ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ «ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

«Σύγχρονοι κίνδυνοι που αντιμετωπίζουν οι ανήλικοι στο διαδίκτυο και τρόποι προστασίας»

Μηλιώνη Ελένη ΜΤΕ1821

Επιβλέπων Καθηγητής: Κωνσταντίνος Λαμπρινουδάκης

Πειραιάς, Φεβρουάριος 2021

Περιεχόμενα

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω θερμά για την εκπόνηση και ολοκλήρωση της παρούσας διπλωματικής τον επιβλέποντα καθηγητή μου κ. Κωνσταντίνο Λαμπρινουδάκη για όλη την βοήθεια και τις συμβουλές που μου προσέφερε και την αμέριστη κατανόηση και ανταπόκρισή του σε όποιο πρόβλημα αντιμετώπισα.

Επίσης θα ήθελα να ευχαριστήσω και τους καθηγητές μου κατά την διάρκεια του μεταπτυχιακού κ.Λίλιαν Μήτρου, κ Χρήστο Ξενάκη, κ Χριστόφορο Νταντογιάν κ. Παναγιώτη Ριζομυλιώτη για όλες τις γνώσεις και βοήθεια που μου προσέφεραν.

Τέλος θα ήθελα να ευχαριστήσω την οικογένεια μου για όλη την συμπαράσταση εμπιστοσύνη και βοήθεια που μου προσέφερε καθ όλη την πορεία του μεταπτυχιακού μου.

Κεφάλαιο 1: Εισαγωγή

Το Internet έχει γίνει μια βασική υποδομή που με σχεδόν 3.5 δισεκατομμύρια χρήστες έχει τη δυνατότητα να συνδέει ανθρώπους επιχειρήσεις και να διευκολύνει την παροχή υπηρεσιών και την οικονομική ανάπτυξη (International Telecommunication Union, ITU, 2016) Σύμφωνα με έρευνες το 1/3 των χρηστών του διαδικτύου είναι παιδιά με το ποσοστό αυτό να αυξάνετε σε χώρες χαμηλού εισοδήματος

Στη σύγχρονη εποχή, με την ραγδαία αύξηση της τεχνολογίας και της κυριαρχίας των μέσων κοινωνικής δικτύωσης, η ζωή του ανηλίκου δεν μπορεί να μείνει ανεπηρέαστη.
Ο ανήλικος, πολύ πρώιμα μπαίνει στον διαδικτυακό κόσμο και έρχεται αντιμέτωπος με σημαντικές προκλήσεις.
Το διαδίκτυο, τα κινητά τηλέφωνα οι υπολογιστές και γενικότερα τα ηλεκτρονικά μέσα της εποχής μας δίνουν σε παιδιά και νέους μια πρόσβαση
σε παιδιά που ούτε θα μπορούσαν να φανταστούν πριν από 20 χρόνια.

Σε αυτό το πλαίσιο, η καθημερινότητά του διαμορφώνεται και καθορίζεται, σε μεγάλη έκταση και σε μεγάλο βαθμό, από τη χρήση της τεχνολογίας
και των μέσων κοινωνικής δικτύωσης τα οποία δημιουργούν νέους τρόπους απασχόλησης του ελεύθερου χρόνου με διαφορετικές δραστηριότητες.
Με αυτά τα δεδομένα είναι πολύ δύσκολο να διασφαλιστεί η ασφάλεια των παιδιών στο διαδίκτυο και κρίνεται απαραίτητη η σωστή κατανόηση και αύξηση του επιπέδου γνώσεων εκείνων που πρέπει να τους προστατέψουν κυρίως των γονέων και των εκπαιδευτικών.
Σε καμία περίπτωση δεν πρέπει να αφεθούν σε αυτόν τον αχανή κόσμο ανεξέλεγκτα καθώς από την νεαρή κιόλας ηλικία χρειάζονται όρια και καθοδήγηση
Είναι απαραίτητο να αναπτυχθούν μηχανισμοί στην συμπεριφορά των παιδιών και εφήβων που θα τα βοηθήσουν στο να διαχωρίζουν και να αποκλείουν ακατάλληλα περιεχόμενα και παράλληλα να είναι σε θέση να πάρουν σωστές αποφάσεις όταν αυτό απαιτηθεί.

Τα παιδιά ως μελλοντικοί «ψηφιακοί πολίτες» βομβαρδίζονται με μηνύματα και υποσχέσεις για έναν τέλειο ψηφιακό κόσμο στον οποίο θα μπορούν να καινοτομούν, να επικοινωνούν και να συνεργάζονται με τον πιο έξυπνο τρόπο. Αυτό όμως θα γίνει πραγματικότητα μόνο αν λαμβάνουν συνεχώς νέες γνώσεις παραμένουν ενήμερα και λαμβάνουν την απαραίτητη προστασία και υποστήριξη κάνοντας την τεχνολογία σύμμαχο για το μέλλον.

Στην παρούσα διπλωματική εργασία θα προσπαθήσουμε να καταλάβουμε και να απαριθμήσουμε τους βασικότερους κινδύνους που μπορεί ένα παιδί να συναντήσει στο διαδίκτυο καθώς και να δώσουμε κάποιες χρήσιμες και κατανοητές συμβουλές σε παιδιά και γονείς που μπορούν να κάνουν την χρήση του διαδικτύου ασφαλέστερη.

1.1 Διαδίκτυο

Το διαδίκτυο αποτελεί μια από τις βάσεις της σημερινής κοινωνίας. Έχει αλλάξει τον τρόπο με τον οποίο ο κόσμος επικοινωνεί δουλεύει μαθαίνει και το σπουδαιότερο ζει. Το διαδίκτυο μπορεί να περιγραφεί ως ένα τεράστιο πλέγμα ψηφιακών γραμμών το οποίο διασυνδέει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα διασκορπισμένα σε όλο τον κόσμο παρέχοντας σε αυτούς ποικιλία υπηρεσιών και εργαλείων.
Στα σπουδαιότερα πλεονεκτήματά του κατατάσσονται η ταχύτητα και η άνεση. Η σωστή χρήση του διαδικτύου μπορεί να ανεβάσει το μορφωτικό επίπεδο των χρηστών καθώς προσφέρει επίκαιρα στοιχεία σε όλους τους τομείς της γνώσης. Το διαδίκτυο και κατ' επέκταση οι ηλεκτρονικοί υπολογιστές, τα ταμπλετ και τα κινητά είναι αναπόσπαστα κομμάτια της καθημερινότητας μας είτε ως μέσα ψυχαγωγία είτε ενημέρωσης είτε ως μέσα διεκπεραίωσης επαγγελματικών υποχρεώσεων. Το διαδίκτυο θεωρείται το μεγαλύτερο παγκοσμίως σύστημα ηλεκτρονικών υπολογιστών το οποίο λόγω της ανοιχτής δομής του συνδέει εκατομμύρια χρήστες σε όλο τον κόσμο

Είναι λοιπόν ένα συνεχόμενα αυξανόμενο μέρος του σημερινού πολιτισμού ειδικά για παιδιά και νέους για τους οποίους οι σχολικές εργασίες, τα διαδικτυακά παιχνίδια και η κοινωνική δικτύωση είναι από τις πιο δημοφιλείς δραστηριότητες.
Ωστόσο η έλλειψη κοινής τακτικής σχετικά με την σωστή προσέγγιση στην εκπαίδευση και προστασία των παιδιών δημιουργεί περαιτέρω προκλήσεις στην διαδικτυακή εμπειρία του παιδιού.
Επιπροσθέτως πολιτισμικές και γεωγραφικές διαφορές στα νομικά και κοινωνικά πρότυπα αντικατοπτρίζουν το γεγονός ότι δεν υπάρχει καθολικά αποδεκτή άποψη για το τι ορίζει ένα άτομο ως παιδί ή για το τι είναι κατάλληλο για παιδιά, καθιστώντας δύσκολο τον ορισμό του «ακατάλληλου περιεχομένου»

Είναι επομένως ζωτικής σημασίας για τους γονείς, τους εκπαιδευτικούς και το κράτος να εκπαιδεύσουν τα παιδιά και τους νέους για τους κινδύνους και τις ευθύνες που ενδέχεται να αντιμετωπίσουν κατά την χρήση του διαδικτύου βοηθώντας τα να αναγνωρίζουν και να αποφεύγουν τους κινδύνους ενώ παράλληλα θα αποκτούν δεξιότητες ώστε να αποκομίσουν τα μέγιστα οφέλη που προσφέρει το διαδίκτυο.

Κεφάλαιο 2: Ανήλικοι και διαδίκτυο

Οι σύγχρονοι νέοι μεγαλώνουν σε ένα κόσμο όπου η ψηφιακή επικοινωνία θεωρείται τόσο φυσιολογική όσο η επαφή πρόσωπο με πρόσωπο και η τηλεφωνική επικοινωνία για τις προηγούμενες γενιές. Ενώ οι ενήλικες αντιλαμβάνονται μια σαφή διαφορά μεταξύ των offline και online κόσμων για τους νέους που έχουν δίκτυα επικοινωνίας και στους δύο κόσμους η διαφοροποίηση μοιάζει ασήμαντη. Τα ηλεκτρονικά μέσα είναι βασικά για την ζωή ενός μεγάλου αυξανόμενου ποσοστού παιδιών όσον αφορά τις σχέσεις και την επικοινωνία. Τους παρέχουν πρόσβαση σε πληροφορίες, παιχνίδια, ψυχαγωγία πολιτισμό και τέχνες καθώς και τρόπους ανταλλαγής περιεχομένου. Επίσης αυξανόμενος φαίνεται να είναι και αριθμός των νέων που δημιουργούν και εξερευνούν τα δικά τους εικονικά κοινωνικά δίκτυα. Με τη χρήση των ιστοσελίδων, των sites, των κινητών τηλεφώνων των εφαρμογών, την χρήση της κάμερας ,κονσόλες παιχνιδιών υπάρχει πρόσβαση σε πληροφορίες, διαδικτυακές διαφημίσεις πολιτικές, θρησκευτικές, σεξουαλικές και πολιτιστικές ιδέες που μπορεί να έρχονται σε αντίθεση με αυτές των γονιών τους. Επομένως φαίνεται πως παιδιά και νέοι δεν είναι απλώς παθητικοί χρήστες τεχνολογιών αλλά συμμετέχουν ενεργά στην διαμόρφωσή τους ώστε να ικανοποιήσουν τις απαιτήσεις και τα συμφέροντά τους.

2.1 Κίνδυνοι του διαδικτύου

Ωστόσο το διαδίκτυο δεν παύει να εγκυμονεί κινδύνους για τους ανηλίκους.

Σύμφωνα με την εφημερίδα Daily Mail , ένα στα 10 παιδιά έχουν προβλήματα ψυχικής υγείας και το 1/3 των εφήβων αισθάνονται κακόκεφοι, λυπημένοι, τουλάχιστον μία φορά την εβδομάδα . Η έρευνα της Daily Mail αναφέρει ότι , «Τα παιδιά που περνούν περισσότερο χρόνο με υπολογιστές , βλέποντας τηλεόραση και παίζοντας βιντεοπαιχνίδια έχουν την τάση να αντιμετωπίζουν υψηλότερα επίπεδα συναισθηματικής δυσφορίας , άγχους και κατάθλιψης . Τα στοιχεία δείχνουν ότι κάθε επιπλέον ώρα χρήσης του υπολογιστή και του Internet, αυξάνει την πιθανότητα των παιδιών που βιώνουν κοινωνικοοικονομικά προβλήματα. Επίσης, αυξάνει τον κίνδυνο τα παιδιά αυτά να γίνουν ενήλικες με εξαιρετικά χαμηλή αυτοεκτίμηση.

Τα προβλήματα ψυχικής αρχίζουν από οκτώ έως δεκαπέντε ετών . Το 50% της κακής ψυχικής υγείας ξεκινά στην ηλικία των δεκατεσσάρων και το 10% των παιδιών σήμερα έχουν κάποιο είδος σοβαρού ψυχολογικού προβλήματος. Επιπλέον 1% των εφήβων είχαν ρεκόρ εθισμού ενώ το 12,8% παρουσίασαν οριακή χρήση που θα μπορούσε να οδηγήσει σε εθισμό στο μέλλον[1]

[1] Βλαβερές συνέπειες του Internet στα παιδιά και τους εφήβους Χ.Τσιώτση www.news.gr

Εκτός όμως από τον εθισμό υπάρχουν βασικές κατηγορίες κινδύνων που μπορεί να αντιμετωπίσουν οι ανήλικοι:2

- **Διαδικτυακός εκφοβισμός(cyber bullying):** Το παιδί ή ο έφηβος δέχεται απειλές, ταπεινώνεται ή γίνεται στόχος από κάποιο άλλο παιδί ή έφηβο συνήθως με επαναλαμβανόμενο τρόπο μέσω της χρήσης του διαδικτύου ή κινητών τηλεφώνων.

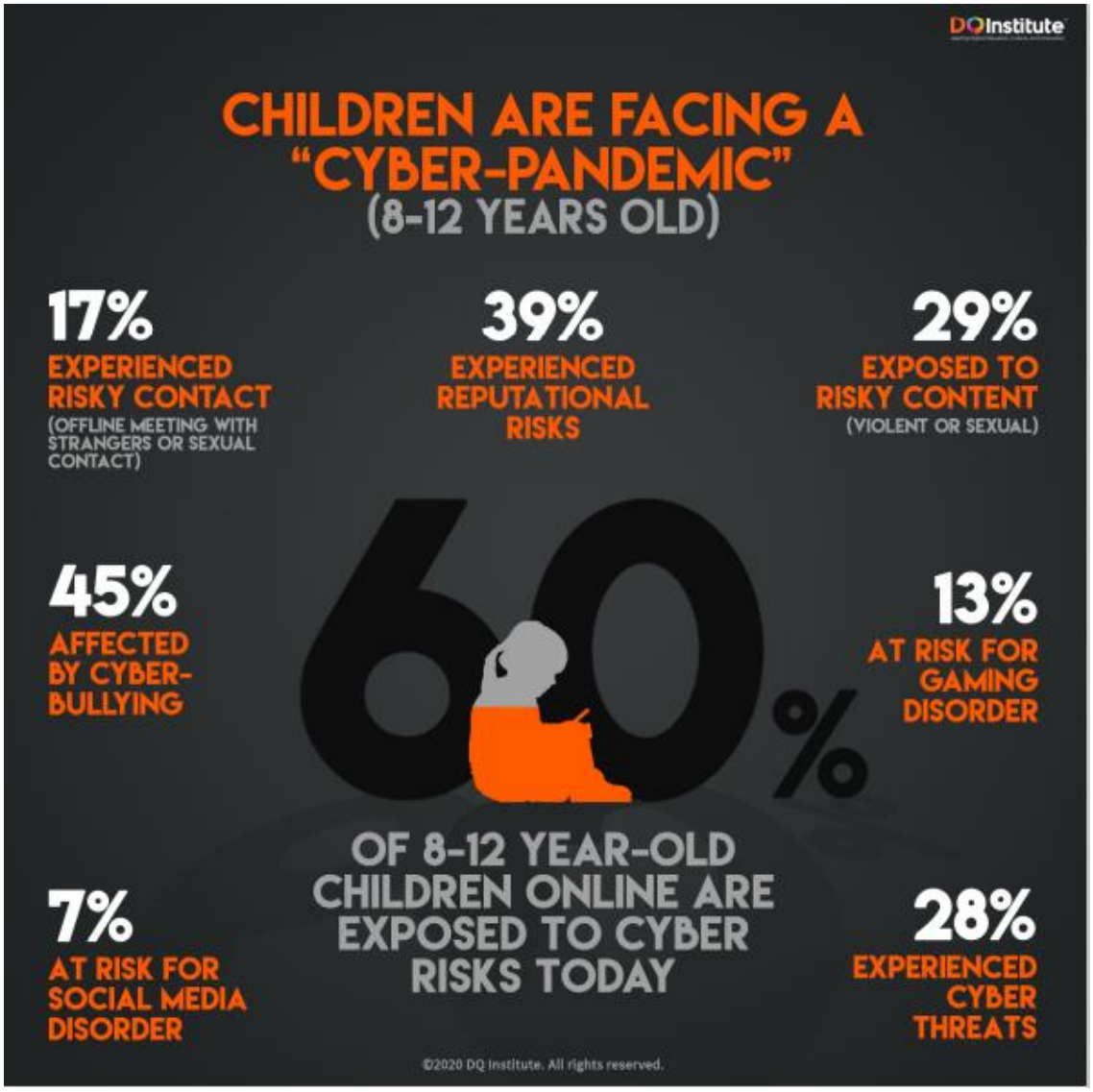
- **Διαδικτυακή αποπλάνηση(grooming):**Ένας διαδικτυακός χρήστης συνήθως ενήλικας προσπαθεί να εμπνεύσει εμπιστοσύνη στο παιδί ώστε να πραγματοποιήσει μια μυστική συνάντηση μαζί του με σκοπό την σεξουαλική εκμετάλλευση.

- **Sexting:** Είναι η αποστολή σεξουαλικών μηνυμάτων και φωτογραφιών μέσω κινητών (SMS) ή μέσω ιστοσελίδων κοινωνικής δικτύωσης (Facebook, Instagram). Επικίνδυνο το καθιστούν οι σοβαρές νομικές συνέπειες που έχει η παραγωγή και διανομή σεξουαλικού περιεχομένου που αφορά ανηλίκους.

- **Ακατάλληλο Περιεχόμενο:** Οποιοδήποτε περιεχόμενο του Διαδικτύου (λεκτικό, ακουστικό, οπτικό) που είναι ακατάλληλο ή επικίνδυνο για παιδιά και παρόλα αυτά δημόσια προσβάσιμο (πορνογραφικό υλικό, βίαιο περιεχόμενο)

- **Διαδικτυακά Παιχνίδια:** Πολλά παιδία (εκτός από τον εθισμό τους σε Video Games και την έκθεση τους σε επικίνδυνες σκηνές βίας μέσα απ' αυτά) έχουν οδηγηθεί στην αυτοκτονία συμμετέχοντας σε επικίνδυνα παιχνίδια τύπου «Μπλε Φάλαινα»

[2] Εθισμός στο Διαδίκτυο www.help-line.gr

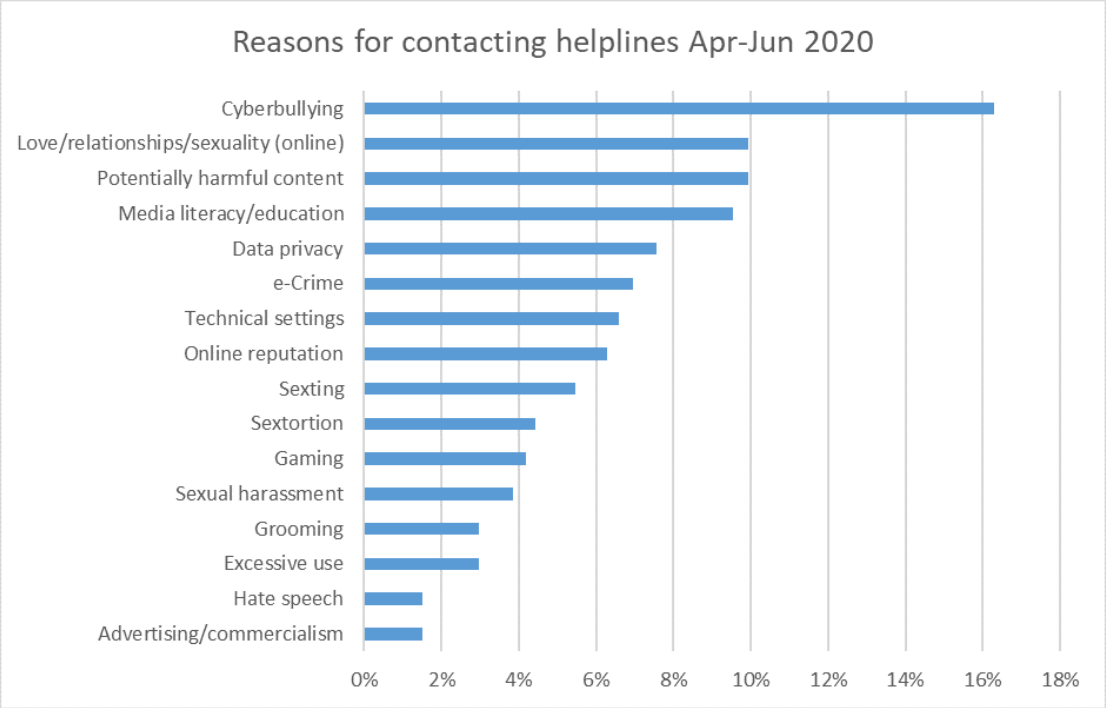


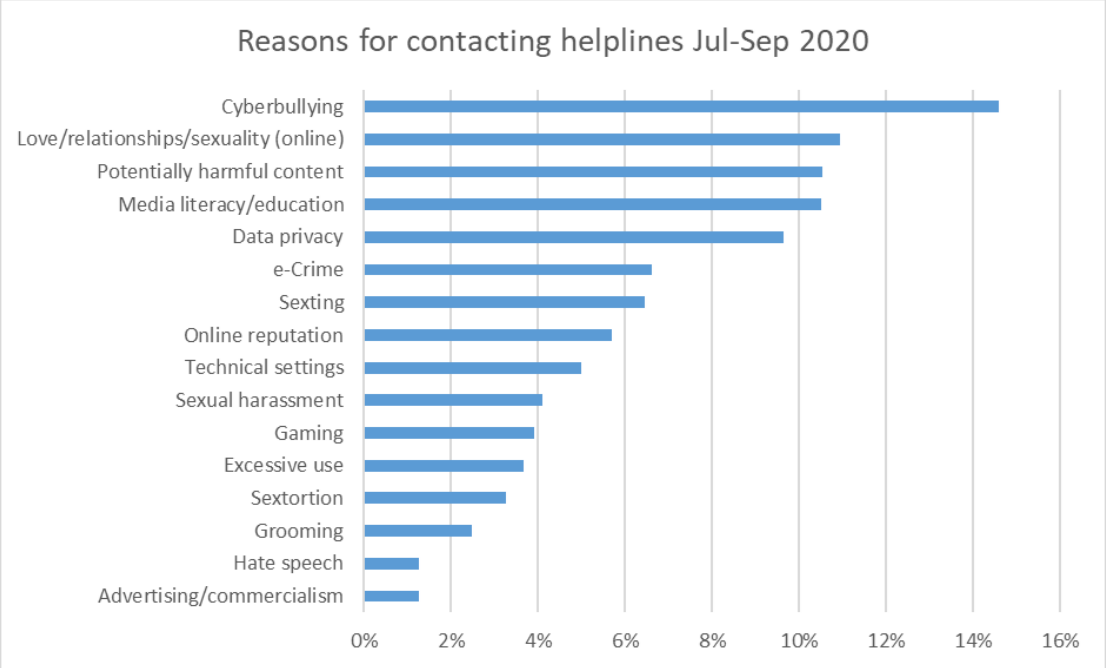
2.2 Covid-19

Κατά την περίοδο της πανδημίας του Covid-19 φαίνεται πως οι κίνδυνοι που αναφέραμε και θα αναλύσουμε στην συνέχεια αυξήθηκαν σημαντικά.

Τα συγκεκριμένα στοιχεία είναι με βάση την έρευνα του INSAFE το οποίο μέσα από τις γραμμές βοηθείας του δέχτηκε συνολικά σε διάστημα τριών μηνών Απρίλιο με Ιούνιο 2020 19,000 κλήσεις. Βασικός λόγος επικοινωνίας παρέμεινε ο διαδικτυακός εκφοβισμός με ποσοστό 16%.
Το 60% πραγματοποιήθηκε από την ηλικιακή ομάδα 12-18 ετών αν και αξίζει να σημειωθεί ότι το 14% των κλήσεων προήλθε από νεότερους χρήστες ηλικίας 5-11 ετών[3]

[3] Better Internet for Kids, Latest helpline trends www.betterinternetforkids.eu





Στην δεύτερη εικόνα φαίνεται η ίδια έρευνα κατά το τρίμηνο Ιουλίου-Σεπτεμβρίου. Βλέπουμε ότι υπάρχει μια σχετική μείωση σε πολλές περιπτώσεις σε σύγκριση με το προηγούμενο τρίμηνο με σύνολο κλήσεων 13,500 δεν μπορεί όμως να αγνοηθεί το γεγονός ότι υπάρχει αύξηση της τάξεως του 33% σε σχέση με το αντίστοιχο τρίμηνο του 2019.

Οι περισσότερες κλήσεις έγιναν από κοπέλες (60%) και παρατηρείται αύξηση των κλήσεων από γονείς και καθηγητές καθώς συμπίπτει με την επιστροφή των μαθητών στα σχολεία δείχνοντας την δυσκολία των παιδιών να ενταχθούν σε αυτό το νέο σύστημα εργασίας/μάθησης από το σπίτι για τόσο μεγάλο διάστημα.

Κεφάλαιο 3 :Cyber Bullying

3.1 Τι είναι το Cyber Bullying?

Το Cyber Bullying (Διαδικτυακός Εκφοβισμός) είναι ο εκφοβισμός ενός ατόμου με την χρήση ψηφιακών τεχνολογιών. Καθώς η τεχνολογία εξελίσσεται υπάρχουν περισσότερες πιθανές δυνατότητες εκφοβισμού στον κυβερνοχώρο.
Σύμφωνα με τους Dehue, Bolman and Völlink (2008) τρεις είναι οι βασικές προϋποθέσεις που πρέπει να πληρούνται για να χαρακτηριστεί μια συμπεριφορά ως κυβερνοεκφοβιστική:
α. να είναι επαναλαμβανόμενη
β. να έχει ψυχολογικές επιπτώσεις στο θύμα και
γ. να γίνεται με πρόθεση
Μπορεί να πραγματοποιηθεί σε μέσα κοινωνικής δικτύωσης, σε πλατφόρμες ανταλλαγής μηνυμάτων, μέσω email,σε πλατφόρμες παιχνιδιών, κινητά τηλέφωνα κ.α.
Είναι επαναλαμβανόμενη συμπεριφορά που στόχο έχει να τρομάξει, να ντροπιάσει να εξοργίσει τα θύματα. Ο εκφοβισμός τέτοιου είδους η παρενόχληση και οι φάρσες έχουν συνδεθεί με την κατάθλιψη των νέων ,κυρίως εφήβων, την χαμηλή αυτοεκτίμηση και τις τραγωδίες αυτοκτονίας.

Παραδείγματα εκφοβισμού στον κυβερνοχώρο περιλαμβάνουν ανάρτηση προσβλητικών σχολίων ή φωτογραφιών στα μέσα κοινωνικής δικτύωσης ή ακόμη και δημιουργία ψεύτικων διαδικτυακών προφίλ για να υποτιμήσουν κάποιο άλλο άτομο. Ο εκφοβισμός στον κυβερνοχώρο είναι ευρέως διαδεδομένος στον κόσμο, ιδίως μεταξύ των νέων. Μια εθνική έρευνα που διενήργησε η φιλανθρωπική οργάνωση BullyingUK διαπίστωσε ότι το 42% των ατόμων κάτω των 25 ετών ένιωσαν ανασφαλή στο διαδίκτυο. Το 56% των κάτω των 25 ετών είπε ότι είδαν άλλους να έχουν εκφοβιστεί στο διαδίκτυο.

3.2 Μορφές Cyber Bullying

Υπάρχουν πολλές διαφορετικές εκδοχές με τις οποίες μπορεί να εκδηλωθεί ο διαδικτυακός εκφοβισμός όμως η πλειοψηφία των διαδικτυακών παρενοχλήσεων αφορά τις παρακάτω:

1)**Αποκλεισμός (Exclusion)**

Αποκλεισμός είναι η πράξη του να αφήνεις κάποιον «εκτός» σκόπιμα και χρησιμοποιείται για στόχευση και εκφοβισμό του θύματος. Στην περίπτωση αυτή το παιδί μπορεί να αποκλειστεί από διαδικτυακές συνομιλίες καθώς μπορεί να έχουν επισημανθεί άλλοι φίλοι του αλλά όχι αυτό. Επίσης σε περίπτωση που δεν έχει κάποιο smartphone ‘η δεν χρησιμοποιεί συγκεκριμένους ισοτόπους κοινωνικής δικτύωση εξαιρείται σκόπιμα από συνομιλίες και δραστηριότητες από άλλους.

2)**Παρενόχληση(Harassment)**

Η παρενόχληση είναι μια ευρεία κατηγορία στην οποία εμπίπτουν πολλοί τύποι εκφοβισμού στον κυβερνοχώρο αλλά γενικότερα αναφέρεται σε μία συνεχή και σκόπιμη μορφή εκφοβισμού που περιλαμβάνει καταχρηστικά ή απειλητικά μηνύματα που αποστέλλονται με την πρόθεση να βλάψουν κάποιον.
Αυτή είναι μια πολύ επικίνδυνη μορφή εκφοβισμού καθώς μπορεί να έχει σοβαρές επιπτώσεις στην υγεία του παιδιού.
Τα μηνύματα συχνά είναι αγενή και επιθετικά ο επιτιθέμενος δεν σταματάει και καταβάλλει μεγάλη προσπάθεια να προκαλέσει φόβο και πόνο, πράγμα που μπορεί να επηρεάσει την αυτοεκτίμηση και αυτοπεποίθηση του παιδιού.

3)**Αποκάλυψη (Outing/Doxing)**

Η αποκάλυψη αφορά την δημοσιοποίηση ευαίσθητων ή προσωπικών πληροφοριών για κάποιον χωρίς την συγκατάθεσή του με σκοπό να νιώσει το θύμα αίσθημα ντροπής και ταπείνωσης για τον δημόσιο εξευτελισμό του.
Αυτό μπορεί να αφορά την δημοσιοποίηση προσωπικών φωτογραφιών ή εγγράφων καθώς και την χρήση αποθηκευμένων προσωπικών μηνυμάτων σε ιδιωτική συνομιλία.
Το βασικό στοιχείο είναι η έλλειψη συναίνεσης από το θύμα.

4)**Εξαπάτηση(Trickery)**

Η εξαπάτηση μοιάζει αρκετά με την αποκάλυψη με ένα επιπλέον στοιχείο.
Σε αυτή την περίπτωση ο εκφοβιστής θα γίνει φίλος με το θύμα και θα το ξεγελάσει με μία ψευδή αίσθηση ασφάλειας. Μόλις αποκτήσει την εμπιστοσύνη του στόχου κάνει κατάχρηση αυτής της εμπιστοσύνης και μοιράζεται τα μυστικά και τις προσωπικές πληροφορίες του θέματος σε τρίτους

5)**Διαδικτυακή Παρακολούθηση(Cyberstalking)**

Η συγκεκριμένη μορφή εκφοβισμού είναι ιδιαίτερα σοβαρή καθώς μπορεί να επηρεάσει την ψυχική αλλά και σωματική υγεία του παιδιού.
Μπορεί αν περιλαμβάνει παρακολούθηση, ψευδείς κατηγορίες, απειλές και συχνά συνοδεύεται και από καταδίωξη εκτός σύνδεσης.
Επίσης μπορεί να αναφερθεί στην χρήση του Διαδικτύου από ενήλικες με σκοπό την επικοινωνία τους αλλά και την συνεύρεσή τους με νέους για σεξουαλικούς σκοπούς.
Κατατάσσετε σε ποινικό αδίκημα και μπορεί να οδηγήσει σε περιοριστικά μέτρα ακόμα και φυλάκιση για τον δράστη.

6**)Fraping**

Η λέξη frape είναι συνδυασμός των λέξεων Facebook και rape (βιασμός) με μία παραφρασμένη έννοια και αναφέρεται στον εκφοβιστή που χρησιμοποιεί το Facebook αλλά και άλλα μέσα κοινωνικής δικτύωσης του θύματος ‘όταν τα έχει χωρίς επίβλεψη για να δημοσιεύσει ακατάλληλο περιεχόμενο με το όνομά του.
Πολλοί το βλέπουν ως αστείο και το θεωρούν ακίνδυνο να αλλάζουν μία εικόνα προφίλ ή να αναρτούν μια δημοσίευση στο προφίλ του άλλου αλλά μπορεί να έχει εξαιρετικά επιβλαβείς συνέπειες για το θύμα.

7)**Μεταμφίεση(Masquerading)**

Σε αυτή την περίπτωση ο εκφοβιστής δημιουργεί ένα ψεύτικο προφίλ ή online ταυτότητα στο διαδίκτυο με σκοπό τον εκφοβισμό κάποιου στο διαδίκτυο.
Αυτό μπορεί να περιλαμβάνει την δημιουργία ψεύτικου λογαριασμού email, ψεύτικου προφίλ κοινωνικής δικτύωσης(Facebook,Instagram κ.α.) με την επιλογή νέων φωτογραφιών με σκοπό να ξεγελάσει το θύμα για την ταυτότητά του.
Σε αυτές τις περιπτώσεις ο εκφοβιστής τείνει να είναι κάποιος που το θύμα γνωρίζει καλά

8)**Προσβολή(Dissing)**

Σε αυτήν την περίπτωση ο εκφοβιστής διαδίδει πληροφορίες για τον στόχο του μέσω δημοσίων δημοσιεύσεων ή ιδιωτικών μηνυμάτων σε τρίτους για να καταστρέψει και να εξευτελίσει το θύμα την φήμη του και την σχέση του με ΄τους άλλους.
Σε αυτές τις καταστάσεις ο εκφοβιστής τείνει να έχει προσωπική σχέση με το θύμα (οικογενειακή, φιλική, ερωτική στις μεγαλύτερες ηλικίες)

9)**Κοροϊδία(Trolling)**

Στην συγκεκριμένη μορφή ο εκφοβιστής θα επιδιώξει να εκνευρίσει/ενοχλήσει σκόπιμα το θύμα αναρτώντας κακοπροαίρετα σχόλια στο διαδίκτυο. Συνήθως δεν έχουν προσωπική σχέση με τα θύματα γι’ αυτό και ψάχνουν ευάλωτα άτομα με στόχο να τα ενοχλήσει τόσο ώστε να ενεργήσουν με τον ίδιο τρόπο και γενικότερα προσπαθούν να κάνουν του άλλους να νιώσουν άσχημα ώστε να αισθανθούν εκείνοι καλά.

Το Trolling μπορεί να μην είναι πάντα μια μορφή εκφοβισμού στον κυβερνοχώρο αλλά μπορεί να χρησιμοποιηθεί σαν εργαλείο για τον διαδικτυακό εκφοβισμό όταν γίνεται με κακόβουλη πρόθεση.

10)**Στην πυρά(Flaming)**

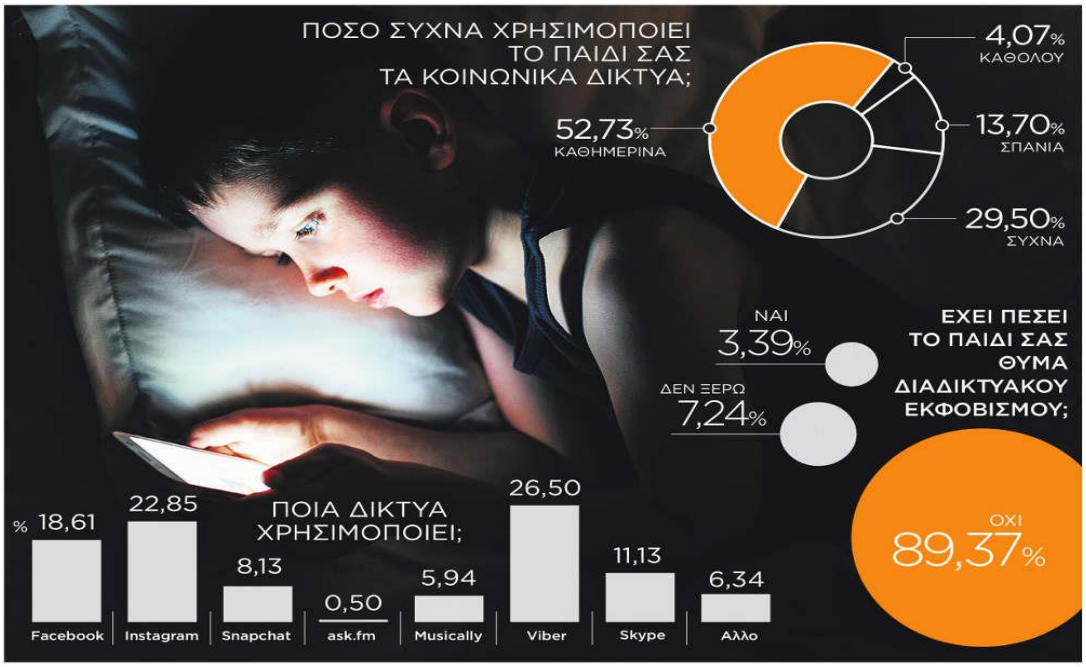
Σε αυτή την περίπτωση ο εκφοβιστής έχει μια άμεση επίθεση ενάντια στο θύμα με την αποστολή προσβολών και βωμολοχιών με σκοπό να τον οδηγήσει σε μια διαδικτυακή «μάχη» πολλών απαντήσεων.
Τέτοιες περιπτώσεις συναντάμε σε ομαδικά γκρουπ οπού ο θύτης επαναλαμβανόμενα αναρτά δημοσιεύσεις με σκοπό να επιβάλει την άποψή του.

11)**Catfishing**

Μοιάζει αρκετά με την μορφή του Masquerading μόνο που σε αυτή την περίπτωση ο εκφοβιστής κλέβει την διαδικτυακή ταυτότητα του παιδιού (συνήθως φωτογραφίες και προσωπικές πληροφορίες) με σκοπό να δημιουργήσει ένα ψεύτικο προφίλ στα μέσα κοινωνικής δικτύωσης με τα στοιχεία του θύματος.
Αυτό έχει σαν στόχο την εξαπάτηση όχι μόνο του θύματος αλλά και του κοινωνικού του περιβάλλοντος καθώς και την καταστροφή της φήμης του.

12)**Χαρωπό Χαστούκισμα(Happy Slapping)**

Η συγκεκριμένη μορφή εκφοβισμού λέγεται ότι ξεκίνησε στο Ηνωμένο Βασίλειο και περιλαμβάνει παιδιά που καταγράφουν σε βίντεο με τα κινητά τους ένα περιστατικό φυσικού εκφοβισμού(το θύμα χτυπάται από ένα ή και περισσότερα παιδιά ταυτόχρονα) το οποίο δημοσιεύουν στο YouTube και στα μέσα κοινωνικής δικτύωσης μέσω μαζικών μηνυμάτων. Στόχος τους είναι να ατιμάσουν και να ντροπιάσουν το θύμα.

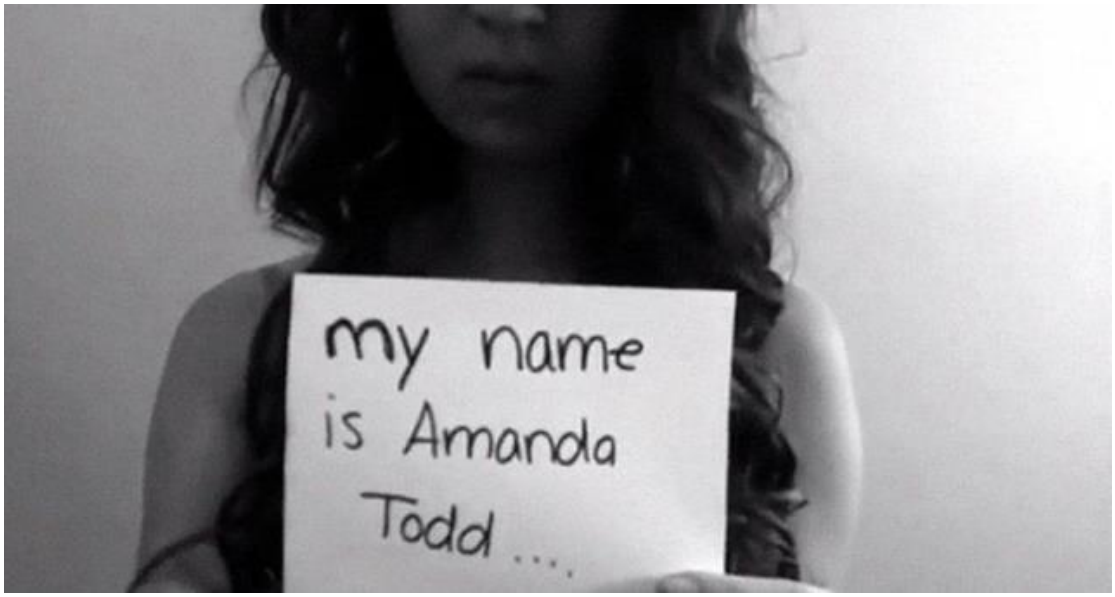


3.3 Συνέπειες του Cyber Bullying

Όταν τα παιδιά βιώνουν περιστατικά bullying αντιμετωπίζουν ένα σύνολο σωματικών ψυχολογικών αλλά και συναισθηματικών επιπτώσεων. Κατά συνέπεια μπορεί να διαμαρτύρονται για τα πάντα από φόβο και άγχος έως κατάθλιψη και χαμηλή αυτοεκτίμηση.
Στην πραγματικότητα, περισσότερο από το 30% των παιδιών που στοχεύουν οι cyberbullies αναφέρουν ότι αντιμετωπίζουν συμπτώματα άγχους και το 93% ανέφεραν αίσθημα θλίψης αδυναμίας και απελπισίας.[4]

Τα θύματα του διαδικτυακού εκφοβισμού δεν ζητάνε εύκολα βοήθεια και δεν παραδέχονται ότι είναι θύματα αντ' αυτού πιστεύουν ότι κανείς δεν μπορεί να τα βοηθήσει και να τα καταλάβει με αποτέλεσμα να φτάνουν σε αυτοκαταστροφικό σημείο ακόμα και στην αυτοκτονία.
Χαρακτηριστικό είναι το παράδειγμα της νεαρής Amanda Todd ως ένα από τα πρώτα θύματα του cyberbullying.

[4] Current perspectives: the impact of cyberbullying on adolescent health by Charisse L Nixon



Στο συγκεκριμένο βίντεο η ίδια η Amanda αφηγείται την ιστορία της με την χρήση καρτών που δείχνει στην κάμερα. Λέει για το πως η ίδια βίωσε τον εκβιασμό και τον διαδικτυακό εκφοβισμό καθώς σε μια διαδικτυακή εφαρμογή γνωριμιών γνώρισε τον εκβιαστή της ο οποίος την παρέσυρε και την τράβηξε κάποιες ερωτικές φωτογραφίες τις οποίες ύστερα απείλησε ότι θα τις δημοσιεύσει, πράγμα που έκανε στο Facebook. Η Amanda αναγκάστηκε να αλλάξει αρκετά σχολεία όμως κάθε φορά ο εκβιαστής της την εντόπιζε και δημοσίευε τις φωτογραφίες της στους νέους της φίλους.
Η Amanda οδηγήθηκε στο αλκοόλ και τις καταχρήσεις απομονωμένη καθώς ήταν από τον κοινωνικό περίγυρο και δημοσιεύει αυτό το βίντεο εξιστορώντας τις δυσκολίες που πέρασε ένα μήνα πριν βάλει τέλος στην ζωή της μην αντέχοντας τον εξευτελισμό.

3.4 Νομοθετικό πλαίσιο

Στην Ελληνική Νομοθεσία δεν υπάρχει ακόμα ορισμός «cyberbullying» ο οποίος να ποινικοποιείται. Επιπροσθέτως, πάρα το γεγονός ότι τόσο σε διεθνές (Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα-CETS No. 185, Budapest, 23.XI.2001, σε ισχύ από τις 01.07.2004) και γνωσιακό επίπεδο (Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου) αλλά και στο Ελληνικό δίκαιο (Ν.4322/2015-ΦΕΚ Α' 42/27-04-2015 & Ν. 4411/2016-ΦΕΚ 142/Α'/03-08-2016) υπάρχει συγκεκριμένο νομοθετικό πλαίσιο ρύθμισης (safeline.gr, 2016), το οποίο δυστυχώς δεν είναι ενιαίο για όλα τα κράτη παγκοσμίως ή τουλάχιστον για τα κράτη που έχουν υπογράψει τη Σύμβαση για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης με απότοκο την ύπαρξη νομικών κενών που καθιστούν δυσχερή την ποινική αντιμετώπιση κολάσιμων συμπεριφορών τόσο διασυνοριακά όσο και μέσα σε μια επικράτεια. Όμως, ο τρόπος με τον οποίο εκφράζεται,

π.χ. με το χλευασμό σε συνδυασμό με παραβίαση προσωπικών δεδομένων ή παραποίηση προσωπικών δεδομένων, σαφώς αποτελεί ποινικό αδίκημα.[5]

Κεφάλαιο 4: Παιδική πορνογραφία

Η εκμετάλλευση των παιδιών σεξουαλικά από ενήλικες είναι κάτι που δυστυχώς υπάρχει εδώ και χιλιετίες στον κόσμο. Με την ραγδαία αύξηση της ψηφιακής τεχνολογίας και την επανάσταση που έχει φέρει στον τομέα των επικοινωνιών αυτό το πρόβλημα διογκώθηκε και επεκτάθηκε μέσα από την χρήση του διαδικτύου.
Δυστυχώς για τα παιδιά οι σεξουαλικοί δράστες ανακάλυψαν γρήγορα τις ευκαιρίες που εμφανίστηκαν σε δύο συγκεκριμένους τομείς:
Στις πλατφόρμες επικοινωνίας που δημιουργήθηκαν μπορώντας έτσι να έρθουν σε επαφή με παιδία και να τα εκμεταλλευτούν σεξουαλικά και στην μεταφορά αλλά και κοινή χρήση εικόνας και βίντεο προωθώντας υλικό πορνογραφικού περιεχομένου σε όλο τον κόσμο.

4.1 Τι είναι? Πως ορίζεται?

Η παιδική πορνογραφία είναι μια μορφή σεξουαλικής εκμετάλλευσης παιδιών. Ο νόμος ορίζει την παιδική πορνογραφία ως οποιαδήποτε οπτική απεικόνιση σεξουαλικής άσεμνης συμπεριφοράς που περιλαμβάνει ανήλικο (άτομα κάτω των 18 ετών). Οι εικόνες παιδικής πορνογραφίας αναφέρονται επίσης ως εικόνες σεξουαλικής κακοποίησης παιδιών.

Ο όρος «παιδική πορνογραφία» χρησιμοποιείται συνήθως από νομοθέτες, εισαγγελείς, ερευνητές και το κοινό για να περιγράψει αυτήν τη μορφή σεξουαλικής εκμετάλλευσης παιδιών. Ωστόσο, αυτός ο όρος δεν περιγράφει τον αληθινό τρόμο που αντιμετωπίζουν αμέτρητα παιδιά κάθε χρόνο. Η παραγωγή παιδικής πορνογραφίας δημιουργεί ένα μόνιμο αρχείο για τη σεξουαλική κακοποίηση ενός παιδιού. Όταν αυτές οι εικόνες τοποθετούνται στο Διαδίκτυο και διαδίδονται στο Διαδίκτυο, η θυματοποίηση των παιδιών συνεχίζεται διαρκώς. Εμπειρογνώμονες και θύματα συμφωνούν ότι τα θύματα που απεικονίζονται στην παιδική πορνογραφία υποφέρουν σε ολόκληρη τη ζωή τους από εκ νέου θυματοποίηση γνωρίζοντας ότι οι εικόνες της σεξουαλικής τους κακοποίησης είναι στο Διαδίκτυο για πάντα. Τα παιδιά που έχουν εκμεταλλευτεί με αυτόν τον τρόπο πρέπει να ζουν γνωρίζοντας την δημοσιοποίηση αυτού του περιεχομένου χωρίς να μπορούν να το ανακαλέσουν .
Αυτό δημιουργεί συχνά διαρκή ψυχολογική βλάβη στο παιδί, συμπεριλαμβανομένων διαταραχών στη σεξουαλική ανάπτυξη, της αυτό-εικόνας και της ανάπτυξης σχέσεων εμπιστοσύνης με άλλους στο μέλλον.

[5] Το φαινόμενο του κυβεροεκφοβισμού(cyberbullying) στην Ελλάδα και το εξωτερικό Θεώνη Σπαθή

4.2 Παιδική Πορνογραφία στο Dark Web

Ένας τεράστιος αριθμός από ιστοσελίδες είναι προσβάσιμες στο ευρύ κοινό. Διάσημες εφαρμογές και site όπως το Facebook, το Instagram ,Twitter Snapchat Wikipedia είναι ελεύθερα προσβάσιμες στο διαδίκτυο το οποίο μπορεί να θεωρηθεί σχετικά ακίνδυνο αν χρησιμοποιείται σωστά. Αυτό είναι που οι περισσότεροι αποκαλούν «επιφανειακό διαδίκτυο» (surface web) με μια συλλογή τουλάχιστον 4,7 δισεκατομμυρίων σελίδων στις οποίες έχει πρόσβαση ο κάθε ένας.

Αυτός ο αριθμός, αν και τεράστιος, μόλις που περιγράφει το πραγματικό μέγεθος του διαδικτύου. Το υπόλοιπο διαδίκτυο γνωστό ως Dark Web 'η Deep Web είναι περίπου 550 φορές μεγαλύτερο από το δημόσιο διαδίκτυο.
Αποτελείται από ιστοτόπους και δεδομένα που δεν βρίσκονται εκεί δωρεάν για όλους απλά με μία αναζήτηση στο Google ή πληκτρολογώντας την διεύθυνση του ιστού τους.
Χρειάζεται ειδικό λογισμικό για να υπάρξει πρόσβαση σε αυτά και το λογισμικό αυτό κάνει τους πάντες ανώνυμους πράγμα που το καθιστά το τέλειο μέρος για κάθε παράνομη δραστηριότητα.

Το να μπει κάποιος στο Dark Web είναι απλό καθώς το μόνο που χρειάζεται να κάνει είναι να κατεβάσει ένα πρόγραμμα περιήγησης που ονομάζεται TOR (το οποίο διατίθεται και ως εφαρμογή για smartphone αλλά και για υπολογιστές) και να συνδεθεί.
Εκεί δεν υπάρχει το Google αλλά μηχανές αναζήτησης όπως το The Hidden wiki, το Duck Duck Go και TOR Links όπου μπορούν να φέρουν αποτελέσματα ιστοτόπων σε μια αναζήτηση για παιδική πορνογραφία που στο επιφανειακό διαδίκτυο θα απαγορευόταν.
Ωστόσο η σύνδεση σε εξειδικευμένες κρυπτογραφημένες μηχανές αναζήτησης όπως το Onion Land και το Onion Dir σε μεταφέρουν σε ένα διαφορετικό κόσμο.
Μόνο στο Onion Land μια αναζήτηση για «παιδική πορνογραφία» εμφανίζει πάνω από 130 συνδέσμους ιστοτόπων. Τα αποτελέσματα είναι σκληρά καθώς υπάρχουν ιστότοποι με εικόνες και βίντεο που κακοποιούν σεξουαλικά παιδιά, τα πωλούν ως σκλάβους κ.α.

Υπάρχουν και ιστότοποι οι οποίοι ακόμα και με αναζήτηση δεν θα σου φέρουν κάποιο αποτέλεσμα αν δεν έχεις πρόσκληση για να μπεις μέσα. Το να προσκληθεί κάποιος δεν είναι εύκολο καθώς θα πρέπει να περάσει ένα crash test καθώς θα πρέπει να αποδείξει ο ενδιαφερόμενος ότι δεν είναι αναλυτής ή ομοσπονδιακός πράκτορας οπότε με αυτά τα τεστ τον αναγκάζουν να κάνει κάτι που νομικά δεν είναι επιτρεπτό.

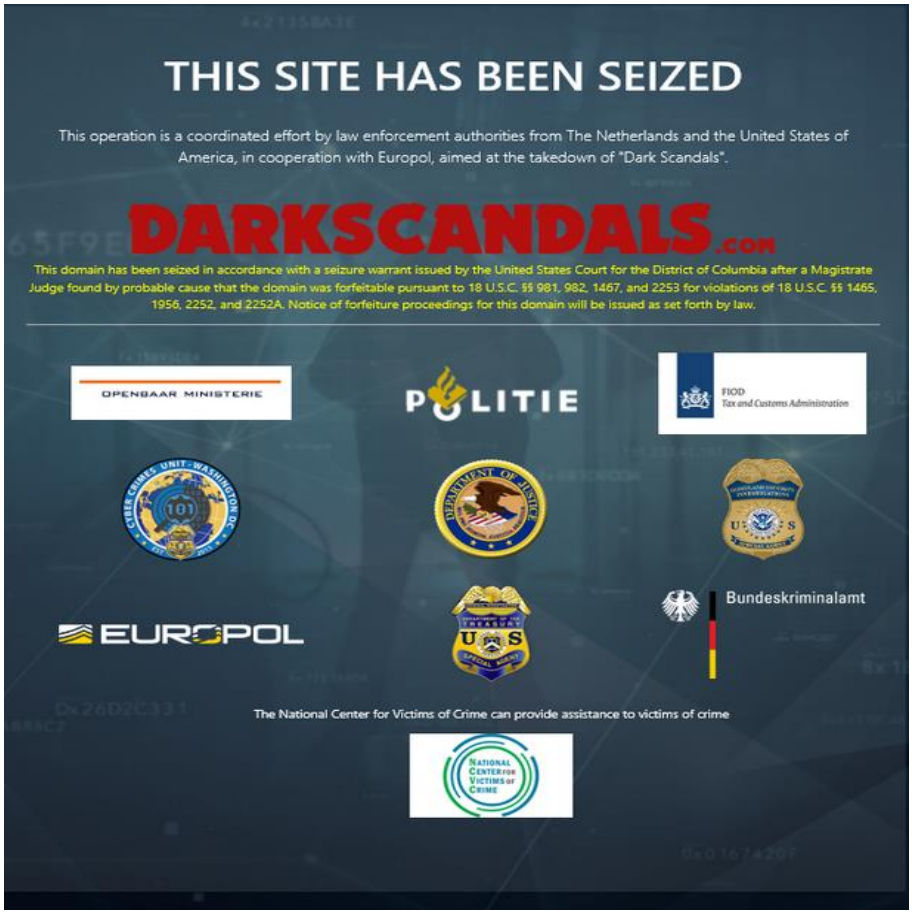
4.3 Πρόσφατα Περιστατικά

Χαρακτηριστικά είναι τα παραδείγματα 2 πρόσφατων επιχειρήσεων που διεξήχθησαν από τις αρχές των Ηνωμένων Πολιτειών και από την Europol.

Το πρώτο αφορά έναν 23χρονο Κορεάτη ο οποίος λειτουργούσε «την μεγαλύτερη αγορά παιδικής πορνογραφίας στο dark web» όπως την αποκαλούσαν.
Το αγγλόγλωσσο site που ονομαζόταν «Welcome to Video» περιείχε περισσότερα από 200,000 μοναδικά βίντεο ή περίπου 8 terabytes δεδομένων που έδειχναν ερωτικές σκηνές παιδιών νηπίων και μωρών. Το 50% του περιεχομένου δεν ήταν γνωστό στις διωκτικές αρχές και υπάρχουν πολλά παιδιά που περιέχονται στα βίντεο και δεν έχουν ταυτοποιηθεί.

Οι χρήστες που ενδιαφερόντουσαν μπορούσαν να αγοράσουν τετοιου ειδους βίντεο ή να έιχαν καποιου είδους ετήσια συνδρομή στην τιμή των 0,03 bitcoin (περίπου 300$)
Τα μέλη του έπαιρναν πόντους κάθε φορά που ανέβαζαν ένα καινούριο βίντεο ή προσκαλούσαν κάποιο νέο μέλος.
Το site κατέβηκε τον Μάρτιο 2018 με τον Κορεάτη να συλλαμβάνεται κατάσχοντας από 24 διαφορετικούς τραπεζικούς λογαριασμούς 7,300 bitcoin (περίπου 730,000$)

Το δεύτερο περιστατικό αφορά μια επιτυχία του Europol's European Cybercrime Centre που ιδρύθηκε το 2013 ώστε να ενδυναμώσει την εφαρμογή του νόμου σε τέτοιου ειδους περιστατικά στην Ευρωπαϊκή Ένωση.
Στις 9 Μαρτίου 2020 ο διαχειριστής του site DarkScandals συλλαμβάνεται στο σπίτι του για κατοχή και διακίνηση παιδικού πορνογραφικού υλικού.
Το DarkScandals φιλοξένησε και διανέμει βίντεο και εικόνες με μη συναινετική και βίαιη σεξουαλική κακοποίηση. Το DarkScandals άρχισε να λειτουργεί περίπου το 2012 και περιείχε πάνω από 2.000 βίντεο και εικόνες και διαφήμιζε ότι προσέφερε «πραγματικό εκβιασμό, βιασμούς και βίαια βίντεο κοριτσιών σε όλο τον κόσμο».
Το DarkScandals προσέφερε στους χρήστες δύο τρόπους πρόσβασης σε αυτό το παράνομο και άσεμνο περιεχόμενο, το οποίο παραδόθηκε σε "πακέτα" μέσω email για λήψη από τους πελάτες. Οι χρήστες θα μπορούσαν είτε να πληρώσουν για τα πακέτα βίντεο χρησιμοποιώντας κρυπτογράφηση, είτε να ανεβάσουν νέα βίντεο για να προσθέσουν στο περιεχόμενο των ιστοτόπων DarkScandals.
Οι ειδικοί κανόνες για τις μεταφορτώσεις βίντεο στους ιστοτόπους περιλάμβαναν περιεχόμενο "πραγματικού βιασμού / καταναγκασμού" και ανέφεραν την προτίμηση για το "δικό τους υλικό/κατασκευασμένο απ' τους ίδιους". Ο ιστότοπος απαγόρευσε συγκεκριμένα τις «ψεύτικες, ερασιτεχνικές… ή ταινίες που έπαιξαν και αλλού», απορρίπτοντας το περιεχόμενο εάν δεν απεικονίζει πραγματική σεξουαλική βία. Ο συλληφθείς διαχειριστής φέρεται να έλαβε σχεδόν 2 εκατομμύρια δολάρια από την πώληση αυτού του άσεμνου και παράνομου περιεχομένου.



4.4 Sextorsion

Έρευνα που διεξήχθη από το IWF(Internet Watch Foundation) του Ηνωμένου Βασιλείου έδειξε ότι το 80% των προσωπικών εικόνων και βίντεο σεξουαλικού περιεχομένου που οι νέοι μοιράστηκαν με άλλους, αντιγράφηκαν ή κλάπηκαν και στην συνέχεια διανεμήθηκαν σε σελίδες κοινωνικής δικτύωσης ή και σελίδες πορνογραφικού περιεχομένου.
Σε μερικές περιπτώσεις έχουμε και αυτό που αποκαλείται sextorsion όπου τα θύματα απειλούνται και πιέζονται στο να πληρώσουν συγκεκριμένα ποσά ή να παρέχουν σεξουαλικές υπηρεσίες ώστε να μην διανεμηθούν οι φωτογραφίες τους στο διαδίκτυο.
Τα ποσά που ζητούνται από τα θύματα για να διαγραφεί το υλικό ανέρχονται από 500-2000 και σε περίπτωση που το θύμα (και κατ' επέκταση η οικογένειά του εφόσον μιλάμε για παιδιά) αρνηθεί να τα καταβάλει τότε το υλικό θα δημοσιοποιηθεί στην οικογένεια και τους φίλους του θύματος αλλά και σε σελίδες κοινωνικής δικτύωσης όπως το Facebook.

Χαρακτηριστικό είναι το παράδειγμα του Viborg Folder που πήρε το όνομά του από την μικρή Δανέζικη πόλη απ' την οποία ήταν τα περισσότερα θύματα. Δεν είναι σίγουρο ποιος βρίσκεται πίσω απ' την δημιουργία αυτού του φακέλου αλλά η ύπαρξή του έγινε γνωστή

στις αρχές το 2011. Σε αυτόν τον φάκελο βρίσκονταν φωτογραφίες 13χρονων κοριτσιών από την περιοχή τα περισσότερα απ' τα οποία ήταν εύκολα αναγνωρίσιμα καθώς υπήρχε και το όνομα σε κάθε μια φωτογραφία από αυτές. Ο φάκελος περιείχε 800 με 900 εικόνες και μοιράστηκε μέσω USB memory sticks αρχικά για περίπου 6,70 ευρώ και μετά ανέβηκε και στο διαδίκτυο.
Ο συγκεκριμένος φάκελος έχει διαγραφεί πολλές φορές από τους ειδικούς όμως επανεμφανίζεται

Σε αυτού του είδους την τρομοκρατία εντάσσεται και το πορνό εκδίκησης (revenge porn) όπως ονομάζεται καθώς σε αυτό τα πρώην αγόρια ή κορίτσια του εκάστοτε θύματος μοιράζονται εικόνες σεξουαλικού περιεχομένου του θύματος ως εκδίκηση επειδή χώρισαν.

4.5 Cyber Grooming

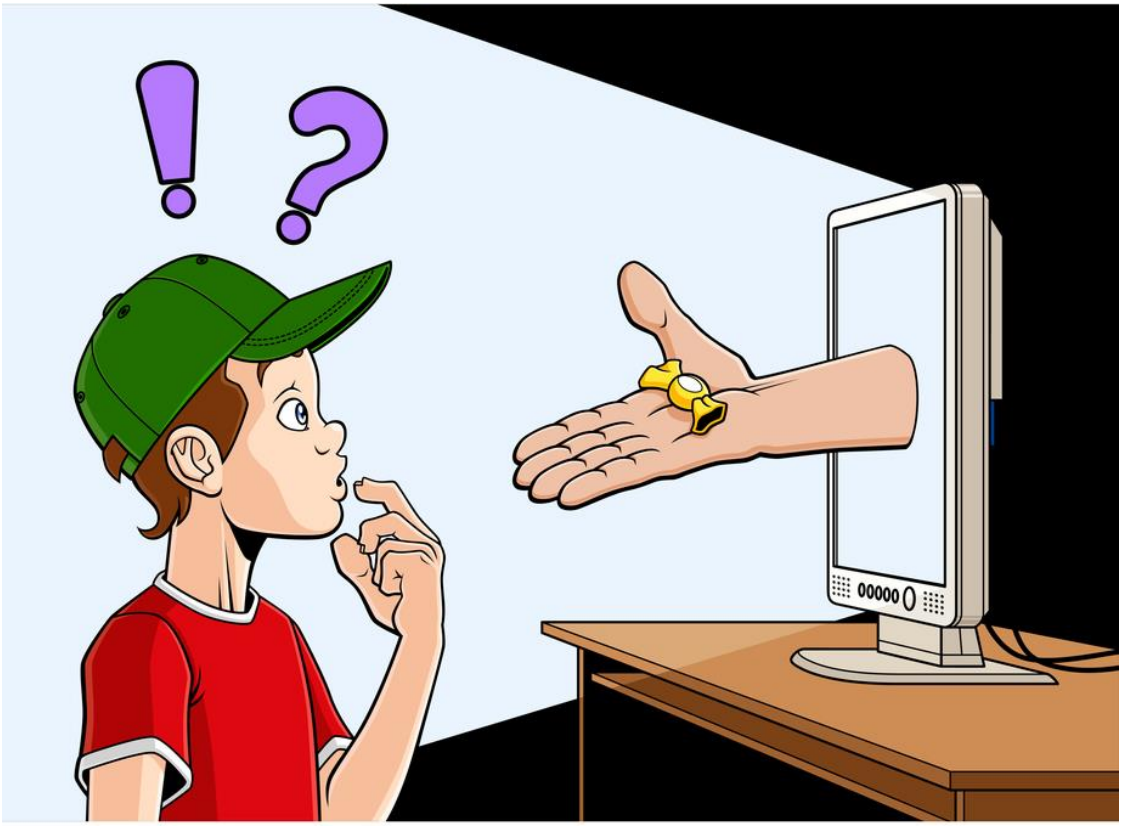
Οι ενήλικες που αναζητούν παιδιά στο διαδίκτυο έχουν διαφορετικές τακτικές.
Υπάρχουν αυτοί που μιλάνε ευθέως και λένε αυτό που αναζητούν. Πολλές φορές βιώνουν την κατακραυγή του κοινού όμως κάποιες φορές βρίσκονται παιδιά που ανταποκρίνονται συνήθως παιδιά που αναζητούν προσοχή ή χρειάζονται χρήματα.
Άλλοι ενήλικες ακολουθούν μια πιο στρατηγική τακτική χρησιμοποιώντας την τακτική του grooming που θα αναλύσουμε παρακάτω δημιουργώντας ένα δεσμό με το παιδί

Τους ενήλικες που αναζητούν την παρέα παιδιών μπορούμε να τους εντάξουμε στις παρακάτω 3 κατηγορίες ανάλογα με τα κίνητρά τους:

- **Αυτοί που αναζητούν φιλία(friendship seekers)**
  Είναι συνήθως οι ενήλικες που αισθάνονται ανεπαρκείς όταν συναναστρέφονται με ενήλικες και νιώθουν ότι επικοινωνούν καλύτερα με τα παιδιά 'η μπορεί να έχουν περιορισμένες πνευματικές ικανότητες. Δεν υπάρχει απαραίτητα κακό πίσω από αυτή την αναζήτηση εφόσον δεν υπάρχει σεξουαλικό ενδιαφέρον ωστόσο είναι εξαιρετικά δύσκολο να καταλάβουμε αν το ενδιαφέρον του ενήλικα είναι φιλικό ή κρύβει σεξουαλική συμπεριφορά.

- **Οι Αυνανιστές(Masturbators)**
  Είναι συνήθως ενήλικες που αναζητούν τετοιου είδους φιλία ώστε να αποκτήσουν διαδικτυακές εμπειρίες σεξουαλικής φύσης χωρίς να σκοπεύουν ούτε να οργανώνουν καμίας μορφής σεξουαλική συνάντηση. Στο λεγόμενο Cybersex συναντάται η ανταλλαγή γραπτών μνημάτων με το παιδί σχετικά με σεξουαλικές φαντασιώσεις ή επιθυμίες. Η επικοινωνία αυτή μπορεί να πάει ένα βήμα παραπέρα όταν οι ενήλικες στέλνουν γυμνές φωτογραφίες του εαυτού τους και ενθαρρύνουν το παιδί να κάνει το ίδιο. Μερικοί μάλιστα πείθουν το παιδί να ανοίξει την web camera και να ανταλλάξουν φωτογραφίες και βίντεο.

- **Φυσικοί Παραβάτες(Physical offenders)**
  Στην κατηγορία αυτή συναντάμε άτομα που συμπεριφέρονται παρόμοια με τις 2 πρώτες κατηγορίες που αναφέραμε με βασική διαφορά πως απώτερος τους στόχος είναι να συναντηθούν με το παιδί και να διαπράξουν σεξουαλική κακοποίηση.



Ο καλλωπισμός(grooming) αναφέρεται στο άτομο που προσπαθεί να χτίσει σχέσεις εμπιστοσύνης με το παιδί ή την οικογένεια του παιδιού για την μετέπειτα σεξουαλική του κακοποίηση. Η διαδικασία μπορεί να πάρει μέρες μήνες ή και χρόνια μέχρι να εδραιωθεί η σχέση του ατόμου με το παιδί. Το συγκεκριμένο άτομο μπορεί να είναι οποιοσδήποτε: μπορεί να είναι συγγενής, στενός οικογενειακός φίλος, γείτονας, δάσκαλος.
Συνήθως στο διαδικτυακό Grooming το άτομο αυτό παριστάνει ότι είναι παιδί ίδιας περίπου ηλικίας με το θύμα ή κάποιο διάσημο πρόσωπο.

Υπάρχουν κάποια βασικά στάδια της διαδικασίας του Grooming:

1. **Στοχοποίηση του παιδιού:** Ο ενήλικας στοχεύει και εκμεταλλεύεται τις αντιληπτές αδυναμίες ενός παιδιού(απομόνωση, παραμέληση, έλλειψη γονικής επίβλεψης, συναισθηματικό κενό χαοτική οικογενειακή ζωή κ.α.)

2. **Κερδίζοντας την εμπιστοσύνη του παιδιού και των οικείων του:** Ο ενήλικας προσπαθεί να κερδίσει την εμπιστοσύνη των γονέων ή των φροντιστών του παιδιού ώστε να μειώσουν τις υποψίες και να αποκτήσουν στο παιδί με μία φαινομενικά ζεστή αλλά υπολογιζόμενη υποστήριξη. Ο ενήλικας κερδίζει την εμπιστοσύνη του παιδιού συγκεντρώνοντας πληροφορίες για αυτό, γνωρίζοντας τις ανάγκες του και βρίσκοντας τρόπους για να καλύψει αυτές τις ανάγκες.

3. **Κάλυψη των αναγκών:** Μόλις ο ενήλικας αρχίσει να καλύπτει τις ανάγκες του παιδιού μπορεί να αναλάβει αισθητά μεγαλύτερο ρόλο στην ζωή του. Κύριες τακτικές για να το επιτύχει αυτό είναι η αγορά δώρων, η δωρεά χρημάτων η κολακεία και η κάλυψη άλλων βασικών αναγκών.

4. **Απομονώνοντας το παιδί:** Ο ενήλικας χρησιμοποιεί τακτικές απομόνωσης για να ενισχύσει την σχέση του με το παιδί δημιουργώντας συνθήκες στις οποίες είναι μόνος του μαζί του(φύλαξη του παιδιού, διδασκαλία του προσωπική καθοδήγηση). Ο δράστης μπορεί να δημιουργήσει την αίσθηση στο παιδί ότι το αγαπά και το κατανοεί με τρόπο που οι γονείς του δεν μπορούν και δημιουργεί στο παιδί την αίσθηση ότι κανένας δεν ενδιαφέρεται για εκείνο παρα μόνο ο ίδιος.

5. **Η σχέση γίνεται σεξουαλική:** Μόλις χτιστεί η συναισθηματική εξάρτηση και εμπιστοσύνη ο ενήλικος δράστης αρχίζει σταδιακά να κάνει την σχέση σεξουαλική. Αυτό μπορεί αν συμβεί μέσω ομιλίας, φωτογραφιών, βίντεο αλλά και καταστάσεων στις οποίες μπορεί να αποπλανήσει το παιδί πχ κολύμπι.

6. **Διατηρώντας τον έλεγχο:** Μόλις διαπραχθεί η σεξουαλική κακοποίηση ο ενήλικας χρησιμοποιεί συνήθως μυστικότητα, ευθύνη και απειλές για να διατηρήσει την συμμετοχή του παιδιού αλλά και να εξασφαλίσει την σιωπή του. Προκειμένου να διατηρηθεί ο έλεγχος ο δράστης χρησιμοποιεί συναισθηματικό χειρισμό. Προσπαθεί να κάνει το παιδί να πιστέψει πως είναι το μόνο άτομο που μπορεί να καλύψει τις συναισθηματικές και υλικές του ανάγκες, Το παιδί μπορεί να αισθανθεί ότι η απώλεια της σχέσης ή οι συνέπειες της έκθεσης μπορούν να είναι πιο επιζήμιες απ’ ότι μια τοξική και ανθυγιεινή σχέση.

Κεφάλαιο 5: Μέσα Κοινωνικής Δικτύωσης και Διαδικτυακά παιχνίδια

5.1 Social Media

- Τα Social Media διαδραματίζουν μεγάλο ρόλο στην κουλτούρα των νέων την σύγχρονη εποχή. Η συντριπτική πλειοψηφία των παιδιών (83%) διαθέτει προφίλ σε κοινωνικό δίκτυο, εκ των οποίων το 70% προκύπτει ότι ξεκινά την ενασχόληση πριν από την επιτρεπόμενη ηλικία των 13 ετών. Το 36% μάλιστα των παιδιών που διαθέτουν προφίλ σε κοινωνικά δίκτυα το άνοιξαν μόνα τους, χωρίς τη συγκατάθεση των γονιών τους.

- Το 18% των παιδιών που χρησιμοποιεί κοινωνικά δίκτυα δεν έχει το προφίλ του ιδιωτικό κι ένα 16% δε γνωρίζει πως να αναφέρει κάποιον ή κάτι που το ενόχλησε στο διαδίκτυο.
- Το κοινωνικό δίκτυο που χρησιμοποιούν περισσότερο τα παιδιά είναι το INSTAGRAM με ποσοστό 51%, ενώ το Facebook χρησιμοποιείται μόλις από το 11% των παιδιών. Ακολουθεί το YouTube με 40%, το Messenger με 19%, το Viber με 17%, το Skype και το Snapchat με 11%.

Η χρήση των μέσων κοινωνικής δικτύωσης μπορεί να έχει και πολλούς κινδύνους. Κάποιοι από αυτούς είναι:

- η έκθεση του παιδιού σε ακατάλληλο ή ενοχλητικό περιεχόμενο (βίαια ή σεξουαλικά σχόλια/εικόνες),
- η μεταφόρτωση ακατάλληλου περιεχομένου (ενοχλητικές ή προκλητικές φωτογραφίες και βίντεο).
- η κοινοποίηση των προσωπικών τους πληροφοριών (π.χ. τοποθεσία, αριθμός τηλεφώνου) και η επικοινωνία με αγνώστους.
- Ο εκφοβισμός στον κυβερνοχώρο
- Η υπερβολικά στοχευμένη διαφήμιση
- οι παραβιάσεις των δεδομένων τους.

Αξίζει να αναφερθεί ότι οι εταιρείες προσπαθώντας να συμμορφωθούν με τα νόμιμα ηλικιακά όρια αλλά και να διατηρήσουν το αγοραστικό τους κοινό, δημιουργούν εφαρμογές που απευθύνονται αποκλειστικά στα παιδιά (π.χ. messenger kids). Κάποιες από αυτές έχουν κατηγορηθεί ότι παραβιάζουν τα προσωπικά δεδομένα και επεξεργάζονται την παρατηρούμενη συμπεριφορά των παιδιών με στόχο τη μεταπώληση σε διαφημιστικές κ.ά. εταιρείες.

Πιο συγκεκριμένα το Tik Tok η εφαρμογή με την ραγδαία αύξηση αλλά και επιρροή μεταξύ των παιδιών προκαλεί αντιδράσεις από φορείς που θεωρούν πως παραβιάζει τα προσωπικά δεδομένα αλλά και ότι καταγράφει την συμπεριφορά των παιδιών προκειμένου στην συνέχεια να τη μεταπωλήσει σε διαφημιστικές και άλλες επιχειρήσεις προϊόντων ή υπηρεσιών. Καθώς υπήρξαν πολλές καταγγελίες και παραβιάσεις η Ολλανδική Αρχή Προστασίας Προσωπικών Δεδομένων εξήγγειλε έρευνα προκειμένου να διαπίστωση αν η εφαρμογή προστατεύει τα προσωπικά δεδομένα των παιδιών και πως τα συλλέγει, επεξεργάζεται και αξιοποιεί.

Με βάση τη συμφωνία με την FTC(Federal Trade Commission-Ομοσπονδιακή Επιτροπή Εμπορίου), η TikTok είχε αρχίσει να **σβήνει** χρήστες κάτω των 13 ετών, το κατώτερο επιτρεπόμενο όριο εγκατάστασης της εφαρμογής. Τώρα οι είκοσι φορείς που προχώρησαν σε νέα καταγγελία υποστηρίζουν πως η Κινέζικη ByteDance που λειτουργεί την γνωστή εφαρμογή παραβιάζει τους συγκεκριμένους όρους και εξακολουθεί να επιτρέπει σε παιδιά κάτω των 13 ετών να χρησιμοποιούν το TikTok, αλλά και να συλλέγει δεδομένα από τη χρήση της εφαρμογής προκειμένου να τα μεταπωλήσει.
Ένα χρόνο μετά τη συμφωνία διευθέτησης, με παιδιά και οικογένειες να εγγράφονται στην εφαρμογή με αριθμούς-ρεκόρ, η TikTok δεν προχώρησε στη διαγραφή προσωπικών στοιχείων που είχε στο παρελθόν συλλέξει από παιδιά ενώ συνεχίζει να συλλέγει προσωπικά στοιχεία των παιδιών, χωρίς να ενημερώνει ή να ζητάει την άδεια των γονιών τους.

Η δράση της TikTok θεωρείται από αρκετούς ως μια **περισσότερο επιθετική μορφή**, αφού αφορά ανηλίκους, καθώς αξιοποιεί στοιχεία για τη συμπεριφορά ανθρώπων στο Internet, αλλά και στον πραγματικό κόσμο (π.χ. καταγράφοντας τις διαδρομές που κάνουν κάθε ημέρα, τις ώρες που περιηγούνται στο Διαδίκτυο, τις ηλεκτρονικές αγορές, κ.α.) για να αποκομίσει δισεκατομμύρια ευρώ.

Παρόμοια περίπτωση αποτελεί και η Google αφού πλήρωσε **170 εκατομμύρια δολάρια** σε μια συμφωνία διευθέτησης με την FTC, ώστε να αντιμετωπίσει καταγγελίες πως παραβίασε τη νομοθεσία Coppa και μάζευε προσωπικά δεδομένα από παιδιά που χρησιμοποιούν το YouTube.[6]

[6] Tik Tok: Σοβαρές καταγγελίες για την εφαρμογή που κάνει θραύση στα παιδιά μας του Φώτη Κόλλια

5.2 Gaming

Τα παιχνίδια στην ζωή του παιδιού είναι αναπόσπαστο κομμάτι της καθημερινότητάς τους. Η άνθιση της τεχνολογίας κατάφερε να μεταφέρει το παιχνίδι του παιδιού από τα πάρκα και τους δρόμους στα κινητά και τα τάμπλετ δεδομένου ότι το μεγαλύτερο ποσοστό των νέων από μικρή ηλικία διαθέτουν κάποιο smartphone.
Σύμφωνα με έρευνα[7] παιδιά ηλικίας 2-4 παίζουν διαδικτυακά παιχνίδια 21 λεπτά ανά ημέρα ενώ παιδιά ηλικίας από 5-8 παίζουν 42 λεπτά ανά ημέρα.
Στις ηλικίες 8-12 το παιχνίδι φαίνεται να διαρκεί 2 ώρες ανά ημέρα ενώ στις ηλικίες από 13-17 περίπου 2.5 ώρες την ημέρα.
Τα αγόρια φαίνεται να παίζουν περισσότερα διαδικτυακά παιχνίδια απ' ότι τα κορίτσια αλλά πάνω από το 80% και των δύο φύλων φαίνεται να έχει μια κονσόλα παιχνιδιού (PlayStation, Xbox, Υπολογιστή)

Οι κίνδυνοι που μπορεί ένα παιδί να αντιμετωπίσει παίζοντας διαδικτυακά παιχνίδια μπορούν να χωριστούν σε 7 κατηγορίες:

1. **Cyber Bullying**: Για πολλά παιδιά το να μπορούν να παίζουν διαδικτυακά παιχνίδια είναι μια έξοδος και μια αποστασιοποίηση από την πραγματικότητά τους καθώς σε αυτά βρίσκουν την ανωνυμία τους τοποθετώντας απλά ένα ψευδώνυμο. Όπως έχει παρατηρηθεί πολλοί παίχτες εκμεταλλεύονται την ανωνυμία τους για να ενοχλήσουν άλλους παίχτες και να κάνουν το παιχνίδι δυσάρεστο γι' αυτούς. Αυτό μπορεί να ξεκινήσει απλά προσπαθώντας να κάνουν παίχτες μικρότερου επιπέδου από τους ίδιους να χάσουν αλλά πολλές φορές καταλήγει και σε φραστική επίθεση προς το θύμα με σκληρά μηνύματα είτε γελοιοποιώντας το και εξευτελίζοντας το στα τσατ των παιχνιδιών που παρακολουθούν παίχτες απ' όλο τον κόσμο.

2. **Προβλήματα Ιδιωτικότητας**: Στα περισσότερα παιχνίδια για να μπορέσεις να συμμετέχεις είναι απαραίτητο να φτιάξεις ένα username το εικονικό σου όνομα στο παιχνίδι. Ένα συχνό λάθος που γίνεται είναι ότι πολλές φορές τα συγκεκριμένα username είναι παράγωγα των πραγματικών ονομάτων των παιδιών ή αποκαλύπτουν κάποιο άλλο αναγνωρίσιμο στοιχείο πχ ηλικία. Αυτό το καθιστά επικίνδυνο καθώς η κοινωνική φύση των παιχνιδιών επιτρέπει στους χάκερς μέσα από γενικά κανάλια συνομιλιών ή και προσωπικά μηνύματα στα παιχνίδια, να χειραγωγούν συνομιλίες και να ζητούν λεπτομερείς προσωπικές πληροφορίες. Συγκεντρώνοντας δεδομένα από παιχνίδια και άλλες πηγές μπορούν αν έχουν πρόσβαση σε άλλους λογαριασμούς πχ μέσα κοινωνικής δικτύωσης ή και να δημιουργήσουν λογαριασμούς ακόμα και ολόκληρες ψηφιακές ταυτότητες στο όνομα του παιδιού.

[7] Video Games from Center on Media and Child health

3. **Προσωπικές πληροφορίες σε κονσόλες και υπολογιστές**: πολλές φορές όταν δεν χρειαζόμαστε άλλο μια κονσόλα παιχνιδιού ή έναν υπολογιστή τους πηγαίνουμε για ανακύκλωση ή τους πουλάμε σε διαδικτυακές αγορές. Τις περισσότερες φορές τα παιδιά άλλα και οι γονείς ξεχνάνε πόσες προσωπικές πληροφορίες υπάρχουν μέσα και τις δίνουν χωρίς να έχουν διαγράψει τα προσωπικά τους αρχεία και χωρίς να έχουν κάνει επαναφορά εργοστασιακών ρυθμίσεων που είναι βασικό με αποτέλεσμα να μπορεί να βρει κάποιος πολύ εύκολα αποθηκευμένα αρχεία και κωδικούς.

4. **Κάμερες**: Οι κάμερες έχουν αποτελέσει στόχο παραβίασης από την αρχή της ανακάλυψής τους ως ξεχωριστά περιφερειακά. Σήμερα τα περισσότερα Smartphones, τα Tablet και Laptop διαθέτουν ενσωματωμένη ψηφιακή κάμερα. Είτε εσωτερικά είτε εξωτερικά οποιαδήποτε συνδεδεμένη συσκευή εγγραφής εικόνας ή ήχου μπορεί να ελεγχθεί από απόσταση και να χρησιμοποιηθεί για την εκμετάλλευση του παιδιού με πολλούς τρόπους.

5. **Διαδικτυακοί «Θηρευτές»**: Σε αυτή την κατηγορία ανήκουν συνήθως παλιοί και έμπειροι παίχτες που χρησιμοποιούν τα παιχνίδια για να δελεάσουν νεότερα θύματα. Αυτό μπορεί να γίνει με ακατάλληλα μηνύματα, συνομιλίες με κάμερα ακόμα και με προσωπικές συναντήσεις που θα μπορούσαν να οδηγήσουν σε σεξουαλική εκμετάλλευση. Τέτοιου είδους διαδικτυακά παιχνίδια (τυχερά παιχνίδια, παιχνίδια επιβίωσης και στρατηγικής) δίνουν την ευκαιρία στους «θηρευτές» να δημιουργήσουν ένα είδος κοινής πορείας και εμπειρίας με το θύμα με την πρόφαση ότι νίκησαν ένα σκληρό αντίπαλο ή εξερεύνησαν νέα επίπεδα στο παιχνίδι. Σε πολλές περιπτώσεις επιδιώκουν να απομονώσουν τα παιδία από τους γονείς και τους φίλους τους με την πρόφαση ότι κανείς δεν τους καταλαβαίνει και μόνο οι ίδιοι έχουν κοινούς στόχους με το θύμα.

6. **Κρυφές Πληρωμές**: Πολλά διαδικτυακά παιχνίδια χρειάζονται πληρωμή για να μπορέσει να παίξει κανείς. Ορισμένα χρησιμοποιούν το μοντέλο «freemium» που σημαίνει ότι δίνουν κάποιο περιεχόμενο δωρεάν όμως για πλήρη πρόσβαση στα χαρακτηριστικά του παιχνιδιού απαιτείται πληρωμή. Πριν από μερικά χρόνια το επιχειρηματικό μοντέλο «freemium» προσφέρθηκε να καταργήσει τις διαφημίσεις εντός εφαρμογής που υπήρχαν μια μια μικρή εφάπαξ χρέωση. Στις περισσότερες περιπτώσεις αυτά τα παιχνίδια απαιτούν από τους χρήστες να επισυνάψουν μια πιστωτική κάρτα στο προφίλ τους και η κάρτα τους να χρεώνεται αυτόματα κάθε φορά που αγοράζουν αντικείμενα ή υπηρεσίες. Πολλές φορές τα στοιχεία των πιστωτικών καρτών χρεώνονται χωρίς να υπάρχει έγκριση από τον χρήστη.

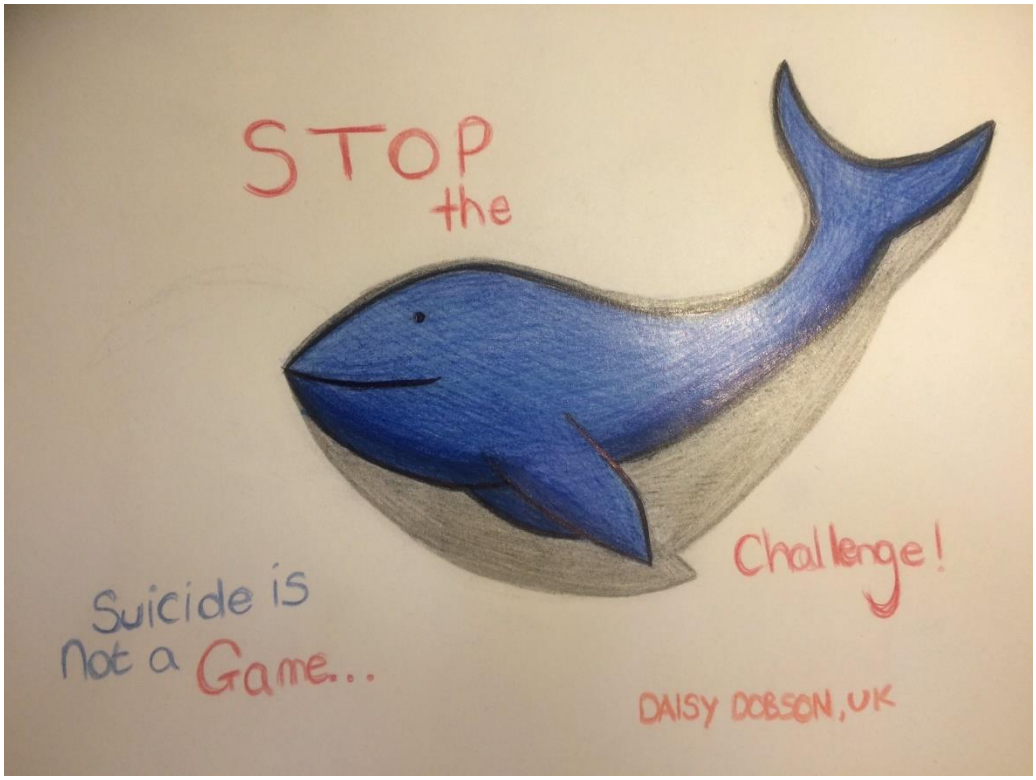
7. **Malware**: Τα κακόβουλα λογισμικά όπως τα Trojans ή τα adware μπορούν να τροποποιήσουν μια νόμιμη εφαρμογή και να ανεβάσουν την κακόβουλή έκδοσή

της στο Google Play ή σε άλλη νόμιμη αγορά. Αυτά τα λογισμικά μετατρέπουν τα μολυσμένα μηχανήματα σε ένα είδος «ζόμπι» σε μεγαλύτερα botnets μολύνοντας ακόμα και τις πιο αξιόπιστες εφαρμογές. Συχνά αυτά τα λογισμικά λειτουργούν με χρονοδιακόπτη επομένως τα θύματα δεν συνδέουν το διαδικτυακό τους παιχνίδι με την επίθεση. Είναι βασικό να ελέγχουμε τις εφαρμογές που κατεβάζουμε ελέγχοντας τις πρόσφατες κριτικές, τον δημιουργό, την αγορά αλλά κάνοντας και έναν έλεγχο με λογισμικά ασφαλείας κατά την λήψη τους.

5.3: Επικίνδυνα παιχνίδια και εφαρμογές

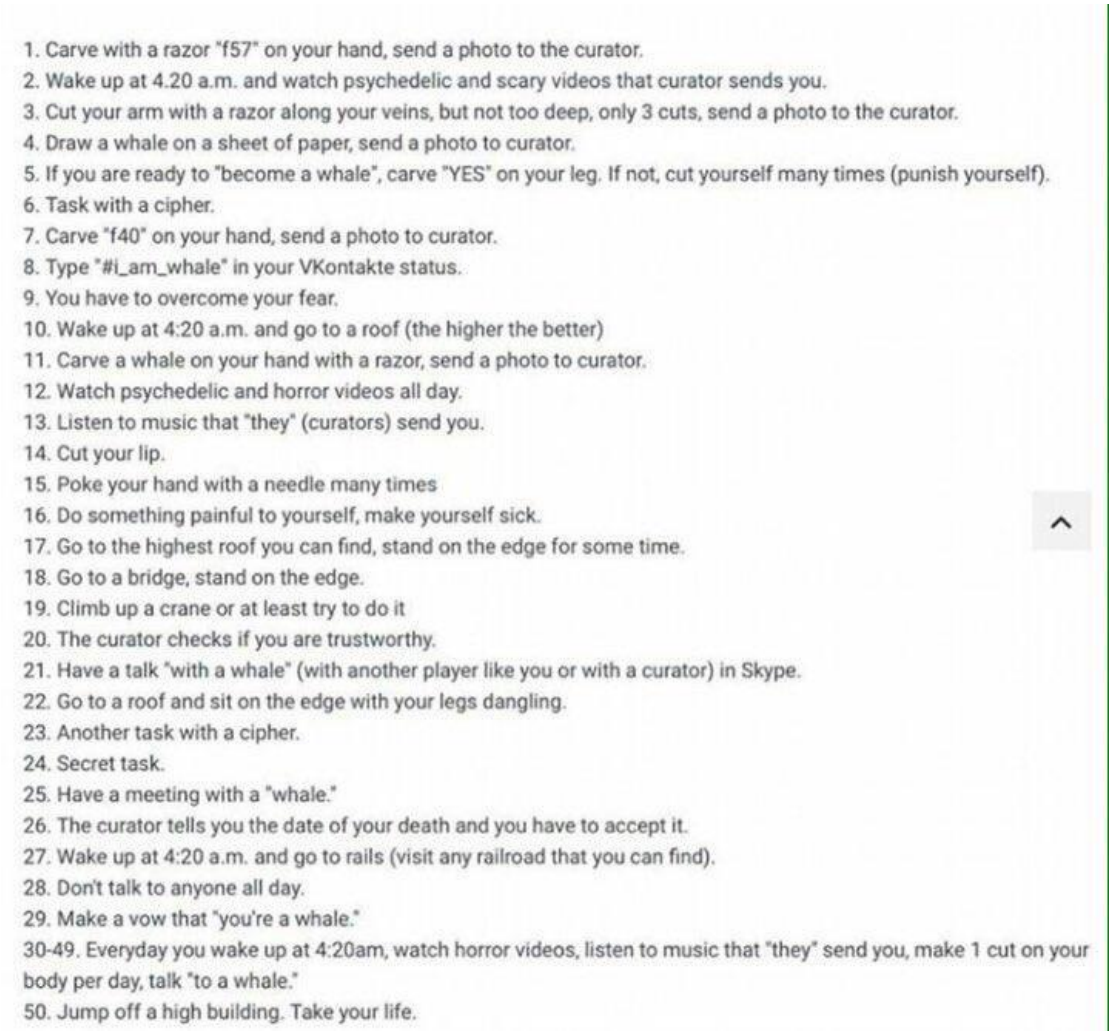
Τα επικίνδυνα διαδικτυακά παιχνίδια έχουν εισβάλλει στην καθημερινή πραγματικότητα της διαδικτυακής ζωής των ανηλίκων απειλώντας ακόμα και την ζωή τους. Τα παιχνίδια ή αλλιώς προκλήσεις(challenges) που δημιουργούνται στο διαδίκτυο και υιοθετούνται από τους νέους δεν είναι τόσο αθώα όσο φαίνονται.

Blue Wale



Ένα από τα πιο γνωστά παιχνίδια που εμφανίστηκε το 2016 είναι το Blue Whale Challenge. Είναι ένα πολύ δημοφιλές παιχνίδι στις τάξεις των εφήβων και η διάρκεια του υπολογίζεται στις 50 ημέρες. Κατά την διάρκεια του παιχνιδιού οι χρήστες λαμβάνουν οδηγίες από

άγνωστο άτομο που έχει οριστεί επικεφαλής, με σκοπό να ολοκληρώσουν με επιτυχία μια σειρά πολύ επικίνδυνων για την υγεία τους και την σωματική τους ακεραιότητα δοκιμασιών(αυτοτραυματισμοί, παρακολούθηση ταινιών τρόμου, αναρρίχηση σε ψηλά κτήρια)



1. Carve with a razor "f57" on your hand, send a photo to the curator.
2. Wake up at 4.20 a.m. and watch psychedelic and scary videos that curator sends you.
3. Cut your arm with a razor along your veins, but not too deep, only 3 cuts, send a photo to the curator.
4. Draw a whale on a sheet of paper, send a photo to curator.
5. If you are ready to "become a whale", carve "YES" on your leg. If not, cut yourself many times (punish yourself).
6. Task with a cipher.
7. Carve "f40" on your hand, send a photo to curator.
8. Type "#i_am_whale" in your VKontakte status.
9. You have to overcome your fear.
10. Wake up at 4:20 a.m. and go to a roof (the higher the better)
11. Carve a whale on your hand with a razor, send a photo to curator.
12. Watch psychedelic and horror videos all day.
13. Listen to music that "they" (curators) send you.
14. Cut your lip.
15. Poke your hand with a needle many times
16. Do something painful to yourself, make yourself sick.
17. Go to the highest roof you can find, stand on the edge for some time.
18. Go to a bridge, stand on the edge.
19. Climb up a crane or at least try to do it
20. The curator checks if you are trustworthy.
21. Have a talk "with a whale" (with another player like you or with a curator) in Skype.
22. Go to a roof and sit on the edge with your legs dangling.
23. Another task with a cipher.
24. Secret task.
25. Have a meeting with a "whale."
26. The curator tells you the date of your death and you have to accept it.
27. Wake up at 4:20 a.m. and go to rails (visit any railroad that you can find).
28. Don't talk to anyone all day.
29. Make a vow that "you're a whale."

30-49. Everyday you wake up at 4:20am, watch horror videos, listen to music that "they" send you, make 1 cut on your body per day, talk "to a whale."

50. Jump off a high building. Take your life.

Η ονομασία του φαινομένου έχει δοθεί στην «μπλε φάλαινα», καθώς το συγκεκριμένο θηλαστικό, πολλές φορές χάνει το προσανατολισμό του από το υπόλοιπο κοπάδι και εξοκείλει στη στεριά, καταλήγοντας σε θάνατο, λόγω έλλειψης οξυγόνου και βλάβης των ζωτικών του οργάνων. Με αυτό το συσχετισμό θέλουν να παρακινήσουν παιδιά νεαρής ηλικίας να απομακρυνθούν από το «κοπάδι της κοινωνίας» και να «ξεχωρίσουν».

<u>Blackout Challenge</u>

Σε αυτή τη δοκιμασία του Tik Tok το παιδί ενθαρρύνεται στο να προκαλέσει ασφυξία στον εαυτό του έως ότου λιποθυμήσει. Είναι παρόμοιο με το Pass Out Challenge που υπήρχε πριν από αυτό στο Tik Tok όπου τα παιδιά γύρναγαν πολύ γρήγορα το κεφάλι τους από την μία μεριά στην άλλη μέχρι να λιποθυμήσουν. Υποτίθεται ότι μετά από λίγο το παιδί ξυπνάει

και βλέπει τι έχει καταγράψει με την κάμερά του. Αυτό μπορεί να προκαλέσει λιποθυμικά επεισόδια, επιληπτικές κρίσεις, πρόβλημα στον εγκέφαλο λόγο του χαμηλού οξυγόνου(που οι γιατροί το παρομοιάζουν με πνιγμό ή ανακοπή καρδιάς)ακόμα και θάνατο.

Roblox

Το διαδικτυακό παιχνίδι Roblox αποκαλείται «το πιο διάσημο παιχνίδι που δεν έχεις ακούσει ποτέ». Το παιχνίδι αυτό είναι μια διαδικτυακή πλατφόρμα 3D όπου τα παιδιά δημιουργούν avatars(παίχτες) για τα οποία αγοράζουν σπίτι έπιπλα διακοσμητικά τα οποία απαιτούν πραγματικά χρήματα. Εκτός όμως από τις επιπλέων χρεώσεις που μπορεί να έχει το παιχνίδι το μεγαλύτερο πρόβλημα είναι οι σχέσεις μεταξύ των παιχτών. Ο ρόλος του παιχνιδιού είναι ο παίχτης να αλληλεπιδράσει με άλλους παίχτες να τους μιλήσει και να κάνει φίλους. Η επικοινωνία αυτή γίνεται μέσω chat και παρόλο που μπορεί να υπάρχει το φιλτράρισμα των λέξεων μπλοκάροντας ακατάλληλες λέξεις και φράσεις, τα παιδιά μπορούν πολύ εύκολα να στοχοποιηθούν από παιδεραστές ή Cyber Bullies.
Το παιχνίδι καλεί τον παίχτη να ανακαλύψει φανταστικούς κόσμους όλων των ειδών ακόμα και σεξουαλικής φύσεως με ακατάλληλες εικόνες για παιδιά.
Το συγκεκριμένο παιχνίδι όπως και άλλα παρόμοια προσπαθούν να επαγρυπνήσουν παιδιά κάτω των 12 τα οποία αποτελούν εύκολους στόχους καθώς δεν μπορούν να διακρίνουν τα ακατάλληλα αιτήματα.

Kik Messenger

Το Kik είναι μια εφαρμογή για ανώνυμο chat όπου οι χρήστες εγγράφονται με το όνομα τους και το εμαιλ τους. Το επικίνδυνο με αυτή την εφαρμογή είναι ότι δεν υπάρχουν δικλείδες ασφαλείας. Οποιοσδήποτε με ένα όνομα και εμαιλ μπορεί να εγγραφεί (ακόμα και ψεύτικα) δεν ζητάει επιβεβαίωση ή σύνδεση με κάποιο τηλέφωνο και μπορείς να αναγνωριστείς μόνο από το username στην εφαρμογή. Το Kik είναι επιτρεπτό σε ηλικίες από 17 και πάνω εφόσον όμως δεν υπάρχει έλεγχος της ηλικίας του χρήστη όλοι το χρησιμοποιούν ακόμα και παιδιά. Η συγκεκριμένη εφαρμογή, που επιτρέπει την επικοινωνία με ξένους που απλά γνωστοποιούν το username τους στην εφαρμογή, έχει ήδη συνδυαστεί με δολοφονία ανηλίκου αλλά και με περιστατικά παιδικής πορνογραφίας.

Tinder/Yubo

Το Tinder είναι μια διαδικτυακή εφαρμογή γνωριμιών όπου ο χρήστης πρέπει να είναι πάνω από 13 χρονών για να μπορέσει να εγγραφεί. Αν και οι διαχειριστές της εφαρμογής υποστηρίζουν ότι είναι ένας διασκεδαστικός τρόπος να γνωρίσεις ανθρώπους το Tinder είναι γνωστό σαν εφαρμογή γνωριμιών για σεξουαλικούς σκοπούς. Η εφαρμογή βοηθάει τους χρήστες να βρουν παρτενέρ μέσα στην γεωγραφική περιοχή τους πράγμα επικίνδυνο καθώς ο οποιοσδήποτε μπορεί να ξέρει την τοποθεσία του παιδιού με ότι κινδύνους αυτό συνεπάγεται.

Το Yubo είναι μια παρόμοια εφαρμογή γνωριμιών με δυνατότητα να μιλάς σε αγνώστους ακόμα και να δείχνεις βίντεο με τον εαυτό σου σε πραγματικό χρόνο(live-streaming) ενώ οι υπόλοιποι χρήστες μπορούν να στέλνουν μηνύματα που εμφανίζονται σαν pop-ups. Υπάρχουν πολλοί κίνδυνοι καθώς οποιοσδήποτε μπορεί να καταγράψει και να αναπαράγει την εικόνα του παιδιού αλλά και να επικοινωνήσουν μαζί του για σεξουαλικούς σκοπούς.

Snapchat

Το Snapchat είναι μια εφαρμογή που αποστέλλει βίντεο και εικόνες οι οποίες εξαφανίζονται μετά το διάστημα μερικών δευτερολέπτων. Πολλοί νέοι έχουν μια ψευδή αίσθηση ασφάλειας ότι αν στείλουν μια εικόνα ή βίντεο δεν θα υπάρχει μετά από λίγο και αυτό τους κάνει ακόμα πιο παράτολμους σε σχέση με το περιεχόμενο που στέλνουν. Επιπλέον αν κάποιος προσπαθήσει να τραβήξει ένα στιγμιότυπο της οθόνης την ώρα που βλέπει το βίντεο ή την εικόνα ο χρήστης που ανέβασε το βίντεο/εικόνα ειδοποιείται όμως τα παιδιά έχουν βρει τρόπο να παρακάμπτουν και αυτό το πρόβλημα χρησιμοποιώντας μια δεύτερη συσκευή ώστε να τραβήξουν φωτογραφία/βίντεο ώστε να υπάρχει μόνιμα στην συσκευή τους χωρίς να το ξέρει άλλα ούτε και να μπορεί να κάνει κάτι για αυτό αυτός που ανέβασε την φωτογραφία/βίντεο.
Επιπλέον το παιδί για να μπορέσει να χρησιμοποιήσει την εφαρμογή που είναι επιτρεπτή σε παιδιά άνω των 13 χρονών, πρέπει να αποδεχτεί τους Όρους και Προϋποθέσεις οι οποίοι ξεκάθαρα αναφέρουν ότι το Snapchat μπορεί να χρησιμοποιεί οποιοδήποτε περιεχόμενο υπάρχει μέσα στην πλατφόρμα πράγμα που σημαίνει ότι μέλλον θεωρείτε άγνωστο για όποιο περιεχόμενο ανεβάσουν τα παιδιά.

Κεφάλαιο 6: Προστασία στο Διαδίκτυο

Στην σημερινή εποχή η χρήση του διαδικτύου έχει γίνει αναπόσπαστο κομμάτι της ζωής μας. Η ασφαλής πλοήγηση στον αχανή αυτόν κόσμο χρειάζεται σωστή ενημέρωση και από την πλευρά των γονέων/εκπαιδευτικών και από την πλευρά του παιδιού. Δεν χρειάζεται φόβος ούτε πανικός όμως πρέπει να υπάρχει σωστή επικοινωνία του παιδιού με τον γονέα ώστε ούτε να φοβάται να του πει αυτό που το προβληματίζει αλλά και να μπορεί να είναι καταδεχτικό στο να μάθει και να πληροφορηθεί.

6.1 Τι μπορεί να κάνει ο γονέας για την προστασία του παιδιού

- Ενημέρωση του παιδιού για τους κινδύνους

Μόλις το παιδί ξεκινήσει να χρησιμοποιεί το διαδίκτυο θα πρέπει να ενημερωθεί για τους κινδύνους που μπορεί να συναντήσει όπως ο κίνδυνος της έκθεσης των προσωπικών δεδομένων στο διαδίκτυο, το ακατάλληλο περιεχόμενο, διαφημίσεις και αγορές

- Να θεσπίσει όρια

Ο υπολογιστής στο σπίτι θα πρέπει να βρίσκεται σε εμφανές σημείο και όχι στο δωμάτιο του παιδιού. Επίσης θα πρέπει να γίνει προγραμματισμός για την ώρα που μπορεί να καταναλώνει το παιδί στο διαδίκτυο ανάλογα με την ηλικία του

- Επιλογή κατάλληλων εφαρμογών για την ηλικία του παιδιού

Οι περισσότερες εφαρμογές καθορίζουν το ηλικιακό κοινό στο οποίο απευθύνονται και αυτό συνήθως ορίζεται με βάση το περιεχόμενο και τις απαιτήσεις τους

- Να φτιάξουν μαζί με το παιδί τις ρυθμίσεις ασφαλείας και απορρήτου

Έλεγχος για την επιλογή διπλού ελέγχου ταυτότητας(two-factor authentication)
Προτρέψτε το παιδί να μην χρησιμοποιεί εύκολους κωδικούς πρόσβασης στις ιστοσελίδες που εγγράφεται, όπως ημερομηνίες γέννησης καθώς είναι εύκολο να τους μαντέψει οποιοσδήποτε.
Διαβάστε τους όρους χρήσης των ιστοσελίδων που επισκέπτεται και εγγράφεται το παιδί σας (ιστοσελίδες κοινωνικής δικτύωσης, στα forums και τα ιστολόγια).

- Τοποθέτηση Γονικού Ελέγχου σε ηλεκτρονικές συσκευές και ιστοσελίδες

Με τις κατάλληλες ρυθμίσεις ο γονέας μπορεί να αποκλείσει ακατάλληλο περιεχόμενο, να θέσει όρια χρήσης του διαδικτύου αλλά και να επιτρέψει συγκεκριμένες εφαρμογές και ιστοσελίδες.

- Επίβλεψη νεαρών παιδιών

Ο γονέας θα πρέπει να είναι γνώστης της διαδικτυακής κίνησης του παιδιού του. Θα πρέπει να ξέρει τί περιεχόμενο δημοσιεύει, δημιουργεί ή παρακολουθεί το παιδί, τις υπηρεσίες και τις πλατφόρμες που χρησιμοποιεί, τα παιχνίδια που παίζει καθώς και με ποιους ανθρώπους επικοινωνεί.

- Οδηγίες για την σωστή διαδικτυακή συμπεριφορά

Το παιδί θα πρέπει να μάθει να εφαρμόζει και διαδικτυακά κάποιους κανόνες σωστής συμπεριφοράς ως προς τους άλλους όπως κάνει και στην καθημερινότητά του εκτός διαδικτύου. Δεν θα πρέπει να κάνει αυτό που δεν θα ήθελε να του κάνουν.
Θα πρέπει να προσέχει πως εκφράζεται ώστε να μην προσβάλει κανέναν, να μην δημοσιεύει περιεχόμενο και προσωπικές πληροφορίες τρίτων χωρίς την γνώση τους.

- Δεν χρειάζεται πανικός.

Σε περίπτωση που ο γονέας αντιληφθεί κάτι ύποπτο στην συμπεριφορά του παιδιού του ή κάποιου διαδικτυακού του φίλου δεν πρέπει να απειλήσει το παιδί ότι θα τιμωρηθεί και θα του αφαιρεθούν οι συσκευές του και η χρήση του Internet θα περιοριστεί καθώς μπορεί αυτό να φέρει αντίθετα αποτελέσματα. Πρέπει το παιδί να είναι σε θέση να εμπιστεύεται τον γονέα ώστε να συζητά μαζί του αυτά που το απασχολούν και ο γονέας με την σειρά του να μπορεί να του συμπαρασταθεί.

6.2 Τι πρέπει να ξέρει το παιδί για την προστασία του στο διαδίκτυο

- Πρέπει να είναι υπεύθυνο με την χρήση της τεχνολογίας και να σέβεται τους ανθρώπους ειδικά όταν έχει να κάνει με αυτούς μέσω τηλεφώνου, κινητού και γενικά μέσω τεχνολογίας

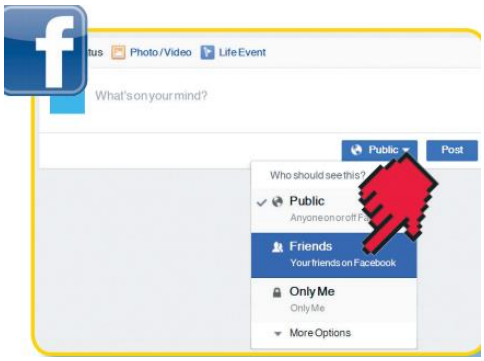
- Θα πρέπει τα μηνύματα που διαλαλεί να είναι θετικού περιεχομένου και όχι μηνύματα θυμού, υβριστικού ή ρατσιστικού περιεχομένου

- Θα πρέπει να σκέφτεται πριν ανεβάσει κοινοποιήσει μια σκέψη του, ένα βίντεο ή μια εικόνα του. Θα πρέπει να θυμάται πως οτιδήποτε υπάρχει στο διαδίκτυο μένει εκεί για πάντα και είναι δύσκολο να διαγραφεί.

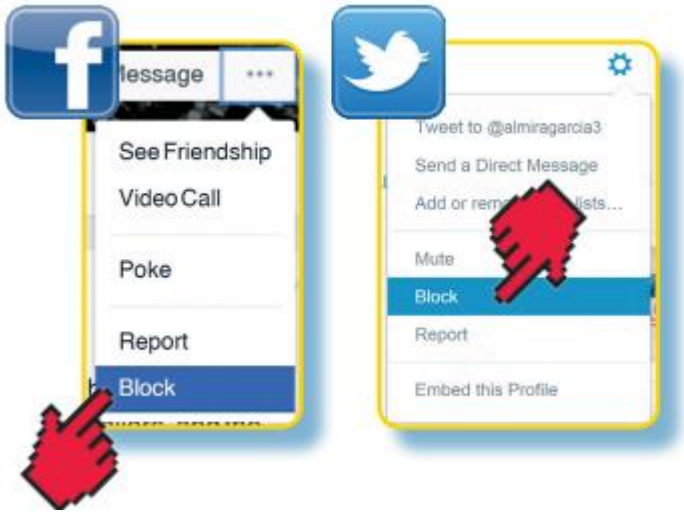
- Θα πρέπει να είναι προσεχτικό όταν χρησιμοποιεί Gadgets. Υπάρχει ο κατάλληλος τόπος και η ώρα για να χρησιμοποιηθούν

- Θα πρέπει να βάζει ένα όριο στην ώρα που χρησιμοποιηθεί το διαδίκτυο. Δεν πρέπει το Internet να ελέγχει την ζωή του καθώς υπάρχουν και άλλες ευθύνες αλλά και ευχαρίστηση και παιχνίδι εκτός αυτού.

- Θα πρέπει να χρησιμοποιεί τις ρυθμίσεις ασφαλείας και απορρήτου στα Social Media. Έτσι θα μπορεί να ελέγξει ποιοι βλέπουν το περιεχόμενό που θα αναρτήσει



- Θα πρέπει να θυμάται ότι μπορεί να σταματήσει την επικοινωνία με άτομα ή σελίδες που το κάνουν να αισθάνεται άβολα. Το Internet μπορεί να αποκλείσει είτε στα social media είτε στα εμαιλ όποιον τα κάνει να φοβούνται, αν πληγώνονται ή να αισθάνονται άσχημα.

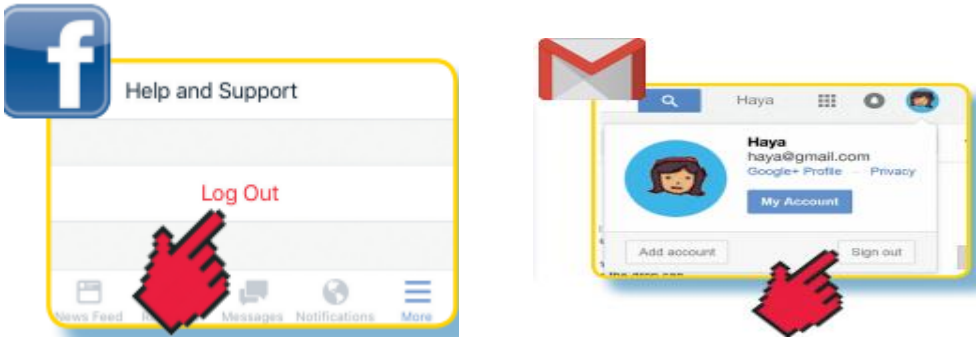


- Θα πρέπει να δημιουργούν κωδικούς που είναι δύσκολο να σπάσουν.

Οι κωδικοί θα πρέπει να περιέχουν κεφάλαια και μικρά γράμματα, αριθμούς και σύμβολα

Weak Passwords	Strong Passwords
Password	\ne2o.P1/
12345678	&k1cO_282.lim)
JimBob	{Tr35uR3_hun2er/}
joedoe120171	

- Θα πρέπει πάντα να κάνουν αποσύνδεση από τις συσκευές και τις εφαρμογές που έχουν συνδεθεί (email, social media,games)



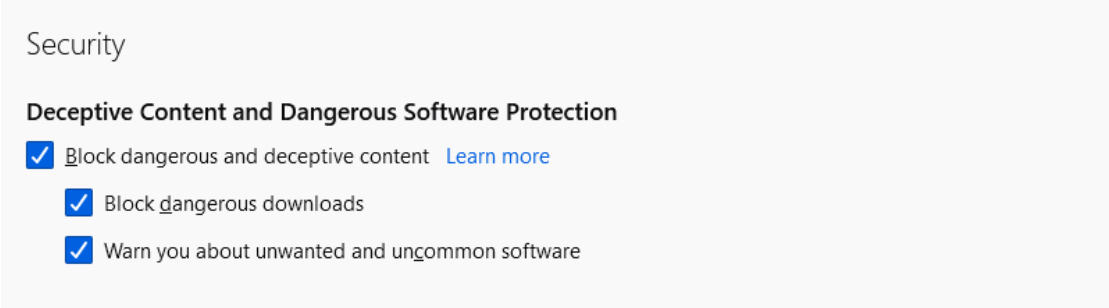
6.3 Τεχνικές συμβουλές

Online Controls

Οι μηχανές αναζήτησης όπως το Google Chrome και ο Firefox έχουν επιλογές ασφάλειας και απορρήτου. Από εκεί με τις κατάλληλες ρυθμίσεις μπορεί να αποκλειστεί ακατάλληλο περιεχόμενο, επικίνδυνες εφαρμογές που μπορεί να προσπαθήσουν αν εγκατασταθούν στον υπολογιστή αλλά και να γίνει φιλτράρισμα των αποτελεσμάτων που εμφανίζονται

Παράδειγμα του Firefox

Menu->Options->Privacy & Security



- Block dangerous and deceptive content: Η επιλογή αυτή μπλοκάρει πιθανά malware ή πιθανά περιεχόμενα ιστοσελίδων που μπορεί να σε εξαπατήσουν ώστε να κατεβάσεις κάποιο malware ή να βάλεις πληροφορίες σε περιβάλλον που δεν χρειάζονται.
- Block dangerous downloads: Μπλοκάρει πιθανούς ιούς ή malware
- Warn you about unwanted and uncommon software: ενημερώνει τον χρήστη αν πρόκειται να κατεβάσει κάποια αχρείαστη ή μη επιθυμητή εφαρμογή που μπορεί να περιέχει ιούς ή να κάνει ανεπιθύμητες αλλαγές στον υπολογιστή.

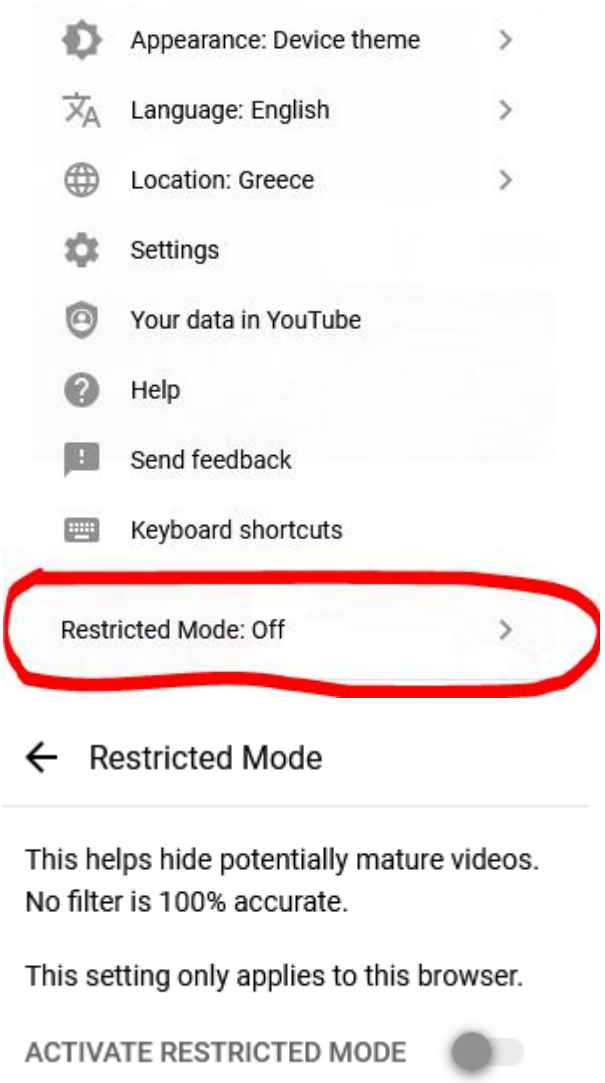
Social Media

Όπως και με τις μηχανές αναζήτησης έτσι και τα Social Media όπως το YouTube έχουν ρυθμίσεις ασφάλειας και απορρήτου. Αυτές μπορούν να αποτρέψουν το παιδί από το να συνομιλήσει με αγνώστους ή να δει ακατάλληλο περιεχόμενο.

Παράδειγμα YouTube

Στο YouTube υπάρχουν αρκετές επιλογές. Η αρχική επιλογή είναι το YouTube Kids μια μορφή της εφαρμογής φιλική προς τα παιδιά και με κατάλληλο περιεχόμενο. Αν ο γονιός έχει συνδεδεμένο το Google account του τότε μπορεί μέσω των ρυθμίσεων να διαμορφώσει τι θα βλέπει το παιδί, αν θα χρειάζεται έγκριση πριν από κάθε αναπαραγωγή βίντεο, τον χρόνο που βρίσκεται το παιδί μπροστά στην οθόνη κ.α.

Για την κανονική έκδοση του YouTube υπάρχει η επιλογή Restricted Mode που φιλτράρει το ακατάλληλο περιεχόμενο πάλι με την σύνδεση στο Google account στο YouTube



Επιπλέον λέγεται πως θα προστεθεί και η λειτουργία γονικού ελέγχου Beyond Content με 3 διαφορετικές ρυθμίσεις περιεχομένου:

Εξερεύνηση (explore): Αυτή η ρύθμιση αφορά στα παιδιά που είναι έτοιμα να προχωρήσουν από το YouTube Kids στο YouTube. Περιλαμβάνει ένα ευρύ φάσμα βίντεο που είναι γενικά κατάλληλα για θεατές ηλικίας άνω των 9 ετών.

-Εξερεύνηση περισσότερων (explore more): Ουσιαστικά είναι μια πιο εμπλουτισμένη έκδοση της πρώτης ρύθμισης (explore) η οποία περιλαμβάνει περιεχόμενο γενικά κατάλληλο για θεατές ηλικίας άνω των 13 ετών.

-Το μεγαλύτερο μέρος του YouTube (Most of YouTube):Αυτή η ρύθμιση περιέχει σχεδόν όλα τα βίντεο στο YouTube, εκτός από περιεχόμενο με περιορισμό ηλικίας και περιλαμβάνει ευαίσθητα θέματα που μπορεί να είναι κατάλληλα μόνο για μεγαλύτερους εφήβους.

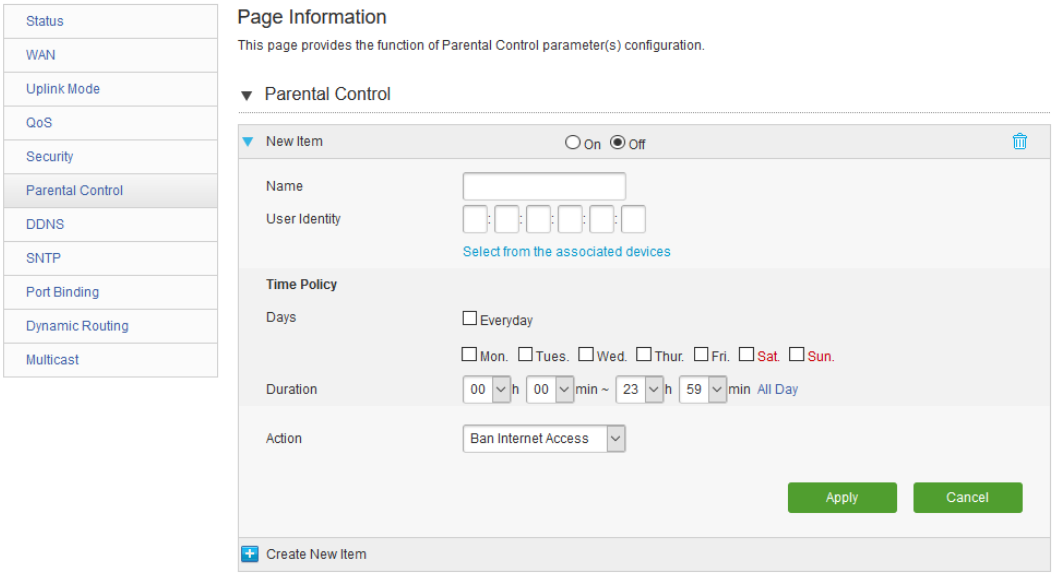
Η νέα επιλογή δεν θα κατηγοριοποιεί τις διαφημίσεις ανάλογα με τις προτιμήσεις των παιδιών και οι in-app αγορές θα είναι απενεργοποιημένες. Παράλληλα, ορισμένα από τα comments και τα creation features θα είναι επίσης απενεργοποιημένα.

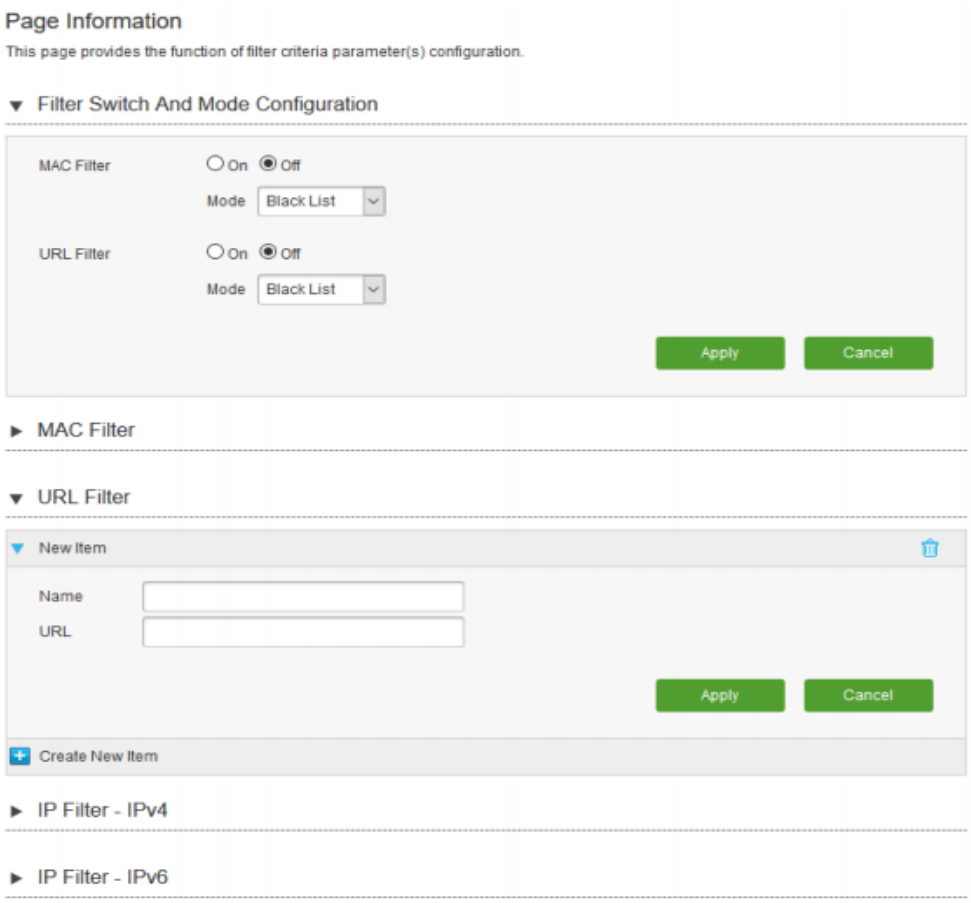
Επιλογές Γονικού Ελέγχου

Οι επιλογές γονικού ελέγχου μπορούν να βρεθούν στις κινητές συσκευές, στα προ εγκατεστημένα λειτουργικά των υπολογιστών, στους παρόχους διαδικτύου ακόμα και να αγοραστούν. Με αυτή την επιλογή έχουμε αρκετές δυνατότητες ελέγχου ως προς το περιεχόμενο που θα βλέπει το παιδί, τις ώρες που βρίσκεται στο διαδίκτυο, την απαγόρευση χρήσης κάμερας όταν το παιδί χρησιμοποιεί τον υπολογιστή κ.α.

Router

Η επιλογή Γονικού ελέγχου υπάρχει στο router που μας έχει προμηθεύσει ο πάροχος του διαδικτύου μας. Αρχικά βρίσκουμε την default gateway (πατώντας ipconfig στο cmd του υπολογιστή μας) και την τοποθετούμε σε έναν browser όπου θα μας ανακατευθύνει στην αρχική σελίδα του router μας. Για να κάνουμε είσοδο πληκτρολογούμε σαν username admin και σαν κωδικό αυτόν που βρίσκεται πάνω στην συσκευή του router μας. Πηγαίνοντας στην επιλογή Internet και έπειτα στις επιλογές Parental Controls ή Security->Filter Criteria μας δίνεται η δυνατότητα να αποκλείσουμε συγκεκριμένες ιστοσελίδες ή να απαγορεύσουμε την πρόσβαση στο Internet μετά από μια συγκεκριμένη ώρα ή συγκεκριμένες μέρες.

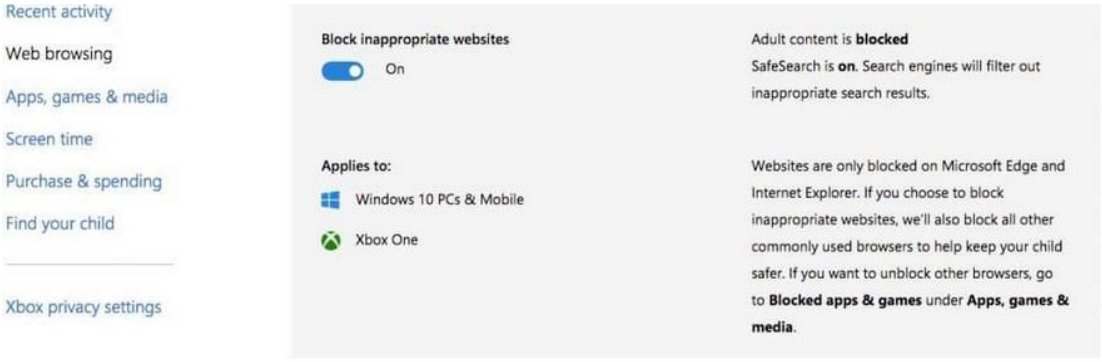


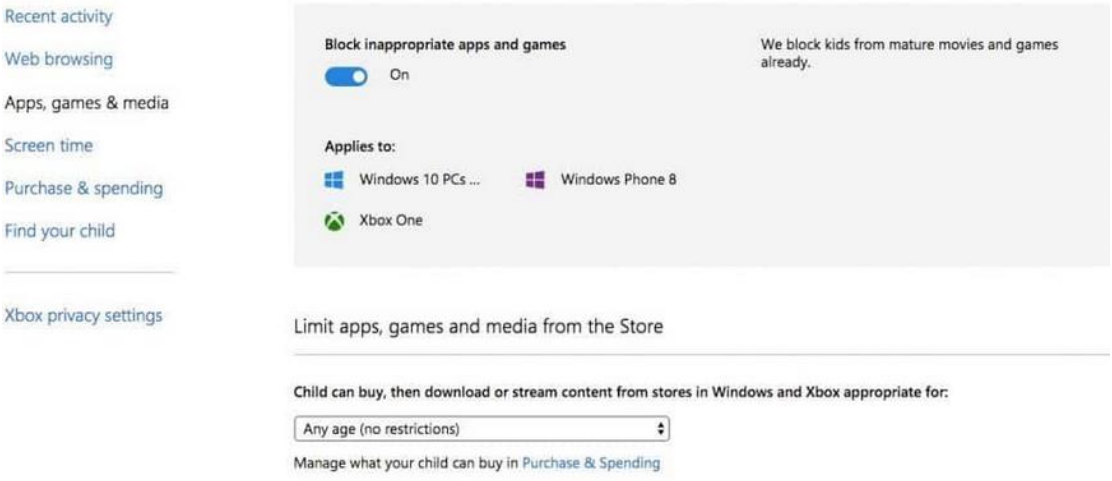


Windows 10

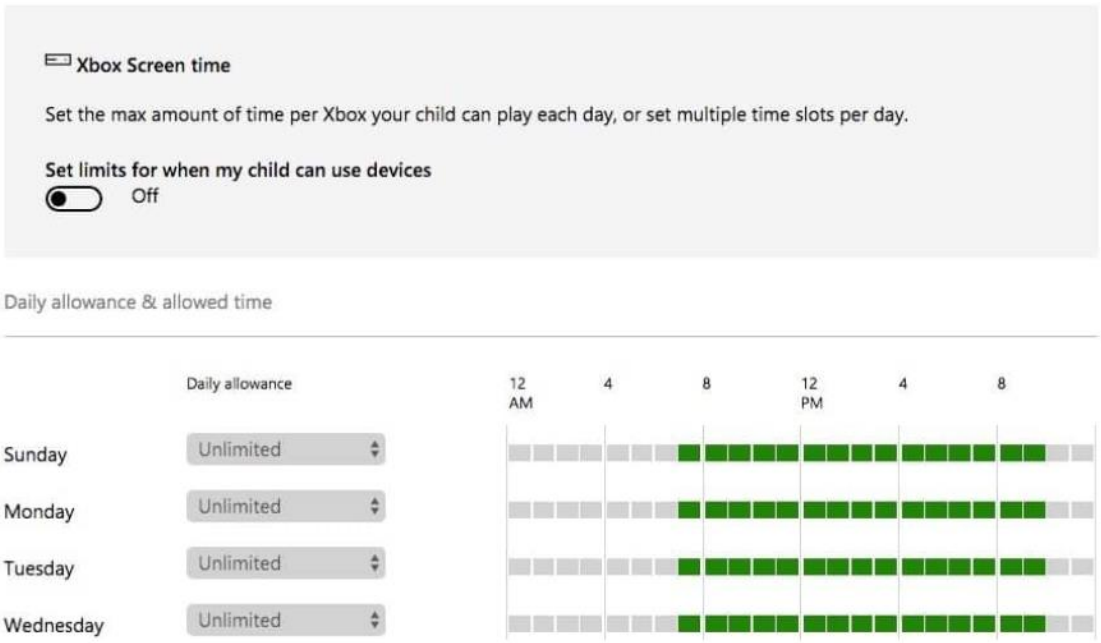
Για να τοποθετηθεί ο Γονικός Έλεγχος στα Windows θα πρέπει να κάνουμε είσοδο στο Microsoft Account στον οποίο θα έχουμε συνδέσει τον λογαριασμό του παιδιού επιτρέποντας να γίνονται οι αλλαγές σε ένα online περιβάλλον που θα τις ρυθμίζει σε όλες τις συσκευές που θα υπάρχει ο λογαριασμός του παιδιού (υπολογιστές, κινητές συσκευές,Xbox). Ο γονέας με τις ρυθμίσεις μπορεί να αποκλείσει ακατάλληλες ιστοσελίδες

πχ πορνογραφικού περιεχομένου, μπορεί να ενεργοποιηθεί η ασφαλής πλοήγηση, να προστεθούν URL's ιστοσελίδων που πάντα θα επιτρέπονται ή αντίστοιχα πάντα θα απαγορεύονται, να τεθούν χρονικά όρια που θα χρησιμοποιείται ο υπολογιστής ή άλλη συσκευή αλλά και να ελέγχονται οι ηλεκτρονικές αγορές που κάνει το παιδί δίνοντας την δυνατότητα να προσθέσουμε εμείς χρήματα στον λογαριασμό του για περιορισμένες αγορές.[8]



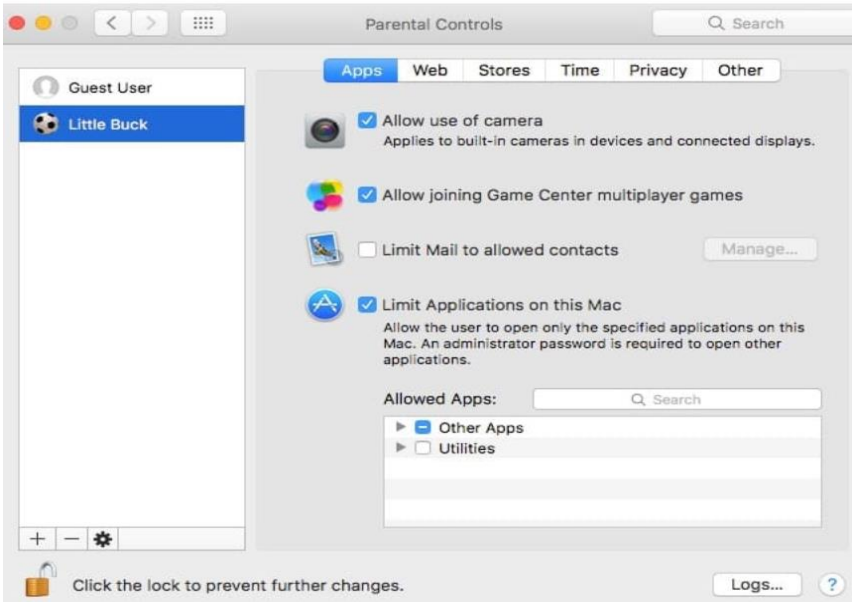


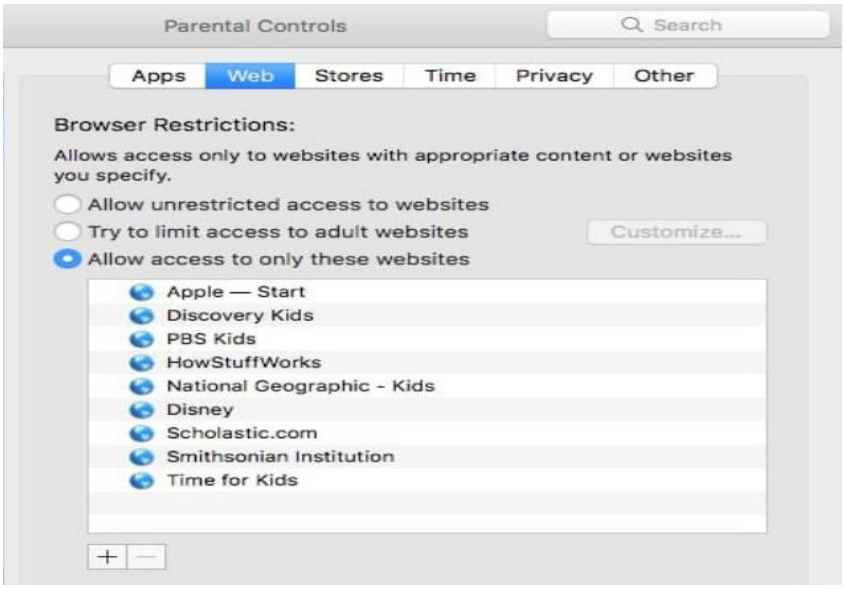
[8] How to Keep Your Children Safe Online by Chris Hauk



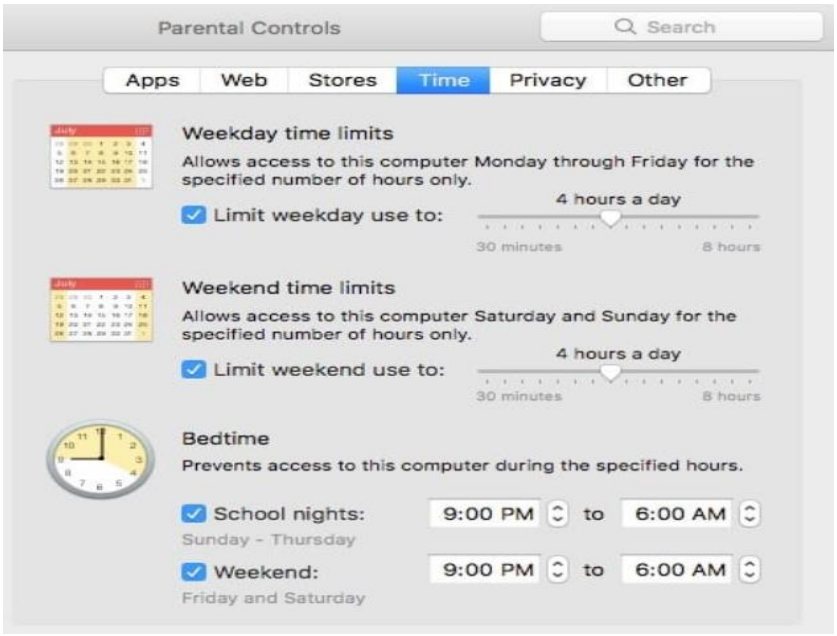
Mac

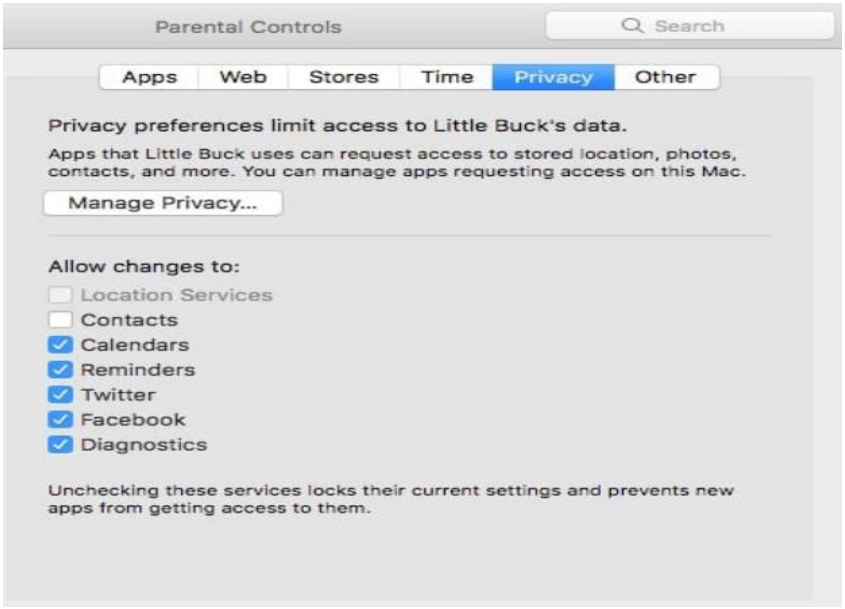
Ο Γονικός έλεγχος στα Mac πρέπει να ενεργοποιηθεί τοπικά (βέβαια όταν τοποθετηθεί και μετά μπορεί να προσαρμοστεί απομακρυσμένα από άλλο Mac). Οι επιλογές που υπάρχουν επιτρέπουν στον γονέα να επιλέξει ποιες εφαρμογές μπορούν να χρησιμοποιηθούν, σε ποιες ιστοσελίδες μπορεί να γίνει είσοδος, την χρονική διάρκεια που θα χρησιμοποιηθεί ο υπολογιστής κ.α.
Αυτό μπορεί να γίνει απλά πατώντας το εικονίδιο της Apple στην επάνω αριστερή γωνία, έπειτα τις Επιλογές Συστήματος(System Preferences) και τέλος την επιλογή Γονικός Έλεγχος(Parental Controls) ώστε να επιλέξουμε τον λογαριασμό του παιδιού.

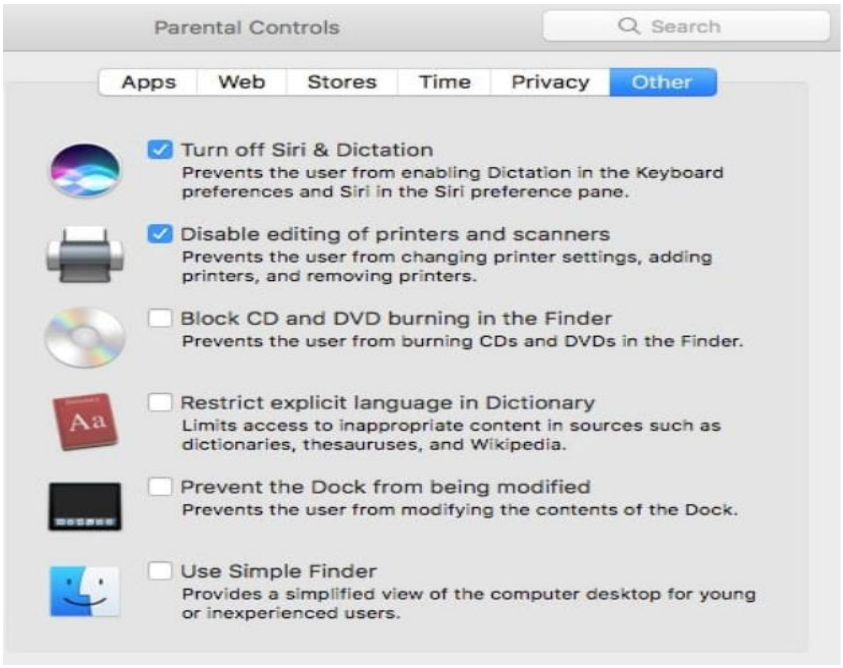



Parental Controls
Search
Apps
Web
Stores
Time
Privacy
Other
Browser Restrictions:
Allows access only to websites with appropriate content or websites you specify.
Allow unrestricted access to websites
Try to limit access to adult websites
Customize...
Allow access to only these websites
Apple — Start
Discovery Kids
PBS Kids
HowStuffWorks
National Geographic - Kids
Disney
Scholastic.com
Smithsonian Institution
Time for Kids


Parental Controls
Search
Apps
Web
Stores
Time
Privacy
Other
Disable:
iTunes Store
iTunes U
iBooks Store
Restrict:
Music with explicit content
Movies to:
PG
TV shows to:
TV-G
Apps to:
9+
Books with explicit sexual content


Parental Controls
Search
Apps
Web
Stores
Time
Privacy
Other
Weekday time limits
Allows access to this computer Monday through Friday for the specified number of hours only.
Limit weekday use to:
4 hours a day
30 minutes
8 hours
Weekend time limits
Allows access to this computer Saturday and Sunday for the specified number of hours only.
Limit weekend use to:
4 hours a day
30 minutes
8 hours
Bedtime
Prevents access to this computer during the specified hours.
School nights:
9:00 PM
to
6:00 AM
Sunday - Thursday
Weekend:
9:00 PM
to
6:00 AM
Friday and Saturday


Parental Controls
Search
Apps
Web
Stores
Time
Privacy
Other
Privacy preferences limit access to Little Buck's data.
Apps that Little Buck uses can request access to stored location, photos, contacts, and more. You can manage apps requesting access on this Mac.
Manage Privacy...
Allow changes to:
Location Services
Contacts
Calendars
Reminders
Twitter
Facebook
Diagnostics
Unchecking these services locks their current settings and prevents new apps from getting access to them.



Επίλογος

Το διαδίκτυο αλλάζει τόσο γρήγορα που τα τεχνολογικά μέτρα είναι απίθανο να μπορούν να συμβαδίσουν. Τα πιο αποτελεσματικά και ανθεκτικά μέτρα είναι εκείνα που βασίζονται στην οικογένεια, την κοινότητα, την εκπαίδευση και την ενδυνάμωση έτσι ώστε τα παιδιά και οι νέοι να είναι σε θέση να κάνουν σωστές επιλογές και να επωφεληθούν από την δύναμη του διαδικτύου.

Οι γονείς, οι κηδεμόνες και οι εκπαιδευτικοί πρέπει να αναλάβουν ενεργό ρόλο στην διδασκαλία των παιδιών και νέων σχετικά με τους κινδύνους που ενδέχεται να αντιμετωπίσουν διαδικτυακά από θηρευτές και απατεώνες και πως να τους αποφύγουν.

Όπως είδαμε οι κίνδυνοι και οι προκλήσεις που θα καλεστεί να αντιμετωπίσει το παιδί είναι πάρα πολλοί και διαφορετικοί. Cyberbullying, Grooming διαδικτυακά παιχνίδια και Social Media περνάνε από δοκιμασίες καθημερινά τα νέα παιδιά.
Γι’ αυτό πρέπει να υπάρχει σωστή ενημέρωση και γνώση και από την μεριά των γονιών/εκπαιδευτικών αλλά και από την μεριά του παιδιού όπως επίσης και αμοιβαία εμπιστοσύνη και κατανόηση για την αντιμετώπιση όλων αυτών των κινδύνων.

Βιβλιογραφία

(χ.χ.). Ανάκτηση από Helpline saferinternet: http://www.help-line.gr/

2020 Child Online Safety Index. (χ.χ.). Ανάκτηση από DQInstitute: https://www.dqinstitute.org/child-online-safety-index/

Bath, G. (χ.χ.). *It could result in death.' Thousands of teens are passing out on TikTok for likes.* Ανάκτηση από Mamamia: https://www.mamamia.com.au/pass-out-challenge-tiktok/

Bobic, C. (χ.χ.). *The Blackout Challenge on TikTok Can Have Deadly Consequences.* Ανάκτηση από Distractify: https://www.distractify.com/p/tiktok-blackout-challenge

Chan, A. (χ.χ.). *Is cyber bullying a cyber crime?* Ανάκτηση από Legal Cheek: https://www.legalcheek.com/lc-journal-posts/is-cyber-bullying-a-cyber-crime/

Child safety online. (χ.χ.). Ανάκτηση από digwatch: https://dig.watch/issues/child-safety-online

Child Safety Online Global challenges and strategies. (χ.χ.). Ανάκτηση από Unicef: https://www.unicef.org/media/66821/file/Child-Safety-Online.pdf

Child Sexual Exploitation and Grooming. (χ.χ.). Ανάκτηση από Victoria State Government Education and Training: https://www.education.vic.gov.au/school/teachers/health/childprotection/Pages/exploitationgrooming.aspx

Children and parents:Media use and attitudes report 2018. (χ.χ.). Ανάκτηση από Ofcom: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf

Children's Guide To Online Safety. (χ.χ.). Ανάκτηση από Save the Children Resource Centre: https://resourcecentre.savethechildren.net/node/10219/pdf/safeweb4kids.pdf

Children's Internet Usage Study. (χ.χ.). Ανάκτηση από Center for Cyber Safet and Education: https://isc2-center.my.salesforce.com/sfc/p/#G0000000iVSt/a/0f000000fyoh/2DH9U7g.6.30FxxqpmE5cAB.DelSYLV_D1mVQ08J8ho

Constine, J. (2018). *Facebook and Instagram Change to Crack Down on Underage Children.* Ανάκτηση από Techcrunch: https://techcrunch.com/2018/07/19/facebok-under-13/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKzQa51TMUcXbSrcQz1gG6dxAQzSIrfcr4031VQdVqPUHJAZUlyMQZlwj6gLGVDlL0VmBcWbptZ56sEuK4mXHtdz28DRpusb0j5QFss7sc-FjwMi5Xgiammqf7

COVID-19 and its implications for protecting children online. (χ.χ.). Ανάκτηση από Unicef: https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf

Cyberbullying. (χ.χ.). Ανάκτηση από kidshelpline: https://kidshelpline.com.au/teens/issues/cyberbullying

Dance, G. J. (2019). Fighting the Good Fight Against Online Child Sexual Abuse. *NYTimes*. Ανάκτηση από https://www.nytimes.com/interactive/2019/12/22/us/child-sex-abuse-websites-shut-down.html?searchResultPosition=7

Dark Web Child Abuse: Administrator of Darkscandals Arrested in the Netherlands . (χ.χ.). Ανάκτηση από Europol: https://www.europol.europa.eu/newsroom/news/dark-web-child-abuse-administrator-of-darkscandals-arrested-in-netherlands

Elgersma, C. (χ.χ.). *18 Social Media Apps and Sites Kids Are Using Right Now.* Ανάκτηση από common sence media: https://www.commonsensemedia.org/blog/16-apps-and-websites-kids-are-heading-to-after-facebook

Farivar, C., & Blankstein, A. (χ.χ.). *Feds take down the world's 'largest dark web child porn marketplace.* Ανάκτηση από nbcnews: https://www.nbcnews.com/news/crime-courts/feds-take-down-world-s-largest-dark-web-child-porn-n1066511

Foster, B. (χ.χ.). *Dangers of Snapchat.* Ανάκτηση από All Pro Dad: https://www.allprodad.com/dangers-of-snapchat/

Fruhlinger, J. (χ.χ.). *10 things you should know about dark web websites.* Ανάκτηση από CSO: https://www.csoonline.com/article/3322134/10-things-you-should-know-about-dark-web-websites.html

Greenberg, A. (χ.χ.). *Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds.* Ανάκτηση από Wired: https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/

Grooming and Red Flag Behaviors. (χ.χ.). Ανάκτηση από Darkness To Light: https://www.d2l.org/child-grooming-signs-behavior-awareness/

Growing Up in a Connected World. (χ.χ.). Ανάκτηση από Unicef: https://www.unicef-irc.org/growing-up-connected

Guckin, C. M., Völlink, T., & Dehue, F. (χ.χ.). *An Introduction in Cyberbullying Research.* Ανάκτηση από ResearchGate: https://www.researchgate.net/publication/283726503_An_Introduction_in_Cyberbullying_Research

Hauk, C. (χ.χ.). *How To Keep Your Children Safe Online: The Ultimate Guide For The Non Techy Parent.* Ανάκτηση από pixelprivacy: https://pixelprivacy.com/resources/keep-children-safe-online/

How to Protect Your Child from the Top 7 Dangers of Online Gaming. (χ.χ.). Ανάκτηση από Kaspersky: https://usa.kaspersky.com/resource-center/threats/top-7-online-gaming-dangers-facing-kids

Ipaidia, N. (χ.χ.). *Οι σύγχρονοι κίνδυνοι ειδικά για τους ανήλικους στο διαδίκτυο.* Ανάκτηση από iPaideia: https://www.ipaidia.gr/eidiseis/oi-sigxronoi-kindinoi-eidika-gia-tous-anilikous-sto-diadiktio

Ivanović, J. (χ.χ.). *Operational Handbook for Child Online.* Ανάκτηση από Save the Children Resource Centre: https://resourcecentre.savethechildren.net/node/15493/pdf/operational_handbook_for_child_online_safety_centres.pdf

Jansen, H. A., Jakobsen, G., Gundorff, H., & Sorensen, K. (χ.χ.). *Is it really that bad?* Ανάκτηση από Save the Children Recource Centre: https://resourcecentre.savethechildren.net/node/12241/pdf/is-it-really-that-bad-an-antholohy-of-online-sexual-abuse-of-children-and-young-people.pdf

John, S. (2019). How to set parental controls on YouTube in 2 different ways. *INSIDER*. Ανάκτηση από https://www.businessinsider.com/how-to-set-parental-controls-on-youtube

Kids, the Internet & COVID-19:How parents can keep children safe online. (χ.χ.). Ανάκτηση από Internet Sociey: https://www.internetsociety.org/wp-content/uploads/2020/04/Online-safety-parents-webinar-draft_final.pdf

Lapset, P., & Barnen, R. (χ.χ.). *Children's experiences of sexual harassment and abuse on the internet.* Ανάκτηση από Save The Children Resource Centre: https://resourcecentre.savethechildren.net/node/6776/pdf/6776.pdf

Latest helpline trends: Quarter 2, 2020. (χ.χ.). Ανάκτηση από Better Internet for Kids: https://www.betterinternetforkids.eu/practice/helplines/article?id=6473739

Newsroom, C. (χ.χ.). *«Μπλε Φάλαινα»: Όλα όσα πρέπει να ξέρετε για το επικίνδυνο διαδικτυακό παιχνίδι.* Ανάκτηση από CNN Greece: https://www.cnn.gr/ellada/story/80885/mple-falaina-ola-osa-prepei-na-xerete-gia-to-epikindyno-diadiktyako-paixnidi

Newsroom, C. (χ.χ.). *Ανήλικοι και διαδίκτυο: Ποιοι κίνδυνοι ελλοχεύουν και τρόποι αντιμετώπισης.* Ανάκτηση από CNN Greece: https://www.cnn.gr/tech/story/107169/anilikoi-kai-diadiktyo-poioi-kindynoi-elloxeyoyn-kai-tropoi-antimetopisis

Notar, C. E., Padgett, S., & Roden, J. (χ.χ.). *Cyberbullying: Resources for Intervention and Prevention.* Ανάκτηση από Horizon Research publishing Corporation: https://www.hrpub.org/

Parker, W. (χ.χ.). *The Dark Side of Snapchat and Teens.* Ανάκτηση από verywell family: https://www.verywellfamily.com/what-is-snapchat-and-its-use-1270338

Ramirez, Z. (χ.χ.). *'Tinder For Teenagers' — Police Warn About New Kid Hookup App.* Ανάκτηση από parentology: https://parentology.com/police-warn-parents-about-tinder-for-teenagers/

Roblox: What parents must know about this dangerous game for kids. (χ.χ.). Ανάκτηση από Family zone: https://www.familyzone.com/anz/families/blog/roblox-parents-review

Sanchez, E. (χ.χ.). *Potentially Dangerous Social Media Apps Kids Love.* Ανάκτηση από parentology: https://parentology.com/potentially-dangerous-social-media-apps-kids-love/

Schillaci, M. (χ.χ.). *#netsmart.* Ανάκτηση από Save the Children Resource Centre: https://resourcecentre.savethechildren.net/node/9481/pdf/rb_netsmart_100dpi.pdf

Tips for Parents and Caregivers: Keeping Children Safe Online During The Covid-19 Pandemic. (χ.χ.). Ανάκτηση από Unicef: https://www.unicef.org/eap/media/5141/file

Video Games. (χ.χ.). Ανάκτηση από Center on Media and Child Health: https://cmch.tv/parents/video-games/

White, D. (χ.χ.). *Keeping Your Kids Safe Online-Safety Tips & Guides.* Ανάκτηση από Trinus: https://www.trinustech.com/blog/keeping-kids-safe-online-security-tips-guides

Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (χ.χ.). *Sextortion: Cybersecurity, teenagers, and remote sexual assault.* Ανάκτηση από Brookings: https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/

Ισμαηλίδου, Ε. (2012). «Cyberbullying» και «sexting» απειλούν τα παιδιά στο Διαδίκτυο. *ToVima*. Ανάκτηση από https://www.tovima.gr/2012/01/13/society/cyberbullying-kai-sexting-apeiloyn-ta-paidia-sto-diadiktyo/

Καρδαρά , Α. (2019). *Ανήλικοι και Διαδίκτυο: οδηγός επιβίωσης στο αχανές, θαυμάσιο αλλά και τρομακτικό, διαδικτυακό σύμπαν.* Ανάκτηση από postmodern: https://www.postmodern.gr/anilikoi-kai-diadiktyo-odigos-epivio/

Κόλλιας, Φ. (χ.χ.). *TikTok: Σοβαρές καταγγελίες για την εφαρμογή που κάνει θραύση στα παιδιά μας.* Ανάκτηση από EURO2day: https://www.euro2day.gr/news/world/article/2023712/tik-tok-sovares-kataggelies-gia-thn-efarmogh-poy-k.html?fbclid=IwAR2HUXLYOArLvk37e4J6tiL5fNPFF20RdJfjcqVKRdCFL_AIy4PsGl5-YQg

Μαγουνάκη, Ρ. (χ.χ.). *Μήπως οι κίνδυνοι του Διαδικτύου για τους ανήλικους είναι μεγαλύτεροι από ότι νομίζουμε?* Ανάκτηση από CSIi Cyber Security International Institute: https://www.csii.gr/%CE%BC%CE%AE%CF%80%CF%89%CF%82-%CE%BF%CE%B9-%CE%BA%CE%AF%CE%BD%CE%B4%CF%85%CE%BD%CE%BF%CE%B9-%CF%84%CE%BF%CF%85-%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85-%CE%B3%CE%B9%CE%B1-%CF%84/

Νέες ρυθμίσεις γονικού ελέγχου για εφήβους και παιδιά από το YouTube. (χ.χ.). Ανάκτηση από SaferInternet4Kids: https://saferinternet4kids.gr/nea/supervisedaccountyoutube/

Οι κίνδυνοι στο διαδίκτυο για τους ανήλικους και οι τρόποι αντιμετώπισής τους. (χ.χ.). Ανάκτηση από newsbeast: https://www.newsbeast.gr/technology/arthro/3032340/i-kindini-sto-diadiktio-gia-tous-anilikous-ke-i-tropi-antimetopisis-tous

Οικονομίδη, Ε. (2018). Ανήλικοι στα «δίχτυα» των social media – Το 55% κάτω των 13 τα χρησιμοποιούν καθημερινά! *Ελεύθερος Τύπος*. Ανάκτηση από https://eleftherostypos.gr/ellada/208528-anilikoi-sta-dixtya-ton-social-media-to-55-kato-ton-13-ta-xrisimopoioun-kathimerina/

Σπαθή, Θ. (χ.χ.). *Το φαινόμενο του κυβερνοεκφοβισμού (cyberbulling) στην Ελλάδα και το εξωτερικό.* Ανάκτηση από CrimeTimes: https://www.crimetimes.gr/to-fainomeno-tou-kyvernoekfovismoy-cyberbulling-sthn-ellada-kai-to-ekswteriko/

Τσιώτση , Χ. (2014). *Βλαβερές συνέπειες του Internet στα παιδιά και τους εφήβους.* Ανάκτηση από News.gr: https://www.news.gr/tech/internet/article/152392/vlaveres-synepeies-toy-internet-sta-paidia-kai-toy.html