

ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΑΣΦΑΛΕΙΑ



Λίγα λόγια...

Η ερευνητική εργασία ξεκίνησε αρκετά αργά. Οι μαθητές χωρίστηκαν σε τέσσερις ομάδες:

ΟΜΑΔΑ Α

Μεταλλίδου Ιωάννα
Μαστραντώνη Ευβουλία
Κοκολάκης Γεώργιος
Σπανέλης Ευάγγελος

ΟΜΑΔΑ Β

Φακούδης Ευάγγελος
Σιώτης Ευάγγελος
Παπαδόπουλος Οδυσσέας
Αναστασόπουλος Παναγιώτης

ΟΜΑΔΑ Γ

Γερογιάννη Ιωάννα
Ρίζος Νικόλαος
Αποστολάκης Σαράντης
Αγγελόπουλος Αριστείδης

ΟΜΑΔΑ Δ

Βελή Αικατερίνη
Ευαγγελάτος Παναγιώτης
Βούρδα Χρυσούλα
Θεοδώρου Αθηνά
Γρηγορίου Ελευθερία

Οι ομάδες αρχικά συνεργάστηκαν για την σχεδίαση του ερωτηματολογίου και στη συνέχεια συμπλήρωσαν το ερωτηματολόγιο, χρησιμοποιώντας τους συμμαθητές τους. Συνολικά ερωτήθηκαν 152 αγόρια και 162 κορίτσια, δηλαδή 314 άτομα. Οι ίδιοι δεν συμμετείχαν στην έρευνα. Κατόπιν όλες οι ομάδες συνεργάστηκαν για να εντοπίσουν τους πιθανούς κινδύνους από τη χρήση του Διαδικτύου. Μετά την καταγραφή:

Η Ομάδα Α ανέλαβε να ερευνήσει για Εθισμό, ψυχικούς και σωματικούς κινδύνους καθώς και την τάση για καταναλωτισμό.

Η Ομάδα Β ανέλαβε να ερευνήσει για κλοπή προσωπικών δεδομένων, κλοπή πνευματικής ιδιοκτησίας καθώς και για τη βία στο Διαδίκτυο.

Η Ομάδα Γ ανέλαβε να ερευνήσει για παραπληροφόρηση, σεξουαλική παρενόχληση, παιδοφιλία στο Διαδίκτυο καθώς και πρόσβαση σε ιστοσελίδες με παράνομο περιεχόμενο.

Η Ομάδα Δ ανέλαβε να ερευνήσει για κινδύνους στον Υπολογιστή, ιούς καθώς και υψηλές χρεώσεις.

Τα αποτελέσματα των ερευνών είναι στα χέρια σας.

Ελπίζω να είσαστε επεικειές, αφενός γιατί είναι η πρώτη επαφή των μαθητών με την έρευνα και αφετέρου γιατί ξεκίνησαν αρκετά αργά.

Ο υπεύθυνος για την έρευνα
Παπαντωνίου Μιχαήλ

Στην έρευνα οι μαθητές απαντούσαν ελεύθερα, χωρίς να έχουν πρόσβαση στο ερωτηματολόγιο.

5ο ΓΕ.Λ. ΙΛΙΟΥ

ΛΟΓΟΙ ΧΡΗΣΗΣ ΔΙΑΔΙΚΤΥΟΥ (INTERNET)

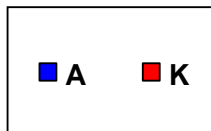
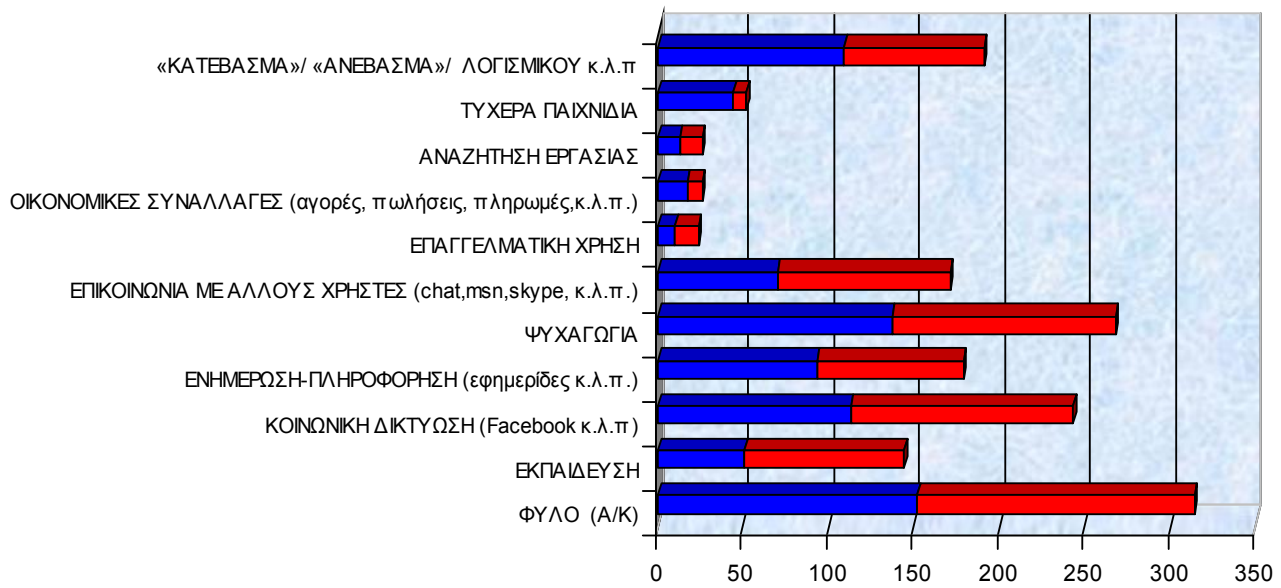
			ΠΟΣΟΣΤΑ		ΣΥΝΟΛΑ	ΣΥΝΟΛΙΚΟ ΠΟΣΟΣΤΟ
	Α	Κ	Α	Κ		
ΦΥΛΟ (Α/Κ)	152	162			314	
	51	93				
ΕΚΠΑΙΔΕΥΣΗ			33,55%	57,41%	144	45,86%
ΚΟΙΝΩΝΙΚΗ ΔΙΚΤΥΩΣΗ (Facebook κ.λ.π)	113	130	74,34%	80,25%	243	77,39%
ΕΝΗΜΕΡΩΣΗ-ΠΛΗΡΟΦΟΡΗΣΗ (εφημερίδες κ.λ.π.)	93	86	61,18%	53,09%	179	57,01%
	137	131				
ΨΥΧΑΓΩΓΙΑ			90,13%	80,86%	268	85,35%
ΕΠΙΚΟΙΝΩΝΙΑ ΜΕ ΑΛΛΟΥΣ ΧΡΗΣΤΕΣ (chat,msn,skype, κ.λ.π.)	70	101	46,05%	62,35%	171	54,46%
	10	14				
ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΧΡΗΣΗ			6,58%	8,64%	24	7,64%
ΟΙΚΟΝΟΜΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ (αγορές, πωλήσεις, πληρωμές,κ.λ.π.)	17	9	11,18%	5,56%	26	8,28%
ΑΝΑΖΗΤΗΣΗ ΕΡΓΑΣΙΑΣ	13	13	8,55%	8,02%	26	8,28%
	44	8				
ΤΥΧΕΡΑ ΠΑΙΧΝΙΔΙΑ			28,95%	4,94%	52	16,56%
	109	82				
«ΚΑΤΕΒΑΣΜΑ»/ «ΑΝΕΒΑΣΜΑ»/ ΛΟΓΙΣΜΙΚΟΥ κ.λ.π			71,71%	50,62%	191	60,83%

ΩΡΕΣ ΗΜΕΡΗΣΙΑΣ ΧΡΗΣΗΣ ΔΙΑΔΙΚΤΥΟΥ (INTERNET)

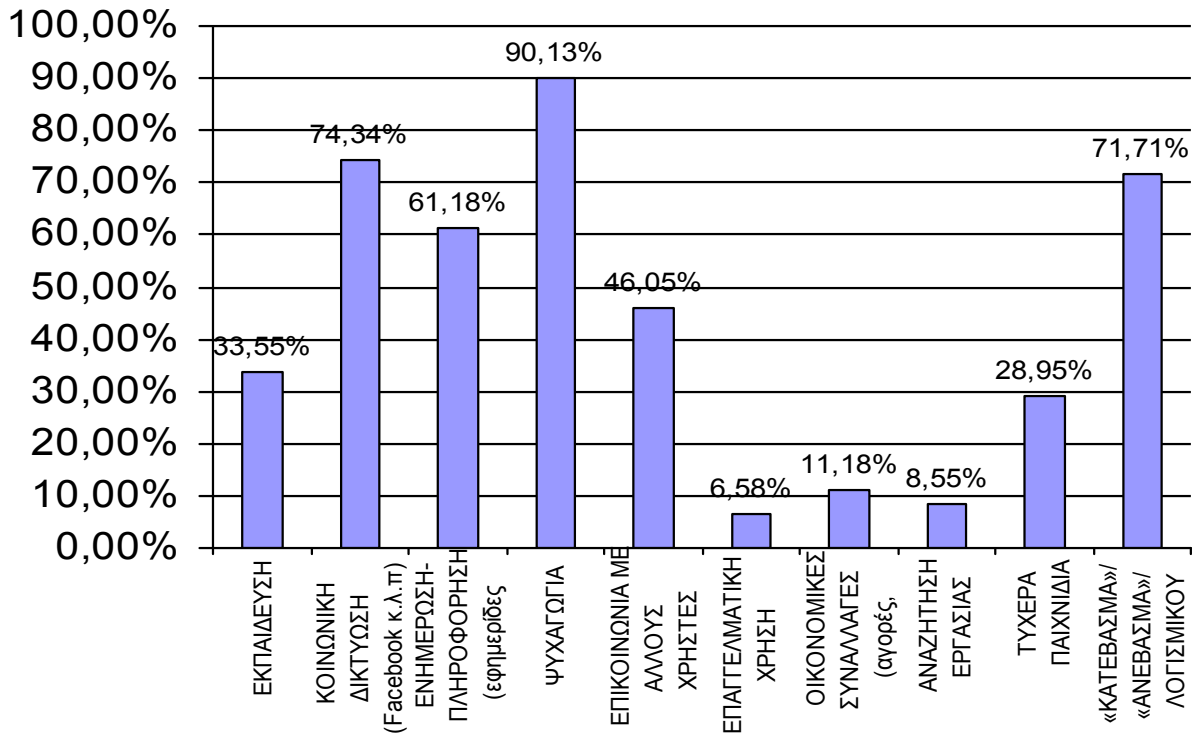
ΦΥΛΟ (Α/Κ)	Α	Κ	ΠΟΣΟΣΤΑ		ΣΥΝΟΛΑ	ΣΥΝΟΛΙΚΑ ΠΟΣΟΣΤΑ
			Α	Κ		
	152	162			314	
Α (ΚΑΘΟΛΟΥ)	3	4	1,97%	2,47%	7	2,23%
Β (1 ΜΕΧΡΙ 2 ΩΡΕΣ)	59	92	38,82%	56,79%	151	48,09%
Γ (2 ΜΕΧΡΙ 4 ΩΡΕΣ)	53	44	34,87%	27,16%	97	30,89%
Δ (4 ΜΕΧΡΙ 6 ΩΡΕΣ)	13	16	8,55%	9,88%	29	9,24%
Ε (ΠΑΝΩ ΑΠΟ 6 ΩΡΕΣ)	24	6	15,79%	3,70%	30	9,55%

ΠΑΡΑΤΗΡΗΣΗ ΕΚΠΛΗΞΗ: Ποσοστό 15,79% στα αγόρια και συνολικά 9,55% ασχολείται με το διαδίκτυο πάνω από 6 ώρες την ημέρα. Εντυπωσιακά υψηλό ποσοστό που σημαίνει εθισμό!

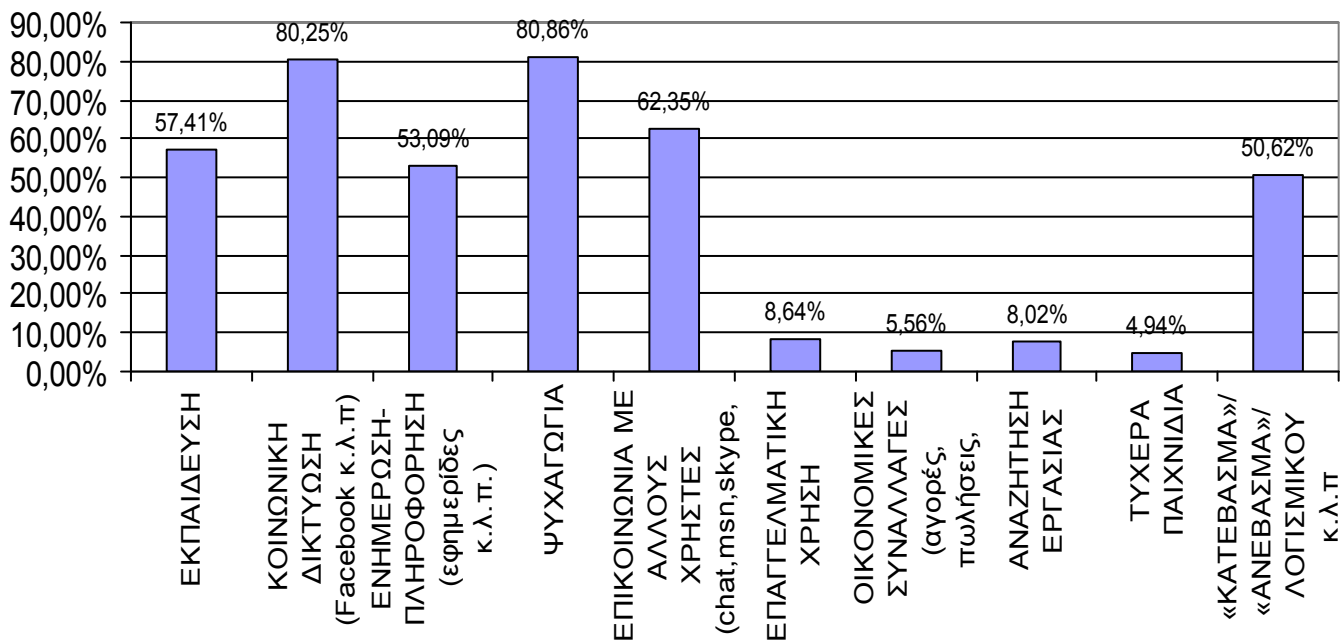
ΛΟΓΟΙ ΧΡΗΣΗΣ ΔΙΑΔΙΚΤΥΟΥ



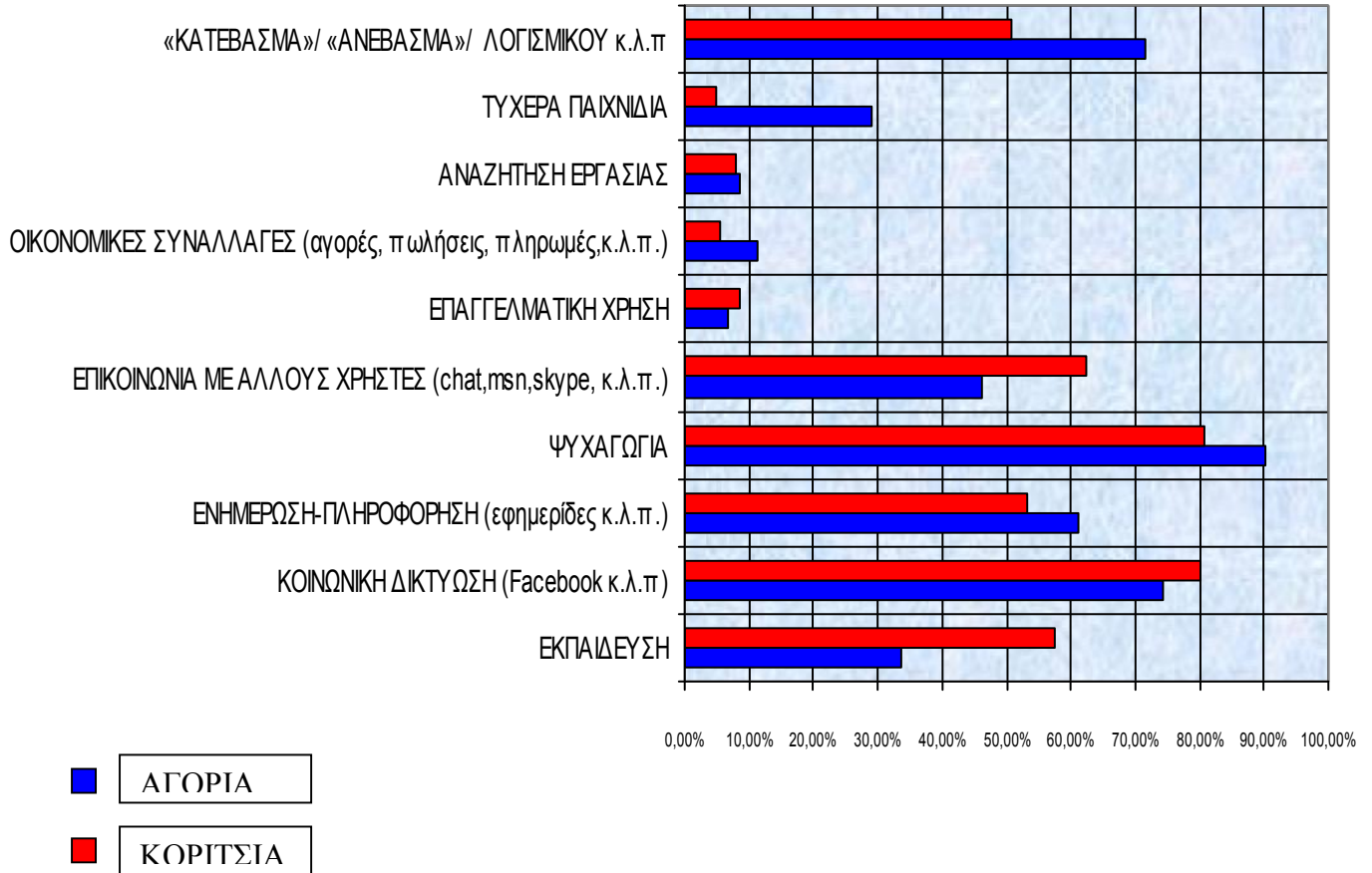
ΑΓΟΡΙΑ



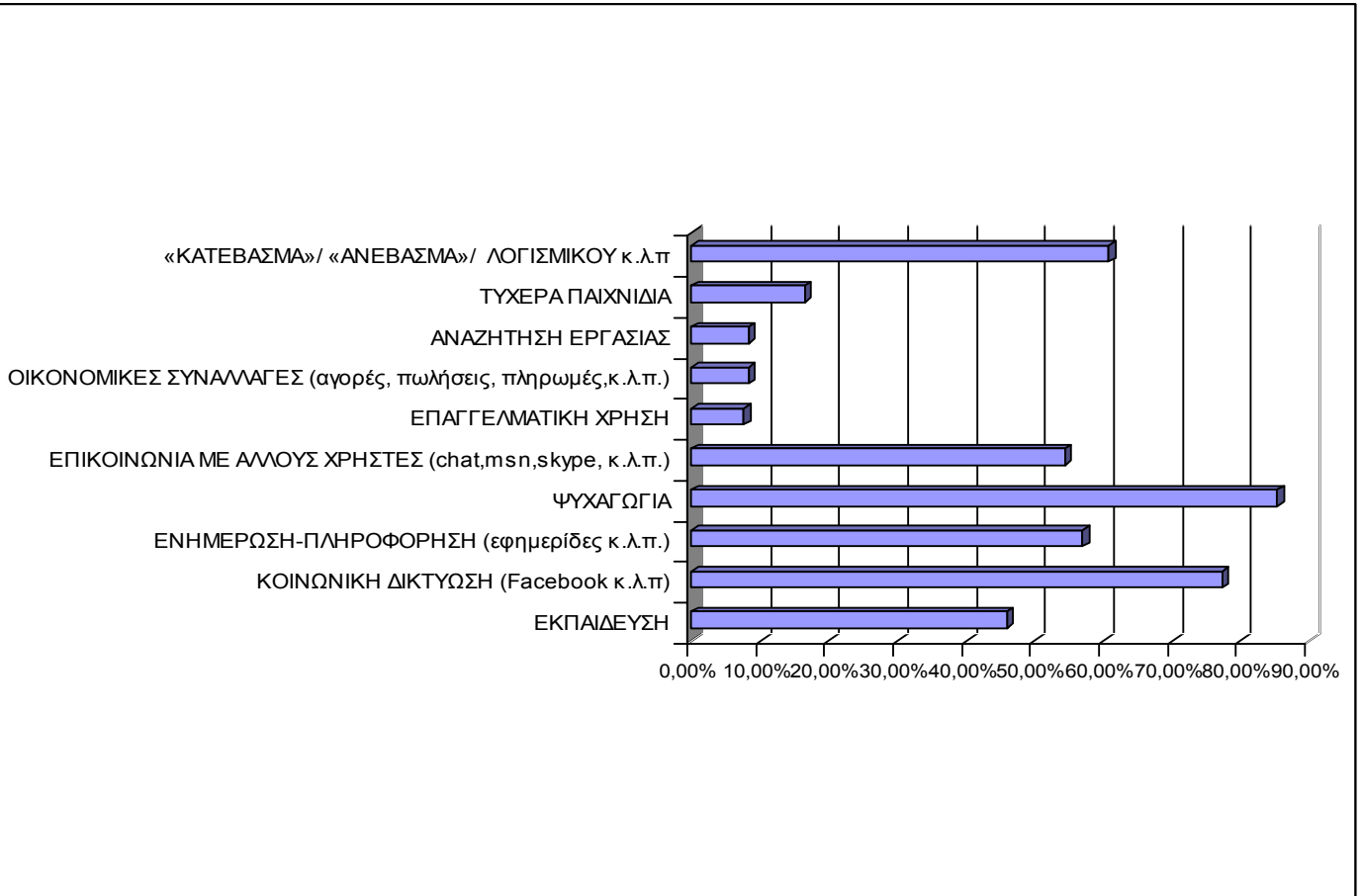
ΚΟΡΙΤΣΙΑ



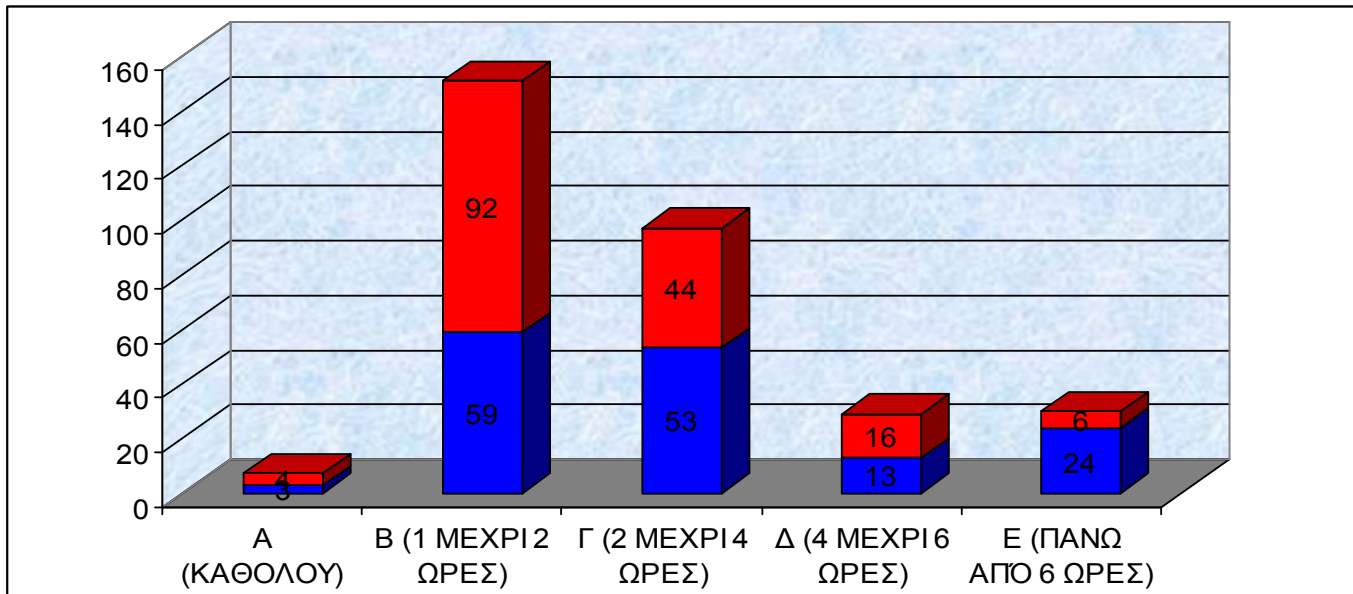
ΠΟΣΟΣΤΑ ΑΓΟΡΙΩΝ-ΚΟΡΙΤΣΙΩΝ



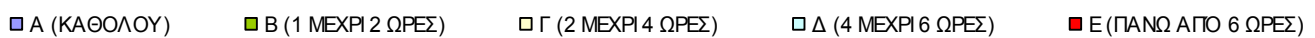
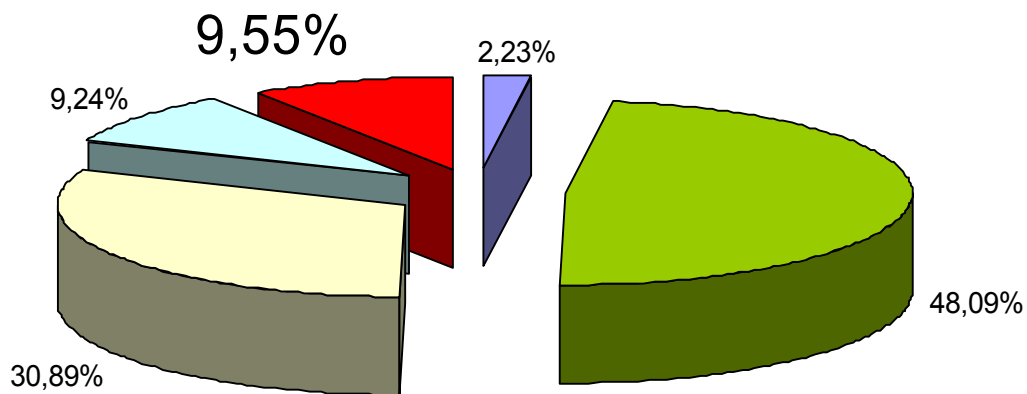
ΣΥΝΟΛΙΚΑ ΠΟΣΟΣΤΑ



ΩΡΕΣ ΧΡΗΣΗΣ ΔΙΑΔΙΚΤΥΟΥ ΑΝΑ ΦΥΛΟ



ΩΡΕΣ ΧΡΗΣΗΣ (ΣΥΝΟΛΙΚΑ ΠΟΣΟΣΤΑ)



ΚΙΝΔΥΝΟΙ ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ (INTERNET)



1. ΨΥΧΙΚΟΙ ΚΑΙ ΣΩΜΑΤΙΚΟΙ ΚΙΝΔΥΝΟΙ.
2. ΕΞΑΠΑΤΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
3. ΒΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
4. ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗ.
5. ΜΟΛΥΝΣΗ ΤΟΥ Η/Υ ΜΕ ΚΑΠΟΙΟ ΙΟ(VIRUS).
6. ΥΨΗΛΕΣ ΧΡΕΩΣΕΙΣ.

1) ΨΥΧΙΚΟΙ ΚΑΙ ΣΩΜΑΤΙΚΟΙ ΚΙΝΔΥΝΟΙ.

Η εξάπλωση των ηλεκτρονικών υπολογιστών, ιδιαίτερα μετά την απελευθέρωση και την ευρεία χρήση του Internet, φαίνεται πως δημιουργεί αυξητικές τάσεις στα προβλήματα υγείας του χρήστη που κρύβονται πίσω από την χωρίς κανόνες και συχνά αλόγιστη χρήση τους.

Η μελέτη αυτή εστιάζει στα προβλήματα υγείας, ψυχικής και σωματικής του χρήστη ηλεκτρονικού υπολογιστή και Internet. Ως τέτοια έχουν αναφερθεί:

- ✓ ΤΟ ΑΓΧΟΣ-ΦΟΒΟΣ ΓΙΑ ΤΟΥΣ Η/Υ
- ✓ ΤΟ ΣΥΝΔΡΟΜΟ ΤΟΥ ΚΑΡΤΣΙΑΙΟΥ ΣΩΛΗΝΑ
- ✓ ΤΟ ΣΥΝΔΡΟΜΟ ΤΗΣ ΟΘΟΝΗΣ
- ✓ ΟΘΟΝΕΣ ΚΑΙ ΑΚΤΙΝΟΒΟΛΙΕΣ
- ✓ Η ΦΩΤΟΕΠΙΛΗΨΙΑ
- ✓ ΟΙ ΚΙΝΔΥΝΟΙ ΑΠΟ ΤΑ ΥΛΙΚΑ ΚΑΤΑΣΚΕΥΗΣ
- ✓ ΠΑΡΑΜΕΛΗΣΗ ΕΡΓΑΣΙΩΝ. ΑΠΟΚΟΠΗ ΑΠΟ ΔΗΜΙΟΥΡΓΙΚΕΣ ΑΠΑΣΧΟΛΗΣΕΙΣ
- ✓ ΔΙΑΤΑΡΑΧΗ ΣΧΕΣΕΩΝ ΜΕ ΓΟΝΕΙΣ, ΦΙΛΟΥΣ ΚΑΙ ΤΟ ΑΛΛΟ ΦΥΛΟ
- ✓ ΚΟΙΝΩΝΙΚΗ ΑΠΟΜΟΝΩΣΗ
- ✓ Η ΕΙΚΟΝΙΚΗ ΖΩΗ ΜΠΕΡΔΕΥΕΤΑΙ ΜΕ ΤΗ ΠΡΑΓΜΑΤΙΚΗ

Με τους περισσότερους από εμάς να χρησιμοποιούν καθημερινά τον υπολογιστή σαν βασικό εργαλείο της δουλειάς, αλλά και στον ελεύθερο χρόνο, δεν αποτελεί και έκπληξη ότι η ένταση και η κούραση των ματιών, είναι το κύριο παράπονο της ημέρας. Οι παρακάτω 10 τρόποι, όμως, μπορούν να σας βοηθήσουν να μειώσετε το ενοχλητικό συναίσθημα κούρασης που αισθάνεστε στα μάτια σας, αλλά και τα περισσότερα συμπτώματα του... συνδρόμου των υπολογιστών.

1. Κάντε μια εξέταση ματιών



2. Χρησιμοποιείτε σωστό φωτισμό

3. Ελαχιστοποιήστε τις αντανάκλασεις και τις λάμπες

4. Αναβαθμίστε την οθόνη σας

Αν πρόκειται να αγοράσετε μια καινούργια LCD οθόνη, επιλέξτε αυτή με την υψηλότερη ανάλυση και όσο το δυνατόν μεγαλύτερο μέγεθος (από 19 ίντσες και πάνω).

5. Κάντε τις κατάλληλες ρυθμίσεις στην οθόνη

6. Ανοίγοκλείνετε συχνά τα μάτια σας

7. Εφαρμόστε τρικ ξεκούρασης

Κοιτάξτε μακριά ένα αντικείμενο για 10-15 δευτερόλεπτα κι έπειτα κοιτάξτε ένα άλλο αντικείμενο που βρίσκεται πιο κοντά, για άλλα 10-15 δευτερόλεπτα.

8. Κάντε συχνά διαλείμματα

9. Φορέστε γυαλιά που σας ξεκουράζουν

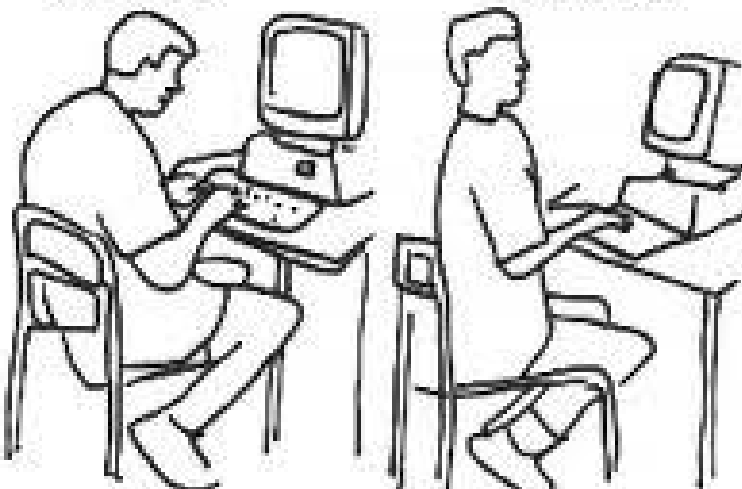
10. Διατηρήστε σωστή στάση σώματος

Μια κακή στάση σώματος στο γραφείο μπροστά στον υπολογιστή, θα πλήξει σίγουρα τη μέση σας, τον αυχένα σας, αλλά και τα μάτια σας. Καταρχάς αγοράστε εργονομικά έπιπλα, που εξασφαλίζουν ότι η οθόνη βρίσκεται περίπου 50-60 εκατοστά μακριά από τα μάτια σας και φροντίστε η γωνία που σχηματίζεται από τα μάτια σας και τις 2 κάτω άκρες της οθόνης να μην ξεπερνά τις 30ο.



ΛΑΘΟΣ

ΣΩΣΤΟ



ΧΡΗΣΗ-ΚΑΤΑΧΡΗΣΗ ΚΑΙ ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ



Ο εθισμός στο Διαδίκτυο (internet addiction) είναι μια σχετικά νέα μορφή εξάρτησης, η οποία βρίσκεται υπό εξέταση από την επιστημονική κοινότητα προκειμένου να οριοθετηθεί, αφού η εξάρτηση από το Ίντερνετ δεν είναι ακόμη μια κλινική οντότητα που συναντάμε σε εγχειρίδια ψυχιατρικά. Αυτή η μορφή εθισμού ορίζεται ως την «ενασχόληση με το Ίντερνετ για άντληση αισθήματος ικανοποίησης που συνοδεύεται με αύξηση του χρόνου που καταναλώνεται για την άντληση αυτού του αισθήματος».

Το Ίντερνετ έχει την ικανότητα να καλύψει συγκεκριμένες ψυχολογικές ανάγκες ενός ατόμου. Ένα από τα πιο χαρακτηριστικά παραδείγματα είναι η δημιουργία μιας «ιδανικής κατάστασης εαυτού», όπου το άτομο μπορεί να εξερευνήσει διάφορες πτυχές της προσωπικότητάς του χωρίς να έχει περιορισμούς και συνέπειες. Στο Διαδίκτυο δεν υπάρχουν άμεσες συνέπειες των πράξεων, αφού ο χρήστης μπορεί να μπει και να βγει όποτε θέλει, ενώ μπορεί να καλύψει και να τροποποιήσει την εξωτερική του εμφάνιση. Ταυτόχρονα, ο έφηβος μπορεί να ενσαρκώσει διαφορετικούς ρόλους, ή να υιοθετήσει διαφορετικές ταυτότητες ανάλογα με την εκάστοτε διαδικτυακή εμπειρία, εξαιτίας της ανωνυμίας, που συνιστά κατεξοχήν χαρακτηριστικό του Διαδικτύου. Το άτομο θα πρέπει να καταλάβει ότι ο εθισμός είναι ένας κρυφός κίνδυνος που δεν γίνεται άμεσα αντιληπτός, αλλά υπάρχει χωρίς να το γνωρίζουμε, λόγω της αλόγιστης χρήσης του. Μελέτες έχουν δείξει πως περισσότερο εθισμένα στο διαδίκτυο είναι τα αγόρια που μεγαλώνουν σε δύσκολες καταστάσεις (δυσλειτουργικές οικογένειες). Επίσης μεγάλο κίνδυνο διατρέχουν και τα άτομα που είναι ήδη εξαρτημένα από κάτι άλλο, όπως αλκοόλ, τσιγάρο, διαταραχές ελέγχου των παρορμήσεων και γενικά έλλειψη αυτοσυγκράτησης. Σύμφωνα με πρόσφατες έρευνες που έχουν το 1% των εφήβων είναι εθισμένοι στο διαδίκτυο, ενώ το 20% τείνει στο να εθιστεί.

Η υπερβολική χρήση του διαδικτύου μπορεί να οδηγήσει σε επιζήμια για το άτομο προβλήματα, όπως κατάθλιψη, κοινωνική φοβία, υπερκινητικότητα, αγχώδεις διαταραχές και ραγδαίες μεταβολές στην προσωπικότητα του ατόμου.

Οι συνηθέστερες ενδείξεις που θα πρέπει να μας θορυβήσουν σχετικά με τη χρήση του Διαδικτύου είναι οι εξής:

- Υπερβολική κούραση, ημερήσια υπνηλία.

- Πτώση της σχολικής επίδοσης απότομη ή σταδιακή.
- Παραμέληση ή διακοπή άλλων αγαπημένων δραστηριοτήτων.
- Κοινωνική απόσυρση.
- Ανυπακοή, εκδραμάτση, ευερεθιστότητα.

Παιδιά που παρουσιάζουν τρεις ή περισσότερες από τις παραπάνω ενδείξεις, ενδεχομένως αντιμετωπίζουν πρόβλημα εθισμού στο Διαδίκτυο. Πρέπει να σημειωθεί όμως ότι τα παραπάνω σημεία δεν είναι ειδικά για τον εθισμό στο Διαδίκτυο και μπορεί να αποτελούν ενδείξεις κάποιας άλλης ψυχικής διαταραχής, κατάχρησης αλκοόλ ή κάποιας άλλης ψυχοδραστικής ουσίας.

Βασικές αρχές αυτοβοήθειας για την ανάκτηση του αυτοελέγχου στο χρόνο χρήση του διαδικτύου

η επίγνωση από την πλευρά του, του χρόνου που αφιερώνει συνδεδεμένος με το διαδίκτυο καθώς και το είδος της δραστηριότητας που εκείνος επιλέγει, θα τον βοηθήσουν σε μια πιο ορθολογική χρήση κυρίως μέσω της αυτοπαρατήρησης και της αυτορύθμισης της διαδικτυακής του συμπεριφοράς.

Ο χρήστης κατακτά την ικανότητα, να διαχειρίζεται και να ελέγχει το χρόνο χρήσης του υπολογιστή με τη βοήθεια τεσσάρων διαφορετικών προσεγγίσεων. Ανάλογα με το ποια προσέγγιση ταιριάζει και αποδίδει καλύτερα για τον κάθε χρήστη μπορεί να χρησιμοποιηθεί μια από αυτές, και οι τέσσερις ή κάποιος συνδυασμός αυτών:

Καλλιέργεια εναλλακτικών ψυχαγωγικών δραστηριοτήτων. Ενθαρρύνεται ο χρήστης, να ξεκινήσει κάποια ευχάριστη ενασχόληση. Η εισαγωγή ευχάριστων δραστηριοτήτων στην καθημερινότητα τον αποσπά από την αδιάκοπη και σχεδόν καταναγκαστική χρήση του υπολογιστή.

Αναγνώριση του πρότυπου χρήσης του υπολογιστή και εφαρμογή ενός διαμετρικά αντίθετου προγράμματος χρήσης. Για παράδειγμα ο χρήστης, που αναλώνει πολλές ώρες τα Σαββατοκύριακα σερφάροντας στο διαδίκτυο, αλλά δεν συνδέεται τις καθημερινές, εφαρμόζει για κάποιο διάστημα ακριβώς το αντίθετο. Αλλάζοντας τις συνήθειες, που αφορούν τη χρήση του υπολογιστή, αποκτά σιγά- σιγά τον έλεγχό τους.

Χρήση εξωτερικών περιορισμών. Οι καθημερινές και σταθερές υποχρεώσεις της καθημερινότητας, όπως π.χ. να πάει κανείς στην εργασία του, χρησιμοποιούνται ως σηματοδότες, που αναγκάζουν το χρήστη να σταματήσει τη χρήση του υπολογιστή. Έτσι ο χρόνος που αναλώνει ο χρήστης γίνεται αυστηρά καθορισμένος. Εναλλακτικά, μπορεί να χρησιμοποιηθεί ένα ξυπνητήρι, που ειδοποιεί το χρήστη, ότι ο προκαθορισμένος χρόνος ενασχόλησης με τον υπολογιστή έληξε.

Ενσωμάτωση καθορισμένων περιόδων χρήσης στο εβδομαδιαίο πρόγραμμα του χρήστη. Η θέσπιση ενός σαφούς ορίου στο συνολικό χρόνο χρήσης και η εισαγωγή στο εβδομαδιαίο πρόγραμμα του χρήστη καθορισμών, συχνά και σύντομων περιόδων χρήσης θα τον βοηθήσουν, να αποκτήσει έναν καλύτερο έλεγχο του χρόνου, που αφιερώνει.



Ο ρόλος των γονέων είναι πολύ σημαντικός τόσο για την πρόληψη όσο και για την αντιμετώπιση του εθισμού. Οι γονείς θα πρέπει να είναι ενήμεροι για την δραστηριότητα των παιδιών τους στο διαδίκτυο και να βάζουν όρια στη χρήση του όσο το παιδί είναι ακόμα μικρό.

Απαραίτητη είναι και η εγκατάσταση κάποιων φίλτρων στον υπολογιστή έτσι ώστε να αποτραπεί η εμφάνιση ακατάλληλων περιεχομένων και ιών από άλλους κακόβουλους χρήστες. Για να γίνουν ωστόσο αυτά θα πρέπει οι γονείς να μπορούν να διαθέσουν τον απαραίτητο χρόνο, αφού είναι δύσκολο για ενοχικούς γονείς να θέσουν όρια. Η συζήτηση είναι το κύριο μέσο επικοινωνίας και κατανοήσεις των κινδύνων που υπάρχουν από τα παιδιά. Ωστόσο είναι απαραίτητο και οι δύο γονείς να τηρούν μια ενιαία στάση στον τρόπο που αντιμετωπίζουν τα παιδιά. Τα επιχειρήματα δεν θα πρέπει να λείπουν και θα πρέπει να είναι σε θέση να αντιμετωπίσουν την αρνητική στάση των παιδιών με νέα επιχειρήματα. Σε πιο πρακτικό επίπεδο, ο υπολογιστής είναι καλό να βρίσκεται σε κοινόχρηστο χώρο και όχι στο δωμάτιο του παιδιού, ώστε να ελέγχεται διακριτικά η δραστηριότητα του παιδιού. Από την άλλη πλευρά εάν ο εθισμός δεν μπορεί να αντιμετωπιστεί η οικογένεια θα πρέπει να στραφεί σε κάποιον εξειδικευμένο ψυχίατρο. Ο εθισμός από το διαδίκτυο αναγνωρίζεται πια από την ψυχιατρική κοινότητα ως ξεχωριστή ψυχοσωματική διαταραχή γι' αυτό χρήζει ειδικής θεραπείας.

ΥΠΕΡΚΑΤΑΝΑΛΩΣΗ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

Με τον όρο υπερκατανάλωση εννοούμε την ανάγκη των ανθρώπων να αγοράζουν αγαθά. Ο σκοπός τους είναι, πρώτον να αποκτήσουν όσο το δυνατόν περισσότερα αγαθά μπορούν ανεξάρτητα από τις πραγματικές τους ανάγκες. Δεύτερον, να καλύψουν το εσωτερικό τους κενό και τέλος η παραγωγή μεγάλων ποσοτήτων για την κάλυψη φανταστικών αναγκών.

Πολλοί άνθρωποι, θέλοντας να κρύψουν ορισμένα από τα προβλήματα τους, "το ρίχνουν" στον καταναλωτισμό προκειμένου να αισθανθούν καλύτερα και να προβάλλουν έναν άλλον εαυτό. Ωστόσο, στις μέρες μας "κρίνεσαι" και από τον τρόπο που ντύνεσαι καθώς και από τα προϊόντα και έτσι θέλεις να δείξεις πως είσαι μοντέρνος και ακολουθείς κατά γράμμα την μόδα και την τεχνολογία.

Επιπλέον, κυρίως ο έφηβος, περνάει πολλές ώρες σερφάροντας στο διαδίκτυο. Όπως παντού, έτσι και εκεί, σχεδόν σε όλα τα sites υπάρχουν διαφημίσεις, οι οποίες σε προκαλούν να αγοράσεις προϊόντα που στην ουσία είναι τελείως άχρηστα. Έτσι, το διαδίκτυο συμβάλει στον υπερκαταναλωτισμό του εφήβου κάνοντας τον πιο άπληστο. Εκτός όμως από τις διαφημίσεις, υπάρχουν και ορισμένες σελίδες, οι οποίες έχουν επώνυμα και ακριβά προϊόντα σε εξαιρετικά οικονομικές τιμές. Τέλος, κάνοντας παραγγελίες μέσω του internet σε ορισμένα καταστήματα έχεις μια μικρή αλλά ικανοποιητική έκπτωση.



ΑΙΤΙΕΣ ΥΠΕΡΚΑΤΑΝΑΛΩΤΙΣΜΟΥ

- ✓ Ανάπτυξη επιστήμης και τεχνολογίας
- ✓ Υπερπαραγωγή
- ✓ Καταναλωτική εποχή-υψηλές ανάγκες εποχής
- ✓ Άνοδος βιοτικού επιπέδου
- ✓ Γρήγορος ρυθμός ζωής
- ✓ Σύγχρονος τρόπος ζωής
- ✓ Ψυχολογικά προβλήματα
- ✓ Μόδα και τάση προβολής
- ✓ Διαφημίσεις
- ✓ Ελκυστικές προσφορές
- ✓ Εύκολος τρόπος πληρωμής (δόσεις, πιστωτικές κάρτες)
- ✓ Μιμητισμός
- ✓ Κενή ζωή

Πώς ένα άτομο, όμως καταλαβαίνει πως έχει υπερκαταναλωτική συμπεριφορά;

Όταν δε νιώθει καλά, έχει τάση για αγορές

Δεν μπορεί να ζήσει χωρίς τις πιστωτικές του

Κατά την διάρκεια των αγορών του αισθάνεται ευτυχισμένος ενώ στην συνέχεια νιώθει τύψεις και ενοχές

Λέει ψέματα για τις αγορές που έκανε και για τα χρήματα που ξόδεψε

Έχει προβλήματα με το οικείο περιβάλλον του λόγω αυτής της συνήθειας
Κρύβει αυτό του το πρόβλημα
Είναι προσκολλημένος στο διαδίκτυο μεγάλο χρονικό διάστημα της ημέρας προσπαθώντας να βρεί υλικά αγαθά που θα ικανοποιήσουν τις πραγματικές αλλά και τις φανταστικές του ανάγκες



Τρόποι αντιμετώπισης του είναι:

Κάθε άτομο που έχει τάση υπερκατανάλωσης, πρέπει να συνειδητοποιήσει το πρόβλημά του και να προσπαθήσει να το αντιμετωπίσει
Επίσης, θα πρέπει να κρίνονται σωστά οι διαφημίσεις και να μην παρασυρόμαστε από τα προϊόντα που παρουσιάζουν
Επιπλέον, θα πρέπει να υπάρχει νομοθετική ρύθμιση διαφημιστικών μηνυμάτων έτσι ώστε να προστατεύονται οι καταναλωτές
Καθένας πρέπει να καλλιεργήσει τις ηθικές του αξίες και να μην επηρεάζεται από μια καλοστημένη διαφήμιση
Θα πρέπει να έχει αυτογνωσία και να γνωρίζει τις πραγματικές του ανάγκες
Η σωστή αξιοποίηση του ελεύθερου χρόνου παίζει ουσιαστικό ρόλο στην αντιμετώπιση του προβλήματος.
Ένα άλλο που πρέπει να αλλάξει είναι η νοοτροπία του ατόμου και ο τρόπος σκέψης του
Καλό θα ήταν να δίνεται περισσότερη σημασία στην ποιότητα και όχι τόσο στη ποσότητα των πραγμάτων που αγοράζονται
Τέλος, η αξιολόγηση των πραγματικών αναγκών είναι ουσιαστικής σημασίας

2) ΕΞΑΠΑΤΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Στο Internet, υπάρχει ένας ανησυχητικά μεγάλος αριθμός ιστοσελίδων, που υποδύονται γνωστά καταστήματα, ενώ στην πραγματικότητα δεν είναι, και δυστυχώς, όλο και πληθαίνουν. Ισχυρίζονται πως προσφέρουν ασφάλεια στην συναλλαγή που θα κάνει ο πελάτης, άμα παραλάβουν τα χρήματα, δεν στέλνουν το προϊόν, η άμα στείλουν, δεν θα είναι το αυθεντικό. Έτσι καταλήγουν να έχουν και προσωπικές σας πληροφορίες, και να έχουν αποσπάσει ένα ποσό χρημάτων από εσάς.

Περιπτώσεις απατηλών συναλλαγών πώλησης ή αγοράς είναι:

Αγορές μέσω διαδικτύου, όπου τα προς πώληση προϊόντα έχουν πολύ χαμηλές τιμές. Συνήθως, απαιτείται η προκαταβολή όλου του ποσού ή ενός μέρους του για τη γρήγορη αποστολή της παραγγελίας. Όταν το θύμα καταβάλλει το ποσό είτε δεν λαμβάνει ποτέ τα παραγγελθέντα προϊόντα είτε παραλαμβάνει κατώτερης αξίας και ποιότητας από τα συμφωνηθέντα...

Ειδική περίπτωση επισφαλών ηλεκτρονικών αγορών αποτελούν τα καταστήματα ηλεκτρονικού εμπορίου (e-shops). Πολλά e-shops στην Κίνα ανήκουν σε ιδιώτες, που αναζητούν ευκαιριακό κέρδος, και όχι σε οργανωμένες επιχειρήσεις.

Σύνηθες είναι, δε, το φαινόμενο να ζητούν τμηματικά διάφορα μικροποσά, χρησιμοποιώντας ως πρόφαση προβλήματα με το τελωνείο ή/και την εταιρεία ταχυμεταφορών, ή να πιέζουν τον πελάτη να καταβάλει επιπλέον χρήματα για να του δώσουν τις πληροφορίες αποστολής του προϊόντος ή τα συνοδευτικά έγγραφα που απαιτούνται για τον εκτελωνισμό του, ώστε να μπορέσει να το παραλάβει.



Κλοπή προσωπικών δεδομένων

Το πιο διαδεδομένο έγκλημα στο διαδίκτυο, και ίσως και το πιο εύκολο να πέσει θύμα κανείς. Τα δεδομένα που αποθηκεύουμε στα κοινωνικά δίκτυα, είτε δημόσια, είτε μόνο για προσωπική προβολή, μπορούν να τα πάρουν «Χάκερς», η να διαρρεύσουν σε ιστοσελίδες στο διαδίκτυο.

Η πιο γνωστή τεχνική κλοπής δεδομένων είναι το Phishing.

Όπως το ίδιο το όνομά του υπονοεί -παραλλαγή του αγγλικού «fishing» (ψάρεμα), το Phishing αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα.



Το Phishing επιχειρείται συνήθως με τη αποστολή κάποιου spam email. Τα email αυτά ισχυρίζονται ότι ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας, και τον οδηγούν μέσω συνδέσμων σε πλαστά web sites, τα οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών.



Αγορά-πώληση προσωπικών δεδομένων

Ιστοσελίδες κοινωνικής δικτύωσης, μπορούν ανά πάσα στιγμή να πουλήσουν στοιχεία σας (Από προσωπικά στοιχεία, μέχρι και φωτογραφίες) σε άλλες εταιρίες, η να τα χρησιμοποιήσουν για διαφημιστικούς σκοπούς, χωρίς να σας προειδοποιήσουν. Ουσιαστικά, κατά την εγγραφή σας στο δίκτυο αυτό, συμφωνείτε στους Όρους Χρήσης, που ένας από αυτούς, λέει ότι οτιδήποτε κοινοποιείτε, ανήκει σε αυτούς.

Παροχή ψευδών πληροφοριών

Στην κατηγορία αυτή υπάγονται περιπτώσεις παροχής ψευδών πληροφοριών από τον απατεώνα με στόχο τη διαστρέβλωση του κανονιστικού πλαισίου των συναλλαγών και την επίτευξη παράνομου κέρδους. Ο απατεώνας στηρίζεται, κατά κύριο λόγο, στην άγνοια ή ελλιπή πληροφόρηση του υποψήφιου θύματος σχετικά με τη νομοθεσία και τις πρακτικές των εμπορικών συναλλαγών είναι πολύ μικρή.

ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Απατηλές συναλλαγές στο διαδίκτυο

Το πιο σημαντικό πράμα που μπορούμε να κάνουμε, είναι να βεβαιωθούμε πως η ιστοσελίδα από την οποία αγοράζουμε είναι αυθεντική, και όχι κάποια απομίμησή της.

Κλοπή προσωπικών δεδομένων

Δεν είναι και πολύ δύσκολο να καταλάβουμε ποια εισερχόμενα Mail είναι ψεύτικα. Άμα είμαστε πιο υποψιασμένοι, και παρατηρούσαμε τις λεπτομέρειες των Mail, όλο και κάποιος λάθος θα βρούμε, που προσδίδει ότι είναι Phishing.

Αγορά-πώληση προσωπικών δεδομένων

Δυστυχώς, δεν υπάρχει κάτι που μπορούμε να κάνουμε εδώ... Αφού συμφωνούμε στους Όρους Χρήσης, έχουν το δικαίωμα οι διαχειριστές τις ιστοσελίδας να κάνουν ότι θέλουν τα προσωπικά δεδομένα μας.

Παροχή ψευδών πληροφοριών

Πρέπει να είμαστε σίγουροι για την εγκυρότητα των πληροφοριών που παίρνουμε από τις ιστοσελίδες. Άμα δεν είμαστε σίγουροι, και δεν εμπιστευόμαστε πλήρως την πηγή αυτή, δεν την χρησιμοποιούμε καν.

Κλοπή Προσωπικών δεδομένων ή Παραβίαση της Ιδιωτικής μας ζωής



Γνωρίζετε πως όταν δημιουργήσουμε ένα λογαριασμό στο Facebook εξ ορισμού όλοι οι χρήστες του Facebook έχουν πρόσβαση σε ότι πληροφορίες, δεδομένα ανεβάσουμε πάνω στο λογαριασμό μας; Μήπως γνωρίζετε για ποιον αριθμό μιλάμε? ... οι χρήστες του Facebook ξεπερνούν τα 400 εκατομμύρια σε όλο τον κόσμο. Αυτό σημαίνει ότι αν εξαιρέσουμε τους φίλους σας περίπου 400 εκατομμύρια άσχετα άτομα με εσάς μπορούν αν το θελήσουν να εισβάλουν στον λογαριασμό σας, να πάρουν τις φωτογραφίες σας και να τις χρησιμοποιήσουν όπως θέλουν αυτοί... Μπορούν επίσης να δουν πληροφορίες όπως για παράδειγμα το πού μένετε, πόσο χρονών είστε και τι κάνετε ανά πάσα στιγμή ... δεν σας τρομάζει αυτό?

Σκεφτείτε το διαφορετικά... Αν έρθει ένας άγνωστος στο δρόμο και σας ζητήσει να του δώσετε μια φωτογραφία σας ή σας ρωτήσει να του πείτε πού μένετε θα του πείτε? Με την ίδια λογική δεν τα το κάνατε ούτε στο Facebook.

Βεβαιωθείτε λοιπόν ότι στο εικονικό σας προφίλ έχουν πρόσβαση μόνο οι φίλοι σας! Τώρα για να δούμε ποιους θεωρούμε ηλεκτρονικούς μας φίλους... Κάντε λίγα μαθηματικά και σκεφτείτε πόσους φίλους έχετε στην πραγματική σας ζωή και πόσους φίλους έχετε στο Facebook! Σίγουρα ο αριθμός δεν είναι καθόλου ο ίδιος. Πολλοί έχουν την τάση να κάνουν add στο προφίλ τους άτομα τα οποία αν τα συναντούσαν στον δρόμο το πιο πιθανό ούτε γεια δεν θα τους έλεγαν! Μην κάνετε φίλους σας οποιονδήποτε σας κάνει "add request". Από την στιγμή που τον κάνετε φίλο σας αυτόματα έχει πρόσβαση στο προφίλ σας. Οι σχέσεις μεταξύ των ατόμων δεν αλλάζουν επειδή αλλάζει ο τρόπος επικοινωνίας. Στην περίπτωση όμως που αποφασίσετε να προσθέσετε στην λίστα των φίλων σας όλο τον

κόσμο που σας το ζητά, προσπαθήστε να μην ανεβάζετε πολύ προσωπικές φωτογραφίες και να μην γράφετε πολύ προσωπικά στοιχεία για σας. Πότε δεν ξέρετε αν κάποιος από τους «φίλους» σας, χρησιμοποιήσει κάποια φωτογραφία σας ή βίντεο, εναντίον σας με σκοπό να σας απομονώσει ή να σας βλάψει.

Επιπλέον η διαδικτυακή απάτη είναι ένα είδος κυβερνοεγκλήματος που πραγματοποιείται μέσω email, ιστοσελίδων, chat rooms ή Forums. Υπάρχουν διάφορα είδη τέτοιων δραστηριοτήτων, συμπεριλαμβανόμενων του phishing και του pharming, στις οποίες χρησιμοποιούνται πλαστά e-mail και ιστοσελίδες για να ξεγελάσουν τους αποδέκτες/επισκέπτες ώστε να αποκαλύψουν προσωπικά δεδομένα, όπως στοιχεία πιστωτικών καρτών και κωδικούς.

Για να αποφύγετε τέτοιες κακόβουλες πράξεις, προτείνονται τα ακόλουθα μέτρα κατά της διαδικτυακής απάτης:

Do's

1. Σκεφτείτε ενδεχομένως να απενεργοποιήσετε τη λειτουργία file sharing στον υπολογιστή σας.
2. Να «ανοίγετε» επισυναπτόμενα αρχεία με προσοχή, ιδίως όταν προέρχονται από άγνωστους αποστολείς.
3. Να εξοικειωθείτε με τις πολιτικές ασφαλείας των ιστοσελίδων, ιδίως όταν σας ζητούνται προσωπικά/ απόρρητα δεδομένα.
4. Να ελέγχετε τους αναλυτικούς λογαριασμούς των πιστωτικών σας καρτών.
5. Να κάνετε εγκατάσταση και συχνές ανανεώσεις προγραμμάτων ασφαλείας. Προτείνουμε το Norton Internet Security για ολοκληρωμένη προστασία.
6. Να διατηρείτε το λειτουργικό σας σύστημα ενημερωμένο όπως και όλες τις λειτουργίες του υπολογιστή σας με τα τελευταία security patches.
7. Να δημιουργείτε ισχυρούς κωδικούς και να τους προστατεύετε με προσοχή ή να χρησιμοποιείτε λογισμικό προστασίας προσωπικών κωδικών. Η λύση, Norton Confidential, κωδικοποιεί τους προσωπικούς σας κωδικούς για ασφαλή αποθήκευση, τους ελέγχει για μη εγκεκριμένη χρήση και σας ενημερώνει όταν μια ιστοσελίδα παρέχει υπηρεσίες ασφαλούς σύνδεσης.
8. Να «κλειδώνετε» το προσωπικό σας mailbox.
9. Να καταστρέψετε λογαριασμούς πιστωτικών καρτών και οικονομικά στοιχεία πριν τα πετάξετε.
10. Οι «δυνατοί» κωδικοί αποτελούνται από 8 χαρακτήρες και πάνω - περιλαμβάνουν έναν συνδυασμό από γράμματα, νούμερα και σύμβολα.
11. Να εκμεταλλευτείτε τη δυνατότητα που παρέχουν οι Τράπεζες για μια δωρεάν ετήσια αναφορά της πιστωτικής σας κάρτας.

Don'ts

1. Μην παρέχετε προσωπικά δεδομένα σε κανέναν μέσω τηλεφώνου ή αυτοπροσώπως (π.χ: για αίτηση δανείου) παρά μόνο αν είστε σίγουροι για την αξιοπιστία του τρίτου ατόμου.

2. Μην δίνετε ποτέ προσωπικά δεδομένα ως απάντηση σε email, σε μια ιστοσελίδα που έχετε συνδεθεί μέσω ενός εξωτερικού link ή σε pop-up παράθυρο που εμφανίζεται σε κανονική ιστοσελίδα.
3. Ανοίξτε ένα νέο παράθυρο και πληκτρολογείτε τη διεύθυνση ώστε να βεβαιωθείτε για την νομιμότητα του Διαδικτυακού τόπου.
4. Μην κρατάτε οικονομικά δεδομένα σε φορητούς υπολογιστές παρά μόνο αν είναι απολύτως απαραίτητο - οι φορητοί υπολογιστές είναι πολύ πιο πιθανό να κλαπούν από τους επιτραπέζιους.
5. Αν πιστεύετε ότι έχετε πέσει θύμα Διαδικτυακής απάτης ή κλοπής προσωπικών δεδομένων, να καταγγείλετε το γεγονός κατευθείαν στις αρχές.

3) ΒΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Μέσα σε λιγότερο από 20 χρόνια το διαδίκτυο από ένα μέσο μεταφοράς πληροφοριών μεταξύ επιστημόνων και μυστικών υπηρεσιών μεταμορφώθηκε σε ένα από τα πιο λαϊκά και πολυχρησιμοποιημένα μέσα επικοινωνίας. Οι αλλαγές που έφερε στον τρόπο ζωής μας πολλές και διάφορες. Κατάφερε να παρεισφρήσει και να αλλάξει τα δεδομένα στον τρόπο οργάνωσης της εργασίας μας, την επικοινωνία με γνωστούς και φίλους, την διασκέδαση και, φυσικά, την ενημέρωση. Όπως συμβαίνει και με κάθε άλλη αλλαγή στο ανθρώπινο περιβάλλον και ιδιαίτερα στον τρόπο επικοινωνίας (π.χ. ανακάλυψη τυπογραφίας, τηλέγραφος, τηλέφωνο κτλ), έτσι και εδώ η συμπεριφορά μας δεν έμεινε ανεπηρέαστη. Όπως ήταν φυσικό το διαδίκτυο έγινε μια νέα δίοδος διοχέτευσης των συναισθημάτων και των σκέψεών μας.

Μία από τις πιο χαρακτηριστικές περιπτώσεις μεταφοράς μοτίβων ανθρώπινης συμπεριφοράς στο διαδίκτυο είναι και η βία. Στην αγγλική βιβλιογραφία μάλιστα το φαινόμενο της διαδικτυακής βίας έχει και όνομα: cyberbullying. Ένας γενικός ορισμός που θα μπορούσαμε να δώσουμε στο φαινόμενο αυτό, ώστε να το διαχωρίσουμε από τις περιπτώσεις ψυχολογικής, λεκτικής και σωματικής βίας εκτός διαδικτύου (bullying) είναι πως πρόκειται για μια επιθετική και συνειδητή ομαδική ή ατομική πράξη μέσω της χρήσης του διαδικτύου και άλλων ηλεκτρονικών μέσων, η οποία στρέφεται εναντίον ενός ατόμου το οποίο είναι δύσκολο να υπερασπιστεί τον εαυτό του. Παραδείγματα τέτοιας συμπεριφοράς είναι η αποστολή απειλητικών ή χλευαστικών e-mails, τα flames, η παρενόχληση μέσω IM, η δημοσίευση προσωπικών στοιχείων και φωτογραφιών χωρίς την συγκατάθεσή μας κ.α.

Αν και οι περισσότερες περιπτώσεις βίαιης παρενόχλησης εκτός διαδικτύου αφορούν κυρίως παιδιά σχολικής και εφηβικής ηλικίας[1], η διαδικτυακή παρενόχληση είναι ένα φαινόμενο που αγγίζει τόσο τους νεαρούς, όσο και τους ενήλικες, καθώς θύτες και θύματα μπορούν να βρεθούν και στις δύο ηλικιακές ομάδες (αν και η αλήθεια είναι πως το φαινόμενο αυτό παρουσιάζεται πιο έντονο στις νεαρότερες ηλικίες).



Αν και το φαινόμενο του cyberbullying δεν έχει ερευνηθεί επαρκώς -ιδιαίτερα στην Ελλάδα- μπορούμε να πούμε με σχετική σιγουριά πως σίγουρα θα παίρνει όλο και μεγαλύτερες διαστάσεις στο μέλλον, καθώς οι νέες γενιές άρχισαν ήδη να μεγαλώνουν μέσα σε έναν κόσμο όπου το διαδίκτυο και η διαδραστική επικοινωνία κυριαρχούν. Αυτό θα οδηγήσει σε σταδιακή μερική αντικατάσταση του "παραδοσιακού" bullying με το cyberbullying.

Αν και ακόμη είναι νωρίς να βγάλουμε ασφαλή συμπεράσματα για τις μακροχρόνιες συνέπειες της διαδικτυακής βίας, υπάρχουν ήδη κάποιες έρευνες για την συσχέτιση

μεταξύ cyberbullying και ανάπτυξης ψυχικών διαταραχών. Μόλις πρόσφατα Φινλανδοί επιστήμονες έκαναν έρευνα σε ένα δείγμα 7000 νεαρών Φινλανδών και βρήκαν πως ένα ποσοστό της τάξεως του 4,8% ήταν μόνο θύματα διαδικτυακής βίας (64% κορίτσια), ένα 7,8% ήταν μόνο θύτες (62% αγόρια), ενώ ένα 5,4% ήταν και θύτες και θύματα (55% αγόρια)[2]. Ένα στα τέσσερα παιδιά που χαρακτηρίστηκαν ως θύματα διαδικτυακής βίας, ανέφεραν έντονο άγχος, φόβο και ανασφάλεια, κάτι που τα κάνει ιδιαίτερα ευάλωτα για την ανάπτυξη συναισθηματικής διαταραχής στο μέλλον.

Από τα πιο ενδιαφέροντα αποτελέσματα της έρευνας αυτής όμως ήταν οι συσχετίσεις που βρήκαν οι ερευνητές μεταξύ της ιδιότητας του θύτη και του θύματος και της ανάπτυξης ψυχοσωματικών, συναισθηματικών και γνωστικών συμπτωμάτων. Οι θύτες βρέθηκαν να έχουν προβλήματα με την οργάνωση και διευθέτηση εργασιών, και παρουσίαζαν συμπτώματα γενικότερης αντικοινωνικής συμπεριφοράς. Από την άλλη πλευρά, τα θύματα σχετίστηκαν θετικά με ανάπτυξη συναισθηματικών προβλημάτων, ανασφάλεια και έντονα σωματικά συμπτώματα (πονοκέφαλος, πόνος στο στομάχι, προβλήματα ύπνου).

Είναι σημαντικό να καταλάβουμε πως μπορεί να επηρεαστεί η ψυχολογική ανάπτυξη ενός ατόμου στο μέλλον εάν πέσει θύμα τέτοιας συμπεριφοράς, αλλά και πως μπορούμε να περιορίσουμε την εξάπλωση της διαδικτυακής βίας. Τα παιδιά θα πρέπει να γνωρίζουν πως μπορούν να προφυλαχθούν από ανεπιθύμητα άτομα, πως μπορούν να μπλοκάρουν και να διαγράψουν συνομιλητές οι οποίοι τα ενοχλούν συστηματικά, αλλά και πως μπορούν να προστατεύσουν τα προσωπικά τους στοιχεία. Η πρόληψη είναι η καλύτερη αντιμετώπιση και σε αυτή την περίπτωση. Ήδη έχουν αρχίσει να δημιουργούνται πυρήνες ενημέρωσης γύρω από τέτοια θέματα στο σύνολο των ευρωπαϊκών κρατών. Για παράδειγμα ένα κέντρο ενημέρωσης και εκπαίδευσης παιδιών για θέματα διαδικτύου έχει δημιουργηθεί στο Βερολίνο (MSPT Museen), ενώ αξίζει να αναφερθεί και η ελληνική ιστοσελίδα SaferInternet.gr που προσπαθεί να ενημερώσει μικρούς και μεγάλους για τους τρόπους με τους οποίους πρέπει να κινούνται στο διαδίκτυο ώστε να παραμένουν ασφαλείς.

Φυσικά, δεν πρέπει να φτάσουμε ούτε στο άλλο άκρο, αυτό της διαδικτυακής απομόνωσης, όπου κάποιος αποφεύγει εντελώς τις ευκολίες του διαδικτύου απλά και μόνο από φόβο μη τυχόν του συμβεί τίποτε. Το διαδίκτυο δεν είναι μπαμπούλας και σίγουρα δεν εγκυμονεί περισσότερους κινδύνους από την ζωή εκτός διαδικτύου. Απλά τυχαίνει να είμαστε λιγότερο εξοικειωμένοι για το πως μπορούμε να προφυλαχθούμε από τα όσα αρνητικά και επικίνδυνα κυκλοφορούν εδώ μέσα.

4) ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗ.



Στην εποχή μας το δικαίωμα των πολιτών στην αντικειμενική και ολόπλευρη ενημέρωση είναι κοινωνικά κατακτημένο και θεσμικά κατοχυρωμένο. Η δημοκρατική πολιτεία δεν ανέχεται τη λογοκρισία και δεν επιτρέπει την αυθαίρετη επέμβαση της εξουσίας στην πληροφόρηση της κοινής γνώμης. Ανώτερη αρχή της είναι η πνευματική ελευθερία και αυτή αναγκαία προϋποθέτει την ελευθερία στη μετάδοση των πληροφοριών και τη διακίνηση των ιδεών. Προϋποθέτει, με άλλα λόγια, την απρόσκοπτη λειτουργία των μέσων ενημέρωσης.

Φαινόμενα, λοιπόν, ασφυκτικού κρατικού ελέγχου στα έντυπα και ηλεκτρονικά μέσα πληροφόρησης δεν υπάρχουν πια στις σύγχρονες αναπτυγμένες κοινωνίες. Είτε είναι ιδιωτικά είτε κρατικά, τα μέσα αυτά λειτουργούν σε καθεστώς ελευθερίας, που εγγυάται την ανεπηρέαστη άσκηση της ενημερωτικής αποστολής τους. Και ενώ θα έπρεπε να προσφέρεται καλύτερη, πληρέστερη και αντικειμενικότερη πληροφόρηση, όλο και περισσότερο διαπιστώνουμε πως ορισμένοι παράγοντες έρχονται να επηρεάσουν αρνητικά τη λειτουργία των μέσων αυτών, να νοθεύσουν την ποιότητα της παρεχόμενης ενημέρωσης και να γεννήσουν φαινόμενα παραπληροφόρησης και παραπλάνησης της κοινής γνώμης.

ΟΡΙΣΜΟΣ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗΣ

Παραπληροφόρηση ονομάζουμε την εσκεμμένη διαστροφή αληθινών πληροφοριών ή την κατασκευή ψευδών με σκοπό την επίτευξη συγκεκριμένων στόχων. Το επιτηδευμένο μήνυμα εισδύει στο υποσυνείδητο του δέκτη ξεπερνώντας τους πνευματικούς αμυντικούς μηχανισμούς και καταλήγει να θεωρείται ως απόλυτα προσωπική επιλογή.

ΑΙΤΙΑ ΤΗΣ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗΣ

Για την ύπαρξη και την ανάπτυξη των ΜΜΕ απαιτούνται σημαντικά χρηματικά ποσά, τα οποία παρέχουν οι οικονομικά ισχυροί. Διαθέτοντας οι τελευταίοι την οικονομική δύναμη, προβάλλουν και επιβάλλουν όποια πρότυπα τρόπου ζωής και συμπεριφοράς τους συμφέρει να ενστερνισθεί ο λαός για να αποκομίσουν οι ίδιοι χρηματικά οφέλη, κατευθύνουν τη σκέψη των ανθρώπων για εξυπηρέτηση ιδιοτελών συμφερόντων.

Η εξάρτηση από τα κόμματα και τον εκάστοτε φορέα της εξουσίας. Η δημοσιογραφία έχει μετατραπεί στις μέρες μας σε θεραπευαίνιδα σκοπιμοτήτων και προπαγάνδας.

Ο σκληρός ανταγωνισμός που κυριαρχεί σε όλα τα επίπεδα, όσον αφορά στα ΜΜΕ ωθεί τους τηλεοπτικούς σταθμούς, ή ακόμη και τον τύπο, στην προβολή θεαμάτων τα οποία

διακρίνει η απλοϊκότητα και ο λαϊκισμός, για να υπάρξει επιτυχής αποδοχή από την ευρεία βάση του λαού. Η αλήθεια λοιπόν και η αντικειμενικότητα θυσιάζονται στο βωμό της εμπορικής επιτυχίας. Ο κιτρινισμός, η σκανδαλοθηρία, η αποσιώπηση και διαστρέβλωση της αλήθειας αποτελούν τις αδιάφευστες αποδείξεις της δυσάρεστης αυτής εξέλιξης. Άμεσο αποτέλεσμα αυτού του γεγονότος είναι η καθοδική πορεία του δείκτη της ποιότητας των προγραμμάτων και η ανοδική του δείκτη της ακροαματικότητας, με ανάλογη επιτυχία στον οικονομικό τομέα των Ιθυόντων.

Στον τομέα των ειδήσεων πολλές φορές για λόγους εντυπωσιασμού δημιουργούνται ανύπαρκτες ειδήσεις και γεγονότα. Τέτοιου είδους φαινόμενα υποβιβάζουν το επίπεδο της πληροφόρησης και επιφορτίζουν την κοινωνία με επιπλέον φαινόμενα κοινωνικής παθογένειας, δημιουργώντας στους πολίτες το αίσθημα της ανασφάλειας.

Υπακούοντας στους κανόνες της υψηλής θεαματικότητας ή αναγνωσιμότητας, ορισμένοι δημοσιογράφοι βιάζονται να μεταδώσουν ειδήσεις, χωρίς να διασταυρώσουν τις πηγές τους, με αποτέλεσμα να παραπληροφορούν το κοινό. Ο δημοσιογράφος, ως άνθρωπος, έχει διαμορφωμένο κοσμοείδωλο, συγκροτημένη ιδεολογία και συγκεκριμένη πολιτική τοποθέτηση. Μπορεί βέβαια, όπως ειπώθηκε, «οι ειδήσεις να ανήκουν στον αναγνώστη και μόνο η ορθογραφία στο δημοσιογράφο», αλλά ο δεύτερος δεν είναι μηχανή συγκέντρωσης και μετάδοσης πληροφοριών. Κατά την εργασία του πολλοί υποκειμενικοί παράγοντες, όπως η ψυχική διάθεση, η πολιτική τοποθέτηση και η κομματική ένταξη, μπορεί να υπεισέλθουν, για να δημιουργήσουν μικρότερα ή μεγαλύτερα προβλήματα στην αντικειμενικότητα της είδησης που μεταδίδει.

ΣΥΝΕΠΕΙΕΣ ΤΗΣ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗΣ

Εξαιτίας του καταγισμού των μηνυμάτων και του επιτηδευμένου τρόπου που αυτά μεταδίδονται παθητικοποιείται ο δέκτης και αποδέχεται άκριτα τα μηνύματα αυτά.

Τα προβαλλόμενα μηνύματα στην εποχή μας εκμεταλλεύονται τα συναισθήματα και την ηθική του δέκτη. Επιπρόσθετα, συνδυάζονται με τακτική επανάληψη και δημιουργούν στο άτομο φοβερή εξάρτηση από τις συγκεκριμένες πηγές που το παράγουν, ενώ το καθιστούν αδύναμο να ανιχνεύσει άλλες πηγές πληροφόρησης.

Ετεροκαθορίζεται και εξωκατευθύνεται η ανθρώπινη σκέψη με αποτέλεσμα αυτή να υιοθετεί λανθασμένα πρότυπα ως ορθά. Με την παραπληροφόρηση χαλκούνται τα αόρατα αλλά πανίσχυρα δεσμά της σύγχρονης δουλείας. Πρόκειται για δουλεία πνευματική και ψυχική που στερεί την αυτοβουλία και την ελευθερία στη σκέψη και στη συμπεριφορά. Γιατί όσο κακοποιείται η αλήθεια, τόσο περισσότερο ο άνθρωπος βυθίζεται στην άγνοια και καθίσταται ευκολότερη η χειραγώγησή του. Αυτός άλλωστε είναι και ο επιδιωκόμενος στόχος, η μετατροπή δηλαδή του πολίτη σε υπήκοο, σε άνθρωπο αδρανή, με εφησυχασμένη συνείδηση και νεκρωμένη σκέψη, ώστε με την επίφαση της ελευθερίας να σκέφτεται και να ενεργεί, όπως άλλοι του υποδεικνύουν.

Οξύνει το φανατισμό, μαζοποιεί τον άνθρωπο, υποβαθμίζει την κριτική σκέψη.

Αποδιοργανώνεται η εσωτερική ζωή των ατόμων.

Επικρατεί φόβος προς τον συνάνθρωπο, ωφελιμισμός και αριθμισμός. Προκειμένου να εξυπηρετηθούν ισχυρά πολιτικά συμφέροντα παραποιείται η ουσία των γεγονότων.

Προκαθορίζονται οι επιλογές του πολίτη βάσει κερδοσκοπικών και πολιτικών συμφερόντων .

Αφαιρείται η πρωτοβουλία από τον άνθρωπο ο οποίος υποτάσσεται πλήρως στις επιταγές των ΜΜΕ

Πλήττεται η δημοκρατία , εφόσον ο πολίτης δε συμμετέχει στα κοινά, είναι αδιάφορος για τις εξελίξεις στον κοινωνικό-πολιτικό χώρο. Η κατευθυνόμενη ενημέρωση δεν ελέγχει τα πολιτικά πρόσωπα με γνώμονα την αξιοότητά τους και δεν αποτιμά τις ενέργειές τους με κριτήριο το κοινό καλό. Προβάλλει μόνο ό,τι και όποιους συγκλίνουν με τα συμφέροντα που υπηρετεί και στην αντίθετη περίπτωση κακοποιεί την αλήθεια. Ο λαός μπορεί τυπικά να κατέχει και να ασκεί την εξουσία, αλλά στην πράξη αυτή περιέχεται στα χέρια των λίγων, αυτών που έχουν τη δύναμη να ελέγχουν την πολιτική βούλησή του.

Η κοινωνία δεν μπορεί να αντιμετωπίσει τα προβλήματά της, εφόσον δεν ενημερώνεται έγκαιρα και έγκυρα για τη φύση τους. Μόνο η γνώση της αλήθειας μπορεί να καταστήσει την κοινωνία ικανή να διορθώσει τα κακώς κείμενα και να επιλύσει τα προβλήματά της.

Όταν όμως η αλήθεια αποσιωπάται, τότε η παραπληροφόρηση αδρανοποιεί το κοινωνικό σώμα, αποπροσανατολίζει τη κοινή γνώμη από τα σημαντικά θέματα και στρέφει το ενδιαφέρον της σε επουσιώδη.

ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΗΣ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗΣ



Για να αντιμετωπισθεί το φαινόμενο της παραπληροφόρησης επιβάλλεται:

- ✓ Ανάπτυξη υγιούς διαλόγου και θεσμική κατοχύρωση μιας πλουραλιστικής ενημέρωσης.
- ✓ Η πληροφόρηση, για να είναι ωφέλιμη για το άτομο-δέκτη πρέπει να προέρχεται από χώρους όπου επικρατεί η δημοκρατία, η ελευθερία του στοχασμού, της άντλησης και μετάδοσης των ειδήσεων.
- ✓ Η αξιοκρατική επιλογή ανθρώπων που θα κατέχουν υπεύθυνες θέσεις
- ✓ Οι εκπρόσωποι των ΜΜΕ να επιλέγονται με βάση το υψηλό εκπαιδευτικό τους επίπεδο.

Καθημερινά παίρνουμε αλλά και δίνουμε πληροφορίες για διάφορα γεγονότα . Από την πλευρά του δέκτη , απαιτείται η αφύπνιση της κριτικής ικανότητας που μπορεί να περιορίσει το φαινόμενο της παθητικοποίησης του πολίτη και να ενισχύσει την αντίσταση του ατόμου στα προβαλλόμενα πρότυπα σκέψης και συμπεριφοράς (καταλυτική στο σημείο αυτό θα είναι η στάση της παιδείας που πρέπει να προσαρμόσει τους στόχους της

στη διεύρυνση των πνευματικών οριζόντων των νέων ατόμων, ώστε αυτά να είναι σε θέση να αντιστέκονται κριτικά στον καταϊγισμό των πληροφοριών που δέχονται). Οφείλει, ακόμη, το άτομο να επεξεργάζεται συστηματικά τις ειδήσεις, να διασταυρώνει τις πληροφορίες, να ενημερώνεται διαρκώς, να αντιστέκεται στον ιδεολογικό δογματισμό και φανατισμό. Από την πλευρά του πομπού, απαιτείται διαχωρισμός της είδησης από το προσωπικό σχόλιο ώστε να υπάρχει αντικειμενικότητα, συστηματικός και μεθοδικός έλεγχος των πηγών πληροφοριοδότησης, διασταύρωση των πληροφοριών, προσοχή στην ακρίβεια και σαφήνεια των πληροφοριών, ιδιαίτερα όταν παρέχουμε πληροφορίες στα παιδιά, που δεν έχουν αναπτύξει πλήρως την κριτική τους ικανότητα .

Πώς θα βοηθήσετε τα παιδιά να εντοπίζουν την παραπληροφόρηση;

Ξεκινήστε όταν τα παιδιά είναι μικρά. Ακόμη και παιδιά προσχολικής ηλικίας χρησιμοποιούν σήμερα το Διαδίκτυο για την αναζήτηση πληροφοριών, γι' αυτό είναι σημαντικό να τα μάθετε από μικρά να διακρίνουν το γεγονός από την άποψη και να αναγνωρίζουν την προκατάληψη, την προπαγάνδα και τις τοποθεσίες που χρησιμοποιούν στερεότυπα.

Ρωτήστε τα παιδιά σχετικά με τις πληροφορίες που βρίσκουν στο Διαδίκτυο. π.χ. ποιος είναι ο σκοπός της διαδικτυακής τοποθεσίας; Η ψυχαγωγία; Οι πωλήσεις; Περιέχει η τοποθεσία πληροφορίες επικοινωνίας με το συγγραφέα ή μια ενότητα "Σχετικά με εμάς"; Η τοποθεσία έχει χορηγό κάποια συγκεκριμένη εταιρεία ή πρόσωπο ή μήπως είναι χώρος δημόσιας συζήτησης; Είναι το Διαδίκτυο ο καταλληλότερος τόπος για να βρείτε τις πληροφορίες που αναζητάτε;

Βεβαιωθείτε ότι τα παιδιά διασταυρώνουν τις πληροφορίες που συλλέγουν από το διαδίκτυο με πληροφορίες από άλλες πηγές. Ανατρέξτε σε άλλες διαδικτυακές τοποθεσίες ή μέσα ενημέρωσης, όπως εφημερίδες, περιοδικά και βιβλία, για να επιβεβαιώσετε τις πληροφορίες.

Ενθαρρύνετε τα παιδιά να χρησιμοποιούν ποικιλία πηγών, όχι απλώς το Διαδίκτυο. Πηγαίνετε τα στη βιβλιοθήκη ή προμηθευτείτε μια καλή εγκυκλοπαίδεια σε δίσκο CD-ROM.

Διδάξτε στα παιδιά αποτελεσματικές τεχνικές για την εύρεση πληροφοριών στο Διαδίκτυο. Έτσι, θα βελτιωθεί σημαντικά η ικανότητά τους να βρίσκουν ποιοτικές πληροφορίες. Ένας τρόπος για να το πετύχετε αυτό είναι να ενθαρρύνετε τα παιδιά να χρησιμοποιούν διάφορες μηχανές αναζήτησης και όχι μόνο μία.

Συζητήστε με τα παιδιά σχετικά με το μίσος και το ρατσισμό. Τα φίλτρα λογισμικού μπορούν να αποκλείσουν ορισμένα από αυτά τα είδη υλικού. Τα παιδιά, ωστόσο, θα πρέπει να μάθουν για το ρατσισμό και τα διεθνή γεγονότα, ώστε να μπορούν να αναγνωρίζουν το εμπαιχθέν περιεχόμενο.

ΠΑΙΔΟΦΙΛΙΑ



Η λέξη «παιδόφιλος» ακούγεται όλο και πιο συχνά τελευταία, λόγω των πολλαπλών συλλήψεων παιδεραστών ή κατόχων παιδικής διαδικτυακής πορνογραφίας, όπως πρόσφατα η περίπτωση ενός αρχιμανδρίτη, ενός γυναικολόγου, ενός νευροχειρουργού, τεσσάρων επιχειρηματιών, δύο ιδιωτικών υπαλλήλων, ενός αξιωματικού του Στρατού, ενός φαντάρου και ενός άεργου, οι οποίοι κατηγορούνται ότι είχαν αυτό το κοινό διαστροφικό στοιχείο και, σύμφωνα με την Αστυνομία, είχαν όλοι τους αγοράσει από το Διαδίκτυο φωτογραφίες που απεικόνιζαν «πολύ μικρά παιδιά, ηλικίας από 6 μηνών και επάνω δεμένα πισθάγκωνα και φιμωμένα, σε σεξουαλική δραστηριότητα.

Η παιδοφιλία είναι ένα είδος *παραφιλίας* (σεξουαλικής παρέκκλισης) που αφορά ένα έντονο, μη φυσιολογικό ενδιαφέρον προς τα παιδιά.

Παραφιλία είναι μια διαταραχή που χαρακτηρίζεται από επανειλημμένες, έντονες και σεξουαλικά διεγερτικές φαντασιώσεις, σεξουαλικές παρορμήσεις ή συμπεριφορές που γενικά αφορούν: μη ανθρώπινα αντικείμενα, βασανισμό ή ταπείνωση του ίδιου του ατόμου ή του συντρόφου του (όχι απλή προσποίηση), ζώα, παιδιά ή άλλα άτομα που δεν συναινούν.

Η παιδοφιλία είναι επίσης μια ψυχοσεξουαλική διαταραχή στην οποία το προτιμώμενο ή αποκλειστικό μέσο σεξουαλικής διέγερσης και ικανοποίησης είναι η φαντασίωση ή η πραγματική συμμετοχή σε σεξουαλική δραστηριότητα με παιδιά προεφηβικής ηλικίας (συνήθως 13 ετών και κάτω). Το ενδιαφέρον μπορεί να στρέφεται σε παιδιά του ίδιου φύλου ή σε παιδιά του άλλου φύλου. Μερικοί παιδόφιλοι έλκονται και από αγόρια και από κορίτσια. Ορισμένοι έλκονται μόνο από παιδιά, ενώ άλλοι έλκονται και από ενήλικους και από παιδιά.

ΣΥΝΕΠΕΙΕΣ ΠΑΙΔΟΦΙΛΙΑΣ



Τα παιδιά πολύ σπάνια αναφέρουν την κακοποίησή τους. Συνήθως φοβούνται μήπως τα κατηγορήσουν οι γονείς τους. Η κακοποίηση συνήθως αποκαλύπτεται όταν ένας ενήλικας την αντιληφθεί ή όταν ένα παιδί το αναφέρει σ' έναν ενήλικα (συνήθως όχι το γονέα), ή

όταν ένας γιατρός διαπιστώσει σημάδια σεξουαλικής κακοποίησης στο σώμα του παιδιού. Επίσης, η κακοποίηση μπορεί να γίνει αντιληπτή ή να αποκαλυφθεί από το ίδιο το παιδί όταν αυτό ενηλικιωθεί κι έχει τη δυνατότητα να αναγνωρίσει τη φύση της εμπειρίας του.

Συνήθως, τα παιδιά των οποίων έχει κακοποιηθεί ο σεξουαλικός τους εαυτός, μπορεί: Να έχουν άστατο ύπνο, συχνούς εφιάλτες και διαταραχές στην όρεξή τους.

Να έχουν νέους φόβους και φοβίες (π.χ. για ένα πρόσωπο, μια κίνηση ή ένα μέρος) που δεν εξηγούνται εύκολα από τους γονείς, και όσους γνωρίζουν την ιδιοσυγκρασία του παιδιού.

Να έχουν περίεργη σεξουαλική συμπεριφορά για την ηλικία τους - που συχνά περιλαμβάνει στοιχεία ενήλικης σεξουαλικής συμπεριφοράς (π.χ. λεξιλόγιο, κινήσεις) που φαίνονται ξένα πάνω τους.

Internet και παιδοφιλία



Οι παιδόφιλοι χρησιμοποιούν το Διαδίκτυο για την διακίνηση παιδικής πορνογραφίας και προκειμένου να εντοπίσουν παιδιά, προκειμένου να τα παρενοχλήσουν σεξουαλικά και να επικοινωνήσουν με άλλους παιδόφιλους.

Για πολλούς το διαδίκτυο είναι ένα εργαλείο δουλειάς ,για άλλους διασκέδαση και για κάποιους άλλους μια οθόνη στην οποία κρύβονται πίσω από αυτή και κάνουν ότι κομπίνα δεν μπορείς να φανταστείς , είτε οικονομική απάτη είτε πουλάνε φύκια για μεταξωτές κορδέλες ,όμως δυστυχώς υπάρχει και κάτι χειρότερο από όλα αυτά ,η παιδική πορνογραφία και η παιδική παιδοφιλία ,παιδάκια εν αγνοία τους πέφτουν θύματα διάφορων ανθρώπων ,που μόνο άνθρωποι δεν θα έπρεπε να λέγονται για να ικανοποιούσαν τις ανώμαλες ορέξεις τους! Το ασύρματο internet ,που όποιος ξέρει μπορεί να προστατεύει ,αυτός όμως που δε ξέρει και είναι πάρα πολλοί αυτοί ,και έχει ασύρματη σύνδεση ,κάλλιστα κάποιος έξω από το σπίτι του με ένα laptop μπορεί να συνδεθεί στη σύνδεση τη δικιά σου και να κάνει ότι δεν κάνεις εσύ! Ξέρετε πολύ καλά ότι ο καθένας μας αφήνει το στίγμα του και η σύνδεση του είναι μια και μοναδική για τον καθένα μας! Λοιπόν κάποιος που δε ξέρει να προστατευτεί ,μπορεί να χρησιμοποιήσει την ασύρματη σύνδεση του κάποιος άλλος, ακόμα και από το διπλανό διαμέρισμα και να κάνει αξιόποινες πράξεις! Εσένα θα βρουν και εσένα θα βγάλουν στη φορά μπορεί ακόμα και πριν ψάξουν τον υπολογιστή σου! και αυτό γιατί εδώ στην Ελλάδα οι απάτες η παιδική πορνογραφία και η παιδοφιλία πάντα στις ειδήσεις μπαίνουν με φανφάρες και με μεγάλα γράμματα, και οι διαψεύσεις όταν αποδεικνύεται ότι έχεις δίκιο πάντα περνάνε στα ψιλά γράμματα! Τους ξέρετε τώρα τους δημοσιογράφους και τα κανάλια! Τι να το κάνει κάποιος να αποδεικνύεται λοιπόν ότι έχει δίκιο όταν πριν από αυτό τον έχουν διαβάσει και το έχει μάθει όλη η Ελλάδα, ενώ στη διάψευση άντε να το μάθουν 100 άτομα!

Για αυτό όταν δεν ξέρετε να βάλετε κωδικούς στην ασύρματη σύνδεση σας ζητήστε βοήθεια από τον πάροχό σας, και το κυριότερο όταν δεν είστε στο internet να βγάξετε το modem από την πρίζα!

10 βήματα ασφάλισης του Wi-Fi δικτύου μας

1. αλλαγή του username και password του router
2. απενεργοποίηση της ad-hoc δυνατότητας (p2p μεταξύ wireless clients)
3. απενεργοποίηση του SSID Broadcast
4. Χρήση MAC access control
5. χρήση WPA/WPA2 κρυπτογράφησης
6. τακτικός έλεγχος για άγνωστα συνδεδεμένα μηχανήματα
7. χρήση firewall
8. προστασία με password του υπολογιστή και των αρχείων
9. διαχωρισμός ασύρματου δικτύου
10. κλείσιμο WiFi εξοπλισμού όταν χρειάζεται.



Στο διαδίκτυο οι παιδόφιλοι, προσποιούνται ότι είναι έφηβοι. Τη δράση τους τη βλέπουμε σε διάφορα website γνωριμιών (π.χ. Chat rooms, κλπ) συνήθως προσελκύουν παιδιά με σκοπό να τα κακοποιήσουν. Αρχικά οι συζητήσεις είναι φιλικές, αργότερα όμως στρέφονται γύρω από σεξουαλικά θέματα, με σκοπό να πείσουν το παιδί ότι η σεξουαλική πράξη είναι αθώα και θεμιτή. Απώτερος σκοπός είναι η συνάντηση και η ανάπτυξη σχέσης έξω από το διαδίκτυο.

ΣΥΜΒΟΥΛΕΣ ΠΡΟΣ ΠΑΙΔΙΑ

Μην αποκαλύπτετε ποτέ το όνομα, την ηλικία, τη διεύθυνσή, το σχολείο, τον αριθμό του τηλεφώνου και τη φωτογραφία σας ή τη φωτογραφία οποιουδήποτε άλλου χωρίς την άδεια των γονιών σας

Μην εμπιστεύεστε ότι διαβάζετε στο Ίντερνετ

Όταν μιλάτε μέσω chatroom ή email, διακόψτε τη συνομιλία όταν κάποιος σας κάνουν να νιώθετε άβολα

Μην απαντάτε σε ηλεκτρονικά μηνύματα μέσω των οποίων σας ζητάνε τα προσωπικά σας στοιχεία

Μην συναντάτε προσωπικά κανένα μέσω του Διαδικτύου, εκτός εάν είναι ενήμεροι οι γονείς σας

Μην αναφέρετε ποτέ σε κάποιο άτομο που βρίσκεστε ή τι κάνετε χωρίς την άδεια των γονέων σας

ΟΡΙΣΜΟΣ ΣΕΞΟΥΑΛΙΚΗΣ ΠΑΡΕΝΟΧΛΗΣΗΣ



Σεξουαλική παρενόχληση θεωρείται οποιαδήποτε ανεπιθύμητη από τον αποδέκτη της συμπεριφορά σεξουαλικής φύσεως, που εκφράζεται με λόγια ή έργα και έχει ως σκοπό ή αποτέλεσμα την προσβολή της αξιοπρέπειας ενός προσώπου.

ΜΟΡΦΕΣ ΣΕΞΟΥΑΛΙΚΗΣ ΠΑΡΕΝΟΧΛΗΣΗΣ



- Φραστική/λεκτική συμπεριφορά
- Διάφορες μορφές επικοινωνίας ηλεκτρονικά και έντυπα μηνύματα (Με σεξουαλικής φύσης περιεχόμενο)

ΑΙΤΙΑ ΚΑΙ ΣΥΝΕΠΕΙΕΣ ΣΕΞΟΥΑΛΙΚΗΣ ΠΑΡΕΝΟΧΛΗΣΕΙΣ

Νέες μορφές εγκληματικών πράξεων δεν εμφανίζονται συχνά στην πορεία της ανθρώπινης ιστορίας. Ωστόσο, τον 21ο αιώνα με αφορμή την ανακάλυψη και τη χρήση του Διαδικτύου ένα νέο είδος εγκλήματος άρχισε να εμφανίζεται και να λαμβάνει ανησυχητικές διαστάσεις, το ονομαζόμενο διαδικτυακό έγκλημα (cybercrime- internet crime).

Η ανησυχία και κατ' επέκταση η ανασφάλεια που συνδέεται με τη χρήση του Διαδικτύου καταφαίνεται από το γεγονός ότι το 70% των ατόμων που χρησιμοποιεί το διαδίκτυο πιστεύει ότι είναι πιο πιθανό να πέσει θύμα διαδικτυακού εγκλήματος(π.χ. κλοπή πιστωτικής κάρτας) από ότι κάποιας άλλης μορφής εγκλήματος (Reisig, et. al., 2009). Οι λόγοι που οι εγκληματίες προτιμούν τη χρήση του Διαδικτύου είναι επειδή τους επιτρέπει πρόσβαση σε ένα μεγάλο εύρος ατόμων, έχει χαμηλό κόστος και κίνδυνο, εξασφαλίζει την ανωνυμία και δεν υπάρχουν καθόλου γεωγραφικοί περιορισμοί, προϋποθέσεις που καθιστούν το Διαδίκτυο ιδανικό μέρος δραστηριοποίησης ατόμων με προβληματικές συμπεριφορές.

Το διαδικτυακό έγκλημα μπορεί να πάρει διάφορες μορφές από την οικονομική απάτη ως την έκθεση σε κίνδυνο ανηλικού. Μια από τις πιο απειλητικές μορφές του ηλεκτρονικού εγκλήματος, δεδομένου ότι ολοένα και περισσότερα παιδιά έχουν πρόσβαση στο διαδίκτυο είναι αυτό που αφορά την παιδική, ηλεκτρονική πορνογραφία ή την σεξουαλική παρενόχληση ανηλικών στο διαδίκτυο.

Τα ερευνητικά δεδομένα επισημαίνουν ότι το 1/5 των ανηλικών που χρησιμοποιούν το Διαδίκτυο έχει προσεγγιστεί σεξουαλικά από άτομα που συνάντησαν σε αυτό, και ενώ πολλά από τα παιδιά είναι σε θέση να προστατεύσουν τον εαυτό τους και να μην ανταποκριθούν στις πιέσεις των ενηλίκων, υπάρχει μια κατηγορία ανηλικών που πέφτει θύμα σεξουαλικής εκμετάλλευσης και επίθεσης.

Πολύ συχνά οι ενήλικες προσεγγίζουν ανηλικούς δημιουργώντας μια ψεύτικη ταυτότητα και παρουσιάζοντας τον εαυτό τους έχοντας την ίδια ηλικία με τον ανήλικο- στόχο. Ενδιαφέρον παρουσιάζουν τα δημογραφικά χαρακτηριστικά αυτών των παραβατών που συνοψίζονται στα ακόλουθα: στην πλειονότητά τους είναι άντρες, μεταξύ 26- 39 ετών, με ανώτερο μορφωτικό επίπεδο, οι οποίοι εργάζονται με πλήρες ωράριο και χαρακτηρίζονται από δυσκολία στη διαμόρφωση και διατήρηση διαπροσωπικών σχέσεων (Mitchell, Wolak and Finkelhor, 2005; Wyker, 2007).

Οι συγκεκριμένοι παραβάτες μπορούν να ταξινομηθούν σε τρεις κατηγορίες:

- σε αυτούς που συλλέγουν πορνογραφικό υλικό στα πλαίσια μιας γενικότερης σεξουαλικής παραβατικότητας
- σε αυτούς που συλλέγουν για να ικανοποιήσουν μια αναπτυσσόμενη σεξουαλική ανάγκη ή ενδιαφέρον για τα παιδιά και
- σε αυτούς που έρχονται σε επαφή με το συγκεκριμένο πορνογραφικό υλικό λόγω περιέργειας.

Το ερώτημα που γεννιέται και στο οποίο δεν μπορεί να δοθεί μια απόλυτη απάντηση είναι το αν αυτή η κατηγορία παραβατών είναι αυτή που διαπράττει και τα εγκλήματα σεξουαλικής παρενόχλησης ανηλικών.

Τα μέχρι τώρα δεδομένα επισημαίνουν ότι είναι μια ετερογενής ομάδα, στα πλαίσια όμως της οποίας υπάρχουν και αυτοί που παρενοχλούν σεξουαλικά παιδιά (13%).

Το προφίλ των παραβατών για τη διακίνηση παιδικού πορνογραφικού υλικού αποτελείται από τα εξής χαρακτηριστικά: είναι μεταξύ 25-50 ετών, τείνουν να έχουν λιγότερα προβλήματα με τη χρήση ουσιών, αποτυγχάνουν στη δημιουργία στενών, διαπροσωπικών σχέσεων, παρουσιάζουν προβλήματα στη σεξουαλική αυτορύθμιση (π.χ. αποκλίνουσες σεξουαλικές συμπεριφορές, έντονη σεξουαλική ενασχόληση, κ.α.), φοβούνται την απόρριψη και έχουν υψηλά επίπεδα ψυχοπαθολογίας (Webb, Craissati and Keen, 2007).

ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Το εύλογο ερώτημα που προκύπτει είναι το κατά πόσο και με ποιον τρόπο μπορεί να προστατευθεί ο κάθε πολίτης και ιδιαίτερα τα παιδιά και οι έφηβοι από αυτή τη μορφή εγκληματικότητας. Τα μέτρα αντιμετώπισης εντάσσονται σε δύο κατηγορίες στα

προληπτικά και στα κατασταλτικά. Στην πρώτη κατηγορία απαιτείται η ενεργοποίηση και η ενημέρωση των πολιτών για τους πιθανούς τρόπους δράσης των εγκληματιών του Διαδικτύου, αξιοποιώντας για παράδειγμα τα μέσα μαζικής ενημέρωσης προς αυτήν την κατεύθυνση. Στα κατασταλτικά μέτρα, πρωταγωνιστικό ρόλο καλούνται να αναλάβουν οι αστυνομικές αρχές κάθε χώρας, οι οποίες θα πρέπει να διαθέτουν τα μέσα και το θεωρητικό υπόβαθρο για τον εντοπισμό και τη σύλληψη αυτών των παραβατών.

Μια διαδεδομένη τεχνική στην περίπτωση της σεξουαλικής παρενόχλησης ανηλίκων στο Διαδίκτυο είναι η χρήση αστυνομικών οργάνων που αναλαμβάνουν να παίξουν το ρόλο ανηλίκων προκειμένου να εντοπιστούν οι δράστες.

Συμπερασματικά, γίνεται σαφές ότι για να μπορέσει να αντιμετωπιστεί αποτελεσματικά αυτό το νέο είδος εγκληματικών ενεργειών χρειάζεται η σύμπραξη των πολιτών, των αστυνομικών δυνάμεων αλλά και της πολιτείας μέσω της θέσπισης ενός νομοθετικού πλαισίου που θα καταδικάζει τέτοιου είδους εγκληματικές πράξεις.

[Το θέμα της ασφάλειας στο Διαδίκτυο](#)



Χωρίς να αναιρείται η θετική πλευρά του Διαδικτύου, θα πρέπει να επισημανθεί ότι το Διαδίκτυο από τη φύση του δεν εγγυάται ασφάλεια για τον ανήλικο χρήστη, καθώς οι δημοσιευμένες πληροφορίες δεν χαρακτηρίζονται απαραίτητα από καταλληλότητα και εγκυρότητα, οι ταυτότητες και οι σκοποί των συντακτών δεν είναι πάντα εμφανείς, ενώ η ιδιωτικότητα των πληροφοριών μας πρέπει να διασφαλιστεί.

Οι κίνδυνοι αυτοί ειδικά για τους ανήλικους, αναδεικνύουν την αναγκαιότητα σχεδιασμού μίας πολιτικής προστασίας τους από την έκθεσή τους σε ακατάλληλο περιεχόμενο, το οποίο μπορεί να καταστεί επιβλαβές στην ανάπτυξη της προσωπικότητάς τους. Χωρίς αυτό να υπονοεί ότι θα πρέπει να καταφύγουμε σε ακραίες λύσεις λογοκρισίας ή ασφυκτικούς περιορισμούς, είναι προφανές ότι πρέπει να οριστούν πολιτικές ελέγχου του περιεχομένου στο Διαδίκτυο και μέτρα για την ενημέρωση και την προστασία των ανήλικων χρηστών του.

[Πολιτική του Υπουργείου Παιδείας, Διά Βίου Μάθησης και Θρησκευμάτων](#)

Το ζήτημα της ασφαλούς πρόσβασης των ανηλίκων στο Διαδίκτυο είναι ιδιαίτερα σημαντικό, αφού έχει κοινωνικές, πολιτισμικές, παιδαγωγικές, επιστημονικές και άλλες πτυχές. Το Υπουργείο Παιδείας, Διά Βίου Μάθησης και Θρησκευμάτων (ΥΠΔΒΜΘ - www.minedu.gov.gr) αναγνωρίζει την Οδηγίες καλής χρήσης Υπηρεσίας Ηλεκτρονικού

Ταχυδρομείου και Ασφαλούς Πλοήγησης στο Διαδίκτυο. Εφαρμόζει μέσω του Πανελληνίου Σχολικού Δικτύου¹ (www.sch.gr) μία συγκεκριμένη πολιτική προστασίας των μαθητών από την έκθεσή τους σε ακατάλληλο περιεχόμενο του Διαδικτύου μέσα από το σχολείο. Η πολιτική είναι εναρμονισμένη με τη διεθνή πρακτική και τις νομικές απαιτήσεις και διαρθρώνεται σε πέντε άξονες:

1. Στον ορισμό των Πολιτικών Αποδεκτής Χρήσης του Διαδικτύου και των Σχολικών Εργαστηρίων Πληροφορικής από τους μαθητές. Για το σκοπό αυτό το ΥΠΔΒΜΘ έχει θεσμοθετήσει τα αρμόδια συλλογικά όργανα, τα οποία έχουν την ευθύνη της χάραξης πολιτικής και διαχείρισης του περιεχομένου που διακινείται μέσω του Πανελληνίου Σχολικού Δικτύου και των υπηρεσιών του.

2. Στην ανάπτυξη και εφαρμογή τεχνικών (φίλτρα) που υλοποιούν τις πολιτικές αυτές. Αντίστοιχες τεχνικές εφαρμόζονται διεθνώς στα εκπαιδευτικά δίκτυα πολλών προηγμένων

χωρών και αποτρέπουν με σημαντικό δείκτη επιτυχίας την πρόσβαση σε ιστοσελίδες που ανήκουν σε κατηγορίες όπως:

«porn» (ιστοσελίδες με πορνογραφικό περιεχόμενο)

«gambling» (ιστοσελίδες με τυχερά παιχνίδια)

«drugs» (ιστοσελίδες που προωθούν τα ναρκωτικά)

«aggressive» (ιστοσελίδες που προπαγανδίζουν την επιθετική συμπεριφορά και το ρατσισμό)

«violence» (ιστοσελίδες που προωθούν την βία)

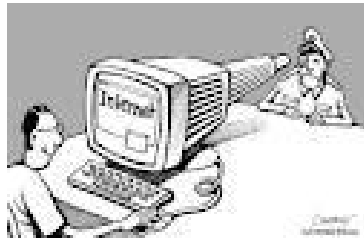
Επειδή η ταξινόμηση των ιστοσελίδων στις παραπάνω κατηγορίες γίνεται με τη χρήση αυτοματοποιημένης διαδικασίας, είναι πιθανό κάποια ιστοσελίδα να ταξινομηθεί λανθασμένα. Για το λόγο το Πανελλήνιο Σχολικό Δίκτυο παρέχει τη δυνατότητα στους χρήστες του να ενημερώνουν τους αρμόδιους τεχνικούς (δ/νση επικοινωνίας cachemaster@sch.gr) όταν διαπιστώσουν οποιαδήποτε δυσλειτουργία της υπηρεσίας.

3. Στη διαρκή ενημέρωση και ευαισθητοποίηση της σχολικής κοινότητας, καθώς οποιαδήποτε τεχνική λύση είναι αδύνατο να αποδώσει αν δεν είναι σωστά ενημερωμένη και ευαισθητοποιημένη η σχολική κοινότητα. Για το σκοπό αυτό το Πανελλήνιο Σχολικό Δίκτυο ενημερώνει τους εκπαιδευτικούς, τους γονείς και τους μαθητές μέσω του δικτυακού τόπου <http://internet-safety.sch.gr> και μέσω της συμμετοχής του σε συναφείς εκδηλώσεις (ημερίδες, συνέδρια, κλπ).

4. Στη συνεργασία με ειδικές δράσεις για την ασφάλεια στο Διαδίκτυο όπως την Ελληνική ανοικτή γραμμή για παράνομο περιεχόμενο στο Διαδίκτυο (Safeline, www.safeline.gr) και το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου (Safer-Internet, www.saferinternet.gr).

5. Στη δημιουργία θετικής αντιπρότασης, δηλαδή στην προβολή ανάπτυξη αξιόλογου ή/και πιστοποιημένου εκπαιδευτικού υλικού στο οποίο αξίζει να έχουν πρόσβαση οι μαθητές και στη διανομή στην εκπαιδευτική κοινότητα του μέσω των εκπαιδευτικών και δικτυακών πυλών όπως (ενδεικτικά): www.e-yliko.gr, www.kee.gr, www.greeklanguage.gr, www.pischools.gr, www.neagenia.gr, κλπ, οι οποίες λειτουργούν είτε υπό την άμεση ευθύνη του ΥΠΔΒΜΘ είτε υπό την ευθύνη εποπτευόμενων φορέων του.

ΔΥΝΗΤΙΚΟΙ ΚΙΝΔΥΝΟΙ ΠΟΥ ΕΝΕΧΕΙ ΤΟ ΔΙΑΔΙΚΤΥΟ ΓΙΑ ΤΟΥΣ ΑΝΗΛΙΚΟΥΣ



Ορισμένοι από τους κινδύνους που μπορεί να συναντήσει ένας ανήλικος κατά την περιήγησή του

στο Διαδίκτυο είναι:

- Προπαγάνδα ιδεών που υποδαυλίζουν το ρατσισμό, το φανατισμό και τη βία
- Προώθηση χρήσης ναρκωτικών ουσιών και αλκοόλ
- Προβολή και παρακίνηση συμμετοχής σε τυχρά παιχνίδια
- Έκθεση σε πορνογραφικό περιεχόμενο
- Κυκλώματα παιδεραστίας
- Οικονομική εκμετάλλευση από αποκάλυψη προσωπικών στοιχείων (αριθμών καρτών κ.λπ.)

Ως προς την προστασία που προσφέρεται στο σχολικό εργαστήριο από το ακατάλληλο και παράνομο περιεχόμενο, το Πανελλήνιο Σχολικό Δίκτυο παρέχει την Υπηρεσία Ελεγχόμενης Πρόσβασης (Web-Filtering) στον Παγκόσμιο Ιστό. Όμως για την προστασία από τους κινδύνους του Διαδικτύου δεν αρκεί η χρήση των φίλτρων αλλά είναι απαραίτητη η ενεργητική και κριτική στάση μαθητών, εκπαιδευτικών και γονέων.

Επιπλέον, οι μαθητές και οι εκπαιδευτικοί σε περίπτωση που συναντήσουν κάποια σελίδα με ακατάλληλο περιεχόμενο μπορούν να επικοινωνήσουν με το διαχειριστή της υπηρεσίας (cachemaster@sch.gr) και να ζητήσουν την απαγόρευση της συγκεκριμένης σελίδας. Αν εντοπίσουν σελίδα που ανήκει στην κατηγορία του παράνομου περιεχομένου, μπορούν να επικοινωνήσουν με την Ελληνική ανοικτή γραμμή για το παράνομο περιεχόμενο στο Διαδίκτυο (www.safeline.gr).

Ανατρέξτε στο <http://internet-safety.sch.gr> για περισσότερη ενημέρωση.

ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ - Συμβουλές ασφαλούς χρήσης του Διαδικτύου



- Προστατεύστε το αγαθό της ιδιωτικότητάς σας! Μην δίνετε ποτέ προσωπικά σας στοιχεία και μην αποκαλύπτετε λεπτομέρειες της προσωπικής σας ζωής σε άλλους χρήστες του Διαδικτύου.
- Μην γνωστοποιείτε μέσω του Διαδικτύου τα στοιχεία επικοινωνίας σας σε αγνώστους.
- Μην αποκαλύπτετε τους κωδικούς πρόσβασης (password) που χρησιμοποιείτε.
- Μην επιχειρείτε συναλλαγές μέσω του Διαδικτύου για την αγορά προϊόντων και μην δίνετε στοιχεία που αφορούν πιστωτικές κάρτες.
- Κατά την επίσκεψή σας σε δικτυακούς τόπους μην συμπληρώνετε φόρμες με τα παραπάνω στοιχεία, όταν σας ζητούνται.
- Τα άτομα που γνωρίζετε στο Διαδίκτυο δεν είναι πάντοτε αυτά που ισχυρίζονται ότι είναι.
- Μην δίνετε πληροφορίες που αφορούν τους φίλους σας, την οικογένειά σας ή το σχολείο σας σε άτομα που γνωρίζετε στο Διαδίκτυο.
- Μην συναντάτε ποτέ μόνοι σας άτομα που γνωρίσατε από το Διαδίκτυο. Ενημερώστε τους γονείς σας και ζητήστε τους να είναι οπωσδήποτε παρόντες.
- Να συζητάτε με τους δασκάλους σας, τους γονείς σας και με πρόσωπα που εμπιστεύεστε για τις δραστηριότητές σας στο Διαδίκτυο, ιδιαίτερα αν αντιμετωπίσετε οτιδήποτε περίεργο ή ασυνήθιστο.
- Να είστε επιφυλακτικοί ως προς την αποδοχή όσων διαβάζετε στο Διαδίκτυο ή αυτών που σας λένε οι άλλοι χρήστες του, πριν το υποβάλετε σε κρίση σας.
- Μην στέλνετε υλικό από το δικό σας υπολογιστή (φωτογραφίες, μουσική, βίντεο) που προστατεύεται από πνευματικά δικαιώματα.
- Να έχετε πάντα υπόψη σας ότι τα προϊόντα της πνευματικής δημιουργίας (Μουσική, Λογοτεχνία, Κινηματογράφος, Video κλπ) προστατεύονται από τους νόμους και η διανομή τους μέσω του Διαδικτύου είναι παράνομη πράξη.
- Το ίδιο παράνομη πράξη θεωρείται και η διακίνηση προγραμμάτων υπολογιστών (Software) εκτός και αν ανήκουν στην κατηγορία του Ελεύθερου Λογισμικού (Open source software). Σε κάθε περίπτωση διαβάστε ή συμβουλευτείτε τους μεγαλύτερους όσον αφορά τους όρους χρήσης και τη δυνατότητα ελεύθερης διακίνησής του.
- Μην χρησιμοποιείτε άκριτα οποιοδήποτε πρόγραμμα βρίσκετε στο Διαδίκτυο. Δεν είναι όλα τα προγράμματα ασφαλή, ακόμα και αν εμφανίζονται ως παιχνίδια. Ίσως περιέχουν προγράμματα Δούρειους Ίππους και ιούς που μπορεί να βλάψουν τον υπολογιστή σας και τα δεδομένα σας.
- Μην ανοίγετε e-mail από αγνώστους αποστολείς με περίεργα θέματα (subject) ή χωρίς θέμα. Είναι πολύ πιθανό να περιέχουν ιούς.
- Προσοχή στα επισυναπτόμενα αρχεία. Πολλά απ' αυτά είναι ιοί ή Δούρειοι Ίπποι και μπορούν να προκαλέσουν σοβαρά προβλήματα στον υπολογιστή σας.
- Ανατρέξτε στο <http://internet-safety.sch.gr> για περισσότερη ενημέρωση.

Οδηγίες καλής χρήσης του Διαδικτύου

Τα μηνύματα Ηλεκτρονικού Ταχυδρομείου και οι πληροφορίες που αποστέλλετε με οποιοδήποτε τρόπο σε χρήστες ή ομάδες χρηστών, πρέπει να χαρακτηρίζονται από τα ακόλουθα:

Το περιεχόμενο των πληροφοριών που αποστέλλετε δεν πρέπει:

- να προσβάλλει άλλους χρήστες του Διαδικτύου, αλλά να ακολουθεί τους νόμους, τα χρηστά ήθη και τα ήθη χρήσης του Διαδικτύου.
- να προσβάλλει τα ανθρώπινα δικαιώματα και τις διάφορες μειονότητες.
- να σχετίζεται με παράνομες πράξεις.
- να έχει υβριστικό χαρακτήρα ή διαφημιστική χροιά (παρά μόνο ενημερωτική-πληροφοριακή).

Μη διακινείτε δικτυακούς τόπους και γενικότερα πληροφορίες που:

- προπαγανδίζουν την επιθετική συμπεριφορά, το μίσος και το ρατσισμό.
- προωθούν τα ναρκωτικά, το αλκοόλ και τα τυχερά παιχνίδια.
- περιέχουν πορνογραφικό περιεχόμενο.
- αναφέρονται σε παραβιάσεις ασφάλειας διαφόρων συστημάτων.
- αφορούν στην παράνομη διανομή προγραμμάτων.
- περιέχουν οπτικοακουστικό υλικό - προϊόν πνευματικής δημιουργίας που προστατεύεται.
- αφορούν σε υλικό με διαφημιστικά banners.

5) ΜΟΛΥΝΣΗ ΤΟΥ Η/Υ ΜΕ ΚΑΤΤΟΙΟ ΙΟ(VIRUS).

ΙΟΙ ΥΠΟΛΟΓΙΣΤΩΝ - SPAM - ΣΚΟΥΛΗΚΙΑ (WORMS) - ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ



Ιός υπολογιστή είναι ένα εκτελέσιμο πρόγραμμα που έχει την ικανότητα να αναπαράγει τον εαυτό του. Ο κώδικα αναπαραγωγής αποτελεί απαραίτητο στοιχείο του ιού καθώς μέσω αυτού ο ιός εξαπλώνεται. Ο κώδικας εκτέλεσης εκτελεί μία συγκεκριμένη λειτουργία ανάλογα με το τι έχει αποφασίσει ο δημιουργός του ιού. Υπάρχουν πολλοί τύποι υπολογιστικών ιών ,όπως ιοί αρχείων , ιοί της περιοχής εκκίνησης ,ιοί σκουλήκια και προγράμματα δούρειοι ίπποι.

Ιοί περιοχής εκκίνησης - Αυτοί οι ιοί μολύνουν δισκέτες και σκληρούς δίσκους. Ο ιός φορτώνεται πριν από το λειτουργικό σύστημα. Ήταν οι πρώτοι ιοί που εμφανίστηκαν

Ιοί αρχείων - σ' αυτή τη κατηγορία ανήκει η πλειοψηφία των ιών και η πιο εύκολα αντιμετωπίσιμη κατηγορία. Είναι μικρά εκτελέσιμα αρχεία. Προσκολλούνται σε ένα αρχείο, συνήθως αρχείο εφαρμογής. Το βασικό γνώρισμα των ιών είναι ότι δημιουργούν αντίγραφα του εαυτού τους μέσα σε άλλα αρχεία. Τα αρχεία αυτά είναι εκτελέσιμα ή αρχεία βιβλιοθηκών. Οι ιοί είτε αντικαθιστούν κάποιο τμήμα του κώδικα του αρχείου (χωρίς να μεταβάλλουν το μέγεθός του) είτε προσκολλώνται σε αυτό.

Ιοί σκουλήκια (Worms) : Έχουν την ικανότητα αναπαραγωγής χωρίς να χρησιμοποιούν άλλα αρχεία. Ο τρόπος διάδοσης τους είναι το διαδίκτυο με τη βοήθεια των δικτυακών πρωτοκόλλων, εκμεταλλευόμενοι τα προβλήματα ασφαλείας των λειτουργικών συστημάτων ή με τη βοήθεια των μηνυμάτων του ηλεκτρονικού ταχυδρομείου.



Οι ιοί σκουλήκια αποκτούν προσπέλαση στο βιβλίο διευθύνσεων του υπολογιστή (όπου κρατούνται οι διευθύνσεις ηλεκτρονικού ταχυδρομείου με τις οποίες επικοινωνεί ο χρήστης του υπολογιστή) και αποστέλλει μολυσμένα μηνύματα. Αρκετές φορές χρησιμοποιούν σαν αποστολέα ένα όνομα από το βιβλίο διευθύνσεων. Όσοι παραλήπτες ανοίξουν το ηλεκτρονικό μήνυμα μολύνονται. Η διάδοση των ιών worm με αυτή τη μέθοδο είναι αστραπιαία. Στη συνέχεια γίνεται αναφορά σε δύο ιούς σκουλήκια τον Blaster και τον Sobig.

** Η έκρηξη του Blaster έγινε την 11η Αυγούστου 2003. Το μεσημέρι της ίδιας μέρας είχαν μολυνθεί 7.000 υπολογιστές και το βράδυ 330.000. Ο ιός ήταν προγραμματισμένος να επιτεθεί στο δικτυακό τόπο της Microsoft στις 16 Αυγούστου. Οι τεχνικοί της Microsoft πρόλαβαν και άλλαξαν τις διευθύνσεις των διακομιστών της εταιρίας και η επίθεση απέτυχε. Μια εβδομάδα αργότερα έκανε την εμφάνισή του η έκτη έκδοση ενός ακόμα ιού του Sobig. Ο ιός αυτός μεταδιδόταν μέσω ηλεκτρονικού ταχυδρομείου και επιβάρυνε τα συστήματα ηλεκτρονικής αλληλογραφίας. Ο Sobig ήταν πολυμορφικός ιός. Όταν οι χρήστες άνοιγαν το μολυσμένο μήνυμα ο κώδικας του ιού ξεκινούσε την αναπαραγωγή του. Έβρισκε τις διευθύνσεις αλληλογραφίας του χρήστη και έστελνε μολυσμένα μηνύματα. Η εξάπλωση του ιού ήταν τεράστια. Οι διακομιστές αλληλογραφίας κατακλύστηκαν από μηνύματα που μετέφεραν τον ιό. Μέσα σε μία εβδομάδα στάλθηκαν 200 εκατομμύρια μολυσμένα μηνύματα.

ΤΡΟΠΟΙ ΜΟΛΥΝΣΗΣ

Ένας ιός εισάγεται σε έναν υπολογιστή μέσω μίας ποικιλίας ενεργειών. Για τους χρήστες του διαδικτύου αυτό μπορεί να συμβεί με το κατέβασμα αρχείων με FTP (file transfer protocol) με τη λήψη ενός ηλεκτρονικού μηνύματος ή και απλά με περιήγηση στο διαδίκτυο. Πλαισιότερα οι ιοί διαδίδονταν με τις δισκέτες. Όταν ένας ιός εισαχθεί σε έναν υπολογιστή προσκολλάται ή αντικαθιστά ένα υπάρχον πρόγραμμα. Έτσι, όταν ο χρήστης εκτελεί το μολυσμένο πρόγραμμα, εκτελείται και ο ιός. Αυτό συνήθως συμβαίνει χωρίς να το αντιλαμβάνεται ο χρήστης.

ΟΙ ΕΠΙΠΤΩΣΕΙΣ

Ένα πρόγραμμα ιός περιλαμβάνει εντολές που εκτελούν κάποια ενέργεια που επηρεάζει τον μολυσμένο υπολογιστή. Κάθε ιός περιλαμβάνει κάποια διαφορετική ενέργεια τα αποτελέσματα της οποίας μπορούν να είναι από απλά έως καταστροφικά:

- ✓ Η εμφάνιση στην οθόνη ενός εκνευριστικού μηνύματος.
- ✓ Μείωση της ελεύθερης μνήμης ή της χωρητικότητας του σκληρού δίσκου.
- ✓ Τροποποίηση δεδομένων.
- ✓ Αντικατάσταση ή καταστροφή αρχείων
- ✓ Διαγραφή σκληρού δίσκου.

Σήμερα οι επιπτώσεις των ιών είναι λιγότερο καταστροφικές αλλά πολύ περισσότερο επικίνδυνες.

- ✓ Δυνατότητα παρακολούθησης των ενεργειών του χρήστη
- ✓ Δυνατότητα κατάληψης του υπολογιστή από άλλο χρήστη μέσω διαδικτύου.

- ✓ Χρήση του υπολογιστή για επιθέσεις σε άλλους υπολογιστές
- ✓ Υποκλοπή κωδικών - στοιχείων πιστωτικών καρτών.

ΑΝΙΧΝΕΥΣΗ

Τα αντιβιοτικά(antivirus) είναι εφαρμογές που προστατεύουν τον υπολογιστή από τους ιούς. Βέβαια πρέπει το αντιβιοτικό να ενημερώνεται τακτικά με τις τελευταίες αναβαθμίσεις. Σε αντίθετη περίπτωση ο υπολογιστής θα μπορεί να προσβληθεί από τους καινούργιους ιούς.

Τα αντιβιοτικά προγράμματα αποτελούνται από δύο τμήματα:

- ✓ τη προστασία από τους ιούς και
- ✓ το τμήμα ανίχνευσης

Το πρόγραμμα προστασίας λειτουργεί σαν ασπίδα και ανιχνεύει τους ιούς τη στιγμή που προσπαθούν να εισχωρήσουν στον υπολογιστή και να εγκατασταθούν στη μνήμη του. Το πρόγραμμα αυτό ελέγχει τη μνήμη του υπολογιστή και τους βασικούς φακέλους με τα αρχεία του λειτουργικού συστήματος. Σε περίπτωση που ένας ιός ενεργοποιηθεί εξαιτίας της εκτέλεσης από το χρήστη μίας μολυσμένης εφαρμογής ή το άνοιγμα ενός μολυσμένου αρχείου, εμφανίζεται το μήνυμα αναφορά ύπαρξης του ιού. Οι περισσότερες εφαρμογές προστασίας από τους ιούς δίνουν την δυνατότητα στο χρήστη να διαγράψει ή να καθαρίσει το μολυσμένο αρχείο. Επίσης τα αντιβιοτικά προγράμματα εκτός από τη μνήμη ελέγχουν και την εισερχόμενη και εξερχόμενη αλληλογραφία. Για την ανίχνευση των ιών χρησιμοποιείται μία βάση δεδομένων ή οποία περιλαμβάνει τμήματα του κώδικα των ιών. Αυτά ονομάζονται ψηφιακές υπογραφές. Με αυτό τον τρόπο αναγνωρίζονται τα μολυσμένα αρχεία καθώς και αν ένας ιός έχει φορτωθεί στη μνήμη του υπολογιστή.

Το τμήμα ανίχνευσης είναι το δεύτερο σημαντικό τμήμα των αντιβιοτικών εφαρμογών. Η ενέργεια αυτή έχει σαν σκοπό αν στο σκληρό δίσκο του υπολογιστή υπάρχει κάποιος ιός σε αναμονή. Το πρόγραμμα ελέγχει όλα τα αρχεία και του φακέλους του σκληρού δίσκου. Η διαδικασία του ελέγχου ξεκινάει με εντολή του χρήστη. Ο χρήστης μπορεί ακόμη να προγραμματίσει την εφαρμογή να προβαίνει αυτόματα σε περιοδικούς ελέγχους. Σε περίπτωση που το πρόγραμμα ανιχνεύσει κάποιο ιό, ενημερώνει το χρήστη και προβαίνει στις προβλεπόμενες διαδικασίες. Συνήθως ολοκληρώνει τον έλεγχο και προβάλλει μία λίστα με τα μολυσμένα αρχεία. Ο χρήστης μπορεί να επιλέξει να διαγράψει ή να καθαρίσει τα αρχεία από τους ιούς.

ΤΙ ΕΙΝΑΙ ΤΟ SPAM :



Spam είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα. Το Spam συχνά έχει την μορφή ενημερωτικών ή διαφημιστικών μηνυμάτων για προϊόντα ή υπηρεσίες τα οποία φθάνουν στο γραμματοκιβώτιο μας χωρίς να έχουμε ζητήσει την εν λόγω πληροφόρηση. Η αλληλογραφία αυτή λοιπόν μπορεί να χαρακτηριστεί ως απρόκλητη ή ανεπιθύμητη αλληλογραφία, δύο όρους που χρησιμοποιούμε για την απόδοση στη γλώσσα μας του όρου Spam.

Τα κυριότερα χαρακτηριστικά του Spam μπορούν να συνοψιστούν στα ακόλουθα σημεία:

Απρόκλητο: Η επικοινωνία που επιχειρείται είναι απρόκλητη, με την έννοια ότι δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα που θα δικαιολογούσε ή θα προκαλούσε την επικοινωνία αυτή.

Εμπορικό : Πολλές φορές το spam αφορά την αποστολή μηνυμάτων εμπορικού σκοπού με σκοπό την προβολή και την διαφήμιση προϊόντων και υπηρεσιών με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.

Μαζικό: Το spam συνίσταται στην μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών. Συνήθως το ίδιο μήνυμα ή ελαφρά διαφοροποιημένο στέλνεται σε ένα μεγάλο πλήθος παραληπτών.

ΤΙ ΜΠΟΡΟΥΜΕ ΝΑ ΚΑΝΟΥΜΕ ΓΙΑ ΝΑ ΑΠΟΦΥΓΟΥΜΕ ΤΟ SPAM;

Οι απλοί χρήστες:

- ✓ Μη δημοσιεύετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σας.
Βάζοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου σε μια ιστοσελίδα είναι σχεδόν σίγουρο ότι σύντομα θα δείτε μηνύματα Spam στο γραμματοκιβώτιο σας.
- ✓ Μη δίνετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας, σε οργανισμούς που δεν εμπιστεύεστε.
Να είστε προσεκτικοί όταν επισκέπτεστε διάφορους δικτυακούς τόπους και σας ζητείτε η συμπλήρωση προσωπικών και στοιχείων επικοινωνίας, όπως το e-mail. Αν είστε αναγκασμένοι να δώσετε τη διεύθυνση ηλ. ταχυδρομείου, διαβάστε προσεκτικά τους όρους χρήσης και την πολιτική εχεμύθειας για την οποία δεσμεύεται ο συγκεκριμένος οργανισμός.
- ✓ Μην απαντάτε στο spam.
- ✓ Αναφέρετε κάθε μήνυμα Spam που λαμβάνετε.
Υπάρχουν σχετικές υπηρεσίες του Διαδικτύου οι οποίες διατηρούν λίστες spammers. Τις λίστες αυτές αξιοποιούν πολλοί εξυπηρετητές ηλεκτρονικού ταχυδρομείου για τον περιορισμό του Spam που φθάνει στους χρήστες. Στις υπηρεσίες αυτές μπορείτε να αναφέρετε τα μηνύματα τύπου Spam που φθάνουν σε σας.
- ✓ Διαδώστε την γνώση σας και την εμπειρία σας σε σχέση με το Spam.
- ✓ Μιλήστε στους χρήστες του δικτύου σας, μαθητές, εκπαιδευτικούς, διοικητικό προσωπικό, στην οικογένεια σας και τους φίλους σας για το θέμα του Spam και την

αντιμετώπιση του. Είναι αρκετά συνηθισμένο οι spammers συγκεντρώνουν e-mail διευθύνσεις από τις απαντήσεις χρηστών του Διαδικτύου.

- ✓ Ελέγξτε τα συστήματα σας ώστε να είναι σωστά διαμορφωμένα και ασφαλή.
Ένα μεγάλο ποσοστό του Spam διαδίδεται από mail servers που δεν είναι σωστά διαμορφωμένοι , αλλά ακόμα και από συστήματα χρηστών.

Οι διαχειριστές εξυπηρετητών ηλεκτρονικού ταχυδρομείου (mail servers):

Θα πρέπει να έχουν κατάλληλο DNS όνομα και διεύθυνση IP

Το λογισμικό του εξυπηρετητή ηλ. ταχυδρομείου θα πρέπει να είναι ασφαλές, εκπληρώνοντας τα διεθνή standards και σωστά ρυθμισμένο.

Παρακολουθείστε τα μηνύματα καταγραφής στον εξυπηρετητή ηλ. ταχυδρομείου, για να δείτε ποιος τον χρησιμοποιεί για την αποστολή μηνυμάτων και ελέγξτε την πιθανότητα να χρησιμοποιηθεί από χρήστες εκτός του δικτύου σας για την αποστολή μηνυμάτων.

Για όλα τα συστήματα

Χρησιμοποιείτε πάντα λογισμικό προστασίας από τους ιούς με δυνατότητα αυτόματης ανανέωσης από τον κατασκευαστή για τους τελευταίους ιούς.

Ενεργοποιείτε τις δυνατότητες προστασίας των συστημάτων σας που διαθέτουν τα σύγχρονα συστήματα.

Μπορείτε να χρησιμοποιήσετε ειδικό λογισμικό για την προστασία του δικτύου σας ή του μεμονωμένου υπολογιστή σας.

FIREWALL

Στην [επιστήμη των υπολογιστών](#) ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή [πρόγραμμα](#) που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα [δίκτυο υπολογιστών](#) σε ένα άλλο.

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο [δίκτυα υπολογιστών](#). Συνήθως τα δύο αυτά δίκτυα είναι το [Διαδίκτυο](#) και το [τοπικό/εταιρικό δίκτυο](#). Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία [Demilitarized Zone \(DMZ\)](#) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης.

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

6) ΥΨΗΛΕΣ ΧΡΕΩΣΕΙΣ.

ΣΥΝΔΕΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΜΕΣΩ ΚΛΗΣΕΩΝ ΥΨΗΛΗΣ ΧΡΕΩΣΕΙΣ - ΠΡΟΓΡΑΜΜΑ DIALERS

Απάτη στο διαδίκτυο νοείται η απάτη που τελείται στο ψηφιακό περιβάλλον και η οποία διακρίνεται από την απάτη με ηλεκτρονικό υπολογιστή, κατά το ότι ο υπολογιστής είναι το βοηθητικό μέσο τέλεσης της πράξης. Γενικά η έννοια της διαδικτυακής απάτης αναφέρεται σε κάθε τρόπο, σχέδιο ή ενέργεια με τους οποίους μπορεί να εμφανιστεί αυτή στο χώρο του διαδικτύου, χρησιμοποιώντας ένα ή περισσότερα μέσα του κυβερνοχώρου, ήτοι ιστοσελίδες, χώρους ανταλλαγής άμεσων μηνυμάτων, παράθυρα ανοιχτών συνομιλιών των χρηστών. Και όλα αυτά μέσα στον αποκαλούμενο «χρόνο Ίντερνετ», που σημαίνει ότι τα πράγματα περνάνε σε μια άλλη διάσταση και κινούνται σε ένα τελείως διαφορετικό χωροχρόνο από τον πραγματικό, κάνοντας έτσι πιο πιθανές τις περιπτώσεις απάτης κάτω από τις ειδικές συνθήκες με τις οποίες είναι γνωστό, αλλά και ελκυστικό το διαδίκτυο



ΠΡΟΓΡΑΜΜΑΤΑ DIALERS

Μία από τις μορφές απάτης είναι και τα προγράμματα dialer που αποτελούν ένα αρκετά μεγάλο πρόβλημα στη χρήση του διαδικτύου. Αυτό που κάνουν οι dialers, αφού εγκατασταθούν στον υπολογιστή σας, είναι να αλλάξουν τις ρυθμίσεις του modem σας από μία συγκεκριμένη σύνδεση στο διαδίκτυο σε μία άλλη. Συνήθως η αλλαγή είναι από το συνήθη αριθμό κλήσης του παροχέα Internet που χρησιμοποιείτε, σε έναν αριθμό αυξημένης χρέωσης.

Οι dialers μπορεί να προέρχονται από επισκέψεις σε ιστοσελίδες με πορνογραφικό περιεχόμενο, σε ιστοσελίδες που παρέχουν πειρατικό λογισμικό, κωδικούς εγκατάστασης και cracks λογισμικού, ιστοσελίδες τυχερών παιχνιδιών μουσικού περιεχομένου, ή ιστοσελίδες με αμφιλεγόμενο περιεχόμενο. Οι ιδιοκτήτες αυτών των σελίδων έχουν τους dialers ενσωματωμένους στον κώδικα του δικτυακού τόπου ώστε να εγκαθίσταται αυτόματα στο σύστημα του χρήστη, χωρίς να γίνεται αντιληπτό και χωρίς να ζητάει απαραίτητα τη συγκατάθεση του. Άλλος τρόπος εμφάνισης αυτών των προγραμμάτων είναι με τη μορφή συνημμένων αρχείων σε ηλεκτρονικά μηνύματα αλληλογραφίας.

Οι dialers ξεκίνησαν ως ένας νόμιμος και βολικός τρόπος για να πληρώσει ο χρήστης πρόσβαση σε ειδικό περιεχόμενο μέσω του διαδικτύου, αντί χρήσης πιστωτικής κάρτας. Στην περίπτωση αυτή, ο χρήστης χρεώνεται για το περιεχόμενο αυτό στο λογαριασμό του τηλεφώνου του, μέσω των αριθμών αυξημένης χρέωσης, όπως ακριβώς συμβαίνει και με τις υπηρεσίες προστιθέμενης αξίας αυξημένης τιμολόγησης που καλεί από το τηλέφωνό του. Όμως, στις περιπτώσεις αυτές θα πρέπει να εμφανιστεί στην οθόνη ένα παράθυρο διαλόγου το οποίο να ρωτά αν θέλετε να εγκαταστήσετε το συγκεκριμένο πρόγραμμα dialer και να ενημερώνει για το είδος της υπηρεσίας την οποία πρόκειται να χρησιμοποιήσετε και για τη χρέωσή της. Επίσης, μόλις αποσυνδεθείτε από τη συγκεκριμένη ιστοσελίδα, θα πρέπει η σύνδεση του modem να επιστρέφει στον αριθμό του παροχέα Internet που χρησιμοποιείτε.

ΤΡΟΠΟΥΣ ΜΕ ΤΟΥΣ ΟΠΟΙΟΥΣ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΤΑΛΑΒΕΤΕ ΟΤΙ ΕΧΕΙ ΕΓΚΑΤΑΣΤΑΘΕΙ ΣΤΟΝ ΥΠΟΛΟΓΙΣΤΗ ΣΑΣ ΕΝΑ DIALER.



Θα ακούσετε το modem σας να αποσυνδέεται και να πραγματοποιεί νέα κλήση (εκτός εάν ο dialer έχει χαμηλώσει τους ήχους κλήσης του modem).

Θα λάβετε έναν απρόσμενα υψηλό λογαριασμό τηλεφώνου, στον οποίο θα βρείτε κλήσεις σε άγνωστους αριθμούς υψηλής χρέωσης ή αριθμούς εξωτερικού.

Είναι πιθανόν, παρά το γεγονός ότι θα είστε συνδεδεμένοι στο διαδίκτυο, να μην μπορείτε να στείλετε ηλεκτρονικά μηνύματα αλληλογραφίας. Πολλές φορές ανοίγουν αυτόματα σελίδες «αμφιλεγόμενου περιεχομένου», χωρίς να έχει ζητηθεί κάτι τέτοιο από τον χρήστη.

Μπορεί να έχουν προστεθεί αυτόματα νέα εικονίδια στην επιφάνεια εργασίας του υπολογιστή σας.

Είναι αρκετά πιθανόν, η ταχύτητα της σύνδεσής σας με το διαδίκτυο να είναι πολύ χαμηλότερη από ότι συνήθως.

ΤΡΟΠΟΙ ΑΠΟΦΥΓΗΣ ΤΩΝ DIALERS ΚΑΙ ΤΩΝ ΥΨΗΛΩΝ ΤΗΛΕΦΩΝΙΚΩΝ ΧΡΕΩΣΕΩΝ



Να κλείνετε τον υπολογιστή σας όταν δεν τον χρησιμοποιείτε.

Ποτέ μην ανοίγετε συνημμένα αρχεία που λαμβάνετε μέσω e-mail αν δεν γνωρίζετε τι είναι.

Εξετάζετε συχνά τις παραμέτρους σύνδεσης του υπολογιστή σας με το διαδίκτυο για να βεβαιώνετε ότι ο αριθμός που καλεί το modem σας για να συνδεθεί είναι ο σωστός.

Ωστόσο, ακόμα κι αν όλα φαίνονται φυσιολογικά δεν αποκλείεται να υπάρχει εγκαταστημένος dialer.

Αποφύγετε επισκέψεις σε ιστοσελίδες αμφιλεγόμενου περιεχομένου. Μην κάνετε λήψη ή εγκατάσταση προγραμμάτων από τέτοιες ιστοσελίδες. Όμως, ακόμη και απλή επίσκεψη στις ιστοσελίδες αυτές μπορεί να μολύνει τον υπολογιστή σας.

Να είστε ιδιαίτερα επιφυλακτικοί αν κατά την περιήγησή σας στο διαδίκτυο μεταφερθείτε σε κάποια ιστοσελίδα την οποία δεν περιμένατε. Εάν κατά λάθος βρεθείτε σε μία τέτοια ιστοσελίδα, κλείστε όλα τα αναδυόμενα παράθυρα που ανοίγουν.

Να έχετε ρυθμίσει δυνατά την ένταση του modem σας έτσι ώστε να ακούσετε τους ήχους στην περίπτωση που το modem σας αποσυνδεθεί και επιχειρήσει να πραγματοποιήσει και πάλι κλήση.

Αν προσέξετε κάποιο άγνωστο εικονίδιο στην επιφάνεια εργασίας του υπολογιστή σας που δεν αντιστοιχεί σε έγκυρη εφαρμογή, τότε εξετάστε το και διαγράψτε το. Βέβαια, θα πρέπει να απεγκαταστήσετε και τη σχετική εφαρμογή.

Οι περισσότεροι dialers ανιχνεύονται από τα αντιικά προγράμματα. Βεβαιωθείτε ότι το αντιικό σας πρόγραμμα παρέχει αυτή τη δυνατότητα και φροντίστε να το ενημερώνετε συστηματικά.

Στην περίπτωση όπου η σύνδεσή σας με το διαδίκτυο είναι αποκλειστικά με ευρυζωνική σύνδεση δεν απειλείστε από προγράμματα dialers. Ωστόσο, στην περίπτωση που ο υπολογιστής εκτός της ADSL σύνδεσης έχει εγκατεστημένο και κάποιο ISDN ή PSTN modem το οποίο είναι συνδεδεμένο μέσω καλωδίου σε τηλεφωνική γραμμή, τότε δεν μπορούμε να αποκλείσουμε τον κίνδυνο.

ΕΙΚΟΝΙΚΗ ΖΩΗ Ή ΠΡΑΓΜΑΤΙΚΗ;



ΑΛΛΙΩΣ ΒΛΕΠΕΙΣ ΤΗ ΖΩΗ ΜΕΣΑ ΑΠΟ ΕΝΑ ΚΑΔΡΟ....



ΚΑΙ ΑΛΛΙΩΣ ΣΤΗΝ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ

BIBΛΙΟΓΡΑΦΙΑ

<http://www.clickatlife.gr/story/euzoia/anakoufiste-ta-matia-sas-apo-ton-upologisti-me-10-tropous?id=2062511>

<http://www.google.gr> Αναζήτηση πληροφοριών-εικόνων

<http://cyberkid.gov.gr/>

<http://www.psychotherapeia.net.gr/index.php/articles-psyxologoi-marousi-psyxotherapeftes-marousi/exartiseis/18-agorastikh-exarthsh/18-yperkatanalwsh-agathwn-agorastikh-exarthsh>

<http://www.vlioras.gr/Philologia/Composition/Katanalosi.htm>

http://www.pi.ac.cy/InternetSafety/sec_facebook.html

Πληροφορίες για την παροχή ψευδών πληροφοριών:

<http://www.cnnic.net.cn/en/index/OQ/index.html>

Πληροφορίες για το Phishing:

<http://www.forthnet.gr/templates/viewcontentTmCh.aspx?c=10009043>

Graham, G. Το Internet μια κοινωνιολογική προσέγγιση, Αθήνα: Εκδόσεις: Περίπλους, 2001

Παναγιωτοπούλου, Ρ. Η ψηφιακή πρόκληση, Αθήνα: Εκδόσεις: Τυποθήτω, 2003

Αγάθωνος - Γεωργοπούλου Ελένη. Κακοποίηση των παιδιών, Αθήνα: Εκδόσεις:

Ινστιτούτο Υγείας του Παιδιού, 1991

Η χρήση του διαδικτύου στην Ελλάδα και στην Ευρώπη, Εφημερίδα Έθνος

«Ενημέρωση» Έκδοση Κέντρου Συμπαραστάσεως Προνοίας Απ. Παύλου «Η Ελπίδα»

Kimberly S. Young, Internet Addiction: The emergence of a new clinical disorder.

Keith W. Beard and EVE M. WOLF, Modification in the proposed Diagnostic Criteria for internet addiction.

www.obrela.gr

www.paideia-news.com

www.vlioras.gr

www.section.gr

www.psych.gr

www.youth-helth.gr

<http://www.plinet.gr/index.php/>

<http://en.wikipedia.org/wiki/Blog>,

<http://pacific.jour.auth.gr>

<http://www.sch.gr>

<http://www.chiosnews.com>

<http://www.zougla.gr>