TLP: WHITE

ΕΞΑΣΦΑΛΙΖΟΝΤΑΣ ΤΗΝ ΔΙΑΔΙΚΤΥΑΚΗ ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΑΙΔΙΩΝ

NCC ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ncc.cy

Ενότητες

- Εισαγωγή
- Συνήθεις Χρήσεις
- Οι Κινδύνοι
- Μέτρα Ασφάλειας & Τρόποι Προστασίας
- Συνεργασία Γονέων και Δασκάλων
- Χρήσιμες Πληροφορίες

Εισαγωγή

Εισαγωγή

Γιατί είναι σημαντική η κυβερνοασφάλεια για τα παιδιά μας;

1. Αυξανόμενη διαδικτυακή παρουσία: Τα παιδιά περνούν περισσότερο χρόνο στο διαδίκτυο από ποτέ.

2. Προστασία του μέλλοντός τους: Οι ασφαλείς διαδικτυακές συνήθειες ξεκινούν από το σπίτι.

3. Μείνετε ενημερωμένοι: Η γνώση είναι το πρώτο βήμα για την πρόληψη.

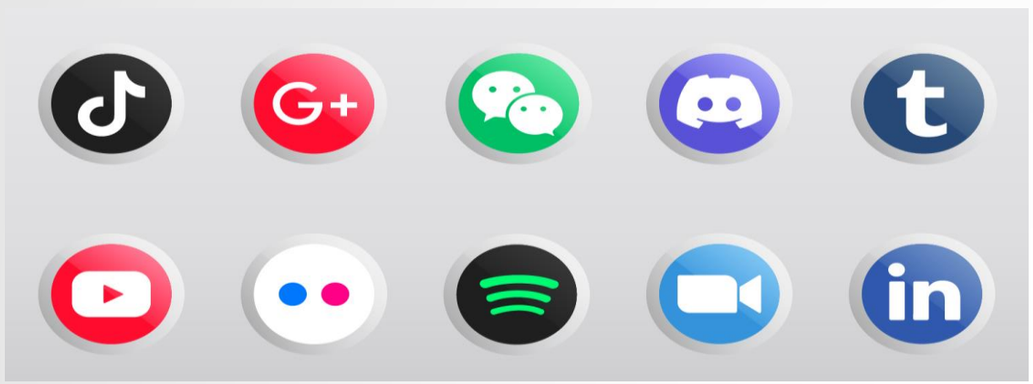
*Το 2023 στην ΕΕ, το 97% των νέων χρησιμοποιούσε το Διαδίκτυο καθημερινά, σε σύγκριση με το 86% του συνόλου των ατόμων.***

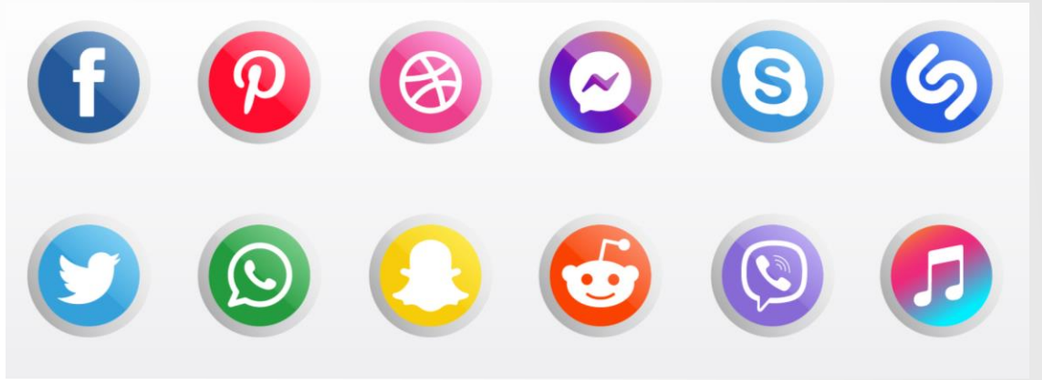
Σήμερα, θα συζητήσουμε τη συχνότερη χρήση του διαδικτύου, τους κινδύνους και τα πιθανά μέτρα που μπορούμε να εφαρμόσουμε για την προστασία τους

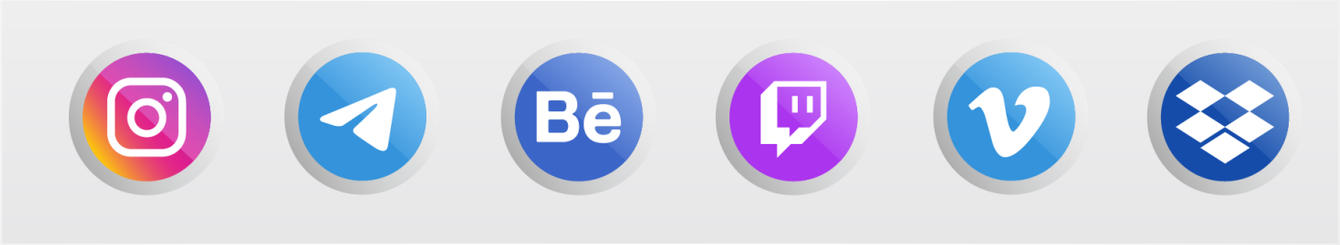
Συνήθεις Χρήσεις

Μέσα Κοινωνικής Δικτύωσης

Γνωρίζετε ποιες πλατφόρμες μέσων κοινωνικής δικτύωσης χρησιμοποιούν;







Το 2022, το 84% των νέων χρησιμοποιούσαν το διαδίκτυο για να συμμετέχουν σε δίκτυα κοινωνικής δικτύωσης.*

Μέσα Κοινωνικής Δικτύωσης

Τι να προσέξετε:

- Κοινοποιούν τα προσωπικά τους στοιχεία;
- Ποιους έχουν στη λίστα των «Φίλων» τους;
- Με ποιον κουβεντιάζουν;
- Μοιράζονται τις φωτογραφίες τους ή οποιουδήποτε άλλου;
- Ποιους λογαριασμούς ακολουθούν;
- Είναι αυτοί οι λογαριασμοί κατάλληλοι για την ηλικία τους;

Διαδυκτιακά Παιχνίδια

- Τα παιδιά ξοδεύουν όλο και περισσότερο χρόνο σε διαδικτυακές πλατφόρμες τυχερών παιχνιδιών

- Τα οφέλη του παιχνιδιού μπορεί να περιλαμβάνουν βελτιωμένο συντονισμό κινήσεων, δεξιότητες επίλυσης προβλημάτων και κοινωνικές συνδέσεις με συνομηλίκους.
- Αλλά… υπάρχουν επίσης κίνδυνοι που σχετίζονται με τα διαδικτυακά παιχνίδια, όπως η έκθεση σε ακατάλληλο περιεχόμενο, ο διαδικτυακός εκφοβισμός και ο πιθανός εθισμός στα παιχνίδια.

Τι να προσέξετε:

- Παιχνίδια κατάλληλα για την ηλικία τους: Βεβαιωθείτε ότι τα παιχνίδια είναι κατάλληλα για την ηλικία του παιδιού σας. Ελέγξτε αξιολογήσεις και κριτικές από αξιόπιστους οργανισμούς όπως το ESBR και το PEGI. Αναζητήστε τα παρακάτω σημάδια

Διαδυκτιακά Παιχνίδια

- Τα παιδιά ξοδεύουν όλο και περισσότερο χρόνο σε διαδικτυακές πλατφόρμες τυχερών παιχνιδιών

- Τα οφέλη του παιχνιδιού μπορεί να περιλαμβάνουν βελτιωμένο συντονισμό κινήσεων, δεξιότητες επίλυσης προβλημάτων και κοινωνικές συνδέσεις με συνομηλίκους.
- Αλλά… υπάρχουν επίσης κίνδυνοι που σχετίζονται με τα διαδικτυακά παιχνίδια, όπως η έκθεση σε ακατάλληλο περιεχόμενο, ο διαδικτυακός εκφοβισμός και ο πιθανός εθισμός στα παιχνίδια.

Τι να προσέξετε:

- Γονικός έλεγχος: Χρησιμοποιήστε τους γονικούς ελέγχους που είναι διαθέσιμοι σε πλατφόρμες παιχνιδιών για να περιορίσετε το ακατάλληλο περιεχόμενο και να διαχειριστείτε τον χρόνο παιχνιδιού.

- Ρυθμίσεις απορρήτου: Μάθετε στο παιδί σας να διατηρεί απόρρητα τα προσωπικά στοιχεία. Βεβαιωθείτε ότι τα προφίλ τους έχουν οριστεί ως ιδιωτικά και περιορίστε τις πληροφορίες που μοιράζονται.

- Ασφαλείς λογαριασμοί: Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης για λογαριασμούς παιχνιδιών και ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων, εάν είναι διαθέσιμος.

Διαδυκτιακές Αγορές

Πώς χρησιμοποιούν τα παιδιά τις διαδικτυακές αγορές;

- Αγορά αντικειμένων: Περιήγηση σε ηλεκτρονικά καταστήματα για παιχνίδια, ρούχα ή άλλα αντικείμενα, συχνά με γονική επίβλεψη.
- Εικονικά αγαθά: Αγορά αντικειμένων εντός παιχνιδιού ή ψηφιακού περιεχομένου.

Τι να προσέξετε:

Όρια στα ποσά που ξοδεύουν:
Εξετάστε το ενδεχόμενο να χρησιμοποιήσετε προπληρωμένες κάρτες με σταθερά ποσά για να περιορίσετε τις δαπάνες. Διδάξτε στα παιδιά σχετικά με τον προϋπολογισμό και την αξία των χρημάτων.

Απάτες:
Εκπαιδεύστε τα παιδιά σχετικά με κοινές διαδικτυακές απάτες, όπως ψεύτικους ιστότοπους, μηνύματα ηλεκτρονικού ψαρέματος (phishing) και προσφορές πολύ καλές έως αληθινές. Ενθαρρύνετέ τους να έρθουν κοντά σας αν συναντήσουν κάτι ύποπτο. Διδάξτε στα παιδιά πώς να διαβάζουν κριτικές προϊόντων και αξιολογήσεις για να λαμβάνουν τεκμηριωμένες αποφάσεις αγοράς.

Οι Κινδύνοι

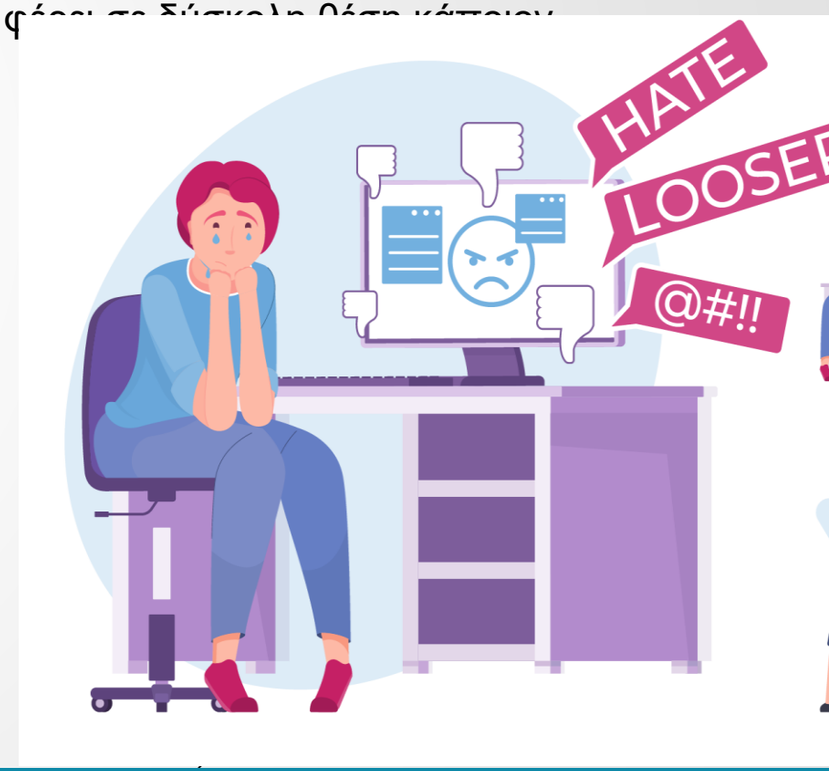
Κυβερνοεκφοβισμός

Τι είναι ο διαδικτυακός εκφοβισμός;

Ο διαδικτυακός εκφοβισμός περιλαμβάνει τη χρήση ψηφιακών πλατφορμών όπως μέσα κοινωνικής δικτύωσης, μηνύματα κειμένου, email και άλλα διαδικτυακά εργαλεία για την παρενόχληση, την απειλή ή τον εξευτελισμό κάποιου.
Μπορεί να πάρει πολλές μορφές, συμπεριλαμβανομένης της διάδοσης φημών, της κοινοποίησης προσωπικών πληροφοριών χωρίς συναίνεση, της αποστολής απειλητικών μηνυμάτων και της δημιουργίας πλαστών προφίλ για να φέρει σε δύσκολη θέση κάποιον.

Τι να προσέξετε:

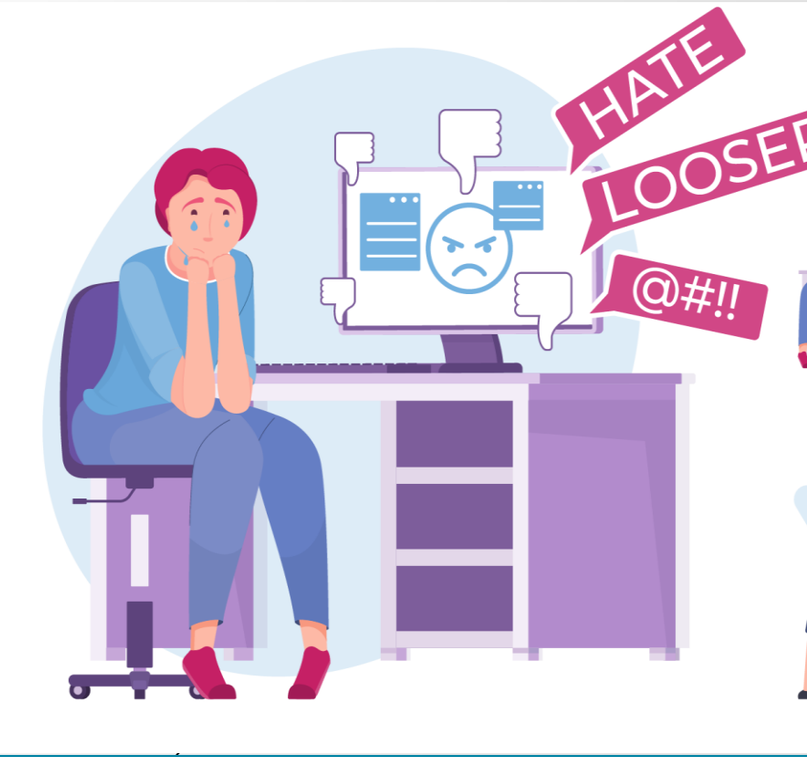
- Συναισθηματικές αλλαγές: Ξαφνικές αλλαγές στη διάθεση, άγχος, κατάθλιψη ή ευερεθιστότητα.
- Αλλαγές συμπεριφοράς: Απροθυμία να πάει στο σχολείο, αποφυγή κοινωνικών αλληλεπιδράσεων ή αλλαγές στις συνήθειες διατροφής και ύπνου.
- Ψηφιακές κόκκινες σημαίες: Απροθυμία να χρησιμοποιήσουν συσκευές, νευρικότητα κατά τη λήψη ειδοποιήσεων ή ξαφνική αλλαγή στον τρόπο χρήσης των συσκευών τους.



Κυβερνοεκφοβισμός

Διαχείιση διαδικτυακού εκφοβισμού:

- Διατηρήστε αρχεία για τυχόν περιστατικά εκφοβισμού, συμπεριλαμβανομένων στιγμιότυπων οθόνης μηνυμάτων ή αναρτήσεων.
- Αναφορά: Αναφέρετε τον εκφοβισμό στη σχετική πλατφόρμα (π.χ. ιστότοπος μέσων κοινωνικής δικτύωσης, εφαρμογή) και, εάν είναι απαραίτητο, στις σχολικές αρχές ή στις τοπικές αρμόδιες αρχές.
- Υποστήριξη: Προσφέρετε συναισθηματική υποστήριξη στο παιδί σας και εξετάστε το ενδεχόμενο επαγγελματικής συμβουλευτικής εάν χρειάζεται.



Κακόβουλοι χρήστες

- Κακόβουλοι χρήστες: Πρόκειται για άτομα που εκμεταλλεύονται την ανωνυμία που προσφέρει το διαδικτύο για να στοχεύσουν και να εκμεταλλευτούν παιδιά.
- Τακτικές δελεασμού: Οι κακόβουλοι χρήστες μπορεί να χρησιμοποιούν κολακείες, δώρα, προσοχή και χειραγώγηση για να κερδίσουν την εμπιστοσύνη του παιδιού και να μειώσουν την άμυνά του.
- Πλατφόρμες που χρησιμοποιούνται: Οι κακόβουλοι χρήστες μπορούν να χρησιμοποιήσουν μέσα κοινωνικής δικτύωσης, πλατφόρμες παιχνιδιών, δωμάτια συνομιλίας και εφαρμογές ανταλλαγής μηνυμάτων.

Ακατάλληλο Περιεχόμενο

Το ακατάλληλο περιεχόμενο μπορεί να έχει τεράστιο αντίκτυπο σε νεαρά άτομα:

- Συναισθηματικές και ψυχολογικές επιπτώσεις: Η έκθεση σε ακατάλληλο περιεχόμενο μπορεί να προκαλέσει φόβο, άγχος ή απευαισθητοποίηση στη βία.
- Αλλαγές συμπεριφοράς: Μπορεί να επηρεάσει τα παιδιά να μιμηθούν ακατάλληλες συμπεριφορές.
- Εθισμός: Ορισμένο περιεχόμενο, όπως η διαδικτυακή πορνογραφία, μπορεί να είναι εθιστικό.
- Απευαισθητοποίηση: Η επανειλημμένη έκθεση σε βίαιο ή άσεμνο περιεχόμενο μπορεί να μειώσει την ευαισθησία σε τέτοιο υλικό.

Το ακατάλληλο περιεχόμενο για παιδιά μπορεί να έχει πολλούς τύπους:

- Πορνογραφία και σεξουαλικό υλικό
- Βία
- Ρητορική μίσους και διακρίσεις
- Κατάχρηση ναρκωτικών και ουσιών
- Παραπληροφόρηση και ψευδείς ειδήσεις
- Απάτες και κακόβουλο λογισμικό Scams and malware

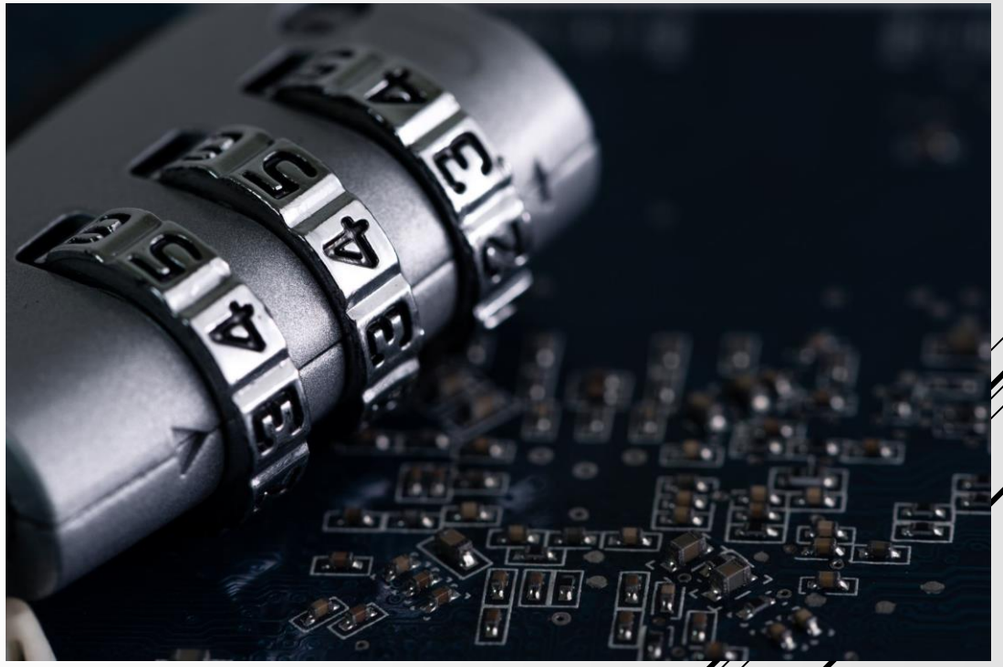
Ακατάλληλο Περιεχόμενο

Απόκριση μετά την έκθεση σε ακατάλληλο περιεχόμενο:

- Μείνετε ήρεμοι: Εάν ένα παιδί συναντήσει ακατάλληλο περιεχόμενο, απαντήστε ήρεμα και αποφύγετε την υπερβολική αντίδραση.
- Συζητήστε το περιεχόμενο: Συζητήστε για το γιατί το περιεχόμενο είναι ακατάλληλο και τον πιθανό αντίκτυπό του.
- Ενισχύστε τις ασφαλείς πρακτικές: Υπενθυμίστε στα παιδιά τα βήματα που μπορούν να κάνουν για να αποφύγουν παρόμοιο περιεχόμενο στο μέλλον.
- Ζητήστε επαγγελματική βοήθεια: Εάν η έκθεση έχει οδηγήσει σε σημαντικές αλλαγές στη συμπεριφορά, σκεφτείτε να συμβουλευτείτε έναν παιδοψυχολόγο.

Απόρρητο και Υποκλοπή Ταυτότητας

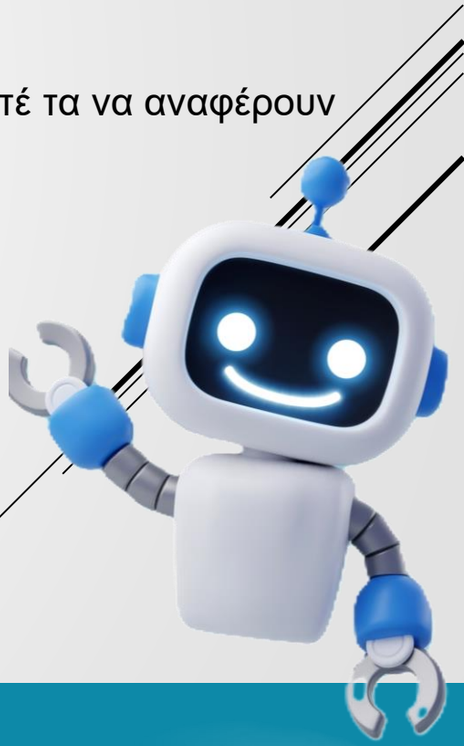
- Προσωπικές πληροφορίες: Τα προσωπικά στοιχεία των παιδιών, όπως ονόματα, ημερομηνίες γέννησης και διευθύνσεις, μπορεί να είναι πολύτιμα για τους εγκληματίες του κυβερνοχώρου.
- Social Media: Οι πλατφόρμες μέσων κοινωνικής δικτύωσης συχνά ενθαρρύνουν την κοινή χρήση προσωπικών στοιχείων.
- Εφαρμογές και παιχνίδια: Πολλές εφαρμογές και διαδικτυακά παιχνίδια συλλέγουν δεδομένα. Μια τέτοια συλλογή περιγράφεται συχνά στις πολιτικές απορρήτου αυτών των εφαρμογών και παιχνιδιών.
- Παραβιάσεις δεδομένων: Τα δεδομένα των παιδιών συχνά παρακολουθούνται λιγότερο από ό,τι των ενηλίκων, γεγονός που τα καθιστά στόχο για παραβιάσεις δεδομένων.



Μέτρα Ασφάλειας & Τρόποι Προστασίας

Εκπαίδευση και Ενημέρωση

- **Ανοιχτή επικοινωνία:** Δημιουργήστε ένα περιβάλλον όπου το παιδί σας νιώθει άνετα να συζητά τις διαδικτυακές του δραστηριότητες και τυχόν άβολες εμπειρίες του.
- **Κριτική σκέψη:** Διδάξτε στα παιδιά πώς να αναγνωρίζουν ύποπτη συμπεριφορά και περιεχόμενο.
- **Συνήθειες ασφαλούς περιήγησης:** Διδάξτε τους πώς να αναγνωρίζουν ιστοσελίδες κατάλληλες για την ηλικία τους.
- **Συμπεριφορά στο Διαδίκτυο:** Διδάξτε τους για τη σημασία της μη κοινοποίησης προσωπικών πληροφοριών (όπως το πλήρες όνομα, τη διεύθυνση ή το σχολείο τους) στο διαδίκτυο.
- **Αναγνώριση τακτικών δελεασμού:** Βοηθήστε τα να καταλάβουν πώς μοιάζει η συμπεριφορά αυτή και ενθαρρύνετέ τα να αναφέρουν οποιαδήποτε ακατάλληλη επαφή.
- **Βεβαιωθείτε ότι γνωρίζουν ότι ό,τι κοινοποιείται στο διαδίκτυο θα παραμείνει εκεί για ΠΑΝΤΑ**



ΝΑ ΘΥΜΑΣΤΕ ΟΜΩΣ! Πρέπει να συνεχίσετε και εσείς να εκπαιδεύεστε

- Μείνετε ενημερωμένοι: Μείνετε ενημερωμένοι με τις τελευταίες τάσεις στα μέσα κοινωνικής δικτύωσης και τη διαδικτυακή συμπεριφορά για να κατανοήσετε καλύτερα τα περιβάλλοντα στα οποία περιηγείται το παιδί σας.
- Χρησιμοποιήστε πόρους από οργανισμούς όπως το "CYberSafety" , το SafeOnline και άλλους οργανισμούς για την ασφάλεια των παιδιών, για να εκπαιδεύσετε τον εαυτό σας και το παιδί σας.

Γονικός Έλεγχος και Παρακολούθηση

- **Εργαλεία γονικού ελέγχου:** Χρησιμοποιήστε λογισμικό γονικού ελέγχου για να παρακολουθείτε και να περιορίζετε τις διαδικτυακές δραστηριότητες του παιδιού σας. Να θυμάστε ότι ορισμένες πλατφόρμες έχουν ενσωματωμένες ρυθμίσεις γονικού ελέγχου (π.χ. λογαριασμοί PlayStation)

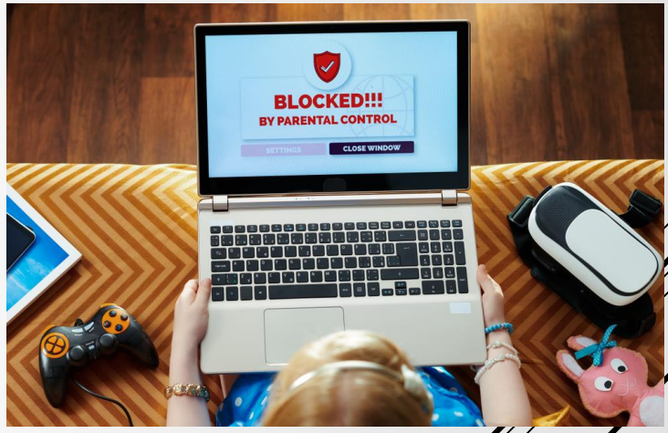
- **Ρύθμιση φίλτρων και περιορισμών:** Αποκλεισμός ακατάλληλου περιεχομένου, περιορισμός χρόνου οθόνης.

- **Παρακολούθηση διαδικτυακής δραστηριότητας:** Τακτικά check-in, έλεγχος ιστορικού προγράμματος περιήγησης και χρήση εφαρμογών παρακολούθησης.

- **Ρυθμίσεις απορρήτου:** Βεβαιωθείτε ότι οι λογαριασμοί κοινωνικών μέσων και άλλα διαδικτυακά προφίλ του παιδιού σας έχουν οριστεί ως ιδιωτικά.

- **Χρόνος στην οθόνη:** Θέστε όρια στον χρόνο που περνάει το παιδί σας στο διαδίκτυο και βεβαιωθείτε ότι έχει έναν ισορροπημένο τρόπο ζωής με δραστηριότητες εκτός διαδικτύου.

- **Ρυθμίσεις ασφαλούς αναζήτησης:** Ενεργοποιήστε τις ρυθμίσεις ασφαλούς αναζήτησης σε προγράμματα περιήγησης και πλατφόρμες όπως το Google και το YouTube.



Να είστε προνοητικοί

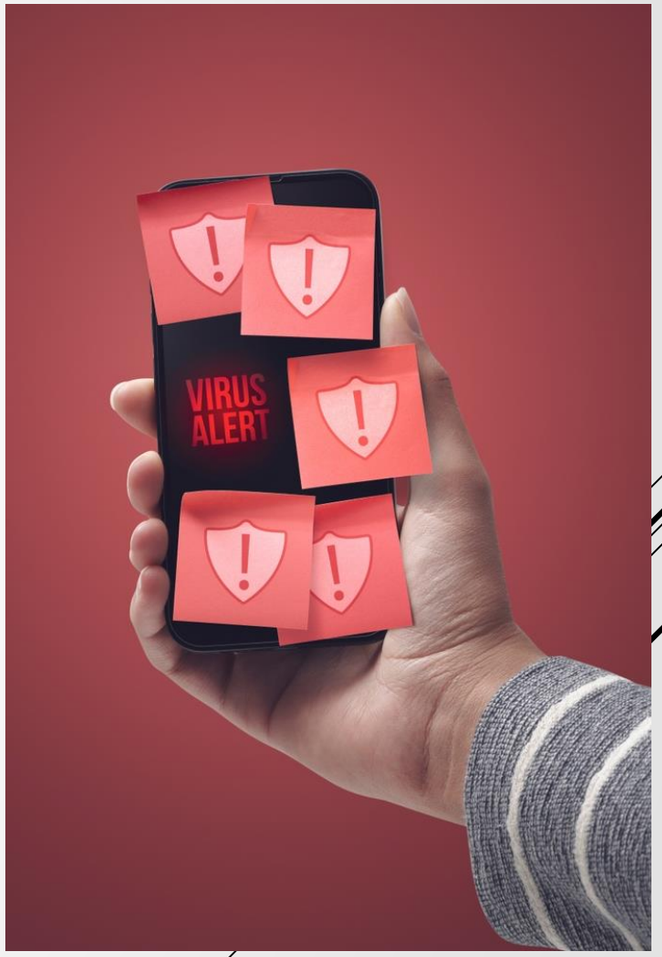
- **Γνωρίστε τους φίλους τους:** Να γνωρίζετε με ποιους αλληλεπιδρά το παιδί σας στο διαδίκτυο και να το ενθαρρύνετε να διατηρεί διαδικτυακές φιλίες μόνο με άτομα που γνωρίζει και στον πραγματικό κοινωνικό κύκλο του.
- **Τακτικά check-in:** Ελέγχετε τακτικά τις συσκευές του παιδιού σας για τυχόν άγνωστες ή ύποπτες επαφές και επικοινωνίες**.**
- **Χρήση τεχνολογίας:** Εξοικειωθείτε με τις εφαρμογές και τους ιστότοπους που χρησιμοποιεί το παιδί σας και κατανοήστε τα χαρακτηριστικά και τους κινδύνους τους.

Ασφάλες Διαδυκτυακό Περιβαλλόν στο Σχολείο

- **Εφαρμογή σχολικών πολιτικών**: Αποδεκτές πολιτικές χρήσης για χρήση στο Διαδίκτυο.
- **Εκπαίδευση μαθητών**: Ενσωμάτωση της ψηφιακής και της διαδικτυακής ασφάλειας στο πρόγραμμα σπουδών.
- **Διαδραστικές συνεδρίες**: Ενθαρρύνετε τις διαδραστικές συνεδρίες όπου τα παιδιά μπορούν να μάθουν για την ασφάλεια στον κυβερνοχώρο μέσω παιχνιδιών, κουίζ και πρακτικών ασκήσεων.

- Να είστε πάντα προσεκτικοί, εάν εντοπίσετε σημάδια, αναφέρετέ το αμέσως

Έλεγχοι και μέτρα κυβερνοασφάλειας:
- Ασφαλή δίκτυα
- Τακτικές ενημερώσεις
- Χρήση κατάλληλου λογισμικού προστασίας από ιούς
- Φίλτρα και μαύρη λίστα/επιλογή ιστοτόπων
- Εκπαίδευση προσωπικού

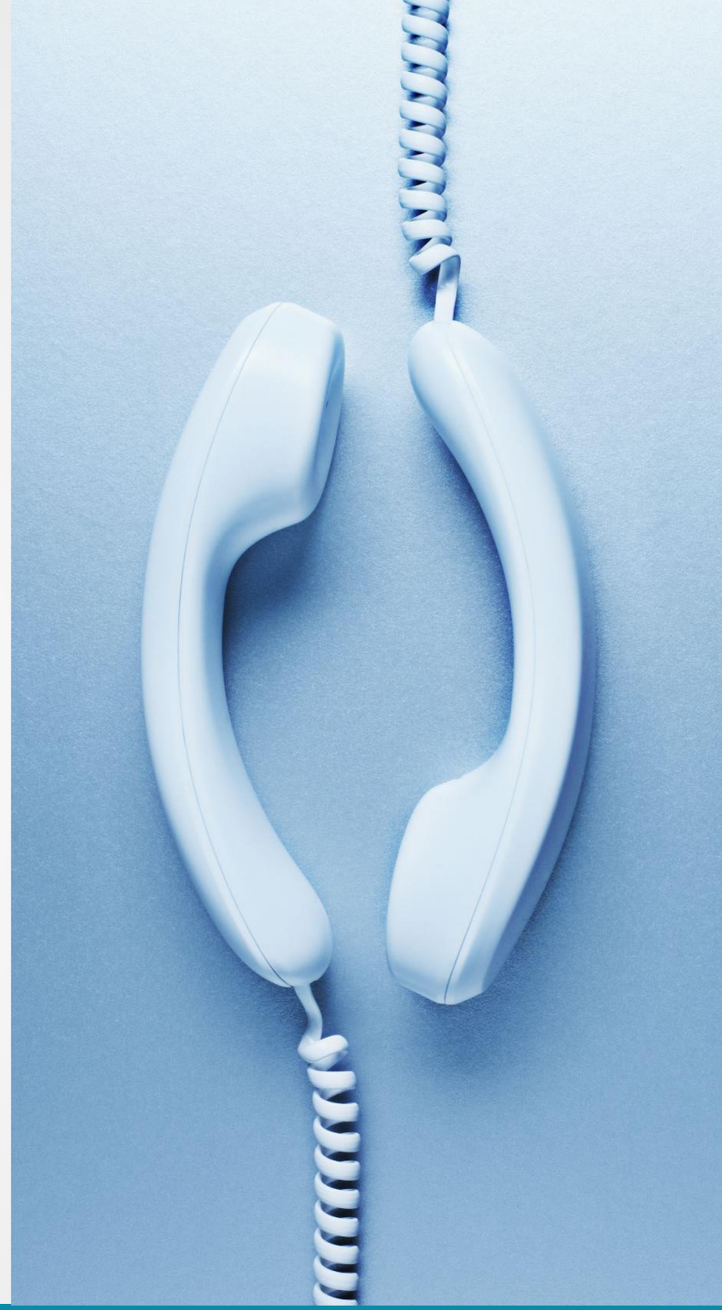


Συνεργασία Γονέων και Δασκάλων

Επικοινωνία

Η αποτελεσματική επικοινωνία μεταξύ γονέων και δασκάλων είναι ζωτικής σημασίας για τη διασφάλιση της κυβερνοασφάλειας των παιδιών.

- **Τακτικές συναντήσεις:** Προγραμματίστε τακτικές συναντήσεις γονέων και δασκάλων για να συζητήσετε θέματα και ενημερώσεις σχετικά με την ασφάλεια στον κυβερνοχώρο.
- **Email και ενημερωτικά δελτία:** Χρησιμοποιήστε μηνύματα ηλεκτρονικού ταχυδρομείου και ενημερωτικά δελτία για να ενημερώνετε τους γονείς σχετικά με πρόσφατες απειλές και συμβουλές για την ασφάλεια στον κυβερνοχώρο.
- **Διαδικτυακές πύλες:** Χρησιμοποιήστε σχολικές διαδικτυακές πύλες για κοινή χρήση πόρων και ενημερώσεων σχετικά με την ασφάλεια στον κυβερνοχώρο.
- **Μηχανισμοί αναφοράς:** Καθιέρωση σαφών διαδικασιών αναφοράς και αντιμετώπισης ανησυχιών σχετικά με την ασφάλεια στο διαδίκτυο με τους γονείς.



Χρήσιμες Πληροφορίες

Αρμόδιοι Φορείς και Εκπαιδεύτικοί Πόροι

- Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY) - https://ncc.cy/
- National CSIRT Cy - https://csirt.cy/
- Αστυνομία (Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος) - https://cyberalert.cy/
- Γραφείο Επιτρόπου Προστασίας Δεδομένων- https://www.dataprotection.gov.cy/

- CyberSafety European Project - https://cybersafety.cy/
- Internet Safety - https://internetsafety.pi.ac.cy/


IS YOUR CHILD
SAFE ONLINE?