



**SMART  
ATTICA** European  
Digital  
Innovation  
Hub



ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΤΕΚΜΗΡΙΩΣΗΣ &  
ΗΛΕΚΤΡΟΝΙΚΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ



# Τάσεις Κυβερνοεγκλήματος και Κυβερνοαπειλές

Γιώργος Παπαπροδρόμου | Αντιστράτηγος εα  
Πρώην Διευθυντής Δνσης Δίωξης Ηλεκτρονικού Εγκλήματος

## AI-powering Greece

**WEBINAR**

Τετάρτη, 18 Σεπτεμβρίου 2024



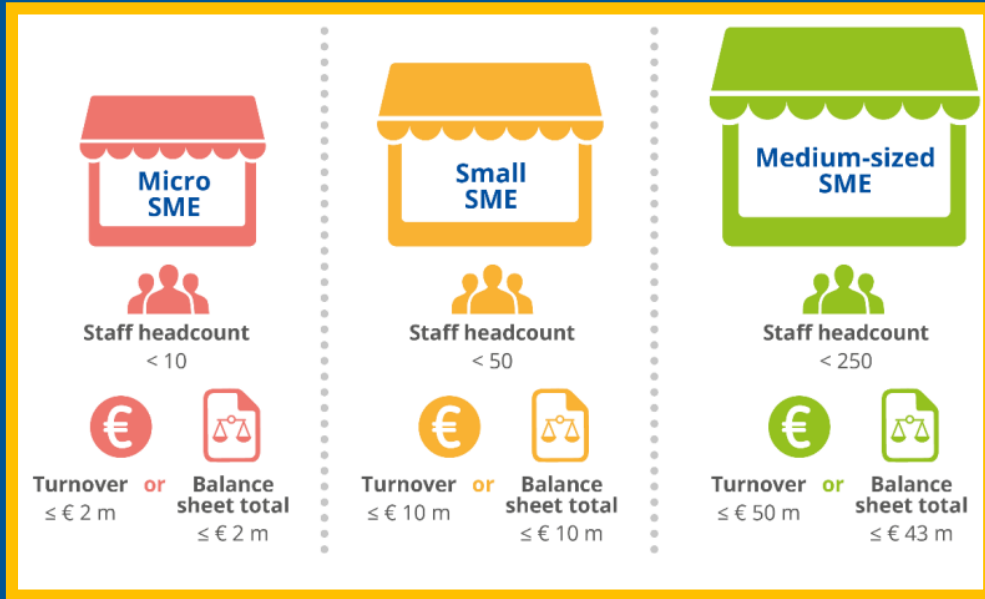
Co-funded by  
the European Union



PROGRAMME 2021 – 2027  
**COMPETITIVENESS**

# Μικρομεσαίες επιχειρήσεις και ΕΕ

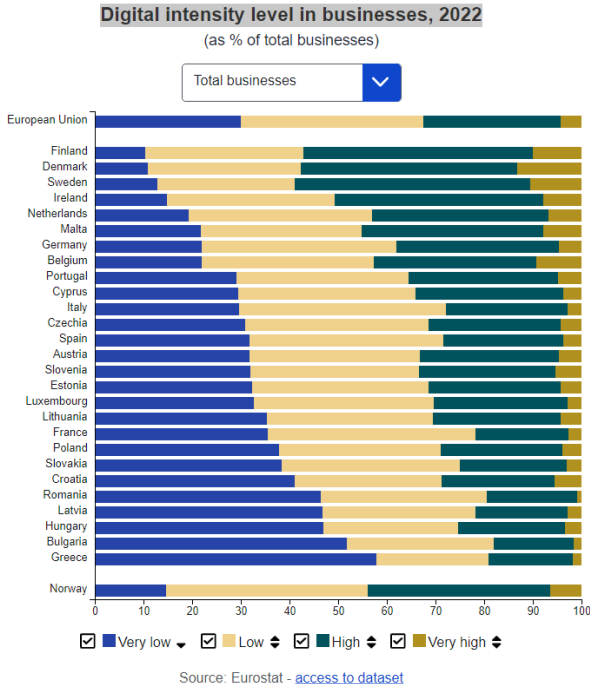
## Άνθρωποι – Διαδικασίες - Τεχνολογία



Πηγές:

1. <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes> p.9, 28
2. <https://www.youtube.com/watch?v=ymLKVtat-IM>

# Μικρομεσαίες επιχειρήσεις στην ΕΕ και Κυβερνοασφάλεια



- ❑ 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 από τα οποία δεν καταγγέλλονται!!!



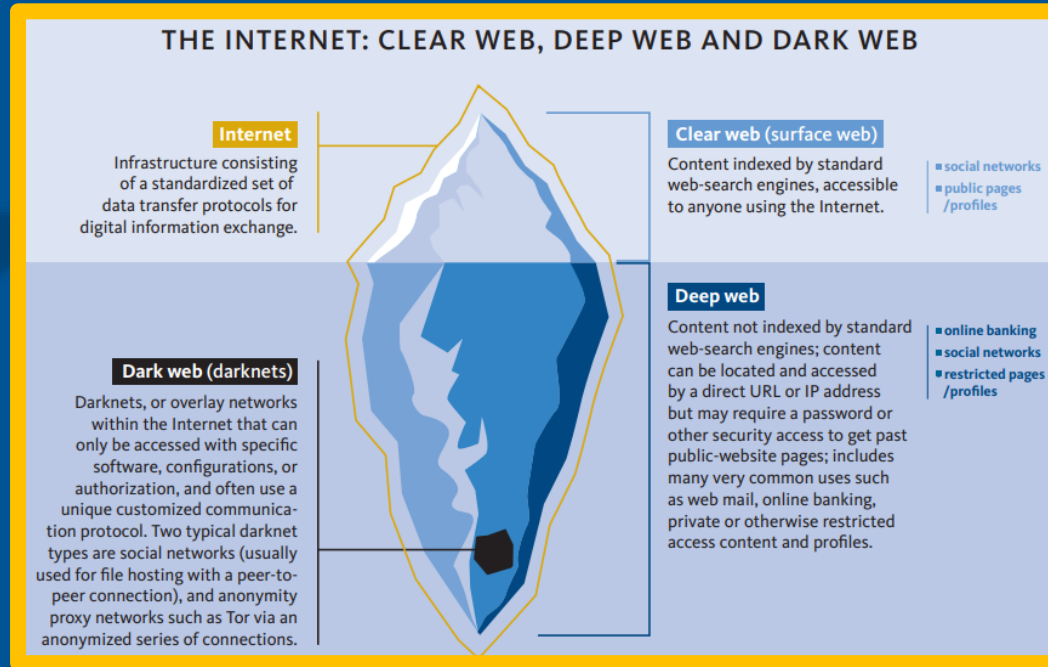
Πηγές:

1. [https://ec.europa.eu/growth/smes\\_en](https://ec.europa.eu/growth/smes_en)
2. [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme\\_cybersecurity](https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme_cybersecurity)
3. <https://www.enisa.europa.eu/news/enisa-news/survey-to-explore-the-preparedness-of-eu-smes-for-cybersecurity-challenges>
4. <https://www.youtube.com/watch?v=ymlKVTat-IM>
5. <https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2023>

# Η κατανόηση του κυβερνοοικουσυστήματος



## Πολύπλοκο - σύνθετο περιβάλλον Με αβεβαιότητες



### Πηγές:

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

# Τι απειλεί σήμερα τις ΜΜΕπιχειρήσεις στον Κυβερνοχώρο; Μορφές **Κυβερνοαπειλών**



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

Δημοσιεύθηκε **19/10/2023**

**Πηγές:**

1. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
2. <https://www.enisa.europa.eu/media/media-press-kits/logos>
3. <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>
4. [https://www.europarl.europa.eu/news/el/headlines/society/20220120STO21428/oi-megaluteris-apeiles-ston-tomea-tis-kuvnoasfaleias?fbclid=IwAR1jJnQz2hSpnHq93o9jqimHIFDgEcBHcEcb-WTFojtP1kwKz\\_qxnmMJgMs](https://www.europarl.europa.eu/news/el/headlines/society/20220120STO21428/oi-megaluteris-apeiles-ston-tomea-tis-kuvnoasfaleias?fbclid=IwAR1jJnQz2hSpnHq93o9jqimHIFDgEcBHcEcb-WTFojtP1kwKz_qxnmMJgMs)
5. <https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection/?tab=publications>
6. <https://id4d.worldbank.org/guide/cybercrime-and-cybersecurity>



# Το τοπίο των Κυβερνοαπειλών ως το 2030



1. **Supply chain** compromise of software dependencies
2. Advanced disinformation campaigns
3. **Rise of digital surveillance authoritarianism/loss of privacy**
4. Human error and exploited legacy systems within cyber-physical ecosystems
5. Targeted attacks enhanced by smart device data
6. Lack of analysis and control of space-based infrastructure and objects
7. Rise of advanced hybrid threats
8. **Skills shortage**
9. Cross-border ICT service providers as a single point of failure
10. **Artificial intelligence abuse**

## Πηγές:

1. <https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030> 11/11/2022
2. <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>
3. <https://id4d.worldbank.org/guide/cybercrime-and-cybersecurity>

# Μορφές και παράμετροι Κυβερνοεγκλήματος

Ιδιωτικότητα



Σεξουαλική  
Εκμετάλλευση  
**Ανηλίκων**

Απάτες

Κυβερνοεπιθέσεις

Κυβερνοέγκλημα

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

**Ναρκωτικά**  
και  
Φάρμακα

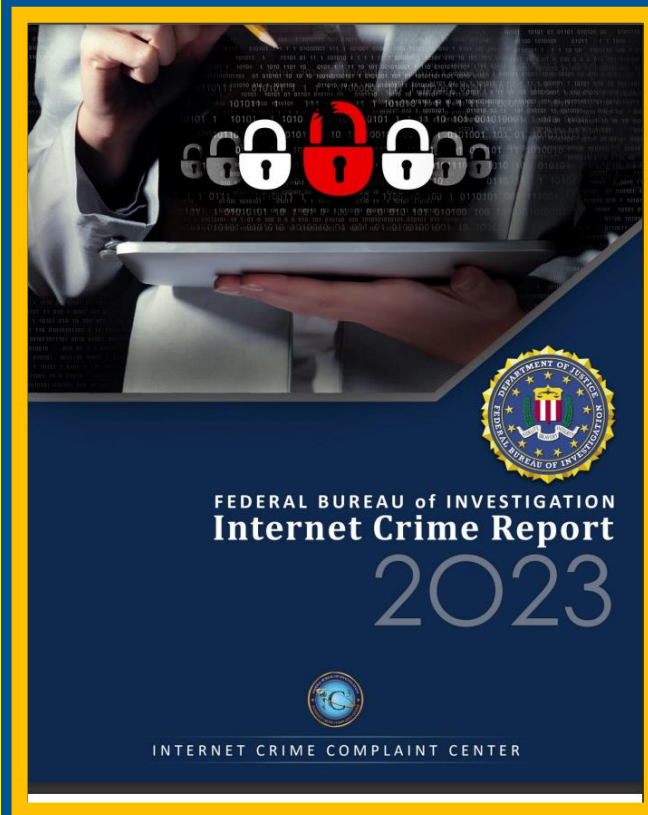
Διανοητική  
Ιδιοκτησία

**Διάφορα αδικήματα**  
**Πχ** διαδικτυακός  
τζόγος

Προστασία κρίσιμων υποδομών



# Το Κυβερνοέγκλημα **αυξάνεται** κάθε χρόνο



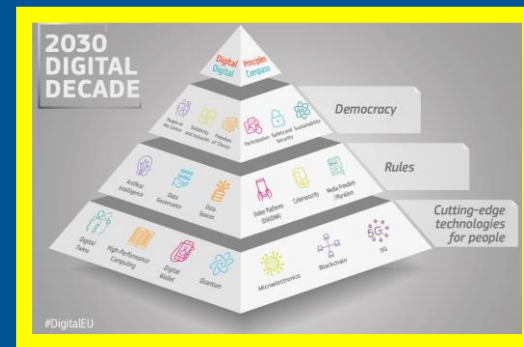
Δημοσιεύθηκαν 26/07/2024 & 07/3/2024

## Πηγές:

1. <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>
2. [https://www.ic3.gov/Media/PDF/AnnualReport/2023\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf)
3. <https://id4d.worldbank.org/guide/cybercrime-and-cybersecurity>



# Στρατηγική Ασφάλειας ΕΕ



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

## Πηγές:

1. [https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en)
2. [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_1379](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379)
3. <https://digital-strategy.ec.europa.eu/el/policies/europes-digital-decade>
4. [https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package?fbclid=IwAR2IWdrlQMiWv3aBNIJzkdDZVsxj12o6gnZK\\_2edWPuWVlbf9Gat\\_cItM\\_aem\\_Abz5czPFhGSttxVQmG\\_U2oaUUIQGd7ogwR0M9948FzcRnZepYGCJv7Uutp6nsyoe1lgGzqPryCwrtwRuLiozYdJW9](https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package?fbclid=IwAR2IWdrlQMiWv3aBNIJzkdDZVsxj12o6gnZK_2edWPuWVlbf9Gat_cItM_aem_Abz5czPFhGSttxVQmG_U2oaUUIQGd7ogwR0M9948FzcRnZepYGCJv7Uutp6nsyoe1lgGzqPryCwrtwRuLiozYdJW9)

# Η Δημοκρατία και τα ανθρώπινα δικαιώματα Με Κυβερνoασφάλεια

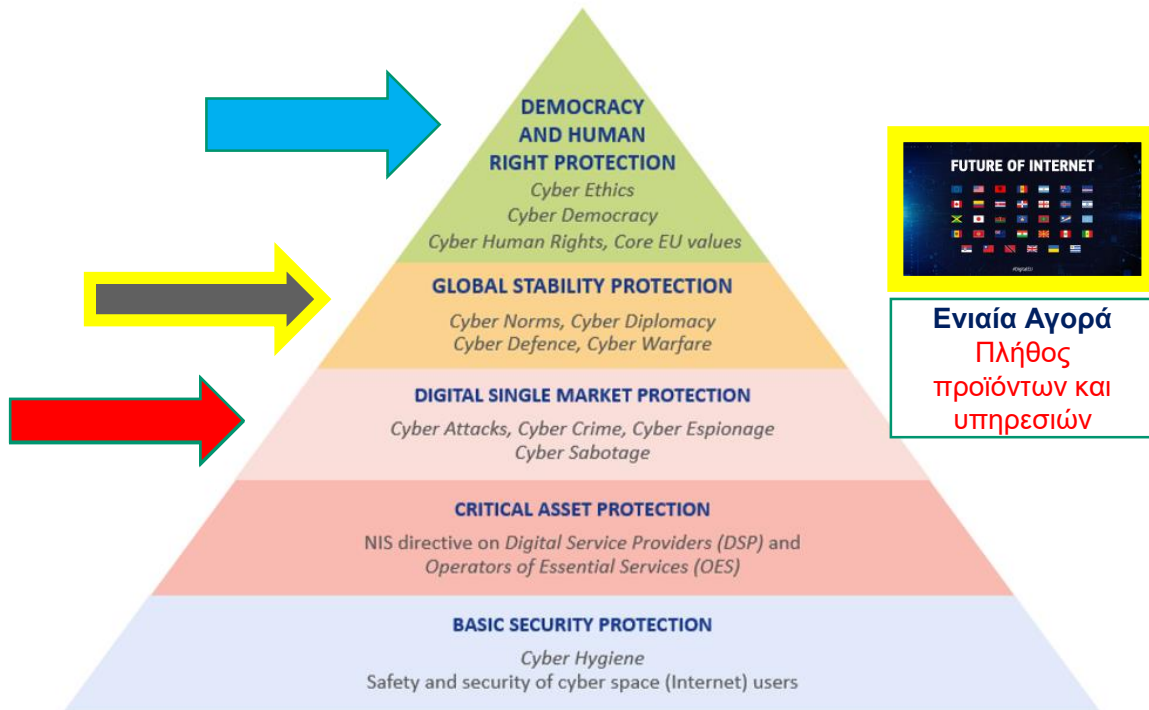
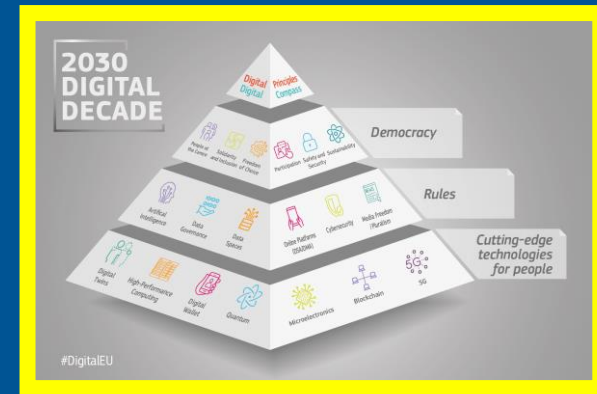


Figure 1. Layers of cybersecurity needs.



**Ενιαία Αγορά  
Πλήθος  
προϊόντων και  
υπηρεσιών**

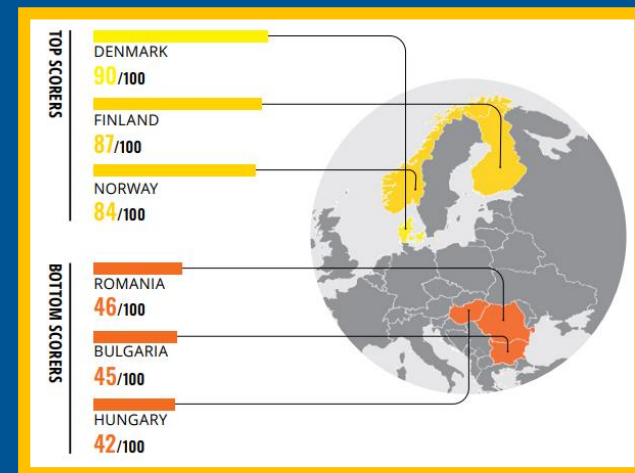
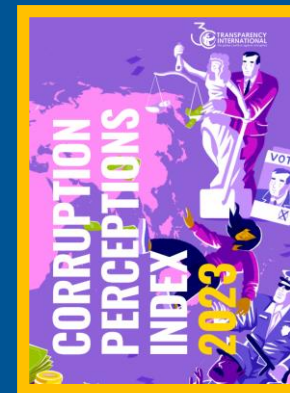
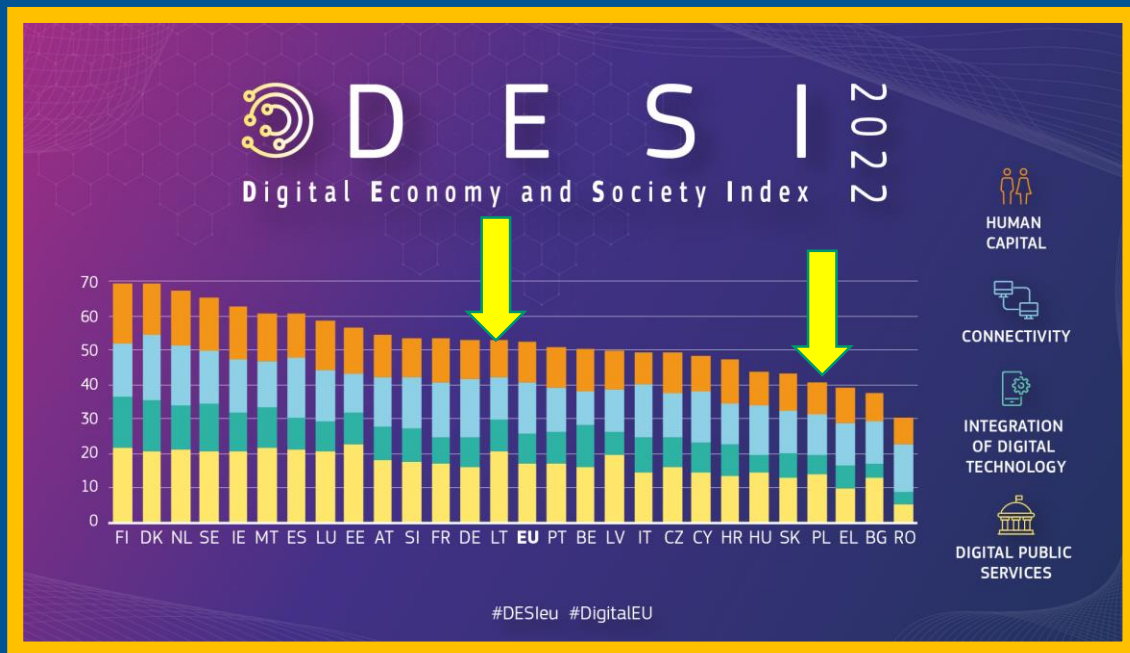


## Πηγές:

- <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/el/policies/europes-digital-decade>

# Δείκτης Ψηφιακής Οικονομίας & Κοινωνίας

## Ψηφιακή Σύγκλιση – Διαφάνεια (CPI 2023)



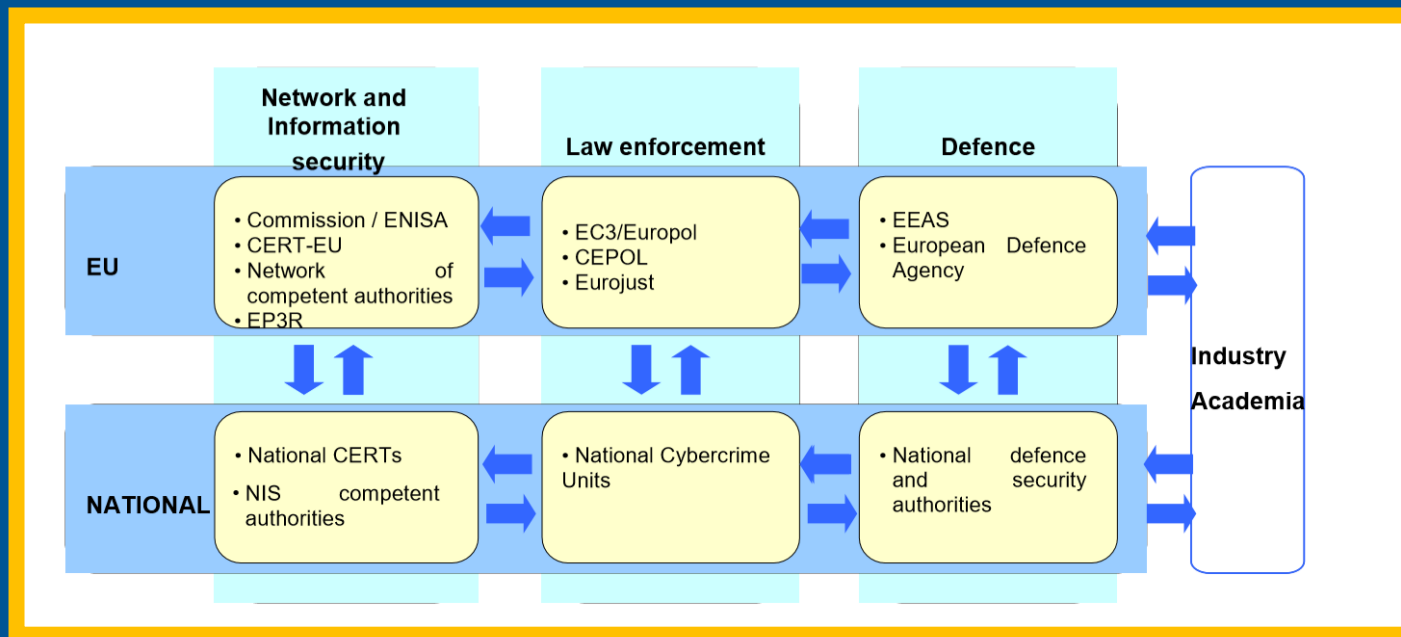
Δημοσιεύθηκαν 28/07/2022 & 30/1/2024

Πηγές:

- <https://digital-strategy.ec.europa.eu/en/policies/desi>
- <https://www.transparency.org/en/cpi/2023> P.19
- <https://www.ethnos.gr/opinions/article/195948/psshfiakosmetasxhmatismoskaidiafaneiahallazoynehboyliazoyme>



# Υποδομές της ΕΕ για το νέο περιβάλλον του Κυβερνοχώρου



# Αναφορά Κυβερνοεγκλημάτων- υπάρχει πλατφόρμα

Εισαγγελία  
Πρωτοδικών

Αρχές Επιβολής  
του Νόμου

Ανεξάρτητες  
Διοικητικές Αρχές

Ειδικές  
Πλατφόρμες

Ηλεκτρονικό  
Ταχυδρομείο

Τηλεφωνικό  
Κέντρο 11188



Καταγγελίες για εγκλήματα κυβερνοχώρου

Καταγγελία για αδικήματα τελούμενα σε βάρος ανηλίκων μέσω διαδικτύου

Καταγγελία για οικονομικά κυβερνοεγκλήματα όπου εμπλέκονται ηλεκτρονικά/ψηφιακά νομίσματα

Καταγγελία για παραβίαση του απορρήτου των ηλεκτρονικών και τηλεφωνικών επικοινωνιών

Καταγγελία για παράνομη διακίνηση οπτικοακουστικών έργων μέσω διαδικτύου

Καταγγελία για παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή

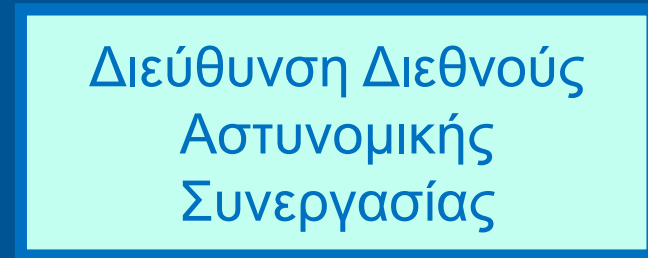
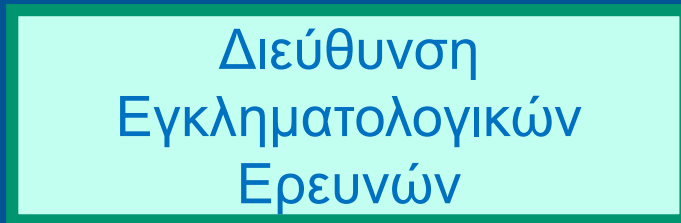
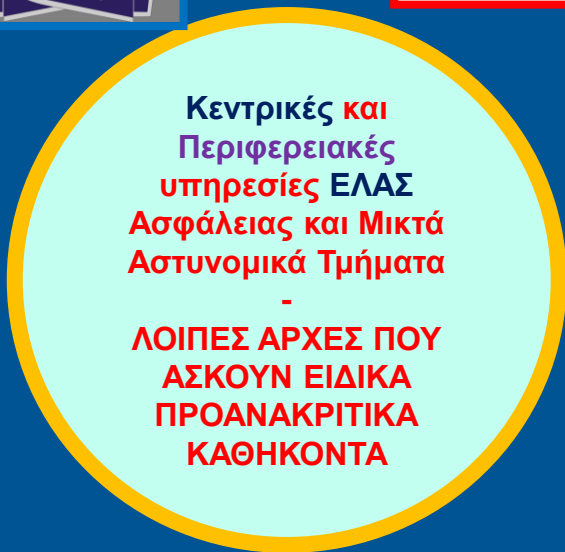
Καταγγελία για περιπτώσεις απάτης με υπολογιστή

Πηγές:

1. <https://www.gov.gr/ipiresies/polites-kai-kathemerinoteta/kataggelies>
2. <https://www.zougla.gr/n/technology/world-of-tech/article/to-sistema-anaforas-kivernoeglimaton-ke-kivernoperistatikon-stin-xora-mas>

18-12-2020

# Υπηρεσίες Αντιμετώπισης Κυβερνοεγκλήματος



Π Ε Ι Σ Τ Η Ρ Ι Α

Π Λ Η Ρ Ο Φ Ο Ρ Ι Α

ΠΔ 178/2014 ΦΕΚ Α 281 «Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας», όπως τροποποιήθηκε και ισχύει σήμερα Άρθρα 31, 30, 8, 27



# Εγκληματολογική Έρευνα Ψηφιακών Πειστηρίων



EUROPEAN NETWORK  
OF FORENSIC SCIENCE  
INSTITUTES



PRECISION  
FORENSICS

## 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/>

## ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (PHISHING)



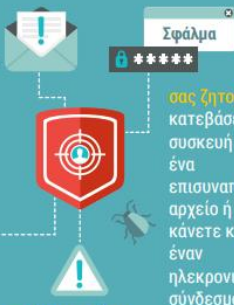
Ο όρος "phishing" αναφέρεται στα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου, που σκοπό έχουν να εξαπατηθούν οι παραλήπτες τους και να γνωστοποιήσουν στους απατεώνες προσωπικές και οικονομικές τους ροφορίες ή κωδικούς ασφαλείας τους.

### 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.



κάνουν χρήση ορολογιάς που δίνει την αίσθηση του κατεπεύγοντος.

Οι εγκληματίες στον κυβερνοχώρο θα ελίζονται στο μενού ε-επιχειρηματίας

### ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

Διατηρείτε το λογισμικό ενημερωμένο, περιλαμβανομένου του φυλλομετρητή ιστοσελίδων (browser), του αντικικού προγράμματος (antivirus) και του λειτουργικού συστήματος.

Να είστε ιδιαίτερα προσεκτικοί εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου "τράπεζα" 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 μόνι σας.

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

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

# Αλίευση Δεδομένων Phishing



Το πακέτο σας φτάνει στα ΕΛΤΑ αούριο

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 αούριο.

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

Λειτουργίες

Με εκτίμηση,

ΕΛΤΑ.

Unsubscribed



### Πηγές:

- <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/e-commerce-tips-and-advice-to-avoid-becoming-fraud-victim>
- [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)
- <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/e-commerce-tips-and-advice-to-avoid-becoming-fraud-victim>
- <https://www.politica.gr/politica-89-8/g-papaprodromou-diarkis-epikairopoisi-tis-atzentas-kubernoasfaleias-na-axiopoithoun-oi-neoi-epistimones/>
- <https://www.facebook.com/hellenicpolice/posts/pfbid02btGBuuZe7n7HTnSsWt8fNtZhfnpu4YAoqK74beG9Y8rBwFfDgPfxkFogcHudl>

# Κακόβουλο λογισμικό

## HOW DOES QAKBOT WORK?



1. The victim receives an email with an attachment or hyperlink and **clicks on it**;



2. Qakbot deceives the victim into **downloading** malicious files by imitating a legitimate process;



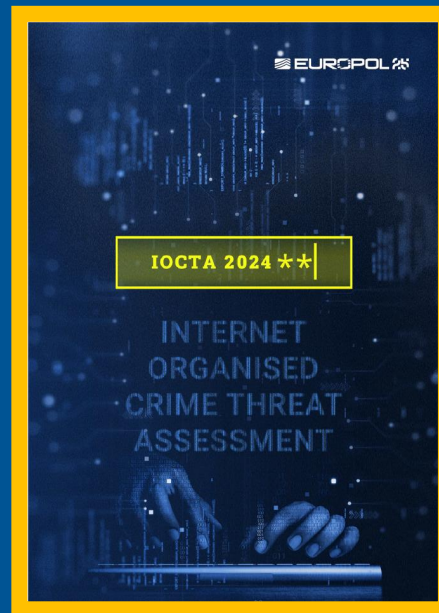
3. Qakbot executes and then installs other **malware**, such as banking Trojans;



4. The attacker then **steals** financial data, browser information/hooks, keystrokes, and/or credentials;



5. Other malware, such as **ransomware**, is placed on the victim's computer.

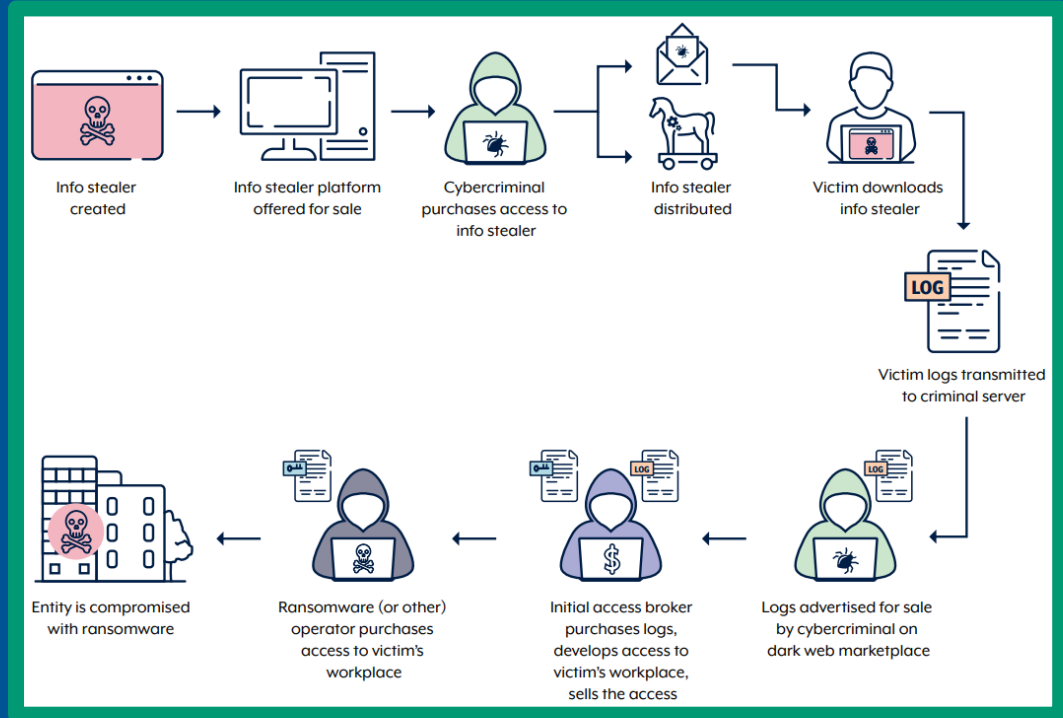


Πηγή:

<https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>

P. 21-22

# Οικοσύστημα Κλοπής Πληροφοριών

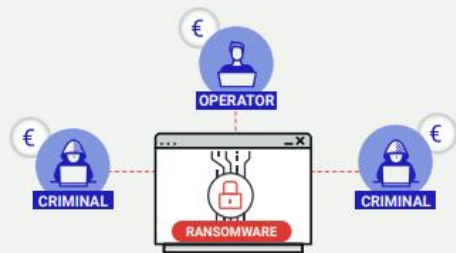


## Πηγή:

[https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/silent-heist-cybercriminals-use-information-stealer-malware-compromise-corporate-networks?fbclid=IwY2xjawFVL5pleHRuA2FibQIxMQABHVR\\_kL-4wT2oBKfZKMd9kJvxu\\_ws1qJ\\_SmDYfLAMOpxZKLyP1HgTa4D\\_8A\\_aem\\_dnyELhhmuZBp7qNX3mBUqg](https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/silent-heist-cybercriminals-use-information-stealer-malware-compromise-corporate-networks?fbclid=IwY2xjawFVL5pleHRuA2FibQIxMQABHVR_kL-4wT2oBKfZKMd9kJvxu_ws1qJ_SmDYfLAMOpxZKLyP1HgTa4D_8A_aem_dnyELhhmuZBp7qNX3mBUqg)

# Ransomware- Λυτρισμικό

## The fight against ransomware



### RANSOMWARE AFFILIATE PROGRAMS



### MULTI-LAYERED EXTORTION METHODS

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

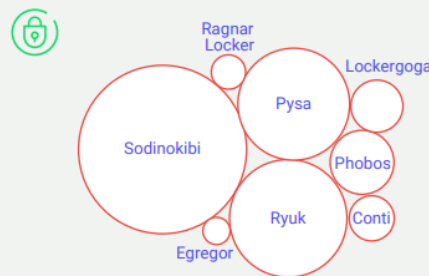
Threatening DDoS attack against victim

Exfiltrating data and threatening publication/action

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

## WHAT EUROPOL IS DOING

### RANSOMWARE CASE REQUESTS TO EUROPOL 2020 - 2021



EUROPEAN MALWARE ANALYSIS SOLUTION (EMAS)  
Contributions increase 2020 - 2021  
100%



Cybercrime – Attacks Against Information Systems



Coordinated action against key cybercrime threats and targets



Provides the victims of ransomware tools to decrypt their systems

Πηγή:

[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



# Νέα δωρεάν χρηστικά εργαλεία



< /> NO MORE RANSOM

Συμβουλές για χρήστες του διαδικτύου

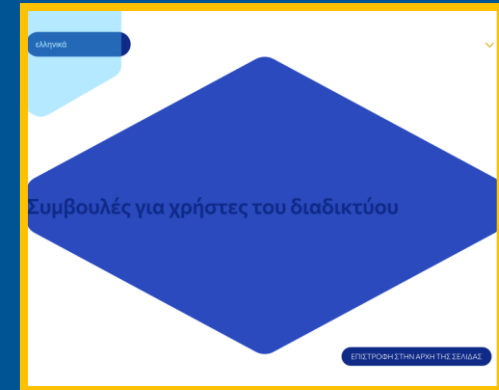
Συνεργάτες Σχετικά με το έργο ελληνικά

Αρχική σελίδα Crypto Sheriff Λυτρισμικό: Ερωτήσεις & απαντήσεις Συμβουλές πρόληψης Εργαλεία αποκρυπτογράφησης Καταγγείτε ένα έγκλημα

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

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

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



ελληνικά

Συμβουλές για χρήστες του διαδικτύου

ΕΠΙΣΤΡΟΦΗ ΣΤΗΝ ΑΡΧΗ ΤΗΣ ΣΕΛΙΔΑΣ

**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>



# Επιγραμμικές απάτες – Online Frauds

Buying on the dark web?  
You are on the menu!

EUROPOL



you



## 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.

### HOW DOES IT WORK?

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

They have a good knowledge about the organization.

They require an urgent payment.

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

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



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

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

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

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

### WHAT ARE THE SIGNS?

- Unsolicited email/phone call
- Direct contact from a senior official you are normally not in contact with
- Request for absolute confidentiality
- Pressure and a sense of urgency
- Unusual request in contradiction with internal procedures
- Threats or unusual flattery/promises of reward

**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>

# Διαδικτυακές απάτες-Οδηγίες της ΤτΕ

## Πώς προστατεύομαι από τις ηλεκτρονικές απάτες

### 1 ΕΝΗΜΕΡΩΝΟΜΑΙ ΔΙΑΡΚΩΣ...

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



### 2 ΕΙΜΑΙ ΣΕ ΕΓΡΗΓΟΡΗ...

...απέναντι σε μη συνήθεις συμπεριφορές και καταστάσεις (π.χ. ενημέρωση για «μεγάλες ευκαιρίες», ατήματα 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...

...ηλεκτρολογώ ενόσω 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 λουκιέτου).



### 3 ΦΡΟΝΤΙΖΩ ΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ ΜΟΥ...



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

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

### 7 ΕΙΜΑΙ ΙΔΙΑΙΤΕΡΑ ΠΡΟΣΕΚΤΙΚΟΣ/-Η...

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



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

...τα μηνύματα που συνοδεύουν κωδικούς μιας χρήσης OTP, ειδοποιήσεις για σύνδεση νέων συσκευών, ψηφιακών πορτοφολιών, υπηρεσιών πληρωμών και επιβεβαιώσω 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 ΔΙΓΕΛΙΑ 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 ΥΠΟΨΗ ΟΤΙ Η ΤΡΑΠΕΖΑ ΔΕΝ ΘΑ ΜΟΥ ΖΗΤΗΣΕΙ ΠΟΤΕ...

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

### 12 ΑΠΟΦΕΥΓΩ ΝΑ ΣΥΝΔΕΘΩΜΑΙ...

...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 απλοικών ή προβλεπόμενων κωδικών.



### 14 ΔΕΝ ΑΝΤΑΠΟΚΡΙΝΟΜΑΙ...

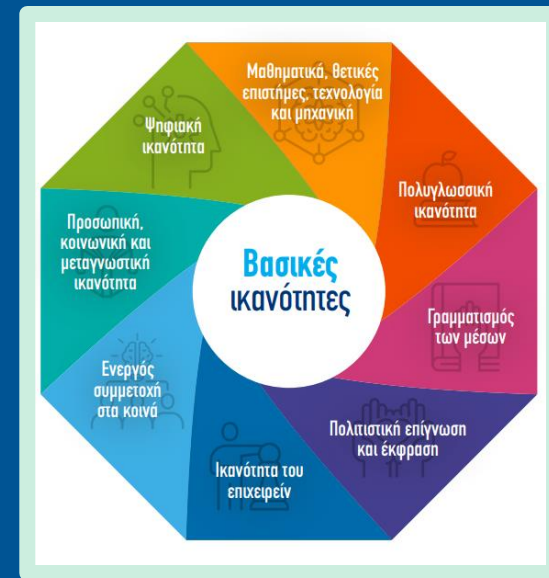
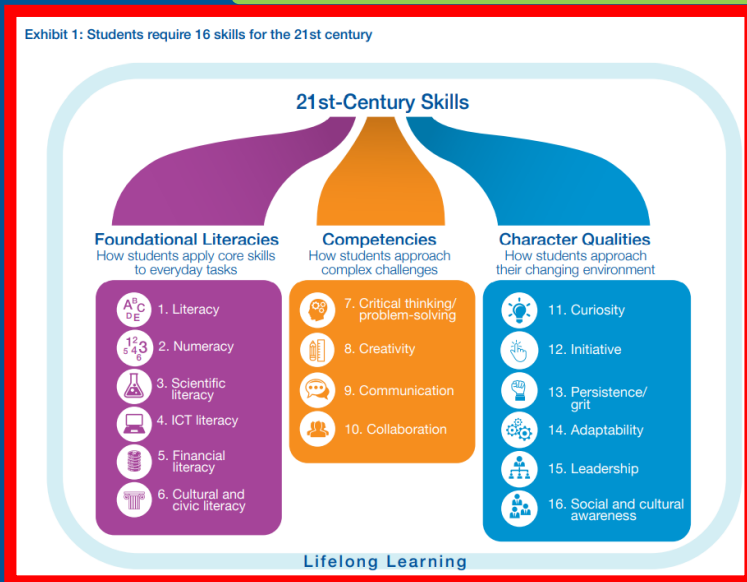
...σε αναπάντεχες κλήσεις από υποτιθέμενους παρόχους υπηρεσιών (Microsoft, EΛΤΑ, ΔΕΗ, Εφορία κλπ) χωρίς να έχει γίνει πρώτα αίτημα από εμένα.

### 15 ΑΚΟΜΑ ΚΑΙ ΜΕ ΤΗΝ ΥΠΟΨΙΑ 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.

# Αιώνας Νέων Δεξιοτήτων-Ψηφιακός Αλφαριθμητισμός

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

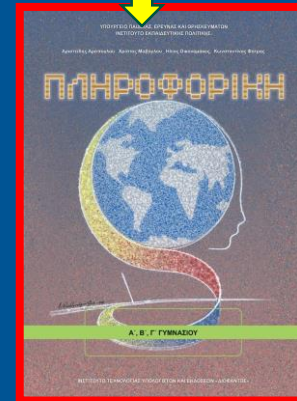


## Πηγές:

1. <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives>
2. <https://www.nationalcoalition.gov.gr/ds-resource/diathesimi-i-elliniki-ekdosi-toy-eyrop/>
3. <https://www.weforum.org/agenda/2016/03/21st-century-skills-future-jobs-students/>
4. [https://www3.weforum.org/docs/WEF\\_Schools\\_of\\_the\\_Future\\_Report\\_2019.pdf](https://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf)
5. <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives>
6. <https://www.weforum.org/agenda/2016/03/21st-century-skills-future-jobs-students/>
7. [https://www3.weforum.org/docs/WEF\\_Schools\\_of\\_the\\_Future\\_Report\\_2019.pdf](https://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf)
8. <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles?fbclid=IwAR0eoti200iJEF4TyAfzDuKMuyiJ2ihlvGQ9yYci32Oai61QSvXNSo7Xad8> σημεία 4 (ψηφιακή **εκπαίδευση** και κατάρτιση και ψηφιακές δεξιότητες), 16 (**ασφαλές** και προστατευμένο ψηφιακό περιβάλλον), 20,21,22 (**προστασία** και ενδυνάμωση των παιδιών και των νέων στο ψηφιακό περιβάλλον)
9. <https://www.unesco.org/en/digital-competencies-skills/ict-cft>

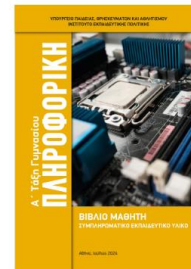
# Εκπαιδευτικό υλικό σύγχρονο και επίκαιρο

!!!!!!!

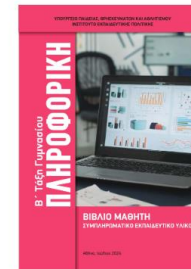


## Πηγές:

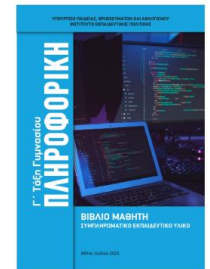
1. <https://nationaldigitalacademy.gov.gr/>
2. <https://iep.edu.gr/el/gymnasio/pliροφοriki>



Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Α' Γυμνασίου



Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Β' Γυμνασίου



Πρόσθετο Ψηφιακό Εγχειρίδιο Πληροφορικής Γ' Γυμνασίου



# Δεξιότητες που συνδέονται **άμεσα** με **επαγγελματικές** 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:**

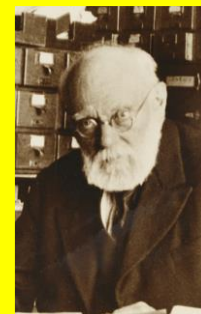
<https://cyber.org/career-exploration>

**SOFTWARE  
DEVELOPER**



# Πληροφορίες & πηγές για καλές πρακτικές

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



Paul Otlet  
1868-1944



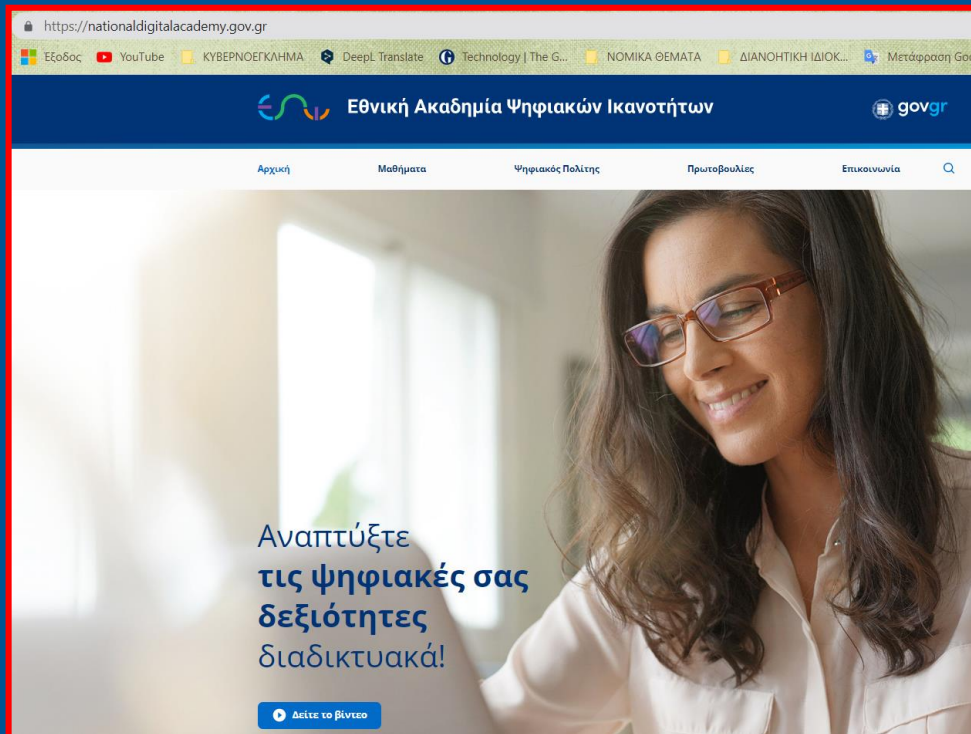
## Πηγές:

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

Κρίσιμο στοιχείο η  
αξιοπιστία και ο βαθμός  
επικαιροποίησης του υλικού



# Εθνική Ακαδημία Ψηφιακών Ικανοτήτων



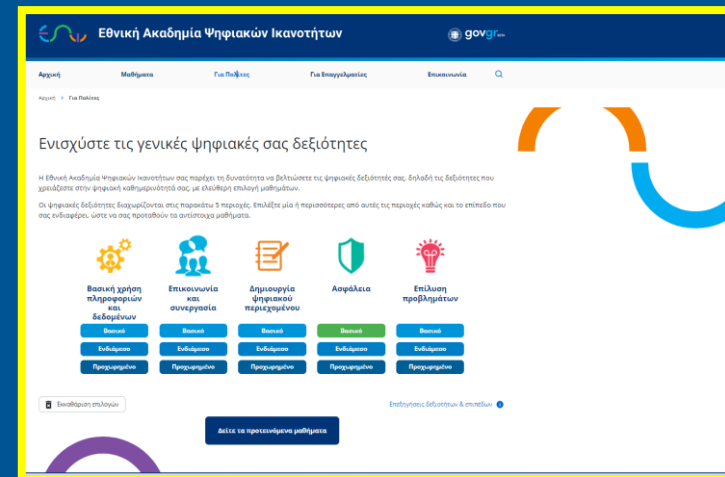
<https://nationaldigitalacademy.gov.gr>

Εθνική Ακαδημία Ψηφιακών Ικανοτήτων govgr

Αρχική Μαθήματα Ψηφιακές Πολιτικές Πρωτοβουλίες Επικοινωνία

Αναπτύξτε τις ψηφιακές σας δεξιότητες διαδικτυακά!

Δείτε το βίντεο



Εθνική Ακαδημία Ψηφιακών Ικανοτήτων govgr

Αρχική Μαθήματα Για Πολίτες Για Επαγγελματίες Επικοινωνία

Ενισχύστε τις γενικές ψηφιακές σας δεξιότητες

Η Εθνική Ακαδημία Ψηφιακών Ικανοτήτων σας παρέχει τη δυνατότητα να βελτιώσετε τις ψηφιακές δεξιότητές σας, δοσολογώντας τις δεξιότητες που χρειάζεστε στον ψηφιακό καθημερινότητά σας, με καλύτερη επιλογή μαθημάτων.

Οι ψηφιακές δεξιότητες διαχωρίζονται στις παρακάτω 5 παραγωγές. Επιλέξτε μία ή περισσότερες από αυτές τις παραγωγές καθώς και το επίπεδο που σας ενδιαφέρει, ώστε να σας προταθούν τα αντίστοιχα μαθήματα.

Βασική χρήση πληροφοριών και δεδομένων	Επικοινωνία και συνεργασία	Δημιουργία ψηφιακού περιεχομένου	Ασφάλεια	Επίλυση προβλημάτων
Βασικό	Βασικό	Βασικό	Βασικό	Βασικό
Επίδειγμα	Επίδειγμα	Επίδειγμα	Επίδειγμα	Επίδειγμα
Προσφιλές	Προσφιλές	Προσφιλές	Προσφιλές	Προσφιλές

Επιλέξτε επίπεδο & επιπέδωση

Δείτε τα προτεινόμενα μαθήματα

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

Με 350 μαθήματα  
35 θεματικές ενότητες  
1800 ώρες εκπαίδευσης

Στοιχεία στις 17/9/2024

# Από πλευράς της πολιτείας

Στρατηγική και Όραμα

Πολιτική βούληση & ευρύτερη δυνατή συναίνεση

Κουλτούρα Συνεργασίας Φορέων (Ακαδημαϊκή Κοινότητα, Δημόσιος και Ιδιωτικός Τομέας)

Κουλτούρα Τεχνηθικής

Θεσμική θωράκιση (2ο πρωτόκολλο Cybercrime Convention, εξειδίκευση δικαστών, τραπεζικό απόρρητο, Medicrime convention, Αναβάθμιση Συστήματος Αναφοράς Κυβερνοεγκλημάτων, κα..)

Διάθεση Πόρων για την Κυβερνοασφάλεια

Αξιοκρατία – Διαφάνεια - Δικαιοσύνη



# Από την πλευρά των επιχειρήσεων

Ανάπτυξη Κουλτούρας Κυβερνοασφάλειας

Διενέργεια Εσωτερικών Ελέγχων Κυβερνοασφάλειας

Δυνατότητες που υπάρχουν στο άμεσο περιβάλλον

Παροχή κατάλληλης εκπαίδευσης – κατάρτισης

Διασφάλιση Διαχείρισης Τρίτων μερών για σεβασμό των πολιτικών κυβερνοασφάλειας και προστασίας των προσωπικών δεδομένων

Σχέδιο Αντιμετώπισης Κυβερνοπεριστατικού

Ασφαλή πρόσβαση στα πληροφοριακά συστήματα

Ασφαλείς συσκευές (με επικαιροποιημένο λογισμικό, Προγράμματα Προστασίας, Κρυπτογράφηση)





**SMART  
ATTICA** European  
Digital  
Innovation  
Hub



ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΤΕΚΜΗΡΙΩΣΗΣ &  
ΗΛΕΚΤΡΟΝΙΚΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ

**Ευχαριστώ!**

*Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης. Ωστόσο, οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης. Ούτε η Ευρωπαϊκή Ένωση ούτε η χορηγούσα αρχή μπορούν να θεωρηθούν υπεύθυνες για αυτές.*