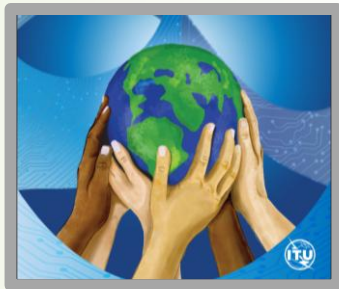
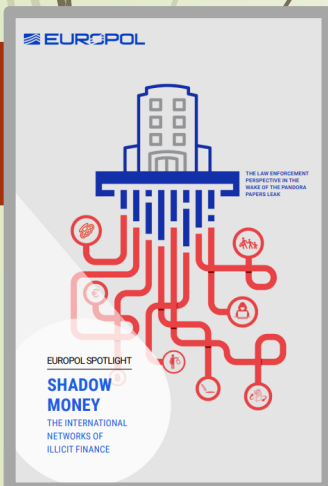


Το Κυβερνοέγκλημα στην εποχή της NIS2 Γιατί οι ΜμΕ βρίσκονται στο στόχαστρο

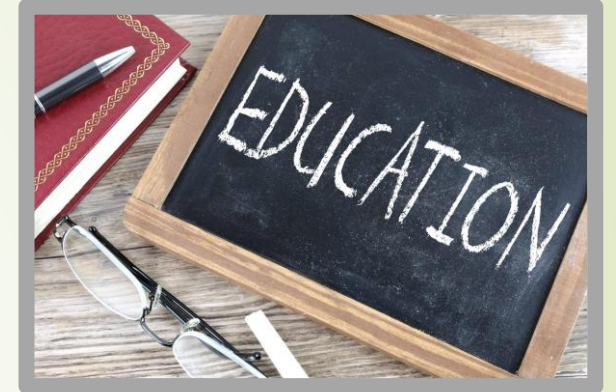


Ηράκλειο, 27/04/2026



Εισηγητής:
Γιώργος Παπαπροδρόμου
Αντιστράτηγος ε.α. (ΕΛ.ΑΣ.)
Πτυχιούχος Νομικής ΑΠΘ – Δικαστικός Γραφολόγος
Ειδικός σε θέματα Αντιμετώπισης Κυβερνοεγκλημάτων

Βασικά σημεία της σημερινής παρουσίασης



1. Τι είναι ο Κυβερνοχώρος;
2. Πως διαμορφώνεται το τοπίο της Κυβερνοασφάλειας;
3. Ποια είναι η τρέχουσα διάσταση του κυβερνοεγκλήματος;
4. Σε ποιο πλαίσιο εντάσσεται η οδηγία NIS2 και πως συνδέεται το θέμα με τις ΜμΕ;
5. Τι πρέπει να γίνει σε θεσμικό και τεχνικό επίπεδο;

Η κατανόηση του Κυβερνοοικοσυστήματος

THE INTERNET: CLEAR WEB, DEEP WEB AND DARK WEB

Internet

Infrastructure consisting of a standardized set of data transfer protocols for digital information exchange.



Clear web (surface web)

Content indexed by standard web-search engines, accessible to anyone using the Internet.

- social networks
- public pages /profiles

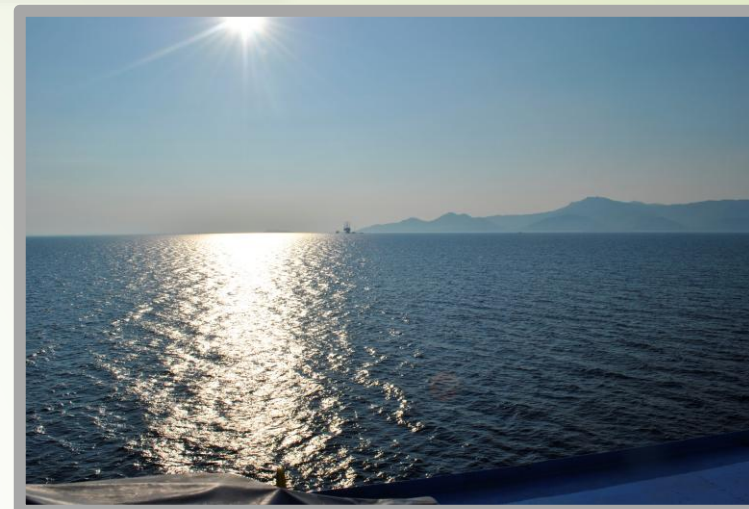
Deep web

Content not indexed by standard web-search engines; content can be located and accessed by a direct URL or IP address but may require a password or other security access to get past public-website pages; includes many very common uses such as web mail, online banking, private or otherwise restricted access content and profiles.

- online banking
- social networks
- restricted pages /profiles

Dark web (darknets)

Darknets, or overlay networks within the Internet that can only be accessed with specific software, configurations, or authorization, and often use a unique customized communication protocol. Two typical darknet types are social networks (usually used for file hosting with a peer-to-peer connection), and anonymity proxy networks such as Tor via an anonymized series of connections.



Πολύπλοκο - σύνθετο περιβάλλον
Με αβεβαιότητες



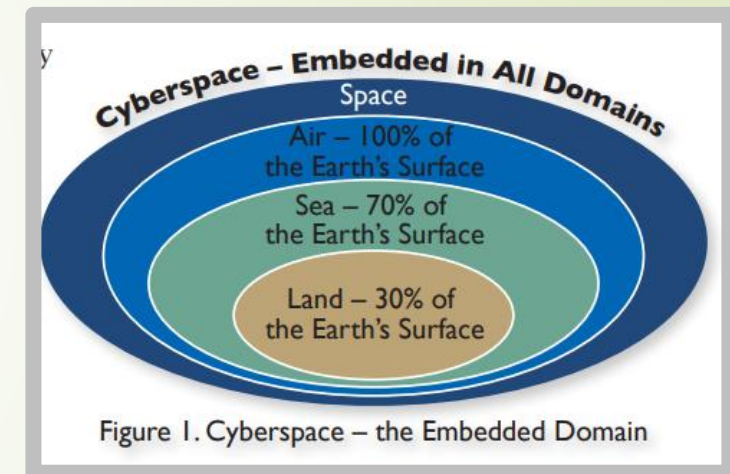
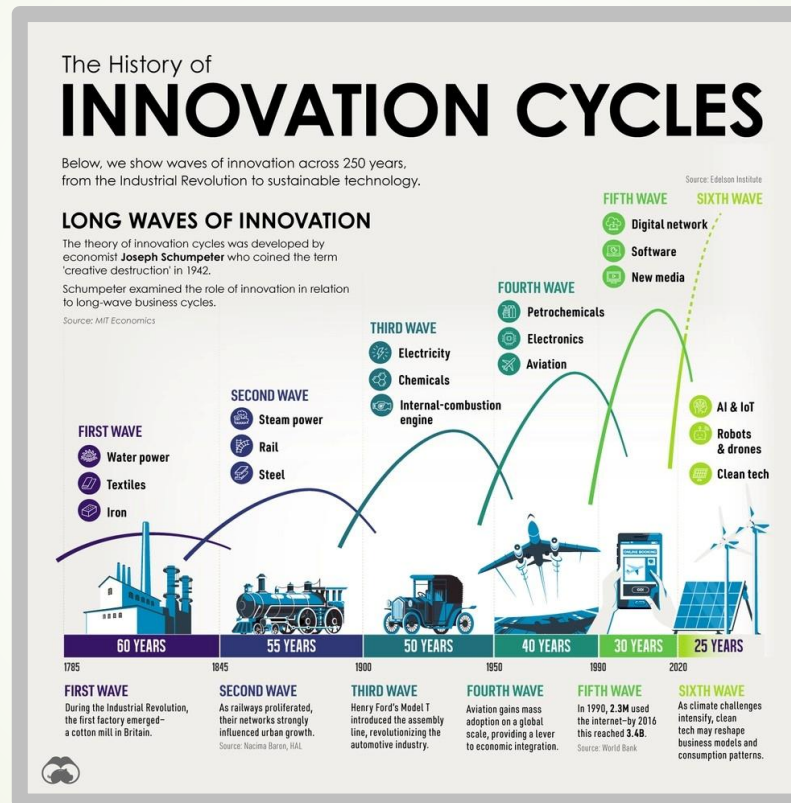
Πηγές:

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 θεωρείται Κυβερνοχώρος; Τεχνολογίες Αιχμής Βιοτεχνολογίες - ΤΝ – Κβαντικές Τεχνολογίες



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/>
4. <https://openknowledge.worldbank.org/server/api/core/bitstreams/692c6149-748f-40dc-b9e6-8e09ba3e47bf/content>

Δισεκατομμύρια άνθρωποι, οντότητες & συσκευές

Χρήστες των νέων τεχνολογιών

1 in 3
internet
users is a child

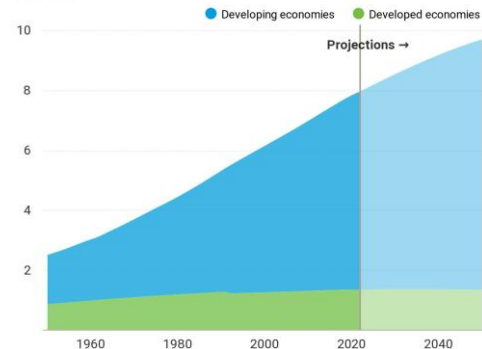
How is the EU protecting them?

#DigitalEU #ChildrensDay



World population growth is mostly in developing economies

People living in developing and developed economies, billions



Source: UNCTADstat based on UN DESA Population Division, World Population Prospects 2022.
Note: The graph provides estimates from 1950 to 2021 and projections from 2022 to 2050 of total population



World Population

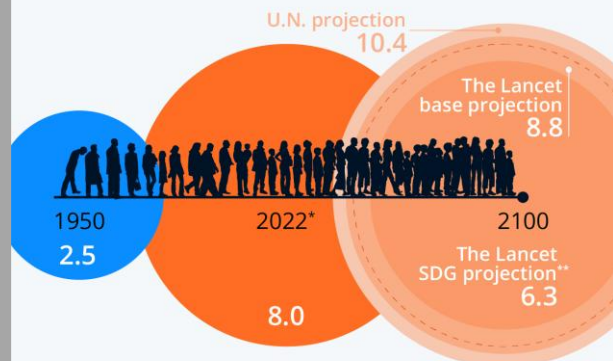
8,180,317,375

TOP 10 MOST POPULOUS COUNTRIES (July 1, 2026)

1. India	1,429,700,205	6. Nigeria	250,228,859
2. China	1,405,918,803	7. Brazil	222,624,000
3. United States	342,620,143	8. Bangladesh	175,927,589
4. Indonesia	285,562,809	9. Russia	139,450,252
5. Pakistan	261,714,024	10. Mexico	132,807,523

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

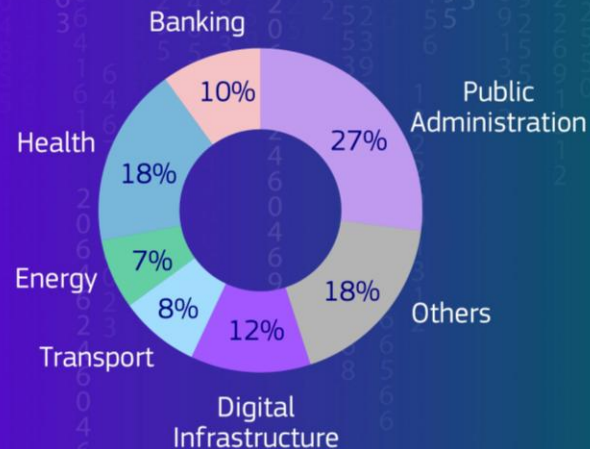
- <https://www.census.gov/popclock/>
- <https://www.worldometers.info/world-population/>
- <https://www.facebook.com/photo?fbid=509355941231664&set=A.298981855602408>
- <https://www.facebook.com/Statista.Inc/photos/pcb.5553912264721206/5553912154721217>
- J. Bradford Delong, Στον δρόμο προς την ουτοπία,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



Απειλές στον Κυβερνοχώρο

1. Λογισμικό εκβιασμού (ransomware)
2. Κακόβουλο λογισμικό (malware)
3. Απειλές κοινωνικής μηχανικής (social engineering)
4. **Απειλές κατά των δεδομένων**
5. Απειλές κατά της διαθεσιμότητας: Άρνηση υπηρεσίας (**Denial of Service**)
6. Απειλές κατά της διαθεσιμότητας: Απειλές στο Διαδίκτυο
7. Παραπληροφόρηση – ψευδείς πληροφορίες
8. Επιθέσεις στην αλυσίδα εφοδιασμού

CYBER INCIDENTS reported in the EU in 2025



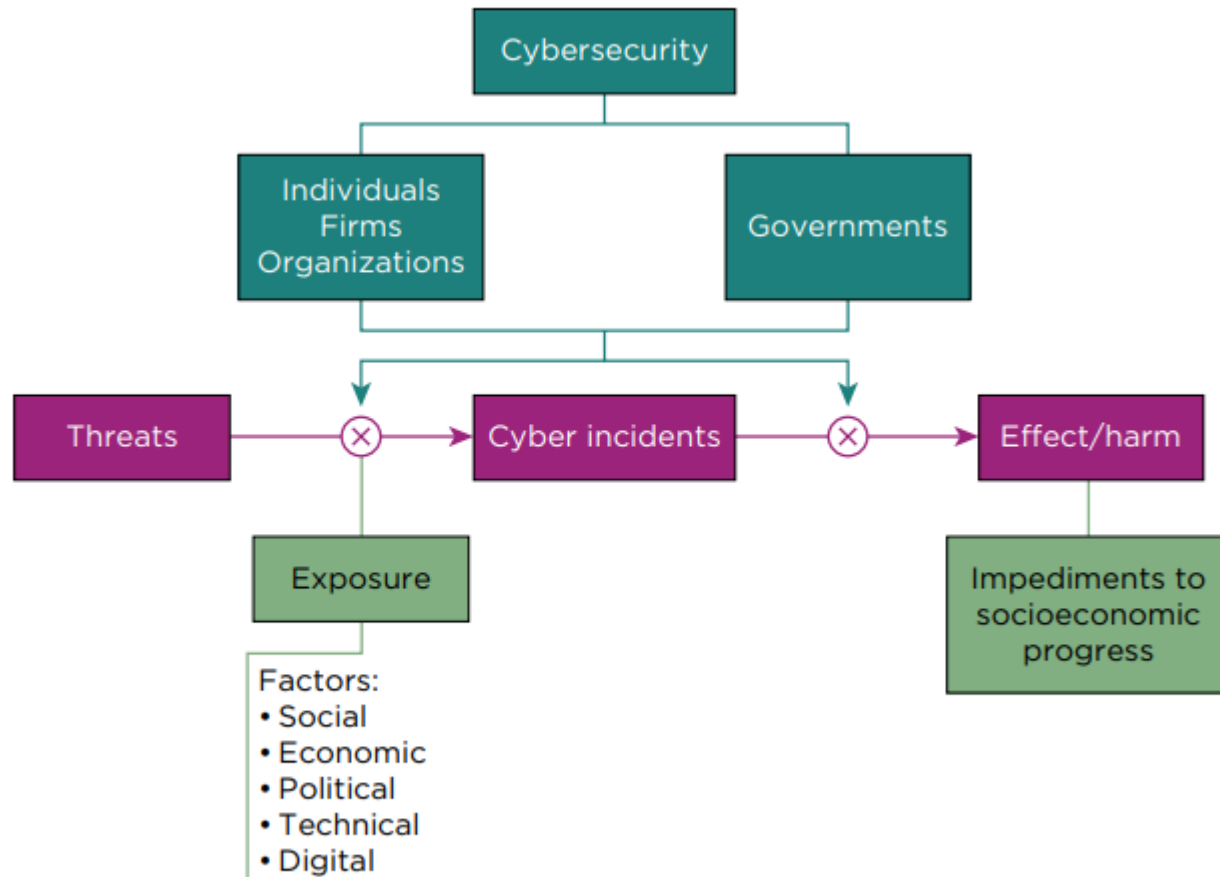
Source: Cybersecurity Incident Reporting and Analysis System 2025

Δημοσιεύθηκε 01/10/2025

Πηγές:

1. <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.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/https://id4d.worldbank.org/guide/cybercrime-and-cybersecurity>
5. <https://www.enisa.europa.eu/search?keys=artificial+intelligence#contentList>
6. <https://ciras.enisa.europa.eu/>

Ποιους επηρεάζει 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

Μικρομεσαίες Επιχειρήσεις και ΕΕ Άνθρωποι – Διαδικασίες - Τεχνολογία



Micro
SME



Staff headcount
< 10



Turnover or Balance
sheet total
≤ € 2 m



Small
SME



Staff headcount
< 50



Turnover or Balance
sheet total
≤ € 10 m



Medium-sized
SME



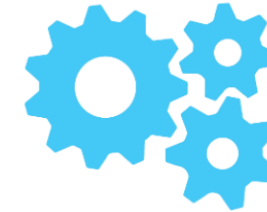
Staff headcount
< 250



Turnover or Balance
sheet total
≤ € 50 m



People



Process



Technology

ΜμΕ

- Χαμηλό επίπεδο άμυνας
- Κόστος ή επένδυση
- Έλλειψη εξειδικευμένου προσωπικού

Πηγές:

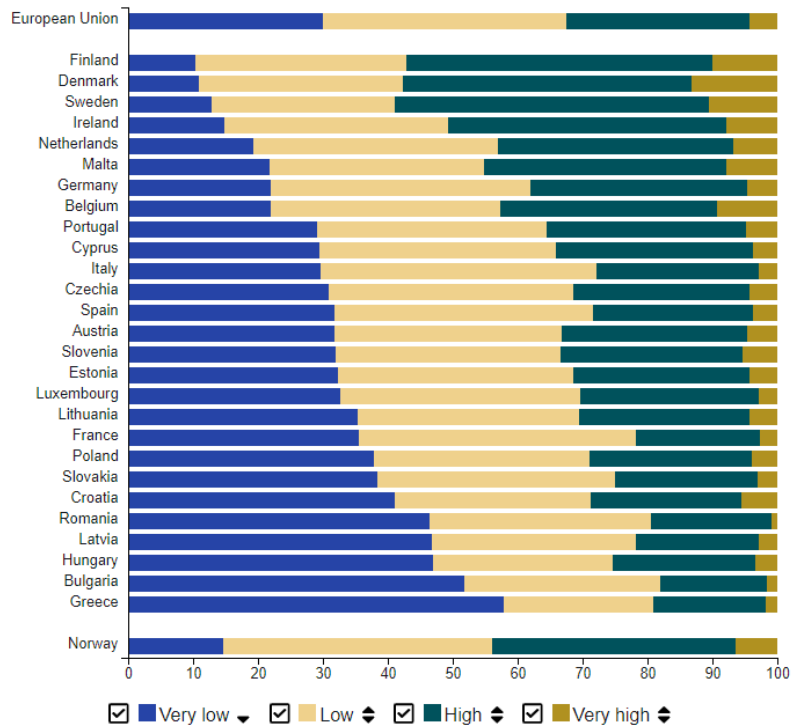
- <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes> p.9, 28
- <https://www.youtube.com/watch?v=ymlKVTat-IM>
- Reinforcing trust and security in the area of electronic communications and online services — ENISA (europa.eu)
- https://cyber.gov.gr/wp-content/uploads/2025/03/250323_%CE%9F%CE%B4%CE%B7%CE%B3%CF%8C%CF%82-%CE%91%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC%CF%82-%CE%9D.-5160_2024-1.pdf

Μικρομεσαίες επιχειρήσεις στην ΕΕ και Κυβερνοασφάλεια

Digital intensity level in businesses, 2022

(as % of total businesses)

Total businesses



Source: Eurostat - [access to dataset](#)

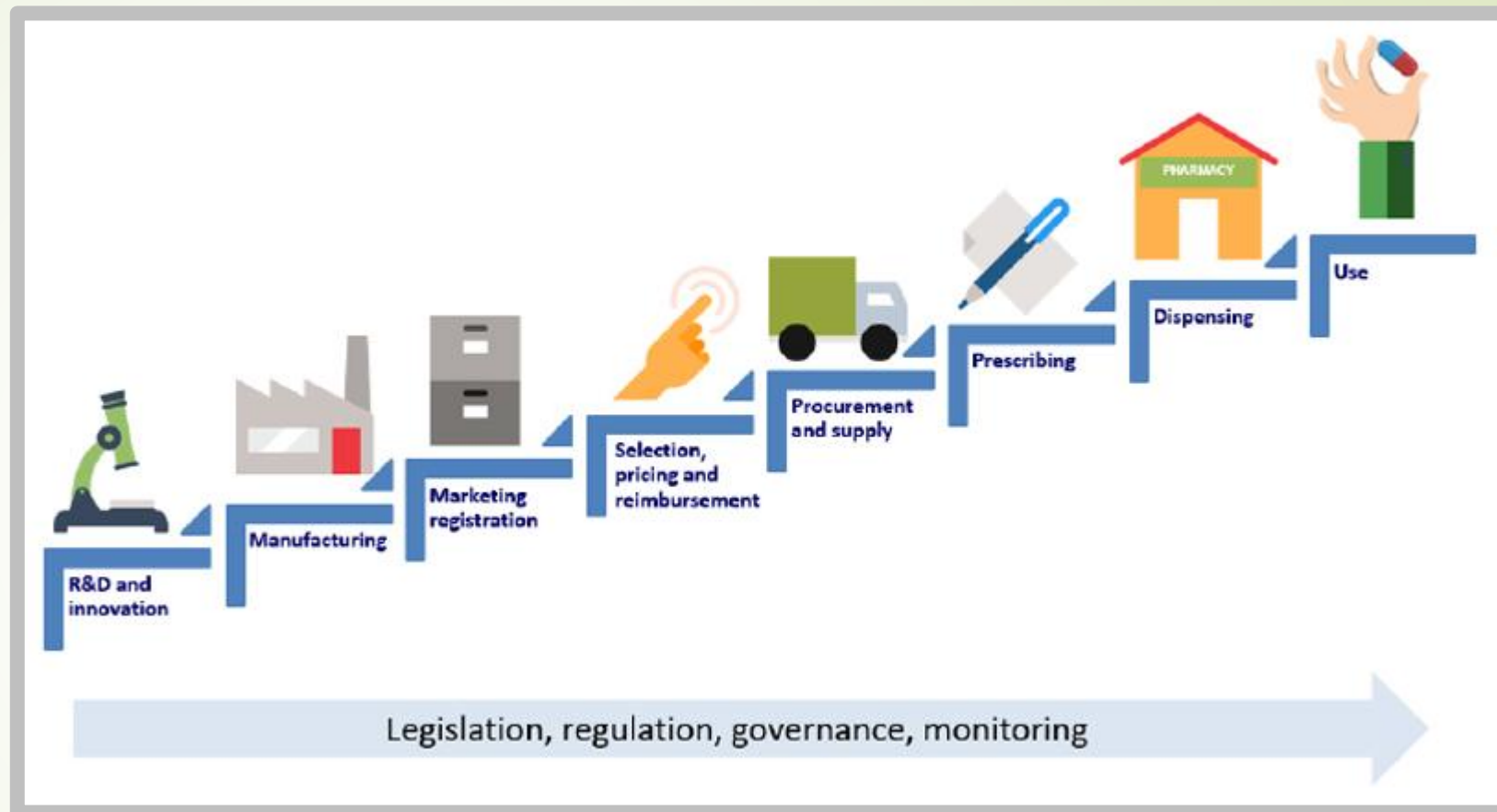
- Αποτελούν την ραχοκοκαλιά της οικονομίας
- Το 99% των επιχειρήσεων στην ΕΕ
- Καταλύτες για τον ψηφιακό μετασχηματισμό όσο και ως βασικό στοιχείο του κοινωνικού ιστού
- Η πανδημία αφορμή για δημιουργία και αλλαγή ψηφιακής νοοτροπίας
- Πληθώρα κυβερνοπεριστατικών και κυβερνοεγκλημάτων
- πολλά περιστατικά δεν καταγγέρονται!!!



Πηγές:

- https://ec.europa.eu/growth/smes_en
- https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme_cybersecurity
- <https://www.enisa.europa.eu/news/enisa-news/survey-to-explore-the-preparedness-of-eu-smes-for-cybersecurity-challenges>
- <https://www.youtube.com/watch?v=ymLKVat-IM>
- <https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2023>
- [Reinforcing trust and security in the area of electronic communications and online services — ENISA \(europa.eu\)](#)

Μελέτη περίπτωσης - Εφοδιαστική Αλυσίδα Φαρμάκου



Δεξιότητες και Ικανότητες απαραίτητες να υποστηρίξουν την ανάγκη όλου του οικοσυστήματος από την Έρευνα, Ανάπτυξη, Καινοτομία έως την χρήση του προϊόντος

Πηγές

1. <https://syntheticdrugs.unodc.org/syntheticdrugs/en/access/pharmaceutical/index.html>
2. <https://www.oecd.org/health/pharmaceuticals.htm>
3. https://www.who.int/health-topics/medicines#tab=tab_1
4. <https://www.ema.europa.eu/en/medicines>
5. <https://www.cancer.gov/publications/dictionaries/cancer-terms/expand/D>
6. <https://www.ema.europa.eu/en/human-regulatory-overview/research-and-development/data-medicines-iso-idmp-standards-overview>

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

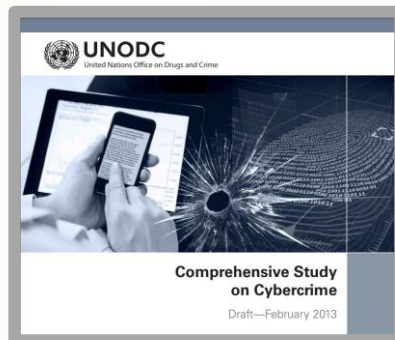
Προστασία κρίσιμων υποδομών



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://www.unodc.org/documents/Cybercrime/publications/un_cyber_policy_processes_links_add_the_links_to_the_web_page.pdf?v=3.6
4. <https://www.eurojust.europa.eu/sites/default/files/assets/files/united-nations-convention-against-cybercrime-sirius-factsheet.pdf>
5. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en

75 κράτη την έχουν υπογράψει
Στοιχεία της **27/04/2026**

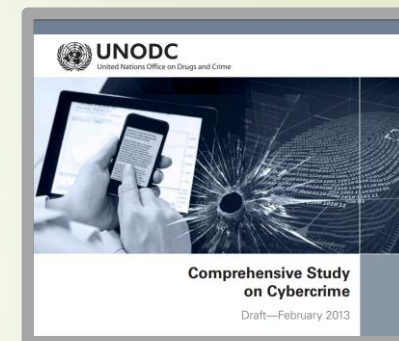
Σύμβαση για το **Κυβερνοέγκλημα** Το πρώτο διεθνές κείμενο Budapest 23/11/2001- CETS No 185



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>
7. https://ministryofjustice.gr/wp-content/uploads/2019/08/2aNomos_N.-4619_2019-%CE%A0.%CE%9A-1.pdf

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

Στοιχεία της 27/04/2026

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

Cybercrime(etymology)

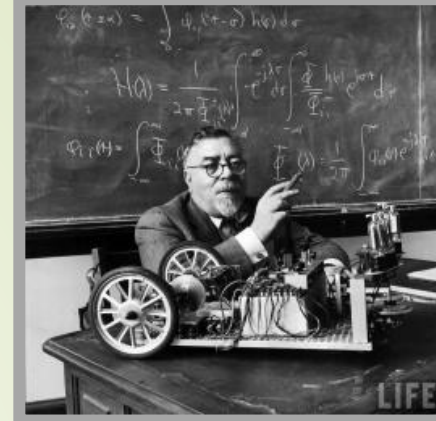
=Κάθε έγκλημα στον Κυβερνοχώρο

Κυβερνήτης
kybernetes
governor of a ship
(captain)



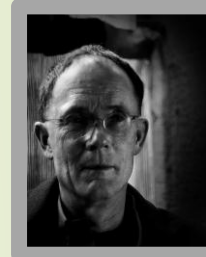
ΠΑΓΚΟΣΜΙΑ ΗΜΕΡΑ
ΕΛΛΗΝΙΚΗΣ ΓΛΩΣΣΑΣ
9 ΦΕΒΡΟΥΑΡΙΟΥ

Norbert Wiener 1894-1964
"Cybernetics", 1948



116 Συνέκδικος Ἱερατικός.
τοῦ διαβόλου. Κρίμα σημαίνει τὸ αὐτὸ καὶ Κρίσις (judgement,) οἷον "Τα κρίματά σου ὡσεὶ ἄβυσσος πολλή." 1) "Κρίματα, ψῆφοι, δικαί" κατὰ τὸν Ἡσύχιον. Σημαίνει ἀκίμη καὶ τὸ Κατάκριμα 2) ἤγουν τὴν Καταδίκην (condamnation) "Κρίμα, τὸ κατάκριμα καὶ ἡ καταδίκη, ὡς τὸ Κρίμα ἑαυτῶ 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,) ὀνομάζοντες οὕτως τὴν ἐγκληματικὴν τῶν πολιτικῶν νόμων παράβασιν, ὡς ἡμεῖς σήμερον ἰνομάζομεν (εἰς θρησκευτικὴν σημασίαν) Κρίμα (péché) τὴν παράβασιν τῶν ἐντολῶν τοῦ Θεοῦ, τὴν συνωνύμως λεγομένην

Crimen
Κρίμα

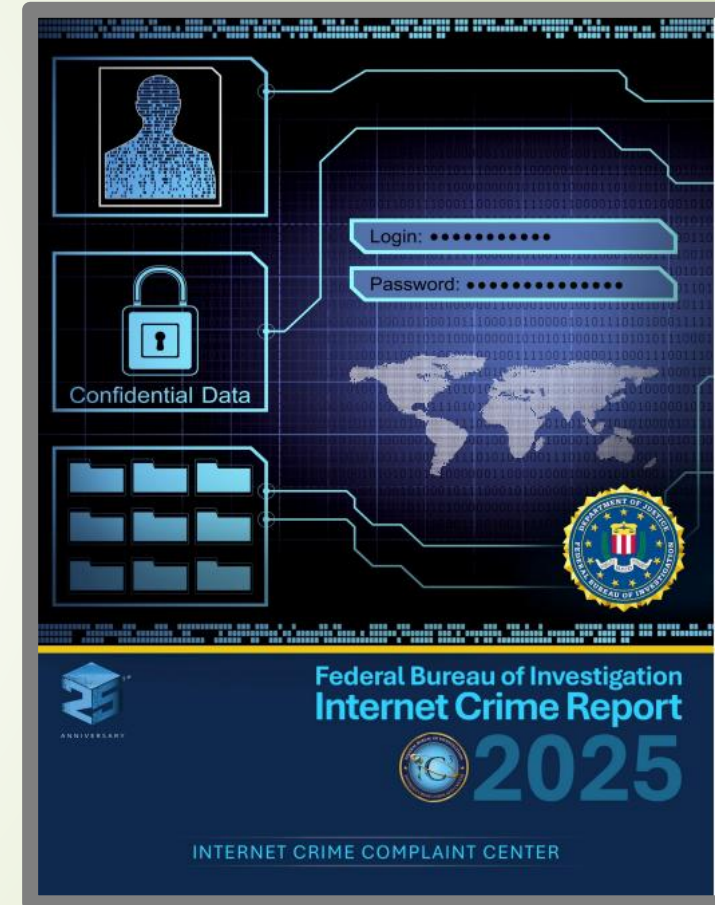


William Gibson 1948-
"Neuromancer"
Cyberspace", 1984

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_fQybbT9RZ0GizSwr7B4n0-MKU3g6rmnsiRkMHxc#imagePopur
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 – τα δεδομένα μας αποτελούν τον 1^ο στόχο



Δημοσιεύθηκαν 11/06/2025 & 06/4/2026

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/2025_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>

Πρόσφατα περιστατικά Κυβερνοεγκλημάτων

Profit - Κέρδος



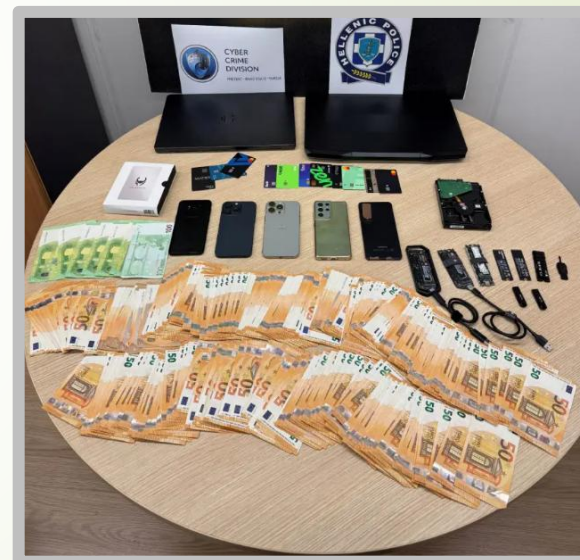
27
NOV
2025

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



19
NOV
2025

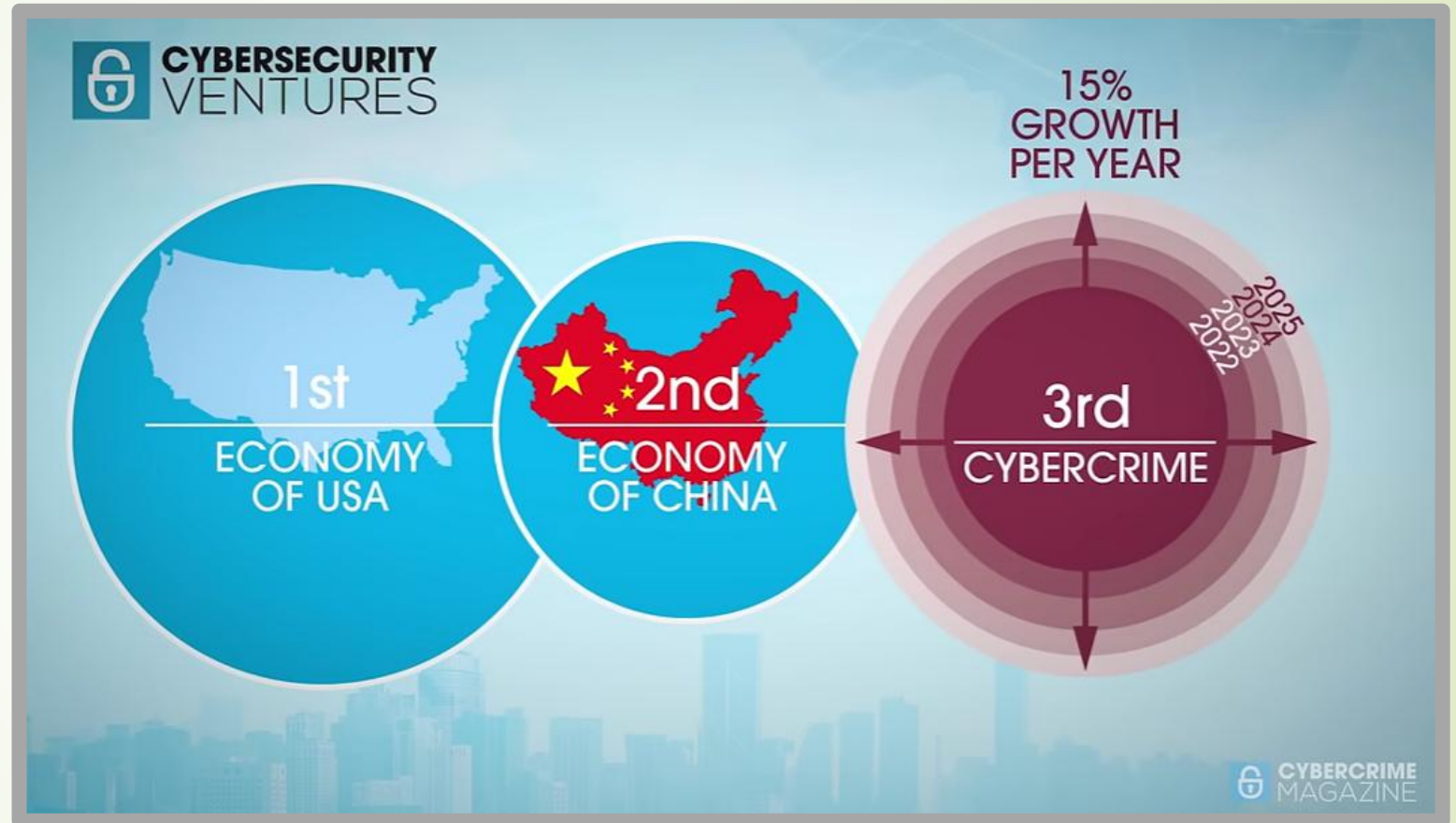
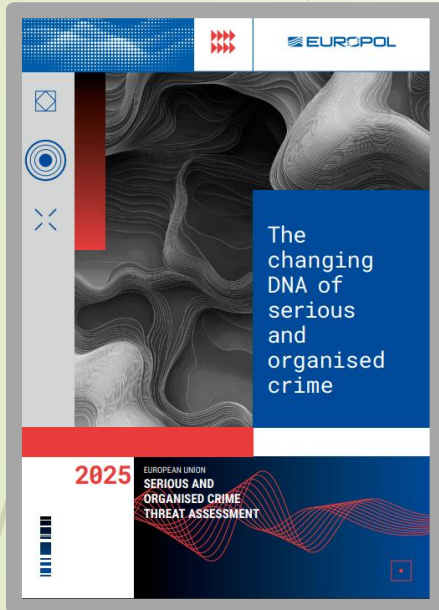
EUR 47 million in crypto traced to disrupt digital piracy services



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>
3. https://www.europol.europa.eu/cms/sites/default/files/documents/The_threat_of_pharmaceutical_crime_in_the_EU_and_beyond.pdf

Η 3^η σε μέγεθος Οικονομία παγκοσμίως



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	\$64.3M
Fishing	\$73	300.5k	\$62.1M
Ransomware attack	\$14,404	2.4k	\$34.4M
Denial of service attack	\$30,105	568	\$7.1M
Online harassment	\$757	14k	\$10.6M
Malware attack	\$12,239	762	\$9.3M

Πηγές

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

Η Ασφάλεια θέμα υψηλής προτεραιότητας

consentmanager

Digital
Service
Act



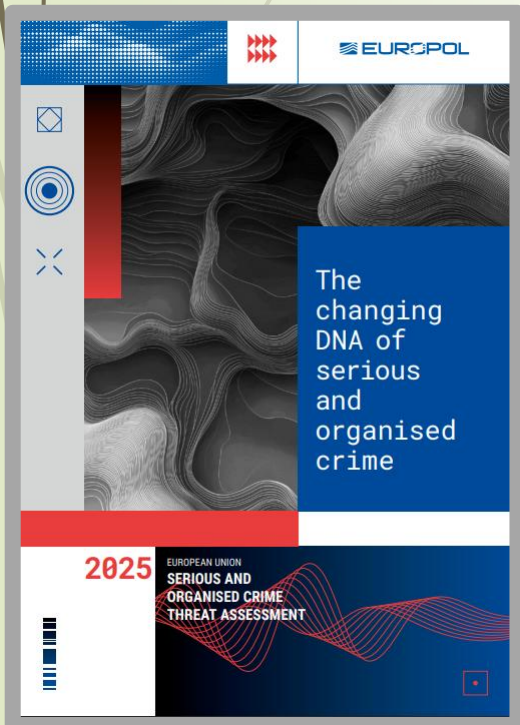
- Ένα ασφαλές για το μέλλον περιβάλλον
- Αντιμετώπιση εξελισσόμενων απειλών
- Προστασία από την τρομοκρατία και το οργανωμένο έγκλημα
- Ένα ισχυρό ευρωπαϊκό οικοσύστημα ασφάλειας

Πηγές:

- https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-of-life/european-security-union_en
- https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379
- <https://digital-strategy.ec.europa.eu/el/policies/europes-digital-decade>
- https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package?fbclid=IwAR2lWdrlQMiWv3aBNIJzkdDZVsxj12o6gn7ZK_2edWPUwVlIbhf9Gat_cltM_aem_Abz5czPFhGStxvQmG_U2oaUUIGQD7ogwR0M9948FzcRnZepyGCJv7Uutp6nsyoe1lgZqgPryCwtwRuLiozYdJW9
- <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)

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>

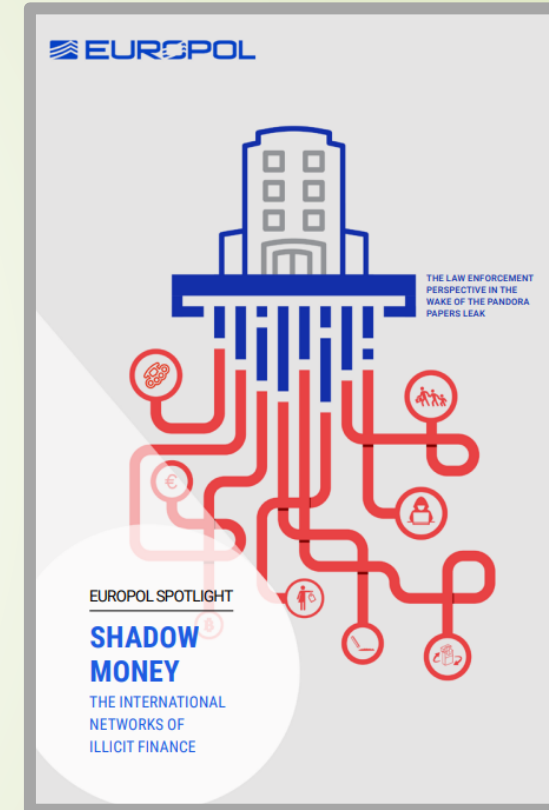
Οικονομικές απώλειες από το κυβερνοέγκλημα

□ 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)



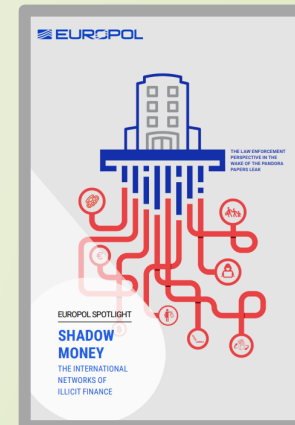
Πηγές

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

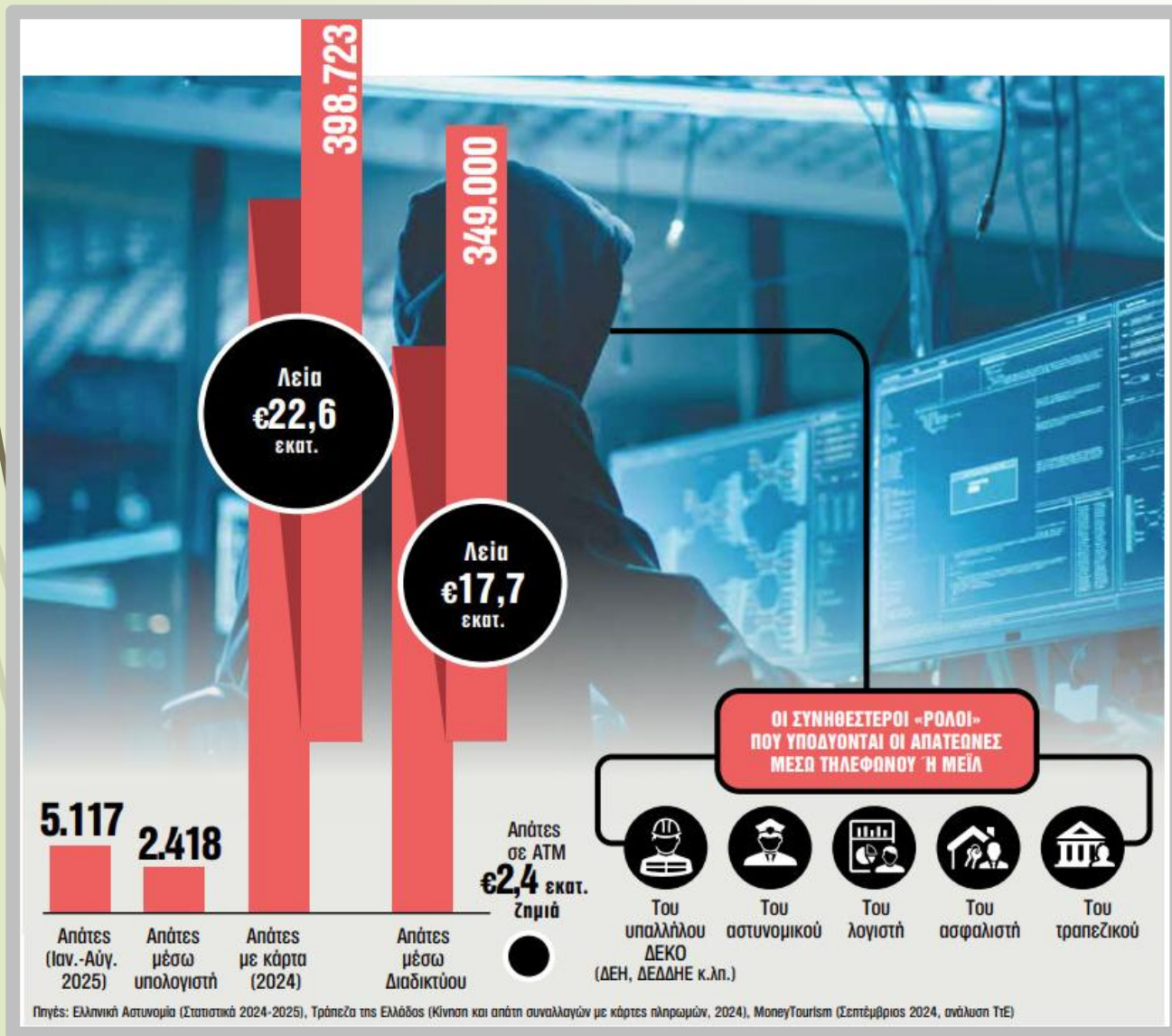
- ❑ Αναξιόπιστα Συστήματα Αναφοράς Κυβερνοεγκλημάτων
- ❑ Απουσία εναρμονισμένου νομικού πλαισίου
- ❑ Μη ολιστική χρήση των ΤΠΕ στο σύστημα απονομής δικαιοσύνης
- ❑ Ελλιπής ενημέρωση των ευάλωτων ατόμων
- ❑ Μειωμένο ενδιαφέρον των συναρμόδιων φορέων (πανεπιστήμια, ερευνητικά κέντρα, επιμελητήρια)



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>

Απάτες στην Ελλάδα



Πηγές

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

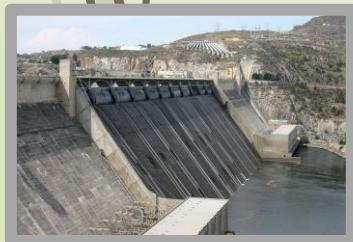













Πως παραβιάζονται τα δεδομένα

- Αλίευση** δεδομένων (παραπλανητικά μηνύματα)
- Κυβερνοεπιθέσεις**
- Κλοπή** δεδομένων
- Μη εξουσιοδοτημένη ή **κακόβουλη χρήση** προσωπικών δεδομένων από άτομα με πρόσβαση στα δεδομένα μας

Βασικές Υποδομές & Δίκτυα

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



Βασικές Οντότητες		
 Ενέργεια	 Υγεία	 Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων)
 Μεταφορές	 Πόσιμο νερό	 Οντότητες δημόσιας διοίκησης
 Τράπεζες	 Λύματα	 Διάστημα
 Υποδομές χρηματοπιστωτικών αγορών	 Ψηφιακές υποδομές	

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

Πηγές:

- <https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2>
- <https://eur-lex.europa.eu/eli/dir/2022/2555>
- <https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive#ecl-include-nis2-directive>
- <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>
- <https://cyber.gov.gr/odigia-nis2/>
- https://cyber.gov.gr/wp-content/uploads/2025/03/250323_%CE%9F%CE%B4%CE%B7%CE%B3%CF%8C%CF%82-%CE%91%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC%CF%82-%CE%9D.-5160_2024-1.pdf



Ransomware- Λυτρισμικό

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

NEW YORK AUCTION
9 OCTOBER

BROWSE & BID

EU cyber agency says airport software held to ransom by criminals

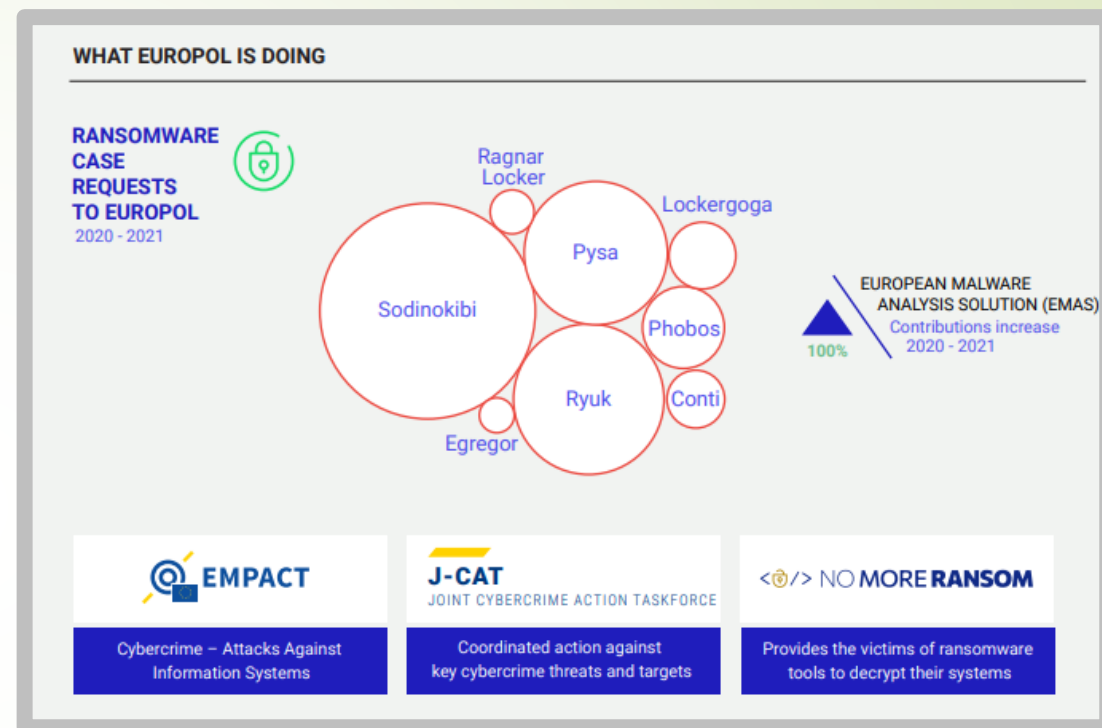
4 days ago

Share Save

Joe Tidy Cyber correspondent and Tabby Wilson



Disruption has continued at some of Europe's busiest airports as they try to recover from Friday's cyber attack.



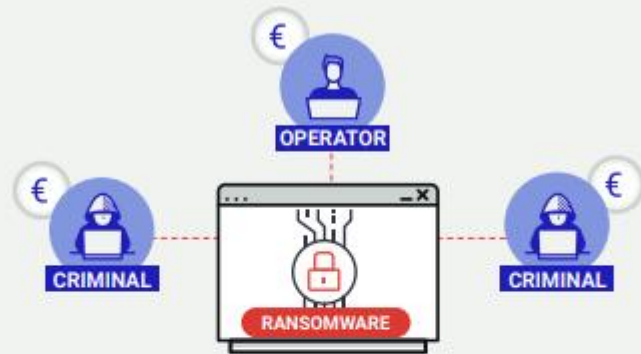
Προσοχή!!!
Δεν δίνουμε ποτέ λύτρα (χρήματα)!!!!

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/cqjeej854520>

Ransomware- Λυτρισμικό

The fight against ransomware



RANSOMWARE AFFILIATE PROGRAMS



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

Threatening DDoS attack against victim

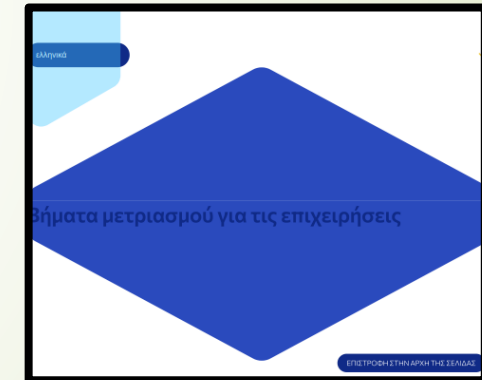
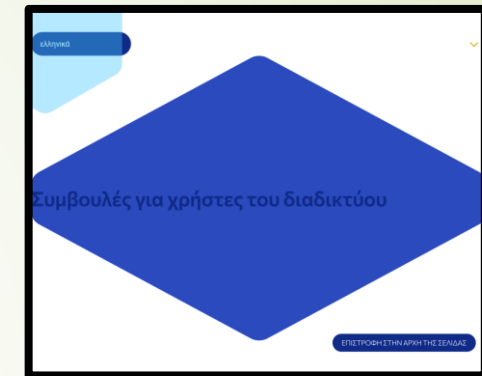
Exfiltrating data and threatening publication/action

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>

Νέα δωρεάν χρηστικά εργαλεία, προϊόντα της διεθνούς συνεργασίας



NO MORE RANSOM!

www.nomoreransom.org

Πηγές:

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

Κυβερνοεπιθέσεις - DDoS επιθέσεις

How can DDoS attacks paralyse the internet

1 The criminal hires a DDoS attack service on the internet

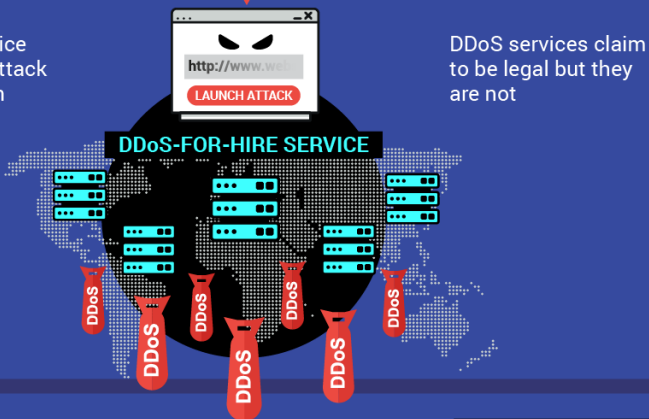


CRIMINAL



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>

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>
11. <https://cyber-news.gr/2026/01/28/%cf%84%ce%b1-%cf%80%cf%81%ce%bf%cf%83%cf%89%cf%80%ce%b9%ce%ba%ce%ac-%ce%b4%ce%b5%ce%b4%ce%bf%ce%bc%ce%ad%ce%bd%ce%b1-%cf%83%cf%84%ce%bf-%ce%bd%ce%ad%ce%bf-%cf%80%ce%b5%cf%81%ce%b9%ce%b2%ce%ac%ce%bb/>



Η αξία των δεδομένων

DIKI or DIKW model

Data -Information- Knowledge -Intelligence



Δεδομένα

Πληροφορίες

Γνώση

Νοημοσύνη

Επίλυση
προβλημάτων

Λήψη αποφάσεων

Πηγές:

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

Μέσα Κοινωνικής Δικτύωσης

NTV **Η ΝΑΥΤΕΜΠΟΡΙΚΗ**

Newsroom Οικονομία & Αγορές Ναυτιλία Επιχειρήσεις Πολιτική Κοινωνία Κόσμος Πολιτισμός Απόψεις Αθλητικά Green Υγεία Stories Clickatlife Tech & Science




Απόψεις

Παιδιά και Social Media: Θέμα απαγόρευσης ή ενσυνείδητη επιλογή

Σάββατο, 7 Φεβρουαρίου 2026 17:47

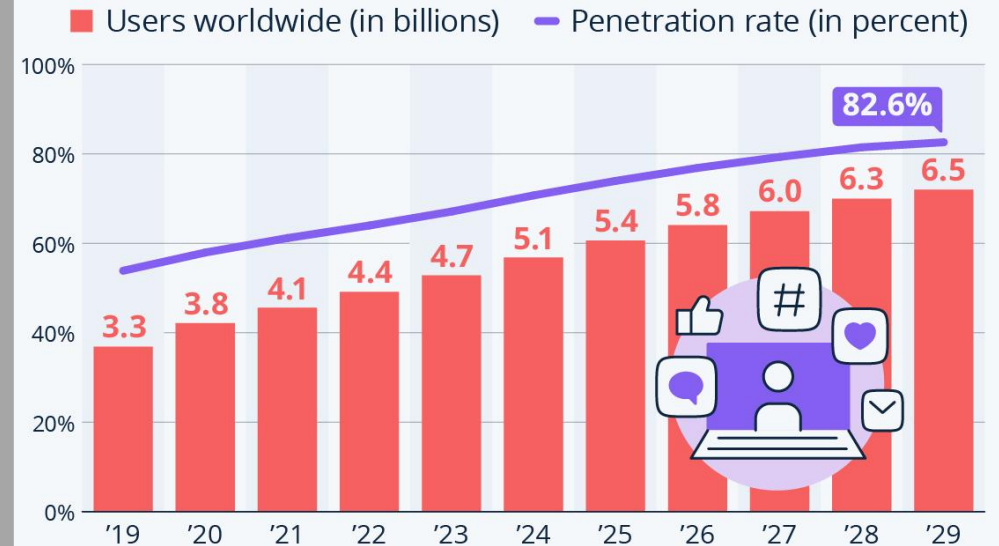
Ο επανακαθορισμός του μοντέλου ανθρωποκεντρικής χρήσης των τεχνολογιών έρχεται στο επίκεντρο της δημόσιας συζήτησης



SHARE:    

80% of the World's Population Will Use Social Media by 2028

Estimated number of social media users worldwide and global penetration rate



As of August 2025

Source: Statista Market Insights



statista

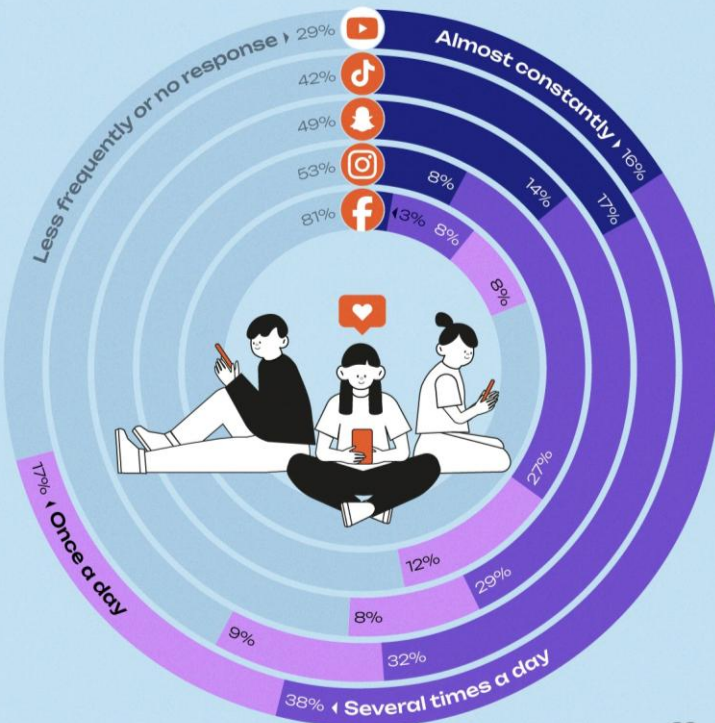
Πηγές:

- <https://www.dpa.gr/el/polites/prostasia>
- <https://www.facebook.com/photo/?fbid=1243308608006506&set=a.561580072846033>
- <https://www.naftemporiki.gr/opinion/2069725/paidia-kai-social-media-thema-apagoreysis-i-ensyneiditi-epilogi/>

Πλατφόρμες ΜΚΔ – Δεδομένα - Στοχευμένες διαφημίσεις

SOCIAL PLATFORM USAGE AMONG U.S. TEENS

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

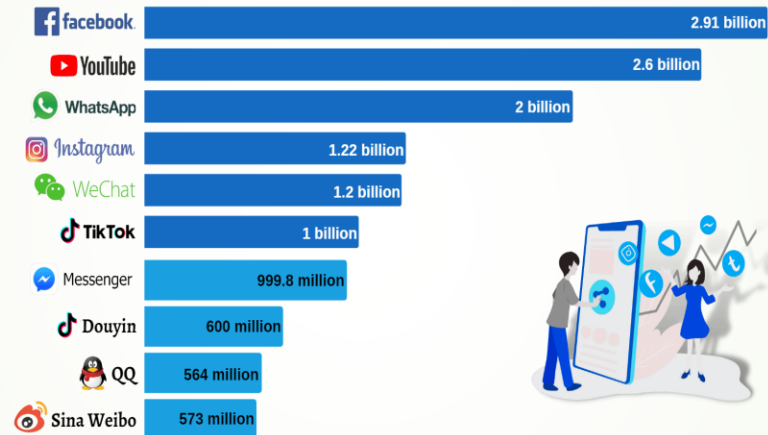


Source: Pew Research Center (2023)

voronoi Where Data Tells the Story

Download on the App Store GET IT ON Google Play

Most Popular Social Platforms

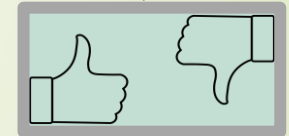


Number of monthly active users

Broadband Search



09/02/2009



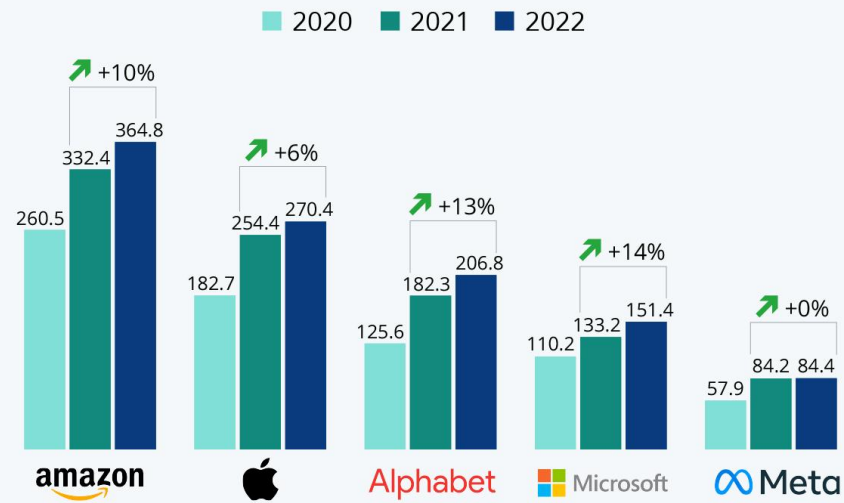
Πηγές:

- <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--joVG9yXiGNnVwqKkD44nVm3qUYc-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>

«Νέος χρυσός» -Νέα Οικονομία – Έσοδα σε Trillions

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.visualcapitalist.com/worlds-top-20-billionaires-in-2026/>
<https://pixabay.com/illustrations/fossil-energy-oil-embargo-7174425/>

Αλίευση Δεδομένων Phishing

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 μιιάζουν 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.



σας ζητούν να κατεβάσετε στη συσκευή σας ένα επισυναπτόμενο αρχείο ή να κάνετε κλικ σε έναν ηλεκτρονικό σύνδεσμο (link).

κάνουν χρήση ορολογίας που δίνει την αίσθηση του κατεπείγοντος.

Οι εγκληματίες στον κυβερνοχώρο

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.



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.

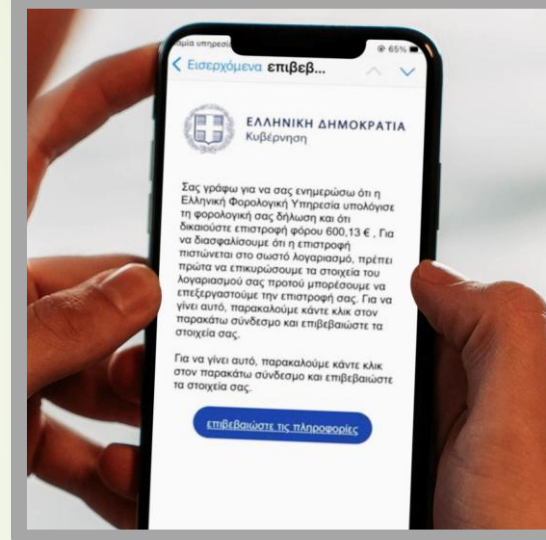
Το πακέτο σας θα αποθηκευτεί στο ΚΕΝΤΡΟ ΔΙΑΛΟΓΗΣ ΑΘΗΝΩΝ μέχρι να επιβεβαιώσετε τα στοιχεία σας:

Λεπτομέρειες

Με εκτίμηση,

ΕΛΤΑ.

Unsubscribe

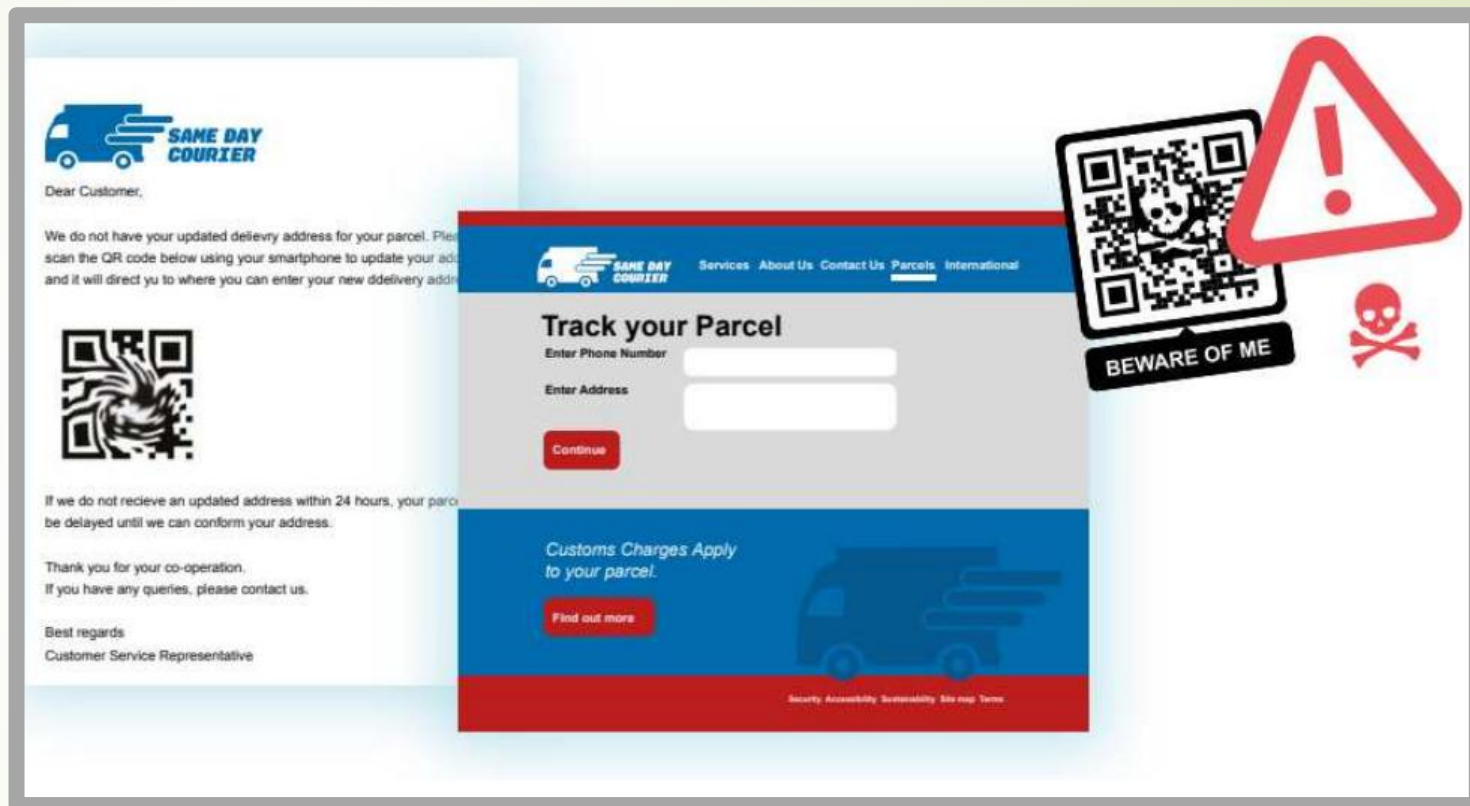


Πηγές:

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-epikairopoisi-tis-atzentas-kubernoasfaleias-na-axiopoithoun-oi-neoi-epistimonες/>
5. <https://www.facebook.com/hellenicpolice/posts/pfbid02btGBuuZe7nx7HTnSsWT8fNtZHfnpu4YAoqK74beG9Ys8rBwFFn7DgPfxkFogcHudl>

Αλίευση Δεδομένων -Quishing

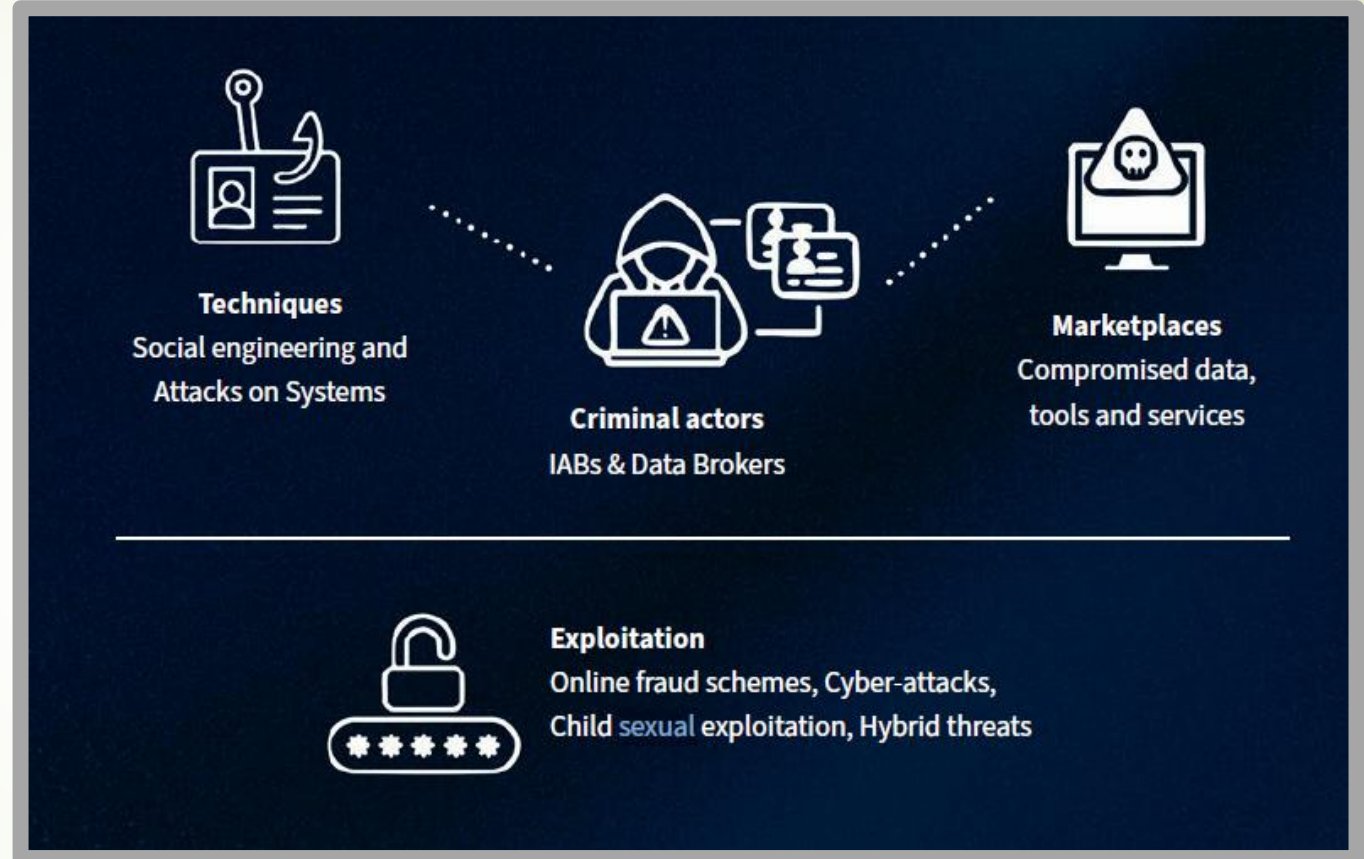
What is a QR Code?



Πηγές:

1. https://www.ncsc.gov.ie/pdfs/Quick_Guide_QR_Code_Phishing_Scams.pdf
2. <https://www.cyber.gov.au/threats/types-threats/quishing>
3. <https://www.ibm.com/think/insights/quishing-growing-threat-hiding-plain-sight>
4. https://www.trendmicro.com/en_us/what-is/phishing/quishing.html

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

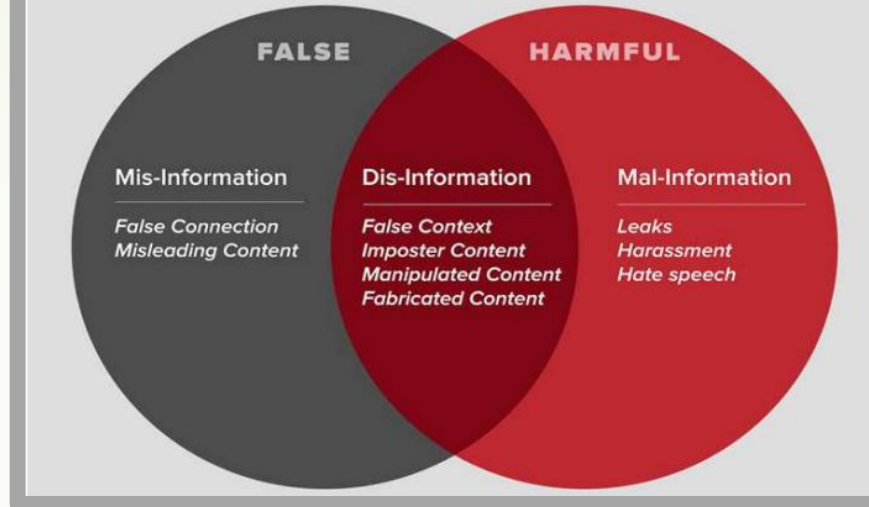
Απρεπής εκφορά του λόγου & Παραπληροφόρηση

Online hate speech doesn't just stay online



#NoToHate

INFORMATION DISORDER



Code of Practice on Disinformation

Transparency Centre



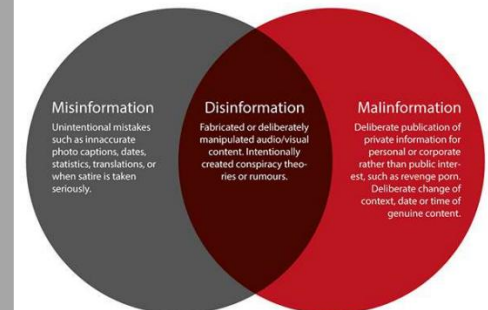
#DigitalEU

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=IwAR3L6vNUXxnQ7n5RGhecG9tUIMTYKGupGXm-XyhweVPsJ55rXptiPA0LbM>
8. <https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech>
9. <https://www.un.org/en/hate-speech>

TYPES OF INFORMATION DISORDER

FALSENESS INTENT TO HARM

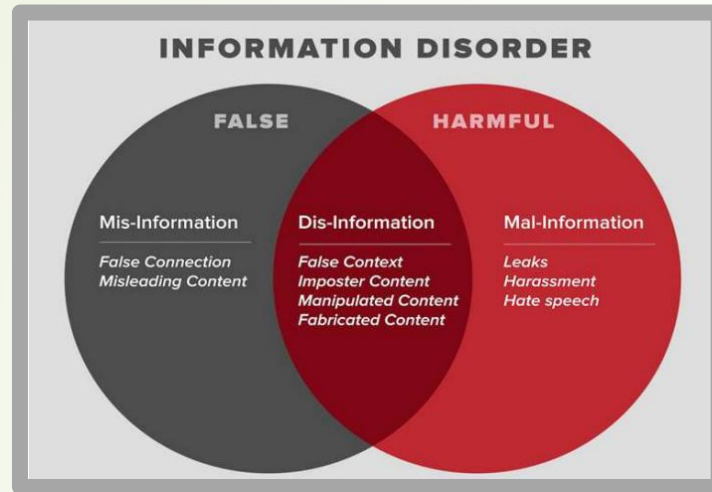


Fake news & πρακτικές αντιμετώπισης

Code of Practice on Disinformation

Transparency Centre

#DigitalEU



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?

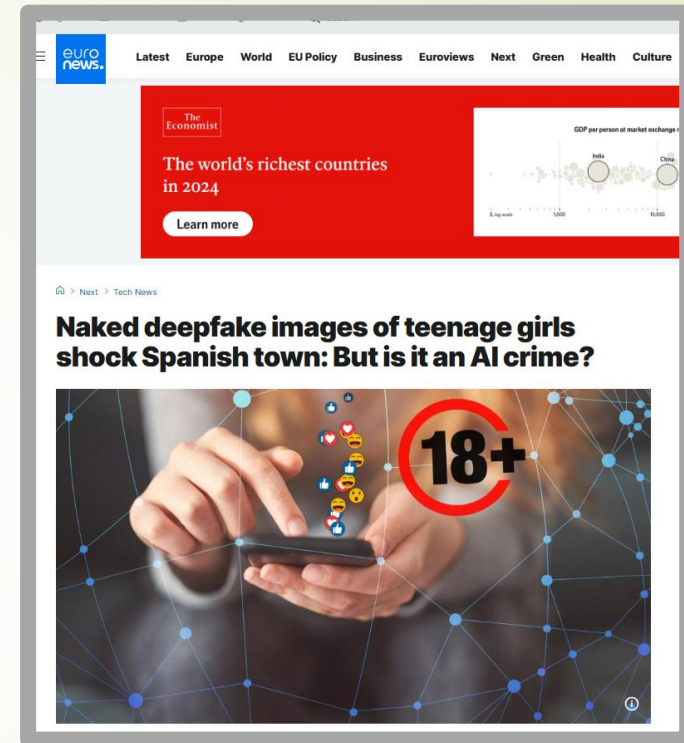


Πηγές

- <https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77> p. 5, 6, 17, 21
- https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210622_Hybrid_CoE_Paper_7_Geopolitics_and_strategies_in_cyberspace_WE_B.pdf
- https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf p. p1, 98
- <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>
- <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>
- <https://digital-strategy.ec.europa.eu/el/policies/europes-digital-decade>
- <https://itif.org/publications/2022/10/11/how-to-address-political-speech-on-social-media-in-the-united-states/?fbclid=IwAR3L6vNUXxnQ7n5RGhecgH9tulIMTYKGupGXm-XyhweVPsJ55rXptiPA0LbM>
- <https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech>
- <https://www.facebook.com/photo?fbid=1069070901915601&set=a.577863084369721>

TN και Deepfakes

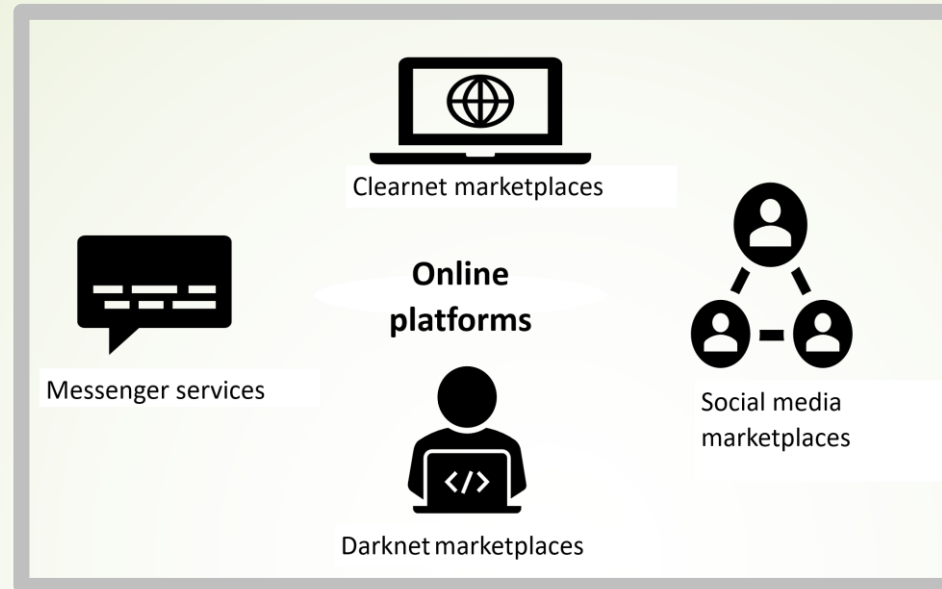
REAL
OR
AI?



Πηγές:

1. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-second-draft-code-practice-marking-and-labelling-ai-generated-content>
2. <https://www.euronews.com/next/2023/09/24/spanish-teens-received-deepfake-ai-nudes-of-themselves-but-is-it-a-crime>
3. <https://www.europol.europa.eu/media-press/europol-podcast/episode-21-how-crime-is-accelerated-by-ai>
4. <https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing>

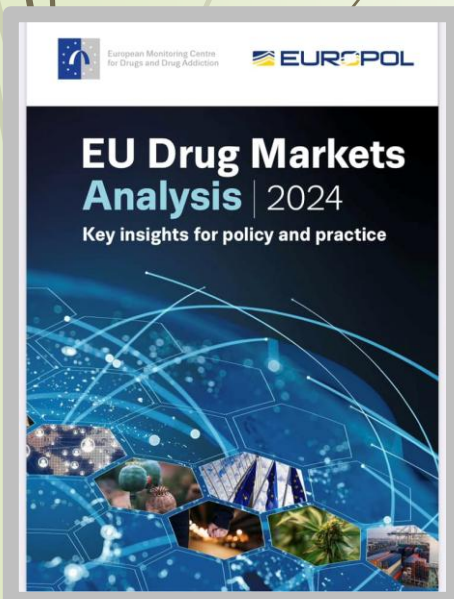
Μετατόπιση της παράνομης αγοράς στο ψηφιακό περιβάλλον



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://vuv.vuv.site/unodc-syntheticdrugstrategy-en/>
5. [https://www.euda.europa.eu/publications/european-drug-report/2025_en#pdf p.14-15](https://www.euda.europa.eu/publications/european-drug-report/2025_en#pdf_p.14-15)

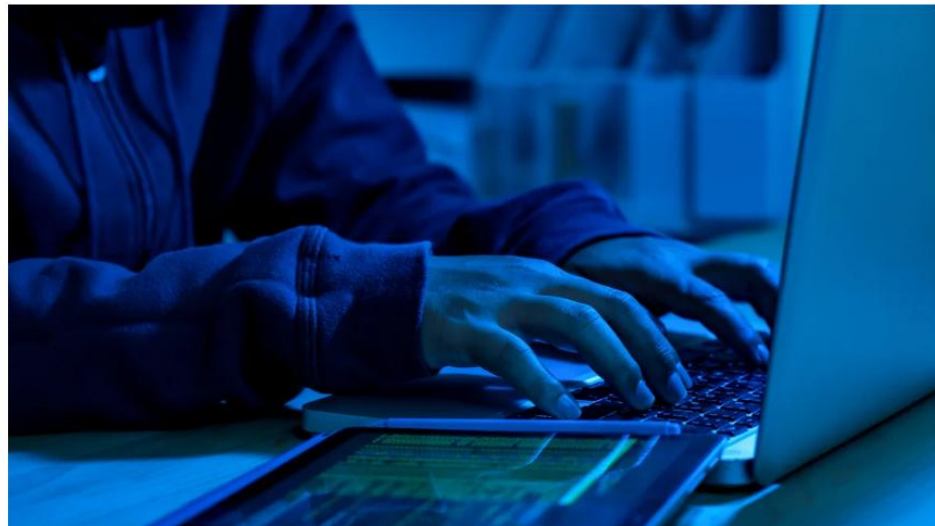
Επιγραμμικές απάτες – Online Frauds

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/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.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).



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



They have good knowledge about the organisation.



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



HOW DOES IT WORK?

They require an urgent payment.



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

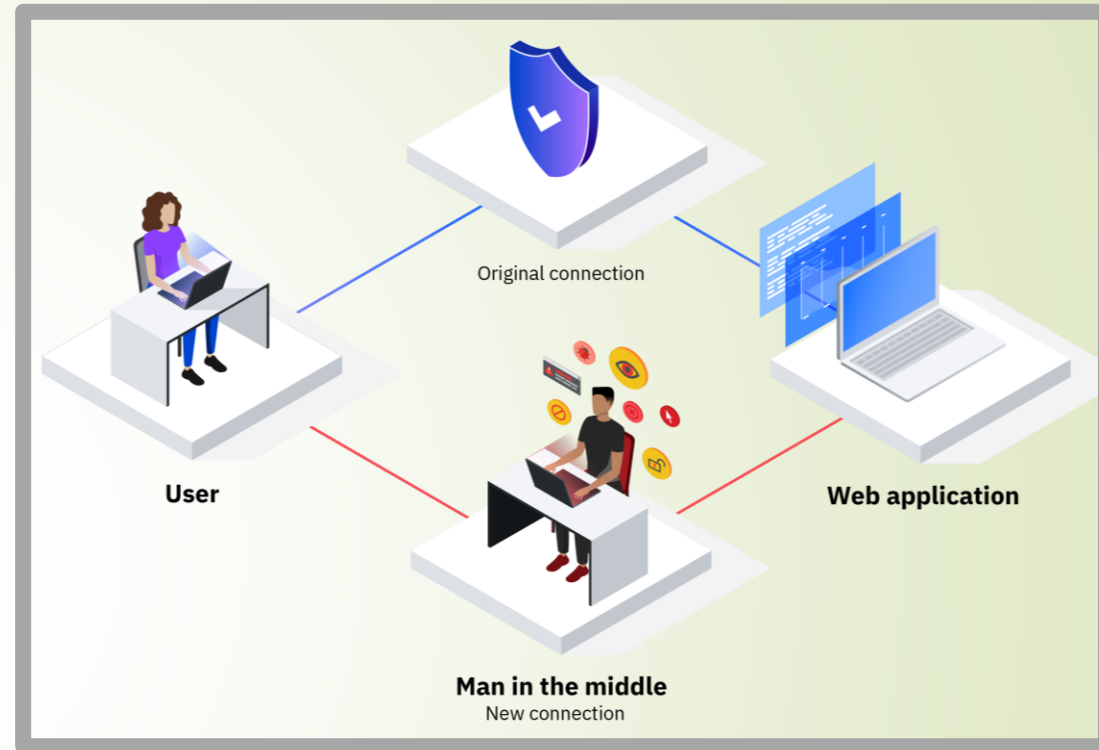


They refer to a sensitive situation (e.g tax control, merger, acquisition).

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



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/iocta_2019.pdf p.41
3. https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf p.96, 43
4. <https://www.youtube.com/watch?v=PehWRZ2816M>

Οδηγίες για Εταιρείες και Απασχολούμενους

WHAT CAN YOU DO?

AS A COMPANY

Be aware of the risks and ensure that **employees are informed and aware too**.

Encourage your staff to **approach payment requests with caution**.

Implement internal protocols concerning payments.

Implement a procedure to verify the legitimacy of payment requests received by email.

Establish **reporting routines** for managing fraud.

Review information posted on your company website, **restrict information and show caution** with regard to social media.

Upgrade and update technical security.



Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

AS AN EMPLOYEE

Strictly apply the security procedures in place for payments and procurement. **Do not skip any steps and do not give in to pressure**.

Always **carefully check email addresses** when dealing with sensitive information/money transfers.

In case of doubt on a transfer order, **consult a competent colleague**.

Never open suspicious links or attachments received by email. Be particularly careful when checking your private email on the company's computers.

Restrict information and show caution with regard to social media.

Avoid sharing information on the company's hierarchy, security or procedures.



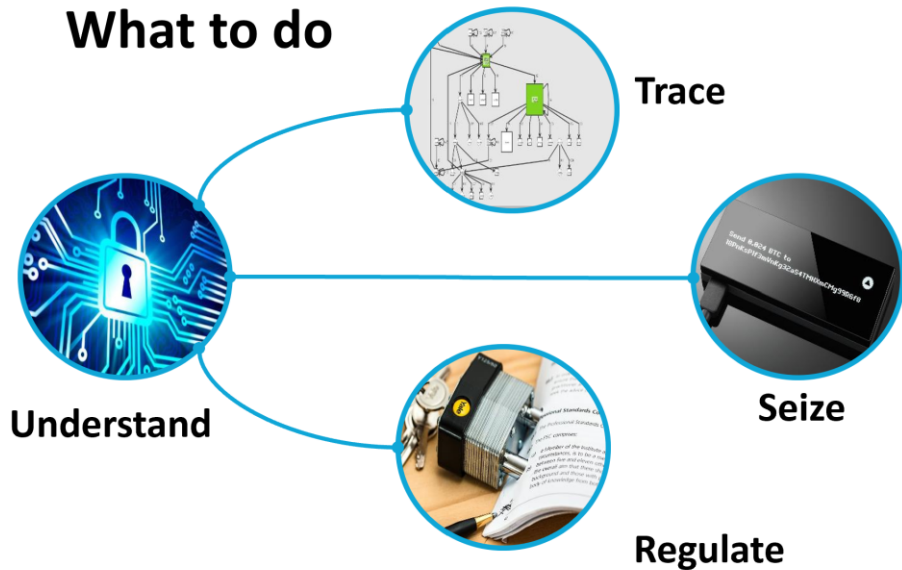
If you receive a suspicious email or call, always inform your IT department.

Πηγές:

1. https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf p.41
2. <https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec>
3. <https://www.ncsc.gov.uk/files/Business-email-compromise-defending-your-organisation-infographic.pdf>
4. <https://www.ncsc.gov.uk/files/Active-Cyber-Defence-2-ASM-experiment.pdf>
5. <https://www.ncsc.gov.uk/guidance/business-email-compromise-defending-your-organisation>
6. <https://www.youtube.com/watch?v=PehWRZ2816M>

Κρυπτοχρήμα & Έγκλημα

What to do



cryptorank Coins Fundraising IDO/ICO Exchanges Token Unlocks Products

Main > Currencies

All Cryptocurrencies

Overview All Coins Performance ATH Gainers Losers IDO/ICO ROI All Categories Ecosystems

Filter coins... LAYOUT FILTERS PRESETS Download Data USD

#	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=HlfGsQ_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



ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ
ΕΥΡΩΣΥΣΤΗΜΑ

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).



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 ΟΤΡ, ειδοποιήσεις για σύνδεση νέων συσκευών, ψηφιακών πορτοφολιών, υπηρεσιών πληρωμών και επιβεβαιώω 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

N. 5019/2023

ΦΕΚ Α

Ενσωματώθηκε στο εσωτερικό δίκαιο
Αποζημίωση
θυμάτων
κυβερνοαπάτης υπό προϋποθέσεις

Πηγές:

- <https://www.bankofgreece.gr/trapeza/koinwnikh-eythynh/xrhmatooikonomikh-ekpaideysh/prostasia-apo-hlektronikes-apates?mode=preview>
- https://museum.bankofgreece.gr/personalfinance/?fbclid=IwY2xjawlr0hFleHRuA2FibQlxMAABHSFZ0ZDekJpQNV1cljHeK8vp6RgpOUhxhbSLssHzWOF8qVL0ZpM8Z2Ax-Q_aem_LUDM7nsjferXu2jXRt366A#/lessons/in_swfHmFJVomcam6z8GDKZikD_f1Qq-

Παραλλαγές διαδικτυακών απατών

ΕΥΡΩΠΑΪΚΗ ΑΣΤΥΝΟΜΙΚΗ ΓΡΑΦΕΙΟ (ΕΥΡΩΠΟΛ)

Είμαι η κα. Catherine Debole, Γενική Διευθύντρια της Ευρωπαϊκής Αστυνομικής Υπηρεσίας (EUROPOL). Σε συνεργασία με την Εθνική Αστυνομία, επικοινωνώ μαζί σας λίγο μετά από μια κατάχρηση μέσω κυβερνοδιαπίδυσης (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 ΙΣΤΟΣΕΛΙΔΑ
- ΠΑΙΔΟΠΟΡΝΟΓΡΑΦΙΑ
- ΕΠΙΔΕΙΞΙΜΟΝΙΑ

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 ιστοτόπους διαφήμισης και άμεσων μηνυμάτων παρουσία ανηλικών (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 είδησεογραφικά κανάλια) για ευρεία διάσημη, 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.

#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=IwY2xjawKIUB1leHRuA2FibQIxBicmlkETBaVzImbWJCejdQXJ5UkQwAR7IJBmyoK0G5_AkG0_6HJ9_su5KQWOfYihaNhCQalwZlyHwzb0Z8tg0x_FuuQ_aem_rzsBtRSvS3RMd_mOyD9uwA

Απάτες Τεχνικής Υποστήριξης – Tech Support Scams

How to recognise tech support scams

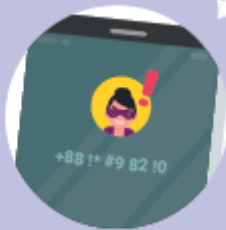


Hi, I'm Tech#-nical S|support



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.



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.



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

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

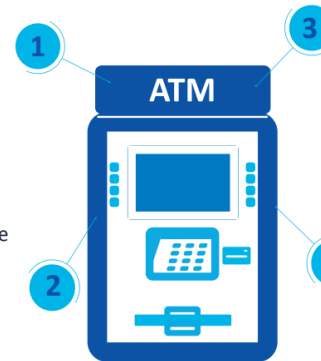
When replacement cards arrive, cut expired/unused/blocked cards into several pieces, including through the magnetic strip and/or chip

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.
- ΣΧΕΦΟΥ ΔΥΟ ΦΟΡΕΣ ΠΡΙΝ ΠΛΗΡΩΣΕΙΣ**
Βεβαιώσου ότι κατανοείς τους κινδύνους των διαδικτυακών αγορών.
- 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 πρότερης παραλαβής των προϊόντων.
- ΕΛΕΓΞΕ ΚΡΙΤΙΚΕΣ ΚΑΙ ΑΞΙΟΛΟΓΗΣΕΙΣ**
Ειδικά αγνώστων καταστημάτων και μεμονωμένων πωλητών.
- ΧΡΗΣΙΜΟΠΟΙΗΣΕ ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ ΟΤΑΝ ΑΓΟΡΑΣΕΙΣ ΔΙΑΔΙΚΤΥΑΚΑ**
Οι περισσότερες πιστωτικές κάρτες έχουν ισχυρή πολιτική προστασίας πελατών. Εάν δεν λάβεις αυτό που παρήγγειλες, ο εκδότης της κάρτας ενδέχεται να σε αποζημιώσει.
- 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 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.
- 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.
- ΔΕΝ ΘΑ ΑΓΟΡΑΣΕΙΣ; ΜΗΝ ΑΦΗΣΕΙΣ ΤΗΝ ΚΑΡΤΑ ΣΟΥ ΠΙΣΩ**
Εάν δεν αγοράσεις κάτι, μην υποβάλεις ή σώσεις τα στοιχεία της κάρτας σου.
- 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).

EUROPOL EC3 European Cybercrime Centre MRC CYBER CRIME DIVISION

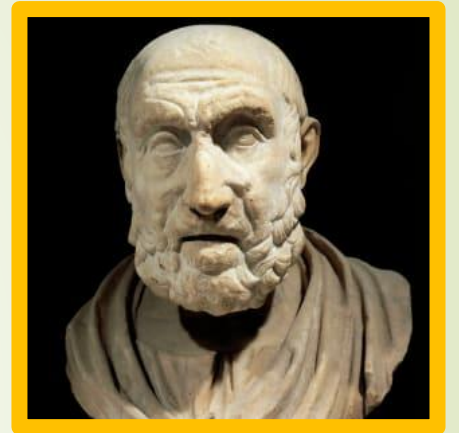
#BuySafePaySafe

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>

Η Στρατηγική της Πρόληψης

Πατέρας της ιατρικής
επιστήμης



Μη
αποτίμηση

Συγκριτικό
πλεονέκτημα



«Κάλλιον το προλαμβάνειν ή το θεραπεύειν»

Δεξιότητες στον 21^ο αιώνα – Δεξιότητες Διαχείρισης Δεδομένων

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

21st-Century Skills

Foundational Literacies
How students apply core skills to everyday tasks

1. Literacy
2. Numeracy
3. Scientific literacy
4. ICT literacy
5. Financial literacy
6. Cultural and civic literacy

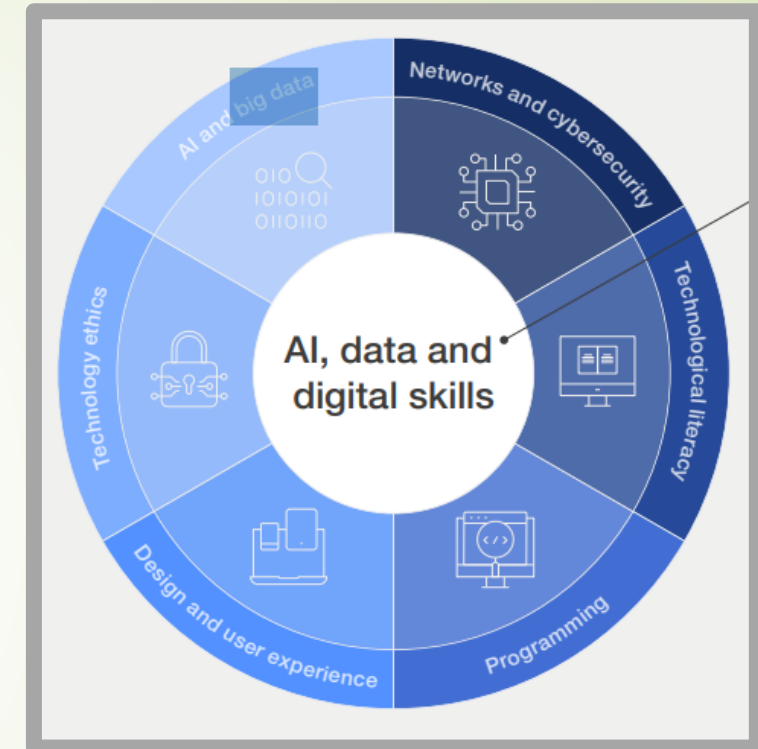
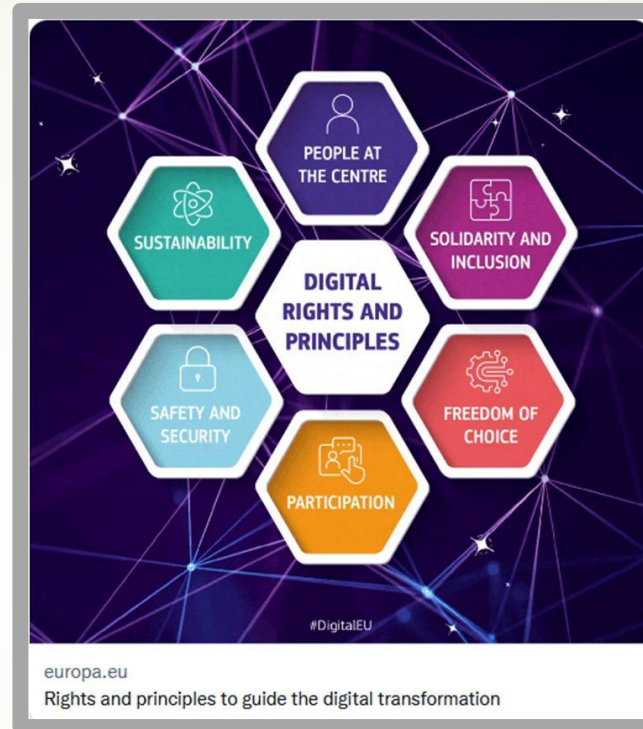
Competencies
How students approach complex challenges

7. Critical thinking/problem-solving
8. Creativity
9. Communication
10. Collaboration

Character Qualities
How students approach their changing environment

11. Curiosity
12. Initiative
13. Persistence/grit
14. Adaptability
15. Leadership
16. Social and cultural awareness

Lifelong Learning



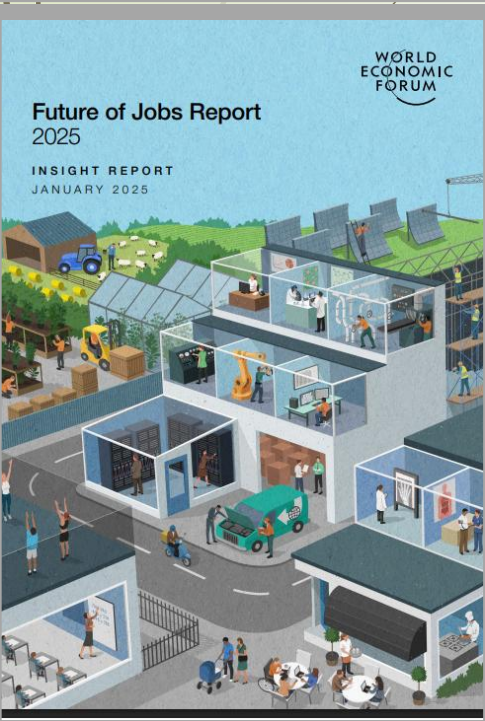
Πηγές:

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://reports.weforum.org/docs/WEF_New_Economy_Skills_2025.pdf p.7
5. https://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf
6. <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives>
7. <https://www.weforum.org/agenda/2016/03/21st-century-skills-future-jobs-students/>
8. https://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf
9. <https://digital-strategy.ec.europa.eu/el/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)
10. <https://www.unesco.org/en/digital-competencies-skills/ict-cft>



Δεξιότητες του Μέλλοντος

- Αναλυτική σκέψη
- Ψηφιακές δεξιότητες
- Δημιουργικότητα
- Προσαρμοστικότητα
- Δια βίου μάθηση



FUTURE JOBS

Robots, Artificial Intelligence, and Digital Platforms in East Asia and Pacific

Omar Arias, Daisuke Fukuzawa, Duong Trung Le, and Aaditya Mattoo



Πηγές:

1. https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf
2. <https://openknowledge.worldbank.org/server/api/core/bitstreams/e98ac135-15f6-47e4-b1d9-07a6415b6e76/content>
3. https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/oecd-skills-outlook-2025_ac37c7d4/26163cd3-en.pdf
4. <https://digital-skills-jobs.europa.eu/en>
5. https://www.cedefop.europa.eu/files/3098_en.pdf

Επαγγέλματα σχετικά με την ΤΝ και την προστασία των δεδομένων



**INFORMATION
SYSTEMS
SECURITY
MANAGER**

JOB PROFILE:

**CYBER
SECURITY
ENGINEER**

JOB PROFILE:

**CRYPTOGRAPHER/
CRYPTANALYST
AKA
ENCRYPTION
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**

Σύγχρονο εκπαιδευτικό υλικό – συνεργασία σχολείων

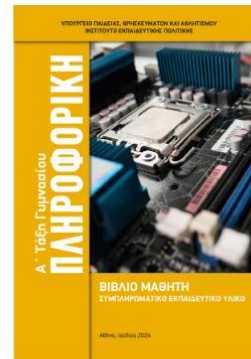


Τα σχολεία των ακριτικών κι όχι μόνο περιοχών μας πήραν άριστα (20)!!!

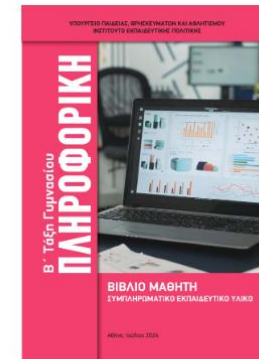


Πηγές:

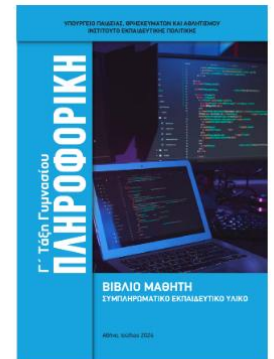
1. <https://nationaldigitalacademy.gov.gr/>
2. <https://iep.edu.gr/el/gymnasio/plifororiki>
3. <https://cyber-news.gr/2026/02/13/%cf%84%ce%b1-%cf%83%cf%87%ce%bf%ce%bb%ce%b5%ce%af%ce%b1-%cf%84%cf%89%ce%bd-%ce%b1%ce%ba%cf%81%ce%b9%cf%84%ce%b9%ce%ba%cf%8e%ce%bd-%ce%ba%ce%b9-%cf%8c%cf%87%ce%b9-%ce%bc%cf%8c%ce%bd%ce%bf-%cf%80%ce%b5/>



Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Α' Γυμνασίου

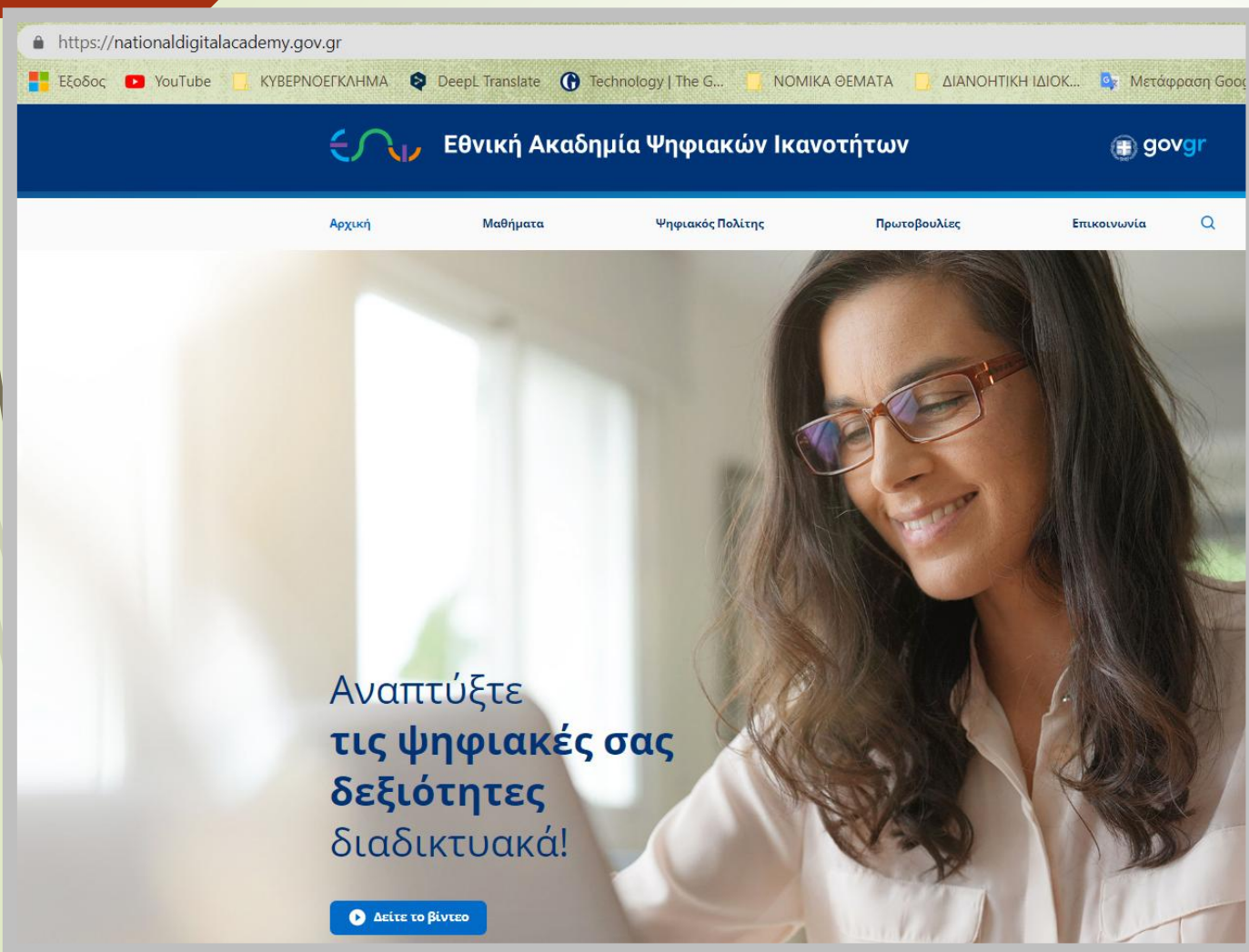


Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Β' Γυμνασίου



Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Γ' Γυμνασίου

Εθνική Ακαδημία Ψηφιακών Ικανοτήτων- ΕΑΨΙ



https://nationaldigitalacademy.gov.gr

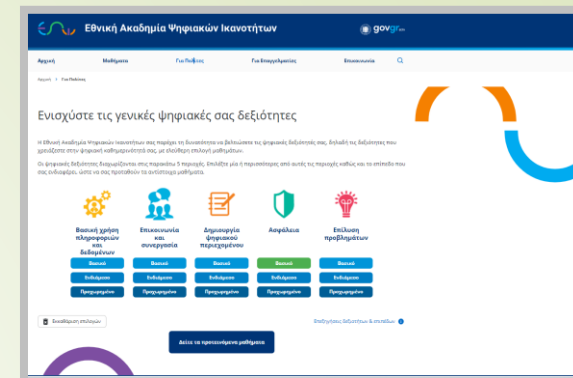
Εθνική Ακαδημία Ψηφιακών Ικανοτήτων govgr

Αρχική Μαθήματα Ψηφιακός Πολίτης Πρωτοβουλίες Επικοινωνία

Αναπτύξτε τις ψηφιακές σας δεξιότητες διαδικτυακά!

Δείτε το βίντεο

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



Εθνική Ακαδημία Ψηφιακών Ικανοτήτων govgr

Εισαχίστε τις γενικές ψηφιακές σας δεξιότητες

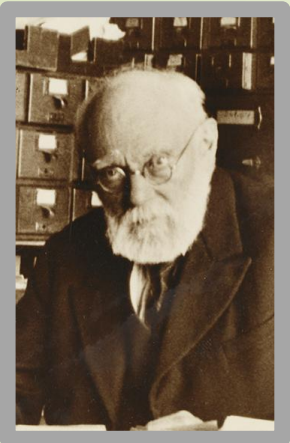
Βασική χρήση ηλεκτρονικών συσκευών
Επικοινωνία και συνεργασία
Ασφάλεια
Εκπαίδευση προγράμματα

Ποια είναι η συνεισφορά των πανεπιστημίων και των ερευνητικών μας κέντρων στην πλατφόρμα;

Με 311 μαθήματα
35 θεματικές ενότητες
1800 ώρες εκπαίδευσης

Στοιχεία στις 27/04/2026

Πληροφορίες & πηγές



Paul Otlet
1868-1944

- ❑ **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)

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>

Κρίσιμο στοιχείο η
αξιοπιστία



Ανεξάρτητες Αρχές & Φορείς



Συνήγορος του Παιδιού



- 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)

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

ΑΠΔΠΧ και ΜμΕ



The screenshot shows the website interface for 'byDesign', a digital compliance tool for SMEs with the GDPR. The header includes the ADPD logo and navigation links: 'Η ΑΡΧΗ', 'ΠΟΛΙΤΕΣ', 'ΦΟΡΕΙΣ', 'ΕΝΗΜΕΡΩΣΗ', 'ΠΡΑΞΕΙΣ ΤΗΣ ΑΡΧΗΣ', 'ΝΟΜΟΘΕΣΙΑ', and 'ΣΥΝΔΕΣΗ'. A search bar is located in the top right corner. The main content area features the title 'byDesign – Ψηφιακός Βοηθός Συμμόρφωσης ΜμΕ με τον GDPR' and the 'byDesign' logo, which consists of a stylized blue butterfly with white eyes and the text 'byDesign' below it.

Πηγή:
https://www.dpa.gr/el/byDesign_toolkit

Ψηφιακός Βοηθός

Διευκόλυνση της συμμόρφωσης μικρομεσαίων επιχειρήσεων με τον GDPR και προώθηση της προστασίας δεδομένων από τον σχεδιασμό σε προϊόντα και υπηρεσίες ΤΠΕ

Επιμελητήριο Πέλλας

pellachamber.gr/kivernoasfalia/

Archive... Βρείτε τη δημόσια... YouTube Μετάφραση Google Live24.gr: Greek Ra... The World Clock... eSafety

ΕΛ

Κυβερνοασφάλεια

Υπηρεσίες Διοικητικής Εξυπηρέτησης

e-επιμελητήριο

Γ.Ε.ΜΗ

Υ.Μ.Σ

Υπηρεσίες Ανάπτυξης & Εξωστρέφειας

Επιχειρηματικός Οδηγός

Ανάρτηση με συναίνεση

Το παρόν βίντεο αναρτάται με την έγκριση και τη συναίνεση του Γεωργίου Παπαπροδρόμου Αντιστράτηγου ε.α. (ΕΛΑΣ) Πτυχιούχου Νομικής ΑΠΘ - Δικαστικό Γραφολόγο, Πρώην Διευθυντή Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος τον οποίο ευχαριστούμε θερμά για την ευγενική του προσφορά. Στόχος είναι η ενημέρωση και υποστήριξη των επιχειρήσεων του νομού Πέλλας σε θέματα κυβερνοασφάλειας. Η συμβολή του είναι ιδιαίτερα σημαντική για την ενίσχυση της ψηφιακής ασφάλειας στον τοπικό επιχειρηματικό κόσμο.

Δείτε το βίντεο εδώ

Ο οδηγός του ΕΣΠΑ για την προστασία των δεδομένων για μικρές επιχειρήσεις

Για αναλυτική καθοδήγηση σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα στις μικρές επιχειρήσεις, μπορείτε να επισκεφθείτε τον οδηγό του

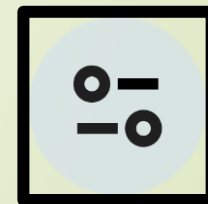
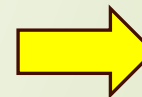
Ειδικό αφιέρωμα στην Κυβερνοασφάλεια

pellachamber.gr/kivernoasfalia/

← Ασφάλεια pellachamber.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](#)

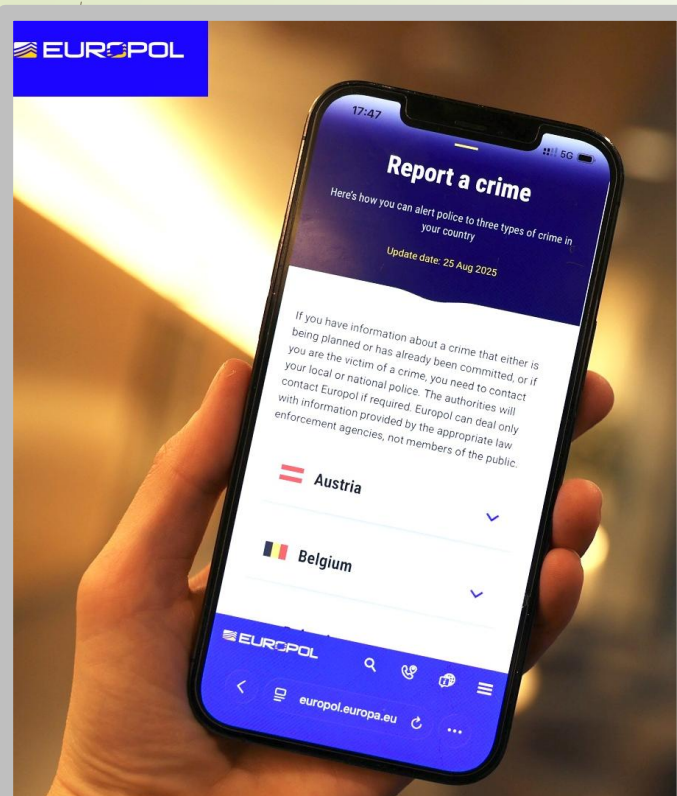
✓ Το πιστοποιητικό είναι έγκυρο



Πηγές:

- <https://www.pellachamber.gr/kivernoasfalia/>
- <https://cyber-news.gr/2026/02/20/%cf%83%ce%b5%ce%bb%ce%af%ce%b4%ce%b5%cf%82-%cf%86%ce%bf%cf%81%ce%ad%cf%89%ce%bd-%ce%ba%ce%b1%ce%b9-%cf%83%cf%87%ce%bf%ce%bb%ce%b5%ce%af%cf%89%ce%bd-%ce%bc%ce%b5-%ce%b1%cf%86%ce%b9%ce%ad%cf%81%cf%89/>

Αναφορά Κυβερνοεγκλημάτων- υπάρχει πλατφόρμα –άμεσα, εύκολα και δωρεάν



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-kivernoperistatikon-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-dieftynsi-dioxis-ilektroniku-egklimatos-einai-apo-tis-ypiresies-aichmis-gia-tin-astynomia-tis-neas-epochis/>
5. <https://www.europol.europa.eu/report-a-crime>

Υπηρεσίες Αντιμετώπισης Κυβερνοεγκλήματος & ΤΝ



Κεντρικές και Περιφερειακές υπηρεσίες ΕΛΑΣ Ασφάλειας και Μικτά Αστυνομικά Τμήματα
-
ΛΟΙΠΕΣ ΑΡΧΕΣ ΠΟΥ ΑΣΚΟΥΝ ΕΙΔΙΚΑ ΠΡΟΑΝΑΚΡΙΤΙΚΑ ΚΑΘΗΚΟΝΤΑ

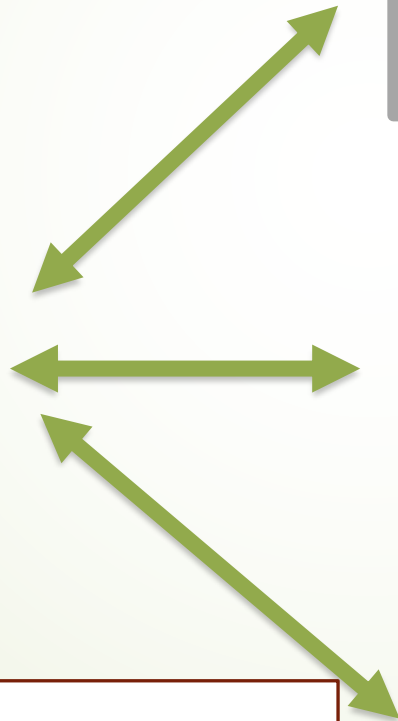
Διεύθυνση Εγκληματολογικών Ερευνών

Διεύθυνση Διεθνούς Αστυνομικής Συνεργασίας

Διεύθυνση Διαχείρισης Πληροφοριών

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

Συνεργασία για περισσότερη Ασφάλεια στον Κυβερνοχώρο



Ακαδημαϊκή Κοινότητα

NO MORE RANSOM!

www.nomoreransom.org



Δημόσιος Τομέας

Ιδιωτικός Τομέας

Επικαιροποίηση **Θεσμικού Πλαισίου** Medicrime Convention (η Σύμβαση για τα φάρμακα που διακινούνται παράνομα στο διαδίκτυο)

Την υπέγραψε η χώρα μας 18/5/2022

Εκκρεμεί η επικύρωση από την
Ελληνική Βουλή
27/04/2026



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/diakinisi-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=IwY2xjawKr4ttleHRuA2FibQIxMABicmlkETB4T1hObDNnNkh4TWZ6SE4wAR7zYLMoQFAYNOXbq7VUbcBMpk0WkCVhgsWCzkrb32_SQWV-jKJpRxtPZjs_4w_aem_00bjjEqYTRQrYa7NFznhNg
5. https://www.opengov.gr/yyka/?c=17616&fbclid=IwY2xjawRakutleHRuA2FibQIxMABicmlkETB2aEIscljJNeEMwWnVyZG1xc3J0YwZhcHBfaWQQMjlyMDM5MTc4ODIwMDg5MgABHmUu0zwYXnw0O4dhTi83hFCr3cm6IVaVVPtTx7D8LxYjzyR00t9xoVV_0Lqr_aem_488086woRUKi9LXibRJSJLg

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)

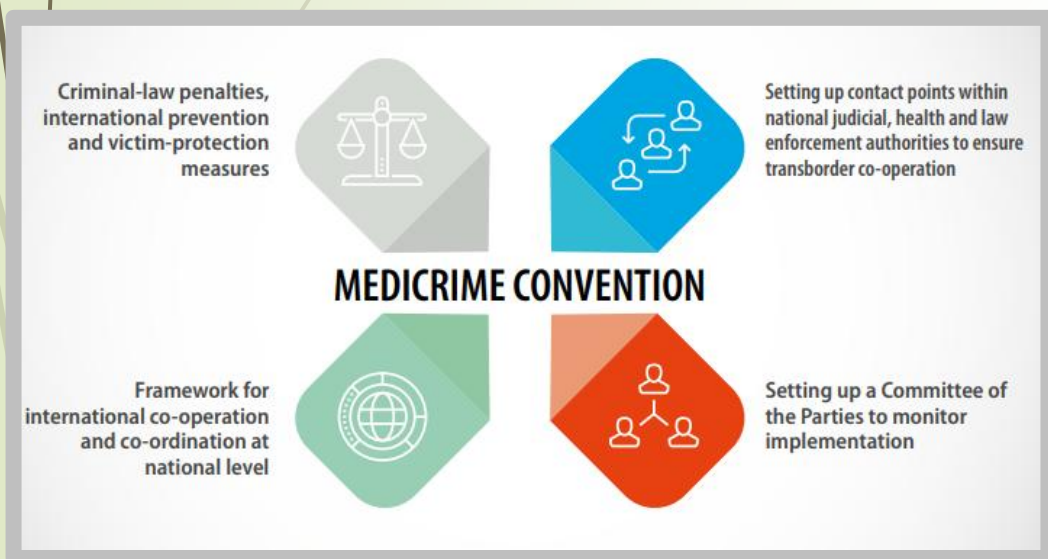
2 INVITATIONS

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 ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΟΥ ΕΛΕΓΧΟΥ

Αρμόχ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 5763
Ημερομ. Καταχώρ.: 29/5/2025

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
Αναστάσιος Δημοσθένης
Βουλευτής Έβρου

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, προέβη στην υπογραφή της ως άνω σύμβασης τον Μάιο του 2022, η οποία ωστόσο δεν έχει ενσωματωθεί στο "νομοθετικό σπαστάσιον" της Χώρας, καθώς εκκρεμεί η διαδικασία της επικύρωσής αυτής.

Όπως επισημαίνεται και στο συνοδευτικό υπόμνημα του π.Διευθυντού της Διεύθυνσης 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.

Σέκηρη 1, Αθήνα | Τηλ: 2103675611 | Φακ: 2103675612 | Κιω.: 697 811 98 63 | admioschakis@outlook.com
Καραϊσκάκη 10, Αλεξανδρούπολη | Τηλ: 25510 27548 | Φακ: 25510 36874 | Ελ. Βενιζέλου 28, Δομοσότορο | Τηλ: 25530 23308



- Υπογραφή Σύμβασης
Μάιος 2022
- Επερώτηση για την μη
Επικύρωση της Σύμβασης
Σεπτέμβριος 2025
- Τοποθέτηση στη
διαβούλευση
Απρίλιος 2026

Πηγές

1. https://www.hellenicparliament.gr/UserFiles/c0d5184d-7550-4265-8e0b-078e1bc7375a/12951870.pdf?fbclid=IwY2xjawKr4ttleHRuA2FibQlXmABicmlkETB4T1hObDNnNkh4TWZ6SE4wAR7zYLMoQFAYNOXbq7VUubCBMpk0WkCVhgsWCzkrb32_SQWV-jKJpRxtPZjs_4w_aem_00bjjEqYTRQrYa7NFznhNg
2. <https://www.hellenicparliament.gr/UserFiles/67715b2c-ec81-4f0c-ad6a-476a34d732bd/12976450.pdf>
3. https://www.opengov.gr/yyka/?c=17616&fbclid=IwY2xjawRakutleHRuA2FibQlXmABicmlkETB2aElscjJNeEMwWnVyZG1xc3J0YwZhcHBfaWQQMjlyMDM5MTc4ODlwMDg5MgABHmUu0zwYXnw0O4dhTi83hFCr3cm6lVaVVPtTx7D8LxYjzyR00t9xoVV_0Lqr_aem_488086woRUKi9LXibRJSLg

Δημοκρατία & Ανθρώπινα Δικαιώματα Το πραγματικό διακύβευμα

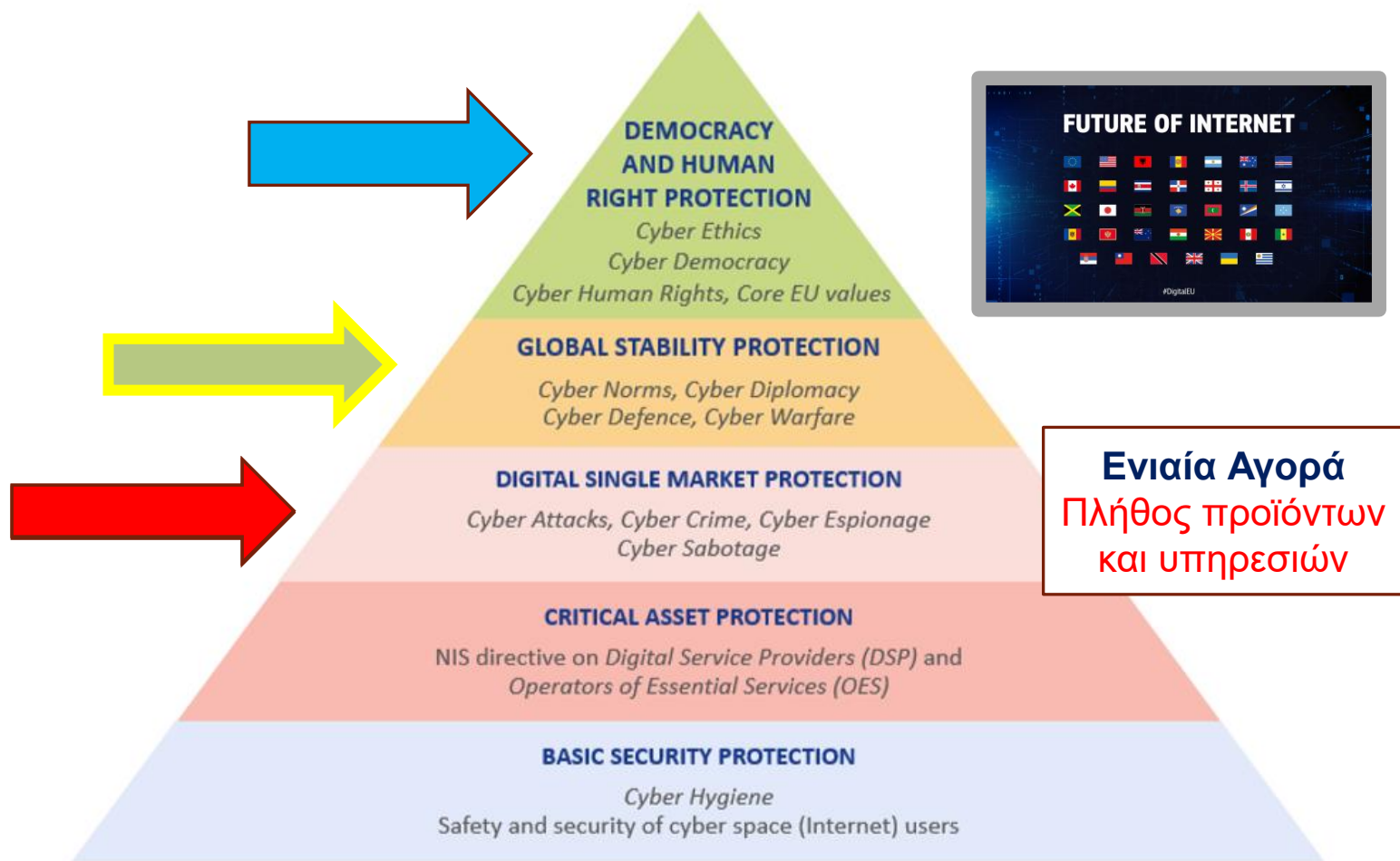
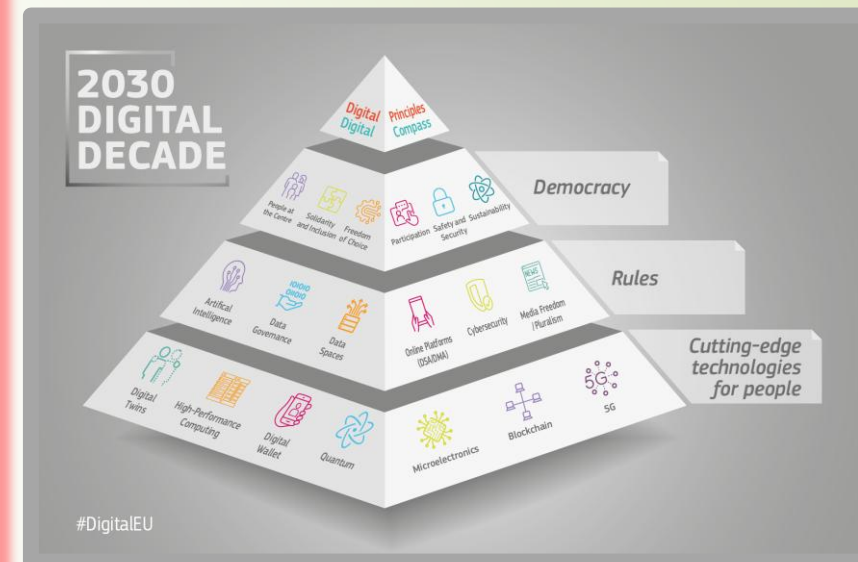


Figure 1. Layers of cybersecurity needs.



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>



Ως Συμπέρασμα

- ❑ Ο **Κυβερνοχώρος** είναι η νέα μας χαοτική πραγματικότητα.
- ❑ Οι σημερινές προκλήσεις & απειλές είναι **ασύμμετρες** και αγγίζουν **άτομα**, **επιχειρήσεις** και **κυβερνήσεις**
- ❑ Απαιτούν δεξιότητες και ικανότητες (πολλαπλοί εγγραμματισμοί)
- ❑ Η **Κυβερνοασφάλεια** είναι **υπόθεση όλων μας** και απαιτεί **διαρκή προετοιμασία**

Τι μπορεί να γίνει

- ❑ Προστασία κι ενδυνάμωση των ευάλωτων ατόμων
- ❑ **Ανάπτυξη Κουλτούρας**
(Κυβερνοασφάλειας – προστασίας δεδομένων – πλαισίου TN- Τεχνοθητική)
- ❑ **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 πολιτείας

- ❑ Στρατηγική και Όραμα
- ❑ Πολιτική βούληση & ευρύτερη δυνατή συναίνεση
- ❑ Κουλτούρα Συνεργασίας Φορέων

[Πανεπιστημιακές Σχολές, Ερευνητικά Κέντρα, Επιστημονικοί Σύλλογοι, **Επιμελητήρια**, Εμπλεκόμενοι φορείς, Ενίσχυση Διεθνούς Συνεργασίας]

- ❑ Κουλτούρα Τεχνοθητικής
- ❑ Θεσμική θωράκιση

[2ο πρωτόκολλο Cybercrime Convention (διαχείριση ψηφιακών πειστηρίων), **Άυλη δικογραφία**, εξειδίκευση δικαστών, **Ειδικός Εισαγγελέας** για το Κυβερνοέγκλημα για όλη την χώρα, ορισμός Εισαγγελικού λειτουργού για **εποπτεία διαδικτυακής πλατφόρμας καταγγελιών**, ενίσχυση με επιστήμονες των εγκληματολογικών εργαστηρίων για την εξέταση των πειστηρίων, κατάργηση τραπεζικού απορρήτου, **επικύρωση** από τη Βουλή κι **εφαρμογή Medicrime Convention**, **ενίσχυση** του θεσμικού πλαισίου για την TN, κα.]

- ❑ Διάθεση Πόρων για την Κυβερνοασφάλεια
- ❑ Αξιοκρατία – Διαφάνεια – Δικαιοσύνη



Χρήσιμες πληροφορίες

στο **κανάλι** του εισηγητή στο Youtube και στη **σελίδα** cyber-news.gr

Γιώργος Παπαπροδρόμου - Giorgos Papaprodromou

Σύνδεσμοι

- Prevention Guides EUROPOL
[europol.europa.eu/operations-services-and-innovation/public-awareness...](http://europol.europa.eu/operations-services-and-innovation/public-awareness)
- Protecting Children COE
coe.int/t/dg3/children
- Cybercrime COE
coe.int/en/web/cybercrime
- Cybercrime Interpol
interpol.int/Crimes/Cybercrime
- Cybersecurity Basics FTC USA
ftc.gov/business-guidance/small-businesses/cybersecurity/basics
- ENISA PUBLICATIONS
enisa.europa.eu/publications#c3=2012&c3=2022&c3=false&c5=publishing
- CYBERSECURITY CISA USA
cisa.gov/cybersecurity
- CYBER AWARE UK
ncsc.gov.uk/cyberaware/home
- CYBERCRIME EUROJUST
eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime
- ΥΛΙΚΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
dipe.art.sch.gr/index.php/2014-06-29-19-31-34/ekp-ko-yliko/dimotiko...
- Κυβερνοασφάλεια ΕΑΨΙ ΥΨΗΔ
nationaldigitalacademy.gov.gr/anazhthsh/?skill=19&q=
- ITU CYBERSECURITY
itu.int/en/action/cybersecurity/Pages/default.aspx
- UN Office on Drugs and Crime
unodc.org/unodc/en/cybercrime
- CSIRT HELLENIC
cyber.gov.gr/el-csirt



Με θεματικά
playlists & links

Αναζήτηση

Κυβερνοχώρο στην καθημερινότητά

Γιώργος Παπαπροδρόμου - Giorgos Papaprodromou

1,311 χιλ. εγγραφμένοι · 241 βίντεο

Χρησιμοποιήστε το φίλτρο για να βρείτε στα playlists του καναλιού... ακόμη

europol.europa.eu/operations-services-and-innovation/public-awareness... και 13 ακόμη σύνδεσμοι

Προσαρμογή καναλιού Διαχείριση βίντεο

Αρχική Βίντεο Playlists Αναρτήσεις

Τρόποι Διαχείρισης Περιστατικών Απάτης στον Κυβερνοχώρο...
27 προβολές · πριν από 1 ημέρα

Η Κωνσταντίνα Δημογλιδου και ο Γιώργος Παπαπροδρόμου καλεσμένοι στην πρωινή εκπομπή του τηλεοπτικού σταθμού ACTION 24, των δημοσιογράφων Ντόρας Κουτροκόη και Γιώργου Γρηγοριάδη συζητούν για την πιο διαδεδομένη μορφή εγκλήματος στον Κυβερνοχώρο που είναι οι απάτες του διαδικτύου.

... ΔΙΑΒΑΣΤΕ ΠΕΡΙΣΣΟΤΕΡΑ

Για εσάς

Πηγές:

1. <https://www.youtube.com/@papaprodromou>
2. www.cyber-news.gr

Σας *ευχαριστώ* πολύ για την προσοχή σας

*Thank
You*

Στη διάθεσή σας για *ερωτήσεις*

Γιώργος Παπαπροδρόμου

Αντιστράτηγος ε.α. (ΕΛ.ΑΣ.)