Πώς να κρατήσετε τα παιδιά σας ασφαλή στο διαδίκτυο: Ένας πρακτικός οδηγός για γονείς

Από το Economistas

www.economistas.gr/tehnologia/76159_pos-na-kratisete-ta-paidia-sas-asfali-sto-diadiktyo-enas-praktikos-odigos-gia

Απόδοση, διασκευή: Α. Καραφωτιάς,
ΠΡΟΤΥΠΟ ΓΥΜΝΑΣΙΟ ΑΝΑΒΡΥΤΩΝ

Μετά την ανακοίνωση της ελληνικής κυβέρνησης για την απαγόρευση χρήσης των social media από ανηλίκους κάτω των 15 ετών, έχει ενταθεί η συζήτηση για τους βέλτιστους τρόπους προστασίας των παιδιών στο διαδίκτυο.

Η συγκεκριμένη πρωτοβουλία στοχεύει στην αντιμετώπιση προβλημάτων όπως **ο ψηφιακός εθισμός, η έκθεση σε επιβλαβές περιεχόμενο και οι διαδικτυακοί κίνδυνοι**, ωστόσο, οι ειδικοί τονίζουν ότι η νομοθετική ρύθμιση **από μόνη της δεν** μπορεί να προστατεύσει πλήρως τους ανήλικους χρήστες.

Κι ενώ το ρυθμιστικό πλαίσιο μπορεί να βοηθήσει, **η πραγματική προστασία των παιδιών ξεκινά από το σπίτι**. Ακολουθεί ένας πρακτικός οδηγός για να περιορίσετε το ψηφιακό αποτύπωμα του παιδιού σας χωρίς να έρχεστε σε συνεχείς συγκρούσεις μαζί του ή να χρειάζεται να επιβάλλετε αυστηρές απαγορεύσεις.

Πώς να περιορίσετε το ψηφιακό αποτύπωμα παιδιών και εφήβων

Το διαδίκτυο αποτελεί πλέον ένα δεύτερο «σπίτι» για τα περισσότερα παιδιά και εφήβους. Πολλά από αυτά αποκτούν την πρώτη τους συσκευή στο δημοτικό ή στο γυμνάσιο, ενώ η σύγχρονη εκπαίδευση βασίζεται σε μεγάλο βαθμό στην τεχνολογία. Οι εγκληματίες του κυβερνοχώρου το γνωρίζουν και έχουν τρόπους να ξεγελάσουν τα παιδιά ώστε να αποκαλύψουν προσωπικά τους στοιχεία, να πατήσουν κακόβουλους συνδέσμους, να τα παρασύρουν σε επικίνδυνα chats ή ακόμη και να αφαιρέσουν χρήματα από τους τραπεζικούς λογαριασμούς των γονιών τους. Για όλους τους παραπάνω λόγους, η κυβερνοασφάλεια πρέπει πρωτίστως να γίνει αναπόσπαστο κομμάτι της καθημερινότητας στο σπίτι των παιδιών.

Τι πρέπει να προσέξετε

Τα ευαίσθητα σημεία στο ψηφιακό περιβάλλον, στα οποία θα πρέπει να εστιάζουν την προσοχή τους οι γονείς:

- **Ομαδικές συνομιλίες** για σχολεία ή πανεπιστήμια που βρίσκονται σε μη ασφαλείς εφαρμογές ανταλλαγής μηνυμάτων.
- **Φωνητικές συνομιλίες** σε βιντεοπαιχνίδια.
- Περιπτώσεις **υπερέκθεσης πληροφοριών** στα social media.
- **Αναζητήσεις** στο διαδίκτυο και στα social media.
- **Χρήση** εργαλείων τεχνητής νοημοσύνης και **δημιουργίας** περιεχομένου μέσω αυτών.
- Γενικές πρακτικές **ασφαλούς χρήσης συσκευών και δημόσιων δικτύων**.

Ο καλύτερος τρόπος να προστατεύσετε τα παιδιά σας δεν είναι μέσω της επιβολής αυστηρών ελέγχων, αλλά μέσω της ειλικρινούς συζήτησης μαζί τους.

Μπορείτε, φυσικά, να μπλοκάρετε ιστοσελίδες, να ορίσετε συγκεκριμένες ώρες για τη χρήση του κινητού ή να επιβλέπετε κάθε φορά που το παιδί σας χρησιμοποιεί το AI. Οι πρωτοβουλίες αυτές, όμως, ενέχουν τον κίνδυνο να χάσετε την εμπιστοσύνη του: μπορεί να δώσετε την εντύπωση του «κακού» που περιορίζει την ελευθερία του. Οι αυστηροί περιορισμοί πάντα οδηγούν σε προσπάθειες παραβίασής τους. Είναι προτιμότερο να καλλιεργήσετε μια σχέση αλληλοκατανόησης, εξηγώντας εξαρχής **γιατί** πρέπει να υπάρχουν κανόνες.

Ακολουθούν ορισμένα πρακτικά βήματα που θα βοηθήσουν το παιδί σας να αποφύγει κινδύνους και να περιορίσει το ψηφιακό του αποτύπωμα.

Προσέξτε τι δημοσιεύετε


Φώτο: Shutterstock

Για τη Gen Z και τη GenAlpha, η δημοσίευση καθημερινών στιγμών στο διαδίκτυο είναι κάτι απολύτως φυσικό. Ωστόσο, η υπερέκθεση συχνά ανοίγει τον δρόμο για επιθέσεις από χάκερ, ακόμη και για κινδύνους εκτός διαδικτύου.

Υπενθυμίστε στο παιδί σας **να μην δημοσιοποιεί ποτέ το επώνυμό του, την ημερομηνία γέννησης, το όνομα του σχολείου ή την πόλη όπου ζει** όταν πραγματοποιεί εγγραφή σε διαδικτυακές υπηρεσίες. Εξηγήστε του τον

κίνδυνο: **επιτήδειοι μπορούν να χρησιμοποιήσουν αυτά τα στοιχεία για να το εντοπίσουν και να δημιουργήσουν μια ψευδή σχέση εμπιστοσύνης — για παράδειγμα, να χαιρετήσουν το παιδί με το όνομά του και να προσποιηθούν ότι είναι συγγενείς κάποιου συμμαθητή του**.

Απενεργοποιήστε την προεπιλογή κοινοποίησης τοποθεσίας (geolocation) σε δημοσιεύσεις και stories. Αν χρειάζεται να αναφερθεί μια τοποθεσία, η δημοσίευση καλό είναι να γίνεται αφού το παιδί έχει ήδη αποχωρήσει από εκεί.

Επίσης, χρειάζεται προσοχή με τα μέρη που επισκέπτεται τακτικά το παιδί σας και καλό είναι να αποφεύγεται να κοινοποιούν ταξιδιωτικά πλάνα. Η «χρυσή πρακτική» είναι να μάθετε στο παιδί σας να αφαιρεί τα γεωγραφικά στοιχεία (geotags) από τις φωτογραφίες του πριν τις ανεβάσει στο διαδίκτυο.

Εξίσου σημαντικό είναι να αποφεύγεται η κοινοποίηση προσωπικών πληροφοριών — και σε ορισμένες περιπτώσεις ακόμη και φωτογραφιών με σχολικές στολές. Αν η στολή είναι χαρακτηριστική, φωτογραφίες ή βίντεο από ρούχα (αθλητικά ή καθημερινά) μπορεί να αποκαλύψουν περισσότερα απ' όσα πρέπει.

Υπενθυμίστε στο παιδί σας τον βασικό κανόνα του διαδικτύου: **ό,τι δημοσιεύεται στο διαδίκτυο παραμένει σε αυτό**. Κάθε ανάρτηση μπορεί να έχει συνέπειες, επηρεάζοντας την κοινωνική ζωή του παιδιού σας, αλλά και εκθέτοντάς το στον κίνδυνο κατάχρησης των προσωπικών του δεδομένων από επιτήδειους.

Προσέξτε τους συνδέσμους που ανοίγετε

Πιθανότατα γνωρίζετε τι είναι το phishing, το παιδί σας, όμως μπορεί να μην γνωρίζει. Εξηγήστε του ότι το phishing (ηλεκτρονικό ψάρεμα) είναι μια μορφή κυβερνοεπίθεσης, όπου απατεώνες υποδύονται αξιόπιστες οντότητες (τράπεζες, εταιρείες, υπηρεσίες) μέσω email, SMS ή μηνυμάτων, με σκοπό να εξαπατήσουν τους χρήστες και να **αποσπάσουν ευαίσθητα προσωπικά δεδομένα, όπως κωδικούς πρόσβασης, στοιχεία πιστωτικών καρτών και προσωπικές πληροφορίες.**

Προσφορές που φαίνονται υπερβολικά καλές για να είναι αληθινές, απροσδόκητα "δώρα" ή άλλες "εκπληκτικές ευκαιρίες" θα πρέπει πάντα να δημιουργούν υποψίες.

Είναι σημαντικό το παιδί σας να σας συμβουλεύεται πριν πατήσει σε οποιονδήποτε σύνδεσμο.

Προσοχή με ποιους παίζει online

Όταν οι έφηβοι συμμετέχουν σε διαδικτυακά παιχνίδια πολλών παικτών με δυνατότητα φωνητικής συνομιλίας, ενδέχεται να παρασυρθούν και να μοιραστούν περισσότερες πληροφορίες απ' όσες πρέπει. Ο χώρος των online παιχνιδιών έχει εξελιχθεί σε βασικό πεδίο εμφάνισης περιστατικών grooming, δηλαδή περιπτώσεων κατά τις οποίες **ενήλικοι επιχειρούν να κερδίσουν την εμπιστοσύνη ανηλίκων για επιβλαβείς σκοπούς**.

Θέστε, λοιπόν, ένα σαφές όριο: **το περιεχόμενο της φωνητικής συνομιλίας να περιορίζεται αποκλειστικά στο παιχνίδι**.

Σε περίπτωση που κάποιος επιχειρήσει να μεταφέρει τη συζήτηση σε προσωπικά θέματα, **είναι σημαντικό το παιδί σας να τη διακόψει**.

Αν η συμπεριφορά επιμείνει, θα πρέπει να προχωρήσει σε αποκλεισμό του χρήστη.

Αποφεύγετε τα δημόσια δίκτυα Wi-Fi

Εξηγήστε στα παιδιά σας ότι **η χρήση δημόσιων δικτύων Wi-Fi δεν είναι ασφαλής**: κακόβουλοι δράστες μπορούν εύκολα να υποκλέψουν στοιχεία σύνδεσης, κωδικούς πρόσβασης, μηνύματα και άλλα ευαίσθητα δεδομένα.

Όποτε είναι δυνατό, προτιμήστε τη χρήση δεδομένων κινητής τηλεφωνίας.

Προσέχετε τι κατεβάζετε

Τα κινητά τηλέφωνα με λειτουργικό σύστημα Android αποτελούν συχνά στόχο για απατεώνες κάθε είδους. Αν και κακόβουλες εφαρμογές εμφανίζονται και σε συσκευές iPhone, οι συσκευές Android θεωρούνται πιο ευάλωτες.

Ενημερώστε το παιδί σας ότι τα κακόβουλα αρχεία μπορούν να εμφανίζονται με πολλές μορφές: ενδέχεται να αποστέλλονται μέσω εφαρμογών ανταλλαγής μηνυμάτων ή ηλεκτρονικού ταχυδρομείου, μεταμφιεσμένα ως φωτογραφίες ή έγγραφα. Σε ορισμένες περιπτώσεις, μπορεί να εμφανίζονται ακόμη και ως "εργασίες για το σπίτι", μέσω προωθημένων μηνυμάτων.

Κατά συνέπεια, κάθε συνημμένο αρχείο θα πρέπει να αντιμετωπίζεται με προσοχή.

Χρησιμοποιείτε την AI με σύνεση και να βασίζεστε στον εαυτό σας

Η ανεξέλεγκτη χρήση των chatbot δεν αποτελεί μόνο ζήτημα ηθικής ή ψυχολογίας, αλλά και ζήτημα ασφάλειας και προστασίας προσωπικών δεδομένων. Έχει παρατηρηθεί ότι συνομιλίες οι οποίες έχουν κοινοποιηθεί δημόσια μέσω συνδέσμων μπορούν, σε ορισμένες περιπτώσεις, να καταστούν **προσβάσιμες από τρίτους** μέσω μηχανών αναζήτησης.

Εξηγείστε στο παιδί σας ότι **δεν** πρέπει να αντιμετωπίζει την AI ως τον "καλύτερο φίλο" με τον οποίο μπορεί να μοιράζεται τα πάντα.

Τα εργαλεία τεχνητής νοημοσύνης ενδέχεται να συλλέγουν και να επεξεργάζονται προσωπικά δεδομένα, συμπεριλαμβανομένων όσων γράφει, ρωτά ή ανεβάζει ο χρήστης κατά τη διάρκεια της συνομιλίας.

Τονίστε επίσης ότι **δεν πρέπει να μοιράζεται το πραγματικό του όνομα, πληροφορίες για το σχολείο στο οποίο φοιτά, φωτογραφίες ή άλλα προσωπικά δεδομένα.**

Ξεκαθαρίστε, ακόμη, ότι **τα chatbot είναι εργαλεία και βοηθοί — όχι «μάγοι» που σκέφτονται αντί για εκείνο**.

Η AI δεν σκέφτεται πραγματικά, επομένως κάθε πληροφορία που δίνει πρέπει να ελέγχεται.

Χρησιμοποιήστε φίλτρα περιεχομένου ή γονικό έλεγχο

Κάντε την αρχή ενεργοποιώντας τον γονικό έλεγχο σε όλες τις συσκευές που χρησιμοποιεί το παιδί σας: κινητά, tablets, υπολογιστές — ακόμη και smart TV. Τα περισσότερα λειτουργικά συστήματα έχουν ενσωματωμένες επιλογές για μπλοκάρισμα ακατάλληλων ιστοσελίδων, περιορισμό εφαρμογών και φιλτράρισμα αναζητήσεων.

Στις πλατφόρμες streaming, ενεργοποιήστε τη λειτουργία «Περιορισμένο» ή «Παιδικό» για να αποφεύγεται το ακατάλληλο περιεχόμενο.

Περάστε χρόνο και συζητήστε με το παιδί σας

Το πιο αποτελεσματικό «φίλτρο» δεν είναι κάποιο πρόγραμμα, αλλά εσείς οι ίδιοι. Περάστε χρόνο βλέποντας σειρές, σερφάροντας και παίζοντας ηλεκτρονικά παιχνίδια μαζί με το παιδί σας.

Έτσι θα καταλάβετε καλύτερα τι συμβαίνει στη ζωή του και θα δημιουργηθούν αφορμές για συζήτηση σχετικά με τις αξίες, τα συναισθήματά του και γεγονότα από την καθημερινότητα.