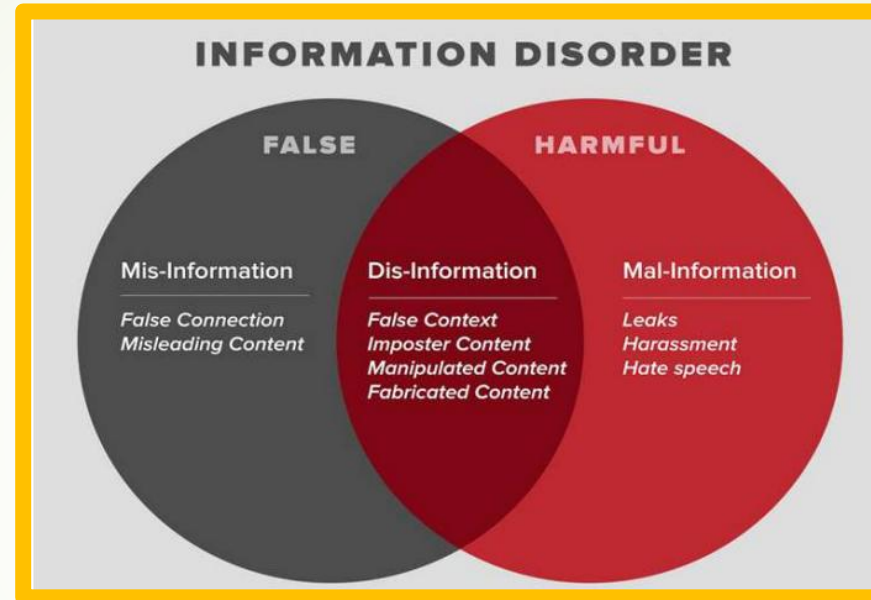
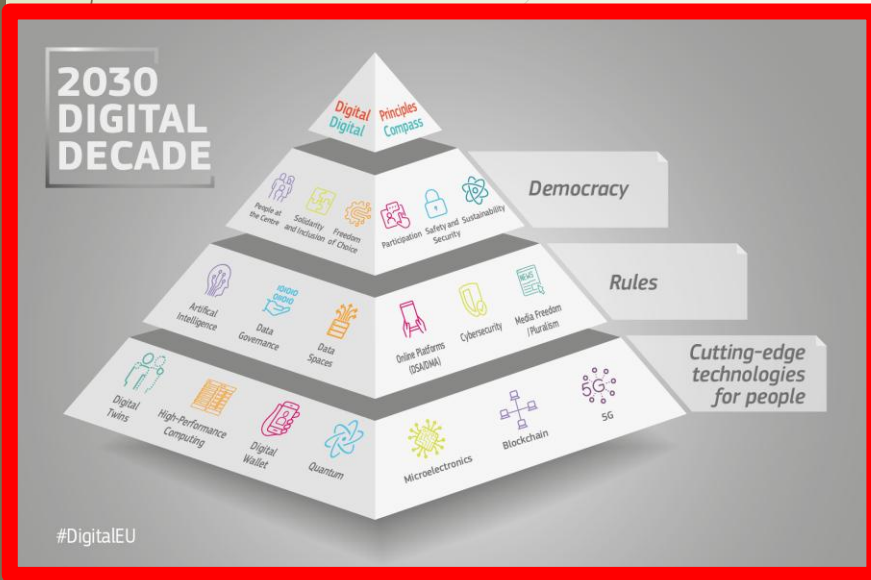
**We can help you.
You are not alone.**

Launched on 19 June 2017

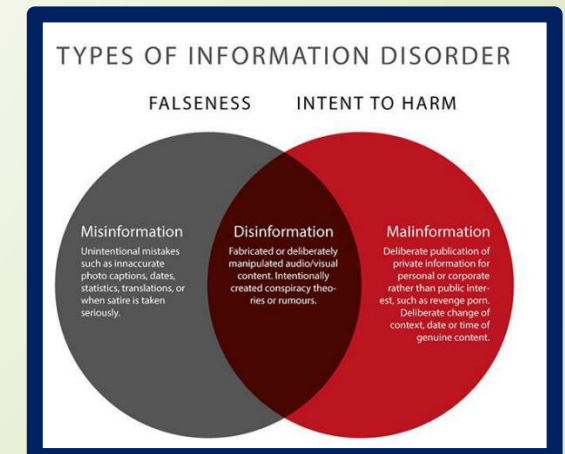
Πηγές

1. <https://eucpn.org/sites/default/files/document/files/3.Say%20No.pdf>
2. <https://www.youtube.com/playlist?list=PL34rDtSSoVq8XYUUVrWCNqCdRftckqzTi>
3. https://www.kodiko.gr/nomologia/document_pdf/530229
4. <https://www.europol.europa.eu/stopchildabuse>

Απρεπής εκφορά του λόγου & ψεύτικες ειδήσεις



- Πηγές
1. <https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77> p. 5, 6, 17, 21
 2. https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210622_Hybrid_CoE_Paper_7_Geopolitics_and_strategies_in_cyberspace_WEB.pdf
 3. https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf p. p1, 98
 4. <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>
 5. <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>
 6. <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>
 7. <https://itif.org/publications/2022/10/11/how-to-address-political-speech-on-social-media-in-the-united-states/?fbclid=IwAR3L6vNUXxnQ7n5RGhecgh9tuIMTYKGupGXm-XyhweVPsJ55rXptiPA0LbM>
 8. <https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech>





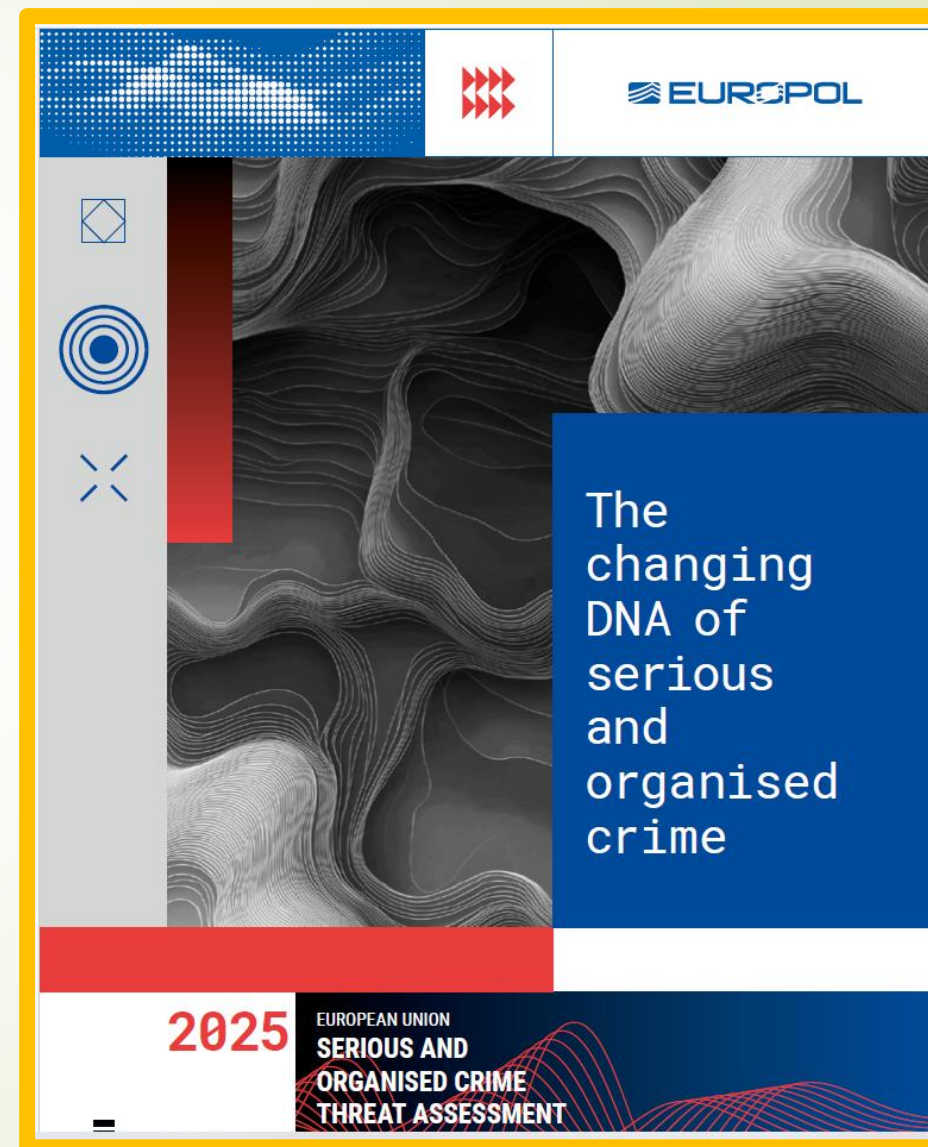
Εκστρατείες παραπληροφόρησης

Additionally, these networks are instrumental for propaganda campaigns aimed at spreading disinformation and influencing political systems. These campaigns often involve fake social media accounts, coordinated troll operations, and manipulated news content, which serve the strategic interests of hybrid threat actors by weakening opponents from within.

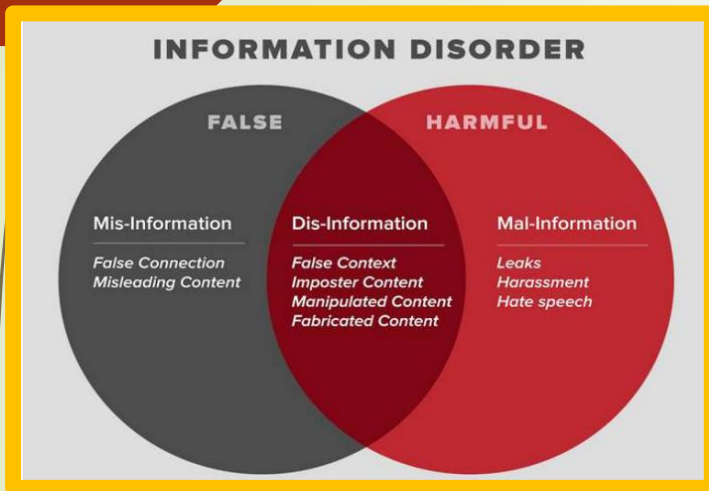
Δημοσιεύθηκε 20/03/2025

Πηγές:

1. <https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime>
2. <https://www.consilium.europa.eu/en/policies/hybrid-threats/>
3. <https://www.hybridcoe.fi/hybrid-threats/>



Fake news & καλές πρακτικές αντιμετώπισης



BEFORE YOU SHARE, THINK:

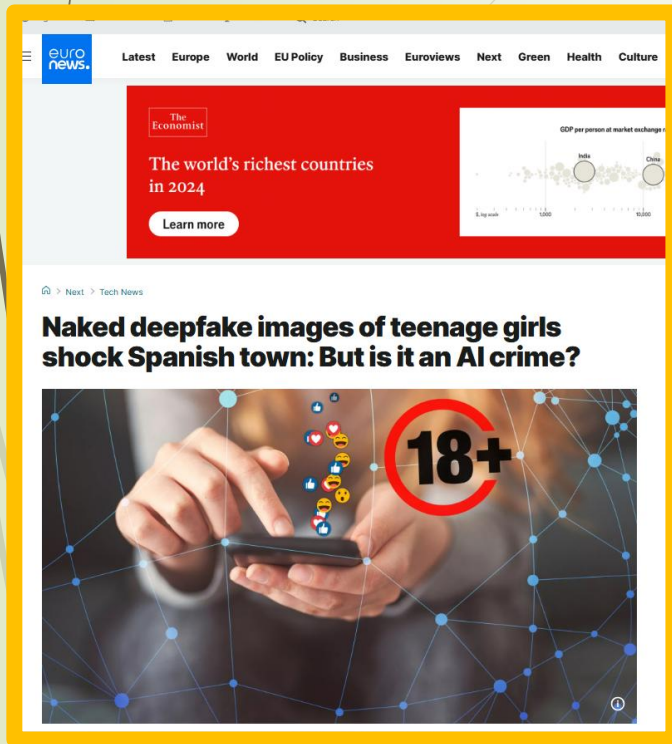
- ⏸ WHO made it?
- ⏸ WHAT is the source?
- ⏸ WHERE did it come from?
- ⏸ WHY are you sharing this?
- ⏸ WHEN was it published?

Πηγές

1. <https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77> p. 5, 6, 17, 21
2. https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210622_Hybrid_CoE_Paper_7_Geopolitics_and_strategies_in_cyberspace_WEB.pdf
3. https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf p. p1, 98
4. <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>
5. <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>
6. <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>
7. <https://itif.org/publications/2022/10/11/how-to-address-political-speech-on-social-media-in-the-united-states/?fbclid=IwAR3L6vNUXxnQ7n5RGhecGh9tulMTYKGupGXm-XyhweVPsJ55rXptiPA0LbM>
8. <https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech>
9. <https://www.facebook.com/photo?fbid=1069070901915601&set=a.577863084369721>



Εκφοβισμός στον Κυβερνοχώρο (Cyber-Bullying)



**Εκφοβισμός, μέσω της χρήσης
ψηφιακών τεχνολογιών (2015, UNICEF)**

*Διαδικτυακή επιθετική συμπεριφορά (μέσω
μηνυμάτων, κλήσεων, αναρτήσεων, διαμοιρασμού
επιβλαβούς περιεχομένου, κλπ)
από τον θύτη προς το θύμα*

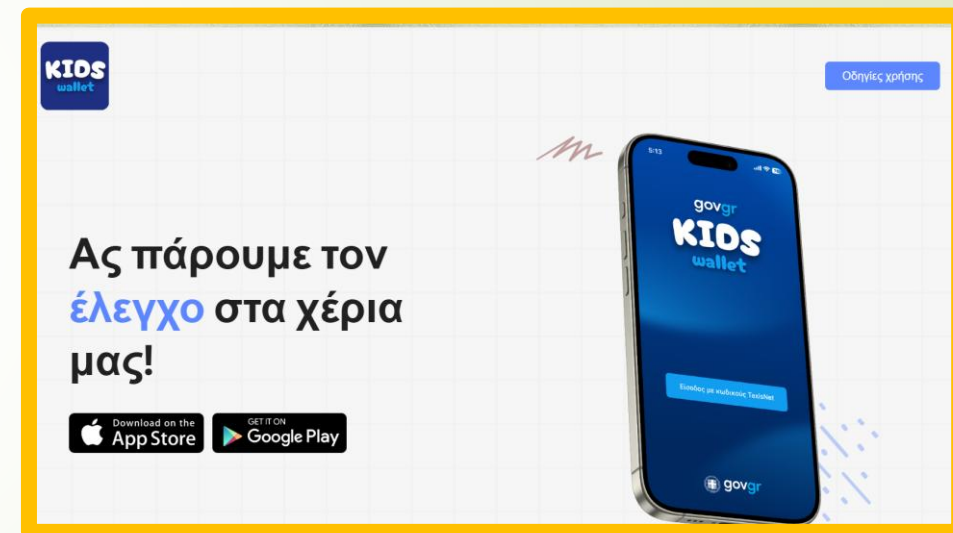
Πρόκληση βλάβης, επαναληπτικότητα, αναντιστοιχία
δύναμης θύτη-θύματος



Πηγές:

1. <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>
2. <https://www.gov.gr/sdg/healthcare/national-emergency-numbers/general/116111/>
3. <https://www.stopbullying.gov/cyberbullying/what-is-it>
4. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2826
5. <https://www.reuters.com/world/europe/spain-readies-age-checking-tech-protect-children-adult-online-content-2023-12-14/>
6. <https://www.euronews.com/next/2023/09/24/spanish-teens-received-deepfake-ai-nudes-of-themselves-but-is-it-a-crime>

Νέα Πλατφόρμα Parco - Kids Wallet app



Πηγές:

1. <https://parco.gov.gr/>
2. <https://www.minocp.gov.gr/2024/11/12/12-11-2024-safe-youth-i-episimi-parousiasi-tis-neas-ilektronikis-efarmogis-gia-tin-prostasia-ton-anilikon/>
3. <https://kidswallet.gov.gr/>

Online Gaming – Διαδικτυακό Παιχνίδι όταν γίνεται θετικά είναι παιχνίδι ζωής



Θετικά

- Διασκέδαση – ψυχαγωγία
- Δημιουργικότητα
- Ανάπτυξη Δεξιοτήτων και Στρατηγικής

Αρνητικά

- Έκθεση προσωπικών δεδομένων
- Εκφοβισμός στο Διαδίκτυο
- Πρόσβαση σε ακατάλληλο περιεχόμενο
- Ανεπιθύμητες επαφές
- Ενθάρρυνση για τυχερά παιχνίδια
- Πολύς χρόνος στην οθόνη - εθισμός

Πηγές

1. <https://www.gamingcommission.gov.gr/index.php/ypeythino-paixnidi/prolipsi-kai-katapolemisi-toy-ethismoy>
2. <https://www.esafety.gov.au/sites/default/files/2022-01/eSafety%20parent%20guide%20to%20online%20gaming.pdf>
3. <https://www.who.int/news-room/questions-and-answers/item/addictive-behaviours-gaming-disorder>

Ενημέρωση γονέων με **χρήσιμες οδηγίες**

ΕΧΕΙΣ
ΦΩΝΗ
ΕΙΜΑΣΤΕ
ΔΙΠΛΑ ΣΟΥ

#exeisfoni

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 πληροφορηθούν 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 (screenshot 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

Πηγή:

<https://www.astynomia.gr/odigos-tou-politi/chrisimes-symvoules/symvoules-gia-asfali-prosvasi-sto-diadiktyo/>

Προστασία **ανηλίκων** καταναλωτών



Οι προμηθευτές **δεν διαθέτουν** στην αγορά προϊόντα, τα οποία λόγω της μορφής, εικόνας και χρήσης, για την οποία προορίζονται ή του τρόπου διάθεσής και προβολής τους:

- α) ενέχουν **κινδύνους** για την ομαλή ψυχική, πνευματική ή ηθική ανάπτυξη των ανήλικων καταναλωτών,
- β) εκθέτουν τους ανήλικους καταναλωτές σε **κίνδυνο σεξουαλικής θυματοποίησης ή εκμετάλλευσης**.

Οι προμηθευτές **δεν προβάλλουν** προϊόντα που απευθύνονται σε ανήλικους καταναλωτές, με τρόπο που στρεβλώνει την εικόνα της παιδικής ηλικίας, ιδίως μέσω της **χρήσης προωθητικών ενεργειών που περιέχουν μηνύματα με σεξουαλικό περιεχόμενο ή σεξουαλικά υπονοούμενα**.

Άρθρο 7α Ν 2251/1994 όπως τροποποιήθηκε με άρθρο 21 Ν. 5019/2023, Ν. 5099/2024

Πηγές:

1. <https://kataggelies.mindev.gov.gr/%CE%B5%CE%BD%CE%B7%CE%BC%CE%AD%CF%81%CF%89%CF%83%CE%B7-%CE%BA%CE%B1%CF%84%CE%B1%CE%BD%CE%B1%CE%BB%CF%89%CF%84%CF%8E%CE%BD/%CE%B1%CE%BD%CE%AE%CE%BB%CE%B9%CE%BA%CE%BF%CF%82-%CE%BA%CE%B1%CF%84%CE%B1%CE%BD%CE%B1%CE%BB%CF%89%CF%84%CE%AE%CF%82/>
2. https://mitos.gov.gr/index.php/%CE%94%CE%94:%CE%9A%CE%B1%CF%84%CE%B1%CE%B3%CE%B3%CE%B5%CE%BB%CE%AF%CE%B1/_%CE%91%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC_%CF%83%CF%84%CE%B7%CE%BD_%CE%95%CF%80%CE%B9%CF%84%CF%81%CE%BF%CF%80%CE%AE_%CE%A0%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82_%CE%91%CE%BD%CE%B7%CE%BB%CE%AF%CE%BA%CF%89%CE%BD
3. <https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act>

Προστασία **ανηλίκων** καταναλωτών



Προϊόντα που παραβιάζουν τις απαγορεύσεις θεωρούνται **ιδίως** τα προϊόντα που άμεσα ή έμμεσα:

- α) προκαλούν **φόβο** ή ανασφάλεια στους ανήλικους,
- β) παροτρύνουν σε παράνομη ή **επιθετική συμπεριφορά** ή χρήση βίας,
- γ) παροτρύνουν σε συμπεριφορές **καταστροφής** του περιβάλλοντος,
- δ) παροτρύνουν σε συμπεριφορές **κακοποίησης ζώων**,
- ε) καλλιεργούν **διακρίσεις** λόγω φυλής, φύλου, θρησκείας, ιθαγένειας, αναπηρίας ή σεξουαλικού προσανατολισμού,
- στ) εγείρουν, άμεσα ή έμμεσα, πρόωρα, τον ερωτισμό μέσω λεκτικών ή εικονικών αναπαραστάσεων με **σεξουαλικά μηνύματα που δεν συνάδουν με την εικόνα της παιδικής ηλικίας** και τα ιδιαίτερα χαρακτηριστικά αυτής,
- ζ) αναπαράγουν **στερεότυπα** που θίγουν την ισότητα των δύο φύλων,
- η) παροτρύνουν σε **πράξεις** που δεν συνάδουν με ευρέως καθιερωμένα **ηθικά πρότυπα και αξίες**,
- θ) παροτρύνουν τους ανήλικους στη **συμμετοχή σε τυχερά παίγνια** ή προσομοιώνουν τυχερά παίγνια δημιουργώντας **κίνδυνο εθισμού**,
- ι) παροτρύνουν σε χρήση **ναρκωτικών ουσιών**,
- ια) μπορεί να **εκθέτουν** τους ανήλικους σε **κίνδυνο σεξουαλικής θυματοποίησης** ή εκμετάλλευσης.

Άρθρο 7α Ν 2251/1994 όπως τροποποιήθηκε με άρθρο 21 Ν. 5019/2023, Ν. 5099/2024

Πηγές:

1. <https://kataggelies.mindev.gov.gr/%CE%B5%CE%BD%CE%B7%CE%BC%CE%AD%CF%81%CF%89%CF%83%CE%B7-%CE%BA%CE%B1%CF%84%CE%B1%CE%BD%CE%B1%CE%BB%CF%89%CF%84%CF%8E%CE%BD/%CE%B1%CE%BD%CE%AE%CE%BB%CE%B9%CE%BA%CE%BF%CF%82-%CE%BA%CE%B1%CF%84%CE%B1%CE%BD%CE%B1%CE%BB%CF%89%CF%84%CE%AE%CF%82/>
2. https://mitos.gov.gr/index.php/%CE%94%CE%94:%CE%9A%CE%B1%CF%84%CE%B1%CE%B3%CE%B3%CE%B5%CE%BB%CE%AF%CE%B1/_%CE%91%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC_%CE%83%CF%84%CE%B7%CE%BD_%CE%95%CF%80%CE%B9%CF%84%CF%81%CE%BF%CF%80%CE%AE_%CE%A0%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82_%CE%91%CE%BD%CE%B7%CE%BB%CE%AF%CE%BA%CF%89%CE%BD
3. <https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act>

Τι μας προτείνει ο Παγκόσμιος Οργανισμός Υγείας



Όρια και
περιθώρια



Avoid eye strain and headaches
Follow the 20-20-20 rule

After 20
minutes
spent using
a screen



Look at an
object 20 feet
(6m) away



For at least
20 seconds



Λιγότερη οθόνη
& περισσότερη κίνηση



Πηγές:

1. <https://www.facebook.com/WHO/posts/1771269776251731>
2. <https://www.who.int/standards/classifications/frequently-asked-questions/gaming-disorder>
3. <https://twitter.com/WHO/status/1699044996995854779>

Τεχνολογία και Περιβάλλον: Ορθολογική χρήση των διαθέσιμων πόρων



Λιγότερη **ενέργεια**
& **περισσότερη**
βιωσιμότητα

Όρια και **περιθώρια**



Πηγές:

1. <https://sdgs.un.org/topics/technology>
2. https://www.epa.gov/recycle/electronics-donation-and-recycling?fbclid=IwAR0k_duNkMC7zuwo9EMFFL8hEsD3vZBbIPwNkg38O6RgGgzlqZUpnj-Z0_A
3. <https://www.weforum.org/agenda/2023/12/green-tech-multiplier-climate-change-goals-cop28/>
4. <https://riversafe.co.uk/resources/tech-blog/how-to-reduce-the-carbon-footprint-of-your-cybersecurity-operations/>
5. <https://www.naftemporiki.gr/techscience/1616449/kyvernoasfaleia-me-perivallontiko-apotypoma/>

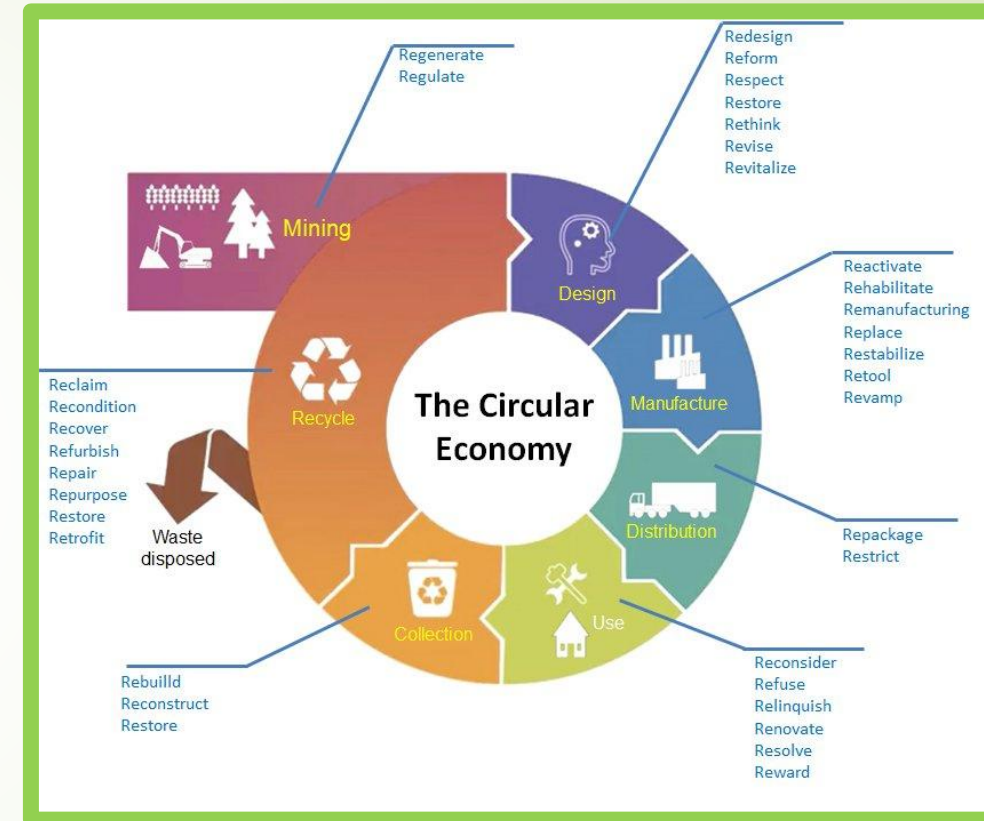
Τεχνολογία και Περιβάλλον: Κυκλική Οικονομία



Recycling your cell phone recovers valuable resources, saves energy, and reduces greenhouse gas emissions.



www.epa.gov/recycle



Πηγές:

1. <https://sdgs.un.org/topics/technology>
2. https://www.epa.gov/recycle/electronics-donation-and-recycling?fbclid=IwAR0k_duNkMC7zuwo9EMFFL8hEsD3vZBbIPwNkg38O6RgGgzlqZUpnj-Z0_A
3. <https://www.weforum.org/agenda/2023/12/green-tech-multiplier-climate-change-goals-cop28/>
4. <https://riversafe.co.uk/resources/tech-blog/how-to-reduce-the-carbon-footprint-of-your-cybersecurity-operations/>
5. <https://www.gdrc.org/uem/waste/more-3r.html>
6. <https://www.naftemporiki.gr/techscience/1616449/kyvernoasfaleia-me-perivallontiko-apotypoma/>

Πρακτικές Συμβουλές - Συσκευές και κωδικοί

- **Χρησιμοποιούμε** λογισμικό προστασίας από ιούς σε όλες τις ψηφιακές μας συσκευές.
- **Διατηρούμε** ενημερωμένο το λογισμικό των συσκευών μας.
- **Είμαστε προσεκτικοί** κατά την περιήγησή μας στο διαδίκτυο,
- **Αποφεύγουμε** να κάνουμε κλικ σε ύποπτους συνδέσμους, αναδυόμενα παράθυρα ή παράθυρα διαλόγου.
- **Σκεφτόμαστε διπλά πριν κάνουμε κλικ** σε συνδέσμους ή συνημμένα αρχεία μέσα σε απροσδόκητα μηνύματα ηλεκτρονικού ταχυδρομείου.
- **Ορίζουμε** μοναδικούς κωδικούς πρόσβασης.
- **Δημιουργούμε ισχυρούς** κωδικούς πρόσβασης.
- **Ενεργοποιούμε** τη λειτουργία ελέγχου ταυτότητας πολλαπλών παραγόντων.



Πηγές:

1. <https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals>
2. <https://www.cisa.gov/secure-our-world/use-strong-passwords?fbclid=IwAR3zicRJ4rBYL2JO35hOgcPPxzEEPp1eLxIZqcXZ4vQFEWDSwrDdJwTzCe0>

Κυβερνοεπιθέσεις - DDoS επιθέσεις



THIS WEBSITE HAS BEEN SEIZED

The FBI has seized this website for operating as a DDoS-for-hire service. This action has been taken in conjunction with Operation PowerOFF, a coordinated international law enforcement effort to dismantle criminal DDoS-for-hire services worldwide. DDoS attacks are illegal.

Law enforcement agencies have seized databases and other information relating to these services. **Anyone operating or utilizing a DDoS service is subject to investigation, prosecution, and other law enforcement action.**

For more information, please visit:
<https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks>

Επιχείρηση
Power Off
15-12-2022

- Με αμοιβή μόλις 10 ευρώ, κάθε άτομο με χαμηλές γνώσεις μπορεί να εξαπολύσει επιθέσεις DDoS με το πάτημα ενός κουμπιού, βγάζοντας εκτός λειτουργίας ολόκληρους ιστότοπους και δίκτυα, κατακλύζοντάς τα με κίνηση.
- Η ζημία που μπορούν να προκαλέσουν στα θύματα μπορεί να είναι σημαντική, παραλύοντας οικονομικά τις επιχειρήσεις και στερώντας από τους πολίτες βασικές υπηρεσίες που προσφέρουν οι τράπεζες, τα κυβερνητικά ιδρύματα και οι αστυνομικές δυνάμεις.

Πηγή:

<https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-against-ddos-services-shuts-down-most-popular-platforms>

Νέα δωρεάν χρηστικά εργαλεία, προϊόντα της διεθνούς συνεργασίας

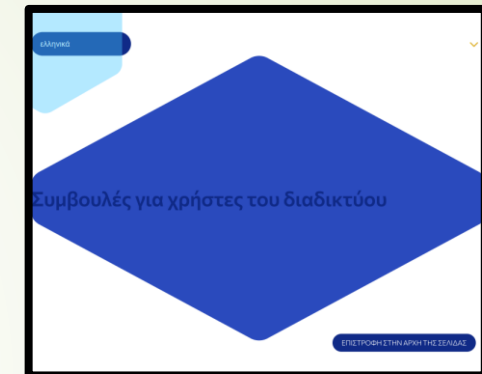
< /> NO MORE RANSOM

Συμβουλές για χρήστες του διαδικτύου

Δημιουργείτε τακτικά αντίγραφα ασφαλείας των δεδομένων που είναι αποθηκευμένα στον υπολογιστή σας, έτσι ώστε μια μόλυνση από λυτρισμικό να μην καταστρέψει τα προσωπικά σας δεδομένα για πάντα.

Είναι καλύτερο να δημιουργήσετε δύο αντίγραφα ασφαλείας: ένα που θα αποθηκευτεί στο σύννεφο (θυμηθείτε να χρησιμοποιήσετε μια υπηρεσία που δημιουργεί ένα αυτόματο αντίγραφο ασφαλείας των αρχείων σας) και ένα για φυσική αποθήκευση (φορητός σκληρός δίσκος, φορητός υπολογιστής κ.λπ.). Αποσυνδέστε τα από τον υπολογιστή σας όταν τελειώσετε.

Τα Windows και η Apple διαθέτουν τους υπολογιστές τους με ενσωματωμένες λειτουργίες δημιουργίας αντιγράφων ασφαλείας στο cloud, όπως το κανονικό αντίγραφο ασφαλείας των Windows ή το Apple Time Machine. Τα αντίγραφα ασφαλείας θα σας βοηθήσουν επίσης αν διαγράψετε κατά λάθος ένα κρίσιμο αρχείο ή αν συμβεί οτιδήποτε με το σκληρό σας δίσκο.



NO MORE RANSOM!

www.nomoreransom.org

Πηγές:

1. <https://www.enisa.europa.eu/secureme/#!/cyber-tips#>
2. <https://www.nomoreransom.org/el/index.html>

Ναρκωτικά στον Κυβερνοχώρο

Το σύγχρονο οργανωμένο έγκλημα «αξιοποιεί» τον Κυβερνοχώρο, δημιουργώντας μια πλήρη υποδομή για τη διακίνηση των ναρκωτικών και νέων ψυχοδραστικών ουσιών

- ✓ **Χρήση Ισχυρής κρυπτογράφησης**
που καθιστά δύσκολο τον εντοπισμό των OCGs.
- ✓ **Εκτεταμένη χρήση των social media για λιανική διάθεση**
ιδίως σε νέα ανήλικα παιδιά.
- ✓ **Αυτοματοποίηση μέσω της TN και των bots**
για επικοινωνίες, πρόβλεψη κινδύνου, έξυπνη αποστολή δεμάτων κ.λπ.



Μετατόπιση της παράνομης αγοράς στο ψηφιακό περιβάλλον

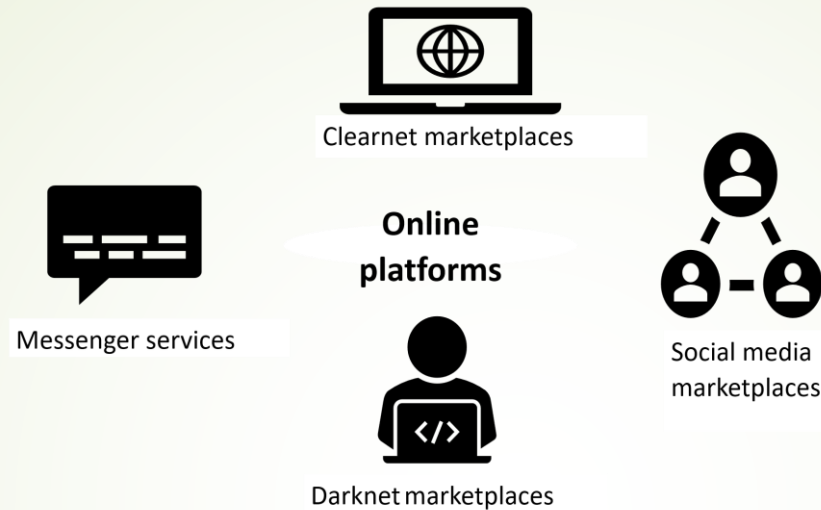
European Drug Report 2025

Trends and developments



EU Drug Markets Analysis | 2024

Key insights for policy and practice



CLEARNET

The publicly-accessible Internet that is easily accessed with a normal Internet connection and a browser.
Examples of content: Google, Facebook, YouTube, Wikipedia, Netflix.

DEEP WEB

The publicly-accessible Internet that is unknown to search engines, such as encrypted or unindexed websites, private databases, and other unlinked content.
Examples of content: Academic databases, medical records, financial records, legal documentation, government information, library access, bank accounts.

DARKWEB

A collection of websites that exist on darknets. These are not directly accessible from the Clearnet and often require special software to access such websites. Websites use hidden IP addresses which are hosted on securely encrypted networks for increased anonymity.
Examples of content: Tor encrypted websites, whistleblowing platforms, ultra-secure email services, darknet markets.

Πηγές:

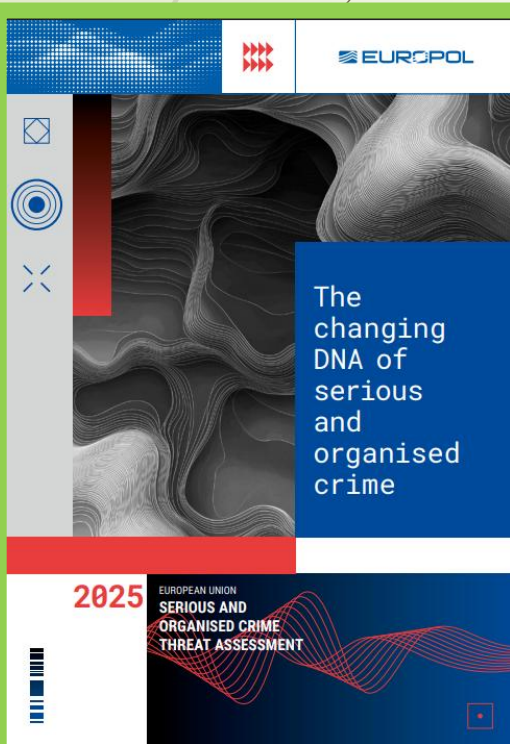
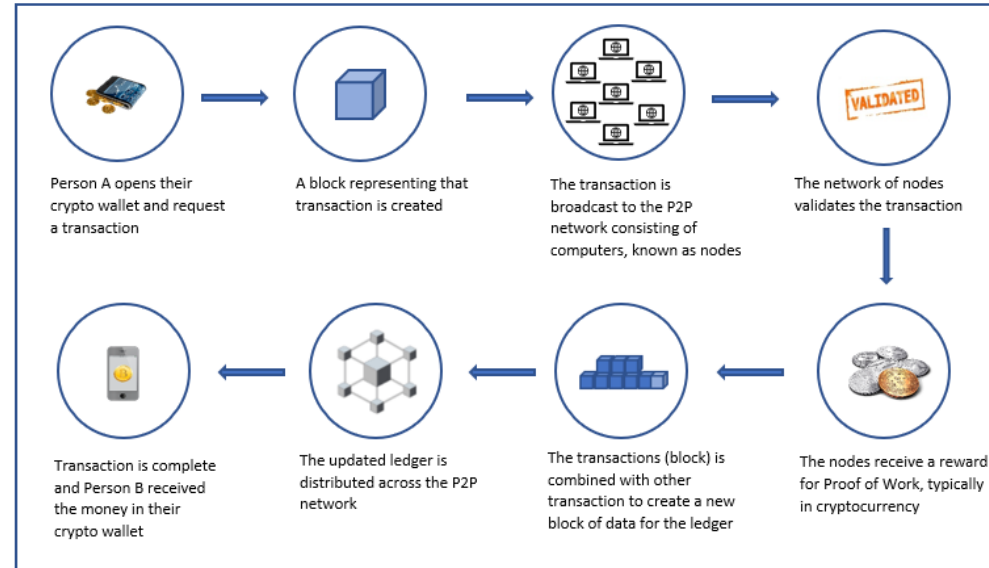
1. <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/onlinetrafficking/onlinesalesplatforms.html>
2. <https://www.interpol.int/Crimes/Illicit-goods/Pharmaceutical-crime-operations>
3. <https://www.europol.europa.eu/publications-events/publications/eu-drug-markets-analysis-2024-key-insights-for-policy-and-practice>
4. <https://www.vew.site/unodc-syntheticdrugstrategy-en/>
5. https://www.euda.europa.eu/publications/european-drug-report/2025_en#pdf_p.14-15

Υπονόμευση των ανθρώπινων κοινωνιών από το **οργανωμένο έγκλημα**

Χρήση της τεχνολογίας για σοβαρές εγκληματικές δραστηριότητες



Person A sends money to person B



Πηγές:

1. <https://www.unodc.org/centralasia/en/news/unodc-explains-the-combined-use-of-unmanned-aerial-vehicles-and-ground-surveillance-systems.html>
2. <https://www.reuters.com/article/crime-europol/technology-is-now-at-root-of-almost-all-serious-crime-europol-idUSL2N1GM27Z/>
3. <https://www.theguardian.com/world/2019/jan/28/spanish-drug-smugglers-who-used-drones-to-spy-on-police-are-arrested>
4. https://www.emcdda.europa.eu/publications/european-drug-report/2023_en
5. <https://lfpres.com/news/local-news/plot-to-fly-drugs-into-emdc-by-drone-foiled-two-charged-opp-say>
6. <https://english.elpais.com/spain/2021-07-15/spanish-police-seize-large-drone-used-to-carry-drugs-from-morocco.html>
7. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>
8. <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/online-trafficking/payment/index.html>
9. https://www.euda.europa.eu/publications/european-drug-report/2025_en#pdf p.14-15

Τεράστια χρηματικά ποσά γύρω από τα ναρκωτικά

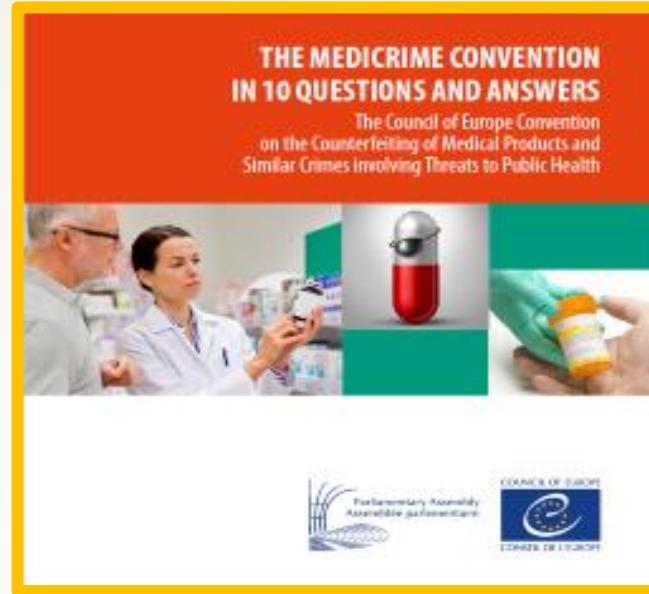
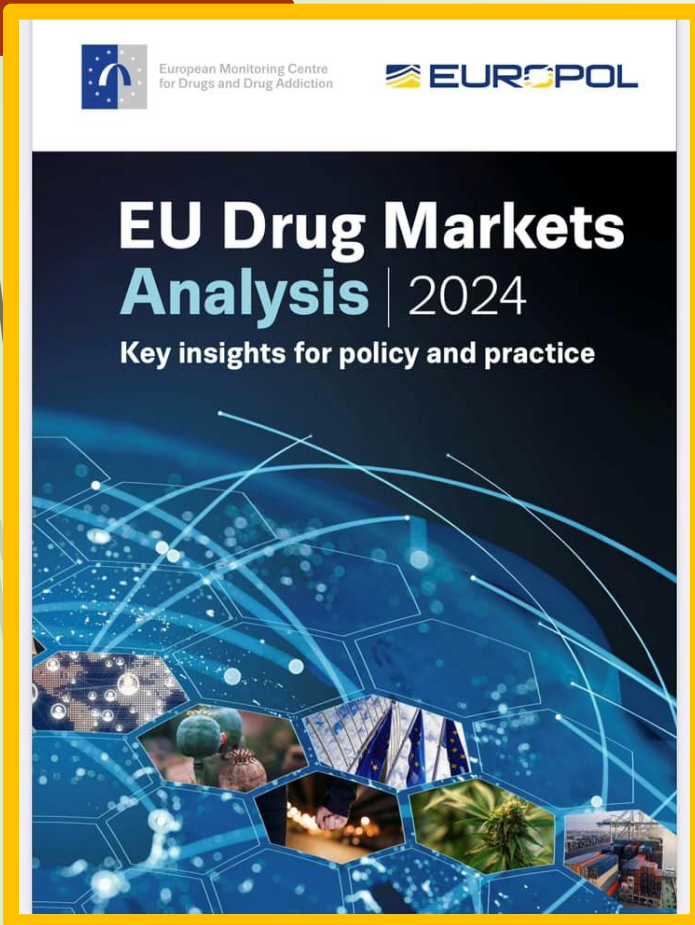


Πηγή
https://www.unodc.org/documents/data-and-analysis/WDR_2025/WDR25_B1_Key_findings.pdf

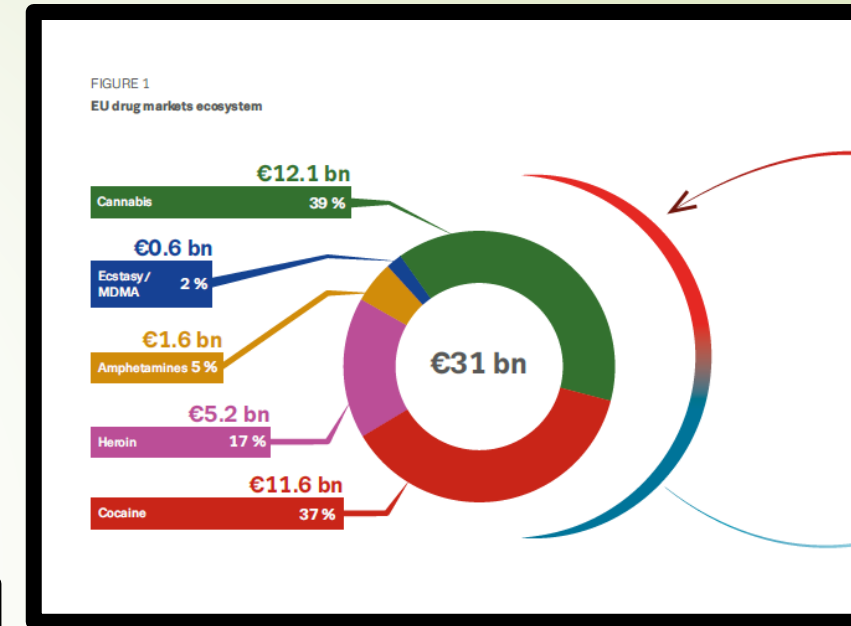
INWARD AND OUTWARD ILLICIT FINANCIAL FLOWS RELATED TO DRUG-TRAFFICKING FOR COUNTRIES WHERE DATA ARE AVAILABLE

COUNTRY	DRUG	AVERAGE ANNUAL INWARD ILLICIT FINANCIAL FLOWS (\$)	AVERAGE ANNUAL OUTWARD ILLICIT FINANCIAL FLOWS (\$)
Colombia (2015–2019)	Cocaine	1.2–2.6 billion	227 million
Mexico (2015–2018)	Cocaine Methamphetamine Heroin	4.5 billion 2.8 billion 4.8 billion	337.5 million
Peru (2015–2017)	Cocaine	1.5 billion	
Afghanistan (2018–2021)	Opiates	1.3–2.2 billion	
Bangladesh (2017–2021)	Heroin “Yaba” (methamphetamine)		61.9 million
	Phensedyl (cough syrup)		140.3 million
	Buprenorphine		215.4 million
			63.1 million
Maldives (2020–2021)	Heroin		7.25 million
	Cannabis		8.7 million
Nepal (2019–2021)	Heroin		4.6 million
Myanmar (2018–2022)	Opiates	0.5–1.3 billion	

Κίνδυνοι και απειλές όχι μόνο από τα φάρμακα



Enhance monitoring and analysis of the use of online platforms to trade and distribute drugs. Particular attention should be paid to developments on the surface web and social media platforms, especially in relation to their use by young people.



ΕΕ 2021, ελάχιστη λιανική αξία
31 δις €

Πηγές:

1. <https://lawandorder.gr/diathesi-farmakon-ston-kyvernochoro-to-thesmiko-plaisio-pote-arga/>
2. <https://newpost.gr/ellada/5dff4032e21f618439dae68b/e-farmak-i-a-sto-diadiktyo-athorakisti-i-hora-sti-mastiga-ton-epikindynon-skeyasmaton>
3. <https://www.interpol.int/Crimes/Illicit-goods/Pharmaceutical-crime-operations>
4. <https://www.europol.europa.eu/publications-events/publications/eu-drug-markets-analysis-2024-key-insights-for-policy-and-practice> p. 10

Επιγραμμικές απάτες – Online Frauds

Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'



By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024



Νέα Οδηγία

2020/1828/EE

αντιπροσωπευτικές αγωγές για την
προστασία των συλλογικών
συμφερόντων των καταναλωτών και
την κατάργηση της Οδηγίας
2009/22/EC

N. 5019/2023 ΦΕΚ Α

Ενσωματώθηκε στο
εσωτερικό δίκαιο

Αποζημίωση θυμάτων
κυβερνοαπάτης υπό
προϋποθέσεις

Buying on the dark web?

You are on the menu!



you



EUROPOL

Πηγές:

1. https://www.europol.europa.eu/cms/sites/default/files/documents/infographic_-_pcf_prevention_alert_0.pdf
2. <https://twitter.com/Europol/status/1084832758801883136/photo/1>
3. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020L1828>
4. <https://eur-lex.europa.eu/EN/legal-content/summary/injunctions-protecting-the-collective-interests-of-consumers-until-2023.html>
5. <https://www.europol.europa.eu/media-press/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web>
6. <https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/>
7. <https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>

Απάτες του Ενδιάμεσου – MITM (Man in the Middle)

CEO/BUSINESS EMAIL COMPROMISE (BEC) FRAUD

CEO/BEC fraud occurs when an employee authorised to make payments is tricked into paying a fake invoice or making an unauthorised transfer out of the business account.

A fraudster calls or emails posing as a high ranking figure within the company (e.g. CEO or CFO).



They have good knowledge about the organisation.

They require an urgent payment.



They use language such as: 'Confidentiality', 'The company trusts you', 'I am currently unavailable'.

HOW DOES IT WORK?

Often, the request is for international payments to banks outside Europe.

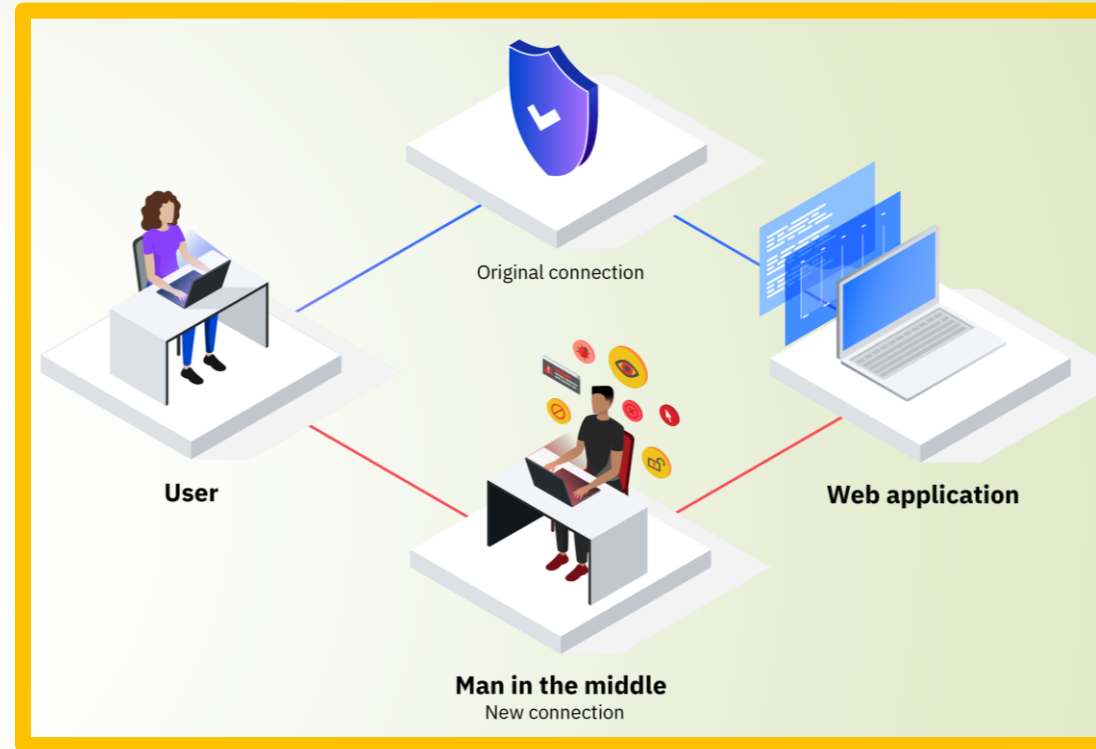


The employee transfers funds to an account controlled by the fraudster.

Instructions on how to proceed may be given later, by a third person or via email.



The employee is requested not to follow the regular authorisation procedures.

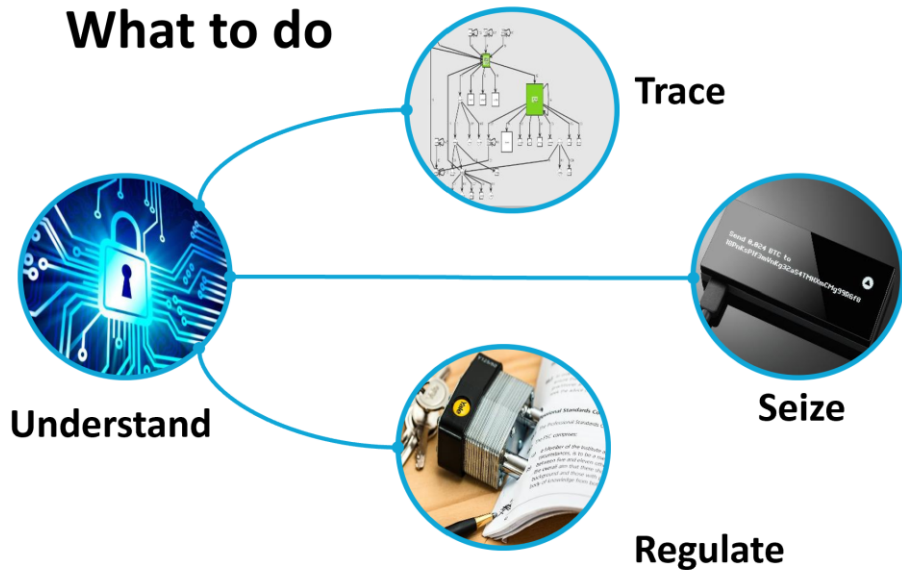


Πηγές:

1. <https://www.ibm.com/think/topics/man-in-the-middle>
2. https://www.europol.europa.eu/sites/default/files/documents/ioc_ta_2019.pdf p.41
3. <https://www.youtube.com/watch?v=PehWRZ2816M>

Κρυπτοχρήμα & Έγκλημα

What to do



The screenshot shows the Cryptorank website with a table of the top cryptocurrencies. The table includes columns for rank, name, price, 24-hour change, market cap, volume, and supply. The top three cryptocurrencies are Bitcoin, Ethereum, and Tether.

#	Name	Price	Chg (24H)	Market Cap	Volume (24H)	Circ. Supply	Price Graph (7D)
1	Bitcoin BTC	\$ 69,515	-0.82%	\$ 1.38T	\$ 13.06B	BTC 19.78M	
2	Ethereum ETH	\$ 2,512	-0.42%	\$ 302.94B	\$ 5.56B	ETH 120.41M	
3	Tether USDT	\$ 1.00	+0.10%	\$ 120.52B	\$ 27.59B	USDT 120.57B	

Πηγές:

- <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/cryptocurrency.html>
- <https://www.youtube.com/watch?v=g7jFA5v6zgY>
- <https://www.europol.europa.eu/media-press/newsroom/news/cryptocurrencies-and-financial-crime-strategic-approach-to-ensure-security>
- <https://cryptorank.io/all-coins-list>

ΕΠΕΝΔΥΤΙΚΕΣ ΑΠΑΤΕΣ – Investment Frauds

Η καλύτερη επένδυση είναι η ενημέρωση



- Είμαστε **επιφυλακτικοί** όταν βλέπουμε διαφημίσεις επενδυτικών προγραμμάτων στο διαδίκτυο που υπόσχονται υψηλές αποδόσεις, ακόμα και όταν εμφανίζονται να συμμετέχουν σε αυτές πρόσωπα υψηλού κύρους και μεγάλης αναγνωρισιμότητας.
- **Δεν επενδύουμε** χρήματά σας σε υπηρεσίες **χωρίς** να είμαστε απολύτως βέβαιοι για την **αξιοπιστία** τους.
- Είμαστε **επιφυλακτικοί** όταν μας προσεγγίζουν τηλεφωνικά ή μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου από επενδυτικές εταιρείες του εξωτερικού.
- **Αναζητούμε** πληροφορίες για την αξιοπιστία των επενδυτικών εταιρειών που μας προσεγγίζουν.
- **Ζητούμε** τους όρους και προϋποθέσεις, πριν πραγματοποιήσουμε κάποια συναλλαγή.
- **Πριν** προβούμε σε οποιαδήποτε χορήγηση στοιχείων μας ή απόφαση για επένδυση, **ελέγχουμε** εάν η εταιρία διαθέτει άδεια από την Επιτροπή Κεφαλαιαγοράς ή την Τράπεζα της Ελλάδος ή ευρωπαϊκό διαβατήριο.
- **Ανατρέχουμε** στη λίστα προειδοποιήσεων της Επιτροπής Κεφαλαιαγοράς για το επενδυτικό κοινό, στο σύνδεσμο <http://www.hcmc.gr/el/warnings1>.

Πηγές:

1. <https://www.astynomia.gr/2024/12/07/07-12-2024-prosochi-stis-paraplanitikes-diafimiseis-pou-proothoun-dithen-ependytika-i-alla-proionta/>
2. <https://www.ic3.gov/CrimeInfo/Investment>
3. https://www.ic3.gov/Outreach/Brochures/2024_ABA_Cryptocurrency_Infographic.pdf
4. <https://www.europol.europa.eu/media-press/newsroom/news/further-action-against-fraudulent-online-investment-platform-five-arrests-of-high-value-targets>
5. https://www.youtube.com/watch?v=HIfGsQ_MkIU

ΕΠΕΝΔΥΤΙΚΕΣ ΑΠΑΤΕΣ – Investment Frauds

Η καλύτερη επένδυση είναι η ενημέρωση

ΚΡΥΠΤΟ«ΝΟΜΙΣΜΑΤΑ»

! Προσέξτε ποιον εμπιστεύεστε.

Ενημερωθείτε πριν επενδύσετε.

Ακολουθήστε επίσημες πηγές για την ενημέρωσή σας.

ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ
ΕΥΡΩΣΥΣΤΗΜΑ

ΚΡΥΠΤΟ«ΝΟΜΙΣΜΑΤΑ»:
Η καλύτερη
επένδυση είναι
η ενημέρωση

ΚΡΥΠΤΟ«ΝΟΜΙΣΜΑΤΑ»

! Αναγνωρίστε τους κινδύνους απάτης

Μηνύματα & e-mails από δήθεν αξιόπιστα ανταλλακτήρια ή πορτοφόλια κλέβουν κωδικούς πρόσβασης & κεφάλαια (phishing scams).

Πηγές:

1. https://www.youtube.com/watch?v=HIfGsQ_MkIU
2. <https://www.bankofgreece.gr/trapeza/koinwnikh-eythynh/xrhmatooikonomikh-ekpaideysh/enhmerwsh-gia-ta-kryptonomismata>
3. https://www.ecb.europa.eu/press/economic-bulletin/articles/2019/html/ecb.ebart201905_03~c83aeaa44c.en.html

Διαδικτυακές απάτες-Οδηγίες της ΤτΕ



Πώς προστατεύομαι από τις ηλεκτρονικές απάτες

1 ΕΝΗΜΕΡΩΝΟΜΑΙ ΔΙΑΡΚΩΣ...

...για τους κινδύνους και τις νέες μορφές απάτης.



2 ΕΙΜΑΙ ΣΕ ΕΓΡΗΓΟΡΣΗ...

...απέναντι σε **μη συνήθεις** συμπεριφορές και καταστάσεις (π.χ. ενημέρωση για «μεγάλες ευκαιρίες», αιτήματα για επείγουσα καταβολή χρημάτων, ύποπτη δραστηριότητα στον τραπεζικό λογαριασμό ή την κάρτα).



4 ΔΕΝ ΑΠΑΝΤΩ...

...σε ύποπτα e-mail, sms, κλήσεις και σε **καμία περίπτωση** δεν ακολουθώ links / QR codes καθώς και **δεν ανοίγω** συνημμένα αρχεία.

5 ΔΕΝ ΜΟΙΡΑΖΟΜΑΙ ΤΑ ΣΤΟΙΧΕΙΑ...

...τραπεζικού λογαριασμού / κάρτας / κωδικούς μιας χρήσης και ευαίσθητα προσωπικά δεδομένα.

6 ΓΙΑ ΝΑ ΜΠΩ ΣΤΟ SITE ΤΗΣ ΤΡΑΠΕΖΑΣ ΜΟΥ...

...**πληκτρολογώ** εγώ την ηλεκτρονική διεύθυνση και δεν ακολουθώ χορηγούμενους συνδέσμους από μηχανές αναζήτησης.
Βεβαιώνομαι ότι βρίσκομαι στο **πραγματικό site** της τράπεζας (ελέγχω ότι είναι το σωστό url και ότι γίνεται η χρήση «https://...» ή ότι εμφανίζεται το σύμβολο του λουκέτου).



3 ΦΡΟΝΤΙΖΩ ΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ ΜΟΥ...

...ώστε να είναι ενημερωμένο και να προστατεύεται από antivirus.

Επίσης, **ενημερώνω** τον browser που χρησιμοποιώ και διασφαλίζω ότι το λογισμικό που εγκαθιστώ είναι αξιόπιστο και από επίσημο φορέα.



7 ΕΙΜΑΙ ΙΔΙΑΙΤΕΡΑ ΠΡΟΣΕΚΤΙΚΟΣ/-Η...

...με τις **διαδικτυακές αγορές** μου και επιλέγω ηλεκτρονικές πλατφόρμες και καταστήματα εμπιστοσύνης ελέγχοντας και τυχόν αξιολογήσεις που υπάρχουν (ελέγχω ότι είναι το σωστό url και ότι γίνεται η χρήση «https://...» ή ότι εμφανίζεται το σύμβολο του λουκέτου).



8 ΕΛΕΓΧΩ ΠΑΝΤΑ ΤΙΣ ΕΙΔΟΠΟΙΗΣΕΙΣ ΠΟΥ ΛΑΜΒΑΝΩ ΑΠΟ ΤΗΝ ΤΡΑΠΕΖΑ ΜΟΥ...

...τα μηνύματα που συνοδεύουν κωδικούς μιας χρήσης OTP, ειδοποιήσεις για σύνδεση νέων συσκευών, ψηφιακών πορτοφολιών, υπηρεσιών πληρωμών και επιβεβαιώσεων ότι αφορούν δικές μου ενέργειες. Τακτικά ελέγχω και τις **κινήσεις των λογαριασμών μου**.



9 ΒΕΒΑΙΩΝΟΜΑΙ ΟΤΙ...

...ο αποστολέας των μηνυμάτων που λαμβάνω **είναι ο πραγματικός** (ακόμα και αν φαίνεται ότι είναι φιλικό μου πρόσωπο ή επίσημος φορέας).

10 ΠΡΙΝ ΑΠΑΝΤΗΣΩ ΣΕ ΑΓΓΕΛΙΑ ΕΡΓΑΣΙΑΣ, ΕΛΕΓΧΩ...

...τα στοιχεία της εταιρίας που προσφέρει τη θέση. Είμαι πολύ προσεκτικός / -ή όταν δημοσιεύω αγγελίες και όταν απαντώ σε αγγελίες άλλων.

11 ΕΧΩ ΥΠΩΣΗ ΟΤΙ Η ΤΡΑΠΕΖΑ ΔΕΝ ΘΑ ΜΟΥ ΖΗΤΗΣΕΙ ΠΟΤΕ...

...το pin της κάρτας ή τον κωδικό του e-banking μου.

12 ΑΠΟΦΕΥΓΩ ΝΑ ΣΥΝΔΕΟΜΑΙ...

...σε δημόσια και απροστάτευτα δίκτυα wi-fi.



13 ΔΕΝ ΑΠΟΘΗΚΕΥΩ ΤΟΥΣ ΚΩΔΙΚΟΥΣ ΜΟΥ...

...στις συσκευές μου και τους **αλλάζω** τουλάχιστον κάθε 6 μήνες. Αποφεύγω τη χρήση απλοϊκών ή προβλέψιμων κωδικών.

14 ΔΕΝ ΑΝΤΑΠΟΚΡΙΝΟΜΑΙ...

...σε **αναπάντεχες** κλήσεις από υποτιθέμενους παρόχους υπηρεσιών (Microsoft, EΛΤΑ, ΔΕΗ, Εφορία κλπ) χωρίς να έχει γίνει πρώτα αίτημα από εμένα.

15 ΑΚΟΜΑ ΚΑΙ ΜΕ ΤΗΝ ΥΠΩΣΙΑ ΟΤΙ ΜΠΟΡΕΙ ΝΑ ΕΧΩ ΠΕΣΕΙ ΘΥΜΑ ΑΠΑΤΗΣ...

...**ειδοποιώ** την τράπεζά μου.
Αν χρειαστεί, επικοινωνώ με την αστυνομία (Δίωξη Ηλεκτρονικού Εγκλήματος) και την υπηρεσία μέσα από την οποία πραγματοποιήσα τη συναλλαγή.

Νέα Οδηγία 2020/1828/ΕΕ

αντιπροσωπευτικές αγωγές για την προστασία των συλλογικών συμφερόντων των καταναλωτών και την κατάργηση της Οδηγίας 2009/22/ΕΚ

Ν. 5019/2023 ΦΕΚ Α

Ενσωματώθηκε στο
εσωτερικό δίκαιο

Αποζημίωση

θυμάτων

κυβερνοαπάτης υπό
προϋποθέσεις

Πηγές:

1. <https://www.bankofgreece.gr/trapeza/koinwnikh-eythynh/xrhmatooikonomikh-ekpaideysh/prostasia-apo-hlektronikes-apates?mode=preview>
2. https://museum.bankofgreece.gr/personalfinance/?fbclid=IwY2xjawlr0hFleHRuA2FIbQ1xMAABHSFZ0ZDekJpQNV1cljHeK8vp6RgpOUhxbSLssHzWOF8qVL0ZpM8Z2Ax-Q_aem_LUDM7nsjerfXu2jXRt366A#/lessons/in_swfHmFJVomcam6z8GDKZikD_f1Qq-

Παραλλαγές διαδικτυακών απτατών



ΕΥΡΩΠΑΪΚΗ ΑΣΤΥΝΟΜΙΚΗ ΓΡΑΦΕΙΟ (ΕΥΡΩΠΟΛ)

Είμαι η κα. Catherine Debolle, Γενική Διευθύντρια της Ευρωπαϊκής Αστυνομικής Υπηρεσίας (EUROPOL). Σε συνεργασία με την Εθνική Αστυνομία, επικοινωνώ μαζί σας λίγο μετά από μια κατάσχεση μέσω κυβερνοδιαδίωξης (που έχει εγκριθεί ιδίως στον τομέα της πορνογραφίας, της κυβερνοπορνογραφίας, της παιδικής πορνογραφίας) για να σας ενημερώσω ότι είστε το αντικείμενο διαφόρων νομικών διαδικασιών, σε ισχύ:

- ΚΥΒΕΡΝΟΠΟΡΝΟΓΡΑΦΙΑ
- ΠΟΡΝΟΓΡΑΦΙΚΗ ΣΤΟΙΧΕΛΙΑ
- ΠΑΙΔΟΠΟΡΝΟΓΡΑΦΙΑ
- ΕΠΙΔΕΙΞΙΜΑΝΙΑ

Προς ενημέρωσή σας, ο νόμος του Μαρτίου 2007 αυξάνει τις ποινές για σεξουαλική επίθεση, βιασμό, χειραγώγηση, δημοσίευση ή προβολή βίντεο ή εικόνων πορνογραφικού χαρακτήρα που αφορούν άτομα κάτω των 18 ετών.

Έχετε διαπράξει αδίκημα επειδή στοχεύσατε σε ιστότοπους διαφήμισης και άμεσων μηνυμάτων παρουσία ανηλίκων (ατόμων κάτω των 18 ετών). Οι δραστηριότητές σας έχουν καταγραφεί από την αστυνομία του κυβερνοχώρου μας και απαιτούν αποδεδειγμένη των αδικημάτων σας.

Παρακαλούμε απαντήστε μας μέσω email και γράψτε τις αιτιολογήσεις σας, ώστε να εξεταστούν και να επαληθευτούν για την αξιολόγηση των κυρώσεων, αυτό εντός αυστηρής προθεσμίας 72 ωρών.

Μετά την παρέλευση αυτής της προθεσμίας, θα είμαστε υποχρεωμένοι να διαβάσουμε την έκθεσή μας στον κ. Γεώργιο Σαββίδη, Γενικό Εισαγγελέα, στο Ποινικό Δικαστήριο, για την έκδοση εντάλματος σύλληψης εναντίον σας.

Θα διαβάσουμε την αναφορά σας στο πληρέστερο αστυνομικό τμήμα στον τόπο κατοικίας σας για τη σύλληψή σας.

Θα εγγραφείτε στο Εθνικό Μητρώο Σεξουαλικών Αδικημάτων.

Το πορτρέτο σας θα σταλεί στα μέσα ενημέρωσης (διαφορα είδησηογραφικά κανάλια) για ευρεία διανομή, έτσι ώστε η οικογένειά σας, τα αγαπημένα σας πρόσωπα και όλοι οι άλλοι να ενημερωθούν για το τι κάνετε μπροστά στον υπολογιστή σας.

Τώρα σας έχουν προειδοποιήσει:

DOCUMENT LEGALISE

Κα. Αικατερίνη Ντεμπολ
Γενικός Διευθυντής της Ευρωπαϊκής Αστυνομικής Υπηρεσίας (EUROPOL)
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΥΡΩΠΑΪΚΗΣ ΑΣΤΥΝΟΜΙΑΣ (ΕΥΡΩΠΟΛ)



 **THE ANATOMY OF BUSINESS EMAIL COMPROMISE**

3 TOXIC INGREDIENTS

1 + **2** + **3** = **Millions in illegal profits**

Hacking
An email account is compromised through malware, employee intrusion, etc.

Social engineering fraud
The victim is manipulated into providing information or funds.

Money laundering
Multiple transfers are made involving foreign banks/institutions.

Low cost!
Low risk!
High rate of return!

#BECareful

ONE CRIME, MANY NAMES

BUSINESS EMAIL COMPROMISE CAN GO BY DIFFERENT NAMES – BE AWARE OF THEM ALL

CEO FRAUD / CEO IMPERSONATION

EMPLOYEE ACCOUNT COMPROMISE

BOGUS INVOICE SCHEME

MAN-IN-THE EMAIL SCAM

#BECareful







Πηγές:

1. <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/beware-scams-involving-fake-correspondence-europol-e>
2. https://www.messinialive.gr/eksarthrothikan-dyo-speires-pou-arpaksan-630-000-evro-eksapatontas-polites-120-peristatika-thymata-kai-stin-kalamata/?fbclid=IwY2xjawKIUB1eHRuA2FibQIxMQBicmlkETBaVzImbWJCejdQXJ5UkUwAR7IJBmyoK0G5_AkG0_6HJ9_su5KQWOfYiiaNhcQalwZlyHwzb0Z8tg0xFuuQ_aem_rzsBtRSvS3RMD_mOyD9uwa

Απάτες Τεχνικής Υποστήριξης – Tech Support Scams

How to recognise tech support scams



Hi, I'm Tech#-nical S)!support

Cybercrook Brooke calls you posing as a technical support provider, claiming that there is a problem with your PC's software.

The caller ID displays a support phone number from a trusted company.

+88 !* #9 82 !0

She tells you to act quickly or you will lose all your data.

Cybercrook Brooke recommends that you download a program that will fix the problem.



The downloaded program gives her access to your computer and data.

She then asks for a small payment for the service to make you log into your online banking.

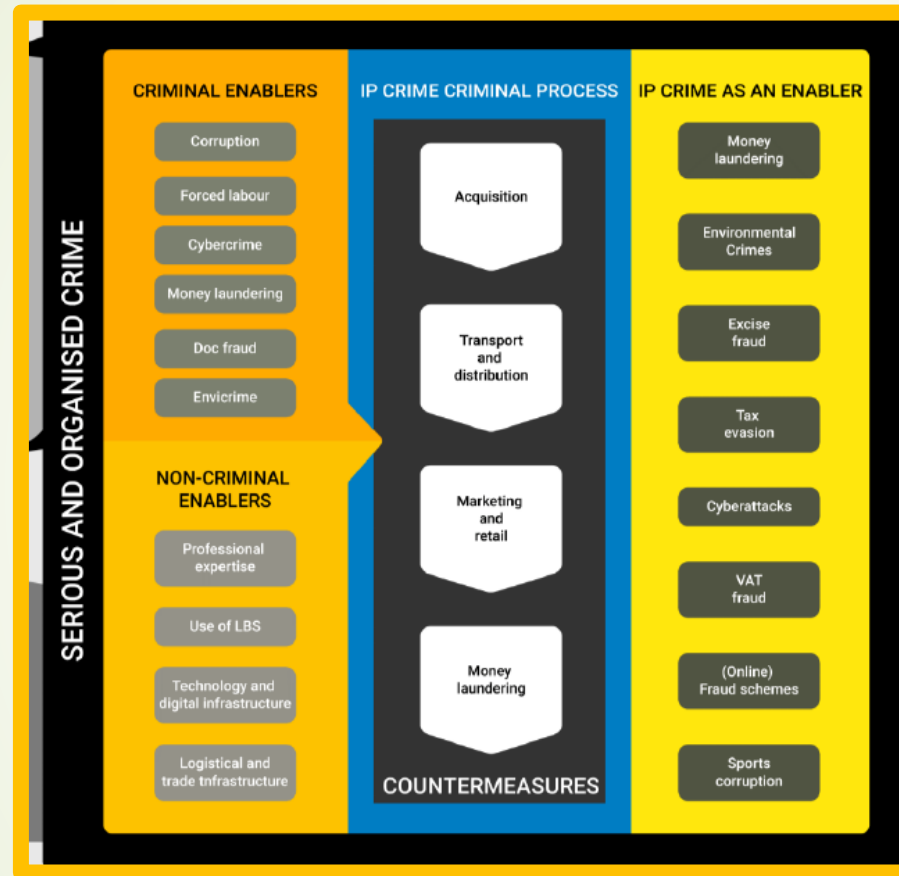
PAY SERVICE

Cybercrook Brooke has now access to your bank account and can perform fraudulent transactions.

Πηγές

1. <https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams>
2. <https://pix4free.org/assets/library/2021-06-16/originals/tech-support.jpg>
3. https://www.europol.europa.eu/cms/sites/default/files/documents/tech_support_scam_en.pdf

IP Crimes - **Money** Mules – Δράσεις της Europol



Πηγές:

- https://www.europol.europa.eu/sites/default/files/documents/gr_posters.pdf
- <https://www.youtube.com/watch?v=TkbgPXUf5eA>
- <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling>
- <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf>
- [https://www.europol.europa.eu/cms/sites/default/files/documents/Uncovering the ecosystem of IP Crime.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Uncovering_the_ecosystem_of_IP_Crime.pdf) p.21
- <https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> p. 31

Συναλλακτικές πρακτικές

Guard your cards and card details

Don't let your card out of sight when making a transaction

Ask the retailer to confirm the amount being debited from your card

Sign new cards as soon as they arrive

Check your receipts against your (online) statements

Carefully discard your receipts from card transactions and information related to your financial affairs

Don't leave your cards unattended in a public place. Keep your personal belongings with you at all times

Never write down your PIN nor disclose it to anyone

When making online transactions, make sure you are using updated antivirus and operating system software

Only buy from trusted sources. For Internet purchases, use the security protocol 3D-Secure

Don't keep your chequebook with your cards

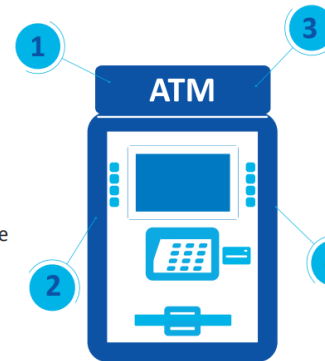
When replacement cards arrive, cut expired/unused/blocked cards into several pieces, including through the magnetic strip and/or chip

EUROPOL

Cash Machines (ATMs)

Be aware of others around you
If someone is watching you choose a different ATM

Stand close to the ATM
Always shield the keypad with your spare hand and your body to avoid anyone seeing your PIN



Assess the ATM
If you spot anything unusual about the ATM or there are signs of tampering, don't use the machine and report it to the bank or police

In case of loss
If the ATM doesn't return your card, report it to your bank

Payment Terminals (POS)

EUROPOL

Card skimming can occur at retail outlets, particularly bars, restaurants, parking ticket machines and (unmanned) petrol stations



Never lose sight (and, if possible, touch) of your card during payment transactions

Insist that your card is visible to you at all times

Πηγή:

https://www.europol.europa.eu/cms/sites/default/files/documents/infographic_-_pcf_prevention_alert_0.pdf

Διαδικτυακές αγορές



σκέφτομαι πριν αγοράσω

ΕΥΚΑΙΡΙΑ - ΕΞΑΠΑΤΗΣΗ;

Οι χρυσοί κανόνες των διαδικτυακών αγορών

ΑΓΟΡΑΣΕ ΑΠΟ ΑΞΙΟΠΙΣΤΕΣ ΠΗΓΕΣ

Χρησιμοποίησε μάρκες και καταστήματα τα οποία γνωρίζεις.

ΕΛΕΓΞΕ ΚΡΙΤΙΚΕΣ ΚΑΙ ΑΞΙΟΛΟΓΗΣΕΙΣ

Ειδικά αγνώστων καταστημάτων και μεμονωμένων πωλητών.

ΕΛΕΓΞΕ ΤΙΣ ΕΠΑΝΑΛΑΜΒΑΝΟΜΕΝΕΣ ΧΡΕΩΣΕΙΣ

Πριν δώσεις τα στοιχεία της κάρτας σου για πληρωμή συνδρομητικής υπηρεσίας, μέσω διαδικτύου, μάθε πώς μπορείς να διακόψεις την υπηρεσία αυτή.

ΒΕΒΑΙΩΣΟΥ ΟΤΙ Η ΜΕΤΑΦΟΡΑ ΔΕΔΟΜΕΝΩΝ ΕΙΝΑΙ ΑΣΦΑΛΗΣ

Χρησιμοποίησε τα πρωτόκολλα HTTPS και SSL όταν περιηγηθείς στο διαδίκτυο. Θυμήσου: μόνο το σύμβολο του λουκέτου δεν κάνει έναν ιστότοπο ασφαλή.

ΣΚΕΨΟΥ ΔΥΟ ΦΟΡΕΣ ΠΡΙΝ ΠΛΗΡΩΣΕΙΣ

Βεβαιώσου ότι κατανοείς τους κινδύνους των διαδικτυακών αγορών.

ΧΡΗΣΙΜΟΠΟΙΗΣΕ ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ ΟΤΑΝ ΑΓΟΡΑΖΕΙΣ ΔΙΑΔΙΚΤΥΑΚΑ

Οι περισσότερες πιστωτικές κάρτες έχουν ισχυρή πολιτική προστασίας πελατών. Εάν δεν λάβεις αυτό που παρήγγειλεις, ο εκδότης της κάρτας ενδέχεται να σε αποζημιώσει.

ΑΠΟΘΗΚΕΥΣΕ ΟΛΑ ΤΑ ΣΧΕΤΙΚΑ ΜΕ ΤΙΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΣΟΥ ΑΓΟΡΕΣ ΕΓΓΡΑΦΑ

Ενδέχεται να χρειαστούν για να αποδείξουν τους όρους και τις προϋποθέσεις της πώλησης ή για να αποδείξουν ότι έχεις πληρώσει για τα αγαθά.

ΜΗ ΣΤΕΛΝΕΙΣ ΧΡΗΜΑΤΑ ΣΕ ΚΑΠΟΙΟΝ ΠΟΥ ΔΕΝ ΓΝΩΡΙΖΕΙΣ

Δεν θα έδινες χρήματα σε ένα τυχαίο άτομο στο δρόμο, μην το κάνεις και στο διαδίκτυο. Εάν είναι δυνατόν, άσκησε το δικαίωμα της προτερής παραλαβής των προϊόντων.

ΜΗ ΣΤΕΛΝΕΙΣ ΠΟΤΕ ΤΑ ΣΤΟΙΧΕΙΑ ΤΗΣ ΚΑΡΤΑΣ ΣΟΥ ΜΕΣΩ E-MAIL

Ποτέ μη στέλνεις αντίγραφο της κάρτας σου, τον αριθμό, το PIN ή οποιοδήποτε άλλο στοιχείο της μέσω e-mail.

ΕΛΕΓΞΕ ΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΩΜΩΝ ΤΗΣ ΙΣΤΟΣΕΛΙΔΑΣ

Πραγματοποίησε τις διαδικτυακές αγορές σου μόνο σε ιστοσελίδες που χρησιμοποιούν πλήρη αυθεντικοποίηση (όπως Verified by Visa /MasterCard Secure Code).

ΔΕΝ ΘΑ ΑΓΟΡΑΖΕΙΣ; ΜΗΝ ΑΦΗΣΕΙΣ ΤΗΝ ΚΑΡΤΑ ΣΟΥ ΠΙΣΩ

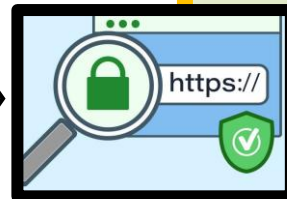
Εάν δεν αγοράσεις κάτι, μην υποβάλεις ή σώσεις τα στοιχεία της κάρτας σου.

#BuySafePaySafe

Πηγές:

1. https://www.europol.europa.eu/sites/default/files/documents/ecommerce_goldenrules_2020_gr_0.pdf
2. <https://www.europol.europa.eu/covid-19/covid-19-shopping-scams>

- ❑ Βασικά μας δικαιώματα ως καταναλωτές (είτε ως ενήλικοι είτε ως ανήλικοι).
- ❑ **Κάνουμε καλή** έρευνα αγοράς (έλεγχος αξιοπιστίας, σύγκριση τιμών, κα).
- ❑ **Βεβαιωνόμαστε** για τα απαραίτητα **βασικά στοιχεία** της διαδικτυακής επιχείρησης (Επωνυμία, ΓΕΜΗ, ΑΦΜ, Διεύθυνση, Σταθερό τηλέφωνο,).
- ❑ **Διαβάζουμε προσεκτικά** σχετικές **κριτικές** για την συνολική εξυπηρέτηση αλλά και την γενική πολιτική της επιχείρησης (περιπτώσεις επιστροφών προϊόντων).
- ❑ **Προσέχουμε** την σελίδα του καταστήματος να παρέχει ασφαλή σύνδεση (**Https**)
- ❑ **Προσέχουμε** τις «ευκαιρίες», τις ασυνήθιστα «χαμηλές τιμές» και τις «προσφορές»
- ❑ **Ενημερωνόμαστε** για την πολιτική ακύρωσης συναλλαγών και επιστροφών προϊόντων που εφαρμόζουν τα καταστήματα, με τα οποία συναλλασσόμαστε



Πηγές:

1. <https://www.synigoroskatanaloti.gr/el/symboyles-gia-exypnes-kai-asfaleis-black-friday-kai-cyber-monday-agores>
2. <https://kataggelies.mindev.gov.gr/%CE%B5%CE%BD%CE%B7%CE%BC%CE%AD%CF%81%CF%89%CF%83%CE%B7-%CE%BA%CE%B1%CF%84%CE%B1%CE%BD%CE%B1%CE%BB%CF%89%CF%84%CF%8E%CE%BD/%CE%B1%CE%BD%CE%AE%CE%BB%CE%B9%CE%BA%CE%BF%CF%82-%CE%BA%CE%B1%CF%84%CE%B1%CE%BD%CE%B1%CE%BB%CF%89%CF%84%CE%AE%CF%82/>
3. <https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals>

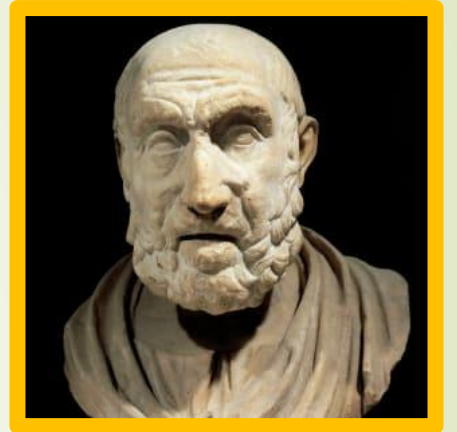
- ☐ Προτιμούμε την πληρωμή με αντικαταβολή.
- ☐ Γνωρίζουμε για το βασικό μας δικαίωμα υπαναχώρησης
- ☐ (επιστροφή αγορασθέντος προϊόντος εντός 14 ημερών από την αγορά)
- ☐ που εφαρμόζεται σε όλα τα εμπορικά καταστήματα (είτε φυσικά είτε διαδικτυακά).
- ☐ Δεν στέλνουμε τον αριθμό της κάρτας μας, το PIN ή οποιαδήποτε άλλη πληροφορία της κάρτας μας σε κανέναν μέσω ηλεκτρονικού ταχυδρομείου.
- ☐ Δεν στέλνουμε χρήματα σε κάποιον που δεν γνωρίζουμε.
- ☐ Αποθηκεύουμε πάντα όλα τα έγγραφα που σχετίζονται με τις διαδικτυακές μας αγορές.
- ☐ Εάν δεν αγοράζουμε κάτι, δεν υποβάλλουμε τα στοιχεία της κάρτας μας.
- ☐ Γνωρίζουμε από πριν που θα καταγγείλουμε περίπτωση απάτης κατά τη διαδικασία της διαδικτυακής αγοράς (ποινικό αδίκημα)
- ☐ Γνωρίζουμε που θα αναφέρουμε το ίδιο περιστατικό για την ενημέρωση της αρμόδιας αρχής για την επιβολή προστίμου (διοικητικό αδίκημα)

Πηγές:

1. <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/e-commerce-tips-and-advice-to-avoid-becoming-fraud-victim>
2. <https://www.fcidoservices.gov.uk/shopping-the-black-friday-sales-safely/>
3. <https://www.ncsc.gov.uk/news/black-friday-shoppers-urged-to-shop-securely>
4. <https://www.gov.gr/ipiresies/polites-kai-kathemerinoteta/kataggelies/kataggelia-gia-periptoseis-apates-me-upologiste>
5. <https://www.gov.gr/ipiresies/polites-kai-kathemerinoteta/kataggelies/anaphora-kataggelia-ston-sunegoro-tou-katanalote>
6. <https://kataggelies.mindev.gov.gr/%CE%BA%CE%B1%CF%84%CE%B1%CE%B3%CE%B3%CE%B5%CE%BB%CE%AF%CE%B1/>

Η Στρατηγική της Πρόληψης

Πατέρας της ιατρικής
επιστήμης



Μη
αποτίμηση

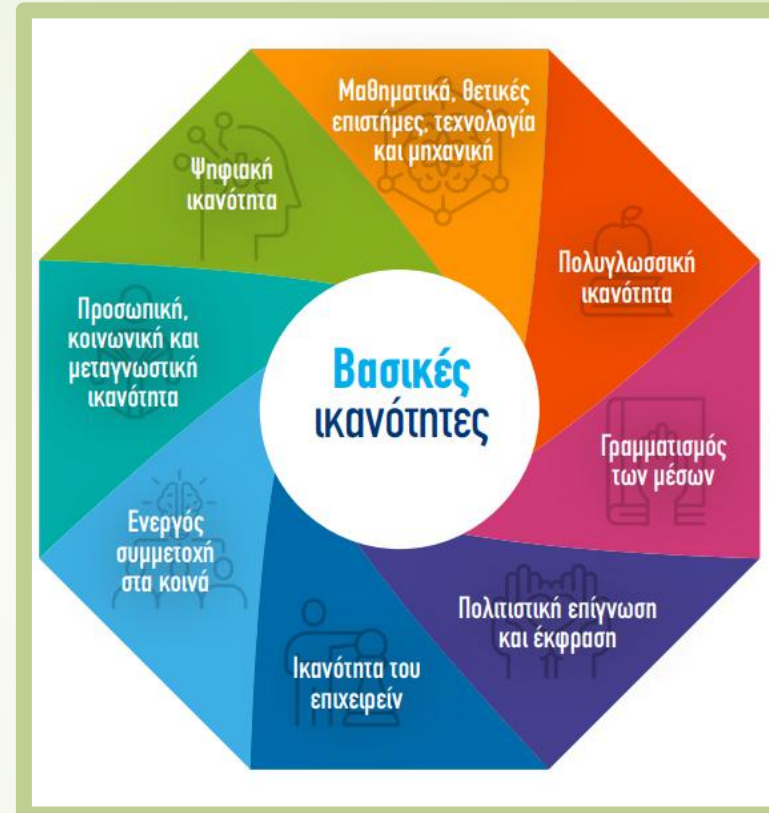
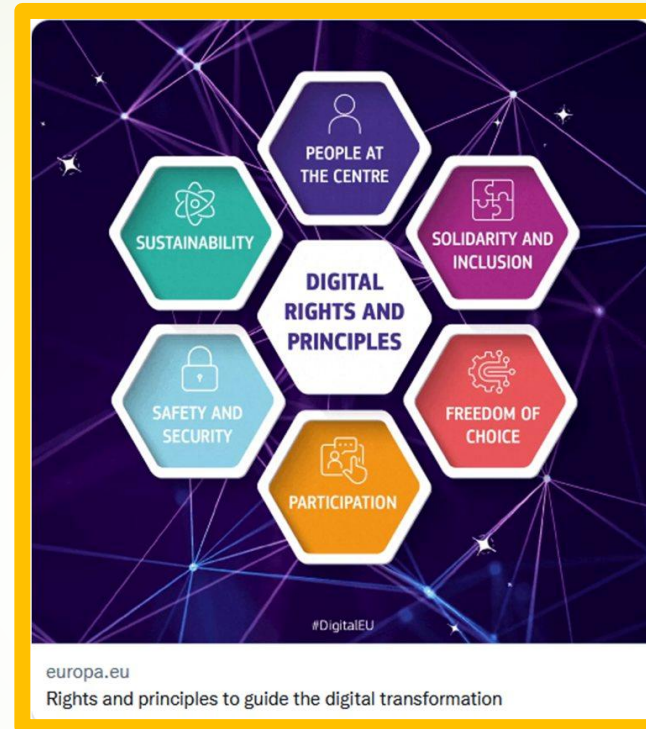
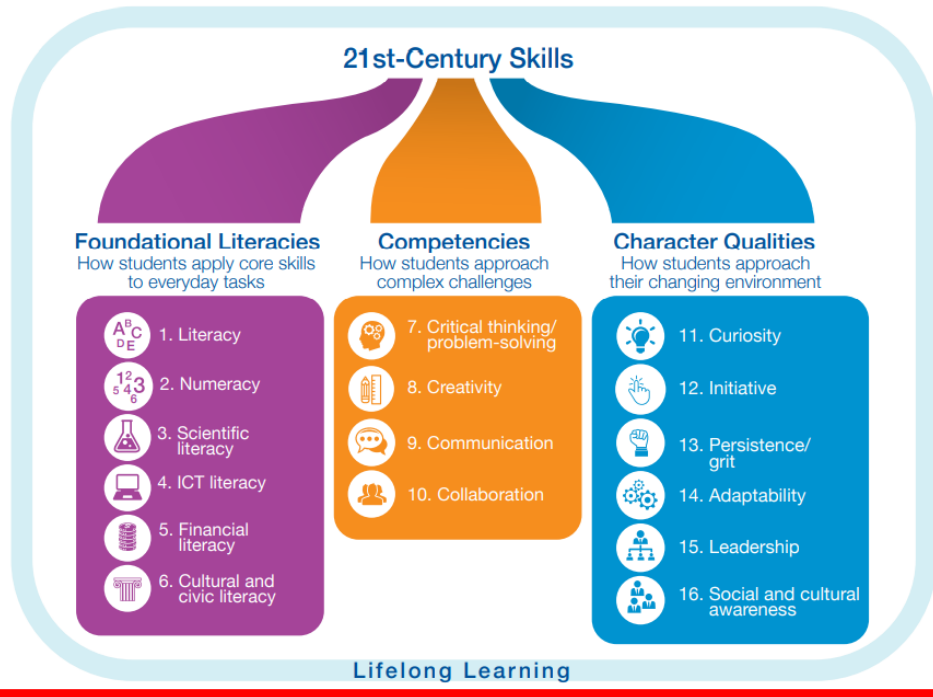
Συγκριτικό
πλεονέκτημα



«Κάλλιον το προλαμβάνειν ή το θεραπεύειν»

Νέες Δεξιότητες στον 21^ο αιώνα – Ο ρόλος της Εκπαίδευσης

Exhibit 1: Students require 16 skills for the 21st century



Πηγές:

1. <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives>
2. <https://www.nationalcoalition.gov.gr/ds-resource/diathesimi-i-elliniki-ekdosi-toy-eyrop/>
3. <https://www.weforum.org/agenda/2016/03/21st-century-skills-future-jobs-students/>
4. https://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf
5. <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives>
6. <https://www.weforum.org/agenda/2016/03/21st-century-skills-future-jobs-students/>
7. https://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf
8. <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles?fbclid=IwAR0eotl200iJEf4TyAfzDuKMuyiJ2ihlvQ9yYci32Oai61QSyxNSo7Xad8> σημεία 4 (ψηφιακή **εκπαίδευση** και κατάρτιση και ψηφιακές δεξιότητες), 16 (**ασφαλές** και προστατευμένο ψηφιακό περιβάλλον), 20,21,22 (**προστασία** και ενδυνάμωση των παιδιών και των νέων στο ψηφιακό περιβάλλον)
9. <https://www.unesco.org/en/digital-competencies-skills/ict-cft>

Ψηφιακό Χάσμα Γενεών – Ψηφιακή Ευχέρεια

Digital generational gap

Percentage of individuals using the Internet in 2023

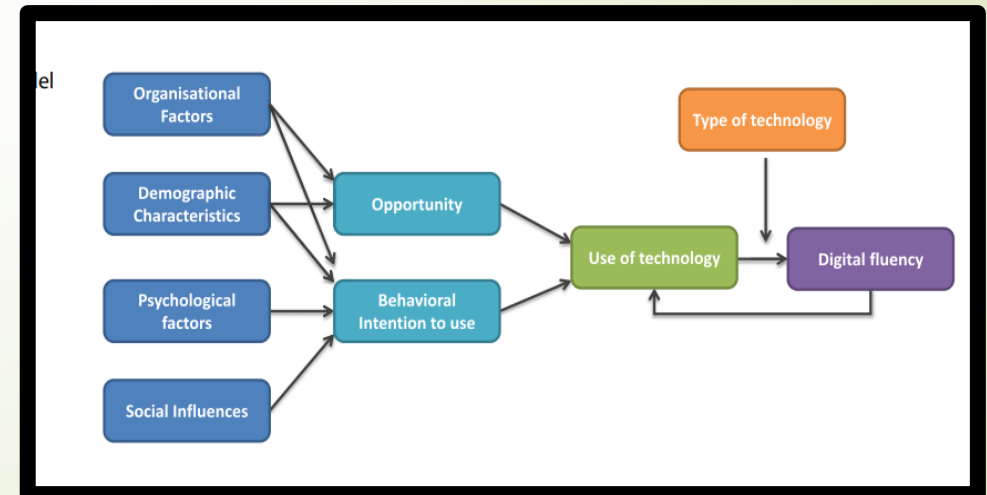
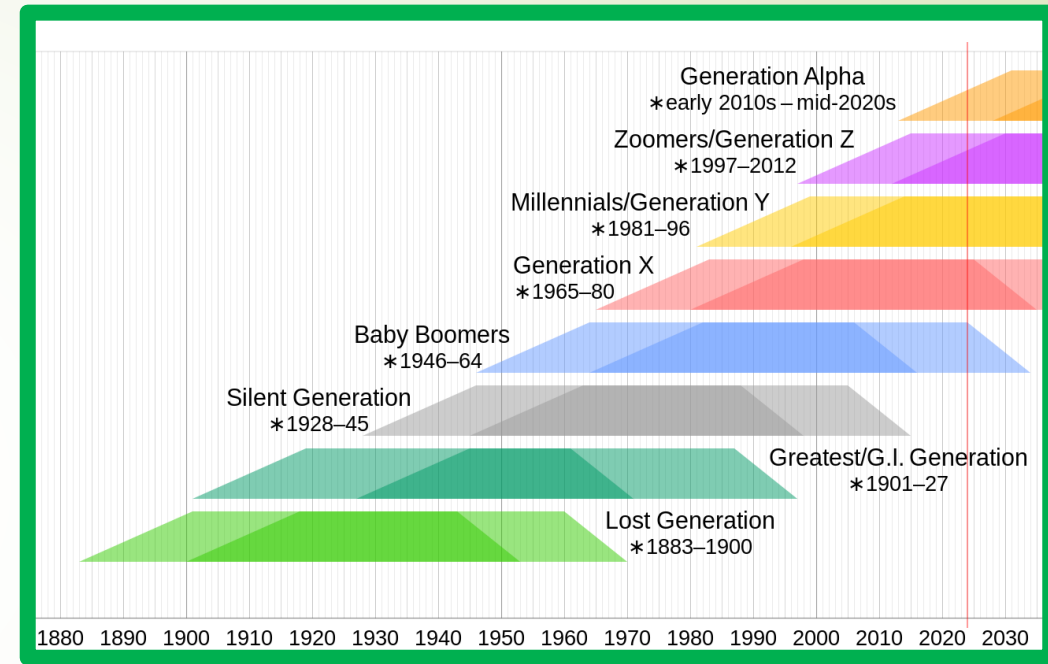


Source : ITU, Facts and Figures 2023
Note: ITU-D regions



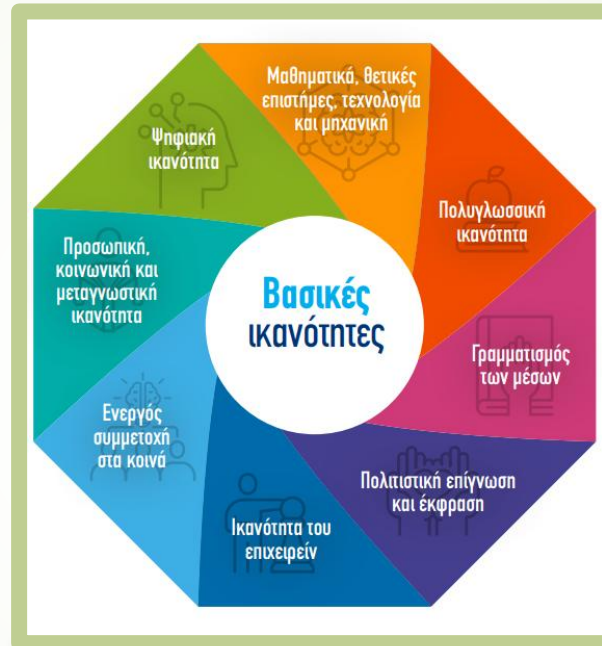
Πηγές:

1. <https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-youth-internet-use/>
2. <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1254&context=bise>
3. https://en.wikipedia.org/wiki/Baby_boomers#/media/File:Generation_timeline.svg



Δεξιότητες & Ικανότητες στο ψηφιακό περιβάλλον

- Δεξιότητες **καινοτομίας** και **δημιουργικότητας**
- Τεχνολογικές δεξιότητες
- Διαπροσωπικές δεξιότητες
- **Εξατομικευμένη** & αυτορρυθμιζόμενη **μάθηση**
- Προσβάσιμη & χωρίς αποκλεισμούς μάθηση
- Μάθηση βασισμένη σε προβλήματα & **συνεργατική** μάθηση
- Δεξιότητες του παγκόσμιου πολίτη
- Δια βίου μάθηση και
- Μάθηση με γνώμονα το μαθητή



	Knowledge Acquisition	Knowledge Deepening	Knowledge Creation
Understanding ICT In Education	Policy Understanding	Policy Application	Policy Innovation
Curriculum and Assessment	Basic Knowledge	Knowledge Application	Knowledge Society Skills
Pedagogy	ICT-enhanced Teaching	Complex Problem-solving	Self-management
Application of Digital Skills	Application	Infusion	Transformation
Organization and Administration	Standard Classroom	Collaborative Groups	Learning Organizations
Teacher Professional Learning	Digital Literacy	Networking	Teacher as Innovator

Πηγές:

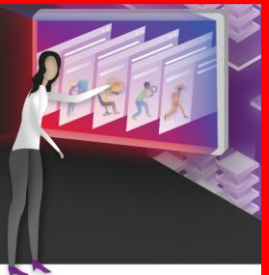
1. <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives>
2. <https://www.weforum.org/agenda/2016/03/21st-century-skills-future-jobs-students/>
3. https://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf p. 4
4. <https://www.nationalcoalition.gov.gr/ds-resource/diathesimi-i-elliniki-ekdosi-toy-eyrop/>
5. <https://www.unesco.org/en/digital-competencies-skills/ict-cft>
6. <https://unesdoc.unesco.org/ark:/48223/pf0000395236>



Δεξιότητες **συνδεδεμένες** με **επαγγελματικές** προοπτικές

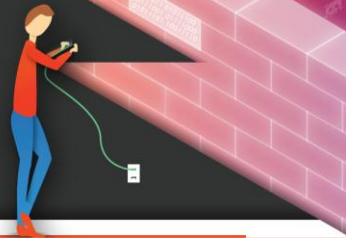


INFORMATION
SYSTEMS
SECURITY
MANAGER



JOB PROFILE:

**CYBER
SECURITY
ENGINEER**



JOB PROFILE:

**CRYPTOGRAPHER/
CRYPTANALYST
AKA
ENCRIPTION
EXPERT**



DEGREE REQUIRED?

COMMON JOB DUTIES

MULTI-DISCIPLINED
LANGUAGE
ANALYST



**CYBER
FORENSICS
EXPERT**



PROFILE:

**CYBER
LEGAL
ADVISOR**



JOB PROFILE:

**CYBER
DEFENSE
INCIDENT
RESPONDER**



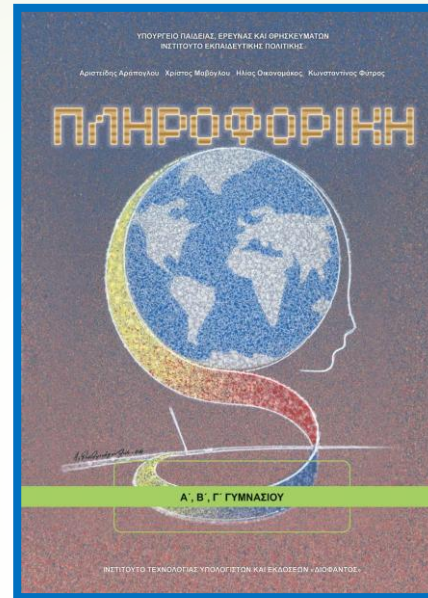
Πηγή:

<https://cyber.org/career-exploration>

**SOFTWARE
DEVELOPER**

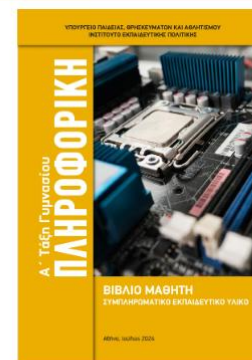


Ανάγκη για εκπαιδευτικό υλικό σύγχρονο και επίκαιρο

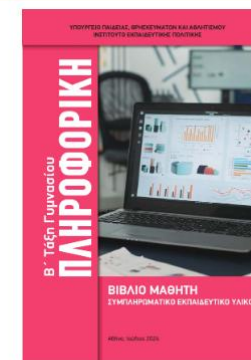


Πηγές:

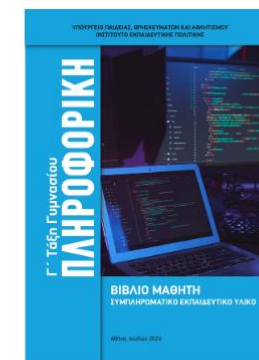
1. <https://nationaldigitalacademy.gov.gr/>
2. <https://iep.edu.gr/el/gymnasio/pliροφοrikι>



Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Α' Γυμνασίου



Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Β' Γυμνασίου



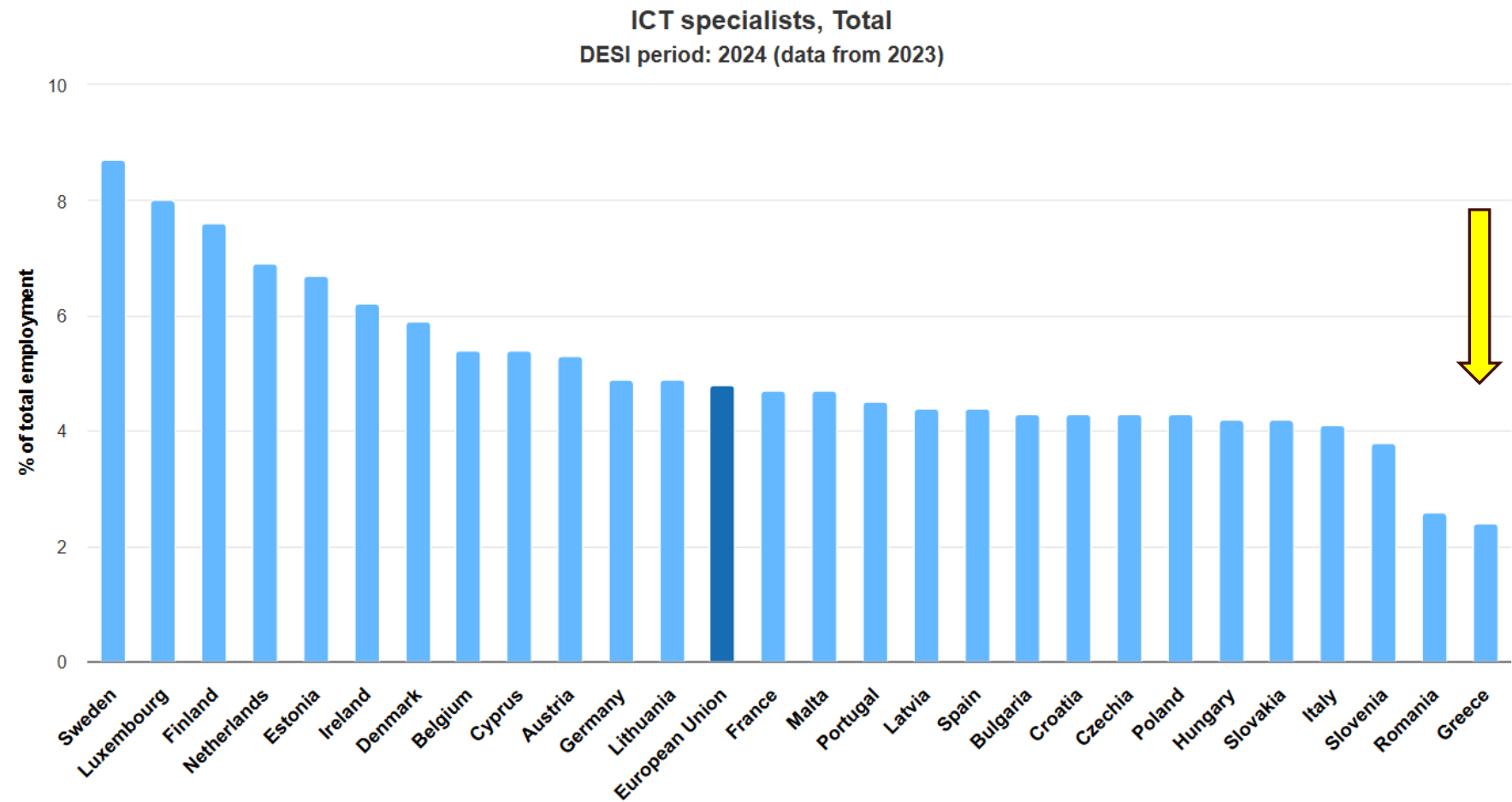
Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Γ' Γυμνασίου

Κατάλληλη προετοιμασία και αποτελέσματα

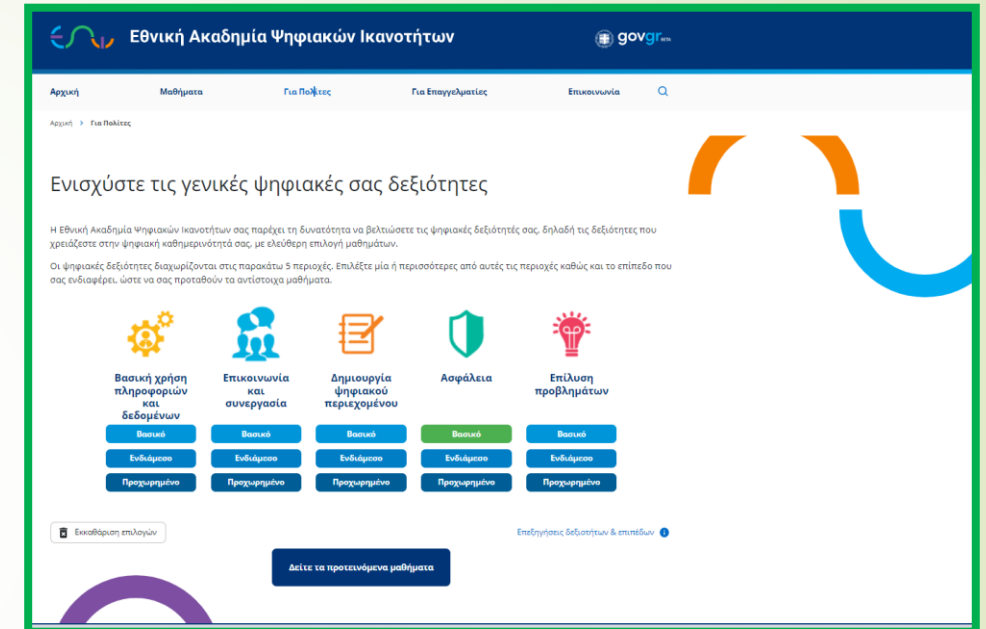
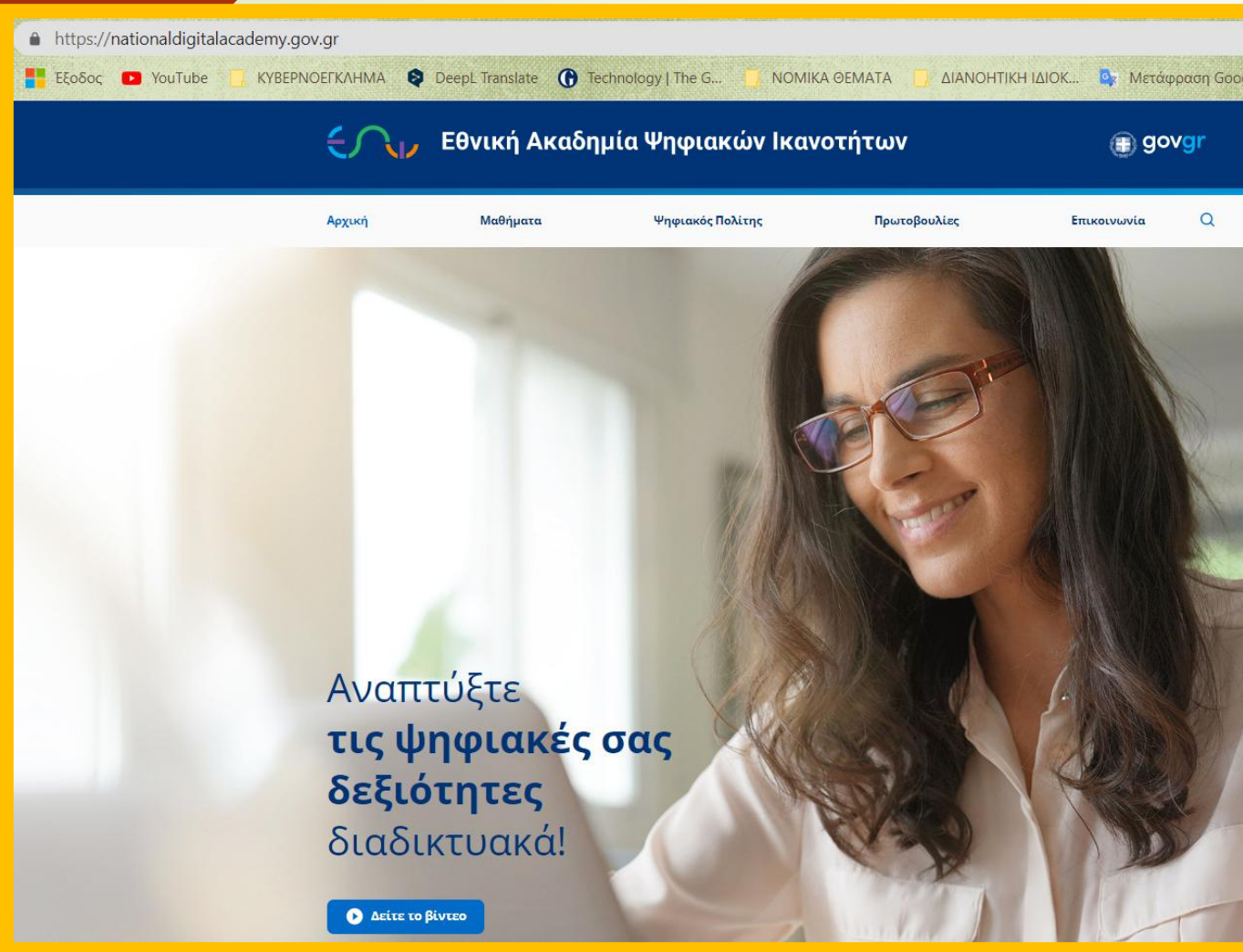
Ειδικοί των ΤΠΕ στην ΕΕ

Πηγή:

https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_ict_spec&breakdown=total&unit=pc_ind_emp&country=AT%2CBE%2CBG%2CHR%2CCY%2CCZ%2CDK%2CEE%2CEU%2CFI%2CFR%2CDE%2CEL%2CHU%2CIE%2CIT%2CLV%2CLT%2CLU%2CMT%2CNL%2CPL%2CPT%2CRO%2CSK%2CSI%2CES%2CSE



Εθνική Ακαδημία Ψηφιακών Ικανοτήτων- ΕΑΨΙ



Με **337** μαθήματα
35 θεματικές ενότητες
1800 ώρες εκπαίδευσης

Στοιχεία στις 01/12/2025

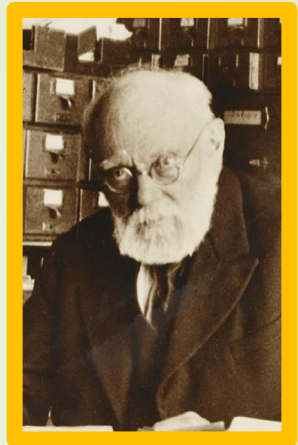
Πηγή: <https://nationaldigitalacademy.gov.gr/>

Πληροφορίες & πηγές για καλές πρακτικές



Κρίσιμο στοιχείο η
αξιοπιστία

- Διεθνείς Οργανισμοί (UN, ITU, EU, ENISA, COE, WHO, OECD, ISO.)
- Ανεξάρτητες Αρχές και δημόσιοι φορείς
- Κρατικοί Οργανισμοί,
- Επιστημονικοί και πιστοποιημένοι Φορείς (Πανεπιστήμια, Ερευνητικά Κέντρα, κα)
- Σχολεία (όλων των βαθμίδων)
- Βιβλιοθήκες (**Δημόσιες**, **Δημοτικές**, **Σχολικές**, κα)
- Φορείς Ιδιωτικού Τομέα (εταιρείες, ΜΚΟ, κα)



Paul Otlet
1868-1944



Πηγές:

1. <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives>
2. <https://daily.jstor.org/internet-before-internet-paul-otlet/>
3. <https://artsandculture.google.com/story/awXRg4ha0wAA8A>
4. Imagining the Internet, Robin Mansell, 2012, Oxford University Press, p. 38-40
5. <https://www.libver.gr/%CE%B5%CE%BA%CF%80%CE%B1%CE%AF%CE%B4%CE%B5%CF%85%CF%83%CE%B7-%CE%BA%CE%B1%CE%B9-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CE%AD%CE%BD%CE%B1-%CF%80/>
6. <https://dipe.art.sch.gr/index.php/home/84-kyvernoasfaleia-cybersecurity>

Ανεξάρτητες Αρχές & Φορείς

Συνήγορος του Παιδιού

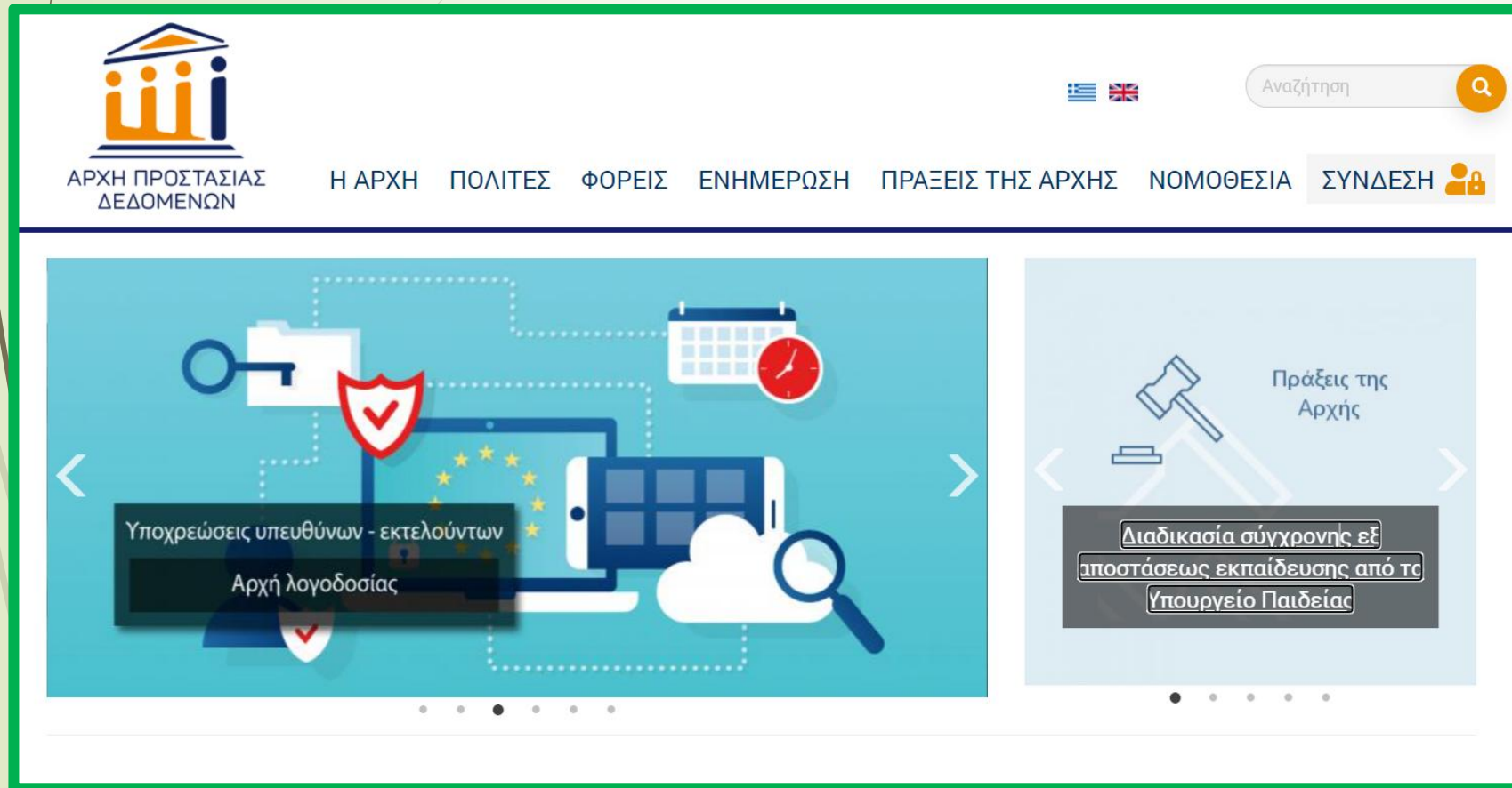
ΣΥΝΗΓΟΡΟΣ
ΤΟΥ ΠΟΛΙΤΗ
ΑΝΕΞΑΡΤΗΤΗ ΑΡΧΗ

Βέλτιστη πρακτική
Φορείς της Εκπαίδευσης, Περιφέρειες, Δήμοι,
Επιμελητήρια μπορούν να εντάξουν στις ιστοσελίδες
τους, τους **συνδέσμους** των Ανεξάρτητων Αρχών



- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Συνήγορος του Καταναλωτή
- Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)
- Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)
- Επιτροπή Εποπτείας και Ελέγχου Παιγνίων (ΕΕΕΠ)
- Τράπεζα της Ελλάδος
- **Συνήγορος του Πολίτη**
- Εθνικός Οργανισμός Φαρμάκων (ΕΟΦ)

Υλικό από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

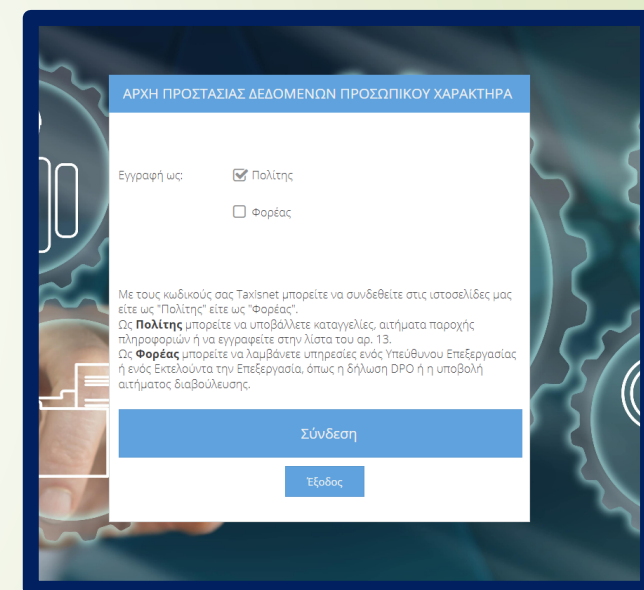


η δημιουργία ειδικής πλατφόρμας παροχής εξειδικευμένης ενημέρωσης προς υπευθύνους προστασίας δεδομένων (DPOs) και επαγγελματίες Κυβερνασφάλειας και η δημιουργία εκπαιδευτικού υλικού σε θέματα προστασίας δεδομένων για μαθητές πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης

Πηγές

1. <https://www.dpa.gr/sites/default/files/2025-06/Annual%202024%20v1.0%20Web.pdf>
2. https://bydefault-project.eu/wp-content/uploads/2024/08/Brochure_3.pdf

Δυνατότητα Αναφοράς πολιτών προς την ΑΠΔΠΧ

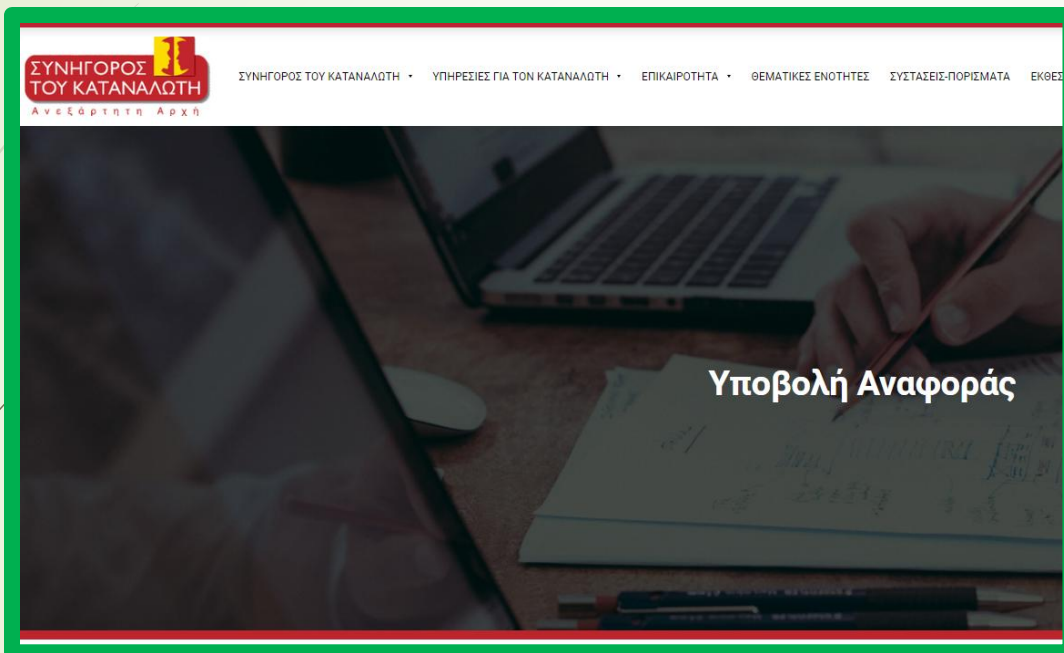


Πηγές

1. <https://eservices.dpa.gr/>
2. <https://www.synigoros.gr/el/category/default/post/eidikh-ek8esh-or-pshfiakes-platformes-kai-dhmosia-dioikhsh>

Αναφορά προς τον Συνήγορο του Καταναλωτή

**ΣΥΝΗΓΟΡΟΣ
ΤΟΥ ΚΑΤΑΝΑΛΩΤΗ**
Ανεξάρτητη Αρχή



Πηγές:

1. <https://www.synigoroskatanaloti.gr/el/etisia-ekthesi-2023> σελ. 5
2. <https://www.synigoroskatanaloti.gr/el/ypoboli-anaforas>
3. <https://www.synigoroskatanaloti.gr/el/deltio-typoy-pagkosmia-imera-katanaloti-0>

Καλή πρακτική από φορείς Διεύθυνση Πρωτοβάθμιας Εκπαίδευσης Άρτας

https://dipe.art.sch.gr/index.php/2014-06-29-19-31-34/ekp-ko-yliko/dimotiko/2-uncategorised/84-kyvernoasfaleia-cybersecurity

Εξοδος YouTube KYBERNOEFKΛHMA DeepL Translate DRUGS AND ORGA... NOMIKA ΘΕΜΑΤΑ Μετάφραση Google ΠΕΡΙΒΑΛΛΟΝ

ΑΡΧΙΚΗ Δ/ΝΣΗ ΣΧΟΛΕΙΑ ΣΥΜΒΟΥΛΟΙ ERASMUS+ ΑΞΙΟΛΟΓΗΣΗ ΝΟΜΟΘΕΣΙΑ ΕΝΤΥΠΑ ΕΠΙΚΟΙΝΩΝΙΑ

Δι.Π.Ε. Άρτας
YouTube channel

Κυβερνοασφάλεια (Cybersecurity)

10

Title	Modified Date	Hits
Εκδήλωση με θέμα "Η Κυβερνοασφάλεια στην καθημερινότητα" με διαδικτυακή κάλυψη ειδική για σχολεία μέσω Webex	16 November 2024	Hits: 2
Εισήγηση με θέμα: "Προστασία Προσωπικών Δεδομένων στον Κυβερνοχώρο" - Λάκωμα Χαλκιδικής: 08-11-2024 - Κοινή Δράση Ιδιωτικού Σχολείου με Δημόσια Σχολεία	16 November 2024	Hits: 3
«Διαδικτυακή πραγματικότητα & προκλήσεις», ημερίδα στις 10/10/2024 στο Δημοτικό Θέατρο Μυτιλήνης	05 October 2024	Hits: 124
Απειλητική έκφανση του Κυβερνοεγκλήματος οι διαδικτυακές απάτες	05 October 2024	Hits: 116
Report on Indicators of School Crime and Safety: 2023	21 October 2024	Hits: 217

myschool

KYBERNOΑΣΦΑΛΕΙΑ

CYBERSECURITY

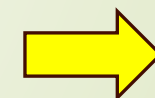
Ειδικό αφιέρωμα στην Κυβερνοασφάλεια

https://dipe.art.sch.gr/index.php/home/84-kyv

← Ασφάλεια
dipe.art.sch.gr

🔒 Η σύνδεση είναι ασφαλής
Οι πληροφορίες σας (για παράδειγμα, οι κωδικοί πρόσβασης ή οι αριθμοί πιστωτικών καρτών) είναι ιδιωτικές κατά την αποστολή σε αυτόν τον ιστότοπο. [Μάθετε περισσότερα](#)

☑️ Το πιστοποιητικό είναι έγκυρο



Πηγή:
<https://dipe.art.sch.gr/index.php/2014-06-29-19-31-34/ekp-ko-yliko/dimotiko/2-uncategorised/84-kyvernoasfaleia-cybersecurity>

Αναφορά Κυβερνοεγκλημάτων- υπάρχει πλέον πλατφόρμα –άμεσα, εύκολα και δωρεάν

Εισαγγελία Πρωτοδικών

Αρχές Επιβολής του
Νόμου

Ανεξάρτητες Διοικητικές
Αρχές

Ειδικές Πλατφόρμες

Ηλεκτρονικό Ταχυδρομείο

Τηλεφωνικό Κέντρο 11188



Καταγγελίες για εγκλήματα κυβερνοχώρου

Καταγγελία για αδικήματα τελούμενα σε βάρος ανηλίκων μέσω διαδικτύου

Καταγγελία για οικονομικά κυβερνοεγκλήματα όπου εμπλέκονται ηλεκτρονικά/ψηφιακά νομίσματα

Καταγγελία για παραβίαση του απορρήτου των ηλεκτρονικών και τηλεφωνικών επικοινωνιών

Καταγγελία για παράνομη διακίνηση οπτικοακουστικών έργων μέσω διαδικτύου

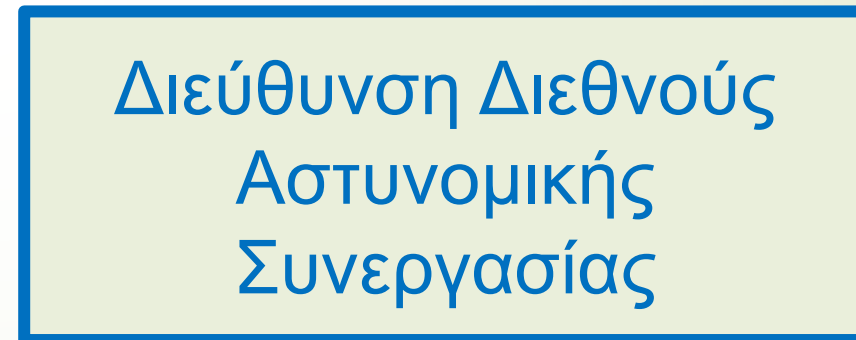
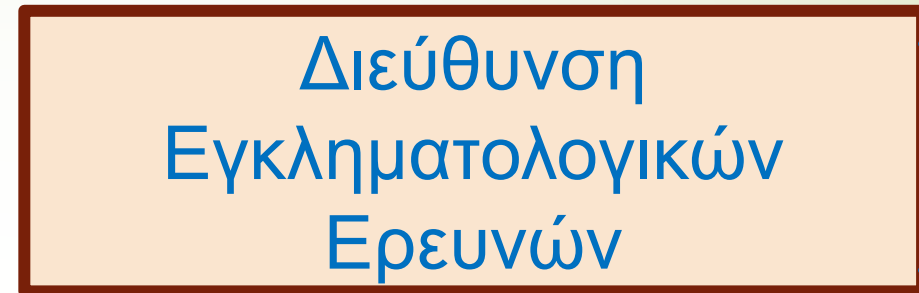
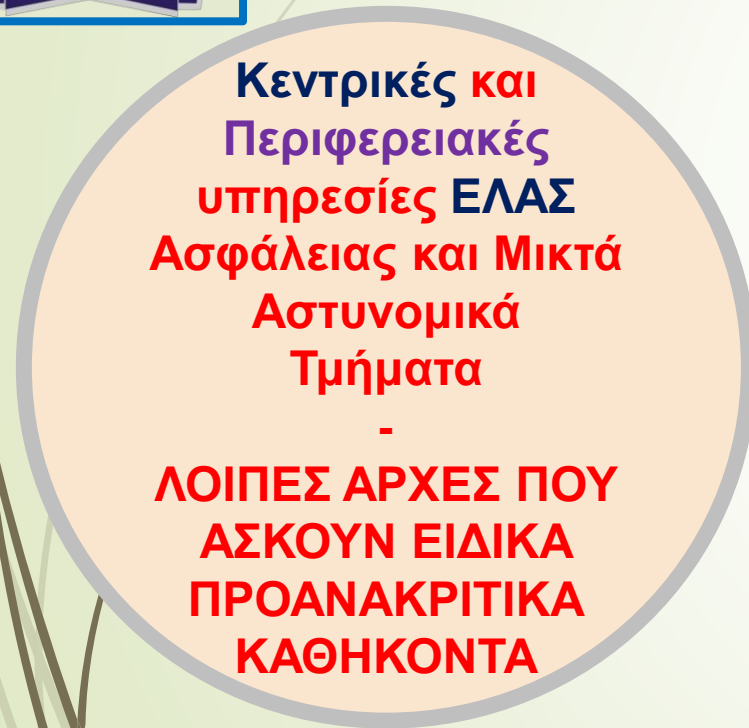
Καταγγελία για παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή

Καταγγελία για περιπτώσεις απάτης με υπολογιστή

Πηγές:

1. <https://www.gov.gr/ipiresies/polites-kai-kathemerinoteta/kataggelies>
2. <https://www.zougla.gr/n/technology/world-of-tech/article/to-sistema-anaforas-kivernoeglimaton-ke-kivnoperistatikon-stin-xora-mas> **18-12-2020**
3. <https://www.synigoros.gr/el/category/default/post/eidikh-ek8esh-or-pshfiakes-platformes-kai-dhmosia-dioikhsh>
4. <https://www.minocp.gov.gr/2025/02/24/24-02-2025-i-diefthynsi-dioxis-ilektronikou-egklimatos-einai-apo-tis-ypiresies-aichmis-gia-tin-astynomia-tis-neas-epochis/>

Υπηρεσίες Αντιμετώπισης Κυβερνοεγκλήματος & ΤΝ



Π Ε Ι Σ Τ Η Ρ Ι Α

Π Λ Η Ρ Ο Φ Ο Ρ Ι Α

Ν 5187/2025 ΦΕΚ Α 48 «Αναδιοργάνωση της δομής της Ελληνικής Αστυνομίας και αναβάθμιση της εκπαίδευσης του ένστολου προσωπικού της Εξουχρονισμός του θεσμού της ηλεκτρονικής επιτήρησης υπόδικων, κατάδικων και κρατούμενων σε άδεια Ρύθμιση θεμάτων κρατούμενων σε σωφρονιστικά καταστήματα και άλλες διατάξεις
Άρθρα 51, 24, 52-60, 44-45

Εγκληματολογική Έρευνα Ψηφιακών Πειστηρίων με εργαλεία ΤΝ



IT'S ALL IN THE NAME

Because 'International Organization for Standardization' would have different acronyms in different languages (IOS in English, OIN in French for *Organisation internationale de normalisation*), our founders decided to give it the short form ISO. ISO is derived from the Greek 'isos', meaning equal. Whatever the country, whatever the language, we are always ISO.

Πρότυπες και πιστοποιημένες διαδικασίες (ISO 9001, ISO 17025)

Πηγές:

1. <https://www.astynomia.gr/elliniki-astynomia/eidikes-ypiresies/diefthynsi-egklimatologikon-erevnon-d-e-e/>
2. <https://www.iso.org/about-us.html>
3. <https://enfsi.eu/>
4. https://enfsi.eu/wp-content/uploads/2024/06/ENFSI_Annual_Report_2023-1.pdf p. 16

Διεθνής Συνεργασία – Ανταλλαγή Πληροφοριών



Πληροφορίες και καλές πρακτικές

Πηγές:

1. https://www.europol.europa.eu/cms/sites/default/files/documents/Grace%20Guidelines%202022_Public_0.pdf
2. <https://www.interpol.int/Crimes/Illicit-goods/Pharmaceutical-crime-operations>



Διεθνής Συνεργασία – Πράξη και Αποτελέσματα



Europol, 11/02/2025

Επιχείρηση «Phobos Ransomware - 8Base»

- Διεθνής επιχείρηση της Europol και Eurojust μαζί με άλλες 14 χώρες συμμετείχαν στην επιχείρηση .
- Οι κυβερνοεγκληματίες κρυπτογράφησαν κρίσιμες υποδομές, επιχειρηματικά συστήματα και προσωπικά δεδομένα έναντι λύτρων.
- επιθέσεις μεγάλου όγκου εναντίον μικρών και μεσαίων επιχειρήσεων, οι οποίες συχνά δεν διαθέτουν τις άμυνες κυβερνοασφάλειας για να προστατευτούν
- αποτέλεσμα:
Συλλήψεις, έρευνες και κατασχέσεις.

Πηγή:

<https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals>



Συνεργασία για περισσότερη Ασφάλεια στον Κυβερνοχώρο

Ακαδημαϊκή Κοινότητα

NO MORE RANSOM!

www.nomoreransom.org



Online child sexual coercion
and extortion is a crime

Has this
happened to you?

SAY NO!

We can help you.
You are not alone.

Δημόσιος Τομέας

Ιδιωτικός Τομέας

Επικαιροποίηση Θεσμικού πλαισίου

Medicrime Convention

(αφορά τα φάρμακα που διακινούνται παράνομα στο διαδίκτυο)

Υπέγραψε η χώρα μας 18/5/2022

Εκκρεμεί η επικύρωση από την
Ελληνική Βουλή
26/09/2025



Πηγές:

1. <https://www.coe.int/en/web/medicrime>
2. https://www.coe.int/en/web/medicrime/newsroom/-/asset_publisher/3N6QmrARke1B/content/greece-signs-the-medicrime-convention?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fmedicrime%2Fnewsroom%3Fp_p_id%3D101_INSTANCE_3N6QmrARke1B%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D1
3. <https://dailypharmanews.gr/politiki-ygeias/diakinesi-farmakon-sto-diadiktyo-amesi-thorakisi-tou-thesmikou-plaiiou-kata-aftou-tou-organomenou-egklimatos/>
4. https://www.hellenicparliament.gr/UserFiles/c0d5184d-7550-4265-8e0b-078e1bc7375a/12951870.pdf?fbclid=IwY2xjawKr4ttleHRuA2FlbQlXMAbIcmIkETB4T1hObDNnNkh4TWZ6SE4wAR7zYLMoQFAYNOXbq7VUbcBmPk0WkCVhgsW-Czkrb32_SQWV-jKJpRxtPZjs_4w_aem_00bjjEqYTRQrYa7NFznhNg

OPENED TO SIGNATURE

28 October 2011

ENTERING INTO FORCE

1st January 2016

1st COMMITTEE OF PARTIES

17 December 2018

23 RATIFICATIONS

15 CoE member States

8 non CoE member States (Belarus, Benin, Burkina Faso, Guinea, Ivory Coast, Morocco, Niger, Russian Federation)

22 SIGNATURES

14 CoE member States

8 non CoE member States (Chad, Chile, Congo, Ecuador, Israel, Mali, Togo, Tunisia)

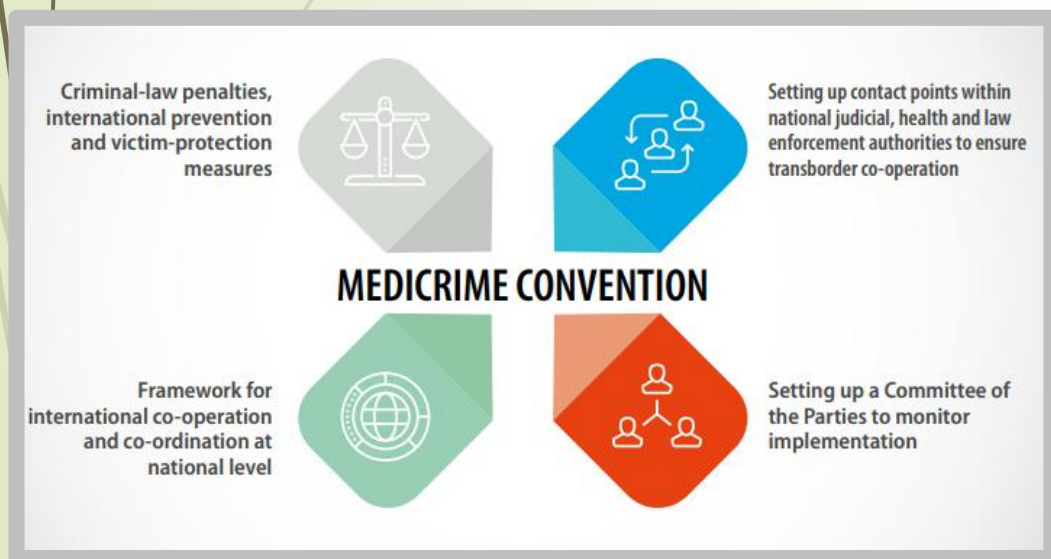
2 INVITATIONS

2 countries invited to sign (Cameroon, Senegal)



Τι προβλέπει η Σύμβαση

Medicrime Convention



- ☐ Ποινικοποιεί την παραγωγή και την διακίνηση των πλαστών φαρμάκων
- ☐ Προβλέπει συνεργασία με διεθνείς οργανισμούς όπως τον ΠΟΥ, την Interpol, την Europol
- ☐ Επικεντρώνεται στην προστασία της δημόσιας υγείας



Τι κάνει η χώρα μας για το θέμα

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
ΔΙΕΥΘΥΝΣΗ ΚΟΙΝΩΝΟΜΑΘΗΤΙΚΟΥ ΕΛΕΓΧΟΥ
Αρμόχ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 5765
Ημερομ. Κατάθεσης: 28/5/2025



ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
Αναστάσιος Δημοσθένης
Βουλευτής Εβρου

Αλεξ/πολη, 29/05/2025

ΕΡΩΤΗΣΗ

ΠΡΟΣ: 1.ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ
2.ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
3.ΥΠΟΥΡΓΕΙΟ ΔΙΚΑΙΟΣΥΝΗΣ
4.ΥΠΟΥΡΓΕΙΟ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΠΟΛΙΤΗ

ΘΕΜΑ: ΑΝΑΓΚΑΙΑ Η ΕΠΙΚΥΡΩΣΗ & ΕΦΑΡΜΟΓΗ ΤΗΣ ΔΙΕΘΝΟΥΣ ΣΥΜΒΑΣΗΣ ΓΙΑ ΤΗΝ ΠΑΡΑΝΟΜΗ ΔΙΑΚΙΝΗΣΗ ΦΑΡΜΑΚΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ (MEDICRIME CONVENTION), ΠΡΟΚΕΙΜΕΝΟΥ ΝΑ ΘΩΡΑΚΙΣΤΕΙ Η ΔΗΜΟΣΙΑ ΥΓΕΙΑ!!

Το Συμβούλιο της Ευρώπης το 2011 προχώρησε, σε επίκαιρο χρόνο, στη θέσπιση συμπαγούς νομοθετικού πλαισίου για την καταπολέμηση της παράνομης διακίνησης φαρμακευτικών σκευασμάτων στον ψηφιακό χώρο, υπογράφοντας την Διεθνή Σύμβαση για τα φάρμακα που διακινούνται στο διαδίκτυο, ευρύτερα γνωστή ως «Medicrime Convention», η οποία και τέθηκε σε ισχύ το 2016.

Η Ελλάδα, αποδίδοντας την δέουσα βαρύτητα στη διαρκή ενίσχυση της δημόσιας υγείας της χώρας, πρόβη στην υπογραφή της ως άνω σύμβασης τον Μάιο του 2022, η οποία ωστόσο δεν έχει ενσωματωθεί στο "νομοθετικό σπλάσασμο" της Χώρας, καθώς εκκρεμεί η διαδικασία της επικύρωσης αυτής.

Όπως επισημαίνεται και στο συνοδευτικό υπόμνημα του π.Διευθυντού της Δίωξης Ηλεκτρονικού Εγκλήματος, Αντιστρατήγου ε.α., Γεωργίου Παπαπροδρόμου, η καθυστέρηση ενέχει σοβαρούς κινδύνους, καθώς και επιχειρησιακές δυσλειτουργίες σε ό,τι αφορά την εφαρμογή του νόμου προστατεύοντας τους πολίτες.

Η επικύρωση της σύμβασης θα ενεργοποιήσει ένα στρατηγικής σημασίας εργαλείο για την προστασία των πολιτών απέναντι σε δυνητικά θανατηφόρα σκευάσματα αγνώστου προέλευσης, ενισχύοντας ως Πολιτεία την εξωτερική μας εικόνα που επιδεικνύει ωριμότητα, μεθοδικότητα και συνέπεια στη προστασία του υπέρτατου αγαθού της υγείας.



Σέκρες 1, Αθήνα | Τηλ.: 2103675611 | Fax: 2103675612 | Κω. - 697 811 98 63 | admoschakis@outlook.com
Καραϊσκάκη 10, Αλεξάνδρουπολη | Τηλ.: 25510 27548 | Fax: 25510 36874 | Ελ. Βενιζέλου 28, Διδυμότειχο | Τηλ.: 25530 23086



- ☐ Υπογραφή Σύμβασης
Μάιος 2022
- ☐ Επερώτηση για την μη Επικύρωση της Σύμβασης
Σεπτέμβριος 2025

Πηγές

- https://www.hellenicparliament.gr/UserFiles/c0d5184d-7550-4265-8e0b-078e1bc7375a/12951870.pdf?fbclid=IwY2xjawKr4ttleHRuA2FlbQlxMABicmlkETB4T1hObDNnNkh4TWZ6SE4wAR7zYLMoQFAYNOXbq7VUbCBMpk0WkCVhgsWCzkrb32_SQWV-jKJpRxtPZjs_4w_aem_00bjjEqYTRQrYa7NFznhNg
- <https://www.hellenicparliament.gr/UserFiles/67715b2c-ec81-4f0c-ad6a-476a34d732bd/12976450.pdf>

Ενίσχυση Καινοτομίας

The History of INNOVATION CYCLES

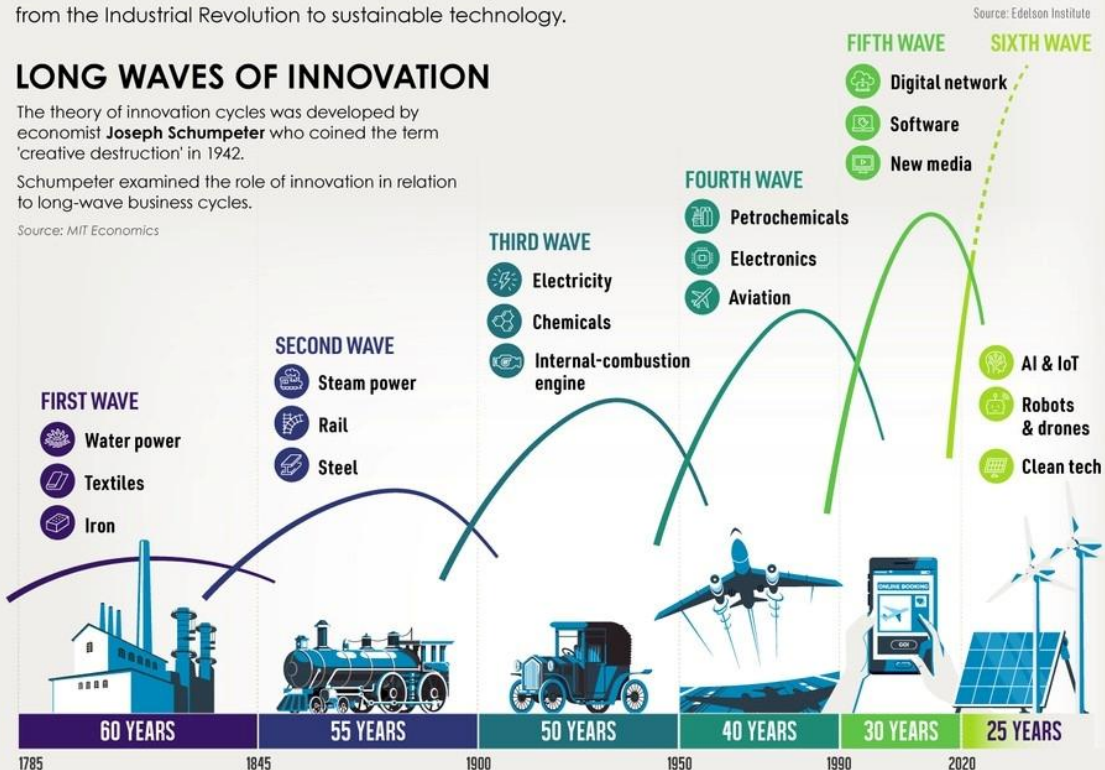
Below, we show waves of innovation across 250 years, from the Industrial Revolution to sustainable technology.

LONG WAVES OF INNOVATION

The theory of innovation cycles was developed by economist **Joseph Schumpeter** who coined the term 'creative destruction' in 1942.

Schumpeter examined the role of innovation in relation to long-wave business cycles.

Source: MIT Economics



FIRST WAVE

During the Industrial Revolution, the first factory emerged—a cotton mill in Britain.

SECOND WAVE

As railways proliferated, their networks strongly influenced urban growth.

Source: Nacima Baron, HAL

THIRD WAVE

Henry Ford's Model T introduced the assembly line, revolutionizing the automotive industry.

FOURTH WAVE

Aviation gains mass adoption on a global scale, providing a lever to economic integration.

FIFTH WAVE

In 1990, 2.3M used the internet—by 2016 this reached 3.4B.

Source: World Bank

SIXTH WAVE

As climate challenges intensify, clean tech may reshape business models and consumption patterns.

Κύκλοι Καινοτομίας – Συστήματα και Συσκευές Μέρος της καθημερινότητάς μας



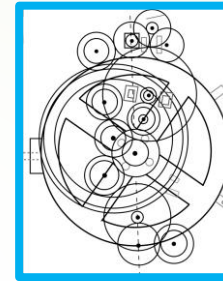
4 WAYS DRONES ARE USED IN AGRICULTURE

Πηγές:

1. https://www.visualcapitalist.com/the-history-of-innovation-cycles/?fbclid=IwAR2BybbJ-LFrcaQCW-qf8O8FluNUhwP0FesuU-EiRNO2-DJGOv_cHXT0vkQ
2. <https://unctad.org/tir2023>
3. <https://itif.org/about/>
4. <https://www.nist.gov/cybersecurity/cybersecurity-awareness-month>
5. <https://nebraskacorn.gov/cornstalk/sustainability/four-ways-drones-are-used-in-agriculture/>

Τεχνολογία - Καινοτομία και Ελλάδα

Μηχανισμός Αντικυθήρων

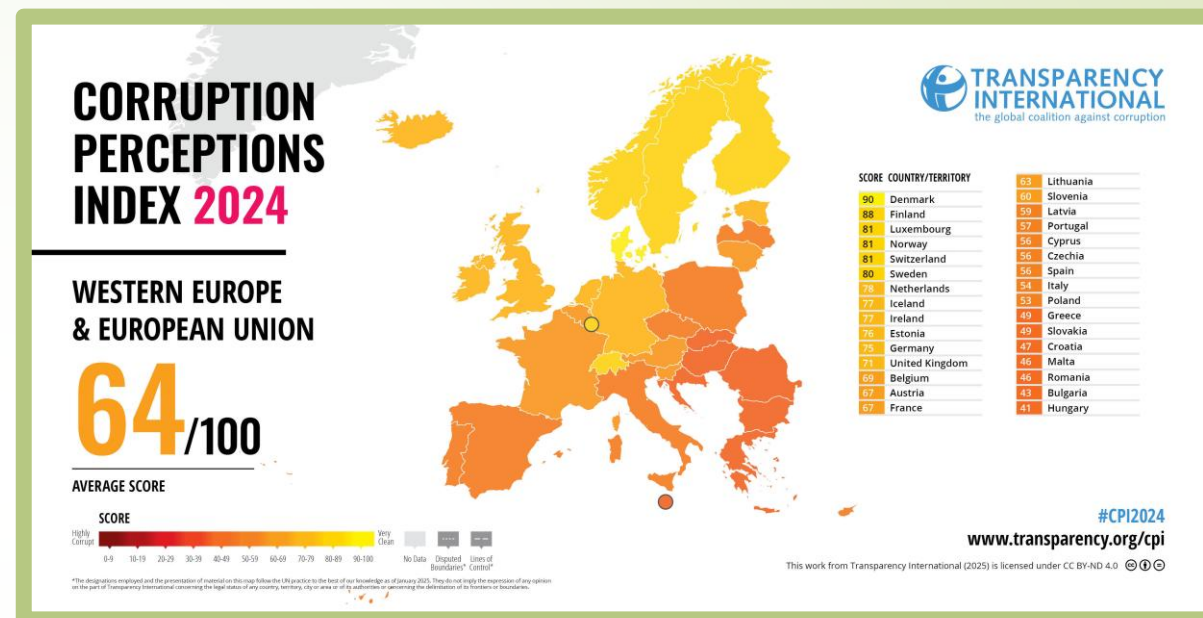
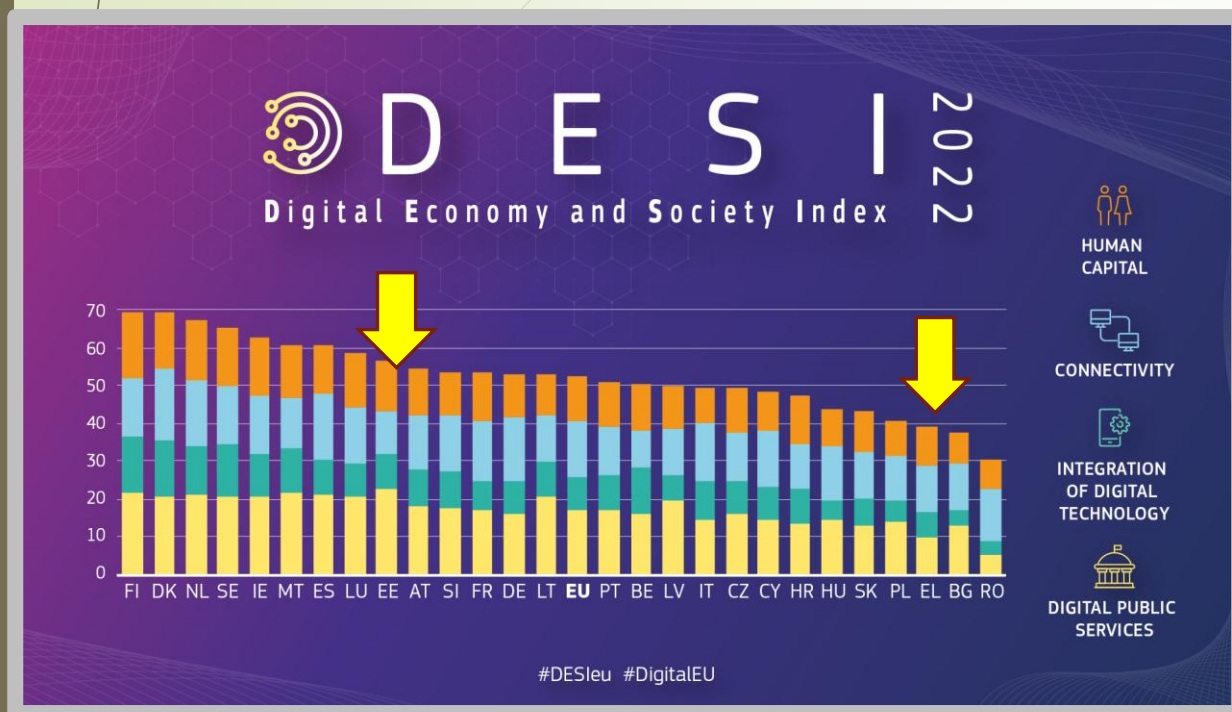


Πηγές:

1. <https://www.thearchaeologist.org/blog/how-does-the-antikythera-mechanism-work>
2. <https://www.theguardian.com/science/2021/mar/12/scientists-move-closer-to-solving-mystery-of-antikythera-mechanism>
3. https://en.wikipedia.org/wiki/Antikythera_mechanism
4. <https://www.namuseum.gr/new/o-michanismos-ton-antikythiron-kai-i-selini/>

Δείκτης Ψηφιακής Οικονομίας & Κοινωνίας

Ψηφιακή Σύγκλιση – Διαφάνεια (CPI 2024)



Δημοσιεύθηκαν 28/07/2022 & 11/2/2025

Πηγές:

1. <https://digital-strategy.ec.europa.eu/en/policies/desi>
2. https://images.transparencycdn.org/images/Report_CPI2024.pdf
3. <https://www.ethnos.gr/opinions/article/195948/pshfiakosmetasxhmatismoskaidiafaneiahallazoynehboyliazyome>
4. <https://digital-strategy.ec.europa.eu/en/library/country-reports-digital-decade-report-2023>



Τι μπορεί να γίνει

- Προστασία κι ενδυνάμωση των ευάλωτων ατόμων στο ψηφιακό περιβάλλον
- Ανάπτυξη Κουλτούρας Κυβερνοασφάλειας (+ Τεχνηθική)
- Αξιοποίηση πόρων και δυνατοτήτων
- Κατάρτιση- εκπαίδευση- μετεκπαίδευση (ανθρώπινων πόρων κι ευάλωτων ομάδων)
- Σεβασμός των πολιτικών κυβερνοασφάλειας και προστασίας των προσωπικών δεδομένων
- Εξάλειψη - περιορισμός ανισοτήτων και συμπερίληψη
- Ενίσχυση Θετικών Δράσεων και Πρωτοβουλιών

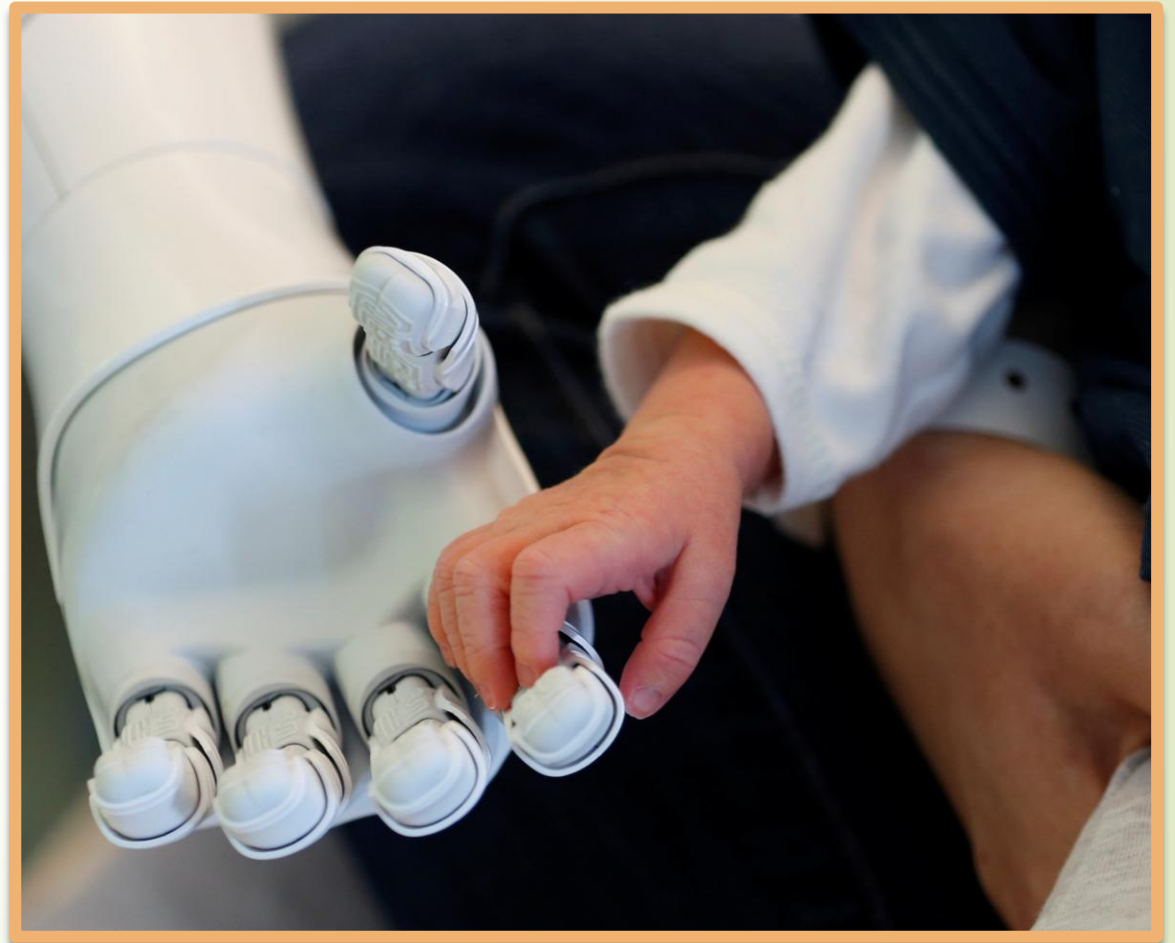
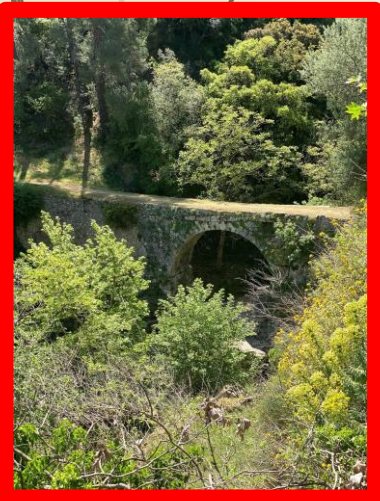


Από πλευράς της πολιτείας

- Στρατηγική και Όραμα
- Πολιτική βούληση & ευρύτερη δυνατή συναίνεση
- Κουλτούρα Συνεργασίας Φορέων [*Πανεπιστημιακές Σχολές, Ερευνητικά Κέντρα, Επιστημονικοί Σύλλογοι, Εμπλεκόμενοι φορείς, Ενίσχυση Διεθνούς Συνεργασίας*]
- Κουλτούρα Τεχνοθικής
- Θεσμική **θωράκιση** (2ο πρωτόκολλο Cybercrime Convention, εξειδίκευση δικαστών, Ειδικός Εισαγγελέας για το Κυβερνοέγκλημα για όλη την χώρα, ορισμός Εισαγγελικού λειτουργού για εποπτεία πλατφόρμας καταγγελιών, ενίσχυση με επιστήμονες των εγκληματολογικών εργαστηρίων για την εξέταση των πειστηρίων, τραπεζικό απόρρητο, Medicrime convention, ενίσχυση του θεσμικού πλαισίου για την TN, κα.)
- Διάθεση Πόρων για την Κυβερνοασφάλεια
- Αξιοκρατία – Διαφάνεια – Δικαιοσύνη



Στο χέρι μας... να είμαστε γεφύρι που
συνδέει την τεχνολογία με την ευημερία μας



Σε κάθε περίπτωση.....

Μια **νέα** **διαχρονική** εφαρμογή
Το καλύτερο **δώρο** για όλους
Κι αυτή λέγεται **“σεβασμός”**

Πηγή:

<https://www.linkedin.com/company/european-leadership/posts/?feedView=all>

Putting your phone away
and paying attention to
those talking to you...
there's an app for that.

It's called respect.



MyPositiveOutlooks.com

Χρήσιμες πληροφορίες στο κανάλι του εισηγητή στο Youtube

Με θεματικά
playlists & links

< Giorgos Papaprodromou...

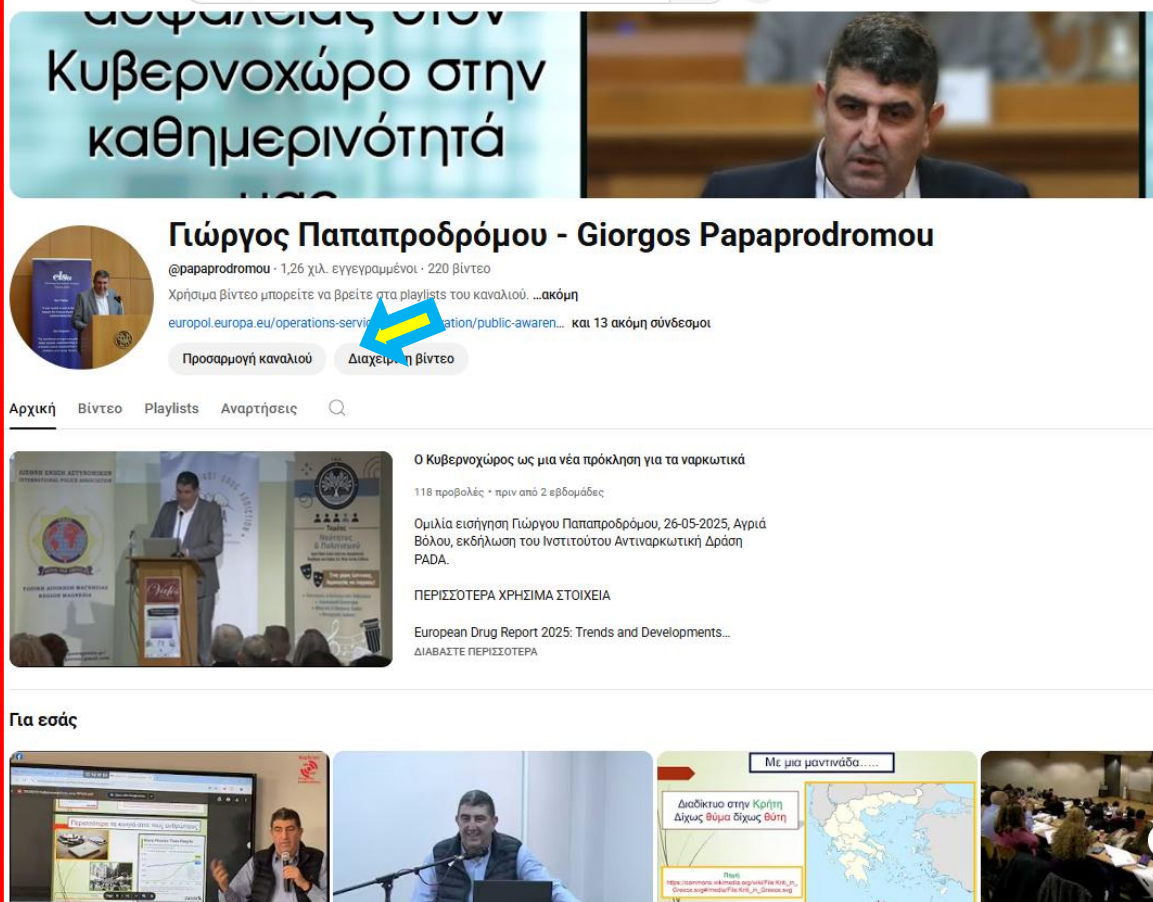
AYLISTS KOINOTHTA KANALIA ΠΛΗΡΟΦ

Σύνδεσμοι

-  Prevention Guides EUROPOL
-  Protecting Children COE
-  Cybercrime COE
-  Cybercrime Interpol
-  Cybersecurity Basics FTC USA
-  ENISA PUBLICATIONS
-  CYBERSECURITY CISA USA
-  CYBER AWARE UK
-  CYBERCRIME EUROJUST
-  CYBER AWARENESS AUSTRALIA
-  Κυβερνοασφάλεια ΕΑΨΙ ΥΨΗΔ
-  CSIRT HELLENIC
-  ITU CYBERSECURITY
-  CYBERSECURITY CANADA

Περισσότερες πληροφορίες

 <http://www.youtube.com/@papaprodromou>



Πηγή:

<https://www.youtube.com/@papaprodromou>

Σας ευχαριστώ πολύ **για την προσοχή σας**
Στη διάθεσή σας για ερωτήσεις



Γιώργος Παπαπροδρόμου

Αντιστράτηγος ε.α. (ΕΛ.ΑΣ.)

Πτυχιούχος Νομικής ΑΠΘ – Δικαστικός Γραφολόγος

Πρώην Διευθυντής Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος