Δίκαιο και Internet – Μέρος 1

Κων/νου Στυλιάδη,

Υπεύθυνου Κέντρου ΠΛΗ.ΝΕ.Τ. (Πληροφορικής και Νέων Τεχνολογιών)

Ν. Φλώρινας

http://dide.flo.sch.gr/Plinet/plinet.html

e-mail : plinet at dide.flo.sch.gr

Η Υπάρχουσα Νομοθεσία για Θέματα Τηλεπικοινωνιών, Πληροφορικής και Internet

Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.)

- Ιδρύθηκε με τους **Ν.2246/1994** και **Ν.2867/2000**, *«Οργάνωση και Λειτουργία του Τομέα των Τηλεπικοινωνιών»*, ως αρμόδια για την εποπτεία της τηλεπικοινωνιακής αγοράς.
- Η Ε.Ε.Τ.Τ. http://www.eett.gr χορηγεί άδειες λειτουργίας σε Πάροχους Τηλεπικοινωνιακών Υπηρεσιών, στους οποίους ανήκουν και οι Πάροχοι Υπηρεσιών Διαδικτύου, οι γνωστοί και ως Παροχείς Υπηρεσιών Internet ή ISP's (Internet Service Providers).

Εθνική Επιτροπή Προστασίας του Απορρήτου των Επικοινωνιών

- Ο **Ν.2225/1994** αναφέρεται στην *«Ίδρυση Εθνικής Επιτροπής Προστασίας του Απορρήτου των Επικοινωνιών»*, με αποστολή την προστασία του απορρήτου των επιστολών και της τηλεφωνικής και κάθε άλλης μορφής τηλεπικοινωνιακής ανταπόκρισης ή επικοινωνίας κατά το άρθρο 19 του Συντάγματος καθώς και τον έλεγχο της τήρησης των όρων άρσης του απορρήτου που έθεσε η δικαστική αρχή.
- Στο άρθρο 3 ορίζονται οι προϋποθέσεις για την άρση του απορρήτου για λόγους εθνικής ασφάλειας και στο άρθρο 4 ορίζονται οι προϋποθέσεις για την άρση του απορρήτου για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Υπουργικές Αποφάσεις

- Η Υπουργική Απόφαση με αριθ. *88141/1995* αποτελεί τον *«Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων»*.
- Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. *268/73/2002* αποτελεί τον *«Κανονισμό Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr»*.

Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

- Με τον **Ν.2472/1997** *«Προστασία του Ατόμου από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα»* ορίζονται οι προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής.
- Με τα άρθρα 15–20 του νόμου αυτού ορίζεται η σύσταση, η συγκρότηση και ο τρόπος λειτουργίας της *Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*.
- Ο **Ν.2774/1999** αναφέρεται στην *«Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Τηλεπικοινωνιακό Τομέα»*.

Οδηγία για το Ηλεκτρονικό Εμπόριο

- Το **ΠΔ.131/2003** αποτελεί την «Ο*δηγία για το Ηλεκτρονικό Εμπόριο*».
- Το άρθρο 6 αναφέρεται στη μη ζητηθείσα εμπορική επικοινωνία (spam e-mail) και τα άρθρα 8 – 10 αναφέρονται στις ηλεκτρονικές συμβάσεις και στους τρόπους ηλεκτρονικής παραγγελίας.
- Τα άρθρα 11 – 14 αναφέρονται στην ευθύνη των μεσαζόντων παροχής υπηρεσιών (ISP's) όταν διαπιστωθούν παράνομες ενέργειες των χρηστών (συνδρομητών) τους.

Ηλεκτρονικές Υπογραφές

- Το **ΠΔ.150/2001** αναφέρεται στο κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές.
- Η ψηφιακή υπογραφή χαρακτηρίζεται ως *«προηγμένη ηλεκτρονική υπογραφή»* και επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.
- Ο Πάροχος Υπηρεσιών Πιστοποίησης ορίζεται ως φυσικό ή νομικό πρόσωπο ή άλλος φορέας, που εκδίδει πιστοποιητικά (ηλεκτρονικές βεβαιώσεις της ταυτότητας ενός ατόμου) ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές.

Πάροχοι Υπηρεσιών Πιστοποίησης

- Η απόφαση της Ε.Ε.Τ.Τ. με αριθ. *248/71/2002* αποτελεί τον *«Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής»*.
- Στο άρθρο 3 αναφέρεται ότι η παροχή υπηρεσιών πιστοποίησης οποιασδήποτε μορφής είναι ελεύθερη και δεν υπόκειται σε προηγούμενη άδεια ή έγκριση.
- Στο άρθρο 9 αναφέρεται ότι η Ε.Ε.Τ.Τ. ασκεί την εποπτεία και τον έλεγχο όλων των εγκατεστημένων στην Ελλάδα Πάροχων Υπηρεσιών Πιστοποίησης.

Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

- Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) http://www.adae.gr λειτουργεί από το 2003 ως ανεξάρτητη αρχή σύμφωνα με τις διατάξεις του **Ν.3115/2003**.
- Σκοπός της ΑΔΑΕ είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο.
- Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

- Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα http://www.dpa.gr (Data Protection Authority) λειτουργεί σύμφωνα με τις διατάξεις του **Ν.2472/1997** (άρθρα 15–20) με αποστολή την εποπτεία της τήρησης του προσωπικού απορρήτου και στο Διαδίκτυο, όπως ορίζεται και από τον μεταγενέστερο **Ν.2774/1999** για την *«Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»*.
- Σύμφωνα με τους παραπάνω νόμους, οι ιστοσελίδες που συγκεντρώνουν προσωπικά στοιχεία των επισκεπτών τους, όπως ονόματα, τηλέφωνα, διευθύνσεις e-mail, έχουν νομική υποχρέωση να τους ενημερώνουν για τον σκοπό που συλλέγονται αυτά τα στοιχεία καθώς και για το αν διατίθενται σε τρίτους.

Ελληνικός Φορέας Πρόληψης Τηλεπικοινωνιακής Απάτης (ΕΦΤΑ)

- Ο ΕΦΤΑ δημιουργήθηκε στις αρχές του 2000 από στελέχη των εταιρειών σταθερών και κινητών επικοινωνιών στην Ελλάδα (OTE, Vodafone, Cosmote, STETHELLAS), τα οποία δραστηριοποιούνται στον εντοπισμό και την πρόληψη της Τηλεπικοινωνιακής Απάτης και του Ηλεκτρονικού Εγκλήματος γενικότερα.
- Ως Τηλεπικοινωνιακή Απάτη θεωρείται :
- Η πρόσβαση σε τηλεπικοινωνιακά δίκτυα για χρήση τηλεπικοινωνιακών υπηρεσιών, χωρίς να πληρώνεται το αντίστοιχο τέλος.
- Η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα με σκοπό την αποκόμιση οικονομικού οφέλους, ή για άλλους αθέμιτους σκοπούς, όπως βιομηχανική κατασκοπεία.
- Η απάτη στις ηλεκτρονικές συναλλαγές και το ηλεκτρονικό εμπόριο.

Άρθρα Ποινικού Κώδικα

- **370Α** (Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας).
- **370Β** (Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα).
- **370Γ** (Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών).
- **386Α** (Απάτη με υπολογιστή).

Εντοπισμός των Χρηστών στο Internet με Χρήση της IP Διεύθυνσης

Internet – Ανωνυμία και Απόλυτη Ελευθερία Κίνησης – Δύο Μύθοι

- Δύο από τις πιο διαδεδομένες ανακρίβειες για το Internet, στις οποίες και οφείλεται σε πολύ μεγάλο ποσοστό η αλματώδης αύξηση των παράνομων δραστηριοτήτων σ' αυτό, είναι ότι είναι ανώνυμο και ότι παρέχει απόλυτη ελευθερία έκφρασης στους χρήστες του.
- Το σίγουρο είναι ότι το Internet ούτε ανώνυμο είναι ούτε παρέχει απόλυτη ελευθερία κινήσεων, εκφράσεων και διατύπωσης απόψεων στους χρήστες του.

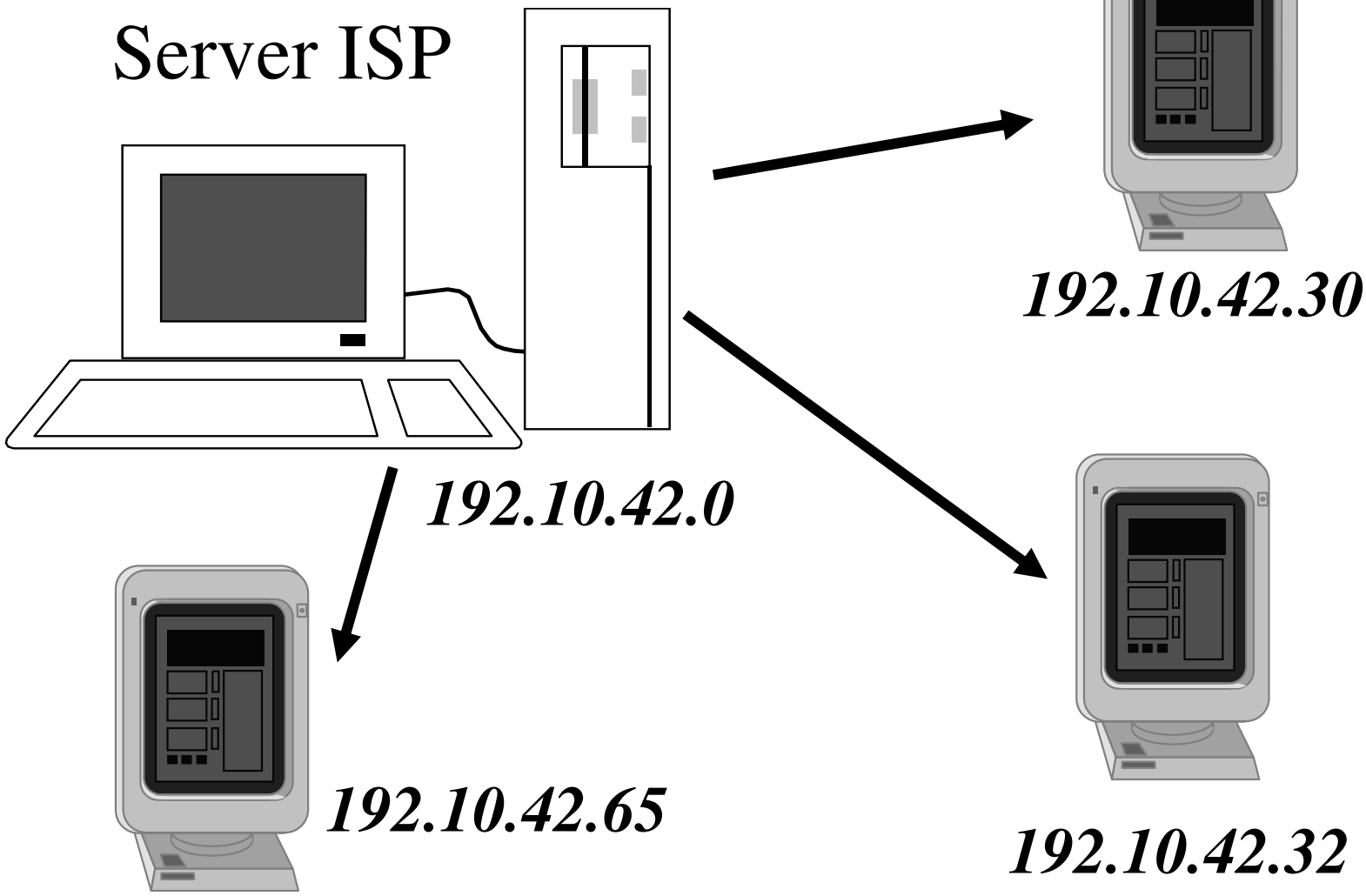
Η IP Διεύθυνση

- Κάθε υπολογιστής που συνδέεται στο Internet, αποκτά μια διεύθυνση που είναι γνωστή με τον όρο IP διεύθυνση (Internet Protocol address) και η οποία είναι μοναδική στον κόσμο.
- Η διεύθυνση αυτή αποτελείται από 4 ακεραίους αριθμούς, όπου ο καθένας μπορεί να πάρει μια τιμή από 0 έως και 255, και ένα χαρακτηριστικό παράδειγμα IP διεύθυνσης είναι το εξής : ***192.10.42.30***.
- Αυτός ο συνδυασμός των τεσσάρων ακεραίων αριθμών της IP διεύθυνσης προσδιορίζει μοναδικά έναν υπολογιστή παγκοσμίως και αποτελεί το κλειδί για τον εντοπισμό των χρηστών που παρανομούν στο Διαδίκτυο.

Σύνδεση στο Internet από το Σπίτι

- Στην περίπτωση που ο χρήστης συνδέεται στο Internet από το σπίτι του μέσω ενός ISP, τότε κάθε φορά που συνδέεται αποκτά και μια διαφορετική IP διεύθυνση, όπως ***192.10.42.30*** ή ***192.10.42.32*** ή ***192.10.42.65*** κοκ.
- Βλέπουμε ότι στην περίπτωση αυτή αλλάζει μόνο ο τελευταίος από τους τέσσερις αριθμούς, ενώ οι τρεις πρώτοι αριθμοί παραμένουν ίδιοι για όλους τους χρήστες που συνδέονται στον συγκεκριμένο ISP.

Απόδοση IP Διεύθυνσης



Καταγραφή των Στοιχείων του Χρήστη

- Ο ISP καταγράφει τα στοιχεία των χρηστών (συνδρομητών) του που συνδέονται στο Internet μέσω των servers που αυτός διαθέτει.
- Τα στοιχεία αυτά είναι τα εξής : όνομα χρήστη (user name), αριθμός τηλεφώνου, ώρα σύνδεσης, IP διεύθυνση, ιστοσελίδες που επισκέφθηκε ο χρήστης κ.ά., σε ειδικά αρχεία που αποκαλούνται *log files (αρχεία καταγραφής)*.

Εντοπισμός του Χρήστη

- Στην περίπτωση λοιπόν που εντοπισθεί κάποια παράνομη ή ύποπτη ενέργεια στο Διαδίκτυο, το πρώτο πράγμα που εντοπίζουν οι Αρχές είναι η IP διεύθυνση του δράστη, κάτι που είναι πολύ εύκολο να επιτευχθεί με απλά προγράμματα, ενσωματωμένα στον κωδικό των ιστοσελίδων.
- Από την IP διεύθυνση εντοπίζουν τον ISP που εξυπηρέτησε τον δράστη και μετά θα πρέπει να εκδοθεί εισαγγελική εντολή ώστε να υποχρεωθεί ο ISP να δώσει τα στοιχεία του συνδρομητή του που κάποια συγκεκριμένη ημέρα και ώρα είχε αποκτήσει την συγκεκριμένη IP διεύθυνση.

Αποκάλυψη των Στοιχείων του Χρήστη

- Τα στοιχεία του συνδρομητή του που μπορεί να αποκαλύψει ο ISP είναι μόνο το τηλέφωνο από το οποίο κάλεσε ο δράστης και το όνομα χρήστη (user name) που χρησιμοποίησε.
- Μετά είναι δουλειά της Αστυνομίας να εντοπίσει ποιος χρησιμοποίησε τα στοιχεία αυτά για να κάνει την όποια παράνομη ενέργεια.
- Δεν είναι σε θέση δηλαδή ο ISP να εντοπίσει συγκεκριμένο πρόσωπο.

Σύνδεση στο Internet από Τοπικό Δίκτυο Υπολογιστών

- Στην περίπτωση που ο χρήστης συνδέεται στο Internet μέσω ενός τοπικού δικτύου υπολογιστών, όπως για παράδειγμα από ένα Internet Cafe ή από ένα πανεπιστημιακό ή σχολικό εργαστήριο, τότε όλοι οι χρήστες του ίδιου δικτύου θα φαίνονται έξω από το δίκτυο και προς το Internet με την ίδια IP διεύθυνση, ενώ μέσα στο τοπικό δίκτυο θα έχει ο καθένας διαφορετική IP διεύθυνση.
- Μάλιστα, στην περίπτωση αυτή η IP διεύθυνση που φαίνεται προς τα έξω είναι συνήθως στατική (μόνιμη) και όχι δυναμική.

Υπεκφυγή των Δραστών

- Αν κάποιος δράστης αποφασίσει να κάνει παράνομες ενέργειες στο Internet και χρησιμοποιεί κάθε φορά διαφορετικά τοπικά δίκτυα υπολογιστών από διαφορετικά Internet Cafe, τότε ο εντοπισμός του θα είναι πολύ δύσκολος αλλά όχι αδύνατος.

Η Υπηρεσία της Παροχής Υπηρεσιών Πιστοποίησης

Οι Πάροχοι Υπηρεσιών Πιστοποίησης

- Με τον όρο *Πάροχος Υπηρεσιών Πιστοποίησης* (ΠΥΠ) – Certification Services Provider ή *Έμπιστη Τρίτη Οντότητα* (ΕΤΟ) – Trusted Third party (TTP) ή και *Δημόσια Αρχή Πιστοποίησης* (Public Certification Authority) αναφερόμαστε σ' έναν φορέα (οργανισμό) που είναι μια ανεξάρτητη επιχείρηση, η οποία μπορεί και προσφέρει υπηρεσίες ασφάλειας και εμπιστοσύνης στο ηλεκτρονικό εμπόριο.
- Ένας Πάροχος Υπηρεσιών Πιστοποίησης χορηγεί ψηφιακά πιστοποιητικά (ψηφιακές ή απλές ηλεκτρονικές υπογραφές) σε μεμονωμένους χρήστες ή και σε εταιρείες και εξασφαλίζει ότι η ψηφιακή (προηγμένη ηλεκτρονική) υπογραφή που χρησιμοποιεί ένας χρήστης ανήκει όντως σ' αυτόν (αποφυγή πλαστοπροσωπίας).

Η Υπηρεσία της Χρονοσήμανσης

- Ένας Πάροχος Υπηρεσιών Πιστοποίησης, εκτός από την βασική λειτουργία της χορήγησης της ψηφιακής υπογραφής, μπορεί να προσφέρει και την υπηρεσία της χρονοσήμανσης, με την οποία τίθεται μια ηλεκτρονική σφραγίδα στο έγγραφο που αποστέλλει ένας χρήστης και η οποία δεν μπορεί να τροποποιηθεί ούτε να αμφισβητηθεί και καθορίζει τον ακριβή χρόνο της αποστολής του μηνύματος.
- Ένα πολύ χαρακτηριστικό παράδειγμα όπου μπορεί να βρει εφαρμογή η υπηρεσία της χρονοσήμανσης είναι η ηλεκτρονική υποβολή δηλώσεων ή αιτήσεων προς μια δημόσια υπηρεσία (π.χ. υποβολή καταστάσεων ΦΠΑ), όπου δεν γίνονται δεκτές αιτήσεις μετά από μια καθορισμένη προθεσμία.

Η Υπηρεσία της Αποθήκευσης Μηνυμάτων

- Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να λειτουργήσει και ως ηλεκτρονικός συμβολαιογράφος, στον οποίο μπορεί κάποιος τρίτος να καταθέσει κείμενα (αντίγραφα) που έχουν αξία, όπως ένα συμβόλαιο ή μια φορολογική δήλωση, έτσι ώστε σ' οποιονδήποτε φορολογικό ή άλλον έλεγχο να μπορεί να πιστοποιηθεί ποιο ήταν το κείμενο που πράγματι εστάλη αρχικά.

Ποινικά Αδικήματα από τη Χρήση του Internet

Τηλεχειρισμός (Κατασκοπεία) του Υπολογιστή μας

- Υπάρχουν ειδικά προγράμματα που δίνουν την δυνατότητα σ' έναν χρήστη να τηλεχειρίζεται τον υπολογιστή ενός άλλου χρήστη που είναι ταυτόχρονα συνδεδεμένος στο Διαδίκτυο, όταν γνωρίζει την IP διεύθυνσή του.
- Και η δυνατότητα αυτή σημαίνει την υποκλοπή αρχείων και προγραμμάτων, τη διαγραφή (format) του σκληρού δίσκου ή την ενεργοποίηση της Web cameras κ.ά.
- Ένας μεσήλικας 47χρονος οικογενειάρχης, τεχνικός υπολογιστών, συνελήφθη στην Κύπρο τον Απρίλιο του 2005 με την κατηγορία ότι έκανε πειρατεία στον υπολογιστή μιας 17χρονης και ενεργοποίησε την Web camera της για να καταγράφει την σεξουαλική της συμπεριφορά. Η Αστυνομία της Κύπρου συνέλαβε τον δράστη με την κατηγορία της σεξουαλικής παρενόχλησης.

Οι Ιοί (Viruses) των Υπολογιστών

- Ο Ιός (Virus) είναι ένα πρόγραμμα, συνήθως μικρό σε χωρητικότητα, αλλά πολύ αποτελεσματικό σε δράση, που έχει την ικανότητα να μεταδίδεται μεταξύ υπολογιστών και δικτύων και να δημιουργηθεί αντίγραφα του εαυτού του χωρίς φυσικά να το γνωρίζει ή να το εγκρίνει ο χρήστης. Άλλες μορφές ιών είναι τα Σκουλήκια (Worms) και οι Δούρειοι Ίπποι (Trojan Horses).
- Η ζημιά που κάνει μπορεί να κυμαίνεται από την απλή εμφάνιση ενός ενοχλητικού μηνύματος έως και τη διαγραφή όλων των δεδομένων του σκληρού δίσκου του υπολογιστή που έχει μολύνει.
- Ο συνηθέστερος τρόπος μόλυνσης ενός υπολογιστή σήμερα είναι μέσω του e-mail με απατηλά μηνύματα που περιέχουν ένα συνημμένο αρχείο με το πρόγραμμα του ιού, το οποίο εκτελείται αυτόματα και μολύνει τον υπολογιστή του χρήστη που θα κάνει το λάθος να ανοίξει το ύποπτο μήνυμα.

Ποινικά Αδικήματα με Ιούς

- Το 2002 αμερικανικό δικαστήριο καταδίκασε σε φυλάκιση 20 μηνών τον δημιουργό του ιού Melissa. Ήταν από τους πρώτους ιούς που μεταδιδόταν μέσω μηνυμάτων e-mail και προξένησε ζημιές εκατομμυρίων δολαρίων. Η ποινή θεωρείται ελαστική καθώς συνεκτιμήθηκε η προσφορά του δράστη στην ανίχνευση και τον εντοπισμό άλλων ιών.
- Πρόσφατα, μεγάλη βρετανική εταιρεία που δραστηριοποιείται στα στοιχήματα μέσω του Διαδικτύου έπεσε θύμα εκβιασμού από σπείρα δημιουργίας ιών υπολογιστών, οι οποίοι της ζήτησαν να καταθέτει τακτικά ένα μεγάλο χρηματικό ποσό σ' έναν λογαριασμό στη Λετονία, προκειμένου να μην γίνονται επιθέσεις ιών στους υπολογιστές της.

Το Μέλλον των Ιών

- Οι ιοί των υπολογιστών έχουν αλλάξει χρήση τελευταία και από ένα παιχνίδι νεαρών κομπιουτεράδων έχουν αρχίσει να προσφέρουν τις υπηρεσίες τους στο οργανωμένο έγκλημα, κλέβοντας αριθμούς πιστωτικών καρτών, κωδικούς λογαριασμών, απόρρητα αρχεία και άλλα ψηφιακά μυστικά που αποκαλύπτουν οι χρήστες όταν κάνουν αγορές και παραγγελίες στο Διαδίκτυο.
- Οι ιοί του μέλλοντος είναι πολύ πιθανό να χρησιμοποιηθούν στην κατασκοπεία και στον στρατό είτε για την καταστροφή αρχείων είτε για τη συλλογή πληροφοριών.
- Οι ημέρες που τους ιούς τούς δημιουργούσαν έφηβοι που ήθελαν να διασκεδάσουν έχουν παρέλθει και είναι πολλοί αυτοί που θα τις αναπολήσουν.

Οι Hackers και οι Crackers

- Το hacking είναι ποινικό αδίκημα σε πολλές χώρες και πιο συγκεκριμένα τιμωρείται όποιος αποκτήσει χωρίς εξουσιοδότηση πρόσβαση σε συστήματα πληροφοριών, προκαλέσει ζημιά, αποκομίσει από τις ενέργειές του οικονομικό όφελος ή αποδειχθεί ότι είναι μέλος δικτύου οργανωμένου εγκλήματος.
- Ο πιο γνωστός hacker παγκοσμίως είναι ο Αμερικανός Kevin Mitnic, ο οποίος αφού εξέτισε πολυετή ποινή φυλάκισης αποφάσισε να συνεργασθεί με τις αρχές στην καταπολέμηση του ηλεκτρονικού εγκλήματος.

Η Νέα Φιλοσοφία στο Hacking

- Η νέα φιλοσοφία που επικρατεί τελευταία στους hackers και τους crackers είναι όχι η πρόκληση ζημιάς στους υπολογιστές, κάτι που είναι πολύ εύκολο να γίνει αντιληπτό, αλλά η παρακολούθηση και η καταγραφή των κινήσεων και των επιλογών των χρηστών που περιηγούνται στο Internet και η πώληση αυτών των στατιστικών στοιχείων σε ενδιαφερόμενες εταιρείες.

Επιθέσεις σε Web Sites Υπηρεσιών και Οργανισμών

- Η ουσία του προβλήματος δεν εντοπίζεται στις επιθέσεις που γίνονται στην πρώτη (αρχική) ιστοσελίδα (Home Page) του δικτυακού τόπου μιας δημόσιας υπηρεσίας ή ενός μεγάλου οργανισμού, κάτι που είναι πολύ εύκολο να γίνει αντιληπτό.
- Άλλο μεγάλο πρόβλημα είναι οι ύπουλες επιθέσεις, το να τροποποιήσει δηλαδή κάποιος χωρίς να γίνει αντιληπτός σημαντικά δεδομένα που τηρούνται από τις δημόσιες υπηρεσίες, όπως είναι η αλλαγή της σειράς επιτυχίας σ' έναν διαγωνισμό, η αλλαγή της προϋπηρεσίας υποψηφίων, ημερομηνιών κοκ.

Τα Cookies

- Τα cookies (μπισκοτάκια) αποτελούν ένα από τα ακανθώδη θέματα του Internet που έχουν να κάνουν με τα προσωπικά δεδομένα και το προσωπικό απόρρητο των χρηστών του Διαδικτύου.
- Η σημαντικότερη χρήση των cookies είναι για να παρακολουθούν και να καταγράφουν (κατασκοπεύουν) τις κινήσεις μας στο Internet, συνήθως τις καταναλωτικές, όπως σε ποια sites περιηγούμαστε και πόσο χρόνο μένουμε σ' αυτά, πόσο συχνά τα επισκεπτόμαστε κ.ά. Ακόμη και μέσα στο ίδιο το site μπορούν να καταγράψουν σε ποιες ιστοσελίδες έχουμε προτίμηση.

Διαχείριση των Προσωπικών Δεδομένων των Χρηστών

- Αυτό που έχει ανησυχήσει πολλούς χρήστες σχετικά με τα cookies είναι ο κίνδυνος να διαρρεύσουν οι πληροφορίες αυτές σε τρίτα άτομα ή και η πιθανότητα τα προσωπικά τους δεδομένα να διατίθενται σε τρίτους χωρίς τη δική τους συναίνεση.
- Οι διαχειριστές ενός Web site που χρησιμοποιεί κατά κόρον τα cookies έχουν τη δυνατότητα να χρησιμοποιήσουν τις πληροφορίες που συγκεντρώνουν σχετικά με τις προσωπικές προτιμήσεις των επισκεπτών (χρηστών) τους είτε για να βελτιώσουν την εικόνα του site τους ή για να προμηθεύσουν αυτά τα πολύτιμα στοιχεία σε τρίτους και κυρίως σε διαφημιστικές εταιρείες.

Το e-marketing

- Μιλάμε συνεπώς για ένα νέο είδος marketing, το e-marketing. Τα cookies αποτελούν παντοδύναμα εργαλεία marketing, καθώς μπορούν να χρησιμοποιηθούν για να δημιουργηθούν λεπτομερή καταναλωτικά προφίλ για τους χρήστες του Internet.
- Οι δημιουργοί των δικτυακών τόπων που χρησιμοποιούν cookies προβάλλουν το επιχείρημα ότι η χρήση των cookies εξυπηρετεί και τους ίδιους τους καταναλωτές – χρήστες του Internet, καθώς μπορούν έτσι να αποκτήσουν ενημέρωση και πληροφόρηση κομμένη και ραμμένη στα μέτρα τους.

Τα Spam e-mails

- Με τον όρο spam εννοούμε την απρόκλητη, εμπορική και μαζική αποστολή μεγάλου αριθμού ηλεκτρονικών μηνυμάτων, τα οποία απευθύνονται σ' ένα σύνολο χρηστών του Internet, χωρίς αυτοί να έχουν ζητήσει ή να επιθυμούν κάτι τέτοιο και χωρίς να έχουν συνειδητά προκαλέσει την επικοινωνία με τον αποστολέα των μηνυμάτων.
- Τα μηνύματα των spam e-mails είναι συνήθως ενημερωτικού ή διαφημιστικού περιεχομένου για προϊόντα ή και υπηρεσίες αμφίβολης ποιότητας και πιο σπάνια σεξουαλικού περιεχομένου.
- Ο όρος spam μπορεί να χαρακτηρισθεί ως *απρόκλητη* ή *αυτόκλητη* ή *ανεπιθύμητη αλληλογραφία* ή και *ανεπιθύμητα ηλεκτρονικά μηνύματα*. Η επίσημη απόδοση στα ελληνικά του αγγλικού όρου spam είναι *μη ζητηθείσα εμπορική επικοινωνία*.

Καταδίκη Spammer

- Σε 9 χρόνια φυλάκιση καταδίκασε αμερικανικό δικαστήριο έναν 30χρονο spammer στις αρχές του 2005, τον οποίο θεώρησε υπεύθυνο για την αποστολή δισεκατομμυρίων αυτόκλητων (ανεπίκλητων) μηνυμάτων ηλεκτρονικού ταχυδρομείου, τα γνωστά με τον όρο spam e-mails.
- Κρίθηκε ένοχος για την αποστολή 10 εκατομμυρίων spam e-mails σε καθημερινή βάση. Παρά το ότι η ανταπόκριση των χρηστών του Internet στις ανύπαρκτες υπηρεσίες και τα προϊόντα που διαφήμιζε ήταν μόλις ένα μήνυμα ανά 30.000 μηνύματα που έστελνε, κατόρθωσε να αποκομίσει περί τα 20 εκατομμύρια ευρώ.

Νομοθεσία για το Spam

- Στην Ελλάδα, για το θέμα της μη ζητηθείσας εμπορικής επικοινωνίας έχει ισχύ το άρθρο 6 του ΠΔ.131/2003 (Οδηγία για το Ηλεκτρονικό Εμπόριο), όπου αναφέρεται ότι οι ISP's που αναλαμβάνουν τέτοιες δραστηριότητες (αποστολή spam e-mails) οφείλουν να τηρούν και να συμβουλεύονται τακτικά, μητρώα «επιλογών», όπου μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μην λαμβάνουν τέτοιες εμπορικές επικοινωνίες.
- Επίσης, στο άρθρο 9 του Ν.2774/1999 «Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Τηλεπικοινωνιακό Τομέα» ορίζεται ότι η με οποιοδήποτε τηλεπικοινωνιακό μέσο απ' ευθείας εμπορική προώθηση προϊόντων ή υπηρεσιών επιτρέπεται μόνον στην περίπτωση συνδρομητών, οι οποίοι έχουν δώσει εκ των προτέρων τη ρητή συγκατάθεσή τους.

Ο Κυβερνοσφετερισμός (Cybersquatting)

- Πρόκειται για ένα φαινόμενο του Internet, όπου διάφοροι επιτήδειοι, τον πρώτο καιρό που το Διαδίκτυο είχε αρχίσει να γίνεται δημοφιλές για εμπορική χρήση, έσπευσαν να κατοχυρώσουν σ' αυτό εμπορικά σήματα εταιρειών (επωνυμίες ή και διακριτικούς τίτλους), αποκτώντας το αντίστοιχο όνομα χώρου (domain name), με απώτερο στόχο να τα πωλήσουν (μεταβιβάσουν) στους νόμιμους ιδιοκτήτες τους όταν αυτοί θελήσουν αργότερα να δραστηριοποιηθούν στο Internet.
- Υπήρξαν περιπτώσεις όπου μεγάλες και επώνυμες εταιρείες αναγκάσθηκαν να πληρώσουν σεβαστά ποσά για να αποκτήσουν μια ιστοσελίδα με το δικό τους όνομα, το οποίο όμως είχε φροντίσει να κατοχυρώσει νωρίτερα κάποιος άλλος.
- Στις ΗΠΑ και τη Γερμανία έχουν εκδοθεί νομοσχέδια που προστατεύουν τις επιχειρήσεις από τις καταχρηστικές καταχωρίσεις ονομάτων χώρου (domain names).

Τα Ονόματα Χώρου (Domain Names)

Η Ελληνική Νομοθεσία για τα Ονόματα Χώρου

- Απόφαση της Ε.Ε.Τ.Τ. με αριθ. *268/73/31-12-2002 «Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr»*.
- Η Ε.Ε.Τ.Τ. έχει στη δικαιοδοσία της την εποπτεία, τον συντονισμό και τον έλεγχο των διαδικασιών που αφορούν στη διαχείριση του top level domain .gr και είναι αποκλειστικά αρμόδια για την εκχώρηση :
- Ονομάτων Χώρου 2ου επιπέδου με κατάληξη .gr, π.χ. *florina.gr*, και
- Ονομάτων Χώρου 3ου επιπέδου με κατάληξη .gr των οποίων μόνο το τρίτο επίπεδο είναι Μεταβλητό Πεδίο (π.χ. *florina.com.gr*, *florina.edu.gr*).

Κανόνες για τα Ονόματα Χώρου

- Τα Ονόματα Χώρου με κατάληξη .gr αποτελούνται από αλφαριθμητικούς χαρακτήρες του λατινικού αλφαβήτου [A-Z, a-z, 0-9] και τον ειδικό χαρακτήρα [-] και έχουν μήκος από 3 έως 63 χαρακτήρες χωρίς την κατάληξη .gr.
- Τα Ονόματα Χώρου δεν μπορούν να αρχίζουν ή να τελειώνουν με τον χαρακτήρα [-] και δεν μπορούν να περιέχουν διαδοχικούς χαρακτήρες [-]. Δεν υπάρχει διαφοροποίηση μεταξύ των μικρών ή κεφαλαίων χαρακτήρων.
- Το δικαίωμα που αποκτάται με την Εκχώρηση Ονόματος Χώρου με κατάληξη .gr διαρκεί για δύο χρόνια.

Χρήση των Γεωγραφικών Ονομάτων

- Δεν επιτρέπεται η χρήση γεωγραφικών ονομάτων, δηλ. ονομάτων που αποτελούν ονόματα πόλεων, κοινοτήτων ή γεωγραφικών περιοχών, παρά μόνο από τις αντίστοιχες αρχές (Περιφέρειες, Νομαρχίες, Δήμοι, Κοινότητες, ΟΤΑ κλπ), ανεξάρτητα αν αναφέρονται ή όχι στο σχέδιο Καποδίστριας.

Οι Καταχωρητές (Registrars)

- Τις 39 είχαν φθάσει στην Ελλάδα στις αρχές του 2005, οι εταιρείες που έχουν λάβει τη σχετική άδεια από την Ε.Ε.Τ.Τ. και αναλαμβάνουν την εκχώρηση σε τρίτους των ονομάτων δικτυακών τόπων ή ονομάτων χώρου (domain names) με κατάληξη .gr, μετά την έναρξη της εφαρμογής του νέου τρόπου εκχώρησης από τις 5 Απριλίου 2004. Οι εταιρείες αυτές αποκαλούνται Καταχωρητές (Registrars).
- Το σχετικό Μητρώο των ονομάτων χώρου τηρείται από το Ίδρυμα Τεχνολογίας και Έρευνας (ΙΤΕ), το οποίο εδρεύει στην Κρήτη, και το οποίο παύει να λειτουργεί ως καταχωρητής.
- Τα καταχωρισμένα ονόματα χώρου με κατάληξη .gr είχαν φθάσει τα 80.000 στις αρχές του 2004.

Δικαιούχοι των Ονομάτων Χώρου

- Δεν υπάρχει περιορισμός στον αριθμό των ονομάτων χώρου που μπορούν να εκχωρηθούν σ' ένα φυσικό ή νομικό πρόσωπο, επιτρέπεται η εκχώρηση σε αλλοδαπά πρόσωπα και προστατεύεται πλήρως ό,τι είναι εμπορικό σήμα ή διακριτικό γνώρισμα.
- Η Ε.Ε.Τ.Τ. μπορεί να δρα αυτεπάγγελτα ή μετά από καταγγελία και να απενεργοποιεί ονόματα χώρου, περιορίζοντας τυχόν απόπειρες για απάτες.
- Τα ονόματα χώρου που δεν έχουν ανανεωθεί και πρόκειται να διαγραφούν, παραμένουν ανενεργά επί 6 μήνες από την ημέρα απενεργοποίησής τους (κατάσταση SUSPENDED) πριν διαγραφούν οριστικά, ώστε να προλάβουν να ενημερωθούν σχετικά οι χρήστες.

Δικαίωμα για Ονόματα Χώρου σε Subdomains

- Επιτρέπεται στους κατόχους κατοχυρωμένου εμπορικού σήματος, η καταχώριση του domain και σ' όλα τα subdomains (.com.gr, .org.gr, .net.gr, .edu.gr) του .gr, χωρίς την ανάγκη ύπαρξης ενός σήματος ανά καταχωρημένο domain.
- Η κάθε καταχώρηση αντιστοιχεί σε νέο όνομα χώρου και έχει την ανάλογη χρέωση, ενώ απαιτείται και η υπογραφή διαφορετικής σύμβασης για κάθε ένα από τα εκχωρηθέντα ονόματα χώρου.

Το Ηλεκτρονικό Έγκλημα

Οι Συνήθεις Μορφές του Ηλεκτρονικού Εγκλήματος

- Συκοφαντική δυσφήμηση προσώπων μέσω του Internet.
- Παράνομη διακίνηση και πώληση προγραμμάτων (πειρατεία λογισμικού).
- Εγκλήματα από hackers ή crackers (δικτυοπειρατεία).
- Διακίνηση υλικού παιδικής πορνογραφίας
- Απάτες με πιστωτικές κάρτες.

Οι Συνηθισμένες Μέθοδοι Ηλεκτρονικής Επίθεσης

- Επίθεση στην ιστοσελίδα μιας εταιρείας ή μιας υπηρεσίας, ώστε να μην λειτουργεί σωστά.
- Εισβολή στους ηλεκτρονικούς υπολογιστές μιας εταιρείας και πρόκληση βλαβών.
- Εγκατάσταση προγραμμάτων-κατασκόπων (spyware) στον υπολογιστή ενός χρήστη, ώστε να παρακολουθούνται και να καταγράφονται οι κινήσεις και οι επιλογές του, για στατιστικούς ή και άλλους πιο κακόβουλους λόγους, όπως εμπορευματοποίηση των προσωπικών του δεδομένων ή των καταναλωτικών του συνηθειών.
- Αποστολή μηνυμάτων με παραπλανητικό περιεχόμενο, ώστε να εξαπατηθεί ο χρήστης και να αποκαλύψει στοιχεία πιστωτικών καρτών, κωδικούς τραπεζικών λογαριασμών κ.ά.

Τα Κυκλώματα Παιδικής Πορνογραφίας

- Σε μάστιγα ή στη Λερναία Ύδρα του Internet, τείνει να εξελιχθεί το φαινόμενο της διακίνησης παιδικού πορνογραφικού υλικού (παιδοφιλία) μέσω του Διαδικτύου.
- Σύμφωνα με τα στατιστικά στοιχεία του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής, από τις αρχές του 2004 έως τον Απρίλιο του 2005 έχουν εξιχνιασθεί 48 υποθέσεις διακίνησης υλικού παιδικής πορνογραφίας μέσω του Internet, έχουν συλληφθεί 68 άτομα και έχουν κατηγορηθεί συνολικά 90.
- Το Τμήμα αυτό έχει εξιχνιάσει 105 τέτοιες υποθέσεις το διάστημα 2002-2005, αλλά σχεδόν καμία δεν έχει λήξει δικαστικά.

Η Νομοθεσία για την Παιδική Πορνογραφία

- Ενώ στο εξωτερικό υπάρχουν οργανωμένα κυκλώματα, κυρίως στις ΗΠΑ και τη Ρωσία, στη χώρα μας οι συγκεκριμένοι δράστες δρουν ακόμα μεμονωμένα. Επίσης, σ' όλες τις υποθέσεις που έχουν αποκαλυφθεί, οι συλληφθέντες είναι και οι ίδιοι παιδόφιλοι.
- Οι υποθέσεις που σχετίζονται με τη δημιουργία, διακίνηση και πώληση πορνογραφικού υλικού ανηλίκων μέχρι τον Οκτώβριο του 2002 τιμωρούνταν στη χώρα μας σύμφωνα με τον νόμο «περί ασέμνων» και το αδίκημα αντιμετωπιζόταν ως πλημμέλημα, ενώ σήμερα προβλέπονται ποινές έως και ισόβιας κάθειρξης.
- Σχετικός είναι ο **Ν.3064/2002** και μέχρι τώρα 80 άτομα έχουν διωχθεί ποινικά σε εφαρμογή του νόμου αυτού. Οι ποινικές διώξεις ήταν για πλημμελήματα και για κακουργήματα.

Οι Δυσκολίες στη Στοιχειοθέτηση Κατηγορίας

- Το κύριο πρόβλημα μ' αυτές τις περιπτώσεις είναι να στοιχειοθετηθούν οι κακουργηματικές κατηγορίες. Το δικαστήριο δυσκολεύεται να ταυτοποιήσει τα στοιχεία των παιδιών – θυμάτων και να πάρει καταθέσεις απ' αυτά για το αν πράγματι τούς ασκήθηκε ψυχολογική ή άλλης μορφής πίεση.
- Τα άτομα που συλλαμβάνονται ισχυρίζονται συνήθως ότι δεν έχουν καμία σχέση με τη φωτογράφιση των ανηλίκων και ότι απλά κατέβασαν από το Internet κάποιες φωτογραφίες και τις τοποθέτησαν στις ιστοσελίδες τους. Ένας μάλιστα από τους συλληφθέντες ισχυρίσθηκε ότι χρησιμοποίησε αυτό το υλικό για την έρευνα που κάνει στο Πανεπιστήμιο.
- Η διαδικασία της συγκέντρωσης του αποδεικτικού υλικού για την τεκμηρίωση των σχετικών δικογραφιών αποδεικνύεται ιδιαίτερα δύσκολη και χρονοβόρα και μπορεί να πάρει μήνες. Πολλές μεγάλες υποθέσεις παιδοφιλίας βρίσκονται για πολύ καιρό στο στάδιο της εργαστηριακής διερεύνησης.

Το Προφίλ των Δραστών

- Οι εξηγήσεις που δίνουν οι ειδικοί για τη ραγδαία εξάπλωση αυτού του φαινομένου είναι ψυχολογικές και κοινωνικές.
- Οι δράστες είναι συνήθως προσωπικότητες με ψυχοπαθολογικά στοιχεία που είναι πολύ πιθανό να κακοποιήθηκαν στην παιδική τους ηλικία.
- Το προφίλ των δραστών είναι άτομα με ανώτερη μόρφωση, οικογενειάρχες, οικονομικά ευκατάστατοι και ηλικίας συνήθως από 30 έως 50 ετών. Μεταξύ των δραστών εντοπίσθηκαν εκπαιδευτικοί και δικηγόροι.

Αυτοκτονία μέσω Internet

- Τον Σεπτέμβριο του 2004, ένας ανήλικος μαθητής Λυκείου στην Αθήνα αυτοκτόνησε μ' ένα πολύ τοξικό γεωργικό φαρμάκο, αφού είχε λάβει προηγουμένως σχετικές οδηγίες από το Internet μέσω e-mail και ενός chat room.
- Καταλυτική υπήρξε η επικοινωνία του μ' έναν 25χρονο σμηνία από τα Χανιά, ο οποίος χρησιμοποιούσε γυναικείο ψευδώνυμο στις επικοινωνίες του με τον αυτόχειρα και ήταν αυτός που τον πληροφόρησε σχετικά με το δραστικό γεωργικό φάρμακο.
- Η Αστυνομία χρειάσθηκε πολύμηνες έρευνες για να φθάσει στα ίχνη του χρήστη-συμβούλου και αυτό γιατί ο τελευταίος χρησιμοποιούσε όχι τον υπολογιστή του σπιτιού του αλλά έναν από τους τρεις υπολογιστές ενός Internet Cafe στα Χανιά. Εις βάρος του 25χρονου σχηματίστηκε δικογραφία για παράβαση του άρθρου 501 «συμμετοχή σε αυτοκτονία», κατηγορία που είναι σε βαθμό πλημμελήματος. Κατά την ανάκριση του 25χρονου προέκυψε νομικό κενό στην υπόθεση αυτή.

Θέματα Πνευματικής Ιδιοκτησίας και Προσωπικών Δεδομένων

Αναμετάδοση Ραδιοφωνικών Εκπομπών μέσω Internet

- Τον Φεβρουάριο του 2002 εκδόθηκε από το τμήμα ασφαλιστικών μέτρων του Πρωτοδικείου Θεσσαλονίκης απόφαση διακοπής της μετάδοσης μουσικών κομματιών και τραγουδιών μέσω της ιστοσελίδας ραδιοφωνικού σταθμού.
- Για την αναμετάδοση μουσικών κομματιών και τραγουδιών μέσω του Internet απαιτείται έγγραφη άδεια από την ΑΕΠΠΙ *(Ανώνυμη Εταιρεία Προστασίας της Πνευματικής Ιδιοκτησίας)*, άσχετα με το αν υπάρχει ήδη αντίστοιχη άδεια για την αναμετάδοση μουσικών κομματιών και τραγουδιών μέσω ραδιοφώνου. Είναι η πρώτη φορά που η ΑΕΠΠΙ κινήθηκε δικαστικά για θέματα πνευματικής ιδιοκτησίας στο Διαδίκτυο.
- Υπεύθυνος για την αναμετάδοση του προγράμματος είναι, εκτός από τον ραδιοφωνικό σταθμό, και ο ISP που παρέχει υπηρεσίες Web hosting και διαμεσολαβεί στην παράνομη αναμετάδοση, παρέχοντας την απαιτούμενη υποστήριξη και σύνδεση στο Internet.

Το e-mail Είναι Απόρρητο

- Με πρόσφατη απόφασή της (61/17-11-2004), ύστερα από σχετική καταγγελία σωματείου εργαζομένων εταιρείας στην Αθήνα, η Αρχή Προστασίας Προσωπικών Δεδομένων απαγορεύει στους εργοδότες τα εξής :
  - 1. Τον έλεγχο του e-mail των υπαλλήλων μιας εταιρείας.
  - 2. Την καταγραφή των ιστοσελίδων που επισκέπτονται οι υπάλληλοι.
  - 3. Τον έλεγχο των προσωπικών αρχείων των εργαζομένων που βρίσκονται στον σκληρό δίσκο του υπολογιστή που χρησιμοποιούν και
  - 4. Τη συλλογή και επεξεργασία δεδομένων από την ηλεκτρονική επικοινωνία των εργαζομένων.

Παρακολούθηση Χωρίς Κατάχρηση

- Στη Βρετανία, ένας νέος νόμος δίνει το δικαίωμα στις επιχειρήσεις να παρακολουθούν το τι κάνουν οι υπάλληλοί τους στο Διαδίκτυο κατά τις ώρες εργασίας χωρίς όμως να γίνεται κατάχρηση αυτού του δικαιώματος.
- Είναι προφανές ότι η βρετανική κυβέρνηση προσπάθησε να ισορροπήσει κάπως τα πράγματα ανάμεσα στις απαιτήσεις μιας επιχείρησης και στην προστασία των ατομικών δικαιωμάτων και του προσωπικού απορρήτου των εργαζομένων.
- Τον τελευταίο λόγο για τις όποιες νομικές υποθέσεις προκύψουν τον έχουν πάντα τα δικαστήρια.

Η Σχέση ISP και Συνδρομητή

Αποκάλυψη της Ταυτότητας του Συνδρομητή από τον ISP

- Η σχετική νομοθεσία (άρθρα 11 – 14 του ΠΔ.131/2003) αναφέρει ότι οι ISP's δεν έχουν υποχρέωση ελέγχου των πληροφοριών που μεταδίδονται μέσα από τα δίκτυά τους και δε φέρουν καμία ευθύνη για τη χρήση των υπηρεσιών τους και αυτό γιατί το όποιο παράνομο υλικό δεν βρίσκεται μόνιμα αποθηκευμένο στο δίκτυό τους, αλλά προσωρινά και για όσο χρόνο απαιτείται για τις ανάγκες της μετάδοσής του προς τον παραλήπτη.
- Οι ISP's είναι, όμως, υποχρεωμένοι να ενημερώνουν τις αρμόδιες κρατικές αρχές για όποιες υπόνοιες υπάρχουν σχετικά με παράνομες πληροφορίες που διακινούν ή δραστηριότητες που κάνουν οι συνδρομητές τους καθώς και να ανακοινώνουν στις αρμόδιες κρατικές αρχές όποια στοιχεία είναι απαραίτητα για τον εντοπισμό των παραβατών και αυτό χωρίς να παραβιάζονται οι σχετικές διατάξεις περί προστασίας του απορρήτου και των προσωπικών δεδομένων.

Άρση της Ανωνυμίας του Χρήστη

- Από τη στιγμή που θα διαπιστωθεί μια παράνομη πράξη ενός χρήστη, όπως είναι το μοίρασμα απαγορευμένων (πειρατικών) αρχείων, καταγράφεται η IP διεύθυνσή του και μετά είναι εύκολη υπόθεση να βρεθεί η εταιρεία (ISP) που του παρέχει την πρόσβαση στο Internet.
- Το επόμενο βήμα είναι να ζητηθεί η άρση της ανωνυμίας του συνδρομητή και να αποκαλυφθούν τα προσωπικά του στοιχεία.
- Το **ΠΔ.47/2005** ορίζει τους όρους και τις προϋποθέσεις άρσης του απορρήτου των επικοινωνιών για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων καθώς και για λόγους εθνικής ασφαλείας.

Ενημέρωση του Χρήστη για την Αποκάλυψη των Στοιχείων του

- Σχετικά με τις προϋποθέσεις άρσης του απορρήτου ενός συνδρομητή, αυτό επιβάλλεται να γίνει όταν ζητείται από εισαγγελείς ή ανακριτές και μάλιστα χωρίς τη συγκατάθεση του χρήστη.
- Στο άρθρο 5 του **Ν.2472/1997** (προσωπικά δεδομένα) προβλέπεται ότι η χορήγηση (αποκάλυψη) των στοιχείων σε τρίτους χωρίς να το γνωρίζει ο συνδρομητής εναπόκειται στην κρίση (διακριτική ευχέρεια) του ISP.
- Λόγο έχει και η Αρχή Προστασίας Προσωπικών Δεδομένων.
- Ο **Ν.2274/1999** (προσωπικά δεδομένα στον τηλεπικοινωνιακό τομέα) προβλέπει ποινικές κυρώσεις για όποιον χρησιμοποιεί δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών.

Σύναψη Συμβολαίου με τον ISP

- Επίσης, στο άρθρο 11 του τροποποιημένου **Ν.2472/1997** προβλέπεται ότι ο χρήστης (συνδρομητής) θα πρέπει να ενημερώνεται για την επικείμενη ανακοίνωση των προσωπικών του στοιχείων πριν ενημερωθούν οι τρίτοι.
- Μπορεί, όμως, να γίνει άρση αυτής της υποχρέωσης ενημέρωσης όταν πρόκειται για θέματα εθνικής ασφαλείας ή για την εξακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.
- Για να διασφαλισθεί, ο ίδιος ο ISP έχει τη δυνατότητα να ορίσει στο συμβόλαιο που συνάπτει με τους συνδρομητές του, ειδικές προβλέψεις απαγόρευσης κάθε είδος ενεργειών που είναι αντίθετες με τον νόμο και τη δεοντολογία του Διαδικτύου.

Η Ευθύνη του ISP για τη Χρήση των Υπηρεσιών του από τους Συνδρομητές του

- Οι ISPs έχουν κάνει προσπάθειες για να αποφύγουν με κάθε τρόπο κάθε νομική υπαιτιότητά τους σχετικά με το περιεχόμενο των ιστοσελίδων που δημοσιεύουν αλλά και των πληροφοριών που διακινούν οι χρήστες μέσα από τους servers τους.
- Αυτό μπορεί να φαίνεται λογικό από τη μια πλευρά αλλά στην πράξη δεν υπάρχει μια κοινά αποδεκτή συμφωνία για τον βαθμό ευθύνης που έχουν οι ISPs σχετικά με τις πληροφορίες που επιτρέπεται να διακινούνται αλλά και να αποθηκεύονται στους υπολογιστές τους.
- Αν το δούμε από πρακτική άποψη είναι τεχνικά αδύνατο να ελέγχεται όλη αυτή η τεράστια ποσότητα δεδομένων που διακινείται καθημερινά μέσα από τους servers των ISPs, όπως είναι τα e-mails, τα μηνύματα στα newsgroups, τα μηνύματα στα chat rooms, οι διάφορες ιστοσελίδες που δημοσιεύουν οι χρήστες (συνδρομητές) ενός ISP κ.ά.

Η Ευθύνη του ISP για τη Χρήση των Υπηρεσιών του από τους Συνδρομητές του

- Στο ερώτημα αν ένας ISP έχει ευθύνη για τις ιστοσελίδες που δημοσιεύει ένας συνδρομητής του, η απάντηση είναι αρχικά όχι εφόσον έχει υπογραφεί ένα κείμενο συμφωνίας (σύμβαση) ανάμεσα στον ISP και τον χρήστη, το οποίο και καθορίζει επακριβώς τι επιτρέπεται να δημοσιευθεί και τι όχι στον χώρο που παραχωρείται στον χρήστη.
- Στην περίπτωση, όμως, που ένας ISP εκτός από υπηρεσίες Web hosting, δηλ. απλής φιλοξενίας ιστοσελίδων, παρέχει και υπηρεσίες Web design, δηλ. δημιουργίας και διαχείρισης ιστοσελίδων, ιδίως εμπορικής φύσης, οπότε ο ISP έχει μερίδιο από τα πιθανά κέρδη ενός δικτυακού τόπου, τότε θα πρέπει και ο ίδιος ο ISP να θεωρείται συνυπεύθυνος για το περιεχόμενο των ιστοσελίδων που φιλοξενούνται αλλά και των πληροφοριών που διακινούνται μέσω αυτού.

Ηλεκτρονικές Απάτες

Η Απάτη των Dialer-1

- Η απάτη λειτουργεί ως εξής : Μια ιστοσελίδα δελεάζει τον επισκέπτη, συνήθως με ανακοινώσεις για γυμνές φωτογραφίες επώνυμων γυναικών ή για καυτά videos on-line κ.ά., οι οποίες υπηρεσίες μάλιστα διαφημίζονται έντονα και τονίζεται ότι παρέχονται δωρεάν.
- Μόλις ο χρήστης κάνει κλικ σ' ένα συγκεκριμένο σημείο, εγκαθίσταται αυτόματα στον υπολογιστή του και χωρίς αυτός να το γνωρίζει, ένα ειδικό πρόγραμμα, με αποτέλεσμα αντί για αστική κλήση στον τοπικό provider (ο γνωστός ΕΠΑΚ, 8962…) να γίνεται εκτροπή και διεθνής κλήση σύνδεσης και μάλιστα υπερπόντια, με πολλαπλάσιο φυσικά κόστος.

Η Απάτη των Dialer-2

- Για παράδειγμα, ο χρήστης αντί για 0,17 – 0,35 € την ώρα, χρεώνεται με 2,50 € ανά λεπτό. Οι δημιουργοί παρόμοιων ιστοσελίδων έχουν κάνει συμβάσεις με τους τηλεπικοινωνιακούς οργανισμούς των χωρών αυτών και μοιράζονται τα κέρδη από τις υπέρογκες χρεώσεις των ανυποψίαστων χρηστών.
- Είναι ποινικό αδίκημα;
- Πάντως έχει γίνει ποινική δίωξη στην Ελλάδα σε βαθμό κακουργήματος το έτος 2004 για μια τέτοια υπόθεση. Οι τηλεφωνικές εταιρείες ισχυρίζονται ότι δεν φέρουν καμία ευθύνη για τις υποθέσεις αυτές και η μόνη παραχώρηση που μπορούν να κάνουν προς τους παθόντες είναι να αποπληρώσουν τα χρέη τους σε δόσεις.

Απάτες με το e-mail

- Διάφοροι επιτήδειοι στέλνουν ηλεκτρονικά μηνύματα με πολύ καλή σχεδίαση (design) και προσεκτικά σχεδιασμένους λογότυπους και σήματα που δίνουν την εντύπωση ότι προέρχονται από μεγάλες και επώνυμες τράπεζες και ζητάνε από τους χρήστες την αποκάλυψη του αριθμού της πιστωτικής τους κάρτας και των κωδικών PIN ώστε να αντιμετωπισθεί κάποιο υποτιθέμενο πρόβλημα με τον τραπεζικό τους λογαριασμό. Τους ενημερώνουν μάλιστα ότι σε περίπτωση μη ανταπόκρισής τους υπάρχει ο κίνδυνος αναστολής λειτουργίας του σχετικού λογαριασμού.
- Αν κάποιος χρήστης πέσει στην παγίδα και αποκαλύψει τον αριθμό του τραπεζικού του λογαριασμού μαζί με το PIN ή τον αριθμό της πιστωτικής του κάρτας, είναι ζήτημα χρόνου το άδειασμα του λογαριασμού του και φυσικά θα είναι σχεδόν αδύνατος ο εντοπισμός των δραστών.

Απάτες στο Ηλεκτρονικό Εμπόριο

Απάτες με Πιστωτικές Κάρτες στο e-commerce

- Το Internet είναι κάτι που δεν μπορεί να ελεγχθεί καθώς υπάρχουν πολλές εταιρείες φαντάσματα που δελεάζουν ανυποψίαστους πελάτες με μεγάλες οικονομικές προσφορές.
- Ο χρήστης – πελάτης όχι μόνο κινδυνεύει να πληρώσει για ένα προϊόν που δεν θα παραλάβει ποτέ αλλά αποκαλύπτει και τον αριθμό της πιστωτικής του κάρτας μ’ ό,τι αυτό συνεπάγεται.
- Οι απάτες με πιστωτικές κάρτες μπορεί να κυμαίνονται από την απλή κλοπή και παράνομη χρήση μιας πιστωτικής κάρτας έως και το σπάσιμο κωδικών στο Internet και την ανάληψη ή μεταφορά χρημάτων από τραπεζικούς λογαριασμούς.

Συνηθισμένες Ηλεκτρονικές Απάτες

- Σπάσιμο προφανών ή εύκολων κωδικών ατόμων που χρησιμοποιούν το Internet για τις τραπεζικές τους συναλλαγές (e-banking) και εν συνεχεία άδειασμα των τραπεζικών τους λογαριασμών.
- Η λεγόμενη «νιγηριανή απάτη», όπου στέλνονται χιλιάδες e-mail σε ανυποψίαστους χρήστες και ζητείται η βοήθειά τους έναντι αμοιβής. Αν κάποιος παραλήπτης του μηνύματος κάνει το λάθος να απαντήσει, τότε ακολουθούν κι άλλα παραπλανητικά μηνύματα μέχρι να ζητηθεί ένας τραπεζικός λογαριασμός του θύματος και να γίνει ανάληψη χρημάτων.
- Πολύ δημοφιλείς είναι και οι απάτες που γίνονται στις ηλεκτρονικές δημοπρασίες (e-auctions), όπου εμφανίζονται κάποιοι να πωλούν διάφορα αντικείμενα αλλά οι αγοραστές ενώ πληρώνουν κανονικά το συμφωνηθέν αντίτιμο δεν παραλαμβάνουν ποτέ το αντικείμενο.

Χαρακτηριστικά Παραδείγματα Απάτης και Παραπλάνησης

Η Περίπτωση του DirtyWorks.gr

- Ο 35χρονος διαδικτυακός καλλιτέχνης και γλύπτης Δημήτρης Φωτίου αναστάτωσε την ελληνική ιντερνετική κοινότητα στις αρχές του 2005, όταν αποφάσισε να διακωμωδήσει το πάθος (ευσεβή πόθο) των Ελλήνων για διορισμό στο Δημόσιο.
- Ο εικαστικός δημιουργός που ασχολείται με το net art, δηλ. την τέχνη του Διαδικτύου, συνελήφθη τον Φεβρουάριο του 2005 από το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής και κατηγορήθηκε για απάτη σε βαθμό κακουργήματος.
- Το αδίκημά του ήταν ότι σχεδίασε την ιστοσελίδα http://www.dirtyworks.gr, στην οποία υποσχόταν προσλήψεις στο Δημόσιο, μετεγγραφές φοιτητών, νομιμοποίηση αυθαιρέτων και εξασφαλισμένη επιτυχία σε διαγωνισμούς του ΑΣΕΠ έναντι αμοιβής και όλα αυτά ως σχόλιο στα ρουσφέτια της εποχής μας.

Δεν Επρόκειτο για Απάτη

- Το πρόβλημα που απασχόλησε την Αστυνομία ήταν βέβαια η πληρωμή των υπηρεσιών, η οποία γινόταν με πιστωτική κάρτα, αδίκημα σε βαθμό κακουργήματος.
- Όμως, η ιστοσελίδα ήταν έτσι σχεδιασμένη ώστε τα προσωπικά στοιχεία του χρήστη ποτέ δε έφευγαν από τον υπολογιστή του, δεν κατέληγαν πουθενά και φυσικά δεν καταχωρούνταν ποτέ στον server του dirtyworks.gr, ώστε να μπορέσει να τα αξιοποιήσει ο οποιοσδήποτε.
- Υπήρχε βέβαια και μια προειδοποίηση (ψιλά γράμματα) στην κάτω δεξιά πλευρά της ιστοσελίδας, με την επισήμανση ότι όσα αναφέρονταν στην ιστοσελίδα είναι εικονικά. Έτσι, ο Δημήτρης Φωτίου αφέθηκε προσωρινά ελεύθερος με εγγύηση.

Η Περίπτωση της Amazon.gr-1

- Το Πρωτοδικείο Σύρου έμελλε να είναι το πρώτο στην Ελλάδα που εκδίκασε υπόθεση ηλεκτρονικού εμπορίου και μάλιστα σε μια εποχή (1999) που η σχετική νομοθεσία ήταν ουσιαστικά ανύπαρκτη.
- Το θέμα είχε να κάνει με την πολύ γνωστή εταιρεία πώλησης βιβλίων και CD's (ηλεκτρονικό βιβλιοπωλείο) amazon, η οποία με έδρα το Delaware των ΗΠΑ κατοχύρωσε το όνομα χώρου (domain name) amazon.com και μέσω της ηλεκτρονικής διεύθυνσης www.amazon.com δεχόταν παραγγελίες απ' όλον τον κόσμο.
- Στην Ελλάδα, όπου η amazon δεν είχε φυσική παρουσία, εμφανίσθηκε μια άλλη εταιρεία η οποία με έδρα την Μύκονο ζήτησε και έλαβε τα domain names amazon.gr και amazon.com.gr από τον τότε αρμόδιο ελληνικό φορέα (ΙΤΕ) και ξεκίνησε να κάνει πωλήσεις βιβλίων και CD's.

Η Περίπτωση της Amazon.gr-2

- Η αμερικανική εταιρεία amazon προσέφυγε στα δικαστήρια και κατέθεσε αίτηση ασφαλιστικών μέτρων τον Αύγουστο του 1999 στο Πρωτοδικείο Σύρου ζητώντας την απαγόρευση χρήσης των παραπάνω domain names θεωρώντας ότι με τη χρήση των παραπάνω ηλεκτρονικών διευθύνσεων δημιουργείται σύγχυση στο καταναλωτικό κοινό καθώς οι αγοραστές έχουν την εντύπωση ότι παραγγέλνουν από το ελληνικό παράρτημα του διεθνούς ηλεκτρονικού βιβλιοπωλείου amazon.com.
- Το δικαστήριο με την υπ' αριθμ. *637/1999* απόφασή του έκρινε ότι η ελληνική εταιρεία προσέβαλε το δικαίωμα της amazon.com στην επωνυμία και τον διακριτικό τη τίτλο.

Η Περίπτωση της Amazon.gr-3

- Έτσι δικαίωσε την αμερικανική εταιρεία καθώς θεώρησε ότι δημιουργείται όντως σύγχυση στο καταναλωτικό κοινό δεδομένης της μεγάλης διεθνούς φήμης της καθώς ο χρήστης που θέλει να συνδεθεί με το ελληνικό παράρτημα του διεθνούς ηλεκτρονικού βιβλιοπωλείου amazon.com, θα βρεθεί άθελά του σε μια άλλη άσχετη εταιρεία.
- Το δικαστήριο έκρινε ότι η ελληνική εταιρεία προσπάθησε να εκμεταλλευθεί τον διακριτικό τίτλο της amazon.com και να αυξήσει έτσι τις πωλήσεις της κατά παράβαση των χρηστών ηθών και της καλής πίστης.
- Το δικαστήριο διέταξε την εταιρεία να σταματήσει να χρησιμοποιεί τον τίτλο amazon και να απενεργοποιήσει τα domain names amazon.gr και amazon.com.gr.

Η Περίπτωση της Εταιρείας Argos (Μεγάλη Βρετανία)-1

- Η βρετανική εταιρεία Argos πραγματοποιεί πωλήσεις μέσω Internet, αλλά ένα τραγικό λάθος των προγραμματιστών της, έφερε μια τηλεόραση των 299,99 λιρών Αγγλίας (περίπου 450 ευρώ) να φαίνεται ότι πωλείται προς 3 λίρες Αγγλίας (περίπου 4,5 ευρώ).
- Το πρόβλημα ήταν ότι κατά τη δημιουργία της σχετικής ιστοσελίδας έγινε στρογγυλοποίηση του ποσού στον πλησιέστερο ακέραιο αριθμό και μετά αποκοπή των 2 μηδενικών από την ακέραια ποσότητα.
- Μέχρι να αντιληφθούν οι υπεύθυνοι της εταιρείας το τραγικό λάθος, είχαν ήδη γίνει εκατοντάδες παραγγελίες συνολικής αξίας πάνω από 1,5 εκατομμύριο ευρώ.
- Η εταιρεία αποφάσισε να μην ικανοποιήσει τις παραγγελίες των πελατών της και ισχυρίσθηκε ότι δεν είχε καταρτισθεί σύμβαση μεταξύ της εταιρείας και των πελατών της, εφόσον η εταιρεία δεν επιβεβαίωσε τις παραγγελίες.

Η Περίπτωση της Εταιρείας Argos (Μεγάλη Βρετανία)-2

- Δικηγόροι που εξέτασαν τις ιστοσελίδες της εταιρείας στο Διαδίκτυο ανέφεραν ότι δεν υπήρχε κάποια σημείωση από την εταιρεία ότι δεν φέρει ευθύνη για τυχόν λάθη αναγραφής στις τιμές των προϊόντων της.
- Ένας άλλος δικηγόρος ισχυρίζεται ότι αν μια εταιρεία αποδεχθεί ηλεκτρονικά μια πώληση ενός προϊόντος της, τότε μπορεί να θεωρηθεί ότι υπάρχει σύμβαση ανάμεσα στην εταιρεία (πωλητής) και τον καταναλωτή (αγοραστής).
- Ο πελάτης (χρήστης του Internet) που καταχώρησε στην ιστοσελίδα της Argos τον αριθμό της πιστωτικής του κάρτας και έλαβε έναν μοναδικό κωδικό παραγγελίας ως επιβεβαίωση, μπορεί να θεωρηθεί ότι έχει συνάψει σύμβαση με την εταιρεία για την πώληση του προϊόντος.

Η Περίπτωση της Εταιρείας Argos (Μεγάλη Βρετανία)-3

- Υπάρχει βέβαια και η περίπτωση, αν η υπόθεση φθάσει στα δικαστήρια, να θεωρηθεί άκυρη η σύμβαση πώλησης αν το δικαστήριο αναγνωρίσει ότι έχει γίνει πράγματι λάθος που δεν ήταν εσκεμμένο.
- Στην περίπτωση αυτή θα πρέπει η εταιρεία να αποδείξει ότι έλαβε όλα τα απαραίτητα μέτρα προφύλαξης για να αποφύγει την παραπλάνηση του καταναλωτή.

Συμπεράσματα

Συμπεράσματα-1

- Η Τεχνολογία προχωράει πιο γρήγορα από το Δίκαιο.
- Το Δίκαιο αρέσκεται να βρίσκεται σε σταθερό περιβάλλον. Κάθε απότομη αλλαγή στις κοινωνικές, οικονομικές, πολιτισμικές ή τεχνολογικές συνθήκες, οι οποίες προκαλούν αναταράξεις στο περιβάλλον αυτό, θέτει το δίκαιο σε έκδηλη αμηχανία.

Συμπεράσματα-2

- Το τέλειο έγκλημα δεν μπορεί να γίνει πουθενά, ούτε και στο Διαδίκτυο. Τα ηλεκτρονικά αποτυπώματα (ψηφιακά ίχνη) που αφήνουν οι δράστες καθώς περιηγούνται στο Internet αποτελούν και την επικήρυξή τους. Από εκεί αρχίζει η εξιχνίαση που οδηγεί τελικά στην σύλληψή τους.

Συμπεράσματα-3

- Όποιος χρησιμοποιεί το Internet, θα πρέπει να γνωρίζει ότι μπορεί ένας άλλος χρήστης να εισέλθει στον υπολογιστή του και να αντιγράψει όλα τα αρχεία του ή να κάνει όποια ζημιά αυτός θέλει.
- Στο Internet έχουν χαθεί οι έννοιες του προσωπικού και του ιδιωτικού και ο παγκόσμιος εγκληματίας έχει εγκατασταθεί στα καλώδια του υπολογιστή που έχουμε στο σπίτι μας.
- Από τη στιγμή που κανείς δεν είναι σε θέση να ελέγξει το περιεχόμενό του, το Internet αποτελεί τον Παράδεισο της παρανομίας, της φάρσας και της απάτης.

Συμπεράσματα-4

- Κανείς δεν μπορεί να γλιτώσει τα προσωπικά δεδομένα του, όσο κι αν προσπαθήσει, από τη στιγμή που θα αποφασίσει να συνδεθεί και να περιπλανηθεί (σερφάρει) στο Internet. Σκοπός της παρακολούθησης και της καταγραφής των προσωπικών μας δεδομένων είναι η σκιαγράφηση του καταναλωτικού μας προφίλ.
- Αυτά τα στοιχεία μπορούν να χρησιμοποιηθούν και από τις διωκτικές αρχές για τον εντοπισμό των κακοποιών που παρανομούν στο Internet ή επικοινωνούν μέσω του Internet.

Συμπεράσματα-5

- Το ηλεκτρονικό έγκλημα, δηλ. το έγκλημα που γίνεται με τη βοήθεια των υπολογιστών και κυρίως μέσω του Διαδικτύου (Internet), οργανώνεται και εξαπλώνεται ολοένα και περισσότερο καθώς οι ηλεκτρονικοί εγκληματίες βρίσκουν πρόσφορο έδαφος στο Διαδίκτυο.
- Το Διαδίκτυο τούς δίνει τη δυνατότητα να δρουν αποτελεσματικά και να κρύβονται εύκολα.