ΠΕΡΙΕΧΟΜΕΝΑ

CONTENTS

ΠΡΟΛΟΓΟΣ

Η πληροφορική και τα πολυμέσα προσφέρουν πολλές δυνατότητες και σε ιδιώτες και σε επιχειρηματίες. Εκτός της ηλεκτρονικής επικοινωνίας μέσα από τηλέφωνο, φαξ και ηλεκτρονικό ταχυδρομείο, τα πολυμέσα έχουν επεκταθεί και σε άλλες καθημερινές μας δραστηριότητες, όπως:

- Ψυχαγωγία
- Αναζήτηση πληροφοριών
- Ηλεκτρονική επικοινωνία
- Ηλεκτρονικές αγορές

Καθώς γίνεται λόγος για τις ηλεκτρονικές αγορές πρέπει να αναφερθεί ότι τα τελευταία χρόνια γενικότερα το ηλεκτρονικό εμπόριο έχει εξελιχθεί ραγδαία. Η εταιρεία ερευνών αγοράς Gartner υπολογίζει ότι οι πωλήσεις μέσω διαδικτύου το 2002 στην Ευρώπη θα φτάσουν σχεδόν τα 98 εκατομμύρια ευρώ-δηλαδή θα ανέβουν κατά 48% σε σχέση με τον προηγούμενο χρόνο. Σύμφωνα με τις προβλέψεις των αναλυτών μέχρι το 2005 οι πωλήσεις μέσω διαδικτύου θα φτάσουν γύρω στα 260 δισεκατομμύρια ευρώ. (***Ημερησία Σαββατοκύριακο 23-24 Νοεμβρίου 2002***). Τι είναι όμως το ηλεκτρονικό εμπόριο;

Ηλεκτρονικό Εμπόριο(Η.Ε.) είναι η επικοινωνία και η σύναψη εμπορικών συναλλαγών μεταξύ επιχειρήσεων ή μεταξύ των επιχειρήσεων και των πελατών τους, με τη χρήση ηλεκτρονικών μέσων (*Ηλεκτρονικό Εμπόριο, Α. Πασχόπουλος Π. Σκαλτσάς. εκδόσεις κλειδάριθμος 2000)*

Το πρόβλημα με τον παραπάνω ορισμό είναι ότι δεν περικλείει τη φιλοσοφία του Η.Ε. η οποία είναι ο επανακαθορισμός του τρόπου με τον οποίο γίνονται οι εμπορικές συναλλαγές και ο οποίος έχει ως στόχο την αμοιβαία ωφέλεια των επιχειρήσεων και των πελατών τους. Ουσιαστικά το ηλεκτρονικό εμπόριο που αφορά τον κοινό καταναλωτή διενεργείται κατά κύριο λόγο μέσω του διαδικτύου, ενώ οι επιχειρήσεις μεταξύ τους χρησιμοποιούν και άλλα δίκτυα (L.A.N.S, M.A.N.S, W.A.N.S, V.A.N.S)

Η διακίνηση του Η.Ε περιλαμβάνει ορισμένα θέματα που σχετίζονται με τα δικαιώματα των πολιτών(νομικά αλλά και ηθικά θέματα)Συνοπτικά μερικά από τα θέματα αυτά είναι:

1.Προστασία Απορρήτου
2.Πνευματική Ιδιοκτησία
3.Ελευθερία Έκφρασης
4.Προστασία Καταναλωτή

Η ΔΙΑΣΦΑΛΙΣΗ ΤΟΥ ΑΠΟΡΡΗΤΟΥ

Η διασφάλιση του απορρήτου είναι ένα παλιό νομικό και ηθικό ζήτημα, σχεδόν σε ολόκληρο τον πλανήτη. **Απόρρητο** είναι η αξίωση ατόμων, ομάδων ή ιδρυμάτων να καθορίζον μόνοι τους πότε και σε ποια έκταση, πληροφορίες για αυτούς γίνονται γνωστές σε κάποιους άλλους(Agranoff 1993). Η παραβίαση του δικαιώματος του απορρήτου στο διαδίκτυο είναι πολύ συχνή και επηρεάζει το ηλεκτρονικό εμπόριο άμεσα. Ίσως από τις πιο γνωστές περιπτώσεις παραβίασης του δικαιώματος του απορρήτου, μπορούν να βρεθούν στο βιβλίο "Ο φάκελος" του Peter Kimball, πρώην καθηγητή δημοσιογραφίας στο Columbia University. Όταν δημοσιοποιήθηκε ο προσωπικός του φάκελος από το F.B.I, έγινε εμφανές ότι για περισσότερα από 30 χρόνια είχε κατηγοριοποιηθεί ως ανεπιθύμητος πολίτης και άτομο που συμπαθούσε τον κομμουνισμό. Αυτό ήταν προϊόν δύο γεγονότων που συνέβησαν νωρίς στη ζωή του. Το πρώτο συνέβη όταν έκανε αίτηση για μια κυβερνητική θέση λίγο μετά την "απόλυσή" του από τους πεζοναύτες στο τέλος του 2ου παγκοσμίου πολέμου. Κάποιος από αυτούς που εξέτασαν την αίτησή του αμφισβήτησε τις πολιτικές του θέσεις αλλά δεν έκανε καμία αναφορά στον κομμουνισμό. Το δεύτερο γεγονός ήταν όταν απέρριψε μια κυβερνητική θέση που του είχε προταθεί ώστε να αναλάβει μια πιο πολλά υποσχόμενη θέση σε μια από τις κορυφαίες αμερικάνικες εφημερίδες. Στο βιβλίο του, ο Kimball δείχνει πως μέσα σε μια περίοδο 30 ετών, αυτά τα γεγονότα καθώς, και οι μετέπειτα έρευνες που έγιναν σε μια προσπάθεια αποσαφηνισμού των λόγων για την απόρριψη της θέσης, συνδυάστηκαν και μεγαλοποιήθηκαν σε τέτοιο βαθμό, ώστε ο φάκελός του να λάβει της προσοχής του J. Edgar Hoover και οι μετέπειτα αιτήσεις του για κυβερνητικές και ακαδημαϊκές θέσεις ακόμη και για διαβατήρια να επηρεαστούν σοβαρά.

Παρόλο που η υπόθεση του Kimball είναι συνυφασμένη με την περίοδο που τα αρχεία κρατούνταν σε φυσικό και όχι ηλεκτρονικό μέσο, οι προεκτάσεις της είναι πιο εφιαλτικές δεδομένης της ευκολίας με την οποίο μπορεί να πραγματοποιηθεί μαζική ηλεκτρονική παρακολούθηση και υψηλής τεχνολογίας συλλογή πληροφοριών. Ακόμη παρότι τις τελευταίες δεκαετίες οι δυνατότητες της τεχνολογίας για συλλογή τεράστιων ποσών πληροφοριών έχουν αυξηθεί εκθετικά, οι δυνατότητες των ανθρώπων να κρίνουν την αξία και την εγκυρότητα τέτοιων πληροφοριών δεν έχει βελτιωθεί καθόλου. Είναι χαρακτηριστικό ότι ανάμεσα στο 77% των χρηστών του Internet που δεν έχουν αγοράσει ποτέ προϊόντα online, το 86% αποτρέπεται από τον φόβο ότι άλλοι μπορούν να χρησιμοποιήσουν τον αριθμό των πιστωτικών τους καρτών ,η άλλες ιδιωτικές πληροφορίες χωρίς την συναίνεση τους.

Σύμφωνα με την Αμερικάνικη Ένωση Δικαιωμάτων του Ανθρώπου (American Civil Liberties Union-***http://forms.aclu.org/***)δεκάδες εκατομμύρια χρηστών υπολογιστών παρακολουθούνται, πολλοί χωρίς να το ξέρουν.

Είναι ίσως περίεργο αλλά η μεγαλύτερη απειλή στην ιδιωτικότητά μας δεν προέρχεται πλέον από το κράτος το οποίο μάλιστα σε ένα βαθμό είναι δημοκρατικά ελέγξιμο, αλλά από τις ιδιωτικές εταιρείες. Έτσι λοιπόν πληροφορίες συλλέγουν διάφορες εταιρείες που παρακολουθούν την πορεία του χρήστη στο διαδίκτυο και προσπαθούν να δημιουργήσουν ένα προφίλ προκειμένου να γνωρίζουν τα ενδιαφέροντα του και να προσφέρουν τα προϊόντα και τις υπηρεσίες που τον ενδιαφέρουν άμεσα.

Η παρακολούθηση γίνεται όμως και από κυβερνήσεις ,μυστικές υπηρεσίες ή την αστυνομία. Προσπαθούν να εντοπίσουν επικίνδυνα άτομα στο διαδίκτυο. Μάλιστα σύμφωνα με τις νέες οδηγίες που εξέδωσε το υπουργείο δικαιοσύνης των Η.Π.Α μετά το χτύπημα της 11ης Σεπτεμβρίου, στον πόλεμο κατά της τρομοκρατίας οι πράκτορες του F.B.I θα μπορούν να παρακολουθούν οποιαδήποτε ιστοσελίδα οποιονδήποτε χρήστη, ακόμη και αν δεν κατατάσσεται στους υπόπτους. Δηλαδή μπορεί κάποιος να διενεργεί απολύτως νόμιμες δραστηριότητες όπως ηλεκτρονικές αγορές και οι πράκτορες του F.B.I να τον παρακολουθούν χωρίς μάλιστα να χρειάζεται να λογοδοτήσουν πουθενά***(Susan Schmidt and Dan Eggen.Washington Post Staff Writers. Thursday, May 30, 2002)***

Το απόρρητο παραβιάζεται ακόμη και από τους εργοδότες. Παρακολουθούν τις διαδικτυακές συναλλαγές, συνομιλίες και άλλες δραστηριότητες των εργαζομένων. Σύμφωνα με μία μελέτη του AMA(American Management Association) πάνω από τα ¾ των μεγάλων αμερικάνικων εταιριών καταγράφουν και παρακολουθούν επικοινωνίες και δραστηριότητες κατά τη διάρκεια της δουλειάς, συμπεριλαμβανομένων E-Mail,αρχεία υπολογιστή και συνδέσεις Internet.Το 2001 το 62% των διευθυντών επιχειρήσεων είπε ότι παρακολουθεί τις διαδικτυακές συνδέσεις. Το 46% αποθηκεύει μηνύματα E-Mail,και το 36% αποθηκεύει και υποκλέπτει αρχεία υπολογιστή (***NewsFactor Network,June 29,2001,Lou Hirsch .The Boss is Watching :Workplace Monitoring on the Rise http://www.newsfactor.com/perl/story/11634.html)***

Κάποιοι άλλοι που συχνά παραβιάζουν το απόρρητο είναι οι γνωστοί Hackers. Αν και υπάρχουν πιθανόν πολλές απαντήσεις γιατί οι Hackers κάνουν Hacking η πιο συνηθισμένη απάντηση είναι ότι μάχονται για ελεύθερο και ανεξάρτητο Internet.Με βάση αυτή τη λογική δεν πρέπει να υπάρχει τίποτα που να μένει κρυφό και για το λόγο αυτόν επιχειρούν να ανοίξουν όλους τους διαδρόμους του Internet στο ευρύ κοινό. Στους πιθανούς στόχους των Hacker δεν βρίσκονται μόνο οι κυβερνήσεις αλλά μεγάλες πολυεθνικές και απλοί χρήστες***.(Chip. Το hacking και πως να το αποφύγετε. Γιώργος Ψαρουλάκης, Νάσια Χρυσουλά, Γιώργος Πολύζος).***

Με ποιο τρόπο όμως παρακολουθούνται οι χρήστες του Internet;Το σίγουρο είναι ότι μόνο ένα μέρος των τρόπων είναι γνωστό στο ευρύ κοινό.

Ένας από αυτούς είναι τα «**cookies**».Ένα «cookie» είναι ένα κομμάτι πληροφορίας που επιτρέπει σε ένα δικτυακό τόπο να καταγράφει τις εισόδους και τις εξόδους ενός ατόμου. Τα cookies βοηθούν τους δικτυακούς τόπους να διατηρούν καταστάσεις χρηστών. Αυτό σημαίνει ότι οι δικτυακοί τόποι μπορούν να «θυμούνται» πληροφορίες για χρήστες και να αποκρίνονται στις προτιμήσεις τους για ένα συγκεκριμένο δικτυακό τόπο, να επεξεργάζονται διαφανείς κωδικούς πρόσβασης χρηστών κλπ.

Ένα «cookie» μπορεί να θεωρηθεί σαν μία προσωρινή ταυτότητα. Κάθε φορά που ένα άτομο μπαίνει σε ένα δικτυακό τόπο, είναι σαν να τον επισκέπτεται για πρώτη φορά. Τα cookies επιτρέπουν σε ένα δικτυακό τόπο να διατηρούν πληροφορίες για ένα συγκεκριμένο χρήστη μέσω συνδέσεων HTTP.

Ειδικότερα τα cookies επιτρέπουν σε δικτυακούς τόπους(servers) να διανέμουν απλά δεδομένα σε ένα πελάτη(χρήστη),να ζητούν από τον πελάτη αποθηκεύει τις πληροφορίες και σε ορισμένες περιπτώσεις να επιστρέφουν τις πληροφορίες στον δικτυακό τόπο.

Τα cookies έχουν δημιουργήσει πάρα πολλά προβλήματα αφού επιτρέπουν σε δικτυακούς τόπους να συλλέγουν ιδιωτικές πληροφορίες όπως προτιμήσεις

ενδιαφέροντα και τρόπους περιήγησης χρηστών στους δικτυακούς τόπους που επισκέπτονται οι χρήστες .

Ακόμη ο Internet Explorer και τα Windows αποτελούν συλλέκτες δεδομένων. Θα μπορούσε να πει κανείς ότι αφήνουν παντού «ίχνη».Πράγμα που καθιστά πολύ εύκολη την παρακολούθηση του προσωπικού Ηλεκτρονικού Υπολογιστή.

Επίσης γίνεται παρακολούθηση με τα προγράμματα PC Activity Monitoring.Τα προγράμματα αυτά σε γενικές γραμμές προσφέρουν αναφορές για προγράμματα και εφαρμογές που χρησιμοποιήθηκαν, για ιστοσελίδες(Web Sites) και Chat Rooms στα οποία έχει πραγματοποιηθεί επίσκεψη, αναλυτική αναφορά σχετικά με τα αρχεία που έχουν διαβαστεί, μετακινηθεί ή διαγραφεί και βέβαια αρκετά από αυτά διαθέτουν και ικανότητα screen capturing.Ορισμένα από τα προγράμματα αυτά είναι τα Iopus Starr pro edition, Net Observer 2.8, Spytech spy agent 4.2,Win recon 2.61,Win What Where Investigator 4.Όλα προσφέρουν στην ουσία τις ίδιες υπηρεσίες, που δεν είναι άλλες από την παρακολούθηση δραστηριοτήτων και την αναφορά τους. Αξίζει εδώ να σημειώσουμε ότι τα προγράμματα αυτά αποτελούν το συνηθέστερο μέσο για την παρακολούθηση των εργαζομένων από τους εργοδότες.

Όσον αφορά την παρακολούθηση και τους τρόπους που υπάρχουν, τα παραπάνω είναι ενδεικτικά. Υπάρχουν χιλιάδες τρόποι να παραβιαστεί το απόρρητο. Ακόμη και το Hardware δεν είναι ασφαλές. Στην εργασία του «Ηλεκτρομαγνητική ακτινοβολία της οθόνης:στόχος επίθεσης»ο Καθηγητής Βιμ Βαν Εκ, επέδειξε παραστατικά πόσο εύκολο είναι να επιτευχθεί μία υποκλοπή των υποσυστημάτων του υπολογιστή όπως είναι η οθόνη. Με έναν ενισχυτή σήματος, έναν δέκτη και μία απλή τηλεόραση μπορεί οποιοσδήποτε να δει τι υπάρχει σε μία οθόνη Η/Υ σε απόσταση 1000 μέτρων… ***(Chip. Το hacking και πως να το αποφύγετε. Γιώργος Ψαρουλάκης, Νάσια Χρυσουλά, Γιώργος Πολύζος).***

Όσον αφορά τα cookies υπάρχουν ορισμένες λύσεις. Πρώτα, οι χρήστες μπορούν να διαγράψουν τα αρχεία cookie.Επίσης μπορούν να χρησιμοποιήσουν λογισμικό αντί- cookie. Μερικά από αυτά είναι το Pretty Good Privacy's cookie Cutter,Luckman's.Anonymouscookie,CookieCrusher,WindowWasher.Πληροφορίες σχετικά με τα cookies και την αντιμετώπιση τους υπάρχουν στην διεύθυνση ***www.kburra.com/support.html***

Για την αντιμετώπιση του προβλήματος των προγραμμάτων περιήγησης όπως:Internet Explorer και Netscape Navigator υπάρχουν ορισμένες λύσεις όπως το I System Wiper 2.1,Virtual PC και VMWare 3.2 **(*Auf ihrer Faehrte,Andreas Perband,PC Welt 12/02*)**

Ένας διαδεδομένος τρόπος προστασίας δεδομένων είναι η κρυπτογράφηση. Κρυπτογράφηση είναι μια επιστήμη που βασίζεται στα μαθηματικά και την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Ο σκοπός των διαφόρων μεθόδων κρυπτογράφησης είναι να εξασφαλίζουν το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών.Το αρχικό μήνυμα ονομάζεται απλό κείμενο(plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα(ciphertext). Αποκρυπτογράφηση είναι ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Υπάρχουν πολλά προγράμματα κρυπτογράφησης όπως το FineCrypt v.NET Invisible Secrets v3.2 κ.α. Η κρυπτογράφηση αποτελεί αμφιλεγόμενο τρόπο προστασίας, αφού από μερικές κυβερνήσεις (π.χ Η.Π.Α) θεωρείται παράνομη.

(Chip. Το hacking και πως να το αποφύγετε. Γιώργος Ψαρουλάκης, Νάσια Χρυσουλά, Γιώργος Πολύζος).

Ένας τρόπος για να προστατευτεί το απόρρητο στο ηλεκτρονικό εμπόριο είναι να αναπτυχθούν πολιτικές προστασίας απορρήτου ή κώδικες, που μπορούν να βοηθήσουν οργανισμούς να αποφύγουν νομικά προβλήματα. Σε πολλούς οργανισμούς, η ανώτερη διοίκηση έχει αρχίσει να κατανοεί ότι η δυνατότητα συλλογής τεράστιων ποσοτήτων προσωπικών πληροφοριών πελατών και υπαλλήλων έρχεται μαζί με την υποχρέωση να σιγουρευτούν ότι οι πληροφορίες-και άρα τα άτομα-προστατεύονται. Ένας κώδικας προστασίας απορρήτου εκδόθηκε στις 22 Ιουνίου 1998 από τις κορυφαίες εταιρείες που ασχολούνται με το Ιντερνετ, περιλαμβανομένων των IBM και Microsoft. Ένα δείγμα πολιτικής προστασίας απορρήτου είναι το παρακάτω.

Κύριες Περιοχές Προβληματισμού είναι:

Συλλογές Δεδομένων

- Τα δεδομένα πρέπει να συλλέγονται για άτομα, μόνο για να επιτευχθεί ένας νόμιμος στόχος της επιχείρησης.
- Τα δεδομένα πρέπει να είναι αρκετά, σχετικά και όχι υπερβολικά σε σχέση με τον επιχειρηματικό στόχο.
- Τα άτομα πρέπει να έχουν δώσει την συναίνεση τους πριν να συλλεγούν δεδομένα που τα αφορούν. Τέτοια συναίνεση μπορεί να υπονοείται από τις ενέργειες του ατόμου(π.χ., αιτήσεις για πίστωση, ασφάλεια ή αίτηση εργασίας)

Ακρίβεια Δεδομένων

- Ευαίσθητα δεδομένα που συλλέγονται πρέπει να επαληθεύονται πριν να εισαχθούν στη βάση δεδομένων.
- Τα δεδομένα πρέπει να είναι ακριβή και όπου είναι αναγκαίο να κρατούνται ενήμερα
- Το αρχείο πρέπει να γίνεται διαθέσιμο έτσι ώστε το άτομο να μπορεί να επιβεβαιώσει ότι τα δεδομένα είναι σωστά.
- Αν υπάρχει ασυμφωνία για την ακρίβεια των δεδομένων, πρέπει να σημειωθεί η εκδοχή που δίνεται από το άτομο και να περιληφθεί μαζί με το αρχείο.

Εμπιστευτικότητα Δεδομένων

- Πρέπει να υλοποιηθούν διαδικασίες ασφάλειας υπολογιστών, που να παρέχουν λογική εξασφάλιση από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων. Αυτές πρέπει να περιλαμβάνουν φυσικά, τεχνικά και διοικητικά μέτρα ασφαλείας .
- Οι τρίτοι δεν πρέπει να έχουν πρόσβαση στα δεδομένα, χωρίς την γνώση ή την άδεια του ατόμου εκτός και αν απαιτείται από τον νόμο.
- Αποκαλύψεις δεδομένων, εκτός των πλέων βασικών πρέπει να σημειώνονται και να διατηρούνται για όσο χρονικό διάστημα διατηρούνται και τα δεδομένα.
- Τα δεδομένα δεν πρέπει να αποκαλύπτονται για λόγους που δεν είναι συμβατοί με τον επιχειρηματικό στόχο για τον οποίο συννελέγησαν

ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ

Η δημιουργία και ανάπτυξη του Internet έχει σίγουρα οδηγήσει στην έλευση ενός ηλεκτρονικά διασυνδεόμενου κόσμου και οι πειρατές των δεδομένων ενδέχεται να μην είναι μακριά . Υποστηρίζεται από πολλούς ότι το διαδίκτυο θα γίνει γρήγορα μία μεγάλη αντιγραφική μηχανή για λογισμικό,CD και ταινίες, καταστρέφοντας χιλιάδες εργασιών και έσοδα εκατομμυρίων δολαρίων. Τρία στα τέσσερα πακέτα επαγγελματικού software που κυκλοφορούν στην Ελλάδα είναι πειρατικά δημιουργώντας μια οιονεί απώλεια εσόδων στις εταιρείες λογισμικού της τάξης των 19,5 δις δραχμών! Αυτές είναι οι εκτιμήσεις της Business Software Alliance (BSA), μιας παγκόσμιας οργάνωσης που δημιουργήθηκε από δεκαπέντε μεγάλες εταιρείες πληροφορικής με αποκλειστικό στόχο την καταπολέμηση της πειρατείας. Στις Ηνωμένες Πολιτείες και οπουδήποτε αλλού στον κόσμο, οι πολιτικοί αγωνίζονται ήδη για να εφαρμόσουν πολιτικές για την προστασία πολύτιμων πληροφοριών από την ηλεκτρονική αρπαγή. Οι εμπνευστές αυτών των πολιτικών διαβλέπουν στον ορίζοντα την πειρατική σημαία των ψηφιακών πειρατών, οι οποίοι θα εξορμούν για να κλέβουν τα προϊόντα των "πλούσιων" παραγωγών της πληροφορίας.

Παρακάτω θα παρατεθούν ορισμένα νομικά περιστατικά σχετικά με την πνευματική ιδιοκτησία(Πνευματική ιδιοκτησία είναι η μη απτή ιδιοκτησία που δημιουργείται από άτομα ή οργανισμούς, που προστατεύεται από το νόμο περί πνευματικών δικαιωμάτων και δίνει την ιδιοκτησία επί του δημιουργήματος για κάποιο χρονικό διάστημα)και τη σημασία της στις σύγχρονες αγορές. Ένα σημαντικό θέμα είναι η χρονική περίοδος κατά την οποία μια πνευματική δημιουργία παραμένει εκμεταλλεύσιμη από τους δικαιούχους. Στις Ηνωμένες Πολιτείες, για παράδειγμα, η περίοδος αυτή είναι 75 χρόνια ή 50 χρόνια μετά το θάνατο του δημιουργού. Μετά το πέρας αυτής της περιόδου, το δημιούργημα καθίσταται δημόσια περιουσία.

Δημοσιεύτηκε στο ένθετο **"New Millenium**" του "**Τύπου της Κυριακής" (31/1/1999)**

Ενώ όλος ο κόσμος ήταν απασχολημένος με τις ανάρμοστες σχέσεις του προέδρου των ΗΠΑ, ο Michael D. Eisner, πρόεδρος του κολοσσού των media Disney Co τρύπωνε κρυφά στην αμερικανική Βουλή για να δώσει προσωπικά μια από τις μεγαλύτερες μάχες της εταιρείας του. Η αποκλειστική εκμετάλλευση του Μίκυ Μάους (του μεγαλύτερου ίσως περιουσιακού της στοιχείου) θα σταματούσε σε δύο χρόνια. Σύμφωνα με την αμερικανική νομοθεσία, κάθε πνευματικό δημιούργημα γίνεται δημόσια περιουσία μετά τα 75 χρόνια εκμετάλλευσης από μια εταιρεία ή 50 χρόνια μετά το θάνατο του δημιουργού του. Ο Michael D. Eisner μίλησε με γερουσιαστές, πίεσε καταστάσεις, θύμισε πόσα έκανε η εταιρεία του για την προεκλογική τους εκστρατεία (και πόσα ίσως θα μπορούσε να κάνει στις ερχόμενες εκλογές) και πέτυχε αυτό που φοβούνταν όλοι. Η περίοδος εκμετάλλευσης των πνευματικών δικαιωμάτων από τις εταιρείες παρατάθηκε κατά 20 χρόνια. Μαζί όμως με το χρυσοφόρο ποντίκι παρατάθηκε στα 95 χρόνια και η εκμετάλλευση όλων των πνευματικών δημιουργημάτων. Πολλά από αυτά ήδη είχαν γίνει δημόσια περιουσία και βρίσκονταν ελεύθερα διαθέσιμα στο Internet. Το νέο νομοθετικό διάταγμα στην ουσία καθιστά παράνομους δεκάδες βιβλιοθήκες και πανεπιστήμια που είχαν ηλεκτρονικά κάποια έργα που εκδόθηκαν πριν το 1923.

Ο Eric Eldred είναι ένας από τους δεκάδες χρήστες, που έχει ως χόμπι να βρίσκει παλιά βιβλία (πριν το 1923) τα οποία περνά στο Internet για να έχουν πρόσβαση όλοι. Οι σελίδες του ξαφνικά έγιναν παράνομες. Όλα τα βιβλία που είχαν γραφεί μεταξύ των ετών 1903-1923 και τα είχε στη σελίδα του, παραβίαζαν το νόμο περί πνευματικής ιδιοκτησίας. Η πρώτη του σκέψη ήταν να "καταστρέψει" τις σελίδες, όταν δέχτηκε το τηλεφώνημα μιας ομάδας διαπρεπών νομικών του **Harvard**, οι οποίοι του ζητούσαν να ασκήσει το δικαίωμα της δημόσιας ανυπακοής σε ένα αντισυνταγματικό νόμο και, μαζί με τη βοήθειά τους, να τον προσβάλει στα δικαστήρια (http://eon.law.harvard.edu/openlaw/eldredvashcroft/)Έτσι κι έγινε. Η ομάδα υπεράσπισής του, που περιλαμβάνει μερικά από τα λαμπρότερα νομικά μυαλά στον τομέα της πνευματικής ιδιοκτησίας, αποφάσισε να πολεμήσει ενάντια στην "παραχώρηση δημόσιας περιουσίας σε ιδιωτικές εταιρείες και μάλιστα χωρίς αντάλλαγμα".

Η ιστορία αυτή της επέκτασης των αποκλειστικών δικαιωμάτων εκμετάλλευσης της πνευματικής ιδιοκτησίας κατά είκοσι χρόνια είναι μια κλασική διαδικασία ιδιωτικοποίησης δημόσιου χώρου προς όφελος του κεφαλαίου και χωρίς αντάλλαγμα για το κοινό. Οι μεγάλες επιχειρήσεις παίρνουν θέση για την πληροφοριακή εποχή και προσπαθούν να ιδιωτικοποιήσουν κάθε δημιουργική έκφραση για όσο μεγαλύτερο χρονικό διάστημα μπορούν. Η προσπάθεια αυτή μεταλλάσσει τη φύση της πληροφορίας, η οποία από ελεύθερο δημόσιο αγαθό γίνεται εμπόρευμα.

Ένα άλλο παράδειγμα όμως είναι το παράδειγμα του Gil Trevizo. Ο Gil Trevizo ήταν ένας 25χρονος σπουδαστής που του άρεσε η τηλεοπτική σειρά επιστημονικής φαντασίας Millennium.Μπόρεσε να βρει βίντεο του 1ου επεισοδίου και άλλες πληροφορίες και εικόνες που αφορούσαν την εκπομπή. Αφιέρωσε τον δικτυακό του τόπο στο Πανεπιστήμιο του Τέξας στην εκπομπή πρίν ακόμα από τη πρεμιέρα της εκπομπής το 1996.Η σειρά ανήκει στην **Twentieth Century-Fox**,που είχε τον δικό της δικτυακό τόπο αφιερωμένο στη σειρά, Το πανεπιστήμιο έσβησε τον λογαριασμό του Gil Trevizo,όταν η Fox τους ειδοποίησε για την πειρατεία του υλικού της που προστατευόταν από πνευματικά δικαιώματα. Ο Trevizo εξάλειψε το υλικό από τον δικτυακό του τόπο.

Αν και ο Trevizo δεν είχε κανένα οικονομικό όφελος, η Fox θα μπορούσε να πληγεί από τον δικτυακό του τόπο. Η Fox ξόδεψε πάνω από $100.000 στον δικτυακό της τόπο όπου πωλείτο προωθητικό υλικό. Αν οι θεατές πήγαιναν στον δικτυακό τόπο του Gil,τότε λιγότεροι θα πήγαιναν στον επίσημο δικτυακό τόπο(**ΗλεκτρονικόΕμπόριο, Turban, Lee, King, Chung. Εκδόσεις Μ.Γκιούρδας, Αθήνα 2002**)

Επίσης χαρακτηριστικές είναι οι εφαρμογές **Peer-to-Peer (P2P)**.Ο ρόλος των εφαρμογών αυτών είναι η διαμοίραση(Sharing)αρχείων σε ένα εικονικό δίκτυο που αποτελείται από ένα σύνολο υπολογιστών που ονομάζονται Peers.

Κάθε Peer μοιράζεται στο εικονικό δίκτυο έναν αριθμό αρχείων, ο οποίος καθορίζεται από το χρήστη και με αυτόν τον τρόπο δημιουργείται μια πολύ μεγάλη βάση δεδομένων, προσπελάσιμη από όλους τους υπολογιστές που είναι συνδεδεμένος στο εικονικό αυτό δίκτυο.

Η ιδιαιτερότητα αυτού του τρόπου δημιουργίας δικτύων είναι ότι κάθε υπολογιστής αναλαμβάνει ταυτόχρονα το ρόλο του server και του client και έχει τα ίδια δικαιώματα με όλους τους υπόλοιπους Peers. Οι εφαρμογές που έχουν να κάνουν με τον συγκεκριμένο τρόπο ανταλλαγής αρχείων ονομάζονται Peer-to-

Peer και είναι φανερό ότι μπορουν να καταπατήσουν πνευματικά δικαιώματα και γιαυτό κάποιες από αυτές εκδιώχθηκαν νομικά(π.χ. το **Napster,Audio Galaxy**).
(Chip 23/2002,28/11/2002,Γιώργος Πολύζος-File sharing στην πράξη)

Αρχικά δεν υπήρχαν νόμοι που να αφορούν δικαιώματα προστασίας λογισμικού. Οι νόμοι που υπήρχαν αναφερόταν σε φυσικά προϊόντα και όχι σε ψηφοποιημένο λογισμικό. Αυτό δημιούργησε αρκετά προβλήματα και είχε ως αποτέλεσμα την προσπάθεια των νομοθετών να προσαρμόσουν την νομοθεσία στα σύγχρονα προβλήματα.Στην Ελλάδα ισχύει Νόμος 2121/1993(περί πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων-**http://aepi.gr/first.htm**)ενώ ισχύει και η οδηγία 2001/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 22ας Μαΐου 2001,για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας(επίσημη εφημερίδα **αριθ.L167** της 22/06/2001 σ.0010-0019:**http://users.otenet.gr/%7Ehatzikal/Pubr-a7-3.html**)

Επειδή οι νόμοι περί πνευματικών δικαιωμάτων στην ψηφιακή εποχή προκαλούνται, απαιτούνται διεθνείς συμφωνίες. Το 1996,ο Διεθνής Οργανισμός Πνευματικής ιδιοκτησίας άρχισε να συζητά την ανάγκη για προστασία των πνευματικών δικαιωμάτων της πνευματικής ιδιοκτησίας που διανέμεται στο Internet.Περισσότερα από 60 κράτη μέλη προσπάθησαν να γεφυρώσουν τις πολιτιστικές και πολιτικές τους διαφορές και έφτασαν σε μία διεθνή συμφωνία. Μέρος της συμφωνίας που έγινε το 1998 ονομάζεται συμφωνία βάσης δεδομένων και ο στόχος της είναι να προστατεύσει την επένδυση των εταιρειών που συλλέγουν και κατατάσσουν πληροφορίες. Αυτός ο οργανισμός εργάζεται συνέχεια επάνω σε πολλά ανεπίλυτα προβλήματα.
Ακόμη όμως και με την ισχύουσα νομοθεσία είναι πολύ δύσκολο να ελεγχθεί ολόκληρο το διαδίκτυο. Αυτήν τη στιγμή λειτουργούν ανενόχλητα αρκετές εφαρμογές **P2P** και φιλοξενούν αρκετά εκατομμύρια χρηστών. Οι πλέον γνωστές είναι:

- Kazaa Media Desktop(www.kazaa.com)
- Gnuttella v0.56(http://gnutella.wego.com/)
- E-Donkey2000(www.edonkey2000.com)

Ακόμη όμως και αν εντοπιστούν οι παραπάνω εφαρμογές, η πειρατεία των αρχείων γίνεται και με άλλους τρόπους. Ενδεικτικά ένας από αυτούς:Όταν ο server δεν επιτρέπει να ανεβούν στις σελίδες αρχεία μουσικής, ταινιών η αρχεία προγραμμάτων μερικοί τα καμουφλάρουν σαν αρχεία JPG.Ένα καλό εργαλείο για το καμουφλάρισμα αυτό είναι το πρόγραμμα Barabbas File Hide(Freeware version 1.2.4 για Windows 95/98/Me,Nt4,2000 και XP στο http://barabbas.da.ru).Έτσι είναι πολύ απλό οποιαδήποτε αρχεία να τα κρεμάσουμε σε ένα JPG αρχείο. Αφού κατεβάσει ο ενδιαφερόμενος το JPG αρχείο σε κάποιον υπολογιστή μπορεί με το Barabbas File Extract να το μετατρέψει στην αρχική του μορφή(**PCWelt 12/02 Geheim,gratis,illegal.Thorsten Eggeling)**

ΕΛΕΥΘΕΡΙΑ ΕΚΦΡΑΣΗΣ

Ο τρόπος με τον οποίο εξελίχθηκε το Ηλεκτρονικό Εμπόριο έφερε στην επιφάνεια πολλές φιλονικίες σχετικά με την ελεύθερη έκφραση και την λογοκρισία.

Πολλές έρευνες δείχνουν ότι το θέμα της λογοκρισίας είναι από τα πιο σημαντικά ζητήματα για τους χρήστες του διαδικτύου. Η λογοκρισία αναφέρεται στην προσπάθεια της κάθε κυβέρνησης(αλλά και ανεξάρτητων φορέων όπως το Enough)να ελέγξει το περιεχόμενο του διαδικτύου.

Σύμφωνα με τους νόμους που αφορούν τα ανθρώπινα δικαιώματα σχεδόν σε όλες τις δημοκρατικές χώρες, θεωρητικά τουλάχιστον ο καθένας έχει το δικαίωμα της γνώμης και της έκφρασης. Αυτό το δικαίωμα περιλαμβάνει την ελευθερία να έχει γνώμη χωρίς παρεμβάσεις και να ψάχνει, να δέχεται και να μεταδίδει πληροφορίες και ιδέες μέσω οποιουδήποτε μέσου και ανεξάρτητα συνόρων. Το internet μπορεί να γίνει ένα ριζικά φιλελεύθερο εργαλείο με ελευθερία έκφρασης. Προσφέρει γρήγορη και (σχετικώς) φτηνή ένα προς ένα επικοινωνία τόσο εθνικά όσο και διεθνώς. Παρέχει επίσης μέσα στους πολίτες που έχουν κάποιο κοινό ενδιαφέρον να βρουν άλλα ομόδοξα πρόσωπα και να επικοινωνήσουν μαζί τους. Υπάρχουν όμως πολλές φωνές που ζητούν τη λογοκρισία στον παγκόσμιο ιστό. Ένα παράδειγμα προσπάθειας λογοκρισίας είναι το παρακάτω:

Ένας Γερμανός δικαστικός λειτουργός, λοιπόν, αποφάσισε ότι κάποια τμήματα του Internet είναι ακατάλληλα για τους νεαρούς βλαστούς της Βαυαρίας. Προφανώς, κάπου άκουσε ότι στο δίκτυο υπάρχουν newsgroups στα οποία συζητώνται άσεμνα θέματα, όπως το σεξ. Η γερμανική νομοθεσία απαγορεύει την δημοσιοποίηση τέτοιων θεμάτων και ξεκίνησε την σταυροφορία του. Πρώτος του στόχος η Compuserve, μια εταιρεία παροχής δικτυακών υπηρεσιών που μαζί με όλα τα άλλα προσφέρει πρόσβαση και στο Internet. Επισκέφθηκε λοιπόν την θυγατρική της εταιρείας στην Γερμανία και τους είπε τα καθέκαστα. Τους διευκρίνισε ότι η γερμανική κοινωνία είναι πολύ ... σεμνή και δεν μπορεί να ανεχθεί κομπιούτερ που φωσφορίζουν στις οθόνες τους «κακές λέξεις», Ο ίδιος είχε ως πρώτιστο καθήκον να σώσει την νεολαία από την καταστροφή που έφερνε η τεχνολογική επανάσταση. Τους απείλησε με αγωγή και η Compuserve «συνεμορφώθει με τας υποδείξεις». (Η Γερμανία είναι μεγάλη αγορά για την εν λόγω εταιρεία και δεν ήθελε να ρισκάρει κάποια αποτυχία.) . Έτσι οι διευθύνοντες σύμβουλοι της Compuserve, αποφάσισαν να κόψουν την πρόσβαση των χρηστών τους από όλα τα newsgroups που έχουν στο όνομά τους το συνθετικό sex ή erotica - άσχετα αν αυτά τα newsgroups συζητούσαν για το ασφαλές σεξ ή το AIDS.

Υπήρχε όμως ένα πρόβλημα: ήταν αδύνατον τεχνολογικά να κόψουν τα newsgroup μόνο στην Γερμανία και να τα αφήσουν στον υπόλοιπο κόσμο. Γι αυτό το μακρύ χέρι του νόμου στης Βαυαρίας άγγιξε όλους τους χρήστες του συγκεκριμένου δικτύου. Όλοι οι συνδρομητές της Compuserve μετείχαν σε αυτές τις συζητήσεις, έμειναν ξεκρέμαστοι. Είτε βρισκόταν στην Γερμανία, είτε στις Η.Π.Α, είτε στην ... Κολομβία οι συνδρομητές των συγκεκριμένων newsgroup -- από το alt.erotica ή το alt.safe.sex, μέχρι το alt.erotica.bestiality) είδαν ένα πρωί ότι δεν μπορούσαν να έχουν (απ ευθείας) πρόσβαση σε αυτά. Διακόσια συνολικά newsgroup είχαν εξαφανιστεί... Αναζήτησαν την αιτία και οι ιθύνοντες της εταιρείας τους είπαν ότι ο Γερμανός εισαγγελέας μπορούσε τελικά να καθορίσει τι θα διαβάσει ή τι δεν θα δει ένας Νεοϋορκέζος! «Ευτυχώς --σχολίασε ένας χρήστης της Compuserve -- ο εισαγγελέας ήταν Γερμανός και όχι Σαουδάραβας. Τότε θα μπορούσε να μας αναγκάσει να βάζουμε τσαντόρ σε όλες τις φωτογραφίες γυναικών που έχει το Internet...». Ένας

άλλος σχολίασε πικρόχολα: «Οι Γερμανοί χτύπησαν για μια ακόμη φορά. Πάλι προσπαθούν να επιβάλλουν τις δικές τους αξίες σε όλο τον κόσμο...» Όπως ήταν επόμενο, υπήρξε θύελλα διαμαρτυριών. Οι φιλελεύθερες οργανώσεις των ΗΠΑ μίλησαν για «εξαγωγές και εισαγωγές ηθικών στάνταρτ», το θέμα πήρε μεγάλη δημοσιότητα στον Τύπο και όλοι αναρωτήθηκαν: πως μπορεί ένας περιφερειακός εισαγγελέας να καθορίσει την ροή των πληροφοριών σε παγκόσμιο επίπεδο; Η απάντηση βέβαια είναι ότι δεν μπορεί. Ότι και να κάνουν οι δικαστικοί του Μονάχου δεν μπορούν να κόψουν την πρόσβαση των «υπηκόων» τους στα «αμφιλεγόμενα» (για αυτούς) newsgroup. Αυτό είναι απόρροια της χαώδους δικτύωσης που έχει το Internet που τόσο ... υμνήθηκε.
Χωρίς κεντρική αρχή, χωρίς ένα συγκεκριμένο πομπό με πολλούς δέκτες είναι αδύνατον να ελεγχθεί η ροή της πληροφορίας. Στην συγκεκριμένη περίπτωση της Compuserve, μπορεί η εταιρεία να έκοψε την πρόσβαση στα επίμαχα newsgroups, οι χρήστες όμως της Compuserve μπορούν εύκολα να έχουν πρόσβαση σε αυτά!... Το πρόβλημα του εισαγγελέα είναι ότι μπορεί οι Γερμανοί χρήστες της Compuserve να μην έχουν απ ευθείας τα επίμαχα newsgroups, μπορούν όμως να μπαίνουν σε άλλα sites και να παίρνουν το περιεχόμενό τους. Το μόνο που κατάφερε η εισαγγελική παρέμβαση είναι να κάνει τα πράγματα πιο δύσκολα. Λογοκρισία, δεν μπόρεσε να επιβάλει. Πέρα από αυτό, οι Γερμανοί μπορούν να έχουν πρόσβαση στο Internet μέσω δεκάδων εταιρειών πλην της Compuserve που δραστηριοποιούνται στην Γερμανία.Οι εταιρείες αυτές πληθύνονται με γεωμετρικό ρυθμό και είναι αδύνατον κάποιος εισαγγελέας να παρακολουθήσει την ροή πληροφοριών που αυτές διοχετεύουν.

Τώρα όλη η προσπάθεια του είναι μάταια. Μπορεί ο ίδιος να μην το ξέρει, μπορεί αυτή η παρέμβαση να δημιούργησε (προσωρινά) προβλήματα σε όλο τον δικτυωμένο κόσμο έχει όμως και τα θετική πλευρά της. Η εισαγγελική αυτή παρέμβαση θέτει επί τάπητος τα μεγάλα προβλήματα και ευκαιρίες που δημιουργεί η κοινωνία των πληροφοριών. Είναι ένα έναυσμα συζήτησης για τους κανόνες που αλλάζουν με ταχύτατους ρυθμούς. Είναι μια ευκαιρία να αλλάξει ένα απαρχαιωμένο και περιοριστικό νομικό πλαίσιο που γεννήθηκε και ανδρώθηκε σε μια άλλη μορφή κοινωνίας -- εκείνης που ονομάζεται «βιομηχανικής κοινωνία» κοινωνία της μαζικότητας. Η νέα κοινωνία, θέλει νέους κανόνες, καινούργιο ρυθμιστικό πλαίσιο. Την επόμενη φορά που κάποιος εισαγγελέας θα προσπαθήσει να επιβάλλει την ηθική του στο «παγκόσμιο χωριό» θα ξέρει ότι θα «φάει τα μούτρα του»...(**Πάσχος Μανδραβέλης, Μια αφελής απόπειρα λογοκρισίας «Έθνος» , 21-1-1996)**

Ένα από τα κύρια σημεία στην φιλονικία της ελευθερίας λόγου εναντίον της λογοκρισίας, είναι η πιθανή βλάβη για τα παιδιά. Το δικτυακό περιεχόμενο στο οποίο μπορεί να έχει πρόσβαση ανά πάσα στιγμή ένα παιδί, είναι πολύ περισσότερο ακραίο από ότι μπορεί να δει στην τηλεόραση το βίντεο η κάποιο περιοδικό. Οι τόποι με βίαιο, άσεμνο, προπαγανδιστικό ή ανίερο περιεχόμενο υπάρχουν σε αφθονία στο Internet οπότε είναι θέμα χρόνου να τους συναντήσει ένας χρήστης.

Υπάρχουν τρείς(3) προσεγγίσεις σε ότι αφορά την προστασία των παιδιών από ακατάλληλο υλικό στο Internet. Η πρώτη άποψη είναι ότι καμία πληροφορία δεν πρέπει να παρακρατείται και ότι οι γονείς πρέπει να είναι υπεύθυνοι για την παρακολούθηση των παιδιών τους .Η δεύτερη είναι ότι μόνο η κυβέρνηση μπορεί να προστατεύει πραγματικά τους ανήλικους από αυτό το υλικό, και η τελευταία προσέγγιση είναι να θεωρούνται υπεύθυνοι οι πάροχοι του Internet για όλο το υλικό και τις πληροφορίες που παρέχουν. Αυτές οι προσεγγίσεις μπορούν να υλοποιηθούν για όλους τους περιηγητές και όχι μόνο για παιδιά.

Οι Γονείς προστατεύουν τα παιδιά

Υπάρχουν κάποιοι που ισχυρίζονται ότι η αποτελεσματικότερη προστασία για τα παιδιά από διαδικτυακούς κινδύνους σαν τους προηγούμενους είναι η απαγόρευση του Internet από τους γονείς. Ωστόσο η εφαρμογή μιας απαγορευτικής απόφασης δεν είναι τόσο εύκολη υπόθεση, όσο αρχικά φαίνεται. Ακόμα και αν εμποδιστεί ένα παιδί να χρησιμοποιήσει το Internet από τον υπολογιστή στο σπίτι, κανείς δεν μπορεί να διασφαλίσει ότι δεν θα το κάνει, π.χ., από το σπίτι ενός φίλου: η ίδια η απαγόρευση συνήθως εξάπτει την φαντασία και εγείρει αντιδράσεις, φέρνοντας τα αντίθετα πολλές φορές αποτελέσματα.

Κάπου μεταξύ της απόλυτης απαγόρευσης και της απόλυτης ελευθερίας βρίσκεται η ελεγχόμενη πρόσβαση στο Διαδίκτυο. Εδώ γίνεται αναφορά στο φιλτράρισμα, με χρήση κατάλληλου λογισμικού του περιεχομένου του Internet στο οποίο είναι δυνατόν να εκτεθεί ένα παιδί. Αναλυτικότερα πρόκειται για προγράμματα που, όταν εγκατασταθούν σε έναν υπολογιστή, φιλτράρουν τις διευθύνσεις των διαδικτυακών τόπων που επισκέπτεται ο χρήστης, απαγορεύοντας την πρόσβαση σε τόπους με βλαπτικό περιεχόμενο (π.χ. Chi Bbrowser, Net Nanny). Αναμφισβήτητα όμως η αποτελεσματικότερη προστασία έρχεται μέσω της ενημέρωσης και της επικοινωνίας μεταξύ γονέων και παιδιών.

Η κυβέρνηση προστατεύει τα παιδιά

Αυτοί που θέλουν η κυβέρνηση να ελέγχει το υλικό που βλέπουν τα παιδιά, πιστεύουν ότι η δουλειά μπορεί να γίνει μέσω νομοθεσίας. Θέλουν να δουν νόμους που θα υποχρεώνουν βιβλιοθήκες και σχολεία που θα χρησιμοποιούν φίλτρα μπλοκαρίσματος.

Ευθύνη για τους Παρόχους Internet

Το America Online, στην προσπάθεια του να πάρει την ευθύνη, προσπαθεί να δημιουργήσει ένα μέσο που είναι φιλικό προς τους καταναλωτές, ασφαλές για οικογένειες και οικονομικά ανεκτό από όλους. Βασίζεται στα μέλη του για να αυτοαστυνομεύουν το σύστημα και να αναφέρουν πράγματα που παραβιάζουν τους όρους λειτουργίας. Μερικά από τα πράγματα που απαγορεύει το AOL είναι η υβριστικές κουβέντες ή η πραγματική προσβλητική ομιλία. Έχει εφαρμόσει την πολιτική του σε καταστάσεις όπως ένα δικτυακό τόπο ΚΚΚ ή σε ένα δικτυακό τόπο για κατ' εξακολούθηση δολοφόνους. Ορισμένοι πιστεύουν ότι οι πάροχοι internet πρέπει να είναι νομικά υπεύθυνοι για όλο το υλικό που επιτρέπουν να προσπελαύνεται.

ΠΡΟΣΤΑΣΙΑ ΚΑΤΑΝΑΛΩΤΗ ΚΑΙ ΠΩΛΗΤΗ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Όταν οι αγοραστές και οι πωλητές δεν μπορούν να δουν ο ένας τον άλλο, και μπορεί να βρίσκονται σε διαφορετικές χώρες, υπάρχει μία πιθανότητα μη έντιμοι άνθρωποι να κάμουν όλων των ειδών τις απάτες και άλλα κακουργήματα μέσω του Internet.Κατά τα πρώτα χρόνια του ηλεκτρονικού εμπορίου έγιναν γνωστές πολλές τέτοιες απάτες, από την δημιουργία μιας εικονικής τράπεζας που εξαφανιζόταν μαζί με τις καταθέσεις των επενδυτών, μέχρι την διαχείριση μετοχών στο Internet.

Η απάτη στον παγκόσμιο ιστό έχει εξελιχθεί πάρα πολύ όπως φαίνεται στα παρακάτω παραδείγματα.

Απάτη on-line Δημοπρασίας:Η πλειοψηφία (68%) των παραπόνων που έχουν καταγραφεί στην Επιτροπή Προστασίας Καταναλωτή (στην Ουάσιγκτον D.C) αφορά δημοπρασίες. Συλλέγονται χρήματα αλλά τα προϊόντα δεν είναι ικανοποιητικά, η δεν διανέμονται και καθόλου

Απάτη Μετοχών στο Internet:Χαρακτηριστικό είναι το παρακάτω παράδειγμα που δημοσιεύθηκε στον **Τύπο της Κυριακής 8.11.1998-ένθετο New Millennium**:

Πανεθνική «επιχείρηση σκούπα» στο Internet ξεκίνησε η επιτροπή Χρηματιστηρίου των ΗΠΑ για να αποκαλύψει πιθανούς απατεώνες που βρήκαν ένα λαμπρό πεδίο δράσης (με πολλά οφέλη) στον κυβερνοχώρο. Μέχρι στιγμής 44 εταιρείες έχουν πέσει στα δίχτυα της. «Αυτό είναι κήρυξη πολέμου στην δικτυακή απάτη» δήλωσε ο Harold F. Degenhardt, δικηγόρος της επιτροπής που ασχολείται με το θέμα. «Αυτή είναι μια πρώτη ομοβροντία, αλλά δεν θα είναι η τελευταία. Οι δυνατότητες να βρεθούν θύματα είναι τεράστιες. Πατώντας ένα κουμπί μπορεί κάποιος να προσεγγίσει δεκάδες εκατομμύρια ανθρώπους. Το Internet δεν έχει όρια».

Οι περισσότερες από τις απάτες που αποκαλύφθηκαν είχαν να κάνουν με ένα παλιό κόλπο που χρησιμοποιούσαν οι επονομαζόμενοι «διαλαλητές μετοχών» στις ΗΠΑ. «Σφύριζαν» ένα δήθεν καυτό μυστικό για κάποια μετοχή στους επενδυτές, αποκρύπτοντας όμως ότι είχαν πληρωθεί για να προωθήσουν την συγκεκριμένη μετοχή. Γι' αυτό τον λόγο παλιά χρησιμοποιούσαν το τηλέφωνο. Σήμερα χρησιμοποιούν το Δίκτυο και ειδικευμένα ηλεκτρονικά newsletters.

Μία από αυτές τις ηλεκτρονικές εκδόσεις ήταν το StocksToWatch.com το οποίο στις 23 Μαΐου 1998 είχε μια καυτή πληροφορία για τους 200.000 συνδρομητές του. Η Midland Inc., μια μικρή εταιρεία, έλεγε, είχε πατεντάρει ένα μηχανισμό ενίσχυσης καυσίμων που θα έφερνε τα πάνω κάτω στην βιομηχανία πετρελαίου. Προέβλεπε μάλιστα πως η μετοχή που είχε τότε 1 περίπου δολάριο θα έφτανε τα 75$, σε σύντομο χρονικό διάστημα.

Ο συντάκτης του newsletter, όμως, Steven A. King είχε παραλείψει μια ουσιαστική λεπτομέρεια. Ήταν ο πρόεδρος της εταιρείας, η οποία είχε την πατέντα. Όταν μετά την δημοσίευση η μετοχή έφτασε τα 2,62 $, άρχισε να πουλά τις δικές του κερδίζοντας σε λίγε μέρες 51 εκατ. δραχμές. Αργότερα βέβαια η μετοχή έπεσε...

Σε μια άλλη περίπτωση το ίδιο newsletter πρότεινε την αγορά μετοχών της εταιρείας Surgical Safety Products. Η μετοχή είχε 96 σεντς και το δημοσίευμα προέβλεπε πως σε 18 μήνες θα έφτανε τα 20 δολάρια. Δύο μέρες μετά η τιμή της τριπλασιάστηκε. Ο King πούλησε τις μετοχές του που του είχε δώσει η εταιρεία σε αντάλλαγμα για την δημοσίευση, κερδίζοντας περί τα 180 εκατ. δραχμές. Βέβαια η μετοχή αργότερα πάλι έπεσε και κάποιοι ανύποπτοι επενδυτές έχασαν τα λεφτά τους.

Στην ίδια πρακτική επιδόθηκε και ένα άλλο newsletter, το Future Superstock, το οποίο πρότεινε στους 100.000 και πλέον συνδρομητές του 25 μετοχές τον τελευταίο χρόνο. Σύμφωνα με το κατηγορητήριο της Επιτροπής Χρηματιστηρίου, για κάθε δημοσίευση η εν λόγω έκδοση έπαιρνε 200 - 300.000 δολάρια (60 - 90 εκατ. δραχμές). Το γεγονός όμως ότι δεν ενημέρωνε τους συνδρομητές του ότι οι «συμβουλές» του ήταν στην ουσία διαφημιστική προώθηση των μετοχών αποτελεί αδίκημα για την αμερικανική νομοθεσία. Γι' αυτό τον λόγο έπεσε στα δίχτυα της επιτροπής και η εταιρεία Δημοσίων σχέσεων Sloane Fitzgerald Inc. Η εν λόγω εταιρεία έστειλε 6 εκατομμύρια διαφημιστικά μηνύματα με ηλεκτρονικό ταχυδρομείο προτείνοντας την αγορά δύο μετοχών. Εμφανιζόταν όμως ως ανεξάρτητη χρηματιστηριακή εταιρεία και δεν αποκάλυπτε τις πελατειακές σχέσεις της με τις εταιρείες που προωθούσε.

Όπως και να έχει το ζήτημα οι χρηματιστηριακές απάτες μέσω Δικτύου που αποκαλύφτηκαν είναι προφανώς η κορυφή του παγόβουνου. Το καινούργιο Μέσο προσφέρει νέες ευκαιρίες για νέου είδους απάτες. Για τον λόγο αυτό η επιτροπή χρηματιστηρίου των ΗΠΑ αποφάσισε να αντεπιτεθεί: Δημιούργησε μια ειδική ομάδα, την «Cyberforce», που αλωνίζει όλη μέρα το Διαδίκτυο ψάχνοντας για πιθανές απάτες, ενώ έχει και ειδική ηλεκτρονική διεύθυνση στην οποία τα θύματα ή τα δυνάμει θύματα αυτών των επιτήδειων μπορούν να καταγγέλλουν ή να ζητούν πληροφορίες για την χρηματιστηριακή νομοθεσία.

Άλλες Οικονομικές Απάτες :Οι μετοχές είναι μόνο μία από τις πολλές περιοχές όπου ενεργοποιούνται οι απατεώνες. Άλλες περιοχές περιλαμβάνουν ψεύτικες επενδύσεις, φανταστικές επιχειρηματικές ευκαιρίες και άλλα σχήματα. Οι οικονομικοί εγκληματίες έχουν πρόσβαση σε πολύ περισσότερους ανθρώπους, κυρίως λόγω της διαθεσιμότητας του E-Mail.

Άλλες Απάτες στο Η.Ε: Υπάρχουν και πολλοί τύποι μη οικονομικής απάτης στο διαδίκτυο. Για παράδειγμα, οι πελάτες μπορούν να πάρουν προϊόντα και υπηρεσίες χαμηλής ποιότητας, να μην παίρνουν τα προϊόντα τους έγκαιρα μπορεί να τους ζητηθεί να πληρώσουν για πράγματα που θα έπρεπε να πληρώνουν οι πωλητές. Ένα πολύ γνωστό παράδειγμα είναι εξής απάτη:Οι χρήστες που επισκέπτονται τόπους πορνογραφικού υλικού, κυρίως, περιεχομένου, παροτρύνονται και πείθονται να κατεβάσουν στον υπολογιστή τους προγράμματα τα οποία υπόσχονται «δωρεάν»παρακολούθηση εικόνων και βίντεο τέτοιου είδους. Εάν κάποιος κατεβάσει και εκτελέσει ένα τέτοιο πρόγραμμα, τότε η σύνδεση που έχει με τον ιντερνετικό φορέα διακόπτεται αυτομάτως και αμέσως μετά το πρόγραμμα πραγματοποιεί υπεραστική κλήση στη βάση με το πορνογραφικό υλικό. Η χρόνο χρέωση που ακολουθεί είναι εξαντλητική(**E-Commerce Security, Anup K. Ghosh,Wiley computer publishing 1998)**

Προειδοποιήσεις για Καταναλωτές από την FTC

Η **FTC** παρέχει μία λίστα κακόβουλων ενεργειών, που ονομάζονται
Ενδεικτικά μερικές από αυτές είναι:

1. **Επιχειρηματικές ευκαιρίες**-εύκολο να εκκινηθεί μια επιχείρηση που θα φέρει μία περιουσία. Επίσης προσφέρονται παράνομα σχήματα πυραμίδας.
2. **Σύμβουλοι μαζικής αλληλογραφίας**- πωλούν λίστες διευθύνσεων email.Αν χρησιμοποιηθούν συνήθως παραβιάζονται οι όροι υπηρεσιών του ISP.

3. **Αλυσίδες επιστολών**-ζητείται να σταλούν χρήματα σε ορισμένους ανθρώπους και το όνομα του αποστολέα μπαίνει σε μία λίστα. Αυτό είναι παράνομο.
4. **Σχήματα εργασίας στο σπίτι**-συνήθως δεν αξίζουν και κοστίζουν πολλά
5. **Σχήματα υγείας και δίαιτας**-συνήθως προσφέρονται άχρηστα προϊόντα που δεν λειτουργούν.
6. **Άκοπο εισόδημα**-οι ευκαιρίες για πολλά λεφτά έχουν ως σκοπό να χαθούν λεφτά παρά να κερδισθούν.

Υπάρχουν αρκετοί τρόποι με τους οποίους οι αγοραστές μπορούν να προστατευθούν από απάτη στο Η.Ε.

Προστασία Αγοραστή

Η προστασία του αγοραστή είναι κρίσιμη για την επιτυχία κάθε εμπορίου, ειδικά του ηλεκτρονικού όπου οι αγοραστές δεν βλέπουν τους πωλητές. Συμβουλές για ασφαλείς ηλεκτρονικές αγορές περιλαμβάνουν τις παρακάτω:

1. Ψάξτε για αξιόπιστα ονόματα σε δικτυακούς τόπους σαν :Wal-Mart online,Disney online και Amazon.com και βεβαιωθείτε ότι εισέρχεστε σε ένα πραγματικό δικτυακό τόπο αυτών των εταιρειών.
2. Σε κάθε άγνωστο δικτυακό τόπο ψάξτε για διεύθυνση, τηλέφωνο και φαξ. Καλέστε και κάντε ερωτήσεις στο άτομο που θα απαντήσει για τους πωλητές
3. Ψάξτε για τον πωλητή στο τοπικό εμπορικό επιμελητήριο, ή σε κάποιον ειδικό οργανισμό, όπως περιγράφουμε στην συνέχεια.
4. Ερευνήστε πόσο ασφαλής είναι ο δικτυακό τόπος του πωλητή και πόσο καλά είναι οργανωμένος.
5. Εξετάστε τις εγγυήσεις επιστροφής χρημάτων ,τις εγγυήσεις χρήσης και τις συμφωνίες εξυπηρέτησης.
6. Συγκρίνετε τις τιμές με αυτές των κανονικών καταστημάτων. Πολύ χαμηλές τιμές ίσως να είναι ψεύτικες.
7. Ρωτήστε φίλους για το τι ξέρουν. Βρείτε μαρτυρίες και προστατευτικό υλικό.
8. Βρείτε τι θα μπορείτε να κάνετε σε περίπτωση διένεξης.
9. Συμβουλευτείτε το Εθνικό Κέντρο Πληροφοριών για Απάτες.
10. Μην Ξεχνάτε ότι έχετε τα δικαιώματα του καταναλωτή.

Αρκετοί δημόσιοι οργανισμοί όπως και ιδιωτικές εταιρείες προσπαθούν να προστατεύσουν τους καταναλωτές. Μερικοί από αυτούς είναι: **TRUSTe's ''Trustmark'',Better Business Bureau(BBB),Online Privacy Alliance.**

Πιστοποίηση και βιομετρικοί έλεγχοι

Στον κυβερνοχώρο ,οι αγοραστές και οι πωλητές δεν βλέπουν οι μεν τους δε. Ακόμη και όταν χρησιμοποιείται βιντεοδιάσκεψη, η αυθεντικότητα του ατόμου με το οποίο γίνονται συναλλαγές πρέπει να επαληθευτεί, εκτός και αν έχουν προηγηθεί και άλλες συναλλαγές. Αν υπάρχει απόλυτη σιγουριά για το για την ταυτότητα του ατόμου στην άλλη άκρη της γραμμής τότε θα μπορούσαν να υπάρξουν βελτιωμένες και νέες εφαρμογές ηλεκτρονικού εμπορίου:

- Οι απατηλοί παραλήπτες κυβερνητικών χορηγιών και άλλων πληρωμών θα μειωθούν στο ελάχιστο.
- Οι αγοραστές θα είναι σίγουροι ποιοι θα είναι οι πωλητές και οι πωλητές θα ξέρουν ποιοι είναι οι αγοραστές με μεγάλο βαθμό εμπιστοσύνης.
- Μπορούν να γίνουν διευθετήσεις έτσι ώστε μόνο εξουσιοδοτημένα άτομα σε εταιρείες να μπορούν να δώσουν ή να παραλάβουν είδη που έχουν παραγγελθεί.
- Η εμπιστοσύνη στους εταίρους κάποιας εταιρείας και στο Η.Ε θα αυξηθεί σημαντικά. κ.α.

Η λύση για μια τέτοια πιστοποίηση παρέχεται από τεχνολογίες της πληροφορίας που είναι γνωστές σαν βιομετρικοί έλεγχοι για πρόσβαση σε δίκτυα Η.Ε.

Οι **βιομετρικοί έλεγχοι** παρέχουν διαδικασίες πρόσβασης που ταιριάζουν κάθε έγκυρο χρήστη με μία μοναδική ταυτότητα χρήστη(UID, unique user identifier). Επίσης παρέχουν μία μέθοδο πιστοποίησης για επαλήθευση ότι οι χρήστες που ζητούν πρόσβαση στο σύστημα υπολογιστή είναι πράγματι αυτοί που ισχυρίζονται ότι είναι. Μια UID μπορεί να επιτευχθεί με ένα ή περισσότερους από τους παρακάτω τρόπους:

- Παρέχει κάτι που μόνο ο χρήστης ξέρει, π.χ., ένα κωδικό πρόσβασης.
- Παρουσιάζει κάτι που μόνο ο χρήστης έχει, π.χ. ,έξυπνη κάρτα ή ένα διακριτικό
- Δηλώνει κάτι που μόνο ο χρήστης είναι , όπως μία υπογραφή, μία φωνή ένα αποτύπωμα ή μία σάρωση αμφιβληστροειδούς του ματιού. Αυτό υλοποιείται με βιομετρικούς ελέγχους.

*Ένας βιομετρικός έλεγχος είναι μία αυτοματοποιημένη μέθοδος επαλήθευσης της ταυτότητας ενός ατόμου , με βάση φυσιολογικά χαρακτηριστικά ή χαρακτηριστικά συμπεριφοράς.(***Forte 1998**).Οι συνηθέστεροι βιομετρικοί έλεγχοι είναι οι παρακάτω.

- **Γεωμετρία Προσώπου**(φωτογραφία).Ο υπολογιστής παίρνει μία εικόνα ενός προσώπου και την ταιριάζει με μια εκ των προτέρων αποθηκευμένη εικόνα. Το 1998, αυτή η μέθοδος ήταν επιτυχημένη για την σωστή αναγνώριση χρηστών, εκτός από τις περιπτώσεις διδύμων (www.mrpayroll.com).
- **Δακτυλικό Αποτύπωμα**(σάρωση δακτύλου). Κάθε φορά πού ένας χρήστης θέλει πρόσβαση, γίνεται ταίριασμα ενός δακτυλικού αποτυπώματος με ένα πρότυπο, που περιέχει το δακτυλικό αποτύπωμα του εξουσιοδοτημένου προσώπου, οπότε αναγνωρίζεται αν είναι ο σωστός χρήστης.
- **Γεωμετρία Χεριού.** Παρόμοιο με το δακτυλικό αποτύπωμα εκτός του ότι ο επαληθευτής μία κάμερα για να πάρει φωτογραφία του χεριού του χρήστη. Ορισμένα χαρακτηριστικά του χεριού(όπως το μήκος και το πάχος του χεριού)συγκρίνονται ηλεκτρονικά με πληροφορίες που είναι αποθηκευμένες στον υπολογιστή.
- **Μοτίβο αγγείου αίματος μέσα στον αμφιβληστροειδή του ματιού ενός ατόμου**. Γίνεται προσπάθεια να γίνει ταίριασμα ανάμεσα στο μοτίβο των αγγείων αίματος στον αμφιβληστροειδή που σαρώνεται και σε μία εκ των προτέρων αποθηκευμένη εικόνα του αμφιβληστροειδούς**.**

- **Φωνή**(αποτύπωμα φωνής)Γίνεται προσπάθεια να γίνει ταίριασμα ανάμεσα στην φωνή του χρήστη και στο μοτίβο φωνής που είναι αποθηκευμένο σε πρότυπα.
- **Υπογραφή**. Ταιριάζονται υπογραφές ως προς εκ των προτέρων αποθηκευμένες αυθεντικές υπογραφές. Αυτή η μέθοδος συμπληρώνει ένα σύστημα ταυτότητας με φωτογραφία.
- **Δυναμική Πληκτρολόγησης**. Γίνεται ταίριασμα της πίεσης του πληκτρολογίου και της ταχύτητας πληκτρολόγησης ως προς εκ των προτέρων αποθηκευμένες πληροφορίες.
- **Άλλες. π.χ.** Pin,σάρωση ίριδας

Προστασία Πωλητών

Το internet κάνει την απάτη από τους πελάτες ευκολότερη,λόγω της ευκολίας της ανωνυμίας. Οι πωλητές πρέπει να προστατεύονται από:

- Χειρισμό πελατών που αρνούνται ότι έδωσαν μία παραγγελία.
- Πελάτες που φορτώνουν προστατευμένο λογισμικό και/ή στοιχεία της γνώσης και το πωλούν σε άλλους
- Σωστή πληρωμή για προϊόντα και υπηρεσίες που παρέχονται.
- Χρήση των ονομάτων τους από άλλους.

(**ΗλεκτρονικόΕμπόριο, Turban, Lee, King, Chung. Εκδόσεις Μ.Γκιούρδας, Αθήνα 2002**)

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ:

1. Αρσένης Πασχόπουλος, Παναγιώτης Σκαλτσας.(2000)Ηλεκτρονικό Εμπόριο. Αθήνα. Εκδόσεις Κλειδάριθμος
2. Efraim Turban, Jae Lee,David King, Michael Chung.(2002).Ηλεκτρονικό Εμπόριο. Αθήνα.Εκδόσεις Μ.Γκιούρδας.

ΞΕΝΗ:

1. Craig Fellenstein, Ron Wood.(2000)Exploring e-commerce .London. Prentice Hall PTR
2. Anup Ghosh (1998)E-Commerce Security. New York.Wiley computer publishing
3. Camp l.Jean.(2000)Trust and risk. Cambridge. Mass MIT Press

ΠΕΡΙΟΔΙΚΑ / ΕΦΗΜΕΡΙΔΕΣ

1. Χρήστος Βαρελάς (2000) Ευαίσθητη προστασία. Ram 1/6/2000
2. Πάσχος Μανδραβέλης(1996) Μια αφελής απόπειρα λογοκρισίας «Έθνος» , 21-1-1996)
3. Γιώργος Πολύζος (2002) File sharing στην πράξη Chip 28/11/2002
4. Γιώργος Ψαρουλάκης, Νάσια Χρυσουλά, Γιώργος Πολύζος(2002).Το hacking και πως να το αποφύγετε.Chip 28/11/2002
5. Χρίστος Τόμπρας(1998)Δικτυακή ασφάλεια και διασφάλιση.Ram Ιούνιος 1998
6. "Ημερησία"(2002)Ηλεκτρονικό Εμπόριο .Σαββατοκύριακο 23-24 Νοεμβρίου
7. Thorsten Eggeling (2002) Geheim, gratis, illegal. PCWelt 12/02
8. Andreas Perband(2002)Auf ihrer Fährte. PC Welt 12/02

ΠΑΡΑΠΟΜΠΕΣ ΑΠΟ ΠΑΓΚΟΣΜΙΟ ΙΣΤΟ

1. kookaburaSoftware(2000)All about cookies [online].Available:http://www.kburra.com/support.html
2. Newsfactor network.(2000)The Boss is Watching[online].Available:http://www.newsfactor.com/perl/story/11634.html)
3. Pulex.(2000)Internet ohne kriminalitaet [online].Available:http://www.publex.de
4. Aclu(2002)Monitoring on the rise[online].Available:http://forms.aclu.org
5. A.E.P.I(1999) Νόμος περι πνευματικης ιδιοκτησιας[online].Available:http://aepi.gr/first.htm
6. Πάσχος Μανδραβέλης(1999)Μια αφελής προσπάθεια λογοκρισίας [online].Available:http://www.medium.gr
7. Juristen Rostocks. InternetRecht[online].Available:http://www.internetrecht-rostock.de