ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΨΥΧΟΛΟΓΙΑΣ – ΤΟΜΕΑΣ ΚΟΙΝΩΝΙΚΗΣ ΘΕΩΡΙΑΣ & ΕΡΕΥΝΑΣ
ΚΕΝΤΡΟ ΨΥΧΟ-ΚΟΙΝΩΝΙΟΛΟΓΙΚΗΣ ΕΡΕΥΝΑΣ ΤΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΤΩΝ ΔΥΝΗΤΙΚΩΝ ΚΟΙΝΟΤΗΤΩΝ – ΕΡΕΥΝΗΤΙΚΟ ΚΕΝΤΡΟ «ΩΜΕΓΑ»

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

ΔΥΝΗΤΙΚΕΣ ΚΟΙΝΟΤΗΤΕΣ: ΚΟΙΝΩΝΙΟ-ΨΥΧΟΛΟΓΙΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ ΚΑΙ ΤΕΧΝΙΚΕΣ ΕΦΑΡΜΟΓΕΣ

ΣΕ ΣΥΜΠΡΑΞΗ ΜΕ ΤΟ
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΑ
Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ

ΚΑΙ ΣΕ ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΟ
ΕΡΕΥΝΗΤΙΚΟ ΑΚΑΔΗΜΑΪΚΟ ΙΝΣΤΙΤΟΥΤΟ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ

29 ΜΑΪΟΣ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΗΛΕΚΤΡΟΝΙΚΟ ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ: Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

ΒΟΛΗ ΜΑΡΓΑΡΙΤΑ
Α.Μ.: **6305ΜΟΟ2**

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:

1. Αναπλ. Καθ. Σ. Συρμακέσης, Επιβλέπων

2. Αναπλ. Καθ. Κ. Κοσκινάς, Μέλος

3. Δρ. Α. Γιαννακουλόπουλος, Μέλος

Μαϊος, 2009

ΠΕΡΙΛΗΨΗ

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του Διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα».Ποια είναι όμως ακριβώς τα ψηφιακά εγκλήματα, που καταστρέφουν την καλή εικόνα της ψηφιακής κοινωνίας και του Internet; Ποιοι τα διαπράττουν και με ποιους τρόπους; Μπορούν να αντιμετωπισθούν και πώς; Πως ερμηνεύεται θεωρητικά η ψηφιακή εγκληματικότητα;

Η Νιγηριανή απάτη είναι μηνύματα ηλεκτρονικού ταχυδρομείου με περιεχόμενο πλασματικές ιστορίες, μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη. Η κεντρική αρχή στις περισσότερες απάτες (και φυσικά και στις απάτες με όχημα το Διαδίκτυο) είναι να πειστεί το υποψήφιο θύμα ότι καταβάλλοντας ένα μικρό ποσό εξασφαλίζει ένα άλλο πολύ μεγαλύτερο, χωρίς να κάνει απολύτως τίποτα . Οι περισσότεροι άνθρωποι είναι, φυσικά, σκεπτικοί απέναντι σε τέτοιου είδους προσεγγίσεις. Υπάρχουν όμως και εκείνοι που κινούμενοι από απληστία, ανάγκη, ή άγνοια μετατρέπονται σε εύκολα θύματα κακοποιών χάνοντας αρκετά χρήματα.

ΛΕΞΕΙΣ – ΚΛΕΙΔΙΑ

Έγκλημα, Οικονομικό Έγκλημα, Ηλεκτρονικό Έγκλημα, Νιγηριανή Απάτη

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

4ο ΚΕΦΑΛΑΙΟ

5ο ΚΕΦΑΛΑΙΟ

6ο ΚΕΦΑΛΑΙΟ

7ο ΚΕΦΑΛΑΙΟ

8ο ΚΕΦΑΛΑΙΟ

9ο ΚΕΦΑΛΑΙΟ

10^{Ο} ΚΕΦΑΛΑΙΟ

Β΄ ΜΕΡΟΣ : Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

11^{Ο} ΚΕΦΑΛΑΙΟ

12^{Ο} ΚΕΦΑΛΑΙΟ

13^{Ο} ΚΕΦΑΛΑΙΟ

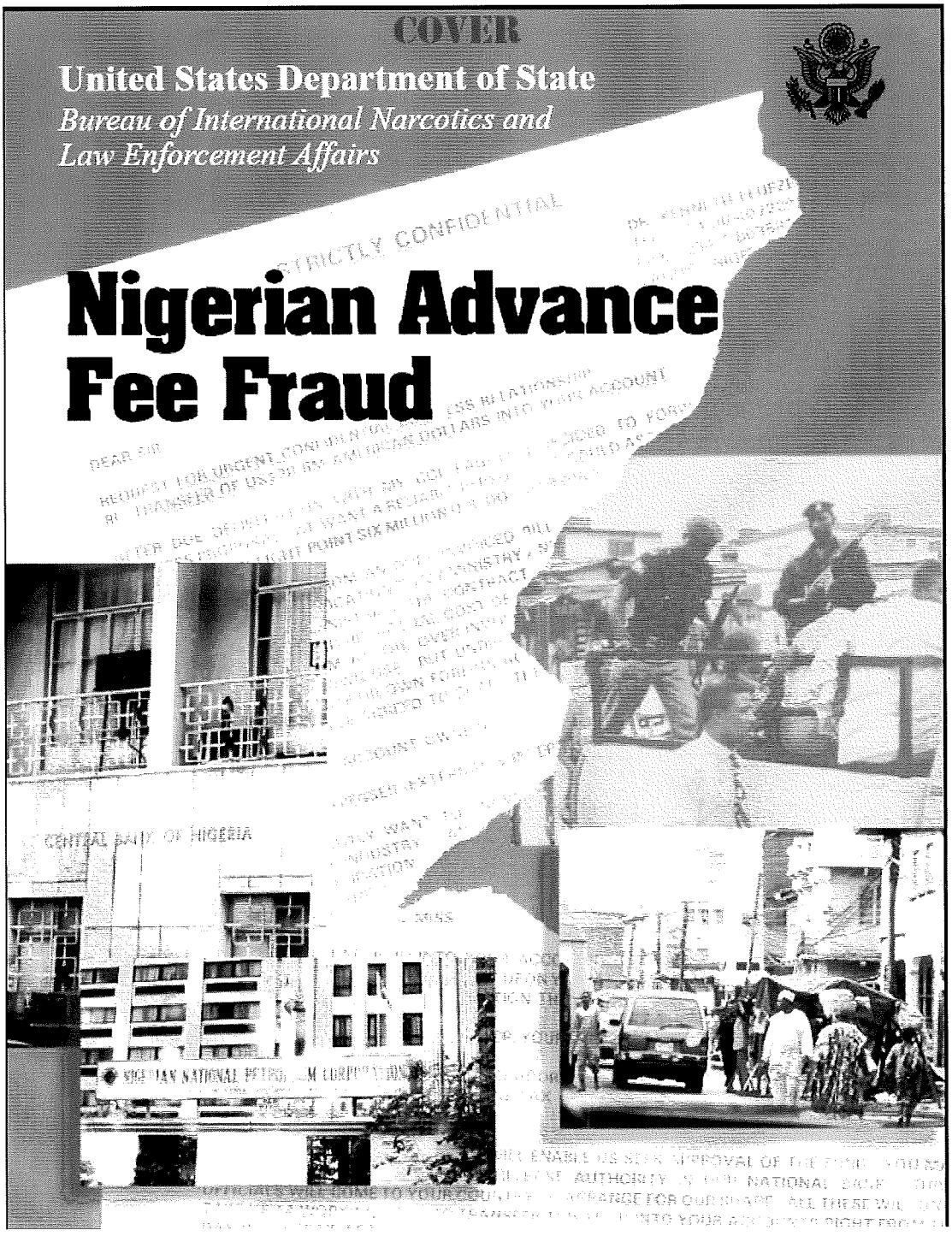
14^{Ο} ΚΕΦΑΛΑΙΟ

15^{Ο} ΚΕΦΑΛΑΙΟ

16^{Ο} ΚΕΦΑΛΑΙΟ

ΠΙΝΑΚΑΣ ΠΙΝΑΚΩΝ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ


COVER
United States Department of State
Bureau of International Narcotics and
Law Enforcement Affairs
Nigerian Advance
Fee Fraud

ΠΡΟΛΟΓΟΣ

Στον ψηφιακό μας κόσμο, που γεννήθηκε και αναπτύχθηκε στο τελευταίο τέταρτο του 20ου αιώνα, ανήκουν οι σημερινές τεχνολογικά εξελιγμένες κοινωνίες, που θα πρέπει να τις χαρακτηρίσουμε και αυτές ψηφιακές. Σκοπός της παρούσας εργασίας είναι να αποσαφηνίσουμε την έννοια της ηλεκτρονικής εγκληματικότητας.

Καθώς η παρουσία των υπολογιστών και των διαφόρων ψηφιακών συστημάτων είναι εμφανής σε όλους τους τομείς της καθημερινής ζωής των πολιτών - τόσο της ιδιωτικής όσο και της δημόσιας – μπορούμε να συμπεράνουμε πως η μη σωστή λειτουργία των συστημάτων αυτών και κατά κύριο λόγο του διαδικτύου και η συνεπακόλουθη διαστρέβλωση ή ακόμα και η καταστροφή των πληροφοριών, που διαχειρίζονται δημιουργεί μια ανασφάλεια, απόρροια της οποίας είναι σοβαρότατα προβλήματα στις ψηφιακές κοινωνίες που εξαρτώνται από αυτά.

Και ποια είναι αυτά τα προβλήματα; Ποιοι τα προκαλούν; Ποιες είναι οι μορφές τους; Ποιες είναι οι επιπτώσεις τους; Ποιοι είναι οι τρόποι αντιμετώπισής τους; Αυτά είναι τα θέματα με τα οποία θα ασχοληθούμε, τα οποία ανήκουν στην έννοια της ηλεκτρονικής εγκληματικότητας.

Ποια είναι όμως ακριβώς τα ψηφιακά εγκλήματα, που καταστρέφουν την καλή εικόνα της *ψηφιακής κοινωνίας* και του Internet; Ποιοι τα διαπράττουν και με ποιους τρόπους; Μπορούν να αντιμετωπισθούν και πώς; Πως ερμηνεύεται θεωρητικά η ψηφιακή εγκληματικότητα;

Στο πρώτο μέρος της εργασίας θα ασχοληθούμε πιο θεωρητικά με την ανάλυση της ηλεκτρονικής εγκληματικότητας. Θα αναλύσουμε όλες τις έννοιες, και θα προσπαθήσουμε να δώσουμε όλους τους απαραίτητους ορισμούς. Θα ξεκινήσουμε κάνοντας μια ιστορική αναδρομή στο έγκλημα, θα μιλήσουμε για το οικονομικό και το ηλεκτρονικό έγκλημα. Στη συνέχεια θα αναλύσουμε τα χαρακτηριστικά του ηλεκτρονικού εγκλήματος, θα σκιαγραφήσουμε τους δράστες και θα κατηγοριοποιήσουμε αυτά τα εγκλήματα. Θα προχωρήσουμε στα ηλεκτρονικά οικονομικά εγκλήματα, στην μέτρηση της ηλεκτρονικής εγκληματικότητας και θα ολοκληρωθεί το πρώτο μέρος με την αστυνομία και την νομοθεσία απέναντι στο ηλεκτρονικό έγκλημα.

Στο δεύτερο μέρος της εργασίας θα ασχοληθούμε αναλυτικά με την περίπτωση της νιγηριανής απάτης. Είναι μια απάτη κατά την οποία το υποψήφιο θύμα λαμβάνει ένα e-mail με το οποίο ο απατεώνας τού υπόσχεται μεγάλη χρηματική αμοιβή αν τον βοηθήσει να μεταφέρει χρήματα από τον τραπεζικό του λογαριασμό στο λογαριασμό του θύματος. Οι λόγοι τους οποίους επικαλείται ο απατεώνας για τη μεταφορά αυτή ποικίλλουν κατά περίπτωση, συνήθως όμως αφορούν γνωστούς διπλωμάτες, επιχειρηματίες ή γόνους πλουσίων οικογενειών που θα πρέπει να εγκαταλείψουν τη χώρα τους εξαιτίας πολιτικών συγκρούσεων. Προτού όμως το θύμα εισπράξει το χρηματικό ποσό που του υποσχέθηκε ο απατεώνας, θα πρέπει να καταβάλει ορισμένα χρήματα για τα έξοδα μεταφοράς ή να δώσει για το λόγο αυτό τα στοιχεία του τραπεζικού του λογαριασμού. Εννοείται ότι στην πρώτη περίπτωση αμέσως μετά την αποστολή των χρημάτων θα διακοπεί η επικοινωνία με τον απατεώνα, ενώ στη δεύτερη το θύμα είναι πολύ πιθανό να χάσει όλα τα χρήματα του τραπεζικού του λογαριασμού. Φυσικά υπάρχει και το ενδεχόμενο με τον τρόπο αυτό ο

απατεώνας έχοντας στη διάθεσή του τα στοιχεία της ταυτότητας του θύματος να το χρεώσει στη συνέχεια, με μεγάλα χρηματικά ποσά.

Αφού ορίσουμε τι είναι η νιγηριανή απάτη, θα προχωρήσουμε στην περιγραφή της και στην ανάλυση των φάσεων και των τύπων της. Έπειτα θα αναφερθούμε στους δράστες, στα θύματα και τα μέσα αυτής της απάτης. Παρουσιάζουμε ένα παράδειγμα νιγηριανής επιστολής, κάποια στατιστικά στοιχεία και τέλος μέτρα προστασίας από τέτοιου είδους απάτες.

Α΄ ΜΕΡΟΣ

ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ

-

ΟΡΙΣΜΟΙ

-

ΑΣΤΥΝΟΜΙΑ

-

ΝΟΜΟΘΕΣΙΑ

1ο ΚΕΦΑΛΑΙΟ

ΕΓΚΛΗΜΑ

ΕΙΣΑΓΩΓΗ 1ΟΥ ΚΕΦΑΛΑΙΟΥ:

Σε αυτό το κεφάλαιο θα γίνει μια σύντομη ανάλυση της έννοιας του εγκλήματος και των χαρακτηριστικών του. Φυσικά θα γίνει μια ιστορική αναδρομή. Τέλος θα γίνει μια αναφορά στην σημερινή εποχή σε σχέση με το έγκλημα και τι κατάσταση επικρατεί στην χώρα μας, την Ελλάδα.

1.1 ΤΙ ΕΙΝΑΙ ΕΓΚΛΗΜΑ;

Έγκλημα είναι κάθε πράξη, που προσβάλλει βαριά την κοινή συνείδηση και γι΄ αυτό αυτή αντιδρά έντονα. Σύμφωνα με τον Durkheim (Φαρσεδάκης, 1996) τα εγκλήματα συνίστανται σε πράξεις, που αποδοκιμάζονται καθολικά από τα μέλη κάθε κοινωνίας.

Επίσης πρέπει να αναφέρουμε πως σύμφωνα με τον Garofalo (Φαρσεδάκης, 1996) έγκλημα διαπράττει εκείνος, που παραβαίνει τα στοιχειώδη αισθήματα φιλαλληλίας – και συγκεκριμένα του οίκτου και της εντιμότητας – μιας συγκεκριμένης κοινωνίας μιας ορισμένης εποχής, τα απαραίτητα για την κοινωνική συμβίωση (κατά τις αντιλήψεις αυτής της κοινωνίας) .

1.2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΓΙΑ ΤΟ ΕΓΚΛΗΜΑ

Το έγκλημα αποτελεί αναπόσπαστο κομμάτι οποιασδήποτε οργανωμένης κοινωνίας. Ανεξάρτητα από τον τόπο και το χρόνο, ορισμένοι άνθρωποι παραβαίνουν τους κοινωνικούς κανόνες με αποτέλεσμα να επιβάλλονται σε αυτούς διάφορες κυρώσεις. Το είδος της αντίδρασης της κοινωνίας, όπως και το είδος της ποινής που θα επιβληθεί σε αυτόν που παρέβη έναν κανόνα, εξαρτώνται από την εποχή και τον πολιτισμό.

Πράγματι, κανένα εθνικό χαρακτηριστικό, πολιτικό, κοινωνικοοικονομικό ή νομικό σύστημα, τιμωρία ή μεταχείριση δεν απήλλαξαν ποτέ μια χώρα από το έγκλημα. Απεναντίας, παρατηρείται μια συνεχής τάση αύξησής του και ταυτόχρονα η εμφάνιση νέων μορφών και η αποποινικοποίηση υφιστάμενων εγκλημάτων.

Σύμφωνα με τον Φαρσεδάκη (Φαρσεδάκης, 1996) τρία είναι τα βασικά στοιχεία που συνθέτουν το εγκληματικό φαινόμενο: α) Ο κανόνας (ποινικός νόμος) β) η παράβαση (έγκλημα) και γ) η κύρωση (ποινή).

α) Ο κανόνας: Ο κανόνας αποτελεί την έκφραση της κοινωνίας έναντι κάποιας συμπεριφοράς. Αν ο κανόνας προβλέπει και την επιβολή ποινών, τότε πρόκειται για ποινικό νόμο. Οι ποινικοί νόμοι δεν είναι σταθεροί, αλλά αλλάζουν με το πέρασμα του χρόνου. Εξαρτώνται από πολλούς παράγοντες όπως κοινωνικούς, ηθικούς, πολιτιστικούς, οικονομικούς κ.ά.

β) Το έγκλημα: Το έγκλημα είναι κάτι το αναμενόμενο και φυσικό μέσα σε μια κοινωνία. Θα ήταν αδύνατο όλα τα μέλη μιας κοινωνίας να συμμορφώνονται με τους ίδιους κανόνες, καθώς είναι αδύνατο να έχουν την ίδια δομή προσωπικότητας, την ίδια κοινωνική και οικονομική κατάσταση και να έχουν κοινωνικοποιηθεί με τον ίδιο τρόπο.

γ) Η κύρωση: Η κύρωση αποτελεί τη συνέπεια της παράβασης του κανόνα και δηλώνει ότι η συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή από την κοινωνία. Ως προς την αιτιολογία της επιβολής της ποινής έχουν κατά καιρούς διατυπωθεί διάφορες θεωρίες. Οι επικρατέστερες είναι της ανταπόδοσης και της κοινωνικής άμυνας. Στην περίπτωση της ανταπόδοσης, η επιβολή της ποινής σκοπεύει στην επανόρθωση των επιβλαβών για την κοινωνία συνεπειών του εγκλήματος, με την πληρωμή του κακού που έγινε με άλλο ισάξιο. Στην περίπτωση της άμυνας, η ποινή έχει ως σκοπό, να αποτρέψει κάποιον να εγκληματήσει είτε με τον εκφοβισμό, είτε με τη γενικότερη καλλιέργεια της ιδέας της αποστροφής προς την αδικία.

Εκτός όμως από αναπόφευκτο, το έγκλημα στα πλαίσια μιας κοινωνικής οργάνωσης, όσο και αν έχει ταυτιστεί με κάτι αρνητικό, είναι και χρήσιμο, είτε έμμεσα, είτε άμεσα. Έμμεσα, υπό την έννοια, ότι αποτελεί προϋπόθεση για κάθε ηθική και νομική αλλαγή, η οποία είναι απαραίτητη για να μην περιέλθει η κοινωνία σε πλήρη αγκύλωση. Άμεσα, υπό την έννοια, ότι αποτελεί την πρόγευση της μέλλουσας ηθικής. Για παράδειγμα, η ελευθερία σκέψης και έκφρασης που απολαμβάνουμε σήμερα δεν θα είχε επιτευχθεί ποτέ, αν κάποιοι δεν παραβίαζαν τους κανόνες που κάποτε την περιόριζαν!

1.3. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ

Τα κύρια χαρακτηριστικά του εγκλήματος σύμφωνα με τον Φαρσεδάκη (Φαρσεδάκης, 1996) είναι:

- Η παγκοσμιότητα: Όσο και αν οι μορφές, η έκταση και το είδος της αντίδρασης της πολιτείας έναντι συγκεκριμένης συμπεριφοράς ποικίλλουν ανά χώρα ενδεχομένως και ανά συγκεκριμένη γεωγραφική περιοχή, το κοινωνικό αυτό φαινόμενο είναι κοινό παντού. Κοινωνία χωρίς έγκλημα δεν υπάρχει.

- Η διαχρονικότητα: Η ιστορική έρευνα έχει αποδείξει ότι εο εγκληματικό φαινόμενο υπήρξε σε όλες τις κοινωνίες, χωρίς καμιά εξαίρεση. Μπορεί να υπήρξαν διαφοροποιήσεις ως προς το περιεχόμενο των νόμων και τα επιμέρους χαρακτηριστικά των παραβάσεων και των παραβατών, όμως πάντοτε υπήρξε παραβίαση κανόνων και επιβολή κυρώσεων.

- Η αλληλεξάρτηση των στοιχείων του εγκληματικού φαινομένου: Τα τρία βασικά στοιχεία του εγκληματικού φαινομένου, δηλαδή ο κανόνας, το έγκλημα και η κύρωση αποτελούν έναν κύκλο, ο οποίος δεν μπορεί να διασπαστεί. Κανένα από τα τρία αυτά στοιχεία δεν μπορεί να υπάρξει χωρίς το άλλο. Δεν θα υπήρχε έγκλημα, αν δεν υπήρχε κανόνας συμπεριφοράς, για να τον παραβεί κάποιος. Η κοινωνικά αντίδραση θα ήταν ανύπαρκτη χωρίς έγκλημα και εγκληματία.

- Η δυσχέρεια ορισμού του εγκλήματος: Όπως ήδη προαναφέρθηκε, το έγκλημα είναι αναπόσπαστο κομμάτι κάθε κοινωνίας, παράλληλα όμως χρησιμοποιεί διαφορετικούς κανόνες ανάλογα με το συγκεκριμένο πολιτικό, κοινωνικό, ηθικό

κ.λπ. καθεστώς που επικρατεί σε κάθε οργανωμένο σύνολο ανθρώπων. Το γεγονός αυτό δυσχεραίνει τον ορισμό και προσδιορισμό του, καθότι τόσο αυτή η διαφοροποίηση όσο και η συνεχής μετεξέλιξη των κοινωνιών καθιστά πολλές φορές δυσδιάκριτο το τι αποτελεί έγκλημα και τι όχι.

1.4 ΤΟ ΕΓΚΛΗΜΑ ΣΤΗΝ ΣΗΜΕΡΙΝΗ ΕΠΟΧΗ

Είναι σε όλους γνωστό ότι το έγκλημα είναι ένα κοινωνικό φαινόμενο που δεν έλειψε ποτέ από τη ζωή του ανθρώπου. Απεναντίας, παρακολουθεί τις κοινωνικές και τις τεχνολογικές εξελίξεις, αναπροσαρμόζεται συνεχώς, με αποτέλεσμα σε κάθε εποχή να παρουσιάζεται με διαφορετική μορφή και ένταση, και διεθνώς, και στη χώρα μας. Το σύνολο δε των διαπραττομένων εγκλημάτων σε συγκεκριμένη περίοδο, σε ορισμένο χώρο, αποτελεί την εγκληματικότητα, η οποία στην εποχή μας οξύνεται υπερβολικά και αποκτά ιδιαίτερη ποικιλομορφία και ένταση, με την εμφάνιση πρωτόγνωρων εγκλημάτων νέας μορφής και την τάση παγίωσης του οργανωμένου εγκλήματος.

Στο σημείο αυτό θα πρέπει να τονιστεί ιδιαίτερα, ότι τα κίνητρα και ο τρόπος τελέσεως των εγκλημάτων της τελευταίας εικοσαετίας, διαφέρουν ουσιωδώς από εκείνα των παλαιοτέρων εποχών. Αυτό βέβαια δεν σημαίνει ότι παύει να υπάρχει το έγκλημα για λόγους ερωτικής αντιζηλίας, για λόγους τιμής, κοινωνικής ντροπής ή για ένα μέτρο γης.

Παράλληλα όμως εμφανίστηκαν και εγκλήματα που τα κίνητρά τους απορρέουν από τις σημαντικές αλλαγές που έφεραν στην ελληνική κοινωνία, η είσοδος και παραμονή λαθρομεταναστών στη χώρα μας και η μεταβιομηχανική πυρηνική εποχή που διανύουμε σε συνδυασμό με την τεχνολογική επανάσταση.

Ειδικότερα, σημαντικό ρόλο έπαιξαν, ο υδροκεφαλισμός των αστικών κέντρων, ο τουρισμός, η κατάργηση των εσωτερικών συνόρων της Ευρωπαϊκής Ένωσης από τα κράτη μέλη της, η διάδοση της εμπορίας και χρήσεως σκληρών πια ναρκωτικών, ο νέος υπερκαταναλωτικός τρόπος ζωής και βέβαια η ευρύτερη αποδοχή της τάσης του εύκολου πλουτισμού, σε μία κοινωνία που κυριαρχείται από τη σύγκρουση συμφερόντων και τη βία ως μέσο επίλυσης των διαφορών, λόγω χαλάρωσης του πνεύματος αλληλεγγύης μεταξύ των πολιτών και εξασθένησης των κοινωνικοποιητικών αξιών που στηρίζονται στο πνεύμα αυτό και συγκρατούν από την τέλεση εγκλημάτων.

Στα «μοντέρνα» αυτά εγκλήματα και σε εκείνα που εμφανίστηκαν παράλληλα με αυτά, της αεροπειρατείας, της ομηρίας προσώπων και της τρομοκρατίας, ο δράστης παρουσιάζεται πιο ψυχρός στη διάπραξή τους, διαθέτει άριστη τεχνογνωσία, χρησιμοποιεί μέσα σύγχρονης τεχνολογίας και οπλισμού, νέες εγκληματικές μεθόδους άγνωστες στη χώρα μας, είναι προσεκτικότερος στο σχεδιασμό του. Κινείται αιφνιδιαστικά και με ταχύτητα, μεγαλύτερη από αυτή της Αστυνομίας, μελετά με λεπτομέρεια το χώρο όπου θα κινηθεί, έχει εξασφαλίσει κατά μεγαλύτερο ποσοστό τη διαφυγή και την απόκρυψή του, καταβάλλει ιδιαίτερη επιμέλεια να μην εγκαταλείψει πίσω του ίχνη, αποπροσανατολίζει την έρευνα και δημιουργεί ισχυρό «άλλοθι». Με άλλα λόγια γίνεται «επαγγελματίας».

1.5 Η ΕΛΛΗΝΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ

Στην Ελλάδα του σήμερα η εγκληματικότητα παρουσιάζει τάση αυξητική σε σύγκριση με άλλες εποχές.

Τα τελούμενα εγκλήματα αποτελούν παραβάσεις τόσο του κοινού Ποινικού Δικαίου (πταίσματα, πλημμελήματα, κακουργήματα), όσο και των λοιπών ειδικών ποινικών νόμων που ισχύουν και τα οποία αποτελούν τον συνήθη όγκο της βεβαιωμένης ελαφράς εγκληματικότητας δευτερεύουσας σημασίας, από απόψεως ποινικής βαρύτητας (π.χ. παραβάσεις δασικού κώδικα, οικοδομικού κανονισμού, αγορανομικού κώδικα, ασφαλιστικών εισφορών, τροχονομικές, αστυϊατρικές κ.λ.π.).

Αν κανείς μελετήσει τα στοιχεία όσον αφορά τα εγκλήματα της τελευταίας πενταετίας που περιήλθαν σε γνώση των Υπηρεσιών του Υπουργείου Δημόσιας Τάξης και τα συγκρίνει με αυτά της περιόδου του 1980 και μετά, εύκολα θα συμπεράνει ότι η βαριά εγκληματικότητα (εκφράζεται με τα κακουργήματα), παρουσιάζει έντονη ανοδική πορεία, ποσοτική και ποιοτική, σε σχέση με την ελαφρά, η οποία παρουσιάζει μεν και αυτή αύξηση, αλλά αυτή είναι μικρότερης κλίμακας και αφανέστερη, ως προς την συνολική της έκταση.

Ειδικότερα κατακόρυφη αύξηση παρουσιάζει το κακούργημα της ληστείας, τα εγκλήματα βίας (ανθρωποκτονίες, σωματικές βλάβες, αυτοδικίες) και αυτά που στρέφονται κατά της περιουσίας (κλοπές, απάτες, διαρρήξεις κ.λ.π). Σε αλματώδη άνοδο επίσης βρίσκονται τα εγκλήματα, γύρω από το όλο φαινόμενο της λαθρομετανάστευσης, της σεξουαλικής εκμετάλλευσης γυναικών και τα οικονομικά εγκλήματα με έμφαση τα ηλεκτρονικά. Ορισμένα από τα εγκλήματα αυτά (παράνομη διακίνηση λαθρομεταναστών, δουλεμπόριο, απάτη μέσω πιστωτικών καρτών κ.λ.π.) είναι πρωτόγνωρα για την ελληνική κοινωνία. Όσον αφορά τη χρήση και διακίνηση ναρκωτικών ουσιών και των συναφών εγκλημάτων που σχετίζονται έμμεσα με αυτά (διαρρήξεις φαρμακείων ή ληστείες προς απόκτηση της αναγκαίας δόσης ναρκωτικού), η αύξηση είναι τρομακτική.

Εκείνο όμως που πρέπει να εμβάλλει τους πάντες σε ανησυχία είναι το γεγονός που παρατηρείται τα τελευταία χρόνια στην Ελλάδα, μιας ευρύτερης μετεξέλιξης και ποιοτικής αναβάθμισης της εγκληματικότητα ς προς την κατεύθυνση του οικονομικού εγκλήματος και του οργανωμένου εγκλήματος.

Τα εγκλήματα αυτά, λόγω του διεθνικού-διακρατικού τους χαρακτήρα, απειλούν την οικονομία και την εθνική ασφάλεια, τόσο σε επίπεδο εθνικό όσο και σε παγκόσμιο.

1.6 ΣΥΜΠΕΡΑΣΜΑΤΑ 1^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Το έγκλημα είναι κάτι το φυσιολογικά αναμενόμενο σε μια κοινωνία. Είναι πρώτα πρώτα αναπόφευκτο ή αναγκαίο, εξαιτίας της διαφοροποίησης των ατομικών συνειδήσεων. Επίσης το έγκλημα είναι χρήσιμο, γιατί ο ατομισμός από τον οποίο προέρχεται αποτελεί προϋπόθεση αναγκαία για κάθε ηθική και νομική αλλαγή. Οι σκέψεις αυτές δεν αποτελούν απολογία του εγκλήματος μια που σύμφωνα με τον Durkheim (Φαρσεδάκης, 1996) «το γεγονός ότι το έγκλημα είναι ένα κανονικό κοινωνικό φαινόμενο δεν σημαίνει πως δεν πρέπει και να το μισούμε».

Οι εγκληματικές ενέργειες απειλούν την συνοχή και την σταθερότητα μέσα σε μια κοινωνία και καταργούν τις κοινωνικές αξίες. Σύμφωνα με τον ποινικό δίκαιο, έγκλημα είναι κάθε πράξη, που τιμωρείται από τον ποινικό νόμο. Η αξιολόγηση των πράξεων ως εγκληματικές αλλάζουν πάρα πολύ στις διάφορες εποχές και χώρες. Οι μορφές των εγκλημάτων, που είναι πράξεις προσβλητικές των δημόσιων αγαθών και η βαρύτητά τους, αλλάζουν από εποχή σε εποχή. Γι΄ αυτό τον λόγο η κάθε κοινωνία σε κάθε εποχή μέσα από τα επίσημα όργανα άσκησης εξουσίας, θεσπίζει νόμους, που απαγορεύουν, αλλά και τιμωρούν τις εγκληματικές ενέργειες στην προσπάθειά της να διατηρήσει την κοινωνική συνοχή και να προστατέψει τα δικαιώματα των μελών της.

2^{Ο} ΚΕΦΑΛΑΙΟ

ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ

ΕΙΣΑΓΩΓΗ 2^{ΟΥ} ΚΕΦΑΛΑΙΟΥ:

Σε αυτό το κεφάλαιο, θα ορίσουμε λίγο σύντομα τι είναι το οικονομικό έγκλημα και τι κατάσταση επικρατεί σήμερα στην Ελλάδα.

2.1 ΤΙ ΕΙΝΑΙ ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ;

Οικονομικό έγκλημα, με την ευρύτερη του όρου έννοια, είναι αυτό που βλάπτει ή θέτει σε κίνδυνο τη λειτουργία της οικονομίας ή λειτουργικά σημαντικών κλάδων και θεσμών της. Κυριαρχείται από το στοιχείο της απάτης, οι δε εκφραστές του είναι προικισμένοι με ιδιαίτερη και θαυμαστή οξύνοια και χρησιμοποιούν με ευχέρεια την, με ραγδαίους ρυθμούς, εξελισσόμενη ηλεκτρονική (δίκτυα υπολογιστών, Internet) και λοιπή τεχνολογία.

2.2 ΤΑ ΟΙΚΟΝΟΜΙΚΑ ΕΓΚΛΗΜΑΤΑ ΣΗΜΕΡΑ

Μετεξελιγμένη σύγχρονη μορφή του οικονομικού εγκλήματος είναι το Ηλεκτρονικό Έγκλημα, γέννημα της συστηματικής διαδικτύωσης του κόσμου και της κοινωνίας των πληροφοριών σε όλες τις πτυχές της ζωής. Θύματα απάτης υπήρξαν ή μπορεί να υπάρξουν, φυσικά πρόσωπα, εταιρείες, οργανισμοί, τράπεζες, κρατικοί φορείς, αρχεία υπηρεσιών, διεθνείς όμιλοι και τέλος η παγκόσμια οικονομία, μέσω της σταθεροποιήσεως, από το «σπάσιμο» κωδικών από κάποιους άγνωστους ή γνωστούς εισβολείς (χάκερς) των ηλεκτρονικών υπολογιστών και του διαδικτύου. Το συνηθέστερο ηλεκτρονικό έγκλημα που παρουσιάζει εσχάτως έξαρση, είναι η ιδιοποίηση τραπεζικών εμβασμάτων από ιδιώτες μέσω ηλεκτρονικών υπολογιστών και απάτες με τη χρήση πιστωτικών καρτών.

Άλλα οικονομικά εγκλήματα που απασχόλησαν τις δικαστικές αρχές με πάταγο, ήταν:

- Εικονική μεταβίβαση κεφαλαίων από την Ελλάδα σε θυγατρικές εταιρείες του εξωτερικού με σκοπό την φοροδιαφυγή,
- Οικειοποίηση κεφαλαίων από στελέχη τραπεζών ή οργανισμών,
- Είσπραξη επιδοτήσεων της Ευρωπαϊκής Κοινότητας ή του Ελληνικού Δημοσίου και «εικονική» εξαγωγή αγροτικών προϊόντων κ.λ.π.

2.3 ΣΥΜΠΕΡΑΣΜΑΤΑ 2^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Είναι γεγονός αναντίρρητο, ότι το έγκλημα (ουδέποτε έλειψε από τη ζωή του ανθρώπου ως κοινωνικό φαινόμενο), παρακολουθεί τις κοινωνικές και τεχνολογικές εξελίξεις και αναπροσαρμόζεται συνεχώς, με αποτέλεσμα σε κάθε εποχή να παρουσιάζεται με διαφορετική μορφή και ένταση, τόσο διεθνώς, όσο και στη χώρα μας. Συνέπεια δε τούτου είναι, ότι, στη σημερινή μεταβιομηχανική πυρηνική εποχή που διανύουμε, σε συνδυασμό με την τεχνολογική επανάσταση και την «επαγγελματοποίηση» του εγκληματία, να εμφανιστούν πρωτόγνωρα εγκλήματα νέας μορφής μέσα σε μία τάση παγίωσης του οργανωμένου εγκλήματος, όπου κυριαρχεί, μεταξύ άλλων, και το οικονομικό έγκλημα.

Το οικονομικό έγκλημα, ως γνωστόν, λόγω του διεθνικού-διακρατικού χαρακτήρα που το διέπει, είναι δυνατόν να απειλήσει την οικονομία και την εθνική ασφάλεια μιας χώρας, αλλά και σε παγκόσμιο επίπεδο, δεδομένου ότι επιπλέον κυριαρχείται από το στοιχείο της απάτης εκφραζόμενο από οργανωμένα κυκλώματα δραστών, προικισμένων με ιδιαίτερη και θαυμαστή οξύνοια, χρησιμοποιώντας ευχερώς την, με εκρηκτικούς ρυθμούς, εξελισσόμενη, πάσης φύσεως, τεχνολογία, κυρίως την ηλεκτρονική, εξ ου και ο όρος «ηλεκτρονικό-οικονομικό έγκλημα», δηλαδή μια μετεξελιγμένη σύγχρονη μορφή του οικονομικού εγκλήματος.

3^{o} ΚΕΦΑΛΑΙΟ

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

ΕΙΣΑΓΩΓΗ 3^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Σε αυτό το κεφάλαιο θα αναφερθούμε εκτενώς στον ορισμό του ηλεκτρονικού εγκλήματος και θα παραθέσουμε τους διάφορους ορισμούς ειδικών επιστημόνων.
Επίσης θα αναλύσουμε τις διαφορές του ηλεκτρονικού εγκλήματος από τα παραδοσιακά και θα προσπαθήσουμε να απαντήσουμε στην ερώτηση: γιατί είναι τόσο σοβαρά τα ηλεκτρονικά εγκλήματα;

3.1 ΤΟ ΠΕΡΑΣΜΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ:

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του Διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα».

Το έγκλημα, ως αναπόσπαστο κομμάτι κάθε κοινωνίας, έχει τη μορφή ενός ζωντανού οργανισμού. Συνεχώς μεταβάλλονται οι μορφές του, τα μέσα διάπραξής του και η νομοθεσία που το διέπει.

Στις αρχές του 20ου αιώνα, καινούριοι τρόποι-τεχνικές για τη διάπραξη εγκλημάτων έκαναν την εμφάνισή τους. Η βιομηχανική επανάσταση εκσυγχρόνισε τα μέσα τέλεσης του εγκλήματος. Σύμφωνα με τους Goodman and Brenner (Furnell, 2006) το τηλέφωνο άρχισε να χρησιμοποιείται για απάτες και άλλα εγκλήματα, τα μεταφορικά μέσα διευκόλυναν τη διάπραξη κλοπών και ληστειών, ενώ διάφορα άλλα τεχνολογικά επιτεύγματα με τη χρήση και λειτουργία τους, επέφεραν μια αρχική διαφοροποίηση στον τρόπο διάπραξης του εγκλήματος.

Ίσως τότε κανείς δεν μπορούσε να φανταστεί τι θα επακολουθούσε. Με την εμφάνιση και ανάπτυξη της τεχνολογίας των ηλεκτρονικών υπολογιστών, συντελούνται αλλαγές στο εγκληματικό φαινόμενο, που ποτέ πριν δεν είχε γνωρίσει η ανθρωπότητα. Οι εγκληματικές απειλές στηρίζονται πλέον σε πιο περίπλοκη τεχνολογία, καταργώντας τα φυσικά όρια. Βέβαια τόσο το συμβατικό έγκλημα όσο και τα μέσα διάπραξής του συνεχίζουν να υπάρχουν, όμως εμφανίζονται νέες μορφές με χαρακτηριστικότερη αυτή του ηλεκτρονικού εγκλήματος, του εγκλήματος δηλαδή που ένας ηλεκτρονικός υπολογιστής ή παρόμοιες συσκευές ηλεκτρονικής επεξεργασίας δεδομένων, διαδραματίζουν κυρίαρχο ρόλο.

Αναζητώντας τις ρίζες του ηλεκτρονικού εγκλήματος, διαπιστώνουμε ότι ταυτόχρονα με την εμφάνιση των υπολογιστών, έγιναν οι πρώτες προσπάθειες από τους επίδοξους «ηλεκτρονικούς εγκληματίες» να βρουν τρόπους να εκμεταλλευτούν τις νέες αυτές τεχνολογίες για να προσπορίσουν όφελος για τους εαυτούς τους ή για τρίτους. Η νέα τεχνολογία, που αναπτυσσόταν με γοργούς ρυθμούς, έδινε νέες ευκαιρίες για εύκολη διάπραξη πλήθους εγκλημάτων.

Ακόμη όμως και τα πρώτα χρόνια έπειτα από την εμφάνιση των υπολογιστών, το ηλεκτρονικό έγκλημα ήταν σπάνιο, διότι ο αριθμός τους ήταν περιορισμένος. Επιπλέον, οι υπάρχοντες υπολογιστές χρησιμοποιούσαν γλώσσα μηχανής, καθιστώντας αδύνατο για τους επίδοξους εγκληματίες να κατέχουν την απαραίτητη γνώση ή τον εξοπλισμό. Ο ηλεκτρονικός υπολογιστής αποτελούσε είδος πολυτελείας και κατ' αυτήν την έννοια το ηλεκτρονικό έγκλημα ήταν έγκλημα για λίγους.

Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα, χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκευάσε τον αργαλειό. Η «συσκευή» αυτή επέτρεπε την επανάληψη μιας σειράς ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία.

Χρονικά, η ανάπτυξη του ηλεκτρονικού εγκλήματος τοποθετείται στην τελευταία δεκαετία του περασμένου αιώνα, σε μια εποχή που χαρακτηρίστηκε από την αλματώδη εξέλιξη των υπολογιστικών συστημάτων. Σήμερα, το μεγαλύτερο ποσοστό του πληθυσμού στις αναπτυγμένες χώρες, έχει πρόσβαση σε έναν Η/Υ, η δε χρήση του έχει απλοποιηθεί τόσο που ακόμη και ένα μικρό παιδί μπορεί να χειρίζεται έναν προσωπικό υπολογιστή με ιδιαίτερη δεξιότητα.

Η μεγάλη επανάσταση στον τομέα του ηλεκτρονικού εγκλήματος, επήλθε μετά την εμφάνιση των δικτύων. Τα δίκτυα, δημιούργησαν νέες διόδους πρόσβασης προς την πληροφορία, καθιστώντας μη αναγκαία την παρουσία του επιτιθέμενου στο χώρο όπου αυτή φυλάσσεται. Η τεράστια πληροφοριακή δεξαμενή που δημιουργήθηκε και συνεχίζει να επεκτείνεται, αποτέλεσμα της διασύνδεσης εκατομμυρίων υπολογιστών ανά τον κόσμο, μετέβαλε ριζικά τον τρόπο ζωής του σύγχρονου ανθρώπου. Σήμερα, οι υπολογιστές χρησιμοποιούνται σε όλες τις εκφάνσεις της καθημερινής μας δραστηριότητας και στους σκληρούς τους δίσκους αποθηκεύονται πληροφορίες για τα προσωπικά μας στοιχεία, τους τραπεζικούς μας λογαριασμούς, τις συνήθειές μας, τις προτιμήσεις μας κ.ά.

Το νέο περιβάλλον χαρακτηρίζεται από την ευρεία ανάπτυξη του ηλεκτρονικού εμπορίου, την πραγματοποίηση τραπεζικών και συναλλαγματικών πράξεων μέσω του Διαδικτύου, την άμεση επικοινωνία σε όλα τα επίπεδα με νέες διόδους (e – mail, chat, newsgroups κ.λπ.), αλλά και την εξ αποστάσεως εκπαίδευση, την πραγματοποίηση συναλλαγών με δημόσιες υπηρεσίες, την τηλεδιάσκεψη κ.ά.

3.2 ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Ο ορισμός του ηλεκτρονικού εγκλήματος εξαρτάται σε μεγάλο βαθμό από την οπτική γωνία που τον εξετάζουμε. Αν αυτός άπτεται της νομικής επιστήμης, απαιτείται πιο αυστηρός προσδιορισμός των όρων, για να είναι δυνατή η στοιχειοθέτηση των εγκλημάτων. Η πολυπλοκότητα της μορφής αυτής της εγκληματικότητας, δυσχεραίνει ακόμα και το νομοθέτη, ο οποίος αποφεύγει να το ορίσει και είτε αφήνει την αρμοδιότητα αυτή στα δικαστήρια και την παραγόμενη νομολογία, είτε δανείζεται τους χρησιμοποιούμενους από την τεχνολογία όρους.

Κρίνεται επίσης σκόπιμο να επισημανθεί, ότι η εμπλοκή ενός ηλεκτρονικού υπολογιστή ή δικτύου δεν σημαίνει αναγκαστικά ότι έχουμε να κάνουμε με ηλεκτρονικό έγκλημα. Για παράδειγμα, αποτελεί ηλεκτρονικό έγκλημα ο βιασμός μιας γυναίκας από έναν άνδρα, τον οποίο γνώρισε μέσω chat room στο Διαδίκτυο και ο χρόνος και τόπος συνάντησης, που διαπράχθηκε το έγκλημα, καθορίστηκε μέσω e-mail; Σαφώς, η απάντηση στο παραπάνω ερώτημα είναι αρνητική. Πρόκειται για ένα συμβατικό έγκλημα (το βιασμό), που διαπράχθηκε με τη βοήθεια των δυνατοτήτων επικοινωνίας που προσφέρει το Διαδίκτυο (chat και e-mail).

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Σύμφωνα με τον Τσουραμάνη (Τσουραμάνης, 2005) ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται ***οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων*** και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Σύμφωνα με τον Λάζο (Λάζος, 2001) ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου.

Ο όρος Ηλεκτρονικό έγκλημα ή Ηλεκτρονική εγκληματικότητα διακρίνεται σε στενή και σε ευρεία έννοια. Η εν στενή έννοια ηλεκτρονική εγκληματικότητα αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη , η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων. Αντίθετα η εν ευρεία έννοια εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό μέσο.

Θα μπορούσαμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

- μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών,
- μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές,
- μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ' οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλλουν: e-crime, cybercrime, computer-crime, internet related crime και hitech-crime είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων είναι

ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους computer-crime, e-crime, hitech-crime ως γενικότερους και τους όρους cybercrime και internet related crime ως ειδικότερους, καθότι στη δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου.

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, ψηφιακό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους.

Τέλος πρέπει να αναφέρουμε πως βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, palmtop, notebook κ.λπ. Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ, ο οποίος μπορεί σύμφωνα με τον Shinder, (Βλαχόπουλος, 2007):

- Να αποτελεί τον στόχο κάποιας επίθεσης. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το «θύμα» της επίθεσης.
- Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή).
- Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

3.3 ΚΑΠΟΙΟΙ ΟΡΙΣΜΟΙ ΕΙΔΙΚΩΝ ΕΠΙΣΤΗΜΟΝΩΝ:

Σύμφωνα με τον Reimer (Λάζος, 2001) τα ηλεκτρονικά εγκλήματα δεν είναι νέα εγκλήματα, είναι τα ίδια παλιά εγκλήματα, που διαπράττονται με νέους και εφευρετικούς τρόπους, που η υψηλή τεχνολογία των σύγχρονων υπολογιστών και τηλεπικοινωνιών καθιστά δυνατούς.

Ο ειδικός στα ηλεκτρονικά εγκλήματα Donn Parker (Furnell, 2006), κάνει διαχωρισμό ανάμεσα στα ζητήματα του ηλεκτρονικού εγκλήματος και του κυβερνοεγκλήματος και τους εξηγεί ως εξής:

- Έγκλημα μέσω ηλεκτρονικού υπολογιστή: ένα έγκλημα στο οποίο ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από την τεχνολογία των υπολογιστών.
- Κυβερνοέγκλημα: ένα έγκλημα στο οποίο ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο.

Σύμφωνα με τον Τσουραμάνη (Τσουραμάνης, 2005) ως ψηφιακό έγκλημα (digital crime) θα μπορούσε να θεωρηθεί κάθε παράνομη πράξη για την διάπραξη, αλλά και για την αντιμετώπιση της οποίας θεωρείται απαραίτητη η γνώση της ψηφιακής τεχνολογίας. Στα ψηφιακά εγκλήματα έχει διαπιστωθεί ότι συνήθως εμπλέκεται είτε από την πλευρά του χρήστη είτε από την πλευρά του θύματος, ένας τουλάχιστον ηλεκτρονικός υπολογιστής. Ο ηλεκτρονικός υπολογιστής στην περίπτωση αυτή μπορεί να είναι: αντικείμενο, μέσο ή ακόμα και ο τόπος διάπραξης του εγκλήματος αυτού. Έτσι ο υπολογιστής αυτός θα ήταν δυνατό να είναι το προϊόν κλοπής ή ληστείας ή να χρησιμοποιήθηκε για παράνομη εισβολή του χρήστη του στα αρχεία ενός άλλου υπολογιστή ή για την τέλεση απάτης σε

βάρος κάποιου άλλου χρήστη ή τέλος στο σκληρό του δίσκο να μπορεί να βρει κανείς ίχνη τέλεσης κάποιας αξιόποινης πράξης.

Τέλος, ο Shackelford (Λάζος, 2001) στηρίζεται στον ορισμό του Beqauai για να προτείνει έναν δικό του ορισμό: έγκλημα σχετιζόμενο με τους υπολογιστές αποτελεί κάθε μη εξουσιοδοτημένη χρήση ενός υπολογιστή, περιλαμβανομένης και της υπέρβασης εξουσιοδότησης ή κάθε ανάλογης προσπάθειας.

3.4 ΔΙΑΦΟΡΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ ΑΠΟ ΤΑ ΠΑΡΑΔΟΣΙΑΚΑ ΕΓΚΛΗΜΑΤΑ

Οι διαφορές των ηλεκτρονικών εγκλημάτων από τα παραδοσιακά εγκλήματα, σύμφωνα με τον Τσουραμάνη (Τσουραμάνης, 2006) μπορούν να εντοπιστούν στα εξής χαρακτηριστικά:

- Διαπράττονται συνήθως από μακρινή απόσταση,
- Ο εντοπισμός του ψηφιακού εγκληματία είναι τεχνολογικά περίπλοκος,
- Αποδίδουν μεγάλα κέρδη, με μικρό κίνδυνο ανακάλυψης του δράστη τους,
- Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος,
- Οι οικονομικές απώλειες, που προξενούνται στα «ψηφιακά» θύματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων και
- Στο μεγαλύτερο μέρος τους δεν καταγράφονται από καμία επίσημη αρχή, δηλαδή ο «σκοτεινός αριθμός» τους είναι ιδιαίτερα σημαντικός

3.5 ΓΙΑΤΙ ΕΙΝΑΙ ΠΙΟ ΣΟΒΑΡΑ ΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΚΛΗΜΑΤΑ ΑΠΟ ΤΑ ΠΑΡΑΔΟΣΙΑΚΑ;

Θα μπορούσαμε να επισημάνουμε ενδεικτικά τα εξής για να τεκμηριώσουμε την πρότασή μας αυτή:

- Οι οικονομικές απώλειες από αυτά είναι πολύ μεγαλύτερες, όπως συνήθως διαπιστώνεται.
- Η ανακάλυψη των ενόχων και η προσαγωγή τους στη δικαιοσύνη συναντάει μεγαλύτερες δυσκολίες απ' ότι στα κοινά εγκλήματα,
- Οι ψηφιακοί εγκληματίες δεν έχουν φυσική παρουσία στον τόπο του εγκλήματος - σε αντίθεση με τους κοινούς εγκληματίες -, πράγμα που καθιστά δυσκολότερο τον εντοπισμό και τη σύλληψή τους και
- Οι πληροφορίες που υποκλέπτονται από μια επιχείρηση είναι δυνατό να είναι τόσο κρίσιμες γι' αυτή που μπορεί να οδηγήσουν στην απώλεια της εμπορικής της πίστης και σε κάποιες περιπτώσεις ακόμα και στη χρεωκοπία της με ότι αυτό συνεπάγεται για τους εργαζόμενους σε αυτή. Κάτι τέτοιο είναι μάλλον αδιανόητο να συμβεί σε περίπτωση που γίνει κάποιο κοινό έγκλημα (π.χ. διάρρηξη, ληστεία) σε βάρος της.

3.6 ΣΥΜΠΕΡΑΣΜΑΤΑ 3^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Στη σημερινή εποχή παρατηρείται μεγάλη αύξηση των ψηφιακών εγκλημάτων και γενικά της ηλεκτρονικής εγκληματικότητας, η οποία είναι ανάλογη με την συνεχώς αυξανόμενη χρήση του Ιντερνετ. Σημαντική ώθηση προς την κατεύθυνση αυτή έχει δώσει η διάδοση του ηλεκτρονικού εμπορίου (e-commerce). Οι εμπορικές συναλλαγές που πραγματοποιούνται στον κυβερνοχώρο προσφέρουν τη δυνατότητα διάπραξης διαφόρων οικονομικών εγκλημάτων. Απάτες, κλοπές πνευματικής ιδιοκτησίας και βιομηχανική κατασκοπεία είναι ορισμένα από αυτά. Τράπεζες και διάφοροι άλλοι οικονομικοί οργανισμοί υφίστανται τεράστιες οικονομικές απώλειες εξαιτίας της παράνομης δραστηριότητας οργανωμένων και μη ψηφιακών εγκληματιών που επεκτείνουν τη δράση τους σε όλη την υφήλιο εκμεταλλευόμενοι τις δυνατότητες μεταφοράς μεγάλων χρηματικών ποσών, που τους προσφέρει το διαδίκτυο.

Σύμφωνα με τον Βλαχόπουλο, (Βλαχόπουλος, 2007) οι ευκαιρίες για εγκληματική δραστηριότητα είναι περισσότερες από ποτέ. Το ηλεκτρονικό έγκλημα είναι ευκολότερο, οι δε δυνατότητες δίωξής του από τις αρμόδιες αρχές είναι περιορισμένες λόγω έλλειψης εμπειρίας στο σχετικό τομέα, ελλιπούς εκπαίδευσης αλλά και ασαφούς νομοθετικού πλαισίου, γεγονός που ενθαρρύνει τους επίδοξους εγκληματίες.

4^{Ο} ΚΕΦΑΛΑΙΟ

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΕΙΣΑΓΩΓΗ 4^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Στο παρών κεφάλαιο θα αναλύσουμε τα χαρακτηριστικά του ηλεκτρονικού εγκλήματος. Εκτός όμως από αυτό θα μιλήσουμε για τον τόπο τέλεσης και τα μέσα τέλεσης του ηλεκτρονικού εγκλήματος. Τέλος θα αναφερθούμε στον παγκόσμιο χαρακτήρα του ηλεκτρονικού εγκλήματος.

4.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΓΝΩΡΙΣΜΑΤΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Ο όρος ηλεκτρονικό έγκλημα, χρησιμοποιείται όλο και πιο συχνά, καθώς η νέα αυτή μορφή εγκλήματος φέρει ορισμένα ιδιαίτερα χαρακτηριστικά (Αγγέλης, 2000), που το διαφοροποιούν από το συμβατικό έγκλημα.

Είναι γεγονός ότι το ηλεκτρονικό έγκλημα διαπράττεται άμεσα, σε ελάχιστα δευτερόλεπτα. Ο επιτιθέμενος με τη χρήση ενός Η/Υ συνδεδεμένου στο Διαδίκτυο, μπορεί να εισβάλει στα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού σε οποιοδήποτε σημείο του κόσμου. Δεν απαιτείται η φυσική μετακίνησή του, καθώς οι ενέργειές του μπορούν να ολοκληρωθούν από την οικία του ή άλλο χώρο, με τη χρήση ενός δικτυωμένου προσωπικού υπολογιστή.

Φαινομενικά, η εισβολή σε κάποιο υπολογιστικό σύστημα φαντάζει δύσκολη. Όμως, η άποψη ότι απαιτούνται εξειδικευμένες γνώσεις για την εξαπόλυση τέτοιου είδους επίθεσης, αποτελεί μύθο. Στο Διαδίκτυο διατίθενται ελεύθερα εφαρμογές λογισμικού, που επιτρέπουν στους επίδοξους hackers την εισβολή σε δίκτυα και υπολογιστικά συστήματα, τη διασπορά ιών και την πραγματοποίηση πλήθους άλλων ηλεκτρονικών επιθέσεων, καθιστώντας περισσότερο εύκολη την διάπραξη του ηλεκτρονικού εγκλήματος σε σχέση με το συμβατικό.

Επιπλέον, το Διαδίκτυο προσφέρει μια σειρά από νέες δυνατότητες επικοινωνίας. Το ηλεκτρονικό ταχυδρομείο (e-mail), τα δωμάτια συζητήσεων (chat rooms) και οι ομάδες ειδήσεων (newsgroups), επιτρέπουν σε πολλά άτομα ταυτόχρονα να επικοινωνούν γρήγορα, σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα και ανέξοδα. Η επανάσταση αυτή στις επικοινωνίες συνέβαλε στη διάδοση εγκλημάτων, όπως η παιδοφιλία, η παιδική πορνογραφία και η ανεπιθύμητη αλληλογραφία (spamming). Στις περιπτώσεις αυτές, τα υποψήφια θύματα αναζητούνται μέσω των νέων καναλιών επικοινωνίας, που προσφέρει το Διαδίκτυο.

Παράλληλα, σύμφωνα με τον Βλαχόπουλο (Βλαχόπουλος. 2007) το ηλεκτρονικό έγκλημα έχει εισαγάγει νέους νομοθετικούς προβληματισμούς. Πολλές φορές, καθίσταται αδύνατο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος, διότι κάθε εγκληματίας μπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου, αρκεί να έχει στη διάθεσή του έναν

ηλεκτρονικό υπολογιστή. Επίσης, είναι δύσκολο να προσδιοριστεί και ο ακριβής χρόνος τέλεσής του, καθώς τα θύματα συχνά αντιλαμβάνονται μια ηλεκτρονική επίθεση πολύ αργότερα από το χρόνο κατά τον οποίο συνέβη. Επίσης, συχνά είναι δυνατή η διαγραφή από τον εισβολέα των «ιχνών» του ηλεκτρονικού εγκλήματος, κάτι που δυσχεραίνει ή εμποδίζει την ανίχνευσή του.

Τέλος, σε σύγκριση με τα συμβατικά εγκλήματα, η διερεύνηση του ηλεκτρονικού εγκλήματος παρουσιάζει ιδιαιτερότητες. Σε μια διαδικτυακή έρευνα, συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών, τα δε αρμόδια όργανα των διωκτικών αρχών πρέπει να κατέχουν εξειδικευμένες γνώσεις και να εκπαιδεύονται συνεχώς στις νέες τεχνολογικές εξελίξεις. Σε ορισμένες περιπτώσεις, τέτοιου είδους γνώσεις απαιτείται να κατέχουν και όσοι άλλοι ασχολούνται με τη δίωξη του ηλεκτρονικού εγκλήματος όπως δικαστές, εισαγγελείς και δικηγόροι.

Δυστυχώς, δεν υπάρχουν επαρκή στατιστικά στοιχεία ακόμη, όχι μόνο στον ελληνικό, αλλά και στο διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται, και αυτό για να μην πλήττεται το κύρος των εταιρειών που τυγχάνουν θύματα τέτοιων επιθέσεων. Κατά συνέπεια, οι διαστάσεις της εγκληματικότητας στο χώρο του Διαδικτύου είναι πιο δύσκολο να καθοριστούν από ότι στον «κοινό» εγκληματικό χώρο – (θεωρία του παγόβουνου) (Ζάννη, 2005).

Πιο συνοπτικά και σύμφωνα με τον Τσουραμάνη (Τσουραμάνης, 2005) το ηλεκτρονικό έγκλημα:

- Είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- Είναι εύκολο στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά...
- Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις.
- Μπορεί να διαπραχθεί χωρίς την μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, μέσω του υπολογιστή του.
- Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεως (news groups) ή μέσα σε chat rooms..
- Οι "εγκληματίες του Κυβερνοχώρου" πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα , αποστέλλουν ηλεκτρονικά μηνύματα(e-mail) με ψευδή στοιχεία.
- Είναι έγκλημα διασυνοριακό και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.
- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεως του και επίσης είναι αρκετά δύσκολη η διερεύνηση και ο εντοπισμός του δράστη. Υπάρχει ενδεχόμενο ο δράστης να εντοπισθεί στην Α χώρα και τα αποδεικτικά στοιχεία μπορεί να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες..
- Η έρευνα απαιτεί κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (του κράτους στο οποίο έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς, και του κράτους όπου βρίσκονται τα

αποδεικτικά στοιχεία). Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνον κράτους είναι σπάνια.

- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου καταγγέλλονται διεθνώς. Κατά συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου είναι «ακόμα πιο σκοτεινό», από ότι στον «κοινό» εγκληματικό χώρο.

4.2 ΤΟΠΟΣ ΤΕΛΕΣΗΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

«Τόπος» τέλεσης των ηλεκτρονικών εγκλημάτων είναι ο αποκαλούμενος κυβερνοχώρος (Τσουραμάνης, 2006), ο οποίος σύμφωνα με το «λεξικό διαδικτύου και δικτύων της Microsoft», προσδιορίζεται ως εξής: « το σύνολο των ηλεκτρονικών κόσμων, όπως το διαδίκτυο, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών. Καθοριστικό χαρακτηριστικό του κυβερνοχώρου είναι ότι η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση».

Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες (www.lawnet.gr):

1. Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθη η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε.
2. Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.
3. Η μικτή θεωρία, όπου ως τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.
4. Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας.

4.3 ΤΑ ΜΕΣΑ ΤΕΛΕΣΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Για να αποκτήσουν πρόσβαση σε ένα δίκτυο ή υπολογιστικό σύστημα, οι hackers χρησιμοποιούν εργαλεία που εκμεταλλεύονται τις αδυναμίες των συστημάτων. Τα εργαλεία αυτά, έχουν δημιουργηθεί, για να χρησιμοποιούνται από τους διαχειριστές δικτύων, προκειμένου να ελέγχουν την ευπάθεια των συστημάτων. Οι hackers, όμως, τα χρησιμοποιούν για τον αντίθετο ακριβώς σκοπό, δηλαδή για να εκμεταλλευτούν τις αδυναμίες των συστημάτων.

Πολλά από τα εργαλεία διανέμονται ελεύθερα στο Διαδίκτυο με αποτέλεσμα ακόμη και αρχάριοι χρήστες να μπορούν να τα εντοπίσουν και να τα χρησιμοποιήσουν εναντίον κάποιου συστήματος.

Τα πιο γνωστά σύμφωνα με τον Βλαχόπουλο (Βλαχόπουλος, 2007) είναι:

Port Scanners: Έχουν τη δυνατότητα να ελέγχουν πολλές IP διευθύνσεις και να δίνουν στο χρήστη πληροφορίες για τις διαθέσιμες θύρες (ports), τα υπάρχοντα λειτουργικά συστήματα, εφαρμογές που εκτελούνται και άλλες σημαντικές πληροφορίες για το σύστημα.

Vulnerability Scanners: Τα εργαλεία αυτά, ελέγχουν το λογισμικό εφαρμογών ενός Η/Υ, προσπαθώντας να εντοπίσουν κάποια ευπάθεια. Συνήθως, χρησιμοποιούνται από τους διαχειριστές για να εντοπίσουν και επιδιορθώσουν τις ευπάθειες των συστημάτων. Οι επιτιθέμενοι τα χρησιμοποιούν για τον αντίθετο, ακριβώς, σκοπό.

Rootkits: Ο όρος, χρησιμοποιείται για να περιγράψει ένα σύνολο από σενάρια (scripts) και εκτελέσιμα πακέτα, τα οποία επιτρέπουν στους εισβολείς, να κρύψουν οποιαδήποτε πληροφορία προδίδει ότι απέκτησαν πρόσβαση σε ένα σύστημα ή δίκτυο. Τα εργαλεία αυτά, επιτελούν μια σειρά από διαδικασίες στο σύστημα στο οποίο επιτέθηκαν, όπως:

- Τροποποίηση των αρχείων καταγραφής (log files).
- Τροποποίηση των εργαλείων του συστήματος.
- Δημιουργία κρυφών σημείων πρόσβασης στο σύστημα (backdoors).
- Χρησιμοποίηση του συστήματος ως το αρχικό σημείο εξαπόλυσης επιθέσεως σε άλλα συστήματα.

Sniffers: Τα προγράμματα αυτά, χρησιμοποιούνται για να αναγνώσουν τις πληροφορίες, που αφορούν την κίνηση σε ένα τοπικό δίκτυο υπολογιστών. Πραγματοποιώντας το κατάλληλο φιλτράρισμα στα δεδομένα που συλλέγουν, έχουν τη δυνατότητα να ανακτούν ευαίσθητες πληροφορίες όπως ονόματα χρηστών, κωδικούς πρόσβασης και δεδομένα συναλλαγών, που διακινούνται σε ένα δίκτυο μέσω των πρωτοκόλλων επικοινωνίας TCP/IP. Οι επιθέσεις τύπου sniffing είναι ιδιαιτέρως αποτελεσματικές όταν δεν γίνεται κρυπτογράφηση των δεδομένων που διακινούνται σε ένα δίκτυο.31

Anonymous re-mailers: Ένας ανώνυμος re-mailer32 είναι ένα πρόγραμμα, το οποίο εκτελείται σε κάποιον υπολογιστή στο Διαδίκτυο και επιτρέπει στον οποιοδήποτε, να στείλει μηνύματα σε ομάδες συζητήσεων ή σε μεμονωμένα άτομα, χωρίς να γίνει γνωστή η ταυτότητά του. Όταν ένα μήνυμα στέλνεται σε μια τέτοια διεύθυνση, το πρόγραμμα αφαιρεί το όνομα και τη διεύθυνση του αποστολέα και το προωθεί στον προορισμό του. Μάλιστα, πολλές φορές, τα μηνύματα αυτά διέρχονται από διαδοχικούς re-mailers, με αποτέλεσμα να καθίσταται δύσκολη η παρακολούθηση ή ο εντοπισμός τους.

Password Crackers: Οι password crackers είναι εργαλεία λογισμικού, τα οποία χρησιμοποιούνται για να ανακτήσουν τους κωδικούς πρόσβασης ενός συστήματος. Για το σκοπό αυτό οι password crackers κάνουν χρήση ενός αρχείου με πιθανούς κωδικούς (δηλαδή ένα σύνολο από λέξεις που έχουν επιλεγεί από κάποιους χρήστες με μεγάλη πιθανότητα), που συχνά αναφέρεται και ως «λεξικό» (dictionary). Ενώ η σχετική επίθεση ως «επίθεση λεξικού» (dictionary attack). Οι επιθέσεις αυτές εκμεταλλεύονται τρεις βασικές ευπάθειες των συστημάτων ελέγχου πρόσβασης με κωδικούς. Πρώτον, το

μήκος των κωδικών είναι μικρό με αποτέλεσμα ένα πρόγραμμα να είναι εύκολο να δοκιμάσει όλους τους κωδικούς μήκους 8 χαρακτήρων που επιλέγονται από τους 96 διαθέσιμους χαρακτήρες του πληκτρολογίου. Δεύτερον, οι χρήστες συχνά επιλέγουν εύκολους κωδικούς, όπως ημερομηνίες γέννησης, ονόματα, τοπωνύμια κ.λπ. κάτι που καθιστά το έργο των crackers ακόμη πιο εύκολο. Και, τρίτον, τα αρχεία με τους κωδικούς των χρηστών δεν προστατεύονται σωστά, με αποτέλεσμα, να είναι συχνά εύκολη η υποκλοπή τους από τον διακομιστή όπου έχουν αποθηκευτεί.

Spoofers: Πρόκειται για προγράμματα που αλλάζουν τη διεύθυνση IP του Η/Υ του επιτιθέμενου ώστε να μην ανιχνεύονται οι επιθέσεις του, ή με σκοπό την ενοχοποίηση κάποιου άλλου χρήστη. Συχνά, ανυποψίαστοι χρήστες του Διαδικτύου κατηγορούνται για ηλεκτρονικά εγκλήματα επειδή κάποιος κακόβουλος χρησιμοποίησε την IP διεύθυνσή τους.

4.4 Ο ΠΑΓΚΟΣΜΙΟΣ ΧΑΡΑΚΤΗΡΑΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Το κύριο χαρακτηριστικό γνώρισμα του ηλεκτρονικού εγκλήματος είναι ο παγκόσμιος χαρακτήρας του. Το ηλεκτρονικό έγκλημα έχει υπερβεί τα στενά γεωγραφικά όρια των κρατών, παρουσιάζοντας ένα «πρόσωπο» παγκόσμιο, το οποίο οφείλεται κυρίως στην ανάπτυξη του Διαδικτύου.

Σε νομοθετικό επίπεδο, η παγκοσμιότητα αυτή δημιουργεί μια σειρά από ερωτήματα. Τι γίνεται όταν ένα έγκλημα διαπράττεται σε δύο ή περισσότερες χώρες ταυτόχρονα, στις οποίες ισχύει διαφορετικό νομοθετικό πλαίσιο ή όταν σε μία από τις χώρες αυτές δεν υπάρχει καθόλου νομοθετικό πλαίσιο για τη συγκεκριμένη συμπεριφορά; Σε περίπτωση διεθνών ερευνών για ένα ηλεκτρονικό έγκλημα, πώς θα γίνουν οι απαιτούμενες ενέργειες σε μια χώρα, που δεν διαθέτει σχετική νομοθεσία;

Οι αποσπασματικές νομοθετικές παρεμβάσεις συγκεκριμένων κρατών για την αντιμετώπιση των προβλημάτων αυτών δεν επαρκούν. Απαιτείται πρωταρχικά εναρμόνιση της διεθνούς νομοθεσίας σχετικά με το ηλεκτρονικό έγκλημα, μέσω συμβάσεων ή άλλων επίσημων εγγράφων. Η διαδικασία αυτή, βέβαια, είναι ιδιαίτερα πολύπλοκη. Ενδεικτικά, αναφέρεται ότι σε κάποιες χώρες δεν έχει καν φθάσει η τεχνολογία των υπολογιστών και του Διαδικτύου, ενώ το ηλεκτρονικό έγκλημα, όπως και πολλές άλλες μορφές εγκλήματος, αντιμετωπίζεται με διαφορετικό τρόπο σε κάθε χώρα, ανάλογα με το συγκεκριμένο κοινωνικοπολιτικό καθεστώς, τα ήθη, τα έθιμα και τις παραδόσεις κάθε λαού.

Όσον αφορά τον καθαυτό νομικό τομέα, μια τέτοια επιχειρούμενη προσπάθεια θα συναντούσε επιπλέον προβλήματα. Για παράδειγμα, σε κάποιες χώρες απαιτείται συνταγματική αναθεώρηση για να ισχύσουν παγκόσμιοι νομοθετικοί κανόνες, οι οποίοι, ενδεχομένως, να μη γίνουν αποδεκτοί, αλλά και στην περίπτωση που γίνουν, θα απαιτηθεί μεγάλο χρονικό διάστημα για να ολοκληρωθούν οι συνταγματικές αναθεωρήσεις.

Εκτός όμως από τον τομέα του ποινικού δικαίου, σημαντικά προβλήματα προκύπτουν και κατά την εφαρμογή του δικονομικού δικαίου. Η διερεύνηση ηλεκτρονικών εγκλημάτων, απαιτεί εξειδικευμένες δυνατότητες έρευνας από τις αρμόδιες αρχές, που έρχονται σε

σύγκρουση με θεμελιώδεις αξίες, όπως η προστασία του απορρήτου και της ιδιωτικότητας του ατόμου. Παράλληλα, ο παγκόσμιος χαρακτήρας του, επιβάλλει την άμεση και συνεχή συνεργασία μεταξύ των χωρών για την αναζήτηση και αποκάλυψη των δραστών.

Μέχρι σήμερα, διάφοροι οργανισμοί, όπως το Συμβούλιο της Ευρώπης και τα Ηνωμένα Έθνη, έχουν επιχειρήσει να πρωτοστατήσουν στην προσπάθεια εναρμόνισης της διεθνούς νομοθεσίας για το ηλεκτρονικό έγκλημα.

4.5 ΣΥΜΠΕΡΑΣΜΑΤΑ 4^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Είναι αλήθεια πως το ηλεκτρονικό έγκλημα διαπράττεται άμεσα και δεν απαιτείται η φυσική παρουσία του δράστη. Επίσης δεν απαιτούνται εξειδικευμένες γνώσεις για την εξαπόλυση κάθε είδους επίθεσης. Οι νέες δυνατότητες επικοινωνίας συμβάλλουν στην δημιουργία και την διάδοση των ηλεκτρονικών εγκλημάτων. Εν συνεχεία, η διερεύνηση του ηλεκτρονικού εγκλήματος παρουσιάζει ιδιαιτερότητες.

Τέλος, θα μπορούσαμε να πούμε, μετά από την παρούσα ανάλυση, πως τα χαρακτηριστικά και οι ιδιαιτερότητες των ηλεκτρονικών εγκλημάτων καθιστούν περισσότερο εύκολη την διάπραξη του ηλεκτρονικού εγκλήματος σε σχέση με το συμβατικό.

5^{Ο} ΚΕΦΑΛΑΙΟ

ΔΡΑΣΤΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

ΕΙΣΑΓΩΓΗ 5^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Σε αυτό το μικρό σχετικά κεφάλαιο, θα παρουσιάσουμε τις κατηγορίες των δραστών των ηλεκτρονικών εγκλημάτων και θα προσπαθήσουμε να δώσουμε ένα πιθανό προφίλ του δράστη ηλεκτρονικών εγκλημάτων.

5.1 ΚΑΤΗΓΟΡΙΕΣ ΔΡΑΣΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Τους εγκληματίες του κυβερνοχώρου μπορούμε να τους διακρίνουμε σε δυο κατηγορίες :

- σ΄ αυτούς που "επιτίθενται" (εισβάλουν) στα computer απλώς από ευχαρίστηση ή περιέργεια, χωρίς όμως να επιδιώκουν (εμφανώς τουλάχιστον) κάποιο οικονομικό όφελος. Στην κατηγορία αυτή ανήκουν, οι δράστες που από το άλλο άκρο του πλανήτη "εισβάλουν " σε υπολογιστή δια της χρήσεως του διαδικτύου (hackers) για να μάθουν απλώς, κάποια προσωπικά στοιχεία,
- σ΄ αυτούς που ενεργούν από οικονομικό όφελος (cracker). Στην δεύτερη ανήκουν αυτοί που δεν " εισβάλουν " απλώς για να μάθουν κάτι, αλλά μόλις μάθουν το στοιχείο που επιθυμούν (π.χ. τον αριθμό της πιστωτικής κάρτας) δίνουν και την κατάλληλη εντολή στην Τράπεζά για την μεταφορά ενός ποσού στον λογαριασμό τους.

Σύμφωνα με Anderson (Furnell, 2006), υπάρχουν οι εξής κατηγορίες δραστών ηλεκτρονικών εγκλημάτων:

- Εξωτερικοί δράστες: Πρόσωπα προερχόμενα από τον εξωτερικό χώρο της επιχείρησης – στόχου τους, που πετυχαίνουν πρόσβαση στο σύστημα της δίχως να έχουν εξουσιοδότηση. Αυτή είναι η κατηγορία η οποία ανταποκρίνεται περισσότερο στην παραδοσιακή εικόνα του χάκερ – δεν έχουν νόμιμο σκοπό και ως εκ τούτου δεν έχουν ρόλο να παίξουν στο σύστημα.
- Εσωτερικοί δράστες: χρήστες του συστήματος, που έχουν εξουσιοδότηση και αποκτούν πρόσβαση σε δεδομένα, πηγές ή προγράμματα δίχως να έχουν τέτοιο δικαίωμα. Οι υποκατηγορίες τους έχουν ως εξής:

Μεταμφιεσμένοι: χρήστες, που δρουν χρησιμοποιώντας την ταυτότητα άλλου χρήστη.
Κρυφοί χρήστες: χρήστες, που επιτυγχάνουν παράνομη πρόσβαση σε αρχεία με σκοπό τον έλεγχο και την εξέταση του περιεχομένου τους.
Έκπτωτοι: χρήστες, που έχουν την άδεια να χρησιμοποιούν το σύστημα και τις πηγές του στις οποίες αποκτούν πρόσβαση, αλλά έχουν απολέσει τα προνόμιά τους. Αυτή η ομάδα είναι τυπικά η πιο δύσκολα αναγνωρίσιμη, επειδή τα πρόσωπα έχουν νόμιμη πρόσβαση στο σύστημα και γνωρίζουν πώς να το χρησιμοποιούν

5.2 ΣΚΙΑΓΡΑΦΗΣΗ ("ΠΡΟΦΙΛ ") ΕΓΚΛΗΜΑΤΙΑ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ.

Ο "εγκληματίας του κυβερνοχώρου" διαφέρει ουσιωδώς από τον "κοινό εγκληματία". Δεν μπορεί ο καθένας να διαπράξει έγκλημα που σχετίζεται με το διαδίκτυο. Ο δράστης πρέπει να διαθέτει ειδικές γνώσεις, τεχνική επιδεξιότητα, τεχνικά μέσα. Χαρακτηριστικώς αναφέρεται ότι, στο έγκλημα στον κυβερνοχώρο (cyber-crime) δεν υπάρχει "Γιάννης - Αγιάννης". Υπάρχουν μόνο " άθλιοι ". Τι σημαίνει αυτό; Ο εγκληματίας του κυβερνοχώρου, (cyber-crook), δεν μπορεί να υποστηρίξει ότι ενήργησε "από ανάγκη" δηλαδή από οικονομική ανέχεια, αφού η ενέργειά του προϋποθέτει την ύπαρξη μιας αρκετά ικανής οικονομικής υποδομής (αγορά και συντήρηση υπολογιστή, αυξημένος τηλεφωνικός λογαριασμός, συνδρομή σε παροχέα πρόσβασης, εκπαίδευση σε υπολογιστές, αγορά σχετικών βιβλίων, κλπ). Δηλαδή χωρίς την κατοχή αυτή των τεχνικών και μη μέσων, είναι αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο.

Σε ειδική έρευνα που έγινε στη Βρετανία από την ``επιτροπή πρόβλεψης και πρόληψης εγκλήματος`` (Foresight Crime Prevention Panel) για το ``ποιόν`` (``who is who``) του μελλοντικού εγκληματία διαπιστώθηκε ότι: Το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια την λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης, θα μπορούν να ξεπεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο, ακόμα Δε και τα εμπόδια που θα αναγνωρίζουν τα δακτυλικά αποτυπώματα ή το χρώμα του οφθαλμού. Ειδικότερα τον ανιχνευτή της ίριδος θα τον ``ξεγελούν`` με την ανάλογη κατασκευή φακών επαφής (Τσουραμάνης, 2005).

6^{Ο} ΚΕΦΑΛΑΙΟ

ΚΑΤΗΓΟΡΙΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

ΕΙΣΑΓΩΓΗ 6^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Σε αυτό το κεφάλαιο θα γίνει μια ανάλυση των κυριότερων κατηγοριών των ηλεκτρονικών εγκλημάτων και θα παραθέσουμε τις απόψεις διαφόρων ειδικών.

6.1 ΔΙΑΧΩΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Για την καταγραφή και ανάλυση των βασικότερων μορφών ηλεκτρονικού εγκλήματος, διακρίνουμε δύο βασικές κατηγορίες σύμφωνα με τον Βλαχόπουλο
(Βλαχόπουλος, 2007):

α) Τα εγκλήματα, που δεν υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και των δικτύων. Τα εγκλήματα αυτά, τα χαρακτηρίζουμε ως «γνήσια»: 1. Κακόβουλες εισβολές σε δίκτυα, 2. Επιθέσεις Άρνησης Εξυπηρέτησης, 3. Κακόβουλο λογισμικό, 4. Ανεπιθύμητη Αλληλογραφία (Spamming), 5. Επιθέσεις σε δικτυακούς τόπους, 6. Πειρατεία ονομάτων χώρου, 8. Πειρατεία λογισμικού

β) Τα εγκλήματα, που υπήρξαν και πριν την εμφάνιση των ηλεκτρονικών υπολογιστών, τελούνται, όμως, με τη χρήση ή βοήθεια των ηλεκτρονικών υπολογιστών ή/και δικτύων, όπως: 1. Απάτη στο Διαδίκτυο, 2. Κλοπή ταυτότητας, 3.Ξέπλυμα χρήματος, 4.Διακίνηση πορνογραφικού υλικού, 5. Διαδικτυακή τρομοκρατία, 6. Επιθέσεις παρενόχλησης

Τέλος υπάρχουν και άλλες μορφές ηλεκτρονικών εγκλημάτων, όπως: στην κινητή τηλεφωνία, στα τηλεπικοινωνιακά δίκτυα, στις παιχνιδομηχανές και στα μηχανήματα αυτόματης ανάληψης μετρητών.

6.2 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ ΣΥΜΦΩΝΑ ΜΕ ΚΑΠΟΙΟΥΣ ΕΠΙΣΤΗΜΟΝΕΣ

Γίνεται διαχωρισμός ανάμεσα σε αυτά τα εγκλήματα που ο ηλεκτρονικός υπολογιστής αποτελεί βοηθητικό μέσο και σε αυτά που ο ηλεκτρονικός υπολογιστής είναι ο κύριος στόχος τους:

- Εγκλήματα με την βοήθεια του ηλεκτρονικού υπολογιστή: περιπτώσεις στις οποίες οι υπολογιστές χρησιμοποιούνται σε βοηθητικό ρόλο, αλλά το κύριο έγκλημα μπορεί να διαπραχθεί και χωρίς αυτούς. Οι περιπτώσεις της απάτης, της κλοπής, της παραβίασης της ιδιωτικής σφαίρας, της παραβίασης των προσωπικών δεδομένων, του σαμποτάζ και της πορνογραφίας μπορούν να συμπεριληφθούν σε αυτήν την κατηγορία.

- Εγκλήματα επικεντρωμένα στους ηλεκτρονικούς υπολογιστές: περιπτώσεις στις οποίες η εγκληματική πράξη αποτελεί το άμεσο αποτέλεσμα της τεχνολογίας των υπολογιστών και δεν υπάρχει παράλληλη εμφάνισή της και σε άλλους τομείς. (hacking, ιοί)

Συνοψίζοντας, διακρίνουμε τρεις βασικές κατηγορίες όσον αφορά στις μορφές του ηλεκτρονικού εγκλήματος σύμφωνα με τον Αργυρόπουλο (Αργυρόπουλος, 2001):

- Σε εγκλήματα που διαπράττονται τόσο σε συμβατικό περιβάλλον όσο και σε περιβάλλον ηλεκτρονικών υπολογιστών. Στην κατηγορία αυτή εντάσσουμε πολλές κατηγορίες εγκλημάτων. Για παράδειγμα, η συκοφαντική δυσφήμηση μπορεί να διαπραχθεί με τη δημοσίευση στο Διαδίκτυο μιας σελίδας με προσβλητικό περιεχόμενο για ένα πρόσωπο. Ουσιαστικά στην περίπτωση αυτή το Διαδίκτυο αποτελεί ένα ακόμη μέσο για την τέλεση ενός εγκλήματος.

- Σε εγκλήματα που διαπράττονται με τη χρήση υπολογιστών χωρίς την ύπαρξη δικτύωσης. Χαρακτηριστικό έγκλημα της κατηγορίας αυτής, είναι η παράνομη αντιγραφή λογισμικού.

- Σε εγκλήματα που έχουν να κάνουν αποκλειστικά με τη χρήση του Διαδικτύου. Η συνηθέστερη εγκληματική συμπεριφορά της κατηγορίας αυτής, είναι η διασπορά κακόβουλου λογισμικού (ιών).

Οι δύο τελευταίες περιπτώσεις, συνιστούν μια εντελώς νέα μορφή εγκλήματος, η οποία δεν υπήρχε πριν την εμφάνιση των ηλεκτρονικών υπολογιστών.

Παρακάτω θα παραθέσουμε τις απόψεις διαφόρων ειδικών επιστημόνων σχετικά με την κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων:

Σύμφωνα με τον Parker (1983) υπάρχουν 4 τύποι πληροφορικής προσβολής:

- Ο υπολογιστής μπορεί να αποτελέσει το αντικείμενο της επίθεσης. Είναι δυνατό να καταστραφούν τα πολύτιμα πράγματα και προγράμματα, που φιλοξενεί.
- Να χρησιμοποιηθεί ο υπολογιστής ως εργαλείο για την διάπραξη αδικημάτων (κλοπή, καταπάτηση, παραβίαση).
- Να αξιοποιηθεί συμβολικά ο υπολογιστής ώστε να συμβάλλει αποφασιστικά στον πειθαναγκασμό, την παραπλάνηση, την εξαπάτηση.
- Οι πληροφορίες σε ηλεκτρονική μορφή μπορούν αν αντιγραφούν, τροποποιηθούν, υπονομευθούν ή διαγραφούν, χωρίς οι αναγκαίες ενέργειες να αφήνουν πίσω τους κάποιο φυσικό ίχνος

Σύμφωνα με το Computer Security Institute (2001) (Furnell, 2006), υπάρχουν οι εξής κατηγορίες ηλεκτρονικών εγκλημάτων:

- Κλοπή πληροφοριών
- Σαμποτάζ σε δεδομένα ή δίκτυα
- Τηλεπικοινωνιακή παρακολούθηση συνομιλιών
- Παραβίαση συστημάτων από εξωτερικά άτομα
- Εσωτερική παρενόχληση ή πρόσβαση σε δίκτυο
- Οικονομική απάτη
- Άρνηση παροχής πληροφοριών
- Απόκρυψη ταυτότητας

- Ιοί
- Εσωτερική παράνομη πρόσβαση
- Τηλεπικοινωνιακή απάτη
- Τηλεφωνικές υποκλοπές
- Κλοπή φορητών υπολογιστών

Πίνακας 6.1. Κατηγορίες ηλεκτρονικών εγκλημάτων και προσβολών κατά την εξεταστική επιτροπή της Μ.Β. (2006):

Έγκλημα / προσβολή	**Περιγραφή**
Απάτη	Για προσωπική ωφέλεια: • Αλλοίωση των εισαγωγών με μη νόμιμο τρόπο -καταστροφή/ συμπίεση/ ακαταλληλότητα εκτροών -αλλοίωση των δεδομένων του Η/Υ -Αλλοίωση ή κακή χρήση των προγραμμάτων (εξαιρουμένων των προσβολών από ιούς)
Κλοπή	• Των δεδομένων • Του λογισμικού
Χρήση λογισμικού χωρίς άδεια	• Χρήση παράνομων αντιγράφων λογισμικού
Ιδιωτική εργασία	• Μη εγκεκριμένη χρήση των δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποκομιδή κέρδους ή για ίδιον όφελος
Κακή χρήση προσωπικών δεδομένων	• Ανεπίσημη «ανάγνωση» των αρχείων ενός συστήματος Η/Υ και παράβαση της σχετικής νομοθεσίας
Χάκινγκ Σαμποτάζ	• Ελεύθερη πρόσβαση σε ένα σύστημα Η/Υ συνήθως με την χρήση των δυνατοτήτων της επικοινωνίας • Η διαμεσολάβηση με την πρόκληση ζημίας στον τρέχοντα κύκλο ή στον εξοπλισμό
Εισαγωγή	• Εισαγωγή πορνογραφικού υλικού, π.χ. πορνογραφικού υλικού μέσω internet
Ιοί	• Διάχυση ενός προγράμματος με σκοπό τη ματαίωση της τρέχουσας εφαρμογής

(Πηγή: Furnell, 2006)

Οι 2 κατηγορίες ηλεκτρονικών εγκλημάτων σύμφωνα με τον Barrett (Τσουραμάνης, 2005):

- Σε εκείνα, που στρέφονται κατά των Η/Υ και στα οποία περιλαμβάνεται η κλοπή των υλικών μερών ενός Η/Υ, η εισβολή σε ηλεκτρονικά αρχεία και ο ψηφιακός βανδαλισμός καθώς και η διασπορά καταστρεπτικών ιών, και
- Σε εκείνα που υποστηρίζονται από τον Η/Υ και στα οποία περιλαμβάνονται η πορνογραφία, η πειρατεία λογισμικού, οι διάφορες απάτες και το ξέπλυμα βρώμικου χρήματος που γίνεται ηλεκτρονικά (Τσουραμάνης, 2005).

Οι 4 κατηγορίες ηλεκτρονικών εγκλημάτων σύμφωνα με τον Pipkin (2003) (Τσουραμάνης, 2005):

- Στην πρώτη κατηγορία ανήκουν τα παραδοσιακά εγκλήματα, τα οποία τελούνται με την χρήση Η/Υ και σαν τέτοια αναφέρει την απάτη, την κλοπή στοιχείων των ιδιοκτητών πιστωτικών καρτών και την κλοπή της (ηλεκτρονικής) ταυτότητας.
- Στην δεύτερη κατηγορία υπάγονται τα ειδικά εγκλήματα των Η/Υ και σαν τέτοια θεωρούνται η επίθεση άρνησης παροχής υπηρεσιών, την άρνηση πρόσβασης σε πληροφορίες και τη διασπορά καταστρεπτικών ιών.
- Στην Τρίτη κατηγορία τοποθετούνται τα εγκλήματα, που στρέφονται κατά της πνευματικής ιδιοκτησίας, όπως είναι η κλοπή πληροφοριών και η εμπορία, εναποθήκευση, έκθεση (διαστρέβλωση) και καταστροφή πληροφοριών που έχουν κλαπεί.
- Στην τέταρτη κατηγορία υπάγονται τα ηλεκτρονικά εγκλήματα που στρέφονται κατά του προσωπικού απορρήτου και σαν τέτοιο θεωρείται η διακίνηση πορνογραφικού υλικού με ανηλίκους, που γίνεται μέσω του διαιδικτύου .

Οι 3 κατηγορίες ηλεκτρονικών εγκλημάτων, σύμφωνα με τους Σουρής, Πατσός, Γρηγοριάδης (2005):

- Εγκλήματα σε υπολογιστή, όπως η μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικό σύστημα και η διασπορά κακόβουλων προγραμμάτων,
- Εγκλήματα που σχετίζονται με Η/Υ, όπως η ηλεκτρονική πορνογραφία και η πειρατεία λογισμικού, και
- Εγκλήματα που διαπράττονται με την βοήθεια Η/Υ, όπως η απάτη σε ηλεκτρονικές συναλλαγές, η υποκλοπή στοιχείων πιστωτικών καρτών και η πλαστογράφηση εντύπων (Τσουραμάνης, 2005).

Οι 3 κατηγορίες ηλεκτρονικών εγκλημάτων σύμφωνα με τον Sieber (Λάζος, 2001):

- Ηλεκτρονικά οικονομικά εγκλήματα (απάτη, ηλεκτρονική κατασκοπεία),
- Ηλεκτρονικά εγκλήματα κατά των προσωπικών δικαιωμάτων (κατά της ιδιωτικότητας),
- Υπερ – ατομικά ηλεκτρονικά εγκλήματα (κατά της εθνικής ασφάλειας, της δημοκρατικής νομιμότητας).

Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες, με τίτλο «Cyber Crime... and Punishment?» κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω κατηγορίες:

- Παρεμπόδιση (κυβερνο)κυκλοφορίας,
- Τροποποίηση και Κλοπή δεδομένων,
- Εισβολή και Σαμποτάζ σε δίκτυο,
- Μη εξουσιοδοτημένη πρόσβαση,
- Διασπορά ιών,
- Υπόθαλψη αδικημάτων,
- Πλαστογραφία και
- Απάτη.

Σύμφωνα με τη διεθνή σύμβαση για το κυβερνοέγκλημα του 2001 (Convention on Cyber Crime 2001) (Τσουραμάνης, 2005) οι κύριες ψηφιακές παραβάσεις (εγκλήματα) είναι οι ακόλουθες :

- Παράνομη πρόσβαση,

- Παράνομη υποκλοπή,
- Παρεμβολή σε δεδομένα,
- Παρεμβολή σε συστήματα,
- Κακή χρήση συσκευών,
- Κλοπή που σχετίζεται με υπολογιστή,
- Απάτη που σχετίζεται με υπολογιστή,
- Παιδική πορνογραφία και
- Προστασία πνευματικών δικαιωμάτων ηλεκτρονικών πληροφοριών.

Τέλος και για τις ανάγκες της ετήσιας έρευνας που διεξάγεται από το Computer Security Institute και το FBI(Τσουραμάνης, 2005) ως ψηφιακά (ηλεκτρονικά) εγκλήματα θεωρούνται :

1. οι επιθέσεις ιών,
2. η επίθεση άρνησης παροχής υπηρεσιών,
3. η κλοπή πνευματικής ιδιοκτησίας,
4. οι παραβιάσεις υπαλλήλων που σχετίζονται με Η/Υ
5. οι παράνομες ακροάσεις τηλεπικοινωνιών,
6. οι οικονομικές απάτες,
7. οι κλοπές φορητών Η/Υ,
8. οι παράνομες εισβολές σε σύστημα Η/Υ,
9. οι τηλεπικοινωνιακές απάτες,
10. η παραποίηση ιστοσελίδων και
11. το σαμποτάζ.

Κύριες μορφές Κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος:

- Απάτες μέσω Διαδικτύου
- Παιδική πορνογραφία
- Cracking και hacking
- Διακίνηση-πειρατεία λογισμικού
- Πιστωτικές κάρτες
- Διακίνηση ναρκωτικών
- Έγκλημα στα chat rooms

6.3 ΣΥΜΠΕΡΑΣΜΑΤΑ 6ΟΥ ΚΕΦΑΛΑΙΟΥ

Το ηλεκτρονικό έγκλημα, σήμερα, έχει εισχωρήσει στη δομή και οργάνωση των ανεπτυγμένων κοινωνιών. Νέες μορφές εμφανίζονται και οι υπάρχουσες αναπτύσσονται και εξελίσσονται με γοργούς ρυθμούς. Το ηλεκτρονικό έγκλημα περιλαμβάνει εγκλήματα, που τελούνται με οποιαδήποτε συσκευή ηλεκτρονικής επεξεργασίας δεδομένων. Πολλά από τα εγκλήματα του κοινού Ποινικού Δικαίου, υπήρχαν πολύ πριν την εμφάνιση των συσκευών αυτών, ωστόσο, οι νέες τεχνολογίες και κυρίως οι ηλεκτρονικοί υπολογιστές και τα δίκτυα, διεύρυναν σε μεγάλο βαθμό τα μέσα διάπραξής τους. Παράλληλα δημιουργήθηκαν νέες εγκληματικές απειλές.

7^{o} ΚΕΦΑΛΑΙΟ

ΗΛΕΚΤΡΟΝΙΚΑ ΟΙΚΟΝΟΜΙΚΑ ΕΓΚΛΗΜΑΤΑ ΑΠΑΤΗ ΜΕΣΩ ΥΠΟΛΟΓΙΣΤΗ

ΕΙΣΑΓΩΓΗ 7^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Σε αυτό το κεφάλαιο θα παρουσιάσουμε τα χαρακτηριστικά και τις κατηγορίες των ηλεκτρονικών οικονομικών εγκλημάτων. Τέλος θα αναλύσουμε την έννοια και τις κατηγορίες της απάτης μέσω υπολογιστή.

7.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΟΙΚΟΝΟΜΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ:

Ο κύριος όγκος των ηλεκτρονικών εγκλημάτων εντάσσεται στη κατηγορία των οικονομικών ηλεκτρονικών εγκλημάτων. Τα ηλεκτρονικά οικονομικά εγκλήματα απαρτίζουν τον κύριο όγκο των διαπιστωμένων ηλεκτρονικών εγκλημάτων και επίσης είναι τα εγκλήματα που τραβούν την προσοχή των ερευνητών.

- Τα ηλεκτρονικά οικονομικά εγκλήματα γίνονται αντιληπτά από τους ενδιαφερόμενους σε σχετικά μικρό χρονικό διάστημα μετά την τέλεσή τους.
- Είναι μετρήσιμα με μεγάλη ακρίβεια – τουλάχιστον όσον αφορά στα άμεσα οικονομικά του μεγέθη.
- Τραβούν το ενδιαφέρον μεγάλων επιχειρήσεων, οι οποίες έχουν διαθέσει πολύ σημαντικούς πόρους για την διερεύνηση τους.

7.2 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΟΙΚΟΝΟΜΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Η συχνότητα και η σημασία του ηλεκτρονικού οικονομικού εγκλήματος έχουν θεωρηθεί επαρκείς λόγοι για την δημιουργία συστηματικών κατηγοριοποιήσεων του. Σημαντικοί επιστήμονες του χώρου, όπως ο Wasik και ο Sieber, έχουν και εκείνοι προχωρήσει σε κατηγοριοποιήσεις του ηλεκτρονικού οικονομικού εγκλήματος, ανάλογα με τα εμπειρικά δεδομένα που ο καθένας είχε στην διάθεσή του.

Κατηγοριοποίηση του Sieber(Λάζος, 2001): οικονομικά εγκλήματα σχετιζόμενα με υπολογιστές:

1. απάτη ηλεκτρονικής παραποίησης ενάντια σε συστήματα επεξεργασίας δεδομένων
2. ηλεκτρονική κατασκοπεία και κλοπή λογισμικού
3. ηλεκτρονική δολιοφθορά
4. κλοπή υπηρεσιών
5. μη εξουσιοδοτημένη πρόσβαση σε συστήματα επεξεργασίας δεδομένων
6. παραδοσιακά οικονομικά αδικήματα με την χρήση επεξεργασίας δεδομένων.

(Γερμανία, 1986)

Κατηγοριοποίηση του Wasik(Λάζος, 2001) : απάτες και ηλεκτρονικές κλοπές:

1. παραπλάνηση
2. κλοπή
3. ψευδή λογιστικά και πλαστογραφία
4. συνωμοσία για εξαπάτηση
5. μη εξουσιοδοτημένη αφαίρεση πληροφοριών
6. εμπορικά μυστικά
7. δικαιώματα αντιγραφής.

(Μ. Βρετανία, 1991)

Ήδη κατά την πενταετία, που ακολούθησε μεταξύ των παραπάνω δημοσιεύσεων το Hacking αυτονομήθηκε ως κατηγορία ηλεκτρονικού εγκλήματος. Επίσης η κατηγορία της ηλεκτρονικής δολιοφθοράς διερευνήθηκε και δεν περιορίζεται στο οικονομικό στοιχείο.

7.3 ΑΠΑΤΗ ΜΕΣΩ ΥΠΟΛΟΓΙΣΤΗ

Στο πλαίσιο των ηλεκτρονικών οικονομικών εγκλημάτων, η απάτη μέσω υπολογιστή περιλαμβάνει την παραποίηση κάποιων δεδομένων ή πληροφοριών, που φιλοξενούνται στις βάσεις δεδομένων ή σε προγράμματα με σκοπό το οικονομικό κέρδος.

Τι αφορά;
Αφορά κυρίως στην κλοπή, διαγραφή, αλλοίωση ή προσθήκη δεδομένων ή πληροφοριών με σκοπό το βραχυπρόθεσμο ή μακροπρόθεσμο οικονομικό κέρδος.

Στόχος της απάτης μέσω υπολογιστή:
Κεντρικό αντικείμενο - στόχος της συγκεκριμένης απάτης είναι τα δεδομένα που φιλοξενούνται στον υπολογιστή και αφορούν σε οικονομικά μεγέθη.

Από τη σκοπιά του ποινικού δικαίου κατά τη χρήση του Διαδικτύου είναι δυνατό να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσω τέλεσης της κοινής απάτης (ΠΚ 386) αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή στο πρόγραμμα και στα δεδομένα του (ΠΚ 386Α). Στην Ευρωπαϊκή ένωση ισχύει η Απόφαση-πλαίσιο του Συμβουλίου με αριθμό 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών .

Κατηγορίες απάτης μέσω υπολογιστή Λάζος, 2001):

1. παραποίηση λογιστικών λογαριασμών
2. παραποιημένη εφαρμογή ηλεκτρονικών πληρωμών
3. προσβολή των τηλεφωνικών δικτύων
4. ηλεκτρονική κατασκοπεία

Πιο αναλυτικά:

Για τις απάτες που γίνονται μέσω του Διαδικτύου.

Οι μορφές των πλέον διαδεδομένων απατών που τελούνται τα τελευταία χρόνια, μέσω του Διαδικτύου σύμφωνα με τον Τσουραμάνη (Τσουραμάνης, 2005) είναι οι ακόλουθες:

1. Η απάτη με τα Νιγηριανά μηνύματα του ηλεκτρονικού ταχυδρομείου (Nigerian e-mail fraud).
2. Η απάτη με το phishing mail (ηλεκτρονικό μήνυμα "ψαρέματος").
3. Άλλος ένας ακόμη τρόπος ψηφιακής απάτης είναι εκείνος που αφορά τη λήψη από το υποψήφιο θύμα ενός e-mail ή ενός Pop-up window που του εμφανίζεται κατά τη διάρκεια ττης περιήγησής του στον Ιστό με το οποίο του γίνεται γνωστό ότι κέρδισε ένα μεγάλο χρηματικό ποσό κάποια κλήρωση.
4. Η απάτη με τα sites – "μαϊμούδες".
5. Η απάτη με τις επιταγές.

8^{Ο} ΚΕΦΑΛΑΙΟ

ΜΕΤΡΗΣΗ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ

ΕΙΣΑΓΩΓΗ 8^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Στο παρών κεφάλαιο θα ασχοληθούμε με τα προβλήματα κατά την συλλογή στατιστικών δεδομένων, με την διαδικτυακή έρευνα, με την ελληνική αστυνομική πραγματικότητα, τον τρόπο εντοπισμού ενός ηλεκτρονικού εγκληματία στο διαδίκτυο και τέλος θα αναφέρουμε και κάποια νομικά ζητήματα, που τίθενται.

8.1 ΠΡΟΒΛΗΜΑΤΑ ΚΑΤΑ ΤΗ ΣΥΛΛΟΓΗ ΣΤΑΤΙΣΤΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Τα στατιστικά στοιχεία που διαθέτουμε για το ηλεκτρονικό έγκλημα και προέρχονται από τις διωκτικές αρχές, δεν μπορούν να χαρακτηριστούν αξιόπιστα. Υπάρχουν δύο βασικά εμπόδια που δεν μας επιτρέπουν να έχουμε ακριβή στοιχεία σύμφωνα με τον Kabay (Βλαχόπουλος, 2007):

- Η δυσκολία εντοπισμού του ηλεκτρονικού εγκλήματος: Το πρόβλημα της λεγόμενης «κρυφής» εγκληματικότητας, που το συναντάμε σε όλες τις μορφές εγκλημάτων, παρουσιάζει μεγάλη συχνότητα στην περίπτωση των ηλεκτρονικών εγκλημάτων. Ο όρος αναφέρεται σε εγκλήματα που έχουν τελεσθεί, χωρίς να το έχουν αντιληφθεί τα θύματα.
- Η διστακτικότητα αναφοράς από τα θύματα: Ακόμη και αν το θύμα αντιληφθεί μια ηλεκτρονική επίθεση εναντίον του, διστάζει να την αναφέρει στις διωκτικές αρχές, με αποτέλεσμα, να μην είναι δυνατή η συστηματική συλλογή στατιστικών στοιχείων. Οι λόγοι για τη μη αναφορά των ηλεκτρονικών εγκλημάτων ποικίλλουν με κυρίαρχο το φόβο της εταιρείας, που δέχθηκε την επίθεση, ότι αν αποκαλυφθεί το γεγονός θα έχει αρνητικές συνέπειες στην εικόνα της προς τους πελάτες της.

Εκτιμάται ότι τα στατιστικά στοιχεία που διαθέτουμε από τις διωκτικές αρχές, αντιπροσωπεύουν μόνο το 10% της πραγματικής έκτασης του φαινομένου. Για το λόγο αυτό, η μέτρηση του ηλεκτρονικού εγκλήματος, γίνεται με εναλλακτικές μεθόδους, όπως συνεντεύξεις και έρευνες σε συγκεκριμένες κατηγορίες ατόμων.

8.2 ΈΡΕΥΝΕΣ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΩΝ

Διάρκεια της διαδικτυακής έρευνας:

Η έρευνα των Ηλεκτρονικών Εγκλημάτων είναι αρκετά δύσκολη και ιδιαίτερα χρονοβόρος η διαδικασία του εντοπισμού των «ηλεκτρονικών ιχνών». Μία έρευνα μπορεί να διαρκέσει από ένα μήνα έως και δύο χρόνια. Ο λόγος της μεγάλης διάρκειας είναι διότι

οι χρήστες του Διαδικτύου που ερευνώνται και που έχουν καταγγελθεί στην υπηρεσία μας ότι έχουν διαπράξει μια αξιόποινη πράξη λαμβάνουν διάφορα διαδικτυακά μέτρα προστασίας, έτσι ώστε ο εντοπισμός του να καθίσταται αρκετά δύσκολος.

Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του «ηλεκτρονικού ίχνους» του δράστη, το οποίο για κάθε χρήστη του Ιντερνέτ είναι μοναδικό, και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο. Η λεγομένη ηλεκτρονική απόδειξη (electronic evidence) δεν ταυτίζεται με τα παραδοσιακά αποδεικτικά μέσα. Τα τελευταία, έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα, τα ηλεκτρονικά αποδεικτικά μέσα είναι ψηφιακά!

8.3 Η ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ:

Στην Ελληνική Αστυνομία δεν υπάρχει ακόμα ειδικό Τμήμα, που να ερευνά αποκλειστικά το έγκλημα στον κυβερνοχώρο. Το ερευνούμενο έγκλημα εξετάζεται από το αντίστοιχο ``συμβατικό`` τμήμα της Αστυνομίας. Έτσι η παιδική πορνογραφία ερευνάται από το τμήμα Ανηλίκων, ενώ μια ανθρωποκτονία θα ερευνηθεί από το Τμήμα ανθρωποκτονιών. Επειδή κατά κανόνα τα περισσότερα εγκλήματα του κυβερνοχώρου έχουν οικονομικό αντικείμενο, το Τμήμα Οικονομικού Εγκλήματος, θεωρείται πιο εξειδικευμένο στο σχετικό αντικείμενο. Έχει μάλιστα συσταθεί ειδική ομάδα αντιμετωπίσεως του Ηλεκτρονικού Οικονομικού Εγκλήματος, το οποίο στελεχώνεται από εκπαιδευμένους στο ηλεκτρονικό έγκλημα αστυνομικούς.

Σε κάθε περίπτωση όμως την σχετική έρευνα συνδράμει με τις ειδικές της γνώσεις η Διεύθυνση Εγκληματολογικών Ερευνών (Δ.Ε.Ε.) και ειδικότερα το εργαστήριο γραφολογίας, στο οποίο υπάγεται και λειτουργεί ο Τομέας Ανάλυσης Ψηφιακών δεδομένων. Ο Τομέας αυτός δημιουργήθηκε το 1992, στελεχώνεται δε από ειδικά εκπαιδευμένους αστυνομικούς, με τεχνογνωσία στην εξέταση λογισμικού κατασχεθέντων ηλεκτρονικών υπολογιστών, στο ``σπάσιμο`` κωδίκων κλπ Επίσης στο Υπουργείο Δημοσίας Τάξεως λειτουργεί η Διεύθυνση Πληροφορικής, η οποία όμως δεν έχει σχέση με την έρευνα των εγκλημάτων του κυβερνοχώρου. Η Διεύθυνση αυτή υπάγεται στον κλάδο Διοικητικής Υποστήριξης του Υ.Δ.Τ. και έχει ως αρμοδιότητα την ανάπτυξη και την τεχνική υποστήριξη στον τομέα της πληροφορικής, για όλες τις υπηρεσίες της Αστυνομίας .

8.4 Ο ΕΝΤΟΠΙΣΜΟΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Αρχεία καταγραφής (log files)

Τα αρχεία καταγραφής διαδραματίζουν σημαντικό ρόλο, καθώς σε αυτά αποθηκεύονται πληροφορίες, που αφορούν τη λειτουργία του συστήματος. Στα λειτουργικά συστήματα της οικογένειας Windows, υπάρχουν τρία βασικά είδη αρχείων καταγραφής: Application log, System log και Security log.162

Ο εντοπισμός όλων των πληροφοριών, που αποθηκεύονται τα αρχεία καταγραφής, μπορεί να πραγματοποιηθεί μέσω της κονσόλας διαχείρισης των Windows.

Η χρησιμότητα των αρχείων καταγραφής των Windows μεγιστοποιείται, όταν έχουν ενεργοποιηθεί συγκεκριμένες πολιτικές ομάδων (group policies). Τα security logs είναι κενά, εάν δεν έχει οριστεί συγκεκριμένη πολιτική ασφάλειας για μια ομάδα χρηστών. Η ευθύνη ορισμού πολιτικών ασφάλειας ανήκει στον διαχειριστή και υπεύθυνο ασφαλείας ενός συστήματος.

Από τα αρχεία καταγραφής, ο ερευνητής του ηλεκτρονικού εγκλήματος μπορεί να διαπιστώσει εάν χρησιμοποιήθηκε συγκεκριμένη εφαρμογή από έναν χρήστη, εάν κάποιος μη εξουσιοδοτημένος χρήστης απέκτησε πρόσβαση στο σύστημα, εάν χρησιμοποιήθηκε κάποια περιφερειακή συσκευή και πλήθος άλλων σημαντικών πληροφοριών.

Εκτός από το λειτουργικό σύστημα, αρχεία καταγραφής δημιουργούνται και από άλλες εφαρμογές. Το firewall, ως βασικό εργαλείο, που ελέγχει την κίνηση από και προς ένα προστατευόμενο δίκτυο ή υπολογιστή, αποθηκεύει σημαντικές πληροφορίες στα αρχεία καταγραφής του. Οι πληροφορίες των αρχείων αυτών, αποτελούν σημαντικό προανακριτικό αλλά και αποδεικτικό υλικό, σε περιπτώσεις μη εξουσιοδοτημένης πρόσβασης σε δίκτυα.

Εντοπισμός ονόματος χώρου και διεύθυνσης IP

Ο εντοπισμός της διεύθυνσης IP, αποτελεί βασική ενέργεια των διωκτικών αρχών για την εξιχνίαση πολλών υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε ένα δίκτυο. Στις επιθέσεις αυτές οι εισβολείς χρησιμοποιούν πλαστές διευθύνσεις IP, προκειμένου να παραπλανήσουν τις διωκτικές αρχές. Κάθε διεύθυνση στο Διαδίκτυο έχει έναν αντίστοιχο αριθμό IP. Το σύστημα, που έχει αναλάβει τη διατήρηση των αντιστοιχιών μεταξύ μιας ηλεκτρονικής διεύθυνσης και του αντίστοιχου IP, είναι το DNS (Domain Name System). Κατά την εκδήλωση μιας επίθεσης, ο επιτιθέμενος πλαστογραφεί τη διεύθυνσή του για να φαίνεται ότι είναι νόμιμος χρήστης, δεν πλαστογραφεί όμως (ή δεν μπορεί να πλαστογραφήσει) τον αντίστοιχο αριθμό IP. Συνήθως, συσκευές, όπως τα firewalls, έχουν τη δυνατότητα να ελέγχουν αν μια διεύθυνση είναι αληθινή ή όχι και ανάλογα να επιτρέπουν ή να απαγορεύουν την πρόσβαση ενός χρήστη. Εφόσον το firewall δεν έχει ρυθμιστεί κατάλληλα, ο ερευνητής θα κληθεί να ελέγξει τις διευθύνσεις όλων όσοι απέκτησαν πρόσβαση, προκειμένου να εξακριβώσει από ποιον προήλθε η κακόβουλη επίθεση. Η εργασία αυτή μπορεί να διεκπεραιωθεί με διάφορα εργαλεία λογισμικού, τα οποία ελέγχουν αν οι ηλεκτρονικές διευθύνσεις, αναλογούν σε σωστούς αριθμούς IP. Επίσης, υπάρχουν και δικτυακοί τόποι που επιτελούν on-line την εργασία αυτή. Για παράδειγμα στο www.dnsreport.com μπορεί να δοθεί μια ηλεκτρονική διεύθυνση ή διεύθυνση ηλεκτρονικού ταχυδρομείου και να ληφθούν διάφορες πληροφορίες για αυτή, όπως το IP, ο server κ.ά.
(Βλαχόπουλος, 2007)

8.5 ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ

Η διερεύνηση μιας υπόθεσης ηλεκτρονικού εγκλήματος εκτός από τεχνικής απόψεως πρέπει να είναι και σύννομη, συμβαδίζοντας με τους ισχύοντες σε κάθε χώρα νόμους και

κανονισμούς. Η Ηλεκτρονική Εγκληματολογία, ως μια σχετικά νέα επιστήμη, έχει προβληματίσει τους νομικούς κύκλους για το κατά πόσο αξιόπιστη είναι και σε ποιο βαθμό οι ψηφιακές αποδείξεις μπορούν να τύχουν εφαρμογής σε μια δίκη. Οι νομικοί προβληματισμοί σχετίζονται με την έρευνα και κατάσχεση (search and seizure) ψηφιακών αποδείξεων, το κατά πόσο οι γνώσεις ενός ερευνητή είναι επαρκείς για τη διεκπεραίωση μιας έρευνας σε έναν Η/Υ και τέλος, αν η ανάλυση και διατήρηση των αποδείξεων έγινε σύμφωνα με τις προβλεπόμενες διαδικασίες.

Η έρευνα και κατάσχεση πληροφοριών είναι η πρώτη διαδικασία που αμφισβητείται σε μια δίκη. Σύμφωνα με το Ελληνικό Δίκαιο, μια έρευνα μπορεί να διενεργηθεί όταν διεξάγεται ανάκριση για κακούργημα ή πλημμέλημα και μόνο με το μέσο αυτό μπορεί να κατορθωθεί ή να διευκολυνθεί η βεβαίωση του εγκλήματος, η ανακάλυψη και σύλληψη των δραστών ή τέλος η βεβαίωση και αποκατάσταση της ζημιάς που προκλήθηκε. Επιπλέον, κατά τη διεξαγωγή μιας έρευνας θα πρέπει να τηρούνται και οι βασικές αρχές της αναγκαίας αναλογίας, της αναγκαιότητας και της απαγορεύσεως του υπέρμετρου. Επειδή δεν υφίσταται συγκεκριμένο νομοθετικό πλαίσιο για τις διαδικτυακές έρευνες, οι ανωτέρω διατάξεις εφαρμόζονται κατά αναλογία και σε περιπτώσεις ηλεκτρονικών εγκλημάτων. Επομένως, μια έρευνα στην οποία δεν έχουν τηρηθεί οι προβλεπόμενες προϋποθέσεις, θα επηρεάσει την αποδεικτικότητα των στοιχείων που συλλέχθηκαν.

Κατά τη διεξαγωγή μιας έρευνας, το βασικό αγαθό, που διακυβεύεται, είναι η ιδιωτικότητα του ατόμου. Το Αμερικανικό Σύνταγμα απαιτεί την ύπαρξη εντάλματος για τη διεξαγωγή μιας έρευνας, το οποίο εκδίδεται αν υπάρχει πιθανή αιτία (probable cause), ότι διαπράχθηκε ένα έγκλημα. Το ένταλμα θα πρέπει να καθορίζει, επακριβώς, το μέρος και τα αντικείμενα που μπορούν να ερευνηθούν. Για παράδειγμα, εάν η πιθανή αιτία υποδεικνύει ότι τα αποδεικτικά στοιχεία είναι αποθηκευμένα σε ένα CD, η αστυνομία δεν έχει το δικαίωμα να ερευνήσει κάθε υπολογιστή που υπάρχει στο χώρο για την εύρεση συμπληρωματικών στοιχείων. Αν το πράξει, έστω και αν βρει επιπρόσθετα αποδεικτικά στοιχεία, αυτά δεν θα έχουν αποδεικτική αξία στο δικαστήριο, γιατί παραβιάστηκε το ένταλμα (Wegman, 2004).

Το δεύτερο νομικό ζήτημα, που σχετίζεται με υποθέσεις που εμπλέκονται αποδεικτικά στοιχεία σε ψηφιακή μορφή, είναι το κατά πόσο τα προσόντα ενός επιστημονικού ερευνητή επαρκούν για τη διεκπεραίωση μιας ηλεκτρονικής έρευνας. Ο μεγαλύτερος προβληματισμός έγκειται στα χρησιμοποιούμενα από τον ερευνητή εργαλεία λογισμικού. Ο ερευνητής, απλά, γνωρίζει τη χρήση ενός εργαλείου λογισμικού. Δεν μπορεί να έχει πρόσβαση στον πηγαίο κώδικα και έτσι δεν γνωρίζει τι εργασίες επιτελεί το λογισμικό. Πώς λοιπόν μπορεί να βεβαιώσει ότι τα ψηφιακά δεδομένα, που συλλέχθηκαν, αποδεικνύουν την ενοχή ή την αθωότητα του κατηγορουμένου; Έως σήμερα, δεν υπάρχει απόφαση δικαστηρίου που να απέρριψε την επιστημονική άποψη ενός ερευνητή, τέτοιο ενδεχόμενο, όμως, δεν αποκλείεται να συμβεί στο μέλλον από τη στιγμή που τα εργαλεία λογισμικού εξελίσσονται με ραγδαίους ρυθμούς και γίνονται όλο και πιο πολύπλοκα.

Το τρίτο και τελευταίο ζήτημα αφορά την ανάλυση και διατήρηση των αποδεικτικών στοιχείων. Είναι κοινή πρακτική των διωκτικών αρχών, η αντιγραφή του μέσου αποθήκευσης, που θα εξεταστεί, (π.χ. ενός σκληρού δίσκου) δημιουργώντας ένα ακριβές αντίγραφο (bit-stream image), του πρωτοτύπου. Τα δικαστήρια έχουν αποδεχθεί, ότι εφόσον το αντίγραφο είναι ακριβές, τότε θεωρείται γνήσιο. Ωστόσο, πρέπει να λαμβάνεται κάθε απαραίτητο μέτρο για την άρτια διατήρησή του. Οι ψηφιακές πληροφορίες μπορούν να επηρεαστούν από μαγνητικά πεδία, καιρικές συνθήκες κ.ά. Για

παράδειγμα, στην υπόθεση Ohio v. Cook,169 ο κατηγορούμενος προέβαλε μια σειρά από ισχυρισμούς έναντι της μη ορθής συλλογής και διατήρησης των ψηφιακών αποδείξεων, που οδήγησαν στην αλλοίωσή τους, όπως η μη τοποθέτηση του σκληρού δίσκου που αφαιρέθηκε σε αντιστατική θήκη. Το δικαστήριο λαμβάνοντας υπόψη τα παραπάνω, καθώς και μια σειρά από άλλες παραλήψεις των διωκτικών αρχών κατά τη διατήρηση των ψηφιακών στοιχείων, έκρινε τον κατηγορούμενο αθώο λόγω αμφιβολιών.
(Βλαχόπουλος, 2007)

8.6 ΣΥΜΠΕΡΑΣΜΑΤΑ 8^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Ο βαθμός εισχώρησης του φαινομένου του ηλεκτρονικού εγκλήματος στη σύγχρονη κοινωνία, αποτελεί αντικείμενο μελέτης πολλών επιστημονικών κλάδων. Στην Ελλάδα, ο κίνδυνος από ηλεκτρονικές επιθέσεις κρίνεται σχετικά μικρός, όμως σε άλλες χώρες (π.χ. ΗΠΑ), αποτελεί μια καθημερινή πραγματικότητα. Δυστυχώς, δεν μπορούμε να έχουμε επαρκή εικόνα για το βαθμό εξάπλωσης του ηλεκτρονικού εγκλήματος, καθώς η συλλογή στατιστικών στοιχείων είναι δυσκολότερη από κάθε άλλη μορφή εγκλήματος.

9^{Ο} ΚΕΦΑΛΑΙΟ

ΑΣΤΥΝΟΜΙΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

ΕΙΣΑΓΩΓΗ 9^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Σε αυτό το κεφάλαιο θα αναφερθούμε στην αστυνομία σε σχέση με το ηλεκτρονικό έγκλημα. Θα αναφέρουμε τις διάφορες υπηρεσίες, που έχουν δημιουργηθεί παγκόσμια, αλλά και στην κατάσταση, που επικρατεί στην Ελλάδα.

9.1 Η ΣΤΑΣΗ ΤΗΣ ΑΣΤΥΝΟΜΙΑΣ ΣΕ ΠΑΓΚΟΣΜΙΟ ΕΠΙΠΕΔΟ

Οι πρώτες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος, ιδρύθηκαν στις Ηνωμένες Πολιτείες της Αμερικής, καθότι από εκεί ξεκίνησε το hacking, στα μέσα της δεκαετίας του '70 και αναπτύχθηκε τόσο η τεχνολογία των ηλεκτρονικών υπολογιστών όσο και το Διαδίκτυο. Σήμερα, στις Η.Π.Α. λειτουργούν υπηρεσίες αντιμετώπισης και δίωξης του ηλεκτρονικού εγκλήματος σε κάθε πολιτεία, οι οποίες έχουν τοπική αρμοδιότητα. Οι απειλές, όμως, που προβάλλουν από το οργανωμένο έγκλημα, μέσω του κυβερνοχώρου, οδήγησαν στη σύσταση της US-CERT170 (United States Computer Emergency Readness Team) μιας εθνικής υπηρεσίας που φέρει την κύρια ευθύνη για την ασφάλεια των Η.Π.Α. από επιθέσεις που μπορεί να προκύψουν από τον κυβερνοχώρο. Η US-CERT αποτελεί το επιχειρησιακό κομμάτι της NCSD (National Cyber Security Division), η οποία με τη σειρά

της υπάγεται στο Υπουργείο Εσωτερικών.171 Οι κύριες αρμοδιότητες της US-CERT είναι:

- Η ανάλυση των πιθανών διαδικτυακών απειλών και ευπαθειών και η καταβολή προσπαθειών για τον περιορισμό τους.
- Η ενημέρωση των συναρμόδιων υπηρεσιών για πιθανές δικτυακές απειλές.
- Ο συντονισμός των ενεργειών αντιμετώπισης συμβάντων σχετικών με το Διαδίκτυο.

Σε επίπεδο εξέτασης ψηφιακών τεκμηρίων, το Ομοσπονδιακό Γραφείο Ερευνών (Federal Bureau Of Investigations – FBI) διαθέτει το πιο σύγχρονο εργαστήριο στον κόσμο. Το εξειδικευμένο προσωπικό της Computer Analysis and Response Team, εξοπλισμένο με τα απαιτούμενα εργαλεία υλικού και λογισμικού, εξετάζει πάσης φύσεως ψηφιακά δεδομένα και υπολογιστικά συστήματα, έχοντας τη δυνατότητα για ανάκτηση και ανάλυση αρχείων, σπάσιμο κωδικών, προσδιορισμό του χρόνου και σειράς δημιουργίας των αρχείων κ.ά.

Στην Αγγλία έχει ιδρυθεί Μονάδα Ηλεκτρονικού Εγκλήματος στη Μητροπολιτική Αστυνομία, για την αντιμετώπιση των απειλών με ηλεκτρονικούς υπολογιστές, που οριοθετούνται από το ισχύον νομικό πλαίσιο και, ειδικότερα, την Computer Misuse Act 1990. Επίσης, στον Καναδά έχει ιδρυθεί η Integrated Technological Crime Unit στη Royal Canadian Mounted Police.

Στην Αυστραλία έχει συσταθεί το Australian High Tech Crime Centre176 υπαγόμενο στην Ομοσπονδιακή Αστυνομία. Σκοπός του είναι ο συντονισμός των εθνικών προσπαθειών για την πάταξη του ηλεκτρονικού εγκλήματος, καθότι αναγνωρίζει ότι, η αντιμετώπισή του δυσχεραίνεται από πλήθος εμποδίων νομικών και μη. Για το σκοπό αυτό συνεργάζεται και με άλλες υπηρεσίες στον κόσμο, με τις οποίες μπορεί από κοινού να ερευνήσουν υποθέσεις παράνομης δραστηριότητας στο Διαδίκτυο και να ανταλλάξουν τεχνογνωσία.
(Βλαχόπουλος, 2007)

9.2 ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ

Η αυξανόμενη διάδοση του Διαδικτύου στη χώρα μας, η χρήση του για διεκπεραίωση καθημερινών εργασιών αλλά και η παροχή από κρατικούς και μη φορείς ηλεκτρονικών υπηρεσιών, έχουν οδηγήσει στην αλματώδη αύξηση των υποθέσεων που σχετίζονται με το ηλεκτρονικό έγκλημα. Ειδικότερα:

Ιανουάριος 2006
Ένας 35χρονος κατηγορείται ότι σε συνεργασία με ουκρανικά κυκλώματα εφάρμοζε την απάτη του ψαρέματος (phishing), στο Διαδίκτυο. Έστελνε παραπλανητικά e-mail και μάζευε στοιχεία, με τα οποία διεκπεραίωναν ηλεκτρονικές συναλλαγές πελάτες ελληνικών τραπεζών, μεταξύ αυτών και της Εθνικής. Ένας 67χρονος συνταξιούχος στρατιωτικός και ένας 50χρονος Νιγηριανός, κάτοικος Κύπρου, είχαν στήσει Λοταρία μέσω ιστοσελίδας και e-mails, που υποσχόταν μυθικά ποσά με την προϋπόθεση ότι, οι νικητές θα πλήρωναν τους φόρους. Μέχτι να συλληφθούν είχαν αποσπάσει από ανυποψίαστους χρήστες πάνω από 3,5 εκατομμύρια ευρώ.

Οκτώβριος 2005

Σύλληψη ενός 40χρονου Δανού, ο οποίος έστελνε ηλεκτρονικά μηνύματα, υφάρπαζε προσωπικά δεδομένα και στη συνέχεια αποσπούσε μεγάλα χρηματικά ποσά από τραπεζικούς λογαριασμούς.

Ιούλιος 2005
Εξιχνιάζεται η πρώτη υπόθεση παράνομης κατασκευής όπλων, που διακινούνταν μέσω Διαδικτύου. Οι πωλήσεις γίνονταν μέσω ιστοσελίδας γνωστής εταιρίας δημοπρασιών και τα όπλα, πιστά αντίγραφα των αυθεντικών, παραδίδονταν στους ενδιαφερόμενους μέσω εταιρίας ταχυμεταφορών.

Σεπτέμβριος 2004
Ένας 27χρονος ομολογεί, ότι έβγαζε κρυφά φωτογραφίες μικρών παιδιών, που εντόπιζε στα αποδυτήρια παιδικών κατασκηνώσεων, ποδοσφαιρικών ομάδων και διαφόρων σχολείων, τις οποίες, στη συνέχεια, διακινούσε σε ξένες ιστοσελίδες αντί αμοιβής. Τον ίδιο μήνα συνελήφθησαν δύο 32χρονοι, οι οποίοι διείσδυσαν στα υπολογιστικά προγράμματα ελληνικής τράπεζας και μετέφεραν χρήματα στους δικούς τους λογαριασμούς.

Η αντιμετώπιση των υποθέσεων ηλεκτρονικού εγκλήματος από την Ελληνική Αστυνομία, ουσιαστικά, αρχίζει με την ίδρυση του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος το 2004. Έως τότε, οι υποθέσεις που σχετίζονταν καθ' οποιονδήποτε τρόπο με ηλεκτρονικούς υπολογιστές αντιμετωπίζονταν από το Τμήμα Δίωξης Οικονομικού Εγκλήματος.

Το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλεια Αττικής ιδρύθηκε με το Π.Δ. 100/2004, έχοντας αρμοδιότητα τη δίωξη των εγκλημάτων, που διαπράττονται στο Διαδίκτυο ή με τη χρήση αυτού εντός της περιοχής δικαιοδοσίας της Διεύθυνσης Ασφάλειας Αττικής, καθώς και την επί 24ώρου βάσεως παρακολούθηση του Διαδικτύου, προς διαπίστωση εγκληματικών πράξεων, που τελούνται στη χώρα και τη διαβίβαση όλων των απαραίτητων συναφών στοιχείων στις αρμόδιες υπηρεσίες.

Επίσης, με το Π.Δ. 48/2006 ιδρύθηκε Τμήμα Δίωξης Ηλεκτρονικού Εγκλήαματος στην Υποδιεύθυνση Δίωξης Οικονομικού Εγκλήματος της Γενικής Αστυνομικής Διεύθυνσης Θεσσαλονίκης, με αρμοδιότητες την εντός της περιοχής δικαιοδοσίας της Διεύθυνσης Ασφαλείας Θεσσαλονίκης, δίωξη των εγκλημάτων που διαπράττονται στο Διαδίκτυο ή με τη χρήση αυτού.

Οι υπηρεσίες αυτές, αν και βρίσκονται στο αρχικό στάδιο σύστασης και λειτουργίας και στερούνται τόσο του απαραίτητου εξοπλισμού (υλικού και λογισμικού) όσο και εξειδικευμένου προσωπικού, έχουν να επιδείξουν σημαντικό έργο στην καταπολέμηση του ηλεκτρονικού εγκλήματος

Η πρώτη υπόθεση που απασχόλησε το εργαστήριο ήταν το 1995. από εκεί και έπειτα, οι υποθέσεις πολλαπλασιάστηκαν με γεωμετρικούς ρυθμούς, όπως φαίνεται και από το παραπάνω γράφημα. Σήμερα, το εργαστήριο διαθέτει εξειδικευμένο προσωπικό και τεχνικά μέσα για τη διεκπεραίωση απαιτητικών εργασιών.

9.3 ΣΥΜΠΕΡΑΣΜΑΤΑ 9^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Η αντιμετώπιση του ηλεκτρονικού εγκλήματος, από τις υπηρεσίες επιβολής του νόμου και ιδιαίτερα την αστυνομία, αποτελεί πρωταρχικό ζήτημα. Ο παραδοσιακός τρόπος προσεγγίσεως του εγκλήματος, δηλαδή της περιγραφής του δράστη με την κατάθεση του θύματος, της συλλογής πληροφοριών από πληροφοριοδότες, τη διεξαγωγή έρευνας, κατάσχεσης κ.λπ. δεν ισχύει στον κυβερνοχώρο. Για την έρευνα ηλεκτρονικών εγκλημάτων, απαιτούνται εξειδικευμένες αστυνομικές υπηρεσίες με εκπαιδευμένο προσωπικό και σύγχρονα τεχνικά μέσα.

10ο ΚΕΦΑΛΑΙΟ

ΝΟΜΟΘΕΣΙΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

ΕΙΣΑΓΩΓΗ 10^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Οι νομοθετικές ρυθμίσεις που αφορούν τα ψηφιακά εγκλήματα παρουσιάζουν αδυναμίες, τόσο στην Ελλάδα όσο και σε άλλες χώρες. Με δεδομένο ότι η ψηφιακή εγκληματικότητα αποτελεί δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, παρουσιάζει προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. Επιπλέον ο νομοθέτης είναι αναγκασμένος να ενημερώνεται συνεχώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθεί με τον τρόπο διάπραξης των σχετικών αξιόποινων πράξεων.

Οι διώξεις των ψηφιακών εγκλημάτων κινούνται σε χαμηλά επίπεδα, εφόσον και οι καταγγελίες είναι περιορισμένες. Γενικά, θα πρέπει να παρατηρήσουμε πως οι επιχειρήσεις – κυρίως - αποφεύγουν να καταγγείλουν παραβάσεις, γιατί φοβούνται επανάληψη των αδικημάτων και πλήγμα στη φήμη τους. Επίσης, θέλουν να αποφεύγουν τα υψηλά δικαστικά έξοδα και το γεγονός ότι δεν γίνεται εύκολη χρηματική και αξιακή αποτίμηση των οικονομικών ζημιών που τελικά υφίστανται. Οι δυσκολίες που αντιμετωπίζουν οι αστυνομικές και οι δικαστικές αρχές στον εντοπισμό και την περαιτέρω δίωξη, σχετίζονται, κυρίως, με το συνήθως, χαμηλό επίπεδο πληροφορικής κατάρτισης των στελεχών τους.

Επίσης απαιτείται συνήθως αρκετός χρόνος, για να διευκρινιστούν οι υποθέσεις, που είναι συνήθως πολύπλοκες και απαιτούν συνεργασία και με άλλες υπηρεσίες. Πολλές φορές οι δικαστές υποβαθμίζουν τη σημασία των ψηφιακών εγκλημάτων, με τη δικαιολογία ότι το σύστημα της ποινικής δικαιοσύνης δεν θα πρέπει να επιβαρυνθεί με τέτοιου είδους εγκληματίες, εφόσον η ποινή που τους επιβάλλεται, δεν είναι ικανή να τους αποτρέψει από την επανάληψη της πράξης.

Ο διεθνής εξάλλου χαρακτήρας του συγκεκριμένων εγκλημάτων δίνει τη δυνατότητα στους δράστες να έχουν γρήγορη πρόσβαση στα στοιχεία, αλλά και εύκολη προσβολή των δεδομένων στα συστήματα Η/Υ παγκοσμίως. Βασικό στοιχείο που εμποδίζει την διωκτική προσπάθεια είναι η διασύνδεση των πιο επικίνδυνων από τους ψηφιακούς εγκληματίες με το οργανωμένο έγκλημα. Θα πρέπει επιπρόσθετα να σημειώσουμε πως τα ψηφιακά εγκλήματα διακρίνονται και για: το μεγάλο όγκο των δεδομένων τους, τον μη οπτικό χαρακτήρα των αποδείξεων, τη δυνατότητα «μεταμφίεσης» τους καθώς και την ταχεία εξαφάνιση των αποδεικτικών στοιχείων από τη μεριά των εγκληματιών.

Ο τεράστιος αριθμός δεδομένων που είναι καταχωρημένα στο Διαδίκτυο και η παγκοσμιότητά του αποτελούν εμπόδιο στην αντιμετώπιση αξιόποινων πράξεων που διαπράττονται σε αυτό. Επιπλέον, υπάρχει το πρόβλημα της δικαιοδοσίας, αφού ο καθένας όπου και αν βρίσκεται μπορεί να έχει πρόσβαση σε οποιαδήποτε πληροφορία θελήσει. Είναι δύσκολο να ορισθεί ο τόπος τέλεσης του αδικήματος και η αρμοδιότητα του δικαστηρίου που θα πρέπει να εκδικάσει την υπόθεση. Στην Ελλάδα και την Ευρώπη κυριαρχεί η θεωρία του βαρύνοντος τόπου, δηλαδή ο τόπος του αδικήματος εντοπίζεται

στο κράτος που εκδηλώθηκε το έγκλημα. Και σε αυτό όμως, παρουσιάζονται προβλήματα, εφόσον είναι δύσκολο να καθοριστεί ο τόπος τέλεσης ενός διαδικτυακού αδικήματος.

Με δεδομένη όμως, την αύξηση των μορφών των ψηφιακών εγκλημάτων η ειδική και εξειδικευμένη νομοθετική αντιμετώπισή τους θεωρείται επιβεβλημένη. Για το λόγο αυτό σχεδόν όλα τα κράτη του κόσμου έχουν θεσπίσει νομοθετικές διατάξεις, σχετικές με τα ψηφιακά εγκλήματα. Ωστόσο, το νομοθετικό πλαίσιο που να αφορά ειδικότερα το ζήτημα είναι σε αρκετές περιπτώσεις εξαιρετικά ελλιπές και συνήθως καλύπτεται από γενικότερες διατάξεις.

Τα τελευταία χρόνια έχουν πραγματοποιηθεί Συνέδρια τόσο στην Ελλάδα, όσο και παγκοσμίως, με σκοπό τη συζήτηση και τη λήψη αποφάσεων, σχετικά με το ζήτημα αυτό. Συγκεκριμένα, πραγματοποιήθηκε Συνέδριο για το Ηλεκτρονικό Έγκλημα στη Βουδαπέστη και υπογράφτηκε συνθήκη, στις 23/11/2001, στην οποία εντάσσονται όλα τα σχετικά συμπεράσματα. Τη Συνθήκη υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας. Αυτή περιλαμβάνει ορισμούς και ρυθμίσεις για όλες τις μορφές των ψηφιακών εγκλημάτων και είναι γνωστή ως "Convention on Cyber Crime 2001".

Στην Ελλάδα δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Internet και ειδικότερα να ρυθμίζει τη συμπεριφορά των χρηστών του διαδικτύου από την πλευρά του ποινικού δικαίου. Ο νόμος 1805/1988 αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές. Συγκεκριμένα: Με το άρθρο 3 του νόμου αυτού προσετέθησαν τρία νέα άρθρα στον Ποινικό Κώδικα, τα 370Β, 370Γ και 386Α.

10.1 ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΝΟΜΟΘΕΣΙΑΣ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Το ηλεκτρονικό έγκλημα είναι μια νέα μορφή εγκλήματος, που οριοθετείται από δύο βασικά στοιχεία: τους ηλεκτρονικούς υπολογιστές και το Διαδίκτυο. Η προσέγγιση των νομικών θεμάτων που αφορούν το ηλεκτρονικό έγκλημα ενέχει τη δυσκολία ότι προϋποθέτει όχο μόνο νομικές, αλλά και σε ένα βαθμό τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών και Διαδικτύου. Τα προβλήματα της νομοθεσίας επικεντρώνονται στη διαμπορφωση της κατάλληλης ορολογίας, στην αρτιότερη εφαρμογή του Ποινικού και Δικονομικού Δικαίου, καθώς και σε ειδικότερα θέματα που άπτονται της διεθνούς συνεργασίας, όπως η διεθνής δικαιοδοσία.

Έως σήμερα, οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα προέρχονται κυρίως από την τεχνολογία. Ο τεχνικός, λόγω έλλειψης νομικών γνώσεων, προσδιορίζει τους όρους με βάση τις επιστημονικές του γνώσεις και τα τεχνολογικά χαρακτηριστικά κάθε αντικειμένου. Στη νομική επιστήμη, ο προσδιορισμός των όρων είναι τελείως διαφορετικός. Για το νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο που με ακρίβεια καθορίζει ο Νόμος. Σε περίπτωση που δεν υπάρχει νόμος ερευνάται η σχετική νομολογία και αν δεν υπάρχει ούτε νομολογία, η ανάλυση ανάγεται στους γενικούς κανόνες του ισχύοντος δικαίου για να βρεθεί κάποια θεωρητική λύση του ζητήματος. Στην πράξη, ο νομοθέτης αποφεύγει να δημιουργήσει ειδική ορολογία για το ηλεκτρονικό έγκλημα και δανείζεται τη χρησιμοποιούμενη από την τεχνολογία, η οποία μπορεί να είναι ασαφής, γενική, αόριστη ή ελλιπής, κατά τρόπο που να εμποδίζει την ορθή απονομή της δικαιοσύνης.

Το ηλεκτρονικό έγκλημα φέρει κάποια ιδιαίτερα χαρακτηριστικά, που το διαφοροποιούν από το συμβατικό έγκλημα. Τα χαρακτηριστικά αυτά, απαιτούν την υιοθέτηση ειδικών νομοθετικών ρυθμίσεων για την αντιμετώπισή του, τόσο στον τομέα του Ποινικού, όσο και στον τομέα του Δικονομικού Δικαίου. Από άποψη Ποινικού Δικαίου, το ηλεκτρονικό έγκλημα σε πολλές χώρες αντιμετωπίζεται με τις υπάρχουσες διατάξεις του κοινού Ποινικού Δικαίου, γεγονός που πολλές φορές, καθιστά αδύνατη τη δίωξή του. Στον τομέα του δικονομικού δικαίου, οι παρεμβάσεις στην ισχύουσα νομοθεσία παγκοσμίως, είναι ελάχιστες, με αποτέλεσμα να δημιουργούνται ανυπέρβλητα προβλήματα, όπως η δυσκολία ασφαλούς καθορισμού της δικαιοδοσίας των δικαστηρίων και της αρμοδιότητας των διωκτικών αρχών.

Με δεδομένο ότι η τεχνολογία προχωρά πολύ πιο γρήγορα από τη νομοθεσία, κάθε νομοθετική ρύθμιση υπόκειται πολύ γρήγορα σε αμφισβήτηση. Αυτό που σήμερα ορίζουμε ως ηλεκτρονικό έγκλημα, πολύ σύντομα δεν θα υπάρχει ως συμπεριφορά ή θα έχει τροποποιηθεί κατά τρόπο ουσιαστικό, που θα καθιστά ανίσχυρο τον υπάρχοντα νόμο. Για την αντιμετώπιση του ηλεκτρονικού εγκλήματος δεν αρκεί μόνο ειδική νομοθεσία, αλλά απαιτείται συνεχής ενημέρωσή της, λαμβάνοντας υπόψη τις τεχνολογικές εξελίξεις. Επιπλέον, για ένα άρτιο σύστημα απονομής δικαιοσύνης, όλοι όσοι εμπλέκονται στη δίωξη του ηλεκτρονικού εγκλήματος όπως αστυνομικοί, εισαγγελείς, δικαστές και δικηγόροι, πρέπει να κατέχουν τόσο νομικές, όσο και τεχνικές γνώσεις, για τη νέα αυτή μορφή εγκληματικής δραστηριότητας.

Τέλος, τα σημαντικότερα νομοθετικά προβλήματα για το ηλεκτρονικό έγκλημα οφείλονται στον παγκόσμιο χαρακτήρα του. Ο τόπος διάπραξης των συμβατικών εγκλημάτων, προσδιορίζεται από έναν συγκεκριμένο γεωγραφικό χώρο. Στα ηλεκτρονικά εγκλήματα, ο τόπος διάπραξης πολλές φορές είναι αδύνατο να προσδιοριστεί, οι δε συνέπειες της εγκληματικής συμπεριφοράς, μπορούν να είναι ορατές σε περισσότερες από μία χώρες, στις οποίες ισχύει διαφορετικό νομοθετικό πλαίσιο. Η δικαιοδοσία, η συνεργασία μεταξύ των κρατών σε διεθνείς έρευνες ηλεκτρονικών εγκλημάτων και η διαδικασία έκδοσης όσων έχουν διαπράξει ηλεκτρονικά εγκλήματα με διεθνικό χαρακτήρα, είναι μερικά μόνο από τα ζητήματα που επιτείνουν τους νομοθετικούς προβληματισμούς.

10.2 ΝΟΜΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελεί η νομική ρύθμιση του Διαδικτύου, ενός «χώρου» τεράστιου και αχανούς, με δυσδιάκριτα όρια και απεριόριστες δυνατότητες ανταλλαγής πληροφοριών. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες, μέσω του Διαδικτύου, υπηρεσίες. Επιπλέον, οποιαδήποτε προσπάθεια ρύθμισης, συναντά φραγμούς, που ανάγονται στις απόψεις δύο αντιμαχόμενων παρατάξεων: αυτών που είναι υπέρ και αυτών που είναι κατά της οποιασδήποτε προσπάθειας ρύθμισης του Διαδικτύου (Ζάννη, 2005).

Τα επιχειρήματα υπέρ της ρύθμισης του Διαδικτύου είναι τα ακόλουθα:

- Το Διαδίκτυο είναι ανοιχτό σε όλους και απαιτείται η ρύθμισή του για τον έλεγχο του παράνομου περιεχομένου του.
- Δεν αποτελεί διαφορετικό μέσο επικοινωνίας, σε σχέση με το ραδιόφωνο και την τηλεόραση, τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις.

- Υπάρχει πολύ επιβλαβές υλικό σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που γεννά την υποχρέωση της πολιτείας για τον έλεγχο και την αντιμετώπισή της.
- Οι περισσότεροι χρήστες, απαιτούν κάποια μορφή ρύθμισης για την προστασία των δεδομένων τους και των περιουσιακών δικαιωμάτων τους, έναντι επιθέσεων κακόβουλων χρηστών.
- Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης συνοψίζονται στα ακόλουθα:
- Η ελευθερία του λόγου που προσφέρεται μέσω του Διαδικτύου είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευόμενο από συνταγματικές διατάξεις.
- Το Διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας, διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός.
- Το Διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια, θα έρχεται πάντοτε αντιμέτωπη με το ζήτημα της λογοκρισίας.
- Οι γονείς είναι υπεύθυνοι για να προστατεύσουν τα παιδιά από το παράνομο περιεχόμενο του Διαδικτύου και όχο τα κράτη με νομοθετικές ρυθμίσεις.

Το Διαδίκτυο, με άξονα τη βασική του χρήση ως μέσο επικοινωνίας, απασχόλησε τον νομοθέτη, ιδιαίτερα από το χρονικό σημείο που άρχισε να αναπτύσσεται και να επεκτείνεται. Στην Ελλάδα έως το 1990, οι υπηρεσίες που στηρίζονταν στην πληροφορική παρέχονταν μονοπωλιακά από τον ΟΤΕ. Το ίδιο συνέβαινε και σε άλλες ευρωπαϊκές χώρες (Καρακώστας, 2003). Το τοπίο διαφοροποιήθηκε με πρωτοβουλία της Ευρωπαϊκής Κοινότητας, η οποία με δύο Οδηγίες την 90/38794 και την 90/388,95 κατήργησε το μονοπώλιο των εθνικών τηλεπικοινωνιακών οργανισμών, δίνοντας τη δυνατότητα σε οποιονδήποτε φορέα να προσφέρει τηλεπικοινωνιακές υπηρεσίες.

Η προσαρμογή της ελληνικής νομοθεσίας προς τις παραπάνω οδηγίες της Ευρωπαϊκής Κοινότητας, προήλθε, κατ' αρχήν, με τον Ν. 2075/92. Ο νόμος αυτός, πολύ σύντομα καταργήθηκε με τον νέο Ν. 2246/94 και στη συνέχεια με τον Ν. 2867/2000, που ως σήμερα είναι σε ισχύ. Με τον νόμο αυτό, ιδρύθηκε ρυθμιστική αρχή, η «Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων», με αποστολή τη διασφάλιση των συμφερόντων των χρηστών του Διαδικτύου. Η αρχή αυτή έχει τη δυνατότητα να ελέγχει τους πάροχους τηλεπικοινωνιακών υπηρεσιών και να επιβάλλει κυρώσεις σε περίπτωση παραβίασης συγκεκριμένων δικαιωμάτων των χρηστών, όπως η διατήρηση του απόρρητου χαρακτήρα των επικοινωνιών τους.
(Βλαχόπουλος, 2007)

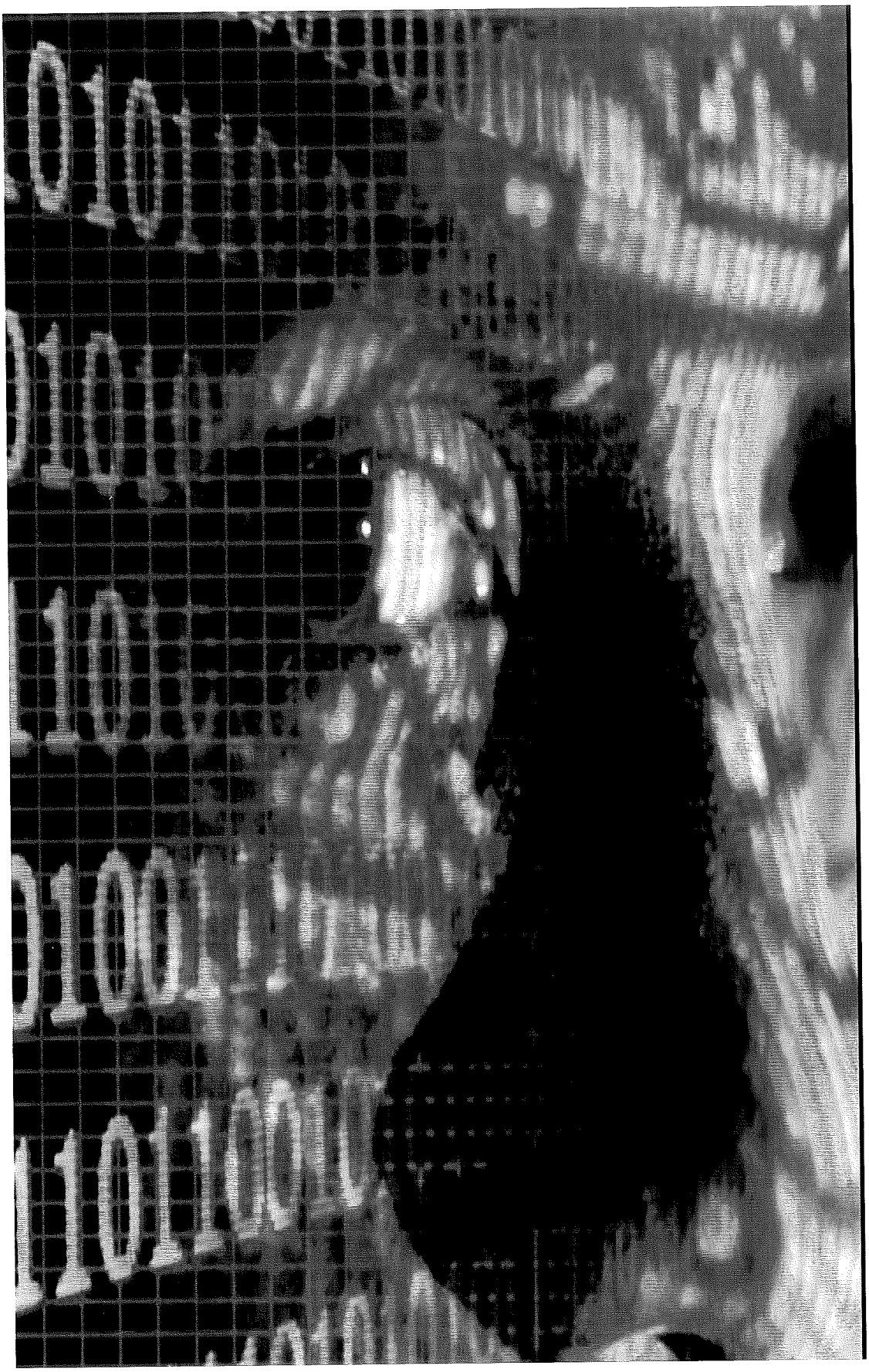
10.3 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

Η Ελληνική νομοθεσία για την προστασία του απορρήτου και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αποτελεί έναν συνδυασμό διεθνών συνθηκών, συνταγματικών διατάξεων, διατάξεων του κοινού ποινικού δικαίου και νόμων που έχουν εκδοθεί βάσει κοινοτικών οδηγιών.

Στο Σύνταγμα της Ελλάδος, περιλαμβάνονται μια σειρά από διατάξεις, για την προστασία της ιδιωτικής σφαίρας του ατόμου. Η θεμελιώδης διάταξη του άρθρου 2 παρ. 1, αναφέρει ότι «ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της πολιτείας». Σημαντικές διατάξεις περιλαμβάνονται στα άρθρα 9 και 19.

Στο άρθρο 9 αναφέρεται ότι «η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη» διάταξη που απαγορεύει τη δημοσιοποίηση της ζωής του ατόμου. Το άρθρο 19 προστατεύει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση και επικοινωνία. Βασικό στοιχείο της επικοινωνίας αποτελεί η μυστικότητα του περιεχομένου της.

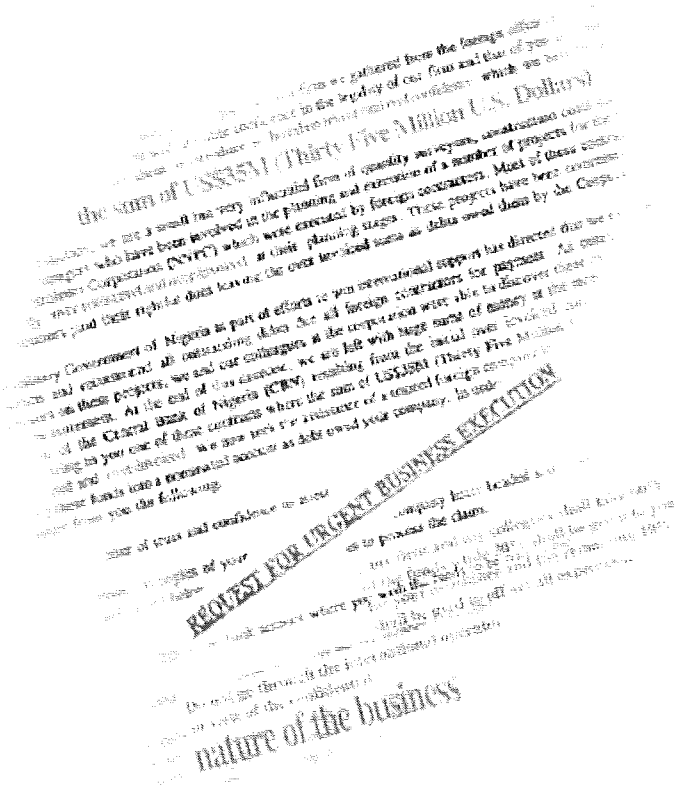
Στον Ποινικό Κώδικα, η προστασία του απορρήτου προβλέπεται από τα άρθρα 370, 370Α, 370Β και 370Γ. Τα άρθρα 370 και 370Α αναφέρονται στην προστασία των επιστολών και την παραβίαση του απορρήτου των τηλεφωνημάτων και της προσωπικής συνομιλίας, αντίστοιχα. Η ανάλογη εφαρμογή των διατάξεων αυτών στο χώρο του Διαδικτύου, έχει προκαλέσει έντονο προβληματισμό στους νομικούς κύκλους, ιδιαίτερα όσον αφορά το άρθρο 370Α, το οποίο κατά πολλούς, θεωρείται ότι δεν μπορεί να τύχει εφαρμογής στο Διαδίκτυο, αν και η σύνδεση γίνεται μέσω μισθωμένης τηλεφωνικής γραμμής (Καράκωστας, 2001). Το άρθρο 370Β, παρέχει ικανοποιητική προστασία μόνο όμως για κρατικά, επιστημονικά και επαγγελματικά απόρρητα, αποκλείοντας τα ιδιωτικά απόρρητα.139 Η πιο ουσιαστική διάταξη, όσον αφορά το χώρο του Διαδικτύου, περιλαμβάνεται στο άρθρο 370Γ, που τιμωρεί τη χωρίς άδεια πρόσβαση σε δεδομένα αποθηκευμένα σε Η/Υ. Το απόρρητο στην περίπτωση αυτή προστατεύεται υπό μία ευρεία έννοια. Δεν περιλαμβάνει μόνο δεδομένα τα οποία χαρακτηρίζονται από τη φύση τους απόρρητα, αλλά προστατεύεται το δικαίωμα του νομίμου κατόχου των δεδομένων να αποκλείει σε άλλους την πρόσβαση σε όλα τα δεδομένα, που είναι αποθηκευμένα στον υπολογιστή του.



Β΄ ΜΕΡΟΣ

Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

NIGERIAN ADVANCE FEE FRAUD



11^{Ο} ΚΕΦΑΛΑΙΟ

ΟΡΙΣΜΟΙ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

ΕΙΣΑΓΩΓΗ 11^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Η εξέλιξη της τεχνολογίας και ιδιαίτερα η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του διαδικτύου, έχουν κατά γενική ομολογία επιφέρει μεγάλες αλλαγές στην καθημερινή ζωή τόσο την ιδιωτική όσο και την επιχειρηματική. Κατά κανόνα η ανάπτυξη αυτή έχει βελτιώσει την ποιότητα ζωής αφού σήμερα μέσω του διαδικτύου μπορούν να αντληθούν απεριόριστες πληροφορίες, οι οποίες χρησιμεύουν στην εκπαίδευση, στις συναλλαγές και στην άμεση επικοινωνία.

Όπως σε όλο το φάσμα της ανθρώπινης δραστηριότητας, έτσι και στην περίπτωση της χρήσης του διαδικτύου, δυστυχώς υπεισέρχονται και στοιχεία που εκμεταλλεύονται το σύστημα και ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας, όπως είναι η παιδική πορνογραφία, ο παράνομος τζόγος, η κλοπή προσωπικών και επιχειρηματικών δεδομένων και αρχείων, η βιομηχανική κατασκοπία και οι διάφορες μορφές απάτης. Οι διάφορες απάτες, είναι και η πιο συνηθισμένη μορφή εγκληματικότητας που παρατηρείται στο διαδίκτυο, Στόχος των στοιχείων αυτών είναι η εύκολη αποκόμιση παράνομων εσόδων.

11.1 ΤΙ ΕΙΝΑΙ Η ΑΠΑΤΗ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ;

Γενικά ο όρος απάτες μέσω διαδικτύου (Internet fraud), αναφέρεται σε οποιαδήποτε μορφή σχεδίου απάτης κατά την οποία οι απατεώνες χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο (e-mail) και τις ιστοσελίδες (web sites), για να παρουσιάσουν σε διάφορους χρήστες του διαδικτύου, διάφορες παραστάσεις που είναι ψευδείς, με σκοπό την καταδολίευση και κυρίως την αποκόμιση οικονομικού οφέλους.

11.2 ΚΥΡΙΟΤΕΡΕΣ ΜΟΡΦΕΣ ΑΠΑΤΗΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Οι κυριότερες μορφές απάτης που παρουσιάζονται παγκόσμια μέσω του διαδικτύου είναι οι πιο κάτω:

- Απάτες στις ηλεκτρονικές δημοπρασίες, όπου δηλαδή τα αντικείμενα που αγοράζονται δεν παραδίδονται ποτέ
- Επίσης αγορές online που δεν παραδίδονται ποτέ
- Απάτες με την μέθοδο της προκαταβολής (Advance Fee Fraud) Απάτη τύπου Νιγηρίας
- Εσκεμμένη παραπληροφόρηση για προϊόντα παντός είδους που αγοράζονται online τα οποία είτε δεν παραδίδονται ποτέ είτε δεν πληρούν τις αρχικές προδιαγραφές
- Απάτες πρόσβασης στο διαδίκτυο, όπου άγνωστοι ISPs χρεώνουν λανθασμένα για υπηρεσίες που ποτέ δεν είχαν ζητηθεί

- Υπέρογκες χρεώσεις σε τηλεφωνικούς λογαριασμούς ή σε πιστωτικές κάρτες, για υπηρεσίες που ποτέ δεν ζητήθηκαν ή είχαν παρουσιαστεί σαν δωρεάν. Πολύ συνηθισμένο για "ροζ" υλικό
- Συστήματα εργασίας στο σπίτι που υπόσχονται ιδιαίτερα αυξημένες πωλήσεις και κέρδη
- Προκαταβολές για δάνεια, όπου τα θύματα εξαπατώνται στο να πληρώσουν προκαταβολικά χρεώσεις για δάνεια με πολύ μικρό επιτόκιο. Βέβαια τα δάνεια ποτέ δεν υλοποιούνται
- Ψευδείς προσφορές για πιστωτικές κάρτες με πολύ μικρό επιτόκιο, πάλι μέσω της πληρωμής προκαταβολών
- Επενδυτικές ευκαιρίες που πωλούνται με την υπόσχεση υπερβολικών εκτιμήσεων κέρδους

11.3 ΟΡΙΣΜΟΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

Είναι μηνύματα ηλεκτρονικού ταχυδρομείου με περιεχόμενο πλασματικές ιστορίες, μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη.

11.4 ΤΙ ΕΙΝΑΙ Η ΝΙΓΗΡΙΑΝΗ ΑΠΑΤΗ;

Η κεντρική αρχή στις περισσότερες απάτες (και φυσικά και στις απάτες με όχημα το Διαδίκτυο) είναι να πειστεί το υποψήφιο θύμα ότι καταβάλλοντας ένα μικρό ποσό εξασφαλίζει ένα άλλο πολύ μεγαλύτερο, χωρίς να κάνει απολύτως τίποτα . Οι περισσότεροι άνθρωποι είναι, φυσικά, σκεπτικοί απέναντι σε τέτοιου είδους προσεγγίσεις. Υπάρχουν όμως και εκείνοι που κινούμενοι από απληστία, ανάγκη, ή άγνοια μετατρέπονται σε εύκολα θύματα κακοποιών χάνοντας αρκετά χρήματα. Μάλιστα σε κάποιες περιπτώσεις το κόστος μπορεί να είναι πολύ μεγαλύτερο από χρήματα...

Μία από τις πλέον κλασικές απάτες που γίνεται με τη μέθοδο του email spamming είναι η απάτη μεταφοράς νιγηριανών κεφαλαίων. Οι λόγοι που χρησιμοποιείται το ηλεκτρονικό ταχυδρομείο για την εξάπλωση της απάτης είναι το εξαιρετικά χαμηλό κόστος επικοινωνίας, το γεγονός της ανωνυμίας που επιτυγχάνουν οι απατεώνες και το μέγεθος του πληθυσμού που καταφέρνουν να προσεγγίσουν (μαζικότητα και εξάλειψη των γεωγραφικών περιορισμών). Οι απατεώνες χρησιμοποιούν διάφορες παραλλαγές αλλά γενικά ο κορμός της εν λόγω διεθνούς απάτης χαρακτηρίζεται από τα παρακάτω σημεία:

1. Ο αποστολέας υποτίθεται πώς είναι κάποιο πολύ σημαντικό πρόσωπο του καθεστώτος στη Νιγηρία (συνήθως του προηγούμενου καθεστώτος). Συνήθως είναι πρώην υψηλόβαθμος αξιωματούχος ή ανώτατο στέλεχος σε κρατική εταιρία.
2. Υπάρχει κάποιο σημαντικό χρηματικό ποσό (της τάξεως των εκατομμυρίων ευρώ) το οποίο για διάφορους λογικοφανείς δεν μπορεί να διοχετευθεί εκτός της χώρας με το όνομα του δικαιούχου / αποστολέα του email.
3. Ο παραλήπτης του email καλείται να διευκολύνει τον αποστολέα λειτουργώντας ως αποδέκτης του ποσού ώστε να γίνει αποδεκτή από την κυβέρνηση η διοχέτευση

των χρημάτων εκτός της Νιγηρίας. Για τη βοήθειά του αυτή θα λάβει ως προμήθεια ένα σημαντικό χρηματικό ποσό. Όταν το σύνολο του ποσού μεταφερθεί στο λογαριασμό του υποψηφίου θύματος, τότε υποτίθεται ότι έναντι μίας (πολύ υψηλής προμήθειας) θα πρέπει να το παραδώσει στον αποστολέα του email.

4. Οι λόγοι επιλογής του παραλήπτη αναφέρεται ότι έγιναν με βάση κάποια πληροφορία σχετικά με την φερεγγυότητά του και την αξιοπιστία του και όχι τυχαία.
5. Γίνεται αναφορά στην ανάγκη τήρησης μυστικότητας η οποία αιτιολογείται από τον κίνδυνο που διατρέχει ο πρώην αξιωματούχος / στέλεχος από την τωρινή κυβέρνηση της Νιγηρίας. Αν πάθει κάτι ο αποστολέας τότε ο παραλήπτης θα χάσει τη "μεγάλη ευκαιρία" που τόσο απρόσμενα του παρουσιάστηκε...

Σε πρώτη φάση ζητείται η συγκατάθεση του παραλήπτη του email και η παροχή πληροφοριών που σχετίζονται με τραπεζικούς λογαριασμούς και άλλα στοιχεία που θα διευκολύνουν τη συναλλαγή. Αν ο παραλήπτης ζητήσει έγγραφα που να αποδεικνύουν το αληθές των όσων ισχυρίζεται ο αποστολέας τότε ο τελευταίος θα φροντίσει να αποστείλει διάφορα πιστοποιητικά (εννοείται πλαστά) που δείχνουν επίσημα και αυθεντικά και που ενισχύουν την αξιοπιστία του, επιβεβαιώνοντας ενδεχομένως και την ύπαρξη του προς μεταφορά ποσού. Έτσι το θύμα προσελκύεται σε κάτι που μοιάζει με απίθανη ευκαιρία. Βέβαια στις περισσότερες περιπτώσεις τα έγγραφα που αποστέλλονται είναι εξόφθαλμα πλαστά, πρόχειρα και γεμάτα τυπογραφικά και συντακτικά λάθη. Και όμως φαίνεται ότι κάποιοι πείθονται... Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίσει να απαντήσει στην αρχική προσφορά και να την αποδεχτεί. Ξεκινάει, λοιπόν, μια διαδικασία ανταλλαγής επιστολών, πιθανόν και κάποια υπογραφή συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει ήδη αρχίσει να πιστεύει ότι βρίσκεται ένα βήμα πριν την απόκτηση ενός πολύ μεγάλου χρηματικού ποσού.

Σε κάποια στιγμή, πριν τη μεταβίβαση των χρημάτων, θα εμφανιστεί κάποιο πρόβλημα (ένα απρόβλεπτο τέλος που πρέπει να πληρωθεί, κάποιος κυβερνητικός ή τραπεζικός υπάλληλος που πρέπει να δωροδοκηθεί, κάποια προμήθεια που απαιτείται από την τράπεζα). Ο απατεώνας προφασίζεται προσωρινή αδυναμία του να καλύψει αυτό το ποσό αφού έχει ήδη προχωρήσει στην εντολή μεταβίβασης των χρημάτων με αποτέλεσμα αυτά να είναι δεσμευμένα μέχρι να λυθεί το πρόβλημα που προέκυψε. Επίσης, μπορεί να προφασισθεί έλλειψη ρευστότητας λόγω κάποιας αιφνίδιας παρέμβασης της κυβέρνησης, δημιουργώντας μια ακόμα πιο επείγουσα και πιεστική για το υποψήφιο θύμα κατάσταση καθώς τα χρήματα κινδυνεύουν να χαθούν.

Στο πλαίσιο, λοιπόν, της συνεργασίας των δύο μερών ζητείται από το θύμα να καταβάλλει αυτό το έκτακτο χρηματικό ποσό, το οποίο "φυσικά" θα πάρει πίσω μόλις ολοκληρωθεί η συναλλαγή. Άλλωστε το ποσό που καλείται να πληρώσει τώρα, ωχριά μπροστά στο ποσό που θα λάβει αργότερα για την εξυπηρέτηση του νέου νιγηριανού φίλου του. Αυτή είναι και η αρχή μια σειράς τέτοιων "προβλημάτων", καθώς εμφανίζονται όλο και νέα ποσά που πρέπει να καταβληθούν άμεσα και ζητούνται από το θύμα. Το θύμα με τη σειρά του, στην προσδοκία μιας προμήθειας της τάξης των εκατομμυρίων δεν διστάζει να πληρώσει κάποιες χιλιάδες ευρώ. Μάλιστα αν κάποιος πληρώσει το αρχικό ποσό, δύσκολα δεν θα συνεχίσει να πληρώνει, προσδοκώντας να αποσβέσει την αρχική του επένδυση. Σε ακραίες περιπτώσεις το θύμα καλείται να ταξιδέψει στη Νιγηρία ή σε κάποια γειτονική χώρα για την ολοκλήρωση της συναλλαγής.

Εικόνα 11.1 Είδη απάτης

Do you recognize these 419 Advance Fee Fraud scams

Lottery scam
Counterfeit Postal draft scam
Over invoiced contract scam
eBay check (over) payment and refund scam
Unclaimed inheritance scam
Unclaimed bank account scam
Counterfeit Check scam
Dating-romance scam
Black (defaced) currency scam
Gold dust scam
Diamond scam
Fake bank scam
Housing scam
Anti-terrorist certificate scam
Disaster relief fund scam
Financial representative in your country scam
Work permit scam
Payment for art scam
Deceased next of kin scam
Construction sub contractor scam
Lower priced crude oil scam
SWIFT transfer scam
Antique export payments scam
University study place scam
Money from former ruler scam
Relative of holocaust victim scam
Identity theft
Jobs for professionals scam
Dead millionaire funds for charities or disaster relief scam
Very low interest loans for relatively small advance fees scam
Hotel bookings and refund
United Nations loan approval scam
Death threat scam

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

11.5 ΓΙΑΤΙ ΟΝΟΜΑΣΤΗΚΕ ΝΙΓΗΡΙΑΝΗ ΑΠΑΤΗ;

Τα Νιγηριανά e-mail ονομάζονται επίσης και "419" από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν.

12^{Ο} ΚΕΦΑΛΑΙΟ

ΠΕΡΙΓΡΑΦΗ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ ΚΑΙ ΤΥΠΟΙ ΝΙΓΗΡΙΑΝΩΝ ΕΠΙΣΤΟΛΩΝ

ΕΙΣΑΓΩΓΗ 12^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Σε αυτό το κεφάλαιο θα παρουσιάσουμε τις πιο χαρακτηριστικές περιπτώσεις νιγηριανών επιστολών, επίσης θα αναλύσουμε τους τύπους των νιγηριανών επιστολών και τα μέρη από τα οποία αποτελούνται, κάνοντας φυσικά και την ανάλογη ανάλυσή τους, όπου αυτό είναι εφικτό.

12.1 ΠΑΡΟΥΣΙΑΣΗ ΤΩΝ ΠΙΟ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΝΙΓΗΡΙΑΝΩΝ ΕΠΙΣΤΟΛΩΝ

Εικόνα 12.1. 1° Παράδειγμα Νιγηριανής Επιστολής

"Having consulted with my colleagues, and based on information gathered from the Nigerian Chamber of Commerce, I am pleased to propose a confidential business transaction to our mutual benefit. I and my colleagues have in our possession instruments to transfer the sum of $35,500,000.00 into a foreign company's account in our favor. This amount emanated as a result from an over-invoiced contract, executed, commissioned, and paid for about two years ago by a foreign contractor. We are therefore seeking your assistance in transferring this money to your account as it can only be remitted to a foreign account, and as civil servants, we are forbidden to operate foreign accounts. The total sum will be shared as follows:

30% for the account owner (you)
60% for us
10% to settle any incidental expenses

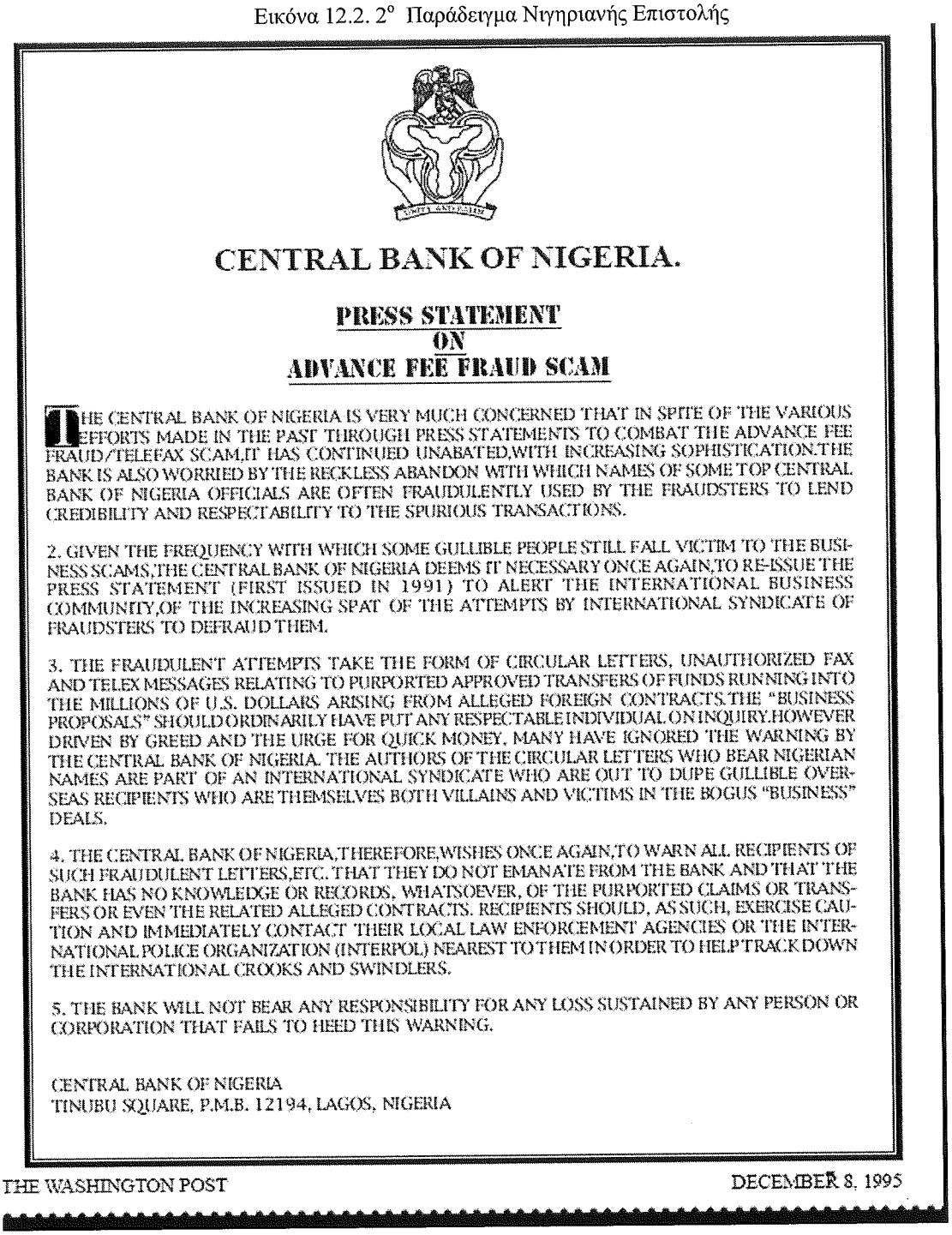
"We shall commence the transfer of funds immediately, as soon as you send the following documents/information through the above fax number.

1. Four copies of your company's letter head and invoice papers signed and stamped
2. Your banker's name, address and fax numbers
3. The account number and name of would be beneficiary.

"Bear in mind that this is absolutely a private and personal deal, nonofficial; and should be treated with all measure of secrecy and confidentiality."

(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Εικόνα 12.2. 2° Παράδειγμα Νιγηριανής Επιστολής



CENTRAL BANK OF NIGERIA.

PRESS STATEMENT
ON
ADVANCE FEE FRAUD SCAM

THE CENTRAL BANK OF NIGERIA IS VERY MUCH CONCERNED THAT IN SPITE OF THE VARIOUS EFFORTS MADE IN THE PAST THROUGH PRESS STATEMENTS TO COMBAT THE ADVANCE FEE FRAUD/TELEFAX SCAM,IT HAS CONTINUED UNABATED,WITH INCREASING SOPHISTICATION.THE BANK IS ALSO WORRIED BY THE RECKLESS ABANDON WITH WHICH NAMES OF SOME TOP CENTRAL BANK OF NIGERIA OFFICIALS ARE OFTEN FRAUDULENTLY USED BY THE FRAUDSTERS TO LEND CREDIBILITY AND RESPECTABILITY TO THE SPURIOUS TRANSACTIONS.

2. GIVEN THE FREQUENCY WITH WHICH SOME GULLIBLE PEOPLE STILL FALL VICTIM TO THE BUSINESS SCAMS,THE CENTRAL BANK OF NIGERIA DEEMS IT NECESSARY ONCE AGAIN,TO RE-ISSUE THE PRESS STATEMENT (FIRST ISSUED IN 1991) TO ALERT THE INTERNATIONAL BUSINESS COMMUNITY,OF THE INCREASING SPAT OF THE ATTEMPTS BY INTERNATIONAL SYNDICATE OF FRAUDSTERS TO DEFRAUD THEM.

3. THE FRAUDULENT ATTEMPTS TAKE THE FORM OF CIRCULAR LETTERS, UNAUTHORIZED FAX AND TELEX MESSAGES RELATING TO PURPORTED APPROVED TRANSFERS OF FUNDS RUNNING INTO THE MILLIONS OF U.S. DOLLARS ARISING FROM ALLEGED FOREIGN CONTRACTS.THE "BUSINESS PROPOSALS" SHOULD ORDINARILY HAVE PUT ANY RESPECTABLE INDIVIDUAL ON INQUIRY.HOWEVER DRIVEN BY GREED AND THE URGE FOR QUICK MONEY, MANY HAVE IGNORED THE WARNING BY THE CENTRAL BANK OF NIGERIA. THE AUTHORS OF THE CIRCULAR LETTERS WHO BEAR NIGERIAN NAMES ARE PART OF AN INTERNATIONAL SYNDICATE WHO ARE OUT TO DUPE GULLIBLE OVERSEAS RECIPIENTS WHO ARE THEMSELVES BOTH VILLAINS AND VICTIMS IN THE BOGUS "BUSINESS" DEALS.

4. THE CENTRAL BANK OF NIGERIA,THEREFORE,WISHES ONCE AGAIN,TO WARN ALL RECIPIENTS OF SUCH FRAUDULENT LETTERS,ETC. THAT THEY DO NOT EMANATE FROM THE BANK AND THAT THE BANK HAS NO KNOWLEDGE OR RECORDS, WHATSOEVER, OF THE PURPORTED CLAIMS OR TRANSFERS OR EVEN THE RELATED ALLEGED CONTRACTS. RECIPIENTS SHOULD, AS SUCH, EXERCISE CAUTION AND IMMEDIATELY CONTACT THEIR LOCAL LAW ENFORCEMENT AGENCIES OR THE INTERNATIONAL POLICE ORGANIZATION (INTERPOL) NEAREST TO THEM IN ORDER TO HELP TRACK DOWN THE INTERNATIONAL CROOKS AND SWINDLERS.

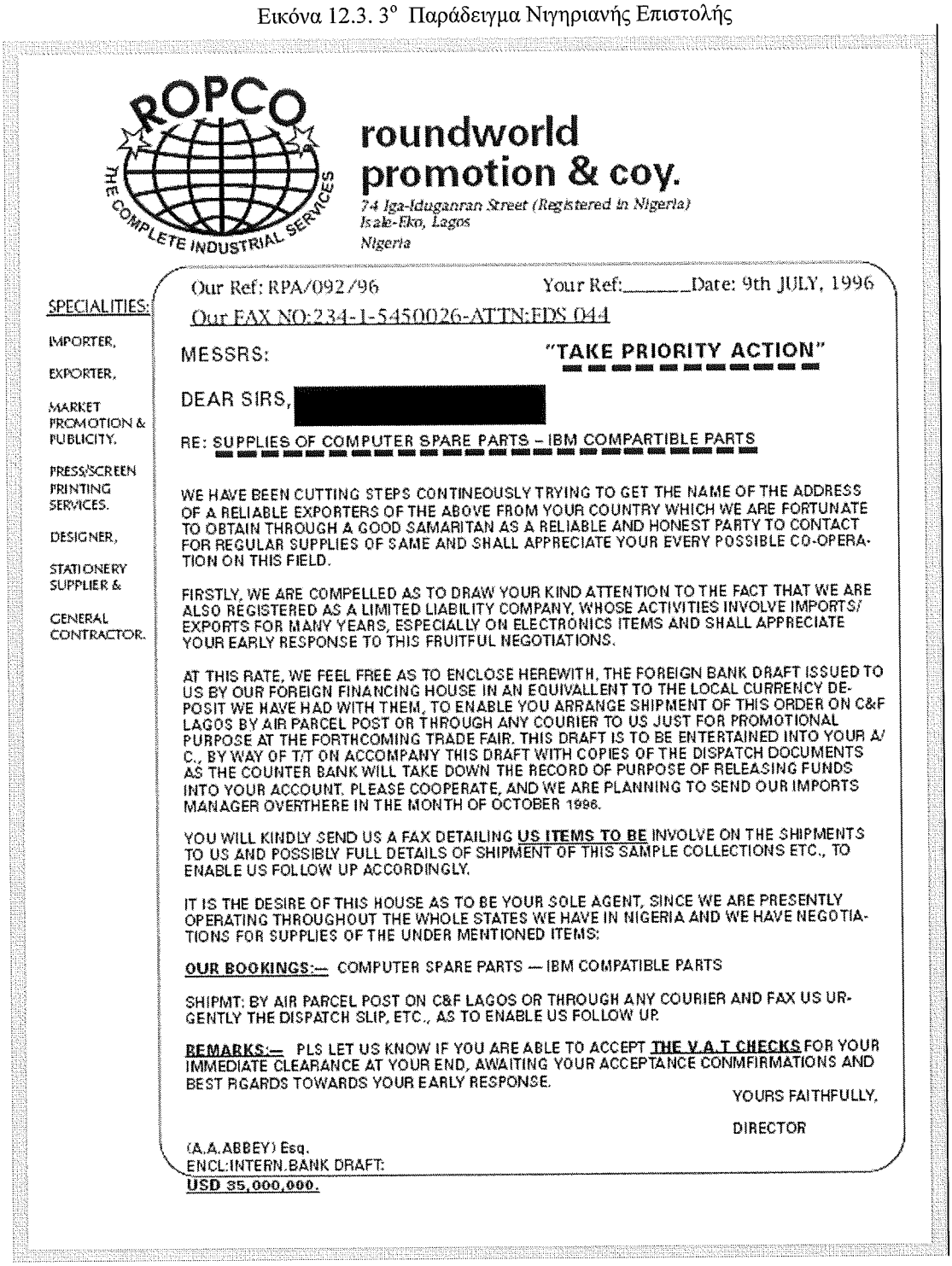
5. THE BANK WILL NOT BEAR ANY RESPONSIBILITY FOR ANY LOSS SUSTAINED BY ANY PERSON OR CORPORATION THAT FAILS TO HEED THIS WARNING.

CENTRAL BANK OF NIGERIA
TINUBU SQUARE, P.M.B. 12194, LAGOS, NIGERIA

THE WASHINGTON POST DECEMBER 8, 1995

(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Εικόνα 12.3. 3° Παράδειγμα Νιγηριανής Επιστολής



ROPCO
THE COMPLETE INDUSTRIAL SERVICES

roundworld promotion & coy.

74 Iga-Iduganran Street (Registered in Nigeria)
Isale-Eko, Lagos
Nigeria

SPECIALITIES:

IMPORTER,

EXPORTER,

MARKET PROMOTION & PUBLICITY.

PRESS/SCREEN PRINTING SERVICES.

DESIGNER,

STATIONERY SUPPLIER &

GENERAL CONTRACTOR.

Our Ref: RPA/092/96 Your Ref:_____Date: 9th JULY, 1996

Our FAX NO:234-1-5450026-ATTN:FDS 044

MESSRS: **"TAKE PRIORITY ACTION"**

DEAR SIRS, [redacted]

RE: SUPPLIES OF COMPUTER SPARE PARTS – IBM COMPARTIBLE PARTS

WE HAVE BEEN CUTTING STEPS CONTINEOUSLY TRYING TO GET THE NAME OF THE ADDRESS OF A RELIABLE EXPORTERS OF THE ABOVE FROM YOUR COUNTRY WHICH WE ARE FORTUNATE TO OBTAIN THROUGH A GOOD SAMARITAN AS A RELIABLE AND HONEST PARTY TO CONTACT FOR REGULAR SUPPLIES OF SAME AND SHALL APPRECIATE YOUR EVERY POSSIBLE CO-OPERATION ON THIS FIELD.

FIRSTLY, WE ARE COMPELLED AS TO DRAW YOUR KIND ATTENTION TO THE FACT THAT WE ARE ALSO REGISTERED AS A LIMITED LIABILITY COMPANY, WHOSE ACTIVITIES INVOLVE IMPORTS/EXPORTS FOR MANY YEARS, ESPECIALLY ON ELECTRONICS ITEMS AND SHALL APPRECIATE YOUR EARLY RESPONSE TO THIS FRUITFUL NEGOTIATIONS.

AT THIS RATE, WE FEEL FREE AS TO ENCLOSE HEREWITH, THE FOREIGN BANK DRAFT ISSUED TO US BY OUR FOREIGN FINANCING HOUSE IN AN EQUIVALLENT TO THE LOCAL CURRENCY DEPOSIT WE HAVE HAD WITH THEM, TO ENABLE YOU ARRANGE SHIPMENT OF THIS ORDER ON C&F LAGOS BY AIR PARCEL POST OR THROUGH ANY COURIER TO US JUST FOR PROMOTIONAL PURPOSE AT THE FORTHCOMING TRADE FAIR. THIS DRAFT IS TO BE ENTERTAINED INTO YOUR A/C., BY WAY OF T/T ON ACCOMPANY THIS DRAFT WITH COPIES OF THE DISPATCH DOCUMENTS AS THE COUNTER BANK WILL TAKE DOWN THE RECORD OF PURPOSE OF RELEASING FUNDS INTO YOUR ACCOUNT. PLEASE COOPERATE, AND WE ARE PLANNING TO SEND OUR IMPORTS MANAGER OVERTHERE IN THE MONTH OF OCTOBER 1996.

YOU WILL KINDLY SEND US A FAX DETAILING **US ITEMS TO BE** INVOLVE ON THE SHIPMENTS TO US AND POSSIBLY FULL DETAILS OF SHIPMENT OF THIS SAMPLE COLLECTIONS ETC., TO ENABLE US FOLLOW UP ACCORDINGLY.

IT IS THE DESIRE OF THIS HOUSE AS TO BE YOUR SOLE AGENT, SINCE WE ARE PRESENTLY OPERATING THROUGHOUT THE WHOLE STATES WE HAVE IN NIGERIA AND WE HAVE NEGOTIATIONS FOR SUPPLIES OF THE UNDER MENTIONED ITEMS:

OUR BOOKINGS:— COMPUTER SPARE PARTS — IBM COMPATIBLE PARTS

SHIPMT: BY AIR PARCEL POST ON C&F LAGOS OR THROUGH ANY COURIER AND FAX US URGENTLY THE DISPATCH SLIP, ETC., AS TO ENABLE US FOLLOW UP.

REMARKS:— PLS LET US KNOW IF YOU ARE ABLE TO ACCEPT **THE V.A.T CHECKS** FOR YOUR IMMEDIATE CLEARANCE AT YOUR END, AWAITING YOUR ACCEPTANCE CONMFIRMATIONS AND BEST RGARDS TOWARDS YOUR EARLY RESPONSE.

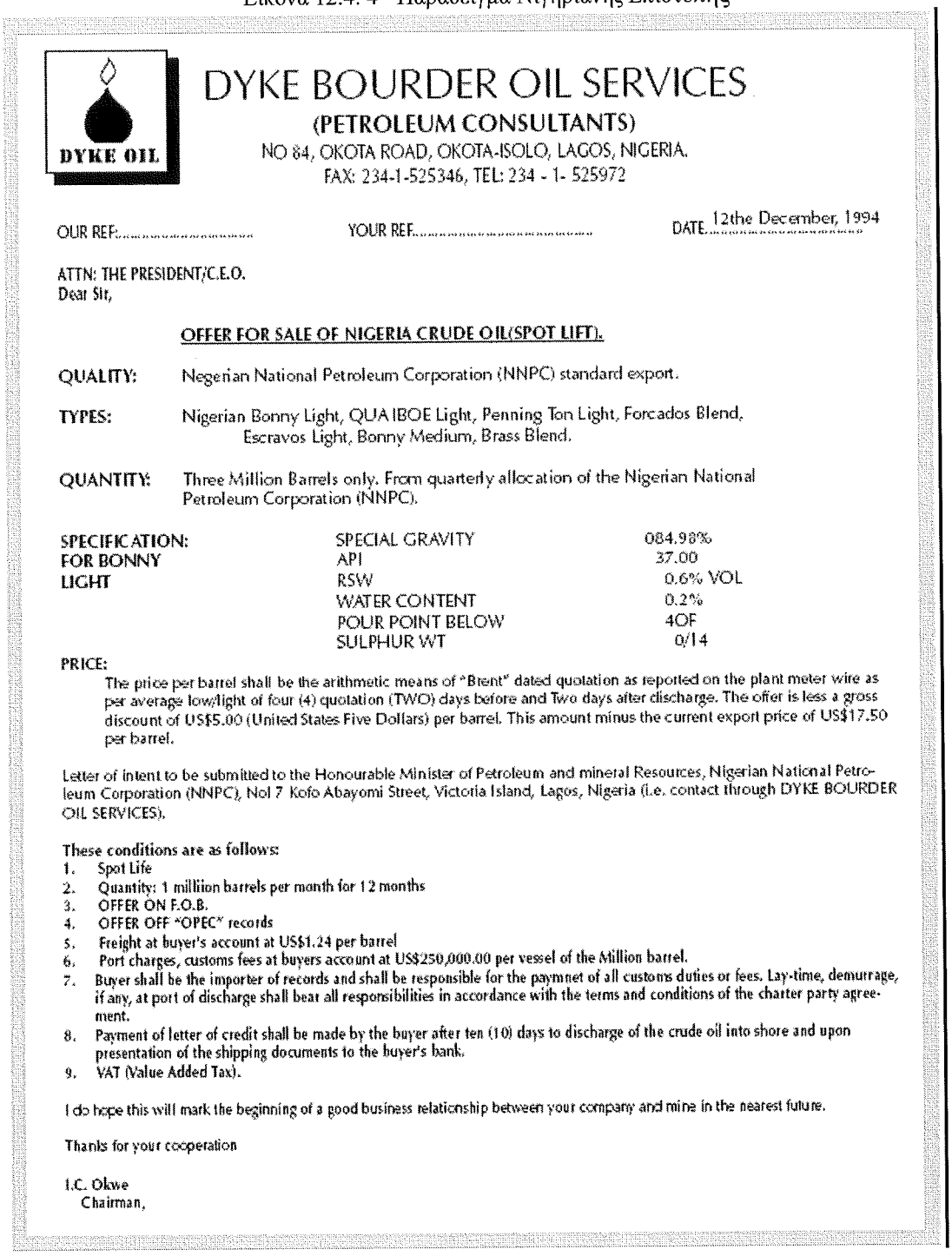
YOURS FAITHFULLY,

DIRECTOR

(A.A.ABBEY) Esq.
ENCL:INTERN.BANK DRAFT:
USD 35,000,000.

(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Εικόνα 12.4. 4° Παράδειγμα Νιγηριανής Επιστολής



DYKE BOURDER OIL SERVICES

(PETROLEUM CONSULTANTS)

NO 84, OKOTA ROAD, OKOTA-ISOLO, LAGOS, NIGERIA.

FAX: 234-1-525346, TEL: 234 - 1- 525972

OUR REF:..... YOUR REF..... DATE..12the December, 1994

ATTN: THE PRESIDENT/C.E.O.
Dear Sir,

OFFER FOR SALE OF NIGERIA CRUDE OIL(SPOT LIFT).

QUALITY: Negerian National Petroleum Corporation (NNPC) standard export.

TYPES: Nigerian Bonny Light, QUA IBOE Light, Penning Ton Light, Forcados Blend, Escravos Light, Bonny Medium, Brass Blend.

QUANTITY: Three Million Barrels only. From quarterly allocation of the Nigerian National Petroleum Corporation (NNPC).

SPECIFICATION: FOR BONNY LIGHT	SPECIAL GRAVITY	084.98%
	API	37.00
	RSW	0.6% VOL
	WATER CONTENT	0.2%
	POUR POINT BELOW	4OF
	SULPHUR WT	0/14

PRICE:

The price per barrel shall be the arithmetic means of "Brent" dated quotation as reported on the plant meter wire as per average low/light of four (4) quotation (TWO) days before and Two days after discharge. The offer is less a gross discount of US$5.00 (United States Five Dollars) per barrel. This amount minus the current export price of US$17.50 per barrel.

Letter of intent to be submitted to the Honourable Minister of Petroleum and mineral Resources, Nigerian National Petroleum Corporation (NNPC), Nol 7 Kofo Abayomi Street, Victoria Island, Lagos, Nigeria (i.e. contact through DYKE BOURDER OIL SERVICES).

These conditions are as follows:

1. Spot Life
2. Quantity: 1 milliion barrels per month for 12 months
3. OFFER ON F.O.B.
4. OFFER OFF "OPEC" records
5. Freight at buyer's account at US$1.24 per barrel
6. Port charges, customs fees at buyers account at US$250,000.00 per vessel of the Million barrel.
7. Buyer shall be the importer of records and shall be responsible for the paymnet of all customs duties or fees. Lay-time, demurrage, if any, at port of discharge shall beat all responsibilities in accordance with the terms and conditions of the charter party agreement.
8. Payment of letter of credit shall be made by the buyer after ten (10) days to discharge of the crude oil into shore and upon presentation of the shipping documents to the buyer's bank.
9. VAT (Value Added Tax).

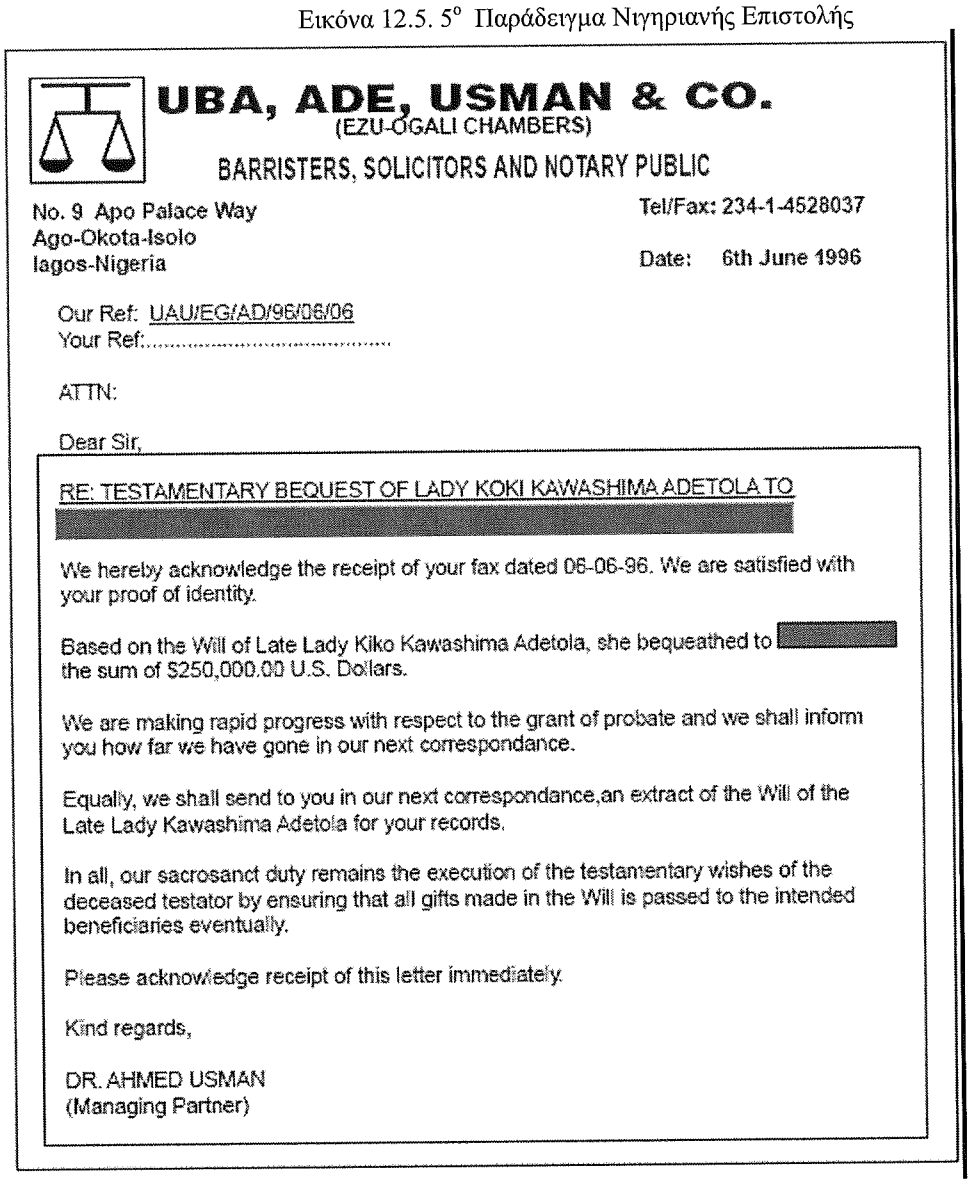
I do hope this will mark the beginning of a good business relationship between your company and mine in the nearest future.

Thanks for your cooperation

I.C. Okwe
Chairman,

(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Εικόνα 12.5. 5° Παράδειγμα Νιγηριανής Επιστολής



UBA, ADE, USMAN & CO.
(EZU-OGALI CHAMBERS)
BARRISTERS, SOLICITORS AND NOTARY PUBLIC

No. 9 Apo Palace Way
Ago-Okota-Isolo
lagos-Nigeria

Tel/Fax: 234-1-4528037

Date: 6th June 1996

Our Ref: UAU/EG/AD/96/06/06
Your Ref:.....

ATTN:

Dear Sir,

RE: TESTAMENTARY BEQUEST OF LADY KOKI KAWASHIMA ADETOLA TO [redacted]

We hereby acknowledge the receipt of your fax dated 06-06-96. We are satisfied with your proof of identity.

Based on the Will of Late Lady Kiko Kawashima Adetola, she bequeathed to [redacted] the sum of $250,000.00 U.S. Dollars.

We are making rapid progress with respect to the grant of probate and we shall inform you how far we have gone in our next correspondance.

Equally, we shall send to you in our next correspondance,an extract of the Will of the Late Lady Kawashima Adetola for your records.

In all, our sacrosanct duty remains the execution of the testamentary wishes of the deceased testator by ensuring that all gifts made in the Will is passed to the intended beneficiaries eventually.

Please acknowledge receipt of this letter immediately.

Kind regards,

DR. AHMED USMAN
(Managing Partner)

(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

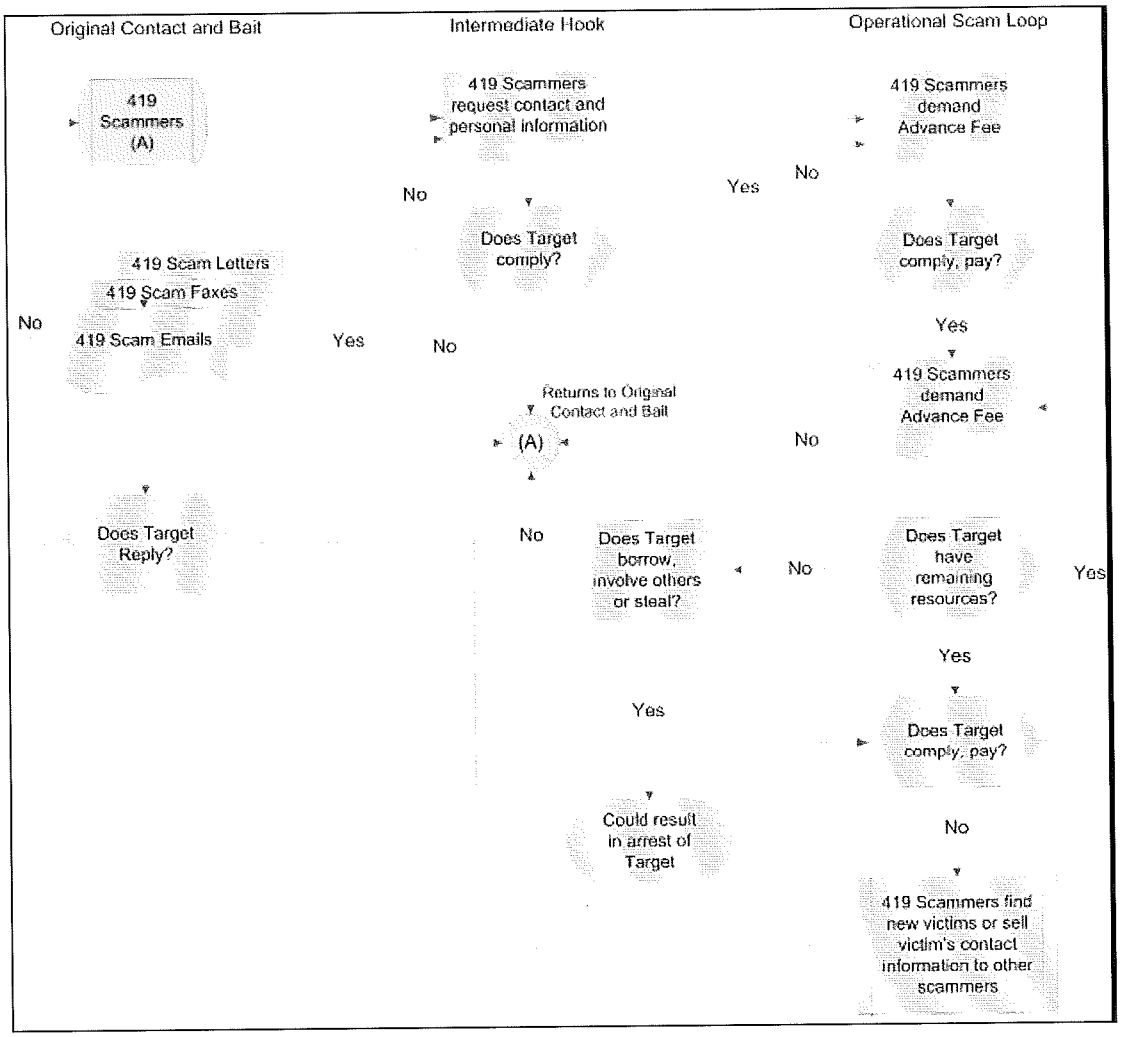
12.2 ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

Σε γενικές γραμμές μια νιγηριανή επιστολή από ακολουθεί το εξής μοντέλο συγγραφής:

- Personal, direct address.
- An apology and introduction.
- A micro-narrative about the origin of the money.
- An invitation to engage in a business transaction.
- Requests for confidentiality.
- Closing formula.

ΦΑΣΕΙΣ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

Εικόνα 12.6 Φάσεις της Νιγηριανής Απάτης



(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Η νιγηριανή απάτη έχει αναδειχθεί σε μια από τις πιο επικερδείς μορφές απάτης που χρησιμοποιούν ως μέσο τις υπηρεσίες του διαδικτύου. Η βασική αρχή σε όλες τις απάτες "προκαταβολής φόρων" είναι το να πειστεί το υποψήφιο θύμα ότι πληρώνοντας ένα μικρό ποσό εξασφαλίζει ένα άλλο πολύ μεγαλύτερο, χωρίς να κάνει απολύτως τίποτα.

12.2.1 ΠΡΩΤΗ ΦΑΣΗ ΝΙΓΗΡΙΑΝΗΣ ΕΠΙΣΤΟΛΗΣ

Θα μπορούσαμε να πούμε πως υπάρχουν διάφοροι τύποι προσφορών σε μια νιγηριανή επιστολή:

1ος τύπος νιγηριανής επιστολής:

Είναι η περίπτωση του αφανούς λογαριασμού και είναι και ο πιο συνηθισμένος τύπος νιγηριανής επιστολής (περίπου το μισό των περιπτώσεων). Σε γενικές γραμμές η επιστολή περιέχει τα παρακάτω στοιχεία:

Εικόνα 12.7. 1ος τύπος νιγηριανής επιστολής

> DEAR PARTNER,
> I guess this letter might come to you as a surprise since I had no previous
> correspondence with you, But with due respect I got your contact in my
> research for a reliable and honest person who will be capable and fit to
> assist me in handling a very confidential transaction involving the transfer
> of US75 million dollars only.
> I want to transfer these funds to overseas(75.000,000.00USD) Seventy Five
> million United States Dollars).For our sharing and investment purposes in
> your country.
> The above fund is not connected with arms, drugs or Money laundering;
> neither
> is it related to any terrorist sponsor of any sort.
> I am Jumbo Williams Akunne,an accountant and Bank manager, The
> Executive and
> the Board of Directors have approved and accredited this reputed Bank with
> the office of the Director,International Remmitance/Foreign Operation, to
> handle and transfer all foreign inherittance funds this final quarter of the
> year. I have my client involved who died in a plane crash with his wife and
> children,though i have tried to contact any of the relatives but to no avail
> and without any traceable next of kin,Hence the dormant nature of His
> account
> and if I do not remit this money out urgently it will be re-channeled into
> the bank's reserve. (Sample 2)

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

Σχολιασμός:

Αυτό είναι ο πιο συχνός τύπος νιγηριανών επιστολών. Μετά από εξέταση διαφόρων τέτοιων επιστολών, μπορούμε να πούμε πως οι επιστολές αυτές, έχουν τα παρακάτω κοινά στοιχεία:

- ο αποστολέας υποτίθεται πώς είναι κάποιο πολύ σημαντικό πρόσωπο του προηγούμενου καθεστώτος και συνήθως μέλος της Νιγηριανής κυβέρνησης.
- υπάρχει κάποιο σημαντικό χρηματικό ποσό (30-100 εκατομμύρια δολάρια) προϊόν υπεξαιρέσεων ή δωροδοκιών το οποίο αυτή τη στιγμή δεν μπορεί να διοχετευθεί εκτός της χώρας με το όνομα του δικαιούχου-αποστολέα του mail
- παρουσιάζονται κάποια επίσημα έγγραφα της κυβέρνησης για να γίνει πιστευτό.
- ο παραλήπτης καλείται να βοηθήσει την κατάσταση λειτουργώντας ως αποδέκτης του ποσού ώστε να γίνει αποδεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός της Νιγηρίας και για τη βοήθειά του αυτή θα λάβει ως προμήθεια ένα σημαντικό ποσό (έως και 30% του συνολικού ποσού)
- η επιλογή του παραλήπτη έγινε με βάση κάποια πληροφορία σχετικά με την φερεγγυότητά του (συχνά αναφέρεται κάποιο επιμελητήριο ή επαγγελματική ένωση) και την αξιοπιστία του και όχι τυχαία
- καλείται συχνά το θύμα να ταξιδέψει στην Νιγηρία για να βεβαιωθεί για όλη την ιστορία.
- ιδιαίτερη αναφορά γίνεται στην ανάγκη τήρησης απόλυτης εμπιστευτικότητας η οποία αιτιολογείται από τον κίνδυνο που διατρέχει ο πρώην αξιωματούχος από την κυβέρνηση της Νιγηρίας.

Εικόνα 12.8. Στοιχεία νιγηριανής επιστολής

A request for confidentiality and an invitation to initiate a procedure of claiming the award.

Ex. 8

> Your fund is now deposited with a Bank in Amsterdam, insured in your name.
> Due to the mix up of some numbers and names, we ask that you keep This award
> strictly from public notice until your claim has been processed and your
> money remitted to your account. This is part of our security protocol to
> avoid double claiming or unscrupulous acts by participants of this program.
>
> To begin your claim, please contact our information centre at:
> infocentre@compaqnet.fr. For due processing and remittance of your prize
> money to a designated account of your choice.
>
> NOTE: In order to avoid unnecessary delays and complications, please
> remember to quote your reference and batch numbers in every one of your
> correspondences with your agent. Furthermore, should there be any change of
> your address, do inform your claims agent as soon as possible.

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

Ανάλυση:

Αρχικά, από το υποψήφιο θύμα ζητείται η συγκατάθεσή του και η παροχή πληροφοριών που σχετίζονται με τραπεζικούς λογαριασμούς, και άλλα στοιχεία που θα διευκολύνουν τη συναλλαγή.

Όταν έχει ζητηθεί ο "Νιγηριανός αξιωματούχος" έχει προσκομίσει στο θύμα έγγραφα που δείχνουν απόλυτα επίσημα και αυθεντικά και ενισχύουν την αξιοπιστία του, επιβεβαιώνοντας και την ύπαρξη του εν λόγω ποσού.

Έτσι το θύμα προσελκύεται σε κάτι που μοιάζει με απίθανη ευκαιρία (από αυτές που εμφανίζονται μόνο μια φορά στη ζωή ενός ανθρώπου).

2ος τύπος νιγηριανής επιστολής:

Είναι η περίπτωση της επιστολής, που αποστέλλεται στο υποψήφιο θύμα, με την αιτιολογία ότι κέρδισε ένα υπέρογκο ποσό σε μια λοταρία στο διαδίκτυο. Είναι περίπου το ¼ των περιπτώσεων και έχουν περίπου την παρακάτω μορφή:

Εικόνα 12.9. 2ος τύπος νιγηριανής επιστολής

> Due to mix up of some numbers and names, we ask that you keep your winning information confidential until your claims has been processed and your money Remitted to you. This is part of our security protocol to avoid double claiming and unwarranted abuse of this program by some participants.
>
> All participants were selected through a computer ballot system drawn from over 20,000 company and 30,000,000 individual email addresses and names from all over the world. This promotional program takes place every three years. We hope with part of your winning you will take part in our next USD 50 million international lottery.
>
> To file for your claim, please contact our fiducial agent/attorney:
> =
> BARRISTER. ROY HANS (ROYAL ADVOCATEN KANTOR)
> Amsterdam-Netherlands.
> Tel: (31) 617 792 760.
> Fax: (31) 847 506 277.
> E-Mail: RoyHansBVA@netscape.net
> =
> We are pleased to inform you of the result of the Our Global Email Lotter program held on the 26th April 2005.
> Your e-mail address attached to ticket number 37511465899-6410 witl serial number 4872-510 drew lucky numbers 7-14-88-23-3545 which consequentl won in the 1st category, you have therefore been approved for a lump sum pa out of US$ 1,000,000.00 (One Million United States Dollars).
>
> CONGRATULATIONS!!!

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

3ος τύπος νιγηριανής επιστολής:

Είναι οι λειτουργίες διάσωσης. Οι δράστες στέλνουν επιστολές ότι αντιμετωπίζουν πρόβλημα με την χώρα καταγωγής τους για να εξάγουν κεφάλαιο και ζητούν βοήθεια από υποψήφια θύματα έναντι μιας καθόλου ευκαταφρόνητης αμοιβής. Η επιστολή αυτή έχει περίπου την εξής μορφή:

Εικόνα 12.10. 3ος τύπος νιγηριανής επιστολής

> My Name is MRS.SUZANA NUHAN VAYE from Liberia, a Country in West Africa. My late Husband is Issac Nuhan Vaye, Deputy Minister of Public Works in Liberia. My Husband was falsely accused of plotting to remove the then PRESIDENT OF LIBERIA CHARLES TAYLOR) from office. Without trial, Charles Taylor killed him. You can verify this from some of the international newspapers posted in the web sites below:
>
> (l)http://www.usatoday.com/news/world/2003-07-15-liberia_x.htm
>
> Before my husband was killed, he moved out the sum of $21.5 million through a diplomatic means, and deposited it with a Security Company Abroad. And this money was meant for importation of agricultural machineries.
>
> All that is needed is for my lawyer to instruct the company to transfer the funds to your account, I will remunerate you with 20% at the end, but most of all is that I solicit your trust and honesty in this transaction. I have been confined only to our country home and all my calls are monitored, so I will advise you contact my private Attorney Barr. P.O.Williams base in United Kingdom on his

contact stated below for onward proceedings:-

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

4ος τύπος νιγηριανής επιστολής:

Είναι η περίπτωση της αγαθοεργίας. Ο δράστης υποτίθεται ότι είναι ένας θρησκευόμενος άνθρωπος, ο οποίος πρόκειται να πεθάνει και στέλνει μια επιστολή για να βοηθήσουν τα υποψήφια θύματα να ολοκληρώσει την αγαθοεργία που έχει ξεκινήσει. Η μορφή, είναι περίπου όπως παρακάτω:

Εικόνα 12.10. 4ος τύπος νιγηριανής επιστολής

> Now that God has called me, I have willed and given most of my property and assets to my immediate and extended family members as well as a few close friends. I want God to be merciful to me and accept my soul, I have decided to give alms to charity organizations, as I want this to be one of the last good deeds, I ever do on earth. So far, I have distributed money to some charity Organizations in the U.A.E, Algeria and Malaysia.
>
> Now that my health has deteriorated so badly, I cannot do this myself anymore. I once asked members of my family to close one of my accounts and distribute the money which I have there to charity organization in Bulgaria and Pakistan; they refused and kept the money to themselves. Hence, I do not trust them anymore, as they seem not to be contended with what I have left for them.
>
> The last of my money which no one knows of is the huge cash deposit in Europe whort eighteen Million US dollars (US$18,000,000.00) that I have with a deposit company abroad.
>
> Acknowledge this message so that I can introduce you to my lawyer who will handle the transfer of receivership by you of the above said funds.
>
> I will want you to help me collect this deposit and dispatched it to charity organizations. My lawyer shall put you in the picture of the funds, tell you where the funds are currently being maintained and also discuss modalities including remuneration for your services.

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

12.2.2 ΔΕΥΤΕΡΗ ΦΑΣΗ ΝΙΓΗΡΙΑΝΗΣ ΕΠΙΣΤΟΛΗΣ

Η 2η φάση του σχεδίου ενεργοποιείται από τη στιγμή που κάποιος αποφασίσει να απαντήσει στην αρχική προσφορά και να την αποδεχτεί. Ξεκινά λοιπόν μια διαδικασία ανταλλαγής επιστολών, πιθανόν και κάποια υπογραφή συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει ήδη αρχίσει να πιστεύει ότι βρίσκεται ένα βήμα πριν την απόκτηση ενός τεράστιου χρηματικού ποσού.

Σε κάποια χρονική στιγμή, ακριβώς πριν τη μεταβίβαση των χρημάτων, θα εμφανιστεί κάποιο πρόβλημα (ένα απρόβλεπτο τέλος που πρέπει να πληρωθεί, κάποιος υπάλληλος που πρέπει να δωροδοκηθεί, κάποια προκαταβολή φόρου που απαιτείται από την τράπεζα).

Ο "Νιγηριανός αξιωματούχος" προφασίζεται προσωρινή αδυναμία του να καλύψει αυτό το ποσό λόγω του ότι έχει ήδη προχωρήσει στην εντολή μεταβίβασης των χρημάτων με αποτέλεσμα αυτά να είναι δεσμευμένα μέχρι να λυθεί το πρόβλημα που ανέκυψε. Επίσης μπορεί να προφασισθεί έλλειψη ρευστότητας λόγω κάποιας αιφνίδιας παρέμβασης της κυβέρνησης που έχει παγώσει όλα τα οικονομικά του στοιχεία, δημιουργώντας με αυτό τον τρόπο μια ακόμα πιο επείγουσα κατάσταση καθώς τα χρήματα κινδυνεύουν να χαθούν.

Στα πλαίσια λοιπόν της συνεργασίας των δύο μερών ζητείται από το θύμα να καταβάλλει αυτό το έκτακτο χρηματικό ποσό, το οποίο "φυσικά" θα πάρει πίσω μόλις

ολοκληρωθεί η συναλλαγή. Αυτή είναι και αρχή μια σειράς τέτοιων "προβλημάτων", καθώς εμφανίζονται όλο και νέα τέλη ή "λαδώματα" που πρέπει να καταβληθούν και ζητούνται από το θύμα. Το θύμα με τη σειρά του, στην προσδοκία μιας προμήθειας της τάξης των 300-1.000 εκατομμύρια δε διστάζει να πληρώσει αρχικά 500.000. Αν δε κάποιος πληρώσει τα πρώτα 500 στη συνέχεια έχει πέρα από την προσδοκία της προμήθειας και την "επένδυσή" του να τον κρατά στο παιχνίδι.

Στις περισσότερες των περιπτώσεων, σε κάποια χρονική στιγμή το θύμα καλείται να ταξιδέψει στη Νιγηρία ή σε κάποια γειτονική χώρα για την ολοκλήρωση της συναλλαγής. Ένα σημαντικό στοιχείο σε αυτό το σημείο είναι ότι το θύμα, εμπιστευόμενο τις πληροφορίες του "συνεργάτη" του πιστεύει ότι δεν είναι απαραίτητη η visa για την είσοδο στη χώρα, ενώ στην πραγματικότητα ισχύει ακριβώς το αντίθετο. Έτσι η ομάδα των κακοποιών επιτυγχάνει την παράνομη είσοδό του στη χώρα μέσω δωροδοκίας κάποιων υπαλλήλων στις αρμόδιες υπηρεσίες και το θύμα βρίσκεται στη Νιγηρία εντελώς παράνομα. Το γεγονός αυτό θα χρησιμοποιηθεί στη συνέχεια ως μέσο εκβιασμού, ενώ παράλληλα το θύμα θα αδυνατεί να εγκαταλείψει τη χώρα με τη νόμιμη οδό. Από το 1992, έχουν αναφερθεί οι θάνατοι 17 ανθρώπων οι οποίοι είτε προσπαθούσαν να πάρουν πίσω χρήματα που είχαν χάσει μέσω της απάτης, είτε είχαν παρασυρθεί εκεί βάσει του παραπάνω σχεδίου.

12.2.3 ΤΟ ΤΕΛΟΣ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΕΠΙΣΤΟΛΗΣ

Συνήθως οι νιγηριανές επιστολές τελειώνουν ως εξής:

Εικόνα 12.10. Το τέλος της νιγηριανής επιστολής

> Congratulations again from all our staff and thank you for being part of our
> promotions program.
>
> Sincerely,
> Zack Sonnie.
> THE PROMOTIONS MANAGER,
> 10TH GLOBAL PROMO-ORGANIZATION INTERNATIONAL PROGRAM,
> THE NETHERLANDS.

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

12.3 ΣΥΜΠΕΡΑΣΜΑΤΑ 12^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Σύμφωνα με τις ενδείξεις, ο "τζίρος" της παραπάνω απάτης ανέρχεται σε εκατοντάδες εκατομμύρια δολάρια κάθε χρόνο με αυξητικές τάσεις. Να σημειωθεί ότι τα νούμερα αυτά δεν περιλαμβάνουν τις απώλειες αυτών που δεν έχουν προχωρήσει σε καταγγελίες, είτε λόγω φόβου, είτε λόγω ντροπής.

Πιστεύεται ότι περισσότερα από 10.000.000 χρήστε του internet έχουν δεχθεί μηνύματα προσέλκυσης στην απάτη και περίπου το 5% από αυτούς (περίπου 500.000) άνθρωποι έχουν προχωρήσει σε περαιτέρω επαφές. Κάποιοι από αυτούς πραγματικά ξεγελάστηκαν σε μικρό ή μεγάλο βαθμό, ενώ άλλοι ήταν απλά περίεργοι να δουν τι θα συμβεί εάν απαντούσαν.

Κάποιοι άνθρωποι προσπάθησαν να κάνουν "δύσκολές, έξυπνες" ερωτήσεις, όπως: *"γιατί διαλέξατε εμένα?"* ή *(δώστε μου αποδείξεις για την ύπαρξη των χρημάτων"*, ή *"εντάξει, ορίστε μια ταχυδρομική θυρίδα, στείλτε μου μια επιταγή, ή σειρά επιταγών, πληρωτέες σε ελληνική τράπεζα"* 'η ακόμα και *"ορίστε κάποιο ελληνικό ή ξένο δικηγορικό γραφείο το οποίο θα συνεννοηθεί με τους δικηγόρους της εταιρείας μας για τη συναλλαγή"*. Σε όλες τις περιπτώσεις υπήρξαν απαντήσεις με αρκετή δόση λογικής.

Διάφορες υπηρεσίες εκτιμούν ότι υπάρχουν αρκετοί ανεξάρτητοι πυρήνες, οι οποίοι όμως διατηρούν μεταξύ τους επαφές.

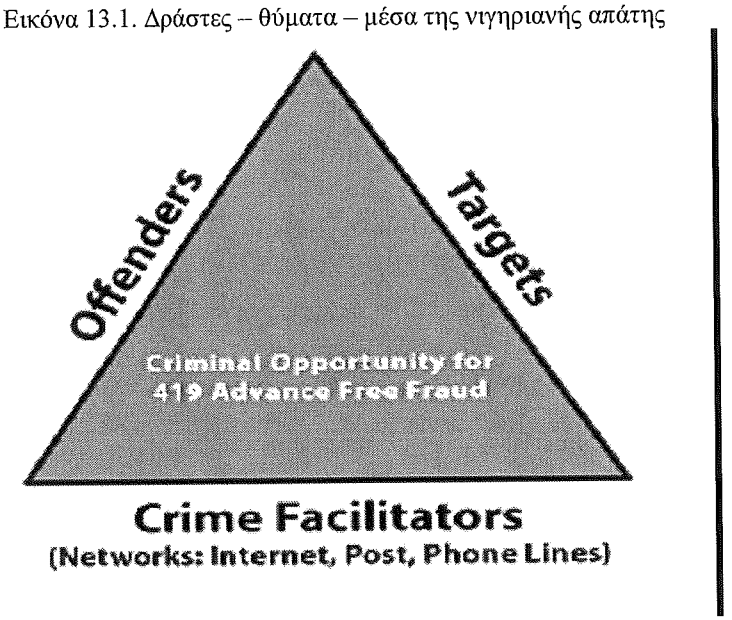
Η Μυστική Υπηρεσία των ΗΠΑ (δεν είναι ίσως γνωστό ότι αρχική αποστολή της, η οποία εξακολουθεί να υφίσταται, δεν ήταν η προστασία του εκάστοτε Προέδρου, αλλά η δίωξη του οικονομικού εγκλήματος), έχει δημιουργήσει ειδικό γραφείο για την εξέταση των περιστατικών του συγκεκριμένου είδους απάτης και, σύμφωνα με τις ανακοινώσεις της, δέχεται καθημερινά εκατοντάδες καταγγελίες. Υπηρεσίες άλλων κρατών, όπως η Μεγάλη Βρετανία έχουν σχηματίσει δικογραφίες εναντίον συγκεκριμένων ατόμων, άλλα από τα οποία έχουν προσαχθεί και άλλα καταζητούνται.

Σημαντική νομική δυσκολία στις περιπτώσεις αυτές, είναι ότι εκτός εκείνων που περιλαμβάνουν σαφή σωματική βία ή απειλή, στις υπόλοιπες είναι δύσκολο να στοιχειοθετηθεί αδίκημα, κυρίως όταν η κατάσταση περιπλέκεται λόγω της εμπλοκής διαφορετικών νομικών συστημάτων (μή ξεχνάμε ότι πρόκειται για διεθνή απάτη και στην πραγματικότητα δεν ξέρουμε σε ποια χώρα βρίσκεται αυτός με τον οποίον έρχεστε σε επαφή) καθώς δεν είναι πάντα σαφές σε ποια χώρα διαπράττεται το αδίκημα.

13^{ο} ΚΕΦΑΛΑΙΟ

ΔΡΑΣΤΕΣ – ΘΥΜΑΤΑ – ΜΕΣΑ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

Εικόνα 13.1. Δράστες – θύματα – μέσα της νιγηριανής απάτης



(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

ΕΙΣΑΓΩΓΗ 13^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Σε αυτό το κεφάλαιο, θα προσπαθήσουμε να ψυχολογήσουμε και να αιτιολογήσουμε τους δράστες της νιγηριανής απάτης, αλλά και των θυμάτων της.

13.1 ΔΡΑΣΤΕΣ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

13.1.1 ΠΡΟΕΛΕΥΣΗ ΔΡΑΣΤΩΝ

Οι απατεώνες προέρχονται κυρίως από χώρες της Αφρικής, ιδιαίτερα τη Νιγηρία , την Ανατολική Ευρώπη, την Νοτιοδυτική Ασία και την Κίνα. Δεν ενεργούν όμως μόνο από τις χώρες τους, γιατι συνήθως είναι εξόριστοι, μέλη του προηγούμενου καθεστώτος της χώρας, οι οποίοι εξακολουθούν να έχουν προσβάσεις σε κάποια κομμάτια του κρατικού μηχανισμού. Έχουν εξαπλωθεί σε διάφορες χώρες και κυρίως στις ΗΠΑ, την Ολλανδία και την Ισπανία, το ΗΒ, τον Καναδά, την Ιαπωνία, την Αυστραλία και άλλες χώρες.

Εικόνα 13.2. Προέλευση δραστών της νιγηριανής απάτης

Origin	n
Nigeria	11
United Kingdom	10
South Africa	7
The Netherlands	7
Benin	5
Ivory Coast	5
Dubai	3
Russia	2
China/Hong Kong	2
Liberia	2
Italy	1
Zimbabwe	1
Ghana	1
Senegal	1

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

13.1.2 Η ΚΑΤΑΣΤΑΣΗ ΣΤΗΝ ΝΙΓΗΡΙΑ

Η παραγωγή πετρελαίου φτάνει τα 2,5 εκατομμύρια βαρέλια την ημέρα και η Νιγηρία φιγουράρει στην πρώτη εξάδα των πετρελαιοπαραγωγών χωρών, ενώ έχει την πέμπτη θέση στις παγκόσμιες εξαγωγές πετρελαίου προς τις ΗΠΑ.

Παρ' όλα αυτά, ενώ η χώρα είναι πλούσια σε μαύρο χρυσό, το μέσο κατά κεφαλή ετήσιο εισόδημα των Νιγηριανών δεν ξεπερνά τα 400 δολάρια και το 37% του πληθυσμού ζει σε συνθήκες απόλυτης φτώχειας, ενώ ένα πολύ μικρό τμήμα ζει... σε συνθήκες παραμυθένιου πλούτου. Η δε περιοχή που παράγει όλο τον πετρελαϊκό πλούτο της Νιγηρίας, το Δέλτα του Νίγηρα, είναι η περιοχή με τους φτωχότερους κατοίκους της χώρας.

Το 70% των ανθρώπων του Δέλτα ζει με λιγότερο από ένα δολάριο την ημέρα σε συνθήκες απόλυτης εξαθλίωσης. Η θνησιμότητα στην περιοχή είναι δυσανάλογα υψηλή σε σχέση με τις άλλες περιοχές της χώρας εξαιτίας των νοσημάτων που προέρχονται από το μολυσμένο νερό, την κακή διατροφή και την κακή ποιότητα των εγκαταστάσεων υγιεινής.

Η παροιμιώδης πλέον φράση "τα παιδιά της Μπιάφρας" βρίσκει ξανά το νόημά της αν κοιτάξει κανείς τους ανήλικους που λιμοκτονούν στην περιοχή. Ο ομώνυμος εμφύλιος πόλεμος άλλωστε, αυτός που από το 1967 έως το 1970 που τερματίστηκε άφησε πίσω του πάνω από ένα εκατομμύριο νεκρούς από ασιτία, συνέβη σε αυτή ακριβώς την περιοχή.

13.1.3 ΠΙΘΑΝΑ ΑΙΤΙΑ ΩΘΗΣΗΣ ΤΩΝ ΝΙΓΗΡΙΑΝΩΝ ΣΤΗΝ ΑΠΑΤΗ

Εξαιτίας του πολιτικού καθεστώτος στην Νιγηρία και της γενικότερης οικονομικής κατάστασης, οι πολίτες, οι οποίοι θεωρούνται αρκετά εύστροφοι, καταφεύγουν σε διάφορες απάτες, προκειμένου να εξασφαλίσουν χρήματα για την επιβίωσή τους.

Οι νιγηριανοί από παλιά (δεκαετίες 1970 και 1980) ήταν ειδικοί στις απάτες. Μαζεύονταν στις καφετέριες και σε άλλα εμπορικά μέρη του Λάγος και κατέστρωναν τα σχέδιά τους και τα υλοποιούσαν. Από πολύ νωρίς, σε σχέση με την μικρή οικονομική ανάπτυξη της χώρας, οι καφετέριες στο Λάγος είχαν τηλέφωνα, φάξ, φωτοτυπικά μηχανήματα, εξοπλισμός, που τους επέτρεπε να οργανώνουν καλά τις απάτες τους. Είναι ευρέως γνωστό πως το Λάγος είναι το κατάλληλο μέρος, όπου μπορούν όλα να συμβούν.

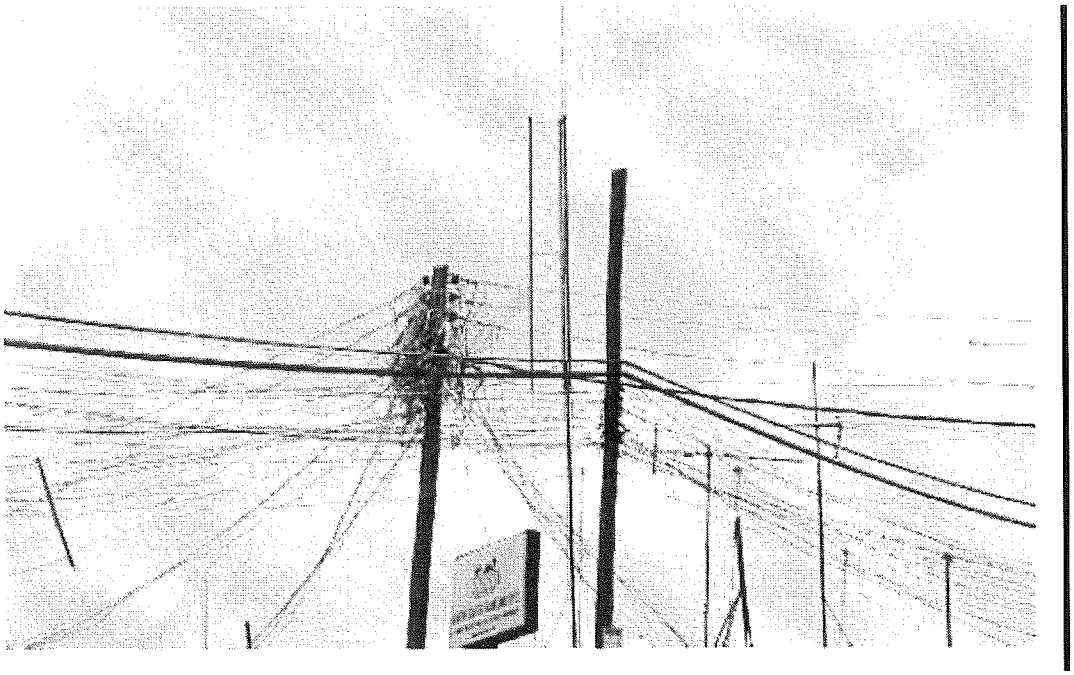
Οι διωκτικές αρχές της Μεγάλης Βρετανίας έχουν ήδη προβεί σε συλλήψεις που κατέληξαν σε καταδίκες, απ' ότι φαίνεται όμως υπάρχουν πολλές ξεχωριστές ομάδες η κάθε μια από τις οποίες "τρέχει" το δικό της σενάριο της απάτης.

Εικόνα 13.3. Τα τηλεφωνικά δίκτυα στο Λάγος

Pictured are some typical telephone lines in Lagos. It is very difficult for law enforcement officials to trace these telephone/fax lines to the perpetrators.

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

Εικόνα 13.4. Τα τηλεφωνικά δίκτυα στο Λάγος



(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

13.2 ΘΥΜΑΤΑ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

Η κεντρική ιδέα αυτής απάτης είναι αρκετά παλιά. Πάντα υπάρχουν άνθρωποι αρκετά εύπιστοι, απελπισμένοι ή άπληστοι που θα σκεφθούν σοβαρά την ιδέα του να πληρώσουν ένα σχετικά μικρό ποσό για να πάρουν ένα αρκετά μεγαλύτερο, από κάποιο άγνωστο και χωρίς να χρειαστεί να ιδρώσουν. Το internet απλά παρέχει ένα μέσο για ευρεία εξάπλωση του φαινομένου με τη ευκολία και την ταχύτητα που παρέχει στις επικοινωνίες.

Τα ερωτήματα, που γεννώνται στους περισσότερους ανθρώπους όταν λαμβάνουν νιγηριανές επιστολές, θα πρέπει να είναι:

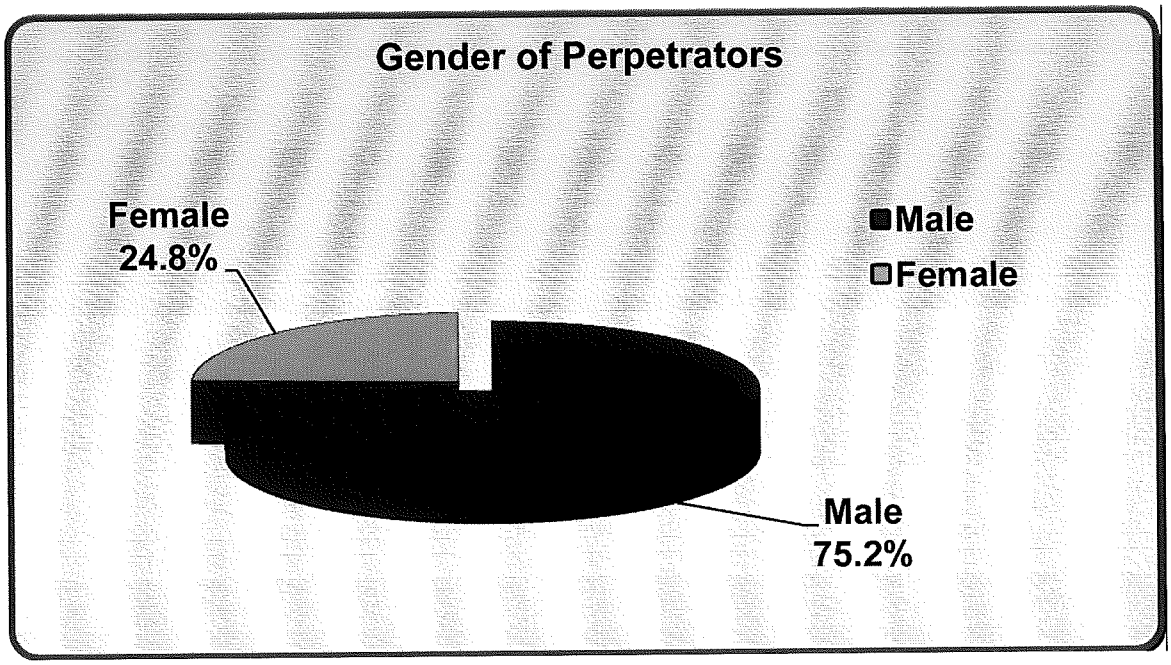
- Γιατί κάποιος να σε δελεάζει και να μοιραστεί μαζί σου μια ολόκληρη περιουσία;
- Γιατί εσύ να μοιραστείς πληροφορίες σχετικά με τον τραπεζικό σου λογαριασμό;
- Για ποιο λόγο να ταξιδέψεις σε μια χώρα σαν την Νιγηρία από την στιγμή που οι περισσότερες χώρες στις ταξιδιωτικές τους οδηγίες το αποτρέπουν;

Σίγουρα, λοιπόν, τα θύματα των νιγηριανών επιστολών:

- Νιώθουν είναι δυνατόν να κερδίσουν τόσα χρήματα τόσο εύκολα
- Νιώθουν ασφάλεια για να κάνουν συναλλαγές μέσω διαδικτύου
- Η ανωνυμία του διαδικτύου τους εξασφαλίζει πως δεν θα έχουν νομικά μπλεξίματα από την στιγμή, που δέχονται να συμμετάσχουν σε παράνομες ενέργειες.
- Είναι άνθρωποι που παίρνουν το ρίσκο να συμμετάσχουν σε μια παράνομη επιχείρηση.
- Κανείς δεν χρειάζεται να παραδεχθεί πως συμμετείχε σε κάτι τέτοιο.
- Το σίγουρο είναι πως θέλουν να γίνουν πλούσιοι γρήγορα. Είναι αυτό που λένε οι Αμερικάνοι «get rich quick».

Σύμφωνα με έρευνες , τα περισσότερα θύματα είναι άντρες.

Εικόνα 13.5. Το γένος των δραστών



(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

Παράλληλα, μιλώντας με όρους ψυχολογίας, ο χρήστης του internet είναι ιδιαίτερα ευάλωτος σε πολλές καταστάσεις, κυρίως εξαιτίας δύο βασικών ψευδαισθήσεων:

1. Η πρώτη έχει να κάνει με το αίσθημα ευφορίας και υπεροχής που του δημιουργεί η πρόσβαση σε τεράστιες ποσότητες πληροφορίας εύκολα, γρήγορα

και απλά. Ο χρήστης νιώθει επίσης ότι μπαίνει σε ένα κόσμο τεράστιων ευκαιριών και δυνατοτήτων οι οποίες τον περιμένουν να τις εκμεταλλευθεί. Πρόκειται για το λεγόμενο "σύνδρομο ευφορίας του διαδικτύου" το οποίο ελαττώνει σε εντυπωσιακό βαθμό τις άμυνες και τις αντιδράσεις που μπορεί ο ίδιος άνθρωπος να έχει στην καθημερινή του ζωή.

2. Η δεύτερη να κάνει με τη αίσθηση της ανωνυμίας πίσω από την οποία κρύβεται ο χρήστης και τον κάνει να νοιώθει πολύ σίγουρος για τον εαυτό του και κατά συνέπεια να τολμά πράγματα που στην "κανονική" ζωή του θα απέφευγε.

Με μια πρώτη ματιά τα δύο παραπάνω σημεία φαίνονται άσχετα με το θέμα μας, συνθέτουν όμως ένα ψυχογράφημα που έμμεσα αλλάζει την κανονική ροή λήψης αποφάσεων στο υποσυνείδητο.

Τέλος πρέπει κανείς να συνυπολογίσει το ότι τα ποσά τα οποία αναφέρονται είναι αρκετά για εξάψουν τη φαντασία και αφήσουν ακόμα και στον πιο λογικό την αμφιβολία "*και αν είναι αλήθεια?*"

Οι παραπάνω παράγοντες, ευπιστία-απελπισία-απληστία, οι ψευδαισθήσεις του διαδικτύου και το "βάρος" των ποσών, δημιουργούν ένα μίγμα εκρηκτικό και ουσιαστικά δίνουν την απάντηση στο ερώτημα που σίγουρα σας έρχεται στο μυαλό: *"είναι δυνατό κάποιος να πιστέψει μια τέτοια προσφορά?"*

Εικόνα 13.6. Ο τόπος της νιγηριανής απάτης

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

13.3 ΜΕΣΑ ΤΗΣ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

Η εκτεταμένη χρήση του διαδικτύου σε παγκόσμιο επίπεδο έχει οδηγήσει σε ελαχιστοποίηση του κόστους και σε μεγιστοποίηση του κέρδους για τους δράστες της νιγηριανής απάτης

Γενικά μέχρι και σήμερα τα μέσα της απατής είναι τα ακολουθά, τα οποία χρησιμοποιούνται και από τους δράστες της νιγηριανής απάτης:

Εικόνα 13.7. Τα μέσα της νιγηριανής απάτης

Mail
Fax
Phone
E-mail
Chat rooms
Dating web sites
Matchmaking web sites
Mobile phone SMS
Internet phone
Internet gaming (new)
Personal introduction
Web sites publishing general business contacts or for specific industries
Call centre / boiler-room
Door-to-door - in countries were an internet connection or sometimes phone or fax connections are not yet common circumstances.

(Πηγή: www.ultrascan.nl/html/419_advance_fee_fraud.html)

13.4 ΣΥΜΠΕΡΑΣΜΑΤΑ 13^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Κατά συνέπεια όλοι οι χρήστες του διαδικτύου είναι υποψήφια θύματα και αυτό αποτελεί μεγάλη πρόκληση για τους απατεώνες διότι καλύπτονται από την ανωνυμία μέσα στο πλήθος. Οι τελευταίοι δεν είναι αναγκασμένοι να αναζητούν τα θύματά τους αλλά αντίθετα τα θύματα πέφτουν από μόνα τους στην παγίδα. Στις περισσότερες φορές μάλιστα, κάποιοι γίνονται θύματα χωρίς καν να το αντιληφθούν, ενώ άλλοι αν και υποψιάζονται ότι κάτι δεν πάει καλά, ρισκάρουν διότι τους ελκύει το άγνωστο. Αυτό που εκμεταλλεύονται οι απατεώνες, είναι η μη επαρκής πληροφόρηση των χρηστών του διαδικτύου για τον κίνδυνο που διατρέχουν σε περίπτωση που "τρέξουν" σε μια άγνωστη ιστοσελίδα ή σε περίπτωση που απαντήσουν σε μήνυμα που απέστειλε κάποιος άγνωστος ή ακόμα στην περίπτωση που κάνουν "κλίκ" σε ένα άγνωστο "μονοπάτι". Γι' αυτό όλοι οι χρήστες του διαδικτύου πρέπει να ενημερώνονται και να λαμβάνουν με δική τους πρωτοβουλία μέτρα ασφαλείας, σε συνεργασία με τον παροχέα τους. Προέχει λοιπόν η πρόληψη, αφού σε περίπτωση που χάσει κάποιος τα χρήματά του, είναι δύσκολο αν όχι αδύνατο να τα ανακτήσει. Ο εντοπισμός των δραστών είναι δύσκολος διότι δεν εμφανίζονται με την πραγματική τους ταυτότητα, οι διευθύνσεις που δίδουν είναι ψευδείς ή ανύπαρκτες και οι αριθμοί τηλεφώνων τους δεν είναι καταχωρημένοι (so easy).

14^{ο} ΚΕΦΑΛΑΙΟ

ΠΑΡΑΔΕΙΓΜΑ ΝΙΓΗΡΙΑΝΗΣ ΑΠΑΤΗΣ

Καθώς δεν κατάφερα να εμπλακώ εγώ η ίδια προσωπικά σε κάποια περίπτωση νιγηριανής απάτης, θεώρησα απαραίτητο να παραθέσω μια περίπτωση ενός χρήστη του διαδικτύου και θύμα νιγηριανής απάτης, που μας εξιστορεί στο www.e-forum.gr τον Φεβρουάριο του 2009. Θα παρακολουθήσουμε το πώς χειρίστηκε τα e-mail, που έλαβε και μέχρι που έφτασε με τους δράστες.

Την πρώτη φορά που επικοινώνησαν μαζί του ανακοίνωσαν ότι κέρδισε €1,000,000 σε κάποια ευρωπαϊκή λοταρία.

Αποφάσισε, λοιπόν, να διεκδικήσει τα χρήματά του!

Προσέξτε το πρώτο email που έλαβε:

CONFIRM YOUR 2009 YEARLY AWARD !!!

We are happy to inform you that you have emerged a winner under the Second Category of our promotion , Winners were picked by computerized system, drawn from companies and individuals e-mail addresses worldwide. The draws are officially announced 17th of Febuary, 2009. You have being therefore been awarded a lump sum of Ƀ1,000,000.00(One Million Euros), which is the winning pay out for Category A winners.

NOTE: For easy reference and identification,find below your Reference Number, Batch numbers, Ticket Number. Remember to quote these numbers in your correspondence to our claim Department and also the following informations;

****
[I] Reference Number: 705/120/422/NL
[ii] Ticket Number: TL072/05/009
[iii]Batch Number: 6994041-033-BN
[iv]Serial Number: 9-60-17-19-1805
[v] Lucky Number: SPL 81/1048
****
Please contact Sponsorlotterij Claim department immediately for due processing and remittance of your prize money to Your designated account of your choice:
****
Dr Deborah Lenert.
Mr.Mirk Van Bossen.
Tel: +31-641-687-250
EMAIL: sponsordptagency@gmail.com

****
Sincerely Yours,
Mrs.Stefania Van Piet.

Public Relation Officer.
http://www.sponsorbingoloterij.nl

Δημιούργησε, λοιπόν, ένα λογαριασμό σε ένα free mail και τους απάντησε παριστάνοντας τον αφελή παραλήπτη που δεν έχει ιδέα για τι πράγμα του μιλάνε:

Dear Mrs Lenert,

I received the following email from you.
I suppose it is a mistake since I have bought anything from your company.

Regards,

Σημειώστε ότι το email το έστειλαν στη διεύθυνση name.surname@mymail.com και εκείνος τους έστειλε το παραπάνω από μία εντελώς διαφορετική διεύθυνση υπογράφοντας με διαφορετικό όνομα. Πάντως του απάντησαν μερικές μέρες μετά για να του επιβεβαιώσουν ότι πραγματικά είμαι αυτός ο νικητής, ότι η ημερομηνία λήξης της προθεσμίας για να παραλάβει το βραβείο των €1,000,000 λήγει στις 15 Μαρτίου και ότι πρέπει να τυπώσει, να συμπληρώσει, να υπογράψει και επιστρέψει μία φόρμα με διάφορα προσωπικά του στοιχεία.

Δείτε αποσπάσματα της επιστολής (με κόκκινο σημειώνω τα αξιοσημείωτα σημεία):

SponsorLoterij/ Financial Bv.
(Financial Consultants and Experts) Amsterdam. The Netherlands.
From The Desk of Mirk Van Bossen.
{Foreign Service manager/Accredited Lottery Claim Agent In Amsterdam}
Direct Phone Line:+31-641-687-250
Direct Fax Line: +31-847-539-067
****
****
****
OUR REF:KFSBV/LPA/SP071/AMS-NL
****
**********A
ttn:Dear Lucky Winner:{S.G}

RE:YOUR LOTTERY PRIZE AWARD CLAIM.
Congratulations and happy new year.

This is to confirm receipt of your messages regarding your Won-Prize Money of 1,000,000.00 euros(One Million Euros only) in the Lottery Promotions of the Sponsor Loterij Awards International Amsterdam The Netherlands.

We quite understand your surprise and skepticism, hence we write to give you clear details and modalities of the Government stipulated requirements for the Claim of Your Won-Prize and to assure you that this is a legitimate and authentic Email Sweepstake lottery promotions which is internet based and was carried out with the aid of the E-ballotting system that randomly selects different email addresses of individuals and organisations

from arround the globe,Hence you did not have to play the lottery directly but because you are an internet user your email address was selected and fortunately it won one of the slots for this prize award.

You must be aware that our management was officially selected as your appointed claim agent in ensuring that your prize is transffered to your custody by the paying bank in accordance with stipulated government laws and we would be deligthed if you gave your full cooperation to make the discharge of our duties easier and straight forward. Be informed that the official paying bank for the lottery promotions is here in European Union and that is why we were appointed your claim agents to help facillitate all processes regarding your prize claim.

It is imperative that we inform you that the deadline for the claim of won-prizes as specified by the organisers of this program is 15TH MARCH, 2009. Hence you are adviced to follow our directives as your approved and appointed agent.We have the expertise and means to assist you have to receive payment of your winning claims being amount due to you as one of the grand prize winners.We are sending you a Payment Scheme/Claim Form attached to this mail which you are required to download, print it out and fill in all required necessary details.This form should either be faxed back or sent through email.

Be informed that you will be required to have the Processing,verification,legalisation and notorisation of your claim to be carried out by yourself or by our attorney in your favour which is very important and necessary because thereafter your Prize Claim Certificate and other Winning documents will be secured giving full authority as lucky winner to receive your prize and with that Transfer Authorisation and Clearance would be obtained in your name and favour so as the Authorized paying bank can transfer your prize to your nominated bank account or send you your winning check depending on the option you prefer to receive your prize. Note that your total prize-money has been insured to its real value and as such cannot be deducted from being in the custody of the paying bank awaiting transfer and payment authorisation. And the Insurance policy of your Won-Prize stipulates this.

This is in accordance with section 13(1) (n) of the national gambling act as adopted in 1993 and amended on 3rd July 1996 by the constitutional assembly, this is to protect winners and to avoid misappropriation of funds. Your certificate of prize Claims would be obtained after our attorney has rounded up with the required processes.Be aware that your winnings will be transferred within 72 banking hours to your nominated bank account after the receipt of all the requirements. If you prefer to receive your winning via certified bank check it is very possible as long as the requirements are met as stipulated by law.You are adviced to send along with the claim form your international passport or Driver's license for proper identification/verification and documentations.

Congratulations once again and for any clarifications do endeavour to call the direct line above.

Best Regards,
Mirk Van Bossen
sponsordptagency@gmail.com
http://www.sponsorbingoloterij.nl

Πρέπει να πούμε πως αναφέρουν νόμους, φαίνεται ότι διαθέτουν τηλεφωνικό κέντρο εξυπηρέτησης, παραθέτουν ένα website που όμως είναι στα ολλανδικά (φαντάζομαι) και η επιστολή είναι επώνυμη. Όλα αυτά φαίνονται καλά αλλά:

- το βρίσκω εξαιρετικά απίθανο να κερδίσει κάποιος οτιδήποτε πόσο μάλλον αν ΔΕΝ έχει καν συμμετάσχει στη λοταρία και μάλιστα για το αστρονομικό ποσό του 1 εκατομμυρίου ευρώ,
- το κείμενο έχει σοβαρά συντακτικά και ορθογραφικά λάθη,
- το περιεχόμενο είναι έτσι σχεδιασμένο για να δίνει την αίσθηση της πλήρους πληροφόρησης,
- το βραβείο το είχε κερδίσει το συγκεκριμένο πρόσωπο και ΟΧΙ ο δεύτερος που τους απάντησε [δεν ξέρουν ότι είναι το ίδιο πρόσωπο],
- καμία λοταρία δεν ειδοποιεί το νικητή με email,
- καμία διαδικασία παραλαβής των χρημάτων δεν γίνεται μέσω internet.

Οι τύποι αυτοί διαθέτουν ένα σωρό από κινητά τηλέφωνα πάνω στα οποία είναι κολλημένα τα εξής δύο στοιχεία ώστε να ξέρουν πώς να απαντήσουν σε κάθε κλήση:

- Το όνομα του αποστολέα του κάθε email
- Το σενάριο που θα πουν στον καλούντα

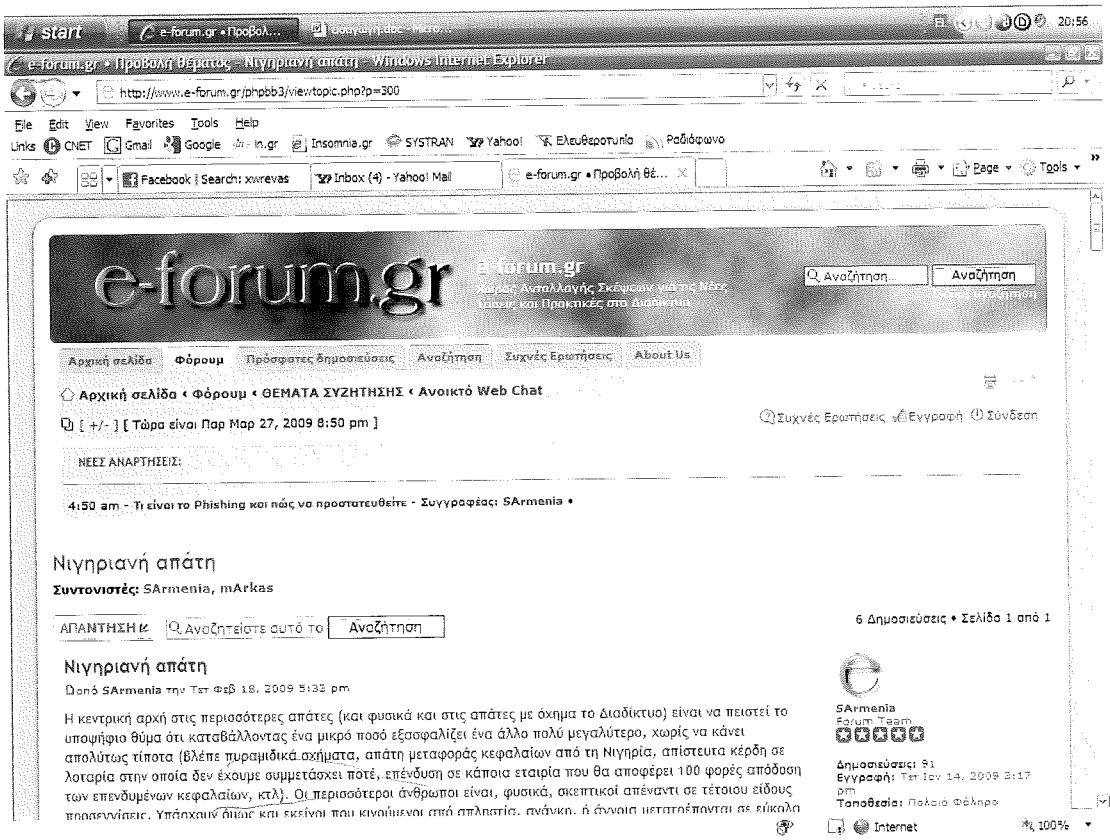
Για να δει μέχρι που θα φτάσουν τους έστειλε ως απάντηση το παρακάτω (επίτηδες ανορθόγραφα ώστε να πιστέψουν [θα το πιστέψουν άραγε;] ότι δεν τους την έχει στημένη:

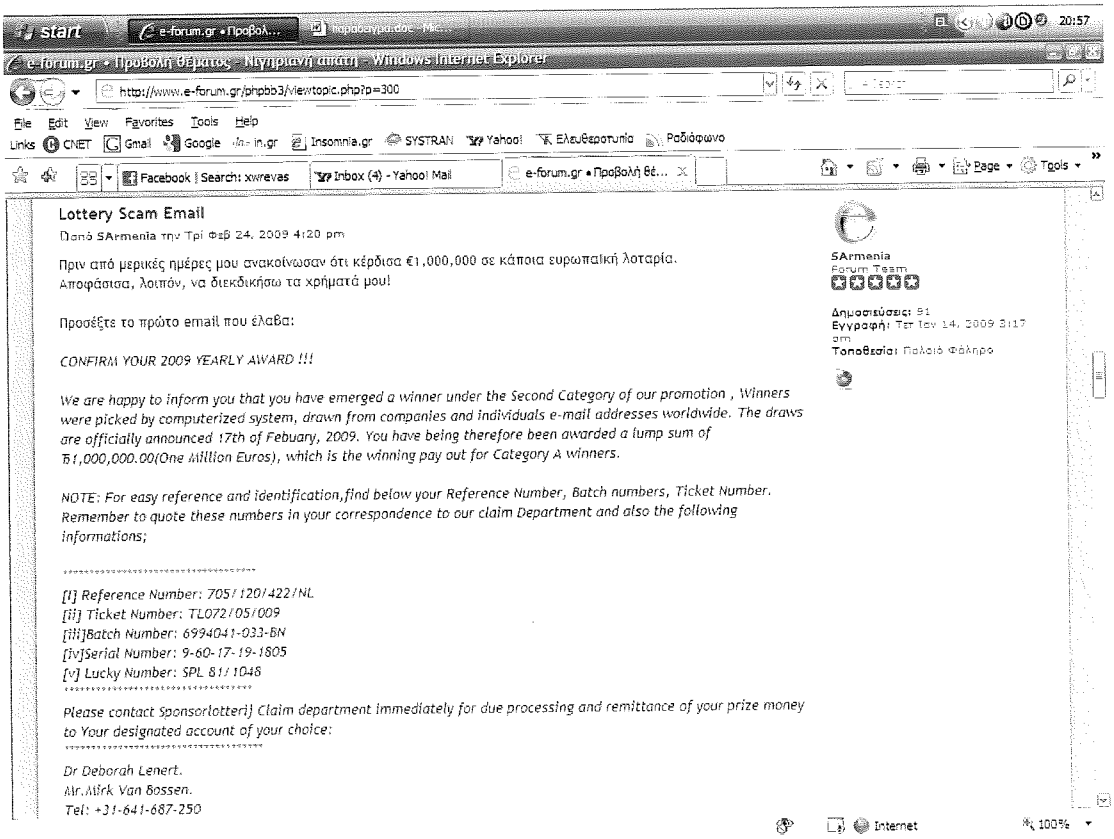
Hi,
I dont have a printer available. Can we speed up the process by senting you the requested information with email;

Σε συνέχεια της αλληλογραφίας με τους απατεώνες στην ερώτησή για το αν μπορει να τους στείλει τα στοιχεία του με ένα απλό email απάντησαν πως ναι μπορει. Και τους έστειλε πλέον το εξής:

I asked a friend and she told me that this is a fraud.
Do you have any proof? Document from the goverment? The picture of your office?

Και φυσικά μετά από αυτό διέκοψαν κάθε επικοινωνία.





Πριν από μερικές ημέρες μου ανακοίνωσαν ότι κέρδισα €1,000,000 σε κάποια ευρωπαϊκή λοταρία.
Αποφάσισα, λοιπόν, να διεκδικήσω τα χρήματά μου!

Προσέξτε το πρώτο email που έλαβα:

CONFIRM YOUR 2009 YEARLY AWARD !!!

We are happy to inform you that you have emerged a winner under the Second Category of our promotion , Winners were picked by computerized system, drawn from companies and individuals e-mail addresses worldwide. The draws are officially announced 17th of Febuary, 2009. You have being therefore been awarded a lump sum of $1,000,000.00(One Million Euros), which is the winning pay out for Category A winners.

NOTE: For easy reference and identification,find below your Reference Number, Batch numbers, Ticket Number. Remember to quote these numbers in your correspondence to our claim Department and also the following informations;

****

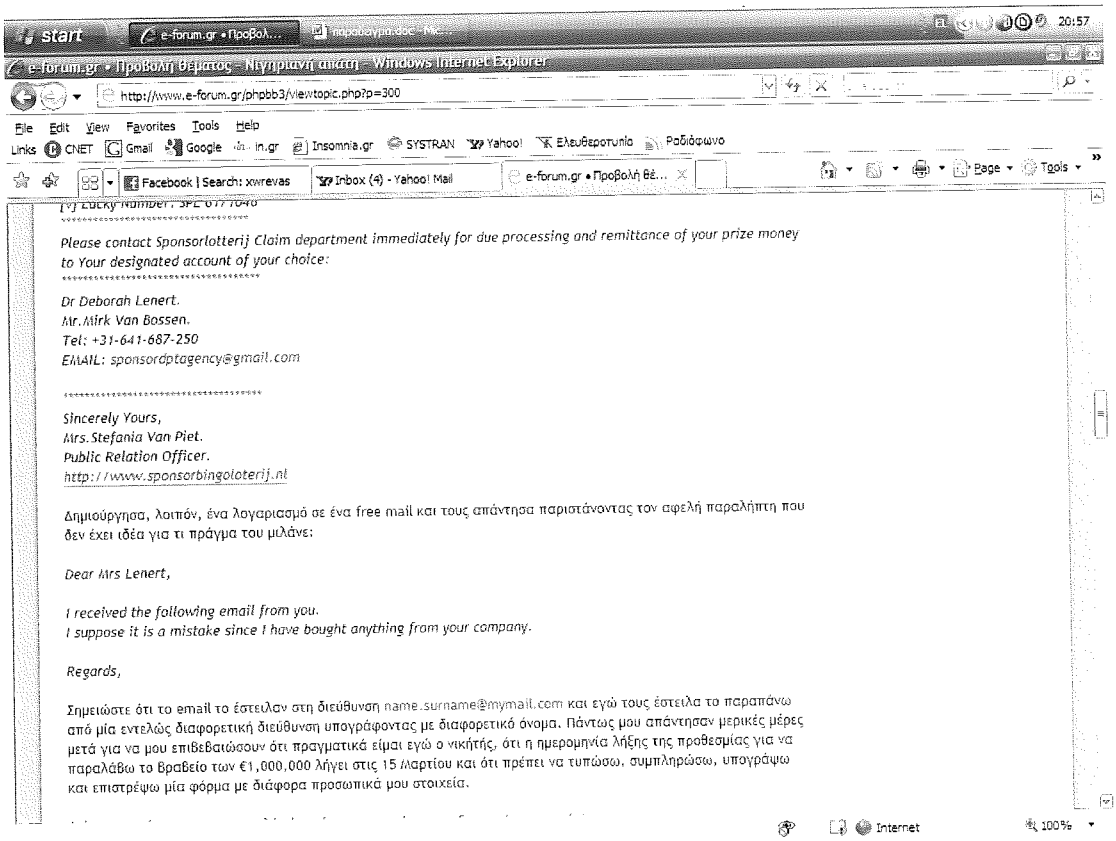
[i] Reference Number: 705/120/422/NL
[ii] Ticket Number: TL072/05/009
[iii]Batch Number: 6994041-033-BN
[iv]Serial Number: 9-60-17-19-1805
[v] Lucky Number: SPL 81/1048

****

Please contact Sponsorlotteri} Claim department immediately for due processing and remittance of your prize money to Your designated account of your choice:

****

Dr Deborah Lenert.
Mr.Mirk Van Bossen.
Tel: +31-641-687-250



Please contact Sponsorlotterij Claim department immediately for due processing and remittance of your prize money to Your designated account of your choice:

Dr Deborah Lenert.
Mr.Mirk Van Bossen.
Tel: +31-641-687-250
EMAIL: sponsordptagency@gmail.com

Sincerely Yours,
Mrs.Stefania Van Piet.
Public Relation Officer.
http://www.sponsorbingoloterij.nl

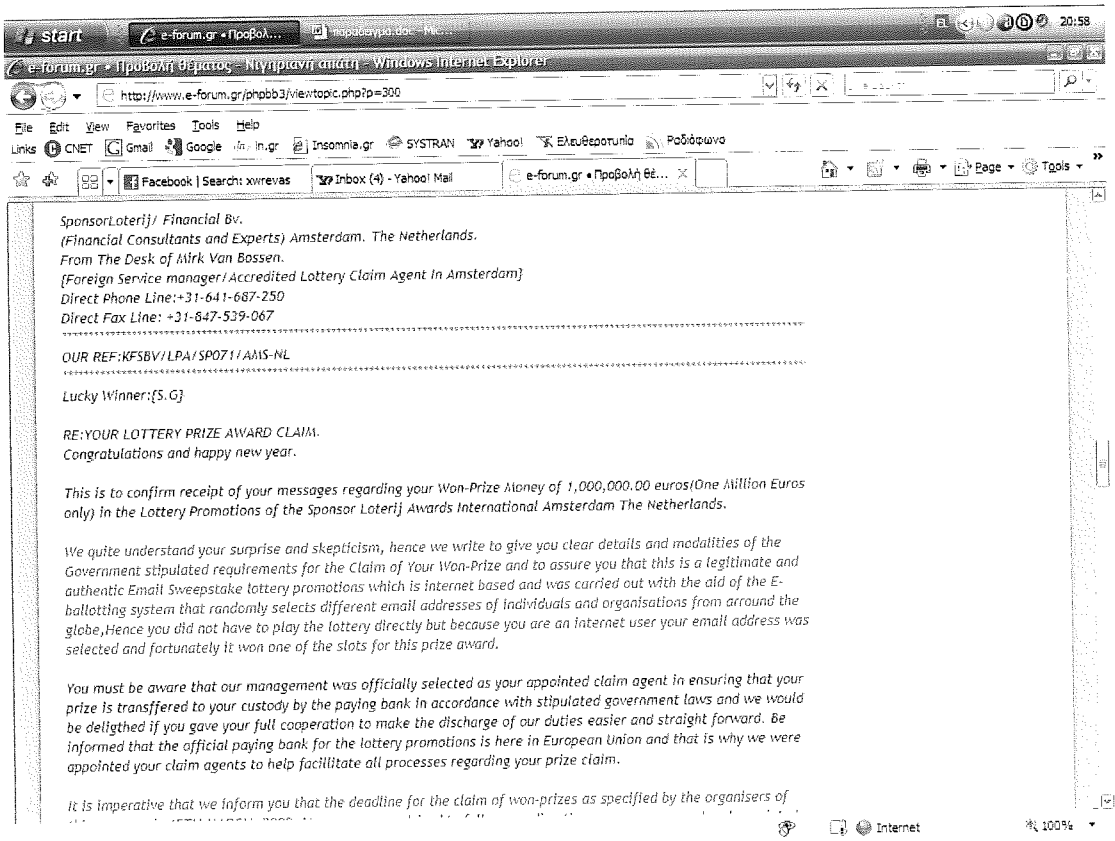
Δημιούργησα, λοιπόν, ένα λογαριασμό σε ένα free mail και τους απάντησα παριστάνοντας τον αφελή παραλήπτη που δεν έχει ιδέα για τι πράγμα του μιλάνε:

Dear Mrs Lenert,

I received the following email from you.
I suppose it is a mistake since I have bought anything from your company.

Regards,

Σημειώστε ότι το email το έστειλαν στη διεύθυνση name.surname@mymail.com και εγώ τους έστειλα το παραπάνω από μία εντελώς διαφορετική διεύθυνση υπογράφοντας με διαφορετικό όνομα. Πάντως μου απάντησαν μερικές μέρες μετά για να μου επιβεβαιώσουν ότι πραγματικά είμαι εγώ ο νικητής, ότι η ημερομηνία λήξης της προθεσμίας για να παραλάβω το βραβείο των €1,000,000 λήγει στις 15 Μαρτίου και ότι πρέπει να τυπώσω, συμπληρώσω, υπογράψω και επιστρέψω μία φόρμα με διάφορα προσωπικά μου στοιχεία.



SponsorLoterij/ Financial Bv.
(Financial Consultants and Experts) Amsterdam. The Netherlands.
From The Desk of Mirk Van Bossen.
(Foreign Service manager/ Accredited Lottery Claim Agent in Amsterdam)
Direct Phone Line:+31-641-687-250
Direct Fax Line: +31-847-539-067

OUR REF:KFSBV/LPA/SP071/AMS-NL

Lucky Winner:(S.G)

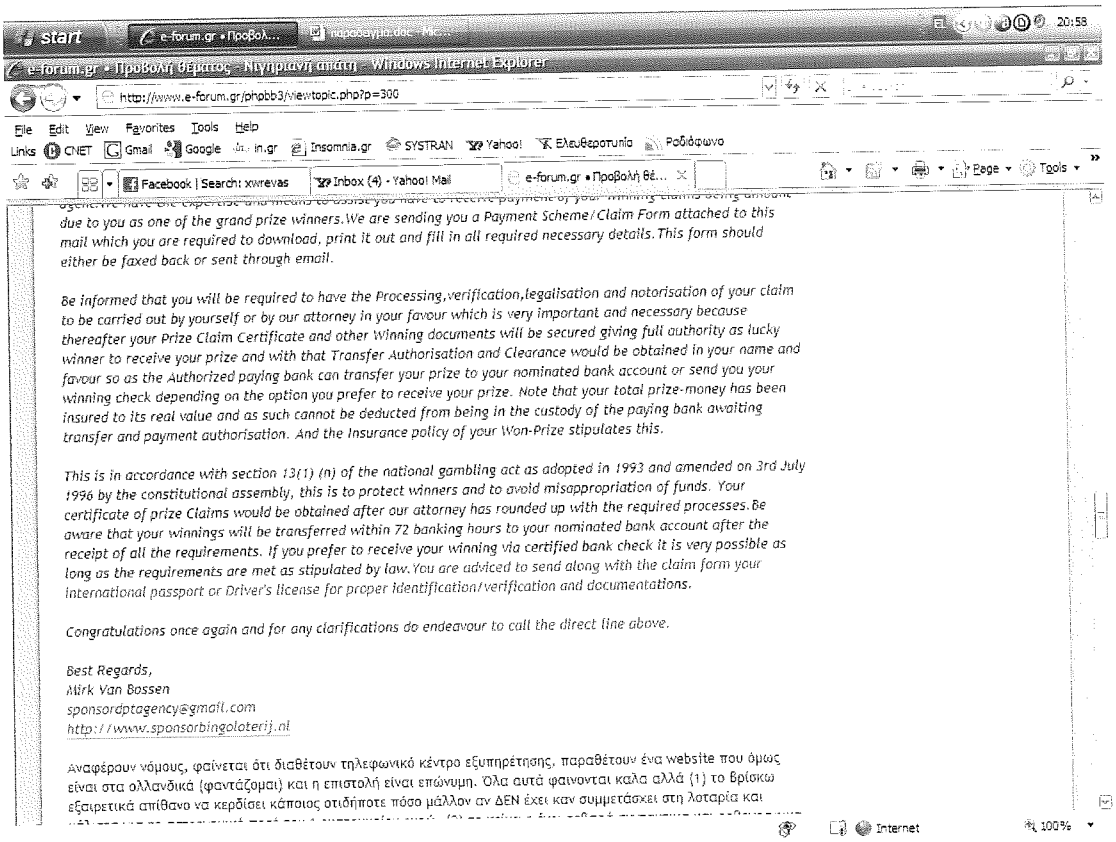
RE:YOUR LOTTERY PRIZE AWARD CLAIM.
Congratulations and happy new year.

This is to confirm receipt of your messages regarding your Won-Prize Money of 1,000,000.00 euros(One Million Euros only) in the Lottery Promotions of the Sponsor Loterij Awards International Amsterdam The Netherlands.

We quite understand your surprise and skepticism, hence we write to give you clear details and modalities of the Government stipulated requirements for the Claim of Your Won-Prize and to assure you that this is a legitimate and autheatic Email Sweepstake lottery promotions which is internet based and was carried out with the aid of the E-ballotting system that randomly selects different email addresses of individuals and organisations from arround the globe,Hence you did not have to play the lottery directly but because you are an internet user your email address was selected and fortunately it won one of the slots for this prize award.

You must be aware that our management was officially selected as your appointed claim agent in ensuring that your prize is transffered to your custody by the paying bank in accordance with stipulated government laws and we would be deligthed if you gave your full cooperation to make the discharge of our duties easier and straight forward. Be informed that the official paying bank for the lottery promotions is here in European Union and that is why we were appointed your claim agents to help facilitate all processes regarding your prize claim.

It is imperative that we inform you that the deadline for the claim of won-prizes as specified by the organisers of



due to you as one of the grand prize winners.We are sending you a Payment Scheme/Claim Form attached to this mail which you are required to download, print it out and fill in all required necessary details.This form should either be faxed back or sent through email.

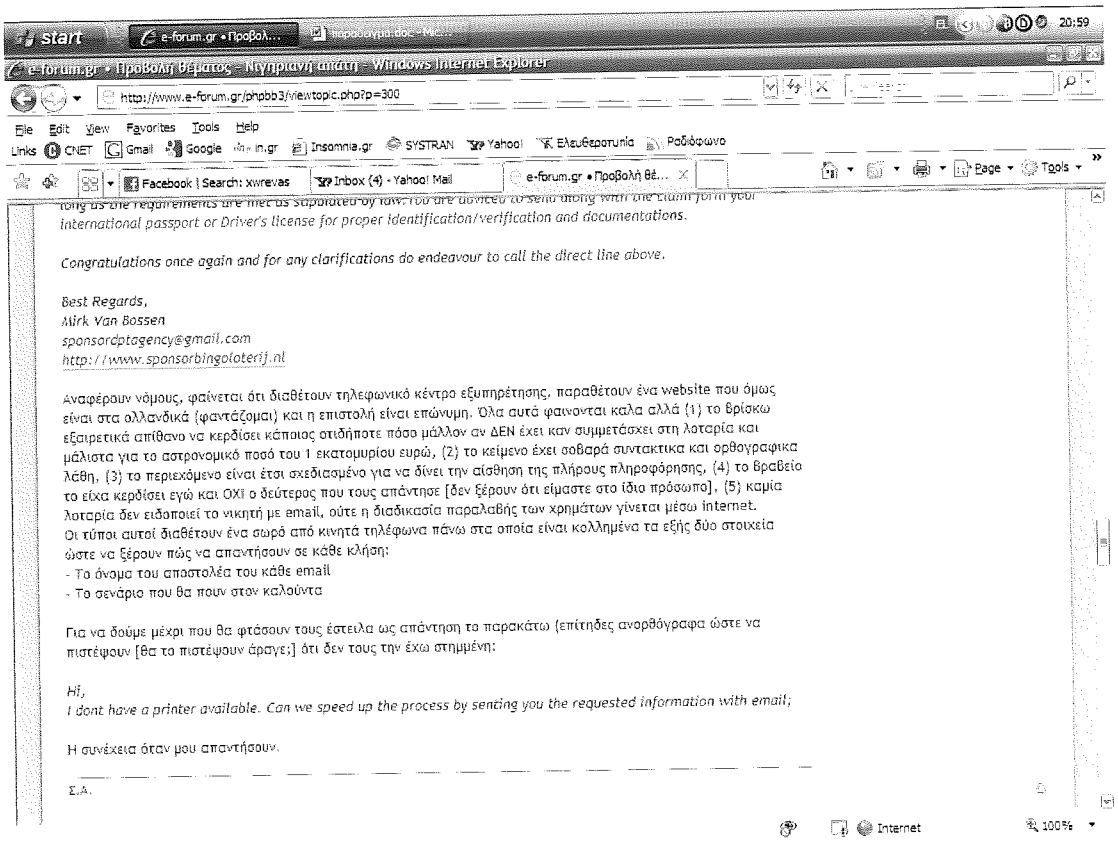
Be informed that you will be required to have the Processing,verification,legalisation and notorisation of your claim to be carried out by yourself or by our attorney in your favour which is very important and necessary because thereafter your Prize Claim Certificate and other Winning documents will be secured giving full authority as lucky winner to receive your prize and with that Transfer Authorisation and Clearance would be obtained in your name and favour so as the Authorized paying bank can transfer your prize to your nominated bank account or send you your winning check depending on the option you prefer to receive your prize. Note that your total prize-money has been insured to its real value and as such cannot be deducted from being in the custody of the paying bank awaiting transfer and payment authorisation. And the Insurance policy of your Won-Prize stipulates this.

This is in accordance with section 13(1) (n) of the national gambling act as adopted in 1993 and amended on 3rd July 1996 by the constitutional assembly, this is to protect winners and to avoid misappropriation of funds. Your certificate of prize Claims would be obtained after our attorney has rounded up with the required processes.Be aware that your winnings will be transferred within 72 banking hours to your nominated bank account after the receipt of all the requirements. If you prefer to receive your winning via certified bank check it is very possible as long as the requirements are met as stipulated by law.You are adviced to send along with the claim form your international passport or Driver's license for proper identification/verification and documentations.

Congratulations once again and for any clarifications do endeavour to call the direct line above.

Best Regards,
Mirk Van Bossen
sponsordptagency@gmail.com
http://www.sponsorbingoloterij.nl

Αναφέρουν νόμους, φαίνεται ότι διαθέτουν τηλεφωνικό κέντρο εξυπηρέτησης, παραθέτουν ένα website που όμως είναι στα ολλανδικά (φαντάζομαι) και η επιστολή είναι επώνυμη. Όλα αυτά φαινονται καλα αλλά (1) το βρίσκω εξαιρετικά απίθανο να κερδίσει κάποιος οτιδήποτε πάσο μάλλον αν ΔΕΝ έχει καν συμμετάσχει στη λοταρία και



long as the requirements are met as stipulated by law.You are adviced to send along with the claim form your international passport or Driver's license for proper identification/verification and documentations.

Congratulations once again and for any clarifications do endeavour to call the direct line above.

Best Regards,
Mirk Van Bossen
sponsordptagency@gmail.com
http://www.sponsorbingoloterij.nl

Αναφέρουν νόμους, φαίνεται ότι διαθέτουν τηλεφωνικό κέντρο εξυπηρέτησης, παραθέτουν ένα website που όμως είναι στα ολλανδικά (φαντάζομαι) και η επιστολή είναι επώνυμη. Όλα αυτά φαινονται καλα αλλά (1) το βρίσκω εξαιρετικά απίθανο να κερδίσει κάποιος οτιδήποτε πάσο μάλλον αν ΔΕΝ έχει καν συμμετάσχει στη λοταρία και μάλιστα για το αστρονομικό ποσό του 1 εκατομμυρίου ευρώ, (2) το κείμενο έχει σοβαρά συντακτικα και ορθογραφικα λάθη, (3) το περιεχόμενο είναι έτσι σχεδιασμένο για να δίνει την αίσθηση της πλήρους πληροφόρησης, (4) το βραβείο το είχα κερδίσει εγώ και ΟΧΙ ο δεύτερος που τους απάντησε [δεν ξέρουν ότι είμαστε στο ίδιο πρόσωπο], (5) καμία λοταρία δεν ειδοποιεί το νικητή με email, ούτε η διαδικασία παραλαβής των χρημάτων γίνεται μέσω internet.
Οι τύποι αυτοί διαθέτουν ένα σωρό από κινητά τηλέφωνα πάνω στα οποία είναι κολλημένα τα εξής δύο στοιχεία ώστε να ξέρουν πώς να απαντήσουν σε κάθε κλήση:
- Το όνομα του αποστολέα του κάθε email
- Το σενάριο που θα πουν στον καλούντα

Για να δούμε μέχρι που θα φτάσουν τους έστειλα ως απάντηση τα παρακάτω (επίτηδες ανορθόγραφα ώστε να πιστέψουν [θα το πιστέψουν άραγε;] ότι δεν τους την έχω στημμένη:

Hi,
I dont have a printer available. Can we speed up the process by senting you the requested information with email;

Η συνέχεια όταν μου απαντήσουν.

Σ.Α.

15^{ο} ΚΕΦΑΛΑΙΟ

ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΓΙΑ ΤΙΣ ΟΙΚΟΝΟΜΙΚΕΣ ΑΠΩΛΕΙΕΣ ΑΠΟ ΤΗΝ ΝΙΓΗΡΙΑΝΗ ΑΠΑΤΗ

Οι υποθέσεις που καταγγέλθηκαν και διερευνήθηκαν από την Αστυνομία σε σχέση με απάτες μέσω διαδικτύου από το γραφείο διερεύνησης οικονομικού εγκλήματος του αρχηγείου της αστυνομίας τον Αύγουστο 2008, είναι:

Κατά το έτος 2003 διερευνήθηκαν οκτώ υποθέσεις

- μια υπόθεση απόσπασης χρημάτων που σχετίζεται με χρήση κλοπιμαίων προσωπικών στοιχείων
- τέσσερις υποθέσεις που σχετίζονται με αγορά εμπορευμάτων
- τρεις υποθέσεις που σχετίζονται με προκαταβολές για δήθεν κέρδη από λαχεία ή κληρονομιές.

Κατά το έτος 2004 διερευνήθηκαν τρεις υποθέσεις

- μια υπόθεση που σχετίζεται με αγορά εμπορευμάτων
- δυο υποθέσεις που σχετίζονται με προκαταβολές για δήθεν κέρδη από λαχεία ή κληρονομιές.

Κατά το έτος 2005 διερευνήθηκαν οκτώ υποθέσεις

- πέντε υποθέσεις απόσπασης χρημάτων που σχετίζεται με χρήση κλοπιμαίων προσωπικών στοιχείων
- δυο υποθέσεις που σχετίζονται με αγορά εμπορευμάτων
- μια υπόθεση που σχετίζεται με προκαταβολές για δήθεν κέρδη από λαχεία ή κληρονομιές.

Κατά το έτος 2006 καταγγέλθηκαν δώδεκα υποθέσεις

- δυο υποθέσεις απόσπασης χρημάτων που σχετίζονται με χρήση κλοπιμαίων προσωπικών στοιχείων τραπεζικών καρτών
- πέντε υποθέσεις που σχετίζονται με αγορά εμπορευμάτων
  (συνολική ζημιά € 44.000)
- πέντε υποθέσεις υποκλοπής προσωπικών στοιχείων πελατών τραπεζών μέσω διαδικτύου και κλοπής χρημάτων από λογαριασμούς τους
  (συνολική ζημιά € 40.000)

ΣΗΜΕΙΩΣΗ: Για τις πέντε τελευταίες υποθέσεις του 2006 συνελήφθηκαν τρία πρόσωπα (δυο από την Νιγηρία και ένας Κύπριος) και καταζητούνται άλλα δυο από την Νιγηρία. Οι συλληφθέντες οδηγήθηκαν στο δικαστήριο και η δίκη τους εκκρεμεί.

Κατά το έτος 2007 καταγγέλθηκαν 26 υποθέσεις:

- Μια υπόθεση απόσπασης χρημάτων που σχετίζεται με απάτη τύπου «Νιγηρίας» « κέρδος σε κλήρωση » , (συνολική ζημιά € 1.500)
- 19 υποθέσεις που σχετίζονται με αγορά εμπορευμάτων (11 αυτοκίνητα, 1 κινητό, Η/Υ, παιχνίδια.) ,(συνολική ζημιά € 200.000 περίπου)
- Μια υπόθεση πώλησης αυτοκινήτου και απόπειρα απόσπασης χρημάτων από τον πωλητή.
- 4 υποθέσεις υποκλοπής προσωπικών στοιχείων πελατών τραπεζών μέσω διαδικτύου και κλοπής χρημάτων από λογαριασμούς τους (συνολική ζημιά £ 20.000 περίπου)
- Μια υπόθεση υποκλοπής προσωπικών στοιχείων πελατών τραπεζών μέσω διαδικτύου και απόπειρας κλοπής χρημάτων από λογαριασμούς τους (αναμενόμενη ζημιά £ 31.600)

Για ορισμένες από τις πιο πάνω υποθέσεις συνελήφθηκαν συνολικά 5 πρόσωπα.

Κατά το έτος 2008 καταγγέλθηκαν μέχρι στιγμής 12 υποθέσεις

- 9 υποθέσεις αγοράς εμπορευμάτων (5 αυτοκίνητα, 1 σκάφος, 2 τηλέφωνα, μέλι) (συνολική ζημιά STR £ 24.000 και $ 144.000 περίπου)
- 2 υποθέσεις αγοράς χρόνου ομιλίας και αεροπορικών εισιτηρίων με την χρήση κλεμμένων αριθμών πιστωτικών καρτών ξένων τραπεζών. (συνολική ζημιά £ 7.000 περίπου), συνελήφθηκαν στην Κύπρο συνολικά 2 πρόσωπα αλλοδαποί.
- Δέκα υποθέσεις μεταφοράς χρημάτων από τραπεζικούς λογαριασμούς Μέθοδος Phishing (€100.000)

www.police.gov.cy/police

Για να τεκμηριώσουμε όλα αυτά που έχουμε παραθέσει μέχρι τώρα θα παρουσιάσουμε στατιστικά στοιχεία σχετικά με την νιγηριανή απάτη και τις χώρες, που εμφανίζεται, με τις οικονομικές απώλειες που επακολουθούν και με τα διάφορα εγκλήματα, που σχετίζεται. Θα παρουσιάσουμε πως η νιγηριανή απάτη αφορά όλες τις χώρες του κόσμου.

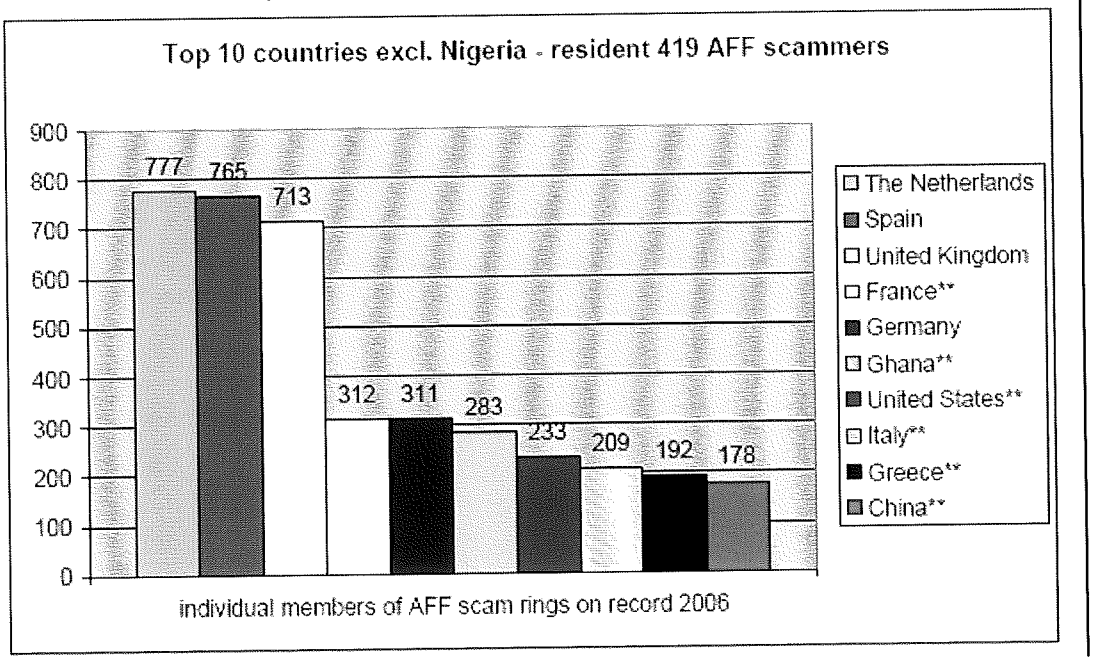
Πίνακας 15.1. Καταγραφή της νιγηριανής απάτης σε διάφορές χώρες

419Unit release January 23 2007		on our records*			
Nigerian Advance Fee Fraud on record* and low estimates for the countries listed below.		AFF resident active scam rings 2006	2005	individual members of AFF scam rings 2006	2005
Argentina				3	
Australia		5	2	23	12
Austria		2	2	51	62
Belgium		4	3	81	72
Bolivia					
Brazil**		3		24	
Bulgaria		1	1	21	32
Cameroon					
Canada***		6	5	62	79
Chile					
China**		12	2	178	73
Colombia		1		3	
Croatia				1	
Cyprus		2	1	5	2
Denmark		2	2	25	26
Dubai		5	2	18	2
Egypt		4	2	19	15
Finland		1	1	6	5
France**		9	7	312	127
Gambia				4	
Germany		9	10	311	275
Ghana**		16	4	283	124
Greece**		12	4	192	155
Hong Kong **		2		12	
Hungary**		2	2	18	16
India**		7	3	107	79
Indonesia		1		6	
Iran				2	
Iraq		2		11	
Ireland		7	6	128	117
Israel		2		3	
Italy**		15	8	209	149
Japan		2	1	5	2
Kenya **		3		8	
Korea, Republic of		5		31	
Kuwait		1		6	
Libya					
Lithuania		2	1	5	3
Luxembourg				1	1
Malaysia**		5	2	53	51
Malta		1	1	4	2
Mauritius				1	
Mexico		1		2	
Morocco				2	
Netherlands		17	24	777	802
Netherlands Antilles					
New Zealand		0		1	
Pakistan		1		4	
Palestinian Territory					
Philipines		4		13	
Poland		2	2	7	11
Portugal**		3	3	26	24
Romania**		5	2	26	19

Russia		1		12	
Saudi Arabia		1		4	
Senegal					
Singapore		3		6	
Slovenia					
South Africa		7	3	173	177
Spain		22	18	765	561
Sweden		2	3	9	11
Switzerland		6	3	12	7
Taiwan		3		12	
Thailand**		2	3	29	31
Tjech Republic**		2	2	13	9
Turkey**		3	3	9	9
United Kingdom		19	20	713	724
United States**		15	8	233	271
Yugoslavia					
other countries**** excl. Nigeria		12	36	310	272
Totals		280	202	5390	4405

(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Πίνακας 15.2. Οι δέκα χώρες που πλήττονται από την νιγηριανή απάτη



(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

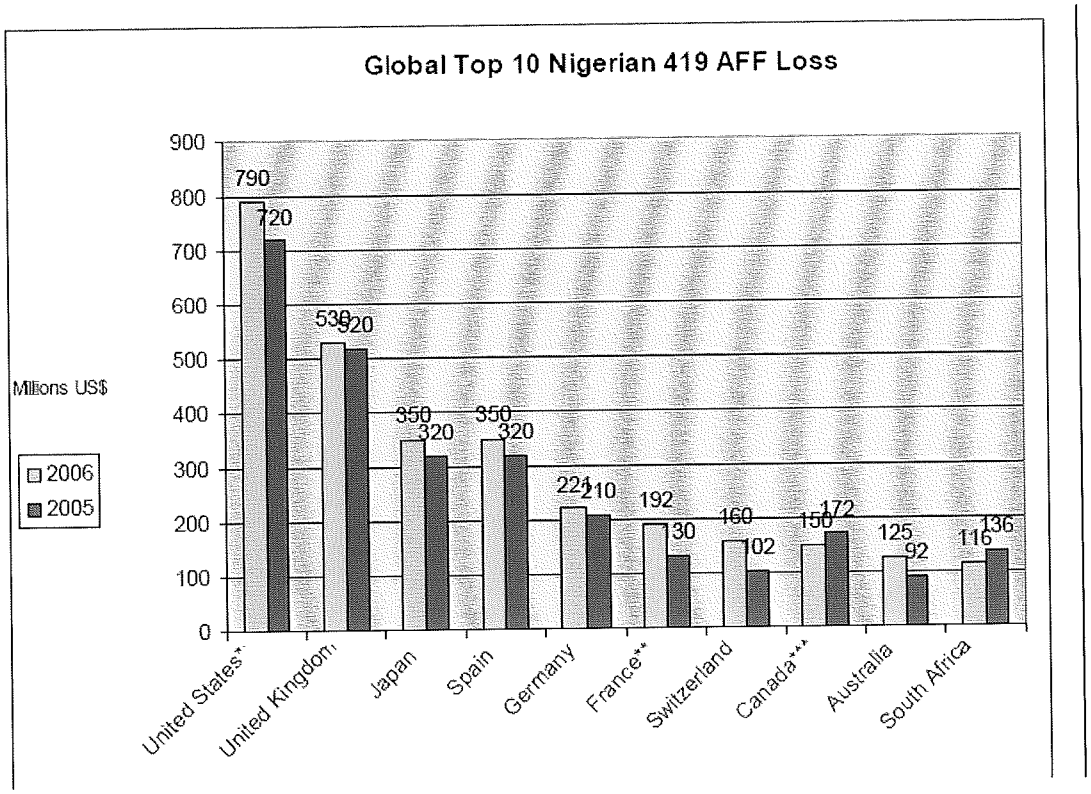
Πίνακας 15.3. Καταγραφή των κερδών από την νιγηριανή απάτη σε διάφορές χώρες

419Unit release January 23 2007		419 AFF low estimates for 2006 & 2005							
Nigerian Advance Fee Fraud on record* and low estimates for the countries listed below.		total active resident AFF scammers 2006	2005	profits before sharing with other scamrings in million US$	2005	profits after sharing with other scamrings in million US$	2005	AFF losses suffered in 2006 by companies and persons in million US$	2005
Argentina						0.0		2.5	
Australia		220	210	34	25	23.1	17.0	125	92
Austria		110	140	22	34	18.9	29.2	5	8
Belgium		300	300	43	51	31.4	37.2	51	70
Bolivia						0.0		1.1	
Brazil**		60		21		16.2		16	
Bulgaria		35	51	1	1	0.7	0.8	0.6	0.3
Cameroon						0.0		0.15	
Canada***		3120	3200	420	410	289.8	307.5	150	172
Chile						0.0		0.12	
China**		2900	85	404	31	141.4	26.4	115	20
Colombia		12		0.6		0.2		1.3	
Croatia						0.0		0.11	
Cyprus		7	4	0.9	0.3	0.7	0.3	0.7	0.6
Denmark		39	42	16	34	11.7	24.8	7	7
Dubai		70	45	161	66	130.4	53.5	45	1.3
Egypt		52	30	31	12	25.1	9.7	32	28
Finland		17	20	0.8	2	0.7	1.8	2	3
France**		515	810	166	115	73.0	55.9	192	130
Gambia						0.0		3.2	
Germany		1210	1270	215	137	117.2	81.5	221	210
Ghana**		1690	290	66	32	39.6	20.8	1.7	0.4
Greece**		210	50	389	85	241.2	52.7	53	11
Hong Kong **		17		66		45.5		32	
Hungary**		50	55	6	6	4.4	5.2	2.7	1.2
India**		190	150	26	22	14.3	12.1	32	3.5
Indonesia		20		16		4.8		4.5	
Iran						0.0		1.7	
Iraq		28		60		12.6		2.1	
Ireland		145	110	93	102	54.9	60.2	35	45
Israel		10		3		1.6		11	
Italy**		610	200	204	70	97.9	33.6	115	120
Japan		8	3	17	21	15.0	18.5	350	320
Kenya **		30		3		1.5		3	
Korea, Republic of		45		70		25.9		63	
Kuwait				3.2		0.9		0.6	
Libya						0.0		0.04	
Lithuania		7	5	33	17	14.9	7.7	0.6	0.7
Luxembourg		3	3	23	17	18.4	15.1	6	3
Malaysia**		85	80	7	6	5.8	5.0	15	11
Malta		2	2	9	4	3.4	1.6	0.1	0.07
Mauritius				0		0.0		0.1	
Mexico		15		40		14.0		17	
Morocco						0.0		0.2	
Netherlands		1552	1610	386	308	135.1	136.6	79	72
Netherlands Antilles						0.0		0.35	
New Zealand		1		0		0.0		6.5	
Pakistan				0		0.0		0.3	
Palestinian Territory				0		0.0		2	
Philipines		35		67		51.6		3	
Poland		20	25	3	3	2.1	2.5	4	1.7
Portugal**		50	30	9.5	9	6.5	7.0	13	12
Romania**		62	10	18	4	11.5	3.0	3.6	0.8

Russia	25		72		23.8		3.7	
Saudi Arabia	10		12		5.0		17	
Senegal					0.0		0.09	
Singapore	20		32		13.8		3.5	
Slovenia					0.0		0.03	
South Africa	1250	780	115	80	48.3	34.4	116	136
Spain	2840	2530	269	262	102.2	99.6	350	320
Sweden	29	33	7	12	2.6	3.2	26	26
Switzerland	115	120	88	65	68.6	50.7	160	102
Taiwan	37		62		16.1		2.2	
Thailand**	110	110	33	35	21.5	24.5	19	1.1
Tjech Republic**	22	17	7	6	5.8	5.0	10.5	9
Turkey**	110	60	17	2	14.8	1.7	26	5
United Kingdom	2120	2030	377	284	158.3	119.3	530	520
United States**	3500	3800	378	370	64.3	62.9	790	720
Yugoslavia					0.0		0.45	
other countries**** excl. Nigeria								
Totals	23740	16310	4622	2744	2249	1430	3883	3184

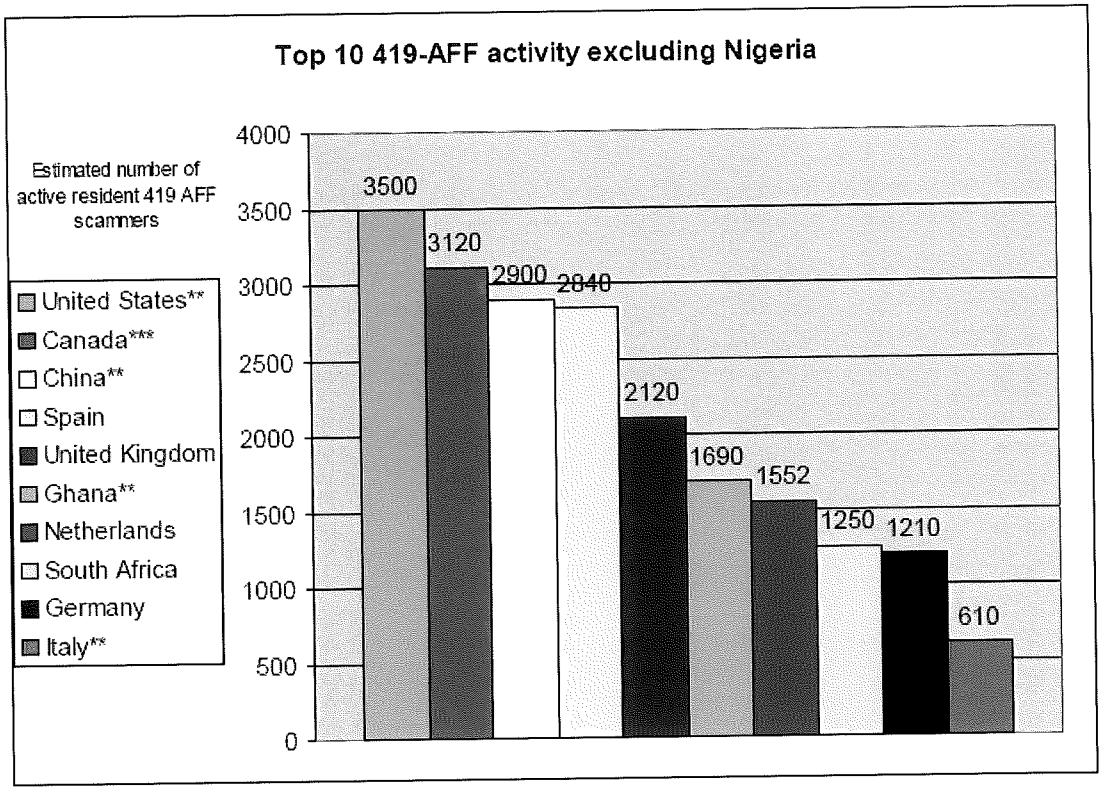
(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Πίνακας 15.4. Καταγραφή των απωλειών από την νιγηριανή απάτη σε δέκα χώρες



(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Πίνακας 15.5. Καταγραφή ενεργών πολιτών σε δέκα χώρες



(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Πίνακας 15.6. Καταγραφή των απωλειών των θυμάτων εξαιτίας της νιγηριανής απάτης

419Unit release January 23 2007		low estimates for period April 1996 - December 2006				
Nigerian Advance Fee Fraud on record* and low estimates for the countries listed below.		bankruptcies caused by 419	loss of careers caused by 419 AFF	loss of home caused by AFF	AFF victims! prosecuted for another fraud caused by AFF	AFF victims that went from savings to serious debt problems
Argentina						
Australia		550	80	90	530	8000
Austria		20		20	110	7000
Belgium		20	62	25	30	3500
Bolivia						30
Brazil**			100			1500
Bulgaria			3			
Cameroon						
Canada***		1550	9000	1100	310	23000
Chile						
China**		270		30		12000
Colombia						
Croatia						
Cyprus						
Denmark		15	35	42	15	12000
Dubai					20	150
Egypt		30	25		35	930
Finland						
France**		113	960	116	135	12600
Gambia						
Germany		122	4600	119	167	16200
Ghana**			10			60
Greece**		25	55	10	10	500
Hong Kong **					120	300
Hungary**			40	10	20	500
India**		10	500	90		5000
Indonesia						900
Iran						
Iraq						
Ireland			600		20	3200
Israel				5		
Italy**		60	320	125	35	3500
Japan			350			11000
Kenya **						
Korea, Republic of						350
Kuwait						
Libya						
Lithuania				10		
Luxembourg			1		3	35
Malaysia**		120	30	150	300	4500
Malta				1		1
Mauritius						60
Mexico						150
Morocco						
Netherlands		360	800	305	68	7000
Netherlands Antilles						
New Zealand						
Pakistan						
Palestinian Territory						30
Philipines						600
Poland						
Portugal**		10	15	15	20	
Romania**			50			1500

Russia						550
Saudi Arabia						
Senegal						
Singapore						
Slovenia						
South Africa		85	35		1200	3000
Spain		80	350	20		250
Sweden		60	10	30	300	6000
Switzerland		130	25	30	180	870
Taiwan						260
Thailand**			30		45	1500
Tjech Republic**		20		10	5	700
Turkey**		15	10	10		800
United Kingdom		1220	3500	840	1160	63000
United States**		8550	72000	9000	2030	350000
Yugoslavia						
other countries**** excl. Nigeria						
Totals		13435	93596	12203	6868	563026

(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Πίνακας 15.7. Καταγραφή εγκλημάτων που σχετίζονται με την νιγηριανή απάτη

419Unit release January 23 2007	recorded* at some point between April 1998 and January 2007					
Nigerian Advance Fee Fraud on record* and low estimates for the countries listed below.	suicides AFF victims	murders related to 419 AFF	kidnappings or taken hostage connected to 419 AFF scam ring	Key positions held by AFF scam ring	Key ownership connected to AFF	AFF scam ring bosses financing political change in Nigeria
Argentina						
Australia				3		1
Austria						1
Belgium			2	83	2	3
Bolivia						
Brazil**						
Bulgaria						
Cameroon						
Canada***	1	3	1	7	7	2
Chile						
China**		2		2	1	1
Colombia						
Croatia						
Cyprus				1		
Denmark				1		
Dubai				1	2	1
Egypt				1	1	
Finland						
France**	1	1		5	3	1
Gambia						
Germany	1			7	3	3
Ghana**		2		16	7	5
Greece**				3	3	2
Hong Kong **			1	15	1	1
Hungary**	1					
India**						1
Indonesia	1					
Iran				1		
Iraq				7		
Ireland				18		5
Israel						
Italy**				2	5	2
Japan	5					
Kenya **				3	1	
Korea, Republic of				1	1	1
Kuwait				1		
Libya						
Lithuania				2	2	1
Luxembourg						
Malaysia**	1			1	2	1
Malta				1	1	
Mauritius						
Mexico						
Morocco						
Netherlands		2	3	4	5	5
Netherlands Antilles						
New Zealand						
Pakistan						
Palestinian Territory						
Philipines				1	1	1
Poland						
Portugal**						

Romania**					1	2	
Russia					1		
Saudi Arabia							
Senegal							
Singapore					3	2	1
Slovenia							
South Africa			5	15	1	5	3
Spain					52	5	4
Sweden					1		
Switzerland					3	1	1
Taiwan					1		
Thailand**					1		
Tjech Republic**			1		3		1
Turkey**					1	2	
United Kingdom					5	4	11
United States**		1	5	5	602	8	4
Yugoslavia							
other countries*** excl. Nigeria			3	8	3	2	
Totals		12	24	35	863	79	63

(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

Πίνακας 15.8. Η νιγηριανή απάτη είναι πρόβλημα για κάθε χώρα

No 419 AFF problem in your country?

The 419 Unit of Ultrascan is not an official reporting centre however in 2006 we did review 16690 complaints from 161 countries. concerning Nigerian 419 advance fee fraud			
Albania	4	Kuwait	35
Algeria	17	Latvia	16
Andorra	1	Lebanon	21
Angola	2	Libya	13
Antigua and Barbuda	6	Lithuania	78
Argentina	57	Luxembourg	28
Armenia	7	Macao	2
Aruba	3	Macedonia	16
Australia	532	Madagascar	4
Austria	30	Malaysia	207
Azerbaijan	21	Maldives	2
Bahamas	6	Mali	3
Bahrain	13	Malta	12
Bangladesh	6	Mauritania	1
Barbados	5	Mauritius	77
Belarus	3	Mexico	145
Belgium	993	Micronesia	2
Benin	22	Moldova, Republic of	1
Bermuda	4	Monaco	8
Bhutan	2	Mongolia	2
Bolivia	64	Morocco	27
Bosnia and Herzegovina	139	Mozambique	10
Botswana	2	Namibia	1
Brazil	286	Netherlands	512
Brunei Darussalam	12	Netherlands Antilles	24
Bulgaria	129	New Zealand	91
Burkina Faso	5	Nicaragua	3
Cambodia	18	Nigeria	478
Cameroon	44	Norway	68
Canada	1130	Oman	17
Cape Verde	1	Pakistan	14
Cayman Islands	1	Palestinian Territory	33
Chile	58	Panama	9
China	216	Papua New Guinea	1
Colombia	32	Paraguay	2
Costa Rica	3	Peru	16
Cote D'Ivoire	283	Philippines	91
Croatia	24	Poland	39
Cyprus	4	Portugal	28
Czech Republic	255	Puerto Rico	8
Denmark	71	Qatar	6
Dominican Republic	12	Romania	511
Ecuador	10	Russian Federation	42
Egypt	51	Rwanda	5
El Salvador	7	Saudi Arabia	87
Eritrea	2	Senegal	36
Estonia	11	Sierra Leone	1
Ethiopia	9	Singapore	37
Faroe Islands	5	Slovakia	11

Finland	118
France	825
Gabon	3
Gambia	25
Georgia	11
Germany	738
Ghana	322
Gibraltar	2
Greece	172
Grenada	2
Guam	3
Guatemala	11
Guinea	2
Guinea-Bissau	3
Guyana	3
Haiti	5
Hong Kong	72
Hungary	39
Iceland	8
India	76
Indonesia	123
Iran, Islamic Republic of	36
Iraq	11
Ireland	43
Israel	80
Italy	162
Jamaica	16
Japan	221
Jordan	4
Kazakhstan	4
Kenya	31
Korea, Republic of	84

Slovenia	28
South Africa	358
Spain	233
Sri Lanka	15
Sudan	3
Sweden	167
Switzerland	176
Syria	8
Taiwan	32
Tanzania	3
Thailand	31
Togo	17
Trinidad and Tobago	6
Tunisia	20
Turkey	104
Uganda	5
Ukraine	19
United Arab Emirates	73
United Kingdom	1766
United States	2801
	0
Uruguay	5
Uzbekistan	4
Vanuatu	1
Venezuela	11
Vietnam	18
Virgin Islands, British	1
Virgin Islands, U.S.	2
Yemen	16
Yugoslavia	9
Zambia	2
Zimbabwe	2

Total	16690

(Πηγή: www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007)

ΣΥΜΠΕΡΑΣΜΑΤΑ 15^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Οι απάτες αυτής της μορφής είναι παγκόσμιο φαινόμενο και κυρίως παρουσιάζεται σε χώρες με ψηλό βιοτικό επίπεδο όπως οι Ηνωμένες Πολιτείες Αμερικής και οι χώρες της Ευρώπης, που η χρήση του διαδικτύου είναι πολύ διαδεδομένη.

16^{Ο} ΚΕΦΑΛΑΙΟ

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΤΗΝ ΝΙΓΗΡΙΑΝΗ ΑΠΑΤΗ

ΕΙΣΑΓΩΓΗ 16^{ΟΥ} ΚΕΦΑΛΑΙΟΥ

Προληπτικά μέτρα προστασίας πρέπει πάντα να λαμβάνονται από τους χρήστες Διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές και υπερβολικές χρεώσεις σε τηλεφωνικούς λογαριασμούς είναι συχνότατοι.

16.1 ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΤΑ ΠΑΙΔΙΑ

- Εξηγείτε στους γονείς σας τις εμπειρίες σας κατά την περιπλάνησή σας στο Διαδίκτυο.
- Πάντα να μιλάτε στους γονείς σας ή σε κάποιον ενήλικα για εικόνες ή κείμενα που βρήκατε στο Διαδίκτυο και σας ανησυχούν ή σας φοβίζουν.
- Διαφυλάσσετε τις προσωπικές σας πληροφορίες. Ποτέ μην δίνετε το όνομα σας, την διεύθυνση σας, την διεύθυνση και το όνομα του σχολείου σας, το τηλέφωνο σας, φωτογραφίες σας σε αγνώστους που συναντάτε στο Διαδίκτυο ακόμη και αν σας το ζητήσουν.
- Κρατάτε τον κωδικό εισόδου στον υπολογιστή σας μυστικό. Είναι σαν το κλειδί του σπιτιού σας που δεν θα το δανείζετε σε κανέναν.
- Μόνο με την άδεια και την παρουσία των γονιών σας μπορείτε να συμφωνήσετε να συναντήσετε κάποιον/κάποια που γνωρίσατε στο Διαδίκτυο.
- Προσέχετε όταν μιλάτε διαμέσου chatroom ή e-mail. Διακόψτε τη συνομιλία όταν κάποιοι σας κάνουν να νιώθετε άβολα.
- Μην εμπιστεύεστε ότι διαβάζετε στο Διαδίκτυο. Μάθετε να βλέπετε το περιεχόμενο με κριτικό μάτι.

16.2 ΓΙΑ ΝΕΟΥΣ

- Μη δίνετε σε κανέναν, ακόμη και στον καλύτερό σας φίλο, τον κωδικό πρόσβασης στο Διαδίκτυο. Τα μόνα άτομα που θα πρέπει να γνωρίζουν τον κωδικό είναι οι γονείς σας.
- Μην απαντάτε σε ηλεκτρονικά μηνύματα που σας κάνουν να αισθάνεσθε «άβολα». Σε περίπτωση που λάβετε ένα τέτοιο μήνυμα, μη διστάστετε να το πείτε στους γονείς σας ή σε κάποιο πρόσωπο που εμπιστεύεστε.
- Αν αισθανθείτε άβολα την ώρα που συνομιλείται μέσω chatroom, διακόψτε αμέσως τη συνομιλία.

- Αποφύγετε να στέλνετε τη φωτογραφία σας και τα προσωπικά στοιχεία σας μέσω Διαδικτύου σε άγνωστο.
- Σκεφθείτε πολύ καλά πριν αποφασίσετε να συναντηθείτε με κάποιο άτομο που γνωρίσατε στο Διαδίκτυο. Ζητείστε την άποψη των γονιών σας σχετικά με αυτό το θέμα.
- Σε περίπτωση που αποφασίσετε να συναντηθείτε με τον "διαδικτυακό σας φίλο». Ενημερώστε τους γονείς σας ή κάποιο άτομο που εμπιστεύεστε και φροντίστε αυτή η συνάντηση να γίνει σε δημόσιο χώρο.
- Αναπτύξτε κριτική διάθεση σε ό,τι διαβάζετε στο Διαδίκτυο. Μην εμπιστεύεστε αμέσως ό,τι δείτε.
- Μιλήστε στους γονείς σας για τα όσα βλέπετε και ζείτε όταν «σερφάρετε» στο Internet.

16.3 ΣΥΜΒΟΥΛΈΣ ΓΙΑ ΤΟΥΣ ΓΟΝΕΊΣ

- Κρατήστε τον ηλεκτρονικό υπολογιστή σε χώρους όπως το σαλόνι και όχι σε υπνοδωμάτια. Ασχοληθείτε με τον τρόπο που δουλεύει το Διαδίκτυο και αφιερώστε χρόνο να περιηγηθείτε μαζί με τα παιδιά σας στον Κυβερνοχώρο και μάθετε από αυτά.
- Σιγουρευτείτε ότι τα παιδιά σας είναι ενήμερα, ότι πρέπει να ανησυχούν για αγνώστους που συναντούν μέσω του ηλεκτρονικού υπολογιστή. Όπως ακριβώς είμαστε ανήσυχοι όταν άγνωστοι χτυπάνε την πόρτα του σπιτιού μας, έτσι δεν πρέπει τα παιδιά να δίνουν προσωπικές πληροφορίες για τους εαυτούς τους.
- Να είστε ιδιαίτερα προσεχτικοί όταν τα παιδιά χρησιμοποιούν τα chatrooms (δωμάτια συνομιλίας), χωρίς την επίβλεψη σας. Μην αφήσετε τα παιδιά σας να συναντήσουν κάποιον που γνώρισαν μέσω του Διαδικτύου χωρίς να είστε και εσείς μαζί.
- Ενθαρρύνετε τα παιδιά σας να προτιμούν τις ιστοσελίδες που εσείς θέλετε και όχι αυτές που θεωρείτε ανάρμοστες.
- Εγκαταστήσετε στον υπολογιστή σας κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του Διαδικτύου.
- Συζητήστε με τα παιδιά σας για την ασφάλεια του Διαδικτύου. Συζητώντας τους μελλοντικούς κινδύνους μέσω του Διαδικτύου με τα παιδιά χρειάζεται να δείξετε ευαισθησία και έγνοια έτσι ώστε να κατανοήσουν και τα ίδια τους κινδύνους.
- Γνωρίστε ποιους πρέπει να ενημερώσετε και εν ανάγκη να καταγγείλετε σε περίπτωση που συναντήσετε βλαβερό και παράνομο περιεχόμενο στο Διαδίκτυο.

16.4 ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΑΣΦΑΛΕΙΣ ΟΙΚΟΝΟΜΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

1. Αποφεύγετε να πραγματοποιείται οικονομικές συναλλαγές μέσω Διαδικτύου από Internet Café, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές. Προτιμήστε τον προσωπικό σας υπολογιστή ή κάποιον για τον οποίο είστε βέβαιοι για το επίπεδο ασφάλειας.

2. Ως προς τους κωδικούς πρόσβασης που χρησιμοποιείται για τις διαδικτυακές συναλλαγές:

- Αλλάζετε συχνά τους κωδικούς πρόσβασης και πάντα στην περίπτωση που υποψιάζεστε ότι έχουν εκτεθεί.

- Αποφεύγετε να χρησιμοποιείται ως κωδικό πρόσβασης την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να βρεθούν και από άλλα έγγραφα.

- Αποφεύγετε να έχετε τον προσωπικό σας κωδικό πρόσβασης μέσα σε πορτοφόλια, τσάντες ή ατζέντες. Σε περίπτωση απώλειας ή κλοπή τους θα διευκολύνετε πολύ τους δράστες.

- Αποφεύγετε να χρησιμοποιείτε τους ίδιους κωδικούς πρόσβασης σε περισσότερες από μία κάρτες σας.

- Μη δίνετε τον κωδικό πρόσβασής σας σε οποιονδήποτε κάτω από οιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεστεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό πρόσβασης για επαλήθευση, μην τον δώσετε. Οι Τράπεζες δεν ακολουθούν αυτήν την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την Αστυνομία.

3. Επικοινωνήστε με την τράπεζά σας αν νομίζετε ότι κάποιος γνωρίζει τον κωδικό σας πρόσβασης στην υπηρεσία Internet Banking.

4. Απενεργοποιήστε τη λειτουργία «Αυτόματης Καταχώρησης» του προγράμματος περιήγησης. Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή, γεγονός που τους καθιστά έκθετους.

5. Κάνετε αγορές μόνο από γνωστές εταιρίες που σας παρέχουν εγγυήσεις ασφάλειας. Αν κάνετε συχνά αγορές από το Διαδίκτυο, χρησιμοποιείτε μία κάρτα, αποκλειστικά για αυτή τη χρήση. Έτσι, αν πέσετε θύμα απάτης δεν θα χρειαστεί να ακυρώσετε όλες τις κάρτες σας.

6. Φροντίστε να διατηρείται σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας. Ειδικότερα:

- Φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιείτε και κυρίως τις «επιδιορθώσεις ασφαλείας». Πρόκειται για προγράμματα που εκδίδουν οι εταιρίες από τις οποίες έχετε αγοράσει το λογισμικό που χρησιμοποιείται και καλύπτουν τυχόν κενά ασφαλείας που διαπιστώθηκαν μετά την έκδοσή του.

- Εγκαταστήστε ένα πρόγραμμα προστασίας από τους ιούς (antivirus) και ένα δίχτυ προστασίας (firewall), και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους. Το δίχτυ προστασίας σας προφυλάσσει σε μεγάλο βαθμό από τις πιθανές «εισβολές» που θα δεχθείτε κατά τις περιηγήσεις σας στο Διαδόκτυο.

- Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση σε αυτόν μη εξουσιοδοτένων χρηστών.

7. Αν είστε χρήστες ηλεκτρονικού ταχυδρομείου (e-mail):

- Μην ανοίγετε τα ηλεκτρονικά μηνύματα (e-mails) για την προέλευση ή τον αποστολέα των οποίων δεν είστε βέβαιοι. Ιδιαίτερα επικίνδυνα είναι τα ηλεκτρονικά μηνύματα άγνωστης προέλευσης που περιέχουν συνημμένα αρχεία με κατάληξη .exe, .pif, ή .vbs. Επίσης, θα πρέπει να γνωρίζετε ότι ορισμένοι ιοί στέλνουν αντίγραφά τους σε όλες τις επαφές που υπάρχουν στο βιβλίο διευθύνσεων του υπολογιστή. Αυτό σημαίνει ότι το ηλεκτρονικό μήνυμα μπορεί να φαίνεται ότι έχει σταλεί από κάποιν γνωστό σας.
- Μην απαντάτε σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά σας στοιχεία. Επίσης, μη στέλνετε ποτέ προσωπικά σας στοιχεία ή στοιχεία των συναλλαγών σας μέσω μιας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου (webmail). Είναι εύκολη η υποκλοπή των στοιχείων από τρίτα, μη εξουσιοδοτημένα άτομα.

8. Να ενημερώνεστε για τους λογαριασμούς σας και να φροντίζετε για την ασφάλεια των προσωπικών σας στοιχείων και εγγράφων. Ειδικότερα:

- Ελέγχετε τακτικά τους τραπεζικούς σας λογαριασμούς και τους λογαριασμούς των πιστωτικών καρτών σας για οποιαδήποτε ασυνήθιστη συναλλαγή ή ανάληψη και ειδοποιήστε αμέσως την τράπεζα σε περίπτωση που διαπιστώσετε οποιαδήποτε διαφορά.

- Φροντίστε να καταστρέφετε όσα έγγραφα δεν σας χρειάζονται πλέον, όπως οι πιστωτικές και τραπεζικές κάρτες που ακυρώνετε, τα αντίγραφα των λογαριασμών σας ακόμα και τις αποδείξεις που λαμβάνετε από τα Α.Τ.Μ.

(Βλαχόπουλος, 2007)

16.5 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΛΟΓΑΡΙΑΣΜΟΥ ΣΑΣ

- Αποφεύγετε να χρησιμοποιείται ως κωδικό (PIN) την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά στοιχεία που μπορεί να γίνουν εύκολα αντιληπτά από επιτήδειους.
- Αποφεύγετε να γράφετε το PIN οπουδήποτε.
- Αποφεύγετε να χρησιμοποιείται το ίδιο PIN σε περισσότερες από μία κάρτες σας.
- Επιλέξτε και απομνημονεύστε τον κωδικό PIN που μόνο εσείς θα γνωρίζετε και που δεν θα μπορεί να προσδιορισθεί από προσωπικά σας αντικείμενα που υπάρχουν στο πορτοφόλι ή την τσάντα σας.
- Μην δίνετε τον κωδικό σας PIN σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεσθεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό του PIN για επαλήθευση, μην τον δώσετε. Οι Τράπεζες δεν ακολουθούν αυτή την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την Αστυνομία.
- Μην αφήνετε ποτέ την απόδειξη συναλλαγής που έχει εκδώσει το Α.Τ.Μ.
- Συγκρίνετε τις αποδείξεις ανάληψης χρημάτων του Α.Τ.Μ. με το μηνιαίο ενημερωτικό δελτίο κίνησης του λογαριασμού σας. Εάν παρατηρήσετε

οποιαδήποτε συναλλαγή που δεν έχετε πραγματοποιήσει ενημερώστε αμέσως την Τράπεζα.

- Να υπογράφετε την κάρτα σας. Αυτό αμποδίζει τον οποιονδήποτε να παραποιήσει το όνομά σας πάνω σε αυτήν.
- Μη δίνετε και μη δανείζετε ποτέ και σε κανέναν την κάρτα σας.

- Όταν κυκλοφορείτε έχετε μαζί σας μόνο τις κάρτες που προτίθεστε να χρησιμοποιήσετε.

- Αναφέρατε αμέσως την κλοπή ή την απώλεια κάρτας στην Τράπεζα και στην Αστυνομία

ΕΠΙΛΟΓΟΣ

Η μορφή του εγκλήματος, όπως τη γνωρίζουμε ως σήμερα, συνεχώς μεταβάλλεται. Οι νέες τεχνολογίες, αλλάζουν τους τρόπους και τα μέσα τέλεσης συμβατικών εγκλημάτων, ενώ νέες μορφές, αμιγώς ηλεκτρονικών εγκλημάτων, κάνουν την εμφάνισή τους. Ως αποτέλεσμα, το έργο των διωκτικών αρχών, η νομοθεσία και γενικά όλοι οι τομείς που επηρεάζουν τη μεθοδολογία διερεύνησης των εγκλημάτων και το σύστημα απονομής δικαιοσύνης σε κάθε χώρα, μεταβάλλονται.

Οι σύγχρονες τεχνολογίες, επέφεραν σημαντικές αλλαγές σε κάθε μορφή εγκληματικής συμπεριφοράς, που ως σήμερα χαρακτηριζόταν συμβατική. Η εισχώρηση της τεχνολογίας στις καθημερινές δραστηριότητες του σύγχρονου ανθρώπου, η διείσδυση και χρήση ηλεκτρονικών συσκευών από το σύνολο του πληθυσμού, οδηγούν σε μια μάλλον υβριδική μορφή εγκλημάτων, όπου σε κάθε συμβατικό έγκλημα, οι τεχνολογικά εξελιγμένες συσκευές, διαδραματίζουν κυρίαρχο ρόλο, χρησιμοποιούνται βοηθητικά ή αποτελούν φορείς σημαντικών αποδείξεων σε ψηφιακή μορφή.

Οι σύγχρονες εγκληματικές απειλές κινούνται σε δύο διαφορετικές διαστάσεις: Αφενός, προβάλλουν τα γνήσια εγκλήματα του κυβερνοχώρου, που δεν υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και του Διαδικτύου. Κύρια χαρακτηριστικά αυτών, είναι η χρησιμοποίηση τεχνολογικά εξελιγμένων συσκευών και υψηλής τεχνογνωσίας. Αφετέρου, τα γνωστά συμβατικά εγκλήματα αποκτούν μια περισσότερο υβριδική μορφή, όπου οι νέες τεχνολογίες διαδραματίζουν σημαντικό ρόλο.

Για την αντιμετώπιση των απειλών αυτών, κάθε οργανισμός πρέπει να μεριμνήσει για την πρόληψη εκδήλωσης των επιθέσεων, την ανίχνευση των επιθέσεων και, τέλος, την αντίδραση προς αποκατάσταση της ζημιάς που προκλήθηκε από μια επίθεση. Το τρίπτυχο αυτό της ασφάλειας, υπάγεται στη γενικότερη πολιτική ασφάλειας, που αποτελεί έναν συνδυασμό τεχνολογικών μέτρων αλλά και συνεχούς εκπαίδευσης και επιμόρφωσης του προσωπικού, σε θέματα ασφαλείας.

Στο νέο αυτό περιβάλλον, οι διωκτικές αρχές καλούνται, επίσης, να αντιμετωπίσουν το έγκλημα κινούμενες προς δύο κατευθύνσεις: (α) Να εκσυγχρονίσουν και να εκπαιδεύσουν τις υφιστάμενες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος και τα εργαστήρια εξέτασης ψηφιακών τεκμηρίων στις υψηλές τεχνολογίες και (β) να εκπαιδεύσουν το προσωπικό των υπηρεσιών στη μεθοδολογία διερεύνησης εγκλημάτων στα οποία συμμετέχει καθ' οποιονδήποτε τρόπο η ψηφιακή τεχνολογία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική Έντυπη Βιβλιογραφία

- Γ. Δ. Μπώκος, 2002Τεχνολογία και Πληροφόρηση: Από τη Διαχείριση του Βιβλίου στη Διαχείριση της Γνώσης, Αθήνα : Παπασωτηρίου,.
- Θεόδωρος Σιδηρόπουλος,Το δίκαιο του διαδικτύου,εκδόσεις Σακκουλα,2003.
- Φαρσεδάκης, ΙΑΚ. Ι.(1996). Στοιχεία Εγκληματολογίας. Αθήνα: Νομική Βιβλιοθήκη.
- Λάζος, Γ. (2001). Πληροφορική & Έγκλημα. Αθήνα: Νομική Βιβλιοθήκη.
- Λάζος, Γ. (1982). Οικονομικό Έγκλημα. Φάκελος σημειώσεων. Πάντειο Πανεπιστήμιο.
- Furnell, S. (2006). Κυβερνοέγκλημα. Αθήνα: Παπαζήση.
- Βλαχόπουλος, Κ. (2007). Ηλεκτρονικό Έγκλημα. Αθήνα: Νομική Βιβλιοθήκη.
- Τσουραμάνης, Χ. (2005). Ψηφιακή Εγκληματικότητα. Αθήνα: Κατσαρού Β.
- Πάγκαλος Γ. – Μαυρίδης Ι. (2002). Ασφάλεια πληροφοριακών συστημάτων και δικτύων, Θεσσαλονίκη, Ανίκουλα.
- Σουρής Α. – Πατσός Δ. – Γρηγοριάδης Ν., (2004). Ασφάλεια της πληροφορίας στους υπολογιστές, στο Internet, στην καθημερινή μας ζωή, Αθήνα, Εκδόσεις Νέων Τεχνολογιών.
- Παπανικολάου Κωνσταντίνος, (2007). Το ηλεκτρονικό έγκλημα και η προστασία δεδομένων προσωπικού χαρακτήρα. Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών.
- Ζάννη Αναστασία, (2005). Το διαδικτυακό έγκλημα. Κομοτηνή : Αντ. Ν. Σάκκουλας

Ξενόγλωσση Έντυπη Βιβλιογραφία

- Angus Marshall, (2008) . Digital Evidence in Criminal Investigation. John Wiley & Sons, Ltd.
- Mandia Kevin, Promise Chris, (2002). Άμεση Δράση. Γκιούρδας.
- Gusson Maurice, (2002). Σύγχρονη Εγκληματολογία. Νομική Βιβλιοθήκη.
- Smith, Russell G., Michael N. Holmes and Philip Kaufmann,(1999). "Nigeria Advance Fee Fraud," Trends and Issues in Crime and Criminal Justice, No. 121, July. Canberra: Australian Institute of Criminology
- U.S. Department of State. 1997. Nigerian Advance Fee Fraud. Bureau of International Narcotics and Law Enforcement Affairs, DOS Publication 10465.
- Thomas J. Holt, Danielle C. Craver, (January, 2007)A Qualitative Analysis of Advance Fee Fraud E-mail Schemes. International Journal of Cyber Criminology.
- Jan Blommaert and Tope Omoniyi, (December, 2006). E-mail Fraud: Language, Technology, and the Indexical of Globalization. Social Semiotics, volume 16 Number 4.

Ηλεκτρονική Βιβλιογραφία

- www.elesme.gr
- http://cybercrime.planetindia.net/intro.htm
- www.lawnet.gr
- www.e-telescope.gr/gr/cat03/art03_010622.htm
- www.potifos.com/fraud
- www.medium.gr/categories/society_ecrime.shtml
- www.marinos.com.gr
- www.NUKED.gr
- www.antiphishing.gr
- www.eviapress.gr
- www.scambusters.org
- www.adslgr.com
- www.safeweb.org.cy
- www.ydt.gr
- http://dide.flo.sch.gr/Plinet/plinet.html
- http://www.pandasecurity.com
- www.e-forum.gr
- www.foxnews.gr
- www.police.gov.cy/police
- www.dart..gov.gr
- www.ebusinessforum.gr
- www.news.kathimerini.gr
- www.go-online.gr/ebusiness/specials/article
- www.apodimos.com/arthra
- www.haef.gr/gre/libraries/acl/eschoolib/digitization
- www.dpa.gr
- www.mohaw.gr/gr/communication/linksgov/link
- www.adae.gr/
- www.diaplous.org/library/nomothesia
- www.in.gr/tech/books/sidhropoulos
- www.state.gov

- www.travel.state.gov
- www.heroes.net
- www. hoaxbusters.ciac.org/HBSearch.html
- http://usembassy.state.gov/posts/ni1/wwwhxrdaug13.html
- http://www.phonebusters.com/
- http://met.police.uk/fraudalert
- http://news.abcsmallbiz.com/bizbasics/misc/nigerian_letter.html
- http://www.rcmp-grc.gc.ca/scams/nigerian.htm
- http://www.secretservice.gov/alert419.shtml
- http://news.abcsmallbiz.com/bizbasics/misc/nigerian_letter.html
- http://wwwl.ifccfbi.gov/strategy/nls.asp
- http://web.lexisnexis.com/universe/document?_m=8df4b2e3b65c89c6ef74c4537c0ca34c
- http://home.rica.net/alphae/419coal/
- http://www.popsubculture.com/pop/bio_project/nigeria-fraud.html
- www.ultrascan.nl/assets/applets/2006_stats_on_419AFF_jan_23_2007
- www.ultrascan.nl/html/419_advance_fee_fraud.html
- http://www.fbi.gov/majcases/fraud/internetschemes.htm
- http://www.ic3.gov/default.aspx