ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
&
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
&
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

«Σχεδιασμός και Υλοποίηση Εκπαιδευτικής Διαδικτυακής Πλατφόρμας για την Ασφαλή Περιήγηση στο Διαδίκτυο»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

των

ΔΑΜΙΑΝΟΥ ΚΕΦΑΛΑ

(ΑΕΜ:151)

ΜΑΓΔΑΛΗΝΗ ΤΣΕΤΟΥ ΚΕΦΑΛΑ

(ΑΕΜ:152)

Επιβλέπων: **Άγγελος Μιχάλας**

Καθηγητής

Καστοριά Απρίλιος – 2022

Η παρούσα σελίδα σκοπίμως παραμένει λευκή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
&
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
&
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

«Σχεδιασμός και Υλοποίηση Εκπαιδευτικής Διαδικτυακής Πλατφόρμας για την Ασφαλή Περιήγηση στο Διαδίκτυο»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

των

ΔΑΜΙΑΝΟΥ ΚΕΦΑΛΑ
(ΑΕΜ:151)

ΜΑΓΔΑΛΗΝΗ ΤΣΕΤΟΥ ΚΕΦΑΛΑ
(ΑΕΜ:152)

Επιβλέπων: **Άγγελος Μιχάλας**
Καθηγητής

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την

…….	…….	…….
Άγγελος Μιχάλας Καθηγητής	Σπυρίδων Νικολάου Λέκτορας	Δημήτριος Βέργαδος Επίκουρος

Καστοριά Απρίλιος – 2022

Ευχαριστίες

Έχοντας φτάσει στο τέλος του δρόμου της ολοκλήρωσης της διπλωματικής εργασίας του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών «Προηγμένες Τεχνολογίες Πληροφορικής και Υπηρεσίες» των Πανεπιστημίων Δυτικής Μακεδονίας και Πειραιά, θα θέλαμε να ευχαριστήσουμε όλους όσους συνδράμανε, τάχθηκαν αρωγοί, στάθηκαν δίπλα μας και μας παραστάθηκαν μέχρι το τέλος σε όλη αυτήν την παρούσα διαδρομή.

Αρχικά, θέλουμε ιδιαιτέρως να ευχαριστούμε τον κ. Άγγελο Μιχάλα, Καθηγητή του τμήματος Πληροφορικής του Πανεπιστημίου Δυτικής Μακεδονίας, που μας παραχώρησε την τρέχουσα διπλωματική εργασία και ανέλαβε την εποπτεία της.

Επίσης, ευχαριστούμε όλους τους καθηγητές για τις πολύτιμες συμβουλές, γνώσεις και το αξιόλογο έργο που μας έδωσαν ανιδιοτελώς καθ' όλη τη διάρκεια των Μεταπτυχιακών μας σπουδών. Ακόμη, να ευχαριστήσουμε όλους τους συμφοιτητές μας με τους οποίους αναπτύξαμε αμοιβαίες σχέσεις βοήθειας και υποστήριξης κατά τη διάρκεια των σπουδών μας. Δε θα μπορούσαμε να μην κάνουμε λόγο για την υποψήφια διδάκτωρ κα. Κλεοπάτρα Γκόλα η οποία μας στήριξε, ενίσχυσε, ενθάρρυνε με τις υποδείξεις της, προσφέροντάς μας στο μέγιστο συμβουλευτική συνεργασία, ώστε να ανταπεξέλθουμε και να αντιμετωπίσουμε στις προκλήσεις που παρουσιάστηκαν.

Τέλος, να ευχαριστήσουμε τα μέλη της οικογένειάς μας για την αναρίθμητη και άφθονη βοήθεια και στήριξη τους όλους αυτούς τους μήνες .

Περίληψη

Στη σύγχρονη εποχή, το διαδίκτυο αποτελεί αναπόσπαστο κομμάτι της καθημερινής ενασχόλησης των νέων αλλά και των παιδιών μικρότερης ηλικίας. Οι καινοτόμες και ψυχαγωγικές υπηρεσίες που προσφέρει είναι αναρίθμητες και εντυπωσιακές. Ωστόσο όμως, οι δραστηριότητες αυτές ελλοχεύουν αρκετούς κινδύνους που υπομονεύουν την ασφαλή πλοήγηση των χρηστών αλλά κυρίως των μικρών παιδιών. Για το λόγο αυτό, τα παιδιά και οι νέοι γενικότερα είναι ανάγκη να γνωρίζουν όλες αυτές τις επικίνδυνες καταστάσεις που είναι πιθανό να συναντήσουν στο διαδίκτυο.

Η τρέχουσα διπλωματική εργασία αποσκοπεί στην ενημέρωση των παιδιών, των γονέων και των εκπαιδευτικών σε θέματα που άπτονται την ασφάλεια στον παγκόσμιο ιστό, το γονικό έλεγχο και τους κινδύνους του διαδικτύου. Η ενημέρωση γίνεται μέσω μιας ιστοσελίδας που δημιουργήθηκε για το σκοπό αυτό, με το όνομα *kidstaysafe*, όπου παρουσιάζονται τα θέματα που προαναφέραμε καθώς επίσης και μία σειρά από δραστηριότητες. Με αυτόν τον τρόπο είναι πιο εύκολη η κατανόηση των σοβαρών εννοιών από τα μικρά παιδιά, αλλά και πιο ευχάριστη για τους μεγαλύτερους.

Επιπλέον, μέσα από άρθρα ελληνικής αλλά και διεθνής βιβλιογραφίας, ο επισκέπτης, μπορεί να ενημερωθεί και να γνωρίσει καλύτερα τους κινδύνους του διαδικτύου και τους αντίστοιχους τρόπους αντιμετώπισης, την ασφάλεια στο διαδίκτυο και οδηγίες ασφαλούς πλοήγησης, την εφαρμογή του γονικού ελέγχου, την προστασία προσωπικών δεδομένων (GDPR) και τη νομοθεσία σε θέματα που αφορούν την συμπεριφορά κατά την πλοήγηση στον παγκόσμιο ιστό. Επίσης, γίνεται μία αναφορά στα οφέλη και τους κινδύνους των πιο διαδεδομένων μέσων κοινωνικής δικτύωσης που χρησιμοποιούν κυρίως οι νέοι και τα μικρά παιδιά.

Στο τέλος της εργασίας, παρουσιάζονται προτάσεις οι οποίες θα μπορούσαν να αποτελέσουν αντικείμενο μελλοντικής έρευνας. Πιο συγκεκριμένα, προτείνεται δημιουργία σχολικών ιστοσελίδων από τα παιδιά με τη βοήθεια των εκπαιδευτικών ώστε να συνδράμουν στην ανατροφοδότηση της γνώσης και της ενημέρωσης για την ασφαλή πλοήγηση στο διαδίκτυο.

Λέξεις Κλειδιά: *Ασφάλεια στο Διαδίκτυο, Γονικός Έλεγχος, Τεχνική Διαμεσολάβηση, Λειτουργικό Σύστημα, Ψηφιακές Δεξιότητες, WordPress, Κίνδυνοι του Διαδικτύου, Κοινωνική Δικτύωση*

Abstract

In modern times, the internet is an integral part of the daily activities of young people and especially younger children. The innovative and entertainment services it offers are innumerable and impressive. However, these activities pose several risks that lurk in the safe navigation of users but especially of young children. For this reason, children and young people in general need to be aware of all these dangerous situations that they are likely to encounter online.

The present dissertation aims to inform children, parents and teachers on issues related to web security, parental control and the dangers of the internet. The information is provided through a website created for this purpose, called *kidstaysafe*, which presents the topics mentioned above as well as a series of activities. This way it is easier for young children to understand serious concepts, but also more enjoyable for older ones.

In addition, through Greek and international bibliography articles, the visitor can be better informed and better acquainted with the dangers of the internet and the corresponding ways of dealing with it, internet security and safe navigation instructions, the application of parental control, the protection of personal data. (GDPR) and legislation on behavior while navigating the World Wide Web. There is also a reference to the benefits and risks of the most popular social media used mainly by young people and young children. At the end of the work, suggestions are presented which could be the subject of future research. More specifically, it is proposed to create school websites by children with the help of teachers to assist in the feedback of knowledge and information for safe internet browsing.

Key Words: *Internet Safety, Parental Control, Technical Mediation, Operating System, Digital Skills, WordPress, Dangers of the Internet, Social Media*

Περιεχόμενα

Λίστα Σχημάτων

Λίστα Πινάκων

Εισαγωγή

Το διαδίκτυο πλέον αποτελεί τον κατεξοχήν χώρο στον οποίο καθημερινά δραστηριοποιούνται ευχάριστα τα παιδιά και γενικότερα οι νέοι. Όμως, οι κίνδυνοι που καραδοκούν από την πλοήγηση στον παγκόσμιο ιστό είναι επιζήμιοι, τόσο στην προσωπική ζωή όσο και στην ασφάλεια των προσωπικών τους δεδομένων. Είναι πολύ συχνό φαινόμενο τα παιδιά, κατά τη διάρκεια ενασχόλησής τους με τις υπηρεσίες του διαδικτύου, να αντιμετωπίσουν ιστοσελίδες με ακατάλληλο περιεχόμενο, επικίνδυνες συμπεριφορές από αγνώστους οι οποίοι επιθυμούν να έρθουν σε επαφή μαζί τους, να εκθέσουν άθελά τους πληροφορίες προσωπικών δεδομένων και να θέσουν τον εαυτό τους σε κίνδυνο χωρίς να γίνει αυτό άμεσα αντιληπτό. Από τα ανωτέρω συμπεραίνεται εύκολα ότι οι επικίνδυνες καταστάσεις στις οποίες μπορεί να βρεθεί ένα παιδί αλλά και ένας ευάλωτος χρήστης του παγκόσμιου ιστού, είναι πάρα πολλοί.

Τα οφέλη του διαδικτύου θα πρέπει να αποτελούν πρωταρχικό μέλημα και να αντισταθμίζονται έτσι όλα τα μειονεκτήματα που απορρέουν από όλες τις επικίνδυνες αυτές καταστάσεις. Αυτό μπορεί να γίνει εφικτό μέσω της σωστής ενημέρωσης και κατάρτισης των παιδιών, των γονέων και των εκπαιδευτικών. Η καθοδήγηση και η επιτήρηση των παιδιών, όσον αφορά τον παγκόσμιο ιστό και τις περαιτέρω υπηρεσίες του, αποτελεί βασικό στόχο των γονιών αλλά και των εκπαιδευτικών ώστε να ενισχύεται η ασφάλειά τους κατά τη δραστηριοποίησή τους στο διαδίκτυο. Για την έμπρακτη εφαρμογή των ανωτέρω, είναι επιτακτική η ανάγκη της ορθής ενημέρωσης επί των θεμάτων ασφάλειας και ελέγχου της πλοήγησης στον παγκόσμιο ιστό.

Επίσης, καλό είναι να αναφέρουμε ότι παρόλο την έξαρση του ηλεκτρονικού εγκλήματος στον παγκόσμιο ιστό, αυτό δε θα πρέπει να αποτελεί εμπόδιο και αιτία απαγόρευσης ή άρνησης από τους γονείς προς τα παιδιά ως προς τη πρόσβαση και τη χρήση υπηρεσιών του διαδικτύου, αλλά η σωστή ενημέρωση και η γνώση μεθόδων γονικού ελέγχου θα μπορέσει υπεύθυνα και σωστά να κατευθύνει τους μικρούς χρήστες στην ασφαλή και μη αλόγιστη χρήση του διαδικτύου.

Στόχος της διπλωματικής εργασίας

Η παρούσα διπλωματική εργασία αποσκοπεί στην ενημέρωση των παιδιών, των γονέων και των εκπαιδευτικών σε θέματα που άπτονται την ασφάλεια στον παγκόσμιο ιστό, το γονικό έλεγχο και τους κινδύνους του διαδικτύου. Η ενημέρωση γίνεται μέσω μιας ιστοσελίδας που δημιουργήθηκε για το σκοπό αυτό, με το όνομα *kidstaysafe*, όπου παρουσιάζονται τα θέματα που προαναφέραμε καθώς επίσης και μία σειρά από δραστηριότητες που βοηθούν τα παιδιά αλλά και τους μεγαλύτερους να γνωρίσουν με έναν πιο εύκολο και συνάμα διασκεδαστικό τρόπο τα οφέλη και τους κινδύνους του διαδικτύου.

Επίσης, όσον αφορά τους γονείς και τους εκπαιδευτικούς, στην ιστοσελίδα υπάρχει συγκεκριμένη ενότητα όπου γίνεται ενημέρωση σχετικά με τον τρόπο εφαρμογής του γονικού ελέγχου και της γενικότερης εποπτείας των ψηφιακών συσκευών που χρησιμοποιούν τα παιδιά και οι μαθητές. Η ενημέρωση αυτή εξειδικεύεται στα δύο πιο γνωστά λειτουργικά συστήματα (Microsoft Windows και Android) τα οποία χρησιμοποιούν οι περισσότερες ψηφιακές συσκευές (π.χ. ηλεκτρονικοί υπολογιστές, έξυπνα τηλέφωνα, tablet).

Για το λόγο αυτό, υπάρχει εκπαιδευτικό υλικό το οποίο καθοδηγεί βήμα-βήμα τον επισκέπτη στον τρόπο με τον οποίο μπορεί και ο ίδιος να ρυθμίσει και να εφαρμόσει το γονικό έλεγχο στις δικές του ψηφιακές συσκευές.

Δομή της διπλωματικής εργασίας

Η διπλωματική εργασία αποτελείται από τα παρακάτω επτά κεφάλαια:

- *Κεφάλαιο 1:* Στο πρώτο κεφάλαιο γίνεται μία εκτενή αναφορά για την πρόσβαση και τη χρήση του διαδικτύου από παιδιά, τις δραστηριότητές τους στο διαδίκτυο, ευκαιρίες που προκύπτουν από τη χρήση του διαδικτύου και τα οφέλη που αποκομίζουν από τη γενικότερη ενασχόλησή τους με τον παγκόσμιο ιστό και τον τεχνολογικό αλφαβητισμό. Επίσης, γίνεται μια αναφορά στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων – GDPR (General Data Protection Regulation) και την εφαρμογή του στην εκπαιδευτική διαδικασία.
- *Κεφάλαιο 2:* Το κεφάλαιο αυτό αφορά την περιγραφή των τεσσάρων δημοφιλέστερων μέσω κοινωνικής δικτύωσης που χρησιμοποιούν οι νέοι για την καθημερινή τους επικοινωνία. Το Facebook, το TikTok, το Viber, το και το Instagram. Γίνεται μια αναφορά στο κάθε ένα από αυτά επικεντρώνοντας κυρίως σε πλεονεκτήματα, στα οφέλη αλλά και στους κινδύνους που μπορούν να παρουσιαστούν από τη χρήση τους.
- *Κεφάλαιο 3:* Η θεματολογία του τρίτου κατά σειρά κεφαλαίου της διπλωματικής εργασίας επικεντρώνεται σε ζητήματα ασφάλειας του διαδικτύου τόσο για τα παιδιά όσο και τους γονείς και τους εκπαιδευτικούς. Επίσης, παρουσιάζονται οι κίνδυνοι που καραδοκούν πίσω από τις περισσότερες δραστηριότητες του παγκόσμιο ιστού και πως αυτοί μπορούν να γίνουν αντιληπτοί και να ληφθούν τα αναγκαία μέτρα για την πρόληψη και αντιμετώπισή τους.
- *Κεφάλαιο 4:* Το τέταρτο κεφάλαιο αφορά τον γονικό έλεγχο. Γίνεται μία εισαγωγή επεξήγησης του γονικού ελέγχου, τα είδη της γονικής διαμεσολάβησης, ο τρόπος εφαρμογής της από τους γονείς και τους εκπαιδευτικούς προς τα ανήλικα παιδιά και μαθητές καθώς και τα αντίστοιχα πλεονεκτήματα και μειονεκτήματα. Επιπλέον, παρουσιάζονται οι τρόποι με τους οποίους μπορεί να εφαρμοστεί ο γονικός έλεγχος στις ψηφιακές συσκευές που διαθέτουν λειτουργικό σύστημα Windows της Microsoft και Android.
- *Κεφάλαιο 5:* Στο σημείο αυτό της εργασίας γίνεται μια αναφορά στη νομοθεσία

που σχετίζεται με το διαδίκτυο, το ηλεκτρονικό έγκλημα και τις παράνομες δραστηριότητες που μπορούν να λάβουν χώρα στο παγκόσμιο ιστό. Αρχικά παρουσιάζεται η ελληνική νομοθεσία και στη συνέχεια η ευρωπαϊκή.

- *Κεφάλαιο 6*: Στο κεφάλαιο αυτό γίνεται μια περιγραφή των εργαλείων που χρησιμοποιήθηκαν για τη δημιουργία της ιστοσελίδας *kidstaysafe* και στη συνέχεια αναλύεται και παρουσιάζεται ο τρόπος με τον οποίο σχεδιάστηκε και αναπτύχθηκε η εν λόγω ιστοσελίδα.
- *Κεφάλαιο 7*: Στο έβδομο και τελευταίο κεφάλαιο της παρούσης διπλωματικής εργασίας γίνεται μία ανασκόπηση της θεματολογίας, που πραγματεύονται τα προηγούμενα κεφάλαια και κατατίθενται προτάσεις που θα μπορούσαν να αποτελέσουν υλικό μελλοντικής έρευνας.

1. Πρόσβαση των παιδιών στο διαδίκτυο

Είναι γενικά αποδεκτό ότι το διαδίκτυο αποτελεί αναπόσπαστο κομμάτι της σύγχρονης κοινωνίας. Κάθε ένας ο οποίος διαθέτει είτε έναν προσωπικό ηλεκτρονικό υπολογιστή είτε ένα έξυπνο κινητό τηλέφωνο (smartphones, tablets) μπορεί να έχει πρόσβαση στον παγκόσμιο ιστό.

Το περιβάλλον του διαδικτύου αποτελείται τόσο από ενήλικους χρήστες όσο και από ανήλικους. Η πρόσβαση στο διαδίκτυο από τα μικρά παιδιά θεωρείται πλέον δεδομένη.

Τα οφέλη που αποκομίζουν τα παιδιά από τη πλοήγηση στο διαδίκτυο είναι πάρα πολλά. Όμως, η ευρεία χρήση του διαδικτύου από τις μικρές ηλικίες εγκυμονεί πολλούς κινδύνους από τους οποίους θα πρέπει να αποφύγουν και να προστατευτούν ώστε να αποτραπούν οι όποιες δυσάρεστες συνέπειες.

1.1 Χρήση του Διαδικτύου από παιδιά

Στον εικονικό κόσμο του Διαδικτύου, όπως και στον πραγματικό κόσμο, τα οφέλη που αποκομίζονται σχετίζονται άμεσα με κινδύνους. Δηλαδή, κάτι το οποίο εμφανίζεται ως ευκαιρία μπορεί συγχρόνως να αποτελεί και μια απειλή. Ειδικότερα στον παγκόσμιο ιστό δεν είναι εύκολα διακριτό αν μια εφαρμογή είναι ωφέλιμη ή επικίνδυνη.

Για να γίνει κατανοητή η παρουσία του γονικού ελέγχου στο περιβάλλον του παγκόσμιου ιστού, θα πρέπει πρώτα να ερευνήσουμε τη συμπεριφορά των μικρών παιδιών στο διαδίκτυο [1]. Έρευνες που έχουν πραγματοποιηθεί σε διεθνές επίπεδο (π.χ. EU Kids Online), έχουν δείξει ότι οι αρνητικές επιπτώσεις της χρήσης του διαδικτύου από τα παιδιά, αφορούν κυρίως κινδύνους εικόνων (π.χ. ακατάλληλου περιεχομένου) και κινδύνους που σχετίζονται με την επικοινωνία όπως για παράδειγμα λήψη ανεπιθύμητης αλληλογραφίας και μηνυμάτων από αγνώστους. Στον αντίποδα, τα θετικά οφέλη και οι ευκαιρίες που αποκομίζονται από την πλοήγηση των νέων στο διαδίκτυο αφορούν κυρίως τη μάθηση και την ανάπτυξη δεξιοτήτων επικοινωνίας και συμπεριφοράς.

Όσον αφορά τα οφέλη αλλά και τους κινδύνους που απορρέουν από την συμμετοχή των παιδιών στον παγκόσμιο ιστό, υπάρχουν σχετικές μελέτες και αναφορές τόσο στην Ευρώπη όσο και στις Ηνωμένες Πολιτείες Αμερικής.

Όμως, η έρευνα για τα μικρότερα παιδιά και η πρόσβασή τους στο διαδίκτυο είναι πιο σπάνια, αλλά λόγω ότι υπάρχει τελευταία μια αύξηση της χρήσης συσκευών που έχουν πρόσβαση στο διαδίκτυο από παιδιά όπως για παράδειγμα έξυπνα τηλέφωνα (smartphones) και tablets, έχει αρχίσει να επεκτείνεται.

1.2 Δραστηριότητες παιδιών μικρής ηλικίας στο διαδίκτυο

Οι νέες τεχνολογίες και ο ψηφιακός κόσμος τους παγκόσμιου ιστού αποτελούν πλέον αναπόσπαστο κομμάτι του σύγχρονου τρόπου ζωής και ειδικότερα των νέων. Τα παιδιά, από πολύ μικρή ηλικία εισέρχονται στον ψηφιακό αυτό κόσμο μέσα από δραστηριότητες ψηφιακής τεχνολογίας. Όπως προαναφέραμε, η ενασχόληση των παιδιών με το διαδίκτυο εγκυμονεί πολλούς κινδύνους. Όμως, σωστό και πρέπον είναι να αναφέρουμε και να γνωρίσουμε τα θετικά οφέλη του διαδικτύου στις μικρές ηλικίες και πως η ενασχόληση με αυτό μπορεί να έχει επηρεάσει θετικά τον τρόπο ζωής τους.

Επίσης, είναι καλό να κατανοήσουμε ότι ενασχόληση αυτή με τις νέες τεχνολογίες και συγκεκριμένα με το διαδίκτυο, δεν μπορούν εύκολα να κατηγοριοποιηθούν σε «ακίνδυνες» και «επικίνδυνες» [2]. Όσον αφορά την κοινωνική δικτύωση, τα παιδιά αποκομίζουν θετικές γνώσεις μέσα από επικίνδυνες δραστηριότητες (S. Livingstone). Παρόλο που οι δραστηριότητες αυτές έχουν τον χαρακτηρισμό του «κινδύνου», η συμβολή τους στο τομέα της εκπαιδευτικής διαδικασίας αλλά και της παιδείας εν γένει είναι σημαντική.

Μέσα από διάφορες μελέτες και έρευνες που έχουν πραγματοποιηθεί έχει παρατηρηθεί ότι η πρόσβαση των νέων στον παγκόσμιο ιστό αφορά δραστηριότητες όπως την κοινωνική δικτύωση, τη λήψη φωτογραφιών και αρχείων μουσικής αλλά και δραστηριότητες που σχετίζονται με την εκπαιδευτική διαδικασία (π.χ. εργασίες, τηλεκπαίδευση κλπ.). Οι δραστηριότητες όμως μέσω του διαδικτύου στα παιδιά μικρότερης ηλικίας είναι πιο περιορισμένη. Σύμφωνα με τη Sonia Livingstone η ενασχόληση των μικρότερων σε ηλικία παιδιών με το διαδίκτυο διαδραματίζεται γύρω από την εκπαίδευση, ψυχαγωγία, και παιχνίδια ψυχαγωγικού και εκπαιδευτικού χαρακτήρα. Όσο μικρότερη είναι η ηλικία τόσο οι δραστηριότητες στο διαδίκτυο επικεντρώνονται γύρω από ψυχαγωγικά παιχνίδια και βίντεο. Ενώ όταν αναφερόμαστε σε παιδιά μεγαλύτερης ηλικίας οι δραστηριότητες και η χρήση του διαδικτύου αφορούν περισσότερο την κοινωνική δικτύωση και τη μουσική.

Σύμφωνα με έρευνες, παιδιά ηλικίας του δημοτικού που χρησιμοποιούν τον παγκόσμιο ιστό και τις νέες τεχνολογίες γενικότερα, στο μέλλον η χρήση τους θα έχει αυξητικές τάσεις. Επίσης, για το λόγω ότι όλο και περισσότερα μικρά παιδιά ασχολούνται με τα μέσα κοινωνικής δικτύωσης, δημιουργείται η ανάγκη για ανάπτυξη ασφαλών τρόπων πλοήγησης και συμμετοχής στα μέσα αυτά. Είναι αξιοσημείωτο ότι τα παιδιά αυτής της ηλικιακής ομάδας αποκρύπτουν τα πραγματικά τους στοιχεία και κυρίως την ηλικία τους όταν πρόκειται να ανοίξουν για πρώτη φορά λογαριασμό στα μέσα κοινωνικής δικτύωσης.

1.3 Ευκαιρίες και οφέλη που προκύπτουν από τη χρήση του διαδικτύου από παιδιά

Η ταχεία εξάπλωση ψηφιακών εφαρμογών λόγω της ραγδαίας ανάπτυξης των νέων τεχνολογιών και η ευρεία χρήση ηλεκτρονικών υπολογιστών, έξυπνων τηλεφώνων (smartphones) και tablets, έχει ως αποτέλεσμα την αύξηση της χρήσης του διαδικτύου από παιδιά δημοτικού. Ο ενθουσιασμός που προκύπτει από τη χρήση νέων εφαρμογών και ψηφιακών δραστηριοτήτων ωθούν ολοένα και περισσότερο τις μικρότερες ηλικίες στη χρήση του διαδικτύου [2]. Τα παιδιά πλέον αντιλαμβάνονται ότι όσο συχνότερα χρησιμοποιούν το διαδίκτυο, τόσα περισσότερα είναι και τα οφέλη που αποκομίζουν.

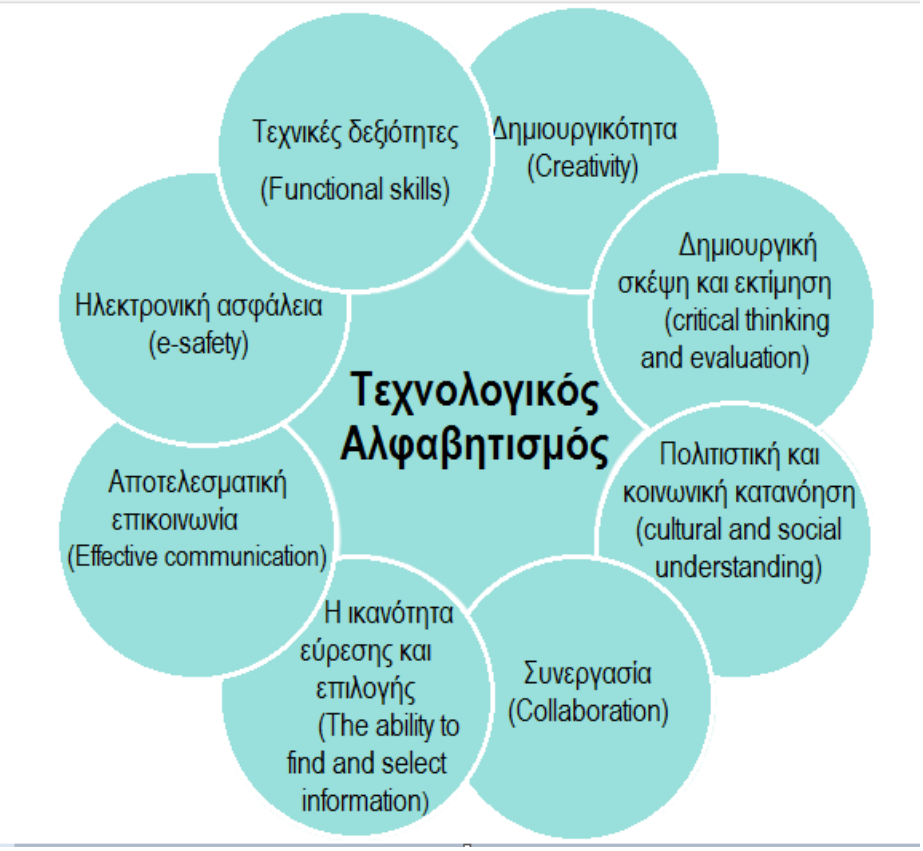
Οι ψηφιακές δεξιότητες [2] που αναπτύσσονται αλλά και οι ευκαιρίες που παρουσιάζονται από τη χρήση του παγκόσμιου ιστού από παιδιά είναι πάρα πολλές. Όμως, το «κυνήγι» των ευκαιριών που προκύπτουν από τη συνεχή χρήση του διαδικτύου χρειάζεται μια ιδιαίτερη προσοχή διότι οι «ευκαιρίες» αυτές που παρουσιάζονται δεν είναι πάντοτε ωφέλιμες για τα παιδιά.

Για το εάν οι «ευκαιρίες» αυτές είναι ωφέλιμες ή όχι, απόκειται πρωτίστως από την ηλικία, την οικονομική και κοινωνική κατάσταση του παιδιού αλλά και κατά πόσο έχουν υποστήριξη από το οικογενειακό και σχολικό τους περιβάλλον.

1.4 Ανάπτυξη ψηφιακών δεξιοτήτων των παιδιών από την ενασχόλησή τους με το διαδίκτυο

Η ανάπτυξη ψηφιακών δεξιοτήτων των παιδιών είναι ίσως από τους βασικότερους λόγους που η ενασχόληση τους με το διαδίκτυο έχει θετική επίδραση.

Συχνά συναντάται ο όρος «τεχνολογικός αλφαβητισμός» ή και «ψηφιακός - πληροφοριακός αλφαβητισμός» [3] ο οποίος αποτελείται από τα παρακάτω αλληλοεξαρτώμενα στοιχεία:



Εικόνα 1: *Τεχνολογικός Αλφαβητισμός*

- Τεχνικές δεξιότητες (functionals kills)
- Δημιουργικότητα
- Δημιουργική σκέψη και εκτίμηση (critical thinking and evaluation)
- Πολιτιστική και κοινωνική κατανόηση (cultural and social under standing)
- Συνεργασία
- Η ικανότητα εύρεσης και επιλογής
- Αποτελεσματική επικοινωνία
- Ηλεκτρονική ασφάλεια (e-safety)

Οι δεξιότητες αυτές του τεχνολογικού αλφαβητισμού ορίζουν με υπευθυνότητα την ασφαλέστερη πρόσβαση στις νέες τεχνολογίες.

Στο σημείο αυτό θεωρήθηκε σωστό να γίνει μια αναφορά στους κανόνες προστασίας προσωπικών δεδομένων.

1.5 Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων – GDPR (General Data Protection Regulation)

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων, (General Data Protection Regulation – GDPR), δείχνει τον τρόπο στις επιχειρήσεις και στους οργανισμούς με τον οποίο μπορούν να συγκεντρώσουν, να επεξεργαστούν, να επιμεληθούν και να χειριστούν τα προσωπικά δεδομένα. Ο κανονισμός GDPR είναι

αυτός που ορίζει τον τρόπο με τον οποίο μπορούμε να φυλάξουμε τα προσωπικά μας δεδομένα καθώς επίσης ορίζει και τις περιπτώσεις στις οποίες εταιρείες ή και οργανισμοί έχουν τη δυνατότητα να τα χρησιμοποιήσουν, να τα συσσωρεύσουν για φύλαξη, να τα ακυρώσουν και να τα σβήσουν και στο τέλος να τα τροποποιήσουν. Ο κανονισμός GDPR έχει επήρεια σε κάθε επιχείρηση που βρίσκεται στην Ευρωπαϊκή Ένωση και η οποία διευθετεί υποθέσεις σχετικά με τα προσωπικά δεδομένα. Οι κανονισμοί και οι μέθοδοι που ισχύουν είναι σύνθετοι και περίπλοκοι καθώς υπάρχουν αυστηρές ποινές για τη μη υπακοή.

Όσον αφορά τα προσωπικά δεδομένα [4], είναι όλες εκείνες οι πληροφορίες οι οποίες μπορούν να ταυτοποιήσουν έναν άνθρωπο. Οι πληροφορίες αυτές είναι μοναδικές για κάθε ένα άτομο και ο κανονισμός GDPR ορίζει τους τρόπους προστασίας των δεδομένων αυτών ανεξάρτητα από το ψηφιακό μέσο στο οποίο χρησιμοποιούνται.

Στη συνέχεια γίνεται μία αναφορά των πιο χαρακτηριστικών προσωπικών δεδομένων που συναντώνται στον παγκόσμιο ιστό:

- Ονοματεπώνυμο
- Ηλικία
- Φύλο
- Τόπος κατοικίας (π.χ. διεύθυνση)
- Αριθμός τηλεφώνου
- Δεδομένα προσωπικού ιατρικού ιστορικού
- Διεύθυνση ηλεκτρονικού ταχυδρομείου
- Τοποθεσία (π.χ. ορισμός θέσης κινητών τηλεφώνων)
- Διεύθυνση IP ψηφιακής συσκευής

Όσον αφορά το διαδίκτυο και τους ασφαλέστερους τρόπους πλοήγησης, ο κανονισμός GDPR έχει τροποποιηθεί αναλόγως.

Οι νέες αλλαγές αφορούν τα παρακάτω:

- Υπεράσπιση των δικαιωμάτων που αφορούν τα παιδιά: Η χρήση των κοινωνικών δικτύων δεν επιτρέπεται σε παιδιά κάτω των δεκαέξι ετών, εκτός αν υπάρχει η σύμφωνη γνώμη των γονέων. Στην Ελλάδα, το ηλικιακό όριο των παιδιών που σχετίζεται με τη γονική συναίνεση ορίζεται στην ηλικία των δεκαπέντε ετών.
- Προσωπικά Δεδομένα: Ο κάθε χρήστης έχει τη δυνατότητα, ύστερα από αίτησή του, να σβηστούν τα προσωπικά του δεδομένα και ο διαχειριστής είναι υποχρεωμένος να τα σβήσει καθώς επίσης και να ενημερώσει σχετικώς σε όλους όσους έχουν κοινοποιηθεί.
- Ενημέρωση για τα προσωπικά δεδομένα: Υπάρχει πληρέστερη ενημέρωση του χρήστη σε θέματα που αφορούν την επεξεργασία, συλλογή και διαχείριση των προσωπικών του δεδομένων.

- Αλλαγή στοιχείων: Ο χρήστης έχει τη δυνατότητα να ζητήσει από το διαχειριστή να βελτιώσει και να αποκαταστήσει τυχόν στοιχεία τα οποία δεν είναι ακριβή καθώς επίσης και να διορθώσει συμπληρώνοντας καθορισμένα στοιχεία τα οποία δεν είναι πλήρη και ολοκληρωμένα τα οποία σχετίζονται με αυτόν.
- Απαγόρευση επεξεργασίας στοιχείων: Ο χρήστης έχει το προνόμιο να αρνηθεί και να μην επιτρέψει τη διαχείριση των προσωπικών του δεδομένων κάτω από εξειδικευμένες περιπτώσεις κυρίως όταν έγκειται η τροποποίηση και επεξεργασία της καρτέλας των προσωπικών του στοιχείων.

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων, ολόκληρος και γραμμένος στα ελληνικά, βρίσκεται αναρτημένος στην επίσημη εφημερίδα της Ευρωπαϊκής Ένωσης. (eur-lex.europa.eu/)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι κατοχυρωμένη από το Ελληνικό Σύνταγμα [5]. Μερικές από τις αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, είναι οι διοικητικοί έλεγχοι, η μελέτη σχετικών κατηγοριών και διαβημάτων που σχετίζονται με την εκτέλεση και εφαρμογή της νομοθεσίας και την προστασία των προσωπικών δεδομένων αυτών που αναφέρονται όταν τα τελευταία επιφέρουν ζημία και προσβάλλονται από την επεξεργασία των δεδομένων.

1.6 Εφαρμογή των κανόνων του Γενικού Κανονισμού GDPR στην εκπαίδευση

Ο Γενικός κανονισμός προστασίας προσωπικών δεδομένων εφαρμόζεται σε όλους τους τομείς της κοινωνίας. Όσον αφορά τον ευαίσθητο τομέα της εκπαίδευσης ο κανονισμός GDPR [6] εφαρμόζεται σε θέματα όπως σε:

- Προσωπικά δεδομένα τα οποία είναι σχετικά με το σχολείο, μαθητές, κηδεμόνες, εκπαιδευτικό προσωπικό, π.χ. ονοματεπώνυμα, τόπος κατοικίας, φύλο, αριθμό τηλεφώνου, δεδομένα προσωπικού ιατρικού ιστορικού, στοιχεία επικοινωνίας γονέων.
- Δεδομένα που αφορούν τα βιομετρικά στοιχεία μαθητών και εκπαιδευτικού προσωπικού.
- Διατροφικές συνήθειες και ιδιαιτερότητες μαθητών.
- Πληροφορίες στην εκπαίδευση π.χ. λίστα των τάξεων με τους μαθητές, διαγωνίσματα, αξιολογήσεις.
- Εγγραφές μαθητών, εκπαιδευτικών, διοικητικού προσωπικού, π.χ. αρχείο μισθοδοσίας εκπαιδευτικών, αδειών και αρχείο αξιολόγησης, ιατρικό ιστορικό μαθητών.
- Οποιαδήποτε άλλες πληροφορίες ή δεδομένα που μπορούν να δημοσιοποιηθούν από μαθητές, γονείς, εκπαιδευτικούς ή άλλους φορείς της εκπαίδευσης.

2. Κοινωνική δικτύωση

Με τον όρο Κοινωνική Δικτύωση [7] καθορίζεται η ομαδική συμμετοχή ατόμων σε ένα δίκτυο με σκοπό την μεταξύ τους επικοινωνία. Σήμερα, τα δίκτυα αυτά αποτελούν το βασικότερο εργαλείο της καθημερινής επικοινωνίας όλων των ανθρώπων και κυρίως των νέων.

Τα Μέσα Κοινωνικής Δικτύωσης αφορούν όλες εκείνες τις πλατφόρμες οι οποίες διαχειρίζονται τις προαναφερθείσες ομάδες και δημιουργούν τις κατάλληλες συνθήκες μέσα από συγκεκριμένους κανόνες και οδηγίες ώστε τα άτομα που συμμετέχουν να μπορούν να αλληλεπιδρούν και να επικοινωνούν.

Το ιδιαίτερο χαρακτηριστικό των μέσων κοινωνικής δικτύωσης είναι η εύκολη και γρήγορη επικοινωνία και διάδοση των πληροφοριών με βασικό γνώρισμα την επίτευξη ζεύξης «σημείο προς σημείο» [8] των χρηστών.

Στον παγκόσμιο ιστό υπάρχει μια πληθώρα εφαρμογών κοινωνική δικτύωσης οι οποίες είναι προσβάσιμες στον απλό χρήστη. Στη συνέχεια γίνεται μια παρουσίαση των τεσσάρων δημοφιλέστερων μέσων κοινωνικής δικτύωσης που χρησιμοποιούνται κυρίως από άτομα νεαρής ηλικίας για τη καθημερινή τους επικοινωνία. Τα μέσα αυτά είναι το Facebook, το Tik Tok, το Viber και το Instagram.

2.1 Facebook

Το Facebook [https://about.facebook.com/] αποτελεί ένα από τα πιο διαδεδομένα μέσα κοινωνικής δικτύωσης. Έκανε την εμφάνισή του στις 4 Φεβρουαρίου 2004 από την εταιρία Facebook Inc. η οποία στις 28 Οκτωβρίου 2021 μετονομάστηκε σε Meta Platforms Inc. και είναι ιδιαίτερα δημοφιλής στις νεαρές ηλικίες.

Η εγγραφή στην εν λόγω πλατφόρμα κοινωνικής δικτύωσης είναι δωρεάν. Για τη δημιουργία νέου λογαριασμού ο χρήστης πρέπει να καταχωρίσει τα προσωπικά του στοιχεία όπως ονοματεπώνυμο, διεύθυνση ηλεκτρονικού ταχυδρομείου, ημερομηνία γέννησης, τόπο κατοικίας κλπ. Αν και η ίδια η πλατφόρμα ορίζει ότι για να αποκτήσει κάποιος λογαριασμό στο facebook θα πρέπει να είναι άνω των δεκατριών ετών, παρόλα αυτά, ο οποιοσδήποτε μπορεί να δηλώσει μια ψεύτικη ηλικία και να δημιουργήσει έναν λογαριασμό χωρίς να μπορεί το facebook να εξακριβώσει τη πιστότητα των δηλωμένων στοιχείων.

Εφόσον, δημιουργηθεί επιτυχώς ο λογαριασμός, ο χρήστης έχει τη δυνατότητα να αναζητήσει και να προσκαλέσει άλλους φίλους με την βασική όμως προϋπόθεση ότι και αυτοί είναι μέλη στο Facebook. Αξιοσημείωτο είναι ότι ως μέλη του facebook μπορεί να είναι άτομα από οποιαδήποτε χώρα του κόσμου.

Η επικοινωνία μεταξύ των χρηστών [9] γίνεται μέσω ανταλλαγής μηνυμάτων, βιντεοκλήσεων, διαμοιρασμού φωτογραφιών, βίντεο κ.α.

Κίνδυνοι & Τρόποι Αντιμετώπισης

- **Ασφάλεια προσωπικών δεδομένων**

Υπάρχει μεγάλος κίνδυνος να κοινοποιηθούν προσωπικά δεδομένα αλλά και των δραστηριοτήτων σε άλλους χρήστες. Για το λόγο αυτό μέσω της επιλογής «Αρχείο δραστηριοτήτων» στις ρυθμίσεις του facebook, ο χρήστης μπορεί να επεξεργαστεί το περιεχόμενο και τα δεδομένα του προσωπικού του προφίλ που κοινοποιούνται σε άλλους χρήστες μέσω του χρονολογίου του. Επίσης, μέσω της επιλογής αυτής, μπορεί να απαγορεύσει ολοκληρωτικά άλλους χρήστες ώστε να μην έχουν πρόσβαση στις δημοσιεύσεις .

- **Αίτημα φιλίας και συνομιλία με άγνωστους χρήστες**

Τα αιτήματα φιλίας που γίνονται από ανθρώπους που δεν γνωρίζουμε είναι καλό να αποφεύγονται. Ειδικότερα, όταν ο χρήστης του facebook είναι ανήλικος τα αιτήματα φιλίας θα πρέπει να απορρίπτονται και να ενημερώνονται οι γονείς όταν γίνονται από αγνώστους.

Επίσης, στη περίπτωση που κάποιος άγνωστος επιδιώκει συνάντηση με τον χρήστη εκτός του facebook ή 'ενοχλεί' μέσω μηνυμάτων συνομιλίας, τότε θα πρέπει να ενημερωθεί άμεσα ο γονέας και να διαγραφεί από τη λίστα με τους φίλους.

- **Διαδικτυακός εκφοβισμός (Cyberbullying)**

Η ανάρμοστη συμπεριφορά χρηστών και σελίδες με ακατάλληλο ή και επικίνδυνο περιεχόμενο αποτελούν κατηγορίες περιπτώσεων όπου οι χρήστες μπορούν να βρεθούν αντιμέτωποι στο facebook.

Για αυτές τις περιπτώσεις και για την άμεση αντιμετώπισή τους συνίσταται η αναφορά (report) αυτών των φαινομένων από τον χρήστη στο facebook. Το σημαντικό είναι ότι η αναφορά είναι ανώνυμη και δεν υπάρχει ο κίνδυνος κοινοποίησης των προσωπικών στοιχείων του χρήστη.

Όσον αφορά περισσότερο το θέμα της προστασίας και της ασφάλειας ιδιαιτέρως των ανηλίκων, το «Κέντρο Βοήθειας» του Facebook παρέχει εμπεριστατωμένη ενημέρωση προς τους χρήστες αλλά και προς τους γονείς και καθοδηγεί διαμέσου συγκεκριμένων λειτουργιών και ρυθμίσεων ώστε να διασφαλίζεται η προστασία του εκάστοτε χρήστη.

2.2 Tik Tok

Το Tik Tok είναι μια πλατφόρμα κοινωνικής δικτύωσης [10] όπου συνδέει τη μουσική με την επικοινωνία. Είναι μία πλατφόρμα στην οποία ο χρήστης δημιουργεί προσωπικά βίντεο, μικρής διάρκειας, για να αλληλεπιδράσει με άλλους χρήστες.

Είναι προφανές ότι η λειτουργία και ο σκοπός του είναι διαφορετικός σε σχέση με το facebook.

Η δημιουργία χρήστη στην εν λόγω πλατφόρμα είναι δωρεάν και μπορεί να γίνει είτε με προσωπικό λογαριασμό ηλεκτρονικού ταχυδρομείου είτε χρησιμοποιώντας τους ήδη υπάρχοντες λογαριασμούς στα άλλα μέσα κοινωνικής δικτύωσης όπως το Facebook, Instagram κλπ.

Μετά τη δημιουργία του λογαριασμού, οι χρήστες επιλέγουν μουσικά κομμάτια καραόκε, μέσα από μία μεγάλη λίστα που διατίθεται από την πλατφόρμα. Επίσης, υπάρχει μία πληθώρα εφαρμογών με εδικά φίλτρα όπου μπορεί να επιλέξει ο χρήστης για να δημιουργήσει διασκεδαστικά βίντεο.

Τα αυτοδημιούργητα βίντεο που παράγονται, οι χρήστες μπορούν να τα δημοσιοποιήσουν στους “φίλους” τους, αλλά μπορούν και να τα κοινοποιήσουν και σε άλλα μέσα κοινωνικής δικτύωσης.

Στο Tik Tok οι υπόλοιποι χρήστες μπορούν να σχολιάσουνε τα βίντεο που κοινοποιούνται, να δηλώσουν ότι τους άρεσαν (like) ή ακόμα και να τα χρησιμοποιήσουν ώστε να δημιουργήσουν δικά τους βίντεο.

<u>Κίνδυνοι & Τρόποι Αντιμετώπισης</u>

Σύμφωνα με το Κέντρο Ασφαλείας του Tik Tok [https://www.tiktok.com/about], οι κίνδυνοι που απορρέουν από τη χρήση του και θα πρέπει να προσέχουν ιδιαιτέρως οι ανήλικοι χρήστες είναι:

- **Επικοινωνία και επαφή με άγνωστους χρήστες**

Στην πλατφόρμα του Tik Tok όλοι οι λογαριασμοί είναι εξορισμού προσβάσιμοι από οποιονδήποτε χρήστη της πλατφόρμας. Για το λόγο αυτό είναι απαραίτητο, κυρίως στους ανήλικους χρήστες, να προστατεύσουν το λογαριασμό τους κάνοντάς τον “ιδιωτικό” με την ενεργοποίηση της σχετικής επιλογής.

- **Διαδικτυακός εκφοβισμός (Cyberbullying)**

Υπάρχει μεγάλη πιθανότητα οι χρήστες να μετατραπούν σε θύματα διαδικτυακού εκφοβισμού και ανάρμοστης συμπεριφοράς ή να βρεθούν αντιμέτωποι με υλικό το οποίο είναι ακατάλληλο για την ηλικία τους.

Ο τρόπος ώστε να αποφευχθούν περιστατικά εκφοβισμού γίνεται μέσω της

αναφοράς ή του μπλοκαρίσματος άλλου χρήστη ή χρηστών ώστε να μην μπορούν να έχουν πρόσβαση στα περιεχόμενα του λογαριασμού.

Για την αντιμετώπιση των φαινομένων ακατάλληλου υλικού ο χρήστης θα πρέπει να ενεργοποιήσει τη λειτουργία περιορισμού με την οποία αποκλείονται τα βίντεο των οποίων το περιεχόμενο δεν είναι κατάλληλο για όλες τις ηλικίες.

- **Υπερβολική χρήση του Tik Tok**

Για να αντιμετωπιστεί το φαινόμενο της πολύωρης χρήσης της πλατφόρμας, στο Tik Tok υπάρχει σχετική επιλογή με την οποία ο χρήστης έχει τη δυνατότητα να ελέγξει το χρόνο που αφιερώνει στη χρήση της εφαρμογής. Με την ενεργοποίηση της επιλογής αυτής, ο χρόνος χρήσης μπορεί να περιοριστεί αναλόγως, όπως για παράδειγμα έως στις δύο ώρες την ημέρα.

2.3 Viber

Άλλη μια δημοφιλής πλατφόρμα είναι το Viber [11]. Είναι μια εφαρμογή επικοινωνίας τύπου messenger, είτε για ηλεκτρονικούς υπολογιστές είτε για έξυπνα τηλέφωνα (smartphones) και tablet. Αποτελεί μια αξιόπιστη και ασφαλής λύση δωρεάν επικοινωνίας, μέσω του παγκόσμιου ιστού, σε όλον τον κόσμο και είναι ιδιαίτερα δημοφιλής στην καθημερινή επικοινωνία συμπεριλαμβανομένου τις νεαρές ηλικίες.

Μετά την εγκατάσταση της εφαρμογής στη ψηφιακή μας συσκευή και τη δημιουργία λογαριασμού στη πλατφόρμα, ο χρήστης, μπορεί να επικοινωνεί με άλλους χρήστες του Viber μέσω της αποστολής γραπτών μηνυμάτων, βιντεοκλήσεων, ανταλλαγή αρχείων (εικόνα, βίντεο κ.α.).

Το Viber δικαίως θεωρείται ως από τα πιο ασφαλή μέσα κοινωνικής δικτύωσης καθώς τα προσωπικά δεδομένα των χρηστών προστατεύονται και σύμφωνα με τον γενικό κανονισμό προστασίας προσωπικών δεδομένων (GDPR).

<u>Κίνδυνοι & Τρόποι Αντιμετώπισης</u>

Όσον αφορά τους κινδύνους που καραδοκούν, το Viber [https://www.viber.com/en/about/] προτείνει συμβουλευτικά στους χρήστες να τηρούν τα κάτωθι:

1. Ο τηλεφωνικός αριθμός είναι το βασικό στοιχείο αναζήτησης χρηστών στη πλατφόρμα του Viber. Μόνο μέσω του τηλεφωνικού αριθμού μπορεί κάποιος να βρει το προφίλ ενός χρήστη της πλατφόρμας. Για το λόγο αυτό θα πρέπει να αποφεύγεται η κοινοποίηση του προσωπικού τηλεφωνικού αριθμού σε αγνώστους ώστε να αποτρέπονται φαινόμενα παρενόχλησης μέσω ανεπιθύμητων μηνυμάτων.

2. Στη περίπτωση εκείνη όπου άγνωστοι χρήστες παρενοχλούν είτε μέσω κλήσεων είτε μέσω μηνυμάτων με προσβλητικό περιεχόμενο, τότε ο

χρήστης μπορεί να διακόψει την επικοινωνία αυτή ενεργοποιώντας την επιλογή του αποκλεισμού η οποία είναι διαθέσιμη στις πληροφορίες κάθε συνομιλίας. Εάν ο χρήστης που λαμβάνει ενοχλητικά μηνύματα είναι ανήλικος τότε θα πρέπει άμεσα να ενημερώσει του γονείς του για να εφαρμόσουν τη παραπάνω διαδικασία.

3. Όταν γίνεται προσθήκη ενός νέου αριθμού τηλεφώνου στη λίστα επαφών στο Viber, θα πρέπει να ελέγχεται εάν ο αριθμός αυτός ανταποκρίνεται στα προσωπικά στοιχεία του κατόχου του και δεν είναι αποτελεί κάποιο ψεύτικο προφίλ ενός αγνώστου που επιθυμεί να έρθει σε επικοινωνία με τον χρήστη.

4. Ένα σημαντικό στοιχείο ασφάλειας της επικοινωνίας που είναι κύριο χαρακτηριστικό της πλατφόρμας του Viber είναι η κρυπτογράφηση «από άκρο σε άκρο» (endtoend – E2EE). Αυτό ενισχύει την ασφάλεια καθώς η επικοινωνία πραγματοποιείται μόνο από χρήστη σε χρήστη. Με αυτό τον τρόπο οι πληροφορίες που ανταλλάσσονται μεταξύ αυτών των δύο χρηστών δεν μπορούν να είναι ορατές από άλλους (ούτε και από τους servers του Viber) και μόνο αυτοί οι δύο χρήστες έχουν την πρόσβαση και τη διαχείρισή τους.

5. Ο κάθε χρήστης της πλατφόρμας του Viber είναι ο υπεύθυνος για την προστασία των προσωπικών του δεδομένων και πληροφοριών. Αυτό συνεπάγεται ότι η κοινοποίηση και δημοσίευση προσωπικών στοιχείων αλλά και φωτογραφιών ή βίντεο μέσω της πλατφόρμα σε άλλους χρήστες εξαρτάται αποκλειστικά και μόνο από τον ίδιο τον χρήστη.

2.4 Instagram

Τα τελευταία χρόνια η ανάγκη για διαμοιρασμό προσωπικών φωτογραφιών μεταξύ των χρηστών των μέσων κοινωνικής δικτύωσης οδήγησε στη δημιουργία μιας πλατφόρμας που βασικό σκοπό έχει τη λήψη καθώς και τον διαμοιρασμό των φωτογραφιών εύκολα και γρήγορα. Η πλατφόρμα αυτή είναι το «Instagram» [12].

Η δημιουργία λογαριασμού στη πλατφόρμα αυτή είναι παρόμοια με τα προαναφερθείσα μέσα κοινωνικής δικτύωσης [https://about.instagram.com/]. Απαραίτητη προϋπόθεση για την εγγραφή και χρήση στη πλατφόρμα του Instagram είναι η ηλικία των χρηστών να είναι μεγαλύτερη από δεκατριών χρονών. Σε περίπτωση που χρήστες εντοπίσουν κάποιον ο οποίος δεν πληρεί αυτή τη συγκεκριμένη υποχρέωση τότε τους δίνεται η δυνατότητα να αναφέρουν το εν λόγω περιστατικό.

Ο νέος χρήστης της πλατφόρμας του «Instagram» και ιδιαιτέρως οι ανήλικοι χρήστες θα πρέπει να δώσουν προσοχή στη κοινοποίηση των βασικών

πληροφοριών του προφίλ τους. Καλό είναι να αποφεύγεται όσο το δυνατόν περισσότερο η δημοσίευση προσωπικών δεδομένων.

Με την ενεργοποίηση της επιλογής του ιδιωτικού λογαριασμού, οι πληροφορίες του προσωπικού προφίλ είναι ορατές μόνο σε όσους επιθυμεί ο χρήστης. Επιπλέον, στις ρυθμίσεις του ιδιωτικού λογαριασμού ορίζεται από τον χρήστη για το ποιος θα μπορεί να τον ακολουθεί στις δημοσίευσης του και ποιος όχι. Έτσι, με αυτόν τον τρόπο ενισχύεται η ιδιωτικότητά του λογαριασμού και η προστασία από ξένους χρήστες.

Αξίζει να σημειωθεί ότι με την ενεργοποίηση της επιλογής ιδιωτικού λογαριασμού προστατεύεται ένα ακόμα ευαίσθητο στοιχείο της ιδιωτικότητας του χρήστη, οι προσωπικές φωτογραφίες.

Στη πλατφόρμα του Instagram δεν υπάρχει ξεχωριστεί ρύθμιση που να αφορά τον γονικό έλεγχο. Παρόλα αυτά, η ίδια η εφαρμογή δεν επιτρέπει την κοινοποίηση και διακίνηση άσεμνων φωτογραφιών. Όμως, έχει παρατηρηθεί το φαινόμενο αρκετοί χρήστες να δημοσιεύουν υλικό με ακατάλληλο για ανηλίκους περιεχόμενο.

Ένας γρήγορος τρόπος αντιμετώπισης και αποφυγής προβολής ακατάλληλων φωτογραφιών ή βίντεο είναι μέσω της επιλογής «*εμφάνιση λιγότερων δημοσιεύσεων σαν αυτή*» ώστε να σταματήσουν την μελλοντική εμφάνισης. Επίσης, μπορούν να το αναφέρουν στο Instagram για να προβεί στις απαραίτητες ενέργε ιες.

Για τους παραπάνω λόγους χρειάζεται ιδιαίτερη προσοχή από τη μεριά των γονέων οι οποίοι θα πρέπει να επιβλέπουν τη δραστηριότητα του παιδιού στο Instagram. Να ελέγχουν ποιους χρήστες ‘ακολουθεί’ ή ποιοι τον ‘ακολουθούν’, ώστε να μπορέσουν άμεσα να προλάβουν και να αντιμετωπίσουν τις όποιες επικίνδυνες καταστάσεις εμφανιστούν.

3. Ασφάλεια στο Διαδίκτυο

Αν θέλουμε να δώσουμε έναν ορισμό για τη λέξη «ασφάλεια» [13] θα λέγαμε ότι ασφάλεια είναι ο όρος της προστασίας από τον κίνδυνο ή την απώλεια. Είναι επίσης η αποφυγή από τον κίνδυνο ή της απειλής και η αίσθηση βεβαιότητας και σιγουριάς. Στην καθημερινότητα, η ασφάλεια ορίζεται σύμφωνα τον τομέα στον οποίο ο καθένας δραστηριοποιείται.

Αλλά και στο ευρύτερο κοινωνικό σύνολο, ο τρόπος που γίνεται αντιληπτός ο όρος της ασφάλειας είναι τελείως διαφορετικός. Για παράδειγμα, ένας μηχανικός πληροφορικής αλλιώς θα περιγράψει και θα οριοθετήσει τον όρο «ασφάλεια» όταν πρόκειται για ένα λογισμικό μια τράπεζας και διαφορετικά όταν πρόκειται για μια εγκατάσταση ενός δικτύου ηλεκτρονικών υπολογιστών.

Γενικότερα θα λέγαμε ότι η αναγνώριση και αποτροπή των κινδύνων και των απειλών αποτελεί σημείο σύγκλισης όλων όσων έχουν υπό την ευθύνη τους ως σκοπό την αποτροπή όλων εκείνων των επικίνδυνων καταστάσεων που θα μπορούσαν να επηρεάσουν την εργασία τους.

Όσον αφορά το διαδίκτυο, το θέμα της ασφάλειας [14] απευθύνεται σε όλους όσους δραστηριοποιούνται στον παγκόσμιο ιστό, είτε ως μεμονωμένα άτομα είτε συλλογικά.

Η πρόσβαση των νέων στον παγκόσμιο ιστό μέσα από μια πληθώρα συσκευών και σε συνάρτηση με την ανάπτυξη του ασύρματου δικτύου ευρείας περιοχής, η διασύνδεση με τις εφαρμογές διαδικτύου καθίσταται πλέον εφικτή σε οποιοδήποτε σημείο. Όμως, η ικανότητα αυτή της πρόσβασης στο διαδίκτυο εκτός από τα αναρίθμητα πλεονεκτήματα και οφέλη που προσφέρει έχει ως αποτέλεσμα και την αυξητική τάση των επικίνδυνων καταστάσεων.

Η απασχόληση των παιδιών για μεγάλα χρονικά διαστήματα με τις νέες ψηφιακές εφαρμογές του διαδικτύου είναι σχεδόν βέβαιο ότι θα τους φέρει αντιμέτωπους με κινδύνους, που αυτό συνεπάγεται δυσάρεστες συνέπειες.

Για το λόγο αυτό, ο εκάστοτε γονέας, προκείμενου να αποφύγει τις αρνητικές συνέπειες που απορρέουν από τη πλοήγηση των μικρών παιδιών στο διαδίκτυο [14], θα πρέπει να είναι σε θέση να διακρίνει και να αξιολογεί τους κινδύνους που παρουσιάζονται.

3.1 Εκπαιδευτικοί και ασφάλεια στο διαδίκτυο

Το βασικότερο ερώτημα που προκύπτει είναι για το πώς ο εκπαιδευτικός μπορεί να επηρεάσει και να διαμορφώσει τους τρόπους με τους οποίους οι μαθητές θα μπορούν να χρησιμοποιήσουν το διαδίκτυο με ασφάλεια.

Σκοπός του εκπαιδευτικού είναι να αποκαλύψει τους κινδύνους του διαδικτύου στους μαθητές ανεξαρτήτου ηλικίας και να τους μυήσει στους τρόπους

εντοπισμού και αντιμετώπισης των κινδύνων του διαδικτύου ώστε η πλοήγησή τους στον παγκόσμιο ιστό να γίνεται με ασφάλεια. Ο εκπαιδευτικός εκείνος που είναι σε θέση να εντοπίζει τις επικίνδυνες καταστάσεις και μπορεί να τις αντιμετωπίσει είναι υποχρεωμένος να βρίσκεται δίπλα στους μαθητές ως σύμβουλός τους και να τους καθοδηγεί στο πως να χρησιμοποιούν ορθά το διαδικτύου εντός αλλά και εκτός του σχολικού περιβάλλοντος.

Η χρήση των ψηφιακών εφαρμογών που σχετίζονται με την ασφάλεια στο διαδίκτυο και η απλή παρουσία του εκπαιδευτικού δεν είναι αρκετή. Η χρήση των εφαρμογών αυτών κατά την πλοήγηση στο διαδίκτυο, αν και είναι απαραίτητη κυρίως για τα μικρά παιδιά, έχει βοηθητικό χαρακτήρα.

Ο πρώτος ο οποίος θα είναι αποδέκτης όλων των απειλών του διαδικτύου και των νεοεμφανιζόμενων ψηφιακών εφαρμογών είναι ο μαθητής. Οπότε, από τα παραπάνω προκύπτει η ανάγκη: αρχικά ο εκπαιδευτικός να καταγράψει και να αναλύσει τις ανάγκες και τις δραστηριότητες των μαθητών που σχετίζονται με την πλοήγησή και το ενδιαφέρον για το διαδίκτυο και εκ των υστέρων να τους βοηθήσει να αντιμετωπίσουν τις όποιες φοβίες προκύψουν από την ενασχόλησή τους με αυτό.

Για να μπορέσουν οι μικροί μαθητές να απευθυνθούν στον εκάστοτε εκπαιδευτικό και να του εκμυστηρευτούν τον τρόπο που δραστηριοποιούνται στο διαδίκτυο θα πρέπει να είναι έντονο το αίσθημα της εμπιστοσύνης και της κατανόησης. Αυτό συνεπάγεται, από τη μεριά του εκπαιδευτικού, την άρτια ενημέρωση και γνώση του όσον αφορά την ασφάλεια, τους τρόπους αντιμετώπισης των κινδύνων και σε θέματα νέων τεχνολογιών και εργαλείων. Με αυτόν τον τρόπο θα μπορέσει να ενθαρρύνει τους μικρούς μαθητές ώστε και αυτοί με τη σειρά τους να δείξουν τη δέουσα εμπιστοσύνη και σεβασμό. Έτσι, θα μπορέσουν ευκολότερα να διδαχτούν και να γνωρίσουν τρόπους αντιμετώπισης των κινδύνων [14] που απορρέουν από την πλοήγησή τους στον παγκόσμιο ιστό.

Ειδικότερα, ο εκπαιδευτικός θα πρέπει να επικεντρωθεί περισσότερο στο:

- Να επικοινωνεί σε επίπεδο διαλόγου με τους μαθητές, στα πλαίσια του μαθήματος, για την πλοήγηση στον παγκόσμιο ιστό.
- Να παρουσιάσει στα παιδιά σελίδες οι οποίες το περιεχόμενό τους θα είναι προσαρμοσμένο στην εκάστοτε ηλιακή ομάδα και αντίστοιχο εκπαιδευτικό υλικό.
- Να επιστήσει την προσοχή στους μαθητές στο να μην αποκαλύπτουν ποτέ προσωπικές πληροφορίες και ατομικά στοιχεία.
- Να πραγματοποιεί τακτικούς ελέγχους σχετικά με τις σελίδες και τις δραστηριότητες των μαθητών κατά την πλοήγηση στο διαδίκτυο, μέσω του Ιστορικού και των Αγαπημένων που αποθηκεύονται στην εφαρμογή πλοήγησης (φυλλομετρητή).
- Να επιτηρεί τα παιδιά για όσο χρόνο χρησιμοποιούν το διαδίκτυο είτε όταν αυτά βρίσκονται στο εργαστήριο της πληροφορικής είτε στη τάξη.

Με την τήρηση των παραπάνω πρακτικών, οι μαθητές εκπαιδεύονται

βιωματικά στον τρόπο με τον οποίο μπορούν να πλοηγηθούν με ασφάλεια στο διαδίκτυο.

3.2 Ασφαλή χρήση του διαδικτύου στο σχολικό περιβάλλον

Σύγχρονες έρευνες έχουν δείξει ότι το σχολείο αποτελεί καθοριστικό παράγοντα στη διαμόρφωση της συμπεριφοράς των μαθητών που σχετίζεται με την ασφαλή χρήση του διαδικτύου και γενικότερα της ασφαλούς πλοήγησης στο διαδίκτυο. Όμως ο τρόπος προσέγγισης των μικρών παιδιών για μείωση των κινδύνων, της ενίσχυσης της ασφαλούς πλοήγησης και τη χρήση του παγκόσμιου ιστού είναι μια ιδιαίτερα απαιτητική και δύσκολη διαδικασία παρά τους κανόνες και τις τακτικές διαχείρισης από το σχολικό περιβάλλον. Αυτό συμβαίνει κυρίως διότι η επικίνδυνη συμπεριφορά των νέων στο διαδίκτυο αποτελεί τρόπο έκφρασης και αυτοπραγμάτωσης.

3.3 Γονείς και ασφάλεια στο διαδίκτυο

Οι κίνδυνοι στο διαδίκτυο και η επικινδυνότητα πλοήγησης σχετίζεται άμεσα με την ηλιακή ομάδα των παιδιών, το γνωστικό τους υπόβαθρό, την εξοικείωσή τους με τις νέες τεχνολογίες αλλά και στο χώρο στον οποίο δραστηριοποιούνται.

Πρωταρχικός στόχος για μια ασφαλή πλοήγηση στο διαδίκτυο είναι η προστασία των προσωπικών δεδομένων και εγγράφων του χρήστη. Το οικιακό ψηφιακό μέσο, είτε αυτό είναι ένας ηλεκτρονικός υπολογιστής, είτε ένα tablet ή ένα έξυπνο τηλέφωνο, θα πρέπει να έχει το κατάλληλο ενημερωμένο λογισμικό ώστε να υπάρχει προστασία έναντι ιών και άλλων κακόβουλων προγραμμάτων. Οι γονείς μπορούν να παρέμβουν ενισχυτικά στην προστασία των υπολογιστικών συστημάτων κάνοντας χρήση ειδικών εφαρμογών ενεργοποιώντας αναλόγως τα σχετικά φίλτρα προστασίας.

Όμως, όπως και στο πραγματικό κόσμο έτσι και στον εικονικό – ψηφιακό κόσμο του διαδικτύου υπάρχει μια κοινωνικοποίηση του χρήστη. Αυτή η κοινωνικοποίηση αφορά την ψηφιακή συναναστροφή με γνωστούς αλλά και με αγνώστους. Έτσι, όπως σε πραγματικές συνθήκες έτσι και στον ψηφιακό κόσμο μπορεί να προκύψουν ανάρμοστες και επικίνδυνες συμπεριφορές. Ο καλύτερος τρόπος αντιμετώπισης είναι η σωστή ενημέρωση γύρω από τους κινδύνους του διαδικτύου και η συνεχής επιτήρηση από τους γονείς προκειμένου να αποφευχθούν οι όποιες δυσάρεστες καταστάσεις.

Ένα αρκετά μεγάλο ποσοστό γονέων οι οποίοι ενημερώνονται μέσα από έρευνες που σχετίζονται με τους κινδύνους που διατρέχουν οι μικρές ηλικίες στο παγκόσμιο ιστό, θεωρεί πως ο καλύτερος τρόπος προστασίας των μικρών παιδιών και η αντιμετώπιση όλων των επικίνδυνων καταστάσεων που μπορούν να προκύψουν είναι η απαγόρευση της πρόσβασης των παιδιών στο διαδίκτυο από το σπίτι.

Όμως, καλό είναι να γνωρίζουν ότι το διαδίκτυο στη σύγχρονή του μορφή αποτελεί μια αστείρευτη πηγή γνώσεων. Τα παιδιά, από μικρή ηλικία, πρέπει να γνωρίσουν το διαδίκτυο και να το χρησιμοποιούν και ως ένα βοηθητικό εργαλείο στη μάθηση αλλά και ως ένα σύγχρονο τρόπο επικοινωνίας.

Για να μπορέσουν λοιπόν τα παιδιά να έχουν μια ασφαλή πλοήγηση στον παγκόσμιο ιστό, οι γονείς [14] θα πρέπει:

1. Να ενημερώνονται σε θέματα νέων τεχνολογιών και διαδικτύου, για νέες εφαρμογές, τα οφέλη και τους κινδύνους που καραδοκούν.
2. Να είναι σε θέση να γνωρίζουν κάθε στιγμή που βρίσκονται τα παιδιά τους στο διαδίκτυο και το λόγο για τον οποίο το χρησιμοποιούν.
3. Να έχουν την γενική εποπτεία και να ελέγχουν το περιεχόμενο των ιστοσελίδων των οποίων επισκέπτονται τα παιδιά μέσα από τη ρύθμιση ειδικών φίλτρων, αποκλείοντας με αυτό τον τρόπο το ενδεχόμενο τα παιδιά να επισκεφτούν σελίδες με επικίνδυνες για αυτά θεματολογίες.
4. Να είναι ενημερωμένοι σχετικά με ειδικές εφαρμογές και προγράμματα με τα οποία μπορούν να ρυθμίσουν τον ηλεκτρονικό υπολογιστή ή τις έξυπνες συσκευές (smartphone, tablet) έτσι ώστε το περιβάλλον του διαδικτύου που επισκέπτονται τα παιδιά να είναι ελεγχόμενο.
5. Να ορίσουν του κανόνες που θα διέπουν τη χρήση των παιδιών στο διαδίκτυο, τον τρόπο με τον οποίο θα συνδέονται και τον χρόνο που θα αφιερώνουν σε αυτό.
6. Να βρίσκονται δίπλα στα παιδιά μικρότερης ηλικίας ως αρωγοί και ιδιαιτέρως όταν συνδέονται στο διαδίκτυο για πρώτη φορά.
7. Να τοποθετούν τους ηλεκτρονικούς υπολογιστές σε εμφανή χώρο του σπιτιού και όχι σε απομονωμένα δωμάτια.
8. Να εκπαιδεύσουν τα παιδιά, έτσι ώστε να είναι σε θέση να προστατεύουν τα προσωπικά τους στοιχεία.
9. Να ελέγχουν ανά τακτά χρονικά διαστήματα το ιστορικό του περιηγητή ιστοσελίδων ώστε να γνωρίζουν τις ιστοσελίδες τις οποίες επισκέπτονται τα παιδιά.
10. Να διατηρούν τον έλεγχο των λογαριασμών που διατηρούν τα παιδιά στα μέσα κοινωνικής δικτύωσης.

Συμπερασματικά λοιπόν, θα μπορούσαμε να πούμε ότι οι γονείς εκτός από την όλη εποπτεία της χρήσης του διαδικτύου θα πρέπει να αναπτύξουν και μια φιλικότερη σχέση με τα παιδιά που θα αποπνέει σεβασμό και εμπιστοσύνη και θα συντελεί στην ασφαλέστερη χρήση του διαδικτύου.

3.4 Παιδιά και ασφάλεια στο διαδίκτυο

Στη σύγχρονη εποχή, τα νέα παιδιά έρχονται σε επαφή από πολύ μικρή ηλικία με τις νέες τεχνολογίες και τα υπολογιστικά συστήματα. Παρόλα αυτά, υπάρχει ελλιπής γνώση και ενημέρωση σε θέματα ασφάλειας και αποφυγής επικίνδυνων καταστάσεων σχετικά με τη χρήση του διαδικτύου.

Το διαδίκτυο και οι εφαρμογές νέων τεχνολογιών χρησιμοποιούνται από τα παιδιά κατά κόρον στην εκπαιδευτική τους διαδικασία, στη ψυχαγωγία τους (π.χ. παιχνίδια, βίντεο, μουσική, φωτογραφίες), στην επικοινωνία (π.χ. μέσα κοινωνικής δικτύωσης).

Όμως, η χρήση των νέων τεχνολογιών, αν και ενθαρρύνει την δημιουργική έκφραση και την ελευθερία εγκυμονεί πολλούς κινδύνους.

Είναι πολύ πιθανόν, οι μικροί μαθητές, κατά τη διάρκεια που χρησιμοποιούν το διαδίκτυο να έρθουν αντιμέτωποι με:

- παράνομο υλικό
- κακή διαχείριση των προσωπικών τους στοιχείων και δεδομένων
- θέματα παρενόχλησης από επιτήδειους
- εθισμό στη χρήση του διαδικτύου

Για την αντιμετώπιση των ανωτέρω αρνητικών καταστάσεων και την εξάλειψη όλων των κινδύνων είναι πολύ σημαντική η ενημέρωση των γονέων, των εκπαιδευτικών και των μαθητών σε θέματα ασφάλειας και αποφυγής κινδύνων. Η συνήθης άποψη της απαγόρευσης και της αποχή από τη χρήση του παγκόσμιου ιστού ή η έντονη απαγόρευση και ο αυστηρός περιορισμός της χρήσης του είναι επί της ουσίας ανέφικτη. Τα παιδιά με τον έναν ή τον άλλο τρόπο θα καταφέρουν, παρόλο τις όποιες απαγορεύσεις, να βρουν τρόπους να συνδεθούν στο διαδίκτυο, εφόσον το επιθυμούν και αυτό παρατηρείται κυρίως σε ηλικίες παιδιών που βρίσκονται στην εφηβεία με τις όποιες ιδιαιτερότητες αυτή περίοδος της ζωής τους ορίζει (π.χ. περιέργεια, αντίδραση, αμφισβήτηση, ανυπακοή).

Έρευνες έδειξαν ότι η αυστηρή απαγόρευση πρόσβασης στο διαδίκτυο επηρεάζει αρνητικά την ψυχολογία των μαθητών. Εν αντιθέσει η ορθή χρήση των εφαρμογών του διαδικτύου από τα παιδιά, όπως για παράδειγμα παιχνίδια δεξιοτήτων, κοινωνική δικτύωση και εφαρμογές που υποστηρίζουν την διαδικασία της μάθησης, με την κατάλληλη υποστήριξη και μέριμνα, μπορούν να προσδώσουν στα παιδιά σημαντικά εκπαιδευτικά οφέλη.

Επίσης, η πρόσβαση στο διαδίκτυο και η χρησιμοποίησή του στον τομέα της επικοινωνίας συμβάλλει σημαντικά:

1. στη διερεύνηση της ταυτότητας του ατόμου/χρήστη

2. στην βελτίωση κοινωνικών δεξιοτήτων
3. στην ανάπτυξη κριτικής σκέψης
4. στην ένταξη στο κοινωνικό σύνολο μέσω των εφαρμογών κοινωνικής δικτύωσης
5. στην άρση απομόνωσης και ικανοποίηση των αναγκών της κοινωνικοποίησης

Συνεπώς, οι μαθητές και ειδικότερα τα παιδιά μικρότερης ηλικίας [14] που έρχονται σε επαφή με το διαδίκτυο για πρώτη φορά, θα πρέπει:

- Να μάθουν να επικοινωνούν και να συζητούν με τους γονείς και τους εκπαιδευτικούς για τη χρήση του διαδικτύου και ειδικότερα όταν αντιλαμβάνονται περίεργες ή ασυνήθιστες δραστηριότητες.
- Να είναι προσεκτικοί στις πληροφορίες που αντλούν από το διαδίκτυο και να ελέγχουν την εγκυρότητά τους.
- Η παρουσία τους στο διαδίκτυο και στα μέσα κοινωνικής δικτύωσης να είναι κόσμια.
- Να καταλάβουν τη σοβαρότητα των προσωπικών δεδομένων και να μη μοιράζονται / γνωστοποιούν τα προσωπικά τους στοιχεία σε αγνώστους στον παγκόσμιο ιστό.
- Να τηρούν το απόρρητο των προσωπικών κωδικών πρόσβασης που χρησιμοποιούν.
- Να μην συμπληρώνουν φόρμες στοιχείων κατά την επίσκεψή τους σε διάφορους δικτυακούς τόπους.
- Να μη διαμοιράζονται προσωπικά αρχεία (μουσικής, βίντεο, φωτογραφίες) με ξένους.
- Να είναι ιδιαίτερα προσεκτικοί στη χρήση εφαρμογών του διαδικτύου. Δεν είναι όλες οι εφαρμογές ασφαλής.
- Να αποφεύγουν την επικοινωνία με αγνώστους και να αγνοούν μηνύματα ηλεκτρονικού ταχυδρομείου όταν δεν γνωρίζουν τον αποστολέα, ενημερώνοντας ταυτόχρονα γονείς και εκπαιδευτικούς.

3.5 Κίνδυνοι του διαδικτύου

Με τον όρο «κίνδυνοι του διαδικτύου» [14] αναφερόμαστε σε όλες εκείνες τις επικίνδυνες καταστάσεις με τις οποίες μπορεί να έρθει αντιμέτωπος ένας χρήστης ψηφιακής συσκευής κατά τη διάρκεια σύνδεσης και πλοήγησής του στον παγκόσμιο ιστό.

Η εισαγωγή των νέων τεχνολογιών και του διαδικτύου στην εκπαιδευτική διαδικασία είναι πλέον γεγονός. Οι ψηφιακές συσκευές (π.χ. ηλεκτρονικός υπολογιστής, tablet) έχουν διαφοροποιήσει τον τρόπο με τον οποίο λειτουργεί πλέον μια σχολική τάξη.

Το διαδίκτυο, εκτός από την εκμηδένιση των αποστάσεων και της γρήγορης διακίνησης των δεδομένων, αποτελεί μια ανεξάντλητη πηγή πληροφοριών. Έτσι, άνθρωποι όλων των κατηγοριών και ηλικιών έχουν άμεση πρόσβαση σε ένα τεράστιο όγκο δεδομένων.

Ο παγκόσμιος ιστός, και η μορφή που έχει λάβει τα τελευταία χρόνια, είναι ιδιαίτερα ελκυστικός στα μικρά παιδιά. Κάνοντας χρήση του διαδικτύου, τα μικρά παιδιά, μπορούν να έχουν πρόσβαση, με ένα «κλικ», σε μια σειρά από εκπαιδευτικές αλλά και ψυχαγωγικές - διασκεδαστικές δραστηριότητες.

Όμως, θα πρέπει να γνωρίζουμε τις παγίδες και τους κινδύνους που πιθανώς να κρύβονται πίσω από τις όποιες δραστηριότητες πραγματοποιούνται στο διαδίκτυο.

Επί της ουσίας, το διαδίκτυο είναι ένα σύνολο ηλεκτρονικών υπολογιστών οι οποίες συνδέονται μεταξύ τους είτε ενσύρματα είτε ασύρματα με βασικό σκοπό την μεταξύ τους επικοινωνία και μετάδοση δεδομένων και πληροφοριών. Είναι δηλαδή, ένα δίκτυο ψηφιακών συσκευών (ηλεκτρονικών συσκευών, έξυπνων τηλέφωνων και tablet) η έκταση και το μέγεθος του οποίου εκτείνεται σε όλο τον κόσμο. Το μέγεθός του και η πολυπλοκότητά του το καθιστούν ιδιαίτερα δύσκολο στον έλεγχο και την επιτήρηση των πληροφοριών που διακινούνται. Αυτό έχει ως συνέπεια να εμφανίζονται, σε παγκόσμιο επίπεδο, πάρα πολλά περιστατικά παράνομων δραστηριοτήτων. Έχει παρατηρηθεί ότι τα μικρά παιδιά μπορούν εύκολα να έχουν πρόσβαση σε ακατάλληλες ιστοσελίδες ή να πέσουν θύμα επιτήδειων μέσα από καλοστημένες εφαρμογές και από προγράμματα κοινωνικής δικτύωσης.

Οι κίνδυνοι των παράνομων δραστηριοτήτων αφορούν ιστοσελίδες που το περιεχόμενό τους μπορεί να είναι ακατάλληλο για ανηλίκους, να περιέχουν παράνομο υλικό ή εφαρμογές επικίνδυνες για τη λειτουργία του ψηφιακού συστήματος του χρήστη (ηλεκτρονικού υπολογιστή, smartphone, tablet). Μπορεί επίσης να αφορούν την έκθεση σε ανεπιθύμητες διαφημίσεις με τη μορφή αναδυόμενων παραθύρων.

Το επικίνδυνο περιεχόμενο μπορεί να ελλοχεύει σε εικόνες, βίντεο και κείμενο με αυστηρώς ακατάλληλο περιεχόμενο για μικρά παιδιά τα οποία μπορούν κάλλιστα να έρθουν σε επαφή κατά τη διάρκεια ενός διαδικτυακού παιχνιδιού ή όταν κατά τη πλοήγησή τους στο διαδίκτυο εμφανίζονται παράθυρα με διαφημιστικά μηνύματα που δελεάζουν τον χρήστη με δώρα ή χρηματικά έπαθλα.

Σύμφωνα με έκθεση του Ευρωπαϊκού Κοινοβουλίου που αφορά την ασφάλεια των ανηλίκων στον παγκόσμιο ιστό, αποτυπώνεται η μεγάλη δυσκολία που υπάρχει στην οριοθέτηση μεταξύ κατάλληλων και ακατάλληλων περιεχομένων των ιστοσελίδων αλλά και των νόμιμων και παράνομων δραστηριοτήτων στο διαδίκτυο.

Η αποσαφήνιση αυτών των ορίων είναι άκρως σημαντική ώστε φαινόμενα

όπως παιδική πορνογραφία και παρενόχληση ανηλίκων να αντιμετωπίζονται άμεσα.

3.6 Κυβερνοεπίθεση - Hacking

Μια από τις πιο επικίνδυνες και παράνομες δραστηριότητες του διαδικτύου είναι το «hacking» [15]. Η βασική επιδίωξη της δραστηριότητας αυτής είναι η απόκτηση πρόσβασης και ελέγχου σε ένα ή περισσότερους ξένους ηλεκτρονικούς υπολογιστές ή ψηφιακά συστήματα χωρίς να υπάρχει η σχετική συναίνεση. Με την ενέργεια αυτή, όποιος καταφέρει να έχει πρόσβαση σε ένα ξένο ηλεκτρονικό υπολογιστικό σύστημα, μπορεί αυτομάτως να ελέγχει παράνομα και να επεξεργάζεται τα αρχεία και τα δεδομένα των συστημάτων αυτών. Έτσι, ο επονομαζόμενος «hacker» αποκτώντας απομακρυσμένη διαχείριση μπορεί να πραγματοποιεί λειτουργίες ως ένας απλός χρήστης του ξένου ηλεκτρονικού υπολογιστή ή ακόμα και να έχει πρόσβαση ως διαχειριστής του συστήματος. Η επικίνδυνη αυτή δραστηριότητα αποτελεί σοβαρό διαδικτυακό έγκλημα και διώκεται από το νόμο.

3.7 Επιβλαβές - Κακόβουλο Λογισμικό

Ως επιβλαβές ή αλλιώς «κακόβουλο λογισμικό» [6] ορίζεται το πρόγραμμα το οποίο όταν εκτελείται σε έναν ηλεκτρονικό υπολογιστή ή σε μια ψηφιακή συσκευή, προκαλεί σοβαρή ζημιά είτε αυτό είναι μερική ή ολοκληρωτική διαγραφή και αλλοίωση αρχείων και δεδομένων, είτε στοχεύει στην υποκλοπή και έλεγχο του υπολογιστικού συστήματος. Όταν μια ψηφιακή συσκευή είναι συνδεδεμένη στο διαδίκτυο είναι πολύ πιθανό να έρθει αντιμέτωπη με αυτού του είδους λογισμικά. Το κακόβουλο λογισμικό χωρίζεται σε τρεις κατηγορίες:

- Ιός (Virus)
- Δούρειος Ίππος (Trojan Horse)
- Σκουλήκια Ηλεκτρονικού Υπολογιστή (Computer Worms)

Ο ιός (Virus) είναι ένα κομμάτι κώδικα ενός προγράμματος το οποίο έχει την ικανότητα να μπορεί να παρεμβαίνει στη λειτουργία του συστήματος του χρήστη χωρίς τη συγκατάθεσή του και να προβαίνει σε κακόβουλες ενέργειες.

Ο δούρειος ίππος (TrojanHorse) είναι στην ουσία ένα πρόγραμμα το οποίο προσπαθεί να παραπλανήσει τον χρήστη και παρουσιάζεται ως χρήσιμο για αυτόν ενώ στη πραγματικότητα λειτουργεί με δόλιο τρόπο εκτελώντας κακόβουλο κώδικα στη ψηφιακή συσκευή στην οποία έχει γίνει η εγκατάστασή του.

Το σκουλήκι ηλεκτρονικού υπολογιστή (Computer Worms) αποτελεί έναν καταστροφικό ιό ο οποίος όταν εισβάλει σε ένα υπολογιστικό σύστημα εξαπλώνεται μέσω του δικτύου σε όλα τα υπόλοιπα συστήματα που είναι συνδεδεμένα σε αυτό προκαλώντας σοβαρά προβλήματα.

3.8 Ψάρεμα ή Phishing Προσωπικών Δεδομένων

Όπως αναφέραμε νωρίτερα, είναι σύνηθες φαινόμενο, όταν ένας χρήστης περιηγείται στο διαδίκτυο να εμφανίζονται παράθυρα (pop-up) με διαφημιστικά μηνύματα που δελεάζουν τον χρήστη με δώρα ή χρηματικά έπαθλα. Βασικός σκοπός των μηνυμάτων αυτών είναι να παραπλανήσουν το χρήστη και να εισάγει προσωπικά του δεδομένα. Η επικίνδυνη αυτή διαδικασία αποκαλείται «Ψάρεμα» ή «Phishing» [16] προσωπικών δεδομένων και τα τελευταία χρόνια εξελίσσεται συνεχώς. Χαρακτηριστικό παράδειγμα σύγχρονης μορφής phishing είναι η δημιουργία ψεύτικων ιστοσελίδων οι οποίες αποτελούν πιστά αντίγραφα των πραγματικών (π.χ. Ιστοσελίδες Τραπεζών).

3.9 Πειρατεία Λογισμικού

Η διαδικασία λήψης αρχείων μουσικής, βίντεο, ταινιών ή και παιχνιδιών αποτελεί μια σχετικά εύκολη διαδικασία για τον μέσο χρήστη του διαδικτύου. Όμως, θα πρέπει να γίνει γνωστό ότι οι παραπάνω διαδικασίες λήψης, αναπαραγωγής και διαμοιρασμού μη αυθεντικών προγραμμάτων ή εφαρμογών δεν είναι νόμιμες. Γίνεται καταπάτηση της πνευματική ιδιοκτησίας και των πνευματικών δικαιωμάτων και ο χρήστης που προβαίνει σε παρόμοιες ενέργειες είτε ως προμηθευτής-διακινητής είτε ως αποδέκτης παράνομου λογισμικού έρχεται αντιμέτωπος με νομικές κυρώσεις. Η ανωτέρω διαδικασία ονομάζεται «Πειρατεία Λογισμικού» [19].

3.10 Εξαπάτηση

Κατά τη διάρκεια αναζήτησης πληροφοριών στο διαδίκτυο υπάρχουν αρκετές ιστοσελίδες που παρουσιάζουν ανυπόστατες πληροφορίες οι οποίες δεν ανταποκρίνονται στην πραγματικότητα. Σκοπός των σελίδων αυτών είναι η παραπληροφόρηση του χρήστη είτε για ιδιωτικό – ψυχαγωγικό όφελος είτε για οικονομικό όφελος. Σε διεθνές επίπεδο, ο ορισμός που μπορεί να περιγράψει τη διαδικασία αυτή είναι «Hoax» [17]. Επιπλέον, η εξαπάτηση στο διαδίκτυο εμφανίζεται σε μηνύματα ηλεκτρονικού ταχυδρομείου και σε μέσα κοινωνικής δικτύωσης.

3.11 Ανεπιθύμητη Ηλεκτρονική Αλληλογραφία (Spam)

Τα μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) τα οποία αποστέλλονται καθημερινά σε διευθύνσεις πολλών ανθρώπων ταυτόχρονα χωρίς οι ίδιοι να το επιθυμούν, με βασικό περιεχόμενο διαφημιστικά προϊόντα ή επιχειρηματικές προτάσεις κ.α., ονομάζονται «spam» [18].

Τα μηνύματα αυτά, αν και τις περισσότερες φορές είναι αδιάφορα προς τους παραλήπτες, αποτελούν έναν φθηνό και γρήγορο τρόπο να διαφημίσουν οι εταιρείες τα προϊόντα τους. Όμως η διαχείριση όλων αυτών των μηνυμάτων

αναλώνει αρκετό χρόνο από τους παραλήπτες, δυσχεραίνοντας έτσι την εργασία τους.

Σκόπιμο κρίνεται να αναφέρουμε ότι στα πλαίσια της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας συγκαταλέγονται και μηνύματα εκείνα που αποστέλλονται σε συγκεκριμένους παραλήπτες και το περιεχόμενό τους είναι αισχρό, προσβλητικό ή ακόμα και απειλητικό.

3.12 Παιδική Πορνογραφία μέσω διαδικτύου

Ένα από τα μεγαλύτερα και σοβαρότερα εγκλήματα που παρουσίασαν έξαρση με την παράλληλη ανάπτυξη και διάδοση του διαδικτύου και των μέσων κοινωνικής δικτύωσης είναι η μάστιγα της «παιδικής πορνογραφίας» [14].

Ως διαδικτυακή παιδική πορνογραφία ορίζεται ο διαμοιρασμός αρχείων και δεδομένων μέσω του διαδικτύου, που περιέχουν εικόνα ή βίντεο τα οποία έχουν ως θεματολογία παιδιά και γενικότερα ανήλικους, που μετέχουν ή παρίστανται σε σεξουαλικές πράξεις.

3.13 Αποπλάνηση μικρών παιδιών - Grooming

Μια από τις πιο σοβαρές και επικίνδυνες απειλές που συναντάμε στο διαδίκτυο είναι η αποπλάνηση παιδιών μικρής ηλικίας «Grooming» [18]. Στον παγκόσμιο ιστό υπάρχει πληθώρα χρηστών οι οποίοι διατηρούν ψεύτικα προφίλ επιδιώκοντας την επικοινωνία με μικρά παιδιά. Απώτερος σκοπός τους είναι να δημιουργήσουν ένα φιλικό περιβάλλον εμπιστοσύνης με τα παιδιά και να τα χρησιμοποιήσουν σε παράνομες σεξουαλικές πράξεις οδηγώντας τα στην παιδική πορνεία.

3.14 Διαδικτυακός Εκφοβισμός

Οποιαδήποτε πράξη παρενόχλησης και προσβλητικής επαναλαμβανόμενης συμπεριφοράς που υλοποιείται μέσω του παγκόσμιου ιστού και των ψηφιακών συσκευών νέας τεχνολογίας, ονομάζεται διαδικτυακός εκφοβισμός [14] (διεθνής ορολογία «cyberbulling»).

Συνεπώς, ο διαδικτυακός εκφοβισμός αφορά την παρενόχληση του χρήστη μέσω απειλητικών μηνυμάτων όπου το περιεχόμενο μπορεί να είναι προσβλητικό, ρατσιστικό ή και εκφοβιστικού χαρακτήρα (μέσω ηλεκτρονικής αλληλογραφίας, μέσα κοινωνικής δικτύωσης και ιστοσελίδων). Οι επιπτώσεις του διαδικτυακού εκφοβισμού στους ανθρώπους και ιδιαιτέρως στα μικρά παιδιά, μπορεί να έχει ολέθριες συνέπειες στην ανάπτυξη και ψυχοσύνθεσή τους αλλά και στην κοινωνία γενικότερα.

Ο διαδικτυακός εκφοβισμός όπως και ο κλασικός εκφοβισμός, έχει ως κύριο στόχο την πρόκληση βλάβης στο υποψήφιο θύμα (είτε ψυχική είτε σωματική).

Έρευνες που έχουν πραγματοποιηθεί, έχουν δείξει ότι η ηλικία και το φύλο διαδραματίζουν σημαντικό ρόλο στις περιπτώσεις διαδικτυακού εκφοβισμού. Έχει παρατηρηθεί ότι τα κορίτσια υπόκεινται διαδικτυακό εκφοβισμό σε μεγαλύτερο βαθμό από τα αγόρια και αυτό γιατί ο εκφοβισμός μέσω διαδικτύου προσφέρεται για ασφαλή επίθεση του θύτη προς το θύμα (μέσω μηνυμάτων), ενώ τα αγόρια συνηθίζουν να επιλέγουν ως εκφοβισμό την άσκηση σωματικής βίας.

Όσον αφορά την ηλικία, οι έρευνες έδειξαν ότι οι πιθανότητες που υπάρχουν να υποστεί κάποιος διαδικτυακό εκφοβισμό, είναι περισσότερες σε παιδιά που φοιτούν σε σχολεία δευτεροβάθμιας εκπαίδευσης (Γυμνάσιο, Λύκειο) από ότι σε παιδιά τάξεων Δημοτικού Σχολείου.

Μέσα από μελέτες που έχουν γίνει, έχει παρατηρηθεί ότι τα παιδιά που κάνουν συστηματική χρήση του διαδικτύου και έχουν αυξημένες γνώσεις σχετικά με τις νέες τεχνολογίες, έχουν μεγαλύτερη πιθανότητα να εμπλακούν σε πράξεις διαδικτυακού εκφοβισμού είτε ως θύτες είτε ως θύματα.

3.15 Ψεύτικη Ταυτότητα

Ο κίνδυνος της «ψεύτικης ταυτότητας» [19] που συναντάται στον παγκόσμιο ιστό, είναι η σύνδεση στο διαδίκτυο με στοιχεία άλλου ατόμου τα οποία έχουνε κλαπεί (κωδικοί πρόσβασης) ή και η δημιουργία ψεύτικου προφίλ στα μέσα κοινωνικής δικτύωσης. Ο χρήστης της ψεύτικης ταυτότητας έχει ως στόχο την εξαπάτηση εις βάρος του ατόμου του οποίου χρησιμοποιεί τα στοιχεία. Η εξαπάτηση αυτή μπορεί να είναι είτε ηθική είτε να αποσκοπεί σε οικονομικά συμφέροντα.

3.16 Εθισμός

Η πολύωρη ενασχόληση των μικρών παιδιών με δραστηριότητες του διαδικτύου καθ’ όλη τη διάρκεια της ημέρας, όπως για παράδειγμα ηλεκτρονικά παιχνίδια ή επικοινωνία με συνομήλικούς τους στα μέσα κοινωνικής δικτύωσης, αποτελεί συχνό φαινόμενο της εποχής μας.

Οι πράξεις αυτές όμως, απομακρύνουν τα παιδιά από τις καθημερινές τους δραστηριότητες αδιαφορώντας είτε για τα μαθήματά τους είτε για την επαφή τους με τον κοινωνικό περίγυρο. Η συνήθεια αυτή πολλές φορές οδηγεί σε εθισμό όπου στην περίπτωση του παγκόσμιου ιστού αποκαλείται «Εθισμός του Διαδικτύου» [20].

3.16.1 Κατηγορίες Εθισμού των παιδιών στο Διαδίκτυο

Ο εθισμός των παιδιών στο διαδίκτυο χωρίζεται σε πέντε διαφορετικές κατηγορίες οι οποίες περιγράφονται παρακάτω:

- Ο εθισμός στην υπερβολική χρήση ηλεκτρονικού υπολογιστή, έξυπνου τηλεφώνου, tablet, με μοναδικό σκοπό τη διασκέδαση μέσω ηλεκτρονικών παιχνιδιών.

- Εθισμός στην ακαταλόγιστη αναζήτηση πληροφοριών και πλοήγηση στον παγκόσμιο ιστό.
- Εθισμός στο διαδικτυακό τζόγο και στα τυχερά παιχνίδια.
- Η ενασχόληση με σελίδες κοινωνικής δικτύωσης και σε σελίδες ακατάλληλου περιεχομένου για αρκετές ώρες.
- Εθισμός στις αγορές προϊόντων μέσω διαδικτύου.

Ο εθισμός αυτός προκαλεί ποικίλες διαταραχές στη συμπεριφορά των παιδιών κυρίως όταν η χρήση του διαδικτύου γίνεται υπερβολική. Τα παιδιά αλλάζουν συνήθειες με συνέπεια να αδιαφορούν για τις υποχρεώσεις τους στο σχολείο (μειωμένη απόδοση στα μαθήματα) και για το οικογενειακό τους περιβάλλον (απουσία επικοινωνίας με τους γονείς, αδιαφορία). Μειώνεται σημαντικά ο χρόνος που ασχολείται το παιδί με την οικογένειά του, τα χόμπι και οι κοινωνικές του δραστηριότητες, και συνάμα μεγαλώνει ο κίνδυνος εμφάνισης πληθώρας προβλημάτων υγείας λόγω της πολύωρης χρήσης του ηλεκτρονικού υπολογιστή και των λοιπών ψηφιακών συσκευών.

Συμπερασματικά λοιπόν, τα συμπτώματα του εθισμού των ανηλίκων στο διαδίκτυο μπορούν επιγραμματικά να καθοριστούν ως ακολούθως:

- Εμμονή με τη συνεχή διασύνδεση στο διαδίκτυο.
- Αδιαφορία για τις σχολικές και τις κοινωνικές υποχρεώσεις.
- Υπάρχει συνεχή κούραση.
- Μειωμένη απόδοση στα μαθήματα.
- Κακή επικοινωνία με το οικογενειακό περιβάλλον.

3.17 Greeklish

Η καθιέρωση του αγγλικού αλφαβήτου στη γραφή ελληνικών λέξεων, αποτελεί τον συνήθη κώδικα επικοινωνίας μεταξύ των παιδιών ανεξαρτήτου ηλικίας στα μέσα κοινωνικής δικτύωσης του διαδικτύου. Η υιοθέτηση αυτή στην επικοινωνία των νέων αποκαλείται «Greeklish» [21]. Μελέτες έδειξαν ότι η συνεχόμενη χρήση του παραπάνω τρόπου γραφής από τους νέους αλλά και κυρίως από τα μικρά παιδιά έχουν αρνητικές συνέπειες στο γραπτό λόγο διότι μέσω της χρήση των greeklish αλλοιώνεται η Ελληνική γλώσσα όσον αφορά τη γραμματική, το συντακτικό και την ορθογραφία. Επίσης, τα παιδιά, μεταφέρουν τη συνήθεια των greeklish που χρησιμοποιούν στο διαδίκτυο, στον πραγματικό κόσμο.

3.18 Trafficking

Η αυξανόμενη χρήση του Διαδικτύου από σχεδόν όλους τους τομείς της σύγχρονης ζωής και η εξάπλωση των μέσων και εφαρμογών κοινωνικής δικτύωσης οδήγησε στην έξαρση ενός παράνομου και επικίνδυνου φαινομένου της διακίνησης και εμπορίας ανθρώπων γνωστή και ως «trafficking». Το trafficking ορίζεται, σε διεθνές επίπεδο, από το πρωτόκολλο του Ο.Η.Ε. «Αποτροπή Καταστολή και τη

Τιμωρία της Παράνομης διακίνησης Προσώπων με σκοπό τη Σεξουαλική και Οικονομική Εκμετάλλευση ιδιαίτερα Γυναικών και Παιδιών» και αφορά τη στρατολόγηση, μεταφορά, μετακίνηση, εγκατάσταση, ή παραλαβή προσώπων, μέσω απειλής ή χρήσης βίας ή άλλων μορφών εξαναγκασμού, της απαγωγής, του δόλου, της εξαπάτησης, της κατάχρησης της δύναμης, της κατάχρησης μιας τρωτής ή ευάλωτης θέσης, της προσφοράς ή της αποδοχής οικονομικού ή άλλου οφέλους για την επίτευξη της σύμφωνης γνώμης ενός προσώπου το οποίο ασκεί έλεγχο ή εξουσία επί άλλου προσώπου για το σκοπό της εκμετάλλευσης.

3.19 Κίνδυνοι μηνυμάτων σεξουαλικού περιεχομένου (sexting)

Ένα ακόμα επικίνδυνο φαινόμενο του διαδικτύου που παρουσιάζει ιδιαίτερη έξαρση τα τελευταία χρόνια και κυρίως μεταξύ των ανηλίκων είναι η αποστολή μηνυμάτων σεξουαλικού περιεχομένου [14]. Η αποστολή των μηνυμάτων αυτών γίνεται είτε μεταξύ των ανηλίκων είτε μεταξύ ανήλικου προς ενήλικα και αντίστροφα.

Σύμφωνα με μελέτες που έχουν πραγματοποιηθεί, οι ηλικιακές ομάδες παιδιών που εμπλέκονται στο παραπάνω φαινόμενο είναι από οχτώ έως δεκαοχτώ χρονών. Αξιοσημείωτο είναι ότι οι γονείς των παιδιών αυτών δεν έχουν γνώση αυτής της επικίνδυνης δραστηριότητας.

3.20 Μέτρα Προστασίας και αποφυγή κινδύνων στο διαδίκτυο

Όσον αφορά τα μέτρα προστασίας που θα πρέπει να λαμβάνονται για την ασφαλή χρήση στο διαδίκτυο ώστε να περιοριστούν οι κίνδυνοι που προαναφέραμε, θα πρέπει να τηρούνται οι ακόλουθες ενέργειες [14]:

- Ενημέρωση του λειτουργικού συστήματος
- Χρήση λογισμικού Antivirus
- Προστασία από ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου
- Δημιουργία Αντιγράφων Ασφαλείας (Back-up)
- Προστασία από Κλοπή Ταυτότητας
- Ενίσχυση Προσωπική Ασφάλειας

3.20.1 Ενημερωμένο λειτουργικό σύστημα

Το λειτουργικό σύστημα που χρησιμοποιείται για την πλοήγηση στον παγκόσμιο ιστό καθώς και οι εφαρμογές πλοήγησης (browsers), θα πρέπει να είναι ενημερωμένα με τις τελευταίες εκδόσεις που ορίζουν οι κατασκευάστριες εταιρίες.

3.20.2 Ευρεία χρήση αντιικού λογισμικού - Antivirus

Κάθε ηλεκτρονικός υπολογιστής ή ψηφιακή συσκευή (smartphone, tablet) από την οποία αποκτούμε πρόσβαση στο διαδίκτυο απαιτείται να υπάρχει εγκατεστημένο πρόγραμμα αντιικής προστασίας (antivirus). Σκοπός της αντιικής εφαρμογής είναι η παροχή προστασίας από κακόβουλο λογισμικό το οποίο μπορεί

να εισέλθει στις ψηφιακές μας συσκευές είτε μέσω ανεπιθύμητων μηνυμάτων του ηλεκτρονικού ταχυδρομείου είτε μέσω εγκατάστασης παράνομων εφαρμογών είτε κατά την περιήγηση σε μη ασφαλές ιστοσελίδες. Επίσης, για την αποτελεσματικότερη λειτουργία του αντιικού προγράμματος είναι ανάγκη να γίνεται συχνά ενημέρωση του λογισμικού από την αντίστοιχη εταιρία.

3.20.3 Αντιμετώπιση ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου (Anti - Spam)

Η διαδικασία της ταυτόχρονης αποστολής πολλών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε πολλούς παραλήπτες του παγκόσμιου ιστού χωρίς τη δική τους συναίνεση, ορίζεται ως «Ανεπιθύμητη αλληλογραφία» (Spam). Τα μηνύματα αυτά συνήθως περιλαμβάνουν διαφημίσεις (π.χ. παροχή υπηρεσιών ή προϊόντων) χωρίς όμως να το επιθυμεί ο παραλήπτης.

Για την αντιμετώπιση της παραπάνω διαδικασίας θα πρέπει:

- Ο χρήστης να προστατεύει τον προσωπικό του λογαριασμό του ηλεκτρονικού του ταχυδρομείου (e-mail) κατά τη σύνδεσή του στο διαδίκτυο και κυρίως από τα μέσα κοινωνικής δικτύωσης.
- Να αποφεύγει την αλληλεπίδραση με μηνύματα ανεπιθύμητης αλληλογραφίας για το λόγο ότι όσο περισσότερο απαντά σε spam μηνύματα τόσο πιο πολλά spam θα λαμβάνει στη θυρίδα του ηλεκτρονικού του ταχυδρομείου.
- Να υπάρχει πάντα στον ηλεκτρονικό υπολογιστή ή στην ψηφιακή συσκευή εγκατεστημένο ειδικό λογισμικό προστασίας από μηνύματα ανεπιθύμητης αλληλογραφίας.

3.20.4 Αντίγραφα Ασφαλείας (Back-up)

Μία ίσως από τις κυριότερες ενέργειες που είναι ανάγκη να πραγματοποιεί ο κάθε χρήστης ηλεκτρονικού υπολογιστή ή ψηφιακής συσκευής είναι η δημιουργία αντιγράφων ασφαλείας γνωστό και ως Back – up. Και αυτό θα πρέπει να γίνεται για το λόγο ότι πολλές φορές κατά τη διάρκεια της πλοήγησης στο διαδίκτυο, το ψηφιακό σύστημα που χρησιμοποιούμε μπορεί να γίνει στόχος επίθεσης κακόβουλων λογισμικών με απώτερο σκοπό είτε την κλοπή προσωπικών αρχείων είτε ακόμη και την καταστροφή όλων των δεδομένων που βρίσκονται αποθηκευμένα στον σκληρό δίσκο.

Τα αντίγραφα ασφαλείας είναι επί της ουσίας δημιουργία αντιγράφων των σπουδαιότερων αρχείων και εγγράφων του χρήστη σε εξωτερικά μέσα αποθήκευσης όπως είναι για παράδειγμα ο εξωτερικός σκληρός δίσκος, οι οπτικοί δίσκοι (CD-R / RW, DVD–R / RW) και σε επανεγγράψιμες μνήμες USB, ώστε να μπορούν να ανακτηθούν σε ενδεχόμενη απώλειά τους.

3.20.5 Προστασία προσωπικών δεδομένων

Η προστασία των προσωπικών δεδομένων αποτελεί το βασικό μέλημα του

χρήστη όταν επισκέπτεται το διαδίκτυο ή τα μέσα κοινωνικής δικτύωσης. Από τις βασικότερες ενέργειες που είναι απαραίτητο να τηρούνται ώστε να διασφαλιστεί η ασφάλεια των στοιχείων της προσωπικής ταυτότητας του χρήστη είναι η διαφύλαξη των κωδικών πρόσβασης (password) που απαιτούνται για την είσοδο σε διαδικτυακές εφαρμογές. Οι κωδικοί αυτοί απαιτείται να διακατέχονται από μία πολυπλοκότητα, δηλαδή να περιέχουν πεζά και κεφαλαία γράμματα, αριθμούς και ειδικούς χαρακτήρες. Δε θα πρέπει ο χρήστης να χρησιμοποιεί ως κωδικό πρόσβασης την ημερομηνία γέννησής του, το ονοματεπώνυμό του, τον αριθμό του τηλεφώνου του και γενικά δε θα πρέπει να χρησιμοποιεί στοιχεία που μπορεί κάποιος εύκολα να μαντέψει.

3.20.6 Ενίσχυση Προσωπικής Ασφάλειας

Τα παιδιά προκειμένου να προστατέψουν τον εαυτό τους από τις επικίνδυνες καταστάσεις κατά την πλοήγησή τους στον παγκόσμιο ιστό, είναι χρήσιμο να τηρούν τους παρακάτω κανόνες:

1. Να μην κάνουν άσκοπη χρήση του διαδικτύου.
2. Να μην εμπιστεύονται συνδέσμους ιστοσελίδων των οποίων το περιεχόμενο δεν είναι γνωστό.
3. Να μην αλληλεπιδρούν με μηνύματα ανεπιθύμητης αλληλογραφίας (Spam).
4. Και να είναι σε συχνή επικοινωνία με τους γονείς τους και τους δασκάλους τους για οποιοδήποτε πρόβλημα αντιμετωπίζουν ή τους φοβίζει στο διαδίκτυο και στα μέσα κοινωνικής δικτύωσης.

4. Γονικός Έλεγχος

Στη σημερινή εποχή, το ενδιαφέρον όλων των ανθρώπων στρέφεται γύρω από τον ψηφιακό κόσμο. Αυτό έχει σαν αποτέλεσμα την αλλαγή του σύγχρονου τρόπου ζωής. Ψηφιακοί φίλοι, ψηφιακές ρυθμίσεις, ψηφιακή εκπαίδευση, ψηφιακά παιχνίδια, ψηφιακά ψώνια, ψηφιακές συναλλαγές και φαινόμενα. Με την τεράστια και ολοένα αυξανόμενη τεχνολογική ανάπτυξη όλο και περισσότερες ψηφιακές δραστηριότητες αναπτύσσονται. Γονείς, κηδεμόνες αλλά και όσοι επιβλέπουν τα παιδιά παίζουν πολύ σημαντικό ρόλο στο πώς αυτά θα χρησιμοποιήσουν σωστά τα μέσα ενημέρωσης που τους δίνονται.

Το ασύρματο δίκτυο πλέον υπάρχει παντού. Τα παιδιά έχουν πρόσβαση σε αυτό μέσω των ηλεκτρονικών υπολογιστών, έξυπνων κινητών και λοιπών ηλεκτρονικών συσκευών (tablet, smartphones), οπότε ξεκινούν και χρησιμοποιούν το διαδίκτυο όλο και από πιο μικρές ηλικίες. Η θέση των γονέων είναι πιο δύσκολη για το λόγω ότι καινούργιες προκλήσεις εμφανίζονται και γίνεται πιο δύσκολο να εξασφαλίσουν την ασφάλεια των παιδιών τους όταν είναι συνδεδεμένα στο διαδίκτυο. Στους μικρούς νέους χρήστες του διαδικτύου εμφανίζονται νέες ευκαιρίες, καθώς χρησιμοποιούν το διαδίκτυο, όπως επίσης και απειλές. Ρόλος και σκοπός του γονέα [22] είναι να αντισταθμίσει τις επικίνδυνες καταστάσεις με τα οφέλη που παρουσιάζονται με βασικό στόχο την εκμηδένιση των κινδύνων του παγκόσμιου ιστού.

Ο τρόπος αυτής της διαχείρισης και ελέγχου που αφορά τα παιδιά και τα μέσα κοινωνικής δικτύωσης - ενημέρωσης ορίζεται ως «γονική διαμεσολάβηση» [22]. Αποτελεί δηλαδή ένα διαφορετικό ορισμό της γονικής μέριμνας και επηρεάζει τη συμπεριφορά των παιδιών στο διαδίκτυο.

Επίσης, η άμεση πρόσβαση στο διαδίκτυο μέσω της χρήσης έξυπνων κινητών τηλεφώνων από τα παιδιά δημιουργεί αρκετές δυσκολίες όσον αφορά την εποπτεία τους από τους γονείς τους.

Σύμφωνα λοιπόν με τα ανωτέρω, η γονική διαμεσολάβηση κατηγοριοποιείται σε πέντε τομείς τους οποίους οι γονείς μπορούν να εφαρμόσουν είτε μεμονωμένα είτε σε συνδυασμό. Επί της ουσίας, δεν υπάρχει μία συγκεκριμένη φόρμουλα που θα μπορούσε να κατευθύνει τους γονείς ώστε να μειωθούν και να απαλειφθούν οι όποιοι κίνδυνοι. Για το λόγο αυτό, η διαμεσολάβηση των γονέων δε θεωρείται εύκολη διαδικασία.

Στη συνέχεια παρουσιάζονται συνοπτικά οι πέντε κατηγορίες της γονικής διαμεσολάβησης.

4.1 Είδη γονικής διαμεσολάβησης

Σύμφωνα με μελέτες που έχουνε πραγματοποιηθεί σε χώρες της Ευρωπαϊκής Ένωσης, το δίκτυο Kids Online της ΕΕ όρισε ότι η γονική διαμεσολάβηση [22] χωρίζεται στις παρακάτω πέντε κατηγορίες:

- Ενεργή Διαμεσολάβηση χρήσης διαδικτύου

Ενεργή μεσολάβηση χρήσης του διαδικτύου σημαίνει ότι ανάμεσα σε γονείς και παιδιά υπάρχει λεκτική επικοινωνία. Οι γονείς συζητούν με τα παιδιά τους για το διαδίκτυο, τις ενέργειες που κάνουν όταν είναι συνδεδεμένα στο διαδίκτυο και τα προτρέπουν να το διερευνήσουν. Όταν οι γονείς διαλέγουν το συγκεκριμένο τύπο διαμεσολάβησης, ενδέχεται να είναι δίπλα στα παιδιά τους όταν αυτά είναι συνδεδεμένα με το διαδίκτυο και να συμμετέχουν στις ενέργειες που κάνουν μαζί τους.

Σύμφωνα με μελέτες του EU Kids Online, αυτές οι δραστηριότητες – πολιτικές των γονέων έχουν ως αποτέλεσμα να μειώσουν κατά πολύ τους διαδικτυακούς κίνδυνους στους οποίους μπορεί να έρθει σε επαφή το παιδί χωρίς όμως αυτό να μειώνει τις ευκαιρίες που τους δίνονται από το διαδίκτυο.

- Ενεργή Διαμεσολάβηση ασφάλειας διαδικτύου

Στο συγκεκριμένο τύπο διαμεσολάβησης υπάρχει η κατεύθυνση και η εποπτεία των γονέων μέσω της συζήτησης με τα παιδιά για θέματα της ασφάλειας του διαδικτύου. Αυτός ο διάλογος πραγματοποιείται πριν και κατά τη διάρκεια της δραστηριοποίησης των παιδιών με το διαδίκτυο. Επίσης, μπορεί να εφαρμοστεί και επικουρικά ακόμα και μετά από άσχημες διαδικτυακές συμπεριφορές.

- Περιοριστική Διαμεσολάβηση

Η περιοριστική διαμεσολάβηση περικλείει τους κανόνες – όρους που βάζουν οι γονείς στα παιδιά τους όσον αφορά τη σωστή χρήση του διαδικτύου. Οι όροι αυτοί μπορεί να περιέχουν διάφορους περιορισμούς και ελέγχους ως προς το χρόνο που είναι online τα παιδιά στο διαδίκτυο, ως προς τις σελίδες τις οποίες επισκέπτονται, ως προς τις εφαρμογές (application) που μπορούν να κατεβάσουν (download) και γενικά ως προς τις ενέργειες που κάνουν τα παιδιά στο διαδικτυακό περιβάλλον.

- Τεχνική Διαμεσολάβηση

Στην τεχνική διαμεσολάβηση οι γονείς για να ελέγξουν ή και να θέσουν όρια στη χρήση που κάνει το παιδί τους στο διαδίκτυο, κάνουν χρήση κατάλληλου λογισμικού ή γονικού ελέγχου. Το λογισμικό αυτό έχει την ικανότητα να φιλτράρει αθέμιτο υλικό, να ελέγχει το χρόνο που προβάλλεται καθώς επίσης και να παρατηρεί, να επιτηρεί και να φρουρεί συμπεριφορές των κοινωνικών μέσων.

Σύμφωνα με τις μελέτες της Ευρωπαϊκής Επιτροπής οι ψηφιακές εφαρμογές γονικού ελέγχου έχουν τις παρακάτω βασικές λειτουργίες:

- **Περιορισμός διευθύνσεων** – ώστε να μην υπάρχει πρόσβαση σε συγκεκριμένες ιστοσελίδες του διαδικτύου είτε αυτές είναι URL διευθύνσεις είτε είναι IP διευθύνσεις.
- **Χρήση φίλτρων που αφορά το περιεχόμενο** – όπου γίνεται έλεγχος του μη κατάλληλου περιεχομένου στο οποίο έγινε η πρόσβαση. Είναι είτε λέξεις, είτε εικόνες (αν οι URL διευθύνσεις βρίσκονται σε blacklist).
- **Έλεγχος χρήσης** – όπου ελέγχεται η είσοδος στο διαδίκτυο ορίζοντας τις χρονικές περιόδους και περιθώρια.
- **Διαχείριση δραστηριοτήτων –** όπου ο έλεγχος των παιδιών για τη δραστηριότητά τους γίνεται με ειδοποιήσεις και αναφορές.

Επίσης, συμπληρωματικά των ανωτέρω, οι τρόποι με τους οποίους μπορούν να χρησιμοποιηθούν τα εργαλεία που αφορούν το γονικό έλεγχο είναι:

- Εγκατάσταση προγραμμάτων ή εφαρμογών στον Ηλεκτρονικό Υπολογιστή, ή στις έξυπνες συσκευές (smartphone, tablet).
- Χρήση φίλτρων που προσφέρονται δωρεάν στον παγκόσμιο ιστό .
- Συνδυασμός των δύο λύσεων.

- Παρακολούθηση

Ο γονικός έλεγχος μπορεί να πραγματοποιηθεί ελέγχοντας [23] όλες τις δραστηριότητες των μικρών παιδιών όπως για παράδειγμα τους ιστότοπους που δραστηριοποιούνται, τα εισερχόμενα και εξερχόμενα μηνύματα του ηλεκτρονικού ταχυδρομείου αλλά και το προσωπικό τους προφίλ σε λογαριασμούς μέσων κοινωνικής δικτύωσης.

4.2 Τρόπος εφαρμογής της Τεχνικής Διαμεσολάβησης

Στο εμπόριο παρουσιάζονται αρκετοί γονικοί έλεγχοι που απευθύνονται στο καταναλωτικό κοινό καθώς και αρκετές τεχνολογίες παρακολούθησης.

Είναι προγράμματα, εφαρμογές, υπηρεσίες και εργαλεία που δίδονται στους γονείς ώστε να προστατεύσουν τα παιδιά τους και να είναι πιο ασφαλή κατά την περιήγησή τους στον παγκόσμιο ιστό. Οι συγκεκριμένοι έλεγχοι δίνουν τη δυνατότητα στους γονείς να αποτρέπουν τα παιδιά τους από άσκοπη χρήση του διαδικτύου, να παρακολουθούν και να περιεργαστούν υλικό και περιεχόμενο το οποίο δεν είναι κατάλληλο για αυτά.

Αρκετές έρευνες που πραγματοποιήθηκαν με πιο πρόσφατη αυτή του EU Kids Online [23] κατατάσσουν το γονικό έλεγχο στις εξής τρεις κατηγορίες:

- σχεδιασμός
- λειτουργία
- πραγμάτωση - εφαρμογή

- Σχεδιασμός

Η πρώτη κατηγορία αφορά κυρίως το δημιουργό, ο οποίος υλοποιεί στην πράξη τη γονική μέριμνα διαμέσου του σχεδιασμού. Η υλοποίηση της φάσης του σχεδιασμού αφορά τις παρακάτω υποκατηγορίες:

- τηλεπικοινωνίες
- κοινωνική δικτύωση
- υλικό (hardware)
- πλατφόρμες παιχνιδιών
- λογισμικό (software)
- εφαρμογές.

Για να υπάρχει σύμπνοια με τη διεθνή νομοθεσία, ο δημιουργός που είναι υπεύθυνος για το σχεδιασμό κυρίως των υποκατηγοριών των τηλεπικοινωνιών και της κοινωνικής δικτύωσης, θα πρέπει να χρησιμοποιεί εφαρμογές γονικού ελέγχου με κύριο στόχο την αποφυγή επικίνδυνων καταστάσεων.

- Λειτουργία

Η δεύτερη κατηγορία της λειτουργίας αφορά το χρονικό περιορισμό, τη διαχείριση περιεχομένου, τον έλεγχο δραστηριοτήτων και τη γενική εποπτεία.

- Χρονικός περιορισμός:

Σε αυτόν τον άξονα, υπάρχουν πολλοί γονικοί έλεγχοι οι οποίοι κινούνται γύρω από τον περιορισμό του χρόνου που τα παιδιά είναι στο διαδίκτυο. Μάλιστα αρκετά από αυτά τα λογισμικά δίνουν τη δυνατότητα στους γονείς να προκαθορίσουν το χρονικό διάστημα το οποίο το παιδί τους θα είναι συνδεδεμένο στον παγκόσμιο ιστό ανάλογα αν είναι τις εργάσιμες ημέρες ή αν είναι Σαββατοκύριακο ή αν είναι γιορτινές μέρες ή μέρες διακοπών.

- Διαχείριση περιεχομένου:

Η κατηγορία αυτή της τεχνικής διαμεσολάβησης αφορά τις τεχνικές εκείνες με τις οποίες το περιεχόμενο φιλτράρεται σε θετικές και αρνητικές λίστες. Δηλαδή σε λίστες που το περιεχόμενό τους είναι επιτρεπτό προς τα μικρά παιδιά και σε λίστες που είναι απαγορευτικό σε ανηλίκους.

Ο τρόπος που υλοποιούνται αυτές οι τεχνικές σε ιστοτόπους γίνεται με τη δημιουργία λέξεων κλειδιών, ηλικιακή κατηγοριοποίηση και αυτόματες τεχνικές αναγνώρισης εικόνων (π.χ. αναγνώριση εικόνων με άσεμνο περιεχόμενο).

Όσον αφορά τους γονείς, μπορούν να διαχειριστούν το επίπεδο της πρόσβασης και του ελέγχου μεταξύ της αυτόματης επιλογής αλλά και των προχωρημένων ρυθμίσεων του χρήστη ώστε να μπορούν να προσαρμόζονται ανάλογα με τις ανάγκες του εκάστοτε παιδιού. Θα μπορούν δηλαδή να επιλέγουν από το μηδενικό επίπεδο προστασίας έως το επίπεδο υψηλής προστασίας.

Επίσης, η διαχείριση περιεχομένου μπορεί να δραστηριοποιείται στον έλεγχο της διακίνησης των πληροφοριών έτσι ώστε οι γονείς να είναι σε θέση να εποπτεύουν την ηλεκτρονική αλληλογραφία και τα μέσα κοινωνικής δικτύωσης γενικότερα.

- Έλεγχος δραστηριοτήτων:

  Ο έλεγχος δραστηριοτήτων χωρίζεται στους εξής τομείς:

  1. Ο πρώτος τομέας αφορά τον περιορισμό των ηλεκτρονικών συναλλαγών (οικονομική δραστηριότητα).

  2. Ο δεύτερος αφορά τις δραστηριότητες κοινωνικής αλληλεπίδρασης (όπως για παράδειγμα να επικοινωνήσει το παιδί με έναν άγνωστο) και τον έλεγχο της διαμοίρασης των προσωπικών δεδομένων και πληροφοριών.

  3. Ο τρίτος τομέας του ελέγχου δραστηριοτήτων αφορά κυρίως το θέμα της ψυχαγωγίας (εφαρμογές ελέγχου διαδικτυακών παιχνιδιών). Και αυτός ο έλεγχος παίζει σημαντικό ρόλο γιατί προστατεύει τα παιδιά που παίζουν διαδικτυακά παιχνίδια να αλληλεπιδράσουν με άγνωστους χρήστες (κατά πάσα πιθανότητα με ενήλικους).

- Γονική επιτήρηση

Η κατηγορία αυτή αναφέρεται στις νέες τεχνολογίες και εφαρμογές που βοηθούν τους γονείς στην εποπτεία όλων των ηλεκτρονικών κινήσεων – δραστηριοτήτων των μικρών παιδιών. Αυτό υλοποιείται είτε μέσω ενημέρωσης (ηλεκτρονική αλληλογραφία) του διαχειριστή του γονικού ελέγχου όσον αφορά το ιστορικό της δραστηριότητας του παιδιού είτε με αποστολή προειδοποιητικών μηνυμάτων στα παιδιά ότι δραστηριοποιούνται σε ιστοτόπους ακατάλληλους για την ηλικία τους.

Οι παραπάνω εφαρμογές μπορούν να λειτουργήσουν ή μεμονωμένα ή συνδυαστικά.

- Πραγμάτωση - εφαρμογή

Η κατηγορία αυτή αφορά την ψηφιακή συσκευή όπου υλοποιούνται όλοι οι έλεγχοι και οι περιορισμοί. Ο γονικός έλεγχος λειτουργεί συνδυαστικά με αντιικές εφαρμογές και εφαρμογές ελέγχου κακόβουλου λογισμικού. Η πραγμάτωση – εφαρμογή χωρίζεται στα παρακάτω επίπεδα:

- λειτουργικού σύστημα (Windows, Linux)
- περιηγητές ιστοτόπων
- ειδικό λογισμικό ελέγχου και εποπτείας ψηφιακής συσκευής
- έξυπνα κινητά τηλέφωνα και tablet που καθορίζουν την πρόσβαση των παιδιών σε συγκεκριμένες εφαρμογές
- φίλτρα διαχείρισης περιεχομένων ιστοσελίδων
- πλατφόρμες παιχνιδιών

4.3 Μειονεκτήματα τεχνικής διαμεσολάβησης

Οι ανησυχίες και τα άγχη που δημιουργούνται στους γονείς συνετέλεσαν στη δημιουργία εργαλείων γονικού ελέγχου. Αυτό οδήγησε στην ελάττωση των κινδύνων με τους οποίους μπορούν να έρθουν αντιμέτωπα τα παιδιά κατά την περιπλάνησή τους στο διαδίκτυο. Ο γονικός έλεγχος εναρμονίζεται με τις τακτικές που ακολουθούν οι γονείς για τη μείωση και τον έλεγχο του χρόνου και την επιτήρηση των ψηφιακών ενεργειών των παιδιών τους.

Όταν ο έλεγχος που πραγματοποιείται προληπτικά και έχει τη μορφή κανόνων και επίβλεψης, τότε τα παιδιά μαθαίνουν τις υποχρεώσεις τους και γνωρίζουν το τι προσδοκούν οι γονείς τους από αυτά.

Όμως, τα μέτρα αυτά εμφανίζουν τα εξής μειονεκτήματα [24]:

- Η απαγόρευση των παιδιών να χρησιμοποιήσουν κάποιο μέσω κοινωνικής δικτύωσης ή να παίξουν κάποιο παιχνίδι έχει ως αποτέλεσμα τη δημιουργία μη επιθυμητών αποτελεσμάτων στο μέλλον. Αυτό οξύνει τις σχέσεις που υπάρχουν μεταξύ γονέα και παιδιού. Οι αξίες και οι κανόνες δε μαθαίνονται στα παιδιά μέσω της τιμωρίας αντίθετα μεγαλώνουν τις πιθανότητες κρυφής και ανεπιθύμητης συμπεριφοράς.

- Οι γονείς δε συνειδητοποιούν πάντα τα ρίσκα και τις απειλές που μπορεί να έρθουν σε επαφή τα παιδιά τους. Για παράδειγμα, οι γονείς μπορεί να εκτιμήσουν λάθος την επαφή των παιδιών τους σε ένα θέαμα σεξουαλικού περιεχομένου και ταυτόχρονα, λόγω των μηνυμάτων των μέσων μαζικής ενημερώσεως, να του δώσουν περισσότερη αξία. Επίσης, ανάμεσα σε γονείς και παιδιά μπορεί να υπάρξει έλλειψη αντιστοιχίας

για το τι είναι επιβλαβή ή όχι.

- Όταν οι γονείς θέλουν να εμποδίσουν τους κινδύνους του διαδικτύου θέτοντας από την αρχή όρια και απαγορεύσεις, είναι πιθανό τα παιδιά να μην έρχονται σε επαφή με συνομηλίκους τους, να μην αλληλοενεργούν και να μην είναι ανεξάρτητοι στον παγκόσμιο ιστό. Ακόμη, οι κινήσεις αυτές δυσχεραίνουν την οικογενειακή κατάσταση ανάμεσα σε γονείς και παιδιά. Επίσης, ενέργειες αυτού του τύπου οδηγούν στην έλλειψη σεβασμού και εμπιστοσύνης προς τους γονείς τους και αυτό επηρεάζει αρνητικά την μεταξύ τους επικοινωνία.

4.4 Εφαρμογές και εργαλεία γονικού ελέγχου

Στη συνέχεια γίνεται μια αναλυτική περιγραφή των εφαρμογών και των εργαλείων εκείνων που έχουν σχεδιαστεί για τη παροχή γονικού ελέγχου αλλά και της εποπτείας του χρονικού διαστήματος που αφιερώνει ένα παιδί στις ψηφιακές συσκευές (ηλεκτρονικός υπολογιστής, έξυπνα τηλέφωνα, tablet) ανάλογα με το λειτουργικό σύστημα που διαθέτουν.

4.5 Microsoft Windows

Η Microsoft, μια από τις πιο γνωστές εταιρίες στο χώρο της πληροφορικής, έχει συμπεριλάβει στο πολύ γνωστό λειτουργικό της σύστημα «Windows» τη δυνατότατα ελέγχου των δραστηριοτήτων χρηστών του ηλεκτρονικού υπολογιστικού συστήματος διαμέσου του εργαλείου του γονικού ελέγχου.

Εικόνα 2: *Γονικός Έλεγχος*

Για να έχουμε τη δυνατότητα να χρησιμοποιήσουμε το εργαλείο αυτό θα πρέπει να έχουμε δικαιώματα ως «Διαχειριστής» του συστήματος. Αυτό γίνεται από τη μεριά της Microsoft ώστε να διασφαλίζεται περισσότερο η ασφάλεια. Γι’ αυτό το λόγο, στον υπολογιστή στον οποίο θέλουμε να έχουμε μια σχετική επιτήρηση θα

πρέπει να ορίσουμε ένα λογαριασμό με δικαιώματα «Διαχειριστή» και ξεχωριστούς λογαριασμούς για τους απλούς χρήστες.

Παρακάτω θα περιγράψουμε τον τρόπο με τον οποίο μπορούμε να ρυθμίσουμε τον ηλεκτρονικό υπολογιστή ή την ψηφιακή μας συσκευή, για την παροχή γονικού ελέγχου, που έχει ως λειτουργικό σύστημα τα «Windows». Λόγω της αναβάθμισης των εκδόσεων των λειτουργικών συστημάτων της Microsoft, η εφαρμογή του γονικού ελέγχου παρουσιάζει αρκετές διαφοροποιήσεις. Για το λόγο αυτό θα αναλύσουμε ξεχωριστά την εφαρμογή του γονικού ελέγχου ανάλογα με την έκδοση του λειτουργικού συστήματος.

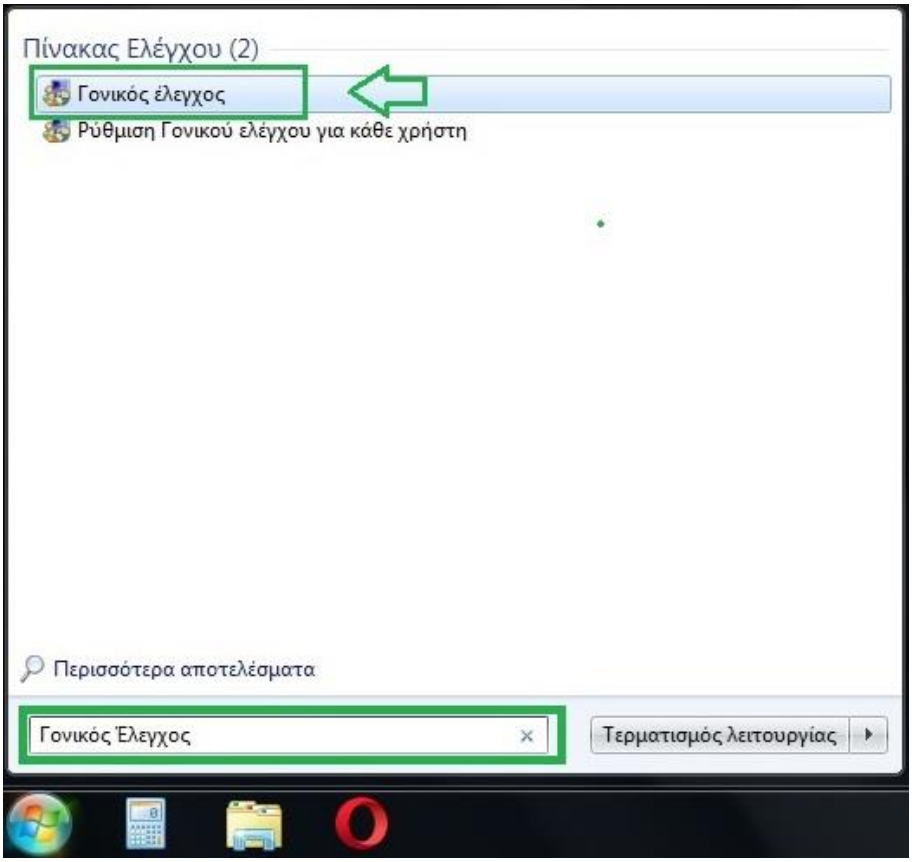
Συγκεκριμένα θα ασχοληθούμε με τις πιο διαδεδομένες εκδόσεις:

- Windows 7
- Windows 8
- Windows 10

Εικόνα 3: *Γονικός Έλεγχος -Microsoft Windows*

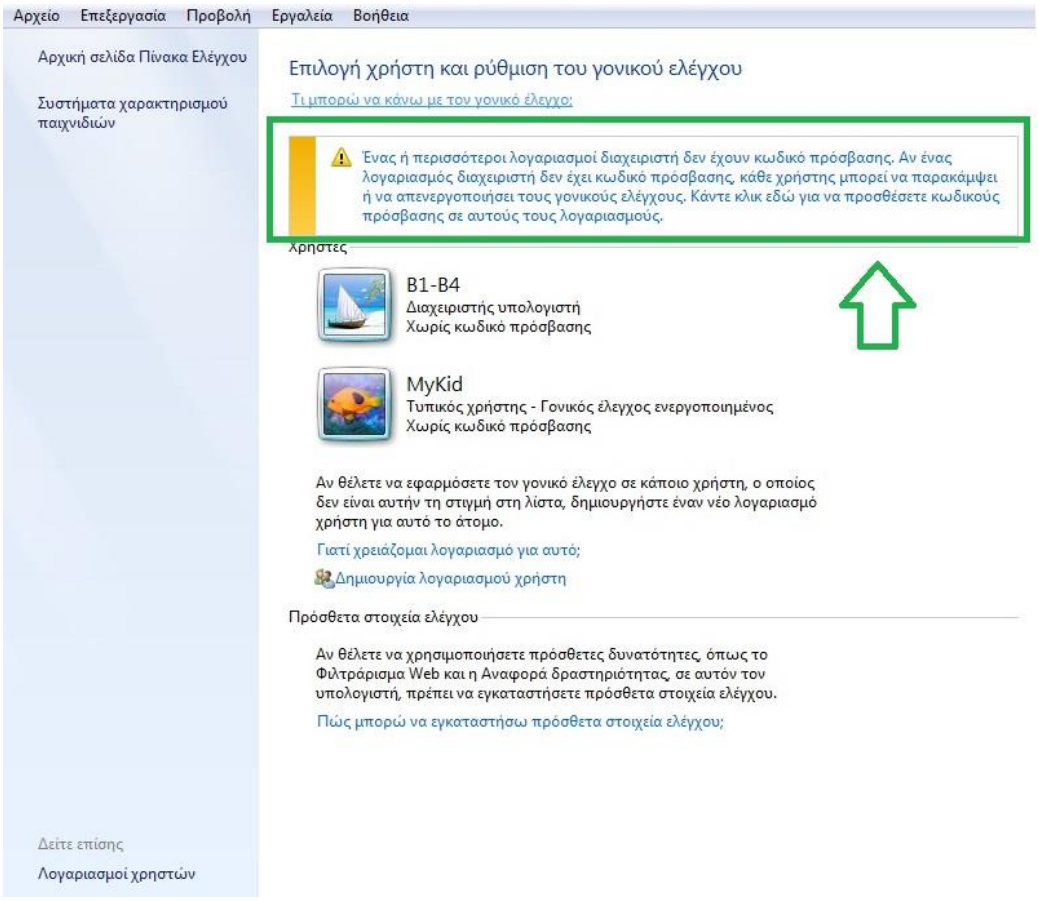
4.5.1 Εφαρμογή γονικού ελέγχου στα Windows 7

Ο πιο απλός τρόπος για την πρόσβαση στο γονικό έλεγχο των Windows 7 γίνεται μέσω του πλαισίου αναζήτησης του μενού «Έναρξη». Στο πλαίσιο αυτό πληκτρολογούμε απλά «Γονικός Έλεγχος» και στη συνέχεια πατάμε το enter.



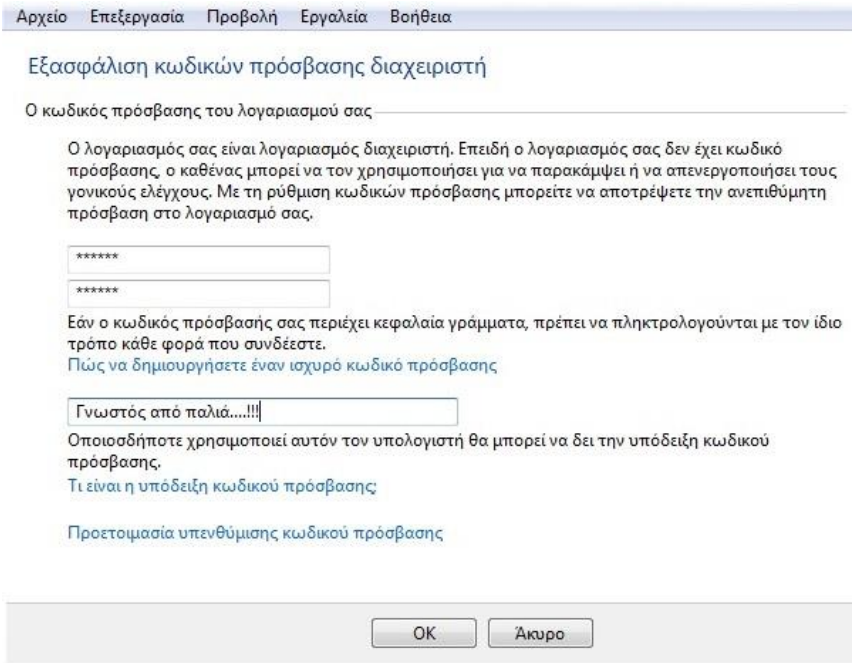
Εικόνα 4: *Windows 7: Γονικός Έλεγχος – Βήμα 1^{ο}*

Βασική προϋπόθεση για τη λειτουργία και εφαρμογή του γονικού ελέγχου είναι η σύνδεση στον ηλεκτρονικό υπολογιστή με δικαιώματα «διαχειριστή». Απαραίτητο είναι να υπάρχει κωδικός πρόσβασης στο λογαριασμό του διαχειριστή για το λόγο ότι ο απλός χρήστης να μη μπορεί να παρακάμψει τη λειτουργία του γονικού ελέγχου.



Εικόνα 5: *Windows 7: Γονικός Έλεγχος – Βήμα 2^{ο}*

Εάν δεν έχουμε δημιουργήσει κωδικό πρόσβασης, το εργαλείο του γονικού ελέγχου μας προτρέπει να πράξουμε αναλόγως.

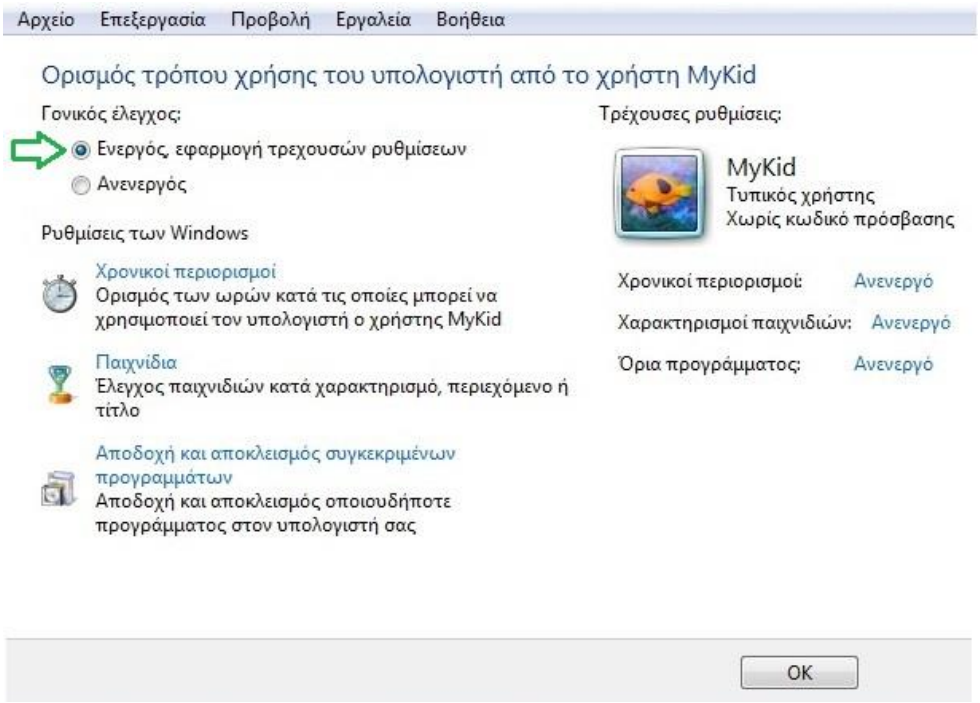


Εικόνα 6: *Windows 7: Γονικός Έλεγχος – Βήμα 3^{ο}*

Στη συνέχεια, επιλέγουμε το χρήστη στον οποίο επιθυμούμε να εφαρμόσουμε το γονικό έλεγχο.

Εικόνα 7: *Windows 7: Γονικός Έλεγχος – Βήμα 4^{ο}*

Στο παράθυρο που ανοίγει ενεργοποιούμε το γονικό έλεγχο επιλέγοντας «Ενεργός εφαρμογή τρεχουσών ρυθμίσεων».



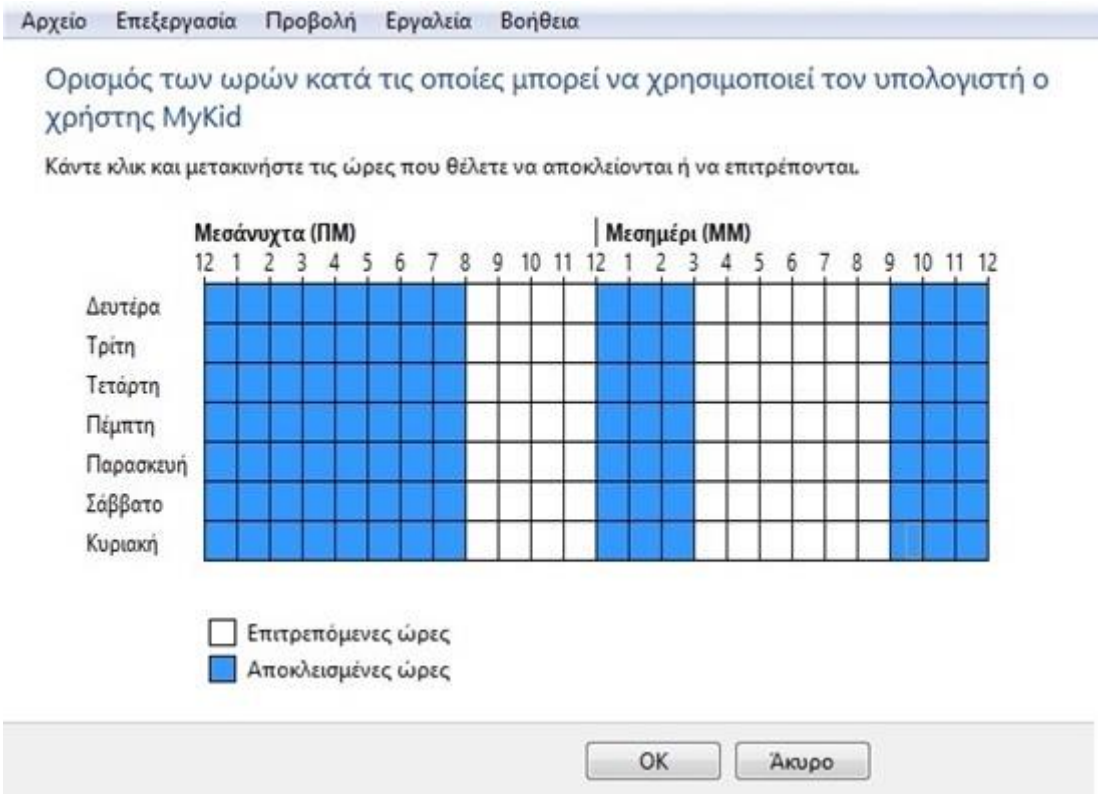
Εικόνα 8: *Windows 7: Γονικός Έλεγχος – Βήμα 5^{ο}*

Οι ρυθμίσεις του γονικού ελέγχου είναι αρκετές και αφορούν το καθορισμό των ωρών κατά τις οποίες ο χρήστης μπορεί να χρησιμοποιεί τον υπολογιστή, τα παιχνίδια τα οποία επιτρέπονται και η αποδοχή ή αποκλεισμός οποιοδήποτε εφαρμογών που είναι εγκατεστημένα στον ηλεκτρονικό υπολογιστή. Στη δεξί μέρος του παραθύρου υπάρχει σχετική πληροφόρηση για το ποιες ρυθμίσεις είναι ενεργές και ποιες όχι.

- Ρυθμίσεις των Windows 7: *Χρονικοί Περιορισμοί*

Στη ρύθμιση «Χρονικοί περιορισμοί» ο διαχειριστής καθορίζει τις ημέρες και τις ώρες της εβδομάδας όπου ο χρήστης μπορεί να χρησιμοποιεί τον ηλεκτρονικό υπολογιστή.

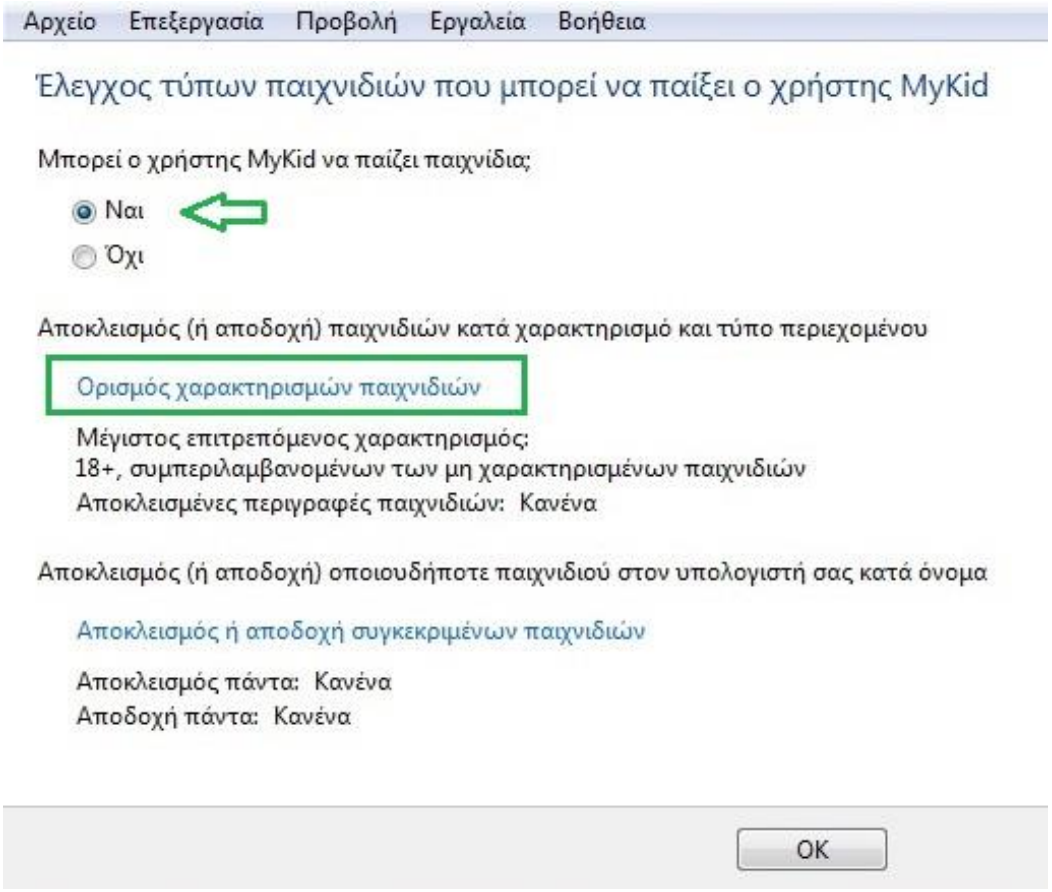
Ο διαχειριστής επιλέγει τις ώρες που θέλει για κάθε μια μέρα της εβδομάδας κάνοντας κλικ σε κάθε ένα κουτάκι. Με άσπρο χρώμα ορίζονται οι επιτρεπόμενες ώρες και με μπλε ορίζονται οι ώρες που δεν επιτρέπεται η πρόσβαση στο υπολογιστικό σύστημα.



Εικόνα 9: *Windows 7: Γονικός Έλεγχος – Βήμα 6^{ο}*

- Ρυθμίσεις των Windows 7: *Παιχνίδια*

Η επόμενη κατά σειρά ρύθμιση του γονικού ελέγχου αφορά τα «Παιχνίδια». Στο σημείο αυτό καθορίζεται από το διαχειριστή η δυνατότητα του χρήστη να παίζει παιχνίδια στον υπολογιστή αλλά και να ορίσει κάποιος περιορισμούς.



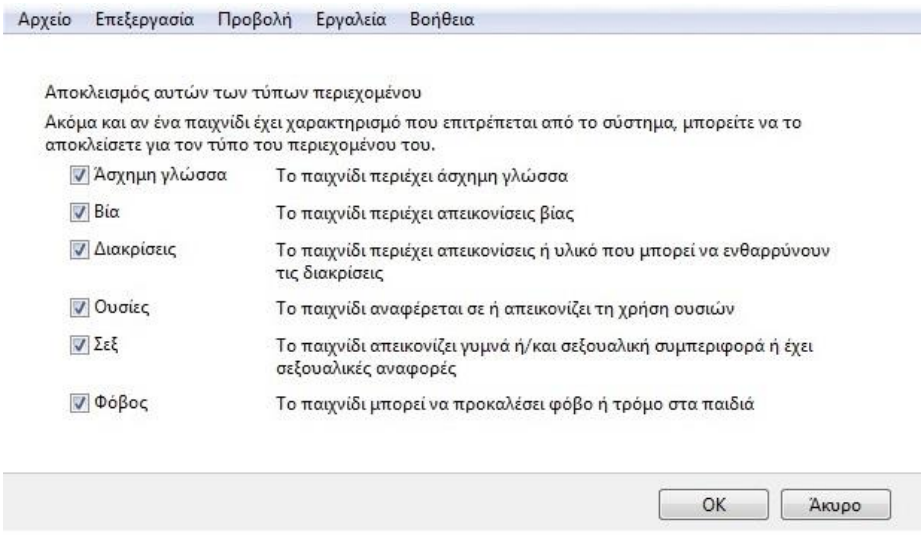
Εικόνα 10: *Windows 7: Γονικός Έλεγχος – Βήμα 7^{ο}*

Εάν θέλουμε ο χρήστης να παίζει παιχνίδια τότε στην ερώτηση «Μπορεί ο χρήστης MyKid να παίζει παιχνίδια;» επιλέγουμε «Ναι». Επίσης, μας δίνεται η δυνατότητα να αποκλείσουμε ή όχι τα παιχνίδια εκείνα τα οποία δεν έχουν τον προαπαιτούμενο χαρακτηρισμό.

Στη συνέχεια καθορίζουμε την επιτρεπόμενη ηλικιακή ομάδα σύμφωνα με το διεθνές πρότυπο PEGI.

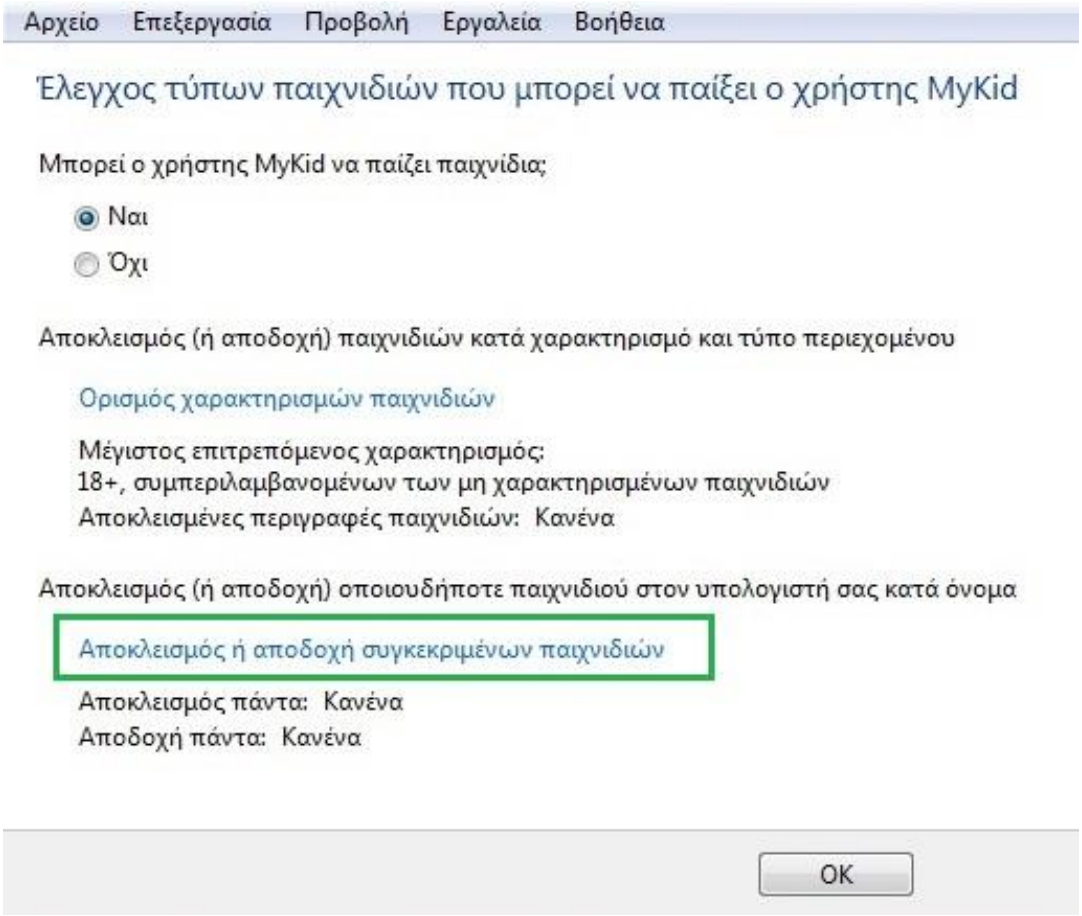
Εικόνα 11: *Windows 7: Γονικός Έλεγχος – Βήμα 8^{ο}*

Επιπλέον, υπάρχει η δυνατότητα αποκλεισμού παιχνιδιών που χαρακτηρίζονται από ένα συγκεκριμένο τύπο περιεχομένου.



Εικόνα 12: *Windows 7: Γονικός Έλεγχος – Βήμα 9^{ο}*

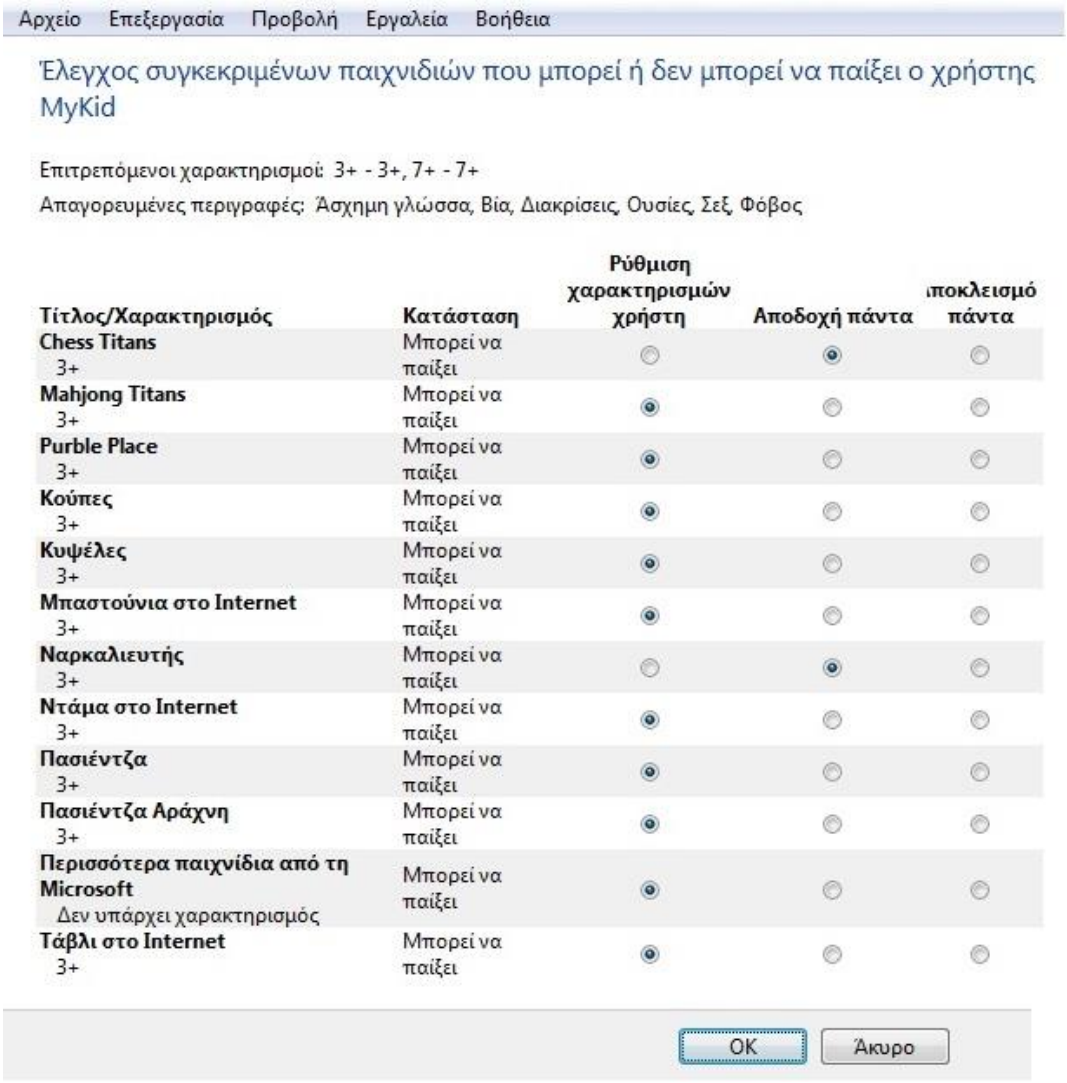
Από τις τελικές ρυθμίσεις που μας παρέχουν τα Windows 7 για την εφαρμογή του γονικού ελέγχου στα παιχνίδια είναι η αποδοχή ή ο αποκλεισμός συγκεκριμένων παιχνιδιών που μπορεί να παίξει ο χρήστης στον υπολογιστή.



Εικόνα 13: *Windows 7: Γονικός Έλεγχος – Βήμα 10^{ο}*

Επιλέγοντας τη ρύθμιση αυτή, ανοίγει ένα παράθυρο το οποίο περιλαμβάνει μια λίστα με όλα τα παιχνίδια τα οποία είναι εγκατεστημένα στον ηλεκτρονικό υπολογιστή.

Στη δεξιά πλευρά ο διαχειριστής καθορίζει για κάθε ένα παιχνίδι χωριστά, εάν ο χρήστης θα μπορεί να έχει πρόσβαση ή όχι.



Εικόνα 14: *Windows 7: Γονικός Έλεγχος – Βήμα 11^{ο}*

Η επιλογή «Ρύθμιση χαρακτηρισμών χρήστη» είναι προεπιλεγμένη και αφορά όλες τις επιλογές που έχει ήδη ρυθμίσει ο διαχειριστής.

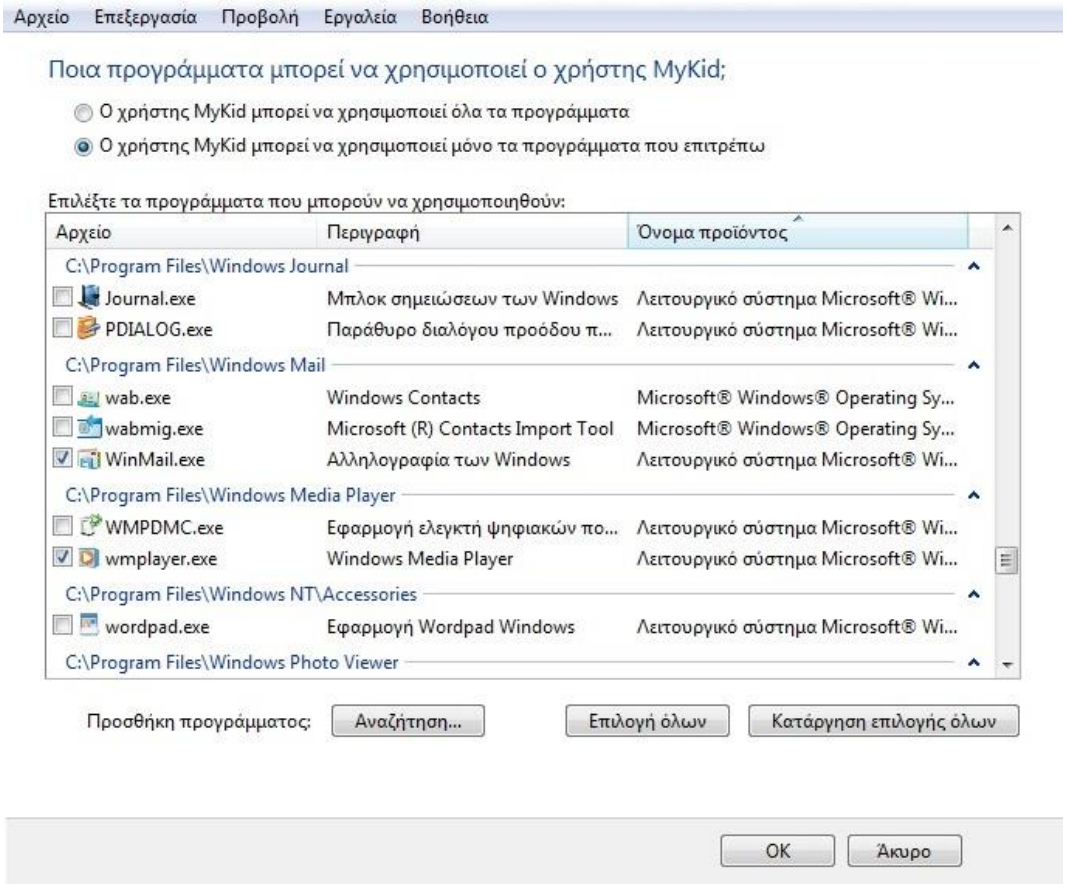
Με την επιλογή «Αποδοχή πάντα» ο χρήστης μπορεί να έχει πρόσβαση στο παιχνίδι παρόλο τους περιορισμούς που ήδη έχουν γίνει νωρίτερα από τον διαχειριστή.

Η επιλογή «Αποκλεισμός πάντα» ο χρήστης δεν μπορεί να έχει πρόσβαση στο παιχνίδι για το οποίο είναι ενεργοποιημένη η εν λόγω επιλογή.

- Ρυθμίσεις των Windows 7: Αποδοχή και αποκλεισμός συγκεκριμένων προγραμμάτων

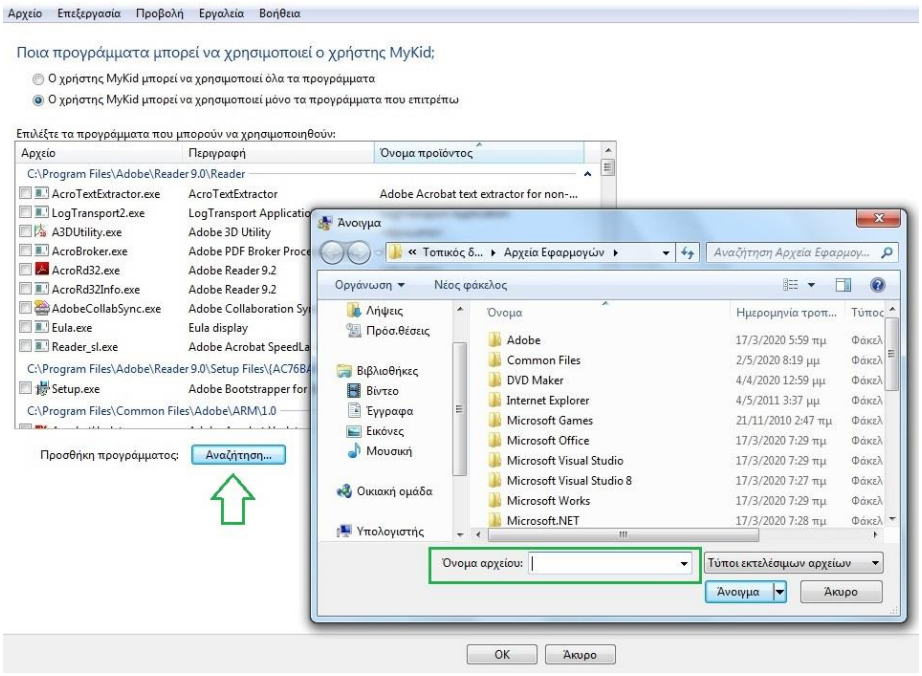
Στη ρύθμιση «Αποδοχή και αποκλεισμός συγκεκριμένων προγραμμάτων» ο διαχειριστής καθορίζει σε ποια προγράμματα και εφαρμογές μπορεί να έχει πρόσβαση ο χρήστης.

Υπάρχουν δύο επιλογές. Η πρώτη επιτρέπει στο χρήστη να χρησιμοποιεί όλα τα προγράμματα και η δεύτερη επιτρέπει στο χρήστη να χρησιμοποιεί μόνο τα προγράμματα που επιθυμεί ο διαχειριστής και έχει επιλέξει από τη λίστα των προγραμμάτων του ηλεκτρονικού υπολογιστή.



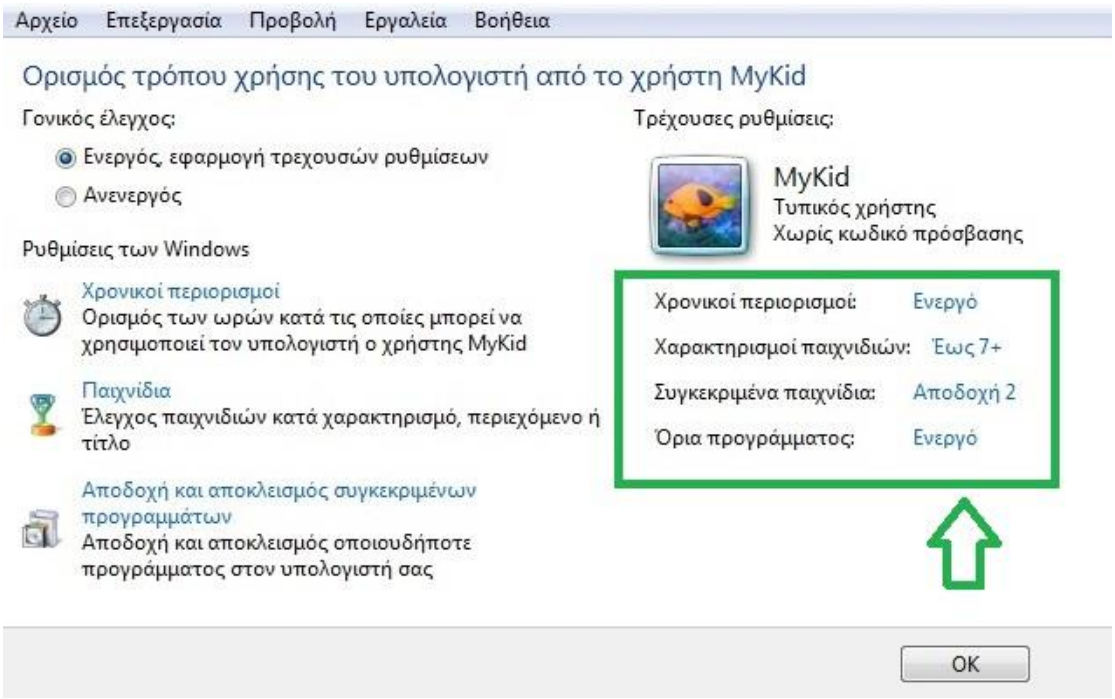
Εικόνα 15: *Windows 7: Γονικός Έλεγχος – Βήμα 12^{ο}*

Στην περίπτωση που κάποια από τις εφαρμογές δεν εμφανίζεται στη λίστα επιλογής αλλά ο διαχειριστής επιθυμεί να δώσει δικαιώματα στο χρήστη να τη χρησιμοποιεί, τότε γίνεται αναζήτηση της εφαρμογής μέσω της σχετικής επιλογής και προσθήκη στη σχετική λίστα.



Εικόνα 16: *Windows 7: Γονικός Έλεγχος – Βήμα 13^{ο}*

Με την ολοκλήρωση των παραπάνω διαδικασιών, οι ρυθμίσεις του γονικού ελέγχου έχουν πλέον ολοκληρωθεί για το λογαριασμό του συγκεκριμένου χρήστη.



Εικόνα 17: *Windows 7: Γονικός Έλεγχος – Βήμα 14^{ο}*

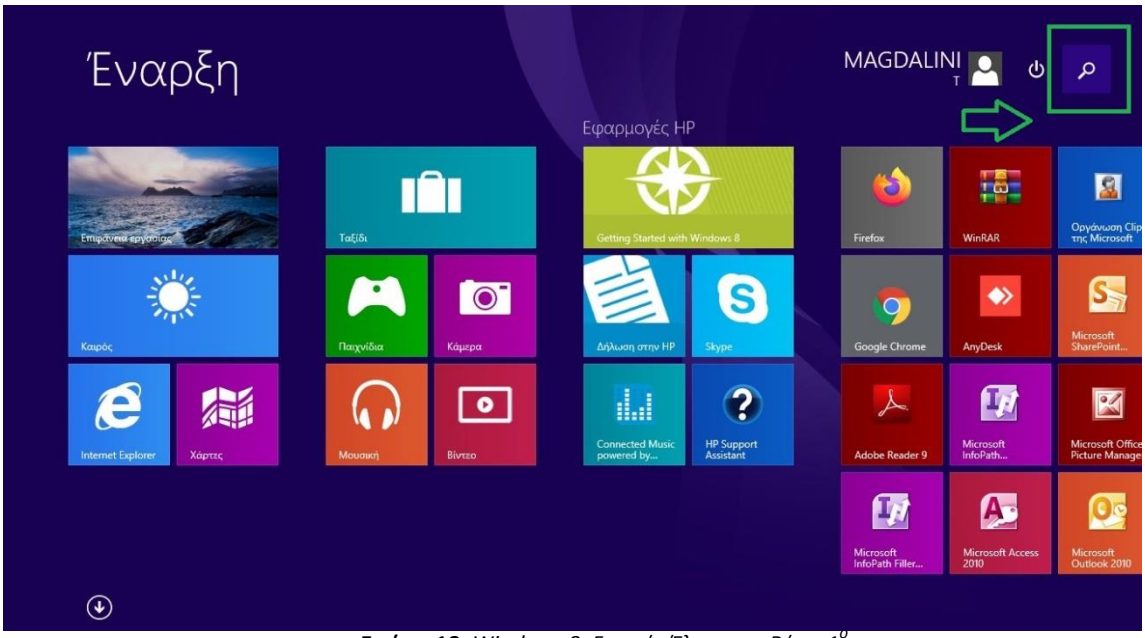
Ένα ο διαχειριστής επιθυμεί να εφαρμόσει το γονικό έλεγχο και σε άλλους λογαριασμούς χρηστών στο συγκεκριμένο υπολογιστικό σύστημα, θα πρέπει να ακολουθηθεί ακριβώς όλη η παραπάνω διαδικασία.

4.5.2 Εφαρμογή γονικού ελέγχου στα Windows 8

Στο λειτουργικό σύστημα των Windows 8, η Microsoft αναβάθμισε τη λειτουργία του γονικού ελέγχου και παρέχει στους χρήστες περισσότερες δυνατότητες και επιλογές από αυτές των Windows 7. Με την αναβάθμιση αυτή ο διαχειριστής μπορεί πλέον να ελέγχει τη δραστηριότητα του χρήστη στον ηλεκτρονικό υπολογιστή αλλά και στον παγκόσμιο ιστό.

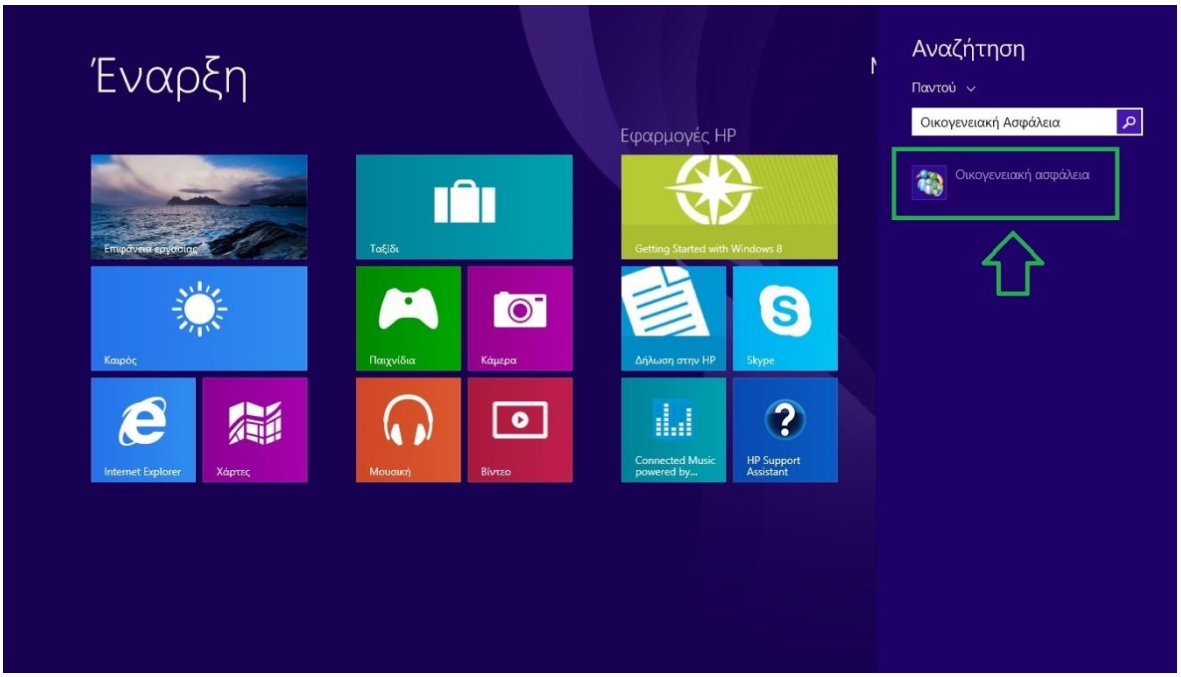
Επίσης, ένα ακόμα σημαντικό πλεονέκτημα που υπάρχει στα Windows 8 είναι η δυνατότητα διαχείρισης του γονικού ελέγχου μέσω διαδικτύου.

Για να μπορέσουμε να έχουμε πρόσβαση και να διαχειριστούμε το γονικό έλεγχο στα **Windows 8**, πληκτρολογούμε «Οικογενειακή ασφάλεια» στην «αναζήτηση» της οθόνης Έναρξης και την επιλέγουμε .



Εικόνα 18: *Windows 8: Γονικός Έλεγχος – Βήμα 1ο*

Εφόσον το επιλέξουμε, θα ανοίξει το σχετικό παράθυρο της «οικογενειακής ασφάλειας» το οποίο είναι παρόμοιο με το παράθυρο ρυθμίσεων γονικού ελέγχου των Windows 7.

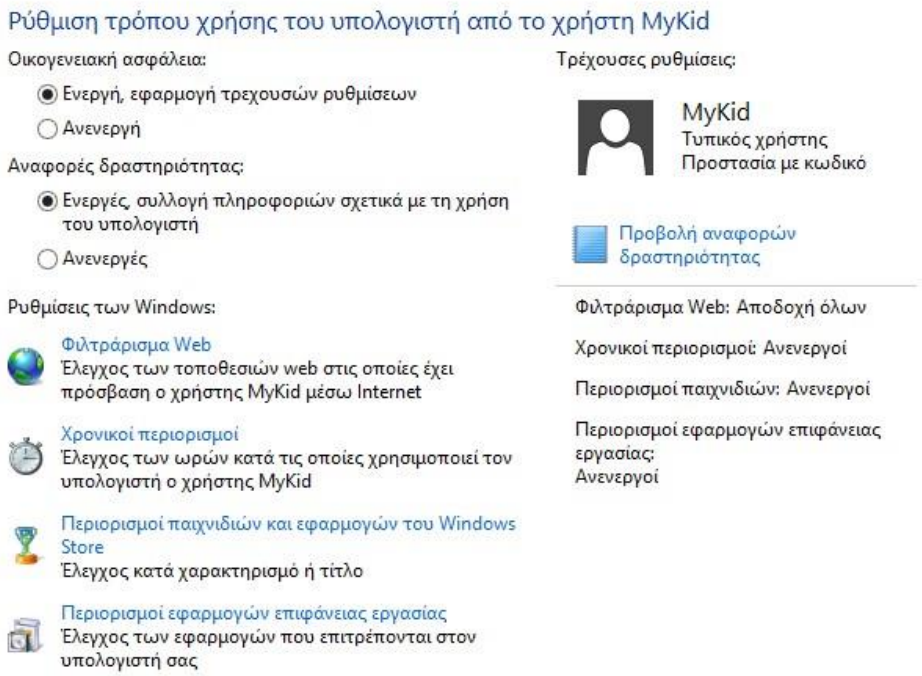


Εικόνα 19: *Windows 8: Γονικός Έλεγχος – Βήμα 2^{ο}*

Στο παράθυρο αυτό, εμφανίζονται οι χρήστες του λειτουργικού συστήματος και διαλέγουμε τον χρήστη εκείνο στον οποίο θέλουμε να κάνουμε τις σχετικές ρυθμίσεις της οικογενειακής ασφάλειας.

Εικόνα 20: *Windows 8: Γονικός Έλεγχος – Βήμα 3^{ο}*

Μόλις επιλέξουμε το χρήστη, ανοίγει το παράθυρο της διαχείρισης των ρυθμίσεων. Στο παράθυρο αυτό εμφανίζονται με τη σειρά όλες οι ρυθμίσεις γονικού ελέγχου που μπορούμε να διαχειριστούμε και οι πληροφορίες με την τρέχουσα κατάσταση που βρισκόμαστε.

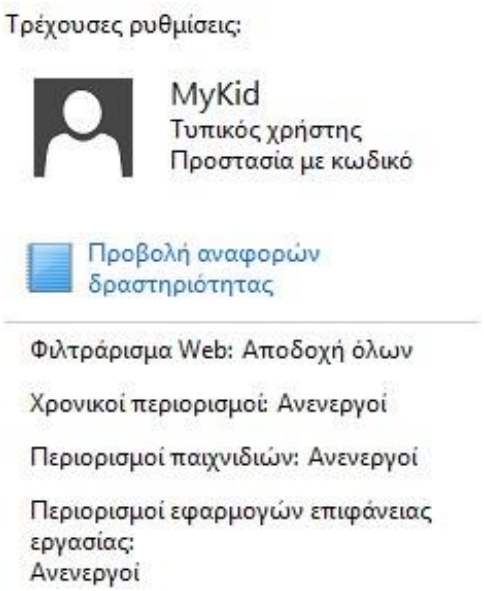


Εικόνα 21: *Windows 8: Γονικός Έλεγχος – Βήμα 4^{ο}*

Η πρώτη μας ενέργεια που πρέπει να κάνουμε είναι η ενεργοποίηση της οικογενειακής ασφάλειας. Εάν η επιλογή «οικογενειακή ασφάλεια» είναι ανενεργή, τότε και ο γονικός έλεγχος είναι ανενεργός και δεν έχουμε πρόσβαση στις σχετικές ρυθμίσεις. Οπότε, κάνουμε κλικ στην επιλογή «Ενεργή, εφαρμογή τρεχουσών ρυθμίσεων» και ξεκινάμε να ρυθμίσουμε τη λειτουργία του γονικού ελέγχου.

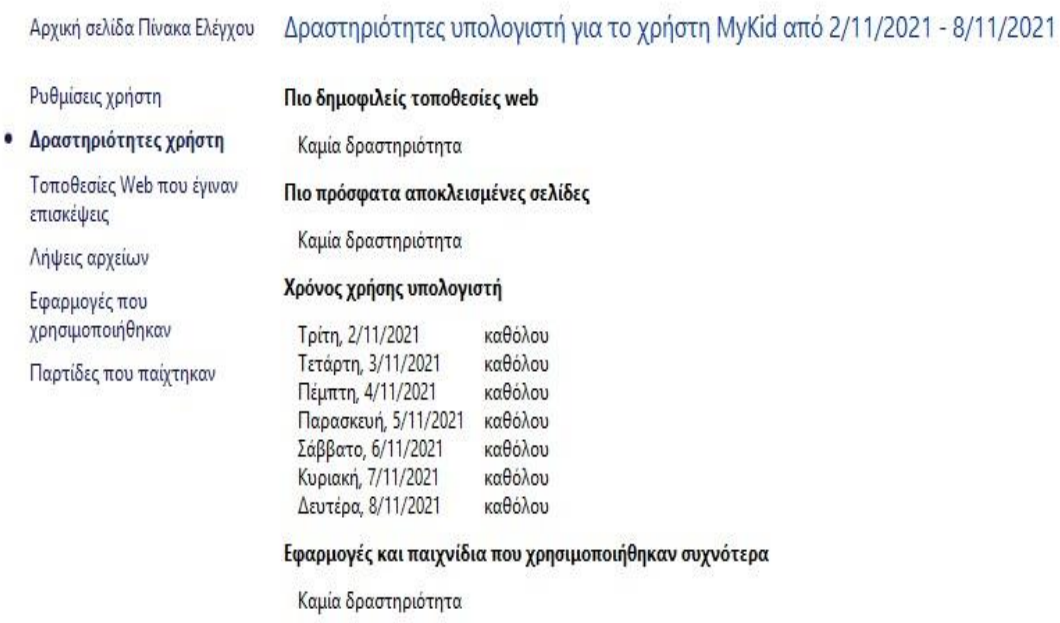
Η ακριβώς επόμενη επιλογή, «Αναφορά δραστηριότητας», όταν είναι ενεργοποιημένη μας πληροφορεί σχετικά με τη δραστηριότητα χρήσης του ηλεκτρονικού υπολογιστή από τον συγκεκριμένο χρήση και δημιουργείται μια λίστα αναφοράς.

Για να μπορέσουμε να προβάλουμε τη λίστα αυτή κάνουμε κλικ στην επιλογή «Προβολή αναφορών δραστηριότητας».



Εικόνα 22: *Windows 8: Γονικός Έλεγχος – Βήμα 5^{ο}*

Οι αναφορές δραστηριότητας αφορούν τις τοποθεσίες στο διαδίκτυο που επισκέπτεται πιο συχνά ο χρήστης, το χρόνο που αφιερώνει στη χρήση του υπολογιστή σε εβδομαδιαία βάση, ποια παιχνίδια και ποιες εφαρμογές χρησιμοποιεί περισσότερο.

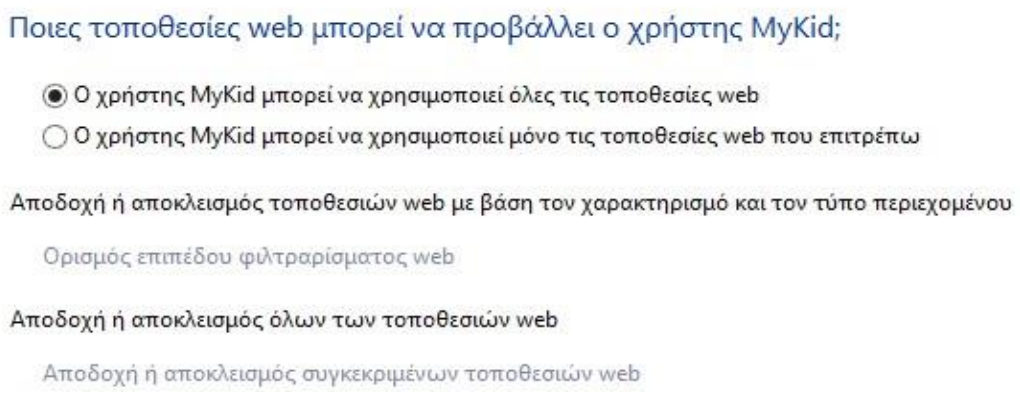


Εικόνα 23: *Windows 8: Γονικός Έλεγχος – Βήμα 6^{ο}*

- Ρυθμίσεις των Windows 8: Φιλτράρισμα Web

Επόμενη κατά σειρά ενέργεια για τη ρύθμιση του γονικού ελέγχου είναι το «Φιλτράρισμα Web». Με την επιλογή αυτή, ορίζουμε τα επίπεδα ασφαλείας για την πλοήγηση στον παγκόσμιο ιστό.

Καθορίζουμε ότι ο χρήστης (στη προκειμένη περίπτωση “MyKid”) θα μπορεί να χρησιμοποιεί ή όλες τις τοποθεσίες web ή μόνο τις τοποθεσίες web του επιτρέπει ο διαχειριστής του συστήματος.



Εικόνα 24: *Windows 8: Γονικός Έλεγχος – Βήμα 7^{ο}*

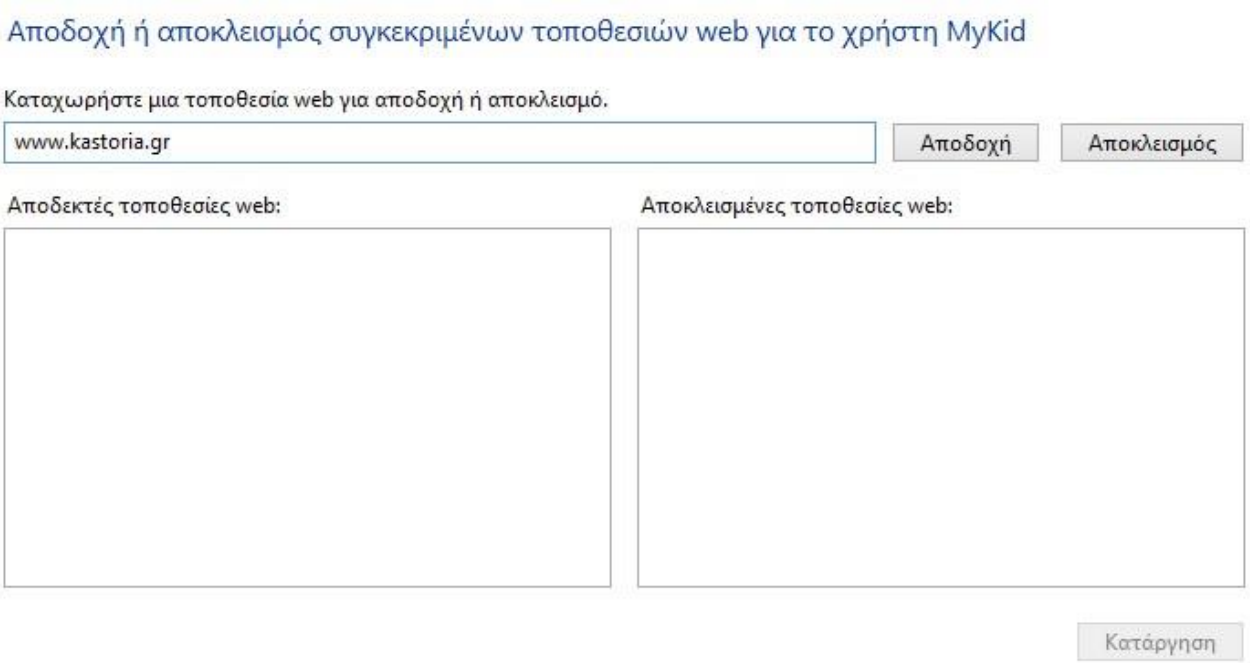
Υπάρχει μια πληθώρα επιλογών για να ρυθμίσουμε τα επίπεδα των περιορισμών της πλοήγησης του χρήστη στο διαδίκτυο. Από τις βασικότερες επιλογές στο σημείο αυτό είναι η δημιουργία λίστας σύμφωνα με την οποία τα παιδιά μπορούν να προβάλλουν μόνο τοποθεσίες που βρίσκονται στη λίστα αποδοχής.

Επίσης, οι τοποθεσίες για ενηλίκους είναι αποκλεισμένες.

Εικόνα 25: *Windows 8: Γονικός Έλεγχος – Βήμα 8^{ο}*

Για τον καθορισμό συγκεκριμένων ιστοτόπων όπου ο χρήστης μπορεί να έχει πρόσβαση, επιλέγουμε την «Αποδοχή ή αποκλεισμός συγκεκριμένων τοποθεσιών web».

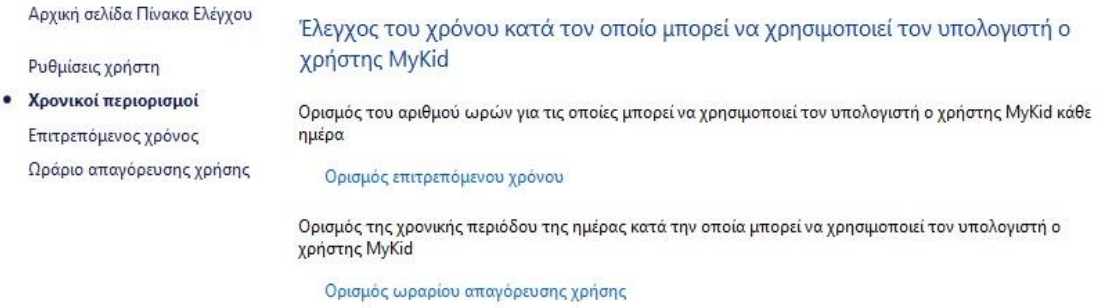
Η διαδικασία καταχώρησης των διευθύνσεων των ιστοτόπων γίνεται με τη πληκτρολόγηση της διεύθυνσης της ιστοσελίδας στο σχετικό πλαίσιο καταχώρησης και αναλόγως επιλέγουμε «Αποδοχή» ή «Αποκλεισμό».



Εικόνα 26: *Windows 8: Γονικός Έλεγχος – Βήμα 9^{ο}*

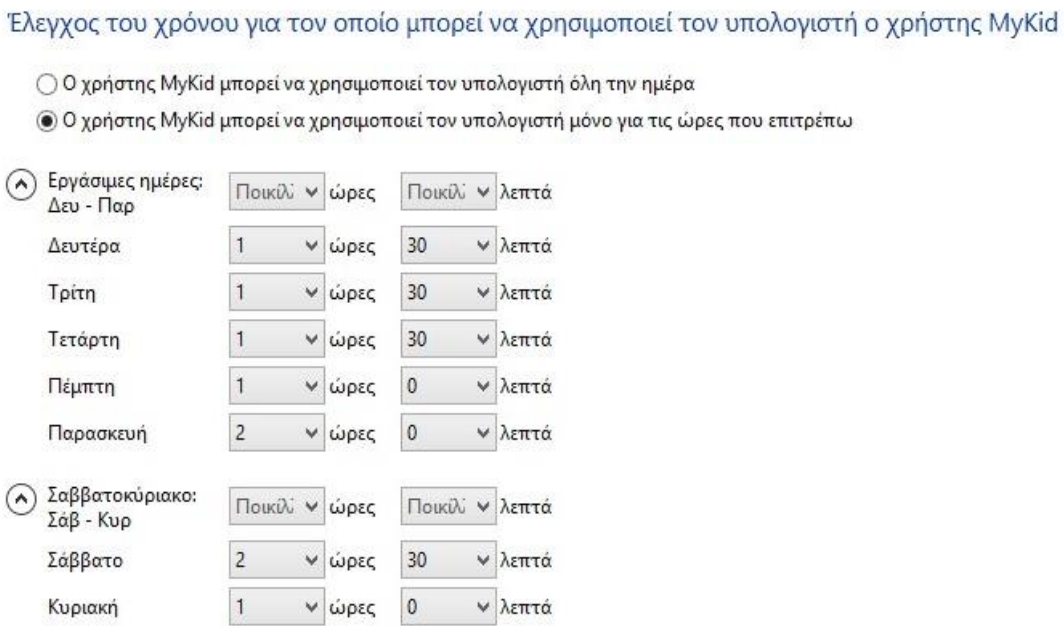
- Ρυθμίσεις των Windows 8: Χρονικοί περιορισμοί

Επιλέγοντας τη ρύθμιση «Χρονικοί περιορισμοί», όπως και στα Windows 7, ο διαχειριστής καθορίζει ποιες μέρες και ώρες την εβδομάδα μπορεί ο χρήστης να χρησιμοποιεί το υπολογιστικό σύστημα. Επιπλέον, οριοθετεί και το συνολικό χρόνο χρήσης του ηλεκτρονικού υπολογιστή.



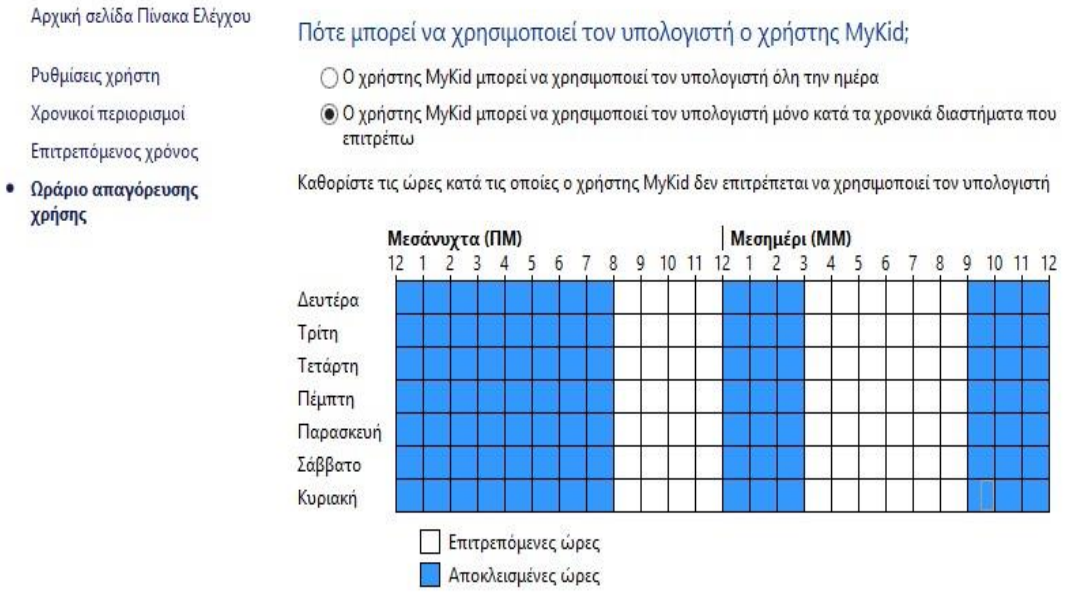
Εικόνα 27: *Windows 8: Γονικός Έλεγχος – Βήμα 10^{ο}*

Ο διαχειριστής έχει τη δυνατότητα να ορίσει τον επιτρεπόμενο χρόνο χρήσης του ηλεκτρονικού υπολογιστή ξεχωριστά για τις ημέρες από Δευτέρα έως Παρασκευή και ξεχωριστά για το Σαββατοκύριακο.



Εικόνα 28: *Windows 8: Γονικός Έλεγχος – Βήμα 11^{ο}*

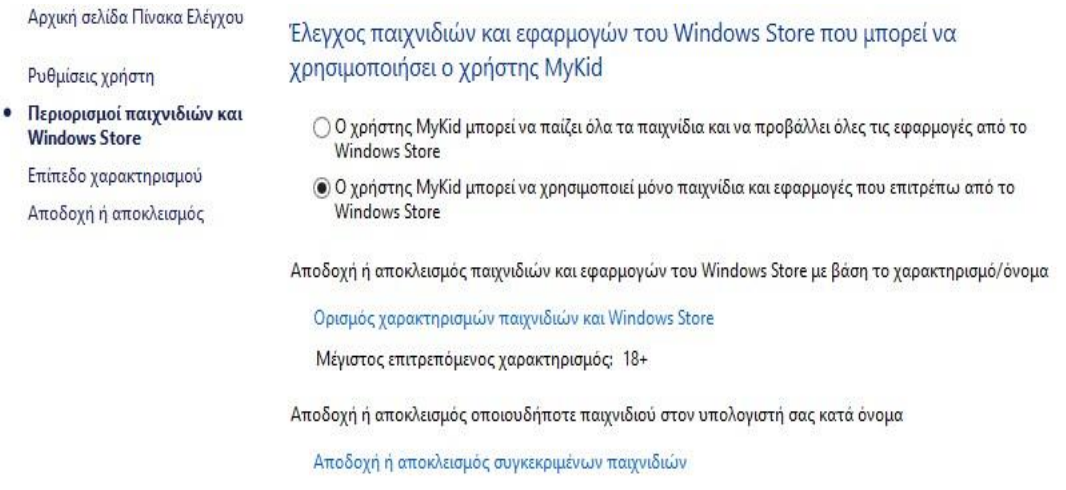
Για να γίνει ο καθορισμός συγκεκριμένων ωρών χρήσης μέσα στη εβδομάδα επιλέγουμε το «Ωράριο απαγόρευσης χρήσης» ορίζουμε τα χρονικά διαστήματα που απαγορεύεται στον χρήστη να χρησιμοποιεί τον ηλεκτρονικό υπολογιστή.



Εικόνα 29: *Windows 8: Γονικός Έλεγχος – Βήμα 12^{ο}*

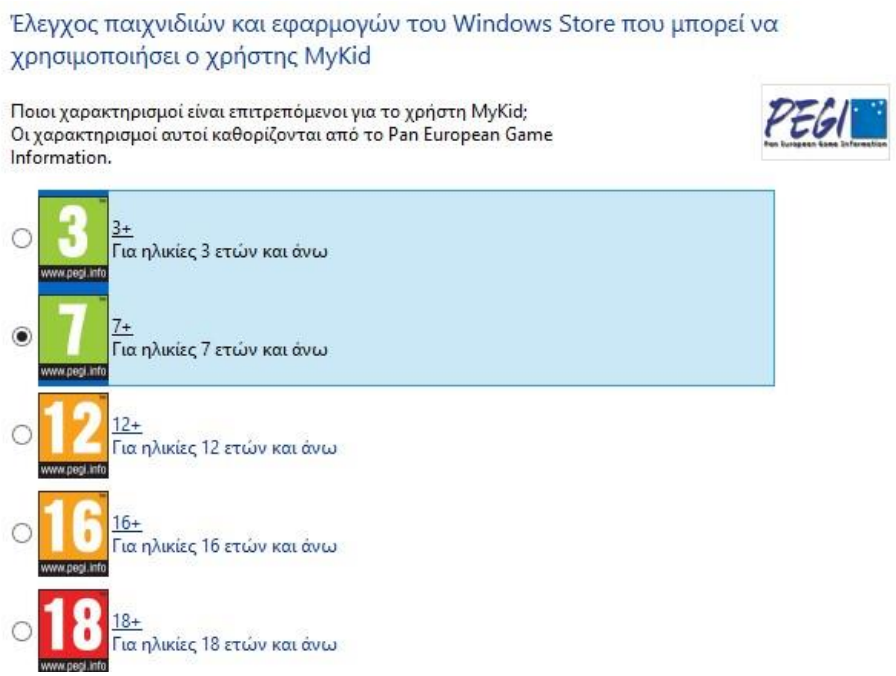
- Ρυθμίσεις των Windows: Περιορισμοί παιχνιδιών και εφαρμογών του Windows Store

Με τους «Περιορισμούς παιχνιδιών και εφαρμογών του Windows Store» ο διαχειριστής του συστήματος έχει την ικανότητα να επιτρέπει ή όχι στον χρήστη την πρόσβαση σε παιχνίδια σύμφωνα με το ηλικιακό χαρακτηρισμό. Η αποδοχή ή ο αποκλεισμός οποιουδήποτε παιχνιδιού στον ηλεκτρονικό υπολογιστή γίνεται με την επιλογή στο «Αποδοχή ή αποκλεισμός συγκεκριμένων παιχνιδιών».



Εικόνα 30: *Windows 8: Γονικός Έλεγχος – Βήμα 13^{ο}*

Ο ορισμός χαρακτηρισμός παιχνιδιών υλοποιείται σύμφωνα με το διεθνές πρότυπο PEGI.

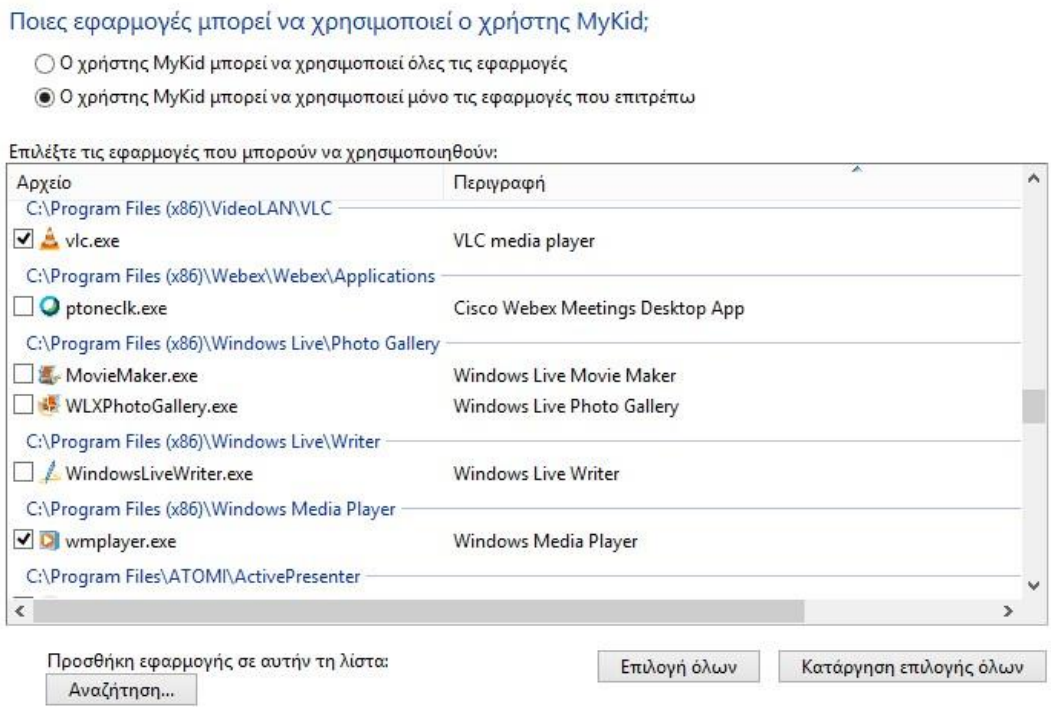


Εικόνα 31: *Windows 8: Γονικός Έλεγχος – Βήμα 14^{ο}*

- *Ρυθμίσεις των Windows:* Περιορισμός εφαρμογών επιφάνειας εργασίας

Πέρα από την εφαρμογή ελέγχου στα παιχνίδια, ο διαχειριστής μπορεί να καθορίσει και τον έλεγχο στις εφαρμογές οι οποίες είναι επιτρεπτές στον χρήστη. Αυτό γίνεται εφικτό από την επιλογή «Περιορισμοί εφαρμογών επιφάνειας εργασίας».

Οπότε κάνοντας, ενεργοποιώντας τη λειτουργία αυτή, επιλέγουμε μέσα από την αντίστοιχη λίστα των Windows, τις εφαρμογές εκείνες οι οποίες είναι εγκατεστημένες στον ηλεκτρονικό υπολογιστή και επιθυμούμε να έχει πρόσβαση ο χρήστης.



Εικόνα 32: *Windows 8: Γονικός Έλεγχος – Βήμα 15^{ο}*

Αν για κάποιο λόγο, θέλουμε να δώσουμε πρόσβαση σε μια συγκεκριμένη εφαρμογή η οποία όμως δεν εμφανίζεται στην αντίστοιχη λίστα, τότε μέσω της επιλογής «Προσθήκη εφαρμογής σε αυτήν τη λίστα», αναζητούμε την εφαρμογή στο σύστημα και την προσθέτουμε.

- Διαχείριση ρυθμίσεων Οικογενειακής ασφάλειας

Εκτός από την τοπική διαχείριση του γονικού ελέγχου στα Windows 8 που αναπτύξαμε, το παραπάνω λειτουργικό σύστημα παρέχει την ικανότητα διαχείρισης της οικογενειακής ασφάλειας μέσω του διαδικτύου.

Η σημαντική αυτή λειτουργία αυτή υλοποιείται μέσω online υπηρεσία της Microsoft που για την ενεργοποίησή της το μόνο που χρειάζεται είναι η ύπαρξη λογαριασμού στη Microsoft. Με αυτόν τον τρόπο η διαχείριση και η εποπτεία της γονικής μέριμνας υλοποιείται απομακρυσμένα και από οπουδήποτε.

Εικόνα 33: *Windows 8: Γονικός Έλεγχος – Βήμα 16^{ο}*

Βασική προϋπόθεση για την ενεργοποίηση της «Διαχείριση ρυθμίσεων στην τοποθεσία web Οικογενειακής ασφάλειας» θα πρέπει να έχουμε συνδεθεί στη Microsoft. Για να το επιτύχουμε αυτό χρειάζεται ο κωδικός πρόσβασης του διαχειριστή και η επιβεβαίωση των στοιχείων μας από τα windows.

Στη συνέχεια πατώντας στην επιλογή «Διαχείριση ρυθμίσεων στην τοποθεσία web Οικογενειακής ασφάλειας» ενεργοποιείται η απομακρυσμένη διαχείριση οικογενειακής ασφάλειας και μεταβαίνουμε στην αντίστοιχη σελίδα.

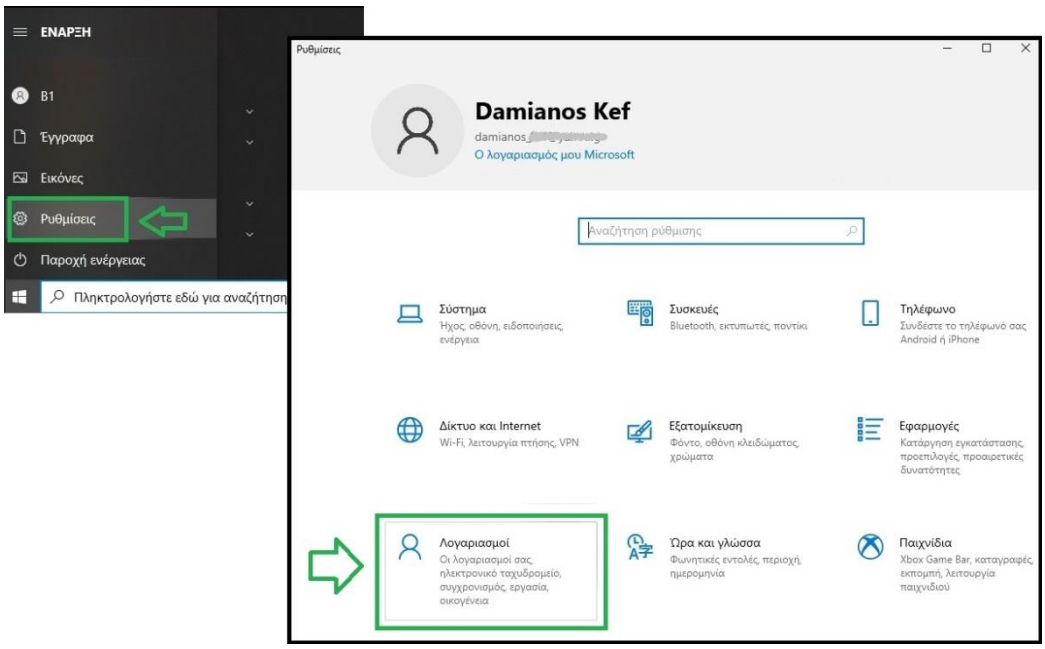
Στο σημείο αυτό μπορούμε πλέον να διαχειριστούμε τον γονικό έλεγχο στους λογαριασμούς των χρηστών του ηλεκτρονικού υπολογιστή για τους οποίους έχει ενεργοποιηθεί. Υπενθυμίζουμε ότι για την εφαρμογή της απομακρυσμένης λειτουργίας του γονικού ελέγχου πρέπει να έχει προηγηθεί και η τοπική ενεργοποίησή του στις εν λόγω ψηφιακές συσκευές.

4.5.3 Εφαρμογή γονικού ελέγχου στα Windows 10

Στο λειτουργικό σύστημα των Windows 10 της Microsoft, η εφαρμογή του γονικού ελέγχου έχει ως απαραίτητη προϋπόθεση ο διαχειριστής (Ενήλικας) και ο χρήστης (Παιδί) να διαθέτουν λογαριασμό στη Microsoft και η διαχείριση για την ασφαλή πλοήγηση των μελών της «οικογένειας» γίνεται αποκλειστικά μέσω του διαδικτύου.

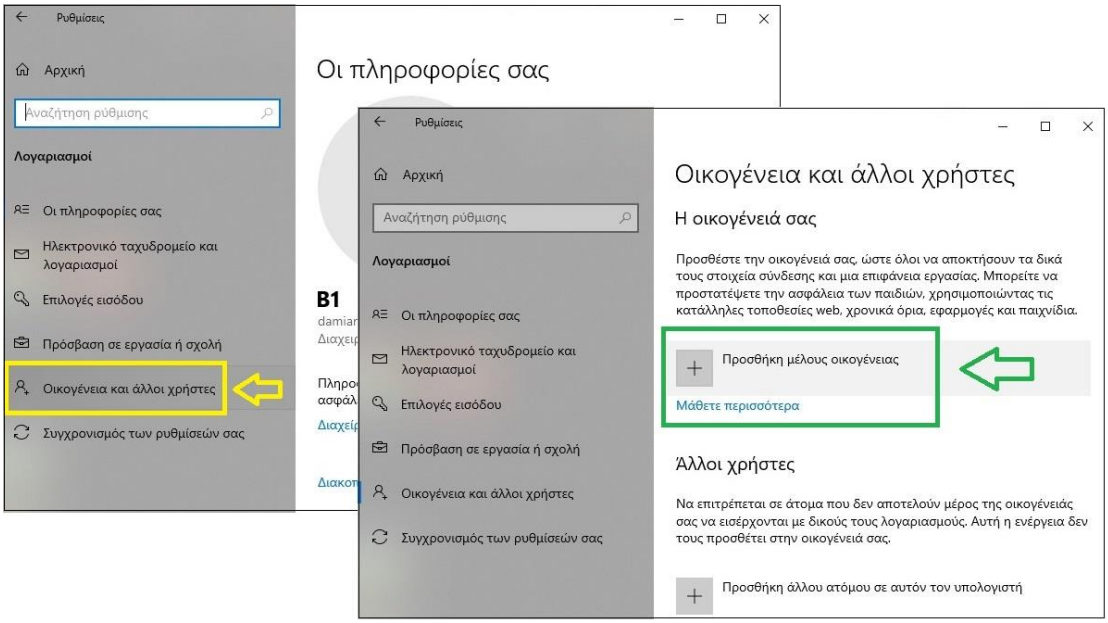
Εικόνα 34: *Microsoft Family Safety*

Για την ενεργοποίηση των ρυθμίσεων του γονικού ελέγχου, πρέπει να καθορίσουμε τους χρήστες που θα είναι τα μέλη της «οικογένειας». Αρχικά, μεταβαίνουμε στους λογαριασμούς χρηστών του ηλεκτρονικού υπολογιστή μέσω των ρυθμίσεων του μενού «Έναρξη» (Μενού Έναρξη → Ρυθμίσεις → Λογαριασμοί).



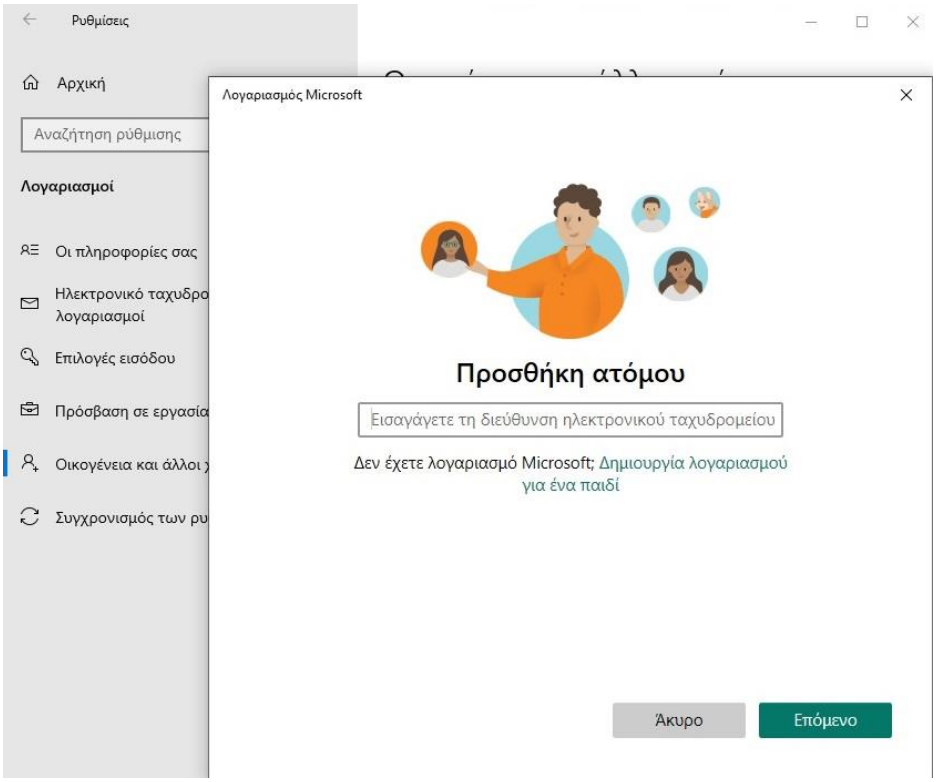
Εικόνα 35: *Windows 10: Γονικός Έλεγχος – Βήμα 1^{ο}*

Στο σημείο αυτό επιλέγουμε «Οικογένεια και άλλοι χρήστες» και στη συνέχεια «Προσθήκη μέλους οικογένειας».



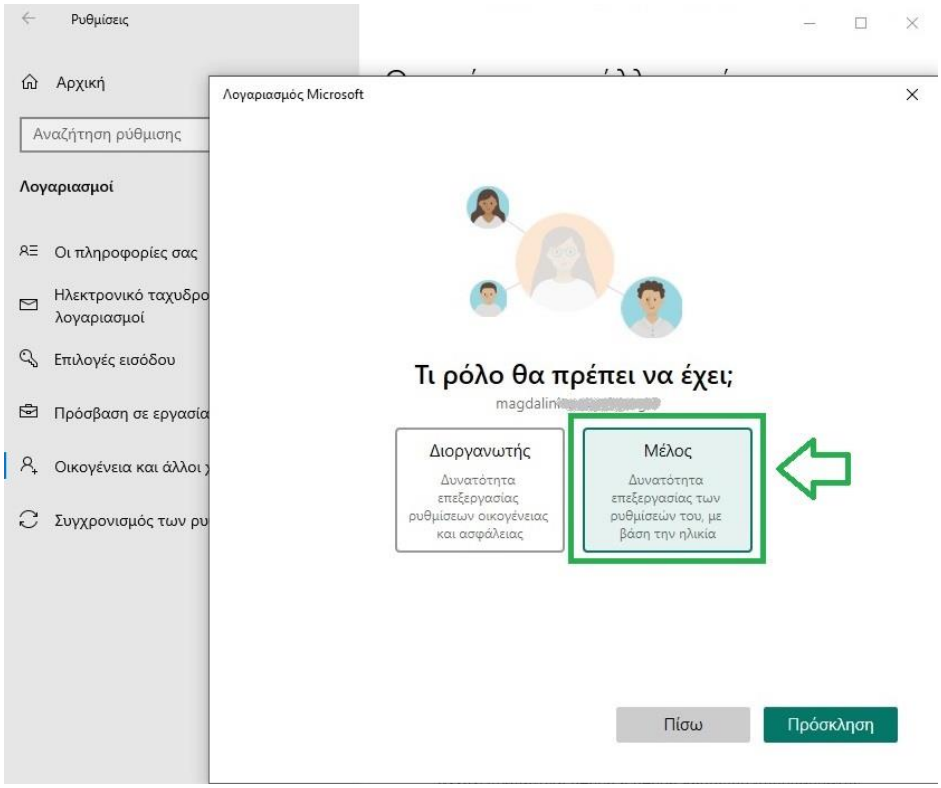
Εικόνα 36: *Windows 10: Γονικός Έλεγχος – Βήμα 2^{ο}*

Με την επιλογή αυτή, ανοίγει ένα νέο παράθυρο όπου μπορούμε να προσθέσουμε ένα νέο μέλος στην οικογένεια. Για να επιτευχθεί αυτό, χρειάζεται να εισάγουμε τη διεύθυνση ηλεκτρονικού ταχυδρομείου που διαθέτει ο χρήστης-μέλος στη Microsoft. Εάν δεν υφίσταται λογαριασμός δημιουργούμε ένα νέο.



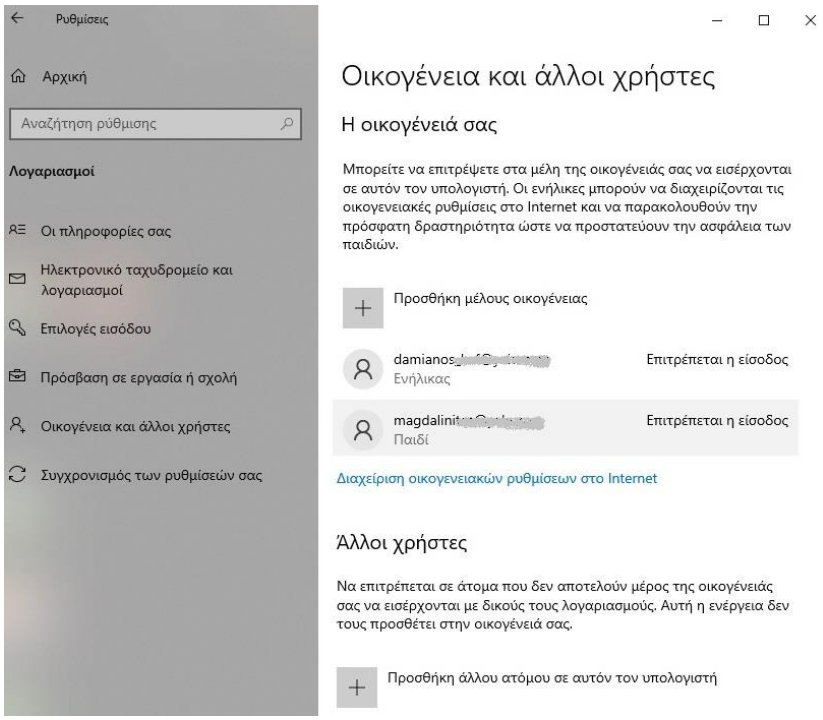
Εικόνα 37: *Windows 10: Γονικός Έλεγχος – Βήμα 3^{ο}*

Μετά την προσθήκη του νέου μέλους, πρέπει να καθοριστεί η ιδιότητα που θα έχει το μέλος στην οικογένεια. Διοργανωτής (διαχειριστής) και Μέλος (χρήστης).



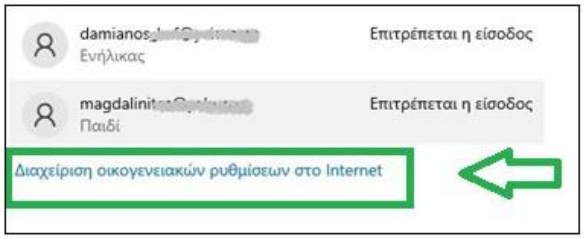
Εικόνα 38: *Windows 10: Γονικός Έλεγχος – Βήμα 4^{ο}*

Τα Windows 10 κατατάσσουν τους χρήστες της οικογένειας σε δύο διακριτές κατηγορίες: «Ενήλικες» και «Παιδιά».



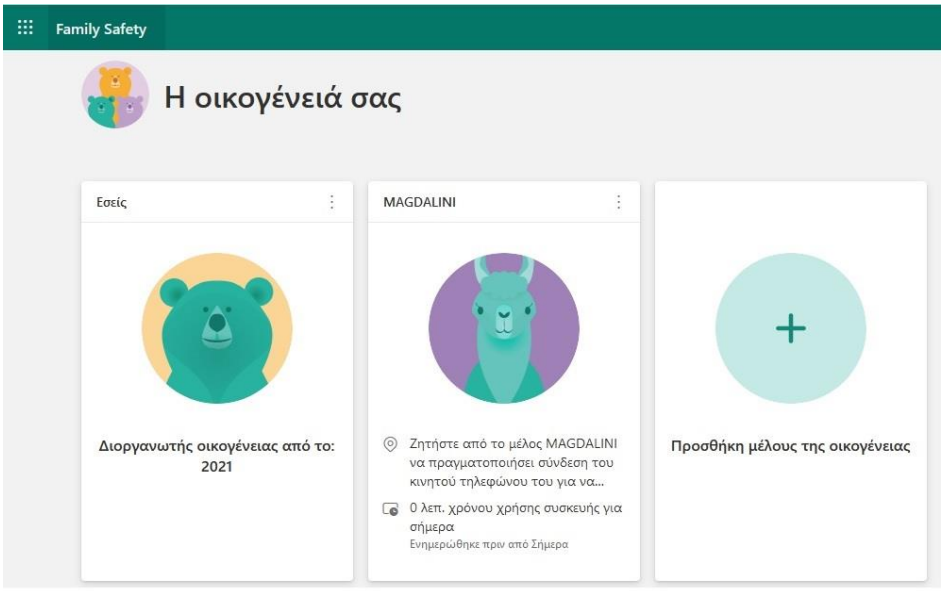
Εικόνα 39: *Windows 10: Γονικός Έλεγχος – Βήμα 5^{ο}*

Οι «Ενήλικες» έχουν την ιδιότητα να διαχειριστούν τις ρυθμίσεις της οικογένειας μέσω του διαδικτύου και είναι υπεύθυνοι για την ασφάλεια και τον έλεγχο των δραστηριοτήτων των «Παιδιών». Για να καθοριστούν οι κανόνες ασφαλείας επιλέγουμε τη «Διαχείριση οικογενειακών ρυθμίσεων στο Internet».



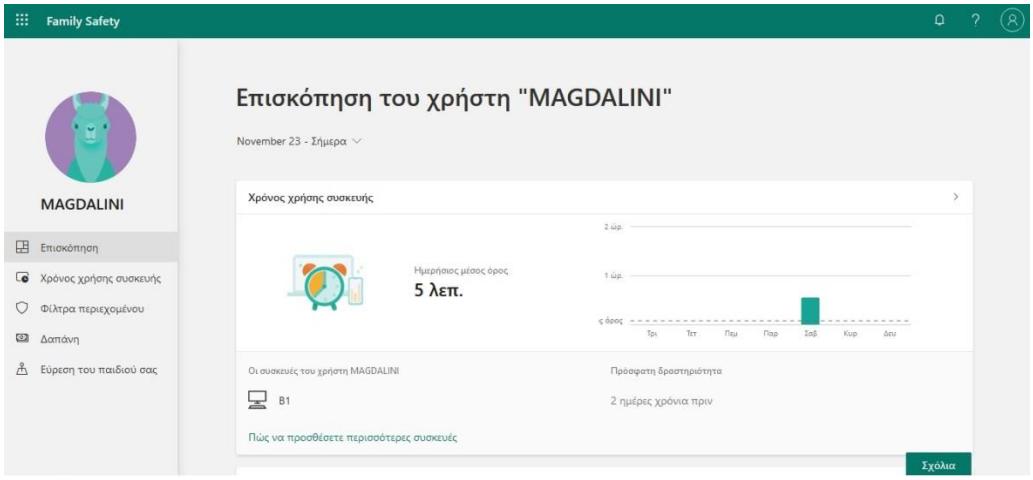
Εικόνα 40: *Windows 10: Γονικός Έλεγχος – Βήμα 6^{ο}*

Μετά την επιλογή ανοίγει ένα νέο παράθυρο φυλλομετρητή (browser) όπου φαίνεται η σελίδα (family.microsoft.com) στην οποία μπορούμε να διαχειριστούμε τους λογαριασμούς των χρηστών της οικογένειά μας μέσω της Microsoft.



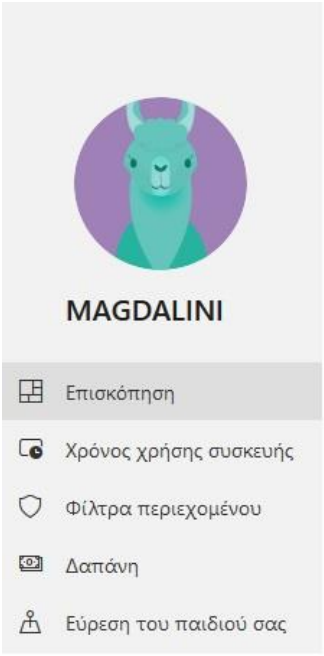
Εικόνα 41: *Windows 10: Γονικός Έλεγχος – Βήμα 7^{ο}*

Για να μπορέσει ο διαχειριστής να καθορίσει και να επεξεργαστεί τις ρυθμίσεις κάθε μέλους της οικογένειας, επιλέγει το αντίστοιχο μέλος και ανοίγει η σχετική καρτέλα.



Εικόνα 42: *Windows 10: Γονικός Έλεγχος – Βήμα 8^{ο}*

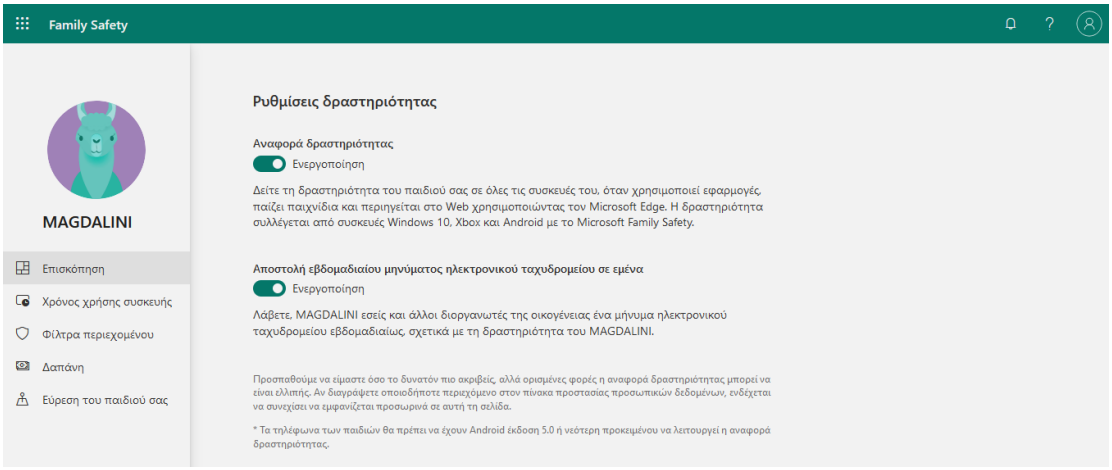
Στην καρτέλα του μέλους, ο διαχειριστής μπορεί να ενημερωθεί για τις δραστηριότητες του χρήστη μέσω της «Επισκόπησης», να παρέμβει και να ρυθμίσει τον «*Χρόνος χρήσης συσκευής*», τα «*Φίλτρα περιεχομένου*», τη «*Δαπάνη*» και την «*Εύρεση του παιδιού*» .



Εικόνα 43: *Windows 10: Γονικός Έλεγχος – Βήμα 9^{ο}*

- Επισκόπηση

Η πρώτη κατά σειρά επιλογή των ρυθμίσεων δραστηριότητας της κατηγορίας «Επισκόπηση» είναι η «Αναφορά δραστηριότητας». Μόλις την ενεργοποιήσει ο διαχειριστής μπορεί να ενημερώνεται για το ποιες εφαρμογές χρησιμοποιεί ο χρήστης, ποια παιχνίδια προτιμά και ποιες ιστοσελίδες επισκέπτεται.



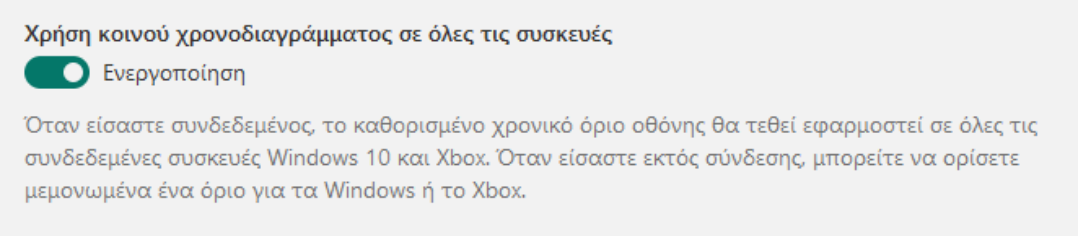
Εικόνα 44: *Windows 10: Γονικός Έλεγχος – Βήμα 10^{ο}*

Καθιστώντας ενεργό τον έλεγχο της «Αποστολής εβδομαδιαίου μηνύματος ηλεκτρονικού ταχυδρομείου», ο διαχειριστής μπορεί να επιλέξει την αποστολή εβδομαδιαίων αναφορών όλων των δραστηριοτήτων του χρήστη μέσω email.

- Χρόνος χρήσης συσκευής

Με την επιλογή του χρονικού ορίου οθόνης ο διαχειριστής μπορεί να καθορίσει το χρονικό διάστημα που μπορεί ένας απλός χρήστης να χρησιμοποιεί τις συσκευές (ηλεκτρονικό υπολογιστή ή τη κονσόλα Xbox) και τις εφαρμογές και παιχνίδια.

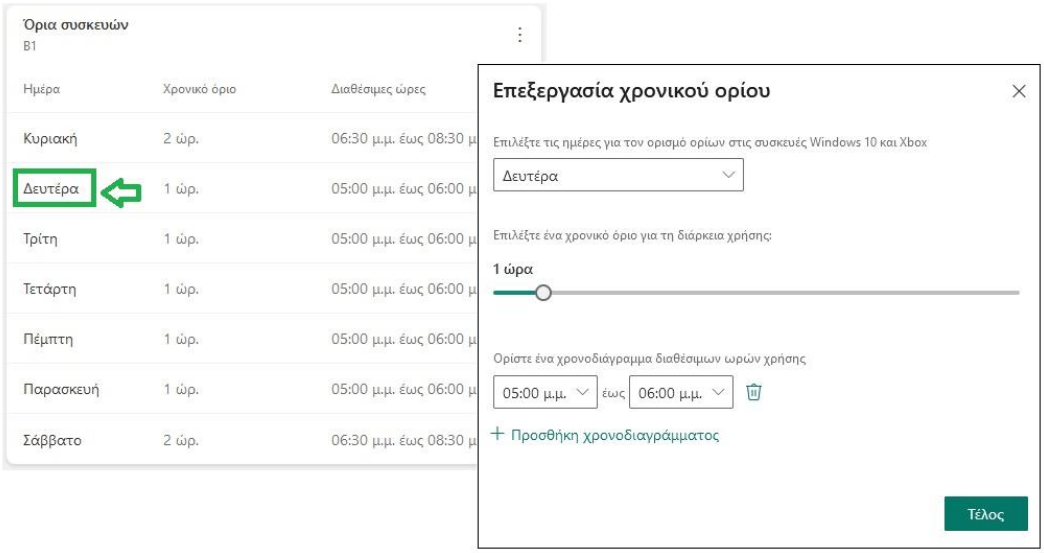
- Συσκευές



Εικόνα 45: *Windows 10: Γονικός Έλεγχος – Βήμα 11^{ο}*

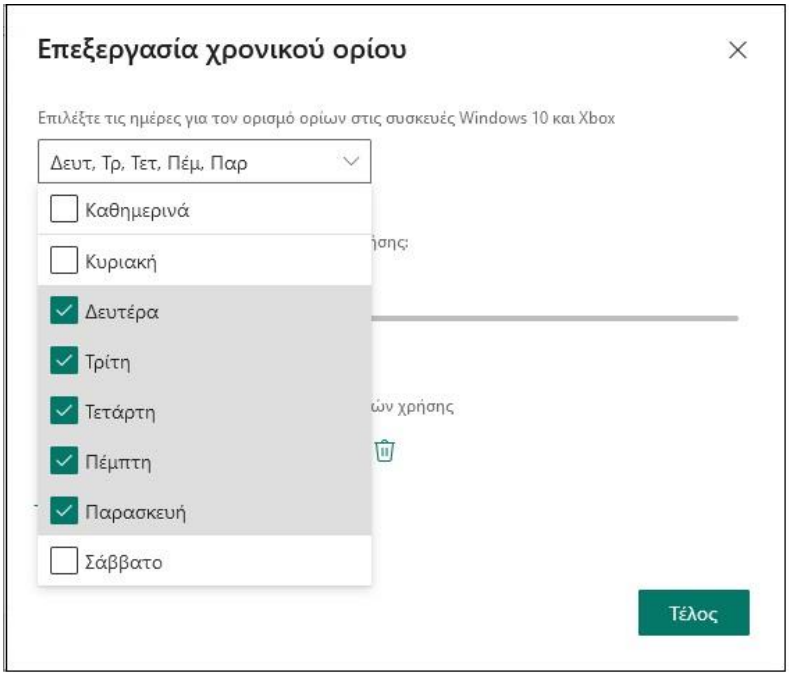
Οι ρυθμίσεις του χρονικού ορίου οθόνης αφορούν τον ορισμό ωριαίας χρήσης της συσκευής για κάθε μια μέρα της εβδομάδας.

Οι επιλογές του διαχειριστή για την ωριαία ρύθμιση κυμαίνονται από την απεριόριστη χρήση έως τον πλήρη αποκλεισμό.



Εικόνα 46: *Windows 10: Γονικός Έλεγχος – Βήμα 12^{ο}*

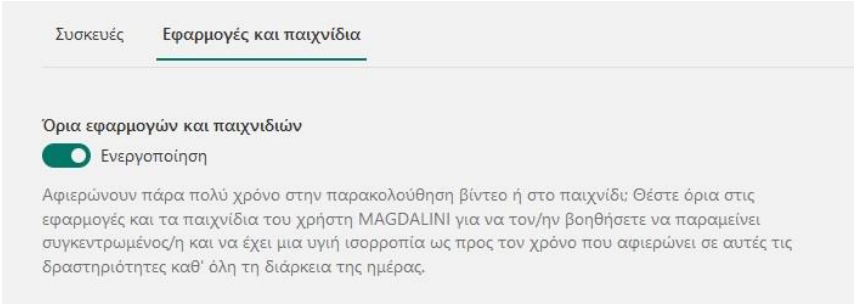
Μπορούν να καταχωρηθούν πολλά διαφορετικά χρονικά όρια για μια συγκεκριμένη μέρα. Για λόγους ευκολίας η «Επεξεργασία χρονικού ορίου» μπορεί να γίνει μαζικά όσες ημέρες της εβδομάδας επιθυμεί ο διαχειριστής.



Εικόνα 47: *Windows 10: Γονικός Έλεγχος – Βήμα 13^{ο}*

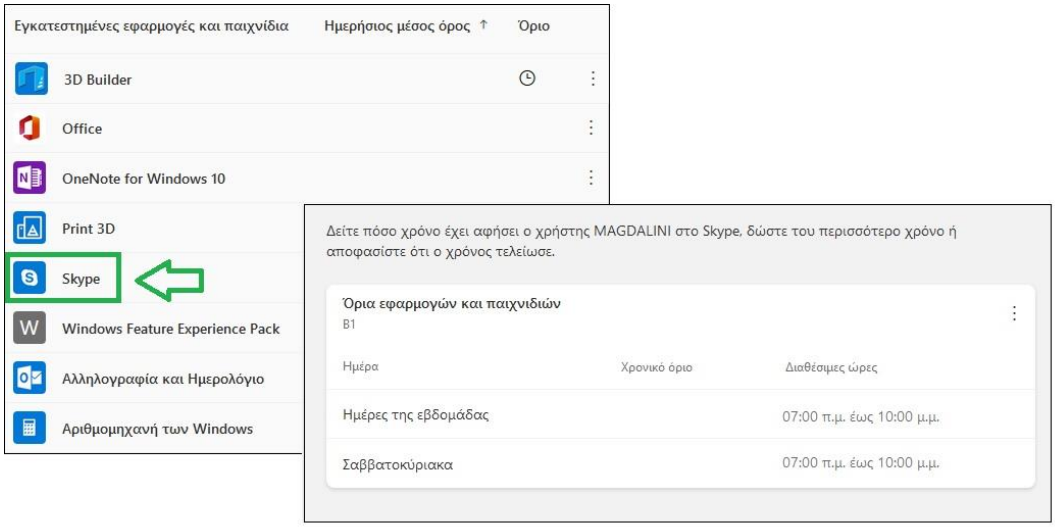
- Εφαρμογές και παιχνίδια

Ενεργοποιώντας τα όρια εφαρμογών και παιχνιδιών περιορίζεται ο καθημερινός χρόνος που αφιερώνει καθημερινά ο χρήστης.



Εικόνα 48: *Windows 10: Γονικός Έλεγχος – Βήμα 14^{ο}*

Στη συνέχεια εμφανίζεται η λίστα με τα εγκατεστημένα προγράμματα της συσκευής και ο διαχειριστής μπορεί να οριοθετήσει το χρόνο που ο χρήστης θα μπορεί να τα χρησιμοποιεί.



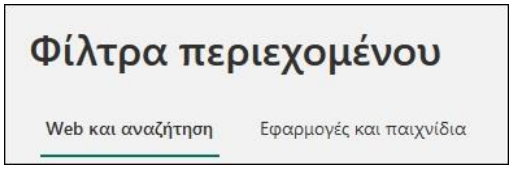
Εικόνα 49: *Windows 10: Γονικός Έλεγχος – Βήμα 15ο*

Επίσης, στο σημείο αυτό εκτός από τη ρύθμιση των χρονικών ορίων, ο διαχειριστής μπορεί να αποκλείσει κάποια εφαρμογή.

Εικόνα 50: *Windows 10: Γονικός Έλεγχος – Βήμα 16ο*

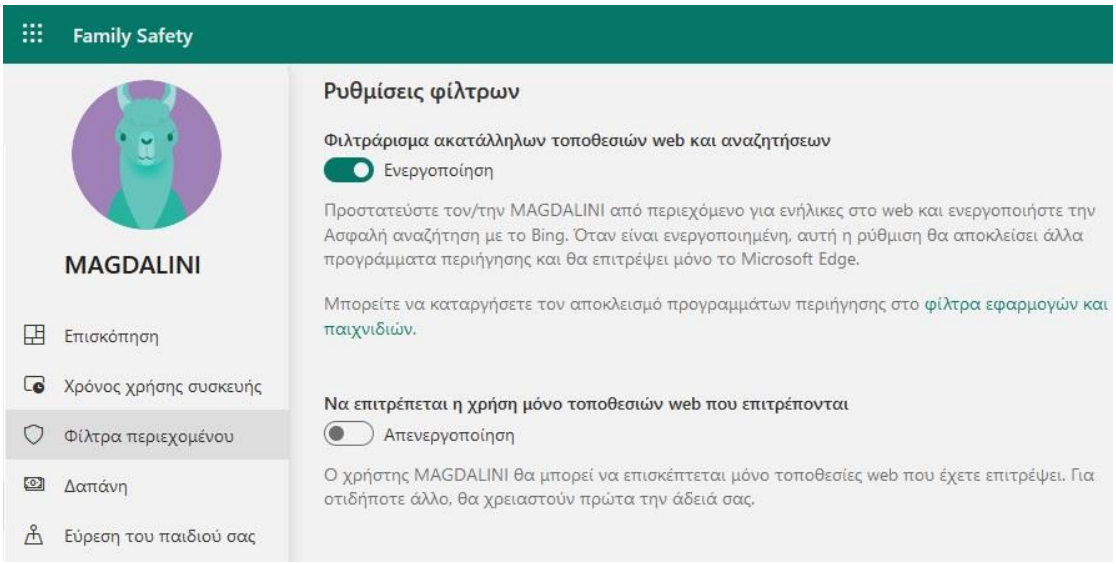
- Φίλτρα περιεχομένου

Επιλέγοντας τα «Φίλτρα περιεχομένου» ο διαχειριστής αποκτά πρόσβαση στον έλεγχος των ιστοσελίδων, των εφαρμογών και των παιχνιδιών που θα επιτρέπεται η πρόσβαση από τον χρήστη.



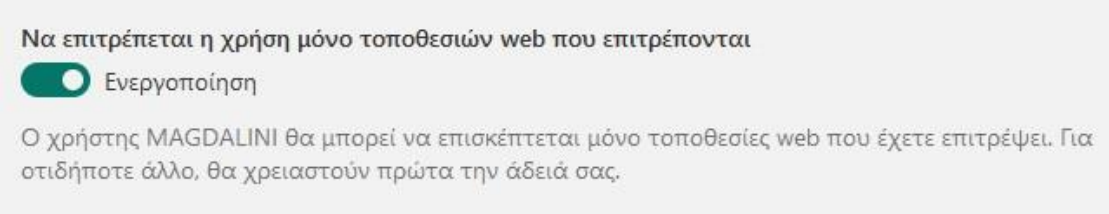
Εικόνα 51: *Windows 10: Γονικός Έλεγχος – Βήμα 17ο*

- *Web και αναζήτηση*



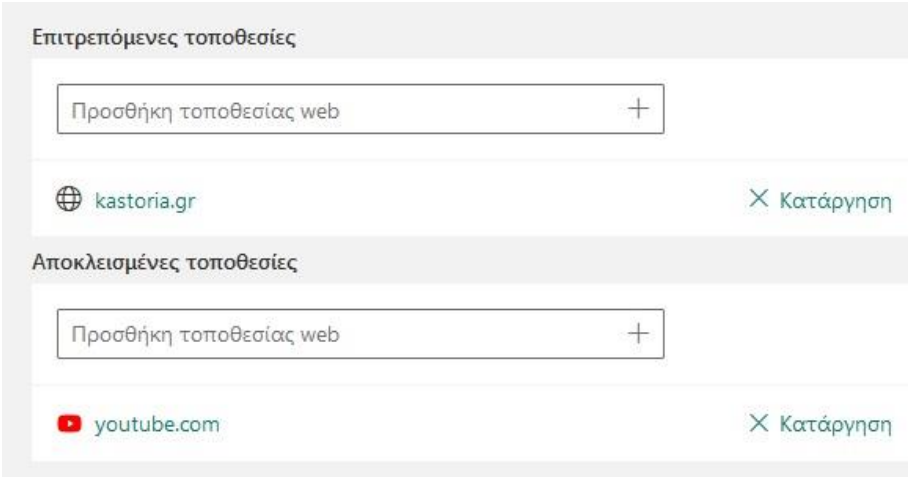
Εικόνα 52: *Windows 10: Γονικός Έλεγχος – Βήμα 18^{ο}*

Από τις πιο σημαντικές ρυθμίσεις είναι ο καθορισμός συγκεκριμένων τοποθεσιών web από το χρήστη και αυτό είναι ιδιαίτερα χρήσιμο όταν ο χρήστης στον οποίο απευθύνεται είναι ανήλικος.



Εικόνα 53: *Windows 10: Γονικός Έλεγχος – Βήμα 19^{ο}*

Το μόνο που πρέπει να κάνει ο διαχειριστής είναι να ορίσει τη λίστα με τις επιτρεπόμενες τοποθεσίες web τις οποίες θα μπορεί να επισκέπτεται και να έχει πρόσβαση ο ανήλικος χρήστης αλλά και τη λίστα με τις τοποθεσίες εκείνες που απαγορεύεται η πρόσβαση.

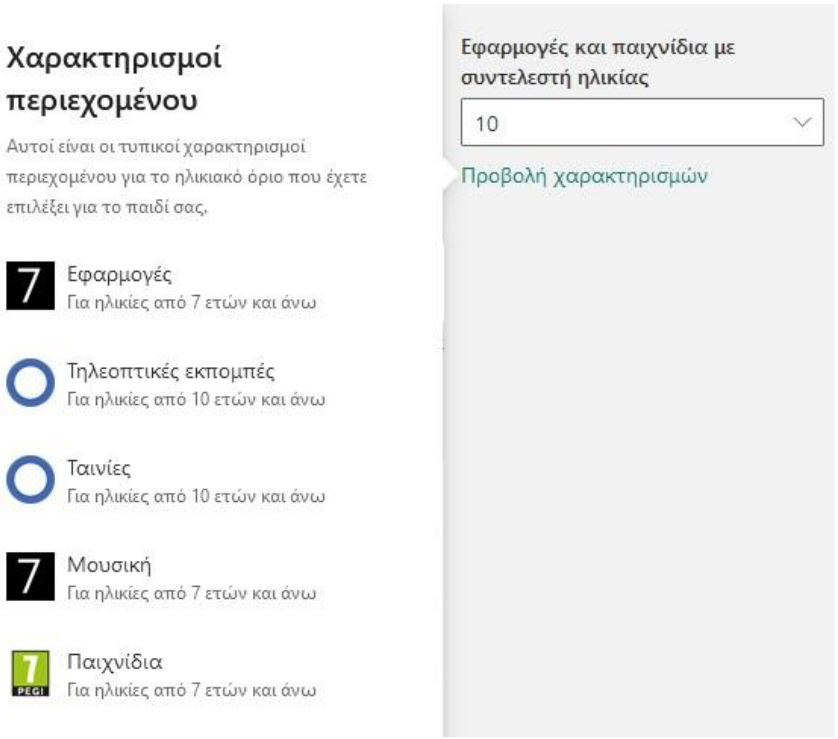


Εικόνα 54: *Windows 10: Γονικός Έλεγχος – Βήμα 20ο*

- *Εφαρμογές και παιχνίδια*

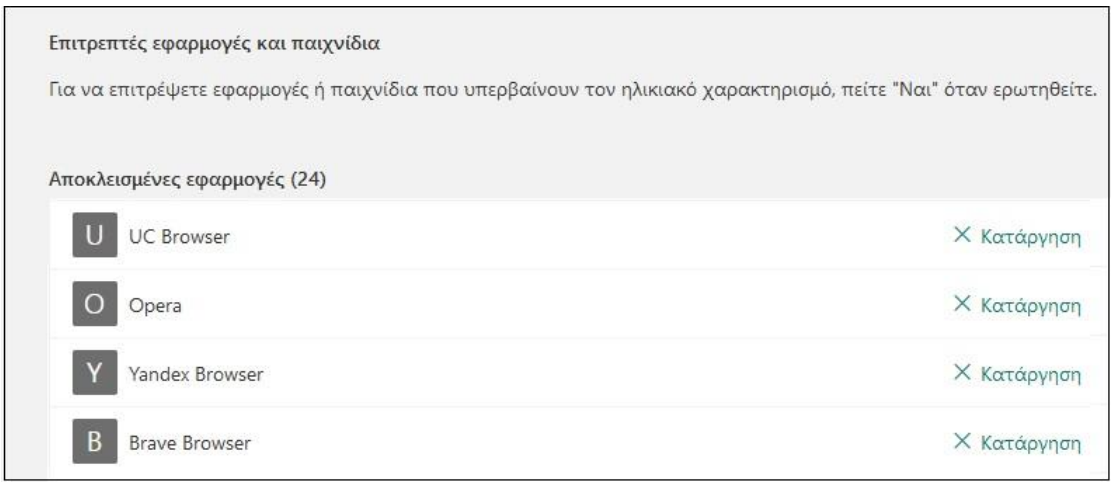
Η επόμενη ρύθμιση αφορά τον ορισμό της ηλικιακής ομάδας όπου θα επιτρέπεται η πρόσβασης σε εφαρμογές, παιχνίδια και πολυμέσα. Εάν ο χρήστης επιχειρήσει να κάνει λήψη εφαρμογής ή παιχνιδιού που είναι εκτός του ορίου ηλικίας, θα απαιτηθεί έγκριση από τον διαχειριστή. Υπενθυμίζεται ότι η λειτουργία αυτή αφορά μόνο συσκευές με λειτουργικό σύστημα Windows 10 και Xbox.

Ο διαχειριστής ορίζει την ηλιακή ομάδα στην οποία θα υπάρχει περιορισμός πρόσβασης. Για κάθε ηλιακή ομάδα εμφανίζονται οι αντίστοιχοι χαρακτηρισμοί περιεχομένου σύμφωνα με το διεθνές πρότυπο PEGI.



Εικόνα 55: *Windows 10: Γονικός Έλεγχος – Βήμα 21ο*

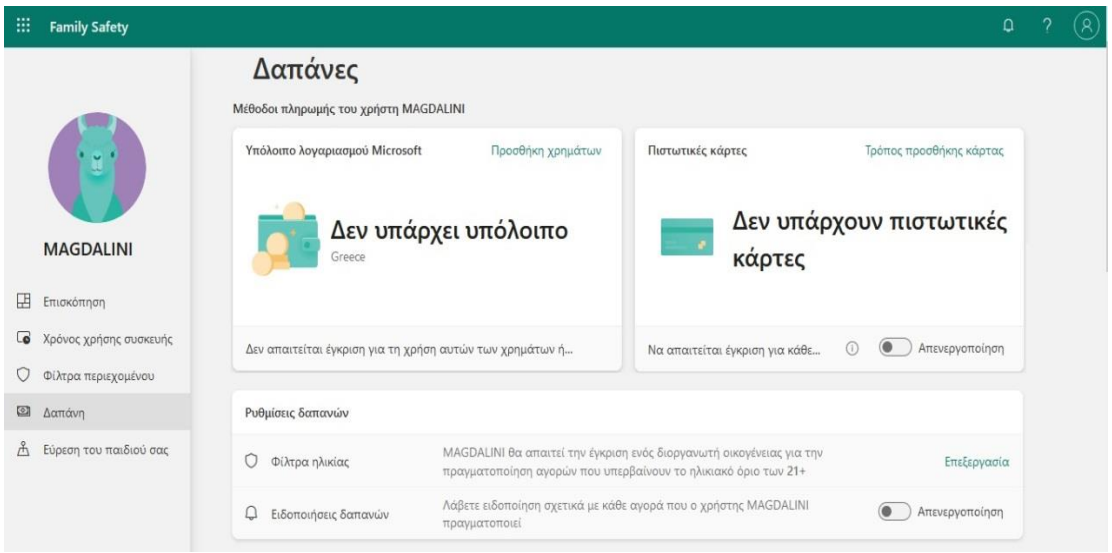
Στη συνέχεια εμφανίζεται η λίστα με όλες τις αποκλειόμενες εφαρμογές και παιχνίδια καθώς επίσης και η ξεχωριστή λίστα με τις επιτρεπόμενες. Υπάρχει όμως πάντα η δυνατότητα ο διαχειριστής να παρέμβει και να ενεργοποιήσει ή να απενεργοποιήσει όποιες εφαρμογές, παιχνίδια και πολυμέσα επιθυμεί.



Εικόνα 56: *Windows 10: Γονικός Έλεγχος – Βήμα 22^{ο}*

- Δαπάνη

Στην επιλογή «Δαπάνες» μπορούμε να επιλέξουμε την «Προσθήκη χρημάτων» για να μεταφέρουμε χρήματα στο λογαριασμό του χρήστη και να προσθέσουμε «Πιστωτική κάρτα». Μέσω του ιστορικού που διατηρείται μπορούμε να ελέγξουμε τις συναλλαγές που έχουν πραγματοποιηθεί. Οι συναλλαγές αυτές δεν αφορούν αγορές μέσω του διαδικτύου αλλά μόνο τις λήψεις και τις αγορές από το Windows Store της Microsoft.

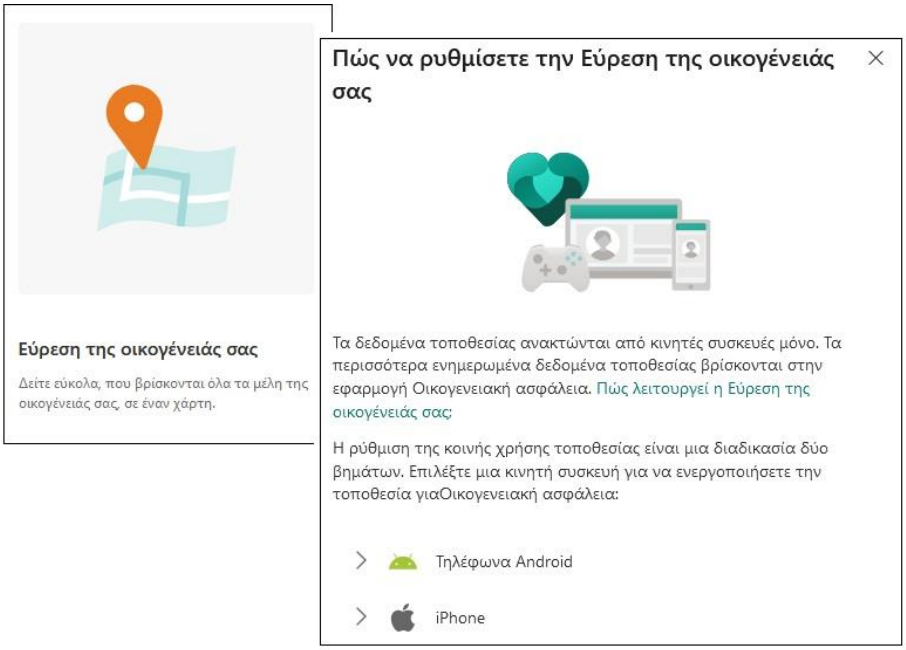


Εικόνα 57: *Windows 10: Γονικός Έλεγχος – Βήμα 23^{ο}*

- Εύρεση του παιδιού σας

Με τη ρύθμισης «Εύρεσης τοποθεσίας παιδιού», ο διαχειριστής του συστήματος αντλεί πληροφορίες σχετικά με την τοποθεσία της συσκευής την οποία χρησιμοποιεί το παιδί και συνδέεται στο διαδίκτυο τη συγκεκριμένη χρονική στιγμή.

Η λειτουργία αυτή αφορά κινητές συσκευές και υλοποιείται μέσω της εφαρμογής «Οικογενειακή ασφάλεια».



Εικόνα 58: *Windows 10: Γονικός Έλεγχος – Βήμα 24^{ο}*

4.6 Γονικός έλεγχος στα έξυπνα τηλέφωνα (smartphones) και τα tablet με λειτουργικό σύστημα Android

Το Android είναι ένα λειτουργικό σύστημα που στηρίζεται στο Linux (λειτουργικό σύστημα ελεύθερου λογισμικού), το οποίο αναπτύχθηκε κυρίως για ψηφιακές συσκευές με οθόνη αφής, όπως τα έξυπνα τηλέφωνα (smartphones) και τα tablet. Αρχικά σχεδιάστηκε από την Google και στη συνέχεια από την OHA (Open Handset Alliance).

Παρά το ότι το Android έχει σχεδιαστεί για τις συγκεκριμένου τύπου συσκευές, χρησιμοποιείται και σε πληθώρα άλλων τύπων ψηφιακών συσκευών (π.χ. φωτογραφικές μηχανές, κονσόλες ηλεκτρονικά παιχνίδια κ.α.).

Για την εφαρμογή του γονικού ελέγχου σε έξυπνα τηλέφωνα (smartphones) που το λειτουργικό τους σύστημα είναι Android, μια εύκολη και άμεση λύση είναι μέσω της εφαρμογής του «FamilyLink» της Google.

Επί της ουσίας, το FamilyLink συμβάλει στη διαχείριση των συσκευών και λογαριασμών των παιδιών και των ανηλίκων γενικότερα. Αποτελεί ένα εργαλείο με

το οποίο οι γονείς ελέγχουν σε εβδομαδιαία βάση τη δραστηριότητα των παιδιών κατά τη περιήγησή τους στο διαδίκτυο. Δίνει το δικαίωμα στους γονείς να επιτρέπουν ή όχι στο παιδί τη χρήση εφαρμογών που είναι ήδη εγκατεστημένες στη συσκευή αλλά και αυτές που επιθυμεί να κατεβάσει από το PlayStore της Google.

Επιπλέον, ο γονέας, μπορεί να καθορίσει το ημερήσιο χρονικό όριο κατά το οποίο το παιδί θα μπορεί να κάνει χρήση της συσκευής καθώς επίσης και να παρακολουθεί την τοποθεσία που βρίσκεται το παιδί του μέσω της συσκευής.

Για τη χρήση και διαχείριση του « FamilyLink» της Google θα πρέπει:

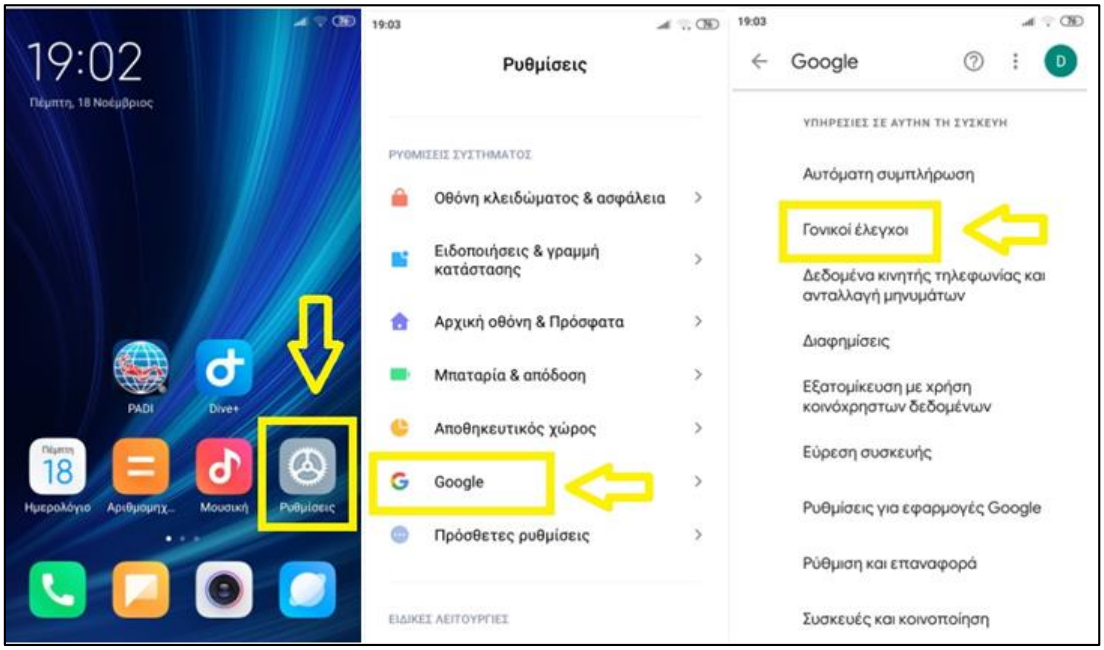
- Ο διαχειριστής της εφαρμογής να είναι ενήλικας άνω των 18.
- Ο γονέας να διαθέτει ή να δημιουργήσει ένα Λογαριασμό στη Google ο οποίος είναι δωρεάν.
- Η συσκευή στην οποία θα εφαρμοστεί ο γονικός έλεγχος να έχει λειτουργικό σύστημα Android (5.0+), iPhone (iOS 9+), iPad (iOS 9+) ή ένα Chromebook που υποστηρίζει εφαρμογές Android.
- Ο διαχειριστής – γονέας να βρίσκεται στην ίδια χώρα με το παιδί.
- Ο γονέας να δημιουργήσει έναν δωρεάν Λογαριασμό στη Google για το παιδί.

Στη συνέχεια θα εξετάσουμε τον τρόπο με τον οποίο μπορούμε εύκολα και γρήγορα να εφαρμόσουμε το γονικό έλεγχο σε ένα έξυπνο τηλέφωνο ή tablet μέσω του « FamilyLink» της Google.

4.6.1 Γονικός Έλεγχος μέσω του «FamilyLink» της Google

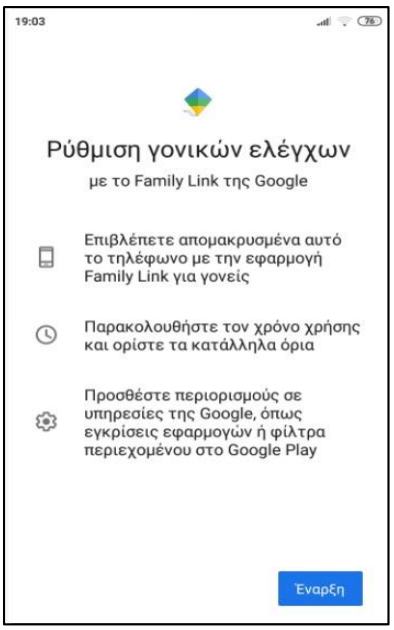
Για να μπορέσουμε να εφαρμόσουμε και να ρυθμίσουμε το γονικό έλεγχο σε ένα έξυπνο κινητό τηλέφωνο (smartphone) με λειτουργικό σύστημα Android μέσω του «FamilyLink», πρέπει πρώτα να δημιουργήσουμε και να διασυνδέσουμε τους λογαριασμούς Google μεταξύ γονέα και παιδιού.

Αρχικά επιλέγουμε «Ρυθμίσεις» στην αρχική οθόνη και στη συνέχεια «Ρυθμίσεις Συστήματος» επιλέγονταςGoogle και «Γονικοί Έλεγχοι».



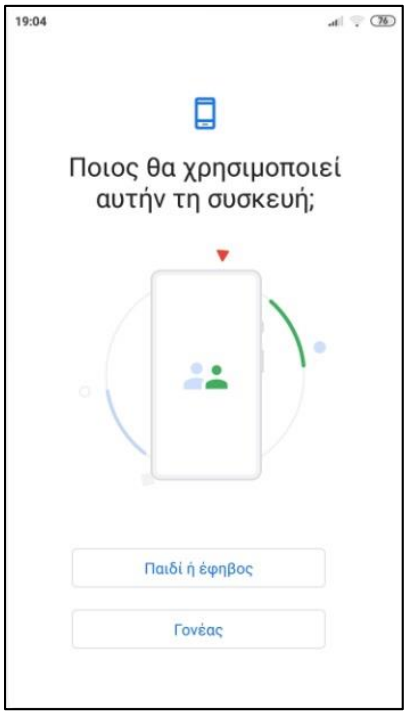
Εικόνα 59: *Family Link: Γονικός Έλεγχος – Βήμα 1ο*

Στη νέα οθόνη «Ρύθμιση γονικών ελέγχων με το FamilyLink της Google» εμφανίζονται οι τρεις βασικές ιδιότητες του FamilyLink που μπορεί να χρησιμοποιήσει ο γονέας. Δηλαδή, μπορεί να επιβλέπει απομακρυσμένα το συγκεκριμένο τηλέφωνο, να παρακολουθεί το χρόνο χρήσης και να ορίσει τα κατάλληλα όρια και περιορισμούς σε υπηρεσίες της Google.



Εικόνα 60: *Family Link: Γονικός Έλεγχος – Βήμα 2ο*

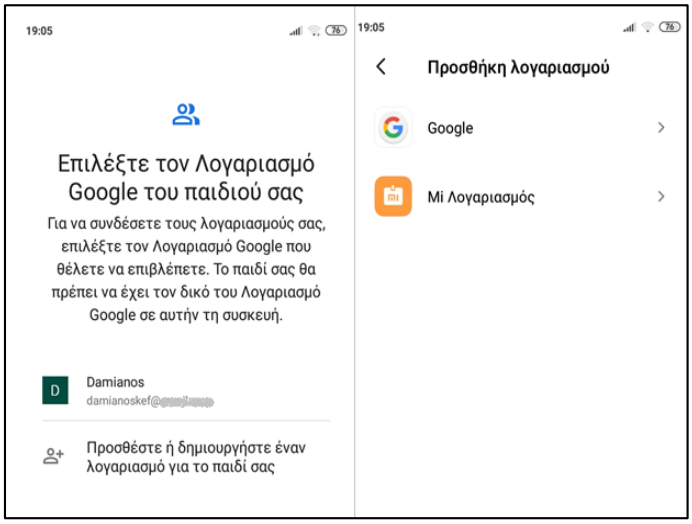
Πατώντας το κουμπί «έναρξη» ξεκινάει η διαδικασία εφαρμογής και ρύθμισης του γονικού ελέγχου. Ο χρήστης καλείται να επιλέξει εάν τη συγκεκριμένη συσκευή θα τη χρησιμοποιεί ο γονέας ή το παιδί.



Εικόνα 61: *Family Link: Γονικός Έλεγχος – Βήμα 3^{ο}*

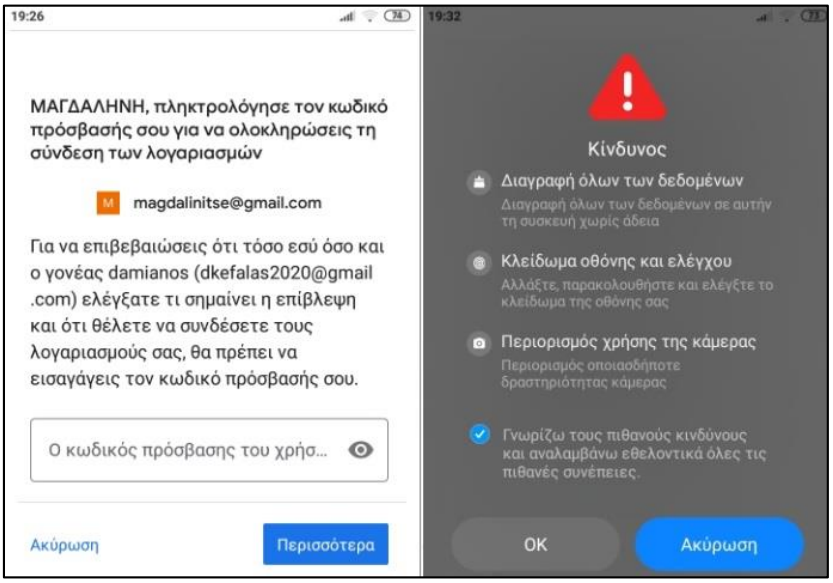
Στην περίπτωση που τη συγκεκριμένη συσκευή θα τη χρησιμοποιεί ο γονέας επιλέγουμε «Γονέας» και ξεκινάει η λήψη του «Familylink» στο κινητό. Γίνεται η σχετική εγκατάσταση της εφαρμογής στη συσκευή και ο γονέας ως διαχειριστής πλέον συνδέει τη συσκευή του με τη συσκευή του παιδιού του μέσω του λογαριασμού της Google και μπορεί να εποπτεύει και να ενημερώνεται για τη χρήση και τις δραστηριότητες στο έξυπνο κινητό τηλέφωνο του παιδιού.

Εάν ο χρήστης της συσκευής είναι παιδί, τότε στην οθόνη αυτή επιλέγουμε «Παιδί ή έφηβος» και στην επόμενη οθόνη εμφανίζεται ο λογαριασμός του γονέα που διαθέτει στη Google. Το επόμενο βήμα είναι να γίνει προσθήκη ή δημιουργία του αντίστοιχου λογαριασμού στη Google του παιδιού το οποίο θα είναι ο χρήστης της συσκευής.



Εικόνα 62: *Family Link: Γονικός Έλεγχος – Βήμα 4^{ο}*

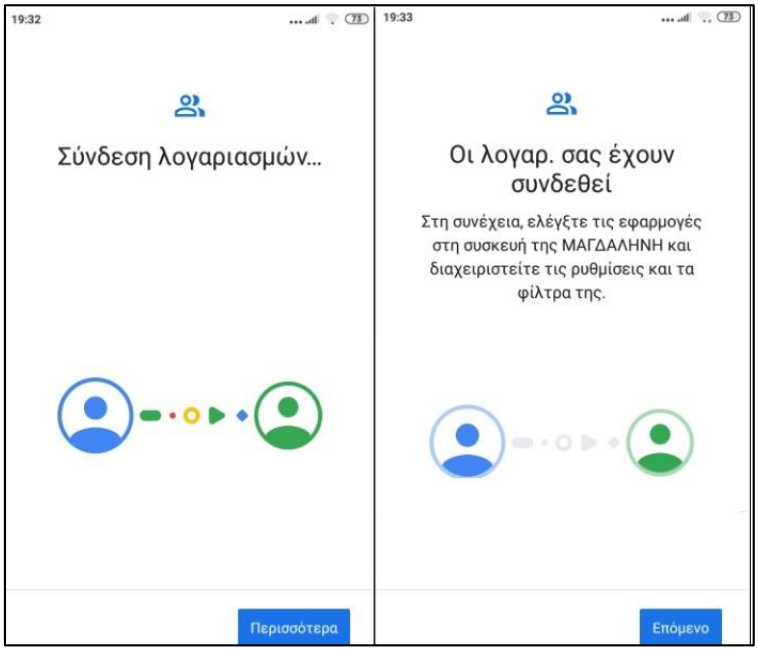
Μετά την προσθήκη ή δημιουργία του λογαριασμού το «Παιδί» καλείται να πληκτρολογήσει τον κωδικό πρόσβασης που διαθέτει ώστε να ολοκληρωθεί η σύνδεση των δύο λογαριασμών (Γονέα – Παιδί)



Εικόνα 63: *Family Link: Γονικός Έλεγχος – Βήμα 5^{ο}*

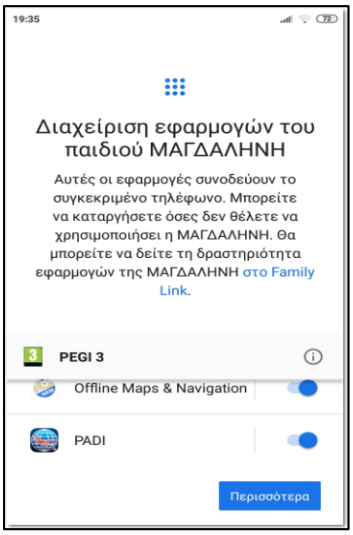
Για λόγους ασφαλείας εμφανίζεται το μήνυμα για τους πιθανούς ‘κινδύνους’ που ενέχει η συγκατάθεση διασύνδεσης των δύο συσκευών όπως είναι η διαγραφή όλων των δεδομένων χωρίς άδεια, κλείδωμα οθόνης, και περιορισμό οποιασδήποτε δραστηριότητας κάμερας.

Ο χρήστης επιλέγοντας ότι συναινεί με τα παραπάνω γίνεται η σύνδεση των λογαριασμών και πλέον ο γονέας μπορεί να διαχειριστεί και να ρυθμίσει τα φίλτρα του γονικού ελέγχου.



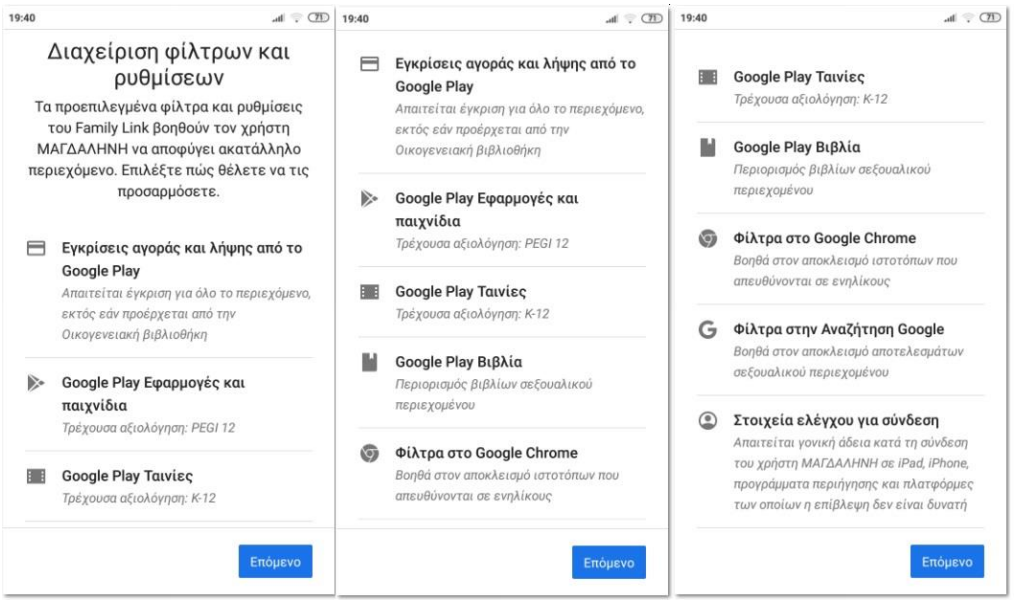
Εικόνα 64: *Family Link: Γονικός Έλεγχος – Βήμα 6ο*

Στο σημείο αυτό ο γονέας ρυθμίζει τις εφαρμογές οι οποίες υπάρχουν στη τηλεφωνική συσκευή και μπορεί να καταργήσει όσες δεν επιθυμεί το 'παιδί' να έχει πρόσβαση.



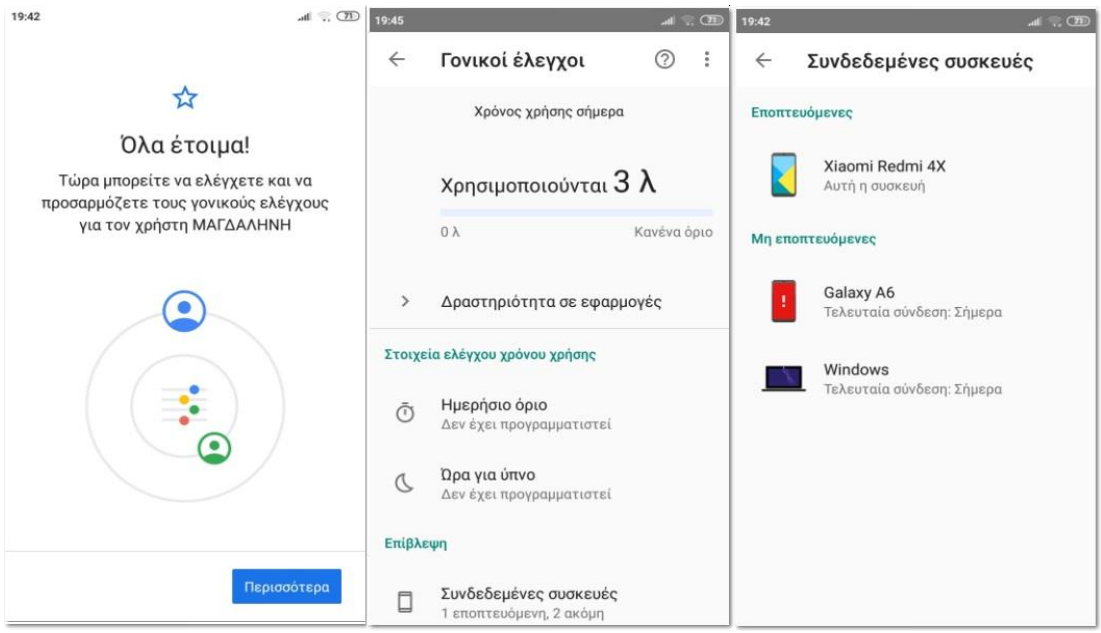
Εικόνα 65: *Family Link: Γονικός Έλεγχος – Βήμα 7ο*

Επίσης, ο γονέας διαχειρίζεται μια σειρά φίλτρων και ρυθμίσεων που παρέχονται από το FamilyLink και βοηθούν τον χρήστη 'Παιδί' να αποφύγει επικίνδυνες καταστάσεις κατά τη χρήση της τηλεφωνικής συσκευής.



Εικόνα 66: *Family Link: Γονικός Έλεγχος – Βήμα 8ο*

Πλέον, όλα είναι έτοιμα για την εφαρμογή του γονικού ελέγχου και ο διαχειριστής – γονέας μπορεί από τη συσκευή του να έχει μια πλήρη εικόνα της δραστηριότητας του χρήστη – 'παιδί' σχετικά με το κινητό του τηλέφωνο αλλά και σε όποια συσκευή είναι συνδεδεμένος ο λογαριασμός Google του παιδιού.



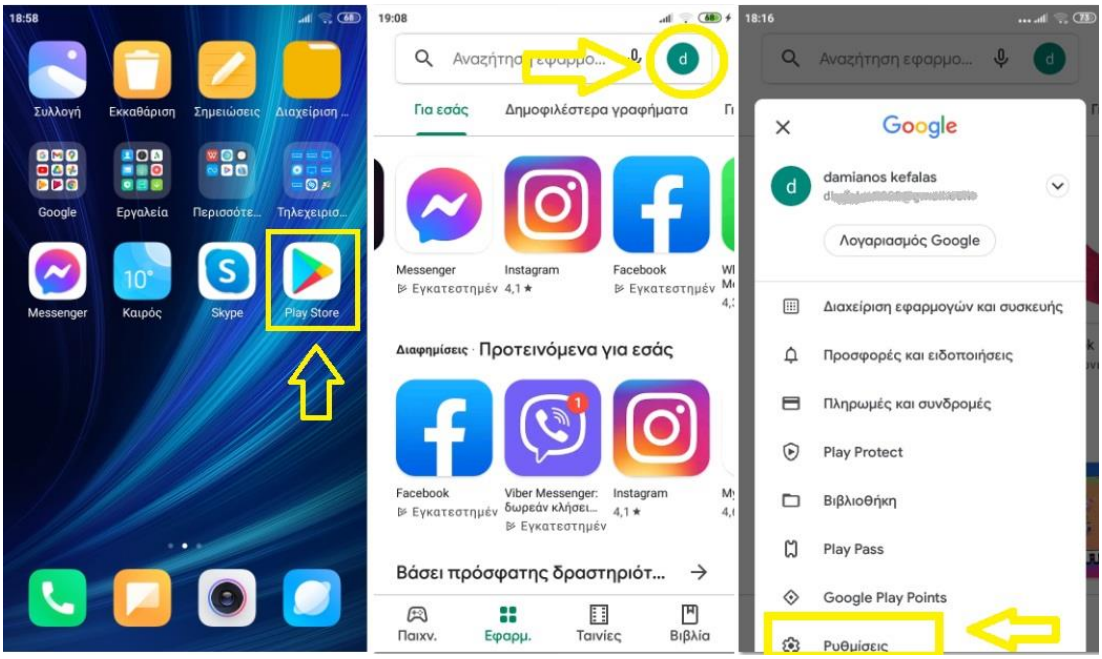
Εικόνα 67: *Family Link: Γονικός Έλεγχος – Βήμα 9ο*

4.6.2 Εφαρμογή γονικού ελέγχου σε εφαρμογές και παιχνίδια της Google

Όπως αναφέρθηκε προηγουμένως, μέσω του «FamilyLink» μπορούμε να διαχειριστούμε μια σειρά φίλτρων και ρυθμίσεων προκειμένου να εφαρμόσουμε το γονικό έλεγχο σε ψηφιακή συσκευή τύπου 'smartphone' ή 'tablet' με λειτουργικό σύστημα Android.

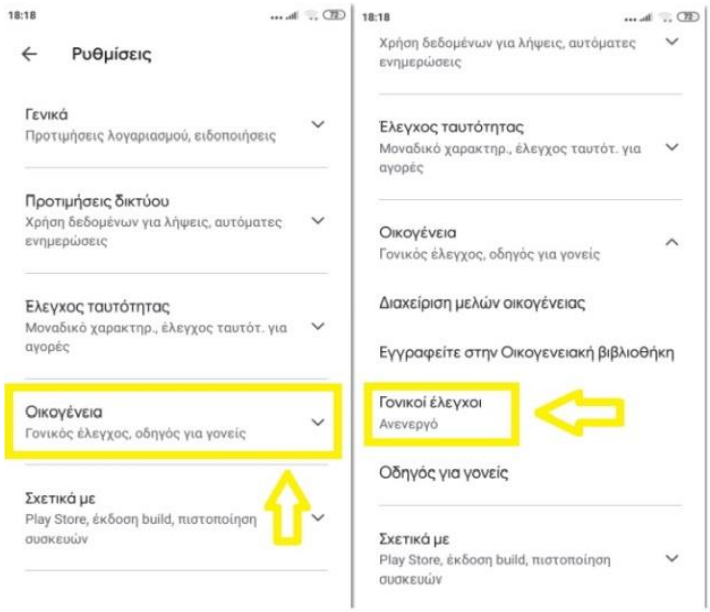
Όμως ο γονικός έλεγχος σε ένα κινητό ή tablet μπορεί να εφαρμοστεί μεμονωμένα και εκτός της λειτουργίας του «FamilyLink» επιλεκτικά και μόνο σε μια συγκεκριμένη εφαρμογή ή εφαρμογές της Google όπως είναι το PlayStore.

Για να ενεργοποιήσουμε τις λειτουργίες του γονικού ελέγχου στην εφαρμογή "PlayStore" της Google, ανοίγουμε την εφαρμογή PlayStore που βρίσκεται εγκατεστημένη στην συσκευή μας, επιλέγουμε πάνω δεξιά στο εικονίδιο του χρήστη και «Ρυθμίσεις».



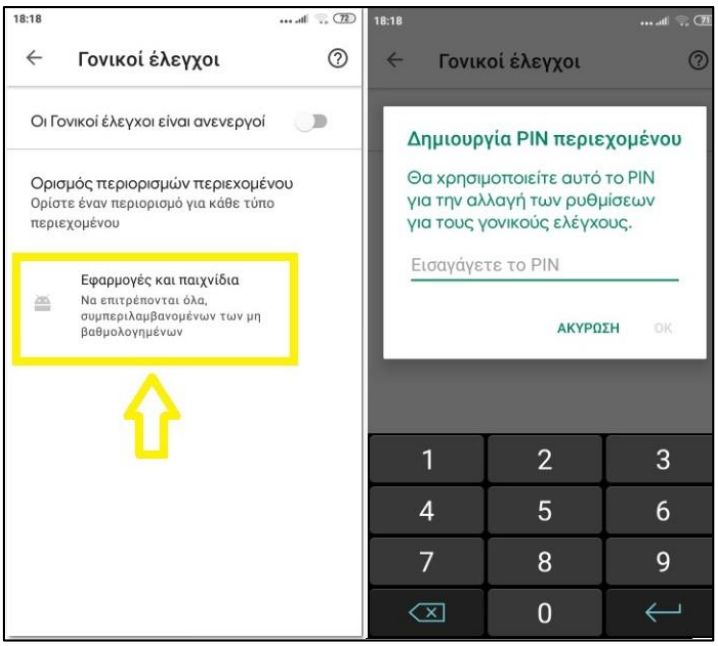
Εικόνα 68: *Family Link: Γονικός Έλεγχος – Βήμα 10ο*

Στη συνέχεια, στη λίστα των ρυθμίσεων που εμφανίζεται επιλέγουμε «Οικογένεια» και «Γονικοί έλεγχοι».



Εικόνα 69: *Family Link: Γονικός Έλεγχος – Βήμα 11ο*

Επιλέγοντας λοιπόν το γονικό έλεγχο, ανοίγει μια νέα οθόνη στην οποία ενεργοποιούμε την ιδιότητα αυτή. Απαιτείται από τον διαχειριστή να εισάγει ένα κωδικό ασφαλείας (PIN) ώστε οι όποιες αλλαγές του γονικού ελέγχου εφαρμοστούν να μη μπορούν να απενεργοποιηθούν από τον απλό χρήστη.

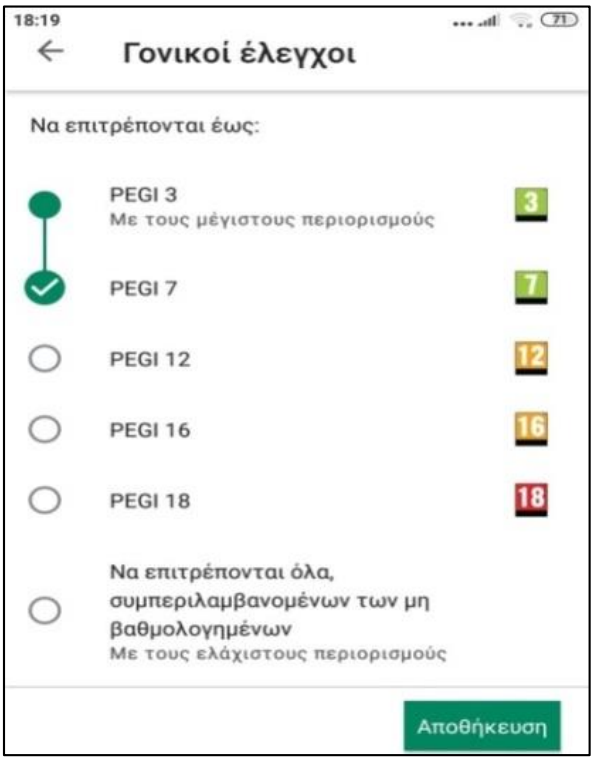


Εικόνα 70: *Family Link: Γονικός Έλεγχος – Βήμα 12ο*

Μετά την εισαγωγή του κωδικού ασφαλείας εμφανίζονται οι κατηγορίες στις οποίες μπορεί ο διαχειριστής να επέμβει και να ρυθμίσει.

Η κύρια κατηγορία του «PlayStore» είναι «Εφαρμογές και παιχνίδια». Επιλέγοντας λοιπόν αυτή την κατηγορία εμφανίζονται το φίλτρο για τα όρια ηλικίας που μπορούν να τεθούν ως προϋπόθεση για την πρόσβαση στις εφαρμογές και τα παιχνίδια που είναι διαθέσιμα. Τα όρια αυτά ορίζονται σύμφωνα με το διεθνές πρότυπο PEGI για το οποίο έγινε σχετική αναφορά νωρίτερα κατά την διαδικασία εφαρμογής του γονικού ελέγχου στα Microsoft Windows.

Αν για παράδειγμα ο διαχειριστής - γονέας επιλέξει το PEGI 7, αυτό σημαίνει ότι ο χρήστης - παιδί μπορεί να έχει πρόσβαση μόνο σε εφαρμογές και παιχνίδια για την ηλικιακή ομάδα επτά ετών και πάνω.



Εικόνα 71: *Family Link: Γονικός Έλεγχος – Βήμα 13^{ο}*

4.7 Χρήση προγραμμάτων και εφαρμογών για Windows και Android

Έως τώρα εξετάστηκε ο τρόπος εφαρμογής του γονικού ελέγχου μέσω των ρυθμίσεων που προσφέρουν οι τρεις πιο διαδεδομένες εκδόσεις των Microsoft Windows αλλά και η διαδικασία εφαρμογής ελέγχου σε συσκευές με λειτουργικό σύστημα Android.

Ο έλεγχος της γονικής επιτήρησης που προσφέρει δωρεάν η Microsoft, αποτελεί ίσως από τις πιο σημαντικές λειτουργίες του λειτουργικού συστήματος των Windows. Όμως, η απαίτηση που υπάρχει στις ψηφιακές συσκευές (έξυπνα τηλέφωνα, tablet κ.α.) προκειμένου να κάνουν χρήση της εφαρμογής του γονικού ελέγχου της Microsoft πρέπει να έχουν λειτουργικό Windows 10 mobile, αποτελεί ένα σοβαρό μειονέκτημα.

Όσον αφορά τις ψηφιακές συσκευές που διαθέτουν λειτουργικό σύστημα Android, οι δωρεάν επιλογές εφαρμογής του γονικού ελέγχου μέσω του "FamilyLink" της Google αλλά και οι μεμονωμένες ρυθμίσεις εφαρμογών όπως αυτή του PlayStore αποτελούν αξιόπιστες λύσεις αλλά με ένα βασικό μειονέκτημα, την παροχή περιορισμένων επιλογών και ρυθμίσεων.

Η λύση και αντιμετώπιση στα παραπάνω μειονεκτήματα δίνεται από μια πληθώρα προγραμμάτων που διατίθενται στον παγκόσμιο ιστό και τα οποία έχουν σχεδιαστεί για την προστασία και την παροχή γονικού ελέγχου για συσκευές διαφόρων λειτουργικών συστημάτων.

5. Νομοθεσία και Ηλεκτρονικό Έγκλημα

Ο παγκόσμιος ιστός, όπως έχουμε ήδη αναφέρει, εκτός από τα πολλά πλεονεκτήματα που προσφέρει καθημερινά στη σύγχρονη κοινωνία και στον άνθρωπο κρύβει και πολλούς κινδύνους.

Όμως, το βασικότερο και ίσως το σημαντικότερο μειονέκτημα του διαδικτύου είναι ίσως ο δύσκολος έως και αδύνατος έλεγχος των εκατομμυρίων πληροφοριών και δεδομένων που διακινούνται σε καθημερινή βάση. Ως «έλεγχο των πληροφοριών» δεν αναφερόμαστε στον έλεγχο του λόγου και της ελεύθερης έκφρασης ιδεών αλλά στον έλεγχο όλων εκείνων των πληροφοριών που παραβιάζουν τα ανθρώπινα δικαιώματα, την πλαστογραφία, την παράνομη διακίνηση αγαθών, την καταπάτηση πνευματικών δικαιωμάτων και γενικά όλες εκείνες τις παράνομες δραστηριότητες που σύμφωνα με τον ποινικό κώδικα συγκαταλέγονται στις αξιόποινες εγκληματικές πράξεις.

Σύμφωνα με τους Morrison και Forester, το έτος 1994 [25], ανέφεραν ότι «μια εγκληματική πράξη όπου έχει ως βασικό εργαλείο για την πραγματοποίησή της έναν ηλεκτρονικό υπολογιστή θα ονομάζεται Ηλεκτρονικό Έγκλημα».

Για το λόγω αυτό, κρατικοί φορείς κάθε χώρας προβαίνουν στη λήψη των απαραίτητων εκείνων μέτρων ώστε οι παράνομες πράξεις που καθιστούν ηλεκτρονικό έγκλημα να διώκονται σύμφωνα με την εκάστοτε νομοθεσία.

Οι κυριότερες κατηγορίες που καθιστούν αξιόποινες εγκληματικές δραστηριότητες μέσω του παγκόσμιου ιστού είναι:

- Παιδική πορνογραφία μέσω διαδικτύου
- Πειρατεία και διακίνηση παράνομου λογισμικού
- Διαδικτυακός Εκφοβισμός (cyberbullying)
- Κυβερνοεπιθέσεις - Hacking
- Οικονομικό Έγκλημα μέσω διαδικτύου
- «Ψάρεμα» Προσωπικών Δεδομένων
- Παραπλάνηση

5.1 Ελληνική Νομοθεσία

Στην ελληνική νομοθεσία και στον ποινικό κώδικα, συμπεριλαμβάνονται αρκετοί νόμοι και άρθρα για αδικήματα και παραβάσεις που μπορούν να τελεστούν στο χώρο του παγκόσμιου ιστού και αποτελούν Ηλεκτρονικό Έγκλημα.

Ακολούθως, γίνεται μια αναφορά στους νόμους, τα άρθρα του ποινικού κώδικα αλλά και στα σχετικά Προεδρικά Διατάγματα του Ελληνικού κράτους που σχετίζονται με το Ηλεκτρονικό Έγκλημα.

- Νόμοι

Νόμος	Τίτλος	ΦΕΚ
Ν.2225/1994	*«Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»*	121/Α/20-07-1994
Ν. 2246/1994	*«Οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών»*	172/Α/20-10-1994
Ν. 2672/1998	*Άρθρο 14 - «Διακίνηση εγγράφων με, ηλεκτρονικά μέσα (τηλεομοιοτυπία ηλεκτρονικό ταχυδρομείο)»*	290/Α/28-12-1998
Ν.2867/2000	*«Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις»*	273/Α/19-12-2000
Ν .3115/2003	*«Αρχή διασφάλισης του απορρήτου των επικοινωνιών»*	47/Α/27-02-2003
Ν.3431/2006	*«Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις»*	13/Α/13-02-2006
Ν. 3471/2006	*«Προστασία Δεδομένων Προσωπικού Χαρακτήρα»*	133/Α/28-06-2006
Ν. 4619/2019	*«Κύρωση του Ποινικού Κώδικα»*	95/Α/11-6-2019

Πίνακας 1: *Νόμοι*

- Άρθρα Ποινικού Κώδικα

Άρθρο Π.Κ.	Τίτλος
348Α	*«Πορνογραφία ανηλίκων»*
370Α	*«Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας»*
370Β	*«Παράνομη πρόσβαση σε σύστημα πληροφοριών ή σε δεδομένα»*
370Γ	*«Παράνομη πρόσβαση σε πληροφοριακό σύστημα»*
386Α	*«Απάτη με υπολογιστή»*

Πίνακας 2: *Άρθρα Ποινικού Κώδικα*

- Προεδρικά Διατάγματα

Π.Δ.	Τίτλος	ΦΕΚ
150/2001	*«Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές».*	125/Α/25-6-2001
131/2003	*«Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά (οδηγία για το ηλεκτρονικό εμπόριο)»*	116/Α/16-5-2003
47/2005	*«Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του»*	64/Α/10-3-2005

Πίνακας 3: *Προεδρικά Διατάγματα*

5.2 Ευρωπαϊκή Νομοθεσία

Σύμφωνα με την υφιστάμενη νομοθεσία της Ευρωπαϊκή Ένωση που σχετίζεται με την πρόσβαση των πολιτών στο διαδίκτυο, σύμφωνα με τον «*Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης*» (2000/C 364/01), αναφέρεται ότι «*…η ένωση αναγνωρίζει τα δικαιώματα, τις ελευθερίες και τις αρχές των πολιτών των κρατών μελών της…*» μέσα από μια σειρά άρθρων.

Μεταξύ αυτών και συγκεκριμένα στο δεύτερο κεφάλαιο, άρθρο 11 με θέμα «*Ελευθερία έκφρασης και πληροφόρησης*» αναφέρει στη πρώτη παράγραφο ότι: «*Κάθε πρόσωπο έχει δικαίωμα στην ελευθερία έκφρασης. Το δικαίωμα αυτό περιλαμβάνει την ελευθερία γνώμης και την ελευθερία λήψης ή μετάδοσης πληροφοριών ή ιδεών, χωρίς την ανάμειξη δημοσίων αρχών και αδιακρίτως συνόρων*».

Με το άρθρο αυτό λοιπόν γίνεται έμμεσα σαφές ότι οι Ευρωπαίοι πολίτες έχουν δικαιωματικά κατοχυρώσει την ελεύθερη πρόσβασή τους στον παγκόσμιο ιστό.

Όσον αφορά το Ηλεκτρονικό Έγκλημα και την ασφάλεια από παράνομες δραστηριότητες στον παγκόσμιο ιστό, ιδρύθηκε το 2004, ο οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (*ENISA*) με αρχική έδρα το Ηράκλειο Κρήτης. Το 2018 μεταφέρθηκε επισήμως στην Αθήνα [https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016R0679&from=EL].

Σκοπός του ENISA είναι να ενημερώνει τόσο του φορείς του δημόσιου και ιδιωτικού τομέων των κρατών μελών της Ευρωπαϊκής Ένωσης σε θέματα Κυβερνοασφάλειας.

Ειδικότερα πραγματεύεται αντικείμενα όπως:

- Αντιμετώπιση κρίσεων στον παγκόσμιο ιστό
- Ασφάλεια στο διαδίκτυο
- Δημιουργία ομάδων αντιμετώπισης θεμάτων επειγουσών αναγκών σε θέματα πληροφορικής
- Προστασία Δεδομένων και ηλεκτρονικών συναλλαγών

Ο Ευρωπαϊκός Οργανισμός ENISA συμμετέχει ενεργά στη δημιουργία και εφαρμογή του νομοθετικού πλαισίου της Ευρωπαϊκής Ένωσης που σχετίζεται με την ασφάλεια στο διαδίκτυο.

Στη συνέχεια παρουσιάζονται οι οδηγίες και νομοθετήματα της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη της που σχετίζονται με τη πρόσβαση των πολιτών στο παγκόσμιο ιστό αλλά και την πρόληψη και αντιμετώπιση του Ηλεκτρονικού Εγκλήματος.

Οδηγίες	Τίτλος
96/9/ΕΟΚ	*«Νομική προστασία των βάσεων δεδομένων»*
97/33/ΕΚ	*«Διασύνδεση στο χώρο των τηλεπικοινωνιών προκειμένου να διασφαλισθεί καθολική υπηρεσία και διαλειτουργικότητα, με εφαρμογή των αρχών παροχής ανοικτού δικτύου (ONP)»*
98/7/ΕΚ	*«Προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη»*
1999/93/ΕΚ	*«Κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές»*
2000/31/ΕΚ	*«Νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά»*
2002/19/ΕΚ	*«Πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους»*
2002/20/ΕΚ	*«Αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση)»*
2002/21/ΕΚ	*«Κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών»*
2002/22/ΕΚ	*«Καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών»*
2002/58/ΕΚ	*«Επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών»*
2002/77/ΕΚ	*«Ανταγωνισμός στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών»*
2009/24/ΕΚ	*«Νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών»*
2011/83/ΕΚ	*«Ενίσχυση των δικαιωμάτων των καταναλωτών στην ΕΕ*
2019/2161/ΕΕ	*«Τροποποιητική οδηγία επεκτείνει το πεδίο εφαρμογής της οδηγίας 2011/83/ΕΕ ώστε να συμπεριληφθούν οι συμβάσεις βάσει των οποίων ο έμπορος παρέχει ή αναλαμβάνει να παράσχει ψηφιακή υπηρεσία* ή ψηφιακό περιεχόμενο* στον καταναλωτή, ο δε καταναλωτής παρέχει ή αναλαμβάνει να παράσχει δεδομένα προσωπικού χαρακτήρα»*

Πίνακας 4: *Οδηγίες και νομοθετήματα της Ε.Ε. για την πρόσβαση στο διαδίκτυο*

6. Δημιουργία διαδικτυακής πλατφόρμας

Σκοπός της παρούσας διπλωματικής εργασίας είναι η ενημέρωση γονέων, εκπαιδευτικών και παιδιών σε θέματα ασφαλούς πλοήγησης στο παγκόσμιο ιστό με την υποστήριξη μιας διαδικτυακής πλατφόρμας (ιστοσελίδας).

Στην ιστοσελίδα αυτή υπάρχει υλικό το οποίο προέρχεται από ελληνικές αλλά και παγκοσμίου επιπέδου έρευνες που σχετίζονται με την ασφάλεια στο διαδίκτυο, το γονικό έλεγχο και την ενημέρωση για τα μέσα κοινωνικής δικτύωσης. Επίσης, γίνεται μια αναφορά στους κινδύνους του διαδικτύου και το πως αυτοί μπορούν να αντιμετωπιστούν. Η ενημέρωση γίνεται:

- Μέσω άρθρων που αφορούν τα πιο σημαντικά θέματα αντιμετώπισης κινδύνων του παγκόσμιου ιστού.
- Μέσω παιχνιδιών γνώσεων για μικρούς και μεγάλους.
- Μέσω παρουσιάσεων – οδηγιών για τη λειτουργία και ρύθμιση των ψηφιακών συσκευών σε θέματα εφαρμογής γονικού ελέγχου.

Η ιστοσελίδα δημιουργήθηκε με ένα από τα πιο γνωστά συστήματα διαχείρισης περιεχομένου ανοιχτού κώδικα (Content Management Systems, CMS) το Wordpress.

6.1 Γνωριμία με το Wordpress

Η εφαρμογή δημιουργίας ιστοσελίδων Wordpress έκανε την εμφάνισή της για πρώτη φορά το 2004. Αποτελεί λογισμικό ανοιχτού κώδικα και διατίθεται δωρεάν σε αρκετές γλώσσες. Η λειτουργία του είναι απλή, αρκετά φιλική προς τον χρήστη (userfriendly) και έχει ως βάση την PHP και MySQL.

Ο αρχικός λόγος σχεδίασης του Wordpress αφορούσε τη δημιουργία ιστολογίων (blogs), όμως σύντομα μετατράπηκε σε ένα εργαλείο δημιουργίας δυναμικών ιστοσελίδων.

Το Wordpress έγινε ιδιαίτερα δημοφιλής γιατί προσφέρει στο χρήστη μια πληθώρα δυνατοτήτων και λειτουργιών. Επίσης, ένα ακόμα πολύ σημαντικό γνώρισμα της πλατφόρμας αυτής είναι ότι για την κατασκευή μιας ιστοσελίδας δεν είναι απαραίτητο ο χρήστης να έχει εξειδικευμένη προγραμματιστική εμπειρία. Γενικά, ο χρήστης δεν εμπλέκεται με το προγραμματιστικό μέρος και τη συγγραφή κώδικα σε HTML ή PHP, παρόλο που το Wordpress δίνει τη δυνατότητα, σε όποιον γνωρίζει, να επέμβει στο προγραμματιστικό περιβάλλον.

Από τα κυριότερα μειονεκτήματα της πλατφόρμας μεταξύ άλλων συγκαταλέγονται οι περιορισμένες δυνατότητες που παρέχει το Wordpress όσον αφορά το σχεδιασμό του περιβάλλοντος, αν και υπάρχει μια πληθώρα θεμάτων/προτύπων (templates) που διατίθενται δωρεάν προς χρήση.

6.2 Διαδικασία υλοποίησης

Η δημιουργία μιας ιστοσελίδας μέσω της εφαρμογής Wordpress απαιτεί τη λήψη και εγκατάσταση του αντίστοιχου λογισμικού από τον χρήστη (https://el.wordpress.org/download/). Στο σημείο αυτό ο χρήστης έχει τη δυνατότητα ***α)*** είτε να εγκαταστήσει το Wordpress στον προσωπικό του ηλεκτρονικό υπολογιστή τοπικά, ***β)*** είτε απευθείας σε έναν server στο διαδίκτυο εφόσον διαθέτει τα σχετικά δικαιώματα. Στην πρώτη περίπτωση, πρέπει να εγκατασταθεί στον ηλεκτρονικό υπολογιστή η εφαρμογή Xampp η οποία έχει ως σκοπό την προσομοίωση ενός διαδικτυακού server και η ιστοσελίδα λειτουργεί μόνο σε τοπικό επίπεδο.

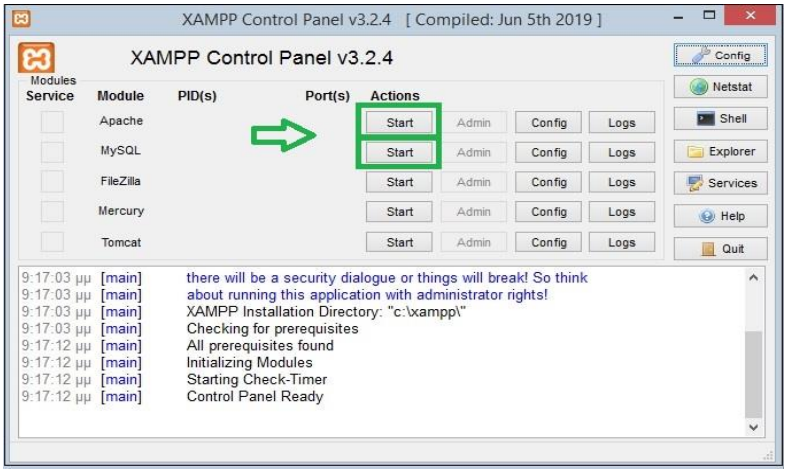
Όσον αφορά το σχεδιασμό και την υλοποίηση της συγκεκριμένης εκπαιδευτικής διαδικτυακής πλατφόρμας για την ασφαλή πλοήγηση στο διαδίκτυο χρησιμοποιήθηκε ο πρώτος τρόπο λειτουργίας της εφαρμογής του Wordpress. Η εγκατάσταση έγινε σε τοπικό ηλεκτρονικό υπολογιστή. Ο σχεδιασμός και η υλοποίηση πραγματοποιήθηκαν με τη βοήθεια του προσομοιωτή Xampp.

6.3 Διαδικασία εγκατάστασης του WordPress τοπικά στον ηλεκτρονικό υπολογιστή μέσω του XAMPP

Το XAMPP είναι μια δωρεάν εφαρμογή όπου η βασική της λειτουργία είναι η προσομοίωση ενός διαδικτυακού server σε έναν τοπικό υπολογιστή όπου είναι εγκατεστημένη και συμπεριλαμβάνει όλες εκείνες τις εφαρμογές που είναι απαραίτητες για τη λειτουργία μιας δυναμικής ιστοσελίδας. Με αυτόν τον τρόπο ο χρήστης μπορεί να σχεδιάσει και να ετοιμάσει την ιστοσελίδα του στον προσωπικό του ηλεκτρονικό υπολογιστή και στη συνέχεια να τη δημοσιεύσει σε έναν webserver της αρεσκείας του.

Καταρχήν πρέπει να γίνει η λήψη του αρχείου του Xampp από την επίσημη ιστοσελίδα (https://www.apachefriends.org/download.html) και η εγκατάστασή του στον ηλεκτρονικό υπολογιστή.

Στη συνέχεια εκτελείται η εφαρμογή από το αρχείο Xampp-control.exe και γίνεται η ενεργοποίηση των ενοτήτων Apache και MySQL.

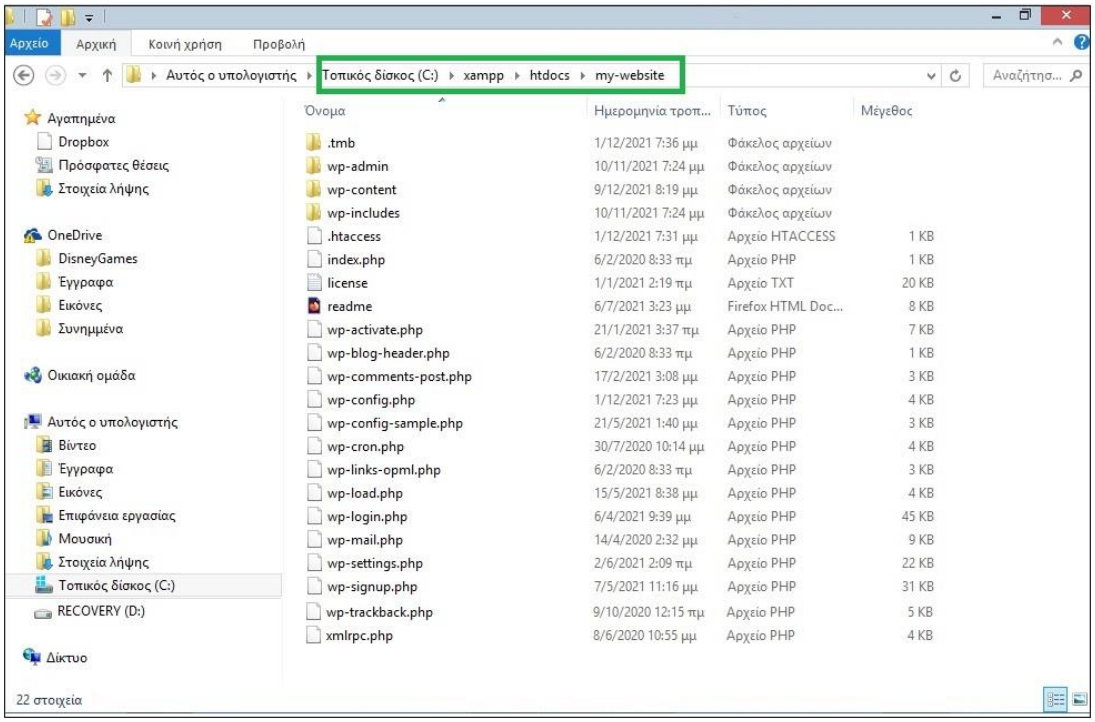


Εικόνα 72: *Ενεργοποίηση ενοτήτων Apache και MySQL*

Με αυτόν τον τρόπο έχει ενεργοποιηθεί ο τοπικός server και μπορεί να γίνει η αλληλεπίδραση των αρχείων με τη βάση δεδομένων ώστε να λειτουργεί κανονικά (σε τοπικό επίπεδο) η ιστοσελίδα.

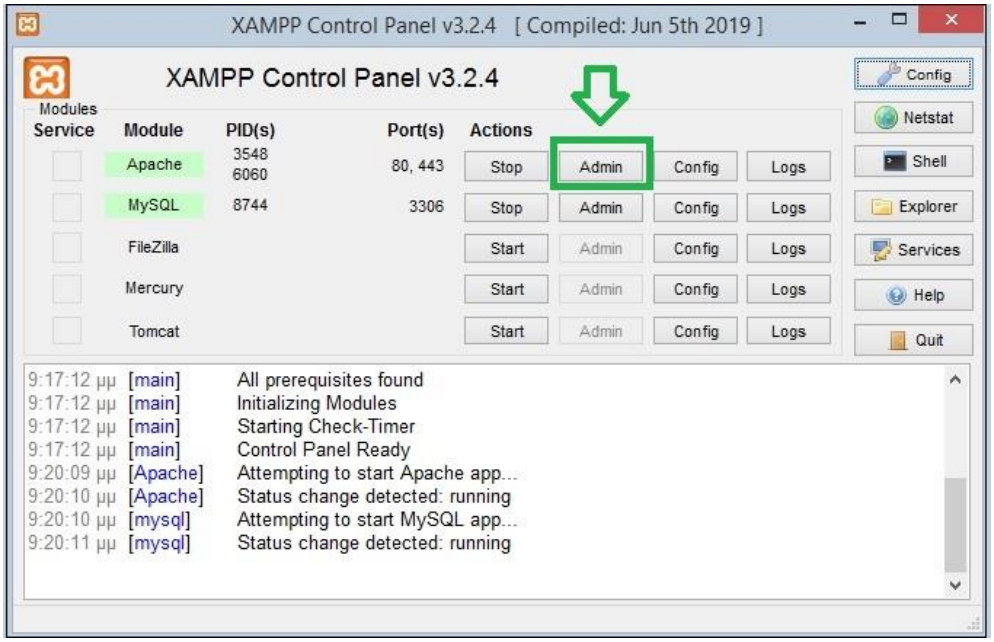
Το επόμενο βήμα είναι η λήψη της εφαρμογής Wordpress. Ο συμπιεσμένος φάκελος που προκύπτει με τα αρχεία του Wordpress θα πρέπει να αποσυμπιεστεί στον υποφάκελο «htdocs» της εφαρμογής Xampp.

Καλό είναι αφού γίνει μετάβαση στον υποφάκελο «htdocs», να δημιουργηθεί ένας νέος υποφάκελος όπου θα αποσυμπιεστούν τα σχετικά αρχεία.



Εικόνα 73: *Δημιουργία υποφακέλου για την αποσυμπίεση των αρχείων*

Μετά την ολοκλήρωση της αποσυμπίεσης των αρχείων του Wordpress, σειρά έχει η δημιουργία της βάσης δεδομένων.

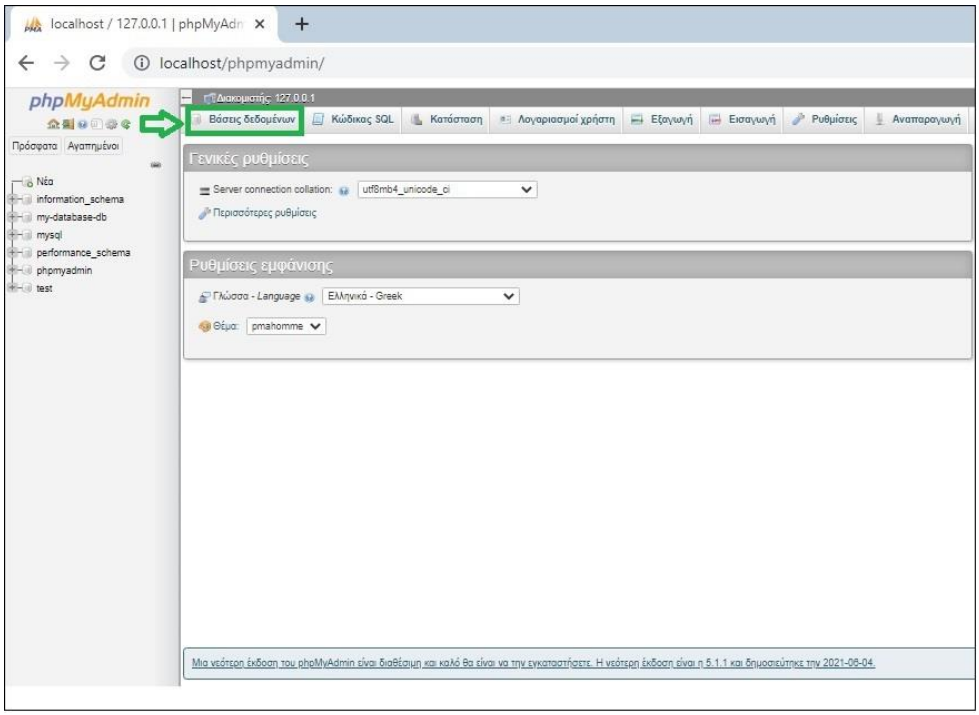


Εικόνα 74: *Διαδικασία δημιουργίας βάσης δεδομένων*

Στο παράθυρο του XAMPP, ο χρήστης επιλέγει από το αντίστοιχο μενού «phpMyAdmin».

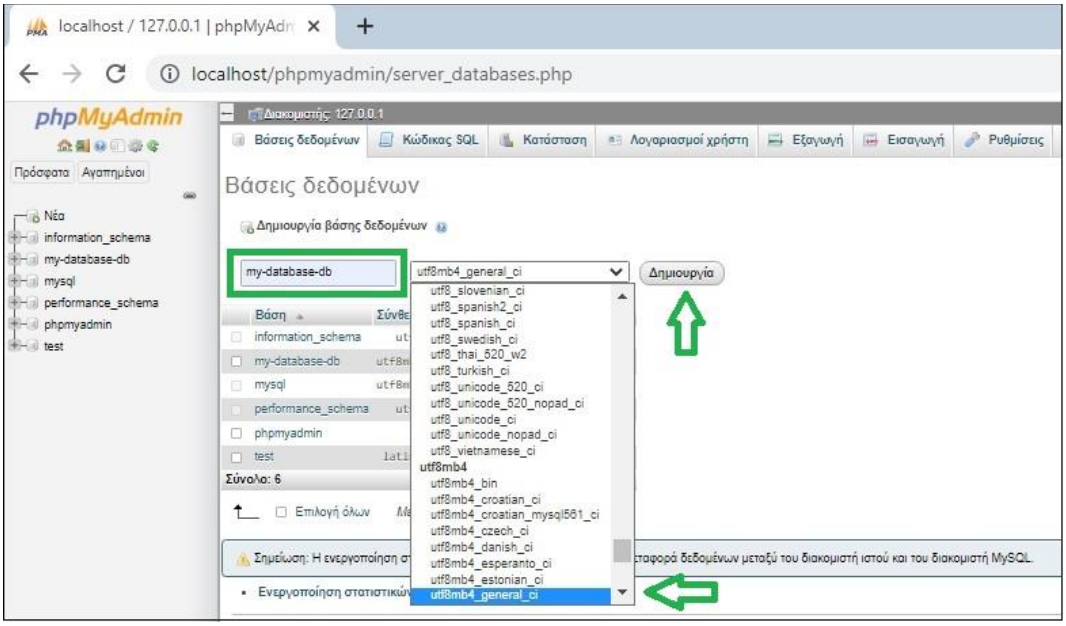
Εικόνα 75: *Δημιουργία Βάσης Δεδομένων*

Στη νέα καρτέλα του μενού, γίνεται η επιλογή «Βάσεις Δεδομένων»



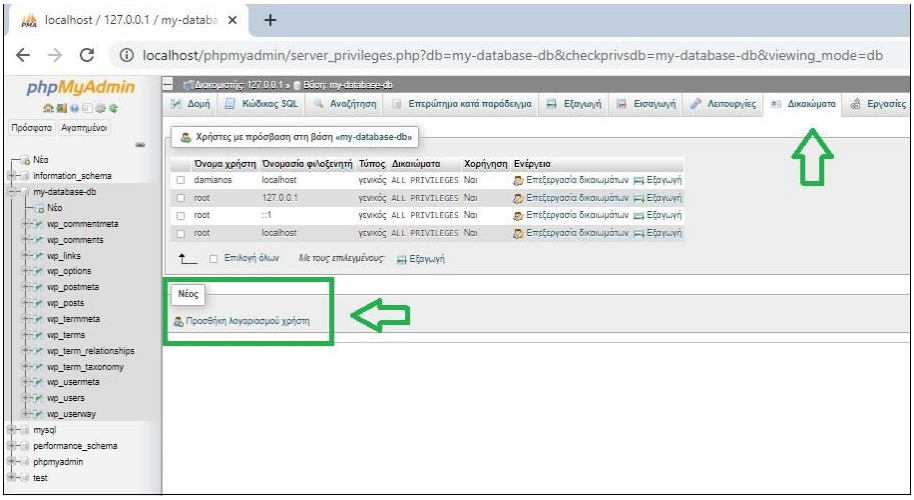
Εικόνα 76: *Ορισμός Βάσης Δεδομένων*

Στο σημείο αυτό ο χρήστης εισάγει το όνομα που επιθυμεί να έχει η βάση δεδομένων (my-database-db), επιλέγει το «utf8mb4_general_ci» για την υποστήριξη της ελληνικής γλώσσας από τη βάση και πατώντας το κουμπί «Δημιουργία» δημιουργεί τη βάση δεδομένων με τα χαρακτηριστικά που έχει ορίσει.



Εικόνα 77: *Καθορισμός και Δημιουργία Βάσης Δεδομένων*

Επόμενο βήμα είναι ο ορισμός του διαχειριστή που θα έχει τα δικαιώματα και πρόσβαση στη βάση. Αυτό γίνεται από τη καρτέλα "Δικαιώματα" και την επιλογή "Προσθήκη λογαριασμού χρήστη".

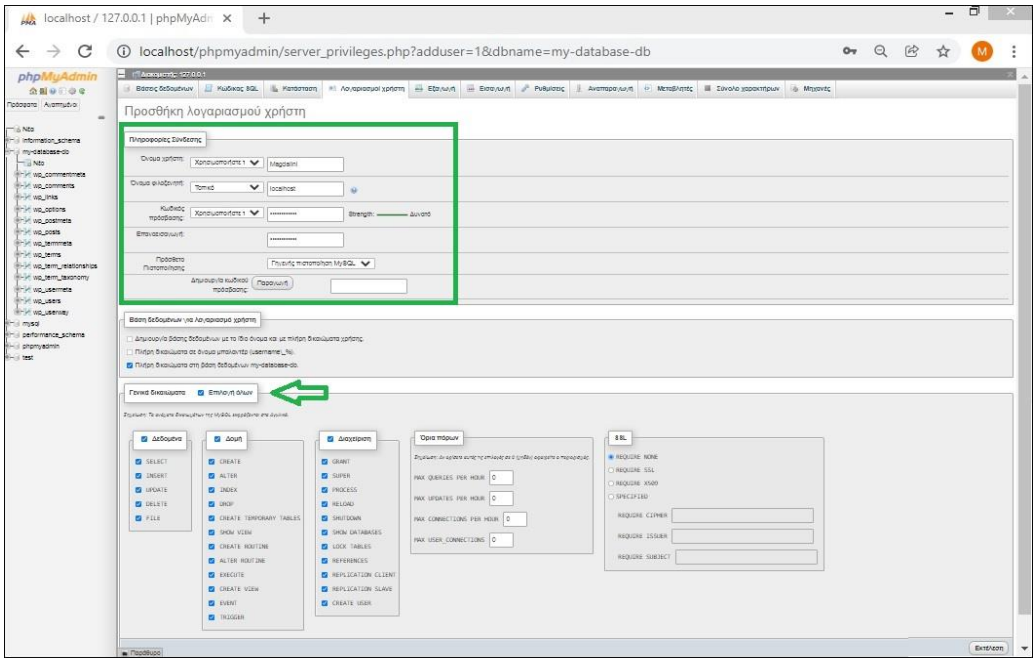


Εικόνα 78: *Προσθήκη λογαριασμού χρήστη*

Στην καρτέλα αυτή γίνεται ο ορισμός:

- του ονόματος του διαχειριστή (Magdalini),
- του ονόματος του κεντρικού υπολογιστή-φιλοξενητή (localhost). Επιλέγουμε "Τοπικό" καθότι ο server είναι ο τοπικός ηλεκτρονικός υπολογιστής.
- του κωδικού πρόσβασης (password). Εναλλακτικά υπάρχει η δυνατότητα δημιουργίας αυτόματου κωδικού πρόσβασης με το κουμπί «Παραγωγή».

Στη συνέχεια, ο χρήστης ορίζει τα δικαιώματα με την επιλογή «Επιλογή όλων» και μόλις ολοκληρώσει τα παραπάνω βήματα πατάει το κουμπί «Εκτέλεση».



Εικόνα 79: *Ορισμός δικαιωμάτων χρήστη*

Εφόσον ολοκληρωθούν οι παραπάνω ενέργειες, το επόμενο βήμα αφορά την εγκατάσταση της εφαρμογής του Wordpress.

Σε έναν νέο φυλλομετρητή (browser) ο χρήστης πληκτρολογεί τη διεύθυνση της ιστοσελίδας η οποία αλληλεπιδρά με τη βάση δεδομένων του τοπικού server Xampp που καθορίστηκε νωρίτερα. Σύμφωνα με τις προηγούμενες ρυθμίσεις η διεύθυνση αυτή είναι: https://localhost/my-website/wordpress.

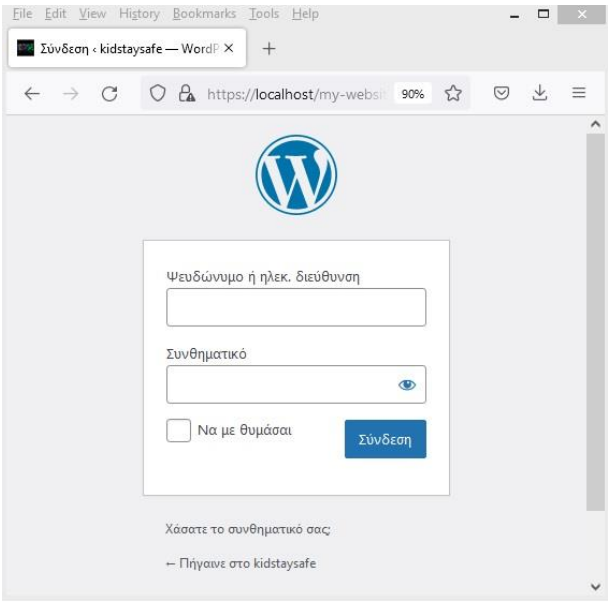
Αμέσως μετά ξεκινά η διαδικασία εγκατάστασης του Wordpress με μια σειρά βημάτων όπου ο χρήστης καταχωρεί τη γλώσσα, το όνομα της βάσης δεδομένων που έχει ήδη οριστεί, το όνομα διαχειριστή της βάσης και τον κωδικό πρόσβασης

Εικόνα 80: *Εγκατάσταση του Wordpress*

Το WordPress αλληλεπιδρά με τη βάση δεδομένων του τοπικού server και απαιτείται από το χρήστη να ορίσει για τη διαχείριση της πλατφόρμας το όνομα της ιστοσελίδας, το όνομα χρήστη, τον κωδικό πρόσβασης και τη διεύθυνση ηλεκτρονικού ταχυδρομείου.

Εικόνα 81: *Διαδικασία εγκατάστασης του Wordpress*

Η εγκατάσταση του WordPress ολοκληρώθηκε στον τοπικό ηλεκτρονικό υπολογιστή και η πρόσβαση πλέον στο περιβάλλον της πλατφόρμας για το σχεδιασμό και την επεξεργασία της ιστοσελίδας https://localhost/my-website/wordpress γίνεται μέσω του συνδέσμου: https://localhost/my-website/wordpress/wp-admin.



Εικόνα 82: *Πρόσβαση στη Πλατφόρμα Σχεδιασμού*

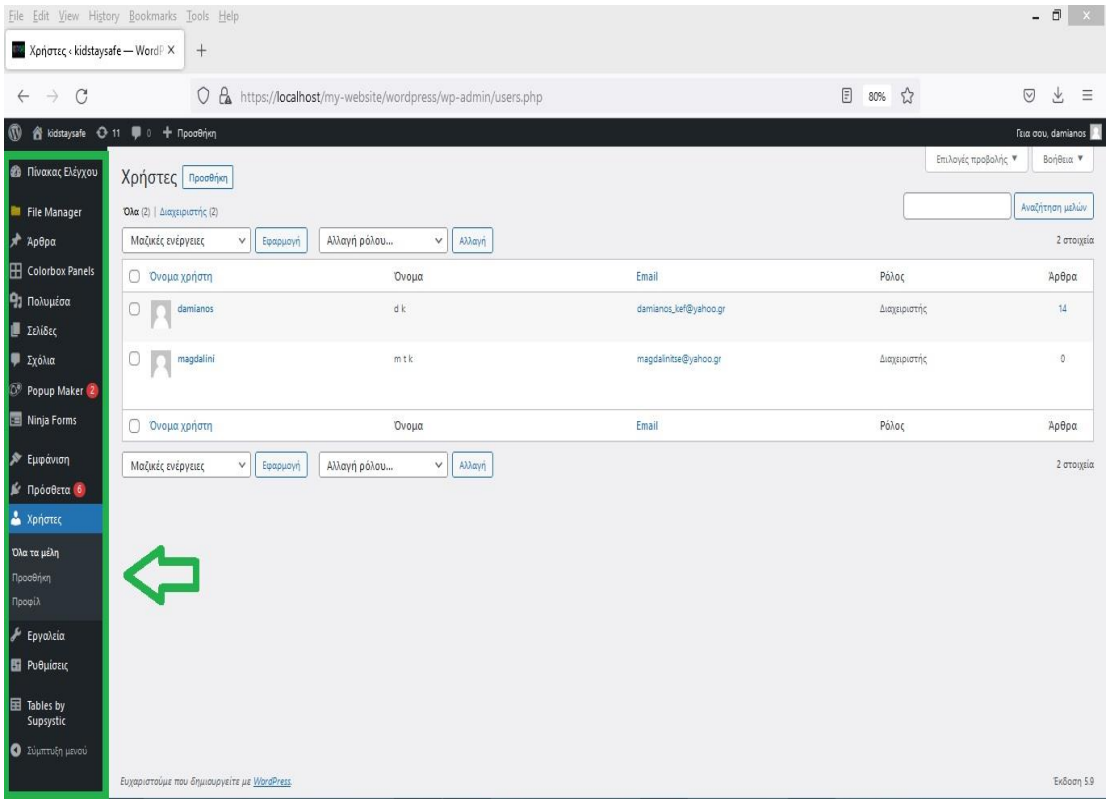
6.4 Σχεδιασμός της ιστοσελίδας kidstaysafe στο Wordpress

Η υλοποίηση της ιστοσελίδας *kidstaysafe* καθορίζεται μέσα από τον σχεδιασμό μιας σειράς σελίδων και την εμφάνιση και διάρθρωση των αντίστοιχων πληροφοριών.

6.4.1 Περιβάλλον Σχεδίασης

Το περιβάλλον σχεδίασης του Wordpress υποστηρίζει την ελληνική γλώσσα και αυτό το καθιστά ιδιαίτερα προσιτό και ευχάριστο. Επίσης, χαρακτηρίζεται από μεγάλη ευκολία και λειτουργικότητα.

Μετά τη σύνδεση του διαχειριστή - σχεδιαστή στην πλατφόρμα του Wordpress, εισέρχεται στο περιβάλλον σχεδίασης όπου στην αριστερή στήλη παρατίθενται όλες οι προσφερόμενες λειτουργίες για τη δημιουργία και μορφοποίηση της ιστοσελίδας.



Εικόνα 83: *Περιβάλλον Σχεδίασης Wordpress*

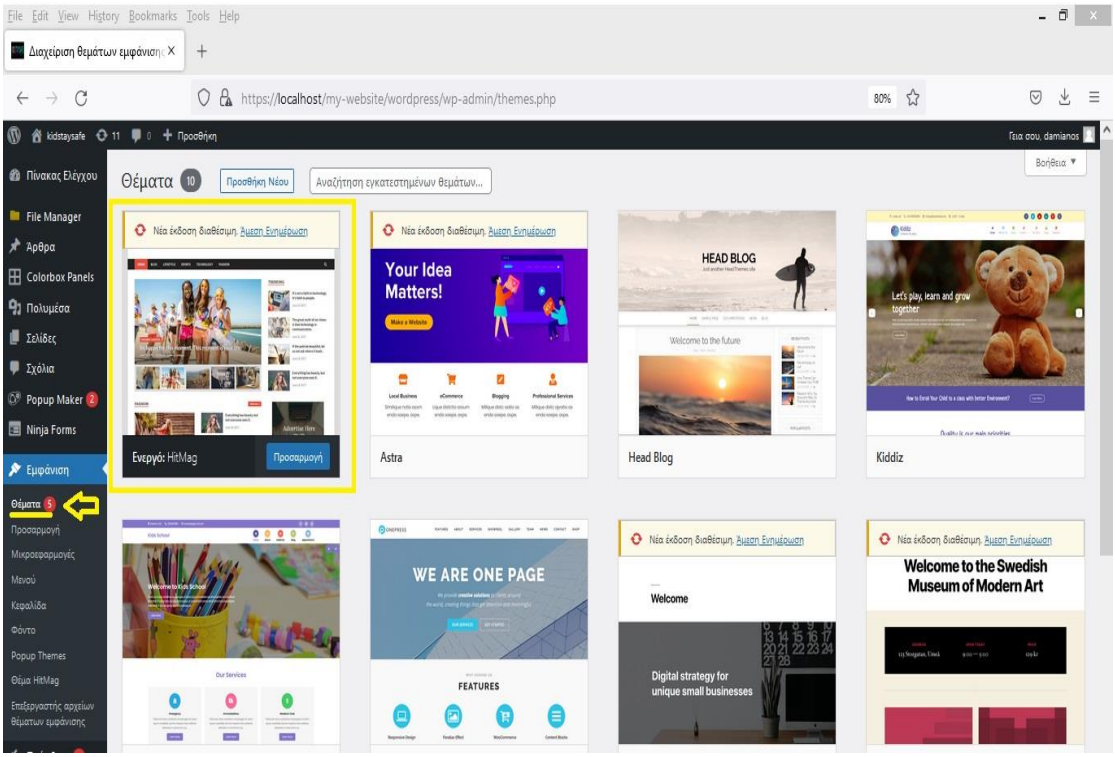
Οι βασικές διαδικασίες μορφοποίησης οι οποίες ακολουθήθηκαν και για τη δημιουργία της ιστοσελίδας kidstaysafe μπορούν να κατηγοριοποιηθούν σε τέσσερα βασικά βήματα:

Βήμα 1ο: Ορισμός Θέματος / Προτύπου (template)

Αρχικά γίνεται η επιλογή του θέματος ή προτύπου (template) το οποίο ορίζει τη μορφή της ιστοσελίδας.

Για την επιλογή του κατάλληλου θέματος επιλέγουμε από τις προσφερόμενες λειτουργίες *Εμφάνιση>Θέματα* και μέσα από μια πληθώρα δωρεάν θεμάτων/προτύπων μπορούμε να επιλέξουμε και να εγκαταστήσουμε το πρότυπο που μας ενδιαφέρει και να το μορφοποιήσουμε αναλόγως.

Στη προκειμένη περίπτωση επιλέχθηκε το θέμα «HitMag».

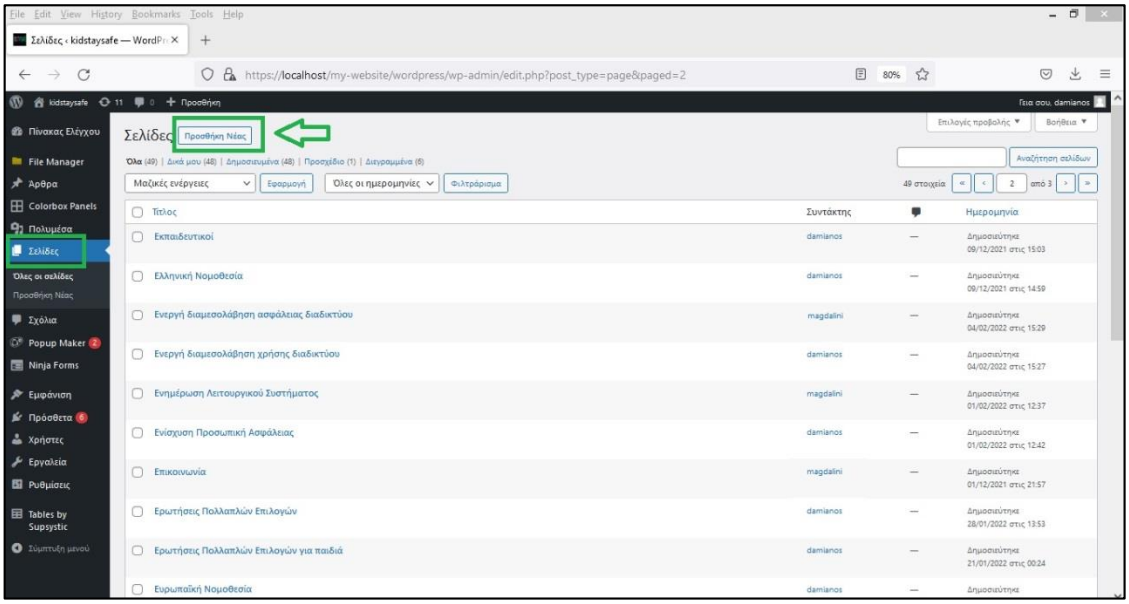


Εικόνα 84: *Ορισμός «Θέματος / Προτύπου»*

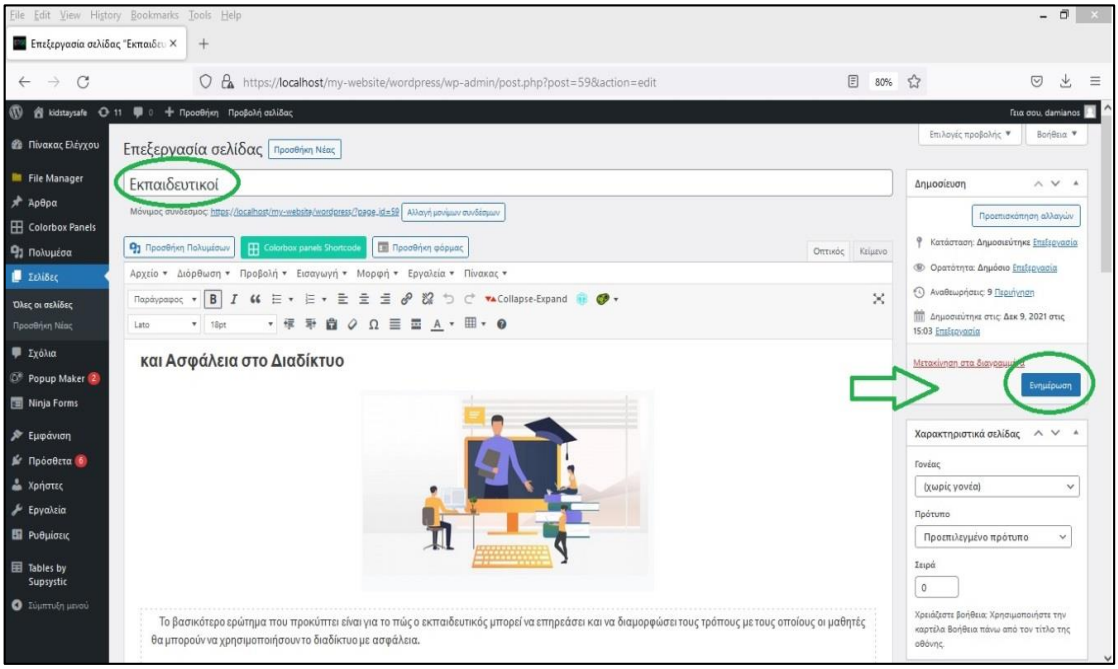
Βήμα 2ο: Δημιουργία Σελίδων και Άρθρων

Στο σημείο αυτό ο διαχειριστής - σχεδιαστής δημιουργεί όλες τις Σελίδες και τα Άρθρα από τα οποία θα αποτελείται η ιστοσελίδα.

Για τη δημιουργία Σελίδων επιλέγουμε *Σελίδες>Προσθήκη Νέας* και στο παράθυρο που ανοίγει με τη μορφή κειμενογράφου δημιουργούμε τη Σελίδα, δίνουμε ένα όνομα σε αυτήν και μετά την ολοκλήρωσή της επιλέγουμε «*Ενημέρωση*» όπου και αποθηκεύεται στον εκάστοτε server (στη περίπτωσή μας στον τοπικό server).

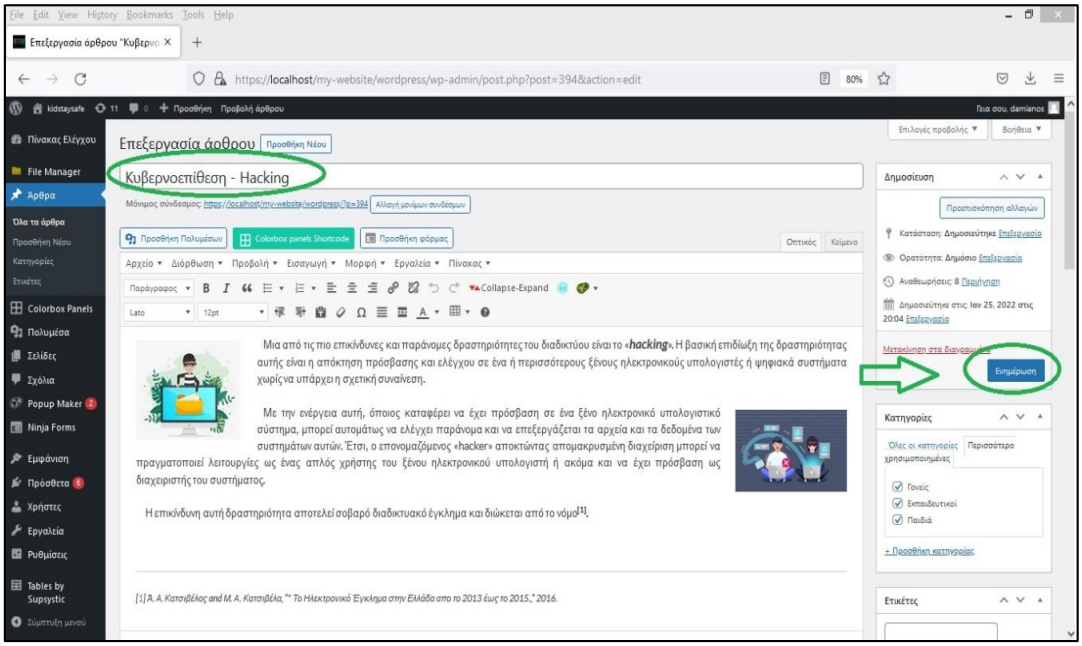


Εικόνα 85: *Προσθήκη Νέας Σελίδας*



Εικόνα 86: *Προσθήκη Νέας Σελίδας*

Με παρόμοιο τρόπο δημιουργούνται τα Άρθρα. Επιλέγουμε από το πλευρικό μενού *Άρθρα>Προσθήκη Νέου* και μετά την ολοκλήρωσή του επιλέγουμε «*Ενημέρωση*».

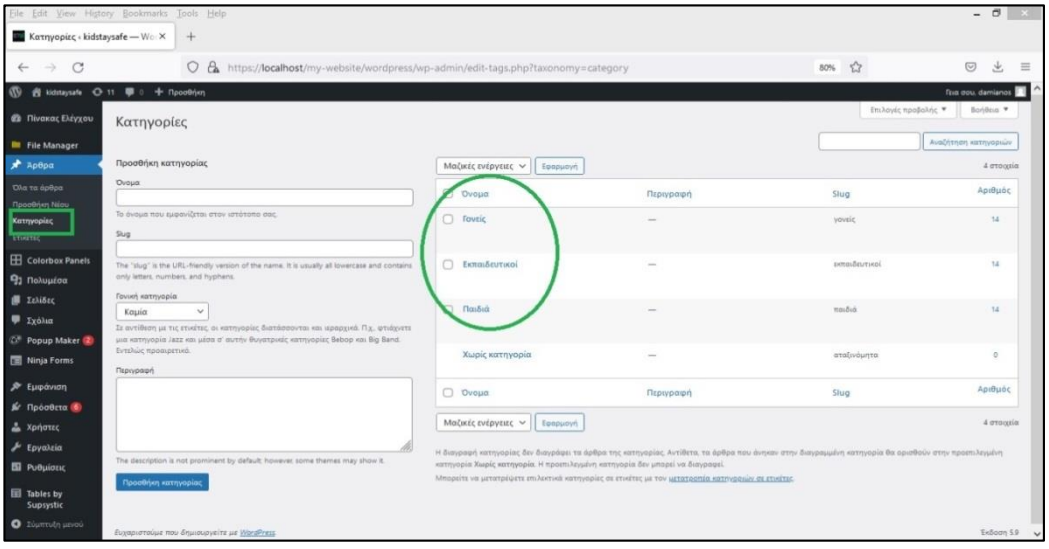


Εικόνα 87: *Προσθήκη / Δημιουργία Νέου Άρθρου*

Υπάρχει επίσης η δυνατότητα δημιουργίας «*Κατηγοριών*». Με αυτό τον τρόπο κατηγοριοποιούνται τα άρθρα σε ομάδες ώστε στη περίπτωση που ο χρήστης ενδιαφέρεται για άρθρα μιας συγκεκριμένης κατηγορίας θα μπορεί να πληκτρολογεί στην αναζήτηση τη κατηγορία που επιθυμεί και να εμφανίζονται όλα τα σχετικά άρθρα.

Στη περίπτωση της τρέχουσας ιστοσελίδας δημιουργήθηκαν τρεις βασικές κατηγορίες:

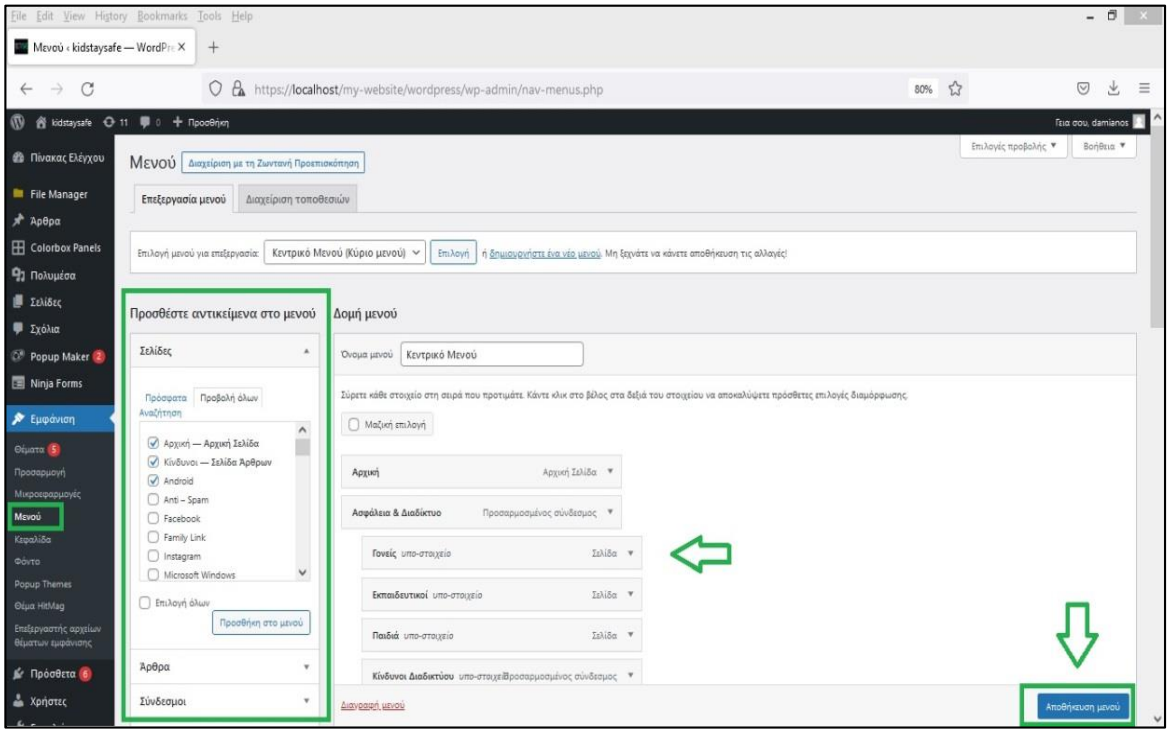
- Γονείς
- Εκπαιδευτικοί
- Παιδιά



Εικόνα 88: *Δημιουργία Κατηγοριών*

Βήμα 3ο: Δημιουργία Μενού

Επόμενο βήμα είναι η δημιουργία του κεντρικού Μενού της ιστοσελίδας. Αυτό γίνεται επιλέγοντας *Εμφάνιση > Μενού*. Από την επιλογή «*Προσθέστε αντικείμενα στο μενού*» εισάγονται Σελίδες και Άρθρα που δημιουργήθηκαν νωρίτερα και αποτελούν μέρος του κεντρικού μενού και στη συνέχεια οριστικοποιείται το μενού επιλέγοντας «*Αποθήκευση Μενού*».

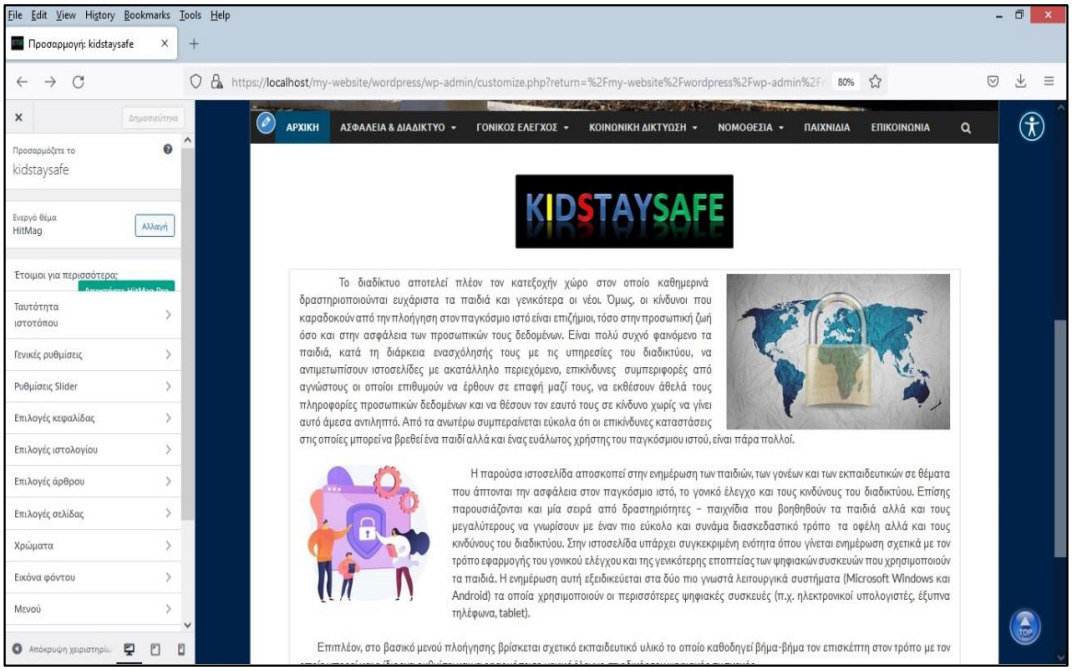


Εικόνα 89: *Δημιουργία Μενού*

Βήμα 4ο: Προσαρμογή

Μετά την ολοκλήρωση των προηγούμενων βημάτων σειρά έχει η διαμόρφωση της ιστοσελίδας όσον αφορά τον ορισμό της ταυτότητας του ιστοτόπου, τους χρωματισμούς, τις επιλογές κεφαλίδας και των άρθρων, τον ορισμό της εικόνα φόντου κ.α. ώστε να αποκτήσει η ιστοσελίδα τη μορφή που επιθυμεί ο διαχειριστής-σχεδιαστής.

Αυτό πραγματοποιείται μέσω της καρτέλας «*Προσαρμογή*» (Εμφάνιση>Προσαρμογή).

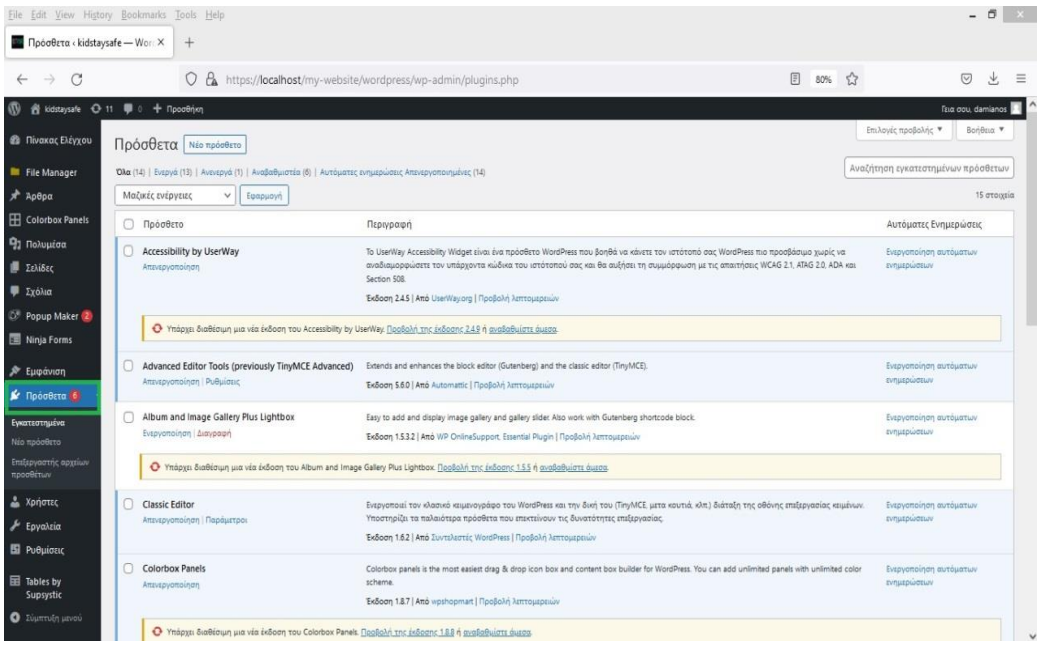


Εικόνα 90: *Προσαρμογή Ιστοσελίδας*

Με τα τέσσερα αυτά βασικά βήματα σχεδιάζεται η ιστοσελίδα και μορφοποιείται σύμφωνα με τις εκάστοτε απαιτήσεις.

Επίσης, θα ήταν παράληψη εάν δεν αναφέραμε ότι η Πλατφόρμα Σχεδίασης του Wordpress προσφέρει μια πληθώρα από δωρεάν πρόσθετες εφαρμογές οι οποίες προσθέτουν στην ιστοσελίδα περισσότερες λειτουργίες κάνοντάς την ακόμα πιο ελκυστική.

Για να έχουμε πρόσβαση στις Πρόσθετες εφαρμογές επιλέγουμε από την πλευρική στήλη «Πρόσθετα» και εγκαθιστούμε την εφαρμογή που μας ενδιαφέρει.



Εικόνα 91: *Προσθήκη Πρόσθετων Εφαρμογών*

Όσον αφορά τη δημιουργία της ιστοσελίδας *kidstaysafe* χρησιμοποιήθηκαν τα ακόλουθα πρόσθετα:

α/α	Πρόσθετο WordPress	*Επεξήγηση*
1.	**Accessibility by UserWay**	*Αφορά τη συμμόρφωση με τις απαιτήσεις WCAG 2.1, ATAG 2.0, ADA και Section 508*
2.	**Advanced Editor Tools (previously TinyMCE Advanced):**	*Εξειδικευμένος Κειμενογράφος*
3.	**Album and Image Gallery Plus Lightbox**	*Εύκολος τρόπος προβολής εικόνων*
4.	**Classic Editor**	*Κειμενογράφος*
5.	**Colorbox Panels**	*Δημιουργεί χρωματιστά πλαίσια διαλόγου*
6.	**Data Tables Generator by Supsystic**	*Δημιουργία Πινάκων*
7.	**File Manager Advanced**	*Διαχείριση των αρχείων*
8.	**Hide Page And Post Title**	*Εύκολος τρόπος απόκρυψης και εμφάνισης σελίδων*
9.	**Iframe**	*Εισαγωγή και διαχείριση iframe*
10.	**Ninja Forms**	*Δημιουργεί έξυπνες φόρμες διαλόγου - επικοινωνίας*
11.	**PHP Compatibility Checker**	*Αφορά την PHP του συστήματος*
12.	**Popup Maker**	*Εύκολη δημιουργία PopUp παραθύρων*
13.	**Show-Hide/Collapse-Expand**	*Αφορά τη διαχείριση των σελίδων*
14.	**WPFront Scroll Top**	*Button που μεταφέρει τον χρήστη στην κορυφή της σελίδας*

Πίνακας 5: *Λίστα Πρόσθετων Εφαρμογών Wordpress*

6.5 Περιγραφή της ιστοσελίδας kidstaysafe στο Wordpress

Στη συνέχεια γίνεται μια συγκεντρωτική περιγραφή των αντικειμένων που πραγματεύεται η ιστοσελίδα *kidstaysafe*.

α/α	ΣΕΛΙΔΕΣ	ΠΕΡΙΓΡΑΦΗ
1.	**Αρχική**	Γίνεται μια γενική περιγραφή του σκοπού υλοποίησης της ιστοσελίδας *kidstaysafe*.
2.	**Ασφάλεια & Διαδίκτυο**	Η ενότητα αυτή χωρίζεται στις εξής υποενότητες: • Γονείς • Εκπαιδευτικοί • Παιδιά • Κίνδυνοι Διαδικτύου Εδώ ο επισκέπτης μπορεί να ενημερωθεί και να γνωρίσει καλύτερα θέματα όπως: • Ασφάλεια στο διαδίκτυο • Οδηγίες ασφαλούς πλοήγησης • Κίνδυνοι του διαδικτύου • Μέτρα προστασίας
3.	**Γονικός Έλεγχος**	Η ενότητα αυτή χωρίζεται στις εξής υποενότητες: • Γονείς & Εκπαιδευτικοί • Υποστήριξη Η ενότητα «Γονείς & Εκπαιδευτικοί» αφορά την ενημέρωση του επισκέπτη και κυρίως των γονέων και των εκπαιδευτικών για τον τρόπο εφαρμογής του γονικού ελέγχου και της γενικότερης εποπτείας των ψηφιακών συσκευών που χρησιμοποιούν τα παιδιά. Η υποενότητα «Υποστήριξη» περιλαμβάνει εκπαιδευτικό υλικό που αφορά τα δύο πιο γνωστά λειτουργικά συστήματα (Microsoft Windows και Android) που χρησιμοποιούν οι περισσότερες ψηφιακές συσκευές (π.χ. ηλεκτρονικοί υπολογιστές, έξυπνα τηλέφωνα, tablets) το οποίο καθοδηγεί τον επισκέπτη έτσι ώστε να μπορεί και ο ίδιος να ρυθμίσει και να εφαρμόσει τον γονικό έλεγχο στις δικές του ψηφιακές συσκευές.

5.	**Κοινωνική Δικτύωση**	Στην ενότητα αυτή γίνεται μια αναφορά στην κοινωνική δικτύωση και παρουσιάζονται τέσσερα από τα πιο διαδεδομένα μέσα κοινωνικής δικτύωσης που χρησιμοποιούν οι νέοι: • Facebook • Tik Tok • Viber • Instagram Στόχος είναι ο επισκέπτης να γνωρίσει τον τρόπο λειτουργίας των μέσων αυτών αλλά και να ενημερωθεί σχετικά με τους κινδύνους που πιθανόν να υπάρχουν από τη μη ορθή χρήση τους και τους αντίστοιχους τρόπους αποφυγής.
6.	**Νομοθεσία**	Στο σημείο αυτό γίνεται μια ενημέρωση όσον αφορά το Ηλεκτρονικό Έγκλημα και την ισχύουσα νομοθεσία, Ελληνική και Ευρωπαϊκή. Επίσης, γίνεται μια αναφορά στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR)
6.	**Παιχνίδια**	Η σελίδα αυτή συμπεριλαμβάνει εκπαιδευτικά παιχνίδια (quiz) που απευθύνονται σε γονείς, εκπαιδευτικούς και παιδιά με σκοπό τη διαδραστική μάθηση σε θέματα ασφαλούς πλοήγησης στο διαδίκτυο.
7.	**Επικοινωνία**	Στην ενότητα αυτή ο επισκέπτης έχει την δυνατότητα να επικοινωνήσει με τους διαχειριστές της ιστοσελίδας για θέματα που σχετίζονται με την ασφάλεια στο διαδίκτυο, τον γονικό έλεγχο και τους κινδύνους του διαδικτύου.

Πίνακας 6: *Συνοπτική περιγραφή ιστοσελίδας kidstaysafe*

6.5.1 Αρχική Σελίδα

Στην Αρχική Σελίδα της ιστοσελίδας *kidstaysafe* γίνεται μια εισαγωγική αναφορά για την ασφάλεια του διαδικτύου και των επικίνδυνων καταστάσεων. Επίσης, γίνεται μια παρουσίαση της τρέχουσας ιστοσελίδας αλλά και μια αναφορά στους λόγους που οδήγησαν στη δημιουργία της.

Εικόνα 92: *Σελίδα «ΑΡΧΙΚΗ»*

6.5.2 Ασφάλεια & Διαδίκτυο

Η δεύτερη ενότητα του Κεντρικού Μενού χωρίζεται στις υποενότητες Γονείς, Εκπαιδευτικοί, Παιδιά και Κίνδυνοι Διαδικτύου. Ο επισκέπτης μπορεί να ενημερωθεί ανά κατηγορία για θέματα ασφάλειας του διαδικτύου και για θέματα που αφορούν τους κινδύνους αλλά και τους τρόπους αντιμετώπισης τους.

Εικόνα 93: *Σελίδα και υποσελίδες «ΑΣΦΑΛΕΙΑ & ΔΙΑΔΙΚΤΥΟ»*

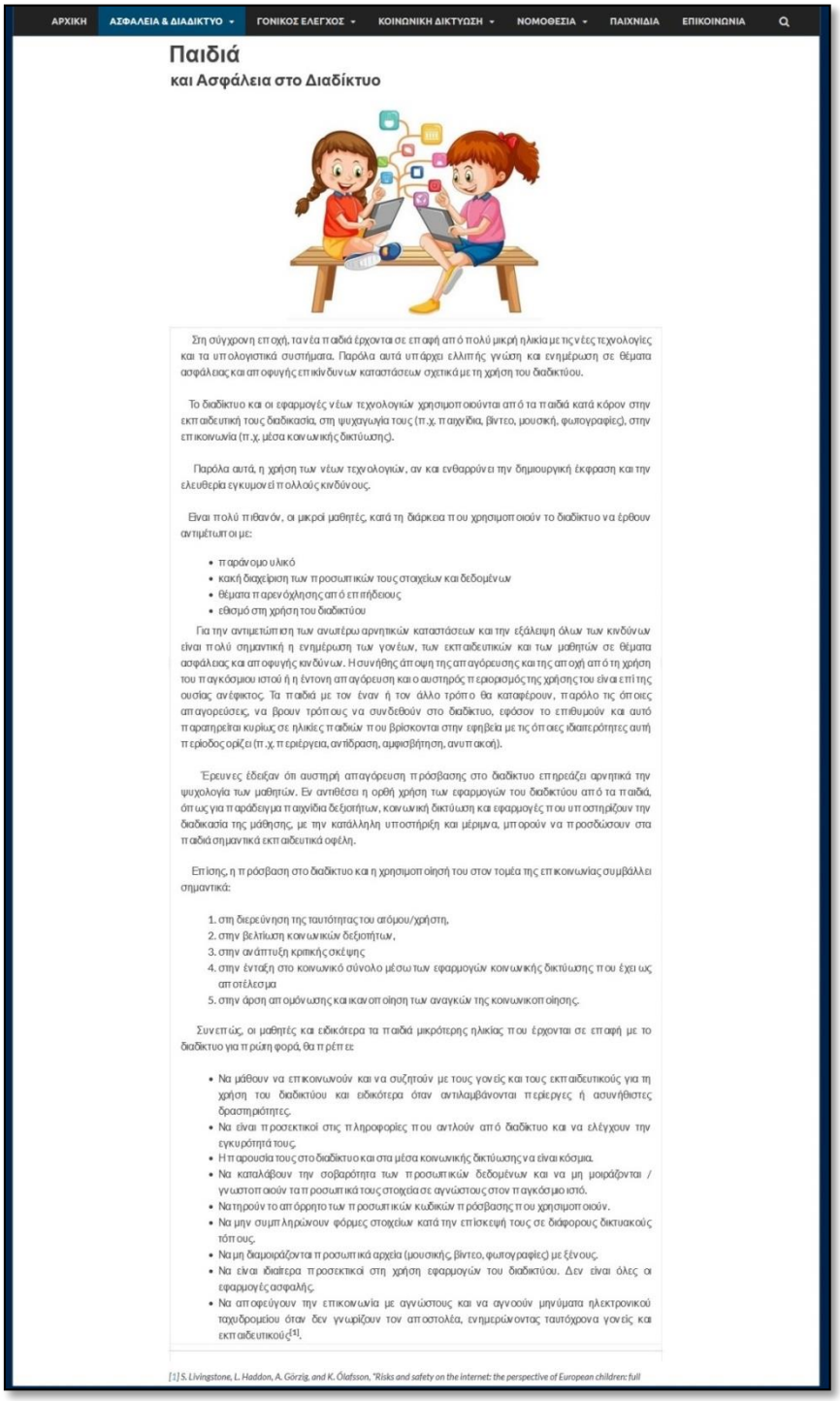
6.5.2.1 Γονείς

Εικόνα 94: *Υποσελίδα «Γονείς»*

6.5.2.2 Εκπαιδευτικοί

Εικόνα 95: *Υποσελίδα «Εκπαιδευτικοί»*

6.5.2.3 Παιδιά



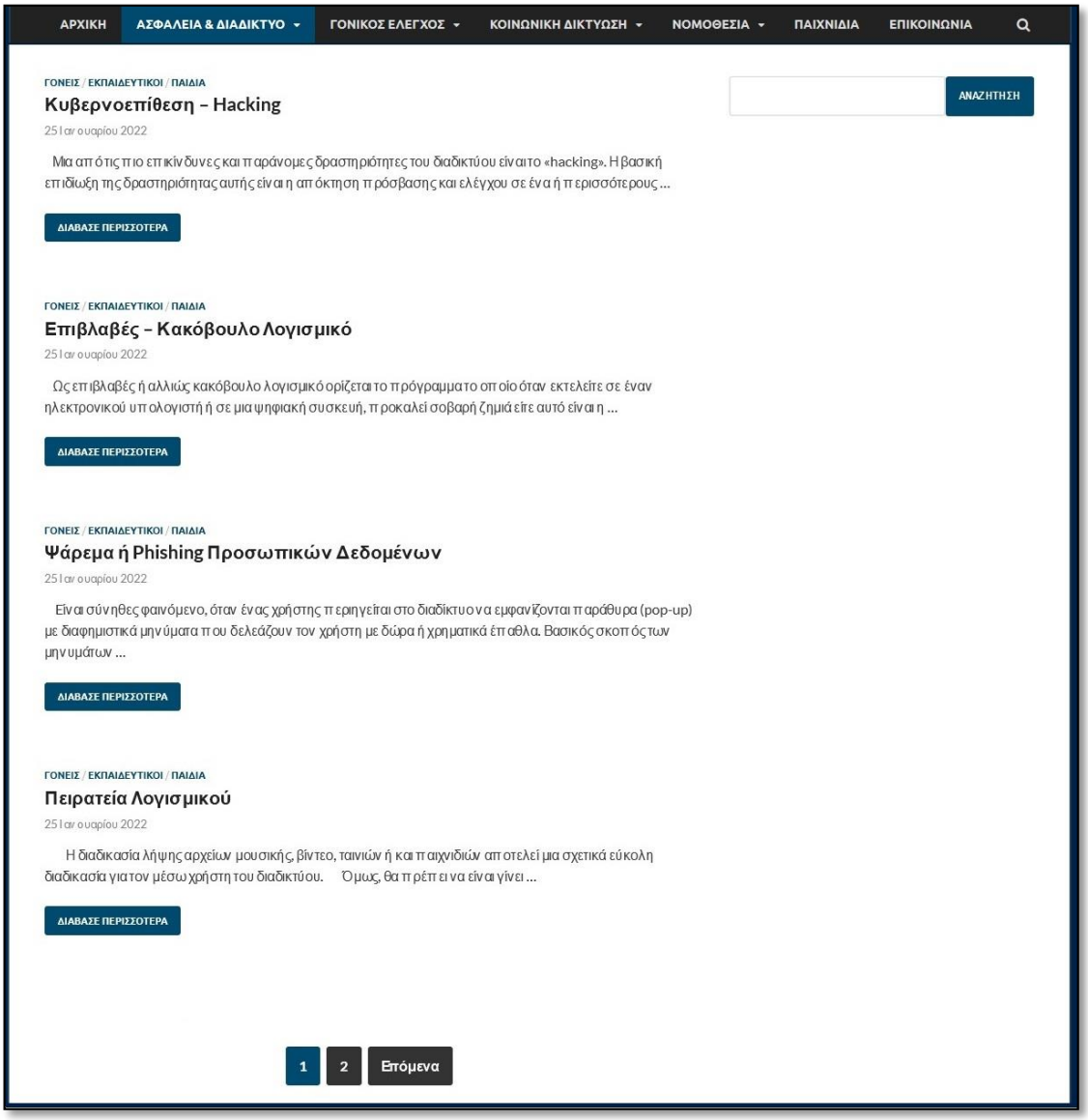
Εικόνα 96: *Υποσελίδα «Παιδιά»*

6.5.2.4 Κίνδυνοι Διαδικτύου

Η υποενότητα Κίνδυνοι Διαδικτύου χωρίζεται σε δύο ακόμα υποενότητες όπου παρουσιάζονται όλοι οι πιθανοί *κίνδυνοι* που μπορεί να βρεθεί αντιμέτωπο ένα παιδί κατά την πλοήγησή του στο παγκόσμιο ιστό και τα *μέτρα προστασίας* που πρέπει να ληφθούν για την αντιμετώπιση έναντι των κινδύνων αυτών.

Κίνδυνοι

Η παρουσίαση των Κινδύνων γίνεται υπό τη μορφή Άρθρων. Κάθε άρθρο αποτελεί και μια ξεχωριστή σελίδα.



Εικόνα 97: *Υποσελίδα «Κίνδυνοι»*

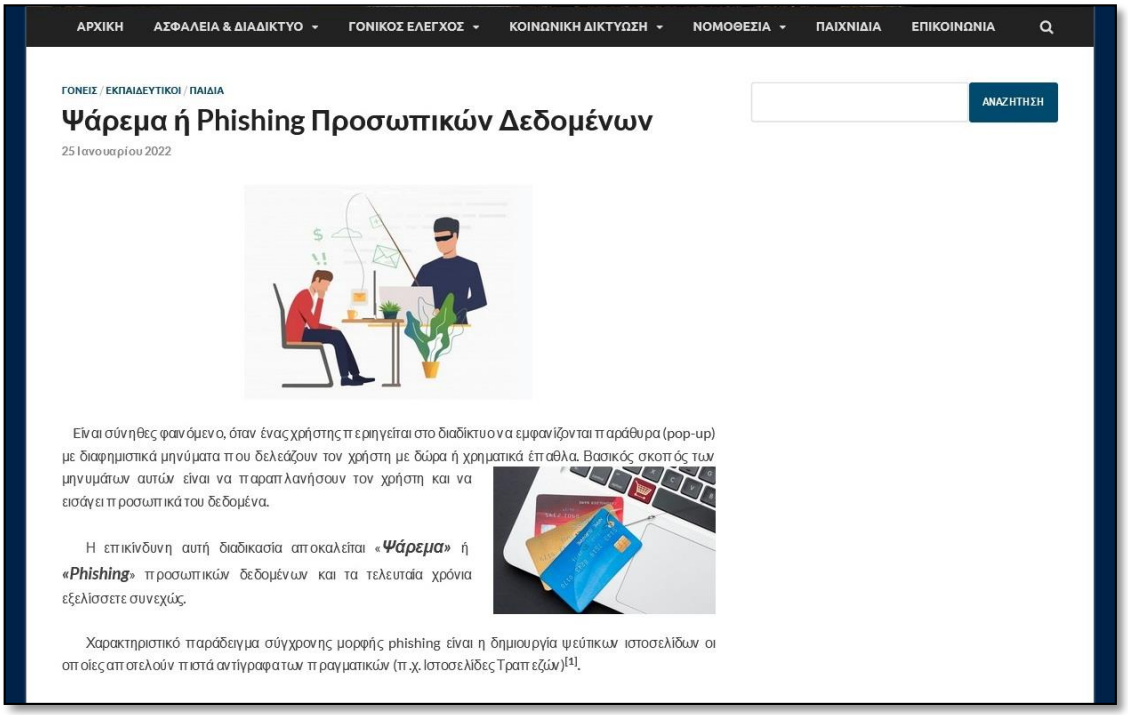
6.5.2.4.1 Κυβερνοεπίθεση – Hacking

Εικόνα 98: *Άρθρο «Κυβερνοεπίθεση - Hacking»*

6.5.2.4.2 Επιβλαβές - Κακόβουλο Λογισμικό

Εικόνα 99: *Άρθρο «Επιβλαβές – Κακόβουλο Λογισμικό»*

6.5.2.4.3 Ψάρεμα ή Phishing Προσωπικών Δεδομένων



Εικόνα 100: *Άρθρο «Ψάρεμα ή Phising Προσωπικών Δεδομένων»*

6.5.2.4.4 Πειρατεία Λογισμικού

Εικόνα 101: *Άρθρο «Πειρατεία Λογισμικού»*

6.5.2.4.5 Εξαπάτηση

Εικόνα 102: *Άρθρο «Εξαπάτηση»*

6.5.2.4.6 Ανεπιθύμητη Ηλεκτρονική Αλληλογραφία (Spam)

Εικόνα 103: *Άρθρο «Ανεπιθύμητη Ηλεκτρονική Αλληλογραφία - Spam»*

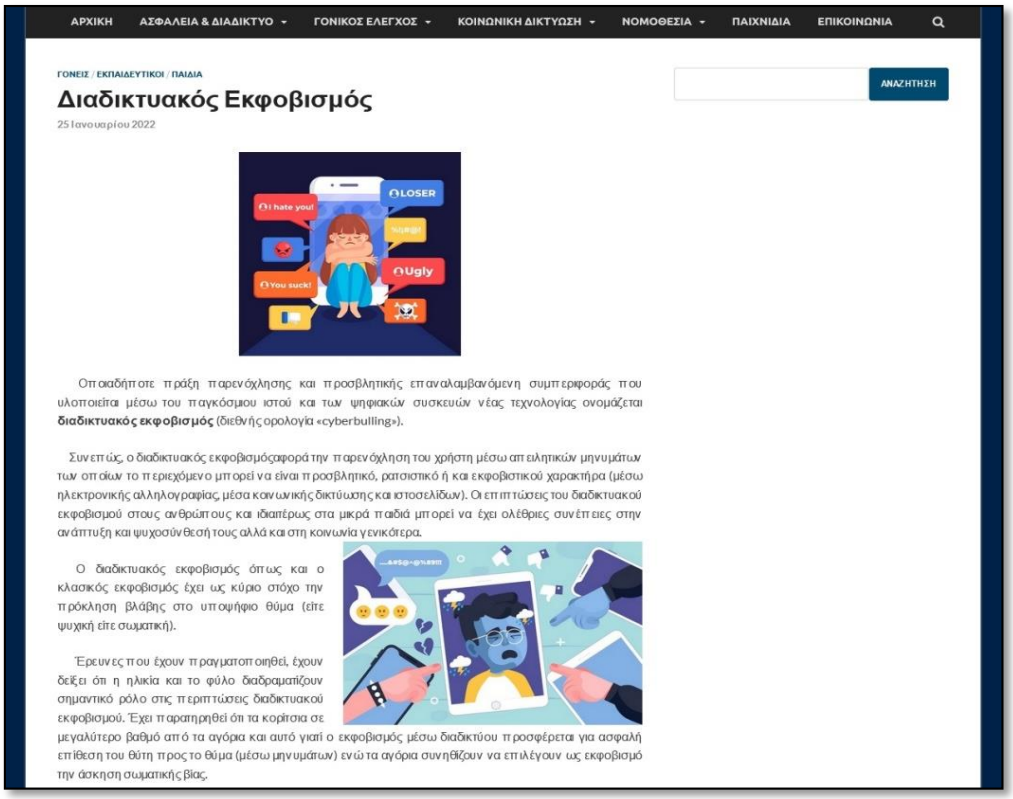
6.5.2.4.7 Παιδική Πορνογραφία μέσω διαδικτύου

Εικόνα 104: *Άρθρο «Παιδική Πορνογραφία μέσω διαδικτύου»*

6.5.2.4.8 Αποπλάνηση μικρών παιδιών – Grooming

Εικόνα 105: *Άρθρο «Αποπλάνηση μικρών παιδιών - Grooming»*

6.5.2.4.9 Διαδικτυακός Εκφοβισμός

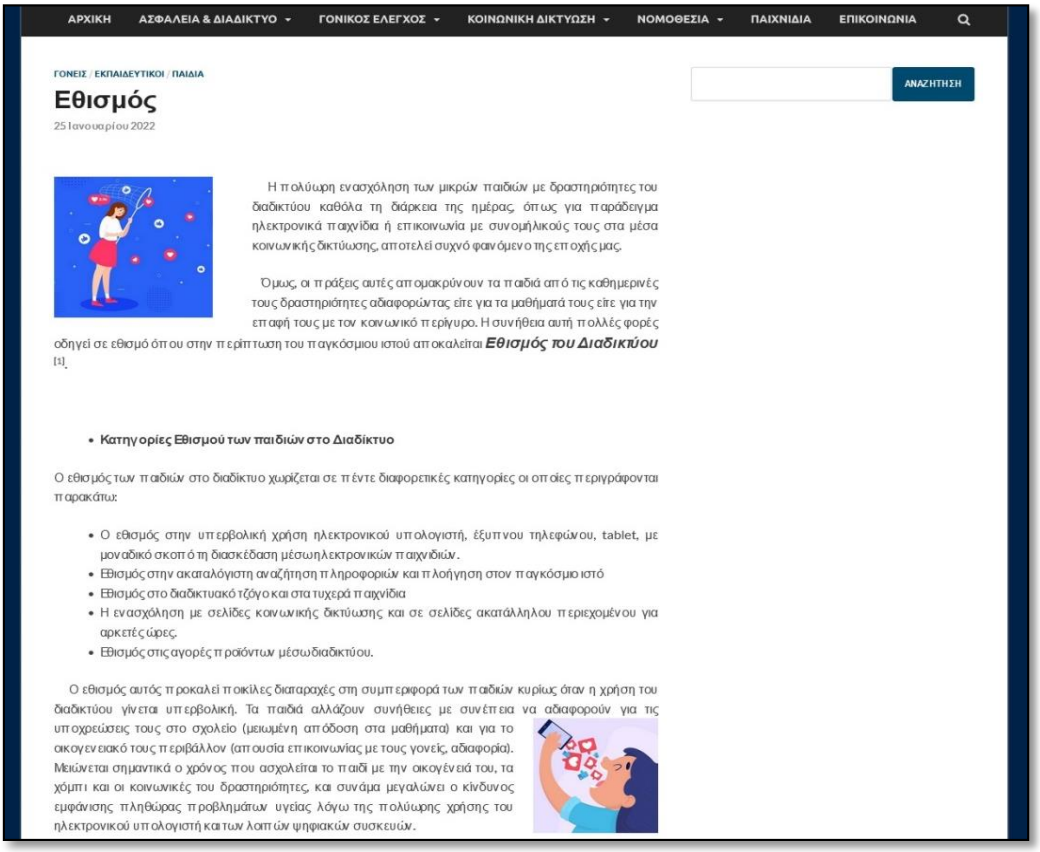


Εικόνα 106: *Άρθρο «Διαδικτυακός Εκφοβισμός»*

6.5.2.4.10 Ψεύτικη Ταυτότητα

Εικόνα 107: *Άρθρο «Ψεύτικη Ταυτότητα»*

6.5.2.4.11 Εθισμός



Εικόνα 108: *Άρθρο «Εθισμός»*

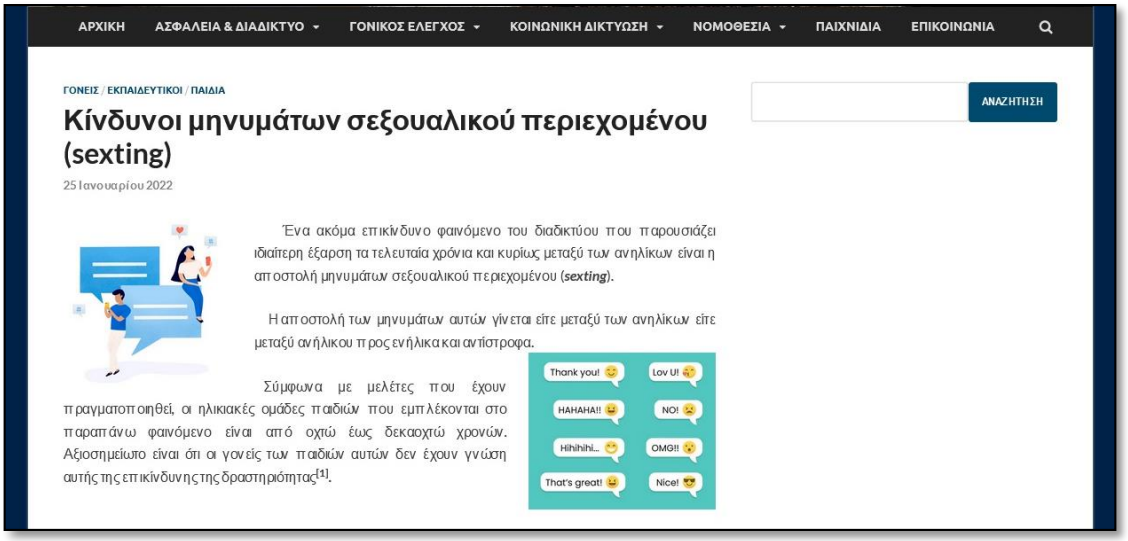
6.5.2.4.12 Greeklish

Εικόνα 109: *Άρθρο «Greeklish»*

6.5.2.4.13 Trafficking

Εικόνα 110: *Άρθρο «Trafficking»*

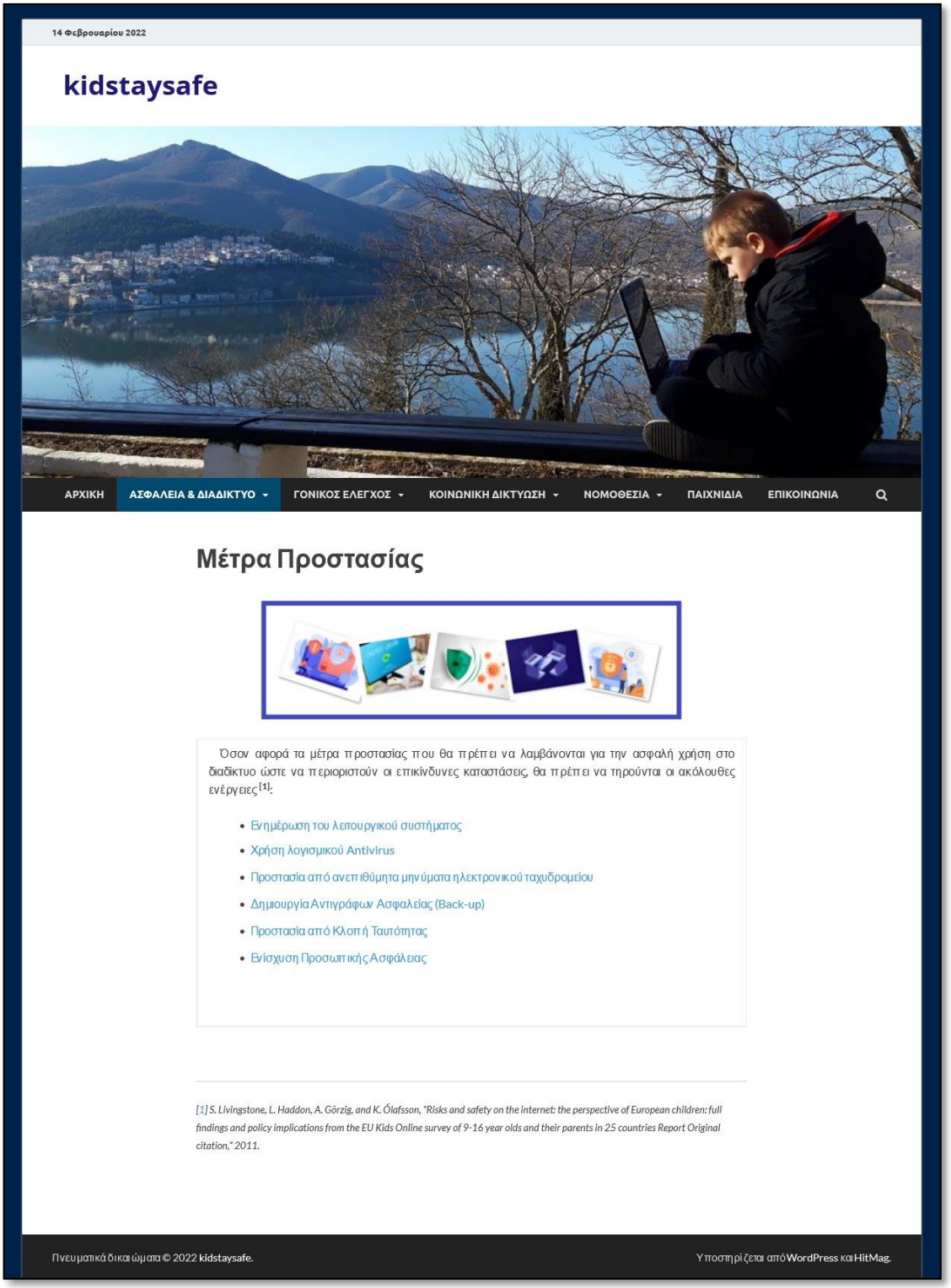
6.5.2.4.14 Κίνδυνοι μηνυμάτων σεξουαλικού περιεχομένου (sexting)



Εικόνα 111: *Άρθρο «Κίνδυνοι μηνυμάτων σεξουαλικού περιεχομένου»*

6.5.2.5 Μέτρα Προστασίας

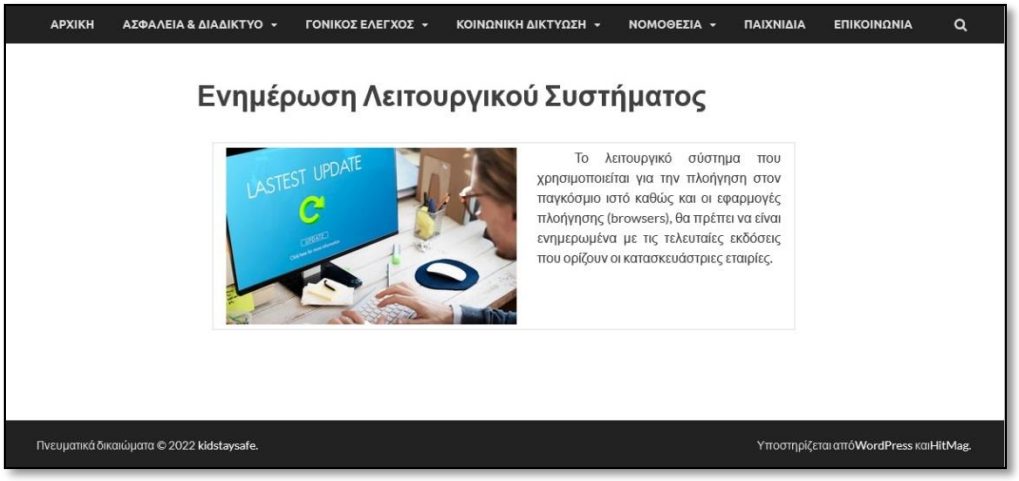
Η υποενότητα των Κινδύνων Διαδικτύου «Μέτρα Προστασίας» περιλαμβάνει έξι βασικές ενέργειες στις οποίες θα πρέπει να τηρεί ο εκάστοτε χρήστης για μια ασφαλή πλοήγηση στον παγκόσμιο ιστό.



Εικόνα 112: *Υποσελίδα «Μέτρα Προστασίας»*

Για κάθε μια ενέργεια υπάρχει και μια συνοπτική περιγραφή η οποία εμφανίζεται σε ξεχωριστή σελίδα μετά από επιλογή του χρήστη.

Ενέργεια 1η: *Ενημέρωση Λειτουργικού Συστήματος*



Εικόνα 113: *Υποσελίδα «Μέτρα Προστασίας» – Ενημέρωση Λ.Σ.*

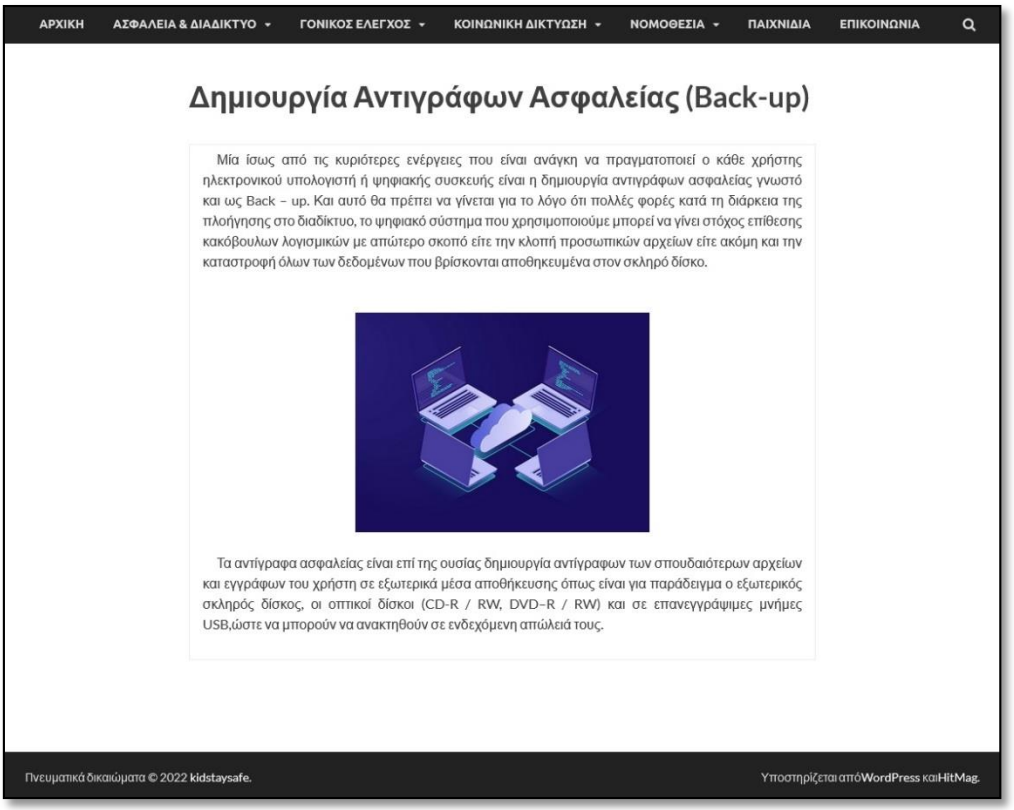
Ενέργεια 2η: *Χρήση λογισμικού Antivirus*

Εικόνα 114: *Υποσελίδα «Μέτρα Προστασίας» - Antivirus*

Ενέργεια 3η : *Προστασία από ανεπιθύμητα μηνύματα ηλ. ταχυδρομείου*

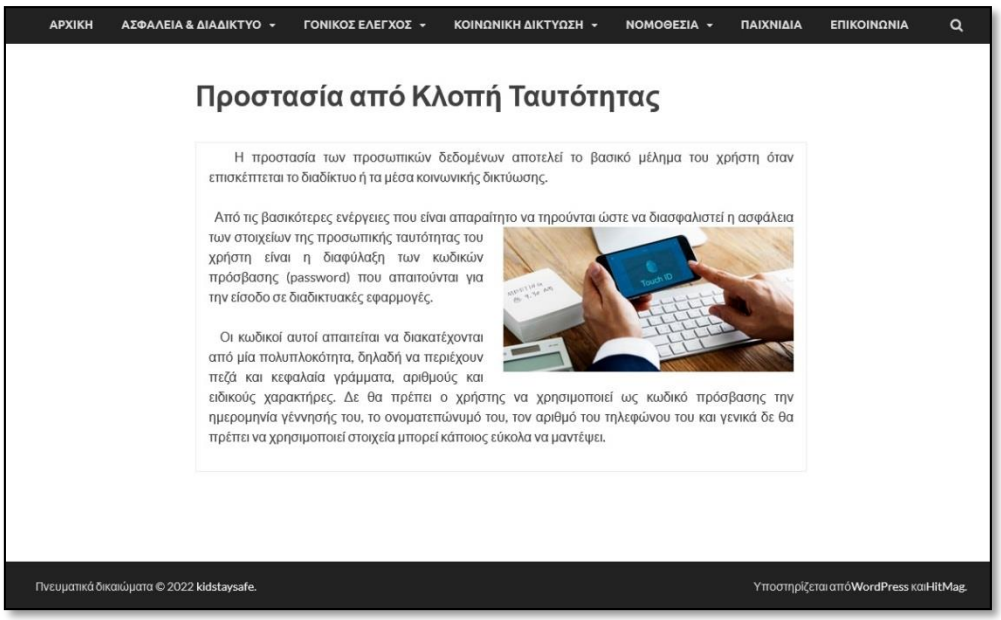
Εικόνα 115: *Υποσελίδα «Μέτρα Προστασίας» - AntiSpam*

Ενέργεια 4η : *Δημιουργία Αντιγράφων Ασφαλείας (Back-Up)*



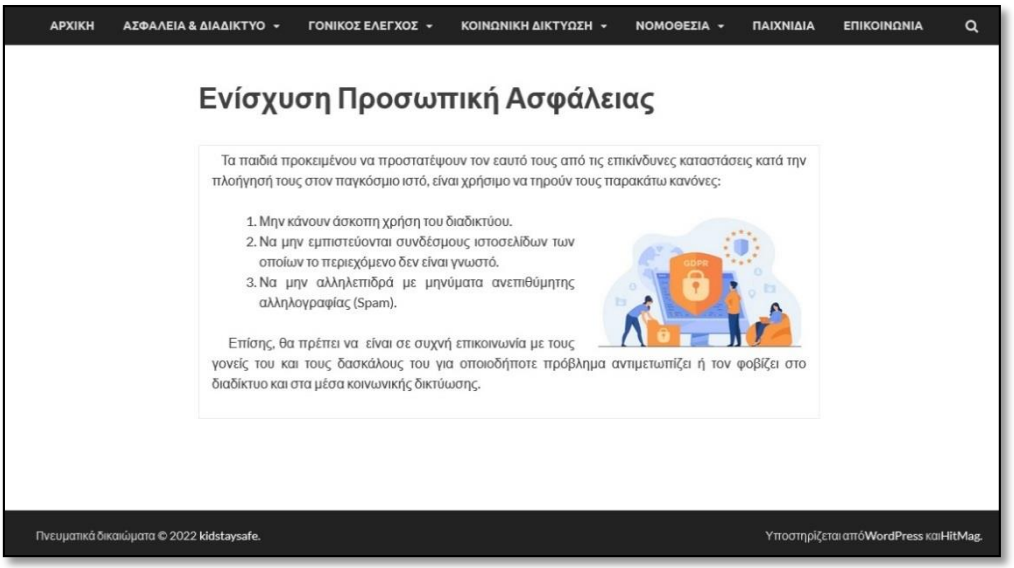
Εικόνα 116: *Υποσελίδα «Μέτρα Προστασίας» - BackUp*

Ενέργεια 5η : *Προστασία από κλοπή Ταυτότητας*



Εικόνα 117: *Υποσελίδα «Μέτρα Προστασίας» – Προστασία από Κλοπή Ταυτότητας*

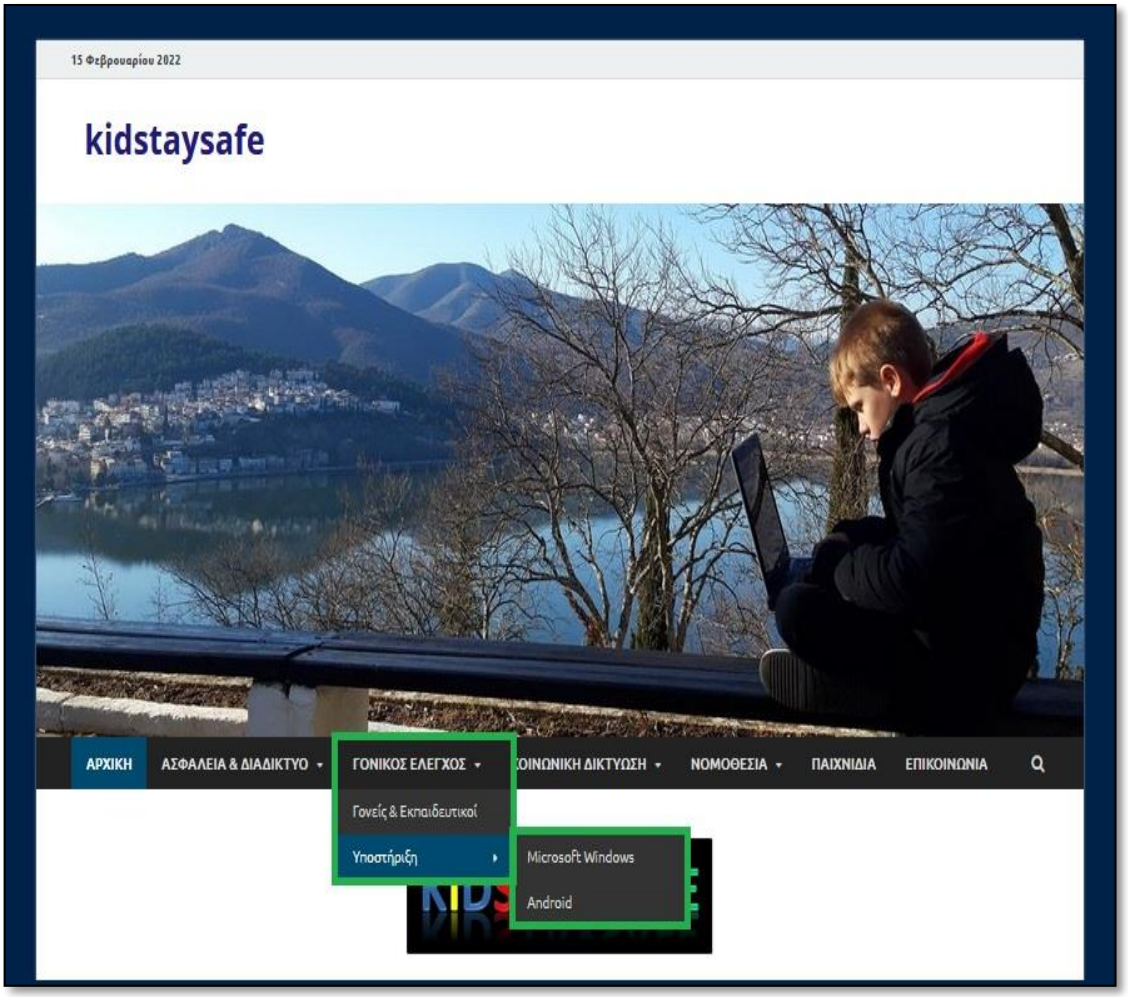
Ενέργεια 6η : *Ενίσχυση Προσωπικής Ασφάλειας*



Εικόνα 118: *Υποσελίδα «Μέτρα Προστασίας» – Ενίσχυση Προσωπικής Ασφάλειας*

6.5.3 Γονικός Έλεγχος

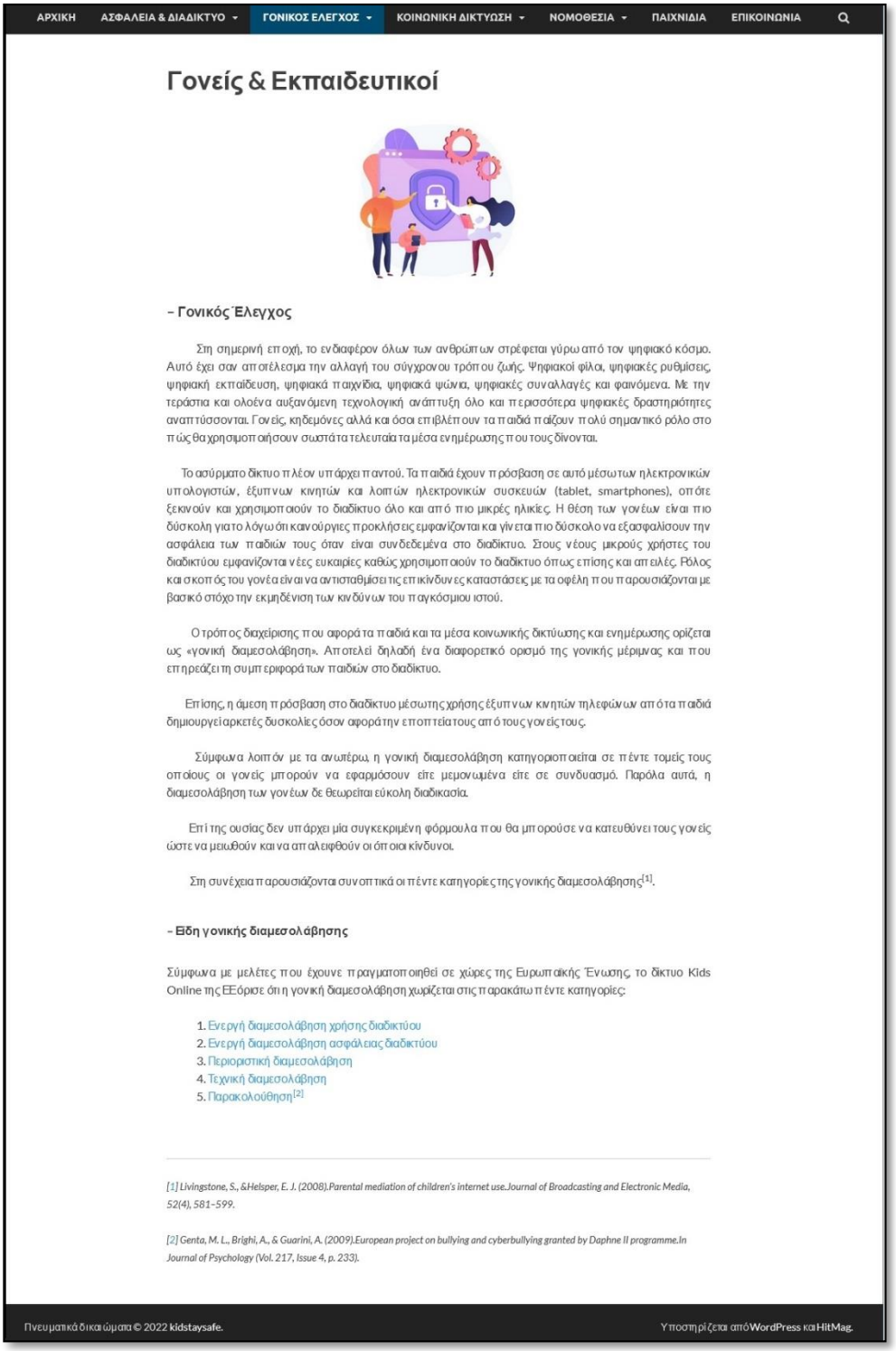
Η τρίτη ενότητα του Κεντρικού Μενού χωρίζεται στις υποενότητες «Γονείς & Εκπαιδευτικοί» και «Υποστήριξη».



Εικόνα 119: *Σελίδα και Υποσελίδες «ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ»*

6.5.3.1 Γονείς & Εκπαιδευτικοί

Η υποενότητα αφορά την ενημέρωση του επισκέπτη για την εφαρμογή του γονικού ελέγχου και της επιτήρησης όλων των ψηφιακών συσκευών που έχουν πρόσβαση στο διαδίκτυο και χρησιμοποιούν τα παιδιά.



Εικόνα 120: *Υποσελίδα «Γονείς & Εκπαιδευτικοί»*

6.5.3.2 Υποστήριξη

Η υποενότητα της υποστήριξης περιλαμβάνει οδηγίες για την εφαρμογή του Γονικού στα δύο δημοφιλέστερα λειτουργικά συστήματα (Microsoft windows και android) που χρησιμοποιούν για τη λειτουργία τους οι περισσότερες ψηφιακές συσκευές.

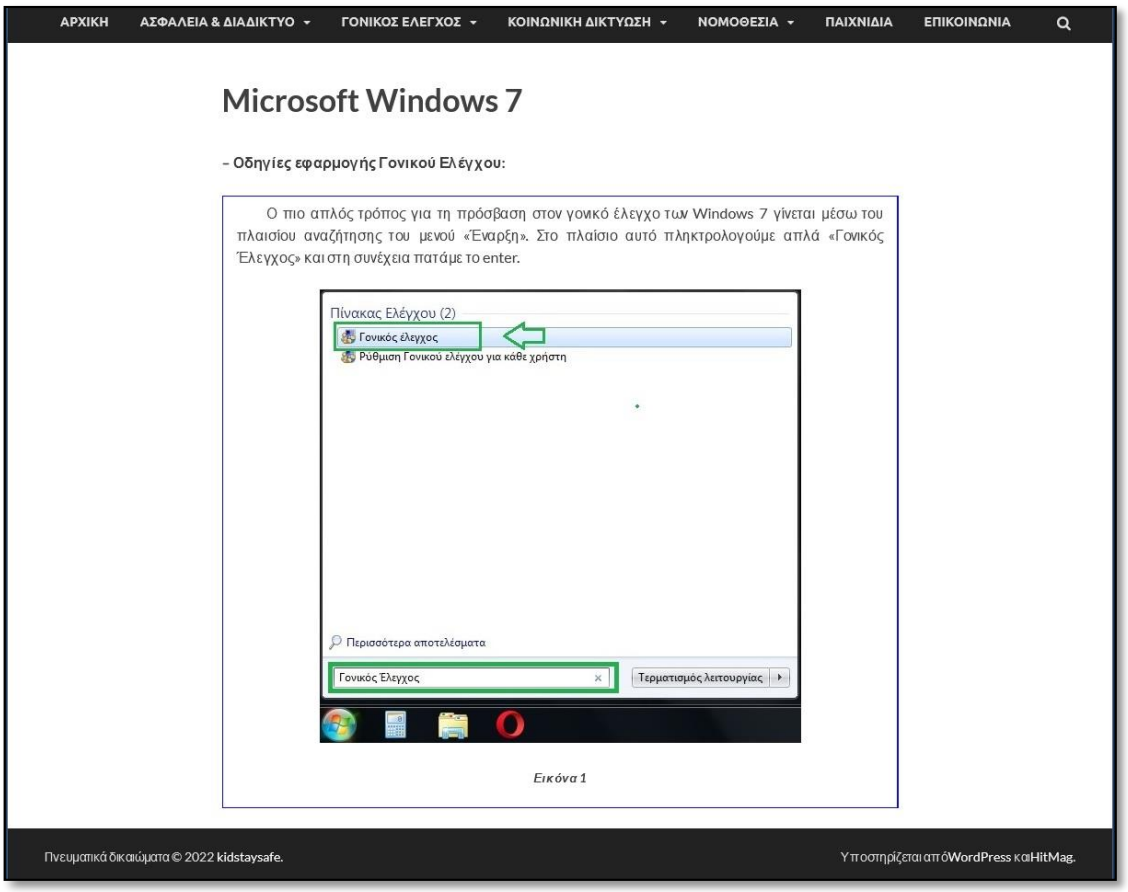
6.5.3.2.1 Microsoft Windows

Εικόνα 121: *Υποσελίδα «Microsoft Windows» – Windows 7*

Η υποενότητα των Microsoft Windows αφορά την εφαρμογή του γονικού ελέγχου στις τρεις πιο διαδεδομένες εκδόσεις: Windows 7 , Windows 8 , Windows 10.

Για κάθε μια από την προαναφερόμενες κατηγορίες εμφανίζεται μια σελίδα όπου γίνεται αναλυτική περιγραφή των ρυθμίσεων εφαρμογής γονικού ελέγχου όπως παρουσιάστηκαν στο Κεφάλαιο 4:

1. Microsoft Windows 7

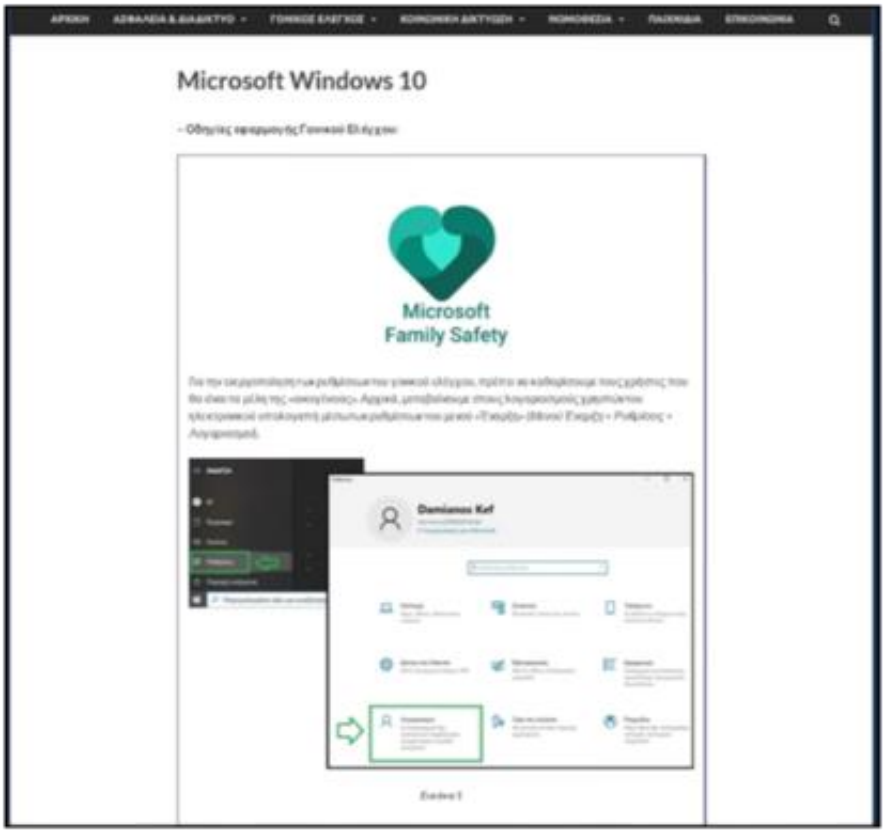


Εικόνα 122: *Υποσελίδα «Microsoft Windows» – Windows 7*

2. Microsoft Windows 8

Εικόνα 123: *Υποσελίδα «Microsoft Windows» – Windows 8*

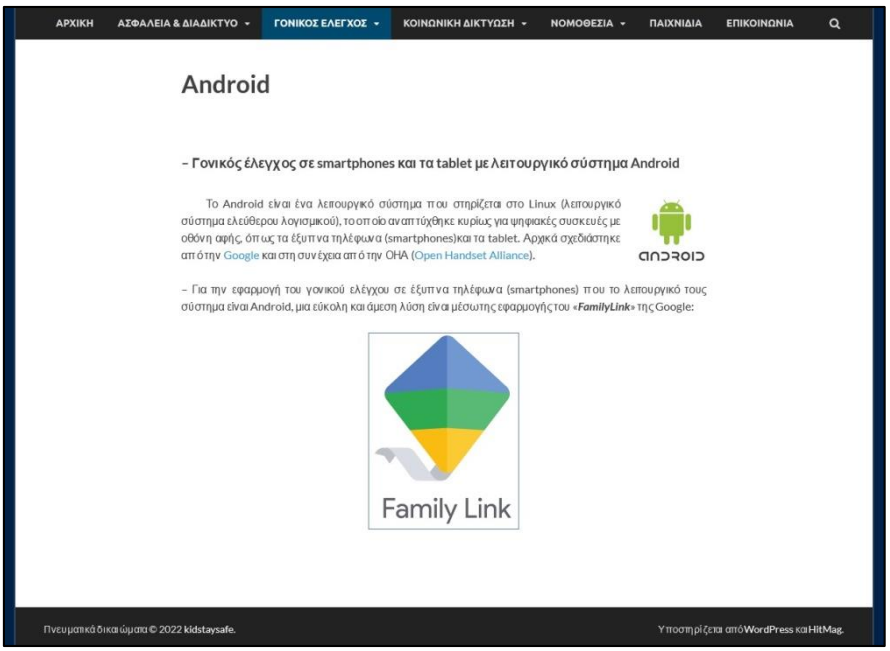
3. Microsoft Windows 10



Εικόνα 124: *Υποσελίδα «Microsoft Windows» – Windows 10*

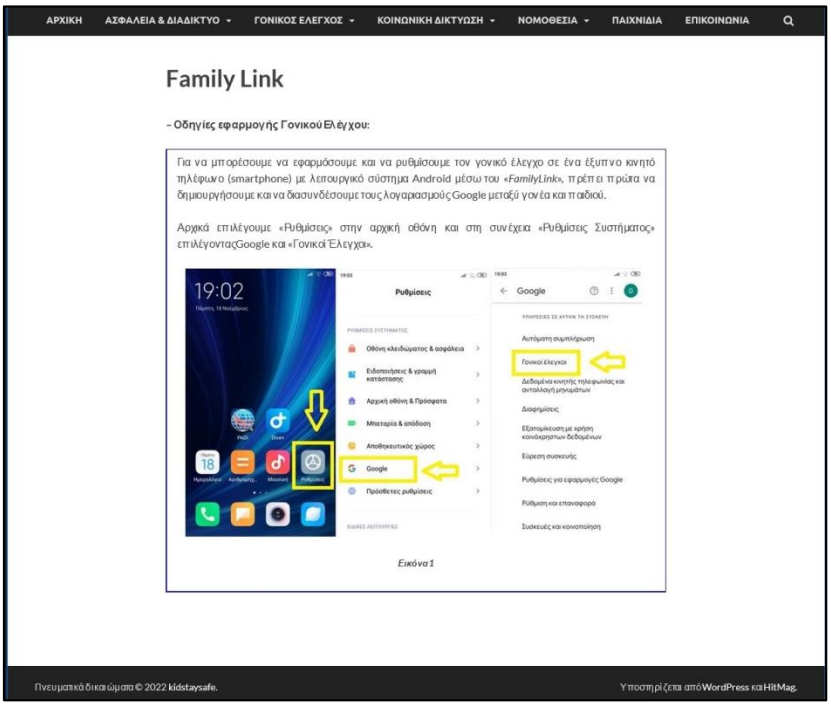
6.5.3.2.2 Android

Στην υποενότητα του λειτουργικού συστήματος Android εμφανίζεται μια σελίδα όπου γίνεται αναλυτική περιγραφή των ρυθμίσεων εφαρμογής γονικού ελέγχου μέσω του «Family Link» της google όπως παρουσιάστηκε στο Κεφάλαιο 4.



Εικόνα 125: *Υποσελίδα «Android»*

Family Link

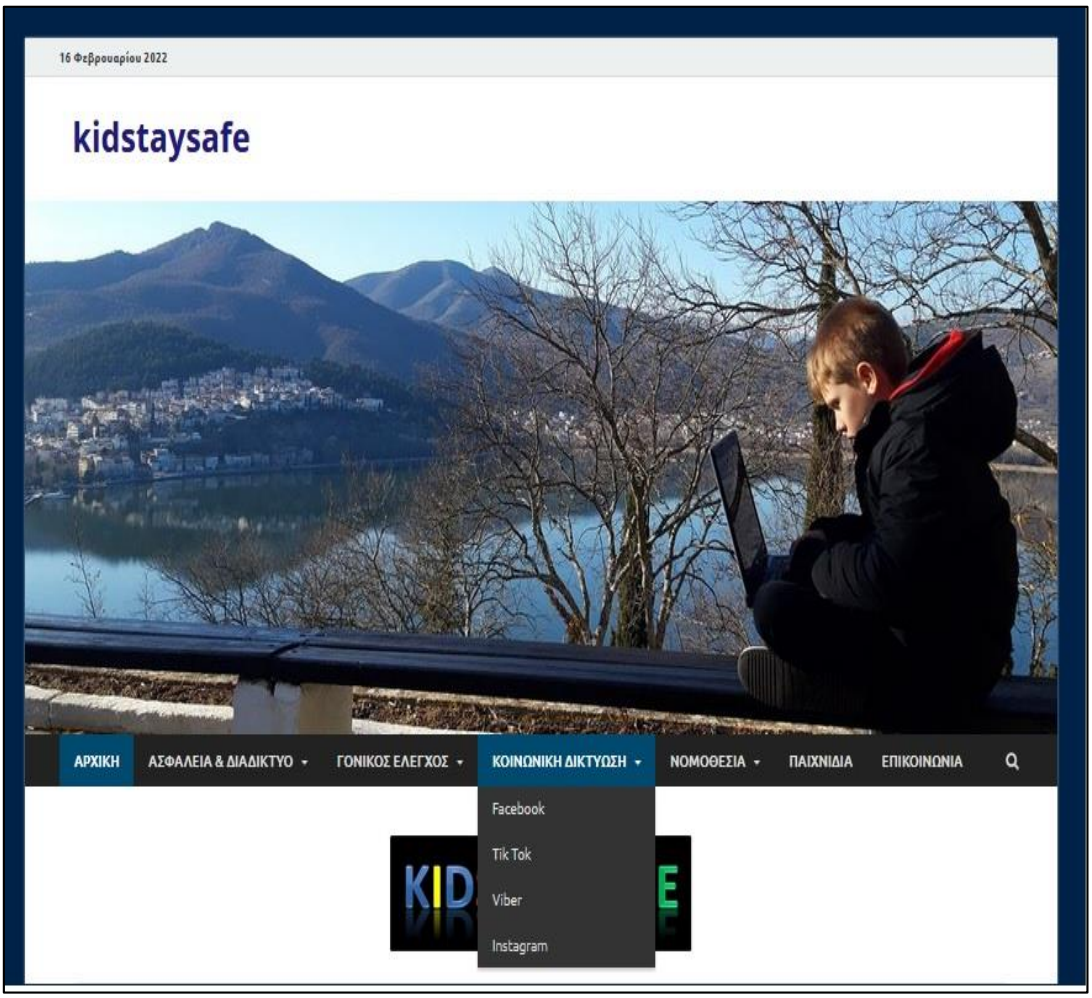


Εικόνα 126: *Υποσελίδα «Android» – Family Link*

6.5.4 Κοινωνική Δικτύωση

Η τέταρτη ενότητα του Κεντρικού Μενού αφορά την Κοινωνική Δικτύωση όπου παρουσιάζονται τα τέσσερα δημοφιλέστερα μέσα κοινωνικής δικτύωσης που χρησιμοποιούν ιδιαίτερα οι νέοι.

Σκοπός είναι η γνωριμία με τον τρόπο λειτουργίας των μέσων καθώς και η ενημέρωση για τους κινδύνους που υπάρχουν αλλά και τους τρόπους αντιμετώπισής τους.



Εικόνα 127: *Σελίδα και Υποσελίδες «ΚΟΙΝΩΝΙΚΗ ΔΙΚΤΥΩΣΗ»*

Στη συνέχεια παρουσιάζονται τα τέσσερα πιο διαδεδομένα μέσα κοινωνικής δικτύωσης που χρησιμοποιούν ιδιαίτερα οι νέοι.

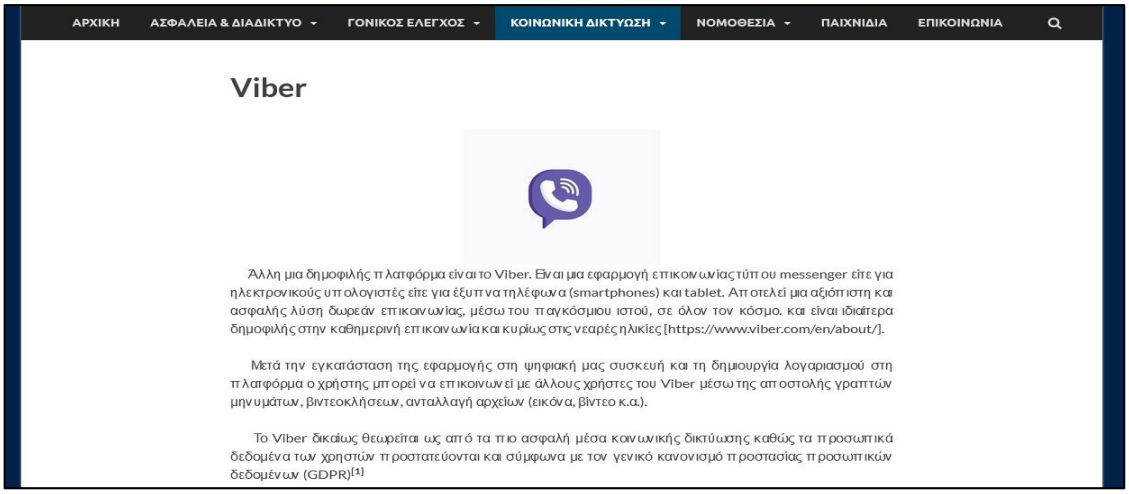
6.5.4.1 Facebook

Εικόνα 128: *Υποσελίδα «Facebook»*

6.5.4.2 Tik Tok

Εικόνα 129: *Υποσελίδα «Tik Tok»*

6.5.4.3 Viber



Εικόνα 130: *Υποσελίδα «Viber»*

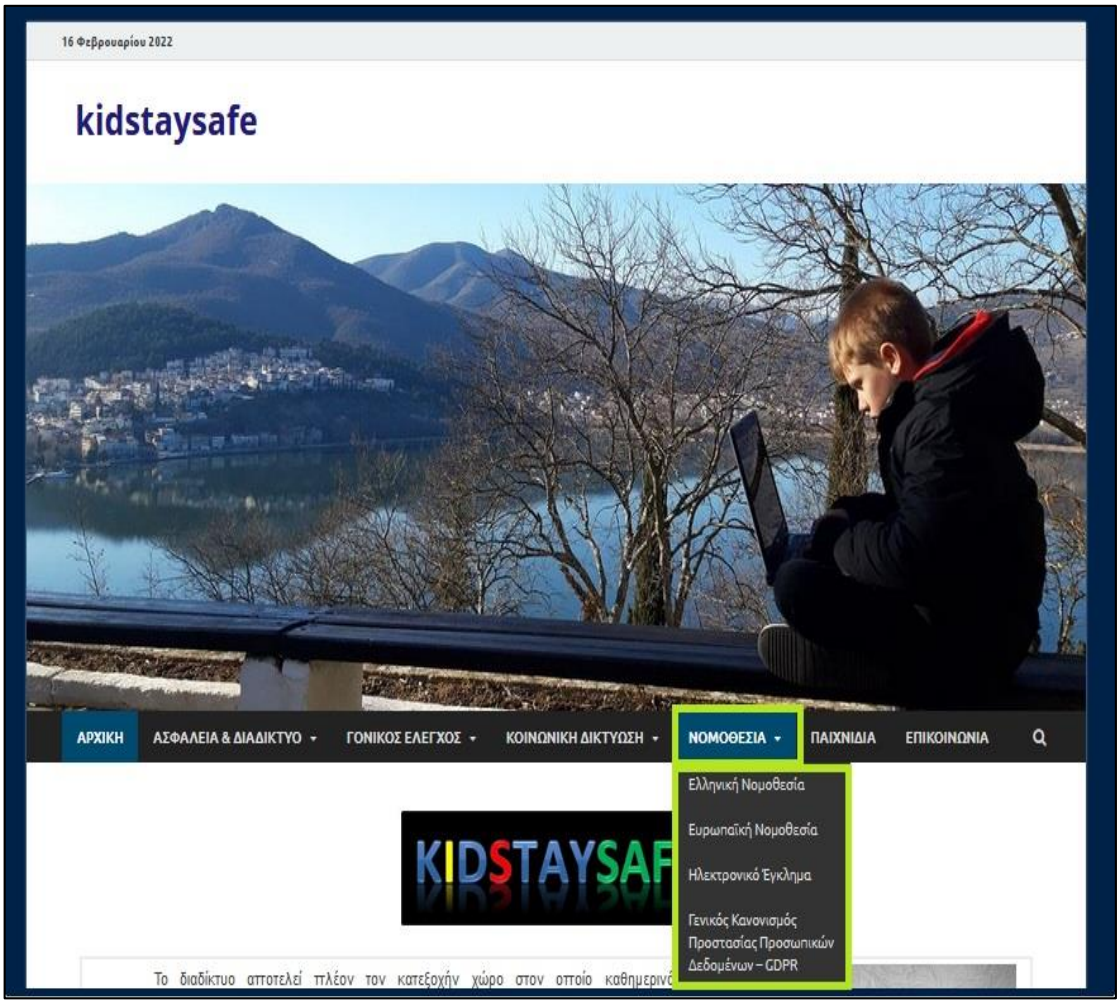
6.5.4.4 Instagram

Εικόνα 131: *Υποσελίδα «Instagram»*

6.5.5 Νομοθεσία

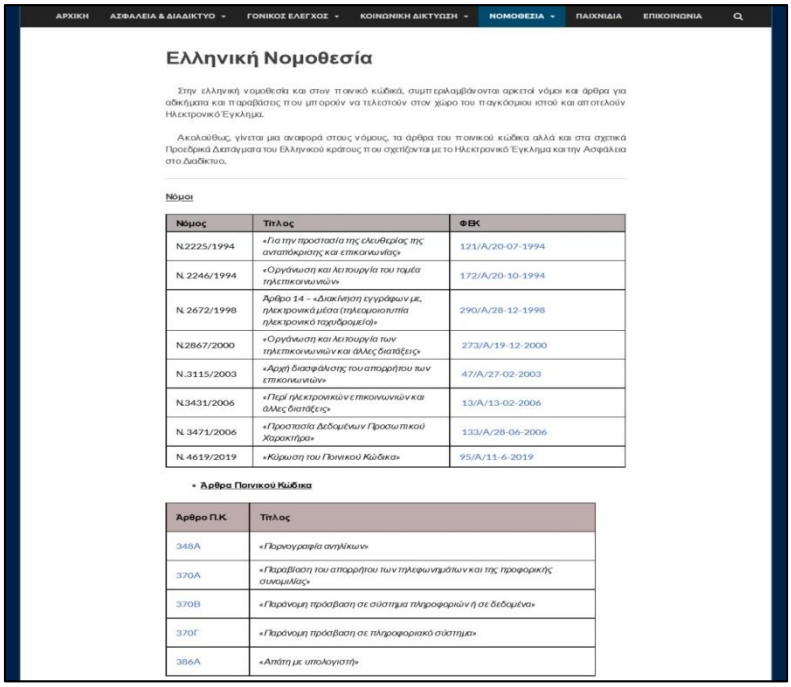
Στο σημείο αυτό γίνεται μια ενημέρωση για την Ελληνική αλλά και την Ευρωπαϊκή Νομοθεσία, όσον αφορά την ασφαλή πλοήγηση στο διαδίκτυο και το ηλεκτρονικό έγκλημα.

Επίσης, γίνεται μια παρουσίαση του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR).



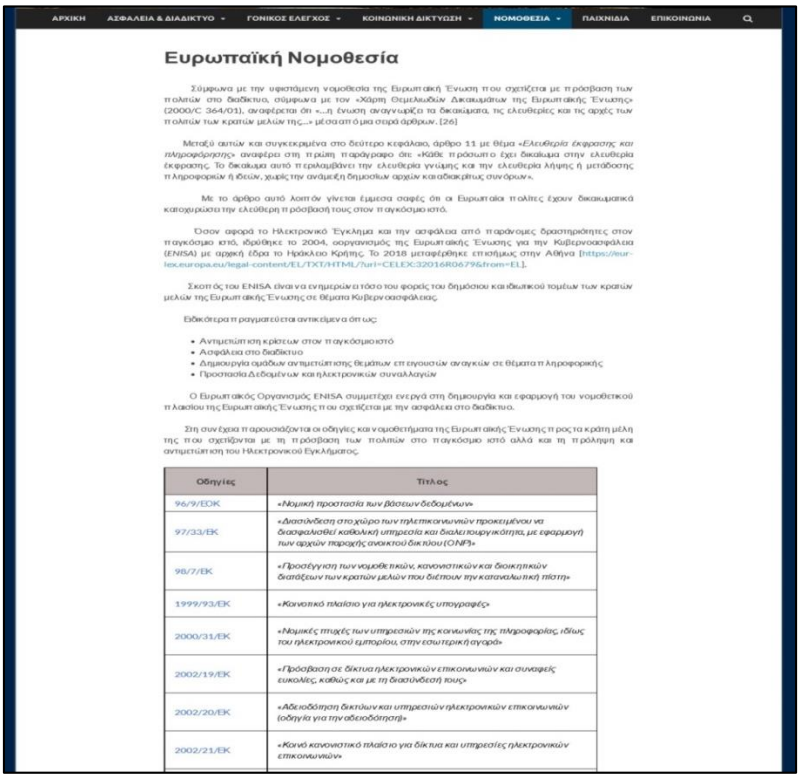
Εικόνα 132: *Σελίδα και Υποσελίδες «ΝΟΜΟΘΕΣΙΑ»*

6.5.5.1 Ελληνική Νομοθεσία



Εικόνα 133: *Υποσελίδα «Ελληνική Νομοθεσία»*

6.5.5.2 Ευρωπαϊκή Νομοθεσία



Εικόνα 134: *Υποσελίδα «Ευρωπαϊκή Νομοθεσία»*

6.5.5.3 Ηλεκτρονικό Έγκλημα

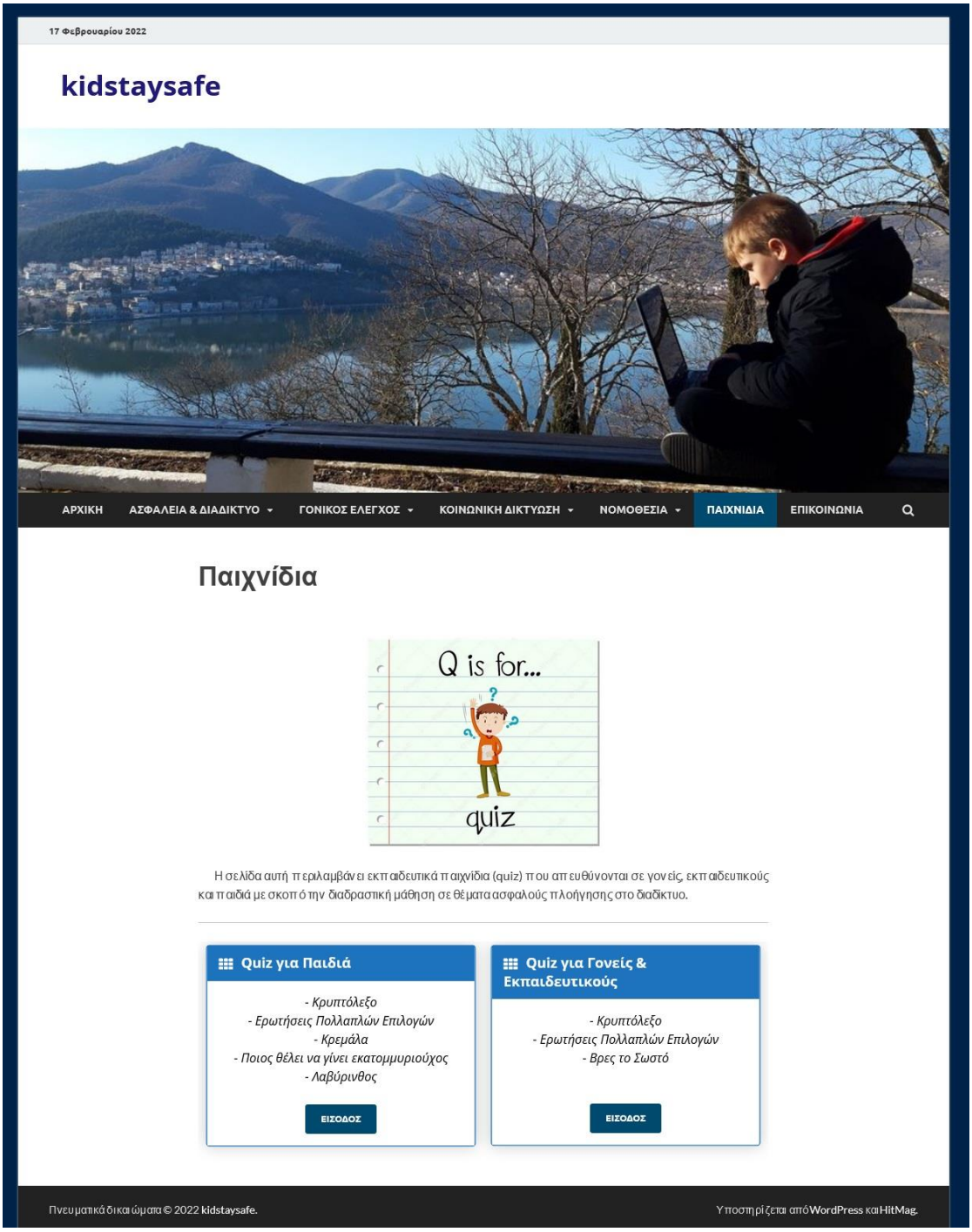
Εικόνα 135: *Υποσελίδα «Ηλεκτρονικό Έγκλημα»*

6.5.5.4 Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

Εικόνα 136: *Υποσελίδα «Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων»*

6.5.6 Παιχνίδια

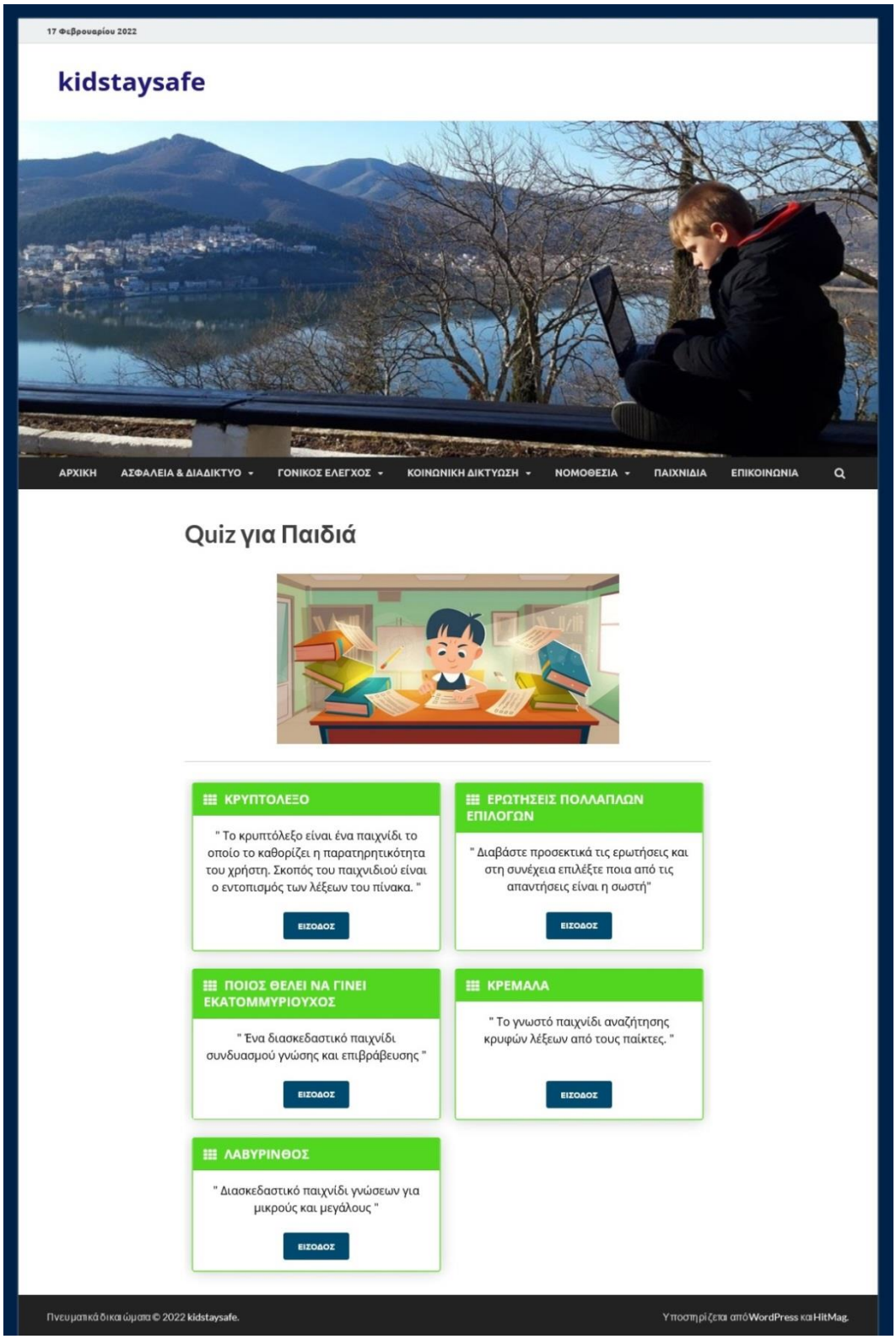
Η σελίδα αυτή περιλαμβάνει παιχνίδια (quiz) εκπαιδευτικού χαρακτήρα (*κρυπτόλεξο, ερωτήσεις πολλαπλών επιλογών, βρες το σωστό, λαβύρινθος, κρεμάλα ποιος θέλει να γίνει εκατομμυριούχος*) και απευθύνεται σε παιδιά, γονείς και εκπαιδευτικούς, με στόχο τη διαδραστική μάθηση σε θέματα ασφάλειας και αποφυγής των κινδύνων του διαδικτύου. Τα παιχνίδια αυτά δημιουργήθηκαν εύκολα και γρήγορα με τις δωρεάν εκπαιδευτικές πλατφόρμες: *e-me, Wordwall* και *LearningApps.*



Εικόνα 137: *Σελίδα «ΠΑΙΧΝΙΔΙΑ»*

6.5.6.1 Quiz για Παιδιά

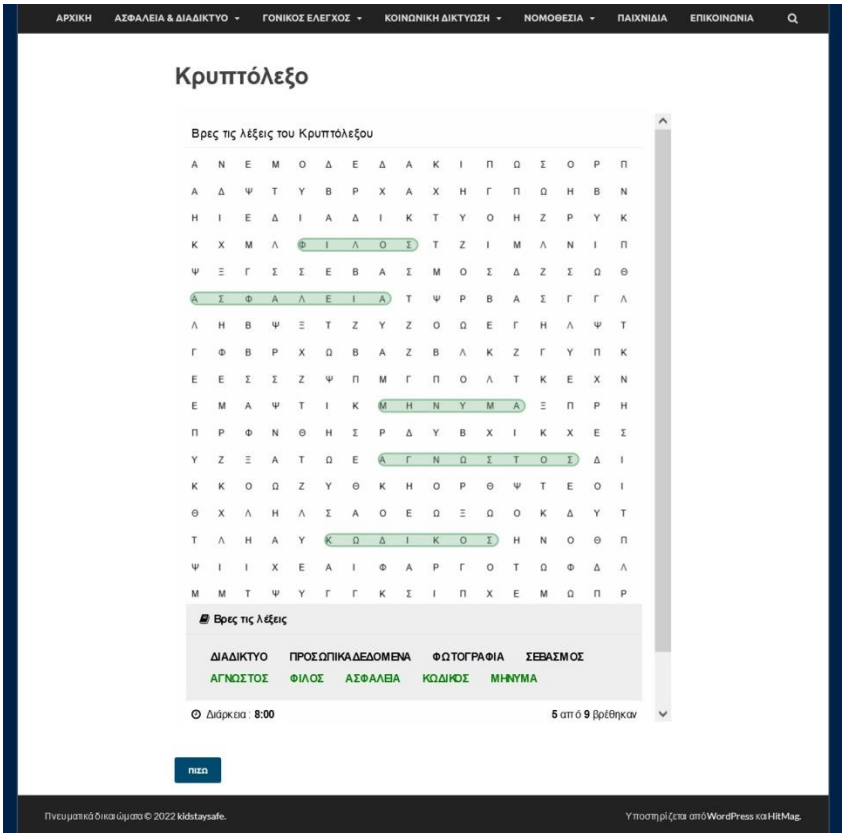
Με την επιλογή του «Quiz για Παιδιά» ανοίγει μια νέα σελίδα όπου εμφανίζονται οι κατηγορίες των παιχνιδιών.



Εικόνα 138: *Σελίδα «ΠΑΙΧΝΙΔΙΑ» - Quiz για Παιδιά*

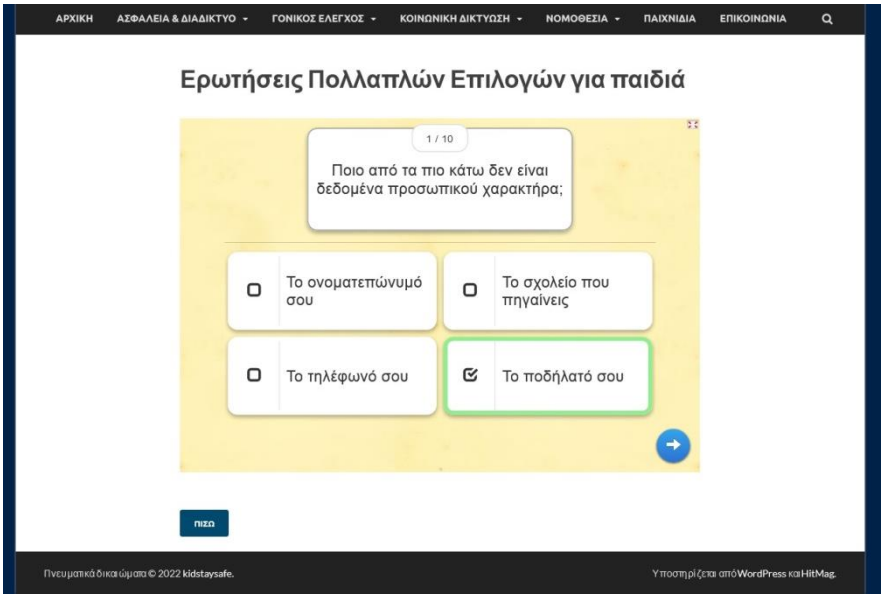
Ο χρήστης μπορεί να επιλέξει όποια κατηγορία επιθυμεί και άμεσα να έχει πρόσβαση στο αντίστοιχο quiz.

1η Κατηγορία: *«Κρυπτόλεξο»*



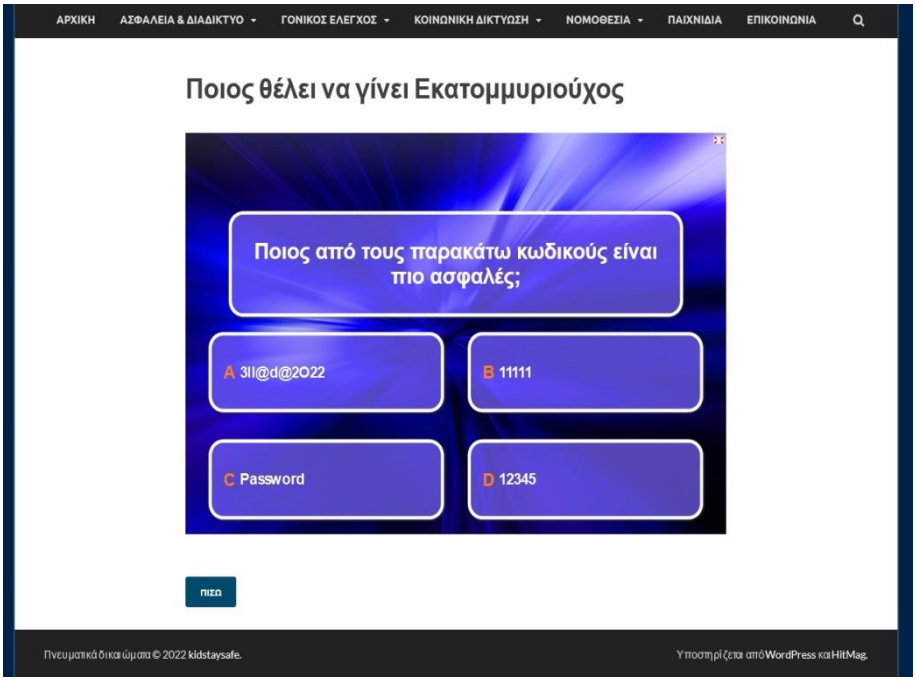
Εικόνα 139: *Quiz για Παιδιά - «Κρυπτόλεξο»*

2η Κατηγορία: *«Ερωτήσεις Πολλαπλών Επιλογών»*



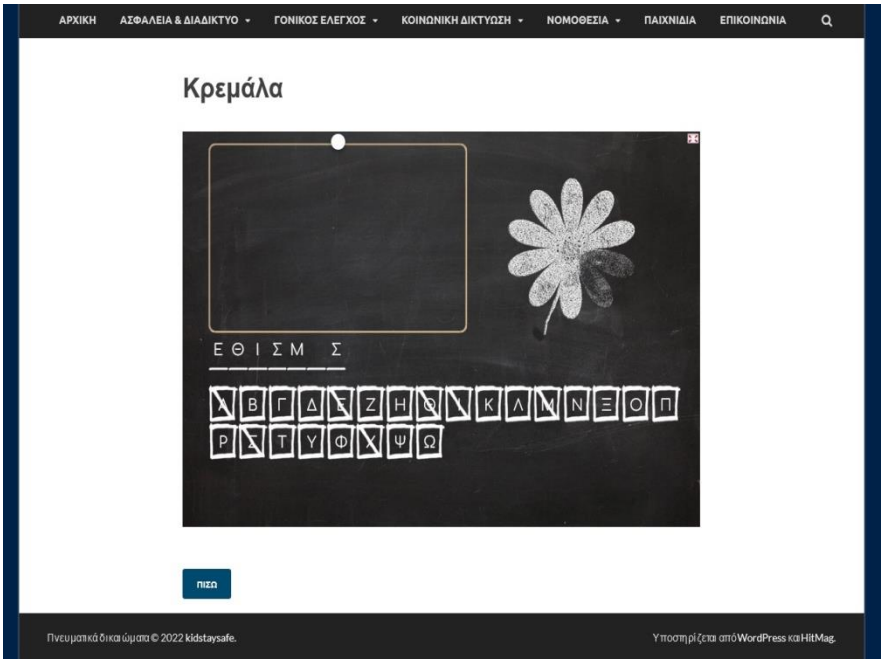
Εικόνα 140: *Quiz για Παιδιά – «Ερωτήσεις Πολλαπλών Επιλογών»*

3η Κατηγορία: *«Ποιος θέλει να γίνει εκατομμυριούχος»*



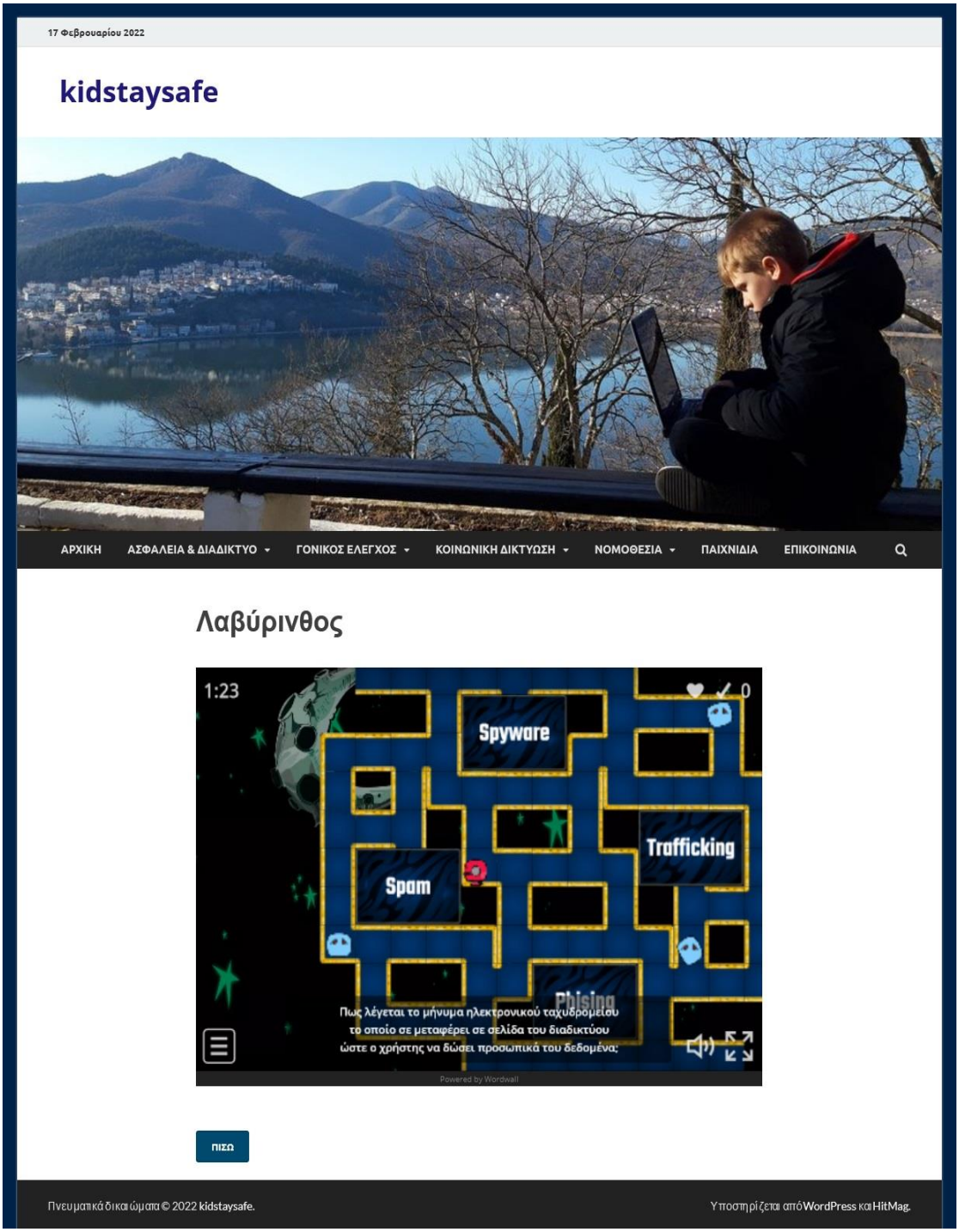
Εικόνα 141: *Quiz για Παιδιά – «Ποιος θέλει να γίνει εκατομμυριούχος»*

4η Κατηγορία: *«Κρεμάλα»*



Εικόνα 142: *Quiz για Παιδιά - «Κρεμάλα»*

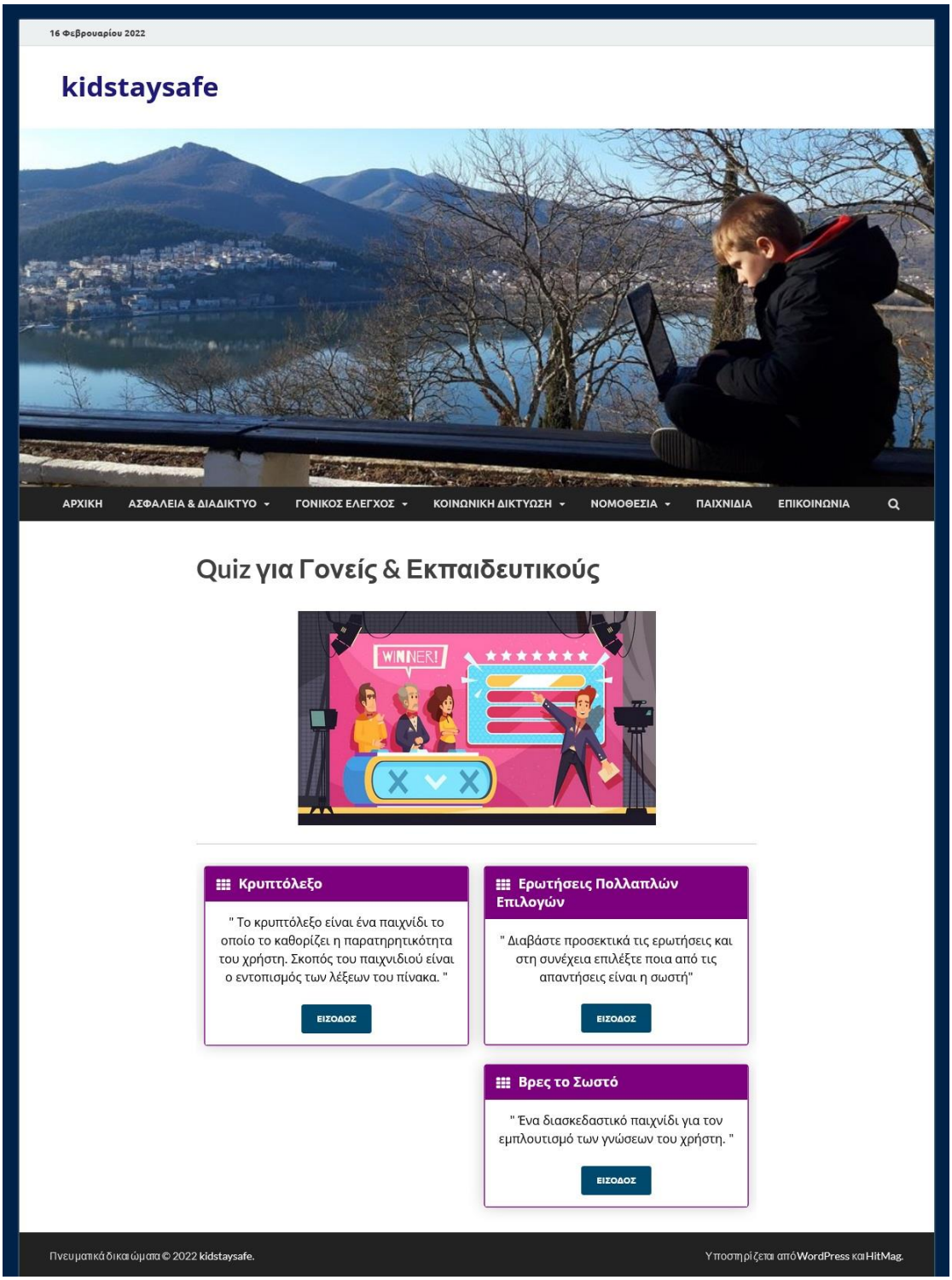
5η Κατηγορία: *«Λαβύρινθος»*



Εικόνα 143: *Quiz για Παιδιά – «Λαβύρινθος»*

6.5.6.2 Quiz για Γονείς & Εκπαιδευτικούς

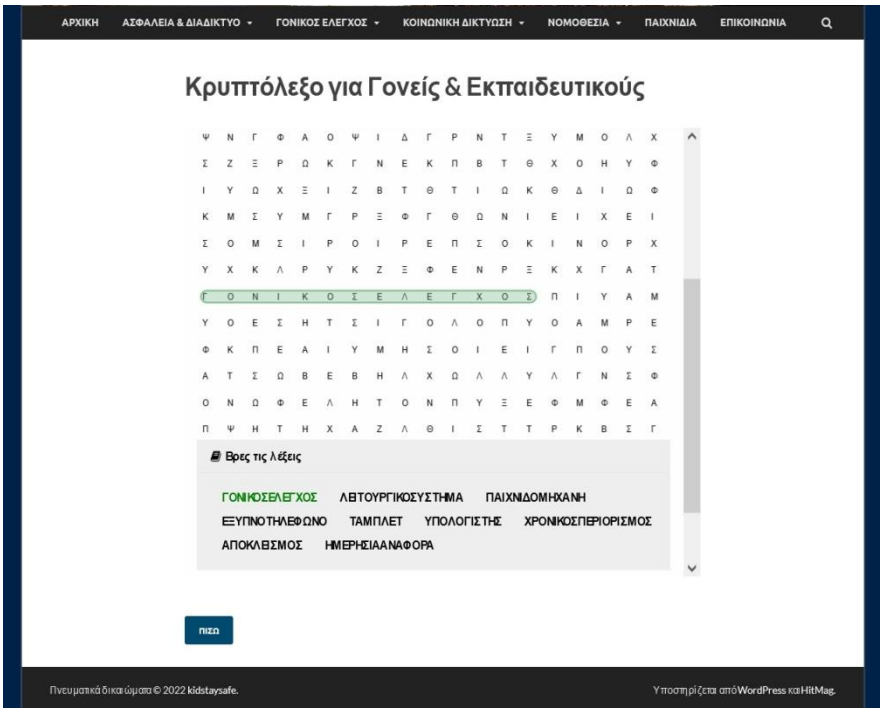
Με την επιλογή του «Quiz για Γονείς & Εκπαιδευτικούς» ανοίγει μια νέα σελίδα όπου εμφανίζονται οι κατηγορίες των παιχνιδιών.



Εικόνα 144: *Σελίδα «ΠΑΙΧΝΙΔΙΑ» - Quiz για Γονείς & Εκπαιδευτικούς*

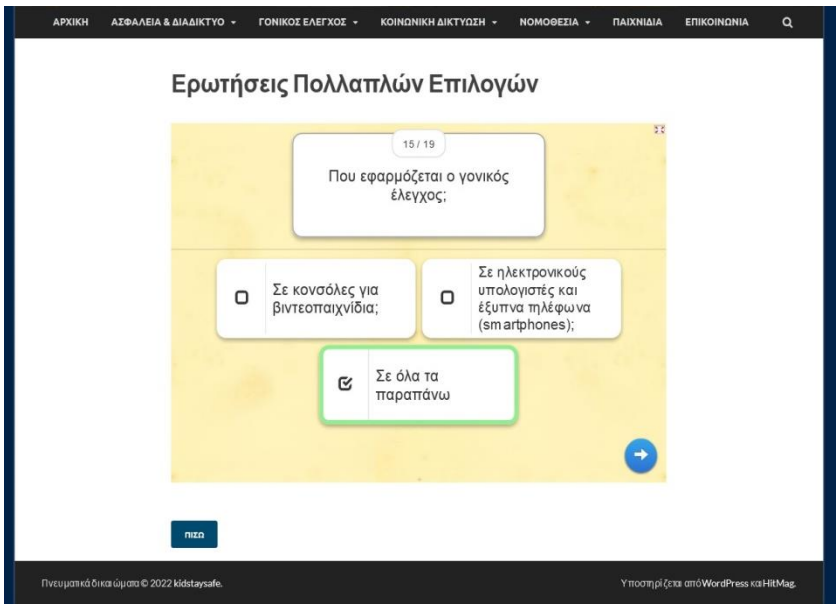
Όπως στα «quiz για παιδιά» έτσι και εδώ ο χρήστης μπορεί να επιλέξει όποια κατηγορία επιθυμεί και άμεσα να έχει πρόσβαση στο αντίστοιχο quiz.

1η Κατηγορία: *«Κρυπτόλεξο»*



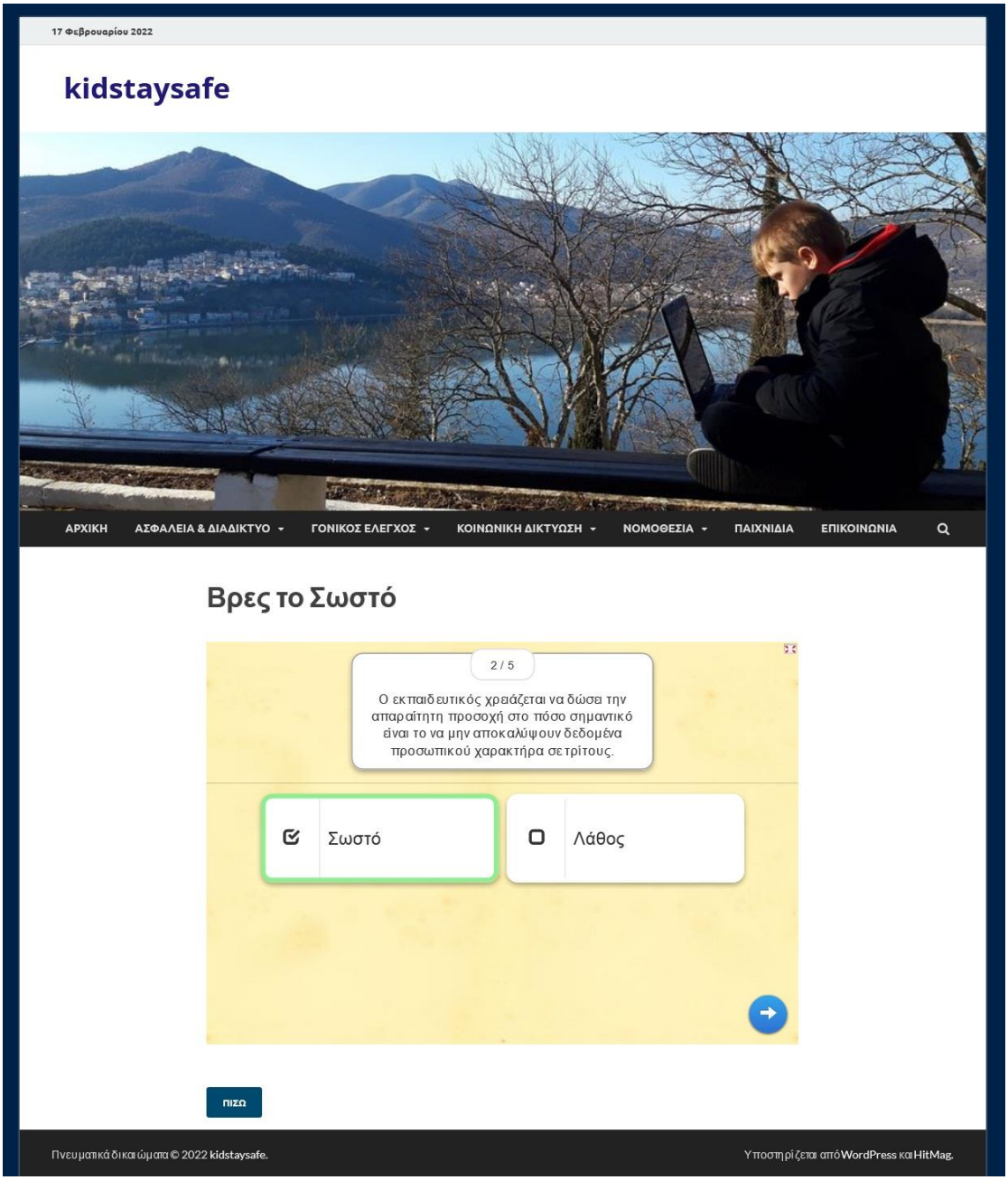
Εικόνα 145: *Quiz για Γονείς & Εκπαιδευτικούς – «Κρυπτόλεξο»*

2η Κατηγορία: *«Ερωτήσεις Πολλαπλών Επιλογών»*



Εικόνα 146: *Quiz για Γονείς & Εκπαιδευτικούς - «Ερωτήσεις Πολλαπλών Επιλογών»*

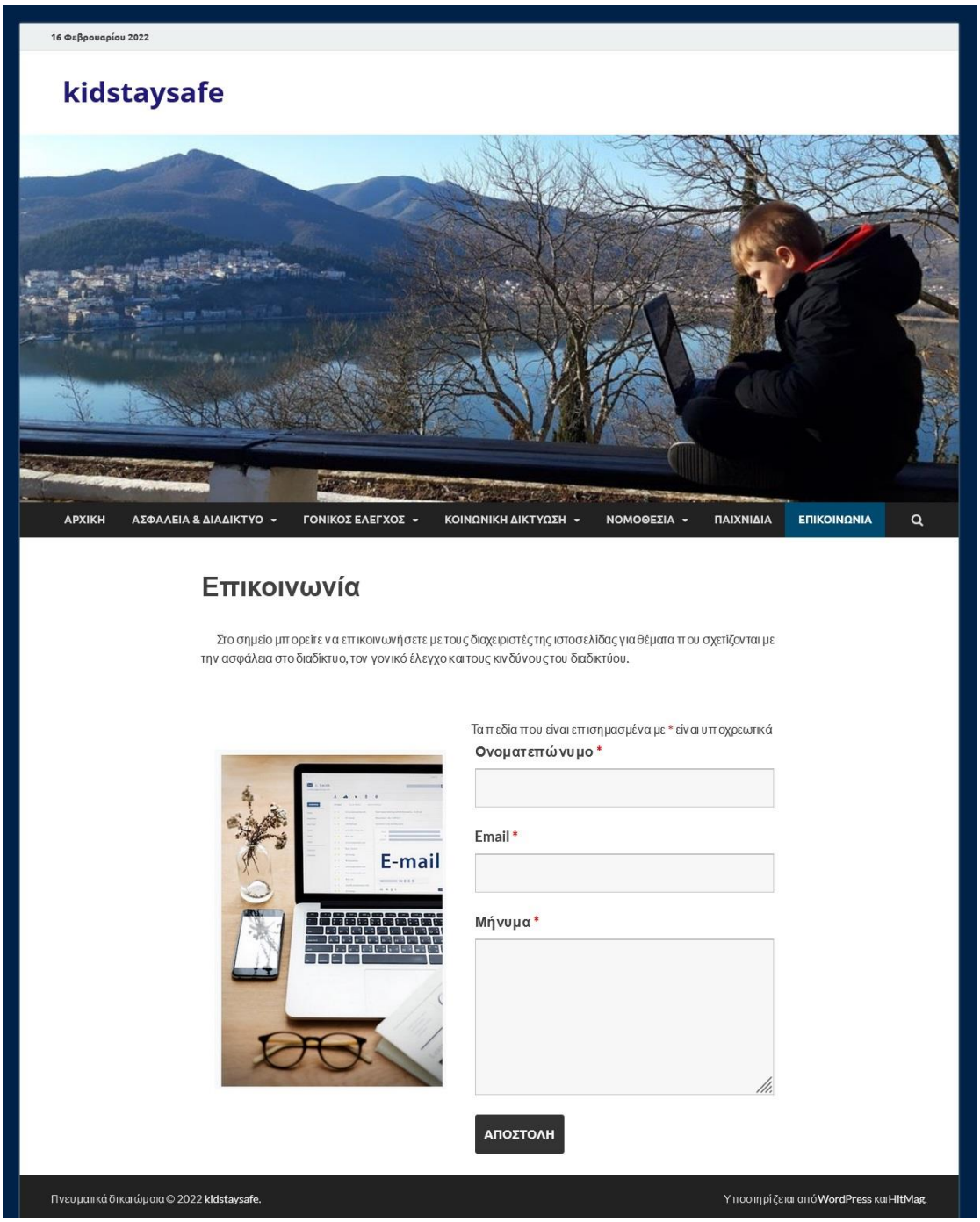
3η Κατηγορία: *«Βρες το Σωστό»*



Εικόνα 147: *Quiz για Γονείς & Εκπαιδευτικούς – «Βρες το Σωστό»*

6.5.7 Επικοινωνία

Στην ενότητα αυτή ο εκάστοτε επισκέπτης μπορεί να επικοινωνήσει με τους διαχειριστές του ιστοτόπου kidstaysafe για ζητήματα που αφορούν την ασφάλεια του διαδίκτυο, τους κινδύνους και τον γονικό έλεγχο.



Εικόνα 148: *Quiz για Γονείς & Εκπαιδευτικούς – «Επικοινωνία»*

7. Συμπεράσματα

Στην παρούσα διπλωματική εργασία, αρχικά έγινε μία μελέτη βασισμένη τόσο στην ελληνική όσο και στην ευρωπαϊκή και διεθνή βιβλιογραφία που αφορά την πρόσβαση και τη χρήση του διαδικτύου από παιδιά μικρής ηλικίας. Τα οφέλη που αποκομίζουν τα παιδιά από τον παγκόσμιο ιστό είναι πάρα πολλά. Πλέον θεωρείται δεδομένο ότι κάθε παιδί, ανεξαρτήτου ηλικίας, έχει στην κατοχή του μία έξυπνη ψηφιακή συσκευή (ηλεκτρονικό υπολογιστή, smartphones, tablet), η οποία έχει πρόσβαση στο διαδίκτυο. Όμως, η καθημερινή ενασχόληση με εφαρμογές του παγκόσμιου ιστού, δεν μπορούν εύκολα να χαρακτηριστούν σε «ασφαλή» και «μη ασφαλή».

Διαπιστώθηκε ότι η ευρεία χρήση των ψηφιακών συσκευών με πρόσβαση στο διαδίκτυο, από την ηλικιακή ομάδα των παιδιών της δημοτικής εκπαίδευσης, απαιτεί συστηματική επιτήρηση και έλεγχο από τους γονείς και τους εκπαιδευτικούς για το λόγο της αποφυγής των κινδύνων και την ενίσχυση της ασφαλούς πλοήγησης.

Από τα παραπάνω, γίνεται σαφές ότι η σωστή και εμπεριστατωμένη ενημέρωση – εκπαίδευση των παιδιών, των γονέων και των εκπαιδευτικών είναι επιτακτική και καθοριστική για την ασφαλή χρήση του διαδικτύου.

Συμπερασματικά λοιπόν, η σπουδαιότητα της γονικής διαμεσολάβησης στην επιτήρηση και προστασία των ανήλικων χρηστών του διαδικτύου, είναι καίριας σημασίας. Βέβαια, το καλύτερο «φίλτρο ελέγχου» δεν θα μπορούσε να είναι άλλο από την αδιάλειπτη επαφή των παιδιών με τους γονείς και των μαθητών με τους εκπαιδευτικούς. Έτσι, ό,τι περίεργο, ασυνήθιστο και συνάμα επικίνδυνο παρουσιάζεται στο διαδίκτυο, το παιδί θα πρέπει να είναι σε θέση να επικοινωνεί άμεσα χωρίς δισταγμό με τους γονείς ή τους εκπαιδευτικούς του, για τη σωστή και έγκυρη αντιμετώπιση των όποιων κινδύνων.

Επιπλέον, όσον αφορά τα μέσα κοινωνικής δικτύωσης, (Facebook, TikTok, Viber και Instagram), συμπεραίνεται ότι οι νέοι τείνουν να αντικαταστήσουν τους παραδοσιακούς τρόπους επικοινωνίας με τα μέσα αυτά. Οι κίνδυνοι σε αυτόν τον τομέα είναι επίσης αρκετοί και οι τρόποι αντιμετώπισής τους αφορούν, όπως και παραπάνω, τη συνεχή ενημέρωση σε θέματα ασφάλειας και ελέγχου των παιδιών, των γονέων και των εκπαιδευτικών.

Καθοριστική σημασία αποτελεί η υλοποίηση του γονικού ελέγχου σε όλες τις ψηφιακές συσκευές που χρησιμοποιούν καθημερινά οι νέοι. Τα λειτουργικά συστήματα της Microsoft (π.χ.Windows 7, Windows 8 και Windows 10) και Android παρέχουν έναν αξιόλογο και αξιόπιστο μηχανισμό γονικής επιτήρησης, ο οποίος διατίθεται δωρεάν και είναι πολύ εύκολο για ένα μέσο ενήλικα χρήστη να το εφαρμόσει σε ψηφιακές συσκευές που χρησιμοποιεί ένα παιδί. Εκτός αυτού, καλό είναι να αναφερθεί ότι στον παγκόσμιο ιστό υπάρχει μία πληθώρα προγραμμάτων

και λογισμικών εφαρμογής του γονικού ελέγχου τα οποία μπορεί να αναζητήσει και να χρησιμοποιήσει ο χρήστης.

Τελειώνοντας θα λέγαμε ότι η ιστοσελίδα που δημιουργήθηκε κατά τη διάρκεια της διπλωματικής αυτής εργασίας, kidstaysafe, αποτελεί ένα εργαλείο βοήθειας και ενημέρωσης των γονέων, των εκπαιδευτικών και των παιδιών σε θέματα της ασφάλειας και του γονικού ελέγχου στο διαδίκτυο.

Προτάσεις για μελλοντική επέκταση της διπλωματικής εργασίας

Ως μελλοντική πορεία της διπλωματικής εργασίας, θα μπορούσε να αποτελέσει η υλοποίηση μίας έρευνας για τους κινδύνους του διαδικτύου και τους τρόπους αντιμετώπισής τους, σε σχολικές μονάδες της πρωτοβάθμιας αλλά και της δευτεροβάθμιας εκπαίδευσης.

Επίσης, μαθητές με τη βοήθεια και τη συμβολή των εκπαιδευτικών, θα μπορούσαν να προβούν στη δημιουργία εκπαιδευτικού διαδραστικού υλικού μέσω 3D Animation και Videos, αλλά και στο σχεδιασμό και τη δημιουργία ιστοσελίδων ή και blogs ώστε να συμβάλουν με τον τρόπο αυτό στην ανατροφοδότηση της γνώσης αλλά και της ενημέρωσης μικρών και μεγάλων για την ασφαλή πλοήγηση στο διαδίκτυο.

8. Αναφορές

[1]D. Holloway, L. Green, and S. Livingstone, "Zero to eight: Young children and their internet use," 2013.

[2]S. Livingstone, J. Davidson, J. Bryce, S. Batool, C. Haughton, and A. Nandi, "Children's online activities, risks and safety: a literature review by the UKCCIS evidence group," 2017.

[3] Γ. Κουστουράκης and Χ. Παναγιωτακόπουλος, "Οι ΤΠΕ στην Πρωτοβάθμια Εκπαίδευση: επιδράσεις και προβλήματα από την προσπάθεια της εφαρμογής τους στην παιδαγωγική πράξη," *Στο Β. Κόμης*, pp. 425–434, 2008.

[4]G. D. P. Regulation, "General data protection regulation (GDPR)," *Intersoft Consulting, Accessed in October*, vol. 24, no. 1, 2018.

[5] Αρχή Προστασίας Δεδομένων, "Ετήσια Έκθεση 2019" , Αθήνα, 2021.

[6]Π. Γαρίνη, "Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (CDPREC679/16) και η εφαρμογή του στο ελληνικό Δημοτικό Σχολείο," 2019.

[7]Brass, D. J., Butterfield, K. D., & Skaggs, B. C. (1998). Relationships and unethical behavior: A social network perspective. *Academy of Management Review*, *23*(1), 14–31.

[8] S. Al-Fedaghi, "A conceptual foundation for the Shannon-Weaver model of communication," *International Journal of Soft Computing*, vol. 7, no. 1, pp. 12–19, 2012.

[9]H. Jones and J. H. Soltren, "Facebook: Threats to privacy," *Project MAC: MIT Project on Mathematics and Computing*, vol. 1, no. 01, p. 2005, 2005.

[10]L. Xu, X. Yan, and Z. Zhang, "Research on the causes of the 'Tik Tok' app becoming popular and the existing problems," *Journal of advanced management science*, vol. 7, no. 2, 2019.

[11] H. M. Ahmed and N. B. Bethoon, "Cybercrime: Suspicious Viber Messages Detection Model," *Int. J. Sci. Eng. Res*, vol. 8, pp. 1496–1502, 2017.

[12]K. H. Landsverk, *The Instagram Handbook: 2014 Edition*. PrimeHead Limited, 2014.

[13] E. Magkos, E. Kleisiari, P. Chanias, and V. Giannakouris-Salalidis, "Parental control and children's internet safety: the good, the bad and the ugly," *Proc. ICIL 2014*, vol. 18, 2014.

[14] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson, "Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries Report Original citation," 2011.

[15] Ά. Α. Κατσιβέλας and Μ. Α. Κατσιβέλα, " Το Ηλεκτρονικό Έγκλημα στην Ελλάδα απο το 2013 έως το 2015.," 2016.

[16] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, "An empirical analysis of phishing blacklists," 2009.

[17] T. Quandt, L. Frischlich, S. Boberg, and T. Schatto-Eckrodt, "Fake news," *The international encyclopedia of journalism studies*, pp. 1–6, 2019.

[18] Z. Tufekci, "Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate?," *Information, Communication & Society*, vol. 11, no. 4, pp. 544–564, 2008.

[19]Χ. Χαράλαμπος, "Κυβερνοέγκλημα-η εκμετάλλευση ανηλίκων στο διαδίκτυο," 2012.

[20]Α. Καραπέτσας, Α. Φώτης, and Ν. Ζυγούρης, "Νέοι και εθισμός στο διαδίκτυο: Ερευνητική προσέγγιση συχνότητας του φαινομένου," *Εγκέφαλος*, vol. 49, pp. 67–72, 2012.

[21]Γ. Μπαμπινιώτης , "Το ελληνικό αλφάβητο: Αλφάβητο – γραφή – ορθογραφία", *Κέντρο Λεξικολογίας, Αθήνα*, 2018

[22]Livingstone, S., &Helsper, E. J. (2008). Parental mediation of children's internet use. *Journal of Broadcasting and Electronic Media*, *52*(4), 581–599.

[23] Genta, M. L., Brighi, A., & Guarini, A. (2009). European project on bullying and cyberbullying granted by Daphne II programme. In *Journal of Psychology* (Vol. 217, Issue 4, p. 233).

[24] Lee, S. J. (2013). Parental restrictive mediation of children's internet use: Effective for what and for whom? *New Media and Society*, *15*(4), 466–481. Ht

[25] Iyadat, W., Iyadat, Y., Ashour, R., &Khasawneh, S. (2012). University students and ethics of computer technology usage: Human resource development. *E-Learning and Digital Media*, *9*(1), 43–49.

Παράρτημα Α: Παιχνίδια για παιδιά

QUIZ: *ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ*

ΚΑΤΗΓΟΡΙΑ ΠΑΙΧΝΙΔΙΟΥ: *ΚΡΥΠΤΟΛΕΞΟ*

ΠΛΑΤΦΟΡΜΑ ΔΗΜΙΟΥΡΓΙΑΣ: https://e-me.edu.gr

ΥΠΟΕΝΟΤΗΤΑ: *ΠΑΙΔΙΑ*

Λέξεις που χρησιμοποιήθηκαν:

1. Διαδίκτυο
2. Προσωπικά δεδομένα
3. Φωτογραφία
4. Σεβασμός
5. Άγνωστος
6. Φίλος
7. Ασφάλεια
8. Κωδικός,
9. Μήνυμα

QUIZ: *ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ*

ΚΑΤΗΓΟΡΙΑ ΠΑΙΧΝΙΔΙΟΥ: *ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ*

ΠΛΑΤΦΟΡΜΑ ΔΗΜΙΟΥΡΓΙΑΣ: www.learningapps.org

ΥΠΟΕΝΟΤΗΤΑ: *ΠΑΙΔΙΑ*

Ασφάλεια στο Διαδίκτυο

1. Τι χρειάζεται να κάνεις όταν ένας άγνωστος σου προτείνει να του δώσεις προσωπικά σου στοιχεία;

   Α) Στέλνεις αμέσως τα πραγματικά σου στοιχεία

   Β) Στέλνεις ψεύτικα/εικονικά στοιχεία

   Γ) Του λες ότι οι γονείς σου δε σου δίνουν την άδεια

   Δ) Καλείς άμεσα τους γονείς σου για να αποκλείσουν τον ανεπιθύμητο επισκέπτη.

2. Ποιο από τα πιο κάτω δεν είναι δεδομένα προσωπικού χαρακτήρα;

   Α) Το ονοματεπώνυμό σου

   Β) Το ποδήλατό σου

   Γ) Το σχολείο που πηγαίνεις

   Δ) Το τηλέφωνό σου

3. Το να χρησιμοποιείς για πολλές ώρες το διαδίκτυο λέγεται:

   Α) Εκφοβισμός

   Β) Έλεγχος

   Γ) Εθισμός

   Δ) Αλλοίωση της γλώσσας

4. Πώς λέγονται οι λανθασμένες ή ψεύτικες πληροφορίες;

   Α) Εθισμός

   Β) Παραπληροφόρηση

   Γ) Παραποίηση της γλώσσας

Δ) Παραχάραξη

5. Τι χρειάζεται να κάνεις εάν στο λογαριασμό του ηλεκτρονικού σου ταχυδρομείου λάβεις κάποιο μήνυμα που ο σύνδεσμος που περιλαμβάνει άγνωστο σύνδεσμο;

Α) Να τον ανοίξεις για να δεις τι περιλαμβάνει

Β) Να μην τον ανοίξεις γιατί γνωρίζεις ότι υπάρχει δυνατότητα να περιλαμβάνει ιό.

Γ) Να αποστείλεις μήνυμα σε άλλους να το ανοίξουν

Δ) Όλα τα παραπάνω

6. Ποιοι κίνδυνοι κρύβονται στο διαδίκτυο;

Α) Εθισμός στο διαδίκτυο

Β) Διαδικτυακή παρενόχληση

Γ) Ανεπιθύμητα μηνύματα

Δ) Βίαια παιχνίδια

Ε) Όλα τα παρακάτω.

7. Αν γνωστοποιήσω μία εικόνα μου στο διαδίκτυο, στο δημόσιο προφίλ μου, ποιος θα τη δει;

Α) Όσοι έχουν πρόσβαση στο διαδίκτυο

Β) Μόνο εσύ που την ανέβασες

Γ) Μόνο οι φίλοι σου

Δ) Οι φίλοι σου και οι φίλοι τους

8. Πώς μπορούν να γίνουν γνωστά τα δεδομένα προσωπικού σου χαρακτήρα χωρίς να το αντιληφθείς;

Α) Μέσω φωτογραφιών

Β) Μέσω των δεδομένων που υπάρχουν στο προφίλ

Γ) Μέσω των παρατηρήσεων που γράφουν οι άλλοι για σένα στον παγκόσμιο ιστό

Δ) Όλα τα παραπάνω

9. Τι χρειάζεται να κάνεις πριν γνωστοποιήσεις μία εικόνα σου από το πάρτι που έκανες στον παγκόσμιο ιστό;

   Α) Να δω αν είμαι όμορφος/όμορφη

   Β) Να πάρω την άδεια από τους γονείς αλλά και από όλους όσους φαίνονται στη φωτογραφία

   Γ) Να δω αν το μενού που πρόσφερες απεικονίζεται καλά στην εικόνα

   Δ) Τίποτα από τα παραπάνω

10. Η Μαγδαληνή είχε μία διαμάχη στο σχολείο και κάποια παιδιά της στέλνουν μηνύματα εκφοβισμού στα social media. Τι χρειάζεται να κάνει;

    Α) Να ενημερώσει αμέσως τους γονείς της και τους εκπαιδευτικούς της

    Β) Να τους αποκλείσει

    Γ) Να αποθηκεύσει τα σχόλια που της αποστέλλουν

    Δ) Όλα τα παραπάνω

QUIZ: *ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ*

ΚΑΤΗΓΟΡΙΑ ΠΑΙΧΝΙΔΙΟΥ: *ΠΟΙΟΣ ΘΕΛΕΙ ΝΑ ΓΙΝΕΙ ΕΚΑΤΟΜΜΥΡΙΟΥΧΟΣ*

ΠΛΑΤΦΟΡΜΑ ΔΗΜΙΟΥΡΓΙΑΣ: www.learningapps.org

ΥΠΟΕΝΟΤΗΤΑ: *ΠΑΙΔΙΑ*

1. Ποιος από τους παρακάτω κωδικούς είναι πιο ασφαλές;

   Α) Password

   Β) 11111

   Γ) 12345

   Δ) 3ll@d@2O22

2. Χρειάζεται η άδεια ενός ενήλικα για να περιηγηθείς στον παγκόσμιο ιστό.

   Α) Σωστό

   Β) Λάθος

3. Λαμβάνεις μήνυμα από γνωστή σου ιστοσελίδα να τους δώσεις τον προσωπικό σου κωδικό για να τροποποιήσουν το λογαριασμό σου. Τι κάνεις;

   Α) Τους αποστέλλεις κατευθείαν τον προσωπικό σου κωδικό

   Β) Αγνοείς το επικίνδυνο μήνυμα και το σβήνεις κατευθείαν

   Γ) Τους αποστέλλεις το τηλέφωνό σου ώστε να έρθετε σε επαφή και να τους δώσεις τον κωδικό σου

4. Τι χρειάζεται να κάνεις πριν γνωστοποιήσεις μία εικόνα σου από το πάρτι που έκανες στον παγκόσμιο ιστό;

   Α) Να δω αν είμαι όμορφος/όμορφη

   Β) Να πάρω την άδεια από τους γονείς αλλά και από όλους όσους φαίνονται στη φωτογραφία

   Γ) Να δω αν το μενού που πρόσφερες απεικονίζεται καλά στην εικόνα

   Δ) Τίποτα από τα παραπάνω

5. Όταν δημοσιοποιείται κάτι στον παγκόσμιο ιστό…

   Α) Το βλέπουν μόνο όσοι εσύ έχεις διαλέξει να βλέπουν τις αναρτήσεις σου

Β) Μένει στον διαδίκτυο για πάντα

Γ) Το βλέπεις μόνο εσύ

Δ) Μπορείς να το σβήσεις όποτε θέλεις

6. Τι θα κάνεις αν ένας άγνωστος επιθυμεί να έρθει σε επαφή μαζί σου στον παγκόσμιο ιστό;

Α) Να του ζητήσεις να γνωριστείτε

Β) Να του αποστείλεις φωτογραφία σου

Γ) Να το πεις σε έναν ενήλικα που του έχεις εμπιστοσύνη

Δ) Να του αποστείλεις τα δεδομένα προσωπικού σου χαρακτήρα

QUIZ: *ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ*

ΚΑΤΗΓΟΡΙΑ ΠΑΙΧΝΙΔΙΟΥ: ΚΡΕΜΑΛΑ

ΠΛΑΤΦΟΡΜΑ ΔΗΜΙΟΥΡΓΙΑΣ: www.learningapps.org

ΥΠΟΕΝΟΤΗΤΑ: ΠΑΙΔΙΑ

Λέξεις που χρησιμοποιήθηκαν:

1. Ασφάλεια Διαδικτύου
2. Προσωπικά Δεδομένα
3. Εθισμός
4. Κωδικός
5. Ηλεκτρονικό Ταχυδρομείο

QUIZ: *ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ*

ΚΑΤΗΓΟΡΙΑ ΠΑΙΧΝΙΔΙΟΥ: *ΛΑΒΥΡΙΝΘΟΣ*

ΠΛΑΤΦΟΡΜΑ ΔΗΜΙΟΥΡΓΙΑΣ: https://wordwall.net/

ΥΠΟΕΝΟΤΗΤΑ: *ΠΑΙΔΙΑ*

1. Είσαι στο διαδίκτυο και παίζεις ένα παιχνίδι. Κατά τη διάρκεια του παιχνιδιού αναδύεται το μήνυμα «Κάνε ΚΛΙΚ εδώ. Μόλις κέρδισες ένα μεγάλο χρηματικό ποσό. Τι θα κάνεις;»

   Α) Κλείνεις το παράθυρο

   Β) Τίποτα

   Γ) Κάνεις ΚΛΙΚ

   Δ) Ρωτάς τους φίλους τι να κάνεις

2. Για να αντιμετωπίσουμε ένα κακόβουλο λογισμικό

   Α) Δημιουργώ αντίγραφα ασφαλείας

   Β) Έχω εγκατεστημένο στον υπολογιστή μου ειδικό λογισμικό(antivirus) πρόγραμμα

   Γ) Είμαι προσεκτικός ποιες ιστοσελίδες χρησιμοποιείς

   Δ) Ανοίγω τα συνημμένα αρχεία. Δεν υπάρχει κίνδυνος

3. Πως λέγεται το μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο σε μεταφέρει σε σελίδα του διαδικτύου ώστε ο χρήστης να δώσει προσωπικά του δεδομένα;

   Α) Spyware

   Β) Phising

   Γ) Spam

   Δ) Trafficking

4. Όταν δημοσιεύσεις κάτι στον παγκόσμιο ιστό, αυτό θα παραμείνει εκεί για:

   Α) Για δύο χρόνια

   Β) Για τρεις μήνες

Γ) Για μία μέρα

Δ) **Για πάντα**

5. Ποιον θα συμβουλευτείς αν δεις κάτι ενοχλητικό στον παγκόσμιο ιστό;

   Α) Έναν μεγαλύτερο, γονέα, εκπαιδευτικό, φίλο, που του έχεις εμπιστοσύνη

   Β) Μόνο τον κολλητό/ή σου

   Γ) Τα μεγαλύτερα αδέλφια σου

   Δ) Μόνο τον εκπαιδευτικό της τάξης σου

6. Ο φίλος σου συνομιλεί με άγνωστο παίχτη στο online, αγαπημένο σας παιχνίδι, ο οποίος συνέχεια βωμολοχεί. Θα συμβούλευες το φίλο σου:

   Α) Να μείνει ήρεμος και να μην απαντάει στον άγνωστο παίχτη

   Β) Να το πει σε ένα μεγαλύτερο που του έχει εμπιστοσύνη

   Γ) Να αποκλείσει τον άγνωστο παίχτη

   Δ) Όλα τα παραπάνω

7. Ποια από τα παρακάτω είναι προσωπικά δεδομένα;

   Α) Το σχολείο που πηγαίνεις

   Β) Τα δεδομένα προσωπικού ιατρικού ιστορικού σου

   Γ) Οι διατροφικές συνήθειες και ιδιαιτερότητες των μαθητών

   Δ) Όλα τα παραπάνω

8. Ο καθένας μπορεί να δημοσιεύσει φωτογραφίες στον παγκόσμιο ιστό.

   Α) **Σωστό**

   Β) Λάθος

Παράρτημα Β: Παιχνίδια για γονείς και εκπαιδευτικούς

QUIZ: *ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ*

ΚΑΤΗΓΟΡΙΑ ΠΑΙΧΝΙΔΙΟΥ: *ΠΟΛΛΑΠΛΩΝ ΕΠΙΛΟΓΩΝ*

ΠΛΑΤΦΟΡΜΑ ΔΗΜΙΟΥΡΓΙΑΣ: www.learningapps.org

ΥΠΟΕΝΟΤΗΤΑ: *ΓΟΝΕΙΣ ΚΑΙ ΕΚΠΑΙΔΕΤΙΚΟΙ*

1. Οι ηλεκτρονικοί υπολογιστές πρέπει να είναι τοποθετημένοι σε εμφανές μέρος του σπιτιού και όχι σε απομονωμένο δωμάτιο

Α) Σωστό

Β) Λάθος

2. Ο γονέας έχει τη δυνατότητα να ελέγξει τον τύπο των παιχνιδιών που μπορεί να παίξει το παιδί του.

Α) Σωστό

Β) Λάθος

3. Για να εφαρμοστεί ο γονικός έλεγχος χρειάζεται μόνο η εγκατάσταση ειδικού προγράμματος.

Α) Σωστό

Β) Λάθος

4. Οι διαχειριστές είναι απαραίτητο να γνωρίζουν το λόγο για τον οποίο οι χρήστες χρησιμοποιούν το διαδίκτυο ώστε μα εφαρμόζεται και να τροποποιείται αναλόγως ο γονικός έλεγχος.

Α) Σωστό

Β) Λάθος

5. Οι γονείς πρέπει να ελέγχουν πολύ συχνά το ιστορικό του φυλλομετρητή ιστοσελίδων για να γνωρίζουν τα site στα οποία επισκέπτονται τα παιδιά τους.

Α) Σωστό

Β) Λάθος

6. Τα επίπεδα γονικού ελέγχου γίνονται σε επίπεδο παρακολούθησης, ελέγχου χρήσης και φιλτραρίσματος.

Α) Σωστό

Β) Λάθος

7. Χρειάζεται να υπάρχει συμφωνία μεταξύ γονιών και παιδιών για το πώς και το πότε θα χρησιμοποιούν τον παγκόσμιο ιστό.

Α) Σωστό

Β) Λάθος

8. Δε χρειάζεται οι γονείς να ελέγχουν τους λογαριασμούς των παιδιών τους στα μέσα κοινωνικής δικτύωσης.

Α) Σωστό

Β) Λάθος

9. Σύμφωνα με το διεθνές πρότυπο PEGI, στα παιχνίδια, υπάρχει η δυνατότητα αποκλεισμού ανάλογα με τον τύπο του περιεχομένου όπως για παράδειγμα άσχημη γλώσσα, βία, διακρίσεις, ουσίες, σεξ και φόβος.

Α) Σωστό

Β) Λάθος

10. Τα λειτουργικά συστήματα Windows της Microsoft και Android έχουν τη δυνατότητα εφαρμογής γονικού ελέγχου

Α) Σωστό

Β) Λάθος

11. Οι γονείς πρέπει να ενημερώνονται συνεχώς για τους κινδύνους και τα οφέλη που υπάρχουν στο διαδίκτυο και για τις νέες τεχνολογίες.

Α) Σωστό

Β) Λάθος

12. Τι χρειάζεται να κάνετε αν ο χρήστης σας αναφέρει ότι συνάντησε

δυσάρεστο ή ανάρμοστο υλικό στον παγκόσμιο ιστό;

Α) Να αντιδράσετε υπερβολικά;

Β) Να επισημάνετε στο χρήστη ότι πρόκειται για δικό τους λάθος

Γ) Να μη διαγράψετε τα ίχνη του ακατάλληλου υλικού.

Δ) Να μιλήσετε στο χρήστη για τους τρόπους με τους οποίους μπορεί να αντιμετωπίζει παρόμοιες καταστάσεις στο μέλλον.

13. Κατά το φιλτράρισμα ο διαχειριστής ορίζει το περιεχόμενο των ιστοσελίδων που επιτρέπεται να επισκεφθεί ο χρήστης μέσω:

Α) Εισερχόμενα δεδομένα

Β) Λέξεις - κλειδιά

Γ) Ελέγχου

Δ) Όλα τα παραπάνω

14. Ποιες δραστηριότητες του υπολογιστή μπορούν να καθοριστούν από το διαχειριστή;

Α) Τις τοποθεσίες web που επισκέφθηκε ο χρήστης

Β) Τις λήψεις αρχείων

Γ) Τις εφαρμογές που χρησιμοποίησε ο χρήστης

Δ) Πόση ώρα αφιέρωσε ο χρήστης

Ε) Όλα τα παραπάνω

15. Ποιες εφαρμογές και ποια προγράμματα μπορεί να χρησιμοποιήσει ο χρήστης;

Α) Ο χρήστης μπορεί να χρησιμοποιήσει όλες τις εφαρμογές καιτα προγράμματα

Β) Ο χρήστης μπορεί να χρησιμοποιήσει τις εφαρμογές και τα προγράμματα που έχει ορίσει ο διαχειριστής

16. Στον έλεγχο χρήσης οι γονείς ελέγχουν:

Α) Να μην υπερβαίνουν οι χρήστες τη χρονική περίοδο που τους έχουν επιτρέψει να χρησιμοποιούν τη συσκευή

Β) Ποιες υπηρεσίες και εφαρμογές χρησιμοποιούν

Γ) Και τα δύο

17. Τι πρέπει να προσέχει ο γονέας στα κινητά τηλέφωνα;

Α) Τις αγορές που γίνονται στο διαδίκτυο

Β) Την καταγραφή θέσης

Γ) Τα προγράμματα που κατεβάζουν τα παιδιά

Δ) Τι κλήσεις και τα μηνύματα που δέχονται και πραγματοποιούν

Ε) Όλα τα παραπάνω

18. Που εφαρμόζεται ο γονικός έλεγχος;

Α) Σε ηλεκτρονικούς υπολογιστές και έξυπνα τηλέφωνα (smartphones);

Β) Σε κονσόλες για βιντεοπαιχνίδια;

Γ) Σε όλα τα παραπάνω

19. Τι πρέπει να προσέχει ο γονέας στις κονσόλες βιντεοπαιχνιδιών;

Α) Το χρόνο που τις θα χρησιμοποιεί το παιδί

Β) Το πόσο κατάλληλο είναι το παιχνίδι σύμφωνα με την ηλικία του παιδιού

Γ) Τη δυνατότητα διαδικτυακή επικοινωνία με τρίτους

Δ) Τη δυνατότητα αγορών που γίνονται στο διαδίκτυο

Ε) Όλα τα παραπάνω

QUIZ: *ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ*

ΚΑΤΗΓΟΡΙΑ ΠΑΙΧΝΙΔΙΟΥ: *ΚΡΥΠΤΟΛΕΞΟ*

ΠΛΑΤΦΟΡΜΑ ΔΗΜΙΟΥΡΓΙΑΣ: https://e-me.edu.gr

ΥΠΟΕΝΟΤΗΤΑ: *ΓΟΝΕΙΣ ΚΑΙ ΕΚΠΑΙΔΕΤΙΚΟΙ*

Λέξεις που χρησιμοποιήθηκαν:

1. Γονικός Έλεγχος
2. Λειτουργικό Σύστημα
3. Παιχνιδομηχανή
4. Έξυπνο Τηλέφωνο
5. Τάμπλετ
6. Υπολογιστής
7. Χρονικός Περιορισμός
8. Αποκλεισμός
9. Ημερήσια Αναφορά

QUIZ: *ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ*

ΚΑΤΗΓΟΡΙΑ ΠΑΙΧΝΙΔΙΟΥ: *ΒΡΕΣ ΤΟ ΣΩΣΤΟ*

ΠΛΑΤΦΟΡΜΑ ΔΗΜΙΟΥΡΓΙΑΣ: www.learningapps.org

ΥΠΟΕΝΟΤΗΤΑ: *ΓΟΝΕΙΣ ΚΑΙ ΕΚΠΑΙΔΕΤΙΚΟΙ*

1. Ο διάλογος μεταξύ εκπαιδευτικών και μαθητών είναι απαραίτητος κατά τη διάρκεια του μαθήματος που αφορά την πλοήγηση στον παγκόσμιο ιστό.

Α) Σωστό

Β) Λάθος

2. Η επιτήρηση των μαθητών από τον εκπαιδευτικό κατά τη διάρκεια χρησιμοποίησης του διαδικτύου, δε χρειάζεται γιατί υπάρχει εμπιστοσύνη.

Α) Σωστό

Β) Λάθος

3. Ο εκπαιδευτικός δεν πρέπει να διεξάγει πολύ συχνά ελέγχους του ιστορικού και των αγαπημένων, σχετικά με τις ιστοσελίδες που επισκέπτονται και δραστηριοποιούνται.

Α) Σωστό

Β) Λάθος

4. Ο εκπαιδευτικός χρειάζεται να δώσει την απαραίτητη προσοχή στο πόσο σημαντικό είναι το να μην αποκαλύψουν δεδομένα προσωπικού χαρακτήρα σε τρίτους.

Α) Σωστό

Β) Λάθος

5. Οι εκπαιδευτικοί θα πρέπει να δείχνουν ιστοσελίδες στα παιδιά ανάλογα με την ηλικία τους.

Α) Σωστό

Β) Λάθος

QUIZ: *ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ*

ΚΑΤΗΓΟΡΙΑ ΠΑΙΧΝΙΔΙΟΥ: *ΣΤΑΥΡΟΛΕΞΟ*

ΠΛΑΤΦΟΡΜΑ ΔΗΜΙΟΥΡΓΙΑΣ: www.learningapps.org

ΥΠΟΕΝΟΤΗΤΑ: *ΓΟΝΕΙΣ ΚΑΙ ΕΚΠΑΙΔΕΤΙΚΟΙ*

1. Ανεπιθύμητα σχόλια ή μηνύματα ηλεκτρονικού ταχυδρομείου που εμπορεύονται ή λένε πράγματα που δε σας ενδιαφέρουν:

Ανεπιθύμητη αλληλογραφία

2. Κάποιος που χρησιμοποιεί το διαδίκτυο για να εκφοβίσει ανθρώπους π.χ. στέλνοντας κακόβουλα μηνύματα στα μέσα κοινωνικής δικτύωσης:

Διαδικτυακός εκφοβισμός

3. Ένας τύπος επιβλαβούς λογισμικού που αναπαράγεται ώστε να μπορεί να εξαπλωθεί σε άλλους υπολογιστές. Συνήθως ταξιδεύουν σε ένα δίκτυο υπολογιστών και μολύνουν πολλούς υπολογιστές:

Ιός

4. Ένα πρόγραμμα που εγκαθιστάτε στον υπολογιστή ή το τηλέφωνο σας για να το προστατεύεστε από ιούς ή κακόβουλο λογισμικό που ενδέχεται να κλέψουν τις πληροφορίες σας ή να καταστρέψουν τη συσκευή σας:

Αντιικό

5. Ένα είδος λογισμικού που σας κατασκοπεύει, κλέβοντας τα δεδομένα και τους κωδικούς πρόσβασης σας:

Κακόβουλο λογισμικό

6. Προσποιηθείτε ότι είστε κάποιος άλλος στο διαδίκτυο κλέβοντας προσωπικές πληροφορίες, όπως στοιχεία τραπεζικού λογαριασμού:

Κλοπή ταυτότητας