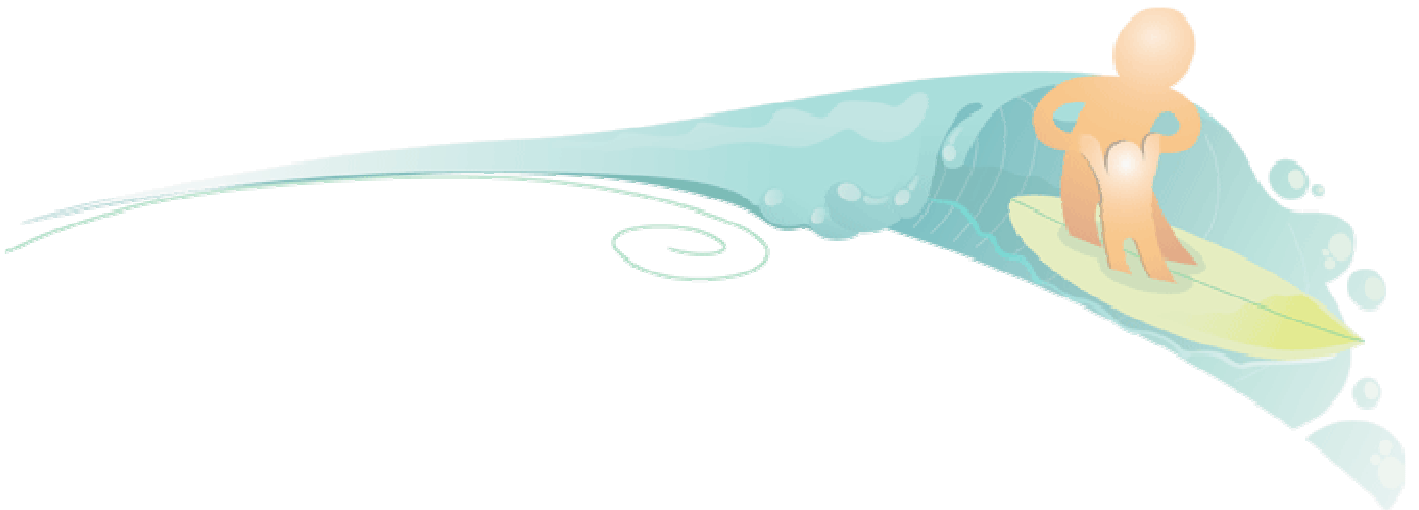




www.myparents.gr – 801-11-57100

Parental Control iProtectU

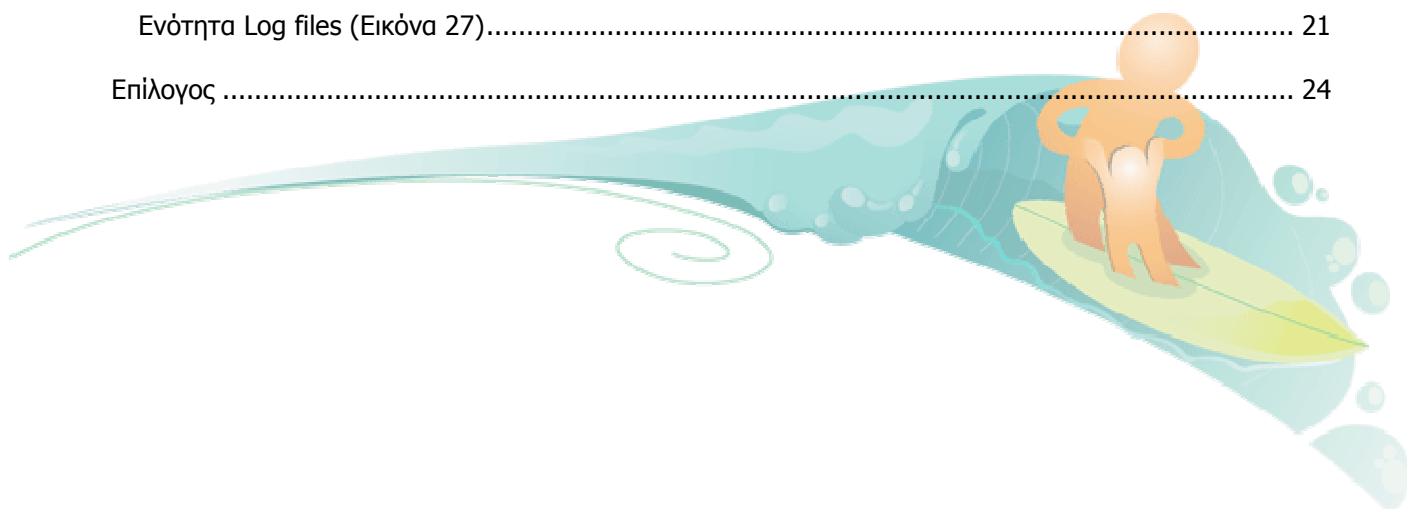


Copyright 2009



Περιεχόμενα

Εφαρμογή iProtectYou.....	3
Συμβατότητα.....	3
Εγκατάσταση.....	4
Αρχικές Ρυθμίσεις.....	5
iProtectYou Control Panel.....	8
Ενότητα Main (Εικόνα 9).....	8
Ενότητα Dictionaries (Εικόνα 18).....	14
Ενότητα Advanced (Εικόνα 26).....	20
Ενότητα Log files (Εικόνα 27).....	21
Επίλογος.....	24



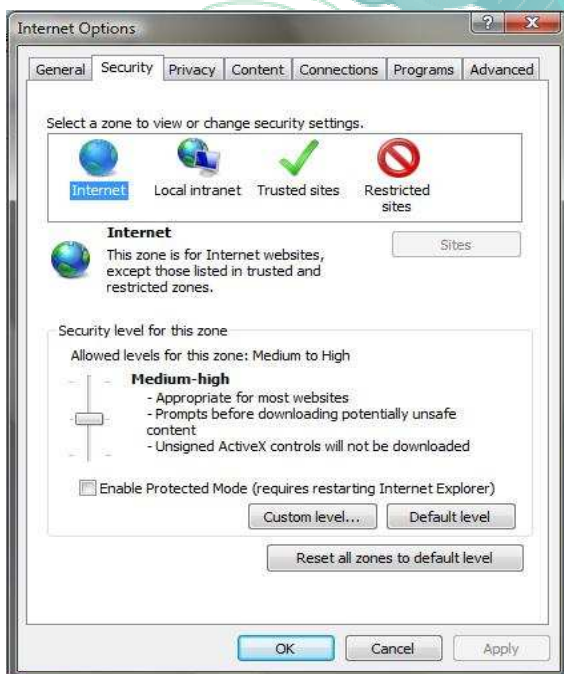
Εφαρμογή iProtectYou

Ο παρακάτω οδηγός αναφέρεται στην εφαρμογή "iProtectYou". Η συγκεκριμένη εφαρμογή παρέχεται δωρεάν από τον Ιστότοπο www.tucows.com και στην ουσία αποτελεί μια από τις πιο ολοκληρωμένες λύσεις προστασίας Παιδιών τα οποία έρχονται σε επαφή με τους Υπολογιστές και το Διαδίκτυο.

Συμβατότητα

Η εφαρμογή "iProtectYou" είναι συμβατή με όλες τις σύγχρονες εκδόσεις του λειτουργικού συστήματος "Microsoft Windows" (Windows 98/Me/2000/XP/Vista), ανεξαρτήτως έκδοσης "Service Pack" ή κύριας γλώσσας. Πραγματοποιεί αυτόματα όλες τις κεντρικές ρυθμίσεις που απαιτούνται για την ομαλή λειτουργία της, ενώ τις επαναφέρει αυτόματα στην αρχική τους κατάσταση μετά την απεγκατάστασή της.

Η "iProtectYou" είναι επίσης συμβατή με όλες τις μοντέρνες εφαρμογές οι οποίες τρέχουν στα προαναφερθέντα Λειτουργικά Συστήματα και οι οποίες θα πρέπει να υφίστανται "γονικό" έλεγχο από αυτήν. Παραδείγματα τέτοιων εφαρμογών είναι οι Internet Explorer, Mozilla Firefox, MSN Live Messenger, Skype κτλ. Δεν απαιτείται, λοιπόν, καμία απολύτως αλλαγή στις ρυθμίσεις τους μετά την εγκατάστασή της "iProtectYou", με μοναδική εξαίρεση τον "Internet Explorer 7". Πιο συγκεκριμένα, θα πρέπει να επισκεφθούμε "Tools (Εργαλεία) > Internet Options (Ρυθμίσεις) > Security [Tab] (Ασφάλεια [Καρτέλα])" και να απενεργοποιήσουμε την επιλογή "Enable Protected Mode" (Εικόνα 1).



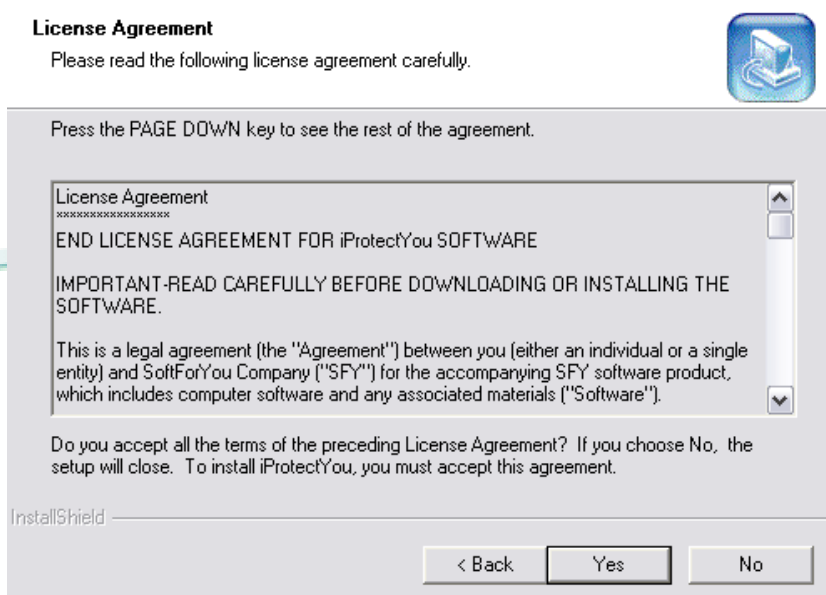
Εικόνα 1

Αμέσως μετά επανεκκινούμε τον "Internet Explorer" ώστε να αποθηκευτούν οι αλλαγές μας και ο "Internet Explorer" είναι έτοιμος προς χρήση.

Εγκατάσταση

ΠΡΟΣΟΧΗ!!! Πριν την έναρξη της διαδικασίας εγκατάστασης θα πρέπει να απενεργοποιήσουμε προσωρινά κάθε εφαρμογή "Anti-Virus", "Anti-Spyware", "Firewall" ή "Registry Monitor" (πχ SpyBot, WinPatrol κτλ). Μετά το πέρας της εγκατάστασης θα πρέπει να μην παραλείψουμε να τα ξαναενεργοποιήσουμε. Σε περίπτωση που μετά την ενεργοποίησή τους συνεχίζουν να εντοπίζουν το εκτελέσιμο "ip.exe" (εκτελέσιμο αρχείο της εφαρμογής iProtectYou) ως Εχθρικό (Malicious), θα πρέπει να αγνοηθούν τα τυχόν αναδυόμενα μηνύματα και να γίνουν οι κατάλληλες, κατά περίπτωση, ρυθμίσεις ώστε να αποχαρακτηριστεί η συγκεκριμένη εφαρμογή και να μην παρεμποδίζεται η ομαλή της λειτουργία.

Καταρχήν, συνδεόμαστε στο λειτουργικό σύστημα "Windows" και "μεταφορτώνουμε" το αρχείο ipfree.exe από τον προαναφερθέν ιστότοπο. Ξεκινούμε την εγκατάσταση απλά κάνοντας "διπλό-κλικ" πάνω στο αρχείο αυτό και συνεχίζουμε τα βήματα της εγκατάστασης πιέζοντας "Επόμενο" ("Next"). Όταν αυτό μας ζητηθεί, αποδεχόμαστε τους όρους χρήσης της συγκεκριμένης εφαρμογής (Εικόνα 2) και συνεχίζουμε την εγκατάσταση.



Εικόνα 2

Λίγο πριν αυτή ολοκληρωθεί, θα ζητηθεί ο ορισμός του φακέλου στον οποίο επιθυμούμε να εγκατασταθεί η συγκεκριμένη εφαρμογή (Εικόνα 3). Εδώ θα πρέπει να **MHN** πραγματοποιήσουμε καμία αλλαγή αλλά να αποδεχτούμε την προτεινόμενη από την εγκατάσταση επιλογή. Σε κάθε άλλη περίπτωση η εφαρμογή μας ενδέχεται να αποτύχει να εκκινήσει αυτόματα όταν ανοίγουμε τον υπολογιστή, πράγμα που την καθιστά άχρηστη.

Choose Destination Location

Select folder where Setup will install files.



Setup will install iProtectYou in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder
C:\Program Files\SoftForYou\iProtectYou

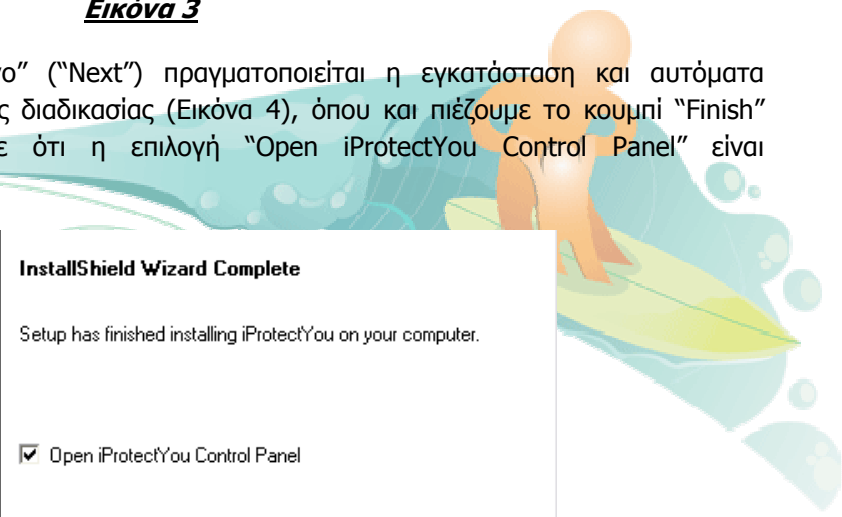
Browse...

InstallShield

< Back Next > Cancel

Εικόνα 3

Πιέζοντας, τέλος, το κουμπι "Επόμενο" ("Next") πραγματοποιείται η εγκατάσταση και αυτόματα μεταβαίνουμε στην τελευταία οθόνη της διαδικασίας (Εικόνα 4), όπου και πιέζουμε το κουμπι "Finish" ("Ολοκλήρωση"), αφού σιγουρευτούμε ότι η επιλογή "Open iProtectYou Control Panel" είναι ενεργοποιημένη.



InstallShield Wizard Complete

Setup has finished installing iProtectYou on your computer.

Open iProtectYou Control Panel

< Back Finish Cancel

Εικόνα 4

Αρχικές Ρυθμίσεις

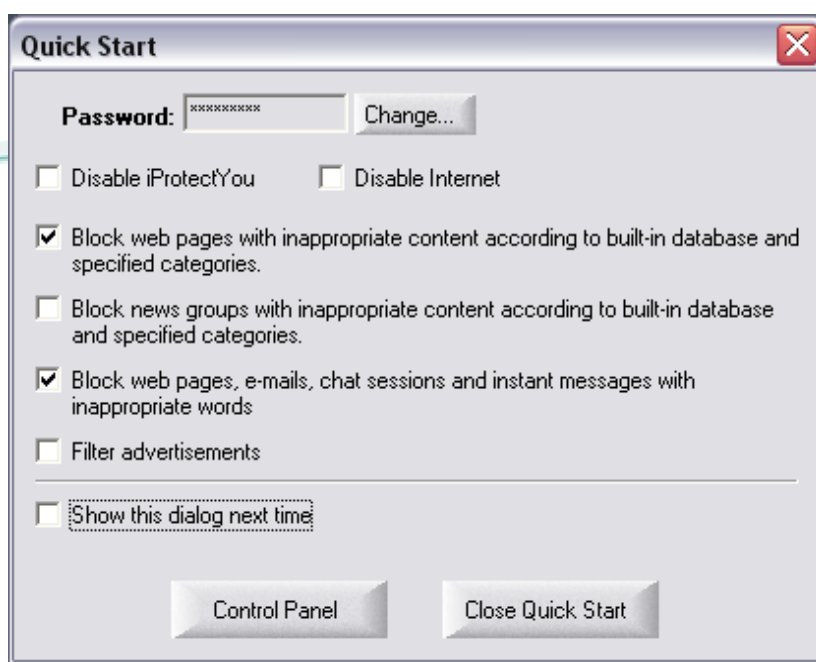
Με σκοπό την πραγματοποίηση των απαιτούμενων βασικών ρυθμίσεων λειτουργίας της συγκεκριμένης εφαρμογής, ακολουθούμε τον αυτοματοποιημένο οδηγό που εκτελείται αμέσως μετά την ολοκλήρωση

εγκατάστασης της εφαρμογής. Αρχικά, εμφανίζεται μια οθόνη (Εικόνα 5) η οποία μας επιτρέπει να επιλέξουμε την έκδοση της παρούσας εφαρμογής την οποία επιθυμούμε να χρησιμοποιήσουμε. Εμείς θα πρέπει να πιάσουμε την επιλογή "Free basic version", έτσι ώστε να απολαύσουμε τις παροχές της εφαρμογής χωρίς περιορισμούς και πρόσθετες χρεώσεις. Πριν από αυτό, όμως, θα πρέπει να ξεμαρκάρουμε την επιλογή "Show this dialog next time", ώστε να αποφύγουμε να απαντάμε συνεχώς στην ίδια ερώτηση κάθε φορά που χρησιμοποιούμε την παρούσα εφαρμογή.




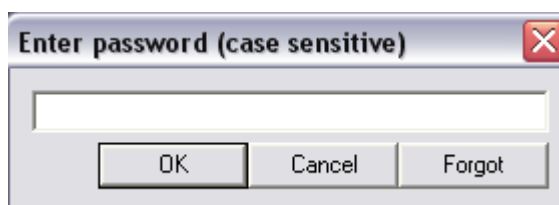
Εικόνα 5

Αμέσως μετά, εμφανίζεται στην οθόνη ένα παράθυρο επιλογών (Εικόνα 6).



Εικόνα 6

Αυτό που αρχικά θα πρέπει να γίνει είναι να οριστεί ένας μυστικός κωδικός ασφαλείας. Μόνο ο Χρήστης-Γονέας θα πρέπει να έχει πρόσβαση τόσο στις επιλογές ρύθμισης της συγκεκριμένης εφαρμογής όσο και στα συλλεγμένα από αυτή δεδομένα. Για να αποκλείσουμε, λοιπόν, τυχόν πρόσβαση σε οποιαδήποτε οθόνη αυτής από το Παιδί, θα πρέπει να θέσουμε έναν μυστικό κωδικό ο οποίος θα επιτρέπει κάτι τέτοιο μόνο στον Γονέα (δηλαδή στον γνώστη του συγκεκριμένου κωδικού). Η εισαγωγή του (Εικόνα 7) θα απαιτείται κάθε φορά που κάποιος προσπαθεί να αποκτήσει πρόσβαση στο γραφικό περιβάλλον της παρούσας εφαρμογής, κάνοντας διπλό-κλικ στο tray-icon (εικονίδιο δίπλα στην ώρα) .



Εικόνα 7

Για να ορίσουμε, λοιπόν, τον συγκεκριμένο κωδικό αρκεί να πιάσουμε την επιλογή "Change" του παραθύρου της Εικόνας 6. Αμέσως εμφανίζεται ένα νέο παράθυρο (Εικόνα 8) το οποίο επιταχύνει την συγκεκριμένη διαδικασία. Εισάγουμε τον επιθυμητό κωδικό στα πεδία "New Password" και "Confirm Password", ενώ στην συνέχεια θα πρέπει να επιλέξουμε μία ερώτηση από το drop-down menu "Security Question: - select a question to answer -" και να εισάγουμε στο πεδίο που βρίσκεται ακριβώς από κάτω την επιθυμητή απάντηση. Έτσι ακόμα και σε περίπτωση που ξεχάσουμε τον κωδικό, αυτός μπορεί εύκολα να ανακτηθεί και να αποκτηθεί εκ νέου πρόσβαση στις ρυθμίσεις της συγκεκριμένης εφαρμογής. Πατώντας το πλήκτρο "OK", τέλος, τα στοιχεία αποθηκεύονται και, αφού ενημερωθούμε σχετικά, το συγκεκριμένο παράθυρο εξαφανίζεται.



Εικόνα 8

Πριν, όμως, ολοκληρώσουμε την παρούσα ενότητα, ας περιγράψουμε καθεμία από τις υπόλοιπες επιλογές όπου μας προσφέρει η οθόνη της Εικόνας 6:

- **Disable iProtectYou:** Απενεργοποίηση κάθε λειτουργικότητας της συγκεκριμένης εφαρμογής.
- **Disable Internet:** Εμποδισμός πρόσβασης του υποκείμενου υπολογιστή στο Διαδίκτυο. Η απαγόρευση ισχύει τόσο για τους Φυλλομετρητές Ιστοσελίδων όσο και για κάθε άλλη εφαρμογή η οποία χρησιμοποιεί το δίκτυο (πχ. Games, E-mail, MSN, Skype, κτλ)
- **Block web pages with inappropriate content according to built-in database and specified categories:** Μπλοκάρισμα πρόσβασης σε Ιστοσελίδες των οποίων το περιεχόμενο θεωρείται "απαγορευμένο". Το τι θεωρείται απαγορευμένο και τι όχι θα δούμε πως καθορίζεται σε επόμενα βήματα.

- Block news groups with inappropriate content according to built-in database and specified categories: Μπλοκάρισμα πρόσβασης σε Ομάδες Ενημέρωσης των οποίων το αντικείμενο θεωρείται “απαγορευμένο”. Το τι θεωρείται απαγορευμένο και τι όχι θα δούμε πως καθορίζεται σε επόμενα βήματα.
- Block Web pages, e-mails, chat sessions and instant messages with inappropriate words: Μπλοκάρισμα πρόσβασης σε Ιστοσελίδες, μηνύματα ηλεκτρονικού ταχυδρομείου και συνδιαλέξεις μέσω MSN ή chats, όταν εντοπιστεί χρήση μιας ή περισσοτέρων “απαγορευμένων” λέξεων. Το ποια λέξη θεωρείται απαγορευμένη και ποια όχι θα δούμε πως καθορίζεται σε επόμενα βήματα.
- Filter Advertisements: Διαγραφή διαφημίσεων, έτσι ώστε να μην εμφανίζονται στους Φυλλομετρητές Ιστοσελίδων. Η επιλογή των κατάλληλων φίλτρων περιγράφεται σε επόμενα βήματα.

Αφού, λοιπόν, ενεργοποιήσουμε τις επιλογές της εφαρμογής τις οποίες εμείς θεωρούμε αναγκαίες (προτεινόμενες επιλογές βλ. Εικόνα 6), σιγουρευόμαστε ότι η επιλογή “Show this dialog Next Time” είναι απενεργοποιημένη και πιέζουμε το πλήκτρο “Control Panel”.

iProtectYou Control Panel

Αφού ολοκληρώθηκε η εγκατάσταση της εφαρμογής και πραγματοποιήθηκαν οι βασικότερες αρχικές ρυθμίσεις, ήρθε η ώρα να πραγματοποιήσουμε τις απαιτούμενες ρυθμίσεις ώστε να φέρουμε την εφαρμογή όσο πιο κοντά στις ανάγκες μας.

Ενότητα Main (Εικόνα 9)

Η πρώτη ενότητα ρυθμίσεων παρέχει το περιβάλλον τροποποίησης των βασικών παραμέτρων λειτουργίας της συγκεκριμένης εφαρμογής και διαχωρίζεται σε τέσσερις υποενότητες:

- Settings: Βασικές ρυθμίσεις, ρυθμίσεις ασφαλείας, ρυθμίσεις διατήρησης ιστορικών
- Categories: Ορισμός φίλτρων ιστοσελίδων, ορισμός περιεχομένων απαγορευμένων κατηγοριών
- Timeline: Χρονοπρογραμματισμός επιτρεπόμενης πρόσβασης στο Διαδίκτυο
- Applications: Διαχείριση δικαιωμάτων πρόσβασης εφαρμογών στο Διαδίκτυο



Εικόνα 9

Υποενότητα Settings

Η οθόνη που αντιστοιχεί στην παρούσα υποενότητα (Εικόνα 10), παρέχει τις εξής ευκολίες:

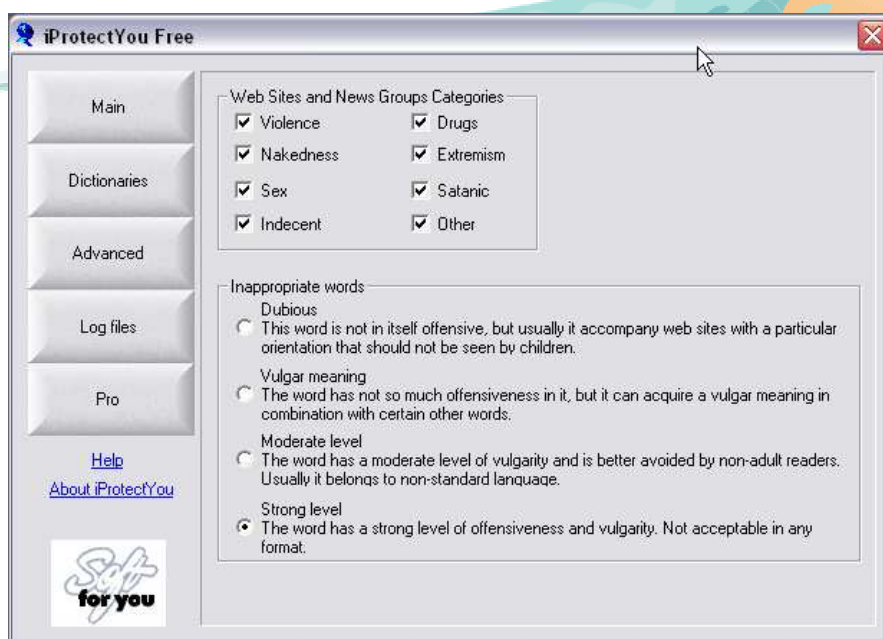
- **Password**: Αλλαγή Μυστικού Κωδικού πρόσβασης
- **Disable iProtectYou**: Απενεργοποίηση κάθε λειτουργικότητας της συγκεκριμένης εφαρμογής
- **Disable Internet**: Εμποδισμός πρόσβασης του υποκειμένου υπολογιστή στο Διαδίκτυο. Η απαγόρευση ισχύει τόσο για τους Φυλλομετρητές Ιστοσελίδων όσο και για κάθε άλλη εφαρμογή η οποία χρησιμοποιεί το δίκτυο (πχ. games, e-mail, MSN, Skype, κτλ)
- **Quick Start**: Ενεργοποίηση / Απενεργοποίηση εμφάνισης Οθόνης Συνοπτικών Ρυθμίσεων πριν την εμφάνιση του Πίνακα Ελέγχου (Control Panel) της εφαρμογής
- **Save content in**: Ορισμός Μονοπατιού Αποθήκευσης Ιστορικών
- **Deny using IP addresses in URL**: Απαγόρευση εισαγωγής Διευθύνσεων IP στις Μπάρες Διευθύνσεων (Address Bars) των Φυλλομετρητών Διαδικτύου. Μόνο πλήρη Ονόματα Ιστοσελίδων μπορούν να Εισαχθούν στα Σημεία αυτά
- **Check URLs**: Κατηγοριοποίηση των επισκεπτόμενων Ιστοσελίδων σύμφωνα με προκαθορισμένα από την εφαρμογή κριτήρια και απαγόρευση πρόσβασης σε όσες εμπίπτουν σε κατηγορίες απαγορευμένες από τον Γονέα
- **Check News groups**: Κατηγοριοποίηση των επισκεπτόμενων Ομάδων Ενημέρωσης σύμφωνα με προκαθορισμένα από την εφαρμογή κριτήρια και απαγόρευση πρόσβασης σε όσα εμπίπτουν σε κατηγορίες απαγορευμένες από τον Γονέα
- **Log Files (KB max)**: Ορισμός μέγιστου μεγέθους αρχείων Ιστορικών Χρήσης της εφαρμογής

Υποενότητα Categories

Η οθόνη που αντιστοιχεί στην παρούσα ενότητα επιτρέπει στον Γονέα να αποφασίσει σχετικά με το ποιες κατηγορίες Διαδικτυακού περιεχομένου θεωρεί αυτός βλαβερές για το Παιδί του. Μπορεί, λοιπόν, να ενεργοποιήσει τα αντίστοιχα checkboxes έτσι ώστε να επιβάλει στο Παιδί του την επιθυμητή πολιτική πρόσβασης σε Ιστοσελίδες.

Άλλη μια επιλογή που παρέχεται από την συγκεκριμένη οθόνη είναι και ο ορισμός της αυστηρότητας που θέλει να επιδείξει ο Γονέας απέναντι στην ύπαρξη συγκεκριμένων λέξεων στο εσωτερικό Ιστοσελίδων ή Αρχείων Κειμένου. Υπάρχουν, λοιπόν, τέσσερις κατηγορίες λέξεων στην βάση δεδομένων της εφαρμογής "iProtectYou":

- ***Dubious***: Λέξεις οι οποίες δεν θεωρούνται από μόνες τους προσβλητικές, αλλά η χρήση τους συχνά παραπέμπει σε περιεχόμενο ακατάλληλο για ανηλικούς
- ***Vulgar meaning***: Λέξεις οι οποίες δεν θεωρούνται από μόνες τους πολύ προσβλητικές, αλλά σε συνδυασμό με άλλες μπορούν να αποκτήσουν απαγορευτική σημασία για ένα ανήλικο
- ***Moderate level***: Λέξεις η ύπαρξη των οποίων καθιστά το προς έκθεση περιεχόμενο κατά κάποιο τρόπο ακατάλληλο για ανηλικούς. Θα ήταν προτιμότερο να μην εκτίθεται σε τέτοιο περιεχόμενο ένα ανήλικο παιδί



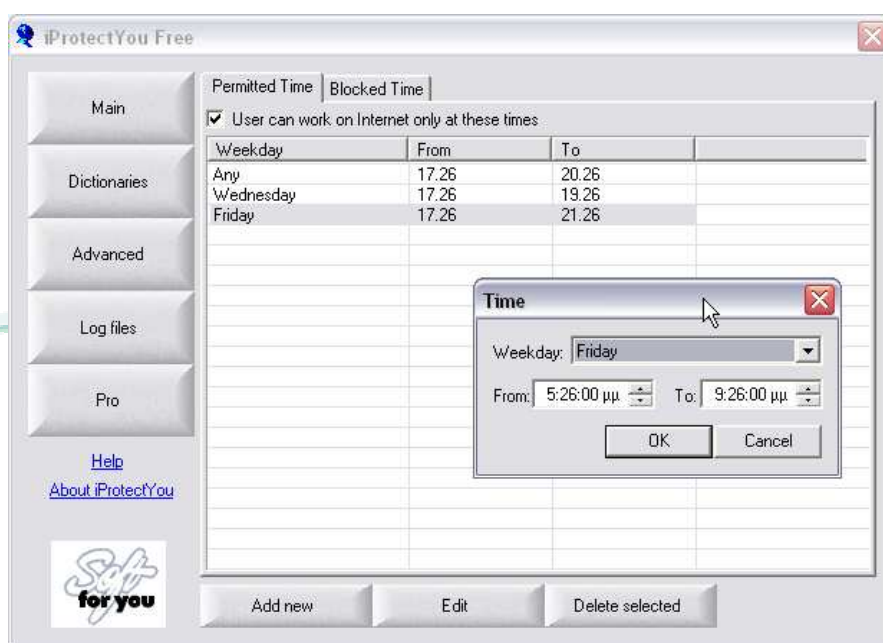
Εικόνα 11

- ***Strong level***: Λέξεις οι οποίες καθιστούν το προς έκθεση περιεχόμενο άκρως ακατάλληλο για ανηλικούς. Τα παιδιά θα πρέπει με κάθε τρόπο να μη εκτίθενται σε τέτοιου είδους περιεχόμενο

Υποενότητα Timeline

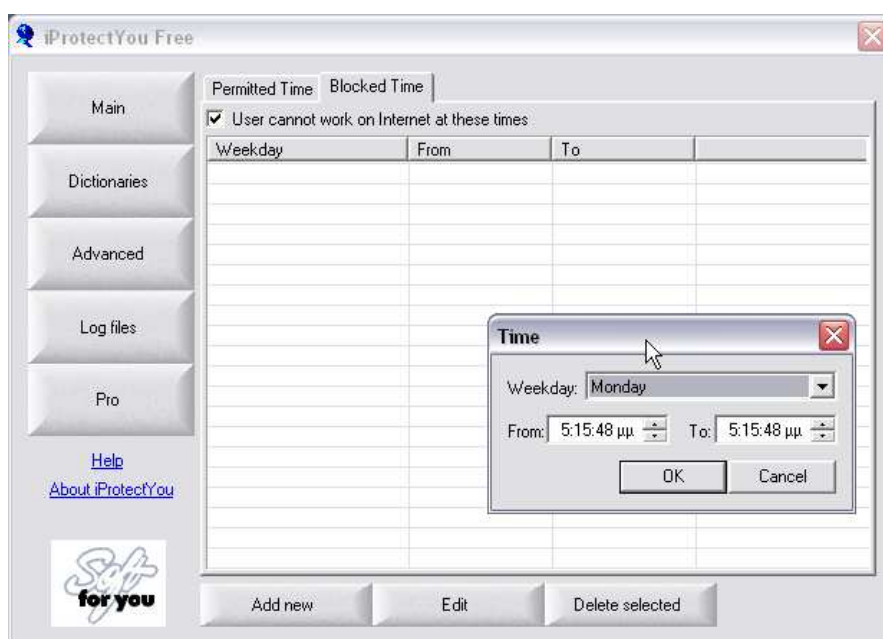
Η παρούσα υποενότητα ρυθμίσεων επιτρέπει στον Γονέα να καθορίσει το πότε επιτρέπει στο Παιδί του να χρησιμοποιεί το Διαδίκτυο και πότε όχι.

Πιο συγκεκριμένα, στην Καρτέλα "Permitted Time" (Εικόνα 12), αφού ενεργοποιηθεί η επιλογή "User can work on Internet only at these times", ο Γονέας μπορεί να ορίσει το ποιες ώρες κάθε ημέρας μόνο θα επιτρέπεται η πρόσβαση του Παιδιού στο Διαδίκτυο. Όταν μιλάμε για αποκλεισμό πρόσβασης στο Διαδίκτυο, δεν εννοούμε μόνο ότι εμποδίζονται οι Φυλλομετρητές από το να εμφανίζουν οποιαδήποτε Ιστοσελίδα, αλλά ότι καμία εφαρμογή, συμπεριλαμβανομένων των MSN, Skype, Video Games κτλ, δεν επιτρέπεται να έρθει σε επαφή με αυτό. Το κουμπί "Add new" χρησιμοποιείται για να εισάγουμε μια προκαθορισμένη περίοδο κατά την οποία θα επιτρέπεται η πρόσβαση στο Διαδίκτυο, ενώ μόλις το πιάσουμε αναδύεται το μικρότερο εκ των δυο παραθύρων της Εικόνας 12, στο οποίο μπορούμε να επιλέξουμε την Ημέρα της Εβδομάδας (Weekday) καθώς και το χρονικό διάστημα, Από: (From:) Μέχρι: (To:), της επιτρεπόμενης πρόσβασης. Πιέζοντας, δε, το πλήκτρο "OK", ο νέος κανόνας αποθηκεύεται και ταυτόχρονα εμφανίζεται στον αντίστοιχο Grid Πίνακα. Τέλος, οι αποθηκευμένοι κανόνες μπορούν να τροποποιηθούν και να διαγραφούν, απλά επιλέγοντας μια καταχώρηση από τον Grid Πίνακα και στη συνέχεια πιέζοντας τα πλήκτρα "Edit" και "Delete Selected", αντίστοιχα.



Εικόνα 12

Στην Καρτέλα "Blocked Time" (Εικόνα 13), τώρα, αφού ενεργοποιηθεί η επιλογή "User cannot work on Internet at these times", ο Γονέας μπορεί να ορίσει το ποιες ώρες κάθε ημέρας δεν θα επιτρέπεται η πρόσβαση του Παιδιού στο Διαδίκτυο. Όταν μιλάμε για απαγόρευση πρόσβασης στο Διαδίκτυο, δεν εννοούμε μόνο ότι εμποδίζονται οι Φυλλομετρητές από το να εμφανίζουν οποιαδήποτε Ιστοσελίδα, αλλά ότι καμία εφαρμογή, συμπεριλαμβανομένων των MSN, Skype, Video Games κτλ, δεν επιτρέπεται να έρθει σε επαφή με αυτό. Το κουμπί "Add new" χρησιμοποιείται για να εισάγουμε μια προκαθορισμένη περίοδο κατά την οποία θα απαγορεύεται η πρόσβαση στο Διαδίκτυο, ενώ μόλις το πιάσουμε αναδύεται το μικρότερο εκ των δυο παραθύρων της Εικόνας 13, στο οποίο μπορούμε να επιλέξουμε την Ημέρα της Εβδομάδας (Weekday) καθώς και το χρονικό διάστημα, Από: (From:) Μέχρι: (To:), απαγορευμένης πρόσβασης. Πιέζοντας, δε, το πλήκτρο "OK", ο νέος κανόνας αποθηκεύεται και ταυτόχρονα εμφανίζεται στον αντίστοιχο Grid Πίνακα. Τέλος, οι αποθηκευμένοι κανόνες μπορούν είτε να τροποποιηθούν είτε να διαγραφούν, απλά επιλέγοντας μία καταχώρηση του Grid Πίνακα και στη συνέχεια πιέζοντας τα πλήκτρα "Edit" και "Delete Selected", αντίστοιχα.

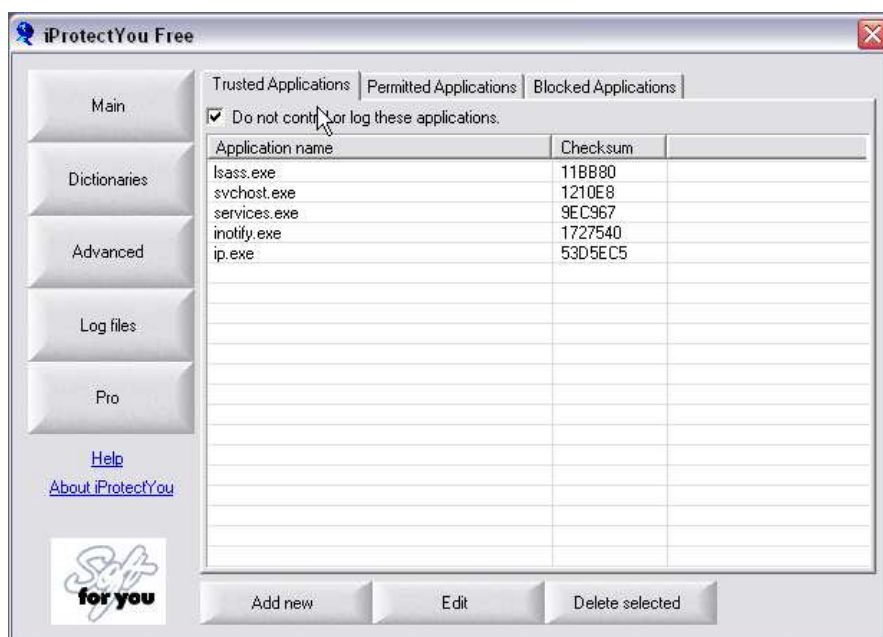


Εικόνα 13

Υποενότητα Applications

Οι θόνοι οι οποίες αντιστοιχούν στην παρούσα υποενότητα επιτρέπουν στον Γονέα να καθορίσει το σε ποιες εφαρμογές θα επιτρέπεται η πρόσβαση στο Διαδίκτυο. Για παράδειγμα, αν ένας Γονέας θεωρεί ότι το Παιδί δεν επιτρέπεται να μιλάει με άλλα άτομα μέσω του Διαδικτύου, αρκεί να εντοπίσει όλες εκείνες τις εφαρμογές τις οποίες χρησιμοποιεί το Παιδί του (πχ Skype, MSN Messenger, Google Talk κτλ) και να τους αποκλείσει την πρόσβαση.

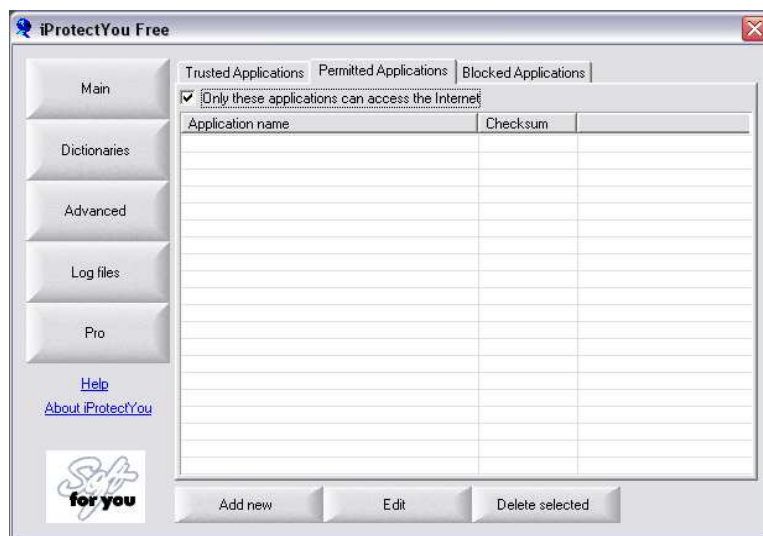
Πιο συγκεκριμένα, στην Καρτέλα "Trusted Applications" (Εικόνα 14), αφού ενεργοποιηθεί η επιλογή "Do not control or log these applications", ο Γονέας μπορεί να υποδείξει στην "iProtectYou" το ποιες εφαρμογές εμπιστεύεται σε τέτοιο βαθμό ώστε να μην επιθυμεί καν την άσκηση ελέγχου πάνω στο περιεχόμενο το οποίο διακινούν. Στην κατηγορία αυτή, συνήθως προστίθενται εφαρμογές των οποίων η ομαλή λειτουργία παρεμποδίζεται από την παρούσα εφαρμογή, ενώ ο Γονέας εκτιμά ότι δεν αποτελούν με κανένα τρόπο απειλή για τον Παιδί τους. Επίσης, εδώ προστίθενται εκτελέσιμα αρχεία του ίδιου του λειτουργικού των οποίων η λειτουργία δεν θα πρέπει με κανένα τρόπο να εμποδιστεί. Το αντίθετο θα έβαζε σε κίνδυνο την σταθερότητα του Υπολογιστή και πιθανόν να τον οδηγούσε στην κατάρρευση.



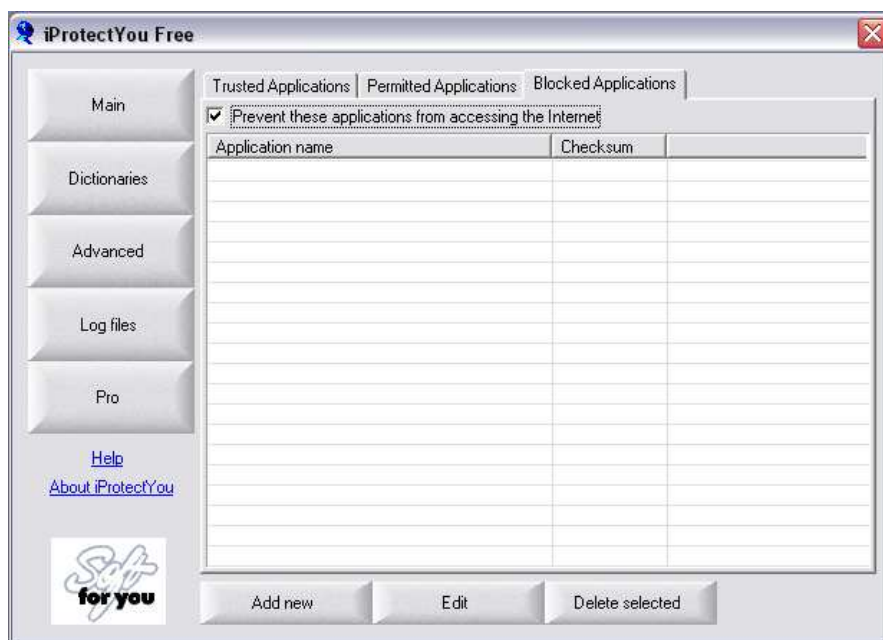
Εικόνα 14

Στην Καρτέλα "Permitted Applications" (Εικόνα 15), τώρα, αφού ενεργοποιηθεί η επιλογή "Only these applications can access the Internet", ο Γονέας μπορεί να υποδείξει στην "iProtectYou" το σε ποιες μόνο εφαρμογές θα επιτρέπεται η πρόσβαση στο Διαδίκτυο. Για παράδειγμα, μπορεί ένας Γονέας να επιθυμεί την πρόσβαση στο Διαδίκτυο αποκλειστικά μίας εφαρμογής εκπαίδευσης του Παιδιού του, και καμίας άλλης. Αρκεί, λοιπόν, να εντοπιστεί την συγκεκριμένη εφαρμογή και να την εισάγει στην παραπάνω λίστα.

Στην Καρτέλα "Blocked Applications" (Εικόνα 16), τέλος, αφού ενεργοποιηθεί η επιλογή "Prevent these applications from accessing the Internet", ο Γονέας μπορεί να υποδείξει τις εφαρμογές στις οποίες θα πρέπει να απαγορεύεται η πρόσβαση στο Διαδίκτυο. Μπορεί, για παράδειγμα, ένας Γονέας να μην επιθυμεί την πρόσβαση στο Διαδίκτυο μίας εφαρμογής Μεταφορτώσεως Παράνομου Υλικού, όπως Τραγουδιών ή/και Ταινιών. Αρκεί, λοιπόν, να εντοπίσει τις συγκεκριμένες εφαρμογές και να τις εισάγει στην παραπάνω λίστα.

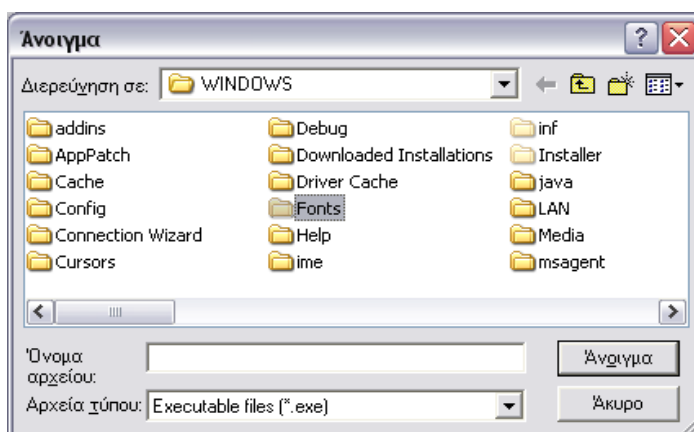


Εικόνα 15



Εικόνα 16

Στο σημείο αυτό θα πρέπει να διευκρινιστεί ότι για να εισαχθεί μια επιθυμητή εφαρμογή στην αντίστοιχη λίστα, ο Γονέας αρκεί να πιάσει το πλήκτρο "Add new" και, χρησιμοποιώντας το αναδυόμενο παράθυρο της Εικόνας 17, να εντοπίσει το επιθυμητό εκτελέσιμο αρχείο. Αφού πιεστεί το πλήκτρο "Άνοιγμα" / "Open", η επιλογή αποθηκεύεται και ταυτόχρονα εμφανίζεται στον αντίστοιχο Grid Πίνακα. Οι αποθηκευμένες στις ανωτέρω λίστες επιλογές μπορούν ακόμα να τροποποιηθούν ή να διαγραφούν, απλά επιλέγοντας την επιθυμητή καταχώρηση από τον αντίστοιχο Grid Πίνακα και πιέζοντας τα πλήκτρα "Edit" και "Delete Selected", αντιστοίχως.



Εικόνα 17

Ενότητα Dictionaries (Εικόνα 18)

Η δεύτερη αυτή ενότητα παρέχει την δυνατότητα καθορισμού των κριτηρίων βάσει των οποίων κατηγοριοποιείται το εμφανιζόμενο περιεχόμενο σε επιτρεπτό / ηθικό / θεμιτό ή απαγορευμένο / ανήθικο / αθέμιτο. Και αυτή η ενότητα διαχωρίζεται σε τέσσερις υποενότητες:



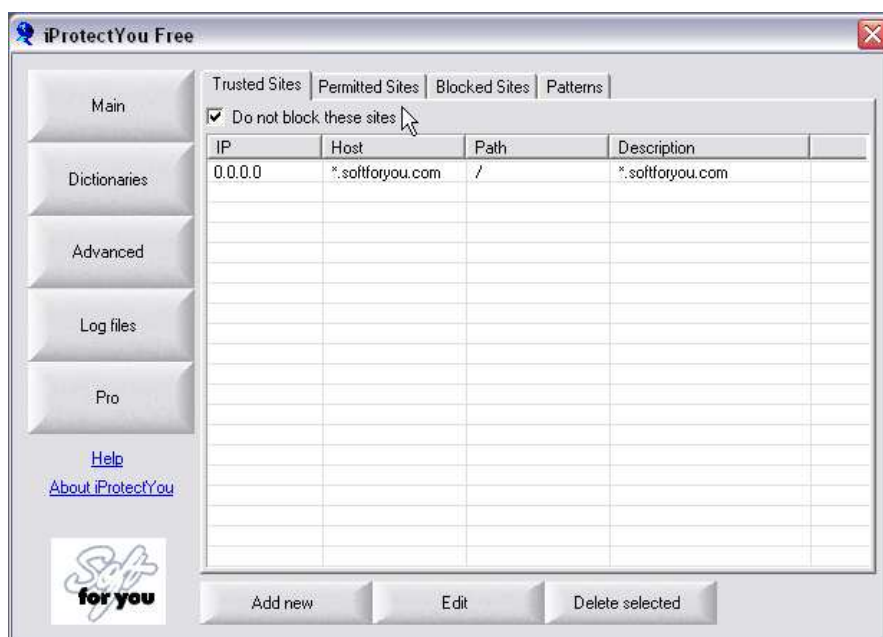
Εικόνα 18

- ***Web Sites***: Ορισμός Διαπιστευμένων / Επιτρεπόμενων / Απαγορευμένων Ιστοσελίδων, Απαγορευτικά Πρότυπα
- ***Inappropriate Words***: Ορισμός Απαγορευμένων Λέξεων περιεχόμενων σε Αρχεία
- ***News Groups***: Επιτρεπτές Λίστες Ενημέρωσης, Απαγορευμένες Λίστες Ενημέρωσης
- ***Blocked Ads***: Πολιτική απόκρυψης ανεπιθύμητων διαδικτυακών διαφημίσεων

Υποενότητα Web Sites

Οι οθόνες οι οποίες αντιστοιχούν στην παρούσα υποενότητα επιτρέπουν στον Γονέα να καθορίσει το σε ποιες Ιστοσελίδες θα επιτρέπεται να έχει πρόσβαση το Παιδί και σε ποιες όχι. Αν, για παράδειγμα, ένας Γονέας θεωρεί ότι το Παιδί του δεν επιτρέπεται να επισκέπτεται σελίδες Κοινωνικής Δικτύωσης (Hi5, MySpace, Facebook), αρκεί να συγκεντρώσει τις διευθύνσεις αυτών και να τους αποκλείσει την πρόσβαση στο Διαδίκτυο.

Πιο συγκεκριμένα, στην Καρτέλα "Trusted Sites" (Εικόνα 19), αφού ενεργοποιηθεί η επιλογή "Do not block these sites", ο Γονέας μπορεί να υποδείξει στην "iProtectYou" το ποιες Ιστοσελίδες εμπιστεύεται σε τέτοιο βαθμό ώστε να μην επιθυμεί καν την άσκηση ελέγχου πάνω στο περιεχόμενο στο οποίο εκθέτουν το Παιδί τους. Στην κατηγορία αυτή συνήθως προστίθενται Ιστοσελίδες για τις οποίες ο Γονέας εκτιμά ότι δεν αποτελούν με κανένα τρόπο απειλή για τον Παιδί τους.



Εικόνα 19

Στην Καρτέλα "Permitted Sites" (Εικόνα 20), τώρα, αφού ενεργοποιηθεί η επιλογή "Only these sites are visible", ο Γονέας μπορεί να υποδείξει στην "iProtectYou" το σε ποιες μόνο Ιστοσελίδες θα επιτρέπεται η πρόσβαση του Παιδιού. Για παράδειγμα, μπορεί ένας Γονέας να επιθυμεί την πρόσβαση του Παιδιού του αποκλειστικά σε μία ομάδα εκπαιδευτικών Ιστοσελίδων, και σε καμία άλλη. Αρκεί, λοιπόν, να εντοπίσει τις διευθύνσεις των συγκεκριμένων Ιστοσελίδων και να τις εισάγει στην λίστα.



Εικόνα 20

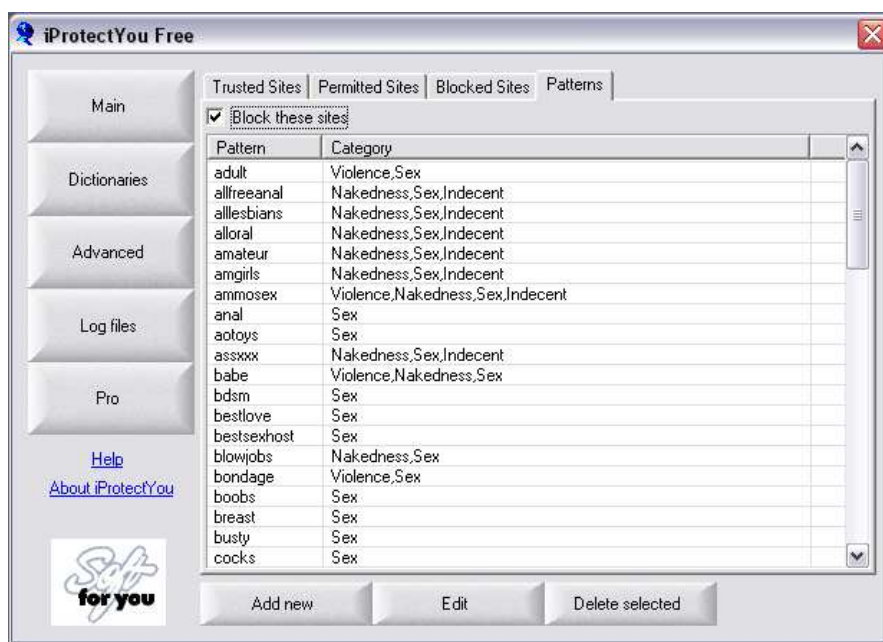
Στην Καρτέλα "Blocked Sites" (Εικόνα 21), τέλος, αφού ενεργοποιηθεί η επιλογή "Block these sites", ο Γονέας μπορεί να υποδείξει στην "iProtectYou" το σε ποιες Ιστοσελίδες θα πρέπει να απαγορεύεται η πρόσβαση του Παιδιού του (αυτό δεν σημαίνει ότι παύει ο έλεγχος και ο αποκλεισμός των υπολοίπων Ιστοσελίδων οι οποίες κατατάσσονται από την εφαρμογή ως απαγορευμένες). Μπορεί, λοιπόν, ένας Γονέας να μην επιθυμεί την πρόσβαση του Παιδιού του σε Ιστοσελίδες Κοινωνικής Δικτύωσης. Για να επιτύχει κάτι τέτοιο αρκεί μόνον να συγκεντρώσει τις διευθύνσεις των συγκεκριμένων Ιστοσελίδων (πχ www.facebook.com, www.hi5.com κτλ) και να τις εισάγει στην λίστα.

Πριν, όμως, αναλύσουμε και της τελευταία Καρτέλα της παρούσας υποενότητας, θα πρέπει να διευκρινίσουμε το πως μπορεί να εισαχθεί μια επιθυμητή Ιστοσελίδα στην αντίστοιχη λίστα. Ο Γονέας, λοιπόν, αρκεί να πιέσει το πλήκτρο "Add new" και, χρησιμοποιώντας το αναδυόμενο παράθυρο που παρουσιάζεται και στην Εικόνα 21, να εισάγει την διεύθυνση της Ιστοσελίδας στο κατάλληλο πεδίο. Αφού πιεστεί το πλήκτρο "OK", η καταχώρηση αποθηκεύεται και ταυτόχρονα εμφανίζεται στον αντίστοιχο Grid Πίνακα. Οι αποθηκευμένες στις ανωτέρω λίστες επιλογές μπορούν και να τροποποιηθούν και να διαγραφούν, απλά επιλέγοντας την επιθυμητή καταχώρηση από τον αντίστοιχο Grid Πίνακα και πιέζοντας τα πλήκτρα "Edit" και "Delete Selected", αντιστοίχως.



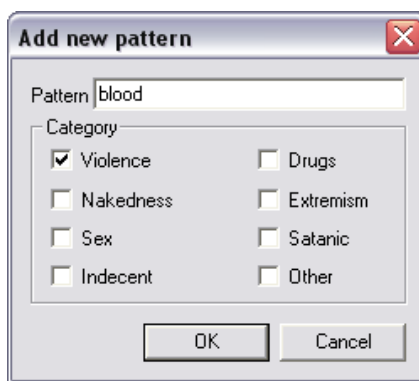
Εικόνα 21

Στην τελευταία, τώρα, Καρτέλα "Patterns" (Εικόνα 22), αφού ενεργοποιηθεί η επιλογή "Block these sites", ο Γονέας μπορεί να διαχειριστεί τις λέξεις βάσει των οποίων πραγματοποιείται η κατηγοριοποίηση του περιεχομένου της εκάστοτε Ιστοσελίδας.



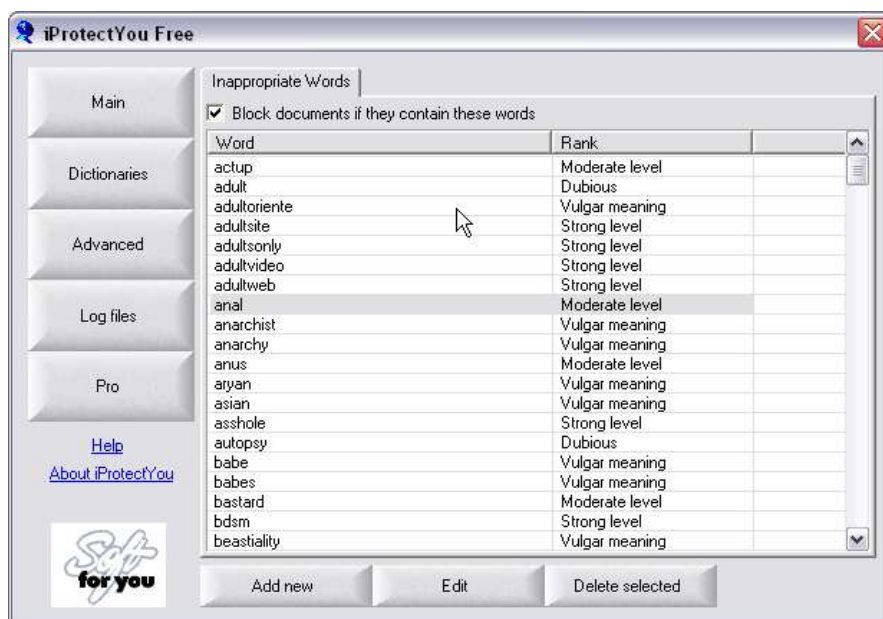
Εικόνα 22

Δίπλα σε κάθε απαγορευμένη λέξη, δε, εμφανίζεται και η κατηγορία στην οποία κατατάσσεται η εκάστοτε Ιστοσελίδα που τυχαίνει να την περιέχει. Ο Γονέας, βέβαια, εκτός από το να πληροφορηθεί σχετικά με τις λέξεις αυτές μπορεί να εισάγει και δικές του τις οποίες θεωρεί απαγορευμένες. Προς αυτήν την κατεύθυνση, αρκεί να πιέσει το πλήκτρο "Add new" και, χρησιμοποιώντας το αναδυόμενο παράθυρο της Εικόνας 23, να εισάγει την επιθυμητή λέξη, συνοδευόμενη από την κατηγορία η οποία βέλτιστα την χαρακτηρίζει (ΠΡΟΣΟΧΗ!!! Δεν υποστηρίζονται ελληνικοί χαρακτήρες). Αφού πιεστεί το πλήκτρο "OK", η καταχώρηση αποθηκεύεται και ταυτόχρονα εμφανίζεται στον Grid Πίνακα. Οι αποθηκευμένες στην ανωτέρω λίστα λέξεις μπορούν να τροποποιηθούν και να διαγραφούν, απλά επιλέγοντας την επιθυμητή καταχώρηση από τον Grid Πίνακα και πιέζοντας τα πλήκτρα "Edit" και "Delete Selected", αντιστοίχως.



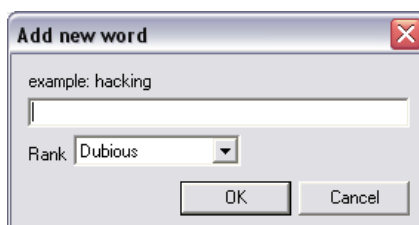
Εικόνα 23

Υποενότητα Inappropriate Words



Εικόνα 24

Η οθόνη που αντιστοιχεί στην παρούσα υποενότητα επιτρέπει στον Γονέα να καθορίσει το ποια αρχεία κείμενου δεν θα επιτρέπεται να είναι προσβάσιμα και αναγνώσιμα από το Παιδί του. Πιο συγκεκριμένα, μέσω της καρτέλας "Inappropriate Words" (Εικόνα 24), και αφού ενεργοποιηθεί η επιλογή "Block documents if they contain these words", δίδεται στον Γονέα η δυνατότητα διαχείρισης των λέξεων βάσει των οποίων πραγματοποιείται η κατηγοριοποίηση και ο αποκλεισμός του εκάστοτε αρχείου κειμένου. Δίπλα σε κάθε απαγορευμένη λέξη, δε, εμφανίζεται και ο βαθμός σχετικότητας αυτής με περιεχόμενο ακατάλληλο για ανηλικούς. Ο Γονέας εκτός από το να πληροφορηθεί σχετικά με τις συγκεκριμένες λέξεις, μπορεί να εισάγει και δικές του τις οποίες θεωρεί απαγορευμένες. Προς αυτήν την κατεύθυνση, αρκεί να πιέσει το πλήκτρο "Add new" και, χρησιμοποιώντας το αναδυόμενο παράθυρο της εικόνας 25, να εισάγει την επιθυμητή λέξη συνοδευόμενη από την κατηγορία η οποία βέλτιστα την χαρακτηρίζει (***ΠΡΟΣΟΧΗ!!! Δεν υποστηρίζονται ελληνικοί χαρακτήρες***). Αφού πιεστεί το πλήκτρο "OK", η καταχώρηση αποθηκεύεται και ταυτόχρονα εμφανίζεται στον Grid Πίνακα. Οι αποθηκευμένες στην ανωτέρω λίστα λέξεις μπορούν να τροποποιηθούν και να διαγραφούν, απλά επιλέγοντας την επιθυμητή καταχώρηση από τον Grid Πίνακα και πιέζοντας τα πλήκτρα "Edit" και "Delete Selected", αντιστοίχως.



Εικόνα 25

Υποενότητα News Groups

Οι θρόνες οι οποίες αντιστοιχούν στην παρούσα υποενότητα επιτρέπουν στον Γονέα να καθορίσει το σε ποιες Ομάδες Ενημέρωσης θα επιτρέπεται να έχει πρόσβαση το Παιδί του και σε ποιες όχι. Δεδομένου, όμως, ότι η συγκεκριμένη μέθοδος ενημέρωσης έχει πάψει πια να χρησιμοποιείται ευρέως στο Διαδίκτυο, καθώς έχει με τα χρόνια αντικατασταθεί από πιο μοντέρνες τεχνολογίες, η αναλυτική περιγραφή των παρεχόμενων δυνατοτήτων κρίνεται σκόπιμο να παραληφθεί. Αν, παρ' όλα αυτά, κάποιος επιθυμεί το φιλτράρισμα και αυτής της κατηγορίας περιεχομένου μπορεί εύκολα, παρατηρώντας όσα έχουμε παρουσιάσει ως τώρα, να πραγματοποιήσει τις κατάλληλες ρυθμίσεις.

Υποενότητα Blocked Ads

Οι θρόνες οι οποίες αντιστοιχούν στην παρούσα υποενότητα επιτρέπουν στον Γονέα να παραμετροποιήσει έτσι το σύστημά του ώστε να μπλοκάρεται η εμφάνιση διαφημίσεων κατά την πλοήγηση του Παιδιού του στο Διαδίκτυο. Δυστυχώς, όμως, οι μέθοδοι ελέγχου που χρησιμοποιούνται προς την κατεύθυνση αυτή πολλές φορές ενέχουν κινδύνους για την ορθή εμφάνιση των μοντέρνων Ιστοσελίδων, κυρίως λόγω των πολυσύνθετων τεχνολογιών πάνω στις οποίες αυτές στηρίζονται. Για να μην επηρεαστεί, λοιπόν, η ορθή λειτουργία του υποκείμενου συστήματος θα πρέπει να αποφευχθεί η τροποποίηση οποιασδήποτε ρύθμισης αντιστοιχεί στην παρούσα υποενότητα. Κρίνεται έτσι σκόπιμο το να παραληφθεί η περαιτέρω ανάλυσή της.

Ενότητα Advanced (Εικόνα 26)

Η τρίτη αυτή ενότητα παρέχει την δυνατότητα καθορισμού εξειδικευμένων παραμέτρων οι οποίες απευθύνονται σε προχωρημένους χρήστες και στην ουσία αφορούν την συνδεσιμότητα του παρόντος υπολογιστικού συστήματος με άλλα συστήματα, είτε του τοπικού δικτύου είτε του Διαδικτύου:



Εικόνα 26

- Outgoing: Λίστα Υπολογιστικών Συστημάτων με τα οποία επιτρέπεται τυχόν Σύνδεση
- Ingoing: Λίστα Υπολογιστικών Συστημάτων τα οποία επιτρέπεται να συνδεθούν με το παρόν Σύστημα
- Ports: Διαχείριση Θυρών Πρόσβασης του παρόντος Συστήματος

Οι οθόνες οι οποίες αντιστοιχούν στην παρούσα ενότητα επιτρέπουν στον Γονέα να παραμετροποιήσει έτσι το σύστημά του ώστε να εμποδίζεται η συνδεσιμότητά του με συγκεκριμένες δικτυακές μηχανές ή να επιτρέπεται μόνο με συγκεκριμένες και προκαθορισμένες μηχανές. Η συγκεκριμένες ευκολίες, όμως, είναι ένα πολύ μικρό υποσύνολο αυτών των οποίων προσφέρονται σήμερα από εξειδικευμένες και ισχυρότατες εφαρμογές, τα Firewalls. Στην περίπτωση, λοιπόν, όπου ένας Γονέας επιθυμεί την πραγματοποίηση τέτοιου είδους ρυθμίσεων στο υποκείμενο υπολογιστικό σύστημα, θα τον προτρέπαμε να προτιμήσει μία εκ των έτοιμων λύσεων Firewall που κυκλοφορούν στο Διαδίκτυο. Μια τέτοια εφαρμογή θεωρείται μακράν ισχυρότερη από την παρούσα για τέτοιου είδους προχωρημένες ρυθμίσεις, ενώ είναι σε θέση να προσφέρει περισσότερες και πιο ισχυρές επιλογές στον τελικό χρήστη. Κρίνεται έτσι σκόπιμο το να παραληφθεί η περαιτέρω ανάλυση της συγκεκριμένης ενότητας και προτρέπουμε τον προχωρημένο χρήστη να προτιμήσει ένα πιο ισχυρό πρόγραμμα ώστε να πραγματοποιήσει τις τέτοιου είδους εξειδικευμένες ρυθμίσεις.



Εικόνα 27

Ενότητα Log files (Εικόνα 27)

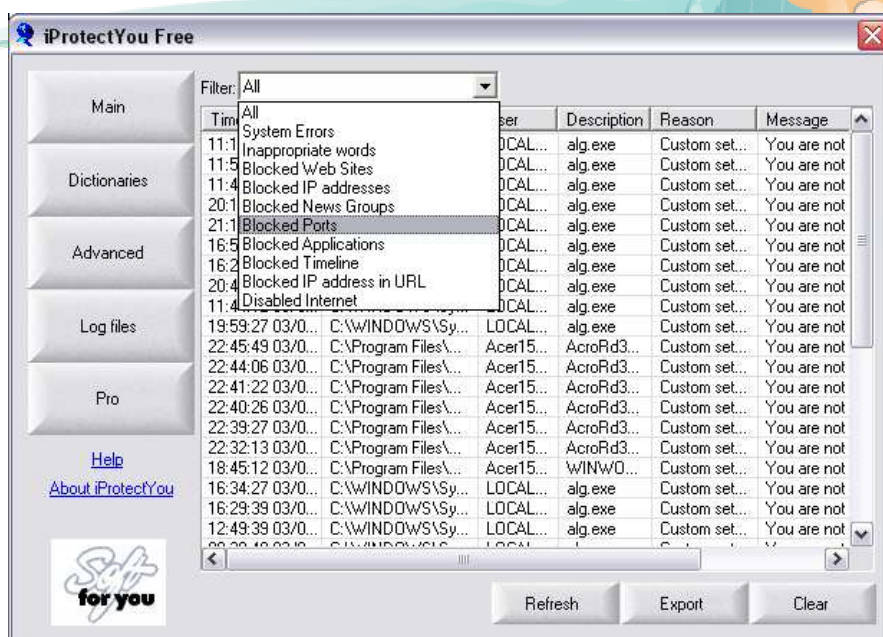
Η τέταρτη και τελευταία ενότητα παρέχει την δυνατότητα διαχείρισης των Αρχείων Ιστορικού τα οποία δημιουργούνται κατά την χρήση του εκάστοτε Υπολογιστικού Συστήματος σύμφωνα με τις υποδείξεις του γονέα. Οι δυνατότητες εδώ περιορίζονται στην ανάγνωση των απαιτούμενων πληροφοριών, στην εξωτερική τους αποθήκευση καθώς και στην διαγραφή τους.

- Warnings: Ιστορικό Προειδοποιήσεων

- **Activity:** Ιστορικό Χρόνου / Διάρκειας / Ποσότητας ανταλλασσόμενων δεδομένων από την εκάστοτε Εφαρμογή
- **Details:** Στατιστικά Στοιχεία αναλωθέντων Διαδικτυακών Πόρων
- **Blocked Ads:** Ιστορικό Εμποδισμένων Διαφημιστικών Μηνυμάτων

Υποενότητα Warnings

Η οθόνη που αντιστοιχεί στην παρούσα υποενότητα (Εικόνα 28) επιτρέπει στον Γονέα να πληροφορηθεί σχετικά με όλες τις προειδοποιήσεις οι οποίες εμφανίστηκαν στο Παιδί του κατά την διάρκεια χρήσης του Υπολογιστή. Μαζί με την ώρα εμφάνισης (Time) της εκάστοτε προειδοποίησης, παρατίθεται το μονοπάτι του εκτελέσιμου αρχείου το οποίο την πυροδότησε, το όνομα του χρήστη (User) ο οποίος εργαζόταν εκείνη την ώρα στον υπολογιστή, το όνομα του προαναφερθέντος εκτελέσιμου, ο λόγος πυροδότησης της προειδοποίησης καθώς και το μήνυμα το οποίο τυπώθηκε στην οθόνη. Ο Γονέας, επίσης, μπορεί χρησιμοποιώντας την λίστα με όνομα Filter να επιλέξει το ποια ομάδα προειδοποιήσεων επιθυμεί να τυπώνεται στον αντίστοιχο Grid Πίνακα, έτσι ώστε να μην χάνεται στο πλήθος των καταχωρήσεων και να εντοπίζει γρηγορότερα αυτό που θέλει. Οι καταχωρήσεις του Grid Πίνακα της Εικόνας 28 δύνανται είτε να Ανανεωθούν ή να Αποθηκευθούν σε Εξωτερικό Αρχείο ή να Διαγραφούν απλά πιέζοντας τα πλήκτρα "Refresh", "Export" και "Clear" αντίστοιχα.

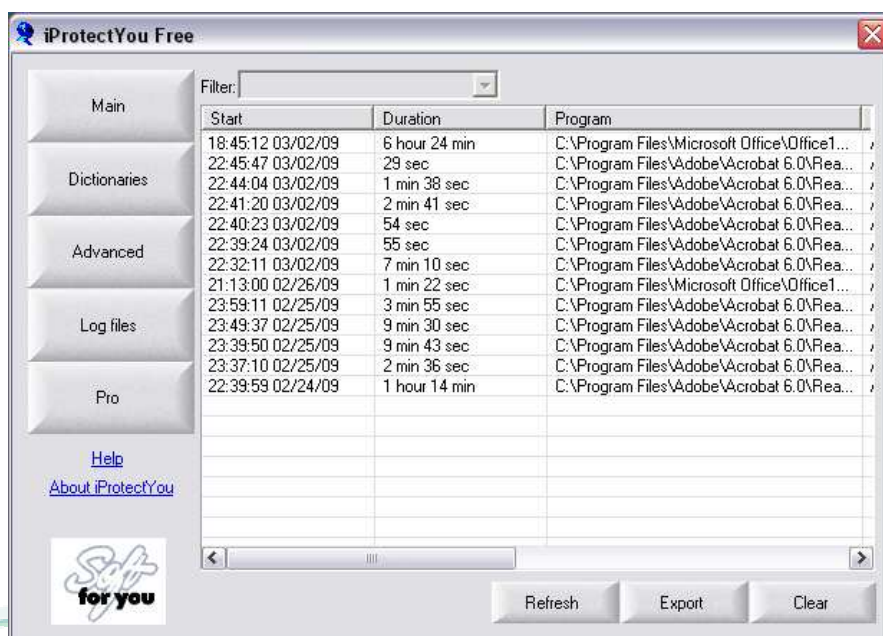


Εικόνα 28

Υποενότητα Activity

Η οθόνη που αντιστοιχεί στην παρούσα υποενότητα (Εικόνα 29) επιτρέπει στον Γονέα να πληροφορηθεί σχετικά με την δραστηριότητα των εφαρμογών οι οποίες εκτελέστηκαν στο εκάστοτε Υπολογιστικό Σύστημα κατά το διάστημα χρήσης του από το Παιδί του. Πιο συγκεκριμένα, ο Γονέας μπορεί να δει το πότε το Παιδί του ξεκίνησε μια συγκεκριμένη εφαρμογή, για πόση ώρα την χρησιμοποίησε καθώς και την ποσότητα των δεδομένων την οποία αυτή αντάλλαξε μέσω του Διαδικτύου. Παράλληλα, ο Γονέας μπορεί

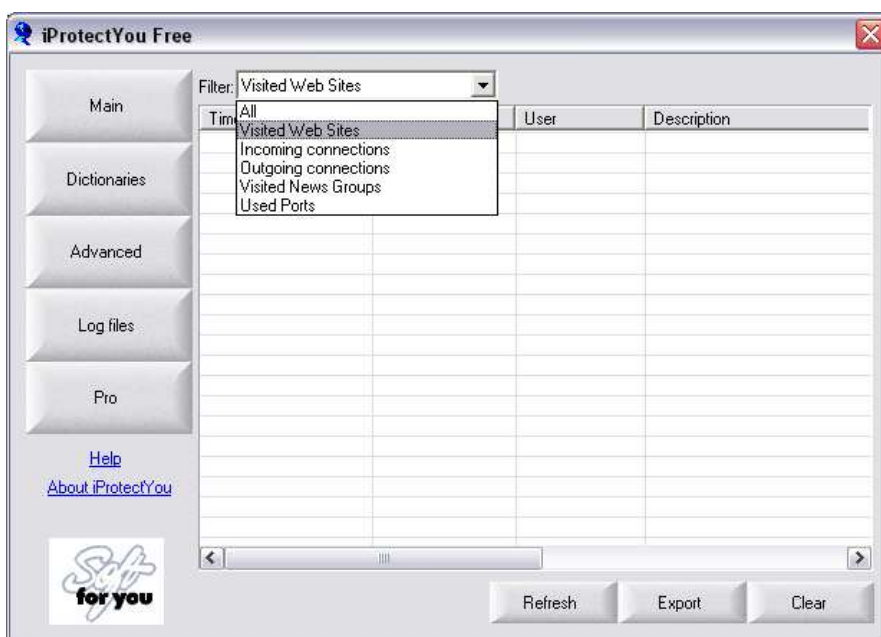
να δει το πλήρες μονοπάτι και όνομα της εκάστοτε εφαρμογής ώστε να την ελέγξει και, αν επιθυμεί, να τις απαγορεύσει την εκτέλεση ακολουθώντας βήματα τα οποία έχουμε ήδη περιγράψει σε προηγούμενες ενότητες. Οι καταχωρήσεις του Grid Πίνακα της Εικόνας 29 δύνανται είτε να Ανανεωθούν ή να Αποθηκευθούν σε Εξωτερικό Αρχείο ή να Διαγραφούν απλά πιέζοντας τα πλήκτρα "Refresh", "Export" και "Clear" αντίστοιχα.



Εικόνα 29

Υποενότητα Details

Η οθόνη που αντιστοιχεί στην παρούσα υποενότητα (Εικόνα 30) επιτρέπει στον Γονέα να πληροφορηθεί σχετικά με την Διαδικτυακή κίνηση η οποία παρατηρήθηκε στο εκάστοτε Υπολογιστικό Σύστημα κατά το διάστημα χρήσης του από το Παιδί. Πιο συγκεκριμένα, ο Γονέας μπορεί να δει ποιος χρήστης επισκέφθηκε μια Ιστοσελίδα, για πόση ώρα παρέμεινε σε αυτήν, καθώς και μια σύντομη περιγραφή αυτής. Ο Γονέας, επίσης, μπορεί χρησιμοποιώντας την λίστα με όνομα Filter να επιλέξει το ποια ομάδα κίνησης επιθυμεί να τυπώνεται στον αντίστοιχο Grid Πίνακα, έτσι ώστε να μην χάνεται στο πλήθος των καταχωρήσεων και να εντοπίζει γρηγορότερα αυτό που θέλει. Οι καταχωρήσεις του Grid Πίνακα της Εικόνας 30 δύνανται είτε να Ανανεωθούν ή να Αποθηκευθούν σε Εξωτερικό Αρχείο ή να Διαγραφούν απλά πιέζοντας τα πλήκτρα "Refresh", "Export" και "Clear" αντίστοιχα.



Εικόνα 30

Υποενότητα Blocked Ads

Για τον ίδιο λόγο όπου δεν αναλύσαμε περαιτέρω τις οθόνες που αντιστοιχούσαν στην συγκεκριμένη υποενότητα ρυθμίσεων σε προηγούμενες σελίδες του παρόντος εγχειριδίου, και εδώ θα αποφύγουμε να αναλύσουμε περισσότερο την συγκεκριμένη επιλογή.

Επίλογος

Κάθε φορά που η εφαρμογή "iProtectYou" θα εντοπίζει ότι το περιεχόμενο στο οποίο εκτίθεται ένας χρήστης είναι ακατάλληλο, θα εμφανίζεται στην οθόνη ένα από τα παρακάτω γραφικά (Εικόνα 31).





Εικόνα 31

Ταυτόχρονα, η σύνδεση της εφαρμογής η οποία πυροδότησε την εκάστοτε προειδοποίηση με το Διαδίκτυο θα αποκλείεται ώστε ο χρήστης να προστατευθεί. Για να εξαφανιστεί το εκάστοτε παράθυρο προειδοποίησης αρκεί να πιεστεί το πλήκτρο (x) στο πάνω δεξιό μέρος αυτού.

