

ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

ΤΡΟΠΟΙ ΑΝΑΓΝΩΡΙΣΗΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ

Βασίλης Χατζής
Δρ. Πληροφορικής
Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας
Διεθνές Πανεπιστήμιο της Ελλάδος

Safer Internet Day takes
place every February



Ημέρα Ασφαλούς Διαδικτύου

Θα μιλήσουμε για...

- τις βασικές αρχές της ηλεκτρονικής εγκληματολογίας,
- τα είδη και τις μορφές των ηλεκτρονικών εγκλημάτων,
- τρόποι προστασίας, εκπαίδευση, φορείς,
- την έννοια, τον τρόπο απόκτησης και διαχείρισης των ψηφιακών αποδεικτικών στοιχείων,
- τα λογισμικά και τα εργαλεία που βοηθάνε στην εξιχνίαση ηλεκτρονικών εγκλημάτων

Εγκληματολογική Επιστήμη

Η Εγκληματολογική Επιστήμη (*Forensic Science*), ασχολείται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων, που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο ή γενικότερα πρόσωπα και αποδεικτικά στοιχεία.

Η ανάλυση του DNA και η εξέταση των δακτυλικών αποτυπωμάτων είναι μερικές από τις δυνατότητες που χρησιμοποιεί η επιστήμη αυτή.

Ηλεκτρονική Εγκληματολογία

Ο πιο αποδεκτός ορισμός της *Ηλεκτρονικής Εγκληματολογίας (Digital Forensic)* προκύπτει από τον ορισμό της *εγκληματολογικής επιστήμης των υπολογιστών (Forensic Computing Science)*.

Η εγκληματολογική επιστήμη υπολογιστών, είναι “η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό”

Ηλεκτρονικό έγκλημα

- Έγκλημα είναι μια επιθετική πράξη εναντίον της κοινωνίας ή ενός ατόμου που παραβιάζει τουλάχιστον έναν νόμο και τιμωρείται.
- Ως ηλεκτρονικό έγκλημα μπορεί να θεωρηθεί *“μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της”*.

Ηλεκτρονικό έγκλημα (2)

- Η Ευρωπαϊκή Ένωση, σύμφωνα με τη Συνθήκη κατά του Ηλεκτρονικού Εγκλήματος ορίζει το Ηλεκτρονικό Έγκλημα ως “οποιαδήποτε εγκληματική ενέργεια διεπράχθη εναντίον ή με τη βοήθεια ενός ηλεκτρονικού υπολογιστή ή δικτύου ηλεκτρονικών υπολογιστών”
- Βρετανική Αστυνομία αναφέρει ότι ηλεκτρονικό έγκλημα είναι “η χρήση ηλεκτρονικού υπολογιστή ή δικτύου ηλεκτρονικών υπολογιστών για την διάπραξη εγκλήματος”

Μορφές Ηλεκτρονικού Εγκλήματος

Στο ηλεκτρονικό έγκλημα η ηλεκτρονική συσκευή μπορεί :

- Να αποτελεί το στόχο κάποιας επίθεσης. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το “θύμα” της επίθεσης.
- Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή).
- Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

Ηλεκτρονικά εγκλήματα σε σχέση με τα παραδοσιακά

- Οι οικονομικές απώλειες που προξενούνται στα “ψηφιακά” θύματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων.
- Ένα μεγάλο μέρος δεν καταγγέλλεται και έτσι δεν καταγράφεται από καμία επίσημη αρχή.
- Ένα μεγάλο μέρος δεν γίνεται αντιληπτό από το θύμα.

Ηλεκτρονικά εγκλήματα σε σχέση με τα παραδοσιακά

- Διαπράττονται συνήθως από μακρινή απόσταση (τρίτες χώρες).
- Ο εντοπισμός του ηλεκτρονικού εγκληματία είναι τεχνολογικά περίπλοκος.
- Αποδίδουν μεγάλα κέρδη με μικρό κίνδυνο ανακάλυψης του δράστη.
- Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος.

Κατηγορίες Ηλεκτρονικών Εγκλημάτων

- Ανεπιθύμητη Αλληλογραφία (Spamming)
- Ηλεκτρονικό ψάρεμα (Phishing)
- Απώλεια Πνευματικών Δικαιωμάτων / Πειρατεία λογισμικού, ταινιών, ψηφιακού υλικού
- Κακόβουλες εισβολές σε δίκτυα φωνής και δεδομένων (π.χ. παρακολουθήσεις)
- Κακόβουλο λογισμικό (ransomware, viruses, worms, trojan horses, bots, keyloggers ...)

CYBERTHREAT REAL-TIME MAP EN

MAP STATISTICS DATA SOURCES BUZZ WIDGET

GREECE

54 MOST-ATTACKED COUNTRY

OAS	19936
ODS	10449
MAV	6566
WAV	41478
IDS	13358
VUL	559
KAS	9328
BAD	0
RAW	92

Detections discovered since 00:00 GMT

[More details](#)

Share data



9550300	4508841	456754	7717211	11013758	153234	6030082	2933	38660
OAS	ODS	MAV	WAV	IDS	VUL	KAS	BAD	RAW

<https://cybermap.kaspersky.com/>

Κατηγορίες Ηλεκτρονικών Εγκλημάτων (2)

- Επιθέσεις Άρνησης Εξυπηρέτησης (DOS - denial of service - attacks)
- Επιθέσεις σε δικτυακούς τόπους
- Hacking / Cracking /Ethical Hacking
- Επιθέσεις παρενόχλησης (cyberbullying)
- Κλοπή ταυτότητας
- Διακίνηση υλικού παιδικής πορνογραφίας

Κατηγορίες Ηλεκτρονικών Εγκλημάτων (3)

- Οικονομικές Απάτες στο Διαδίκτυο
- Ξέπλυμα χρήματος / Ηλεκτρονικο-οικονομικά εγκλήματα / Ψηφιακά νομίσματα (4038)
- Man in the middle
- Τρομοκρατία
- Κατασκοπεία (βιομηχανική, κρατική, πολιτική)

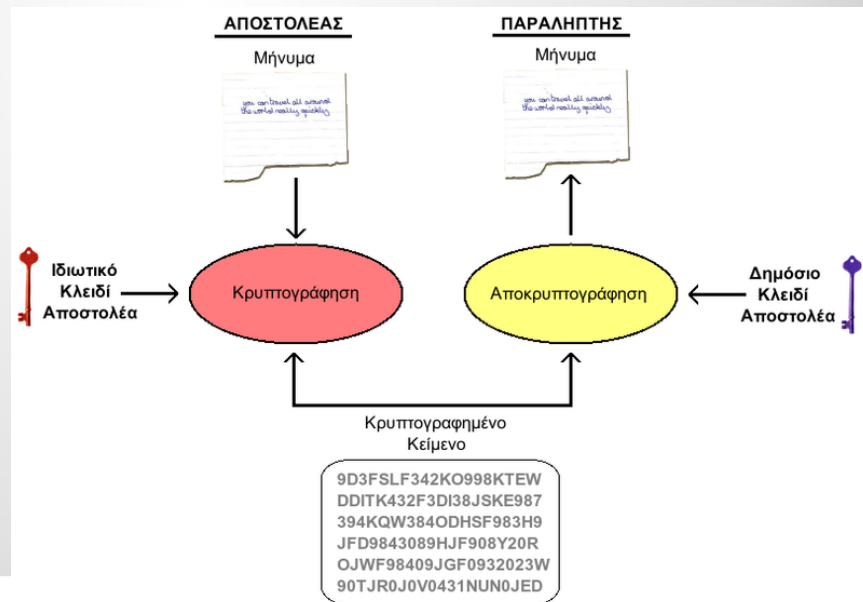
Τεχνολογίες Προστασίας

Passwords (π.χ. 123, qwerty, 15011975, apostolos)

Antivirus, Antimalware, Online & email protection κ.α.

Ασφαλή πρωτόκολλα επικοινωνίας (π.χ. https)

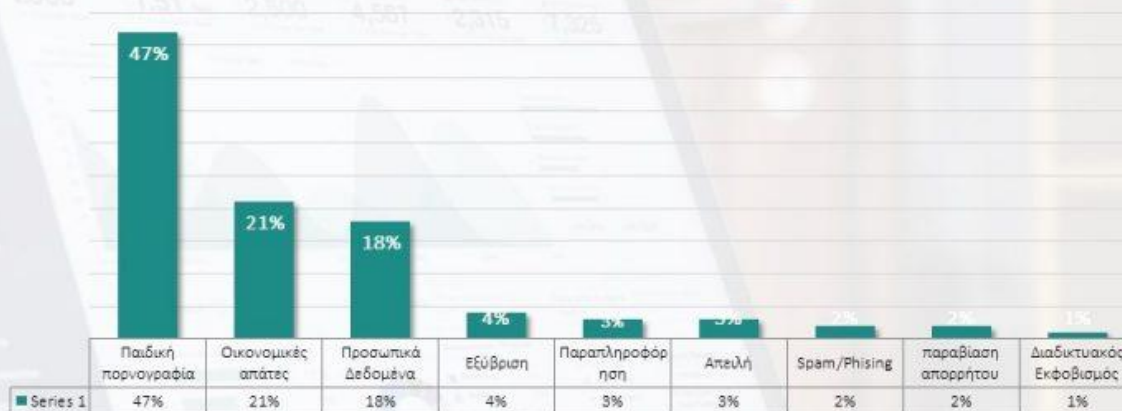
Κρυπτογράφηση



Στατιστικά Στοιχεία

Καταγγελίες στο safeline.gr

ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ SafeLine.gr ΓΙΑ ΤΟ 2020



Για πρώτη φορά η γραμμή δέχτηκε καταγγελίες για ψευδείς ειδήσεις.



47%

Καταγγελίες για υλικό παιδικής κακοποίησης



21%

Καταγγελίες για οικονομικές απάτες.



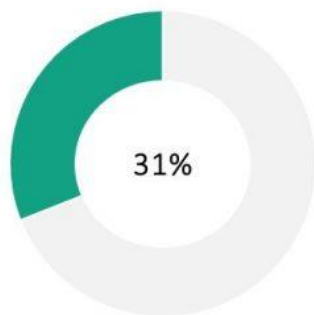
18%

Καταγγελίες για αποκάλυψη προσωπικών δεδομένων.

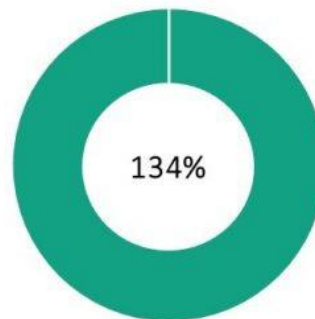
Στατιστικά Στοιχεία

Καταγγελίες στο safeline.gr

Στατιστικά στοιχεία SafeLine.gr για το 2020



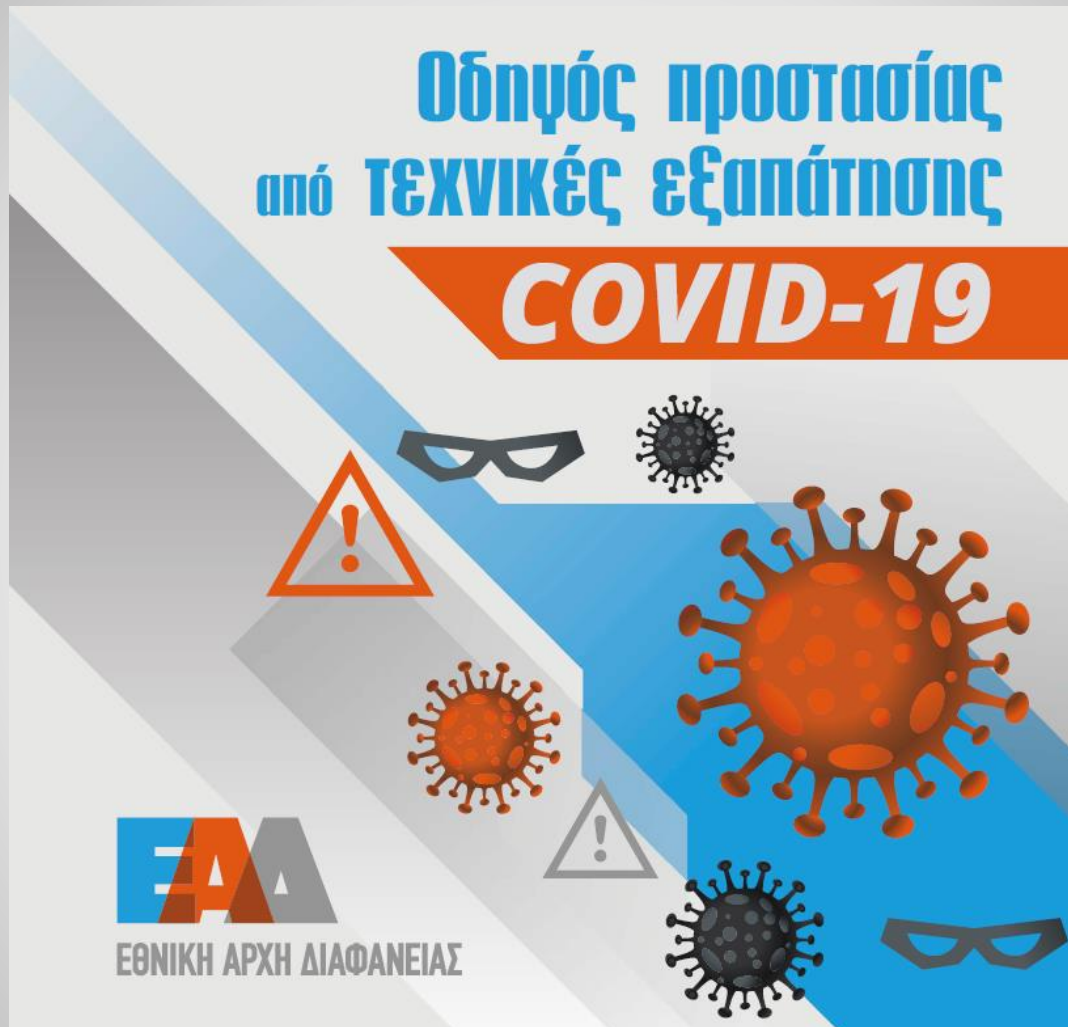
› Αύξηση 31% στο σύνολο των καταγγελιών που δέχτηκε η SafeLine.gr κατά το 2020



› Αύξηση 134% στις καταγγελίες για οικονομικές απάτες στη διάρκεια του πρώτου lockdown (Απρίλιος-Μάιος 2020) σε σχέση με το αντίστοιχο διάστημα το 2019.

Οδηγός προστασίας από ΤΕΧΝΙΚΕΣ εξαπάτησης

COVID-19



<https://aead.gr/publications/manuals>

Οδηγός προστασίας

- Η πανδημία της νόσου του κορωνοϊού - COVID 19 επηρεάζει άμεσα την καθημερινότητά μας, την οικονομία, τη δημόσια υγεία, τις μεταφορές και τα δίκτυα επικοινωνίας.
- Δημιουργεί πρόσφορο έδαφος και «ευκαιρίες» για απάτες και παράνομες ενέργειες.
- Σε διεθνές επίπεδο και στη χώρα μας έχουν ήδη καταγραφεί πολυάριθμα σχήματα και πρακτικές απάτης που εκμεταλλεύονται τον φόβο και την ανασφάλεια των ανθρώπων για τον κορωνοϊό.

Πρακτικές εξαπάτησης

- **Θεραπεία (Treatment scams)**

Οι απατεώνες προσφέρουν ψεύτικες θεραπείες, εμβόλια και ιατρικές συμβουλές σχετικά με μη δοκιμασμένες θεραπείες για τον COVID-19.

- **Πάροχοι υπηρεσιών υγείας (Health provider scams)**

Οι απατεώνες επικοινωνούν με τηλεφωνικά και ηλεκτρονικά μηνύματα, προσποιούμενοι ότι είναι εκπρόσωποι δημόσιων φορέων (Υπουργείο Υγείας, Ε.Ο.Δ.Υ. κ.α.) ή / και επαγγελματίες υγείας (γιατροί, νοσηλευτές, επόπτες υγείας κ.ά.) που νοσηλεύουν έναν φίλο ή συγγενή για τον COVID-19 και απαιτούν πληρωμή για την περίθαλψή του.

Πρακτικές εξαπάτησης

- **Προμήθεια (Supply scams)**

Οι απατεώνες δημιουργούν ψεύτικα ηλεκτρονικά καταστήματα, ιστότοπους, λογαριασμούς μέσων κοινωνικής δικτύωσης και διευθύνσεις ηλεκτρονικού ταχυδρομείου, μέσω των οποίων ισχυρίζονται ότι πωλούν ιατρικά προϊόντα που στην παρούσα φάση βρίσκονται σε μεγάλη ζήτηση, όπως χειρουργικές μάσκες.

Όταν οι καταναλωτές επιχειρούν να αγοράσουν προϊόντα μέσω αυτών των καναλιών, οι απατεώνες εισπράττουν τα χρήματα και δεν παρέχουν ποτέ τις υποσχεθείσες προμήθειες ή παραδίδουν ελαττωματικά ή μη ανταποκρινόμενα στις διαφημιζόμενες ιδιότητες προϊόντα.

Σε αυτές τις περιπτώσεις εκτός από την οικονομική ζημία ενδέχεται τα προϊόντα αυτά να είναι και επιβλαβή για την υγεία των καταναλωτών.

Πρακτικές εξαπάτησης

- **Έρανοι / Φιλανθρωπίες (Charity scams)**

Οι απατεώνες ζητούν δωρεές για άτομα, ομάδες και περιοχές που έχουν πληγεί από τον COVID-19 ή για να χρηματοδοτήσουν την ιατρική έρευνα για το εμβόλιο, την αγορά ιατρικού εξοπλισμού κ.ά.

- **Εφαρμογές Κινητών / Tablets (App scams)**

Οι απατεώνες επίσης δημιουργούν και χειραγωγούν εφαρμογές για κινητά που έχουν σχεδιαστεί για την παρακολούθηση της εξάπλωσης του COVID-19 προκειμένου να παρασύρουν τους χρήστες να κατεβάσουν κακόβουλο λογισμικό που θέτει σε κίνδυνο τις συσκευές και τις προσωπικές πληροφορίες τους.

Πρακτικές εξαπάτησης

- **Ηλεκτρονικό «ψάρεμα» (e-Phishing scams)**

Οι απατεώνες εμφανίζονται ως δήθεν εκπρόσωποι εθνικών και παγκόσμιων υγειονομικών Αρχών, συμπεριλαμβανομένου του Παγκόσμιου Οργανισμού Υγείας (WHO) και των Κέντρων Ελέγχου και Πρόληψης Νοσημάτων (CDC), αποστέλλοντας μηνύματα ηλεκτρονικού «ψαρέματος» (phishing e-mails) που αποσκοπούν στο να παρασύρουν τους παραλήπτες στο «κατέβασμα» κακόβουλου λογισμικού, προκειμένου να υποκλέψουν προσωπικά στοιχεία ταυτοποίησης και τραπεζικές πληροφορίες.

Οδηγός προστασίας

- Επαληθεύστε τα στοιχεία, την έδρα και τη φήμη της εταιρείας / προσώπου που προσφέρει τα αγαθά ή τις υπηρεσίες πριν από την πραγματοποίηση οποιωνδήποτε αγορών.
- Να είστε ιδιαίτερα επιφυλακτικοί με πολύ δελεαστικές προσφορές που υπόσχονται να σας αποστείλουν αγαθά, για τα οποία μάλιστα δεν υπάρχει μεγάλη διαθεσιμότητα στην αγορά (χειρουργικές μάσκες, αντισηπτικά κ.ά.), σε πολύ καλές τιμές ή διαφημίζουν φαρμακευτικά προϊόντα που θωρακίζουν ή / και θεραπεύουν τον οργανισμό από τον κορωνοϊό.
- Να είστε σε εγρήγορση για τον εντοπισμό ψεύτικων ιστότοπων δεδομένου ότι οι εγκληματίες συχνά χρησιμοποιούν μια διεύθυνση ιστού που μοιάζει σχεδόν με τη νόμιμη διεύθυνση, π.χ. "Abc.org" αντί για "abc.com".

Οδηγός προστασίας

- Επαληθεύστε προσωπικά ότι ο ιστότοπος ή η διεύθυνση ηλεκτρονικού ταχυδρομείου προέρχεται πραγματικά από τον Οργανισμό που φαίνεται με την πρώτη ματιά. Για παράδειγμα, ο Παγκόσμιος Οργανισμός Υγείας συστήνει να επαληθεύετε τον αποστολέα ελέγχοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου: ένα επίσημο μήνυμα ηλεκτρονικού ταχυδρομείου του Π.Ο.Υ. θα αποσταλεί μόνο από μια διεύθυνση που τελειώνει σε @who.int
- Ελέγξτε τις on-line αξιολογήσεις (reviews) των καταναλωτών για την πωλήτρια εταιρεία πριν πραγματοποιήσετε μια αγορά - για παράδειγμα, έχουν υπάρξει παράπονα άλλων πελατών που δεν λαμβάνουν τα υποσχεθέντα αγαθά / υπηρεσίες.
- Να είστε ιδιαίτερα επιφυλακτικοί, εάν σας ζητείται να κάνετε μια πληρωμή σε τραπεζικό λογαριασμό που βρίσκεται σε διαφορετική χώρα από εκεί που βρίσκεται η πωλήτρια εταιρεία και σε κάθε περίπτωση να παρακολουθείτε σε καθημερινή βάση την κίνηση των τραπεζικών λογαριασμών σας.

Οδηγός προστασίας

- Ειδοποιήστε αμέσως την Τράπεζά σας για να σταματήσετε την πληρωμή, εάν πιστεύετε ότι έχετε πέσει θύμα διαδικτυακής απάτης.
- Χρησιμοποιήστε προπληρωμένες πιστωτικές κάρτες ή τη μέθοδο της αντικαταβολής όταν κάνετε μια αγορά μέσω διαδικτύου για μεγαλύτερη προστασία και μην στέλνετε προκαταβολικά χρήματα σε άτομα που δεν γνωρίζετε.
- Μην κάνετε κλικ σε ηλεκτρονικούς συνδέσμους (links) και μην ανοίγετε συνημμένα αρχεία που δεν περιμένατε να λάβετε, ή προέρχονται από άγνωστο αποστολέα.
- Μην μοιράζετε διαδικτυακά ειδήσεις που δεν προέρχονται από επίσημες πηγές και δεν μπορείτε να τις επαληθεύσετε.
- Μην κάνετε δωρεές μέσω ηλεκτρονικών πλατφορμών / συνδέσμων σε φιλανθρωπικές οργανώσεις χωρίς να ελέγχετε εάν όντως πρόκειται για νόμιμες οργανώσεις ή νόμιμους φορείς.

Οδηγός προστασίας

- Μην αποκαλύπτετε προσωπικά, τραπεζικά ή οικονομικά στοιχεία (ΑΔΤ, κωδικούς e-banking, κωδικούς τραπεζικών καρτών, passwords και login κωδικούς ηλεκτρονικού ταχυδρομείου κ.ά.) σε απάντηση ηλεκτρονικών μηνυμάτων, καθώς και σε εφαρμογές ή links που αποστέλλονται με την ένδειξη κάποιας επιβράβευσης ή προσφοράς.
- Να είστε προσεκτικοί σε μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν τα προσωπικά σας στοιχεία για να προγραμματίσουν ιατρικούς ελέγχους ή έρευνες. Οι δημόσιες υγειονομικές Αρχές κατά κανόνα δεν έρχονται σε επαφή με το ευρύ κοινό κατ' αυτόν τον τρόπο.
- Μην ενδίδετε σε πιέσεις για να αποκαλύψετε οποιαδήποτε προσωπική πληροφορία. Οι κυβερνοεγκληματίες χρησιμοποιούν καταστάσεις έκτακτης ανάγκης, όπως ο κορωνοϊός, για να τρομάξουν τους ανθρώπους και να τους ωθήσουν σε επιπόλαιες αποφάσεις.

Οδηγός προστασίας

Οι χρήστες του διαδικτύου καλούνται

- να ασφαλίζουν το wifi του σπιτιού τους,
 - να ασφαλίζουν όλες τις συσκευές τους με κωδικούς, PIN ή βιομετρικά στοιχεία (αποτύπωμα ή αναγνώριση προσώπου),
 - να εγκαθιστούν λογισμικό προστασίας από ιούς,
 - να ενημερώνουν το λογισμικό που χρησιμοποιούν,
 - να βάζουν ισχυρούς και διαφορετικούς ανά εφαρμογή κωδικούς πρόσβασης (passwords),
 - να τηρούν αντίγραφα ασφαλείας σε εξωτερικά αποθηκευτικά μέσα, μη συνδεδεμένα με τις συσκευές,
 - να ελέγχουν τις ρυθμίσεις απορρήτου των λογαριασμών των μέσων κοινωνικής δικτύωσης και τα δικαιώματα των εφαρμογών που είναι εγκατεστημένες στις συσκευές τους διαγράφοντας όποιες δεν χρησιμοποιούνται.
-
- **Να ενημερώνουν τις αστυνομικές Αρχές, σε κάθε περίπτωση απόπειρας απάτης**

Φορείς

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας

<https://cyberalert.gr/>

Ελληνική Ένωση Τραπεζών

<https://www.hba.gr/Media/Details/457>

Ανεξάρτητη Εθνική Αρχή Διαφάνειας

<https://aead.gr/>

Συνήγορος του καταναλωτή

<http://www.synigoroskatanaloti.gr/index.html>

Ελληνικός Σύνδεσμος Ηλεκτρονικού Εμπορίου (GRECA)

<http://www.greekecommerce.gr/>



[Οφέλη](#)[Λίστα Μελών](#)[Διαδικασία Εγγραφής](#)[Αίτηση Μέλους](#)[Σήμα GRECA](#)[GR.EC.A Trustmark](#)[Αρχική](#) > [Μέλη](#) > [Σήμα GRECA](#)

Σήμα GRECA



Όλα τα ταμειακά ενήμερα μέλη του GRECA έχουν δικαίωμα να τοποθετήσουν στις ιστοσελίδες τους το παρακάτω σήμα, το οποίο πιστοποιεί ότι είναι μέλη του συνδέσμου. Προσδίδουν έτσι αξιοπιστία στο ηλεκτρονικό τους κατάστημα, καθώς οι χρήστες θα γνωρίζουν ότι το εν λόγω κατάστημα είναι μέλος του Ελληνικού Συνδέσμου Ηλεκτρονικού Εμπορίου.





Εργαλείο αυτοαξιολόγησης

Αξιολογήστε τις γενικές ψηφιακές δεξιότητές σας κι αναγνωρίστε το επίπεδό σας με βάση το DigComp.

Ενισχύστε τις γενικές ψηφιακές σας δεξιότητες

Αναζητήστε μαθήματα με βάση τις δεξιότητες που χρειάζεστε ως πολίτης.

Εμπλουτίστε τις εξειδικευμένες ψηφιακές σας δεξιότητες

Αναζητήστε μαθήματα με βάση τις δεξιότητες που χρειάζεστε ως επαγγελματίας.

Κατηγορίες Μαθημάτων

214 μαθήματα για την βελτίωση των ψηφιακών δεξιοτήτων των πολιτών.

Επικοινωνία και συνεργασία

Κινητές συσκευές, κοινωνικά δίκτυα, εφαρμογές επικοινωνίας, εργασία από το σπίτι.

Διαδίκτυο

Ασφαλής περιήγηση, μηχανές αναζήτησης, προστασία προσωπικών δεδομένων, ανάπτυξη και αξιολόγηση περιεχομένου.

Εργαλεία καθημερινής χρήσης

Χρήση υπολογιστή, εφαρμογές γραφείου.

Ψηφιακή επιχειρηματικότητα

Ψηφιακό μάρκετινγκ, σύγχρονο επιχειρηματικό πλαίσιο.

Επιστήμη υπολογιστών

Ανάπτυξη λογισμικού, ανάπτυξη εφαρμογών διαδικτύου και κινητών συσκευών κ.ά.

Τεχνολογίες αιχμής

Υπολογιστικό Νέφος, Τεχνητή Νοημοσύνη, Μηχανική Μάθηση, Μεγάλα Δεδομένα.



Ενισχύστε τις γενικές ψηφιακές σας δεξιότητες

Η Ψηφιακή Ακαδημία Πολιτών σας παρέχει τη δυνατότητα να βελτιώσετε τις γενικές ψηφιακές δεξιότητές σας, δηλαδή τις δεξιότητες που χρειάζεστε στην ψηφιακή καθημερινότητά σας, με ελεύθερη επιλογή μαθημάτων ανά επίπεδο στις 5 περιοχές ψηφιακών δεξιοτήτων.

Επιλέξτε μία ή περισσότερες περιοχές δεξιοτήτων καθώς και το επίπεδο που σας ενδιαφέρει ώστε να σας προταθούν τα αντίστοιχα μαθήματα.



**Βασική χρήση
πληροφοριών
και
δεδομένων**

Βασικό

Ενδιάμεσο

Προχωρημένο



**Επικοινωνία
και
συνεργασία**

Βασικό

Ενδιάμεσο

Προχωρημένο



**Δημιουργία
ψηφιακού
περιεχομένου**

Βασικό

Ενδιάμεσο

Προχωρημένο



Ασφάλεια

Βασικό

Ενδιάμεσο

Προχωρημένο



**Επίλυση
προβλημάτων**

Βασικό

Ενδιάμεσο

Προχωρημένο

<https://nationaldigitalacademy.gov.gr/enisxyste-tis-genikes-pshfiakes-sas-deksiothtes>

Συμπεράσματα

Ραγδαία αύξηση στα ηλεκτρονικά εγκλήματα και στο κόστος αυτών για τις επιχειρήσεις και οργανισμούς

Λήψη μέτρων ασφαλείας - Εγρήγορση των επιχειρήσεων και εκπαίδευση των εργαζομένων

Προσοχή στη διαχείριση των ευαίσθητων δεδομένων από ιδιώτες και επιχειρήσεις

Δυσκολίες στην αντιμετώπιση / εξιχνίαση των ηλεκτρονικών εγκλημάτων - Διεθνείς συνεργασίες και συνεχή εκπαίδευση των επαγγελματιών του χώρου