



Χρήστου Γεώργιος

Τίτλος πτυχιακής εργασίας

Περιήγηση στο διαδίκτυο:

Ελευθερία επικοινωνίας ή

Πεδίο παραβατικής δράσης

ΕΙΣΗΓΗΤΡΙΑ: ΑΛΕΞΑΝΔΡΑ ΣΤΡΑΤΗ-BANTZOY



*Η Υπάρχουσα Νομοθεσία για
Θέματα Τηλεπικοινωνιών,
Πληροφορικής και Internet*

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

- ✦ Ιδρύθηκε με τους N.2246/1994 και N.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 **N.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 **N.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 **N.2774/1999** αναφέρεται στην «Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Τηλεπικοινωνιακό Τομέα».

Οδηγία για το Ηλεκτρονικό Εμπόριο

- ✦ Το ΠΔ.131/2003 αποτελεί την «Οδηγία 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 **N.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

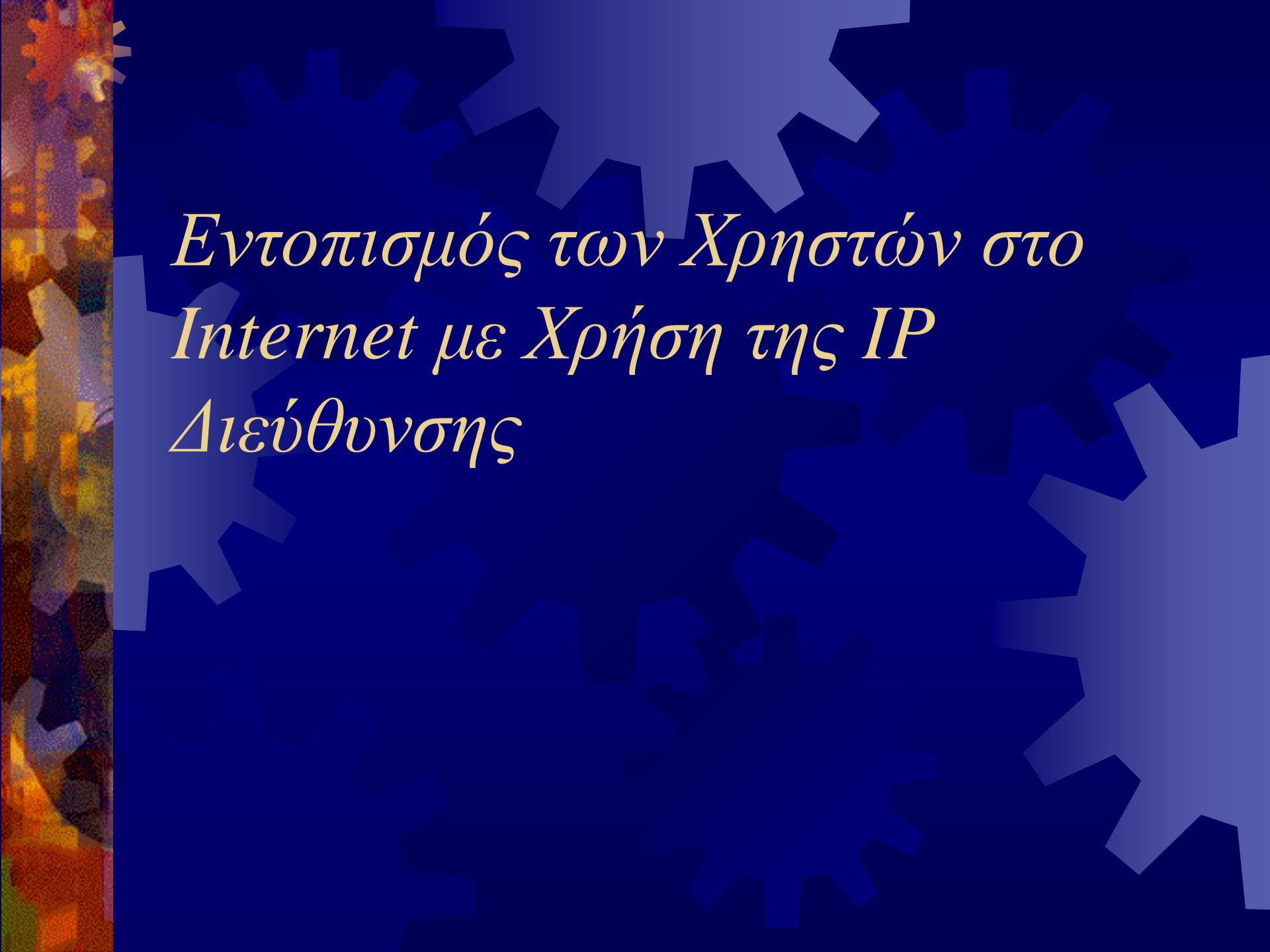
- ☀ Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα <http://www.dpa.gr> (Data Protection Authority) λειτουργεί σύμφωνα με τις διατάξεις του N.2472/1997 (άρθρα 15–20) με αποστολή την εποπτεία της τήρησης του προσωπικού απορρήτου και στο Διαδίκτυο, όπως ορίζεται και από τον μεταγενέστερο N.2774/1999 για 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 (ΟΤΕ, 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.

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.



*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 καταγράψει την σεξουαλική της συμπεριφορά. Η Αστυνομία της Κύπρου συνέλαβε τον δράστη με την κατηγορία της σεξουαλικής

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 δημιουργήσει 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.

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.

Ta 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.

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 χαρακτηριστεί 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*.

Ο Κυβερνοσφετερισμός (Cybersquatting)

- ✦ Πρόκειται για ένα φαινόμενο του Internet, όπου διάφοροι επιτήδριοι, 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 αώτερο στόχο να τα πωλήσουν (μεταβιβάσουν) στους νόμιμους ιδιοκτήτες τους όταν αυτοί θελήσουν αργότερα να δραστηριοποιηθούν στο Internet.
- ✦ Υπήρξαν περιπτώσεις όπου μεγάλες και επώνυμες εταιρείες αναγκάστηκαν 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).



Το Ηλεκτρονικό Έγκλημα

Οι Συνήθειες Μορφές του Ηλεκτρονικού Εγκλήματος

- ✱ Συκοφαντική δυσφήμιση 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 μάλιστα 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 ισχυρίστηκε 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 εντοπίστηκαν εκπαιδευτικοί και δικηγόροι.



*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 σωματίου 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.



Ηλεκτρονικές Απάτες

Η Απάτη των Dialer

- ☀ Η απάτη λειτουργεί ως εξής : Μια ιστοσελίδα δαλεάζει 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.

Απάτες με το *e-mail*

- ✿ Διάφοροι επιτήδαιοι 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 της τίτλο.



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 τους δίνει τη δυνατότητα να δρουν αποτελεσματικά και να κρύβονται εύκολα.



ΤΕΛΟΣ