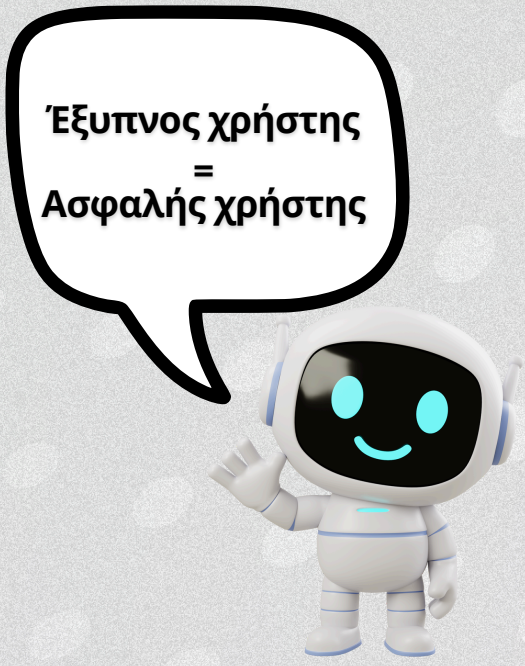
5+1 Ψηφιακοί Οδηγοί
*για όλους

Περιφέρεια Δυτικής Μακεδονίας
Αντιπεριφέρεια Διαφάνειας, Ηλεκτρονικής Διακυβέρνησης & Ψηφιακού Μετασχηματισμού

SYNERGINN EDIH

Ψηφιακός οδηγός

Ασφαλής Πλοήγηση στο Διαδίκτυο



Το διαδίκτυο: ευκαιρίες και κίνδυνοι



Το Διαδίκτυο έχει αλλάξει ριζικά τη ζωή μας. Μας δίνει τη δυνατότητα να ενημερωνόμαστε, να επικοινωνούμε, να ψυχαγωγούμαστε και να εργαζόμαστε από οπουδήποτε. Επιπλέον, προσφέρει τη δυνατότητα για ηλεκτρονικές πληρωμές και αγορές, κάνοντας τις οικονομικές μας συναλλαγές πιο εύκολες και γρήγορες.

Παράλληλα όμως, κρύβει και κινδύνους, ειδικά για όσους δεν έχουν εμπειρία στη χρήση του, καθώς απαιτείται προσοχή για την προστασία των προσωπικών δεδομένων και των οικονομικών στοιχείων.

Ο στόχος αυτού του οδηγού είναι να παρουσιάσει με απλό τρόπο όλα όσα χρειάζεται να γνωρίζει κάποιος για να προστατεύει τα προσωπικά του δεδομένα, τη συσκευή του και, πάνω απ' όλα, τον εαυτό του.

Κάθε φορά που συνδέεσαι στο **Διαδίκτυο,** θυμήσου ότι αφήνεις πίσω σου ίχνη.
Φρόντισε να είναι θετικά!

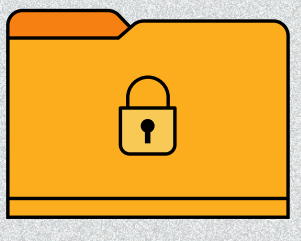
Ψηφιακό αποτύπωμα και προσωπικά δεδομένα



Κάθε ενέργεια που κάνεις στο Διαδίκτυο αφήνει ένα ίχνος: αυτό είναι το **ψηφιακό σου αποτύπωμα.**

Το **ψηφιακό αποτύπωμα** περιλαμβάνει τις αναρτήσεις σου, τα σχόλια, τις αναζητήσεις σου και τις φωτογραφίες που ανεβάζεις. Τα προσωπικά δεδομένα είναι πληροφορίες μέσω των οποίων μπορούν να σε ταυτοποιήσουν.





Η προστασία τους είναι απαραίτητη, γιατί μπορούν να χρησιμοποιηθούν για απάτες, διαφημίσεις ή ακόμη και κλοπή ταυτότητας.

Πριν δημοσιεύσεις κάτι, σκέψου:
«Θα ήθελα να το δουν όλοι;»
Αν **όχι**, μην το ανεβάζεις.



Οι πιο συχνοί κίνδυνοι στο Διαδίκτυο



Παρότι το Διαδίκτυο είναι χρήσιμο, δεν είναι πάντα ασφαλές. Ορισμένοι από τους πιο συχνούς κινδύνους είναι:

- **Ψεύτικες ιστοσελίδες (phishing)**
- **Απάτες μέσω e-mail ή SMS**
- **Ιοί και κακόβουλα λογισμικά**
- **Κλοπή προσωπικών δεδομένων**
- **Fake news και παραπληροφόρηση**

Αν ένα μήνυμα ή μια προσφορά φαίνεται “πολύ καλή για να είναι αληθινή”, πιθανότατα δεν είναι.

Βασικοί κανόνες ασφαλούς πλοήγησης

Η ασφάλεια στο διαδίκτυο ξεκινά από απλές καθημερινές συνήθειες. Ακολούθησε αυτούς τους βασικούς κανόνες και πλοηγήσου με σιγουριά, όπου κι αν βρίσκεσαι.

- Μην ανοίγεις άγνωστους συνδέσμους ή επισυναπτόμενα αρχεία. ✓
- Ενημέρωνε συχνά το λειτουργικό σύστημα και τις εφαρμογές σου. ✓
- Έλεγξε ότι η διεύθυνση της ιστοσελίδας αρχίζει με https://. ✓
- Χρησιμοποίησε ισχυρούς και διαφορετικούς κωδικούς. ✓
- Ενεργοποίησε διπλό έλεγχο ταυτότητας (2FA). ✓
- Απέφυγε τις συναλλαγές σε δημόσια Wi-Fi. ✓



Αν δεν είσαι σίγουρος τι να κάνεις, ρώτα ή έλεγξε πρώτα — δεν υπάρχει «λάθος» στο να είσαι προσεκτικός.

Κωδικοί πρόσβασης

Οι κωδικοί είναι το «κλειδί» για κάθε λογαριασμό μας στο διαδίκτυο. Με λίγες απλές κινήσεις μπορείς να προστατέψεις όλα τα ψηφιακά σου δεδομένα.

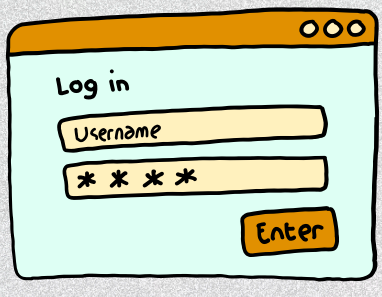
Χρησιμοποίησε τουλάχιστον 12 χαρακτήρες με γράμματα, αριθμούς και σύμβολα.

Μην επαναλαμβάνεις τον ίδιο κωδικό σε διαφορετικούς λογαριασμούς.

Χρησιμοποίησε έναν password manager για να τους αποθηκεύεις με ασφάλεια.

Άλλαζέ τους κάθε 6–12 μήνες ή αμέσως αν υποψιαστείς παραβίαση.

Οι δυνατοί κωδικοί δεν χρειάζεται να είναι περίπλοκοι — αρκεί να είναι μοναδικοί και μόνο δικοί σου!



Προστασία προσωπικών δεδομένων (GDPR)

- Μην κοινοποιείς στοιχεία ταυτότητας, ΑΦΜ, τραπεζικούς λογαριασμούς μέσω e-mail ή social.
- Εσύ είσαι ο ιδιοκτήτης των δεδομένων σου — όχι η πλατφόρμα που τα φιλοξενεί.
- Απέφυγε την αποστολή φωτογραφιών ή εγγράφων χωρίς λόγο.
- Έλεγξε ποια δικαιώματα έχουν οι εφαρμογές στο κινητό σου.



Αν μια εφαρμογή ζητά «περίεργες» άδειες (π.χ. μικρόφωνο ή κάμερα χωρίς λόγο), απέρριψέ τες.

Μέσα κοινωνικής δικτύωσης (1/2)

Μην αναρτάς προσωπικά δεδομένα (π.χ. διεύθυνση ή πού ταξιδεύεις).



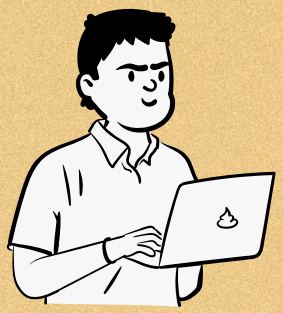
Μην ανοίγεις ύποπτα link — ακόμη κι αν σου τα στείλει “φίλος”.



Μην αποδέχεσαι αιτήματα φιλίας από αγνώστους.



Έλεγξε ποιος βλέπει τις αναρτήσεις σου.



Μέσα κοινωνικής δικτύωσης (2/2)

Χρησιμοποίησε τα social media με σεβασμό. Σκέψου πριν δημοσιεύσεις ή σχολιάσεις κάτι.

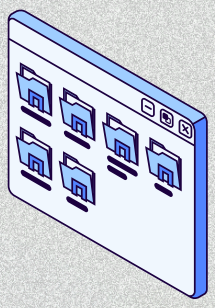


Μην απαντάς με επιθετικά σχόλια. Αντιδράσεις με θυμό μπορεί να επιδεινώσουν την κατάσταση.

Αν δεις κακοποιητικό περιεχόμενο μην το αγνοείς. Κάνε αναφορά στην πλατφόρμα.

Αν νιώσεις άβολα ή απειλημένος, μίλησε σε έναν ενήλικα ή υπεύθυνο ασφάλειας.

Ενημερώσεις & εργαλεία ασφαλείας



Κάνε συχνά αντίγραφα ασφαλείας (backup) των αρχείων σου.



Ενεργοποίησε antivirus και firewall.



Ρύθμισε τον browser σου ώστε να κάνει αυτόματο καθαρισμό cookies και cache.



Ενημέρωνε τακτικά τον υπολογιστή και τον browser.

Οι ενημερώσεις δεν είναι ενόχληση — είναι η ασπίδα σου απέναντι στις νέες απειλές.

Ασφαλείς online αγορές & πληρωμές



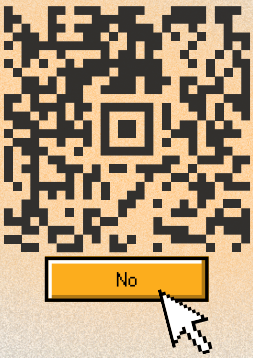
Αγόραζε μόνο από αξιόπιστα e-shops με https:// και 🔒 στη γραμμή διεύθυνσης.

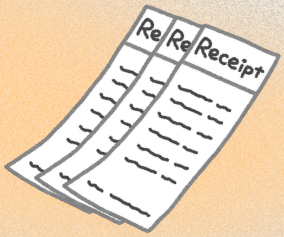




Αν κάτι φαίνεται ύποπτο, σταμάτα τη διαδικασία και έλεγξέ το.

Απόφυγε πληρωμές μέσω links ή QR που σου έστειλαν με μήνυμα.





Κράτα αποδείξεις αγορών.

Για online αγορές, προτίμησε προπληρωμένη κάρτα ή PayPal για μεγαλύτερη ασφάλεια.

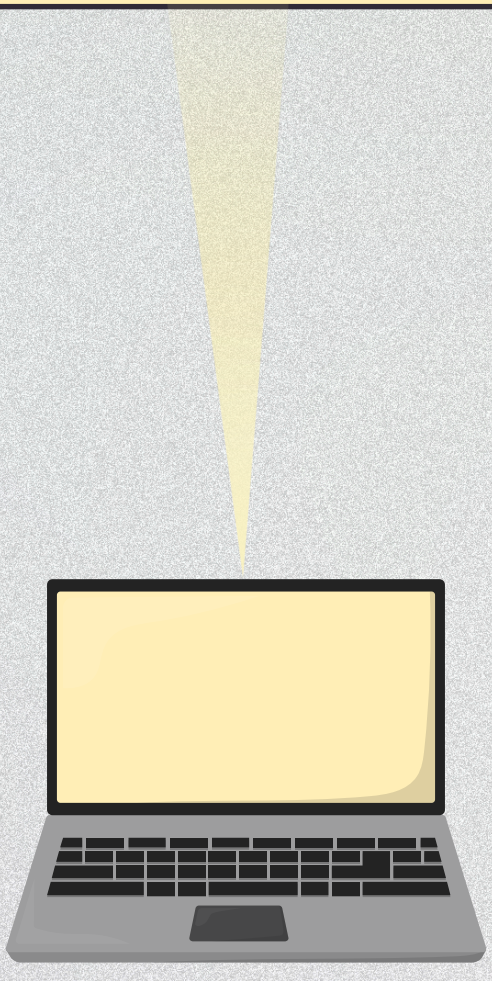
Αν πέσεις θύμα απάτης

Ενημέρωσε γνωστούς σου αν τους έστειλες ύποπτα links.

Επικοινώνησε άμεσα με την τράπεζά σου.

Μην πανικοβληθείς.

Άλλαξε τους κωδικούς σου. Password Protected



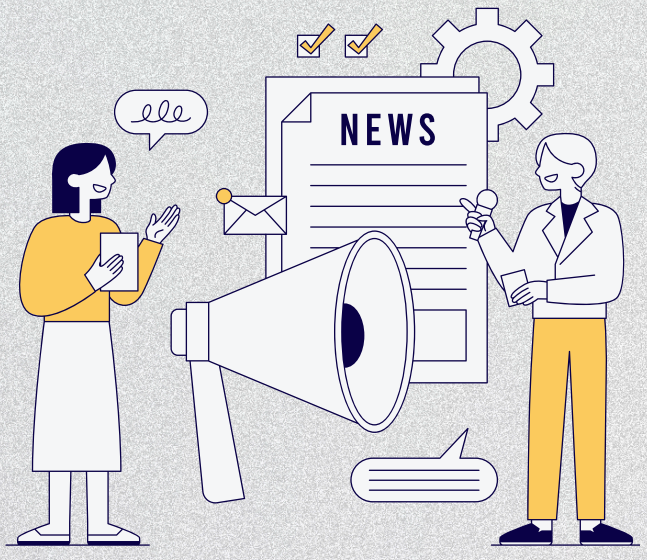
Fake news & παραπληροφόρηση

1. Πρόσεχε τίτλους που προκαλούν έντονο συναίσθημα.

2. Χρησιμοποίησε αξιόπιστες πηγές.

3. Έλεγξε ποιος δημοσίευσε την είδηση και πότε.

4. Επαλήθευσε πριν κοινοποιήσεις.



Ψυχολογική ισορροπία & διαδίκτυο



Η υπερβολική χρήση του Διαδικτύου μπορεί να οδηγήσει σε άγχος, απομόνωση και εξάρτηση. Βάλε όρια στον χρόνο οθόνης και δώσε προτεραιότητα στις ανθρώπινες σχέσεις.

Μάθε να αποσυνδέεσαι — κυριολεκτικά και μεταφορικά.

Κάνε «ψηφιακά διαλείμματα».



Ένα απόγευμα χωρίς οθόνες
είναι δώρο για το μυαλό σου.

Ασφαλής πλοήγηση για παιδιά (1/2)



Μίλησε ανοιχτά στο παιδί σου για το τι βλέπει και κάνει στο Διαδίκτυο.

Εγκατέστησε φίλτρα ή γονικό έλεγχο — π.χ. Kids Wallet (gov.gr), Google Family Link, Qustodio.

Δίδαξέ τους ότι δεν μιλάμε με αγνώστους online — όπως στον δρόμο, έτσι και στο διαδίκτυο.

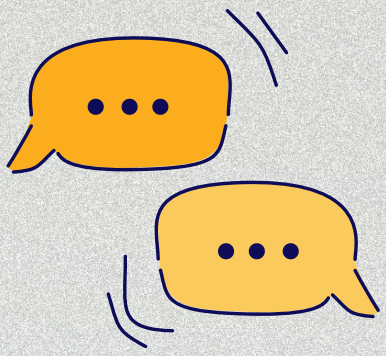
Όρισε χρονικά όρια χρήσης (π.χ. για παιχνίδι, σχολείο, ύπνο).

Ασφαλής πλοήγηση για παιδιά (2/2)



Μην είσαι εσύ συνέχεια στο κινητό — τα παιδιά παρατηρούν.

Εξήγησέ τους τι σημαίνει ψηφιακό αποτύπωμα: ό,τι κάνουμε online μένει.





Χρησιμοποιήστε μαζί την εφαρμογή Kids Wallet (gov.gr):

- για να επαληθεύσεις ηλικία & ταυτότητα παιδιού.
- για να θέσετε όρια χρήσης εφαρμογών και κινητής συσκευής.
- για να παρακολουθείτε με ασφάλεια τη χρήση της συσκευής.



Τα παιδιά να χρησιμοποιούν το Διαδίκτυο ως εργαλείο μάθησης και δημιουργίας — όχι ως πηγή κινδύνου.

Χρήσιμες πηγές

Το Διαδίκτυο είναι γεμάτο πληροφορίες και ευτυχώς υπάρχουν αξιόπιστοι φορείς που μπορούν να μας βοηθήσουν όταν κάτι δεν πάει καλά.

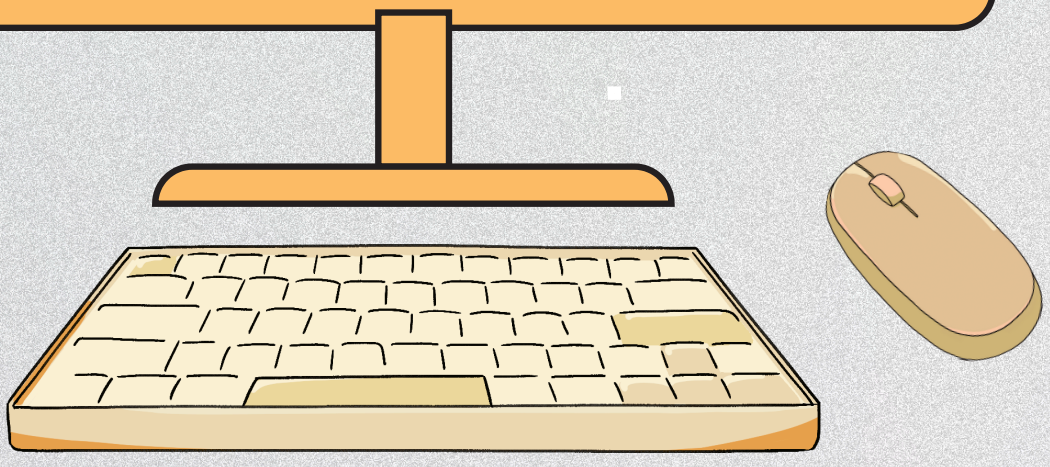
Αν δε νιώθεις σίγουρος για μια κατάσταση μην προσπαθείς να το λύσεις μόνος σου.
Οι παρακάτω οργανισμοί μπορούν να σε καθοδηγήσουν με ασφάλεια και εμπιστευτικότητα:

www.cyberkid.gov.gr – Ελληνική Αστυνομία

www.europol.europa.eu – Ευρωπαϊκή Αστυνομία

www.saferinternet.gr – Ελληνικό Κέντρο Ασφαλούς Διαδικτύου

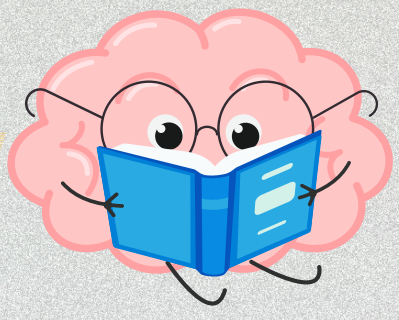
www.helpline.gr – Γραμμή Βοήθειας για Θέματα Διαδικτύου



Η ασφάλεια ξεκινά από εμάς

Η ασφάλεια στο Διαδίκτυο είναι ευθύνη όλων μας. Με ενημέρωση, προσοχή και σωστές συνήθειες μπορούμε να το απολαμβάνουμε χωρίς φόβο. Να θυμάσαι:

Η γνώση είναι η καλύτερη άμυνα απέναντι σε κάθε ηλεκτρονική απειλή.



Μείνε ενημερωμένος. Οι κίνδυνοι εξελίσσονται, αλλά και οι λύσεις επίσης.



5+1
Ψηφιακοί Οδηγοί
*για όλους

Περιφέρεια Δυτικής Μακεδονίας
Αντιπεριφέρεια Διαφάνειας, Ηλεκτρονικής Διακυβέρνησης
& Ψηφιακού Μετασχηματισμού

SYNERGINN EDIH