



# ΟΔΗΓΟΣ ΓΙΑ ΠΑΙΔΙΑ

## Ασφαλές Διαδίκτυο σε 4 Βήματα!



### Αίτημα Φιλίας **1**

Μην αποδέχεσαι αιτήματα φιλίας από αγνώστους και μην συνομιλείς με ανθρώπους που δεν γνωρίζεις. Σε καμία περίπτωση δεν πρέπει να συνομιλείς με αγνώστους ή να συναντηθείς μαζί τους. Ακόμη και αν το προφίλ τους φαίνεται αληθινό με φωτογραφίες ή κοινά ενδιαφέροντα, ποτέ δεν μπορείς να είσαι σίγουρος για τις προθέσεις του κάθε χρήστη.

### 2 Προσωπικά Στοιχεία

Ποτέ μην μοιράζεσαι τα προσωπικά σου στοιχεία με αγνώστους, όπως το όνομά σου, τη διεύθυνσή σου, το σχολείο σου, κωδικούς πρόσβασης και το κινητό σου. Προστάτευσε την ιδιωτικότητά σου. Ζήτησε από κάποιον ενήλικα που εμπιστεύεσαι να προσαρμόσει τις ρυθμίσεις απορρήτου, ώστε να μην επιτρέπεις σε οποιονδήποτε να διαβάσει τις δημοσιεύσεις σου, να βλέπει τις φωτογραφίες σου ή να αλληλεπιδρά μαζί σου.

### 3 Διαδικτυακός Εκφοβισμός (Cyberbullying) **3**

Ο διαδικτυακός εκφοβισμός περιλαμβάνει: αποστολή ανήθικων μηνυμάτων, αποκλεισμό ατόμων από εφαρμογές συνομιλιών, δημοσίευση ενοχλητικών φωτογραφιών, διάδοση προσβλητικών φημών κ.ά. Εάν κάτι σε ενοχλήσει ή σε κάνει να νιώσεις περίεργα, μη διστάσεις να το μοιραστείς με κάποιον ενήλικα που εμπιστεύεσαι.

### 4 Ρώτησε Πριν Κάνεις Κλικ

Η επιλογή ενός διαδικτυακού παιχνιδιού και μιας ιστοσελίδας πρέπει να γίνεται βάση ηλικιακής σήμανσης. Μην κάνεις κλικ σε συνδέσμους που ζητούν τα προσωπικά σου στοιχεία. Πάντα ρώτα έναν ενήλικα που εμπιστεύεσαι πριν κάνεις κλικ σε συνδέσμους. Αρχεία, εφαρμογές ή παιχνίδια μπορεί να αποτελέσουν αιτία για να προσβληθούν οι ψηφιακές συσκευές με ιούς.



Κέντρο Ασφαλούς Διαδικτύου - Γραμμή  
Βοήθειας & Καταγγελιών: 1480



Οι κανόνες συμπεριφοράς στο διαδίκτυο είναι οι ίδιοι με τους κανόνες της πραγματικής ζωής: Φερόμαστε στους άλλους όπως θα θέλαμε να μας φέρονται, μακριά από εκφοβιστικές ή άλλες ενοχλητικές συμπεριφορές.

# ΟΔΗΓΟΣ ΓΙΑ ΓΟΝΕΙΣ

## Φροντίστε για την ασφάλεια των παιδιών σας στο διαδίκτυο



### Μιλήστε και Ακούστε

1

Μιλήστε στο παιδί σας για την ασφάλεια στο διαδίκτυο, συζητώντας ανοιχτά τους κινδύνους και επιτηρώντας ενεργά τις διαδικτυακές τους δραστηριότητες. Δημιουργήστε ένα περιβάλλον εμπιστοσύνης ώστε το παιδί να νιώθει άνετα να μοιραστεί τις ανησυχίες του μαζί σας. Συζητήστε επίσης θέματα όπως οι κίνδυνοι στο διαδίκτυο, το ακατάλληλο περιεχόμενο και ο διαδικτυακός εκφοβισμός.

2

### Θέστε όρια και κανόνες

Περιορίστε τον χρόνο που περνούν τα παιδιά στο διαδίκτυο και καθορίστε ποιες ιστοσελίδες ή εφαρμογές μπορούν να χρησιμοποιούν, ανάλογα με την ηλικία τους. Οριοθετήστε μαζί πότε το παιδί μπορεί να χρησιμοποιεί το διαδίκτυο, πόσο χρόνο μπορεί να διαθέτει σε αυτό, ποιες ιστοσελίδες μπορεί να επισκέπτεται, το είδος της δραστηριότητας που επιτρέπεται να έχει, αν μπορεί να μοιράζεται φωτογραφίες και βίντεο, και πώς να συμπεριφέρεται διαδικτυακά.

### Χρήση «ασφαλών» και ενημερωμένων συσκευών

3

Φροντίστε για την ασφάλεια των συσκευών που χρησιμοποιούν τα παιδιά σας με: την εγκατάσταση και ρύθμιση προγράμματος προστασίας από ιούς (antivirus), ενεργοποίηση κλειδώματος οθόνης, διασφάλιση ότι το λειτουργικό σύστημα και οι εφαρμογές της συσκευής είναι συνεχώς ενημερωμένα, ενεργοποίηση περιορισμού για την εγκατάσταση εφαρμογών από άγνωστες πηγές έτσι ώστε να περιορίζεται ο κίνδυνος εγκατάστασης κακόβουλων εφαρμογών.

4

### Εργαλεία γονικού ελέγχου

Υπάρχουν πολλά εργαλεία που θα σας βοηθήσουν να διαχειριστείτε τις συσκευές που χρησιμοποιούν τα παιδιά σας. Για παράδειγμα, η γνώση του τρόπου ενεργοποίησης και χρήσης των ρυθμίσεων γονικού ελέγχου μπορεί να βοηθήσει στην προστασία του παιδιού σας από την εμφάνιση ακατάλληλου περιεχομένου στο διαδίκτυο.



Κέντρο Ασφαλούς Διαδικτύου - Γραμμή  
Βοήθειας & Καταγγελιών. 1480

Ο δρόμος για την σωστή και ασφαλή χρήση του διαδικτύου αρχίζει από τους γονείς!

# ΟΔΗΓΟΣ ΓΙΑ 65+

## Ασφαλής πλοήγηση στον κόσμο του διαδικτύου!



1

### Ηλεκτρονικό Ψάρεμα(Phishing)

Αναγνωρίστε τα σημάδια του phishing, όπως αιτήματα για προσωπικές πληροφορίες ή επείγοντα μηνύματα που προέρχονται από τράπεζες ή άλλους φορείς. Το phishing συχνά χρησιμοποιεί ψεύτικα emails ή μηνύματα για να παραπλανήσει ώστε να αποκαλύψετε ευαίσθητες πληροφορίες. Πάντα να επαληθεύετε την πηγή πριν κάνετε κλικ ή δώσετε προσωπικές πληροφορίες όπως αριθμό ταυτότητας, πιστωτικής κάρτας ή τραπεζικού λογαριασμού, διεύθυνση οικίας κ.α.

2

### Δημιουργία Ισχυρών Κωδικών

Δημιουργήστε ισχυρούς και μοναδικούς κωδικούς για τους λογαριασμούς σας, απομνημονεύοντας και αλλάζοντας τους τακτικά. Βεβαιωθείτε ότι οι κωδικοί σας διαφέρουν για κάθε λογαριασμό και περιλαμβάνουν συνδυασμό γραμμάτων (Α- Ζ και α-ζ), αριθμών (0-9) και ειδικών χαρακτήρων (!,@,#). Αυτό θα προστατεύσει τα προσωπικά σας δεδομένα από πιθανές επιθέσεις και απάτες. Αποφεύγουμε ονόματα και ημερομηνίες που σχετίζονται με εμάς.

3

### Δεν είστε σίγουροι για κάτι;

Ζητήστε τη γνώμη ενός μέλους της οικογένειας ή ενός φίλου πριν κάνετε σημαντικές ενέργειες στο διαδίκτυο, όπως την αποδοχή ενός αιτήματος φιλίας ή την πραγματοποίηση μιας αγοράς μέσω διαδικτύου. Η δεύτερη γνώμη μπορεί να σας βοηθήσει να αποφύγετε λάθη ή κινδύνους και να διασφαλίσετε ότι οι ενέργειές σας είναι ασφαλείς.

4

### Παραπληροφόρηση

Ελέγξτε την αξιοπιστία των πηγών και διασταυρώστε τις πληροφορίες με άλλες αξιόπιστες πηγές. Να είστε προσεκτικοί και πάντα να επιβεβαιώνετε τα δεδομένα. Βεβαιωθείτε ότι οι πληροφορίες που διαβάζετε είναι ακριβείς και αντικατοπτρίζουν τα πραγματικά γεγονότα, αποφεύγοντας την παραπληροφόρηση. Σκεφτείτε πριν κάνετε κλικ σε συνδέσμους ή ανοίξετε αρχεία από αγνώστες πηγές.



Κέντρο Ασφαλούς Διαδικτύου - Γραμμή  
Βοήθειας & Καταγγελιών: 1480



**Παραμένουμε ενήμεροι και υποψιασμένοι!**