

# Η Κυβερνοασφάλεια στη Σύγχρονη Εποχή: Προστασία Καταναλωτών και Επιχειρήσεων



**ΔΗΜΟΣ ΠΕΛΛΑΣ** **ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ**  
ΙΣΤΟΡΙΚΗ & ΛΟΓΟΓΡΑΦΙΚΗ ΕΤΑΙΡΕΙΑ ΚΛΑΜΑΤΙΣΤΩΝ "Ο ΦΙΛΙΠΠΟΣ"

**ΗΜΕΡΙΔΑ ΜΕ ΘΕΜΑ**  
**"Κυβερνοασφάλεια στη Σύγχρονη Εποχή"**

Συνδιοργάνωση Δήμος Πέλλας, Διεύθυνση Αστυνομίας Πέλλας, Διημεροεξέταση Σύλλογος Γιαννιτών και Ιστορική και Λογογραφική Εταιρεία Κλαματιστών "Ο Φίλιππος"

**Θεματικές:**

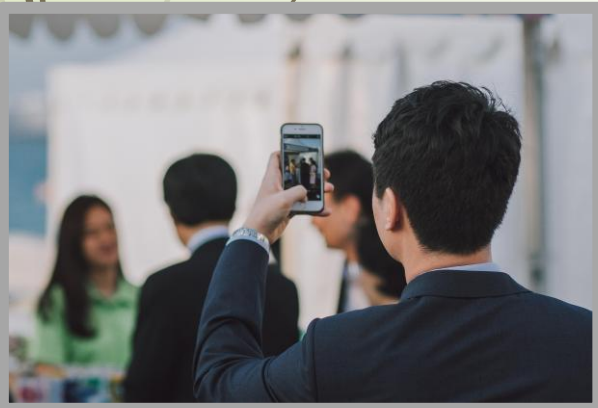
i) ΘΕΜΑ: "Προστασία Καταναλωτών και Επιχειρήσεων"  
Εισηγητής: Αντιστράτηγος ε.α. ΠΑΠΑΠΡΟΔΡΟΜΟΥ Γεώργιος,  
Πτυχιούχος Νομικής ΑΠΘ - Δικαστικός Γραφολόγος,  
Πρώην Διευθυντής Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος

ii) ΘΕΜΑ: "Ηλεκτρονικές Απάτες - Εντοπισμός και Αποφυγή τους!"  
Εισηγητής: Αστυνομικός Β' ΒΑΣΙΛΕΙΟΥ Εμμανουήλ,  
Αξιωματικός Τμήματος Δίωξης και Εξιχνίασης Εγκλημάτων Πέλλας

Τετάρτη 13 Μαΐου 2026 και ώρα 19:00'  
Αίθουσα Συνεδριάσεων Δημοτικού Συμβουλίου Δήμου Πέλλας

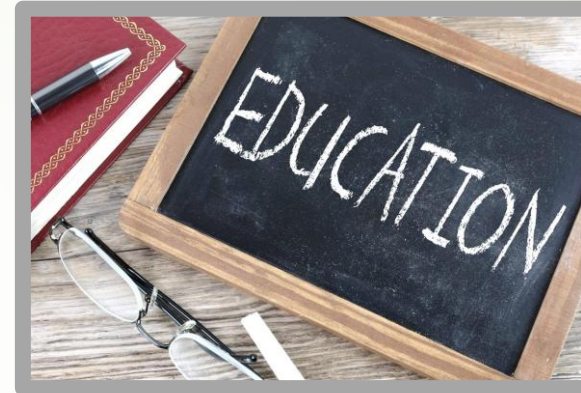


**Γιαννιτσά, 13/05/2026**



Εισηγητής:  
**Γιώργος Παπαπροδρόμου**  
Αντιστράτηγος ε.α. (ΕΛ.ΑΣ.)

# Βασικά σημεία της σημερινής παρουσίασης



1. Τι γνωρίζουμε για το οικοσύστημα του **Κυβερνοχώρου**;
2. Ποιες είναι οι σημερινές προκλήσεις για **καταναλωτές** και **επιχειρήσεις**;
3. Τι ψηφιακές ικανότητες και δεξιότητες διαθέτουμε;
4. Τα εργαλεία και οι καλές πρακτικές που θα μας βοηθήσουν

# 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

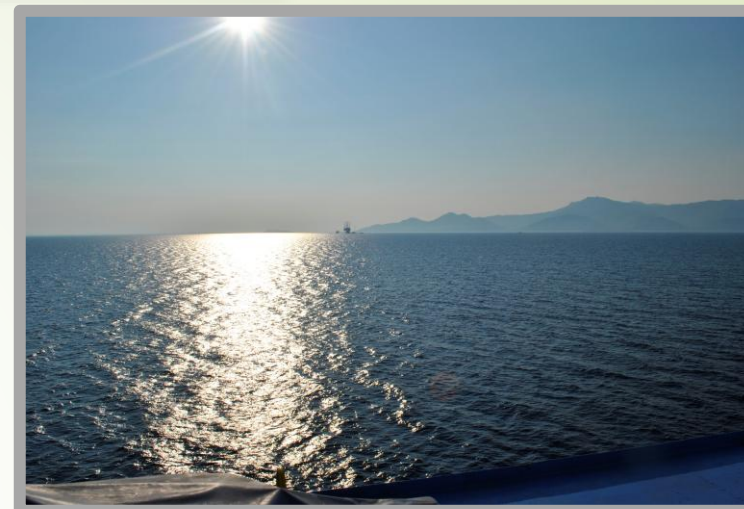
### Deep web

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**



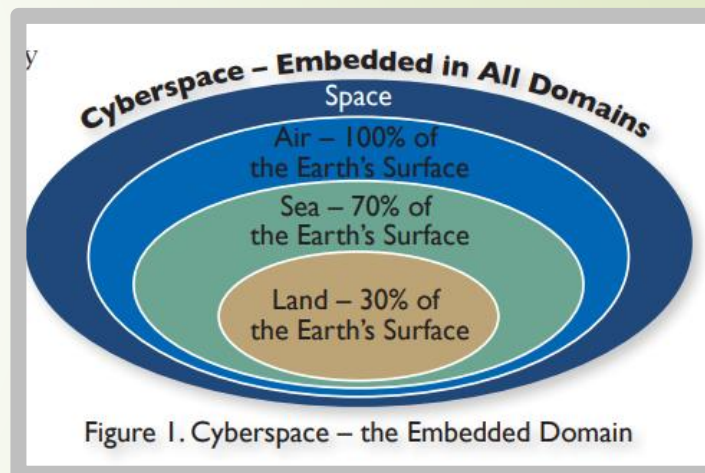
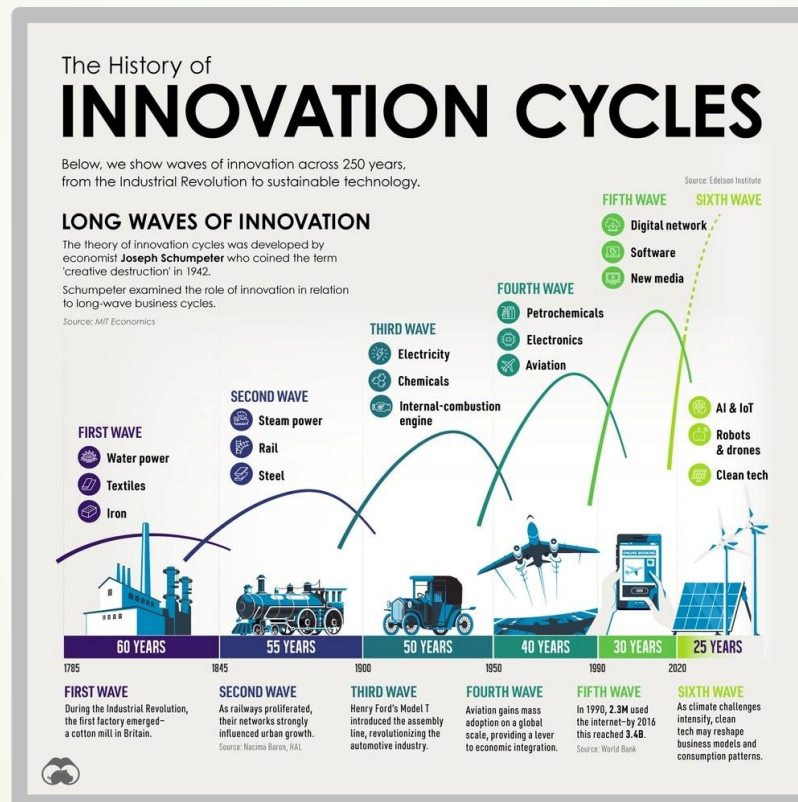
## Πηγές:

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>

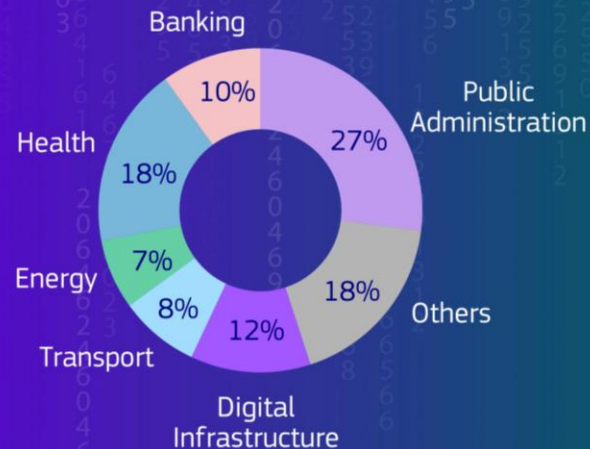
**Δισεκατομμύρια  
άνθρωποι  
& συσκευές**



# 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



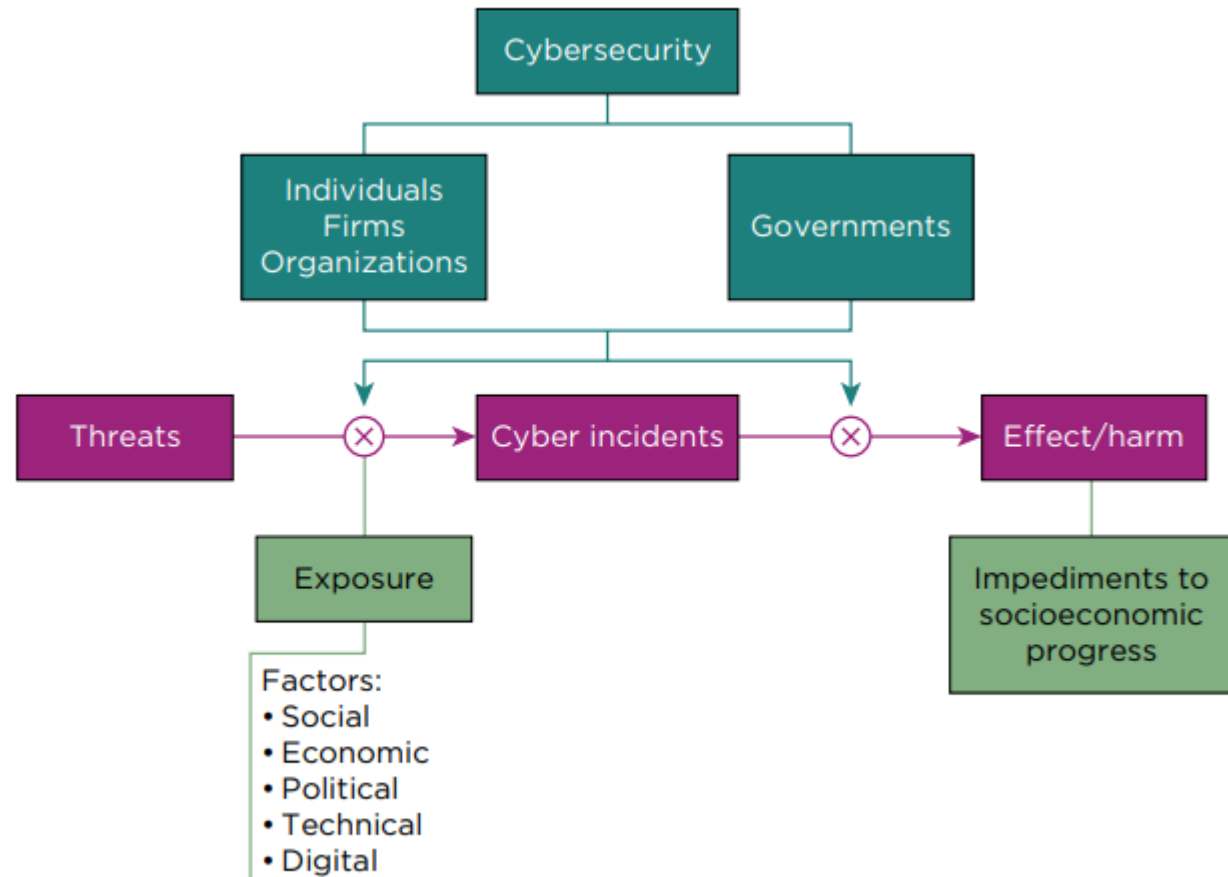
Source: Cybersecurity Incident Reporting and Analysis System 2025

**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](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



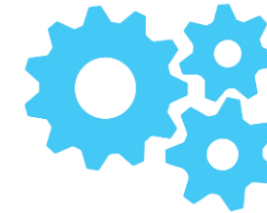
Staff headcount  
< 250



Turnover or Balance  
sheet total  
≤ € 50 m



People



Process



Technology

ΜμΕ

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

Πηγές:

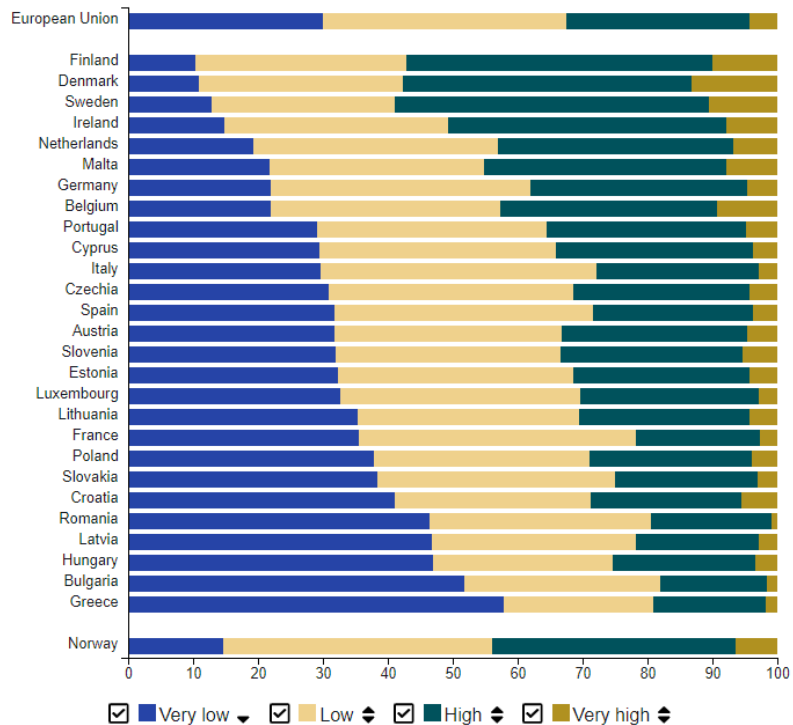
- <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes> p.9, 28
- <https://www.youtube.com/watch?v=ymlKVTat-IM>
- Reinforcing trust and security in the area of electronic communications and online services — ENISA (europa.eu)
- [https://cyber.gov.gr/wp-content/uploads/2025/03/250323\\_%CE%9F%CE%B4%CE%B7%CE%B3%CF%8C%CF%82-%CE%91%CE%BD%CE%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

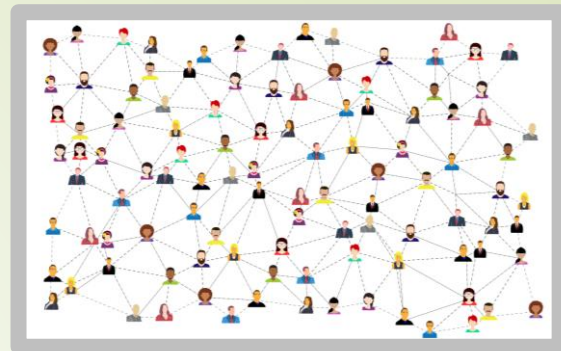


Πηγές:

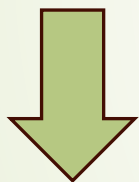
- [https://ec.europa.eu/growth/smes\\_en](https://ec.europa.eu/growth/smes_en)
- [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme\\_cybersecurity](https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme_cybersecurity)
- <https://www.enisa.europa.eu/news/enisa-news/survey-to-explore-the-preparedness-of-eu-smes-for-cybersecurity-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 \(europa.eu\)](#)



**Ο άνθρωπος  
διακινδυνεύει τα δεδομένα  
Ο άνθρωπος τα προστατεύει**



**Ως αδύναμος κρίκος**



- Μη επαρκή γνώση κυβερνοασφάλειας
- Τάση για ευκολία
- Υπερβολική εμπιστοσύνη σε μηνύματα

**Ως μηχανισμός άμυνας**



- Κριτική σκέψη
- Ψηφιακός εγγραμματισμός
- Υπεύθυνη χρήση των τεχνολογιών

# 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)**



116

Συνέκδικος Ἱερατικό.

τοῦ διαβόλου. Κρίμα σημαίνει τὸ αὐτὸ καὶ Κρίσις (judgement,) οἷον “Τα κρίματά σου ὡσεὶ ἄβυσσος πολλή.” 1) “Κρίματα, ψῆφοι, δικαί” κατὰ τὸν Ἡσύχιον. Σημαίνει ἀκρίμη καὶ τὸ Κατάκριμα 2) ἤγουν τὴν Καταδίκην (condamnation) “Κρίμα, τὸ κατάκριμα καὶ ἡ καταδίκη, ὡς τὸ Κρίμα ἐαυτῶ ἐσθίει καὶ πίνει κ. τ. λ.” 3) Λέγει καὶ ὁ Ἡσύχιος “Κρίμα, ἀνταπόδοσις Θεοῦ.” Καὶ τρίτον, αὐτὸ τὸ κρινόμενον ἔγκλημα ἢ ἀμαρτήμα, λέγεται Κρίμα, ὅθεν οἱ Ῥωμαῖοι ἔλαβαν τὸ Crimen (crime,) ὀνομαζόντες οὕτως τὴν ἐγκληματικὴν τῶν πολιτικῶν νόμων παράβασιν, ὡς ἡμεῖς σήμερον ἰνομάζομεν (εἰς θεησκικὴν 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, Μία 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#imagePopUp](https://www.allthescience.org/what-is-cybernetics.htm?fbclid=IwAR1a3OvyGvUZirN6zSd_fQybbT9RZ0GizSwr7B4n0-MKU3g6rmnsiRkMHxc#imagePopUp)
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
12. Γιάννης Τόλιας, Ψηφιακή Εποχή, Εκδόσεις Τόπος, 2021, σελ. 62-64



ΠΑΓΚΟΣΜΙΑ ΗΜΕΡΑ  
ΕΛΛΗΝΙΚΗΣ ΓΛΩΣΣΑΣ  
9 ΦΕΒΡΟΥΑΡΙΟΥ

# Το Κυβερνοέγκλημα αυξάνεται Τα δεδομένα μας **πρώτος** στόχος



**IOCTA 2026**  
Internet Organised Crime Threat Assessment

**The evolving threat landscape**  
How encryption, proxies and AI are expanding cybercrime

EUROPOL

**Federal Bureau of Investigation  
Internet Crime Report  
2025**

INTERNET CRIME COMPLAINT CENTER

DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION

CONFIDENTIAL DATA

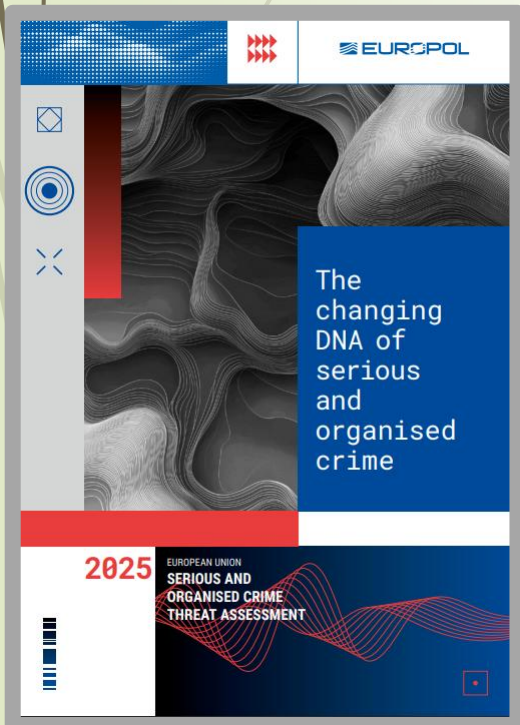
Login: .....  
Password: .....

Δημοσιεύθηκαν **28/04/2026 & 06/4/2026**

**Πηγές:**

1. <https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf>
2. [https://www.ic3.gov/AnnualReport/Reports/2025\\_IC3Report.pdf](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>

# 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>

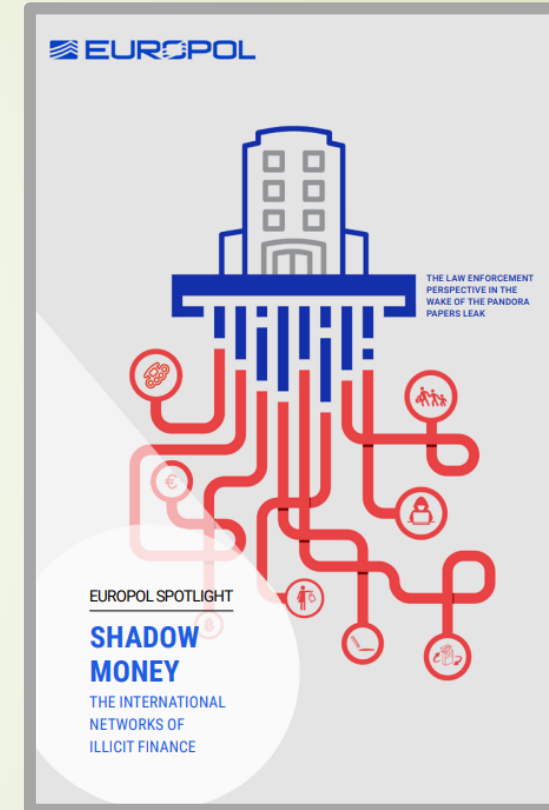
# Οικονομικές απώλειες από το κυβερνοέγκλημα

## □ 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](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>



# Πρόσφατα περιστατικά Κυβερνοεγκλημάτων

Profit - Κέρδος



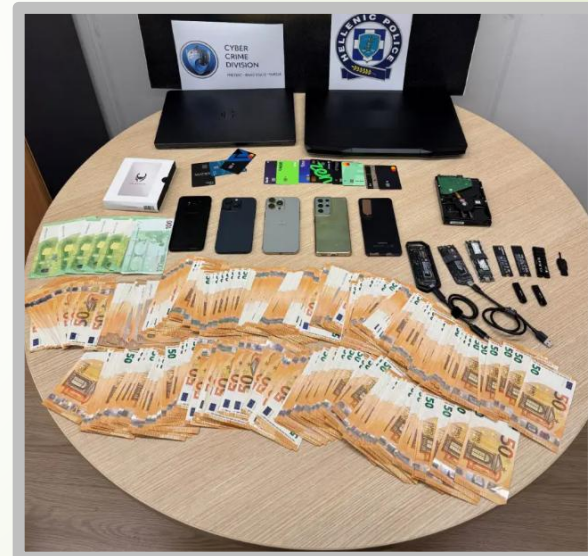
27  
NOV  
2025

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

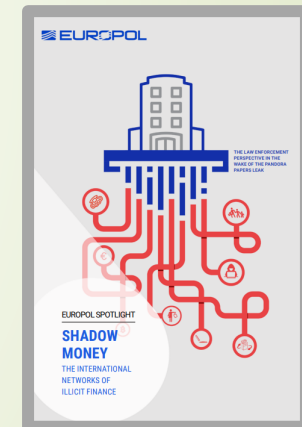


Πηγές

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>

# 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)



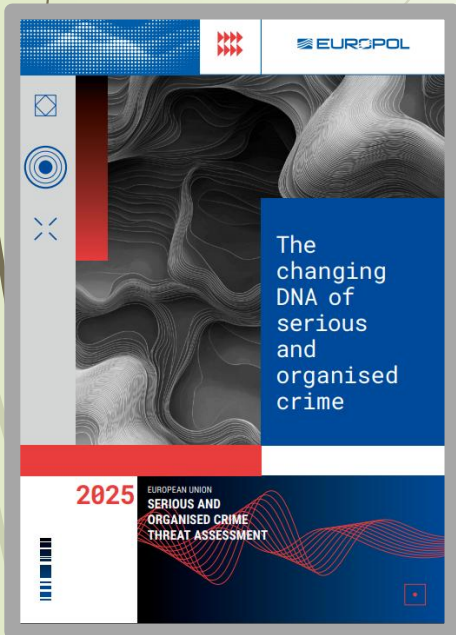
## Πηγές

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](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>

# Η 3η σε μέγεθος Οικονομία παγκοσμίως

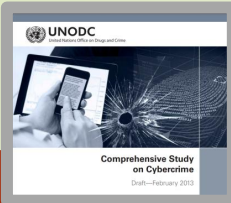


 **CYBERSECURITY  
VENTURES**



## 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/>
5. [worldometers.info/gdp/gdp-by-country/](http://worldometers.info/gdp/gdp-by-country/)
6. <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=1>



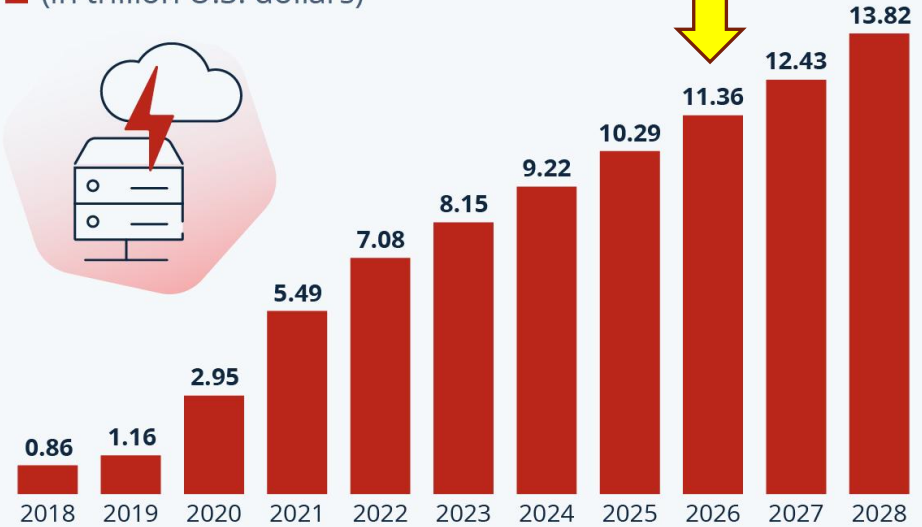
# Αντίκτυπος του Κυβερνοεγκλήματος

## 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



### Πηγές:

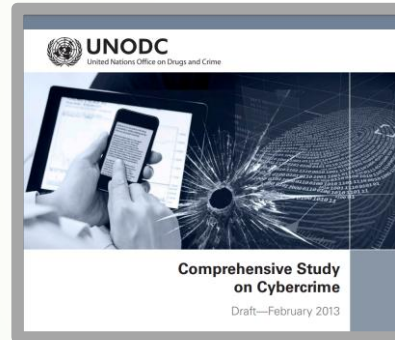
- <https://www.itsecuritypro.gr/kyvernoasfaleia-kai-mikromesaies-epicheiriseis/>
- <https://elisme.gr/to-pragmatiko-timima-toy-kyvernoegkl/>
- [https://surfshark.com/research/data-breach-impact/statistics?fbclid=IwAR0AQp4OOnT3\\_hyJPbUEcf2d8SZelUUcwY\\_NSrPFa2-rwyg4KKNj-aw\\_Cfw](https://surfshark.com/research/data-breach-impact/statistics?fbclid=IwAR0AQp4OOnT3_hyJPbUEcf2d8SZelUUcwY_NSrPFa2-rwyg4KKNj-aw_Cfw)
- <https://www.facebook.com/photo/?fbid=711019361235436&set=a.561580072846033>



# 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](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](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>

**76 κράτη** την έχουν υπογράψει  
**Στοιχεία της 13/05/2026**

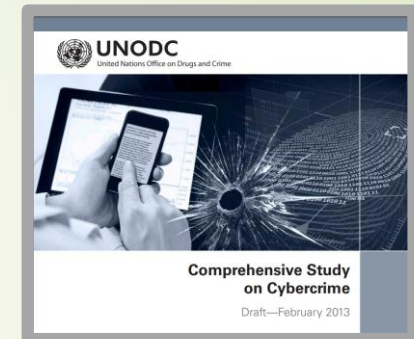
# Σύμβαση για το **Κυβερνοέγκλημα** Το πρώτο διεθνές κείμενο Budapest 23/11/2001- CETS No 185



## 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:

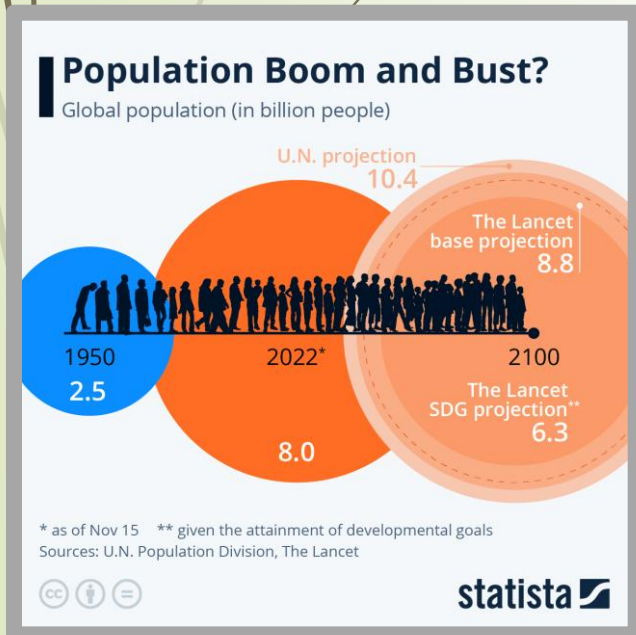
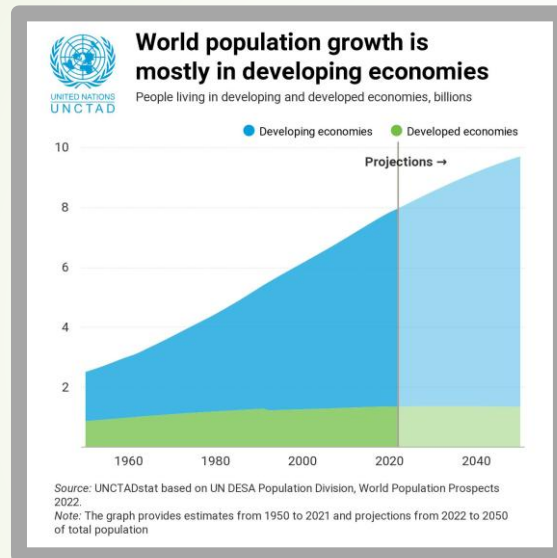
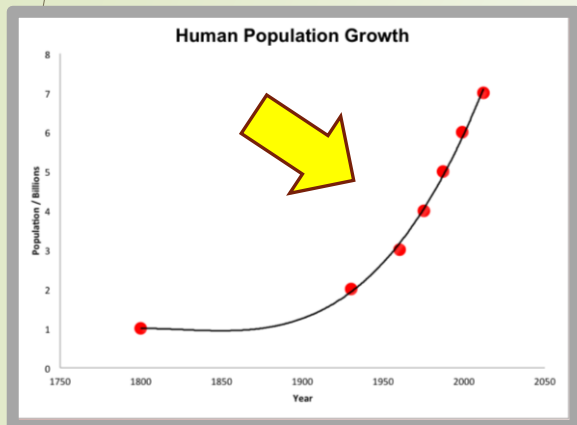
1. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
2. [https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME\\_STUDY\\_210213.pdf](https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf)
3. <https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan-2023-public-v1/1680a99137>
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](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 13/05/2026**

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

# Πληθυσμιακή αύξηση και τεχνολογία

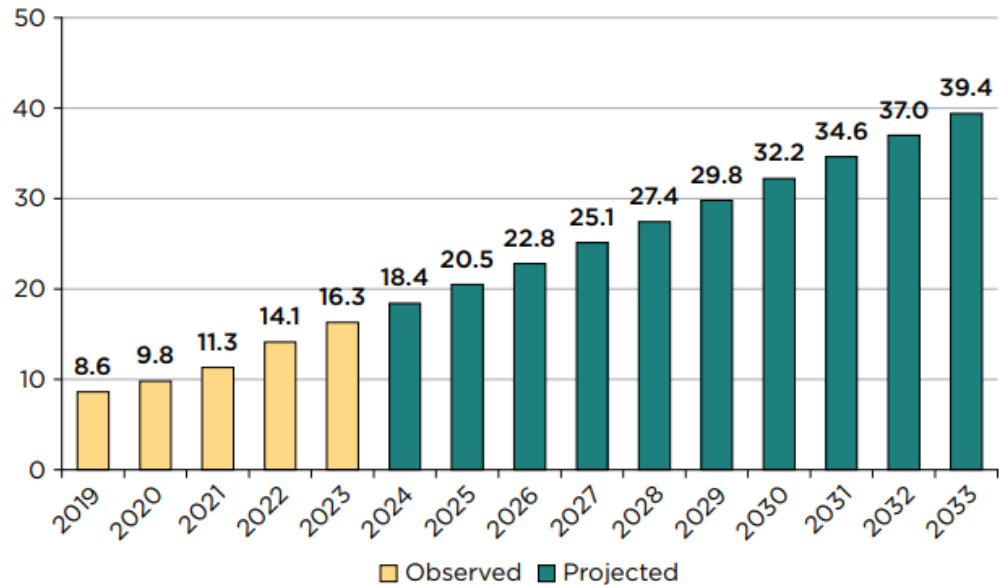


**Πηγές**

- <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, Μεταίχιμο, σελ. 25-26, 36-40, 42

# Περισσότερα τα κινητά από τους ανθρώπους

Number of Internet of Things connected devices (billions)

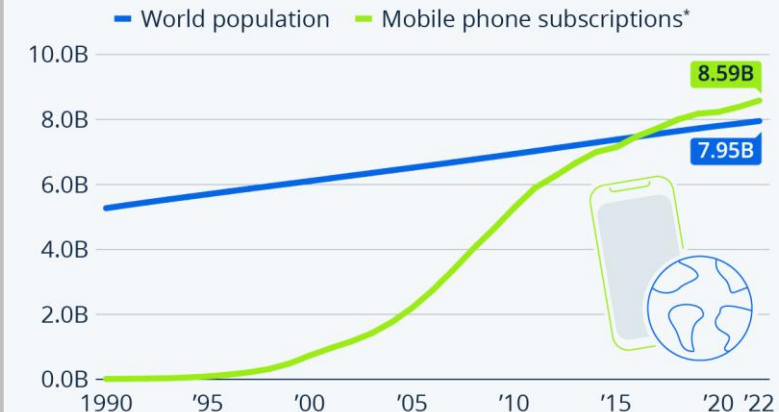


Source: Original figure for this book, based on data from Transforma Insights 2024.



## 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

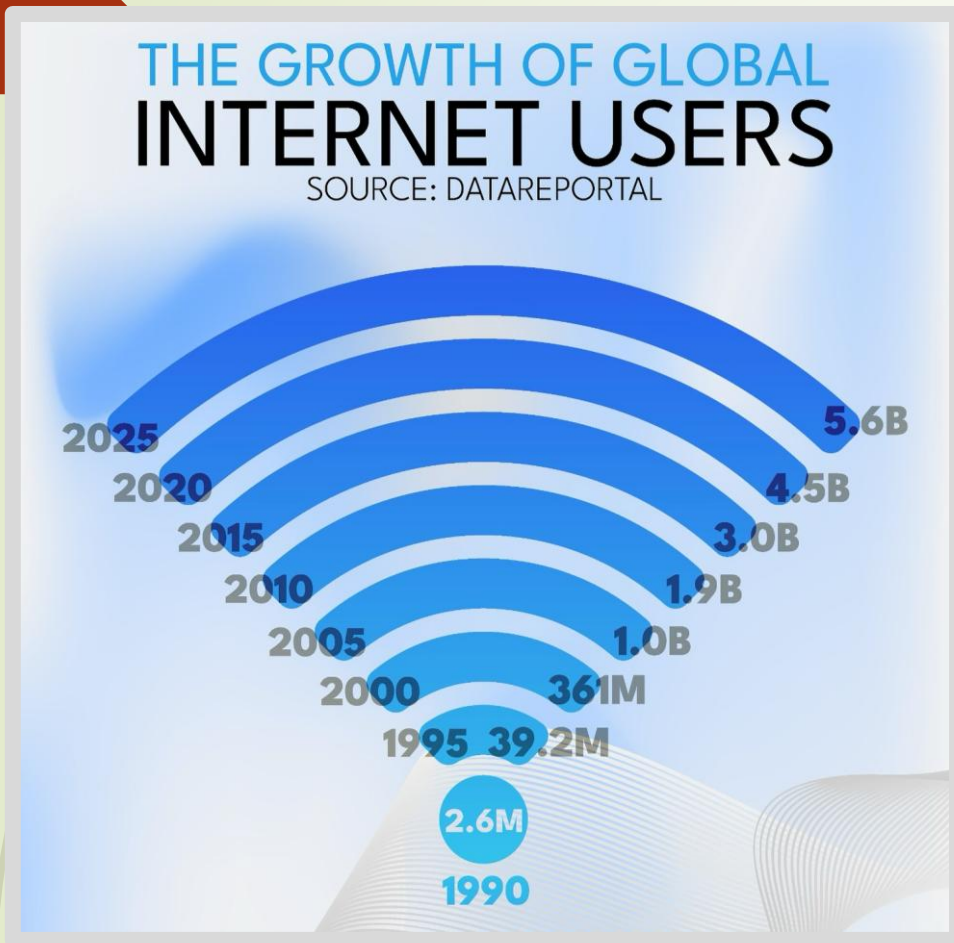


statista

## 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**

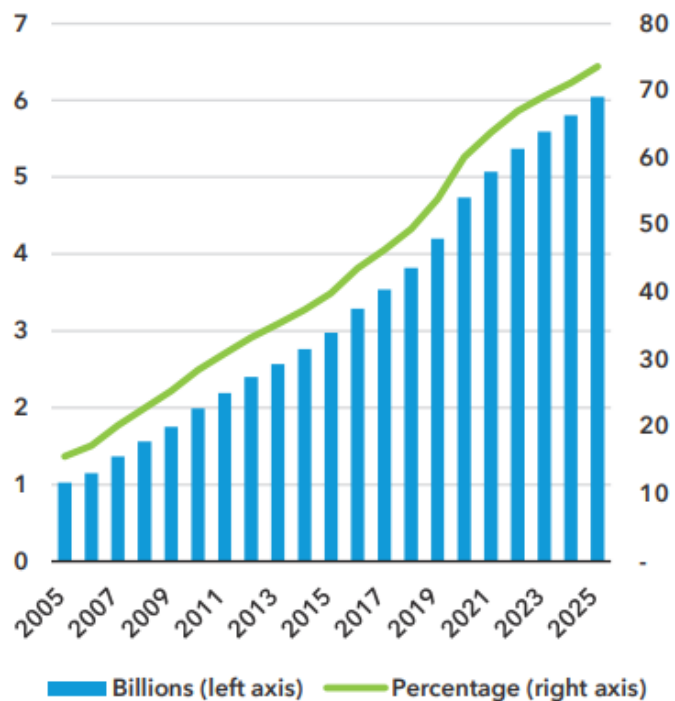


Πηγές:

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/](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



Note: Includes ITU estimates.  
Source: ITU

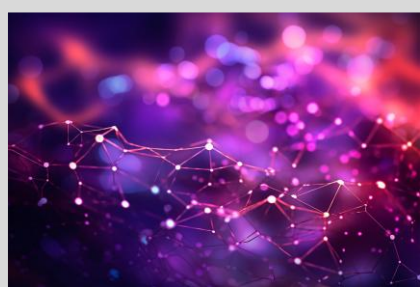
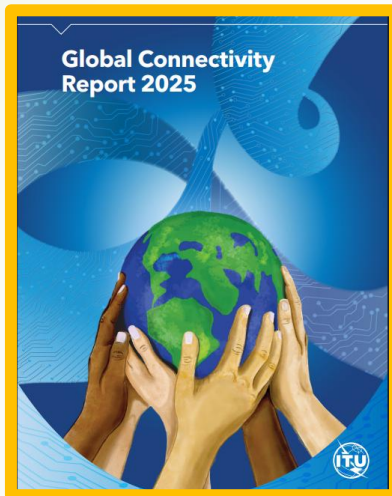
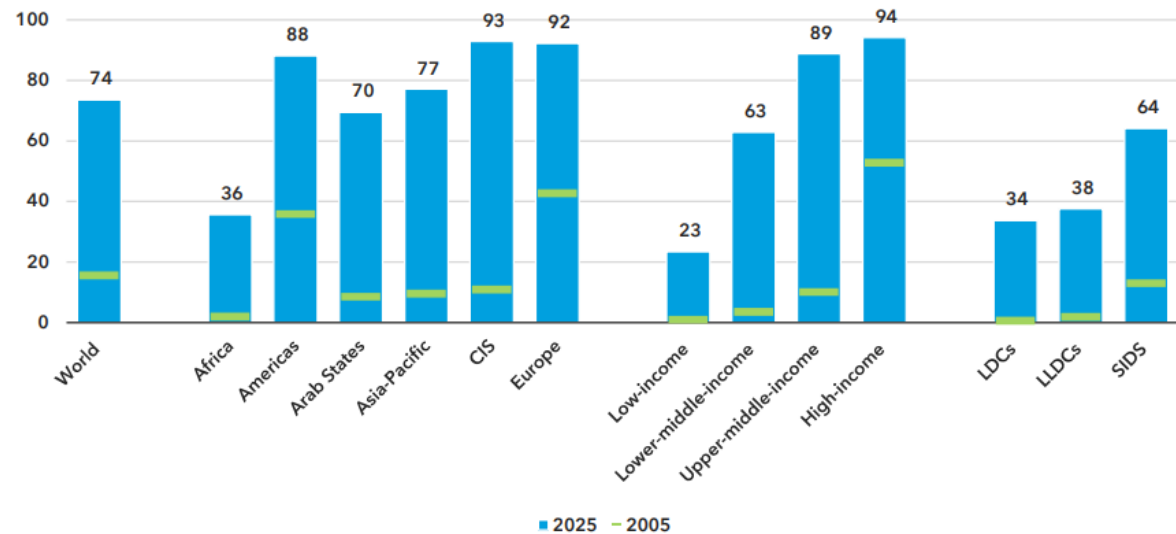


Figure 2.2: Percentage of individuals using the Internet by region and special groups 2005 and 2025



Note: Includes ITU estimates.

Source: ITU

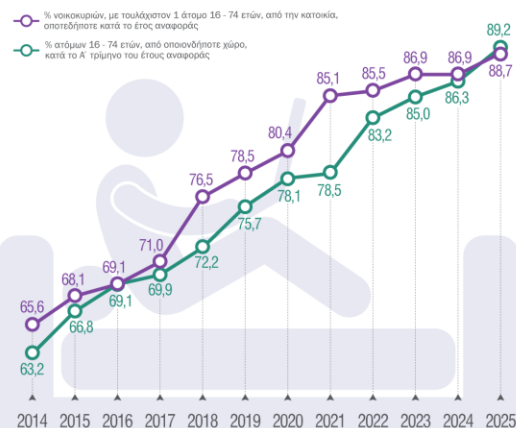
Συνδεδεμένοι 73,17 %  
Μη Συνδεδεμένοι 26,83 %

Πηγές:

- <https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx>
- [https://www.itu.int/hub/publication/D-IND-ICT\\_MDD.GCR-2025-4/](https://www.itu.int/hub/publication/D-IND-ICT_MDD.GCR-2025-4/) p.22-23

# ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΣ από νοικοκυριά και άτομα, 2025

## ΠΡΟΣΒΑΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ



## ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

% ατόμων 16 - 74 ετών που έχουν χρησιμοποιήσει το διαδίκτυο, Απρίλιος 2024 - Μάρτιος 2025



## ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

% ατόμων 16 - 74 ετών που έχουν χρησιμοποιήσει το διαδίκτυο, Α' τρίμηνο 2025



## ΧΡΗΣΗ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

% ατόμων 16 - 74 ετών που έχουν χρησιμοποιήσει το διαδίκτυο, Α' τρίμηνο 2025



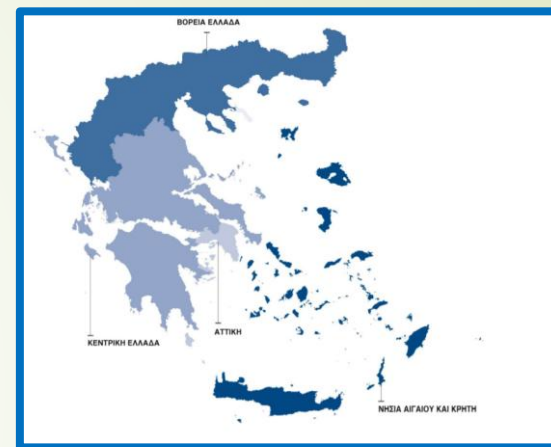
## ΣΥΣΚΕΥΕΣ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

% ατόμων 16 - 74 ετών που έχουν χρησιμοποιήσει το διαδίκτυο, Α' τρίμηνο 2025



# Ανοδική χρήση των ΤΠΕ στην Ελλάδα

Ημερομηνία δημοσίευσης:  
**10.12.2025**



GR - 10,341,683 population (2022) - Country Area: 131,957 sq km

Capital city: Athens - population 3,153,000 (2021)

GDP (per capita): \$17,647 (2020) per World Bank.

8,115,397 Internet users in JAN/2022, 78.5% penetration, per IWS.

7,657,000 Facebook subscribers in JAN/2022, 74.0% penetration rate.

Πηγές:

- [https://www.statistics.gr/documents/20181/18723345/DT\\_tehnologies\\_noiko\\_kyria\\_2025\\_new\\_gr.png/aa6d7da4-7259-a607-8629-54c813912b87](https://www.statistics.gr/documents/20181/18723345/DT_tehnologies_noiko_kyria_2025_new_gr.png/aa6d7da4-7259-a607-8629-54c813912b87)
- <https://www.statistics.gr/en/statistics/-/publication/SFA20/>
- <https://www.internetworldstats.com/europa.htm#gr>



Πηγή: Ελληνική Στατιστική Αρχή / 10 Δεκεμβρίου 2025

#GreekDataMatter

# Η Ασφάλεια θέμα υψηλής προτεραιότητας

consentmanager

Digital Service Act



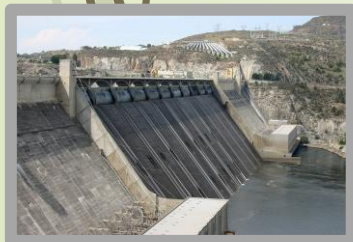
- Ασφαλές για το μέλλον περιβάλλον
- Αντιμετώπιση εξελισσόμενων απειλών
- Προστασία από τρομοκρατία και οργανωμένο έγκλημα
- Ισχυρό οικοσύστημα ασφάλειας












## Πηγές:

- [https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-of-life/european-security-union\\_en](https://ec.europa.eu/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://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\\_U2oaUUIGQD7ogwR0M9948FzcRnZepyGCJv7Uutp6nsyoe1lgGzqPryCwtwRuLiozYdJW9](https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package?fbclid=IwAR2lWdrlQMiWv3aBNIJzkdDZVsxj12o6gn7ZK_2edWPUwVlIbhf9Gat_cltM_aem_Abz5czPFhGStxvQmG_U2oaUUIGQD7ogwR0M9948FzcRnZepyGCJv7Uutp6nsyoe1lgGzqPryCwtwRuLiozYdJW9)
- <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0148>

# 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](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

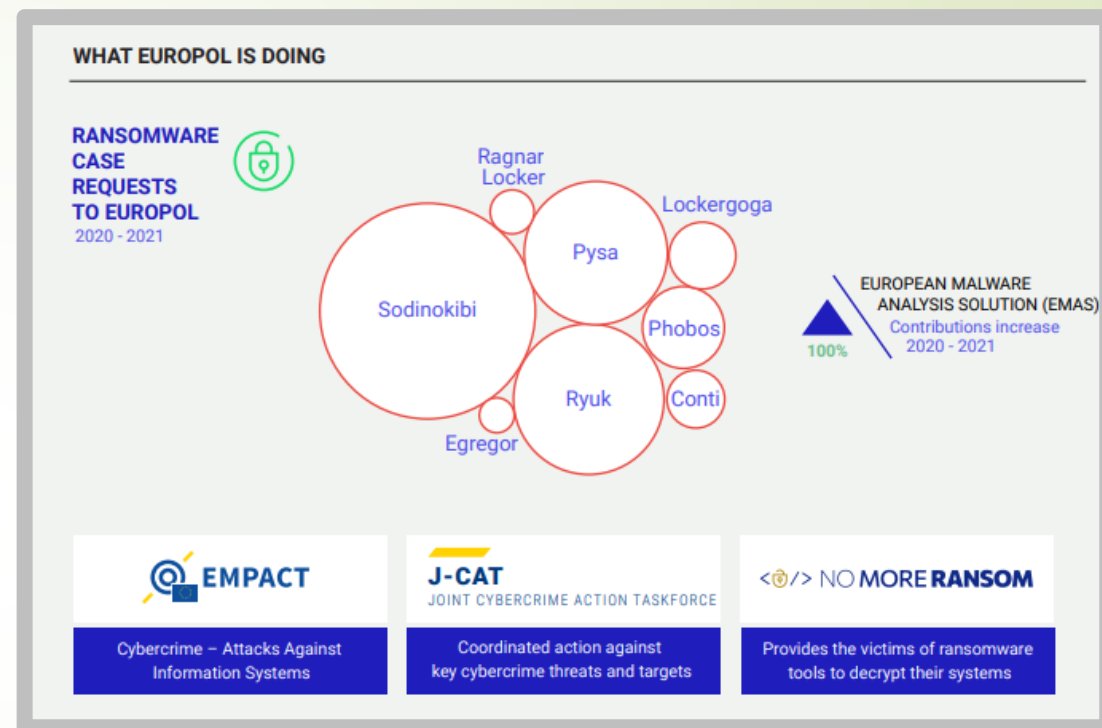
4 days ago

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](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>

# Νέα δωρεάν χρηστικά εργαλεία, προϊόντα της διεθνούς συνεργασίας

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 στιδήποτε με το σκληρό σας δίσκο.

Συμβουλές για χρήστες του διαδικτύου

Βήματα μετριασμού για τις επιχειρήσεις

**NO MORE RANSOM!**

[www.nomoreransom.org](http://www.nomoreransom.org)

Πηγές:

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

# Κυβερνοεπιθέσεις - DDoS επιθέσεις

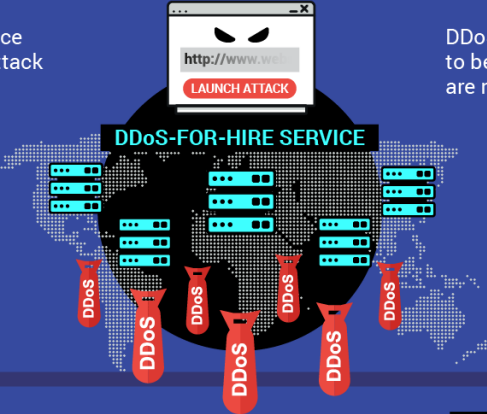
## How can DDoS attacks paralyse the internet

**1** The criminal hires a DDoS attack service on the internet



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



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

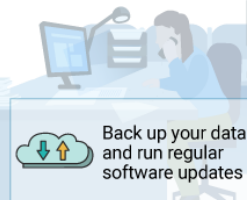
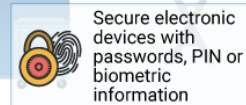
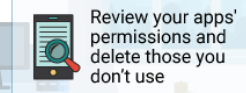
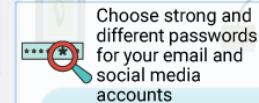
Πηγή:

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

# Προστατεύοντας συσκευές, προστατεύουμε δεδομένα, προστατεύουμε ανθρώπους



## MAKE YOUR HOME A CYBER SAFE STRONGHOLD



**WHAT DO YOUR DEVICES KNOW ABOUT YOU?**

When it's connected to your device or app, it can collect information about you. Some of this information may be sensitive or important.

<b>Passwords</b>	<b>Credit Card Numbers</b>	<b>Social Security Number</b>
<b>Deleted Files</b>	<b>Text Messages</b>	<b>Phone Calls</b>
<b>Bank Account Info</b>	<b>Name and Address</b>	<b>Recently Visited Sites</b>
<b>Recent Files</b>	<b>Contacts</b>	<b>Current Location</b>
<b>Recent Locations</b>		

**CYBER CRIME STATISTICS**

Average total cost of a data breach	75 MILLION	Percentage of organizations that have experienced a data breach	73%
Total number of data breaches in 2022	2,000	Percentage of organizations that have experienced a data breach in the last 12 months	78%
Percentage of data breaches that were preventable	2%		



## Πηγές:

- <https://www.enisa.europa.eu/secureme/#/cyber-tips#>
- <https://www.nomoreransom.org/el/index.html>
- <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold>
- <https://nonprofitcyber.org/common-guidance-on-passwords/?fbclid=IwAR3zicRj4rBYL2JO35hOgcPPxzEEPp1eLxIZqcXZ4vQFEWDSwrDdJwTzCe0>
- <https://www.cisa.gov/sites/default/files/2023-08/Secure-Our-World-Passwords-Tip-Sheet.pdf>
- <https://www.cisa.gov/secure-our-world/use-strong-passwords?fbclid=IwAR3zicRj4rBYL2JO35hOgcPPxzEEPp1eLxIZqcXZ4vQFEWDSwrDdJwTzCe0>

## Πρακτικές Συμβουλές – Ένα λάθος κλικ στοιχίζει



- **Χρησιμοποιούμε** λογισμικό προστασίας
- **Διατηρούμε** ενημερωμένο το λογισμικό.
- **Προσεκτικοί** κατά την περιήγησή μας,
- **Αποφεύγουμε** το κλικ σε ύποπτους συνδέσμους.



### 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=IwAR3zicRJ4rBYL2JO35hOgcPPxzEPPp1eLxIZqcXZ4vQFEWDSwrDdJwTzCe0>

## Πρακτικές Συμβουλές – Ένας κλεμμένος κωδικός στοιχίζει



ONE WRONG CLICK  
ONE FRAUDULENT CALL  
ONE STOLEN PASSWORD

THIS IS ALL IT TAKES TO BE  
**VICTIM OF  
CYBERCRIME**

- **Ορίζουμε** μοναδικούς κωδικούς πρόσβασης.
- Δημιουργούμε **ισχυρούς** κωδικούς.
- **Ενεργοποιούμε** τη λειτουργία ελέγχου ταυτότητας πολλαπλών παραγόντων.



retina scan



fingerprint



password

### 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>

# Προσωπικά δεδομένα (personal data)

**Ποιος τα κατέχει;**



**«Ό,τι είναι δικό μου»**

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



Cloud storage

# Δεδομένα προσωπικού χαρακτήρα (personal data)

«**κάθε πληροφορία** που αφορά **ταυτοποιημένο** ή **ταυτοποιήσιμο φυσικό πρόσωπο** («**υποκείμενο των δεδομένων**»),

**ταυτοποιήσιμο φυσικό πρόσωπο** είναι εκείνο του οποίου η ταυτότητα **μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως**

**όνομα, αριθμό ταυτότητας, δεδομένα θέσης, επιγραμμικό αναγνωριστικό ταυτότητας** ή έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική **ταυτότητα** του εν λόγω φυσικού προσώπου»



Location sharing

Άρθρο 4 περ. 1 του **Κανονισμού 2016/679/ΕΕ** και άρθρο 3 περ 1 **Οδηγίας 2016/680/ΕΕ** και άρθρο 43 παρ 1 περ. α του **N 4624/2019** (ΦΕΚ Α 137), όπως τροποποιήθηκε και ισχύει σήμερα

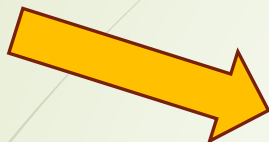


# Πως παραβιάζονται τα δεδομένα

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

Προσοχή με τα δεδομένα των **παιδιών** μας

# Τα Μαζικά Δεδομένα στο «Νέο Περιβάλλον»



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)			

## Το κόστος των διαρροών



### Πηγές:

- <https://cyber.gov.gr/antimetopisi-apeilon/systaseis-pros-polites/>
- <https://www.cima.ned.org/publication/big-data-not-big-brother>
- <https://www.dpa.gr/el/polites/gkpd>
- <https://www.coe.int/en/web/data-protection>
- [https://unsdg.un.org/sites/default/files/UNDG\\_BigData\\_final\\_web.pdf](https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf)
- <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>
- <https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection/?tab=publications>
- [https://edps.europa.eu/data-protection/data-protection\\_en](https://edps.europa.eu/data-protection/data-protection_en)
- <https://www.facebook.com/photo/?fbid=122202984878146486&set=a.122121627272146486>
- <https://www.ibm.com/reports/data-breach>
- <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/>

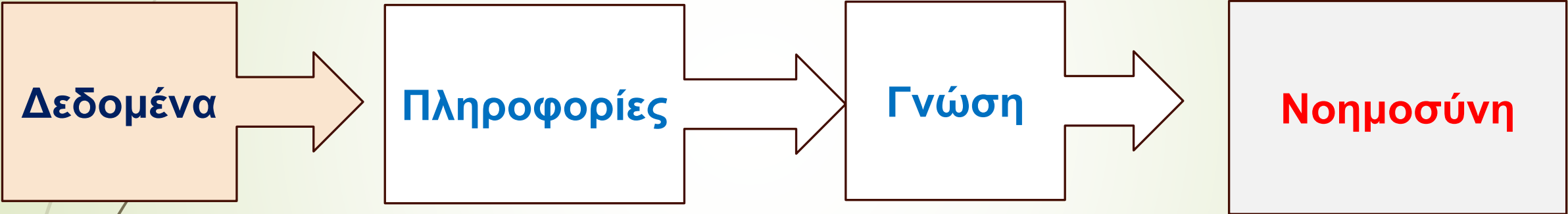




# Η αξία των δεδομένων

## DIKI or DIKW model

### Data -Information- Knowledge -Intelligence



**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](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

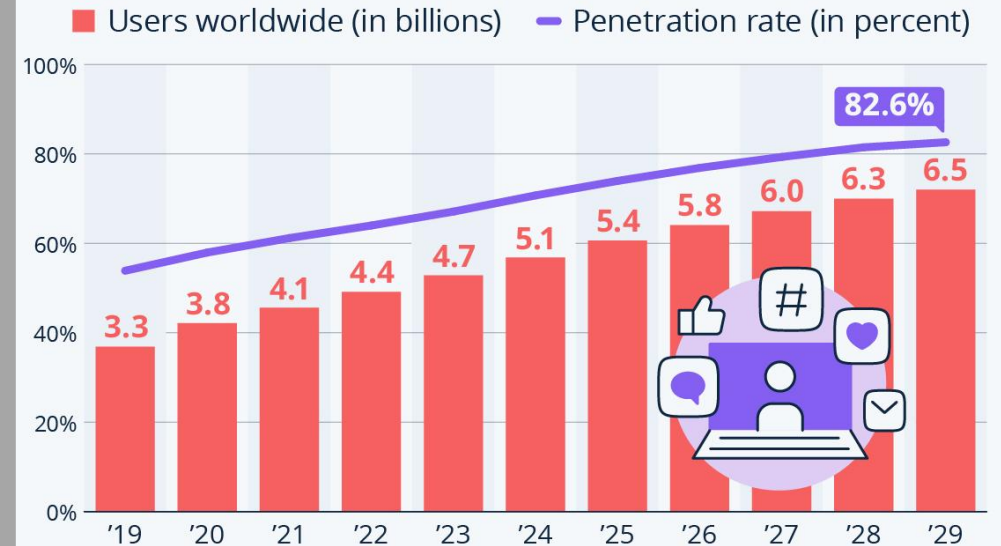
Ο επανακαθορισμός του μοντέλου ανθρωποκεντρικής χρήσης των τεχνολογιών έρχεται στο επίκεντρο της δημόσιας συζήτησης



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

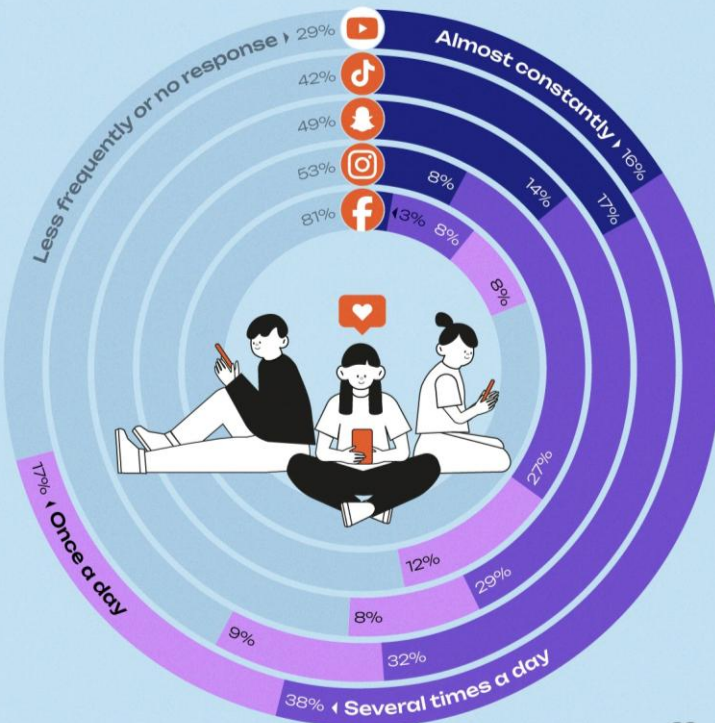
### Πηγές:

1. <https://www.dpa.gr/el/polites/prostasia>
2. <https://www.facebook.com/photo/?fbid=1243308608006506&set=a.561580072846033>
3. <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...

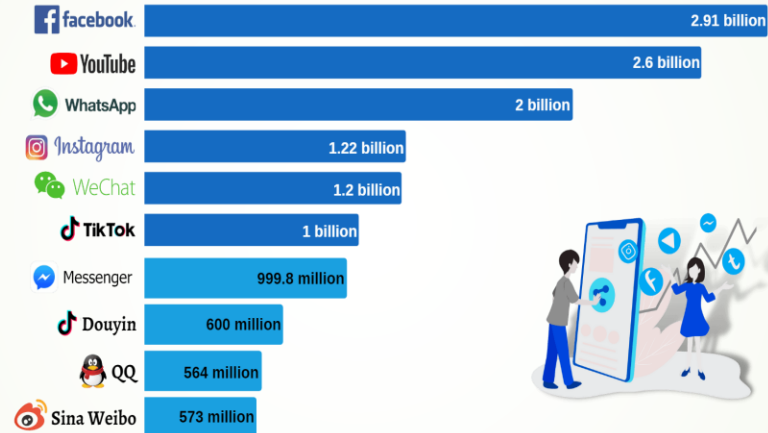


Source: Pew Research Center (2023)

voronoi Where Data Tells the Story

Download on the App Store GET IT ON Google Play

## Most Popular Social Platforms

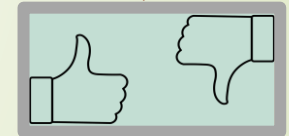


Number of monthly active users

Broadband Search



09/02/2009



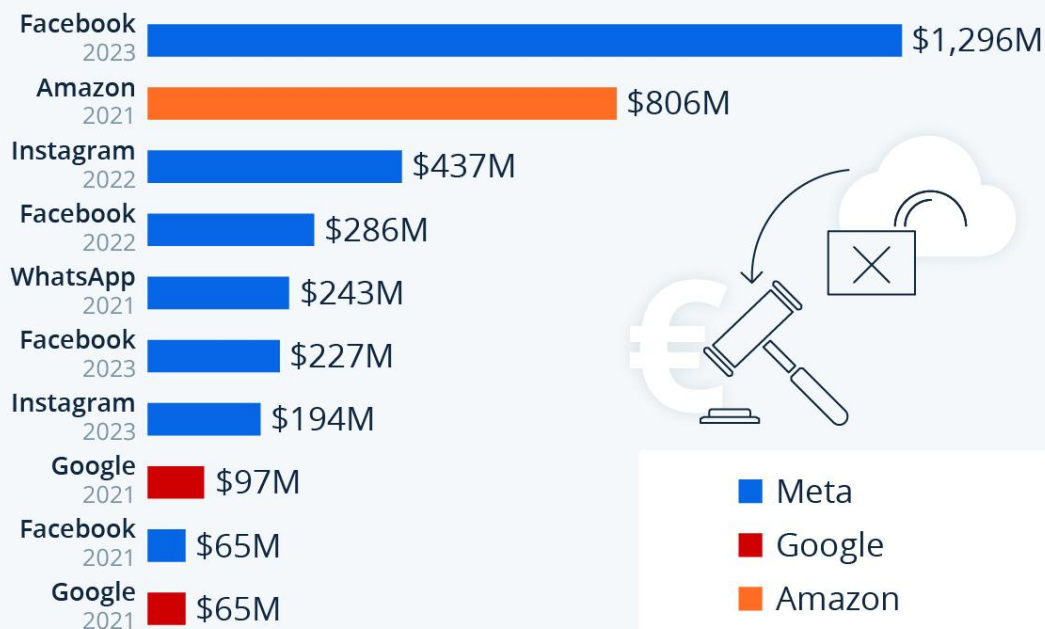
### Πηγές:

- <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=AQAAAHjAogdfUs5MX2xkxydv8nAa Sxh1gYdVW2la\\_YpxBQnv3X5hYg5TL7pe9boB--joVG9yXiGNnVwqKkD44nVm3qUYc-olMwfHj4pyYDd50Ay9O2Z7CBdRoDUiQzyJ1UJG6DoYhHAMxyh6C7OvdF1XTdBupwUD3FN8GTel07yTbr9a](https://techcrunch.com/2009/02/09/facebook-activates-like-button-friendfeed-tires-of-sincere-flattery/?guce_referrer=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAHjAogdfUs5MX2xkxydv8nAa Sxh1gYdVW2la_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>

# 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

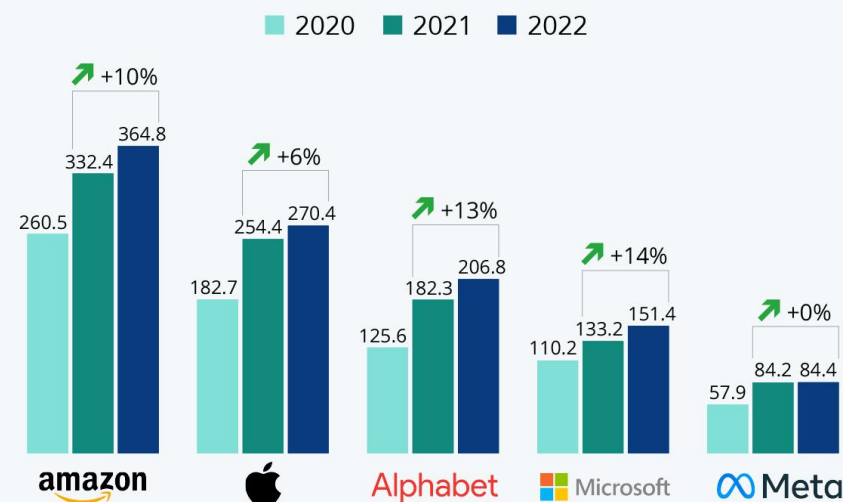
Sources: CMS GDPR Enforcement Tracker, European Data Protection Board



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

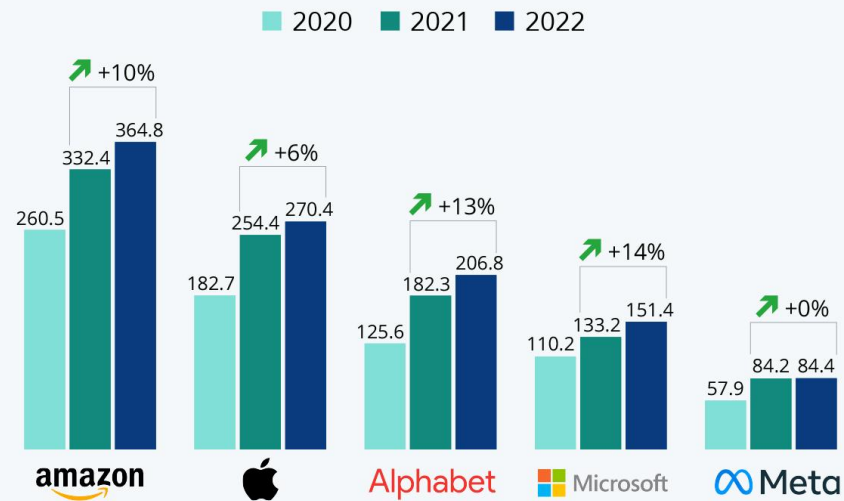
## Πηγές:

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

# «Νέος χρυσός» -Νέα Οικονομία – Έσοδα σε Trillions

## Is Big Tech Growth Losing Steam?

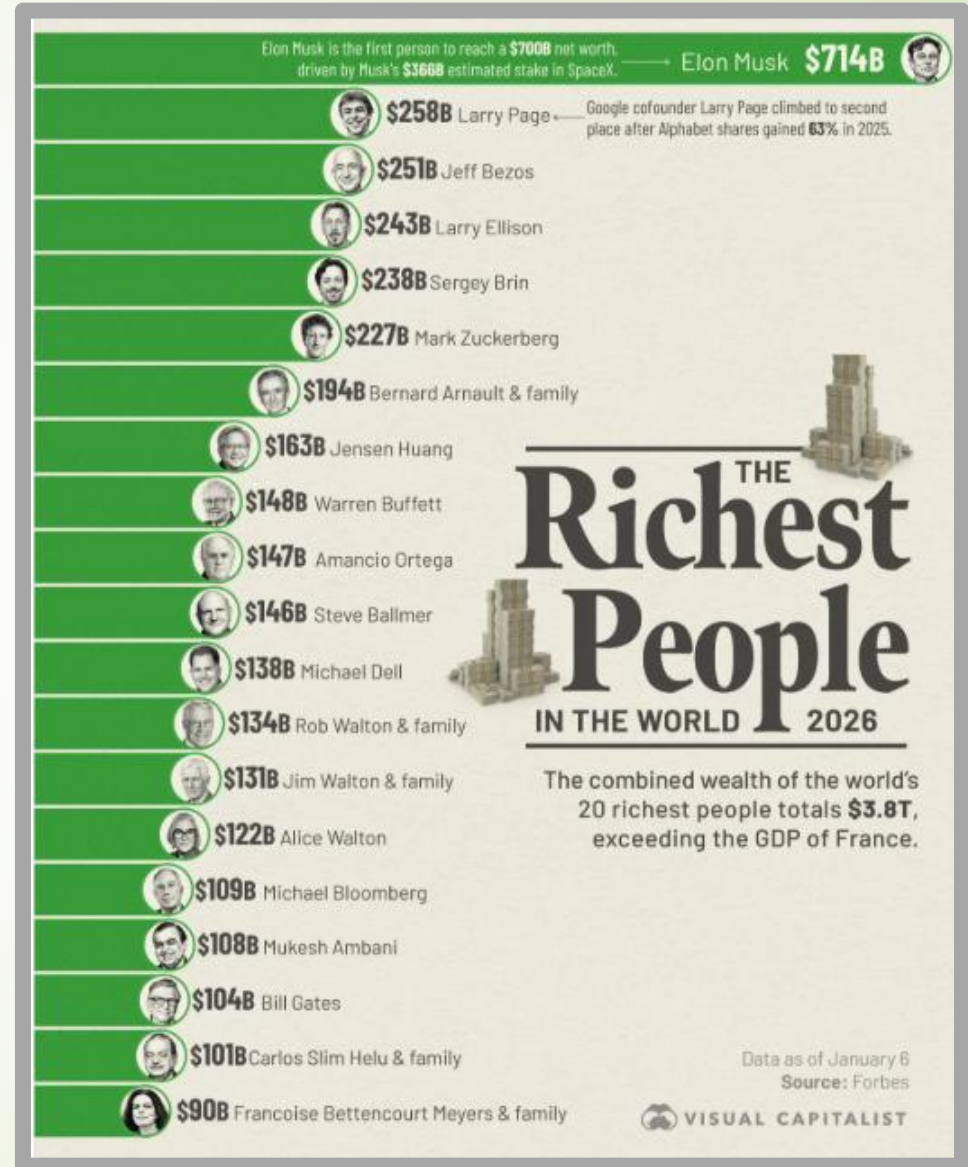
GAMAM revenue in the first nine months of the following years (in billion U.S. dollars)



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 πραγματοποιήσετε 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.

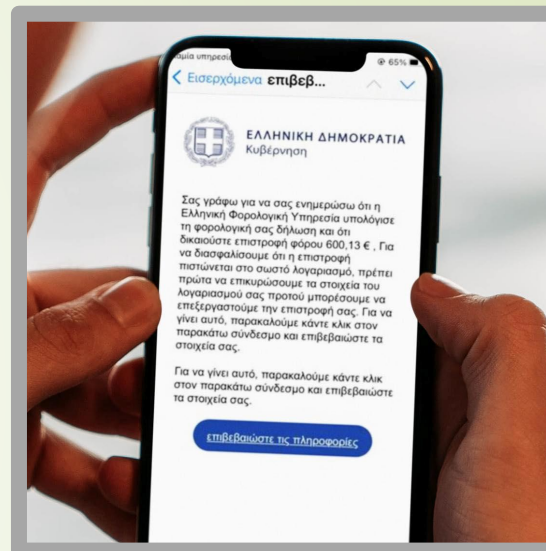
Το πακέτο σας θα αποθηκευτεί στο ΚΕΝΤΡΟ ΔΙΑΛΟΓΗΣ ΑΘΗΝΩΝ μέχρι να επιβεβαιώσετε τα στοιχεία σας:

Λεπτομέρειες

Με εκτίμηση,

ΕΛΤΑ.

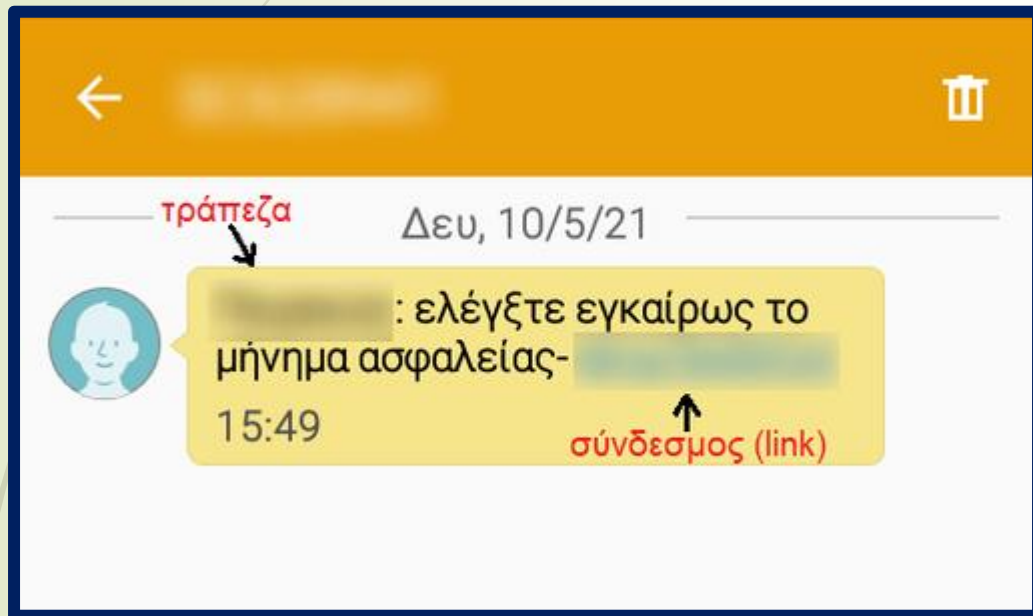
Unsubscribe



#### 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](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-epistimones/>
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

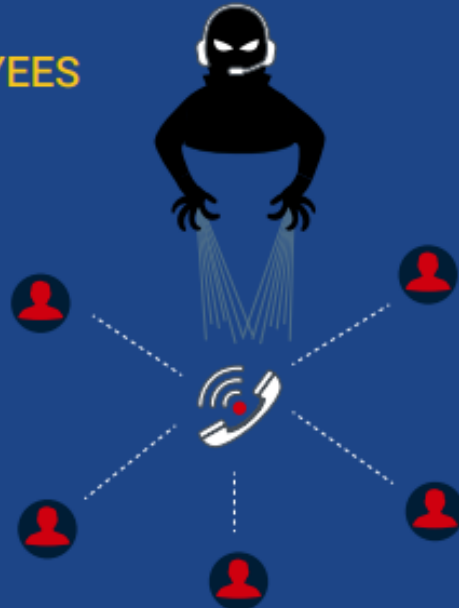
### Πηγές:

1. [https://www.europol.europa.eu/sites/default/files/documents/3\\_phishing\\_vishing\\_sms.pdf](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/>

# Αλίευση Δεδομένων -Vishing





## VISHING THE VOICE PHISHING SCAM ADVICE FOR CORPORATE EMPLOYEES

A fraudulent practice where verbal communication technology (e.g. VOIP or telephone) is used by an unauthorised entity pretending to be a reputable company. The aim is to manipulate individuals into revealing financial or personal information, or into providing unlawful access to their corporate networks.



EUROPOL  
EC3 | European Cybercrime  
Centre

### BE AWARE OF THE SCAM - HOW TO RECOGNISE THE CALL?

 <p>Generic greeting. The attacker rarely knows your name</p>	 <p>Sense of urgency due to different reasons: detected unsecure systems, bank account problems, package delivery, etc.</p>
 <p>Impersonation of a trusted third party, such as banks, technological or telecommunications companies, courier, etc.</p>	 <p>Reference to personal information available on public corporate websites or social media profiles</p>

Το vishing (συνδυασμός των λέξεων Voice και Phishing) είναι μια **τηλεφωνική απάτη** κατά την οποία απατεώνες προσπαθούν να σας εξαπατήσουν ώστε να αποκαλύψετε προσωπικά, οικονομικά ή εταιρικά στοιχεία ή να μεταφέρετε χρήματα

Γίνεται με *τεχνολογία φωνητικής επικοινωνίας* (π.χ. τηλεφωνικές κλήσεις ή VOIP) από *μη εξουσιοδοτημένα άτομα* που προσποιούνται αξιόπιστες εταιρείες.

### Πηγές:

1. [https://www.europol.europa.eu/cms/sites/default/files/documents/vishing\\_final\\_version.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/vishing_final_version.pdf)
2. [https://www.europol.europa.eu/cms/sites/default/files/documents/vishing\\_-\\_irsf\\_0.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/vishing_-_irsf_0.pdf)
3. <https://www.astynomia.gr/odigos-tou-politi/chrisimes-symvoules/symvoules-gia-asfali-prosvasi-sto-diadiktyo/>

# Αλίευση Δεδομένων -Quishing

What is a QR Code?

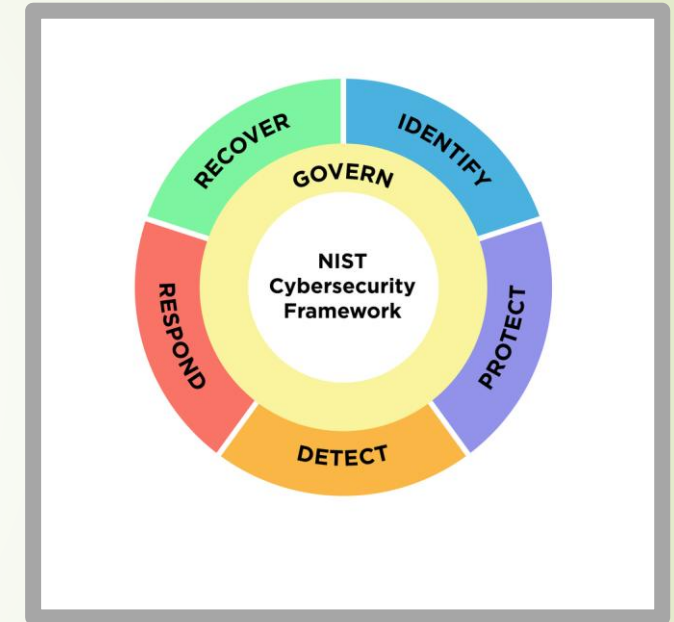
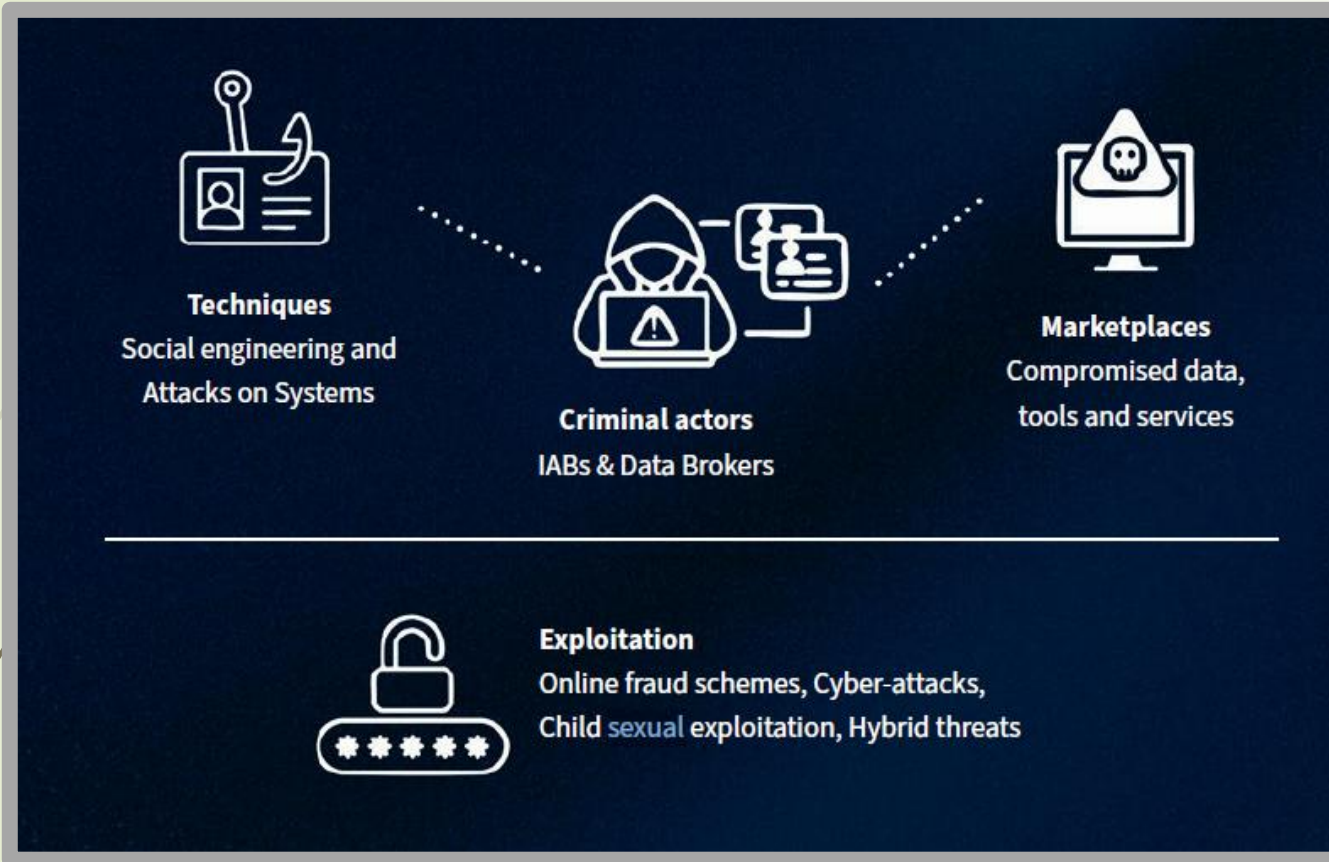


A screenshot of a phishing website for 'SAME DAY COURIER'. The page has a blue and white color scheme. It features a QR code on the left side, a 'Track your Parcel' section with input fields for 'Enter Phone Number' and 'Enter Address', and a 'Customs Charges Apply to your parcel' section. A red warning triangle with an exclamation mark and a skull and crossbones icon is overlaid on the right side of the page, with a 'BEWARE OF ME' sign below it.

Πηγές:

1. [https://www.ncsc.gov.ie/pdfs/Quick\\_Guide\\_QR\\_Code\\_Phishing\\_Scams.pdf](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](https://www.trendmicro.com/en_us/what-is/phishing/quishing.html)

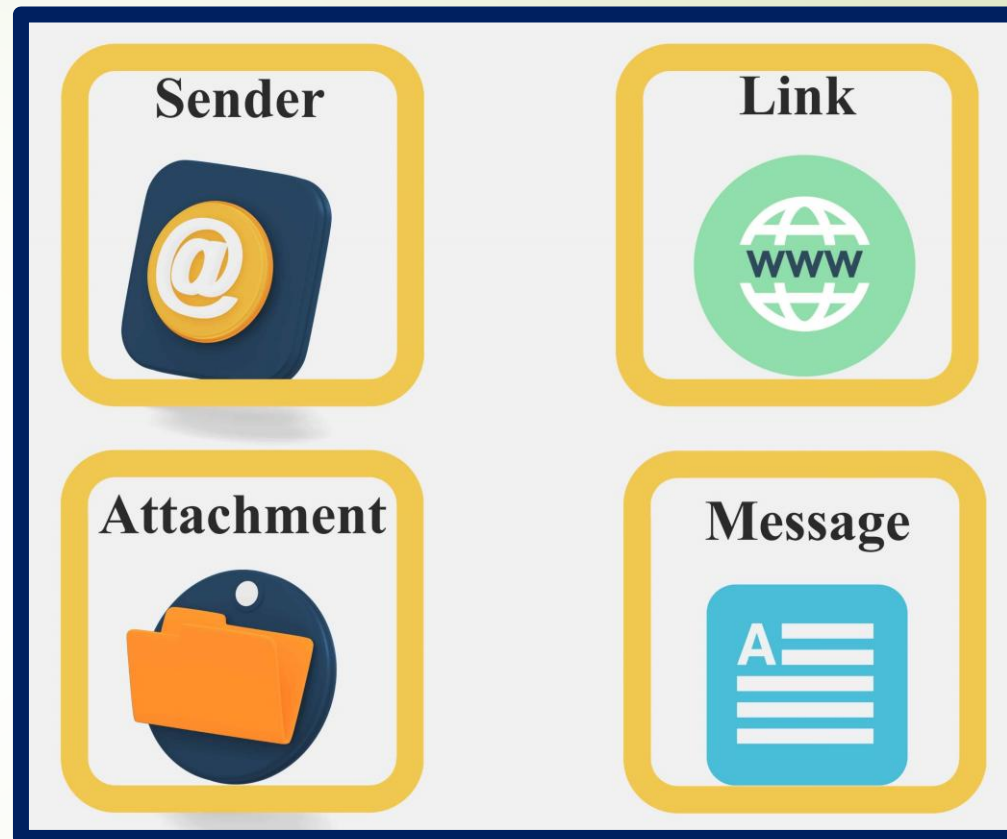
# Κακόβουλο Λογισμικό & Αλίευση Δεδομένων



## Πηγές:

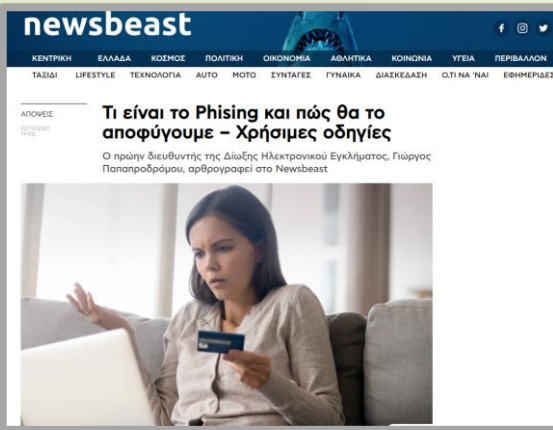
1. [https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA\\_2025.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf) p. 17
2. <https://encyclopedia.kaspersky.com/glossary/trojan-droppers/>
3. <https://www.nist.gov/image/nist-cybersecurity-framework-20-draft>
4. [https://www.cisa.gov/sites/default/files/2024-08/Federal\\_Government\\_Cybersecurity\\_Incident\\_and\\_Vulnerability\\_Response\\_Playbooks\\_508C.pdf](https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf) p. 12

# Αλίευση Δεδομένων- Μέθοδος SLAM



## 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.politica.gr/politica-89-8/g-papaprodromou-diarkis-epikairopoiisi-tis-atzentas-kubernoasfaleias-na-axiopoithoun-oi-neoi-epistimones/>
3. <https://www.facebook.com/hellenicpolice/posts/pfbid02btGBuuZe7nx7HTnSsWT8fNtZHfnpu4YAoqK74beG9Ys8rBwFFn7DgPfxkFogcHudl>



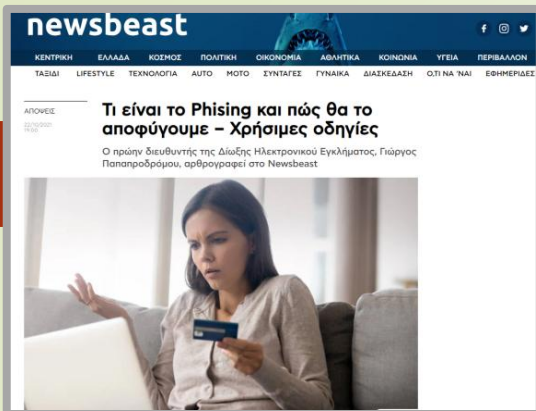
## Αλίευση Δεδομένων και πως θα την αποφύγουμε;

1

- Δεν δίνουμε** κωδικούς πρόσβασης από λογαριασμούς (τραπεζικούς κλπ)
- Δεν ακολουθούμε** συνδέσμους και **δεν ανοίγουμε** συνημμένα αρχεία από άγνωστους αποστολείς μηνυμάτων (ηλεκτρονικού ταχυδρομείου, sms)
- Χρήση** ασφαλέστερων κωδικών (*συνδυασμός γραμμάτων, αριθμών, συμβόλων*)

Πηγή:

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



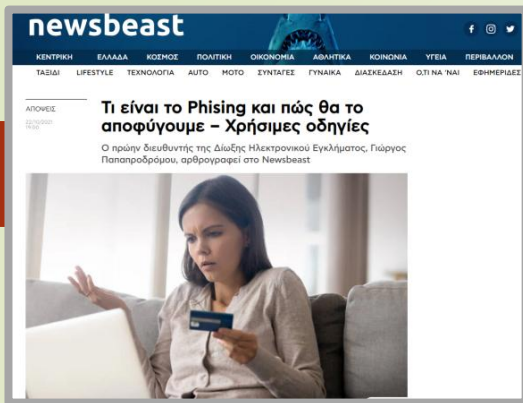
## Αλίευση Δεδομένων και πώς θα την αποφύγουμε;

2

- Αποφεύγουμε τον ίδιο κωδικό για κάθε λογαριασμό μας
- Αλλάζουμε κωδικό σε τακτά χρονικά διαστήματα
- Δεν δίνουμε τον αριθμό κινητού μας στα ΜΚΔ
- Επισκεπτόμαστε ασφαείς δικτυακούς τόπους

Πηγή:

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



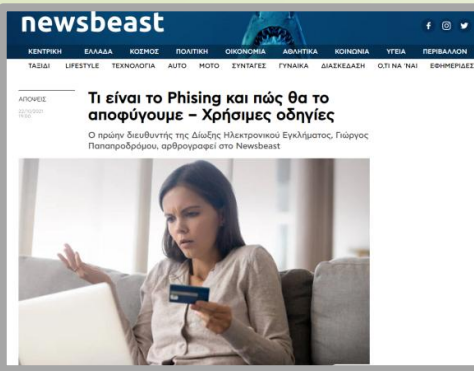
## Αλίευση Δεδομένων και πως θα την αποφύγουμε;

3

- Συντακτικά & ορθογραφικά λάθη** στα μηνύματα μας
- Επικαιροποιημένο λογισμικό** για τις συσκευές μας
- Παρακολουθούμε την **κίνηση του λογαριασμού** μας
- Παρακολουθούμε την **λειτουργία του κινητού** μας

Πηγή:

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



## Αλίευση Δεδομένων και πως θα την αποφύγουμε;

4

- ❑ **Αναφέρουμε** οπωσδήποτε οποιαδήποτε απόπειρα απάτης
- ❑ **Διαδικασία αμφισβήτησης συναλλαγής** τράπεζας μας  
(προσοχή το πρώτο εικοσιτετράωρο)
- ❑ **Συζητούμε** το θέμα με το άμεσο περιβάλλον μας και
- ❑ **Αναζητούμε βοήθεια**  
(*Η σιωπή βοηθά και ενθαρρύνει τους απατεώνες του Κυβερνοχώρου*)

Πηγή:

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

# Παιδιά θύματα κυβερνοεγκλημάτων

## Connected baby monitor



**1 in 3**  
**internet**  
**users is a child**  
How is the EU protecting them?

#DigitalEU #ChildrensDay

## 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](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>

International Edition

## **COVID-19** **Global** **ONLINE SAFETY** **ADVICE** **for parents** **and carers**



eSafety Commissioner

In collaboration with  
**EUROPOL**

[esafety.gov.au](mailto:esafety.gov.au)  
[europol.europa.eu](https://www.europol.europa.eu)



INTERPOL

THREATS AND TRENDS  
CHILD SEXUAL EXPLOITATION AND ABUSE

**COVID-19 IMPACT**

# Σεξουαλική Εκμετάλλευση Ανηλίκων (ΣΕΑ)



1. **Αύξηση** στη διακίνηση υλικού
2. Εγκατάσταση κακόβουλου λογισμικού και αλίευση δεδομένων
3. Αύξηση της **διαδικτυακής αποπλάνησης** στα ΜΚΔ και στις διαδικτυακές πλατφόρμες παιχνιδιών
4. Χρήση **κρυπτογραφημένων εφαρμογών** δυσχεραίνει το έργο των Αρχών Επιβολής του Νόμου -ΑΕΝ
5. Οι κυβερνοεγκληματίες του χώρου **εξελίσσονται** (χρήση TN)
6. Ο **σκοτεινός ιστός** εξακολουθεί να παραμένει σαν μια σημαντική πλατφόρμα για την ανταλλαγή υλικού ΣΕΑ
7. Αύξηση των περιπτώσεων ζωντανής μετάδοσης περιπτώσεων ΣΕΑ (LDCA-Live Distant Child Abuse)
8. Εμπορευματοποίηση της διαδικτυακής ΣΕΑ

IOCTA 2026 p. 8, 15, 27, 31-36



## Πηγές:

1. <https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf>
2. <https://www.eurojust.europa.eu/term/crimes-against-children>
3. <https://www.coe.int/en/web/children/lanzarote-convention>

# 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%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](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%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\\_%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](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>

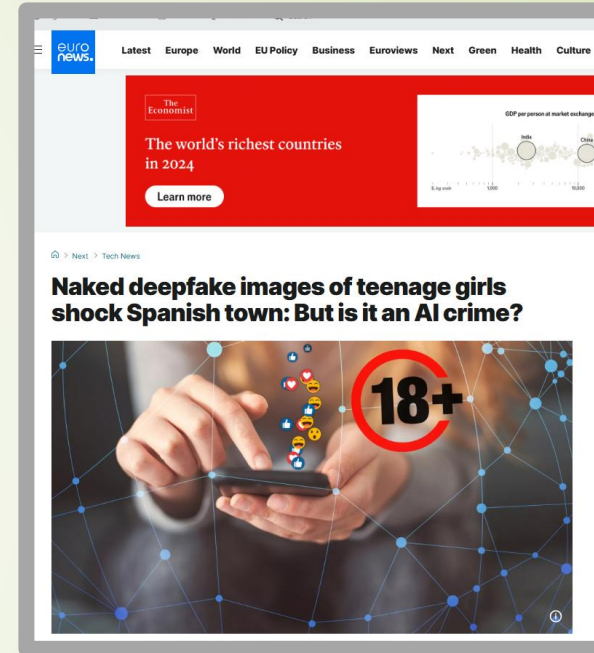
# Εκφοβισμός στον Κυβερνοχώρο (Cyber-Bullying)



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

Ο όρος «**κυβερνοεκφοβισμός**» αναφέρεται σε συμπεριφορές που εκδηλώνονται μέσω ψηφιακών τεχνολογιών, με πρωταρχικό σκοπό ή αποτέλεσμα την επαναλαμβανόμενη ή συνεχή **ταπείνωση**, κοινωνική απομόνωση, **κακοποίηση**, **παρενόχληση** ή βλάβη, ιδίως σε παιδιά ή νέους

ΕΕ, 10-02-2026, Action plan against cyberbullying "Safer online, stronger together" p. 3



## 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](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.jmir.org/2025/1/e70508>
7. <https://digital-strategy.ec.europa.eu/en/library/action-plan-against-cyberbullying>
8. <https://www.euronews.com/next/2023/09/24/spanish-teens-received-deepfake-ai-nudes-of-themselves-but-is-it-a-crime>

# Εκφοβισμός στο Σχολικό Περιβάλλον Νέα πλατφόρμα

The screenshot shows the website interface for reporting an incident. The main navigation bar includes 'bullying', 'govgr', and several menu items: 'Αρχική', 'Νέα', 'Για γονείς/κηδεμόνες', 'Για μαθητές/τριες', and 'Για εκπαιδευτικούς και υπηρεσίες της εκπαίδευσης'. A red button labeled 'ΑΝΑΦΟΡΑ ΠΕΡΙΣΤΑΤΙΚΟΥ' is prominently displayed. Below the navigation, the article title 'Το Σπίτι των Παιδιών – Πρόληψη Επιθετικότητας και Σχολικού Εκφοβισμού' is visible, along with the date '17 Νοεμβρίου, 2023'. On the right side, there is a search bar labeled 'Αναζήτηση' with a yellow arrow pointing to it, and a 'Αρχείο' (Archive) section listing months from February 2024 to November 2023. Below the archive, there is an 'Ετικέτες' (Tags) section with categories like 'Ανθρώπινα Δικαιώματα (9)', 'Γυμνάσιο (38)', 'Δημοτικό (48)', 'Διαδραστικός Εκφοβισμός (4)', and 'Διαμεσολάβηση/Επίλυση Συγκρούσεων (11)'.

## Δυνατότητα Αναφοράς Περιστατικού

### Ενημερωτικό υλικό για

- Μαθητές/τριες
- Γονείς/Κηδεμόνες
- Εκπαιδευτικούς

[ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 5029/2023 – «Ζούμε Αρμονικά Μαζί – Σπάμε τη Σιωπή»: Ρυθμίσεις για την πρόληψη και αντιμετώπιση της βίας και του εκφοβισμού στα σχολεία και άλλες διατάξεις](#)

### Πηγές:

1. <https://stop-bullying.gov.gr/>
2. <https://stop-bullying.gov.gr/institutional-framework>
3. <https://www.astynomia.gr/odigos-tou-politi/chrisimes-symvoules/scholikos-ekfovismos-schoolbullying-i-ekfovismos-bullying/an-eisai-goneas/>

Η εφαρμογή **SAFE.YOUTH** περιλαμβάνει τις εξής λειτουργίες:

- Emergency Button
- Υποβολή **καταγγελίας** μέσω του **gov.gr**
- Επικοινωνία με τη Διεύθυνση Άμεσης Δράσης Αττικής "100"
- Επικοινωνία με τη Γραμμή Καταγγελιών για ανηλίκους "10201"
- Ενημερωτικό υλικό

**Emergency Button** είναι ένα **εργαλείο** το οποίο χρησιμοποιείται σε περιπτώσεις κινδύνου ζωής. Ενεργοποιώντας το κουμπί ειδοποιείται και **παρεμβαίνει άμεσα η Ελληνική Αστυνομία** για την παροχή βοήθειας.

Απαιτείται η **προσυμπλήρωση μίας φόρμας με προσωπικά στοιχεία του ανηλίκου (προεγγραφή)** για να ενεργοποιηθεί ως δυνατότητα, εντός της εφαρμογής.



### Πηγές:

1. <https://www.safeyouth.gov.gr/>
2. <https://www.safeyouth.gov.gr/oroi-chrisis>
3. <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/>

# Νέα Πλατφόρμα Parco - Kids Wallet app



The screenshot shows the top navigation bar of the Parco website. On the left is the "parental control" logo with a shield icon, and on the right is the "govgr" logo with the Greek flag. Below the navigation bar are links for "Αρχική", "Δυνατότητες", "Οδηγίες για συσκευές Android", "Οδηγίες για συσκευές iOS", and "Συχνές Ερωτήσεις". The main banner features a young boy lying in bed, looking at a smartphone. The text on the banner reads: "Τώρα, έχετε τον έλεγχο! Δημιουργήστε ένα ασφαλές ψηφιακό περιβάλλον."

The screenshot shows an advertisement for the Kids Wallet app. It features the "KIDS wallet" logo in the top left corner and a "Οδηγίες χρήσης" link in the top right. The main text says "Ας πάρουμε τον έλεγχο στα χέρια μας!". Below this are the "Download on the App Store" and "GET IT ON Google Play" buttons. On the right, a smartphone displays the app's interface, which includes the "govgr KIDS wallet" logo and a button that says "Εισαγωγή με αριθμό κάρτας Τετάρτης".

## 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/>
4. <https://kidswallet.gov.gr/ios.pdf>
5. <https://kidswallet.gov.gr/android.pdf>

# 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

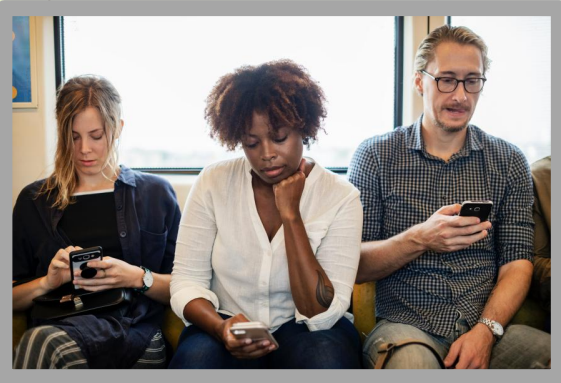
## Πηγές

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>



World Health  
Organization

# Το ατέλειωτο σκρολάρισμα στοιχίζει στην υγεία μας



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>

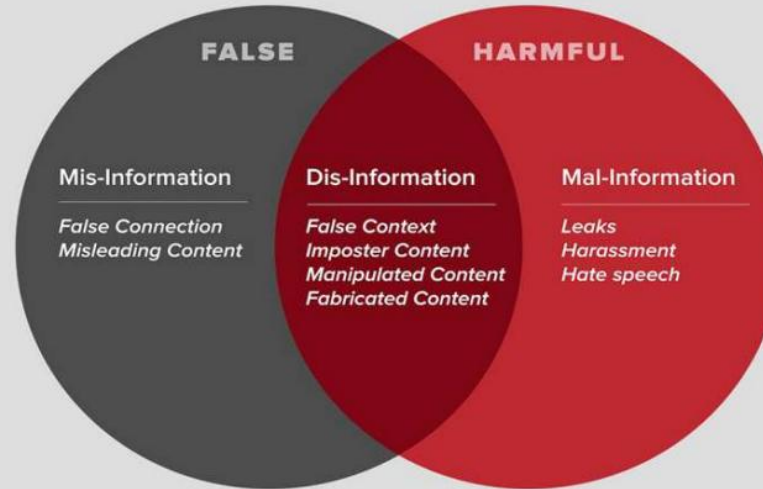
# Απρεπής εκφορά του λόγου & Παραπληροφόρηση

Online hate speech doesn't just stay online



#NoToHate

## INFORMATION DISORDER



## Code of Practice on Disinformation

Transparency Centre



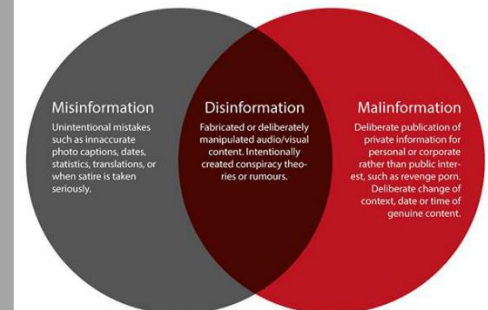
#DigitalEU

## 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](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](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>

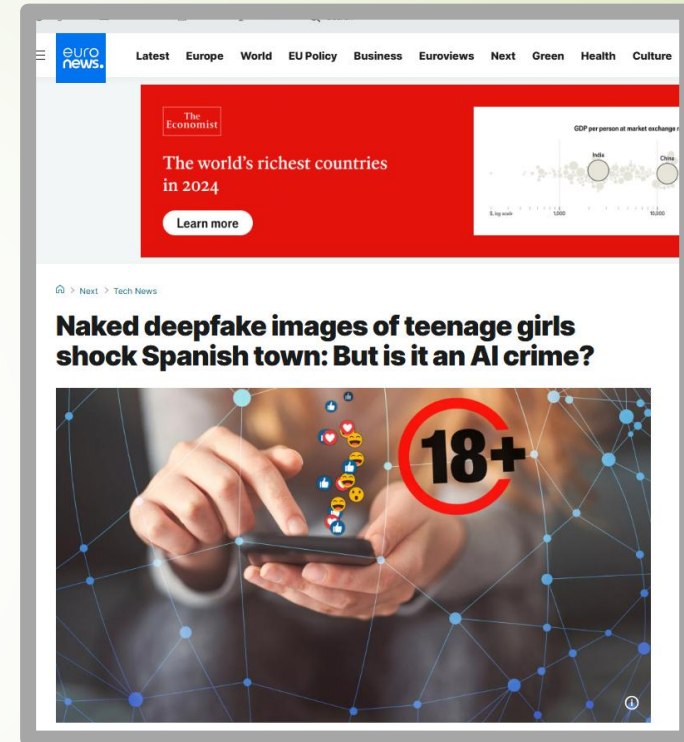
## TYPES OF INFORMATION DISORDER

FALSENESS      INTENT TO HARM



# TN και Deepfakes

REAL  
OR  
AI?



## Πηγές:

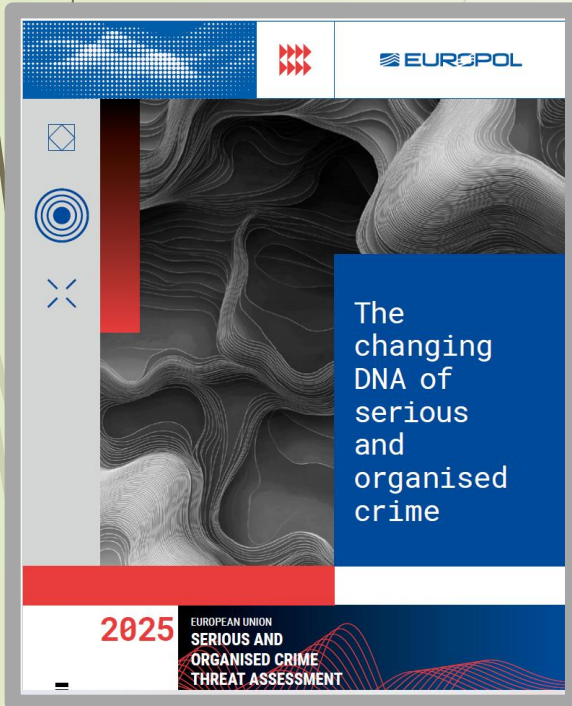
1. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-second-draft-code-practice-marking-and-labelling-ai-generated-content>
2. <https://www.euronews.com/next/2023/09/24/spanish-teens-received-deepfake-ai-nudes-of-themselves-but-is-it-a-crime>
3. <https://www.europol.europa.eu/media-press/europol-podcast/episode-21-how-crime-is-accelerated-by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



# Εκστρατείες παραπληροφόρησης

Δίκτυα διαδραματίζουν καθοριστικό ρόλο στην **προπαγάνδα** με σκοπό την διάδοση παραπληροφόρησης και τον επηρεασμό των πολιτικών συστημάτων.

Οι εκστρατείες συχνά περιλαμβάνουν **ψεύτικους λογαριασμούς** στα **ΜΚΔ**, επιχειρήσεις **τρολ** και **παραποιημένο περιεχόμενο** ειδήσεων, εξυπηρετώντας τα στρατηγικά συμφέροντα των **υβριδικών απειλών**, αποδυναμώνοντας τους αντιπάλους από μέσα.



## Χειραγωγούν και υποκινούν τη βία

Δημοσιεύθηκε **20/03/2025**

**Πηγές:**

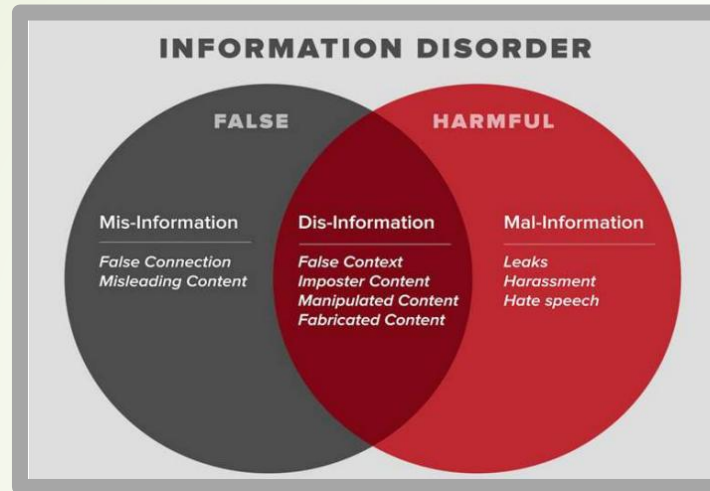
1. <https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime>
2. <https://www.consilium.europa.eu/en/policies/hybrid-threats/>
3. <https://www.hybridcoe.fi/hybrid-threats/>

# Fake news & 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?

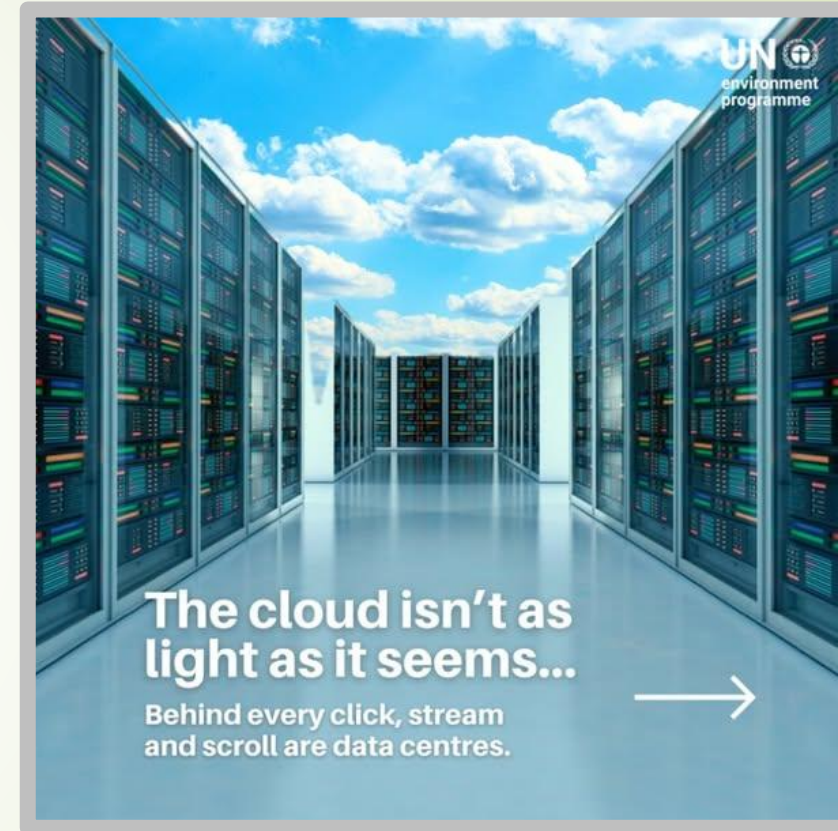
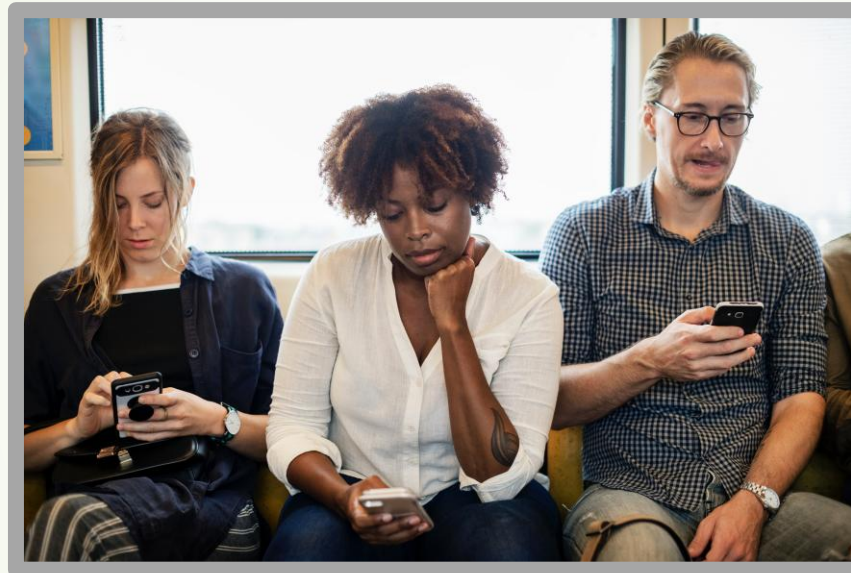
### Πηγές

- <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://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](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>



# Τεχνολογία – Μαζικά δεδομένα & Περιβάλλον: Ορθολογική χρήση των διαθέσιμων πόρων

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



EPA

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



[www.epa.gov/recycle](http://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](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/>
6. <https://www.unep.org/resources/toolkits-manuals-and-guides/sustainable-procurement-guidelines-data-centres-and-servers>

# Μετατόπιση της παράνομης αγοράς στο ψηφιακό περιβάλλον

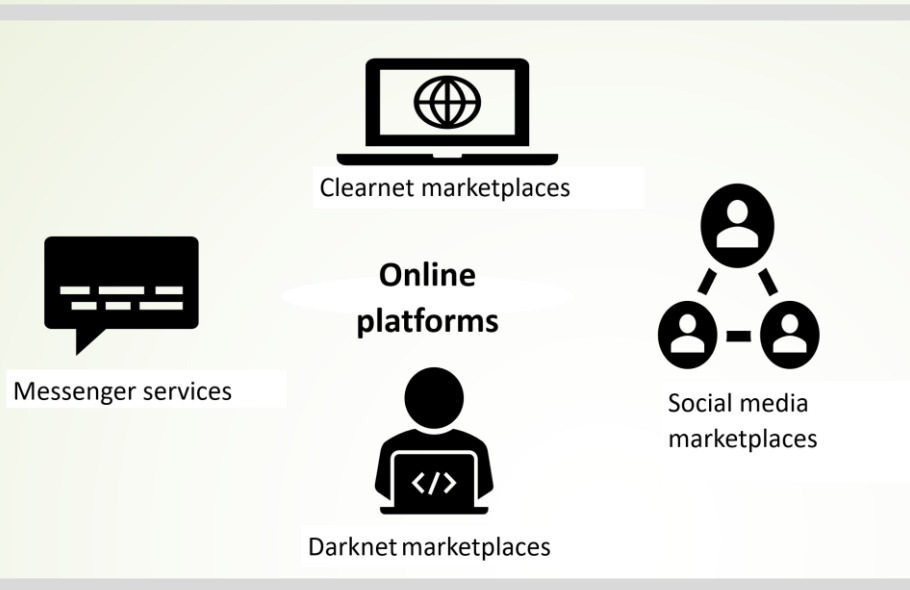
## European Drug Report 2025

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://v.vv.vev.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)

# Ναρκωτικά στον Κυβερνοχώρο

*Το σύγχρονο οργανωμένο έγκλημα «αξιοποιεί»  
τον Κυβερνοχώρο 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.

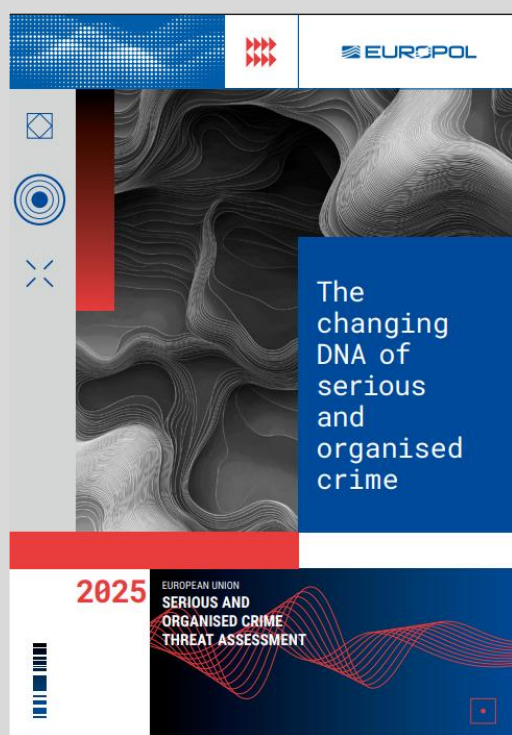
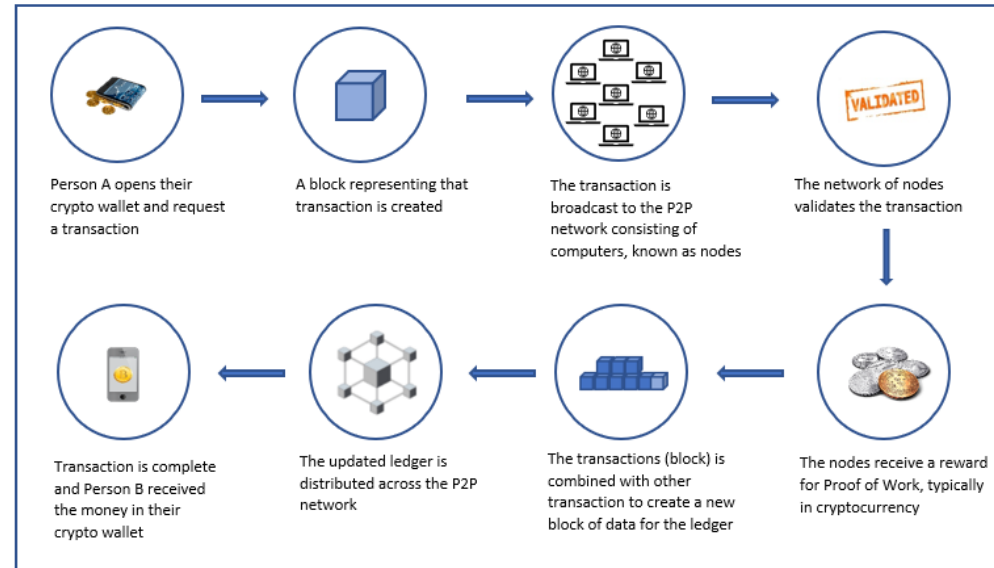
Παραγωγή  
Μεταφορά  
Πώληση  
Πληρωμές  
Ξέπλυμα



# Υπονόμευση των Κοινωνιών από το οργανωμένο έγκλημα



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-publications/europeandrugreport/2023\\_en](https://www.emcdda.europa.eu/publications/european-publications/europeandrugreport/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/onlinetrafficking/payment/index.html>
9. [https://www.euda.europa.eu/publications/european-drug-report/2025\\_en#pdf](https://www.euda.europa.eu/publications/european-drug-report/2025_en#pdf) p.14-15
10. Eric Schmidt, Jared Cohen, Η Νέα Ψηφιακή Εποχή, 2014, Εκδόσεις Δίαυλος, σελ. 208, 216

# Κίνδυνοι και απειλές όχι μόνο από τα φάρμακα

## EU Drug Markets Analysis | 2024

Key insights for policy and practice



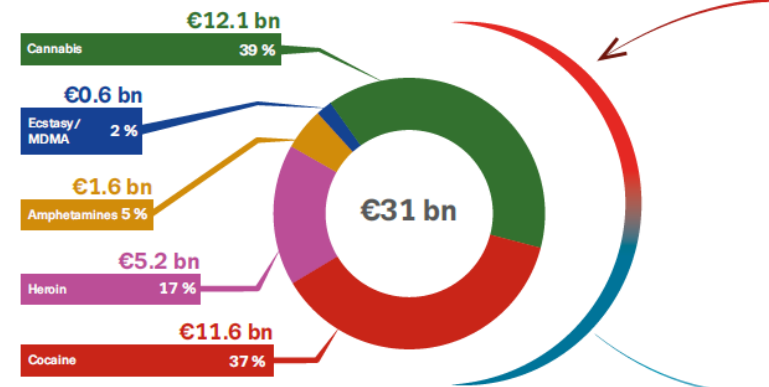
### THE MEDICRIME CONVENTION IN 10 QUESTIONS AND ANSWERS

The Council of Europe Convention  
on the Counterfeiting of Medical Products and  
Similar Crimes Involving Threats to Public Health



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.

FIGURE 1  
EU drug markets ecosystem



ΕΕ 2021, ελάχιστη λιανική αξία  
31 δις €

### Πηγές:

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

# Τεράστια χρηματικά ποσά γύρω από τα ναρκωτικά



## 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	4.5 billion	337.5 million
	Methamphetamine	2.8 billion	
	Heroin	4.8 billion	
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
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	

Πηγή

[https://www.unodc.org/documents/data-and-analysis/WDR\\_2025/WDR25\\_B1\\_Key\\_findings.pdf](https://www.unodc.org/documents/data-and-analysis/WDR_2025/WDR25_B1_Key_findings.pdf)

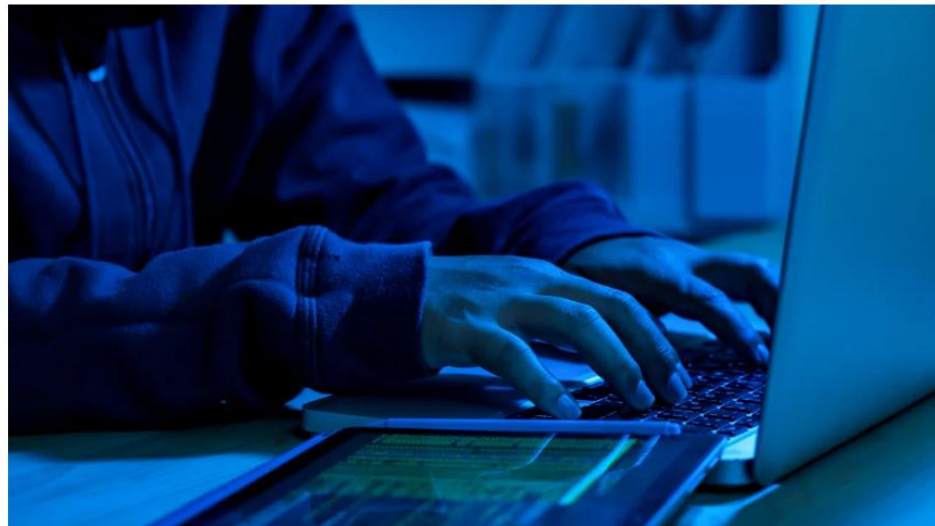
# Επιγραμμικές απάτες – Online Frauds

## 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

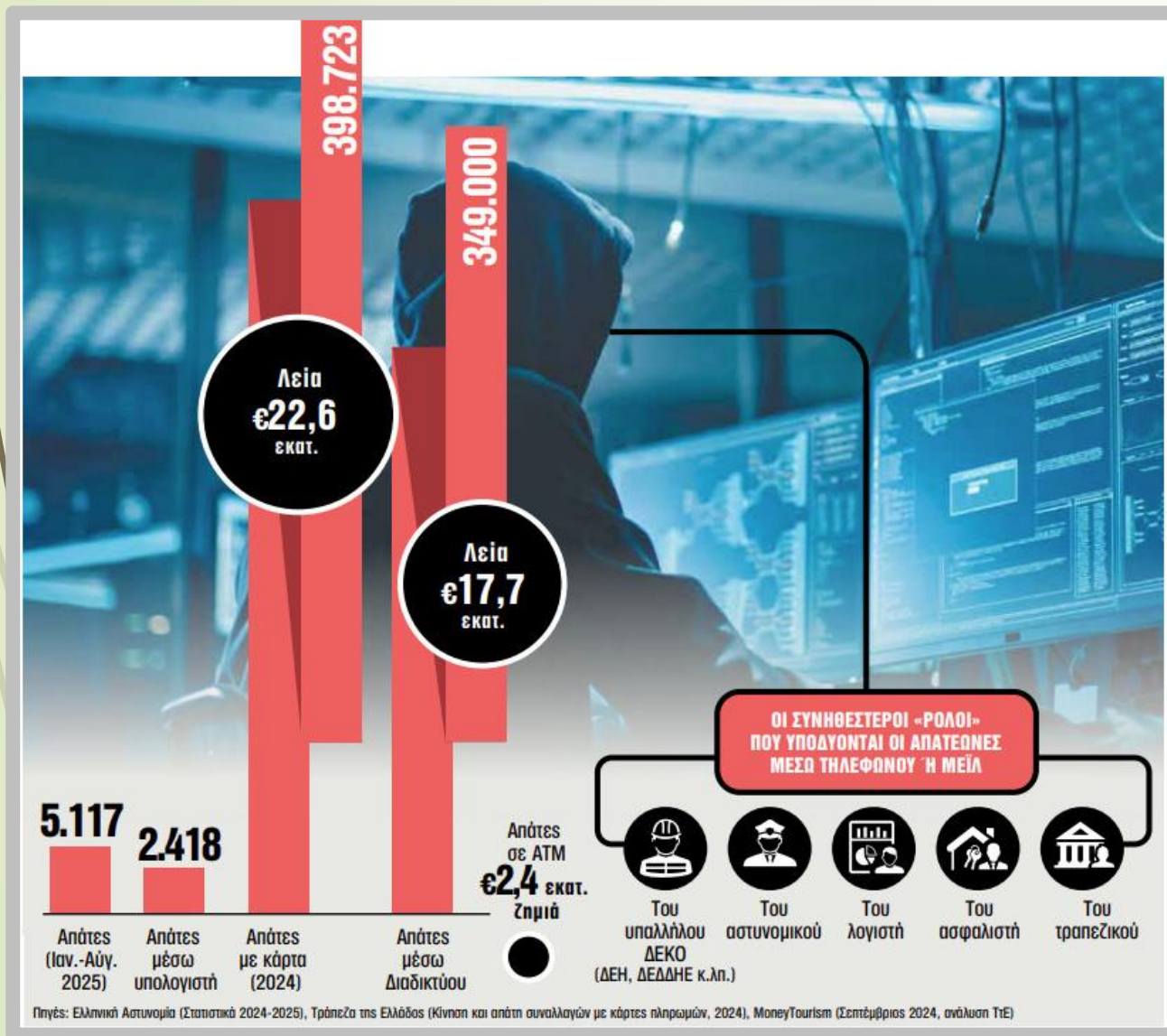
**Αποζημίωση** θυμάτων κυβερνοαπάτης υπό προϋποθέσεις



## Πηγές:

1. [https://www.europol.europa.eu/cms/sites/default/files/documents/infographic\\_-\\_pcf\\_prevention\\_alert\\_0.pdf](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 στην Ελλάδα



Πηγές

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

# 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.



They require an urgent payment.



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

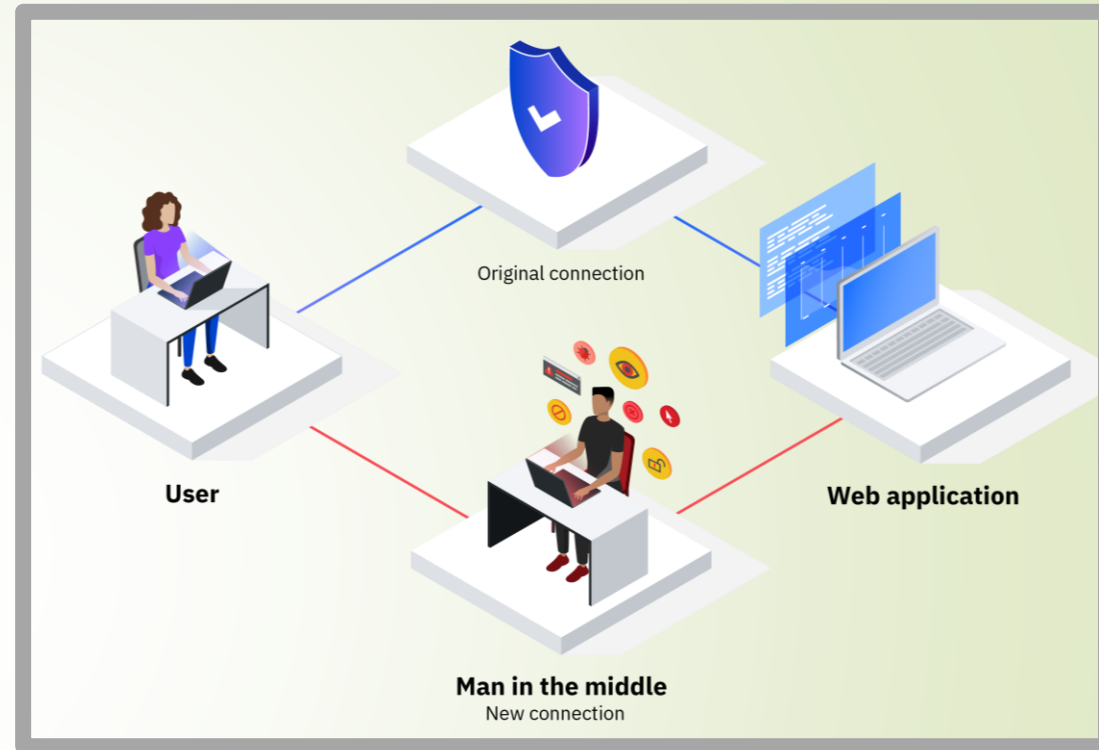


They refer to a sensitive situation (e.g tax control, merger, acquisition).

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](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](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](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>

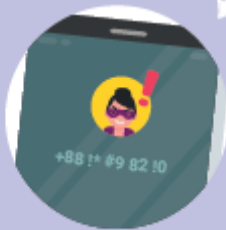
# Απάτες Τεχνικής Υποστήριξης – Tech Support Scams

## How to recognise tech support scams



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.



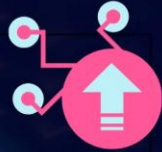
Cybercrook Brooke has now access to your bank account and can perform fraudulent transactions.

## 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](https://www.europol.europa.eu/cms/sites/default/files/documents/tech_support_scam_en.pdf)

# 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](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](https://www.ecb.europa.eu/press/economic-bulletin/articles/2019/html/ecb.ebart201905_03~c83aeaa44c.en.html)

# 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](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](https://www.youtube.com/watch?v=HIfGsQ_MkIU)

# 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**

INTERPOL



- 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=IwY2xjawKIUB1leHRuA2FibQIxBQbicmlkETBaVzImbWJCejdQXJ5UkQwAR7IJBmyoK0G5\\_AkG0\\_6HJ9\\_su5KQWOfYihaNhCQalwZlyHwzb0Z8tg0x\\_FuuQ\\_aem\\_rzsBtRSvS3RMd\\_mOyD9uwA](https://www.messinialive.gr/eksarthrothikan-dyo-speires-pou-arpaksan-630-000-evro-eksapatontas-polites-120-peristatika-thymata-kai-stin-kalamata/?fbclid=IwY2xjawKIUB1leHRuA2FibQIxBQbicmlkETBaVzImbWJCejdQXJ5UkQwAR7IJBmyoK0G5_AkG0_6HJ9_su5KQWOfYihaNhCQalwZlyHwzb0Z8tg0x_FuuQ_aem_rzsBtRSvS3RMd_mOyD9uwA)

# 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...

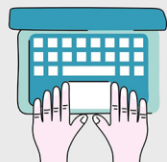
...σε ύποπτα e-mail, sms, κλήσεις και σε **καμία περίπτωση** δεν ακολουθώ links / QR codes καθώς και **δεν ανοίγω συνημμένα αρχεία**.

### 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 χρησιμοποιούμενους 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, ΕΛΤΑ, 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 Εγκλημάτων) 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=IwY2xjawlr0hFleHRuA2FibQlxMAABHSFZ0ZDekJpQNV1cljHeK8vp6RgpOUhxhbSLssHhZwOF8qVL0ZpM8Z2Ax-Q\\_aem\\_LUDM7nsjferXu2jXRt366A#/lessons/in\\_swfHmFJVomcam6z8GDKZikD\\_f1Qq-](https://museum.bankofgreece.gr/personalfinance/?fbclid=IwY2xjawlr0hFleHRuA2FibQlxMAABHSFZ0ZDekJpQNV1cljHeK8vp6RgpOUhxhbSLssHhZwOF8qVL0ZpM8Z2Ax-Q_aem_LUDM7nsjferXu2jXRt366A#/lessons/in_swfHmFJVomcam6z8GDKZikD_f1Qq-)

# 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](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%BFCF%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>

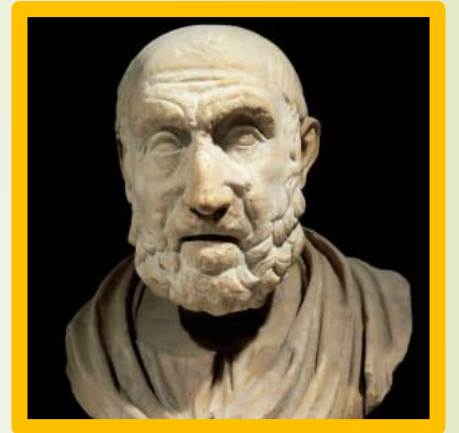
- Προτιμούμε την πληρωμή με αντικαταβολή.
- Γνωρίζουμε για το βασικό μας δικαίωμα υπαναχώρησης
- (επιστροφή αγορασθέντος προϊόντος εντός 14 ημερών από την αγορά)
- που εφαρμόζεται σε όλα τα εμπορικά καταστήματα (είτε φυσικά είτε διαδικτυακά).
- Δεν στέλνουμε τον αριθμό της κάρτας μας, το PIN ή οποιαδήποτε 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<sup>ο</sup> αιώνα – Ο ρόλος της Εκπαίδευσης

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

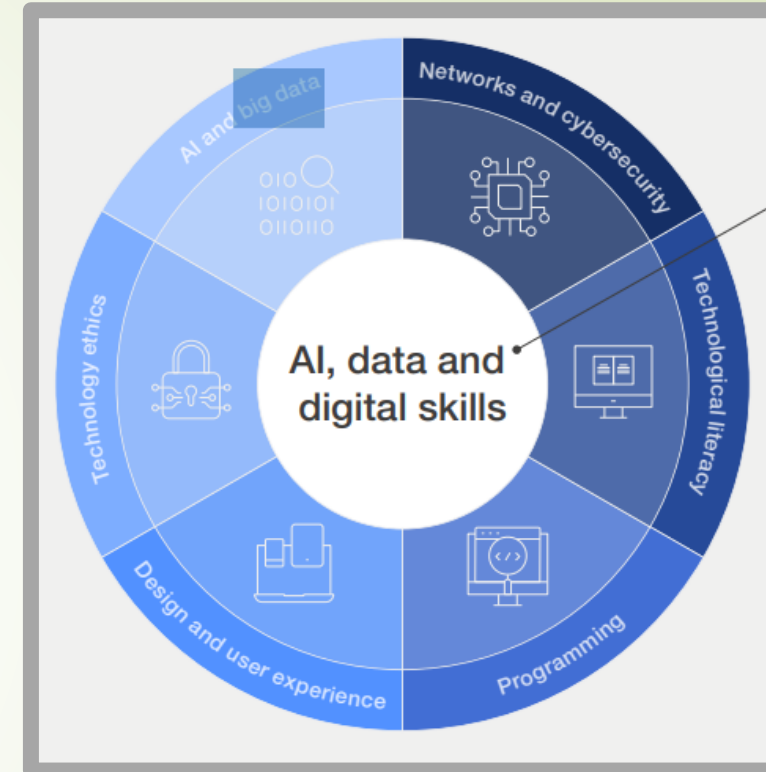
**Competencies**  
How students approach complex challenges

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](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](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](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=IwAR0eotl20OijEF4TyAfzDuKMuyiJ2ihlvqQ9yYci32Oai61QSyxNSo7Xad8> 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



## Future of Jobs Report 2025

INSIGHT REPORT  
JANUARY 2025

WORLD  
ECONOMIC  
FORUM



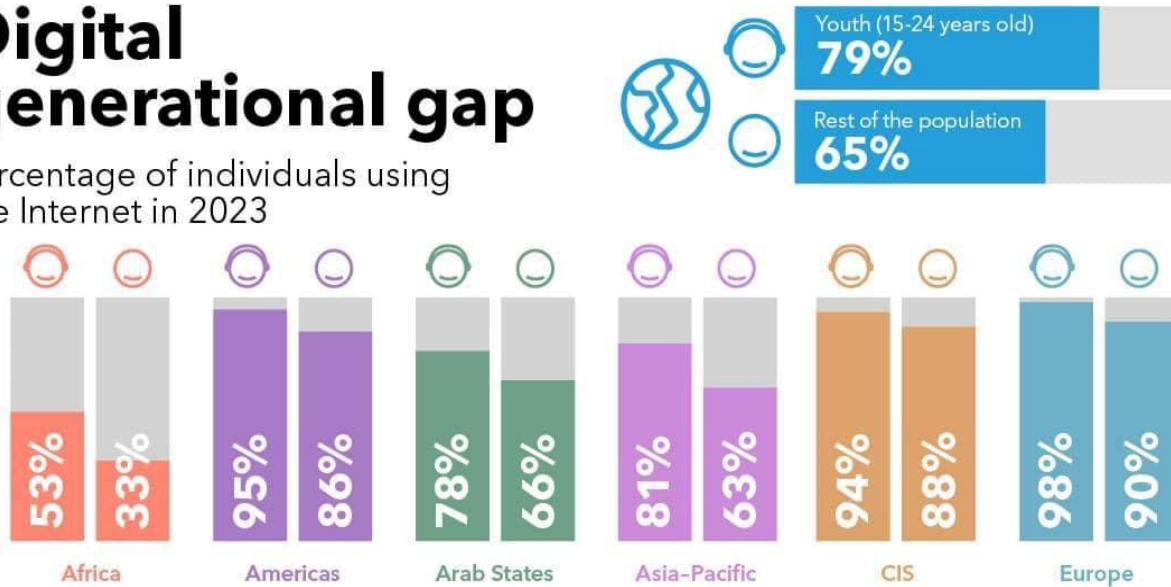
### Πηγές:

1. [https://reports.weforum.org/docs/WEF\\_Future\\_of\\_Jobs\\_Report\\_2025.pdf](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](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](https://www.cedefop.europa.eu/files/3098_en.pdf)

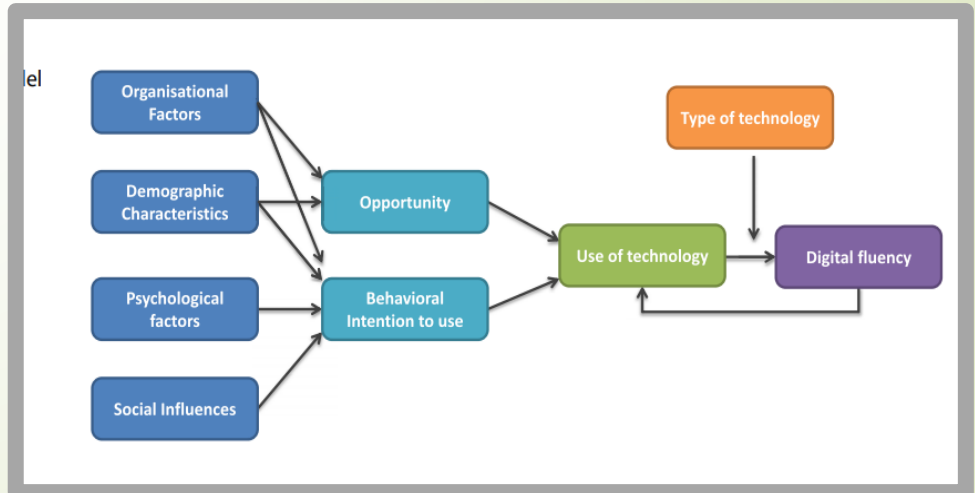
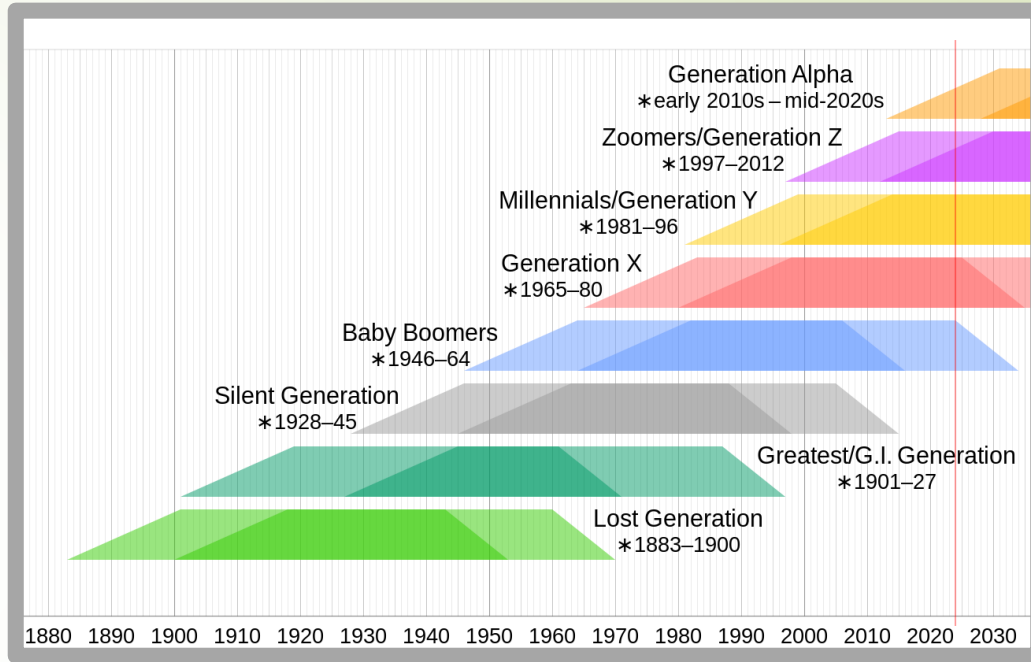
# Ψηφιακό Χάσμα Γενεών

## Digital generational gap

Percentage of individuals using the Internet in 2023



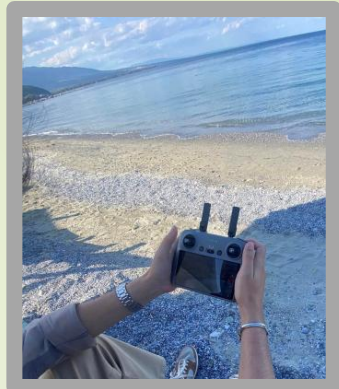
Source : ITU, Facts and Figures 2023  
Note: ITU-D regions



### Πηγές:

- <https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-youth-internet-use/>
- <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1254&context=bise>
- [https://en.wikipedia.org/wiki/Baby\\_boomers#/media/File:Generation\\_timeline.svg](https://en.wikipedia.org/wiki/Baby_boomers#/media/File:Generation_timeline.svg)

# Νέα επαγγέλματα - νέες προοπτικές



**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**

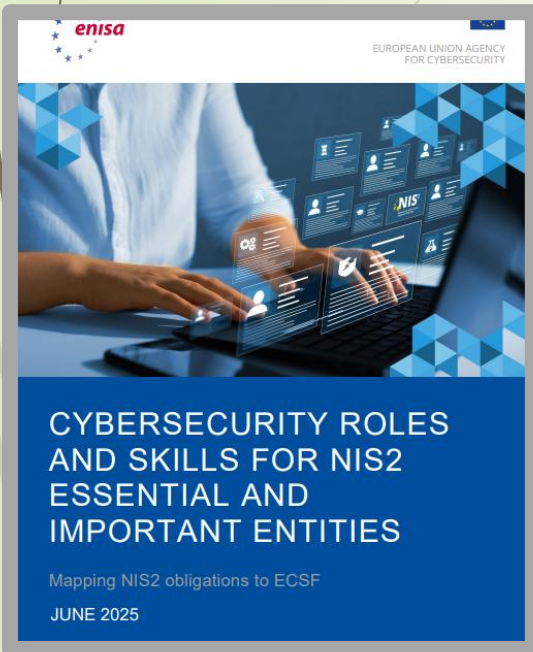
**Πηγή:**  
<https://cyber.org/career-exploration>

**SOFTWARE DEVELOPER**



# Νέα επαγγέλματα για την κυβερνοασφάλεια

- ❑ Ειδικός σε θέματα Ασφάλειας Τεχνητής Νοημοσύνης
- ❑ Αρχιτέκτονας Ασφάλειας Νεφοϋπολογιστικής
- ❑ Αναλυτής πληροφοριών για Κυβερνοαπειλές
- ❑ Ερευνητής ψηφιακής εγκληματολογίας

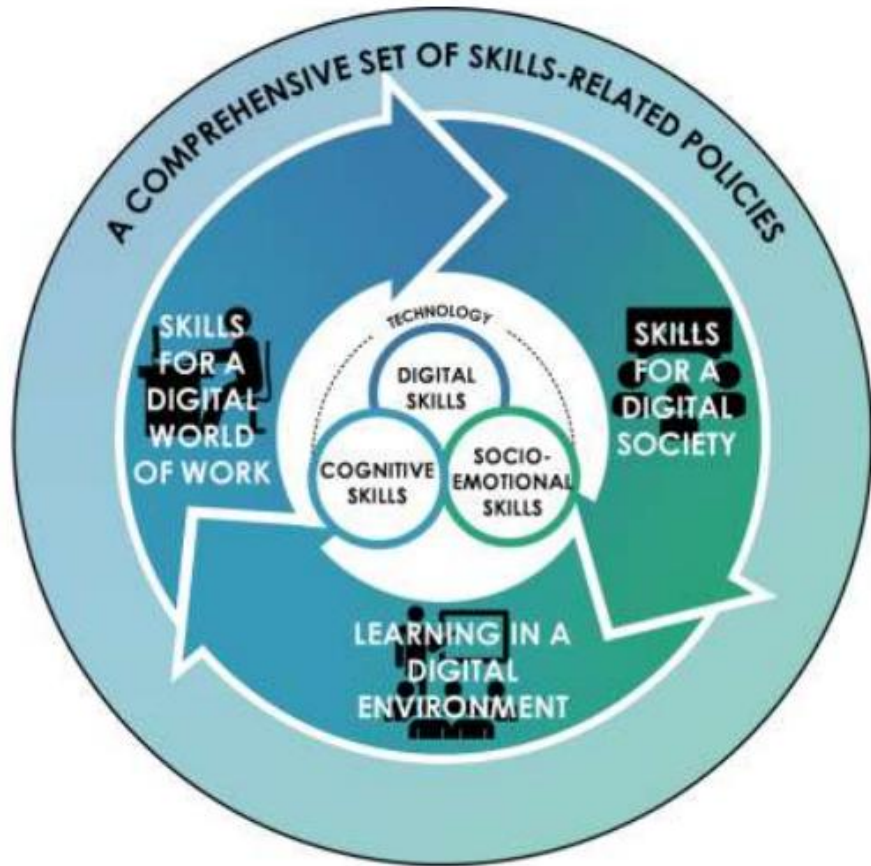


## Πηγές

1. <https://www.oecd.org/en/topics/cyber-security-skills.html>
2. <https://www.enisa.europa.eu/sites/default/files/2025-06/Mapping%20NIS%20%20obligations%20with%20ECSSF%20role%20profiles.pdf>
3. <https://www.enisa.europa.eu/topics/skills-and-competences>
4. <https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf>



# Τάσεις της αγοράς εργασίας



- ❑ Μεγαλύτερη ζήτηση για εξειδικευμένες δεξιότητες
- ❑ **Αύξηση** κυβερνοεπιθέσεων παγκοσμίως
- ❑ **Στροφή** από reactive σε proactive ασφάλεια
- ❑ Μεγάλη **έλλειψη** επαγγελματιών κυβερνοασφάλειας

# Σύγχρονο εκπαιδευτικό υλικό – συνεργασία σχολείων

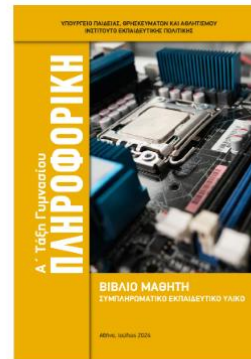


Τα σχολεία των ακριτικών κι όχι μόνο περιοχών μας πήραν άριστα (20)!!!

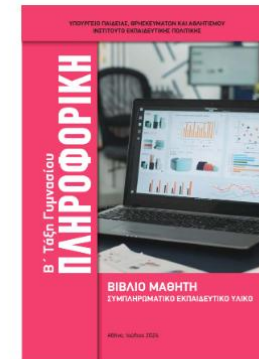


## Πηγές:

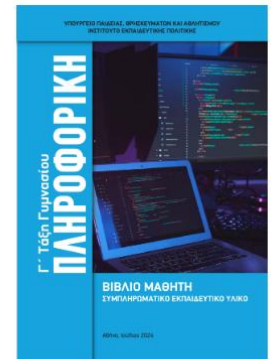
1. <https://nationaldigitalacademy.gov.gr/>
2. <https://iep.edu.gr/el/gymnasio/pliinfoforiki>
3. <https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools>
4. <https://cyber-news.gr/2026/02/13/%cf%84%ce%b1-%cf%83%cf%87%ce%bf%ce%bb%ce%b5%ce%af%ce%b1-%cf%84%cf%89%ce%bd-%ce%b1%ce%ba%cf%81%ce%b9%cf%84%ce%b9%ce%ba%cf%8e%ce%bd-%ce%ba%ce%b9-%cf%8c%cf%87%ce%b9-%ce%bc%cf%8c%ce%bd%ce%bf-%cf%80%ce%b5/>



Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Α' Γυμνασίου

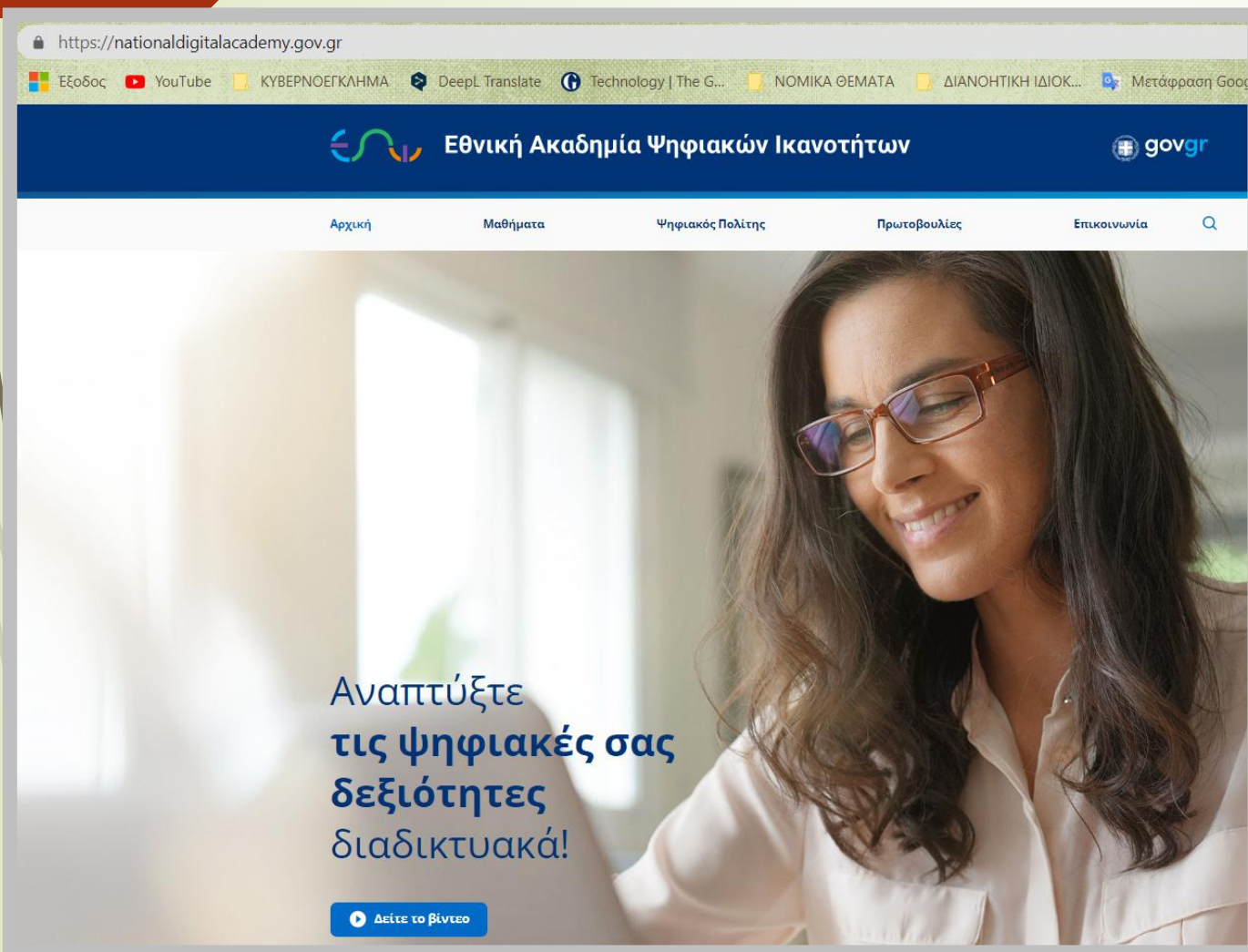
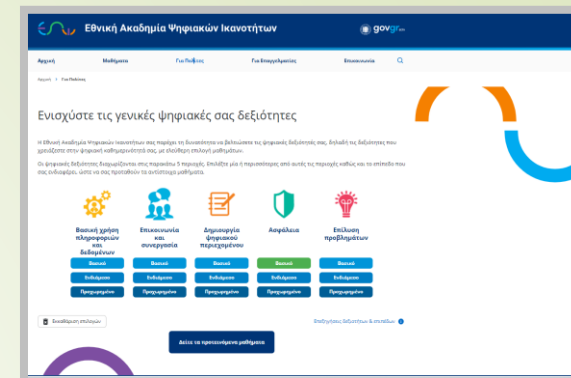


Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Β' Γυμνασίου



Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Γ' Γυμνασίου

# Εθνική Ακαδημία Ψηφιακών Ικανοτήτων- ΕΑΨΙ



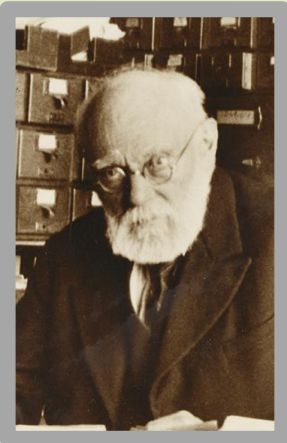
**Ποια είναι η συνεισφορά των πανεπιστημίων και των ερευνητικών μας κέντρων στην πλατφόρμα;**

**Με 311 μαθήματα  
35 θεματικές ενότητες  
1800 ώρες εκπαίδευσης**

**Στοιχεία στις 08/05/2026**

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

# 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**



# Καλές πρακτικές από φορείς Διεύθυνση Πρωτοβάθμιας Εκπαίδευσης Άρτας

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" - Λάκκωμα 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 έκφραση του Κυβερνοεγκλήματος οι διαδικτυακές απάτες	05 October 2024	Hits: 116
Report on Indicators of School Crime and Safety: 2023	21 October 2024	Hits: 217

**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

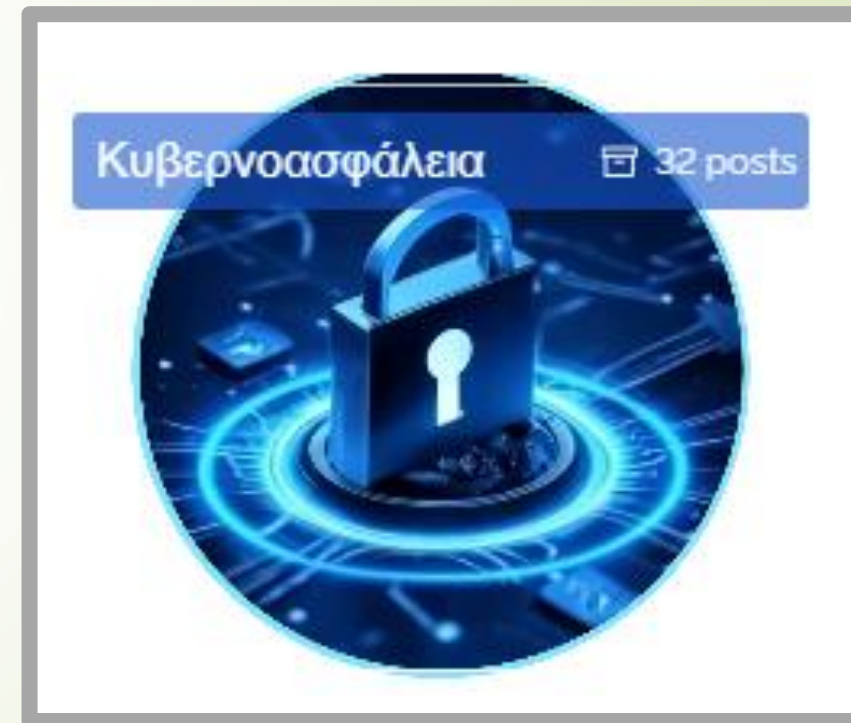
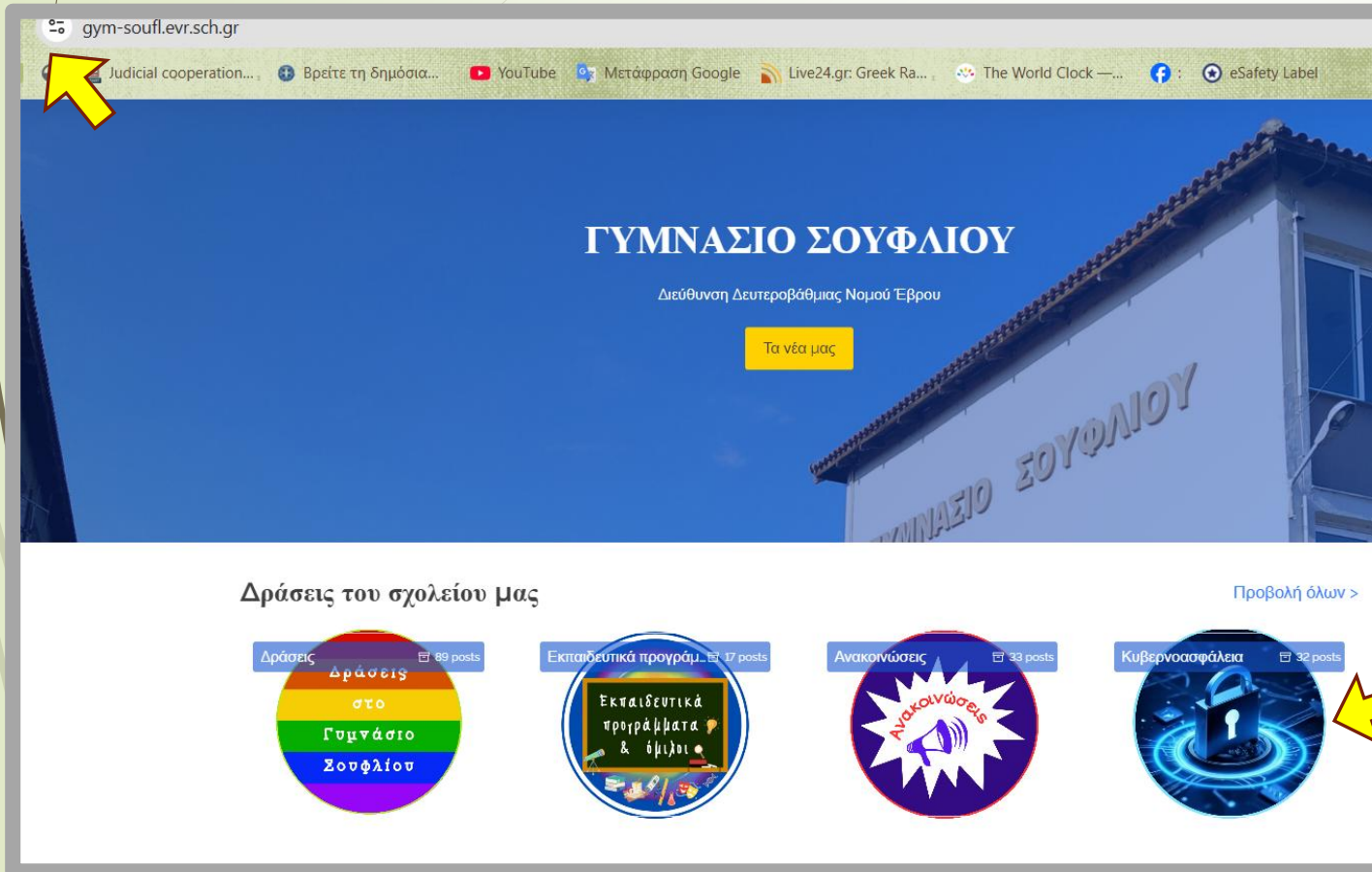


## Πηγές:

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

# Γυμνάσιο Σουφλίου Έβρου Κριτικά κι ακριτικά

Ειδικό αφιέρωμα  
στην **Κυβερνοασφάλεια**



Πηγές:

1. <https://gym-soufl.evr.sch.gr/category/esafety/>
2. <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/>

# Επιμελητήριο Πέλλας

The screenshot shows the website's navigation menu with options: Αρχική, Νέα, Δράσεις, Πληροφορίες, Εξυπηρέτηση, Πέλλα, and Επικοινωνία. The main content area is titled 'Κυβερνοασφάλεια' and features a video announcement about the approval of a law on cybersecurity. A sidebar on the right lists services: 'Υπηρεσίες Διοικητικής Εξυπηρέτησης' (e-επιμελητήριο, Γ.Ε.ΜΗ, Υ.Μ.Σ) and 'Υπηρεσίες Ανάπτυξης & Εξωστρέφειας' (Επιχειρηματικός Οδηγός).

**Ειδικό αφιέρωμα**  
στην **Κυβερνοασφάλεια**

The screenshot shows a mobile browser interface with a security warning. The address bar displays 'pellachamber.gr/kivernoasfalia/'. The warning message reads: '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.' A checkmark icon indicates 'Το πιστοποιητικό είναι έγκυρο'.

## Πηγές:

1. <https://www.pellachamber.gr/kivernoasfalia/>
2. <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/>

# Ανεξάρτητες Αρχές & Φορείς

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



ΣΥΝΗΓΟΡΟΣ  
ΤΟΥ ΠΟΛΙΤΗ  
ΑΝΕΞΑΡΤΗΤΗ ΑΡΧΗ



Συνήγορος του Παιδιού



ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ



ΣΥΝΗΓΟΡΟΣ  
ΤΟΥ ΚΑΤΑΝΑΛΩΤΗ  
Ανεξάρτητη Αρχή



ΑΔΑΕ



ΕΕΤΤ  
ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

- ❑ 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)

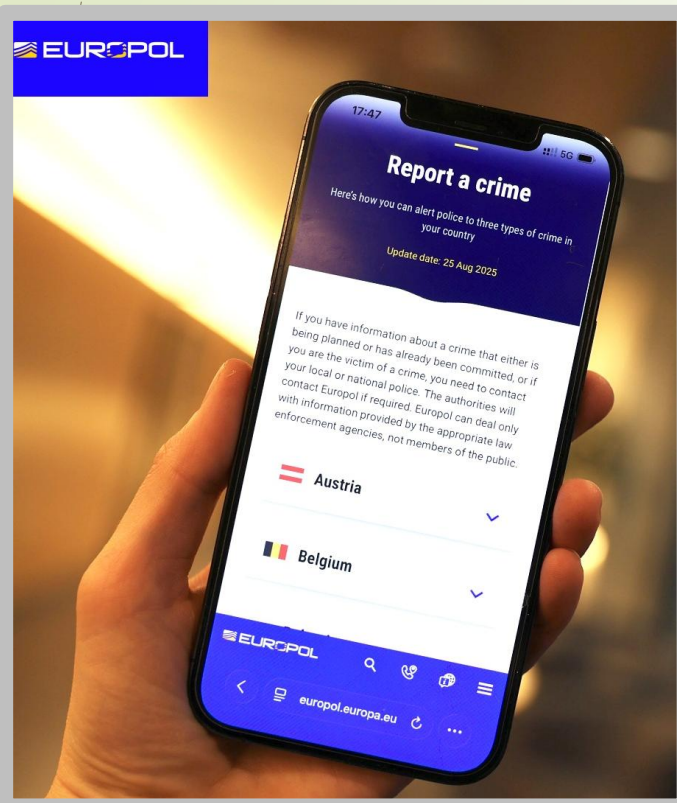


ΟΡΓΑΝΙΣΜΟΣ  
ΠΝΕΥΜΑΤΙΚΗΣ  
ΙΔΙΟΚΤΗΣΙΑΣ  
HELLENIC  
COPYRIGHT  
ORGANIZATION



Εθνικός Οργανισμός Φαρμάκων  
National Organization for Medicines

# 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/eU/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/>
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

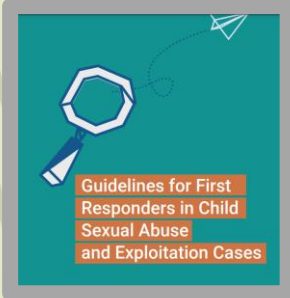
Because 'International Organization for Standardization' would have different acronyms in different languages (IOS in English, OIN in French for *Organisation internationale de normalisation*), our founders decided to give it the short form ISO. ISO is derived from the Greek 'isos', meaning equal. Whatever 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](https://enfsi.eu/wp-content/uploads/2024/06/ENFSI_Annual_Report_2023-1.pdf) p. 16

# Διεθνής Συνεργασία – Ανταλλαγή Πληροφοριών



## Πληροφορίες & καλές πρακτικές

### Πηγές:

1. [https://www.europol.europa.eu/cms/sites/default/files/documents/Grace%20Guidelines%202022\\_Public\\_0.pdf](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, 02/04/2025

## Επιχείρηση «Kidflix»

- Διεθνής επιχείρηση της Europol και Eurojust μαζί με άλλες 38 χώρες συμμετείχαν στην επιχείρηση . Η έρευνα ξεκίνησε το 2022 και κατέληξε σε εβδομάδες δράσης από τις 10 έως τις 23 Μαρτίου 2025. Μέχρι στιγμής, έχει οδηγήσει στα ακόλουθα αποτελέσματα:
  - 91.000 video ΣΕΑ
  - 1.393 ύποπτοι ταυτοποιήθηκαν
  - 79 ύποπτοι συνελήφθησαν
  - > 3.000 ψηφιακές συσκευές κατασχέθηκαν
  - 39 παιδιά προστατεύθηκαν

Πηγή:

<https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users>

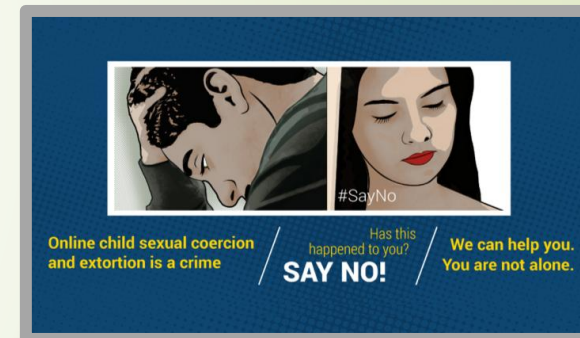
# Συνεργασία για περισσότερη Ασφάλεια **Σήμερα** το κάνετε πράξη



Ακαδημαϊκή Κοινότητα

**NO MORE RANSOM!**

[www.nomoreransom.org](http://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  
**08/05/2026**



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](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\\_SQVW-jKJpRxtPZjs\\_4w\\_aem\\_00bjjEqYTRQrYa7NFznhNg](https://www.hellenicparliament.gr/UserFiles/c0d5184d-7550-4265-8e0b-078e1bc7375a/12951870.pdf?fbclid=IwY2xjawKr4ttleHRuA2FibQIxMABicmlkETB4T1hObDNnNkh4TWZ6SE4wAR7zYLMoQFAYNOXbq7VUbcBMpk0WkCVhgsWCzkrb32_SQVW-jKJpRxtPZjs_4w_aem_00bjjEqYTRQrYa7NFznhNg)
5. [https://www.opengov.gr/yyka/?c=17616&fbclid=IwY2xjawRakutleHRuA2FibQIxMABicmlkETB2aElscjJNeEMwWnVyZG1xc3J0YwZhcHBfaWQQMjlyMDM5MTc4ODIwMDg5MgABHmUu0zwYXnw004dhTi83hFCr3cm6IVaVVpTtx7D8LxYjzyR00t9xoVV\\_0Lqr\\_aem\\_488086woRUKi9LXibRJSJLg](https://www.opengov.gr/yyka/?c=17616&fbclid=IwY2xjawRakutleHRuA2FibQIxMABicmlkETB2aElscjJNeEMwWnVyZG1xc3J0YwZhcHBfaWQQMjlyMDM5MTc4ODIwMDg5MgABHmUu0zwYXnw004dhTi83hFCr3cm6IVaVVpTtx7D8LxYjzyR00t9xoVV_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)

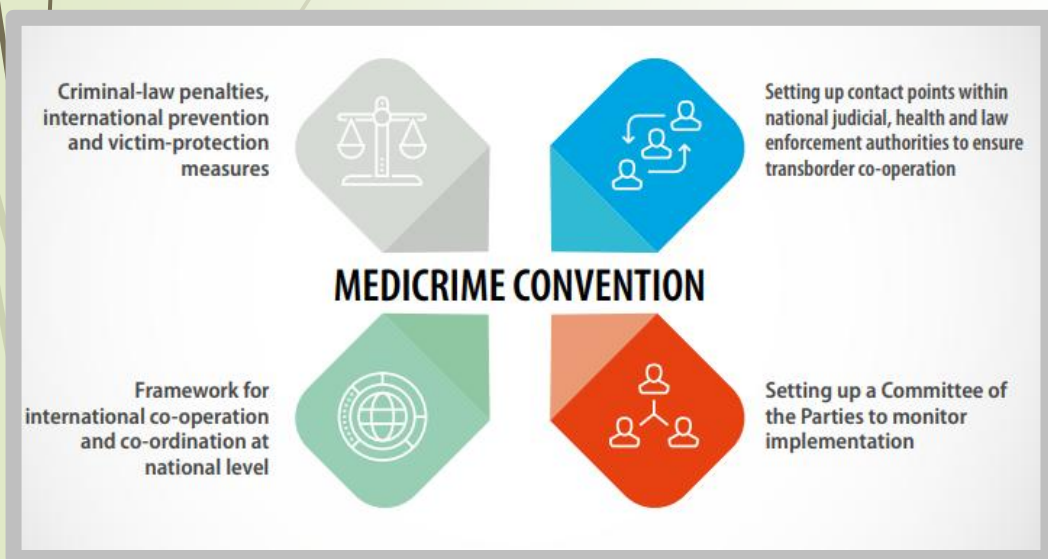
## 2 INVITATIONS

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 επικύρωσης 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 | Κιμ. : 697 811 98 63 | admioschakis@outlook.com  
Καραϊσκάκη 10, Αλεξανδρούπολη | Τηλ: 25510 27548 | Φακ: 25510 36874 | Ελ. Βενιζέλου 28, Δουρούμιατο | Τηλ: 25530 23086



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

**Πηγές**

- [https://www.hellenicparliament.gr/UserFiles/c0d5184d-7550-4265-8e0b-078e1bc7375a/12951870.pdf?fbclid=IwY2xjawKr4ttleHRuA2FibQlXmABicmlkETB4T1hObDNnNkh4TWZ6SE4wAR7zYLMoQFAYNOXbq7VUubCBMpk0WkCVhgsWCzkrb32\\_SQWV-jkJPxrtPZjs\\_4w\\_aem\\_00bjjEqYTRQrYa7NFznhNg](https://www.hellenicparliament.gr/UserFiles/c0d5184d-7550-4265-8e0b-078e1bc7375a/12951870.pdf?fbclid=IwY2xjawKr4ttleHRuA2FibQlXmABicmlkETB4T1hObDNnNkh4TWZ6SE4wAR7zYLMoQFAYNOXbq7VUubCBMpk0WkCVhgsWCzkrb32_SQWV-jkJPxrtPZjs_4w_aem_00bjjEqYTRQrYa7NFznhNg)
- <https://www.hellenicparliament.gr/UserFiles/67715b2c-ec81-4f0c-ad6a-476a34d732bd/12976450.pdf>
- [https://www.opengov.gr/yyka/?c=17616&fbclid=IwY2xjawRakutleHRuA2FibQlXmABicmlkETB2aElscjJNeEMwWnVyZG1xc3J0YwZhcHBfaWQQMjlyMDM5MTc4ODlwMDg5MgABHmUu0zwYXnw0O4dhTi83hFCr3cm6lVaVVPtTx7D8LxYjzyR00t9xoVV\\_0Lqr\\_aem\\_488086woRUKi9LXibRJSLg](https://www.opengov.gr/yyka/?c=17616&fbclid=IwY2xjawRakutleHRuA2FibQlXmABicmlkETB2aElscjJNeEMwWnVyZG1xc3J0YwZhcHBfaWQQMjlyMDM5MTc4ODlwMDg5MgABHmUu0zwYXnw0O4dhTi83hFCr3cm6lVaVVPtTx7D8LxYjzyR00t9xoVV_0Lqr_aem_488086woRUKi9LXibRJSLg)

# Δημοκρατία & Ανθρώπινα Δικαιώματα

## Το πραγματικό διακύβευμα

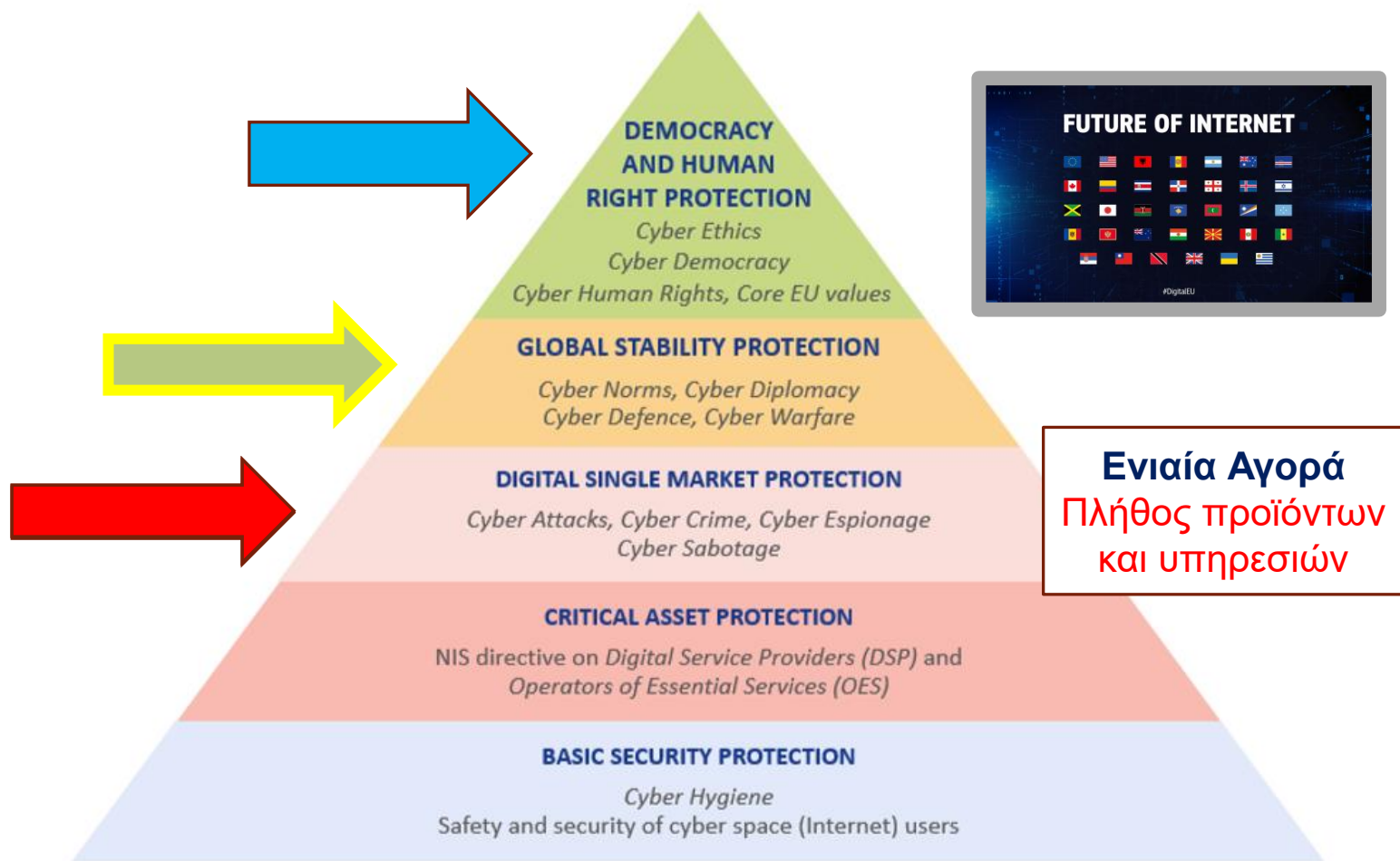
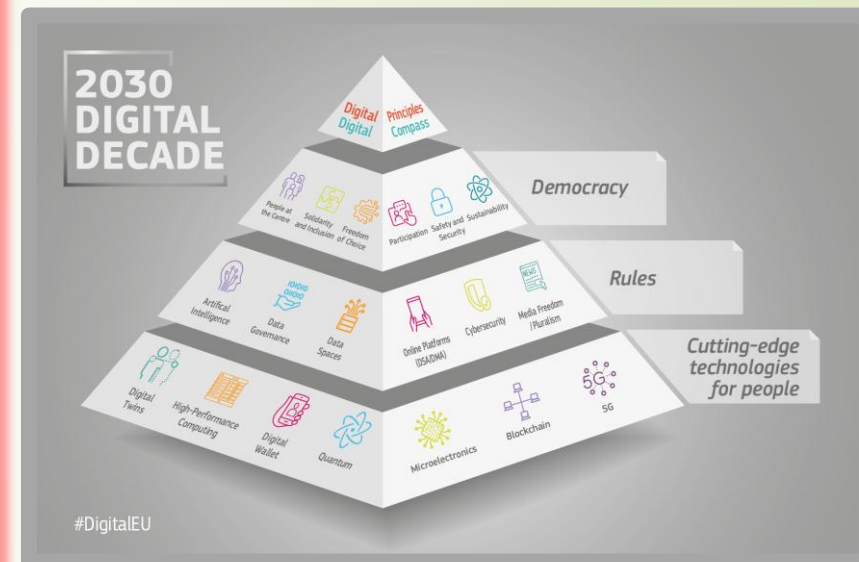


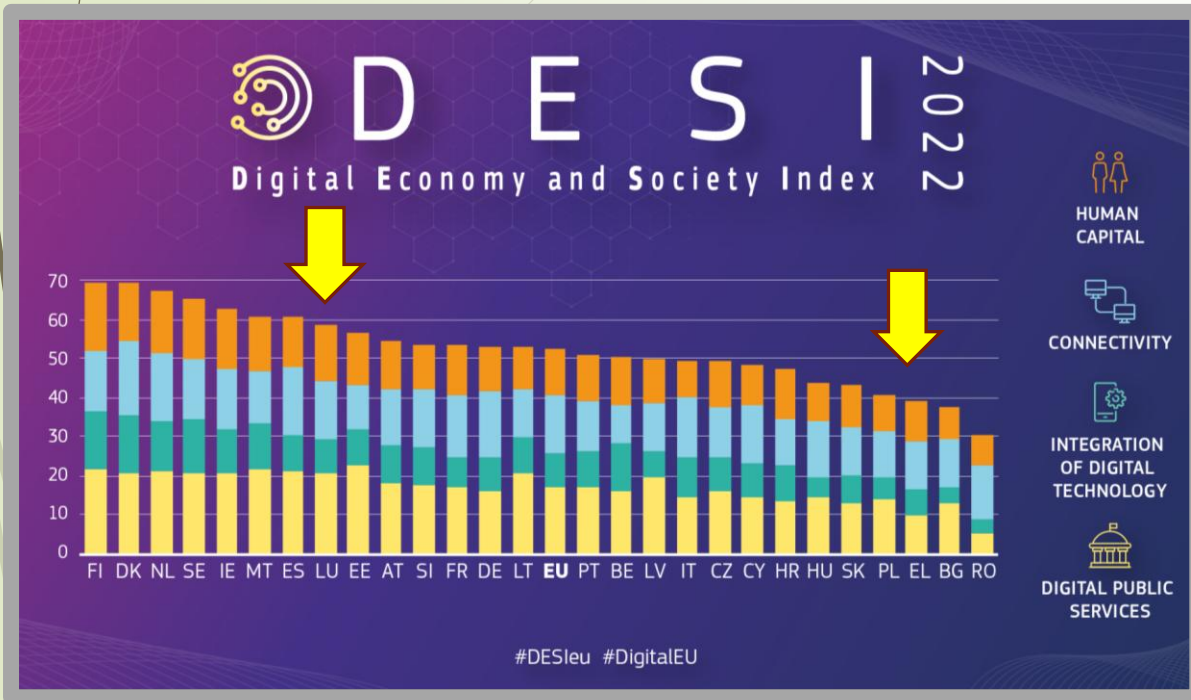
Figure 1. Layers of cybersecurity needs.



### Πηγές:

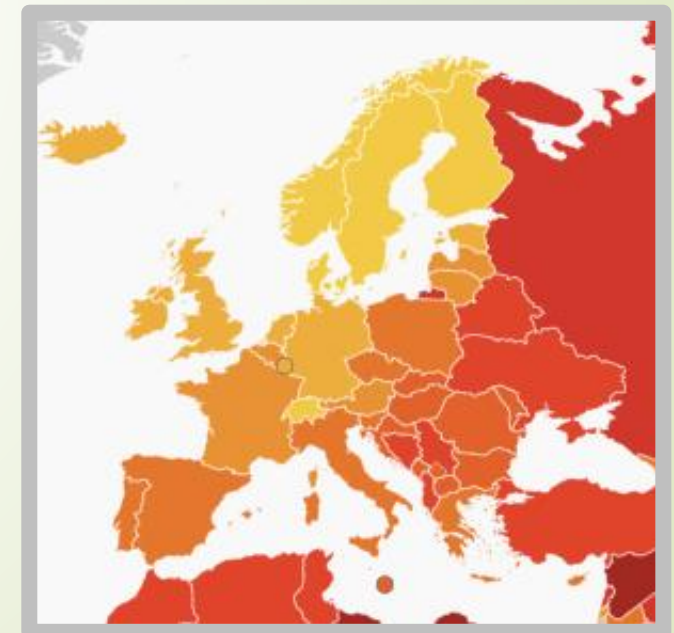
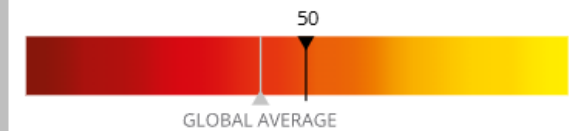
- <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-input-to-the-css-review-b-p.7>
- [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_22\\_2695](https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2695)
- [https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210622\\_Hybrid\\_CoE\\_Paper\\_7\\_Geopolitics\\_and\\_strategies\\_in\\_cyberspace\\_WEB.pdf](https://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>

# Ψηφιακή Σύγκλιση – Διαφάνεια (CPI 2025)



## GREECE

Score **50/100** Rank **56/182** Score change **↑ +1** since 2024



Δημοσιεύθηκαν 28/07/2022 & 10/2/2026

Πηγές:

1. <https://digital-strategy.ec.europa.eu/en/policies/desi>
2. <https://files.transparencycdn.org/images/CPI-2025-Report-EN.pdf>
3. <https://www.ethnos.gr/opinions/article/195948/pshfiakosmetasxhmatismoskaidiafaneiahallazoymehboyliazoyme>
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
- ❑ **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, Εμπλεκόμενοι φορείς, Ενίσχυση Διεθνούς Συνεργασίας]*

- ❑ Κουλτούρα Τεχνοηθικής
- ❑ 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 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





## Ως τελικό Συμπέρασμα

- ❑ Ο Κυβερνοχώρος μια νέα χασοτική πραγματικότητα.
- ❑ Απαιτούνται δεξιότητες και ικανότητες
- ❑ Η Κυβερνοασφάλεια είναι υπόθεση όλων μας κι απαιτεί προετοιμασία
- ❑ Η κουλτούρα κυβερνοασφάλειας έχει στο επίκεντρο τον άνθρωπο και τα δεδομένα του.
- ❑ Ο σεβασμός των προσωπικών δεδομένων χτίζει τις ανθρώπινες σχέσεις και φέρνει την ευημερία

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

Σε **κάθε** περίπτωση.....

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

**It's called respect.**



MyPositiveOutlooks.com

**Πηγή:**  
[https://www.linkedin.com/  
company/european-  
leadership/posts/?feedVie  
w=all](https://www.linkedin.com/company/european-leadership/posts/?feedView=all)



**«ενωμένοι μπορούμε πολλά,  
μόνοι μας τίποτα»**

# 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](http://coe.int/t/dg3/children)
- Cybercrime COE  
[coe.int/en/web/cybercrime](http://coe.int/en/web/cybercrime)
- Cybercrime Interpol  
[interpol.int/Crimes/Cybercrime](http://interpol.int/Crimes/Cybercrime)
- Cybersecurity Basics FTC USA  
[ftc.gov/business-guidance/small-businesses/cybersecurity/basics](http://ftc.gov/business-guidance/small-businesses/cybersecurity/basics)
- ENISA PUBLICATIONS  
[enisa.europa.eu/publications#c3=2012&c3=2022&c3=false&c5=publishing](http://enisa.europa.eu/publications#c3=2012&c3=2022&c3=false&c5=publishing)
- CYBERSECURITY CISA USA  
[cisa.gov/cybersecurity](http://cisa.gov/cybersecurity)
- CYBER AWARE UK  
[ncsc.gov.uk/cyberaware/home](http://ncsc.gov.uk/cyberaware/home)
- CYBERCRIME EUROJUST  
[eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime](http://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...](http://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=](http://nationaldigitalacademy.gov.gr/anazhthsh/?skill=19&q=)
- ITU CYBERSECURITY  
[itu.int/en/action/cybersecurity/Pages/default.aspx](http://itu.int/en/action/cybersecurity/Pages/default.aspx)
- UN Office on Drugs and Crime  
[unodc.org/unodc/en/cybercrime](http://unodc.org/unodc/en/cybercrime)
- CSIRT HELLENIC  
[cyber.gov.gr/el-csirt](http://cyber.gov.gr/el-csirt)



Με θεματικά  
**playlists & links**

Αναζήτηση

Κυβερνοχώρο στην καθημερινότητά

**Γιώργος Παπαπροδρόμου - Giorgos Papaprodromou**  
1,311 εγγραφμένοι · 241 βίντεο

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

[europol.europa.eu/operations-services-and-innovation/public-awareness...](http://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 Δημογλίδου και ο Γιώργος Παπαπροδρόμου καλεσμένοι στην πρωινή εκπομπή του τηλεοπτικού σταθμού ACTION 24, των δημοσιογράφων Ντόρας Κουτροκλή 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](http://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.)