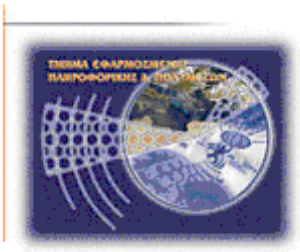
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Προστασία από κλοπή προσωπικών στοιχείων

Παρασκευή Βαγγελάτου (ΑΜ: 1523)
E-mail: epp1523@epp.teicrete.gr

Ηράκλειο – 10/09/2009

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Προστασία από κλοπή προσωπικών στοιχείων

***<u>Υπεύθυνη Δήλωση</u>**: Βεβαιώνω ότι είμαι συγγραφέας της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Τις έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Της βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για της απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή κ. **Μανιφάβα Χαράλαμπο** που μου έδωσε την ευκαιρία να αναπτύξω τη πτυχιακή εργασία καθώς και για την υποστήριξη και την καθοδήγησή του κατά τη διάρκεια της εκπόνησης της παρούσης εργασίας.

Θα ήθελα, επίσης, να ευχαριστήσω όλους όσους με βοήθησαν και με στήριξαν τα χρόνια της φοίτησής μου στο Τ.Ε.Ι., του γονείς μου, τα αδέρφια μου, της καθηγητές και του συμφοιτητές μου.

Περίληψη

Η παρούσα πτυχιακή εργασία αναφέρεται στην κλοπή προσωπικών δεδομένων καθώς και στην προστασία αυτών, όχι μόνο, στον πραγματικό κόσμο αλλά και στο Διαδίκτυο. Είναι σημαντικό να γνωρίζει κανείς ότι, όσα πλεονεκτήματα και αν προσφέρουν οι σύγχρονες τεχνολογίες και τα νέα μέσα, υπάρχουν και πολλοί κίνδυνοι. Σε αυτούς περιλαμβάνεται και η κλοπή προσωπικών δεδομένων.

Επιπλέον, είναι σημαντικό να γνωρίζουμε και μερικούς τρόπους που ακολουθούν οι απατεώνες για να ξεγελάσουν το θύμα, κάποιοι από τους οποίους αναφέρονται και στην εργασία αυτή.

Στη συνέχεια, θα συναντήσουμε πολλούς και διάφορους τρόπους άμυνας απέναντι στην κλοπή των προσωπικών δεδομένων, έτσι ώστε να περιοριστεί και ο κίνδυνος της κλοπής. Είναι σημαντικό να δώσει σημασία κάποιος, ιδιαίτερα όταν έχει πέσει θύμα απάτης.

Η αλήθεια είναι ότι τα τελευταία χρόνια οι κλοπές έχουν αυξηθεί ραγδαία, οπότε οι άνθρωποι και κυρίως οι κάτοχοι πιστωτικών καρτών πρέπει να είναι ιδιαίτερα προσεχτικοί. Επιπλέον, στο ίδιο κεφάλαιο θα αναφέρουμε και διάφορους τρόπους προστασίας των κατόχων πιστωτικών καρτών και προσωπικών εγγράφων.

Έπειτα, θα ασχοληθούμε με την νομοθεσία που διέπει την κλοπή ταυτότητας και θα αναφέρουμε αναλυτικά τις διατάξεις του ελληνικού συντάγματος και της Ευρωπαϊκής Ένωσης που αφορούν το θέμα αυτό.

Και στο τελευταίο κεφάλαιο της πτυχιακής, θα αναφέρουμε και θα παρουσιάσουμε το εργαλείο **Cyberciege**, το οποίο καλύπτει μια σειρά ζητημάτων διαχείρισης δικτύου.

Abstract

This work refers to identity theft and identity protection, not only in the real world but also, over the Internet. It is important to know that despite the advantages that current technology has to offer, there is also a great number of risks. One of them is identity theft.

Additionally, it is important to know a few of the means that deceivers use to trick the victims. Some of them are described in this work.

On the next chapter we will describe many different ways to defend against identity theft, in order to contain the danger. This chapter should be taken into account by those who have been deceived.

Truth is that identity theft has rapidly increased over the last few years. In the same chapter, a variety of ways is presented for the protection of credit card owners and personal documentation.

Next, we will examing the legal response to identity theft in various countries and we will present in detail the chapters of the greek constitution and the rules of the Europian Union that refer to identity theft.

In the last chapter of this work, we will present the **Cyberciege** tool which helps in network administration.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Κεφάλαιο 1 Εισαγωγή

1.1 Γενικά

Η κλοπή ταυτότητας και η απάτη ταυτότητας αναφέρονται σε κάθε έγκλημα όπου κάποιος αποκτά και χρησιμοποιεί κακόβουλα τα προσωπικά στοιχεία κάποιου άλλου κυρίως για οικονομικό όφελος.

Σε αντίθεση με τα δακτυλικά αποτυπώματα που δεν μπορούν να κλαπούν, άλλα προσωπικά στοιχεία ενός ατόμου όπως ο Αριθμός Αστυνομικής Ταυτότητας, αριθμός Πιστωτικής Κάρτας κοκ, μπορούν να χρησιμοποιηθούν σε πράξεις που είναι εις βάρος του κατόχου τους αν πέσουν σε λάθος χέρια.

Για παράδειγμα, υπάρχουν πολλές αναφορές στις Η.Π.Α[1], όπου απατεώνες κλέβουν τα προσωπικά στοιχεία ανθρώπων και μετά διαπράττουν εγκλήματα οικονομικά και μη, με την ταυτότητα των ανθρώπων αυτών.

Σε πολλές περιπτώσεις οι απώλειες του θύματος δεν είναι μόνο οικονομικές αλλά και ηθικές όπου το θύμα χρειάζεται να αποκαταστήσει το καλό του όνομα ή να διορθώσει παρεξηγήσεις που έχει δημιουργήσει ο απατεώνας.

[1] http://www.usdoj.gov/criminal/fraud/websites/idtheft.html#whatdoing

1.2 Στόχοι της πτυχιακής

ΤΙΤΛΟΣ ΠΤΥΧΙΑΚΗΣ:	Προστασία από κλοπή προσωπικών στοιχείων (Identity theft protection)
Στοιχεία Εισηγητή: Όνομα:	Χάρης Μανιφάβας
Τηλ.:	
Email:	harryman@epp.teicrete.gr
Περίοδος:	2009-2010
Τομέας:	Πληροφορικής
Αριθμός σπουδαστών:	1
Ονόματα σπουδαστών:	Βαγγελάτου Παρασκευή (ΑΜ 1523)

Περιγραφή Πτυχιακής Εργασίας:

Η παρούσα πτυχιακή εργασία αναφέρεται στην κλοπή προσωπικών δεδομένων καθώς και σε τεχνικές για την προστασία αυτών, όχι μόνο στον πραγματικό κόσμο αλλά και στο Διαδίκτυο. Οι σύγχρονες τεχνολογίες προσφέρουν διάφορα πλεονεκτήματα συνοδεύονται όμως και από πολλούς κινδύνους. Σε αυτούς περιλαμβάνεται και η κλοπή προσωπικών δεδομένων.

Η κλοπή ταυτότητας και η απάτη ταυτότητας αναφέρονται σε κάθε έγκλημα όπου κάποιος αποκτά και χρησιμοποιεί κακόβουλα τα προσωπικά στοιχεία κάποιου άλλου κυρίως για οικονομικό όφελος. Σε πολλές περιπτώσεις οι απώλειες του θύματος δεν είναι μόνο οικονομικές αλλά και ηθικές όπου το θύμα χρειάζεται να αποκαταστήσει το καλό του όνομα ή να διορθώσει παρεξηγήσεις που έχει δημιουργήσει ο απατεώνας.

Στην πτυχιακή θα παρουσιαστούν, αναλυθούν και υλοποιηθούν τα παρακάτω:

- Μέθοδοι που ακολουθούν οι απατεώνες για να ξεγελάσουν το θύμα. Παραδείγματα από την ιστορία αλλά και τα τελευταία χρόνια με τη χρήση ον-λινε υπηρεσιών
- Διαδικασίες και τεχνικές άμυνας απέναντι στην κλοπή των προσωπικών δεδομένων, έτσι ώστε να περιοριστεί και ο κίνδυνος της κλοπής
- Μέθοδοι προστασίας των κατόχων πιστωτικών καρτών και προσωπικών εγγράφων.
- Παρουσίαση του νομικού καθεστώτος που διέπει τα προσωπικά δεδομένα και την κλοπή ταυτότητας (διατάξεις-νόμοι-κανονισμοί του ελληνικού δικαίου και της Ευρωπαϊκής Ένωσης).
- Παρουσίαση, εγκατάσταση και διαμόρφωση του εκπαιδευτικού εργαλείου-παιγνιδιού **Cyberciege**, το οποίο καλύπτει μια σειρά ζητημάτων διαχείρισης ασφάλειας. Στόχος του είναι να εμπεδώσει μία συνείδηση ασφάλειας σε διάφορα θέματα, μεταξύ των οποίων και η προστασία ευαίσθητων δεδομένων.

1.3 Διάρθρωση της πτυχιακής

Πιο συγκεκριμένα αναλύονται τα παρακάτω θέματα:

1. **Εισαγωγή**

   Στην εισαγωγή θα δούμε τι σημαίνει κλοπή ταυτότητας

2. **Ιστορική αναδρομή**

   Στην αρχή της πτυχιακής γίνεται μια ιστορική αναδρομή πάνω στο θέμα της κλοπής προσωπικών δεδομένων καθώς επίσης γίνεται και μια αναφορά στο ghosting που είναι ένας τύπος κλοπής ταυτότητας. Αναφέρονται παρακάτω περισσότερα γι αυτό.

3. **Σημερινή κατάσταση**

   Στο κεφάλαιο αυτό θα δούμε τί μορφή έχει πάρει η κλοπή ταυτότητας από απατεώνες τη σημερινή εποχή. Επιπλέον, θα συναντήσουμε και κάποιες έρευνες σχετικά με το θέμα αυτό που είναι οι εξής:

   - Τρόποι ανακάλυψης της απάτης
   - Πολλαπλές επιθέσεις κλοπής στοιχείων σε ένα θύμα
   - Νέοι λογαριασμοί που ανοίχτηκαν το 2005 από απατεώνες
   - Παρέλευση χρόνου για την ανακάλυψη της απάτης
   - Προσωπικές σχέσεις θυμάτων και απατεώνων
   - Επικοινωνία με τις αρχές

4. **Επιθέσεις για κλοπή στοιχείων**

   Εδώ αναλύονται θέματα που σχετίζονται με τις τεχνικές άντλησης προσωπικών δεδομένων καθώς και τους τρόπους κλοπής αυτών.

   Επιπλέον, γίνεται μια αναφορά στους dialers που δεν είναι τίποτε άλλο από κακόβουλα προγράμματα τα οποία έχουν τη δυνατότητα να αποσυνδέουν την υπάρχουσα κλήση της τηλεφωνικής γραμμής με τον τοπικό πάροχο υπηρεσιών Internet (και να καλούν αυτόματα ένα υψηλής χρέωσης αριθμό (π.χ. 901 ή αριθμούς εξωτερικού π.χ. 00xx) για πρόσβαση σε συγκεκριμένες υπηρεσίες χωρίς την συνειδητή συγκατάθεση του χρήστη.

   Επιπλέον, στο ίδιο κεφάλαιο αναλύεται το θέμα των ύποπτων εμπορικών σελίδων, οι οποίες πολλές φορές κρύβουν παγίδες για να εξαπατήσουν το θύμα. Τέλος, γίνεται αναφορά στην κατάχρηση λογαριασμών από τους απατεώνες.

   Στο τέλος, γίνεται αναφορά σε κάποιους διάσημους κλέφτες ταυτοτήτων, όπου ο πιο γνωστός από αυτούς είναι ο Radovan Karadzic.

5. Τρόποι προστασίας από κλοπή προσωπικών στοιχείων

Στο κεφάλαιο αυτό θα συναντήσουμε τρόπους για την αντιμετώπιση του προβλήματος της κλοπής καθώς και τρόπους προστασίας των προσωπικών μας δεδομένων, του φορητού μας υπολογιστή κ.α.

6. Νομικό καθεστώς σε σχέση με την προστασία προσωπικών στοιχείων

Στο κεφάλαιο αυτό θα ασχοληθούμε με την νομοθεσία σε Ελλάδα και εξωτερικό, που διέπει την κλοπή ταυτότητας.

7. Αναφορά στο εργαλείο προστασίας CyberCIEGE

Στο κεφάλαιο αυτό θα συναντήσουμε το CyberCIEGE που είναι ένα παιχνίδι – εξομοιωτής, με βασικό σκοπό να διδάξει τρόπους ασφάλειας υπολογιστών και δικτύων

1.3 Σχεδιάγραμμα Αναφοράς

Αριθμός κεφαλαίου	Τίτλος	Σύντομη περιγραφή
1	Εισαγωγή	Περιγράφονται οι ορισμοί κλοπή και απάτη ταυτότητας.
2	Ιστορική Αναδρομή	Μια σύντομη ιστορική αναδρομή στο θέμα της κλοπής ταυτότητας.
3	Σημερινή κατάσταση	Μια σύντομη αναφορά στη σημερινή κατάσταση.
4	Επιθέσεις για κλοπή στοιχείων	Αναφέρονται διάφοροι τρόποι κλοπής των δεδομένων από τους απατεώνες.
5	Τρόποι προστασίας από κλοπή προσωπικών στοιχείων	Αναφέρονται τρόποι αντιμετώπισης του προβλήματος της κλοπής στοιχείων.
6	Νομικό καθεστώς σε σχέση με την προστασία προσωπικών στοιχείων	Αναφέρεται το νομικό καθεστώς σε Ελλάδα και εξωτερικό
7	Αναφορά στο εργαλείο προστασίας CyberCIEGE	Εργαλείο εκμάθησης και εξάσκησης για την ασφάλεια των πληροφοριών.
Παράρτημα Α	Παράδειγμα πολιτικής απορρήτου	Παρατίθεται πολιτική απορρήτου του ηλεκτρονικού καταστήματος πληροφορικής E-shop.
	Συμπεράσματα	Αναφέρεται μια σύντομη περιγραφή για το κάθε κεφάλαιο.
	Βιβλιογραφία	Αναφέρονται πηγές που χρησιμοποιήθηκαν για την πτυχιακή εργασία.

Κεφάλαιο 2 Ιστορική Αναδρομή

Η κλοπή ταυτότητας θεωρείται το πιο γρήγορα αναπτυσσόμενο έγκλημα στο κόσμο. Η γρήγορη αυτή εξέλιξη οφείλεται στην αλλαγή του τρόπου διακίνησης και φύλαξης των προσωπικών δεδομένων. Στις μέρες μας έχουν πολλοί πρόσβαση στα προσωπικά δεδομένα άλλων, χωρίς να είναι πάντα καλοπροαίρετη.

Οι στατιστικές λένε ότι η κλοπή ταυτότητας είναι πιο διαδεδομένη τώρα παρά ποτέ. Αυτό συμβαίνει κυρίως εξαιτίας της εξάπλωσης και της ευρύτατης χρήσης του Διαδικτύου και των ηλεκτρονικών υπολογιστών. Όμως, η κλοπή ταυτότητας δεν ξεκίνησε από το Διαδίκτυο.

Για την ακρίβεια, η κλοπή ταυτότητας είναι τόσο παλιά όσο ο ίδιος ο άνθρωπος. Οι εγκληματίες πάντα προσπαθούσαν να εκμεταλλευτούν αθώους ανθρώπους οι οποίοι κατείχαν πλούτο και αξιώματα.

2.1 Η κλοπή ταυτότητας πριν την εμφάνιση του Internet

Σε παλαιότερες εποχές, η κλοπή ταυτότητας δεν ήταν απλή απάτη αλλά βίαιο έγκλημα. Οι απατεώνες για να υποδυθούν κάποιον έπρεπε να τον ‘βγάλουν από τη μέση’. Αυτό το πετύχαιναν είτε σκοτώνοντας το θύμα (συνήθως κάποιο άτομο με αξιοσέβαστο πλούτο ή αξιώματα) ή απλά του έκλεβαν την ταυτότητα μετά θάνατον.

Το έργο τους γινόταν ευκολότερο, αφού τότε δεν υπήρχαν μέσα ταυτοποίησης, όπως δίπλωμα οδήγησης ή αριθμός ταυτότητας, οπότε το μόνο εμπόδιο που είχαν να ξεπεράσουν οι εγκληματίες ήταν η εμφάνιση. Για όσους ήταν ιδιαίτερα πονηροί και θρασείς, αυτό γινόταν εύκολα.

Μερικοί πιστεύουν ότι η κλοπή ταυτότητας ξεκίνησε από ένα βιβλίο. Ο τίτλος του βιβλίου αυτού είναι: ‘The Day of the Jackal’ του Frederick Forsyth. Στο βιβλίο αυτό πρωταγωνιστεί ένας πληρωμένος δολοφόνος που είχε σκοπό να χτυπήσει τον αρχηγό του κράτους στη Γαλλία. Φυσικά, αφού είχε σκοπό να κάνει μια τέτοια πράξη, έπρεπε να προετοιμάσει ένα σχέδιο διαφυγής.

Για να καταφέρει να ξεφύγει χρησιμοποίησε 4 πλαστές ταυτότητες για την είσοδο και την έξοδο από τη χώρα και την αγορά του κατάλληλου εξοπλισμού. Ο δολοφόνος για την δημιουργία μίας εκ των πλαστών ταυτοτήτων, χρησιμοποίησε την παρακάτω μέθοδο: πήγε στα νεκροταφεία της Αγγλίας και έψαξε για τάφους νεογνών που αν ζούσαν θα είχαν παρόμοια ηλικία με αυτόν.

Στη συνέχεια, έβγαλε ένα πιστοποιητικό γέννησης από ένα τοπικό ληξιαρχείο. Να σημειωθεί ότι εκείνη την εποχή ήταν δύσκολο να διασταυρωθεί ένα πιστοποιητικό γέννησης με ένα πιστοποιητικό θανάτου. Μετά από αυτό μπορούσε να βγάλει ταυτότητα στο νέο του όνομα, να ενοικιάσει διαμέρισμα, να ανοίξει λογαριασμό σε τράπεζα κ.α. Όπως μπορεί κανείς να φανταστεί, η παραπάνω ιστορία γέννησε την κλοπή ταυτότητας στον κοινό νου.

Προστασία από κλοπή προσωπικών στοιχείων

Δεν ήταν όμως μόνο αυτό το βιβλίο που άντλησε τη θεματολογία του από την κλοπή και την απάτη ταυτότητας. Υπάρχει ένα άλλο βιβλίο, που μάλιστα έχει μεταφερθεί και στη μεγάλη οθόνη με τίτλο ‘Catch Me If You Can’.

Η ταινία και το βιβλίο περιγράφουν τη ζωή και τα κατορθώματα του Frank Abagnale, ενός απατεώνα που δραστηριοποιήθηκε τη δεκαετία του ’60 και στις αρχές του ’70. Αυτός υποδυόταν ρόλους γιατρών, δικηγόρων, πιλότων και γενικά ανθρώπων που θεωρούνταν αξιόπιστοι στην κοινωνία. Οι απάτες που διέπραξε είχαν να κάνουν κυρίως με πλαστές επιταγές και την απόκτηση χρήματος.

Η ταινία αυτή αντικατοπτρίζει την πραγματικότητα και ταιριάζει περισσότερο με τη σύγχρονη κατάσταση. Με τη μόνη διαφορά ότι σήμερα στο έργο των απατεώνων συνδράμει και η τεχνολογία.

Πολλοί μπορεί να υποθέσουν ότι οι περισσότερες απάτες που έχουν να κάνουν με την κλοπή ταυτότητας γίνονται μέσω του Διαδικτύου. Στην πραγματικότητα, πάνω από το 60% των περιπτώσεων συμβαίνει χωρίς καν να χρησιμοποιηθεί υπολογιστής.

Στα μέσα του 20ού αιώνα ήταν δύσκολο να αποκτήσει κάποιος πιστωτική κάρτα. Η διαδικασία έκδοσης πιστωτικής κάρτας ήταν παρόμοια με την σημερινή διαδικασία έκδοσης δανείου. Η πιστωτικοί οργανισμοί χρειάζονταν πολλές πληροφορίες και απόδειξη της ταυτότητας του ατόμου, προκειμένου να προχωρήσουν στη διαδικασία έκδοσης πιστωτικής κάρτας.

Στις δεκαετίες του '80 και '90, η χρήση πιστωτικής κάρτας έγινε ιδιαίτερα διαδεδομένη και όλο και μεγαλύτερος αριθμός ατόμων, είχε πρόσβαση στο "εύκολο χρήμα". Τότε ήταν που ξεκίνησαν τη λειτουργία τους οι οργανισμοί που μετρούσαν την πιστοληπτική ικανότητα των κατόχων πιστωτικών καρτών και δανείων. Την ίδια περίοδο εμφανίστηκαν και οι πιστωτικές αναφορές. Αυτό το φαινόμενο της ανεξέλεγκτης χρήσης πλαστικού χρήματος, ευνοούσε τους εγκληματίες που το έβλεπαν σαν μια άλλη μια πηγή πλουτισμού.

Όμως, πριν την έξαρση του προαναφερθέντος φαινομένου οι εγκληματίες κατέφευγαν σε έναν πρακτικό αλλά ιδιαίτερα αηδιαστικό τρόπο κλοπής προσωπικών πληροφοριών. Αυτός δεν ήταν άλλος από το ψάξιμο των απορριμμάτων του θύματος για προσωπικές πληροφορίες. Αυτό γινόταν (και γίνεται) είτε σε χώρους υγειονομικής ταφής είτε σε οικιακά απορρίμματα.

Ένα τέτοιο περιστατικό συνέβη σε μια ηλικιωμένη γυναίκα στην Αμερική. Οι κλέφτες ψάχνοντας στα σκουπίδια του σπιτιού της, ανακάλυψαν το πεταμένο μπλοκ επιταγών της γυναίκας. Στη συνέχεια ξεκίνησαν να γράφουν επιταγές στον εαυτό τους πλαστογραφώντας την υπογραφή της.

Ακόμα, λοιπόν, και αν κάποιος είναι ελάχιστα ενημερωμένος γύρω από το θέμα της κλοπής ταυτότητας, πρέπει να γνωρίζει ότι το πρώτο βήμα για την αποφυγή του φαινομένου είναι η καταστροφή των σημαντικών εγγράφων όπως το μπλοκ επιταγών.

Οι εγκληματίες λοιπόν, βασιζόταν κατά κόρον στο ψάξιμο των απορριμμάτων για να πραγματοποιήσουν κλοπή ταυτότητας. Οι πιο φιλόδοξοι από αυτούς είτε λήστευαν ή έκλεβαν γυναικείες τσάντες και αντρικά πορτοφόλια. Άλλη μία συνήθης πρακτική ήταν η κλοπή της αλληλογραφίας.

Ακόμα χρησιμοποιούσαν τηλεφωνικές απάτες, για να "ψαρέψουν" προσωπικά στοιχεία. Κλασικό παράδειγμα: Ο κλέφτης ταυτότητας τηλεφωνούσε σε κάποιον και του έλεγε ότι έχει κερδίσει ένα σημαντικό βραβείο, όμως για να το παραλάβει έπρεπε να δώσει τα στοιχεία του για να επιβεβαιωθεί η ταυτότητά του. Στη συνέχεια ο κλέφτης, μπορούσε να χρησιμοποιήσει τα στοιχεία όπως επιθυμούσε.

Φυσικά όπως όλοι γνωρίζουν, η κλοπή ταυτότητας έγινε πιο πολύπλοκη με την είσοδο του Διαδικτύου στη ζωή των ανθρώπων. Πολλά από τα ανόητα e-mail που λαμβάνει κανείς, μπορεί να κρύβουν πίσω τους έναν εγκληματία, ο οποίος περιμένει κάποιον αδαή να του δώσει τα προσωπικά του στοιχεία. Ευτυχώς αυτά τα e-mail συνήθως είναι αποτυχημένα και σπάνια ξεγελούν τα υποψήφια θύματα.

Γενικά όμως, με την χρήση του Διαδικτύου η κλοπή ταυτότητας μπορεί να γίνει ευκολότερα και χωρίς να συλληφθούν οι απατεώνες[2].

2.1 Ghosting

Το Ghosting είναι ένας τύπος κλοπής ταυτότητας[3], όπου ο απατεώνας κλέβει την ταυτότητα και μερικές φορές, ακόμα και τον κοινωνικό ρόλο ενός πεθαμένου ανθρώπου (του φαντάσματος). Ο θάνατος του προσώπου αυτού δεν είναι ευρέως γνωστός. Συνήθως, το άτομο που κλέβει την ταυτότητα (ghoster) έχει περίπου την ίδια ηλικία που θα είχε το φάντασμα εάν βρισκόταν στη ζωή, έτσι ώστε κάθε είδους έγγραφο που σχετίζεται με την χρονολογία γέννησης του φαντάσματος, να μην κινήσει υποψίες.

Η χρήση πλαστής ταυτότητας, που απεικονίζει ένα μη υπαρκτό πρόσωπο, δεν είναι ghosting, καθώς η πλαστή ταυτότητα δεν μπορεί να χρησιμοποιηθεί για να αποκτηθούν υπηρεσίες από δημόσιους φορείς καθώς και να γίνει αλληλεπίδραση με την αστυνομία.

Σκοπός του ghosting είναι να επιτρέψει στον απατεώνα να χρησιμοποιήσει μια υπάρχουσα ταυτότητα που είναι ήδη καταχωρημένη στα κυβερνητικά μητρώα και είναι αδρανής διότι ο πραγματικός κάτοχός της έχει πεθάνει.

Το ghosting βασίζεται στην αρχή ότι διαφορετικές κυβερνητικές υπηρεσίες δεν μοιράζονται τις ίδιες πληροφορίες. Γι αυτό τον λόγο ο απατεώνας μπορεί να λάβει, για παράδειγμα, ένα διαβατήριο στο όνομα ενός αποθανόντος γιατί οι υπηρεσία που είναι υπεύθυνη για τα διαβατήρια συνήθως δεν ελέγχει εάν στο όνομα του συγκεκριμένου ατόμου έχει εκδοθεί πιστοποιητικό θανάτου.

[2] http://www.idtheft-prevent-and-restore.com/history-of-identity-theft.html
[3] http://en.wikipedia.org/wiki/Ghosting_(identity_theft)#General_description

2.1.1 Γνωστές περιπτώσεις ghosting

Ο πιο γνωστός ghoster είναι ο Ferdinand Waldo Demara, με το ψευδώνυμο '*ο μεγάλος απατεώνας*'. Η περίπτωσή του είναι ασυνήθιστη για δύο λόγους: 1) χρησιμοποίησε τις ταυτότητες πολλών διαφορετικών ανδρών και 2) όλα τα θύματα του Demara ήταν στη ζωή την εποχή της δράσης του. Μετά το θάνατό του το 1982, αποκαλύφθηκε ότι συνελήφθη δύο φορές με κατηγορίες για σεξουαλική κακοποίηση ανηλίκων.

Ο Αμερικανός ηθοποιός Wallace Ford, ήταν ένας επιτυχημένος ghoster. Γεννήθηκε στην Αγγλία με το όνομα Samuel Jones, απομακρύνθηκε από την οικογένειά του σε μικρή ηλικία και φοίτησε σε ένα σχολείο του Καναδά. Στην ηλικία των 15 ο Jones ήταν περιφερόμενος άστεγος και πηδούσε σε εμπορικά τρένα για να μεταναστεύσει από περιοχή σε περιοχή. Αυτό το έκανε με την παρέα ενός φίλου του ονόματι Wallace Ford.

Κάποτε βρέθηκαν πάνω σε ένα τρένο, το οποίο ενεπλάκη σε ένα σοβαρό σιδηροδρομικό ατύχημα. Ο Jones επιβίωσε αλλά ο Ford σκοτώθηκε. Τότε ο Jones οικειοποιήθηκε την ταυτότητα και μέρη της βιογραφίας του νεκρού φίλου του και έγινε ένας επιτυχημένος ηθοποιός με το όνομα Wallace Ford, ο οποίος πρωταγωνίστησε σε πολλές ταινίες του Hollywood καθώς και στα θέατρα του Broadway.

Ο ηθοποιός χρησιμοποίησε την πραγματική ημερομηνία γέννησης του Ford καθώς και τα φορολογικά του στοιχεία και έβγαλε ακόμα και διαβατήριο στο όνομα αυτό για να επιστρέψει στην Αγγλία το 1937. Λίγο πριν το θάνατό του, το 1966 αποκάλυψε την αλήθεια για την ταυτότητά του.

Αξίζει να σημειωθεί ότι ο Jones είχε ένα ιδανικό υποψήφιο φάντασμα: ένα νεκρό που είχε τη ίδια ηλικία, το ίδιο φύλο και ανήκε στην ίδια φυλή και ο θάνατός του δεν κατεγράφη ποτέ επίσημα, αού δεν υπήρχε κανείς για να τον αναγνωρίσει.

Άλλος ένας πιθανός ghoster ήταν ο Larry Semon. Γεννημένος το 1889, ο Semon είχε μια επιτυχημένη καριέρα ως κωμικός του βουβού κινηματογράφου. Όταν όμως ξεκίνησαν να κυκλοφορούν οι ταινίες με ήχο αντιμετώπισε σοβαρά οικονομικά προβλήματα και αναγκάστηκε να κηρύξει πτώχευση.

Σύντομα, το 1928 η οικογένεια του Semon δήλωσε τον ξαφνικό θάνατό του από πνευμονία σε ηλικία 39 ετών. Πιστεύεται, ότι οι συγγενείς του Semon έκαναν ψευδή δήλωση θανάτου για να εξαπατήσουν τους πιστωτές του και ο Semon ξεκίνησε μια νέα καριέρα με μία νέα άγνωστη ταυτότητα.

2.1.2 Μέτρα αντιμετώπισης του ghosting

Το ghosting δεν είναι τόσο εύκολο όσο παλαιότερα. Αυτό οφείλεται στη χρήση των υπολογιστών και στην μηχανογράφηση των ζωτικών στοιχείων των ανθρώπων καθώς και στην αυξανόμενη ισχύ των μηχανών αναζήτησης.

Προστασία από κλοπή προσωπικών στοιχείων

Μέχρι την δεκαετία του ’90 οι πολιτείες των Η.Π.Α. διατηρούσαν τα στοιχεία γεννήσεων και θανάτων σε διαφορετικά μητρώα. Τώρα πια, με τις μηχανές αναζήτησης οι υπάλληλοι μπορούν εύκολα να διασταυρώσουν τα στοιχεία αυτά. Πολλοί ghosters έχουν μαύρο ποινικό μητρώο στη πραγματική τους ταυτότητα.

Γι’ αυτό ψάχνουν νέες ταυτότητες για να κάνουν μία νέα αρχή για να ξεκινήσουν μία νέα εγκληματική καριέρα. Πριν τις μέρες της μηχανογράφησης και της εικόνας, αν ο απατεώνας πιανόταν με τη νέα του ταυτότητα, θα ήταν πολύ δύσκολο για τις αρχές να ψάξει τα αποτυπώματα για να δει αν το άτομο αυτό έχει συλληφθεί ξανά.

Πλέον, οι υπολογιστές μπορούν να συγκρίνουν εικόνες μεταξύ τους. Έτσι, μπορούν εύκολα και γρήγορα να συγκριθούν τα αποτυπώματα του συλληφθέντος με αυτά που βρίσκονται στα αρχεία της αστυνομίας.

Ένας άλλος παράγοντας που αποτρέπει τους επίδοξους ghosters είναι η χρήση των βιομετρικών στοιχείων και του DNA για ταυτοποίηση. Για παράδειγμα, ένας φυγάς με γνωστή ταυτότητα καταζητείται για φόνο. Η αστυνομία εντοπίζει κάποιον που η περιγραφή του ταιριάζει στο φυγά. Αυτός όμως ισχυρίζεται ότι είναι κάποιος άλλος και δεν υπάρχουν συγγενείς για να τον αναγνωρίσουν. Με την μέθοδο της ταυτοποίησης μέσω DNA, η αστυνομία μπορεί να διαπιστώσει εάν ο ύποπτος είναι πραγματικά αυτός που καταζητείται.

Παλαιοτέρα στις Η.Π.Α.[4], οι πολίτες δεν αποκτούσαν Αριθμό Κοινωνικής Ασφάλισης, εάν δεν έβρισκαν δουλεία. Το 1975, ένας ghoster θα μπορούσε να εκδώσει πιστοποιητικό γέννησης στο όνομα ενός αγοριού, που είχε πεθάνει πριν τα 15 του χρόνια και αν ζούσε θα είχε παρόμοια ηλικία με αυτόν.

Επειδή το αγόρι σίγουρα δεν είχε προλάβει να εκδώσει Αριθμό Κοινωνικής Ασφάλισης, ο απατεώνας θα μπορούσε να λάβει το πιστοποιητικό αφού θα ήταν δύσκολο να διασταυρωθεί ότι το αγόρι είχε πεθάνει. Μία τέτοια ενέργεια, θα ήταν αδύνατη το 2000 αφού οι γονείς είναι υποχρεωμένοι να εκδώσουν Αριθμό Κοινωνικής Ασφάλισης για το νεογνό τους πριν συμπληρώσουν την επόμενή τους φορολογική δήλωση.

Τέλος, μετά τα γεγονότα της 11ης Σεπτεμβρίου 2001, τα μέτρα ασφαλείας έχουν αυξηθεί δραματικά στις Η.Π.Α.. Συνήθως, όποιος χρησιμοποιεί την μέθοδο του ghosting, θεωρείται τρομοκράτης και διώκεται με αυστηρότατες ποινές.

[4] http://en.wikipedia.org/wiki/Ghosting_(identity_theft)#Drawbacks

Κεφάλαιο 3 Η κλοπή προσωπικών στοιχείων τη σημερινή εποχή

Οι διάφορες έρευνες στις Η.Π.Α από το 2003 έως το 2006 έδειξαν μείωση στο συνολικό αριθμό των θυμάτων και μείωση στην οικονομική επίπτωση της κλοπής ταυτότητας. Από $47600000000 του συνολικού κόστους των θυμάτων το 2003 σε $15600000000 το 2006. Το μέσο κόστος της απάτης ανά άτομο μειώθηκε από $4,789 το 2003 σε $1,882 το 2006.

Μία έρευνα που έγινε το 2003[5], από τον οργανισμό *Identity Theft Resource Center*, έδειξε ότι:

- το 15% των θυμάτων ανακαλύπτουν για την κλοπή μέσα από ενέργειες που κάνουν κάποιες επιχειρήσεις εναντίον του.
- Ο μέσος χρόνος που δαπανάται από τα θύματα για την επίλυση του προβλήματος είναι 330 ώρες.
- το 73% των ερωτηθέντων κατέδειξε ότι το έγκλημα έγινε μέσω κλοπής πιστωτικής κάρτας
- Ο συναισθηματικός αντίκτυπος των θυμάτων της κλοπής ταυτότητας είναι αντίστοιχος με αυτόν των θυμάτων βίαιων εγκλημάτων

Σε μία δίκη που έγινε στην Αμερική, η Michelle Brown που ήταν θύμα απάτης, κατέθεσε ότι η απατεώνισσα σε διάστημα 18 μηνών κατάφερε με την κλεμμένη της ταυτότητα να αποσπάσει αγαθά αξίας $50.000. Εκτός από οικονομική ζημιά η απατεώνισσα ενέπλεξε το όνομα της Κυρίας Brown σε ένα σοβαρό έγκλημα που ήτανε διακίνηση ναρκωτικών. Ακόμα και μετά τη σύλληψή της η απατεώνισσα φυλακίστηκε με τα στοιχεία της Κυρίας Brown.

Στην Αυστραλία το κόστος της κλοπής ταυτότητας ήταν το 2001 μεταξύ AU$1000000000 και AU$4000000000.

Στο Ηνωμένο Βασίλειο το κόστος της κλοπής ταυτότητος ανέρχεται στα £1200000000 κάθε χρόνο (αν και ειδικοί πιστεύουν ότι το νούμερο είναι πολύ μεγαλύτερο).

3.1 Πρόσφατες έρευνες σχετικά με την κλοπή ταυτότητας

Στην ενότητα αυτή θα συναντήσουμε διάφορες έρευνες οι οποίες αναφέρονται σε πολλές μορφές απάτης σχετικά με την κλοπή ταυτότητας, όπως για παράδειγμα τρόπους με τους οποίους το θύμα ανακάλυψε την απάτη και άλλες πολλές τις οποίες θα δούμε στην συνέχεια:

[5] http://en.wikipedia.org/wiki/Identity_theft#Spread_and_impact

3.1.1 Τρόποι ανακάλυψης της απάτης

Σύμφωνα με πρόσφατες έρευνες[6], ο πιο συνηθισμένος τρόπος με τον οποίο ανακαλύπτουν τα θύματα ότι τους έχουν κλέψει τα προσωπικά στοιχεία είναι οι κινήσεις των λογαριασμών τους (37% των θυμάτων). Αυτό ισχύει και για τα θύματα που πραγματοποιούν ηλεκτρονικές συναλλαγές (12%), γι αυτούς που συναλλάσσονται με κλασικό τρόπο (6%) αλλά και γι αυτούς που δεν ήταν σίγουροι για το αν το ανακάλυψαν σε διαδικτυακούς ή φυσικούς λογαριασμούς (8%). Η έρευνα ισχύει και γι αυτούς που το ανακάλυψαν χρησιμοποιώντας μία ειδική υπηρεσία παρακολούθησης συναλλαγών (11%).

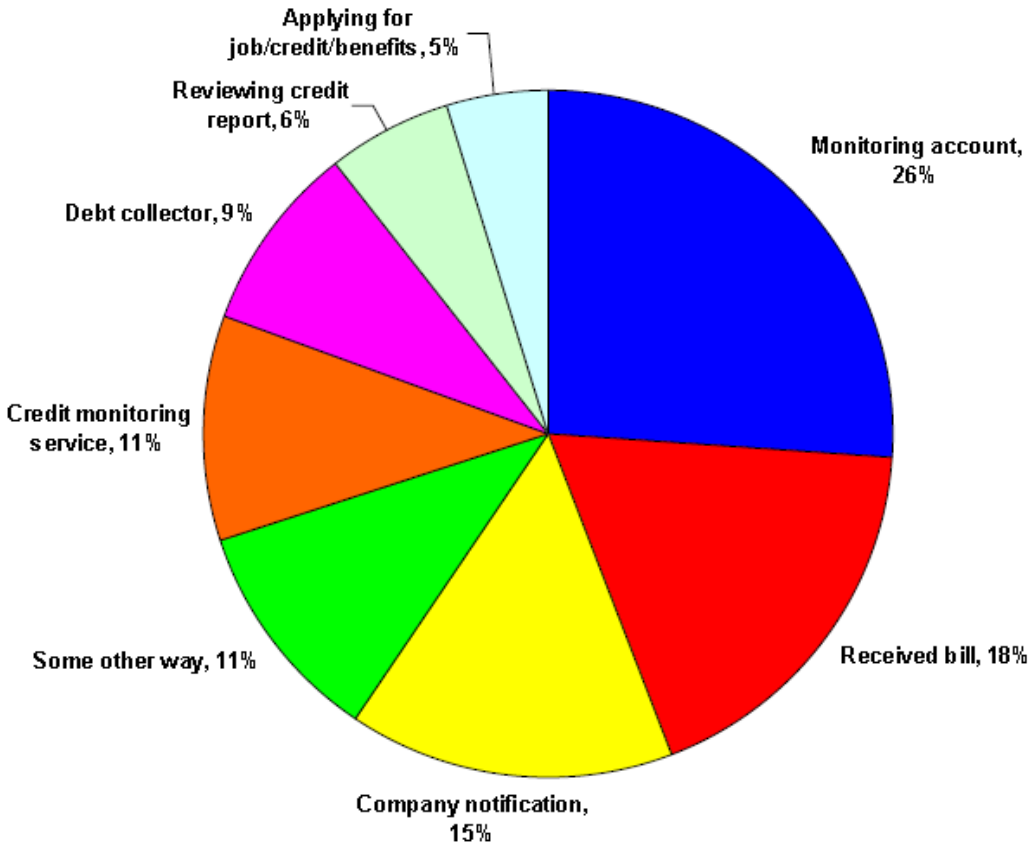
Ο πιθανότερος τρόπος να ανακαλύψει το θύμα την απάτη εξαρτάται από το τύπο της κλοπής που του έχει συμβεί. Όταν λοιπόν η απάτη περιορίζεται σε μια υπάρχουσα πιστωτική κάρτα, το θύμα το ανακαλύπτει όταν λάβει ένα λογαριασμό με παράλογες χρεώσεις (25%), όταν παρακολουθεί τους λογαριασμούς του (24%), ή αν ειδοποιηθεί το θύμα από υπερβολική κίνηση λογαριασμών από την εταιρεία που επηρεάζεται (23%).

Όσον αφορά τους υπάρχοντες λογαριασμούς που δεν έχουν σχέση με πιστωτική κάρτα, το 41% των θυμάτων ανακάλυψαν την απάτη παρακολουθώντας την κίνηση των λογαριασμών τους. Τα θύματα στων οποίων το όνομα ανοίχτηκαν νέοι λογαριασμοί, το ανακάλυψαν όταν επικοινώνησε μαζί τους μια εισπρακτική εταιρεία (σε ποσοστό 23%).

Η παρακολούθηση των λογαριασμών είναι ο πιθανότερος τρόπος να ανακαλύψει το θύμα την απάτη στην περίπτωση υπάρχοντος λογαριασμού χωρίς πιστωτική κάρτα (41%), και στην περίπτωση λογαριασμού με πιστωτική κάρτα (24%). Η μέθοδος αυτή χρησίμευσε σε αυτούς στων οποίων το όνομα είχαν ανοιχτεί νέοι λογαριασμοί ή είχε γίνει κάποια άλλη απάτη σε βάρος τους σε ποσοστό 11%.

Τα αποτελέσματα των παραπάνω ερευνών απεικονίζονται στο ακόλουθο διάγραμμα:

[6] Federal Trade Commission: 2006 Identity Theft Survey Report: Prepared for the Commission by Synovate (November 2007)

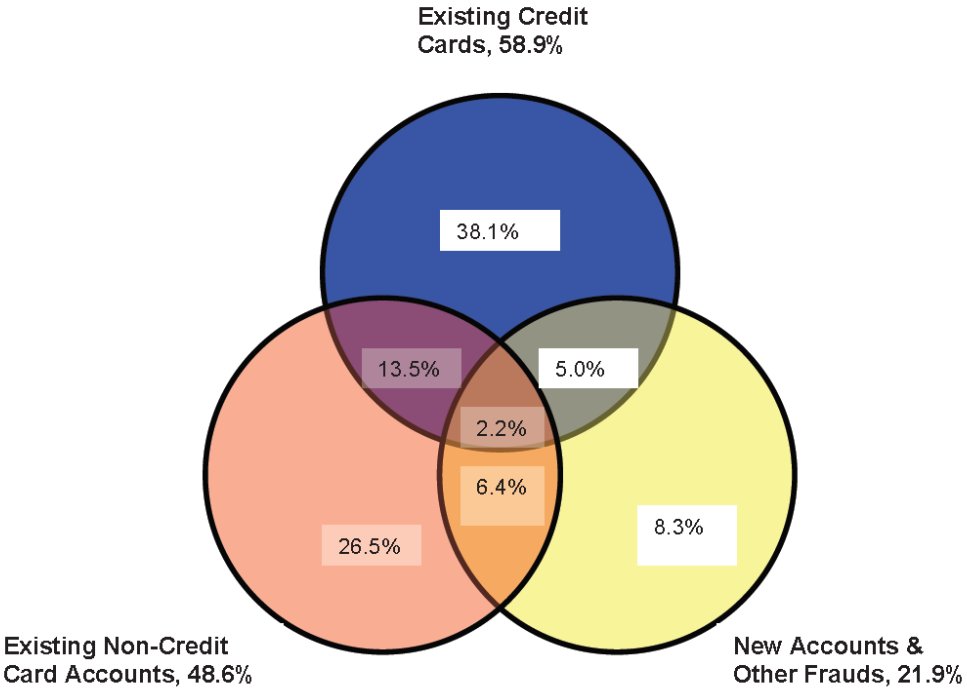


Εικόνα 1: Μερικοί από τους τρόπους που το θύμα ανακάλυψε την απάτη

3.1.1 Πολλαπλές επιθέσεις κλοπής στοιχείων σε ένα θύμα[7]

Για τις περισσότερες περιπτώσεις αυτή η αναφορά ομαδοποιεί τα θύματα ανάλογα με τη σοβαρότερη μορφή κλοπής που συνέβη στο κάθε θύμα. Πολλά θύματα έχουν υποστεί διαφορετικούς τύπους κλοπής και στο παρακάτω διάγραμμα φαίνεται η επικάλυψη μεταξύ των τύπων:

[7] Federal Trade Commission: 2006 Identity Theft Survey Report: Prepared for the Commission by Synovate (November 2007)



Εικόνα 2: Επικάλυψη μεταξύ των κατηγοριών

- 58,9% των θυμάτων υπέστησαν κατάχρηση της πιστωτικής τους κάρτας.
- 48,6% των θυμάτων υπέστησαν κατάχρηση των λογαριασμών τους.
- Για το 21,9% των θυμάτων χρησιμοποιήθηκαν τα προσωπικά στοιχεία για να ανοίξει ένας νέος λογαριασμός ή για τη διάπραξη κάποιας άλλης απάτης.
- Για το 38,1% των θυμάτων η κατάχρηση της πιστωτικής κάρτας ήτανε η μόνη ζημιά που υπέστησαν.
- Τα θύματα που υπέστησαν κατάχρηση υπαρχόντων λογαριασμών, εκτός από πιστωτική κάρτα, περιλαμβάνονται στο σχήμα.
- Όλα τα θύματα των οποίων οι προσωπικές πληροφορίες χρησιμοποιήθηκαν για να ανοίξουν νέοι λογαριασμοί, περιλαμβάνονται επίσης στο σχήμα. Αυτοί αποτελούν το 21,9%.

3.1.2 Νέοι λογαριασμοί που ανοίχτηκαν το 2005 από απατεώνες

Η έρευνα αυτή[8], αφορά τους τύπους νέων λογαριασμών που ανοίχτηκαν από τους κλέφτες ταυτότητας εν αγνοία των θυμάτων. Οι τύποι αυτοί φαίνονται στο επόμενο σχήμα.

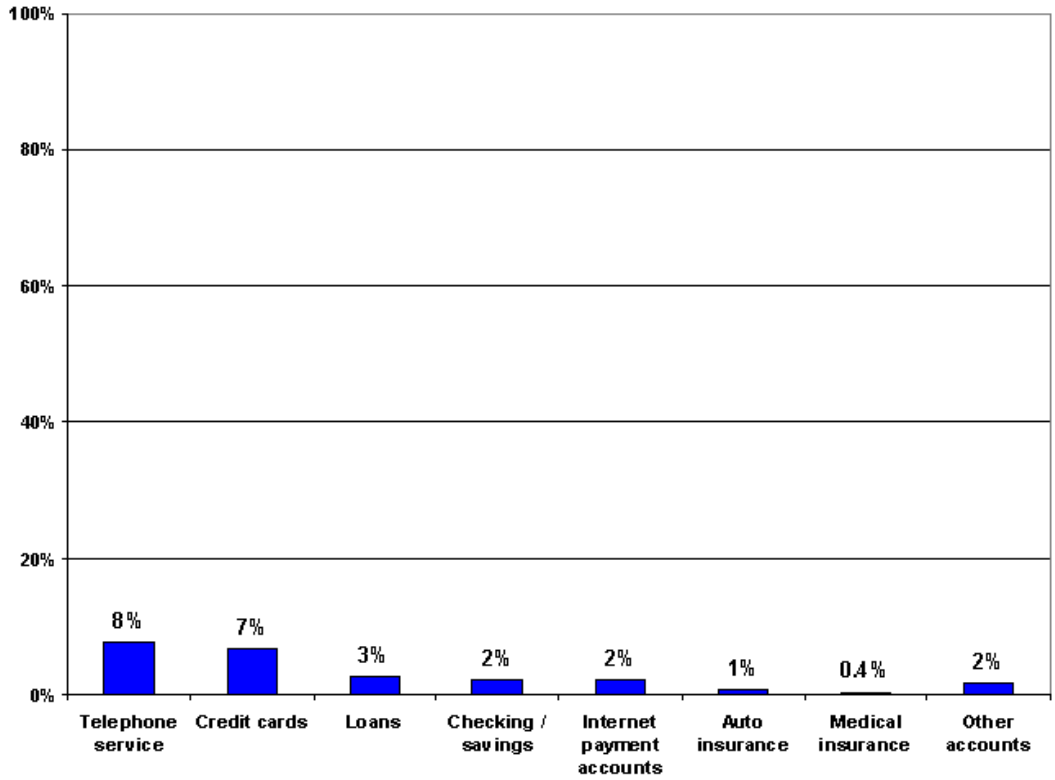
[8] Federal Trade Commission: 2006 Identity Theft Survey Report: Prepared for the Commission by Synovate (November 2007)

- 17% του συνόλου των θυμάτων δήλωσαν ότι οι κλέφτες χρησιμοποίησαν τις προσωπικές τους πληροφορίες για να ανοίξουν τουλάχιστον ένα λογαριασμό.

- Οι δύο πιο συνηθισμένες κατηγορίες νέων λογαριασμών που ανοίχτηκαν, ήταν 1) τηλεφωνικών υπηρεσιών (κινητών και σταθερών) και 2) λογαριασμοί πιστωτικών καρτών (8% και 7% των θυμάτων αντίστοιχα).

- Κάτι παραπάνω από τα μισά θύματα που κατήγγειλαν άνοιγμα νέου λογαριασμού, δήλωσαν ότι είχε ανοιχθεί ένας λογαριασμός στο όνομά τους

- ¼ των θυμάτων δήλωσε ότι ανοίχτηκαν στο όνομά τους νέοι λογαριασμοί.



Εικόνα 3: Τύποι νέων λογαριασμών που ανοίχθηκαν από τους κλέφτες

3.1.3 Παρέλευση χρόνου για την ανακάλυψη της απάτης

Σχεδόν το 40% των θυμάτων ανακάλυψαν την κατάχρηση των προσωπικών τους στοιχείων μέσα σε μία εβδομάδα από τότε που ξεκίνησε. Παρόλα αυτά η περίοδος της ανακάλυψης διέφερε ανάλογα με το τύπο της απάτης[9].

- Τα θύματα απάτης με υπάρχουσες πιστωτικές κάρτες (22%) και με υπάρχοντες λογαριασμούς (21%), συνήθως ανακάλυπταν την απάτη την μέρα που ξεκίνησε, σε αντίθεση με τα θύματα νέων λογαριασμών (10%)

[9] Federal Trade Commission: 2006 Identity Theft Survey Report: Prepared for the Commission by Synovate (November 2007)

- Σχεδόν το ¼ των θυμάτων με νέους λογαριασμούς και άλλες απάτες, ανακάλυψαν το γεγονός τουλάχιστον 6 μήνες μετά που ξεκίνησε. Τα θύματα με υπάρχοντες λογαριασμούς και πιστωτικές κάρτες, που ανακάλυψαν την απάτη σε τόσο μεγάλο χρονικό διάστημα αποτελούν μόλις το 3%.

- Στην κατηγορία των θυμάτων υπαρχόντων λογαριασμών, ο μέσος χρόνος ανακάλυψης ήταν μεταξύ μιας εβδομάδας και ενός μήνα. Για τους νέους λογαριασμούς ο μέσος χρόνος ήταν μεταξύ ενός και δύο μηνών.

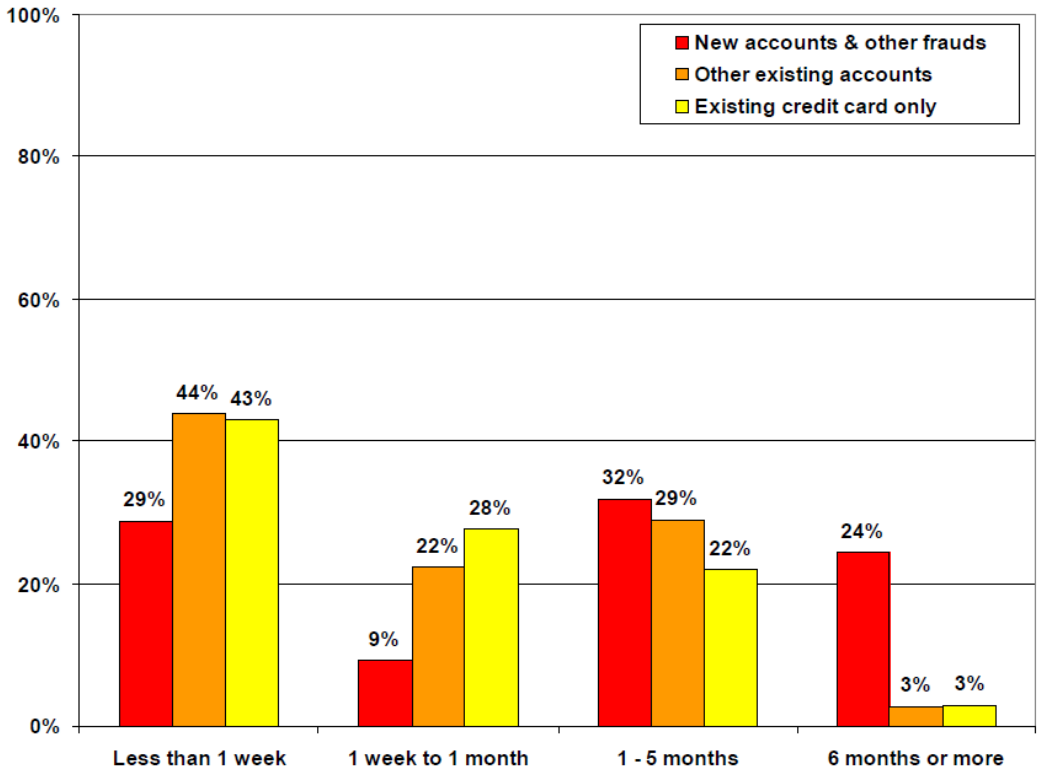
Στις περιπτώσεις που η ανακάλυψη του γεγονότος έγινε πιο γρήγορα, τα θύματα ανέφεραν ότι είχαν μικρότερες απώλειες χρημάτων.

- 30% αυτών που ανακάλυψαν την απάτη μετά από 6 μήνες ή περισσότερο, έχασαν $1000 τουλάχιστον παραπάνω από αυτούς που την ανακάλυψαν μέσα σε 6 μήνες.

- 69% αυτών που ανακάλυψαν την απάτη μέσα σε 6 μήνες, ξόδεψαν λιγότερο από 10 ώρες σε σχέση με το 32% αυτών που την ανακάλυψαν σε πάνω από 6 μήνες.

- 31% αυτών που ανακάλυψαν την απάτη σε πάνω από 6 μήνες, υπέστησαν ζημιά τουλάχιστον $5000, σε σύγκριση με το 10% αυτών που την ανακάλυψαν μέσα σε 6 μήνες.

Τα ποσοστά φαίνονται και στην παρακάτω εικόνα:



Εικόνα 4: Παρέλευση χρόνου για την ανακάλυψη της απάτης

3.1.4 Προσωπικές σχέσεις θυμάτων και απατεώνων

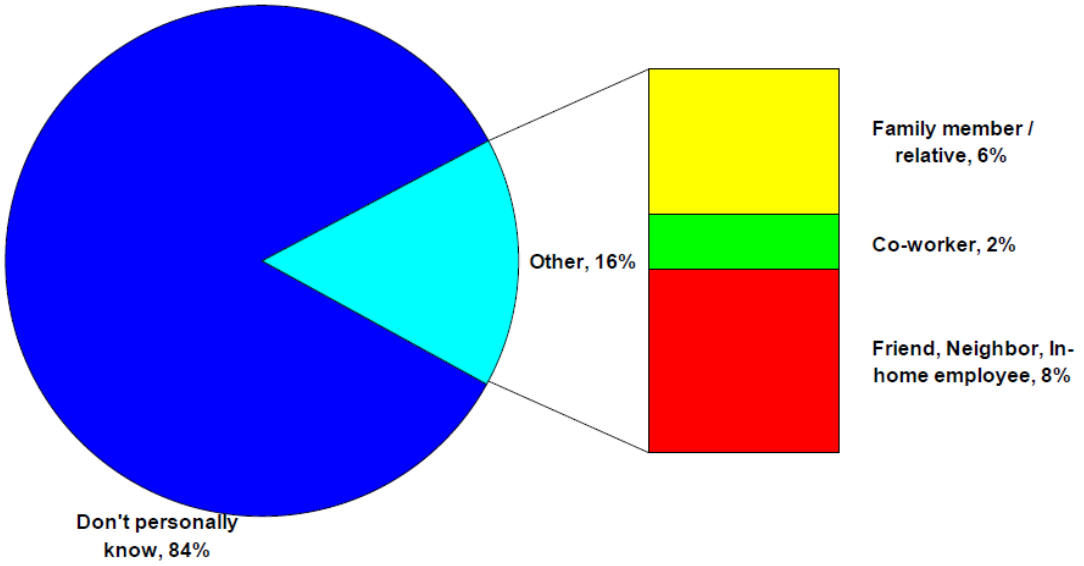
Η παρακάτω έρευνα διεξήχθη επίσης το 2005[10], δείχνει τυχόν προσωπικές σχέσεις μεταξύ θυμάτων και απατεώνων.

- Τα θύματα σε ποσοστό 84%, ανέφεραν ότι δεν γνώριζαν και δεν είχαν προσωπικές σχέσεις με το κλέφτη παρόλο που μπορεί να είχαν πληροφορίες σχετικά με τη ταυτότητά του.

- Το 16% των θυμάτων ανέφεραν ότι γνώριζαν το κλέφτη.

    - Το 6% των θυμάτων δήλωσαν ότι ο κλέφτης ήταν συγγενικό πρόσωπο
    - Το 8% δήλωσε ότι ο κλέφτης ήταν φίλος γείτονας
    - Το 2% των θυμάτων δήλωσαν ότι ο κλέφτης προερχόταν από το εργασιακό τους περιβάλλον

- Τα θύματα στις κατηγορίες των νέων λογαριασμών, είχαν 5πλάσια πιθανότητα να γνωρίζουν τον απατεώνα, από τα θύματα υπαρχόντων πιστωτικών καρτών.

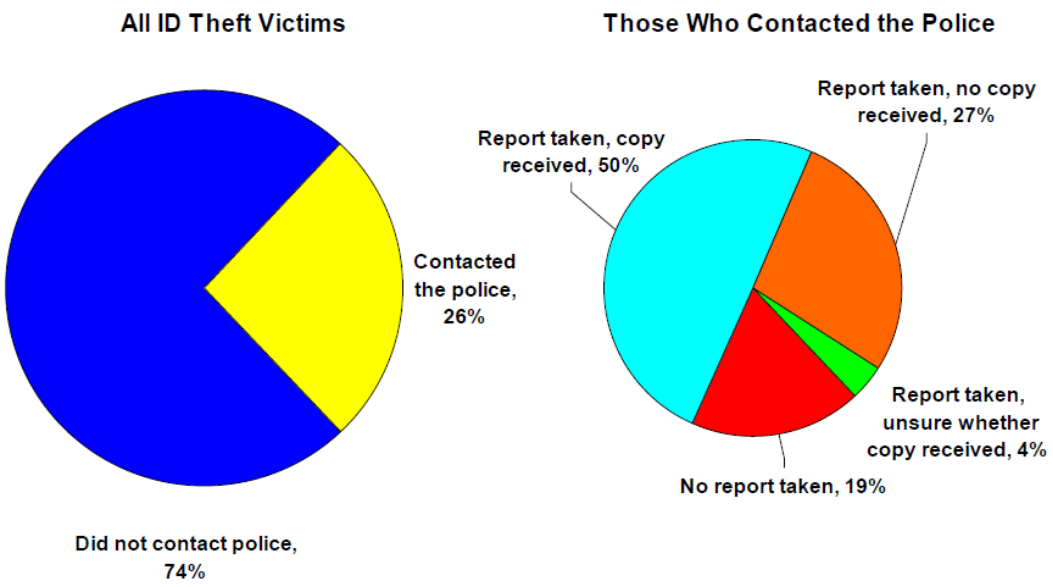


Εικόνα 5: Σχέσεις των θυμάτων με τους κλέφτες

[10] Federal Trade Commission: 2006 Identity Theft Survey Report: Prepared for the Commission by Synovate (November 2007)

3.1.5 Ποσοστό των θυμάτων που επικοινωνεί με τις αρχές[11]

- Το 26% των θυμάτων επικοινώνησε με μία τοπική αρχή.
- Από τα θύματα υπαρχόντων πιστωτικών καρτών, το 9% επικοινώνησε με την αστυνομία και από τα θύματα νέων λογαριασμών το 44% επικοινώνησε με την αστυνομία.
- Το 81% των θυμάτων που επικοινώνησε με ένα τοπικό φορέα, ανέφερε ότι για το περιστατικό έλαβε γνώση η αστυνομία.
- Η αστυνομία δεν έλαβε αναφορά από το 19% των θυμάτων που επικοινώνησαν μαζί της.
- Από αυτούς που έκαναν αναφορά στην αστυνομία, το 60% έλαβε αντίγραφο της αναφοράς, το 40% δεν έλαβε αντίγραφο ή δεν θυμάται να έλαβε.



Εικόνα 6: Επικοινωνία των θυμάτων με τις αρχές

[11] Federal Trade Commission: 2006 Identity Theft Survey Report: Prepared for the Commission by Synovate (November 2007)

Κεφάλαιο 4 Επιθέσεις για κλοπή στοιχείων

Η κλοπή της ταυτότητας ενός ατόμου ορίζεται ως η χρήση προσωπικών στοιχείων ενός ατόμου από τρίτο κυρίως προς οικονομικό όφελος του εγκληματία σε βάρος του ιδιοκτήτη των στοιχείων.

Σε πολλές χώρες αυτό συνεπάγεται τη γνώση στοιχείων πιστωτικών καρτών, ΑΦΜ, προσωπικών στοιχείων όπως ημερομηνίας γεννήσεως και πατρικό όνομα του ίδιου του ατόμου ή της μητρός του. Με λίγα λόγια λοιπόν η κλοπή ταυτότητας είναι έγκλημα.

4.1 Τεχνικές άντλησης προσωπικών στοιχείων

Στις πιο πολλές περιπτώσεις ο απατεώνας χρειάζεται να βρει στοιχεία ταυτότητας ή προσωπικά έγγραφα για να παραστήσει με επιτυχία το θύμα. Οι τεχνικές που μπορούν να χρησιμοποιηθούν για το σκοπό αυτό είναι οι εξής:

- Ανάκτηση πληροφοριών από άχρηστους servers που τους έχουν εναποθέσει σε δημόσιους χώρους υγειονομικής ταφής.
- Ψάχνοντας πληροφορίες για το θύμα σε κρατικά μητρώα, σε μηχανές αναζήτησης, ή δημόσια έγγραφα.
- Διαβάζοντας από μακριά πληροφορίες από το RFID chip μιας έξυπνης κάρτας.
- Κλέβοντας προσωπικές πληροφορίες από υπολογιστές και βάσεις δεδομένων (μέσω Trojan horses και hacking).
- Εισχώρηση σε οργανισμούς που αποθηκεύουν μεγάλες ποσότητες προσωπικών πληροφοριών.
- Χρησιμοποιώντας ψεύτικους ισχυρισμούς για να αποσπάσει προσωπικές πληροφορίες πελατών από επιχειρήσεις.
- Διαφημίζοντας ψεύτικες προσφορές για εργασία ώστε το θύμα να απαντήσει με τα πλήρη στοιχεία του.
- Προσποίηση του απατεώνα ότι είναι μια έμπιστη οντότητα σε μία ηλεκτρονική επικοινωνία.
- Ψάχνοντας σε ιστοσελίδες κοινωνικών επαφών (για παράδειγμα τα MySpace και Facebook).
- Αλλάζοντας την διεύθυνση του θύματος ώστε η σημαντική αλληλογραφία να προωθείται σε μια διεύθυνση του απατεώνα.

- Κλοπή αλληλογραφίας ή ψάξιμο στα σκουπίδια για προσωπικές πληροφορίες.
- Κλέβοντας ταυτότητες από την τσέπη του θύματος με φυσικό τρόπο.
- Παρακολουθώντας κρυφά το θύμα όταν δίνει προσωπικές πληροφορίες.
- Παραβίαση δεδομένων που έχει σαν αποτέλεσμα κοινοποίησης προσωπικών πληροφοριών.

4.2 Παραδείγματα επιθέσεων

Οι υπηρεσίες όπως η πληρωμή λογαριασμών, τραπεζικές συναλλαγές, αγοραπωλησία μετοχών και αγορές προϊόντων, μέσω Διαδικτύου, έχουν γίνει τη σημερινή εποχή ιδιαίτερα διαδεδομένες.

Μετά από έρευνα που διεξήχθη στην Αμερική το 2003[12], το 13% των συμμετεχόντων δήλωσε ότι τα προσωπικά του στοιχεία εκλάπησαν κατά την διάρκεια συναλλαγών μέσω Διαδικτύου. Πολλές διαδικτυακές υπηρεσίες περιλαμβάνουν μία φόρμα ταυτοποίησης και αυθεντικοποίησης μέσω ονόματος χρήστη (username) και κωδικού πρόσβασης (password). Παρόλο που είναι πιο άνετο να γίνονται οι συναλλαγές μέσω του Διαδικτύου, αφήνονται τα προσωπικά στοιχεία εκτεθειμένα σε διαδικτυακές απειλές.

Πολλές φορές οι άνθρωποι γίνονται εχθροί του ίδιου τους του εαυτού, ειδικά όταν εμπλέκονται δωρεάν αγαθά. Υπάρχουν, για παράδειγμα, πολλές περιπτώσεις όπου ένα κατάστημα προσφέρει εκπτωτικές κάρτες σε αντάλλαγμα με τα προσωπικά στοιχεία και την υπογραφή των πελατών. Υπάρχει ακόμη περίπτωση οι απατεώνες με κάποιο τρόπο να αποκτήσουν προσωπικά στοιχεία πελατών από οργανισμούς που τα συλλέγουν.

Ένα τέτοιο παράδειγμα εμφανίστηκε στην Ατλάντα με θύματα ηλικιωμένους. Κάποια άτομα ισχυρίστηκαν πως είναι από μια εταιρεία φαρμάκων την Medicare και πρόσφεραν υποτιθέμενες εκπτωτικές κάρτες για τα φάρμακα. Αυτές οι κάρτες φυσικά, δεν ήταν εγκεκριμένες και δεν έκαναν κανένα καλό στους ηλικιωμένους. Απλά, οι απατεώνες εκμεταλλεύτηκαν το γεγονός ότι οι ηλικιωμένοι είναι ευκολόπιστοι και αποτελούν εύκολα θύματα.

Σε κάθε περίπτωση οι άνθρωποι πρέπει να προσέχουν σε ποιον δίνουν τα προσωπικά τους στοιχεία και γιατί θα χρησιμοποιηθούν αυτά. Ακόμα, πρέπει να ελέγχουν αν οι εταιρείες που συλλέγουν τα προσωπικά τους στοιχεία έχουν κάποια πολιτική απορρήτου.

Κάτι άλλο που πρέπει να προσέχουν οι καταναλωτές είναι η *διαχείριση των κωδικών πρόσβασης (password)*. Δηλαδή δεν πρέπει να χρησιμοποιούν το ίδιο password σε όλους τους διαδικτυακούς τόπους (websites).

[12] http://theses.nps.navy.mil/05Dec_Ruppar.pdf

Μια έρευνα που διεξήχθη από την εταιρεία VeriSign και δημοσιεύθηκε το 2005[13], κατέληξε στο συμπέρασμα ότι το 79% των συμμετεχόντων χρησιμοποιούν το ίδιο password σε διαφορετικά websites και εφαρμογές. Φυσικά είναι απαραίτητο τα passwords να έχουν ένα βαθμό δυσκολίας που να παρέχει αρκετή ασφάλεια. Να μην είναι δηλαδή ονόματα ή κοινές λέξεις από το λεξικό.

Η ανάγκη που έχει κάποιος να κατέχει την τελευταία τεχνολογία μπορεί να τον αφήσει εκτεθειμένο σε απειλές. Η συγκέντρωση, για παράδειγμα, πληροφοριών σε συσκευές όπως PDA και κινητά τηλέφωνα μπορεί να θέσει ένα άτομο σε κίνδυνο αν η συσκευή πέσει σε λάθος χέρια.

Στα κινητά βρίσκονται αποθηκευμένες πληροφορίες όπως αριθμοί τηλεφώνων, ιστορικό κλήσεων και φωτογραφίες. Ακόμα, συσκευές όπως fax, εκτυπωτές, φωτοαντιγραφικά αποθηκεύουν πληροφορίες που τους στέλνονται, οι οποίες μπορούν να ανακληθούν.

Παράδειγμα: Στην περίπτωση αυτή, δεν εκλάπη κάποιο PDA ή κινητό τηλέφωνο αλλά κάποιο laptop που είναι και αυτό φορητή συσκευή, και μπορεί να περιέχει επίσης πολύ σημαντικά δεδομένα.

Το παράδειγμα έρχεται από την Αμερική[14], από το κολλέγιο Berkeley του Ohio. Εκεί εκλάπη ένα laptop από το γραφείο υποδοχής σπουδαστών. Αυτό περιείχε τα προσωπικά δεδομένα 98000 περίπου φοιτητών και αιτούντων φοίτησης.

Όπως γνωρίζουμε, τα δεδομένα αυτά θα μπορούσαν να χρησιμοποιηθούν για πλήθος παράνομων δραστηριοτήτων κυρίως οικονομικής φύσεως. Στην πραγματικότητα, κανείς δεν έμαθε ποτέ αν τελικά έγινε κάποια απάτη.

Η Αστυνομία συνέλαβε έναν άνδρα από το San Francisco, ο οποίος κατείχε αρχικά το laptop και αργότερα το πούλησε μέσω Διαδικτύου. Ο άνδρας δήλωσε ότι είχε αγοράσει τη συσκευή από μία γυναίκα της οποίας η περιγραφή ταίριαζε με αυτή του βασικού υπόπτου της κλοπής.

Παρόλο που ήταν αδύνατον να εντοπιστεί εάν είχαν παραβιαστεί τα δεδομένα, η Αστυνομία υποστήριξε ότι δεν εντοπίστηκε κάποια περίπτωση κλοπής ταυτότητας και ο σκοπός της γυναίκας ήταν απλά η κλοπή και η μεταπώληση του υπολογιστή.

Οι άνθρωποι τη σημερινή εποχή δίνουν τα προσωπικά τους στοιχεί για διάφορους σκοπούς. Μετά από μία έρευνα που έγινε από μία εταιρεία, εξήχθη το συμπέρασμα ότι πολλοί άνθρωποι δίνουν προσωπικές πληροφορίες ακόμα και σε μία δημοσκόπηση στο δρόμο.

Αυτό που πρέπει να γίνει είναι να αλλάξει η νοοτροπία των ανθρώπων ώστε να μην βλέπουν τα προσωπικά στοιχεία απλά σαν μέσω ταυτοποίησης αλλά ως πολύτιμες πληροφορίες που πρέπει να διαφυλαχθούν.

[13] http://theses.nps.navy.mil/05Dec_Ruppar.pdf
[14] https://www.securityfocus.com/news/11319

4.3 Συχνοί τρόποι κλοπής στοιχείων και απάτης

Πολλοί άνθρωποι δεν μπορούν να καταλάβουν πόσο εύκολο είναι να τους κλέψει κάποιος τα προσωπικά στοιχεία χωρίς να τους διαρρήξει το σπίτι. Για παράδειγμα, σε δημόσιους χώρους ο επιτιθέμενος μπορεί να παρακολουθεί το θύμα από κοντινή απόσταση ή να ακούει μια συνομιλία του θύματος όπου γίνεται κάποια παράθεση προσωπικών στοιχείων.

4.3.1 Άντληση στοιχείων σχετικών με τραπεζικές κάρτες

Τα κρούσματα εντοπίστηκαν τόσο στις περιπτώσεις χρήσης χρεωστικών καρτών όσο και πιστωτικών.

Οι επιτήδειοι έκαναν το εξής: Ο ανυποψίαστος πελάτης καθόταν μπροστά από το ATM προκειμένου να κάνει τη συναλλαγή του. Ένας από την ομάδα καθόταν αρκετά πίσω του, δείχνοντας ότι περιμένει υπομονετικά τη σειρά του.

Ένας άλλος της ομάδας πετούσε ένα χαρτονόμισμα, σχετικά μεγάλης αξίας (50 ευρώ, 100 ευρώ κ.λπ.), στα πόδια του πελάτη της τράπεζας. Ο επιτήδειος τον ρωτούσε μήπως είναι δικό του. Κοιτάζοντας κάτω ο πελάτης, αποσπώντας την προσοχή, ο «συνεργάτης» παρακολουθούσε και προσπαθούσε να απομνημονεύσει τον αριθμό της κάρτας και το pin (κωδικός) που θα πληκτρολογούσε ο κάτοχος της κάρτας. Μετά η έκδοση πλαστής χρεωστικής κάρτας (αλλά και πιστωτικής) είναι «απλή» για τους αετονύχηδες και κοστίζει γύρω στα 10 ευρώ το κομμάτι.

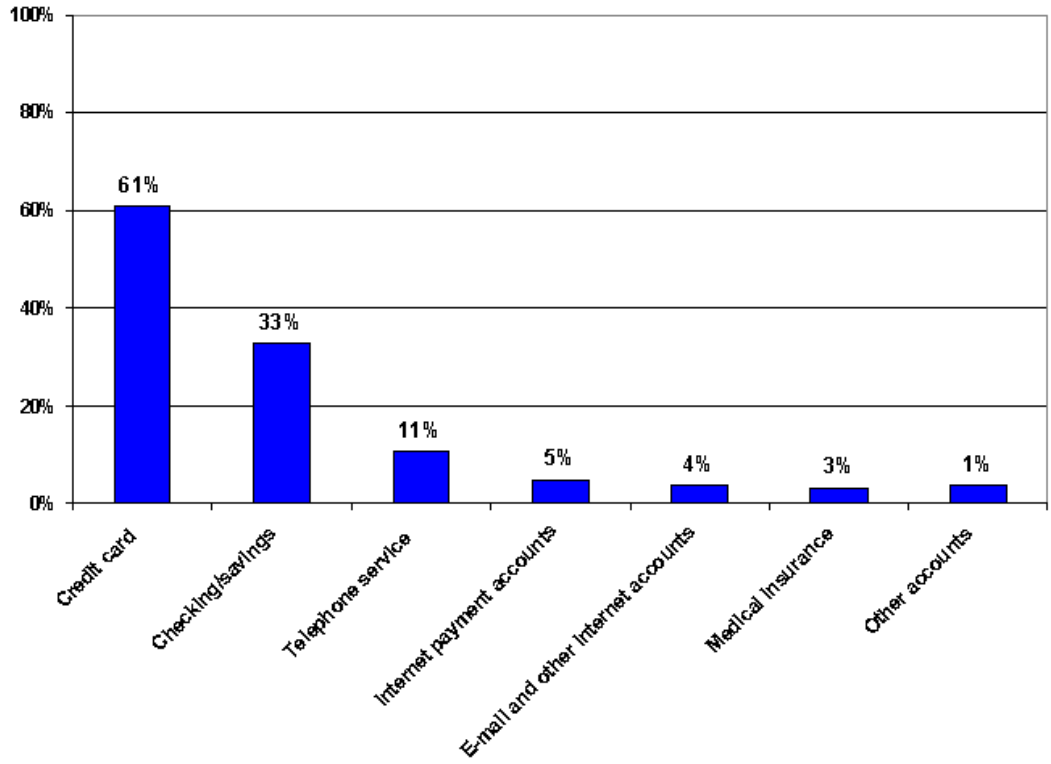
4.3.2 Κατάχρηση υπαρχόντων λογαριασμών[15]

Μερικές φορές οι απατεώνες κάνουν διάφορους ελιγμούς για να διευκολύνουν την παράνομη χρήση των λογαριασμών των θυμάτων. Μπορεί να αλλάξουν τις διευθύνσεις αποστολής των λογαριασμών για να κρυφτούν ή να προχωρήσουν σε έκδοση κάρτας στο όνομά τους. Αυτές οι παράνομες δράσεις έχουν σαν αποτέλεσμα τον πλήρη έλεγχο των λογαριασμών του θύματος από τους απατεώνες (**account takeover**).

Το παρακάτω διάγραμμα βασίζεται στις απαντήσεις των ανθρώπων που ανέφεραν ότι ανακάλυψαν την κατάχρηση των προσωπικών τους πληροφοριών μεταξύ του 2001 και 2005. Στην συγκεκριμένη έρευνα συμμετείχαν 559 άτομα.

Όπως βλέπουμε και στην Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε. **7**, το 85% των θυμάτων της κλοπής ταυτότητας, ανέφεραν ότι ένας ή περισσότερους από τους λογαριασμούς τους είχαν χρησιμοποιηθεί από τους απατεώνες. Στο σχήμα περιλαμβάνονται στοιχεία που αφορούν πιστωτικές κάρτες και στοιχεία που δεν αφορούν.

[15] Federal Trade Commission: 2006 Identity Theft Survey Report: Prepared for the Commission by Synovate (November 2007)



Εικόνα 7: Τρόποι με τους οποίους τα θύματα ανακάλυψαν την κατάχρηση των λογαριασμών τους

Τα περισσότερα από τα στοιχεία της παραγράφου αυτής αντλήθηκαν από μια έρευνα που δημοσιοποιήθηκε το 2006 από την υπηρεσία εμπορίου της Αμερικής (Federal Trade Commission).

Παράδειγμα: *Οι απάτες με λογαριασμούς επιταγών αυξάνονται*[16]

Όταν η Shereen Greene έλεγξε την οικονομική αναφορά της τράπεζάς της, ανακάλυψε μία χρέωση $139 από μία εταιρεία που δεν είχε ποτέ ακούσει την Pharmacycards.com. Οι διωκτικές αρχές της Ατλάντα ανακάλυψαν την επιταγή που είχε χρησιμοποιηθεί για τη συναλλαγή και είδαν πως ήταν πλαστή.

Το όνομα που ήταν πάνω στην επιταγή, ήταν το πατρικό της γυναίκας, το οποίο δεν είχε χρησιμοποιήσει για 7 χρόνια. Η διεύθυνση ήταν 5 ετών και η υπογραφή έλλειπε. Στη θέση της υπογραφής υπήρχε το παρακάτω μήνυμα.:
'*Εγκεκριμένο από το πελάτη – δεν απαιτείται υπογραφή*'. Ακόμα ο αριθμός στο κάτω μέρος της επιταγής ανήκε στο τραπεζικό λογαριασμό της κας Greene.

Η κα Greene είναι ένα από τα πιο πρόσφατα θύματα μιας μεγάλης κλίμακας απάτης με λογαριασμούς επιταγών. Οι απατεώνες προσπάθησαν να αποσπάσουν $12000000 από 90000 τραπεζικούς λογαριασμούς σύμφωνα με τα στοιχεία της μήνυσης που υπέβαλε το Federal Trade Commission.

Τέτοιου είδους απάτες αυξάνονται συνεχώς και βασίζονται σε μεγάλο βαθμό στο αυτοματοποιημένο σύστημα επιταγών και στην αύξηση των ηλεκτρονικών συναλλαγών.

[16] http://www.washingtonpost.com/wp-dyn/articles/A60345-2004Jul18.html

Το ηλεκτρονικό τραπεζικό σύστημα διεκπεραιώνει 10000000000 ηλεκτρονικές συναλλαγές το χρόνο καθώς οι καταναλωτές εγκαταλείπουν τις παραδοσιακές χάρτινες επιταγές. Οι καταναλωτές προτιμούν να κατατίθεται ο μισθός τους κατευθείαν στον τραπεζικό τους λογαριασμό καθώς και οι υπόλοιποί τους λογαριασμοί να πληρώνονται αυτόματα μέσω των χρημάτων που έχουν στην τράπεζα.

Οι απατεώνες εκμεταλλεύονται το αυτοματοποιημένο τραπεζικό σύστημα για να προσθέσουν ψευδή χρέη σε ανυποψίαστους καταναλωτές. Ακόμα μερικοί χρησιμοποιούν πολύπλοκη αλλά φθηνή τεχνολογία για να τυπώσουν επιταγές και εκμεταλλεύονται μία τραπεζική πρακτική που επιτρέπει σε εταιρείες να γράφουν ανυπόγραφες επιταγές για λογαριασμό των καταναλωτών που έχουν ισχύ για μία συναλλαγή.

Στις περιπτώσεις αυτές οι απατεώνες αποκομίζουν πολλά χρήματα χωρίς ιδιαίτερο κόπο (ίσως έχουν μία τηλεφωνική συζήτηση με το θύμα που εξαπατούν) οι τράπεζες είναι υποχρεωμένες να αποζημιώσουν το πελάτη τους για κάθε παράνομη ανάληψη από το λογαριασμό του αλλά στις περισσότερες περιπτώσεις είναι δύσκολο να αποδειχθεί ότι μία χρέωση είναι ψευδής και είναι αποτέλεσμα απάτης.

Παράδειγμα: ***Ένας υπάλληλος της τράπεζας είναι ένοχος για απάτη $1300000***[17]

Ένας υπάλληλος τράπεζας αντιμετώπισε κατηγορίες για συνέργια σε απάτη ύψους £1300000000 που διαπράχτηκε από κλέφτες ταυτότητας. Για ένα χρόνο η Shana Campbell μεταβίβαζε εμπιστευτικές πληροφορίες σε απατεώνες απολαμβάνοντας μία πολυτελή ζωή σε βάρος των πελατών.

Οι απατεώνες παρίσταναν τους πελάτες και με χρήση πλαστών εγγράφων, έβαζαν στόχο καταθέσεις υψηλής αξίας και στη συνέχεια ξέπλεναν τα χρήματα μέσω εμπόρων αυτοκινήτων.

Στο δικαστήριο του Λονδίνου κατέθεσαν πολλά θύματα, στα οποία συμπεριλαμβάνονταν ένας εφημέριος, πολλοί επιχειρηματίες και μερικοί συνταξιούχοι που έχασαν τις οικονομίες τους. Ένας Νιγηριανός πρίγκιπας και μερικοί Αφρικανοί πολιτικοί έπεσαν θύματα επίσης.

Ακόμα και οι νεκροί δεν ήταν ασφαλείς. Τρεις λογαριασμοί της τράπεζας της Σκοτίας, που ανήκαν σε μία προσφάτως αποθανούσα γυναίκα, παραβιάστηκαν και εκλάπησαν από αυτούς £114,000. Τις μεγαλύτερες απόλυες τις είχε ένα ζευγάρι από το οποίο εκλάπησαν £158,700. Πολλοί από τους απατεώνες ομολόγησαν την πράξη τους.

Ένας από αυτούς ήταν ο Olawasegun Adekunle, 27 ετών, που συνελήφθη φορώντας ένα ρολόι αξίας £18,500. Ακόμα στο σπίτι του βρέθηκε ένα άλλο ρολόι αξίας £37,500 καθώς και ένας αυτοκίνητο αξίας £87,000. Ακόμα, οι αστυνομικοί βρήκαν ένα πανάκριβο ήχο-σύστημα καθώς και στοιχεία για πτήσεις 1ης θέσεις σε όλο τον κόσμο.

[17] http://www.thisismoney.co.uk/news/article.html?in_article_id=417505&in_page_id=2

Ένας άλλος συνεργός της συμμορίας, ήταν ο Steven Fabian, 44 ετών, θείος του Adekunle, ο οποίος προδόθηκε από τον ανιψιό του. Ο Fabian κατηγορήθηκε για συνομωσία, για ξέπλυμα χρήματος και αφέθηκε ελεύθερος με εγγύηση, αφού ο ρόλος του ήταν απλά να μεταφέρει το αυτοκίνητο του Adekunle στη Νιγηρία.

Τρία ακόμη άτομα συνελήφθησαν: ο Emmanuel Imbrah, ο Ayodeji Osibogun και ο Dominic Almond.

4.3.3 Κλοπή οικονομικών στοιχείων

Υπάρχουν δύο βασικές περιπτώσεις της κλοπής οικονομικών στοιχείων, οι οποίες αναφέρονται και παρακάτω:

1η κατηγορία: ***Πρόσβαση σε υπάρχοντα λογαριασμό του θύματος.***

Στη περίπτωση αυτή ο επιτιθέμενος παριστάνει το θύμα ώστε να έχει πρόσβαση σε ένα νόμιμο τραπεζικό λογαριασμό. Αυτό επιτυγχάνεται με τη κλοπή ενός ή περισσότερων οικονομικών στοιχείων και χρήση τους σε διάφορες τραπεζικές συναλλαγές.

Οι απάτες αυτές αφορούν κυρίως συναλλαγές σε ATM, σε χρεωστικές και πιστωτικές, όπου ο ετήσιος τζίρος στην Ελλάδα ξεπερνά τα 12,5 δισ. Ευρώ[18]. Σύμφωνα με στοιχεία τραπεζών, το 0,035% του τζίρου με πιστωτικές κάρτες είναι προϊόν απάτης.

Με δεδομένο ότι ο τζίρος μέσω πιστωτικών καρτών στην Ελλάδα ανέρχεται σε 10 δισ. ευρώ, τότε το κόστος της απάτης υπολογίζεται σε περίπου 3,5 εκατ. ευρώ. Σημειώνεται ότι από τα 10 δισ. ευρώ, τα 3,5 δισ. ευρώ αφορούν αναλήψεις μετρητών από πιστωτική κάρτα.

Όμως, η ηλεκτρονική απάτη δεν περιορίζεται μόνο στις κάρτες. Εκτιμάται ότι το 0,5-1% όσων κάνουν χρήση ηλεκτρονικών μεθόδων στις συναλλαγές πέφτουν θύματα. Αυτό μεταφράζεται σε περίπου 1.300 - 2.500 Έλληνες ετησίως.

2η κατηγορία: ***Ο επιτιθέμενος δημιουργεί νέους τραπεζικούς λογαριασμούς χρησιμοποιώντας την ταυτότητα του θύματος***.

Ο σκοπός είναι να χρησιμοποιήσει ο επιτιθέμενος την καλή πιστοληπτική ικανότητα του θύματος για να αποκτήσει χρήματα υπό την μορφή πιστωτικών καρτών και δανείων.

Κλασικό παράδειγμα είναι *η απόκτηση δανείου* από ένα απατεώνα. Ο απατεώνας προσποιείται ότι είναι το θύμα παρουσιάζοντας έγκυρο όνομα, διεύθυνση, ημερομηνία γέννησης κοκ. Τα στοιχεία αυτά ακόμα και αν διασταυρωθούν από την τράπεζα θα φανεί ότι είναι σωστά και το δάνειο θα εκδοθεί χωρίς πρόβλημα.

[18] http://www.hotstation.gr/article-print-1702.html

Η τράπεζα δεν μπορεί να εντοπίσει εύκολα ότι ο δανειζόμενος είναι απατεώνας ειδικά αν δεν παρουσιάσει έγκυρο δελτίο ταυτότητας. Αυτό συμβαίνει στις περιπτώσεις των συναλλαγών μέσω διαδικτύου, τηλεφώνου ή φαξ. Τελικά, ο επιτιθέμενος κρατάει τα χρήματα, η τράπεζα δεν πληρώνεται και το θύμα κατηγορείται ότι δεν εξοφλεί ένα δάνειο που στην πραγματικότητα δεν έχει λάβει.

Υπάρχει περίπτωση ο επιτιθέμενος να συνεχίσει να κάνει συναλλαγές εις βάρος του θύματος χωρίς το θύμα να έχει καταλάβει κάτι. Φυσικά, με τις πράξεις αυτές του απατεώνα, η πιστοληπτική ικανότητα του θύματος μειώνεται.

Ακόμη, υπάρχει περίπτωση το θύμα να κάνει αίτηση για δάνειο ή πιστωτική κάρτα και να απορριφθεί γιατί φαίνεται ότι δεν είναι φερέγγυος. Αν το θύμα δεν εντοπίσει την απάτη και το περιστατικό αυτό δε χρίσει νομικής αντιμετώπισης μπορεί να αντιμετωπίσει στο μέλλον παρόμοια ή μεγαλύτερα προβλήματα.

4.3.4 Ύποπτες εμπορικές σελίδες

Το ηλεκτρονικό εμπόριο διευκολύνει καθημερινά εκατομμύρια ανθρώπους και επιχειρήσεις. Είναι όμως βασικό η πρόσβαση σε εμπορικές ιστοσελίδες να γίνεται με ιδιαίτερη προσοχή και με τη σιγουριά ότι αυτές λαμβάνουν υπόψη τους την επικείμενη νομοθεσία και παρέχουν την υποχρεωτική ασφάλεια συναλλαγών και προσωπικών δεδομένων.

Δυστυχώς όμως υπάρχει μια ανησυχητική αύξηση ύποπτων εμπορικών ιστοχώρων που ζητούν την αποστολή προσωπικών δεδομένων και πληρωμή μέσω πιστωτικής κάρτας. Σε πολλές από τις περιπτώσεις αυτές, τα αγαθά που έχουν αγοραστεί ουδέποτε φθάνουν στα χέρια σας, σε κάποιες άλλες ακόμα τα προσωπικά δεδομένα σας και πολύ χειρότερα η πιστωτική σας κάρτα χρησιμοποιείται από τρίτους χωρίς την δική σας γνώση και συναίνεση. Συνήθως αυτές οι ιστοσελίδες προέρχονται από τις λιγότερο ανεπτυγμένες χώρες, στις οποίες δεν υπάρχει η πρέπουσα νομοθεσία.

Ένα ιστοχώρος μπορεί να δημοσιευθεί στο Διαδίκτυο από οποιαδήποτε χώρα και μέσω οποιουδήποτε Παροχέα Υπηρεσιών Διαδικτύου (Internet Service Provider). Στους εμπορικούς ιστοχώρους συνήθως δίνεται ελεγχόμενη πρόσβαση μέσω κωδικών. Πολλές φορές συνδρομητικοί ιστοχώροι λειτουργούν σε βάση τέτοιων κωδικών που παρέχουν πρόσβαση σε συγκεκριμένες υπηρεσίες (ανάλογα της συνδρομής) στον ιστοχώρο και για ορισμένο χρονικό διάστημα.

Υπάρχουν και οι δημόσιοι εμπορικοί ιστοχώροι, όπου μέσω ασφαλούς ηλεκτρονικής συναλλαγής (secure electronic transaction) ο οποιοσδήποτε μπορεί να ολοκληρώσει από οπουδήποτε και σε οποιαδήποτε στιγμή μια εμπορική συναλλαγή.

Είναι πολύ βασικό, όταν γίνεται μια τέτοια συναλλαγή να δίνεται προσοχή στην ηλεκτρονική διεύθυνση η οποία ξεκινά με «https://» και όχι με «http://». Έτσι θα είναι γνωστό εάν το πρωτόκολλο που χρησιμοποιείται από τον ιστοχώρο παρέχει ασφαλή συναλλαγή ή όχι.

Οι ύποπτοι εμπορικοί ιστοχώροι συνήθως δεν βρίσκονται σε μια τέτοια διεύθυνση και πουθενά στον ιστοχώρο τους δεν βρίσκονται πληροφορίες σχετικά με τον τρόπο ασφαλούς συναλλαγής. Τέτοιοι ιστοχώροι μπορούν να ασχολούνται με πώληση αγαθών, με ηλεκτρονικό τζόγο, ή ακόμα και με πορνογραφία.

Επίσης, εάν ακόμα υπάρχει πρόσβαση στο Διαδίκτυο μέσω τηλεφωνικής σύνδεσης, (dial-up), σε τέτοιες ιστοσελίδες μπορεί να διακοπεί η σύνδεση με τον οικείο παροχέα υπηρεσιών διαδικτύου για κάποια δευτερόλεπτα και να επανέλθει αυτή τη φορά ως σύνδεση από κάποιο «εξωτικό» μέρος (συνήθως κλήση σε κάποιον αριθμό αντίστοιχου του γνωστού «090» στο εξωτερικό από το σταθερό τηλέφωνο του κατόχου), στο οποίο στον επόμενο λογαριασμό ο κάτοχος θα πληρώσει αστρονομικά ποσά σύνδεσης.

Πιθανά προβλήματα

Μη αξιόπιστες ιστοσελίδες ενδέχεται:

- να μην εκτελούν τις υποχρεώσεις τους προς τους πελάτες τους, π.χ. μπορεί να μην παραδώσουν προϊόντα που έχουν αγοραστεί.
- να κάνουν κακή χρήση των προσωπικών δεδομένων που καταχωρούνται σε αυτές.
- να κάνουν κακή χρήση των πληροφοριών πληρωμής (στοιχεία πιστωτικής κάρτας).

Τέτοιοι εμπορικοί ιστοχώροι μπορεί ακόμη να προσφέρουν ανεπιθύμητες ή παράνομες υπηρεσίες σε παιδιά (τζόγος, πορνογραφικό υλικό κ.α.) Συνήθως, οι ιστοσελίδες αυτές προέρχονται από χώρες όπου δεν υπάρχει το κατάλληλο νομοθετικό πλαίσιο που να απαγορεύει τέτοιου είδους δραστηριότητες.

Σύμφωνα με στοιχεία που δημοσιεύθηκαν στον Ελληνικό Τύπο[19]:

- Κάθε λεπτό διακινούνται μέσω πληροφοριακών δικτύων και συστημάτων 3,5 δισεκατομμύρια ευρώ. Το αντίστοιχο ποσό στην Ελλάδα φτάνει τα 150 εκατομμύρια ευρώ.
- Η Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος της ΕΛ.ΑΣ. δέχεται καθημερινά γύρω στις 15 καταγγελίες.
- Υπολογίζεται πως 2.500 Έλληνες έχουν πέσει θύματα ηλεκτρονικής απάτης.
- 4.000.000 ευρώ χάνονται κάθε χρόνο από κλοπή στοιχείων που αφορούν πιστωτικές και χρεωστικές κάρτες στην Ελλάδα.

19 http://www.saferinternet.gr/%CE%98%CE%AD%CE%BC%CE%B1%CF%84%CE%B1/%CE%95%CE%95%CF%80%CE%B9%CF%87%CE%B5%CE%B9%CF%81%CE%B5%CE%AF%CE%BD/%CE%8E%CF%80%CE%BF%CF%80%CF%84%CE%B5%CF%82%CE%B5%CE%BC%CF%80%CE%BF%CF%81%CE%B9%CE%BA%CE%AD%CF%82%CF%83%CE%B5%CE%BB%CE%AF%CE%B4%CE%B5%CF%82/tabid/58/Default.aspx

4.3.5 Phishing[20]

Τα τελευταία χρόνια πολλοί εγκληματίες βρίσκουν πρόσφορο έδαφος στο Διαδίκτυο, για να πραγματοποιήσουν κλοπή ταυτότητας προσωπικών στοιχείων. Πολλοί χρήστες του Διαδικτύου ανταποκρίνονται σε παραπλανητικά e-mail από υποτιθέμενες εταιρείες, που τους ζητούν προσωπικά στοιχεία για να τους προσφέρουν κάποια υπηρεσία ή κάποιο όφελος.

Για παράδειγμα, μπορεί οι απατεώνες να στείλουν σε κάποιον ένα e-mail και να εμφανίζονται ως η τράπεζα με την οποία συναλλάσσεται. Στο e-mail αυτό, μπορεί να του ζητούν προσωπικά στοιχεία δήθεν για να τα επιβεβαιώσουν. Αν το υποψήφιο θύμα πειστεί, το πιθανότερο είναι να αποκαλύψει τα στοιχεία που του ζητά ο απατεώνας. Αυτό ονομάζεται ***phishing***.

4.3.5.1 Τεχνικές του phishing

Το phishing βασίζεται στην έμφυτη αντίδραση των ανθρώπων απέναντι σε γεγονότα που φαίνονται σημαντικά. Μηνύματα ηλεκτρονικού ταχυδρομείου που είναι γραμμένα με συγκεκριμένο τρόπο, μπορούν να προκαλέσουν άγχος και να κάνουν κάποιον που θα τα διαβάσει, να ανταποκριθεί σε αυτό που του ζητούν να κάνει.

Παρακάτω ακολουθούν μερικές τεχνικές που χρησιμοποιούνται από τους phishers[21]:

- **Εξαπάτηση με ψεύτικα links:** Οι πιο πολλές μέθοδοι του phishing χρησιμοποιούν μία μορφή τεχνικής, ώστε να εμφανίζουν το link που υπάρχει σε ένα e-mail (καθώς και τη σελίδα στην οποία οδηγεί), σαν να είναι αυθεντικά και να ανήκουν στον οργανισμό τον οποίο οι απατεώνες παριστάνουν.

- **Εξαπάτηση των φίλτρων:** Πολλές φορές οι απατεώνες χρησιμοποιούν εικόνες αντί για κείμενο για να ξεγελάσουν τα φίλτρα προστασίας, τα οποία εντοπίζουν λέξεις που χρησιμοποιούνται συχνά σε παραπλανητικά e-mails. Άλλος τρόπος που χρησιμοποιούν οι επιτήδειοι για να ξεγελάσουν τα φίλτρα που σκανάρουν τις ιστοσελίδες, είναι η χρήση του Flash και η απόκρυψη του κειμένου σε ένα αντικείμενο πολυμέσων (multimedia object).

- **Πλαστογράφηση Website:** Όταν το θύμα επισκεφθεί το πλαστό site, η απάτη δεν τελειώνει εκεί. Οι απατεώνες χρησιμοποιούν εντολές JavaScript, για να αλλάξουν την γραμμή διεύθυνσης. Αυτό γίνεται είτε τοποθετώντας μια εικόνα με ένα έγκυρο URL πάνω από τη γραμμή διεύθυνσης, είτε κλείνοντας την γραμμή διεύθυνσης και ανοίγοντας μία καινούργια με έγκυρο URL.

  Μια άλλη τεχνική που χρησιμοποιείται επιτυχώς, είναι η προώθηση του πελάτη στα γνήσια site των οργανισμών και στη συνέχεια η χρήση ενός αναδυόμενου παραθύρου που ζητάει ευαίσθητα δεδομένα και φαίνεται πως ανήκει στον οργανισμό.

---

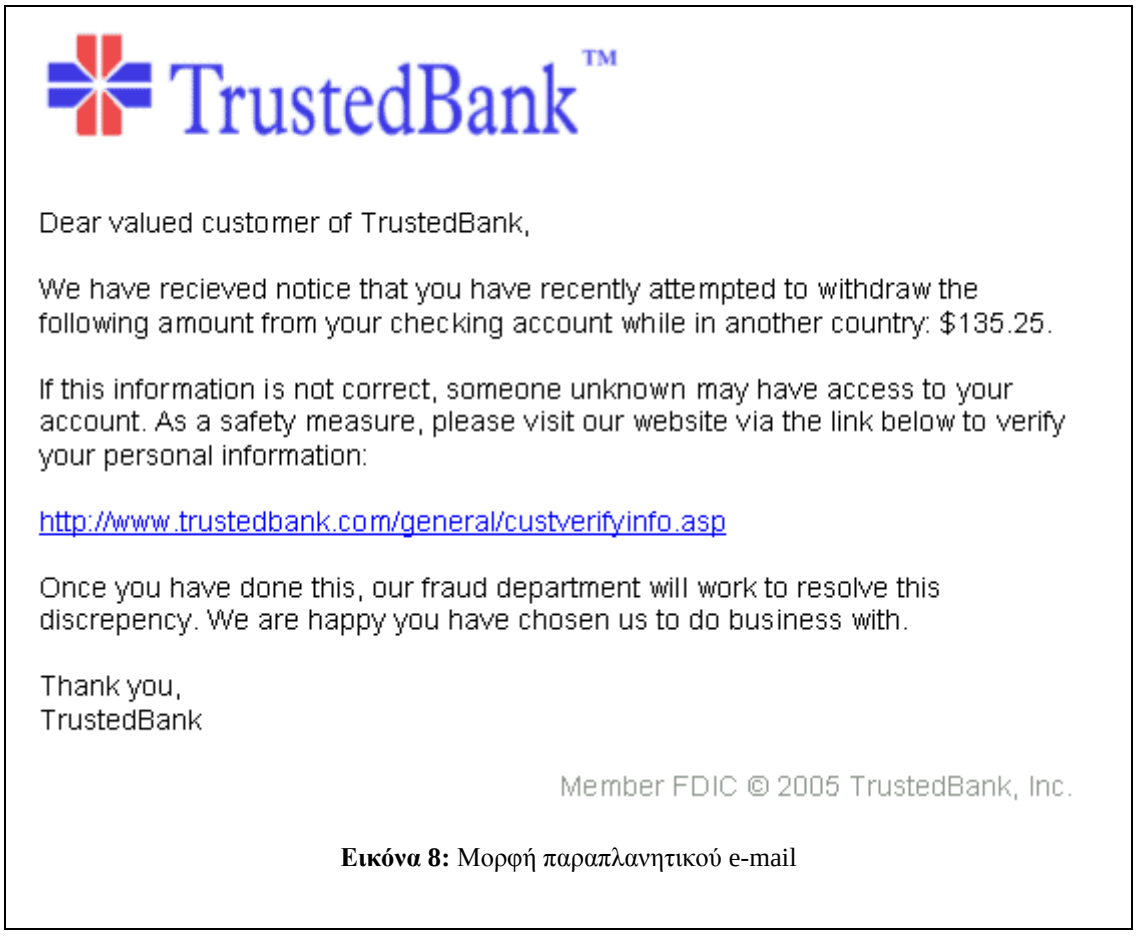
[20] http://en.wikipedia.org/wiki/Phishing
[21] http://en.wikipedia.org/wiki/Phishing#Social_engineering

- **Phishing μέσω τηλεφώνου:** Δεν είναι απαραίτητο όμως οι επιθέσεις phishing να γίνονται με τη χρήση πλαστής ιστοσελίδας. Τα μηνύματα που στέλνονται σε χρήστες, μπορεί να μην περιέχουν κάποιο link αλλά κάποιον αριθμό που πρέπει να καλέσει ο χρήστης. Ο αριθμός αυτός (που ανήκει στους απατεώνες και παρέχεται από μία υπηρεσία Voice over IP), όταν κληθεί ζητάει από τους χρήστες να εισάγουν προσωπικά δεδομένα.

  Καμιά φορά οι phishers χρησιμοποιούν ψευδή στοιχεία καλούντος για να φαίνεται ότι προέρχονται από ένα έμπιστο οργανισμό. Η τεχνική αυτή ονομάζεται και Vishing (voice phishing).

Ένα παράδειγμα παραπλανητικού e-mail φαίνεται στην ***Εικόνα 8: Μορφή παραπλανητικού e-mail***. Η τράπεζα που παρουσιάζεται στο e-mail αυτό είναι φανταστική, αλλά στην πραγματικότητα οι απατεώνες θα ισχυριζόταν ότι εκπροσωπούν μια πραγματική τράπεζα με την οποία συναλλάσσεται το υποψήφιο θύμα.

Όπως βλέπουμε, γίνεται μια προσπάθεια να παρουσιαστεί όσο πιο πιστικό γίνεται φέροντας το λογότυπο της τράπεζας, καθώς και ένα link σε ένα site που ο πελάτης φαίνεται ότι το έχει επισκεφθεί πολλές φορές.



Εικόνα 8: Μορφή παραπλανητικού e-mail

Παράδειγμα: Ένα παράδειγμα σχετικό με phishing, αποτελεί το ***Monster Worldwide***[22], ένα site για εύρεση εργασίας, το οποίο έπεσε θύμα χάκερ εκθέτοντας τα προσωπικά στοιχεία χιλιάδων υποψηφίων που είχαν υποβάλει βιογραφικό στις βάσεις δεδομένων του. Οι χάκερ κατάφεραν να διεισδύσουν στη βάση δεδομένων του δικτύου και να αποκτήσουν πρόσβαση στα προσωπικά δεδομένα χιλιάδων χρηστών.

Τα στοιχεία σύνδεσης καθώς και τα e-mail, τα πλήρη ονόματα, τηλεφωνικοί αριθμοί και μερικά βασικά δημογραφικά στοιχεία βρίσκονται στα χέρια κακόβουλων χρηστών. Η εταιρεία προειδοποιεί ότι οι hackers ενδέχεται να χρησιμοποιήσουν τα e-mail των χρηστών για να αποσπάσουν από τους ίδιους περισσότερες πληροφορίες σχετικά με τις πιστωτικές κάρτες κλπ.

Γενικά, όταν ο επιτιθέμενος έχει συγκεντρώσει αρκετά στοιχεία για κάποιο άτομο, μπορεί να χρησιμοποιήσει την ταυτότητά του για να πραγματοποιήσει πληθώρα εγκλημάτων. Παραδείγματα αποτελούν: *η αίτηση για δάνειο* ή *πιστωτική κάρτα, ανάληψη χρημάτων από το λογαριασμό του θύματος* και γενικά *η απόκτηση αγαθών σε βάρος του θύματος*.

4.3.6 Κλωνοποίηση ταυτότητας

Αυτή είναι από τις χειρότερες περιπτώσεις κλοπής ταυτότητας. Στην περίπτωση, λοιπόν, αυτή ο απατεώνας αποκτά τα προσωπικά στοιχεία κάποιου ή κάποιων και στη συνέχεια παριστάνει κάποιον άλλο για να κρυφτεί από τις αρχές.

Αυτό μπορεί να γίνει από κάποιον που θέλει να αποφύγει τη σύλληψη για ένα έγκλημα που έχει διαπράξει, από κάποιον που δουλεύει παράνομα σε ξένη χώρα ή από κάποιον που κρύβεται από τους πιστωτές του ή από κάποια άλλη απειλή. Μπορεί ακόμη ο απατεώνας να αποκτήσει έγγραφα ή δελτίο ταυτότητας για να γίνεται πιο πειστικός.

Παράδειγμα: Ένα χαρακτηριστικό περιστατικό που συνέβη στην Αμερική με θύμα μια εικοσιτετράχρονη γυναίκα[23], μας δείχνει την σοβαρότητα αυτού του τύπου κλοπής. Από την γυναίκα αυτή, εκλάπη η τσάντα την ώρα που γευμάτιζε σε ένα εστιατόριο.

Μετά από λίγο καιρό, η τσάντα της παραδόθηκε στην αστυνομία από μία γυναίκα. Η ταυτότητα και πιστωτική κάρτα καθώς και όλα τα υπόλοιπα αντικείμενα της κοπέλας βρισκόταν μέσα και μόνο τα χρήματα έλλειπαν.

Έπειτα από λίγες μέρες, η κοπέλα ξεκίνησε να λαμβάνει λογαριασμούς για πράγματα που δεν είχε αγοράσει και παρατήρησε ότι της έλλειπαν χρήματα από το λογαριασμό της τράπεζας. Επικοινωνώντας με τις εταιρείες στις οποίες φαινόταν ότι χρεωστάει, έμαθε έκπληκτη ότι τα τηλεφωνήματα είχαν γίνει από το σπίτι της και τα αντικείμενα είχαν σταλεί στην δική της διεύθυνση, χωρίς αυτή να έχει λάβει τίποτα.

[22] http://new.e-go.gr/tech/article.asp?catid=6424&subid=2&tag=4885&pubid=1693751
[23] http://www.myidfix.com/identity-theft-stories3.php

Προστασία από κλοπή προσωπικών στοιχείων

Μία μέρα που επέστρεψε νωρίτερα από την δουλειά λόγω αδιαθεσίας, είδε ένα van μεταφορικής εταιρείας έξω από το σπίτι της. Πλησιάζοντας διακριτικά είδε μία γυναίκα να στέκεται στην πόρτα της.

Η γυναίκα αυτή είχε μια καταπληκτική ομοιότητα με την κοπέλα, αφού χρησιμοποιούσε το ίδιο μακιγιάζ, είχε την ίδια κόμμωση και φορούσε τα ίδια γυαλιά. Επίσης, είχε το ίδιο αυτοκίνητο με τις ίδιες πινακίδες, ακόμα και με τα ίδια λούτρινα κουκλάκια στο πίσω τζάμι. Όταν η απατεώνισσα αντιλήφθηκε την κοπέλα, μπήκε στο αυτοκίνητο και έφυγε με ταχύτητα.

Φυσικά η κοπέλα κατήγγειλε το περιστατικό στην αστυνομία, η οποία με τη σειρά της ανέκρινε τους γείτονες. Σύμφωνα με τις μαρτυρίες των γειτόνων, η απατεώνισσα πήγαινε κάθε μέρα με το αυτοκίνητο στο σπίτι της κοπέλας, έπαιρνε την αλληλογραφία, έμπαινε μέσα στο σπίτι και για να μην αποκαλυφθεί έβγαζε βόλτα και το σκύλο.

Οι γείτονες λόγω της εξαιρετικής μεταμφίεσης νόμιζαν ότι έβλεπαν την γειτόνισσα τους. Όποτε, λοιπόν, η κοπέλα έλλειπε η απατεώνισσα έμπαινε στο σπίτι της και έκανε διάφορες τηλεφωνικές παραγγελίες και έκανε παραλαβές των αντικειμένων που είχε αγοράσει σε βάρος της κοπέλας. Μετά από λίγο καιρό η αστυνομία συνέλαβε την απατεώνισσα ενώ προσπαθούσε να κάνει ανάληψη χρημάτων από το λογαριασμό της κοπέλας.

Τελικά, αποδείχτηκε ότι η απατεώνισσα ήταν η γυναίκα που είχε παραδώσει την τσάντα στην αστυνομία. Είχε αντιγράψει τα κλειδιά της κοπέλας, είχε μία πλαστή ταυτότητα εργασίας καθώς και το ημερολόγιο της κοπέλας. Ομολόγησε ότι παρακολουθούσε την κοπέλα για μερικούς μήνες για να μάθει τις συνήθειές της και να μπορέσει να την αντιγράψει.

4.3.7 Κίνδυνοι κατά την υποσχόμενη παροχή υπηρεσιών

Σε πολλές περιπτώσεις στο διαδίκτυο εταιρίες ή άτομα φέρονται να προσφέρουν υπηρεσίες στους χρήστες -καταναλωτές, οι οποίοι, όμως, αφού πληρώσουν για αυτές τις υπηρεσίες δεν τις λαμβάνουν ποτέ.

Κλασικές περιπτώσεις τέτοιας μορφής εξαπάτησης είναι οι παρακάτω:

- Προκαταβολή εξόδων δανείου
- Απάτες με φιλανθρωπικές προσφορές
- Επαναφορά πιστοληπτικής ικανότητας

Παράδειγμα: *Ισπανικό Λόττο*[24]

Τα εγκλήματα που τελούνται μέσω του διαδικτύου θεωρούνται ως ιδιαίτερα έξυπνα και δύσκολα στη δίωξή τους. Ιδιαίτερα οι λεγόμενες «απάτες» που τελούνται μέσω του διαδικτύου φημίζονται για τον ιδιαίτερα ευφυή τρόπο με τον οποίο διεξάγονται.

Ένα χαρακτηριστικό παράδειγμα είναι οι απάτες του τύπου «*ισπανικό λόττο*». Στην απάτη τύπου «ισπανικό λόττο», ο ανυποψίαστος χρήστης του διαδικτύου βλέπει ένα μήνυμα στο ηλεκτρονικό του ταχυδρομείο, το οποίο τον ενημερώνει ότι είχε κερδίσει ένα υπέρογκο ποσό στο λόττο μίας άλλης χώρας (συνήθως της Ισπανίας, γι' αυτό και η ονομασία «ισπανικό λόττο») και του ζητείται να συμπληρώσει μία φόρμα με τα προσωπικά του στοιχεία, προκειμένου να του κατατεθούν τα χρήματα.

Μόλις όμως εκείνος συμπλήρωνε τη φόρμα και την έστελνε μέσω ηλεκτρονικού ταχυδρομείου, οι δράστες του ζητούσαν να τους αποστείλει ένα ποσό της τάξης των 2.000 Ευρώ ή και παραπάνω, προκειμένου να καλυφθούν τα έξοδα αποστολής, ανοίγματος λογαριασμού κ.λπ. Ο ανυποψίαστος χρήστης «έστελνε» φυσικά τα χρήματα, αλλά ποτέ δεν παραλάμβανε το υπέρογκο χρηματικό ποσό.

Παράδειγμα: *Γράμμα από τη Νιγηρία*

Αξιωματούχοι από τη Νιγηρία θέλουν τη βοήθεια μας για να βγάλουν χρήματα από τη χώρα, με αντάλλαγμα ποσοστό των χρημάτων αυτών. Ζητούν τον τραπεζικό μας λογαριασμό, που, αφού τους τον δώσουμε, τον αδειάζουν[25].

Σχετικά πρόσφατα στις 02/06/2005 χρησιμοποιήθηκε μία παραλλαγή της τεχνικής αυτής, για να εξαπατηθεί το διεθνές γραφείο εξαγωγών.

Οι απατεώνες, στην περίπτωση αυτή που ήταν αναμφίβολα Νιγηριανοί, έστειλαν ένα e-mail παριστάνοντας μια Κινέζικη εταιρεία εξαγωγών.

Το e-mail παρατίθεται αυτούσιο αμέσως παρακάτω:

---

24 http://www.securitymanager.gr/it_security/contents_article.php?id=21&category=REFERENCE&month=%CE%A3%CE%95%CE%A0%CE%A4%CE%95%CE%9C%CE%92%CE%A1%CE%99%CE%9F%CE%A3-%CE%9F%CE%9A%CE%A4%CE%A9%CE%92%CE%A1%CE%99%CE%9F%CE%A3&year=2008&issue=6

25 http://www.exportbureau.com/fraud_report.html?story=21&news=fake_job_offers_from_nigeria

---

> THEIR EMAIL ADDRESS: metallurgical_chem_company@yahoo.com
> Company Name: china metallurgical company
> Contact Person: mr woo fang
> Contact Phone No: 23456976
> Country: China
> Company Type: Distributor,
>
> I am Mr. Woo Fang, Vice President of China
> metallurgical import and export company.
>
> We are a group of business men who deal on Raw
> Materials and My company was established in 2001 we
> export raw materials such as non-metallic minerals
> such as Calcite, Barytes, Manganese Dioxide, Dolomite
> Mica China Clay, Manganese Dioxide, Ferrous (Irona)
> Oxide.
>
> The various industries we cater to are Paints, Rubber,
> and Plastics, Construction chemicals. My sales vary
> from different sizes and we export them into Canada,
> Europe and America.
>
> We are searching for representatives who can help us
> establish a medium of getting to our costumers in
> Canada, Europe and America as well as making payments
> through you to us and earn 10% of every payment made
> through you to us.
>
> Subject to your satisfaction you will be given the
> opportunity to negotiate your mode of which we will
> pay for your services as our representative.

> If you are interested, please fill inn the blank
> spaces below:
> 1.Your Full
> Names.....
> 2.Your Full Contact
> Address.....
> 3.State/Country.....
> 4.Your Phone/Fax
> Numbers.....
> I await your prompt response.
> Yours faithfully,
> Mr. Woo Fang.

4.3.8 Κλοπή αλληλογραφίας[26]

Οι απατεώνες που χρησιμοποιούν αυτή τη μέθοδο κλοπής, συνήθως κυνηγούν απλά ευκαιρίες χωρίς να ανήκουν σε κάποια συγκεκριμένη κατηγορία ή ομάδα. Αυτή είναι μια επικίνδυνη μορφή κλοπής γιατί οι απατεώνες συνήθως δεν είναι οργανωμένοι απλά αρπάζουν όποια ευκαιρία τους δοθεί για να αποκτήσουν τα προσωπικά στοιχεία άλλων.

Υπάρχουν βέβαια και μικρές οργανωμένες συμμορίες που μελετούν τις διαδρομές των ταχυδρομικών υπαλλήλων, ώστε να χτυπήσουν πολλά κουτιά αλληλογραφίας ταυτόχρονα σε μια στιγμή που είναι ασφαλείς.

Σε πιο ακραίες περιπτώσεις και αν η αλληλογραφία βρίσκεται σε ένα ασφαλές κουτί, οι απατεώνες ξεριζώνουν όλο το κουτί από τη βάση του, δένοντας το στο πίσω μέρος ενός αυτοκινήτου και τραβώντας το.

Σε μερικές περιπτώσεις στην Καλιφόρνια, οι κλέφτες μεταμφιέζονταν ως ταχυδρομικοί υπάλληλοι για να έχουν πρόσβαση στην αλληλογραφία. Στο Oakland, πολλοί κάτοικοι κατήγγειλαν ότι είδαν ένα λευκό Jeep που έμοιαζε με ταχυδρομικό όχημα να πλησιάζει τα κουτιά αλληλογραφίας στις γειτονιές. Αυτό που τους κίνησε τις υποψίες ήταν το γεγονός ότι το Jeep πλησίαζε αμέσως μετά την παράδοση της αλληλογραφίας.

Μία πιο σπάνια περίπτωση είναι η ληστεία ταχυδρομικών οχημάτων που μπορεί να αποφέρει στοιχεία για χιλιάδες ταυτότητες. Άλλες δύο περιπτώσεις που συμβαίνουν αρκετά συχνά είναι η κλοπή αλληλογραφίας από τους γείτονες καθώς και η υπεξαίρεση αλληλογραφίας ή χαρτοφυλάκων που περιέχουν πλήθος πολύτιμων πληροφοριών και ανήκουν σε (μεγάλες) επιχειρήσεις.

4.3.9 Αναζήτηση στοιχείων από τα σκουπίδια

Ένας τρόπος κλοπής είναι η αναζήτηση στοιχείων από τα σκουπίδια που πετάει το θύμα. Δηλαδή, ο επιτιθέμενος ψάχνει τα σκουπίδια για να βρει πεταμένες τραπεζικές αποδείξεις ή τραπεζικά έγγραφα που φυσικά φέρουν τα προσωπικά στοιχεία του κατόχου τους.

Παράδειγμα: Αν κάποιος λάβει μία προ-εγκεκριμένη πιστωτική κάρτα και την πετάξει χωρίς να καταστρέψει τα περιεχόμενα έγγραφα μπορεί κάποιος απατεώνας να την ανακτήσει και να την χρησιμοποιήσει χωρίς να το γνωρίζει και ο νόμιμος κάτοχος.

Περιστατικά[27] που αξίζει να σημειωθούν είναι τα παρακάτω:

- Την **δεκαετία του '60** ο Jerry Schneider ανέκτησε από τα σκουπίδια, βιβλία οδηγιών από την εταιρεία The Pacific Telephone & Telegraph Company. Χρησιμοποιώντας τα, εκμεταλλεύτηκε την εταιρεία για πολλά χρόνια και έκανε ζημιές χιλιάδων δολαρίων μέχρι την σύλληψή του.

[26] http://www.privacymatters.com/identity-theft-information/mail-theft.aspx
[27] http://en.wikipedia.org/wiki/Dumpster_diving

- Ο οργανισμός Food Not Bombs **(*βλ. εικ. 9*)** ξεκίνησε τη δράση του την **δεκαετία του ’80** και είναι ένας οργανισμός κατά της πείνας, που συγκεντρώνει φαγητά από τα σκουπίδια σε λαχαναγορές στην Αμερική και Ηνωμένο Βασίλειο.

Εικόνα 9: Τα μέλη του Food Not Bombs εν δράσει

- **6 Δεκεμβρίου 1983** - Juarez Mexico, ένας ντόπιος έκλεψε από τα σκουπίδια μία πεταμένη συσκευή ακτινοθεραπείας η οποία περιείχε το ραδιοϊσότοπο κοβάλτιο. Στη συνέχεια, εξαιτίας της συσκευής αυτής, μολύνθηκαν 5000 μετρικοί τόνοι ατσάλι, μέρος του οποίου εξήχθη στις Η.Π.Α.

- **13 Σεπτεμβρίου 1987** – Στην κεντρική Βραζιλία κάποιοι έκλεψαν μια συσκευή ακτινοθεραπείας που περιείχε το caesium-137 και το πούλησαν στους αδαείς σαν διακοσμητικό (το στοιχείο αυτό λάμπει). 400 άνθρωποι μολύνθηκαν και 4 πέθαναν.

- Ο Charles Manson έγραψε εν έτι **1987**, ένα τραγούδι που λεγόταν "Garbage Dump" το οποίο είχε να κάνει με το φαινόμενο του dumpster diving.

- Το παιχνίδι Castle Infinity, που αρχικά κυκλοφόρησε το **1996**, μετά τη διακοπή του, επανήλθε στη “ζωή” αφού κάποιοι ανέκτησαν από τα σκουπίδια τους servers που το περιείχαν.

- **18 Μαρτίου 2000**, 55 αγαλματίδια των βραβείων Oscar, που είχαν κλαπεί, βρέθηκαν από τον Willie Fulgear στα σκουπίδια πίσω από ένα μανάβικο. Ο άνθρωπος αυτός έλαβε $50000 ως βραβείο και δύο εισιτήρια για τα Oscar. Τα χρήματα αυτά αργότερα εκλάπησαν από το χρηματοκιβώτιο του διαμερίσματος του.

- Το **2001**, το ψάξιμο στα σκουπίδια εμφανίστηκε στο βιβλίο *Evasion*.

Οι κλέφτες μπορεί να μην κλέψουν απαραίτητα προσωπικά έγγραφα αλλά αρχεία σε ηλεκτρονική μορφή ανακτώντας σκληρούς δίσκους από πεταμένους servers ή προσωπικούς υπολογιστές. Κρατικές υπηρεσίες, οργανισμοί και ιδιώτες φέρονται απερίσκεπτα και δεν καταστρέφουν τους παλιούς σκληρούς δίσκους τους.

Παράδειγμα:

Ένα πρόσφατο περιστατικό συνέβη στο Λονδίνο και αναφέρεται παρακάτω: Σε ένα σκληρό δίσκο που αγοράστηκε από το eBay εντοπίστηκαν δεδομένα για τη διαδικασία εκτόξευσης των πυραύλων εδάφους-αέρος του αμερικανικού αντιπυραυλικού συστήματος THAAD[28].

Στον ίδιο δίσκο βρέθηκαν πρωτόκολλα ασφάλειας, σχέδια των εγκαταστάσεων και πληροφορίες για υπαλλήλους της αεροδιαστημικής βιομηχανίας Lockheed Martin, εργολάβο του THAAD.

Η εταιρεία ανακοίνωσε ότι δεν είχε πληροφορίες για την απώλεια δεδομένων του προγράμματος THAAD.

Σε άλλο σκληρό δίσκο, ο οποίος προήλθε από συμβουλευτική εταιρεία με έδρα στις ΗΠΑ που είχε σχέσεις με κατασκευαστή οπλικών συστημάτων, οι ερευνητές εντόπισαν προτάσεις για μεταφορά συναλλάγματος μέσω Ισπανίας, ύψους 50 δισ. δολαρίων. Εντόπισαν επίσης αριθμούς λογαριασμών και λεπτομέρειες για εμπορικές συμφωνίες ανάμεσα σε εταιρείες των ΗΠΑ, της Βενεζουέλας, της Τυνησίας και της Νιγηρίας.

Ακόμα, παλιοί υπολογιστές από τη Σκοτία έκρυβαν δεδομένα από δύο δημόσια νοσοκομεία της Σκοτίας: ιστορικά ασθενών, ακτινογραφίες, πίνακες με τις βάρδιες του προσωπικού και εμπιστευτικές αλληλογραφίες.

Άλλος δίσκος από τη Γαλλία περιείχε καταγραφές του συστήματος ασφάλειας από πρεσβεία στο Παρίσι, ενώ ένας υπολογιστής που είχε πετάξει «μεγάλη ευρωπαϊκή τράπεζα» διατηρούσε αποθηκευμένες προσωπικές επιστολές.

Συνολικά οι ερευνητές εντόπισαν προσωπικά δεδομένα στο 34% των 300 σκληρών δίσκων που εξέτασαν.

4.3.10 Συνθετική κλοπή ταυτότητας

Η **συνθετική κλοπή ταυτότητας** είναι μία παραλλαγή της κλοπής ταυτότητας που έχει αρχίσει πρόσφατα να χρησιμοποιείται. Στη περίπτωση αυτή τα στοιχεία μίας πλαστής ταυτότητας μπορεί να είναι σύνθεση μίας ταυτότητας που κάθε στοιχείο της προέρχεται από μία διαφορετική γνήσια ταυτότητα.

Η πιο συνηθισμένη τεχνική είναι να συνδυαστεί ένας πραγματικός Αριθμός Αστυνομικής ταυτότητας με ένα όνομα και μία ημερομηνία γέννησης που ανήκουν σε άλλο άτομο.

[28] http://www.in.gr/news/article.asp?lngEntityID=1011508&lngDtrID=252

Η συνθετική κλοπή είναι πιο δύσκολο να εντοπιστεί γιατί δεν φαίνεται άμεσα στα στοιχεία που διατηρούν οι τράπεζες για τα θύματα. Ουσιαστικά, η κλοπή αυτή ζημιώνει τους πιστωτικούς οργανισμούς γιατί προσφέρουν πίστωση στους απατεώνες χωρίς να το γνωρίζουν. Και τα θύματα μπορεί να επηρεαστούν εάν για κάποιο λόγο το όνομά τους μπερδευτεί με τα στοιχεία μιας συνθετικής ταυτότητας.

Παράδειγμα: Χαρακτηριστική είναι η περίπτωση ενός κλέφτη ταυτότητας ονόματι James Rose, ο οποίος χρησιμοποιούσε συνθετικές ταυτότητες. Αυτές φαινόταν αληθινές στο χαρτί αλλά στην πραγματικότητα είχαν σκοπό να εξαπατήσουν τους πιστωτικούς οργανισμούς για να προχωρήσουν σε έκδοση δανείων ή πιστωτικών καρτών[29].

Ο κύριος Rose που είχε και συνεργό, κατάφερε να ξεγελάσει ολόκληρο το πιστωτικό σύστημα με αποτέλεσμα οι πλαστές του ταυτότητες να φαίνεται ότι ανήκουν σε πραγματικούς ανθρώπους με καλή πιστοληπτική ικανότητα. Σε διάστημα 2 ετών, χρησιμοποίησε 500 περίπου διαφορετικές πλαστές ταυτότητες και κατάφερε την έκδοση εκατοντάδων πιστωτικών καρτών αποκομίζοντας περίπου $750000.

Στο περιστατικό αυτό φαίνεται και ο πραγματικός χαρακτήρας της συνθετικής κλοπής ταυτότητας. Οι απατεώνες χρησιμοποιούν μεν μέρος των στοιχείων μερικών ανθρώπων για να εξαπατήσουν τους πιστωτικούς οργανισμούς αλλά συνήθως δεν έχουν σκοπό να βλάψουν τα θύματα της κλοπής. Σκοπός τους τις περισσότερες φορές είναι να βγάλουν πολλά χρήματα κάνοντας ζημιά μόνο στους πιστωτικούς οργανισμούς.

4.3.11 Συμμετοχή σε επενδυτικά σχέδια και παραπληροφόρηση της αγοράς

Οι απάτες αυτές σχετίζονται είτε με την παραπλάνηση και την προώθηση πλασματικών επενδυτικών σχεδίων είτε με προσπάθεια χειραγώγησης της χρηματιστηριακής αγοράς και της τιμής συγκεκριμένης μετοχής - μέσω της διασποράς πλαστών ειδήσεων. Αν κάτι φαίνεται πολύ καλό για να είναι αληθινό, συνήθως μόνο αληθινό δεν είναι.

Η απάτη αυτή εμφανίζεται με τις παρακάτω μορφές:

- **Πλασματικές επενδύσεις**: Οι πλασματικές επενδύσεις είναι μία πρακτική κατά την οποία οι επενδυτές αγοράζουν οι πωλούν μετοχές με βάση ψευδείς πληροφορίες και έχει σαν αποτέλεσμα απώλεια χρημάτων[30].

  Γενικά, ο τύπος αυτός απάτης, αποτελείται από κακόβουλες πρακτικές που έχουν σαν σκοπό να εξαπατήσουν τον επενδυτή για να επενδύσει τα χρήματά του σε μη υπάρχουσες μετοχές ή ομόλογα.

  Το παραπάνω φαινόμενο αποτελεί ξεκάθαρη κλοπή από τους επενδυτές και να επιφέρει λάθη στις οικονομικές αναφορές ανωνύμων εταιρειών.

[29] http://idsafeguards.blogspot.com/2007/10/synthetic-id-theft.html
[30] http://en.wikipedia.org/wiki/Investment_fraud

Παράδειγμα: Ένα πολύ πρόσφατο παράδειγμα πλασματικών επενδύσεων είναι αυτό του Bernie Madoff[31]. Ο **Bernard Lawrence "Bernie" Madoff (*βλ. εικ. 9*)** είναι ένα πρώην στέλεχος του χρηματιστηρίου NASDAQ, ο οποίος παραδέχτηκε ότι έστησε μία απάτη σε βάρος επενδυτών που του απέφερε δισεκατομμύρια δολάρια.

Εικόνα 9: Bernard Madoff

Στις 10 Δεκεμβρίου 2008, ο Madoff ενημέρωσε τους γιους του Mark και Andrew, ότι σκόπευε να δώσει πολλά εκατομμύρια δολάρια σε bonus δύο μήνες νωρίτερα από τότε που ήταν προγραμματισμένο. Οι γιοι του απαίτησαν να μάθουν πώς ήταν δυνατόν ο πατέρας τους να πληρώσει τόσα χρήματα σε bonus ενώ δεν είχε χρήματα να πληρώσει τους επενδυτές.

Ο Madoff αποκάλυψε στους γιους του την απάτη την οποία είχε στήσει. Αυτοί μέσω του δικηγόρου τους, πρόδωσαν τον πατέρα τους στις Αρχές.
Στις 11 Δεκεμβρίου συνελήφθη.

Στις 12 Μαρτίου 2009, ο Madoff βρέθηκε ένοχος για 11 αδικήματα που του είχαν αποφέρει $65000000000 σε βάρος των πελατών του. Παρά την έκταση της απάτης, ο Madoff ισχυρίστηκε πως ήταν μόνος του και δεν έδωσε ονόματα συνεργατών του.

- **Πυραμίδες:** Η απάτη πυραμίδας (Ponzi scheme), είναι μία επενδυτική απάτη, σύμφωνα με την οποία η ‘εταιρεία’ πληρώνει τους επενδυτές με τα δικά τους χρήματα ή με χρήματα άλλων επενδυτών και όχι από πραγματικά κέρδη.
  Για να δελεάσουν τους επενδυτές, οι απατεώνες εγγυώνται γρήγορα και μεγάλα κέρδη. Για να πετύχει το σχέδιο αυτό, χρειάζεται συνεχής και αυξανόμενη ροή χρημάτων από επενδυτές.

[31] http://en.wikipedia.org/wiki/Bernie_Madoff

Το σύστημα αυτό μοιραία καταρρέει, διότι τα κέρδη είναι πολύ μικρότερα από τις πληρωμές. Συνήθως, οι οργανωτές τέτοιου τύπου απάτης, συλλαμβάνονται πριν καταρρεύσει το σύστημά τους.

Η απάτη πυραμίδας, πήρε το όνομά της από τον Charles ponzi ***(βλ. εικ. 10)***, ένα ιταλό μετανάστη στην Αμερική. Αυτός δεν ανακάλυψε το Ponzi scheme, αλλά ήταν ο πρώτος που έγινε γνωστός για τα πολλά χρήματα που υπεξαίρεσε[32].

Εικόνα 10: Ο Charles ponzi κατά την προσαγωγή του (1910)

Παράδειγμα: Ένα πρόσφατο παράδειγμα απάτης πυραμίδας μας έρχεται από το Λονδίνο. Η βρετανική αστυνομία ανακοίνωσε ότι ένας trader από το Σίτυ του Λονδίνου, συνελήφθη για ξέπλυμα χρήματος, στο πλαίσιο έρευνας για επενδυτική απάτη ύψους 40 εκατομμυρίων ευρώ, γράφει την Παρασκευή ο βρετανικός τύπος[33].

Ο άντρας, ηλικίας 60 ετών, συνελήφθη στις 9 Φεβρουαρίου 2009 στο σπίτι του στο Έσσεξ, από αστυνομικούς που ερευνούσαν την υπόθεση της GFX Capital Markets Ltd, μίας χρηματιστηριακής εταιρείας, η οποία ανέστειλε πρόσφατα τις δραστηριότητές της.

Ο χρηματιστής είναι ύποπτος για "ξέπλυμα χρήματος" και αφέθηκε ελεύθερος υπό όρους, ανέφερε εκπρόσωπος της αστυνομίας του Σίτυ, ο οποίος αρνήθηκε να αποκαλύψει το εύρος της απάτης, περιοριζόμενος να πει ότι είναι ‘σημαντική’.

Σύμφωνα με την εφημερίδα *The Times*, η οποία δεν κατονομάζει τις πηγές της, πρόκειται για απάτη τύπου "πυραμίδας" ύψους 40 εκατομμυρίων λιρών (45 εκατομμυρίων ευρώ), τη μεγαλύτερη στη Μεγάλη Βρετανία από την αρχή της τρέχουσας οικονομικής κρίσης.

[32] http://en.wikipedia.org/wiki/Ponzi_scheme
[33] http://wallstfolly.typepad.com/wallstfolly/2009/02/uk-ponzi-scheme-gfx-capital-markets-ltd-director-terry-freeman-was-arrested-in-an-alleged-40-investm.html

Η αστυνομία του Σίτυ, η οποία δρα αποκλειστικά στην χρηματοοικονομική καρδιά του Λονδίνου και ειδικεύεται στη δίωξη του οικονομικού εγκλήματος, κάλεσε τους πελάτες-επενδυτές της GFX να επικοινωνήσουν μαζί της.

- **Χειραγώγηση μετοχών[34]:** Η χειραγώγηση μετοχών είναι μία πρακτική κατά την οποία οι ιδιοκτήτες μιας εμπορικής ή επενδυτικής εταιρείας παίρνουν μέτρα ώστε να αυξήσουν ή να μειώσουν την αξία των μετοχών τους, για να τις πωλήσουν ή να αγοράσουν επιπλέον κέρδος. Αυτή η πρακτική εκτός από παράνομη θεωρείται και ανήθικη.

  Παράδειγμα: Σε μία πρόσφατη απάτη τέτοιου τύπου[35], στην Αμερική συνελήφθησαν τρία άτομα, ο Stephen Luscko ετών 39, ο Gregory Neu ετών 30 και ο Justin Medlin ετών 24. Οι Luscko και Neu σχημάτισαν τέσσερις εταιρείες και στρατολόγησαν φίλους και άλλες επιχειρήσεις για να παριστάνουν τα στελέχη των εταιρειών.

  Σύμφωνα με το κατηγορητήριο, οι δύο αυτοί φρόντισαν ώστε να μεταφερθούν εκατομμύρια μετοχών στο δικό τους λογαριασμό ή σε λογαριασμό φίλων τους. Οι παραπάνω διαβιβάσεις, έγιναν με τέτοιο τρόπο ώστε να παρακάμψουν τους κανόνες του χρηματιστηρίου.

  Ο τρίτος της συμμορίας, ο Medlin, βοήθησε το σχέδιο στέλνωντας spam e-mails στο κόσμο με αποτέλεσμα να αυξηθεί το ενδιαφέρον για τις εταιρείες τους και κατά συνέπεια να ανέβουν οι τιμές και ο όγκος των μετοχών.
  Όταν οι τιμές των μετοχών είχαν αυξηθεί αρκετά, οι κατηγορούμενοι τις προωθούσαν στην ανοιχτεί αγορά με αποτέλεσμα οι τιμές να πέφτουν ραγδαία.

[34] http://en.wikipedia.org/wiki/Stock_manipulation
[35] http://findarticles.com/p/articles/mi_hb5247/is_19_28/ai_n29351033/?tag=content;col

Οι ενέργειές τους αυτές τους απέφεραν $6500000. Ο Neu καταδικάστηκε σε πέντε χρόνια φυλάκιση και τρία χρόνια ελεύθερος με περιοριστικούς όρους. Ο Luscko καταδικάστηκε σε πέντε χρόνια φυλάκιση και δύο χρόνια ελεύθερος με περιοριστικούς όρους.

4.3.12 Dialers

Μια πολύ διαδεδομένη παράνομη δραστηριότητα του διαδικτύου είναι οι **dialers**. Χρησιμοποιώντας προγράμματα που εγκαθίστανται στον υπολογιστή μας εν αγνοία μας, οι απατεώνες, είτε μεταφέρουν τη σύνδεση μας σε γραμμές υψηλής χρέωσης είτε χρησιμοποιούν τη γραμμή μας για κλήσεις στο εξωτερικό.

Η λειτουργία του λογισμικού αυτού, που εγκαθίσταται στον υπολογιστή συνήθως μεταμφιεσμένο σε ένα χρήσιμο πρόγραμμα, ανοίγει ουσιαστικά μια κερκόπορτα στο λειτουργικό σύστημα, την οποία χρησιμοποιούν οι απατεώνες για να κερδίζουν χρήματα.

Την ίδια λειτουργία επιτελούν και κάποιες ιστοσελίδες που παρέχουν ‘δωρεάν’ προγράμματα και υπηρεσίες, οι οποίες όμως ειδοποιούν πρώτα το χρήστη στους όρους χρήσης της ιστοσελίδας.

Για την προστασία μας απέναντι σε αυτή τη μορφή απάτης υπάρχουν πρακτικοί τρόποι προφύλαξης, όπως η *φραγή κλήσεων προς το εξωτερικό* και *η χρήση κωδικού για την ενεργοποίηση της υπηρεσίας* ή το *να βγάζουμε το modem από την πρίζα* όταν δε χρησιμοποιούμε το διαδίκτυο. Το πρόβλημα αυτό δεν εμφανίζεται συνήθως σε ADSL συνδέσεις.

Παράδειγμα: Τον Ιούνιο του 2004, η Ισπανική Αστυνομία ξεσκέπασε ένα κύκλωμα που με τη βοήθεια dialers, κατάφερε να αποσπάσει μεγάλο ποσό χρημάτων από ανυποψίαστα θύματα. Συγκεκριμένα, συνελήφθησαν 5 άτομα τα οποία είχαν εξαπατήσει περισσότερα από 45000 θύματα και τους είχαν αποσπάσει €35000000[36].

Οι 5 απατεώνες δρούσαν έξω από τη Μαδρίτη και την Pontevedra. Η ομάδα αυτή, που αποτελούνταν μόνο από άνδρες μεταξύ 30 - 40 ετών, δημιούργησε περισσότερες από 150 ιστοσελίδες με αυτοκίνητα, μουσική και πορνογραφία. Όταν τα θύματα επισκεπτόταν τις ιστοσελίδες αυτές, ένας dialer εγκαθίσταντο στον υπολογιστή τους. Στη συνέχεια το πρόγραμμα καλούσε αριθμούς υψηλής χρέωσης με τα προθέματα 906, 907 και 806.

Πολλά από τα θύματα του κυκλώματος, αναγκάστηκαν να πληρώσουν πάνω από €3000. Αξίζει να σημειωθεί ότι αυτή θεωρείται η μεγαλύτερη απάτη με dialers στην ιστορία.

[36] http://www.theregister.co.uk/2004/06/23/spain_dial_scam/

Αφαίρεση Dialer

Τα περισσότερα dialers λειτουργούν με τον ίδιο τρόπο με τους ιούς υπολογιστών και επομένως μπορούν να βρεθούν και να αφαιρεθούν με τη βοήθεια των αποτελεσματικών προϊόντων αντί-ιών όπως Symantec Norton AntiVirus, Kaspersky, McAfee VirusScan, Panda, AVG.

Και προηγμένα spyware removers, που είναι σε θέση να ανιχνεύσουν το σύστημα σε παρόμοιο λογισμικό αντί-ιών τρόπων κάνουν και έχουν τις εκτενείς βάσεις δεδομένων να μπορούν επίσης να ανιχνεύσουν και να αφαιρέσουν τα dialers και τα σχετικά συστατικά.

Ισχυρές λύσεις σε μια τέτοια περίπτωση είναι: **Microsoft AntiSpyware Beta**, **Spyware Doctor**, **Ad-Aware SE**, **SpyHunter**, **eTrust PestPatrol** or **Spybot - Search & Destroy** και σίγουρα πολύ περισσότερες από αυτές που αναφέρονται εδώ για λόγους συντομίας.

4.3.13 Εγκληματική κλοπή ταυτότητας (για τέλεση αδικήματος)

Όταν λοιπόν ένας εγκληματίας, εμφανίζεται στην αστυνομία ως ένα άλλο άτομο ονομάζεται **εγκληματική κλοπή ταυτότητας**. Σε μερικές περιπτώσεις ο εγκληματίας θα χρησιμοποιήσει μία ταυτότητα βασισμένη σε κλεμμένα προσωπικά στοιχεία κάποιου άλλου, ή ψεύτικα στοιχεία. Όταν λοιπόν ο εγκληματίας συλληφθεί για κάποιο έγκλημα, παρουσιάζει την κλεμμένη αυτή ταυτότητα.

Στη συνέχεια αποδίδονται κατηγορίες από τις αρχές στο θύμα ουσιαστικά της κλοπής. Όταν γίνει η δίκη και ο πραγματικός εγκληματίας δεν εμφανιστεί τότε εκδίδεται ένταλμα εις βάρος του θύματος της κλοπής.

Το θύμα μπορεί να μάθει για το γεγονός εάν για παράδειγμα ακυρωθεί το δίπλωμα οδήγησής του ή αν συλληφθεί κατά τη διάρκεια κάποιου αστυνομικού ελέγχου ρουτίνας (για μία ασήμαντη τροχαία παράβαση).

Είναι δύσκολο για ένα θύμα τέτοιας κλοπής, να καθαρίσει το ποινικό του μητρώο. Οι διαδικασίες που χρειάζονται για να διορθωθεί το λάθος ποινικό μητρώο του θύματος, εξαρτώνται από το αν μπορεί να καθοριστεί η πραγματική ταυτότητα του εγκληματία.

Το θύμα, δηλαδή, πρέπει να εντοπίσει τους αστυνομικούς που συνέλαβαν τον εγκληματία ή μπορεί να χρειαστεί να δώσει αποτυπώματα για να αποδείξει την ταυτότητά του και τελικά θα πάει σε δικαστήριο για να απαλλαχθεί από τις κατηγορίες.

Παρόλα αυτά οι αρχές μπορεί να διατηρήσουν μόνιμα στα αρχεία τους, το όνομα του θύματος ως ψευδώνυμο του εγκληματία. Και ένα πρόβλημα που μπορεί να αντιμετωπίσει το θύμα είναι η ύπαρξη λάθος στοιχείων στις βάσεις δεδομένων μερικών οργανισμών ή υπηρεσιών ακόμα και μετά την απαλλαγή από τις κατηγορίες.

Παράδειγμα: Κάτι παρόμοιο συνέβη στον Daryl A. Landry 41 ετών τότε, στην Αμερική[37]. Για 10 χρόνια ένα άλλο άτομο, ο Darryl M. Landry 39 ετών, χρησιμοποιούσε την ταυτότητα του πρώτου για να διαπράττει ποινικά αδικήματα.

Η ιστορία λοιπόν, έχει ως εξής: Ο Daryl A. Landry πήγε το 1998 να ανανεώσει το δίπλωμα οδήγησης στην αρμόδια αρχή της Αμερικής. Εκεί ο υπάλληλος τον πληροφόρησε ότι υπάρχει ένα ένταλμα σύλληψης σε βάρος του για επίθεση σε αστυνομικό. Αυτό ήταν μόνο η αρχή.

Το άτομο που επιτέθηκε στον αστυνομικό πραγματοποίησε και απαγωγές παιδιών. Ακολούθησε έρευνα της αστυνομίας στο σπίτι του Daryl A. Landry. Για σχεδόν 10 χρόνια ο Daryl A. Landry, παρευρισκόταν σε δίκες για εγκλήματα που είχε διαπράξει ο Darryl M. Landry. Πολλές φορές αναγνωρίστηκε ότι τα εγκλήματα δεν τα είχε διαπράξει ο Daryl A. Landry αλλά διαφορετικό άτομο και οι αρχές δεσμεύθηκαν να βρουν τον πραγματικό ένοχο, αλλά δεν το έκαναν ποτέ.

Σε αντίθεση με τις περιπτώσεις κλοπής οικονομικής ταυτότητας όπου οι υποθέσεις ξεκαθαρίζονται σε 2-4 χρόνια, τα θύματα της εγκληματικής κλοπής ταυτότητας, μπορεί να ζήσουν την υπόλοιπη ζωή τους με βεβαρημένο ποινικό μητρώο. Γι αυτό το λόγο λοιπόν, η υπόθεση αυτή έκανε τόσα χρόνια να ξεκαθαριστεί.

Όλα τελείωσαν στις 6 Μαρτίου 2007, όταν η αστυνομία συνέλαβε τον Darryl M. Landry και του απαγγέλθηκαν κατηγορίες για κλοπή ταυτότητας καθώς και για σωρεία άλλων αδικημάτων.

4.3.14 Κλοπή στοιχείων ασθενή

Η **κλοπή στοιχείων ιατρικής ταυτότητας** συμβαίνει όταν ένας απατεώνας χρησιμοποιεί το όνομα ενός άλλου ατόμου συνδυασμένο καμιά φορά με άλλα στοιχεία (π.χ. Αριθμό μητρώου Ασφαλιστικού φορέα), χωρίς φυσικά το θύμα να γνωρίζει το παραμικρό. Αυτό γίνεται για να έχει πρόσβαση ο απατεώνας σε ιατρικές υπηρεσίες.

Αυτό συχνά έχει σαν αποτέλεσμα να καταγράφονται λανθασμένες πληροφορίες στον ηλεκτρονικό φάκελο ασθενή του θύματος.

Παράδειγμα: Το 2004 η Lind Weaver, κάτοικος της Florida, έπαθε σοκ όταν έλαβε ένα λογαριασμό από ένα νοσοκομείο που της χρέωνε μία επέμβαση ακρωτηριασμού στο πόδι. Επικοινωνώντας με το λογιστήριο του νοσοκομείου, προσπάθησε να τους πείσει ότι δεν έκανε μια τέτοια επέμβαση αλλά δεν την πίστεψαν και αναγκάστηκε να πάει η ίδια να τους δείξει ότι έχει και τα δύο της πόδια[38].

Τον επόμενο χρόνο εισήχθη στο νοσοκομείο για υστερεκτομή. Τότε ανακάλυψε ότι ο κλέφτης ταυτότητάς της, της είχε προσθέσει στο ιατρικό ιστορικό διάφορες ασθένειες που η ίδια δεν είχε.

---

[37] http://www.eagletribune.com/punewsnh/local_story_080093930
[38] http://crime.suite101.com/article.cfm/what_is_medical_identity_theft

4.4 Διάσημοι κλέφτες ταυτοτήτων

Ο πιο διάσημος κλέφτης ταυτοτήτων είναι ο **Radovan Karadzic *(βλ. εικ. 11)***, ο οποίος γεννήθηκε στη γιουγκοσλαβική πόλη Πετνίτσα (στο σημερινό Μαυροβούνιο) στις 19 Ιουνίου 1945. Αυτός είναι ένας πρώην πολιτικός από τα ιδρυτικά μέλη του Δημοκρατικού κόμματος της Σερβίας. Ήταν ο πρώτος πρόεδρος της Βοσνίας και Ερζεγοβίνης.

Το 1960 μετακόμισε στο Σαράγεβο για να σπουδάσει Ψυχιατρική, ενώ τα έτη 1974 - 1975 παρακολούθησε μαθήματα Ιατρικής στο Πανεπιστήμιο Κολούμπια της Νέας Υόρκης.

Επιστρέφοντας στη Γιουγκοσλαβία, εργάστηκε στο νοσοκομείο του Κόσσοβο. Παράλληλα ασχολήθηκε με την ποίηση (βραβεύτηκε με δύο λογοτεχνικά βραβεία) και επηρεάστηκε από το Σέρβο συγγραφέα Ντόμπριτσα Τσόσιτς, ο οποίος τον παρότρυνε να ασχοληθεί με την πολιτική.

Το 1984 κατηγορήθηκε για κατάχρηση χρημάτων του νοσοκομείου όπου εργαζόταν στο Βελιγράδι, με σκοπό να κτίσει εξοχικό σπίτι στο βοσνιακό χωριό Πάλε. Αναμένοντας τη δίκη του, παρέμεινε υπό κράτηση για 11 μήνες και η δίκη του ξανάρχισε το 1985, καθώς σε πρώτη φάση απελευθερώθηκε με εγγύηση. Τελικά καταδικάστηκε σε κάθειρξη τριών ετών για κατάχρηση και απάτη, ποινή που όμως δεν εξέτισε, αφού είχε ήδη εκτίσει έναν χρόνο στη φυλακή.

4.4.1 Radovan Karadzic

Ο Karadzic κατηγορείται ως υπεύθυνος, τόσο ατομικά όσο και σαν πρόεδρος του Συμβουλίου Ασφαλείας και ανώτατος διοικητικής του Σερβοβοσνιακού στρατού, για πολλά εγκλήματα πολέμου που διαπράχθηκαν κατά του μη σερβικού πληθυσμού της Βοσνίας.

Σύμφωνα με το κατηγορητήριο, οι σερβοβοσνιακές δυνάμεις υπό τις εντολές του ξεκίνησαν την πολιορκία του Σαράγεβο και διέπραξαν αρκετά εγκλήματα κατά των μουσουλμάνων-μεταξύ άλλων εκτελέσεις, εκτοπισμούς πληθυσμών και εγκλεισμούς σε στρατόπεδα συγκέντρωσης.

Κατηγορείται επίσης ότι διέταξε τη *Σφαγή της Σρεμπρένιτσα* το 1995, όπου εκτελέστηκαν χιλιάδες μουσουλμάνοι, καθώς και την ομηρία προσωπικού του ΟΗΕ το Μάιο - Ιούνιο του ιδίου έτους.

Αναλυτικότερα, οι κατηγορίες προς τον Karadzic όπως διατυπώθηκαν από το «Διεθνές Ποινικό Δικαστήριο για την πρώην Γιουγκοσλαβία» το 1995, είναι οι ακόλουθες:

- Πέντε περιπτώσεις εγκλημάτων κατά της ανθρωπότητας (εξόντωση, φόνος, διώξεις για πολιτικούς, φυλετικούς και θρησκευτικούς λόγους, απάνθρωπες πράξεις - μετακίνηση δια της βίας).

- Τρεις περιπτώσεις παραβιάσεων του εθιμικού δικαίου του πολέμου (φόνος, τρομοκράτηση αμάχων, ομηρία).

- Μια περίπτωση σοβαρής παραβίασης των Συνθηκών της Γενεύης (απρόκλητος φόνος εκ προθέσεως).

- Παράνομος εκτοπισμός πληθυσμών αμάχων λόγω της θρησκευτικής ή εθνοτικής τους ταυτότητας

Τελικά ο Karadzic συνελήφθη στο Βελιγράδι στις 21 Ιουλίου του 2008[39], όπως ανακοινώθηκε από επίσημες κυβερνητικές πηγές. Η κυβέρνηση των ΗΠΑ είχε επικηρύξει τον Karadzic και τον άμεσο συνεργάτη του Ράτκο Μλάντιτς με 5 εκατομμύρια δολάρια. Ο Karadzic δεν αρνήθηκε την ταυτότητά του, συνελήφθη και οδηγήθηκε σε ειδικό δικαστήριο στη Σερβία. Το Διεθνές Δικαστήριο επιβεβαίωσε τη σύλληψη.

Τότε αποκαλύφθηκε πως ο Karadzic ζούσε στην συνοικία Νόβι Μπέογκραντ («Νέο Βελιγράδι») και χρησιμοποιούσε πλαστή ταυτότητα με το όνομα Dragan Dabić. Όταν συνελήφθη, η εμφάνισή του με λευκά μακριά μαλλιά και μακριά λευκή γενειάδα ***(βλ. εικ. 12)***[40] , ήταν εντελώς διαφορετική από αυτή της δεκαετίας του '90.

Ασκούσε το ιατρικό επάγγελμα σε ιδιωτική κλινική, με ειδικότητα στην εναλλακτική ιατρική και την Ψυχολογία. Έδινε σεμινάρια, που κάποιες φορές καλύπτονταν από την τηλεόραση, ενώ διαπιστώθηκε πως με το πλαστό διαβατήριό του είχε ταξιδεύσει σε χώρες της Ευρωπαϊκής Ένωσης.

Αρχικά είχε διαδοθεί ότι διατηρούσε και προσωπική ιστοσελίδα ως Ντάμπιτς, αργότερα όμως αποδείχθηκε ότι η εν λόγω σελίδα είχε αναρτηθεί από τρίτους μετά την σύλληψη του. Τόσο ο σπιτονοικοκύρης του όσο και οι γείτονες δήλωσαν ότι δε γνώριζαν την πραγματική του ταυτότητα.

Τη νύχτα της σύλληψής του, εκατοντάδες Βόσνιοι πανηγύρισαν στους δρόμους του Σεράγεβο. Οι διεθνείς αντιδράσεις ήταν επίσης θετικές. Τα δυτικά μέσα προεξόφλησαν την ενοχή του, εντούτοις στη Σερβία δεν έλειψαν οι εκδηλώσεις αλληλεγγύης προς το πρόσωπό του κυρίως από το σερβικό εθνικιστικό κόμμα SRS.

Στις 30 Ιουλίου του 2008 έγινε η έκδοση του Karadzic στη Χάγη, για να δικαστεί από το Διεθνές Δικαστήριο για τα Εγκλήματα στην πρώην Γιουγκοσλαβία (ICTY).

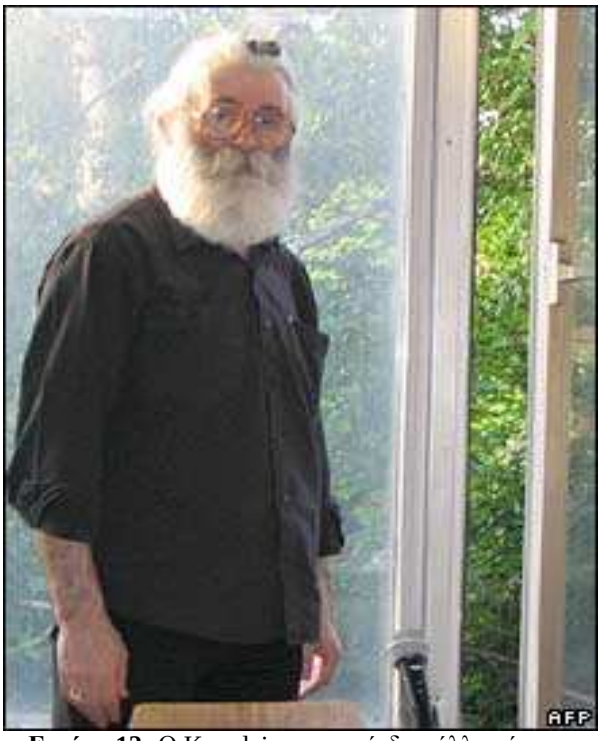
Ο Karadzic οδηγήθηκε αεροπορικώς σε ειδικό χώρο κράτησης στο Σεβένινγκεν, κοντά στη Χάγη, όπου και θα παραμείνει έως ότου να δικαστεί. Στις 31 Ιουλίου παρουσιάστηκε ενώπιον του Διεθνούς Δικαστηρίου και εξέφρασε φόβους για τη ζωή του, κάνοντας λόγο για "παρατυπίες κατά τη σύλληψή του" στην περιοχή του Βελιγραδίου.

---

39 http://el.wikipedia.org/wiki/%CE%A1%CE%AC%CE%BD%CF%84%CE%BF%CE%B2%CE%B1%CE%BD_%CE%9A%CE%AC%CF%81%CE%B1%CF%84%CE%B6%CE%B9%CF%84%CF%82#.CE.A3.CF.8D.CE.BB.CE.BB.CE.B7.CF.88.CE.B7

40 http://news.bbc.co.uk/2/hi/in_pictures/7518646.stm

Εικόνα 11: Ο Karadzic την δεκαετία του '90



Εικόνα 12: Ο Karadzic την περίοδο σύλληψής του

4.4.2 Jocelyn S. Kirsch και Edward Kyle Anderton

Άλλοι διάσημοι κλέφτες ταυτοτήτων, είναι οι **Jocelyn S. Kirsch (*βλ. εικ.13)*** και **Edward Kyle Anderton (*βλ. εικ.14*)**[41]. Οι κατηγορίες που τους βάρυναν όταν συνελήφθηκαν, είχαν όλες να κάνουν με απάτες βασισμένες σε κλοπή ταυτότητας.

Και οι δύο προέρχονταν από εύπορες οικογένειες που τους έστειλαν στα καλύτερα ιδιωτικά σχολεία. Η Kirsch σπούδαζε στο πανεπιστήμιο Drexel και ο Anderton βοηθούμενος από τις διασυνδέσεις της οικογένειάς του είχε μία καλοπληρωμένη δουλειά ως οικονομικός αναλυτής.

Γενικά ζούσαν μια άνετη και πολυτελή ζωή και μάλιστα νοίκιαζαν ένα διαμέρισμα στο Rittenhouse με $3000 ενοίκιο το μήνα. Το αρκετό, όμως, δεν ήταν αρκετό και το ζευγάρι ξεκίνησε να γίνεται άπληστο.

Η Kirsch και ο Anderton ξεκίνησαν να 'ψαχουλεύουν' στα γραμματοκιβώτια και στα σπίτια των γειτόνων τους, και έκλεβαν οτιδήποτε περιείχε προσωπικά στοιχεία άλλων. Χρησιμοποιώντας τα προσωπικά στοιχεία των άλλων ξεκίνησαν να κάνουν απάτες. Αυτό συνεχίστηκε για 2 χρόνια χωρίς να τους πάρει κανείς χαμπάρι.

Η ιστορία αυτή τους απέφερε τουλάχιστον $100000 μόνο το 2007, με τα οποία χρηματοδότησαν τα ταξίδια τους στο Παρίσι **(*βλ. εικ.15*)**, τη Χαβάη και το Λονδίνο.

Η απάτη ξεκίνησε να ξετυλίγεται στις 19 Νοεμβρίου 2007, όταν μία γειτόνισσα υποψιάστηκε ότι η ταυτότητά της έχει κλαπεί και αποφάσισε να διερευνήσει το θέμα. Στις 20 Νοεμβρίου μία άλλη γειτόνισσα ειδοποιήθηκε από την μεταφορική εταιρεία UPS ότι υπάρχει γι αυτήν ένα δέμα το οποίο δεν είχε παραγγείλει ούτε περίμενε και ειδοποίησε τις Αρχές.

Η αστυνομία περίμενε στο τοπικό κατάστημα της εταιρείας μέχρι να έρθει αυτός που θα παραλάβει το δέμα. Στις 30 Νοεμβρίου η Kirsch και ο Anderton μπήκαν στο κατάστημα να παραλάβουν το δέμα όπου και συνελήφθησαν.

Μετά από ένταλμα έρευνας στο διαμέρισμά τους, η αστυνομία ανακάλυψε ότι δεν ήταν κοινοί κλέφτες ταυτοτήτων. Κατείχαν 4 υπολογιστές, 2 εκτυπωτές, 1 scanner καθώς και ένα μηχάνημα το οποίο φτιάχνει ταυτότητες. Ακόμη η αστυνομία βρήκε $17000 σε μετρητά, 20 κλεμμένες πιστωτικές κάρτες, πολλά πλαστά διπλώματα οδήγησης καθώς και κλειδιά για τα γραμματοκιβώτια και τα σπίτια των γειτόνων.

Τελικά, στις 17 Οκτώβρη 2008, η Kirsch καταδικάστηκε σε 5 χρόνια φυλάκισης και στις 14 Νοεμβρίου του ίδιου έτους ο Anderton, καταδικάστηκε σε 4 χρόνια φυλάκισης.

---

[41] http://pysih.com/2007/12/07/jocelyn-kirsch-and-edward-k-anderton/

Εικόνα 13: Jocelyn S.Kirsch

Εικόνα 14: Edward Kyle Anderton

Εικόνα 15: Jocelyn S. Kirsch και Edward Kyle Anderton στο Παρίσι

Κεφάλαιο 5 Τρόποι προστασίας από κλοπή προσωπικών στοιχείων

5.1 Πότε έχω πέσει θύμα απάτης;

Κάποιος κινδυνεύει ή έχει πέσει ήδη θύμα απάτης εάν συμβαίνει κάτι από τα ακόλουθα:

- έχει χάσει ή του έχουν κλαπεί σημαντικά έγγραφα όπως δίπλωμα οδήγησης ή διαβατήριο,
- η αλληλογραφία που αναμένει από την τράπεζα, δεν έχει φτάσει ή δεν λαμβάνει καθόλου αλληλογραφία,
- στο πιστωτικό του φάκελο βρίσκει στοιχεία από οργανισμούς με τους οποίους δεν συνεργάζεται,
- εμφανίζονται στο λογαριασμό της πιστωτικής κάρτας αγαθά που δεν έχει λάβει,
- κάνει αίτηση για μία κρατική χορήγηση και μαθαίνει πως την έχει κάνει ήδη,
- λαμβάνει λογαριασμούς, ειδοποιήσεις ή αποδείξεις για αγαθά , υπηρεσίες που δεν έχει ζητήσει,
- δεν του έχει εγκριθεί ένα δάνειο ή πιστωτική κάρτα παρά το καλό πιστωτικό ιστορικό,
- έχει γίνει ένα συμβόλαιο κινητής τηλεφωνίας στο όνομά του χωρίς να το ξέρει,
- λαμβάνει γράμματα από εισπρακτικές εταιρείες, για χρέη που δεν είναι δικά του,
- πιστωτικοί οργανισμοί με τους οποίους δεν συναλλάσσεται, επικοινωνούν μαζί του ζητώντας τη πληρωμή ενός τεράστιου χρέους.

5.2 Οι ανησυχίες των καταναλωτών

Τα στοιχεία αυτής της έρευνας[42] είναι βέβαια σχετικά παλιά. Σε μια αγορά που αναπτύσσεται με τόσο γρήγορους ρυθμούς η κατάσταση έχει σαφώς διαφοροποιηθεί στα δύο περίπου χρόνια που μεσολάβησαν. Η Διεθνής των Καταναλωτών έχει ήδη σε εξέλιξη μια νέα έρευνα που θα απεικονίσει την σημερινή κατάσταση στον τομέα αυτό.

[42] http://kepka.org/index.php?option=com_content&task=view&id=294&Itemid=50

Ο on line καταναλωτής πρέπει να απολαμβάνει με την εθνική νομοθεσία και πρακτική, τουλάχιστο το ίδιο επίπεδο προστασίας που απολαμβάνει για τους άλλους (παραδοσιακούς) τρόπους αγορών στην χώρα του. Πέρα από αυτό τον γενικό κανόνα, πρέπει να επισημάνουμε επίσης:

Ασφάλεια πληρωμών

Όταν οι καταναλωτές κάνουν χρήση της πιστωτικής τους κάρτας για να πληρώσουν προϊόντα που έχουν παραγγείλει, θέλουν να είναι βέβαιοι ότι τα στοιχεία της συναλλαγής δεν θα υποκλαπούν με κανένα τρόπο από τρίτους. Θα πρέπει λοιπόν να χρησιμοποιηθούν τα πλέον σύγχρονα τεχνικά μέσα για την παροχή υψηλού επιπέδου ασφάλειας στις on line συναλλαγές, και τα μέσα αυτά να εκσυγχρονίζονται με τους ρυθμούς που απαιτείται ώστε να διατηρούν το επίπεδο αυτό σταθερά υψηλό.

Ιδιωτικότητα και ασφάλεια των προσωπικών δεδομένων

Οι καταναλωτές θα πρέπει να είναι σίγουροι ότι οι πληροφορίες που δίνουν on line, όπως η διεύθυνσή τους, οι τραπεζικοί λογαριασμοί τους και οι αγορές τους, παραμένουν ιδιωτικές και δεν προωθούνται σε τρίτους για οποιασδήποτε μορφής χρήση ή εκμετάλλευση.

Ο καταναλωτής θα πρέπει να ενημερωθεί για τον τρόπο χρήσης των προσωπικών δεδομένων του και να του δοθεί η δυνατότητα να συμφωνήσει ή όχι σε συγκεκριμένες χρήσεις. Θα πρέπει επίσης να προστατευθεί από ανεπιθύμητες επιθετικές διαφημίσεις και ηλεκτρονική αλληλογραφία.

5.3 Τα προσωπικά δεδομένα των καταναλωτών απειλούνται στο Internet

Αμερικανικές και Ευρωπαϊκές ιστοσελίδες αποτυγχάνουν να εφαρμόσουν τα κριτήρια της προστασίας των προσωπικών δεδομένων. Διεθνής έρευνα αποκαλύπτει ότι Καταναλωτές αγνοούν τις πιο βασικές αρχές της σωστής χρήσης του διαδικτύου.

Η Διεθνής των Καταναλωτών, Παγκόσμια Ομοσπονδία αποτελούμενη από 263 Καταναλωτικούς Οργανισμούς, παρουσίασε τα αποτελέσματα συγκριτικής μελέτης, που αφορά την προστασία των προσωπικών δεδομένων. Η έρευνα έγινε σε 751 ιστοσελίδες, μέσα από τις οποίες διάφορες εταιρίες πωλούν προϊόντα και υπηρεσίες στους Καταναλωτές.

Τα κύρια ευρήματα της μελέτης αποκαλύπτουν πως τα μέτρα, τα οποία παίρνουν διάφορες Κυβερνήσεις για να προστατεύσουν τα προσωπικά δεδομένα των Καταναλωτών, δεν είναι επαρκή.

Η έρευνα της Διεθνούς των Καταναλωτών[43], δείχνει ξεκάθαρα πως πολλές αμερικάνικες και ευρωπαϊκές ιστοσελίδες, οι οποίες απευθύνονται σε Καταναλωτές, απέτυχαν οικτρά στην προστασία των προσωπικών δεδομένων.

[43] http://kepka.org/index.php?option=com_content&task=view&id=793&Itemid=61

Προστασία από κλοπή προσωπικών στοιχείων

Συγκεκριμένα η C.I. επισημαίνει:

- Πάνω από τα δύο τρίτα των ιστοσελίδων συλλέγουν κάποιες προσωπικές πληροφορίες και σχεδόν όλες αυτές οι ιστοσελίδες ζητούν τέτοιες λεπτομέρειες, ώστε να καθίσταται εύκολη η αναγνώριση και η επικοινωνία με τον επισκέπτη τους.

- Η συντριπτική πλειοψηφία των ιστοσελίδων κατά την εγγραφή του χρήστη στην λίστα των διαφημιστικών e-mail τους, μοιράζει τα στοιχεία του σε λίστες άλλων εταιριών με τις οποίες σχετίζεται, χωρίς να δίνει το περιθώριο επιλογής στον Καταναλωτή.

- Παρά το γεγονός ότι υπάρχει αυστηρή Ευρωπαϊκή Νομοθεσία, που διέπει την προστασία των προσωπικών δεδομένων των χρηστών, η πλειοψηφία των ευρωπαϊκών ιστοσελίδων δεν ενημερώνει τους Καταναλωτές για την ακριβή χρήση των προσωπικών δεδομένων τους, ούτε ζητά την άδειά τους για το μοίρασμα των στοιχείων τους σε άλλες εταιρίες.

- Μόνο το 10% των ιστοσελίδων, οι οποίες στοχεύουν στην πώληση προϊόντων σε παιδιά- Καταναλωτές, ζητούν από αυτά να πάρουν την συγκατάθεση των γονέων τους, πριν δώσουν τα προσωπικά τους στοιχεία, ή έστω να ενημερώσουν τους γονείς τους μετά.

Η προστασία των προσωπικών δεδομένων είναι αναγνωρισμένο ως βασικό ανθρώπινο δικαίωμα, αλλά βρήκαμε πως πάρα πολλές εταιρίες συλλέγουν όχι απαραίτητες και πολύ προσωπικές πληροφορίες για τους πελάτες τους.

'Σε ορισμένες χώρες υπάρχει νομοθετικό πλαίσιο, αλλά δυστυχώς υλοποιείται ανεπαρκώς με αποτέλεσμα οι Καταναλωτές να μην έχουν τον έλεγχο των προσωπικών δεδομένων τους', λέει η κα Anna Fielder, Διευθύντρια του Γραφείου για τις Αναπτυγμένες και τις Μεταβατικές Οικονομίες της Διεθνούς των Καταναλωτών. *'Αυτή η παραμέληση της προστασίας των προσωπικών δεδομένων, σε παγκόσμιο επίπεδο, μας ανησυχεί όλο και περισσότερο, δεδομένου ότι οι τεχνολογίες ηλεκτρονικής συλλογής πληροφοριών αναπτύσσονται τόσο γρήγορα'*.

Η Διεθνής των Καταναλωτών καλεί τους πολιτικούς σε εθνικό και διεθνές επίπεδο να πάρουν μέτρα, άμεσα, για να υιοθετηθούν νόμοι, κανόνες και διαδικασίες ώστε:

- Οι Καταναλωτές να έχουν τη δυνατότητα να ελέγχουν τον τρόπο που συλλέγονται, χρησιμοποιούνται ή αποκαλύπτονται σε τρίτους τα προσωπικά τους δεδομένα. Οι πληροφορίες, που δίνουν οι Καταναλωτές, να χρησιμοποιούνται μόνο όσο είναι απαραίτητο για να ολοκληρωθούν οι διαδικασίες αγοράς προϊόντων ή υπηρεσιών, που διατίθενται στις συγκεκριμένες ιστοσελίδες.

- Οι Καταναλωτές να μπορούν εύκολα να ελέγξουν, να διορθώσουν ή να διαγράψουν οποιαδήποτε πληροφορία μπορεί κάποια ιστοσελίδα να έχει για αυτούς. Οι πληροφορίες αυτές πρέπει να συλλέγονται, αποθηκεύονται και μεταδίδονται με ασφαλή τρόπο, μια και πρόκειται για "ευαίσθητες" πληροφορίες.

- Να καθιερωθεί ανεξάρτητο σώμα Ελεγκτών, για να επιβλέπει την λειτουργία των ιστοσελίδων, την συμμόρφωση τους με τους κανόνες σωστής λειτουργίας, να επιβάλλει κυρώσεις για παραβάσεις, και να εξασφαλίζει γρήγορα και ανέξοδα αποζημίωση στον Καταναλωτή, στην περίπτωση που θίγεται από τη μη σωστή χρήση των στοιχείων του.

5.4 Τρόποι αυτοπροστασίας σε περίπτωση κλοπής

Το πρώτο και σημαντικότερο που πρέπει να θυμάται κάποιος είναι ότι τα προσωπικά δεδομένα είναι πολύτιμα και δεν πρέπει να δίδονται σε άτομα άγνωστα ή αμφιβόλου εμπιστοσύνης.

Κάποιες χρήσιμες συμβουλές:

- Οι προσωπικές πληροφορίες του κάθε ανθρώπου είναι πολύτιμες και πρέπει να διαφυλάσσονται.

- Κάποιος πρέπει να ζητάει συχνά μια αναφορά του προσωπικού του πιστωτικού φακέλου για να επιβεβαιώσει ποιοι οικονομικοί οργανισμοί έχουν πρόσβαση στα στοιχεία του. Αυτό είναι ιδιαίτερα χρήσιμο, δύο ή τρεις μήνες μετά από μετακόμιση

- Πρέπει να είναι κάποιος ιδιαίτερα προσεχτικός όταν κατοικεί κάπου όπου μπορεί να έχουν πρόσβαση στην αλληλογραφία του κάποιοι τρίτοι. Μετά από συνεννόηση με την τράπεζα, ο πελάτης μπορεί να παραλαμβάνει πιστωτικές κάρτες και βιβλιάρια επιταγών από τοπικό υποκατάστημα.

- Εάν κάποιος υποπτεύεται ότι του έχει κλαπεί η αλληλογραφία, μπορεί να επικοινωνήσει με τις υπηρεσίες ταχυδρομείου, για να ελέγξει εάν έχει γίνει ανακατεύθυνση της αλληλογραφίας του χωρίς να το γνωρίζει.

- Όταν κάποιος μετακομίσει, πρέπει να ειδοποιήσει τους οικονομικούς οργανισμούς με τους οποίους συναλλάσσεται. Ακόμα πρέπει να ειδοποιήσει τις ταχυδρομικές υπηρεσίες, να κάνουν ανακατεύθυνση της αλληλογραφίας του που προορίζεται για την παλιά του διεύθυνση για τουλάχιστον ένα χρόνο.

- Για να γίνουν τηλεφωνικές συναλλαγές με την τράπεζα, μπορεί να υπάρχει μια πληροφορία "κλειδί", ώστε όταν ο πελάτης τηλεφωνεί, να μπορεί να ταυτοποιηθεί. Αν όμως κάποιος τηλεφωνήσει στον πελάτη, ισχυριστεί ότι είναι από την τράπεζα και του ζητήσει αυτή την πληροφορία, πιθανότατα είναι απατεώνας.

- Αν τηλεφωνήσει κάποιος άγνωστος και ισχυριστεί ότι έχουμε κερδίσει κάποιο βραβείο και για να το παραλάβουμε πρέπει να δώσουμε τα προσωπικά μας στοιχεία, του ζητάμε να μας στείλει μια έγγραφη φόρμα στοιχείων.

    - Αν αρνηθεί, αρνούμαστε και εμείς την υποτιθέμενη προσφορά.

- Αν μας τη στείλει σιγουρευόμαστε ότι η φόρμα αυτή θα καταλήξει σε κάποιο αξιόπιστο οργανισμό.

- Όταν κάποιος ταξιδεύει πρέπει να ειδοποιήσει το ταχυδρομείο να του κρατά την αλληλογραφία, ή να ζητήσει από κάποιο αξιόπιστο άτομο να την παραλαμβάνει.

- Αν κατά τη διάρκεια ταξιδιού χρειαστεί να γίνει ανταλλαγή προσωπικών πληροφοριών μέσω τηλεφώνου, καλό θα είναι να πραγματοποιηθεί σε μέρος με όσο το δυνατό λιγότερο κόσμο ή αν είναι δυνατό σε κλειστό τηλεφωνικό θάλαμο.

5.5 Τρόποι άμυνας που αφορούν την ασφάλεια ηλεκτρονικών συναλλαγών

Οι τράπεζες και τα ηλεκτρονικά καταστήματα χρησιμοποιούν διάφορα μέσα για την ασφάλεια των συναλλαγών και την προστασία των προσωπικών δεδομένων των πελατών.

Πρώτα απ' όλα γίνεται ταυτοποίηση των πελατών με username και password. Αφού γίνει ταυτοποίηση, από την αρχή μέχρι το τέλος κάθε συνεδρίας, γίνεται κρυπτογράφηση με χρήση κάποιου πρωτοκόλλου που τις περισσότερες φορές είναι το SSL.

Ακόμα η πρόσβαση στα συστήματα της τράπεζας, ελέγχεται με τοίχος προστασίας (Firewall). Αν δεν υπάρξει δραστηριότητα για ένα προκαθορισμένο χρονικό διάστημα ("Idle Timeout") γίνεται αυτόματη αποσύνδεση από το σύστημα.

Φυσικά, όλες οι πληροφορίες που διαβιβάζονται από τον πελάτη προς την τράπεζα είναι εμπιστευτικές και η τράπεζα έχει λάβει όλα τα απαραίτητα μέτρα ώστε να γίνεται χρήση τους μόνο στο βαθμό που αυτό κρίνεται αναγκαίο στο πλαίσιο των παρεχόμενων υπηρεσιών.

Όπως βλέπουμε, οι τράπεζες και πολλά ηλεκτρονικά καταστήματα λαμβάνουν τα απαραίτητα μέτρα για την προστασία των ηλεκτρονικών συναλλαγών. Πολλές φορές όμως αυτό δεν επαρκεί. Πάνω απ' όλα, χρειάζεται η επαγρύπνηση των καταναλωτών για να μην πέσουν θύματα μιας καλοστημένης ηλεκτρονικής απάτης.

Το βασικότερο είναι η διαφύλαξη των **Username** και **Password**. Ο πελάτης όταν κάνει login θα πρέπει να είναι σίγουρος ότι η ιστοσελίδα στην οποία βρίσκεται, ανήκει στη τράπεζα ή στο κατάστημα με το οποίο συναλλάσσεται.

Αυτό επιτυγχάνεται ελέγχοντας αν στην οθόνη υπάρχει ένα εικονίδιο λουκετάκι. Επιπλέον, υποδηλώνει το ψηφιακό πιστοποιητικό και πατώντας το εικονίδιο, ο πελάτης μπορεί να ελέγξει αν τα στοιχεία του πιστοποιητικού ανήκουν στη τράπεζα.

Τέλος, ο πελάτης πρέπει να θυμάται ότι η τράπεζα δεν θα του ζητήσει ποτέ εμπιστευτικά προσωπικά δεδομένα, όπως UserID, password, αριθμούς λογαριασμών μέσω ηλεκτρονικού ταχυδρομείου (e-mail), ούτε του στέλνει εμπιστευτικές πληροφορίες μέσω αυτού.

5.5.1 Κλοπή προσωπικών στοιχείων μέσω φορητού υπολογιστή

Ένας άλλος τρόπος να αντλήσουν οι εγκληματίες προσωπικά δεδομένα, είναι μέσω του φορητού υπολογιστή του θύματος[44]. Λόγω της φύσης του, ο φορητός υπολογιστής είναι εύκολο να κλαπεί. Γι αυτό το λόγο, οι κάτοχοι τέτοιων υπολογιστών θα πρέπει να είναι ιδιαίτερα προσεχτικοί και να μην τους αφήνουν εκτεθειμένους σε δημόσιους χώρους.

Επειδή αυτό δεν είναι πάντοτε εφικτό, καλό θα ήταν να μην υπάρχουν αρχεία που περιέχουν ευαίσθητα δεδομένα ή έγγραφα αποθηκευμένα στο σκληρό δίσκο. Σε περίπτωση που υπάρχουν, θα πρέπει να προστατεύονται με κάποιο δύσκολο password ή να είναι κρυπτογραφημένα.

5.5.1.1 Βασικά μέτρα ασφάλειας φορητού υπολογιστή

- Πρέπει να επιλέξει κάποιος ένα ασφαλές λειτουργικό σύστημα και να το κλειδώσει με Password
- Καλό θα ήταν να υπάρχει Password και στο BIOS
- Κάποιος θα μπορούσε να τοποθετήσει αναγνωριστικό ταμπελάκι ‘η να χαράξει κάποιο αναγνωριστικό σημάδι πάνω στο laptop.
- Ακόμα κάθε αγοραστής του laptop θα μπορούσε να κάνει δήλωση του προϊόντος στο κατασκευαστή

5.5.1.2 Μέτρα φυσικής ασφάλειας φορητού υπολογιστή

- Το πιο απλό μέτρο είναι το κλείδωμα της συσκευής με ένα ειδικό καλώδιο και λουκέτο.
- Για να αποτραπούν οι κλοπές φορητών υπολογιστών από γραφεία ή σπίτια μπορεί να χρησιμοποιηθεί βάση στήριξης.
- Δεν πρέπει να ξεχνάει κανείς να ασφαλίζει τις κάρτες PCMCIA όταν δεν χρησιμοποιούνται.
- Πρέπει να είναι εγκατεστημένο Firewall στο φορητό υπολογιστή.
- Επίσης καλό είναι αν κάποιος έχει εγκατεστημένο στο φορητό του υπολογιστή ειδικό λογισμικό εντοπισμού για να μπορεί να βρεθεί σε περίπτωση κλοπής.

[44] http://labmice.techtarget.com/articles/laptopsecurity.htm

5.5.1.3 Προστασία ευαίσθητων δεδομένων

- Εάν κάποιος διαθέτει το κατάλληλο Λειτουργικό σύστημα θα πρέπει να χρησιμοποιήσει σύστημα διαμόρφωσης αρχείων NTFS.

- Πρέπει να απενεργοποιηθεί ο λογαριασμός επισκέπτη

- Ένα μέτρο που δεν θα προσφέρει ουσιαστική ασφάλεια, αλλά θα καθυστερήσει τους επίδοξους hacker είναι η μετονομασία του λογαριασμού Administrator.

- Ένα άλλο μέτρο που μπορεί να χρησιμοποιηθεί είναι η δημιουργία ενός ψεύτικου λογαριασμού Administrator.

- Μέσω των ρυθμίσεων ασφαλείας θα πρέπει η οθόνη login να μην εμφανίζει το τελευταίο username που χρησιμοποιήθηκε.

- Σε λειτουργικά συστήματα που υποστηρίζεται θα πρέπει να ενεργοποιηθεί το EFS (Encrypting File System).

- Εάν υπάρχει θύρα υπερύθρων στο φορητό υπολογιστή, θα πρέπει να απενεργοποιηθεί.

- Αν κάποιος πρόκειται να φύγει για διακοπές, θα μπορούσε να κάνει backup τα δεδομένα.

- Για την μεταφορά ευαίσθητων δεδομένων, μπορούν να χρησιμοποιηθούν και φυσικές μέθοδοι, π.χ. USB stick, για να μην μεταδοθούν online.

5.5.1.4 Αποτροπή κλοπής της συσκευής

- Το πρώτο πράγμα που χρειάζεται να θυμάται κάποιος, είναι ότι κανένα μέρος δεν είναι ασφαλές.

- Για την μεταφορά του φορητού υπολογιστή, θα βοηθούσε μία τσάντα η οποία δεν μαρτυρά την ύπαρξη του.

- Σε περίπτωση που χρειαστεί να σταματήσει κάποιος σε τηλεφωνικό θάλαμο, θα πρέπει να προσέχει το φορητό του υπολογιστή.

- Ιδιαίτερη προσοχή πρέπει να επιδείξουν οι ταξιδιώτες όταν χρησιμοποιούν οποιοδήποτε μέσο μεταφοράς και μεταφέρουν το φορητό τους υπολογιστή. Ακόμα, θα πρέπει να προσέχουν και όταν αφήνουν τον υπολογιστή τους στο ξενοδοχείο.

- Τέλος, ιδιαίτερα προσεχτικοί πρέπει να είναι και οι σύνεδροι, καθώς ένας φορητός υπολογιστής ή και τα δεδομένα του μπορεί να κλαπούν εύκολα όταν υπάρχει πολυκοσμία.

5.6 Προστασία προσωπικών εγγράφων

Μεγάλη σημασία πρέπει να δοθεί στην μυστικότητα των προσωπικών εγγράφων. Τα έγγραφα πρέπει να φυλάσσονται σε ασφαλές μέρος, κατά προτίμηση σε ένα συρτάρι ή ντουλάπι που κλειδώνει.

Μια άλλη καλή ιδέα θα ήταν να φυλαχθούν τα πολύτιμα οικονομικά στοιχεία σε θυρίδα της τράπεζας. Εάν το διαβατήριο ή το δίπλωμα οδήγησης κάποιου κλαπούν ή χαθούν, πρέπει να ειδοποιήσει αμέσως την αρμόδια αρχή.

Ιδιαίτερα προσεχτικός πρέπει να είναι κάποιος με την αλληλογραφία του. Συγκεκριμένα δεν πρέπει να πετάει ολόκληρους λογαριασμούς, αποδείξεις, συνοδευτικά έγγραφα πιστωτικών καρτών, ακόμη και ανεπιθύμητη αλληλογραφία. Αντίθετα, θα πρέπει να τα καταστρέφει χρησιμοποιώντας καταστροφέα εγγράφων.

Ακόμα πρέπει οι πελάτες τραπεζών, να ελέγχουν την κίνηση του λογαριασμού τους. Εάν υπάρχουν συναλλαγές τις οποίες δεν έχουν κάνει οι ίδιοι πρέπει να ειδοποιήσουν την τράπεζα αμέσως.

5.6.1 Καταστροφέας εγγράφων

Οι καταστροφείς εγγράφων (***βλ. εικ.16***) [45], χρησιμοποιούνται για να κόψουν το χαρτί σε κομμάτια συνήθως είτε σε λωρίδες, είτε σε κομφετί. Οι κυβερνητικοί οργανισμοί, οι εταιρείες καθώς και οι ιδιώτες χρησιμοποιούν τους καταστροφείς για να καταστρέψουν εμπιστευτικά και γενικά ευαίσθητα έγγραφα.

Οι ειδικοί στην ασφάλεια προσωπικών δεδομένων συνιστούν στο κόσμο, να καταστρέφει τους λογαριασμούς, τα φορολογικά έγγραφα, τις πιστωτικές κάρτες καθώς καθώς και κάθε παρόμοιο έγγραφο που μπορεί να χρησιμοποιηθεί από τους κλέφτες για να διαπράξουν απάτη ταυτότητας.

Εικόνα 16: Καταστροφέας εγγράφων με ενσωματωμένο καλάθι

[45] http://en.wikipedia.org/wiki/Paper_shredder

5.6.1.1 Τύποι καταστροφέων εγγράφων

Οι καταστροφείς εγγράφων υπάρχουν σε διάφορα μεγέθη και τιμές από μικρούς και οικονομικούς για την καταστροφή λίγων σελίδων μέχρι μεγάλες συσκευές που χρησιμοποιούνται από εταιρείες που προσφέρουν υπηρεσίες καταστροφής εγγράφων και κοστίζουν εκατοντάδες χιλιάδες δολάρια και μπορούν να καταστρέψουν εκατομμύρια εγγράφων την ώρα[46].

Ένας απλός καταστροφές λειτουργεί με ηλεκτρικό ρεύμα αλλά υπάρχουν και συσκευές που δεν απαιτούν την χρήση ρεύματος, όπως τα ειδικά ψαλίδια με πολλαπλές λεπίδες (***βλ. εικ.17***).

Εικόνα 17: Ειδικό ψαλίδι καταστροφής εγγράφων

Αυτές οι μηχανές κατηγοριοποιούνται σύμφωνα με το μέγεθος και το σχήμα των κομματιών χαρτιού που παράγουν. Όσον αφορά το μέγεθος, υπάρχουν καταστροφείς στο μέγεθος ενός ψαλιδιού και άλλοι που έχουν μέγεθος αυτοκινήτου.

Όσον αφορά το είδος κοπής υπάρχουν πολλοί τύποι με τους βασικότερους να είναι τρεις:

- Υπάρχουν καταστροφείς που κόβουν σε λωρίδες. Αυτή είναι η λιγότερο ασφαλής επιλογή, καθότι ένας αποφασισμένος ‘ερευνητής’ μπορεί να ξανά συναρμολογήσει τα κομμάτια.

- Υπάρχουν καταστροφείς που κόβουν χιαστί ή σε κομφετί.

- Υπάρχουν αυτοί που κόβουν το χαρτί σε πολύ μικρά τετράγωνα ή στρογγυλά κομματάκια.

Οι παραπάνω τρεις τύποι είναι οι περισσότεροι διαδεδομένοι στο εμπόριο αλά όταν απαιτείται μεγαλύτερη ασφάλεια, υπάρχουν και άλλοι τύποι καταστροφέων οι οποίοι κυριολεκτικά διαλύουν το χαρτί σε κομμάτια τόσο μικρά όσο οι κόκκοι της σκόνης.

5.6.1.2 Καινοτομίες στους καταστροφείς

Όσο αυξάνονται οι απατήσεις στην βιομηχανία των καταστροφέων, οι κατασκευαστές αναπτύσσουν συνεχώς νέα χαρακτηριστικά που βελτιώνουν την αποτελεσματικότητα, την ευκολία χρήσης και την ασφάλεια των συσκευών τους.

[46] http://en.wikipedia.org/wiki/Paper_shredder

Υπάρχουν, λοιπόν, σήμερα καταστροφείς που ανιχνεύουν το πάχος του χαρτιού για να αποφύγουν τα κολλήματα όταν η ποσότητα του χαρτιού είναι παραπάνω από την επιτρεπτή.

Υπάρχουν άλλοι που διαθέτουν αισθητήρα και σβήνουν αυτόματα όταν τα χέρια πλησιάζουν κοντά στην τροφοδοσία του χαρτιού.

Ακόμη, υπάρχουν αυτοί που έχουν αθόρυβη λειτουργία και αυτοί που μπαίνουν σε κατάσταση αναμονής όταν δεν χρησιμοποιούνται, κάνοντας οικονομία στο ρεύμα.

Τέλος, υπάρχουν αυτοί που διαθέτουν αυτοκαθαριζόμενους κόπτες για να αποφύγουν τη συγκέντρωση κομματιών χαρτιού.

5.7 Προστασία πιστωτικών καρτών

Εάν η πιστωτική κάρτα κάποιου χαθεί ή κλαπεί πρέπει να ακυρωθεί αμέσως. Πρέπει κάποιος να έχει εύκαιρους τους αριθμούς που πρέπει να καλέσει στην περίπτωση αυτή.

Σημαντικό είναι όταν κάποιος δίνει τις πληροφορίες της κάρτας του ή όποιου άλλου είδους προσωπικά στοιχεία (μέσω τηλεφώνου, Διαδικτύου ή σε δημόσιο χώρο) να προσέχει ώστε οι άλλοι να μην ακούν ή να βλέπουν τις πληροφορίες αυτές.

Τέλος, προσωπικά έγγραφα και πιστωτικές κάρτες δεν πρέπει να μεταφέρονται από το κάτοχό τους άσκοπα. Όταν δεν χρησιμοποιούνται πρέπει να φυλάσσονται σε ασφαλές μέρος.

Παράδειγμα: *Εχεμύθεια και Προστασία Δεδομένων Προσωπικού Χαρακτήρα*[47]

citibank
Ελλάδα

Σας καλωσορίζουμε στην ιστοσελίδα της Citibank. Σκοπός μας είναι να προστατεύσουμε τα προσωπικά στοιχεία σας στο Διαδίκτυο με τον ίδιο τρόπο που τα προστατεύουμε σε κάθε περίπτωση που συναλλάσσεστε μαζί μας: στα καταστήματα, στα ATM και στο τηλέφωνο.

Εχεμύθεια της Citibank για το Διαδίκτυο:

- *Μπορείτε να επισκέπτεστε την ιστοσελίδα της Citibank και να πληροφορείστε τα προϊόντα και τις υπηρεσίες μας, να διαβάσετε τις εταιρικές ανακοινώσεις μας, να ενημερωθείτε για την ζήτηση σε νέες θέσεις εργασίας ή να χρησιμοποιήσετε οποιαδήποτε άλλη υπηρεσία, χωρίς να μας δώσετε πληροφορίες που σας αφορούν.*

[47] http://www.citibank.com/greece/homepage/index.htm

- *Αν μας δώσετε πληροφορίες που αφορούν προσωπικά στοιχεία σας, σας προτρέπουμε να διαβάσετε τους "όρους εχεμύθειας του ομίλου Citi για τους ιδιώτες."*

Για την καλύτερη εξυπηρέτησή σας ή για λόγους ασφαλείας, θα χρησιμοποιούμε σε κάποιες περιπτώσεις ένα "cookie". Το cookie είναι μια πληροφορία την οποία μια ιστοσελίδα μπορεί να αποθηκεύσει στην εφαρμογή πλοήγησης / browser που έχετε εγκαταστήσει στον υπολογιστή σας και στη συνέχεια να ανακτηθεί. Το cookie δεν μπορεί να χρησιμοποιηθεί από άλλη ιστοσελίδα εκτός από εκείνη που το δημιούργησε.

Χρησιμοποιούμε τα cookies για να προσφέρουμε καλύτερη εξυπηρέτηση όπως π.χ. για να καταγράψουμε το ενδιαφέρον σας για ενημέρωση σε προϊόντα μας ή για να αποθηκεύσουμε κάποιον κωδικό σας, ώστε να μην χρειάζεται να τον πληκτρολογείτε κάθε φορά που επισκέπτεστε την ιστοσελίδα μας. Τα περισσότερα cookies διατηρούνται μόνο όσο διαρκεί η επίσκεψη σας στην ιστοσελίδα μας.

Σε καμμία περίπτωση τα cookies δεν περιέχουν πληροφορίες που θα επιτρέψουν σε οποιονδήποτε να επικοινωνήσει μαζί σας μέσω τηλεφώνου, e-mail, ή με άλλο μέσο. Μπορείτε να ρυθμίσετε την εφαρμογή πλοήγησης / browser που χρησιμοποιείτε, ώστε να σας ειδοποιεί κάθε φορά που σας αποστέλλονται cookies, ώστε να τα αποφεύγετε.

Προστασία δεδομένων προσωπικού χαρακτήρα κατά τις μεταφορές κεφαλαίων μέσω SWIFT

Η Citibank International plc σας ενημερώνει ότι, εφόσον για την ολοκλήρωση της συναλλαγής χρησιμοποιηθούν οι υπηρεσίες της SWIFT (Society of Worldwide Interbank Financial Telecommunication), που εδρεύει στο Βέλγιο (διαδικτυακός τόπος www.swift.com), τα δεδομένα που αφορούν στη συναλλαγή θα διαβιβαστούν σε αυτή, η οποία στη συνέχεια τα διαβιβάζει για λόγους ασφαλείας σε εφεδρικό αρχείο (back up) που τηρεί στις ΗΠΑ.

Στο αρχείο αυτό, στο οποίο καταχωρούνται όμοια δεδομένα από τις Τράπεζες όλων των κρατών μελών της Ευρωπαϊκής Ένωσης, δικαίωμα πρόσβασης έχουν αρχές των ΗΠΑ (όπως το Υπουργείο Οικονομικών), με σκοπό την καταπολέμηση της τρομοκρατίας και της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.

5.8 Προστασία προσωπικών στοιχείων των αποθανόντων

Πολλές φορές οι απατεώνες χρησιμοποιούν την ταυτότητα ενός ανθρώπου που έχει πεθάνει. Αυτό εκτός μακάβριο μπορεί να βάλει τους συγγενείς του νεκρού σε μπελάδες, να προσπαθούν δηλαδή να ξεκαθαρίσουν τις ανοιχτές υποθέσεις που έχει αφήσει ο απατεώνας.

Αξίζει να σημειωθεί ότι στην Αμερική υπάρχουν πάνω από 400.000 λογαριασμοί επιταγών που έχουν ανοιχτεί στο όνομα αποθανόντων. Αυτό μπορεί να αντιμετωπιστεί με δύο τρόπους.

Ο ένας είναι να γίνει ένας έλεγχος στο όνομα του αποθανόντος, αρκετές εβδομάδες μετά το θάνατο, για να διαπιστωθεί εάν υπάρχουν συναλλαγές που φαίνεται να έχουν γίνει από αυτόν.

Ο άλλος είναι (εφαρμόζεται ήδη σε μερικές χώρες του κόσμου) να εκδίδεται μία λίστα μηνιαία με τα ονόματα των αποθανόντων και να αποστέλλεται στις τράπεζες, ώστε να μην μπορεί να πραγματοποιηθεί συναλλαγή με χρήση των ονομάτων αυτών.

5.9 Προστασία ατομικής ταυτότητας

Η απόκτηση προσωπικών στοιχείων από τους εγκληματίες μπορεί να γίνει με διάφορους τρόπους. Μπορεί να οφείλεται στην άγνοια των καταναλωτών που δίνουν τα στοιχεία τους σε λάθος ανθρώπους ή ακόμα μπορεί οι ίδιοι οι απατεώνες να τα κλέψουν με φυσικό τρόπο.

Η προστασία των προσωπικών δεδομένων είναι μια υποχρέωση του καταναλωτή απέναντι στον εαυτό του. Ο καλύτερος τρόπος να προστατευθεί κάποιος από την κλοπή ταυτότητας, είναι να μην δώσει καθόλου τα στοιχεία του εάν δεν είναι απαραίτητο.

Στη σημερινή κοινωνία όμως είναι πολλές οι περιπτώσεις όπου κάποιος θα χρειαστεί να δώσει τα πλήρη στοιχεία του, ακόμη και τα πιο ευαίσθητα. Θα ήταν καλύτερα ευαίσθητα στοιχεία να μην δίνονται μέσω τηλεφώνου ή να στέλνονται μέσω ηλεκτρονικού ταχυδρομείου.

Ακόμα ο καταναλωτής όταν συναλλάσσεται μέσω Διαδικτύου, θα πρέπει να είναι σίγουρος ότι ο υπολογιστής του είναι επαρκώς προστατευμένος από κακόβουλο λογισμικό π.χ. spyware. Γενικά, ο καταναλωτής θα πρέπει να προσέχει που δίνει τα στοιχεία του και πως τα μεταβιβάζει.

5.10 Προστασία προσωπικού υπολογιστή[48]

- **Ξεκινώντας: Εντοπίζοντας και εξουδετερώνοντας τις απειλές**

    - Το πρώτο βήμα για την προστασία του προσωπικού υπολογιστή είναι η χρήση ενός τείχους ασφαλείας (firewall), το οποίο αποτρέπει τις διάφορες απειλές από το να εισέλθουν στον υπολογιστή ενώ ταυτόχρονα αφήνει τις ασφαλείς πληροφορίες να περάσουν μέσα.

    - Επειδή, όμως, το κακόβουλο λογισμικό πάντα βρίσκει το δρόμο του για το σκληρό δίσκο του υπολογιστή μας, το τείχος ασφαλείας δεν επαρκεί. Χρειάζεται και ένα πρόγραμμα προστασίας από ιούς, στο οποίο πρέπει να γίνεται αναβάθμιση σε τακτική βάση.

[48] http://www.itsecurity.com/features/20-minute-guide-pc-security-021307

- Το τείχος προστασίας και τα anti-virus είναι οι βασικοί τρόποι προστασίας του υπολογιστή από τις απειλές. Υπάρχει και ένας τρίτος τύπος προγραμμάτων ο οποίος μπορεί να κάνει την διαφορά στην ασφάλεια του προσωπικού υπολογιστή. Αυτά τα προγράμματα είναι τα anti-spyware.

- Εκτός από τα τρία αναφερθέντα, υπάρχουν και άλλα προγράμματα τα οποία μπορεί να συμβάλλουν στην ασφάλεια του προσωπικού υπολογιστή. Παράδειγμα τέτοιων προγραμμάτων είναι αυτά που ανιχνεύουν τα Rootkits.

- **Κατάλληλες αναβαθμίσεις και ρυθμίσεις**

  - Το πρώτο βήμα είναι η επιλογή ενός ασφαλούς browser. Μερικοί browser είναι πιο ανθεκτικοί στις απειλές σε σχέση με άλλους (π.χ. Mozilla Firefox σε σχέση με τον Internet Explorer της Microsoft). Στη συνέχεια, μπορούν να προσαρμοστούν οι ρυθμίσεις ασφαλείας του προγράμματος σε υψηλότερο επίπεδο.

  - Για την ενίσχυση της ασφάλειας του υπολογιστή οι χρήστες πρέπει να κατεβάσουν το τελευταίο Service Pack του υπολογιστή.

  - Ένα άλλο μέτρο είναι η επιλογή ασφαλούς software αξιόπιστης προέλευσης και τακτική αναβάθμισή του.

  - Θα βοηθούσε η απενεργοποίηση του διαμοιρασμού των αρχείων. Αυτό είναι ιδιαίτερα χρήσιμο σε περιπτώσεις που υπάρχει ένα ανοιχτό ασύρματο δίκτυο όπου πρέπει να απαγορευθεί η πρόσβαση σε αγνωστους υπολογιστές.

  - Ένα από τα βασικότερα μέτρα προστασίας πηγάζει από τον ίδιο το χρήστη του υπολογιστή ο οποίος πρέπει να είναι ιδιαίτερα προσεχτικός όταν κατεβάζει αρχεία από το Διαδίκτυο. Πρέπει να γνωρίζει τι κατεβάζει και από πού το κατεβάζει.

- **Ασφάλεια του Ηλεκτρονικού ταχυδρομείου**

  - Το πρώτο βήμα για την προστασία του ηλεκτρονικού ταχυδρομείου είναι η χρήση ενός e-mail client, που παρέχει υψηλά επίπεδα ασφάλειας. Παραδείγματα τέτοιων client, είναι το Google Mail (web-based) και ο Thunderbird της Mozilla (standalone).

  - Οι χρήστες πρέπει να διαχειρίζονται τα συνημμένα με προσοχή. Όταν κάποιος κατεβάζει ένα συνημμένο, το firewall υποθέτει ότι ο χρήστης γνωρίζει τι κάνει και κατά συνέπεια δεν θα τον προστατέψει. Αξίζει να σημειωθεί ότι 90% των ιών, μπαίνουν στον υπολογιστή με τέτοιο τρόπο.

  - Δεν πρέπει κάποιος να κάνει απερίσκεπτα κλικ σε συνδέσμους που περιέχονται σε e-mail. Πολλές φορές οι απατεώνες θα παρουσιάζονται ως κάποιοι άλλοι στο e-mail και ο σύνδεσμος θα οδηγεί το χρήστη σε μία μη ασφαλή τοποθεσία.

- Παρόλο που οι παροχείς υπηρεσιών Διαδικτύου και το φιλτράρισμα του e-mail client μπορούν να μειώσουν δραματικά τον αριθμό των spam e-mail, μπορεί να εγκατασταθούν πρόσθετα φίλτρα για τον εκμηδενσμό των παραπάνω.

- **Προστασία των Password**

  - Ένα password θα πρέπει να είναι πρωτότυπο και δύσκολο. Με αυτό τον τρόπο θα αντιμετωπιστούν οι επιθέσεις των hackers οι οποίοι χρησιμοποιούν προγράμματα τα οποία δοκιμάζουν τα πιο συχνα χρησιμοποιούμενα passwords.

  - Πολύ σημαντικό, επίσης, για τον καθένα είναι να χρησιμοποιεί διαφορετικά password σε κάθε λογαριασμό, έτσι εάν διαρρεύσει το password ενός λογαριασμού, ο επιτιθέμενος δεν θα έχει πρόσβαση σε όλους τους λογαριασμούς του θύματος.

  - Παρόλο που πολλοί ψάχνουν δύσκολα password για τις online υπηρεσίες, ξεχνούν να προστατέψουν την πρόσβαση στον υπολογιστή τους με κάποιο password.

- **Προστασία ασύρματου δικτύου**

  - Είναι σημαντικό κάποιος να προστατέψει το δίκτυό του από μη εξουσιοδοτημένη χρήση. Για να γίνει αυτό, θα πρέπει πρώτα απ’όλα να αλλαχτεί το όνομα του δικτύου αφού οι hackers θα θεωρήσουν εύκολο στόχο ένα δίκτυο που έχει ως όνομα, π.χ. την μάρκα του router. Ακόμα, το κλειδί WEP δεν θεωρείται πλέον αποτελεσματικό. Πρέπει το ασύρματο δίκτυο να αναβαθμιστεί ώστε να υποστηρίζει το πρότυπο WPA2.

  - Δεν πρέπει κάποιος να ψάχνει στη γειτονιά του για αφύλακτα ασύρματα δίκτυα. Υπάρχει πιθανότητα το δίκτυο που θα βρει να μην ανήκει σε κάποιον απρόσεκτο γείτονα αλλά να έχει στηθεί από κάποιο hacker σαν παγίδα για να αποκτήσει πρόσβαση στο laptop.

- **Φυσική προστασία φορητού υπολογιστή**

  - Για να αποτραπεί η κλοπή του φορητού υπολογιστή σε κάποιο δημόσιο χώρο, θα μπορούσε να χρησιμοποιηθεί μία λιγότερο εμφανής τσάντα μεταφοράς. Οι τσάντες των laptop προσελκύουν τους επίδοξους κλέφτες σε αντίθεση με τις περισσότερο συμβατικές τσάντες, π.χ. τις σχολικές ή τις αθλητικές.

  - Μπορούν να χρησιμοποιηθούν και αντικλεπτικές λύσεις όπως τα αυτοκόλλητα ασφαλείας που ουσιαστικά δηλώνουν σε ποιον ανήκει το laptop και το software εντοπισμού, το οποίο θα ειδοποιήσει μία προκαθορισμένη βάση για την τοποθεσία του, όταν ο κλέφτης μπει στο Internet.

5.11 Προστασία ατομικής ταυτότητας από οργανισμούς

Το Μάιο του 1998 η ομοσπονδιακή ένωση εμπορίου των Η.Π.Α. συζήτησε το θέμα της πώλησης αριθμών ταυτότητας και άλλων προσωπικών στοιχείων από οργανισμούς που τα κατείχαν. Η ένωση εμπορίου αποφάσισε να περιοριστεί η πρόσβαση στις πιστωτικές αναφορές.

Όμως και η κακή διαχείριση των προσωπικών στοιχείων από διάφορους οργανισμούς μπορεί να καταστήσει τους πελάτες υποψήφια θύματα απάτης.

Όταν λέμε κακή διαχείριση εννοούμε:

- να πετάγονται εμπιστευτικά έγγραφα χωρίς πρώτα να έχουν καταστραφεί.
- Να μην υπάρχει επαρκής προστασία του δικτύου του οργανισμού
- Η κλοπή σταθερών 'η φορητών υπολογιστών που περιέχουν ευαίσθητα δεδομένα, το καλύτερο είναι σε αυτήν την περίπτωση τα δεδομένα να έχουν κρυπτογραφηθεί
- Όταν ένας οργανισμός μεταβιβάζει προσωπικά στοιχεία πελατών του σε δεύτερο οργανισμό, και ο δεύτερος αυτός οργανισμός να μην διαθέτει σωστή διαχείριση των δεδομένων

Ένας τρόπος αντιμετώπισης των παραπάνω φαινομένων είναι η χρήση βιομετρικών στοιχείων για την ταυτοποίηση των ατόμων. Υπάρχουν βέβαια διάφορες αμφιβολίες ως προς την αποτελεσματικότητα και αυτών των μεθόδων.

Κεφάλαιο 6 Νομικό καθεστώς σε σχέση με την προστασία προσωπικών στοιχείων

6.1 Προστασία προσωπικών δεδομένων

6.1.1 Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα (ΑΠΔΠΧ)

Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί θεμελιώδες ανθρώπινο δικαίωμα[49]. Ο νόμος παρέχει ορισμένα δικαιώματα στα φυσικά πρόσωπα (τα υποκείμενα των δεδομένων) και θέτει συγκεκριμένες υποχρεώσεις σε όσους τηρούν και επεξεργάζονται προσωπικά δεδομένα (τους υπευθύνους επεξεργασίας).

6.1.1.1 Σκοπός της Αρχής

Ο σεβασμός και η προστασία της αξιοπρέπειας, της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας αποτελούν θεμελιώδη και πρωταρχική επιδίωξη κάθε δημοκρατικής κοινωνίας[50]. Με την πάροδο του χρόνου, η τεράστια πρόοδος στον τομέα της πληροφορικής, η ανάπτυξη νέων τεχνολογιών, οι νέες μορφές διαφήμησης και ηλεκτρονικών συναλλαγών και η ανάγκη της ηλεκτρονικής οργάνωσης του κράτους έχουν σαν συνέπεια την αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα.

Η ανεξέλεγκτη καταχώριση και επεξεργασία των προσωπικών δεδομένων σε ηλεκτρονικά και χειρόγραφα αρχεία υπηρεσιών, εταιρειών και οργανισμών μπορεί να προκαλέσει προβλήματα στην ιδιωτική ζωή του πολίτη.

Οι κίνδυνοι αυτοί αυξάνονται με τις νέες δυνατότητες ταχύτατης επεξεργασίας εκατομμυρίων δεδομένων μέσω ηλεκτρονικού υπολογιστή και μεταφοράς πληροφοριών παγκοσμίως μέσω του Διαδικτύου. Αποθήκευση και έρευνα μεγάλου όγκου δεδομένων που παλαιότερα θα απαιτούσε μεγάλους αποθηκευτικούς χώρους και επίπονη εργασία έχει πλέον απλοποιηθεί και γίνεται πολύ πιο εύκολα και ανέξοδα.

Για την προστασία του ατόμου στην κοινωνία της πληροφορίας δεν επαρκούν οι παραδοσιακές θεσμικές εγγυήσεις και ρυθμίσεις, αλλά χρειάζεται ειδική αντιμετώπιση. Για τον σκοπό αυτό στην Ελλάδα ιδρύθηκε με τον Νόμο 2472/1997 ως ανεξάρτητος διοικητικός φορέας η *ΑΠΔΠΧ*, η οποία λειτουργεί από τον Νοέμβριο του 1997.

---

[49] http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL

[50] http://el.wikipedia.org/wiki/%CE%91%CF%81%CF%87%CE%AE_%CE%A0%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD_%CE%A0%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%BF%CF%8D_%CE%A7%CE%B1%CF%81%CE%B1%CE%BA%CF%84%CE%AE%CF%81%CE%B1#.CE.97.CE.BC.CE.AD.CF.81.CE.B1_.CE.A0.CF.81.CE.BF.CF.83.CF.84.CE.B1.CF.83.CE.AF.CE.B1.CF.82_.CE.A0.CF.81.CE.BF.CF.83.CF.89.CF.80.CE.B9.CE.BA.CF.8E.CE.BD_.CE.94.CE.B5.CE.B4.CE.BF.CE.BC.CE.AD.CE.BD.CF.89.CE.BD

Άλλες αρχές που εποπτεύουν την επεξεργασία προσωπικών δεδομένων είναι στην Ελλάδα η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και στην Ευρώπη ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων.

6.1.2 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών είναι μια από τις συνταγματικά καθιερωμένες Ανεξάρτητες Αρχές με διοικητική αυτοτέλεια, η οποία συστάθηκε ως ειδικός εποπτεύοντας φορέας για να προστατεύσει το απόρρητο της επικοινωνίας.

Η Α.Δ.Α.Ε. στο πλαίσιο των αρμοδιοτήτων της, οι οποίες περιγράφονται παρακάτω, έχει σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο. Επιπλέον, στις αρμοδιότητές της, περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου που προβλέπονται από το νόμο.

Ποιες είναι οι σημαντικότερες αρμοδιότητες της Α.Δ.Α.Ε.;

Η Α.Δ.Α.Ε. για την εκπλήρωση του σκοπού της σύμφωνα με το νόμο μπορεί:

- Να εκδίδει κανονισμούς, να γνωμοδοτεί και να απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων προστασίας του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

- Να διενεργεί αυτεπάγγελτα ή έπειτα από καταγγελία τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.

- Να συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς ή διεθνείς οργανισμούς.

Στα πλαίσια αυτά η Αρχή έχει εκδώσει κανονισμούς οι οποίοι προβλέπουν πολιτικές ασφάλειας που θα πρέπει να εφαρμόζουν οι εταιρείες παροχής επικοινωνιακών υπηρεσιών και παρακολουθεί με ελέγχους την εφαρμογή τους για την προστασία του απορρήτου των επικοινωνιών.

Επιπλέον, οι χρήστες και οι συνδρομητές ηλεκτρονικών επικοινωνιών και ταχυδρομικών υπηρεσιών μπορούν να υποβάλλουν καταγγελίες στην Αρχή, όταν αντιληφθούν ότι υπάρχει παραβίαση του απορρήτου των επικοινωνιών τους.

Η Α.Δ.Α.Ε. διερευνά τις καταγγελίες αυτές προκειμένου να διαπιστώσει την πιθανή παραβίαση του απορρήτου και την ευθύνη την οποία φέρει ο εμπλεκόμενος πάροχος τηλεπικοινωνιακών ή ταχυδρομικών υπηρεσιών.

Σε περίπτωση που κατά τον έλεγχο της καταγγελίας διαπιστωθεί παραβίαση του απορρήτου, η Α.Δ.Α.Ε. μπορεί να επιβάλει διοικητικά πρόστιμα, να κατασχέσει τα μέσα με τα οποία πραγματοποιείται η παραβίαση αυτή, ενώ παράλληλα καταστρέφει τις πληροφορίες, τα δεδομένα ή τα στοιχεία που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.

6.1.2.1 Ποιοι προστατεύουν το απόρρητο των επικοινωνιών

Σύμφωνα με τις κατευθυντήριες γραμμές ασφάλειας του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) και της Ευρωπαϊκής Ένωσης, η ασφάλεια των τηλεπικοινωνιακών δικτύων και πληροφοριών αποτελεί ευθύνη όλων των ενδιαφερόμενων μερών.

Με άλλα λόγια, τα μέτρα που λαμβάνει η Πολιτεία και οι εταιρείες παροχής υπηρεσιών επικοινωνιών για την ασφάλεια των επικοινωνιών είναι απαραίτητο να συμπληρώνονται από την εφαρμογή κανόνων ασφαλείας από τους ίδιους τους χρήστες και συνδρομητές ηλεκτρονικών επικοινωνιών για τη δική τους πρωτίστως προστασία.

Η πλήρης επίγνωση των κινδύνων και των διαθέσιμων μέσων ασφαλείας σε προσωπικό επίπεδο αποτελεί την πρώτη γραμμή άμυνας για την ασφάλεια συστημάτων, πληροφοριών και δικτύων.

Κρίσιμο ρόλο στην προστασία του απορρήτου των επικοινωνιών διαδραματίζουν :

• Η Πολιτεία

Η Πολιτεία θεσπίζει το κατάλληλο θεσμικό πλαίσιο, το οποίο προσαρμόζει στις εκάστοτε τεχνολογικές εξελίξεις, για την προάσπιση του απορρήτου των επικοινωνιών.
Στα πλαίσια του παραπάνω θεσμικού πλαισίου δημιουργήθηκε η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), κατ' εντολή του άρθρου 19 παρ. 2 του Συντάγματος.

• Οι εταιρείες παροχής υπηρεσιών επικοινωνιών

(ηλεκτρονικών επικοινωνιών, παροχής δικτύου & ταχυδρομικών υπηρεσιών)
Οι εταιρείες αυτές οφείλουν να προστατεύουν το απόρρητο των επικοινωνιών για τις υπηρεσίες που παρέχουν και να ενημερώνουν τους χρήστες συνδρομητές τους για πιθανούς κινδύνους και τα ενδεικνυόμενα μέτρα αυτοπροστασίας.

• Οι χρήστες και οι συνδρομητές ηλεκτρονικών επικοινωνιών

Οι χρήστες και οι συνδρομητές ηλεκτρονικών επικοινωνιών πρέπει να λαμβάνουν τα απαραίτητα μέτρα αυτοπροστασίας.

6.1.2.2 Τι θεωρείται απόρρητο στις επικοινωνίες

Μερικά βασικά στοιχεία που καλύπτει η νομοθεσία περί απορρήτου των επικοινωνιών είναι:

- Για τις ηλεκτρονικές επικοινωνίες
    - Το περιεχόμενο της επικοινωνίας (φωνή, εικόνα, δεδομένα)
    - Η ταυτότητα του καλούντος και του καλουμένου
    - Η ταυτότητα του αποστολέα και του παραλήπτη ηλεκτρονικού ταχυδρομείου
- Τα δεδομένα θέσης της τερματικής συσκευής (γεωγραφικός εντοπισμός)
- Για τις ταχυδρομικές υπηρεσίες
    - Το περιεχόμενο της αλληλογραφίας
    - Ο αποστολέας
    - Ο παραλήπτης

6.1.2.3 Ποιες είναι οι περιοχές ευθύνης παροχών και χρηστών/συνδρομητών ηλεκτρονικών επικοινωνιών

Οι πάροχοι ηλεκτρονικών επικοινωνιών είναι υπεύθυνοι για τη διασφάλιση του απορρήτου των επικοινωνιών στο δημόσιο τηλεπικοινωνιακό δίκτυο (δίκτυα κορμού και πρόσβασης)[51]. Οι συνδρομητές και οι χρήστες οφείλουν να μεριμνούν για το απόρρητο της επικοινωνίας στα ιδιωτικά δίκτυα τα οποία περιλαμβάνουν τις καλωδιώσεις στα κτίρια, τα εσωτερικά δίκτυα (LAN) και τις τερματικές συσκευές (σταθερά ενσύρματα και ασύρματα τηλέφωνα, κινητά τηλέφωνα, fax, προσωπικοί υπολογιστές). Ακολουθούν μέτρα αυτοπροστασίας για τις πλέον διαδεδομένες μορφές επικοινωνίας.

6.2 Πολιτική απορρήτου

Πολιτική απορρήτου είναι ένα νομικό έγγραφο[52], που περιγράφει πώς ένας οργανισμός διατηρεί, επεξεργάζεται και αποκαλύπτει τα στοιχεία των πελατών. Τέτοιο παράδειγμα θα μπορούσε να είναι το κομμάτι μιας ιστοσελίδας, που παρέχει πληροφορίες για την χρήση των προσωπικών δεδομένων από τον ιδιοκτήτη της σελίδας.

Οι πολιτικές απορρήτου συνήθως, περιέχουν λεπτομέρειες για το είδος των προσωπικών πληροφοριών που συλλέγονται, πώς μπορούν να χρησιμοποιηθούν τα δεδομένα αυτά, αν πρόκειται να αποκαλυφθούν σε κάποιον και σε ποιον, τα μέτρα ασφαλείας που παίρνονται για την προστασία τους και εάν η ιστοσελίδα χρησιμοποιεί cookies.

---

[51] http://www.adae.gr/adae/viewarticle.html?langid=el&articleid=129
[52] http://en.wikipedia.org/wiki/Privacy_policy

Τα ακριβή περιεχόμενα μιας πολιτικής απορρήτου, εξαρτώνται από τον ισχύοντα νόμο. Για παράδειγμα, υπάρχουν σημαντικές διαφορές ανάμεσα στους σχετικούς νόμους της Ευρωπαϊκής Ένωσης και των Η.Π.Α..

Μερικές ιστοσελίδες καθορίζουν την πολιτική τους, χρησιμοποιώντας το P3P ή Internet Content Rating Association (ICRA). Έτσι, επιτρέπουν στον browser να εκτιμήσει αυτόματα το επίπεδο του απορρήτου που προσφέρεται από την σελίδα.

6.2.1 Κύρια σημεία μιας πολιτικής απορρήτου[53]

Οι περισσότερες πολιτικές απορρήτου ξεκινούν με μία παράγραφο που αποτελεί εισαγωγή στο έγγραφο. Συνήθως, υπάρχει ένα μήνυμα από τον οργανισμό, το οποίο δηλώνει την πρόθεσή του να προστατέψει τα προσωπικά δεδομένα των πελατών.

Στην επόμενη παράγραφο της πολιτικής απορρήτου, περιγράφεται ο τύπος των πληροφοριών που συλλέγεται. Ο οργανισμός παραθέτει αναλυτικά τα προσωπικά στοιχεία που θα ζητήσει από έναν πελάτη, για να του παρέχει μια υπηρεσία. Ακόμα, ίσως υπάρχουν διευκρινήσεις για το πώς πρέπει να δοθούν οι πληροφορίες ή για τυχόν άλλες δυνατότητες που έχει ο πελάτης (π.χ. αν μπορεί να δώσει τα στοιχεία κάποιου άλλου ατόμου για να του στείλει ένα δώρο).

Στη συνέχεια, αναλύονται οι πιθανές χρήσεις των προσωπικών δεδομένων. Ο οργανισμός ενημερώνει τους υποψήφιους πελάτες για το πώς προτίθεται να χρησιμοποιήσει τα προσωπικά τους στοιχεία.

Οι περισσότεροι οργανισμοί διαβεβαιώνουν το κοινό ότι χρειάζονται τα προσωπικά στοιχεία μόνο για την ολοκλήρωση συναλλαγών με τους πελάτες και δεν τα μοιράζονται με κανένα άλλο οργανισμό ή φορέα. Πρέπει ακόμη να αναφέρεται εάν θα χρησιμοποιηθούν για την αποστολή διαφημιστικού υλικού ή όχι.

Άλλη μια παράγραφος που υπάρχει σίγουρα είναι αυτή που αναφέρει τα μέτρα που παίρνει ο οργανισμός για να διασφαλίσει το απόρρητο των πληροφοριών που συλλέγονται μέσω διαδικτύου.

Στο προ τελευταίο τμήμα του εγγράφου ενημερώνονται οι υποψήφιοι πελάτες για τους τρόπους με τους οποίους μπορούν να δουν και να κάνουν αλλαγές στα προσωπικά τους στοιχεία.

Στην τελευταία παράγραφο συνήθως υπάρχουν οι τρόποι επικοινωνίας με τον οργανισμό, κυρίως για θέματα που έχουν να κάνουν με την διαφύλαξη των πληροφοριών. Παρατίθενται τηλεφωνικός αριθμός και διεύθυνση e-mail.

Ίσως σε κάποιο σημείο του εγγράφου, να υπάρχει και μία παράγραφος που ασχολείται με την προστασία των παιδιών και των ανηλίκων. Πιο συγκεκριμένα, μπορεί να αναφέρεται ότι η σελίδα είναι κατασκευασμένη ώστε να μην ελκύει παιδιά και επίσης ότι ο οργανισμός δεν κρατάει στοιχεία ατόμων που γνωρίζει πως είναι ανήλικα. Ένα παράδειγμα πολιτικής απορρήτου[54], υπάρχει στο **Παράρτημα Α.**

[53] http://www.bbbonline.org/privacy/sample_privacy.asp
[54] http://www.e-shop.gr/protection.phtml

6.2.2 Ευθύνη των εταιρειών και των οργανισμών

Οι οργανισμοί επεξεργάζονται πληροφορίες που μπορεί να θεωρηθούν ευαίσθητες είτε από επιχειρηματική είτε από νομική άποψη[55]. Εκτός από τον κίνδυνο εισβολής και απόκτησης δεδομένων από μη εξουσιοδοτημένα άτομα, υπάρχει επίσης κίνδυνος ηθελημένης ή μη μετάβασης των πληροφοριών έξω από τον οργανισμό.

Η απώλεια μεγάλου όγκου προστατευμένων πληροφοριών είναι πλέον συνήθης και αναγκάζει τις εταιρείες να ξανά-εκδώσουν πιστωτικές κάρτες, να ειδοποιήσουν τους πελάτες και να αντιμετωπίσουν την δυσφήμηση.

Χαρακτηριστικά παραδείγματα οργανισμών που έχουν αποτύχει να προστατέψουν τα προσωπικά δεδομένα χρηστών είναι το **Facebook** και το **Google**. Συγκεκριμένα, το Facebook έχει αποτύχει και συνεχίζει να αποτυγχάνει στις παρακάτω περιπτώσεις[56]:

- **Διαρροή πηγαίου κώδικα**

  Τον Αύγουστο του 2007, ο κώδικας που δημιουργεί δυναμικά την αρχική σελίδα και τις σελίδες αναζήτησης, έγινε κατά λάθος γνωστός στο ευρύ κοινό. Ένα πρόβλημα στην ρύθμιση του server είχε σαν αποτέλεσμα να εμφανίζεται ο PHP κώδικας αντί για την κανονική σελίδα.

  Ένας επισκέπτης αντέγραψε και δημοσίευσε τον κώδικα σε ένα forum αλλά αργότερα τον αφαίρεσε μετά από προειδοποίηση για νομικές συνέπειες από τους ιθύνοντες. Ήταν τότε που γεννήθηκαν αμφιβολίες για την ασφάλεια των δεδομένων στο Facebook.

- **Παρακολούθηση και υπονόμευση ατόμων**

  Πολλοί έχουν εκφράσει την ανησυχία τους για την χρήση του Facebook ως μέσω παρακολούθησης, αφού μέσα από αυτό μπορεί να αποκαλυφθούν εύκολα πληροφορίες για την ζωή κάποιου. Υπάρχει έντονη κριτική ακόμα στην πολιτική απορρήτου του Facebook.

  Σύμφωνα με αυτήν, οι υπεύθυνοι του site, μπορούν να χρησιμοποιήσουν πληροφορίες που συλλέγουν για ένα μέλος από εξωτερικές πηγές, π.χ. εφημερίδες και να τις προσθέσουν στο προφίλ τους.

  Ακόμα, παραμένει ανοιχτό το ενδεχόμενο της παράνομης απόκτησης δεδομένων του Facebook από τρίτους. Αυτό το απέδειξαν δύο φοιτητές του MIT, που κατάφεραν να κατεβάσουν πάνω από 70000 προφίλ του Facebook ως μέρος μίας έρευνας για την ασφάλεια δεδομένων στο site.

---

[55] http://en.wikipedia.org/wiki/Data_Loss_Prevention.
[56] http://en.wikipedia.org/wiki/Criticism_of_Facebook#Privacy_concerns

Ένα άλλο σημείο της πολιτικής απορρήτου που προκάλεσε την έντονη αντίδραση πολλών χρηστών, είναι αυτό σύμφωνα με το οποίο το Facebook μπορεί να μοιραστεί τις πληροφορίες των μελών με τρίτους οργανισμούς που τους θεωρεί έμπιστους. Τελικά, αναγκάστηκαν να αφαιρέσουν το κομμάτι αυτό.

Ένα άλλο πρόβλημα είναι ότι εφαρμογές τρίτων έχουν πρόσβαση στις πληροφορίες των χρηστών και το Facebook δεν μπορεί να ελέγξει πώς αυτοί οι τρίτοι θα διαχειριστούν τα δεδομένα αυτά.

Τον Οκτώβριο του 2007, στο πρόγραμμα Watchdog του BBC, το Facebook παρουσιάστηκε ως ένας εύκολος τρόπος συλλογής πληροφοριών για ένα άτομο, με σκοπό την διάπραξη κλοπής ταυτότητας.

- **Αδυναμία διαγραφής δεδομένων**

  Το Facebook πάντα επέτρεπε στους χρήστες του να καταργήσουν τους λογαριασμούς τους, χωρίς όμως να αφαιρούνται τα περιεχόμενα του λογαριασμού από τους servers.

  Για να γίνει κάτι τέτοιο, πρέπει οι χρήστες να διαγράψουν χειροκίνητα όλα τα περιεχόμενα του λογαριασμού τους συμπεριλαμβανομένων των δημοσιεύσεων και των φίλων. Η μεγάλη προσπάθεια που απαιτείται για κάτι τέτοιο, αποτρέπει τους ανθρώπους από το να το κάνουν.

Όσον αφορά το **Google**[57], υπάρχουν τα παρακάτω προβλήματα:

- **Η χρήση Cookies**

  Το Google τοποθετεί ένα cookie στους εγγεγραμμένους χρήστες για να παρακολουθεί το ιστορικό των αναζητήσεων του κάθε ατόμου. Στην αρχή αυτό το cookie ήταν προγραμματισμένο να λήγει το 2038.

  Από το 2007 και μετά, το cookie αυτό, λήγει σε δύο χρόνια αλλά ανανεώνεται κάθε φορά που χρησιμοποιείται μια υπηρεσία του Google.

  Παρόλο που δεν υπάρχουν στοιχεία ότι το Google αποκαλύπτει πληροφορίες στο FBI και στο NSA, πολλοί χρήστες φοβούνται ότι κάτι τέτοιο δεν ισχύει.

- **Συγκέντρωση δεδομένων σε ένα μέρος**

  Όλα τα δεδομένα του Google, είναι συγκεντρωμένα σε μία κεντρική βάση δεδομένων. Σε αυτά περιλαμβάνονται όλες οι αναζητήσεις των χρηστών παγκοσμίως. Σύμφωνα με ένα αμφιλεγόμενο αμερικάνικο νόμο, το Google είναι υποχρεωμένο να παραδώσει όλες αυτές τις πληροφορίες στην αμερικανική κυβέρνηση, όποτε του ζητηθεί.

[57] http://en.wikipedia.org/wiki/Criticism_of_Google#Privacy

- **Πρόβλημα με το Gmail**

  Πολλοί πιστεύουν ότι η επεξεργασία των μηνυμάτων από την υπηρεσία Gmail του Google, γίνεται με ανορθόδοξο τρόπο. Η Google ισχυρίζεται ότι κανένας άνθρωπος πέραν του χρήστη του λογαριασμού, δεν διαβάζει τα μηνύματα που στέλνονται από ή προς το Gmail.

- **Αμφιβολίες για το "Street View"**

  Η διαδικτυακή υπηρεσία προβολής χαρτών Street View του Google, έχει κατηγορηθεί ότι τραβάει φωτογραφίες και πλησιάζει πολύ κοντά στα σπίτια των ανθρώπων και σε πεζούς που περπατούν στο δρόμο, χωρίς φυσικά να γνωρίζουν ότι παρακολουθούνται από μία υπηρεσία του Google.

  Ένα ζευγάρι από το Pittsburgh, μήνυσε το Google για παραβίαση προσωπικής ζωής. Ισχυρίστηκαν ότι το Street View, έβγαλε μία φωτογραφία του σπιτιού τους και την διέθεσε στο διαδίκτυο, ελαχιστοποιώντας έτσι την αξία του, αφού το είχαν αγοράσει επειδή ήταν απομονωμένο και ήσυχο. Τελικά, το ζευγάρι έχασε την δικαστική μάχη, αφού θεωρήθηκε ότι δεν προσεβλήθη η προσωπική τους ζωή.

6.2.3 Τύποι δεδομένων που πρέπει να προστατευτούν

Εκτός από τα προσωπικά στοιχεία κάποιου (π.χ. ταυτότητα), υπάρχουν και άλλοι τύποι προσωπικών δεδομένων που χρήζουν προστασίας[58].

- **Τρόπος ζωής**

  Για διάφορους λόγους οι άνθρωποι μπορεί να μην θέλουν να αποκαλυφθούν προσωπικές τους πληροφορίες, όπως το θρήσκευμα, οι σεξουαλικές προτιμήσεις, οι πολιτικές πεποιθήσεις, οι προσωπικές δραστηριότητες. Η αποκάλυψή τους μπορεί να οδηγήσει σε ρατσισμό, προσωπική ταπείνωση ή ζημιά στην καριέρα κάποιου.

- **Οικονομικές πληροφορίες**

  Οι πληροφορίες για τις οικονομικές συναλλαγές κάποιου, τα περιουσιακά του στοιχεία, τα χρέη και τις αγορές του, μπορεί να είναι ευαίσθητες. Εάν οι εγκληματίες αποκτήσουν πρόσβαση σε λογαριασμούς ή σε αριθμούς πιστωτικής κάρτας κάποιου, τότε το άτομο μπορεί να γίνει θύμα απάτης ή κλοπής ταυτότητας.

  Οι πληροφορίες για τις αγορές κάποιου, μπορεί να αποκαλύψουν πολλά για την ιστορία του ατόμου, π.χ. τα μέρη που έχει επισκεφθεί, τις επαφές που είχε, δραστηριότητες ή φάρμακα που πήρε.

[58] http://en.wikipedia.org/wiki/Data_protection

Σε μερικές περιπτώσεις οι εταιρείες μπορούν να χρησιμοποιήσουν τις πληροφορίες αυτές για να διαμορφώσουν μία στρατηγική προώθησης προϊόντων, για κάθε άτομο ξεχωριστά.

- **Απόρρητο του Internet**

Είναι σημαντικό να ελέγχει κάποιος τις πληροφορίες που αποκαλύπτει για τον εαυτό του, μέσω του Διαδικτύου καθώς και το ποιός θα έχει πρόσβαση στις πληροφορίες αυτές.

Ένα ερώτημα που υπάρχει είναι το αν τα e-mail, μπορούν να αποθηκευθούν ή να διαβαστούν από κάποιον τρίτο, ή αν αυτός ο τρίτος μπορεί να εντοπίσει τις ιστοσελίδες που έχει επισκεφθεί κάποιος.

Ένα άλλο ερώτημα είναι το αν οι ιστοσελίδες συλλέγουν, αποθηκεύουν και πιθανόν μοιράζονται προσωπικές πληροφορίες των χρηστών. Οι σημερινές μηχανές αναζήτησης καθώς και διάφοροι μέθοδοι υπονόμευσης επιτρέπουν την συλλογή στοιχείων για κάποιο άτομο από διάφορες πηγές.

- **Ιατρικό απόρρητο**

Ένα άτομο μπορεί να μην επιθυμεί το ιατρικό του μητρώο να αποκαλυφθεί σε άλλους. Αυτό μπορεί να επηρεάσει τις παροχές του ασφαλιστικού του φορέα ή την εργασία του. Η’ απλά κάποιος ντρέπεται να αποκαλύψει στους άλλους τη κατάσταση της σωματικής και ψυχολογικής του υγείας.

Με την αποκάλυψη των ιατρικών δεδομένων, μπορεί να έλθουν στο φως και άλλες πληροφορίες για την προσωπική ζωή κάποιου και κυρίως για την σεξουαλική του ζωή. Οι γιατροί στις περισσότερες χώρες, είναι υποχρεωμένοι να σέβονται το ιατρικό απόρρητο.

- **Πολιτικό απόρρητο**

Το πολιτικό απόρρητο υφίσταται σαν έννοια από τότε που ανακαλύφθηκε το σύστημα των ψήφων. Ο πιο απλός και διαδεδομένος τρόπος για να εξασφαλιστεί είναι η χρήση του παραβάν κατά την διάρκεια της ψηφοφορίας.

Στη σύγχρονη δημοκρατία το πολιτικό απόρρητο είναι δεδομένο και θεωρείται βασικό δικαίωμα. Ακόμα και σε μέρη όπου δεν υφίσταται δικαίωμα απορρήτου, το πολιτικό απόρρητο υπάρχει.

6.3 Νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε Ελλάδα και Ευρωπαϊκή Ένωση

Παρακάτω παρατίθεται ο πίνακας με τις διατάξεις του ελληνικού συντάγματος που αφορούν την προστασία των προσωπικών δεδομένων[59]:

Νόμος 2472/1997

Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Κατεβάστε το Ν. 2472/1997 **εδώ** (PDF Αρχείο) (με ενσωματωμένες και τις τελευταίες τροποποιήσεις βάσει του Ν. 3625/2007)	Δείτε το Νόμο αναλυτικά **εδώ**

Νόμος 3471/2006

Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97.

Κατεβάστε το Ν. 3471/2006 **εδώ**

---

[59] http://www.dpa.gr/portal/page?_pageid=33,23367&_dad=portal&_schema=PORTAL

Κανονιστικές πράξεις της ΑΠΔΠΧ

Οργάνωση της Γραμματείας της Αρχής	Π.Δ. 206/1998
Κανονισμός Λειτουργίας της Αρχής προστασίας Δεδομένων προσωπικού Χαρακτήρα	Αριθμ. 209/2000
Ενημέρωση υποκειμένων επεξεργασίας δεδομένων προσωπικού χαρακτήρα δια του τύπου	408/1998
Ενημέρωση υποκειμένων των δεδομένων κατ' άρθρο 11 Ν. 2472/1999	1/1999
Καθορισμός των παραβόλων (σε ευρώ) για τις χορηγούμενες από την Αρχή άδειες συλλογής και επεξεργασίας ευαίσθητων δεδομένων και διασύνδεσης αρχείων	121/2001
Ορισμός ύψους του χρηματικού ποσού για την άσκηση από το υποκείμενο των δεδομένων των δικαιωμάτων πρόσβασης και αντίρρησης	122/2001
Προϋποθέσεις τήρησης αρχείου από την ΤΕΙΡΕΣΙΑΣ Α.Ε. (πρώην υπ' αριθμ. 109/31.3.1999)	24/2004
Κανόνες κατηγοριοποίησης Δεδομένων της ΤΕΙΡΕΣΙΑΣ ΑΕ (ΦΕΚ Β 684/2004) βλ. άρθρο 70 Ν. 3746/2009 (ΦΕΚ Α-27) με το οποίο τροποποιήθηκε ο χρόνος τήρησης δεδομένων	25/2004
Όροι για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας (πρώην υπ' αριθμ. 050/20.1.2000) (ΦΕΚ Β -684/2004)	26/2004

Οδηγίες της ΑΠΔΠΧ

Οδηγία για τους όρους της νόμιμης επεξεργασίας δεδομένων προσωπικού χαρακτήρα νέων μητέρων για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης στο χώρο των μαιευτηρίων.	523/18-25.5.2000 (α')523523/18-25.5.2000(β')
Οδηγία για την εφαρμογή του άρθρου 28 του νέου Υπαλληλικού Κώδικα (Ν. 2683/1999).	1619/6.12.2000
Οδηγία για τα κλειστά κυκλώματα τηλεόρασης	1122/26.9.2000
Οδηγία για την ανάλυση γενετικού υλικού με σκοπό την εξιχνίαση εγκληματικών πράξεων	401/15.2.2001
Οδηγία για τους όρους της νόμιμης επεξεργασίας δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.	50/20.1.2001
Οδηγία για την επεξεργασία δεδομένων των εργαζομένων	1830/20.9.2001 (115/2001)
Οδηγία για την μεταγραφή με λατινικά στοιχεία του ονόματος των προσώπων στα δελτία ταυτότητας και στα διαβατήρια	2368/7-10-2003 (2/2003)
Οδηγία για την ασφαλή καταστροφή προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού επεξεργασίας	3845/17-10-2005 (1/2005)

Στην συνέχεια παρατίθεται ο πίνακας με τις οδηγίες της Ευρωπαϊκής Ένωσης:

Ευρωπαϊκή Ένωση	Συνθήκη για την Ευρωπαϊκή Ένωση (Άρθρο 6) Ευρωπαϊκή Σύμβαση των δικαιωμάτων του Ανθρώπου (Άρθρο 8) Χάρτης των Θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης (Άρθρο 8)
Οδηγία 95/46/ΕΚ	Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών
Οδηγία 2002/58/ΕΚ	Για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών
Οδηγία 2006/24/ΕΚ	ΟΔΗΓΙΑ 2006/24/ΕΚ ΤΟΥ ΕΥΡΩΠΑΙΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 15ης Μαρτίου 2006 για την διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ

6.4 Νομική προστασία σε χώρες του εξωτερικού[60]

6.4.1 Αυστραλία

Στην Αυστραλία, κάθε πολιτεία έχει θεσπίσει νόμους που ασχολούνται με διαφορετικά είδη της κλοπής ταυτότητας.

Σύμφωνα με την Αυστραλιανή νομοθεσία, κάποιος είναι ένοχος για ένα έγκλημα εάν κάνει μία πράξη με δόλιο σκοπό που θα προκαλέσει απώλεια σε κάποιο άλλο άτομο. Ποινή γι αυτό είναι 5τής φυλάκιση.

Αυτό ισχύει γενικά στην Αυστραλία αφού είπαμε ότι κάθε πολιτεία αντιμετωπίζει το θέμα με διαφορετικό νομικό πλαίσιο.

6.4.2 Καναδά

Σύμφωνα με την παράγραφο 403 του ποινικού κώδικα του Καναδά οποιοσδήποτε παριστάνει ένα άλλο άτομο ζώντα ή νεκρό με σκοπό:

- να αποκτήσει κάποιο κέρδος δικό του ή κάποιου άλλου
- να αποκτήσει κάποια περιουσία

[60] http://en.wikipedia.org/wiki/Identity_theft#Regional_Legal_responses

- να βλάψει το άτομο το οποίο μιμείται ή κάποιο άλλο άτομο, τότε είναι ένοχος για ποινικό αδίκημα και τιμωρείται με φυλάκιση που δεν ξεπερνά τα 10 έτη.

Όπως και στην περίπτωση της Αυστραλίας τα παραπάνω είναι γενικά αφού κάθε πολιτεία του Καναδά έχει θεσπίσει το δικό της νομικό πλαίσιο.

6.4.3 Γαλλία

Στη Γαλλία, το άτομο το οποίο συλλαμβάνεται για κλοπή ταυτότητας, μπορεί να καταδικαστεί σε φυλάκιση μέχρι 5 έτη και να του υποβληθεί πρόστιμο έως €75000.

6.4.4 Χονγκ Κονγκ

Σύμφωνα με την παράγραφο 210 του νόμου του Χονγκ Κονγκ, εάν ένα άτομο με οποιοδήποτε τρόπο διαπράξει κλοπή ταυτότητας, με σκοπό την απάτη το οποίο έχει σαν αποτέλεσμα:

- το όφελος, οποιουδήποτε ανθρώπου εκτός του θύματος

- το στιγματισμό ή την πιθανότητα στιγματισμό εις βάρος κάποιου ατόμου μπορεί να καταδικαστεί σε φυλάκιση 14 ετών.

6.4.5 Ινδία

Σύμφωνα με την ινδική νομοθεσία, όποιος επιχειρήσει να αντιγράψει δεδομένα που βρίσκονται αποθηκευμένα σε:

- προσωπικό υπολογιστή,

- δίκτυο υπολογιστών

- ή αφαιρούμενο μέσο αποθήκευσης χωρίς την άδεια του ιδιοκτήτη/διαχειριστή είναι υποχρεωμένος να καλύψει τις ζημιές που τυχόν θα προκληθούν από την πράξη του (μέχρι βέβαια ενός συγκεκριμένου ποσού).

6.4.6 Ηνωμένο Βασίλειο

Στο Ηνωμένο Βασίλειο τα προσωπικά δεδομένα προστατεύονται από ένα νόμο που θεσπίστηκε το 1998. Ο νόμος καλύπτει όλα τα προσωπικά δεδομένα ατόμων που μπορεί να υπάρχουν σε διάφορους οργανισμούς.

Υπήρχε μια περίπτωση με κάποιον ο οποίος ήταν "μεσάζων" και αποκτούσε αγαθά για λογαριασμό άλλων με τη μέθοδο της κλεμμένης ταυτότητας. Τελικά συνελήφθη χωρίς όμως να κατονομαστεί ποτέ κάποιος από τους "πελάτες" του. Τα κλεμμένα αγαθά άγγιξαν τις £10000 σε αξία. Το δικαστήριο θεώρησε ότι η απάτη που περιλαμβάνει κλοπή ταυτότητας είναι σοβαρό ποινικό αδίκημα και πρέπει να τιμωρηθεί με αυστηρή ποινή φυλάκισης.

Οι οργανισμοί, ακόμα και οι κρατικοί θα πρέπει να αυξήσουν τα μέτρα ασφάλειας των δεδομένων των χρηστών τους.

6.4.7 Η.Π.Α

Σύμφωνα με το αμερικανικό σύνταγμα, η κατοχή και χρήση μέσων ταυτοποίησης που δεν έχουν εκδοθεί από επίσημους οργανισμούς, είναι ποινικό αδίκημα.

Για να καταδικαστεί ο εγκληματίας από τις ΗΠΑ, πρέπει η πλαστή ταυτότητα είτε να:

- έχει εκδοθεί στις ΗΠΑ
- προορίζεται για απάτη σε βάρος των ΗΠΑ
- στέλνεται στη χώρα μέσω ταχυδρομείου
- χρησιμοποιείται για επηρεάσει το εσωτερικό ή ξένο εμπόριο.

Οι ποινές μπορεί να φτάσουν τα 5,15,20 ή 30 χρόνια σε ομοσπονδιακή φυλακή και επιβολή προστίμου ανάλογα με τη σοβαρότητα και την έκταση του αδικήματος. Οι ποινές μπορεί να διαφέρουν ανάλογα με την πολιτεία.

Έξι ομοσπονδιακές υπηρεσίες των ΗΠΑ ένωσαν τις δυνάμεις τους για να βοηθήσουν στον εντοπισμό της κλοπής ταυτότητας. Αυτή η συμμαχία έχει θεσπίσει κάποιες αρχές που πρέπει να ακολουθούνται από τους οργανισμούς που διαχειρίζονται προσωπικά και οικονομικά στοιχεία πολιτών. Οι κλοπές ταυτότητας μειώθηκαν την περίοδο 2004-2006.

Σε μια έρευνα που έγινε το 2003 το ποσοστό των αμερικάνων που είχαν πέσει θύματα κλοπής ταυτότητας ήταν 4,6% . Σε μια άλλη έρευνα που έγινε το 2005 το ποσοστό είχε μειωθεί σε 3,7%.

Αξίζει να σημειωθεί ότι δύο πολιτείες, η California και το Wisconsin έχουν ιδρύσει υπηρεσία προστασίας ιδιοκτησίας, που βοηθά τους πολίτες να προστατευτούν και να ορθοποδήσουν μετά από κλοπή ταυτότητας.

6.4.7.1 Ενέργειες προστασίας από το Υπουργείο Δικαιοσύνης

Το υπουργείο δικαιοσύνης καταδιώκει τις υποθέσεις κλοπής ταυτότητας και απάτης ταυτότητας με διάφορους τρόπους.

Το φθινόπωρο του 1998 για παράδειγμα το υπουργείο δικαιοσύνης των ΗΠΑ θέσπισε ένα νόμο που αντιμετώπιζε ένα νέο αδίκημα. Σύμφωνα με το νόμο αυτό, όποιος εν γνώσι του φέρει μέσο ταυτοποίησης που ανήκει σε άλλον, με σκοπό να διαπράξει ή να συνεργήσει σε παράνομες δραστηριότητες, θα διώκεται ποινικά.

Προστασία από κλοπή προσωπικών στοιχείων

Οι ποινές που προβλέπονται είναι:

- φυλάκιση μέχρι 15 έτη,
- χρηματικό πρόστιμο και
- κατάσχεση κάθε αντικειμένου που χρησιμοποιήθηκε ή επρόκειτο να χρησιμοποιηθεί για την απάτη.

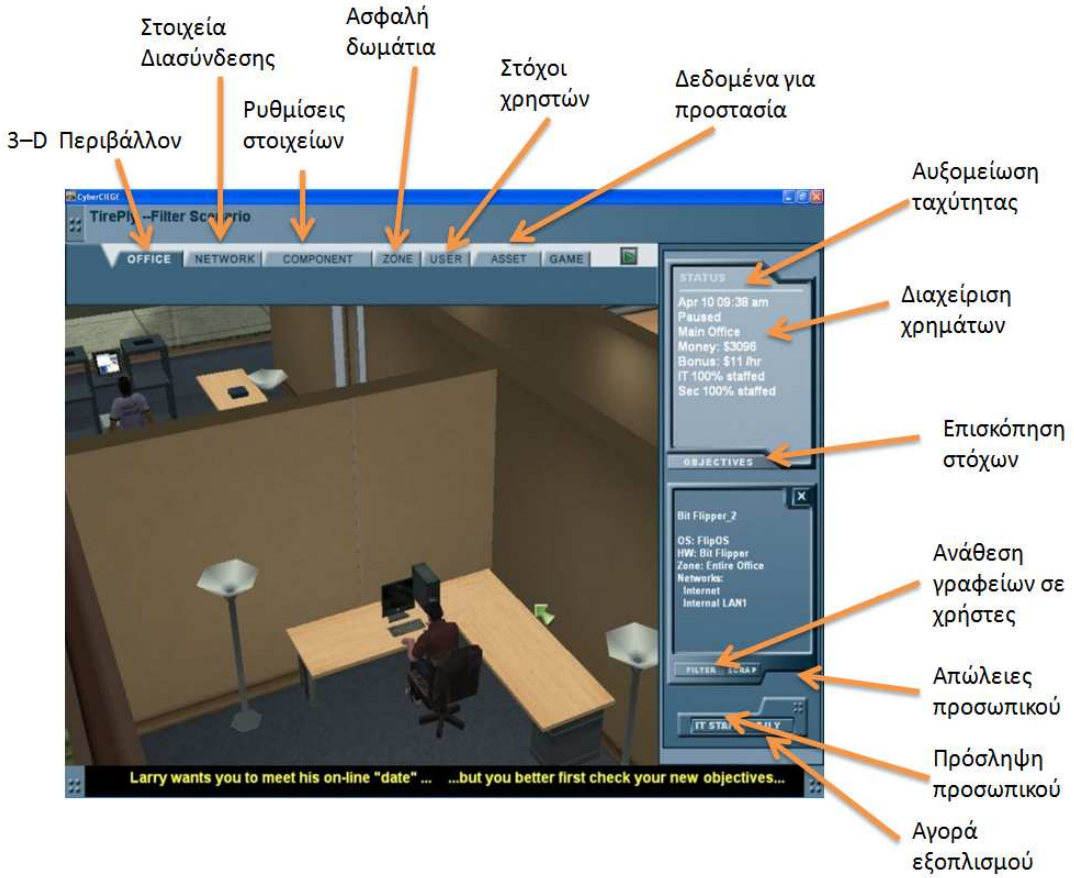
Ακόμα το υπουργείο δικαιοσύνης διαθέτει νομικό πλαίσιο για την αντιμετώπιση κάθε είδους απάτης σχετικής με κλοπή ταυτότητας όπως: απάτη με πιστωτικές κάρτες, κλοπή στοιχείων από υπολογιστή, απάτη μέσω ηλεκτρονικού ταχυδρομείου, σε βάρος οικονομικού οργανισμού κ.α.

Τα παραπάνω αδικήματα τιμωρούνται με βαρύτατες ποινές, που μπορεί να φτάσουν και τα 30 χρόνια φυλάκιση. Στην Αμερική υπάρχει μια συνεργασία φορέων
(FBI, μυστικές υπηρεσίες και ταχυδρομεία) για να εντοπίζονται τα περιστατικά απάτης.

Κεφάλαιο 7 Το εργαλείο CyberCIEGE

7.1 Εισαγωγή στο CyberCIEGE

Το **CyberCIEGE**[61] είναι ένα σοβαρό παιχνίδι (***βλ. εικ.18***) που έχει σαν σκοπό να διδάξει αρχές ασφαλείας δικτύων. Αναπτύχθηκε με την χρηματοδότηση του Αμερικάνικου ναυτικού και χρησιμοποιείται σαν εκπαιδευτικό εργαλείο από τις Αμερικάνικες υπηρεσίες, πανεπιστήμια και κολλέγια.



Εικόνα 18 CyberCIEGE: Στιγμιότυπο από το παιχνίδι[62]

Το CyberCIEGE καλύπτει μία σειρά από θέματα ασφάλειας δικτύων και υπολογιστών. Στο κόσμο του παιχνιδιού, ο παίκτης αγοράζει υπολογιστές και συσκευές δικτύου. Τις συσκευές αυτές πρέπει να τις ρυθμίσει κατάλληλα ώστε να ικανοποιήσει τις ανάγκες των απαιτητικών χρηστών και ταυτόχρονα να προστατέψει τις πληροφορίες από διάφορες επιθέσεις.

[61] http://en.wikipedia.org/wiki/CyberCIEGE
[62] http://cisr.nps.edu/cyberciege/downloads/CCIEGEbrochure.pdf

Το παιχνίδι περιλαμβάνει ένα αριθμό από διαφορετικά σενάρια με κλιμακούμενα επίπεδα δυσκολίας. Ακόμα, υπάρχει διαθέσιμο ένα εργαλείο ανάπτυξης σεναρίων ('Scenario Development Kit'), όπου ο παίκτης δημιουργεί και επεξεργάζεται τα δικά του σενάρια.

Τα στοιχεία της ασφάλειας δικτύων περιλαμβάνουν μεταξύ άλλων firewalls, VPN gateways, VPN clients, link encryptors και authentication servers. Οι σταθμοί εργασίας και οι servers περιλαμβάνουν λίστες ελεγχόμενης πρόσβασης (access control lists - ACLs). Το παιχνίδι επίσης περιλαμβάνει συσκευές ταυτοποίησης όπως scanners βιομετρικών στοιχείων και card readers για ελεγχόμενη πρόσβαση σε φυσικές περιοχές και σταθμούς εργασίας.

Οι τύποι των επιθέσεων που περιλαμβάνονται επίσης ποικίλουν. Υπάρχουν φυσικές επιθέσεις, Trojan horses, επιθέσεις στο δίκτυο και εκμετάλλευση των αδυναμιών του λειτουργικού συστήματος και των εφαρμογών.

Το παιχνίδι είναι ουσιαστικά ένας εξομοιωτής που λαμβάνει χώρα σε ένα τρισδιάστατο εικονικό κόσμο. Ο παίκτης δημιουργεί δίκτυα και παρατηρεί τους εικονικούς χρήστες. Η μηχανή του CyberCIEGE χρησιμοποιεί μία ειδική γλώσσα (scenario development language) που περιγράφει κάθε σενάριο, όσον αφορά τους χρήστες και τους στόχους τους, τον εξοπλισμό και την αξία του, αρχική κατάσταση του συστήματος καθώς και τις συνθήκες ομαλής λειτουργίας του σεναρίου.

7.2 Γιατί χρησιμοποιούμε εργαλεία τύπου CyberCIEGE

Μία τυπική μέρα ένας κυβερνητικός υπάλληλος μπορεί να έλθει σε επαφή με διάφορα προβλήματα ασφαλείας[63]. Κοιτώντας για πρώτη φορά τα e-mail του κάθε πρωί, σίγουρα θα βρει πολλά spam και fishing e-mails. Ακόμα, μπορεί να λάβει διάφορες προειδοποιήσεις για νέες απειλές ασφαλείας από κάποιο επιστημονικό άρθρο.

Παρά τη συνεχή ενημέρωση, η πλειοψηφία των υπαλλήλων αλλά και του κοινού, διατηρεί μία στάση απάθειας απέναντι στην ασφάλεια των πληροφοριακών συστημάτων. Ακόμα και μέσα σε μεγάλους οργανισμούς, διαλέγουν εύκολα password και θεωρούν ότι όσο κρατούν οπτική επαφή με το μηχάνημά τους δεν υπάρχει κάποιος κίνδυνος.

Εκτός από τους χρήστες και οι διαχειριστές των συστημάτων λαμβάνουν ανεπαρκή μέτρα. Σε πολλούς, το πρόβλημα της ηλεκτρονικής ασφάλειας, φαίνεται άλυτο και προτιμούν να το αγνοήσουν. Αυτή η απάθεια πρέπει να αντιμετωπιστεί.

Πρώτα απ' όλα οι χρήστες πρέπει να μάθουν να εκτιμούν το αντίκτυπο της ελλιπούς ασφάλειας στη σωστή λειτουργία του οργανισμού. Δεύτερον, οι χρήστες θα πρέπει να καθοδηγηθούν ώστε να καταλάβουν τα πάγια βήματα για την βελτίωση της ηλεκτρονικής ασφάλειας μέσα στον οργανισμό.

[63] http://cisr.nps.edu/cyberciege/downloads/FISSEA_CyberCIEGE_PreConf.pdf

Πρακτικά, για τον απλό χρήστη, αυτό μπορεί να σημαίνει χρησιμοποίηση ενός δύσκολου password που αλλάζεται συχνά. Για τον ειδικό σε τέτοια θέματα, αυτό μπορεί να σημαίνει τοπολογίες δικτύων και συνδέσεις ασφαλείας.

Άλλο ένα πρόβλημα που ανακύπτει είναι ο τρόπος εκπαίδευσης των χρηστών. Τα παραδοσιακά σεμινάρια και οι διαλέξεις, είναι συνήθως βαρετά τόσο στους χρήστες όσο και στους διαχειριστές.

Ακόμα, μπορεί να είναι δύσκολο για κάποιον να καταλάβει όλες τις αρχές της ασφάλειας των πληροφοριών σε θεωρητικό επίπεδο. Γι' αυτό προέκυψε η ανάγκη για εις βάθος κατανόηση των μηχανισμών ασφαλείας.

Οι διαδραστικές εξομοιώσεις προσφέρουν πολλά σαν εκπαιδευτικά εργαλεία. Τα εργαλεία αυτά, που συχνά εμφανίζονται με την μορφή παιχνιδιών, δημιουργούν μία αίσθηση ανταγωνισμού σε ένα συναρπαστικό περιβάλλον χρήσης, όπου ο κάθε συμμετέχων διεκδικεί ένα μερίδιο του αποτελέσματος. Τέτοιου τύπου εργαλείο είναι και το CyberCIEGE, το οποίο περιγράφεται αναλυτικότερα παρακάτω.

7.3 Εξομοιώσεις διαχείρισης πόρων

Το CyberCIEGE είναι ένα εργαλείο εξομοίωσης διαχείρισης πόρων, στο οποίο ο χρήστης αναλαμβάνει το ρόλο του λήπτη αποφάσεων ενός οργανισμού που βασίζεται σε πληροφοριακά συστήματα[64]. Ο στόχος είναι να παραμείνουν οι εικονικοί χρήστες του οργανισμού ευχαριστημένοι και παραγωγικοί ενώ ταυτόχρονα προστατεύονται πολύτιμα δεδομένα του οργανισμού.

Σε ένα τυπικό σενάριο του CyberCIEGE, ο χρήστης διαθέτει ένα συγκεκριμένο budget και πρέπει να πάρει αποφάσεις για την διαδικαστική τεχνική και φυσική ασφάλεια. Με σωστές επιλογές, ο οργανισμός ευημερεί και το σενάριο προχωράει. Με λάθος αποφάσεις επέρχεται καταστροφή.

Η δυναμική των εξομοιωτών αυτού του τύπου, τραβάει την προσοχή του χρήστη όπως έχει αποδειχτεί από την επιτυχία των παιχνιδιών SimCity, RollerCoaster Tycoon κ.α. Στα παιχνίδια αυτά, ο παίκτης σχεδιάζει, κατασκευάζει και παρατηρεί τα αποτελέσματα των επιλογών του.

Το CyberCIEGE έχει ένα παρόμοιο στόχο. Οι παίκτες βυθίζονται σε ένα περιβάλλον όπου οι επιλογές τους έχουν ορατό αντίκτυπο στην παραγωγικότητα των εικονικών χρηστών και στην ικανότητα των επιτιθέμενων να κλέψουν πληροφορίες. Ο παίκτης αναπτύσσει ένα συναισθηματικό δεσμό με αυτό που έχει κατασκευάσει και κατ' επέκταση μαθαίνει από τα λάθη του όταν οι αποφάσεις του αποδειχθούν ανεπαρκείς.

Το παιχνίδι περιλαμβάνει πολλά διαφορετικά σενάρια και το καθένα τρέχει ξεχωριστά. Κάθε σενάριο περιλαμβάνει τη περιγραφή μίας επιχείρησης και δίνει πληροφορίες στο παίκτη για το τι πρέπει να γίνει για να πετύχει η επιχείρηση.

[64] http://cisr.nps.edu/cyberciege/downloads/FISSEA_CyberCIEGE_PreConf.pdf

Σε κάθε σενάριο η επιχείρηση έχει ένα καθορισμένο αριθμό χρηστών και δεδομένων. Οι χρήστες είναι συνήθως υπάλληλοι της επιχείρησης ενώ τα δεδομένα είναι διαφόρων ειδών πληροφορίες στις οποίες πρέπει να έχουν πρόσβαση οι χρήστες.

Υπάρχουν στόχοι χρηστών και μερικές φορές τα δεδομένα μπορεί να χρειαστεί να μοιραστούν ανάμεσα στους χρήστες οι οποίοι με τη σειρά τους μπορούν να έχουν πρόσβαση σε διαφορετικά δεδομένα ταυτόχρονα.

Τα διάφορα δεδομένα έχουν διαφορετικά επίπεδα μυστικότητας, ακεραιότητας και διαθεσιμότητας και κάθε ομάδα χρηστών έχει διαφορετικό επίπεδο εξουσιοδότησης για την πρόσβαση στα δεδομένα.

Κάθε σενάριο μετά την δημιουργία του, δεν μπορεί να τροποποιηθεί. Αυτό που ξεχωρίζει στο CyberCIEGE είναι οι απεριόριστοι συνδυασμοί σεναρίων που μπορούν να δημιουργηθούν και να παιχτούν.

7.4 Στοιχεία του CyberCIEGE

Το CyberCIEGE αποτελείται από πολλά στοιχεία: μία μοναδική μηχανή εξομοίωσης, μία γλώσσα περιγραφής σεναρίων, εργαλείο ανάπτυξης σεναρίων και μία εγκυκλοπαίδεια βασισμένη σε βίντεο[65].

Το CyberCIEGE είναι επεκτάσιμο με διαφορετικά σενάρια δημιουργημένα για συγκεκριμένους αποδέκτες. Γεγονότα σκανδαλισμού βασισμένα στο σενάριο, δίνουν στους παίκτες νέα προβλήματα προς λύση.

[65] http://cisr.nps.edu/cyberciege/downloads/FISSEA_CyberCIEGE_PreConf.pdf

Εικόνα 19 CyberCIEGE: Οι χρήστες του CyberCIEGE εν ώρα εργασίας

Βασικός στόχος κατά την ανάπτυξη του CyberCIEGE, ήταν να δημιουργηθεί ένα εργαλείο για το οποίο θα μπορούσε να υπάρξει μεγάλος αριθμός σεναρίων. Αυτός ο στόχος προέκυψε από δύο παράγοντες. Πρώτον, ο τομέας της διασφάλισης της πληροφορίας είναι τεράστιος.

Γι' αυτό χρειάζονται πολλά σενάρια με διαφορετικό αντικείμενο εστίασης το καθένα. Δεύτερον, θα πρέπει να δίνεται η δυνατότητα στους προχωρημένους χρήστες να αξιοποιούν τις γνώσεις τους και να τις συνδυάζουν δημιουργώντας δικά τους σενάρια.

7.4.1 Μηχανή Εξομοίωσης

Στη βάση του, το CyberCIEGE περιέχει μία πολύπλοκη μηχανή παιχνιδιού, που ονομάζεται TYBOLT της εταιρείας River mind. Η μηχανή αυτή, μπορεί να χρησιμοποιηθεί σε υπολογιστές και κονσόλες νέας γενιάς και έχει σχεδιαστεί για παιχνίδια και εξομοιωτές.

Στο πυρήνα της, η γλώσσα αυτή, είναι μία βιβλιοθήκη τρισδιάστατων γραφικών. Γραφικά κάθε τύπου, από στατικά αντικείμενα μέχρι κινούμενους χαρακτήρες, μπορούν να εισαχθούν μέσα στην TYBOLT από διάφορα εργαλεία παραγωγής γραφικών.

Εικόνα 20 CyberCIEGE: Άλλη μια εικόνα από το περιβάλλον χρήσης του CyberCIEGE

Άλλη μία καινοτομία της TYBOLT, είναι η τρισδιάστατη διεπαφή χρήστη. Ακόμα, περιέχει ένα σύστημα τεχνητής νοημοσύνης, μία βιβλιοθήκη αναπαραγωγής βίντεο και μία ήχου, ένα σύστημα διαχείρισης μνήμης, ένα σύστημα διαχείρισης πόρων και μία μηχανή στρατηγικής πραγματικού χρόνου.

Όταν χρησιμοποιείται σε εφαρμογές του υπολογιστή ή του XBOX, η TYBOLT εκμεταλλεύεται το DirectX 9, για να διασφάλιση την όσο το δυνατόν καλύτερη συμβατότητα με σύγχρονες κάρτες γραφικών.

7.4.2 Γλώσσα περιγραφής σεναρίων

Το CyberCIEGE είναι κτισμένο γύρω από μία γλώσσα που εκφράζει διάφορα θέματα ασφαλείας με διαφορετικά σενάρια. Η μηχανή εξομοίωσης του CyberCIEGE, μεταφράζει τη γλώσσα αυτή και παρουσιάζει την εξομοίωση που προκύπτει. Η γλώσσα αυτή, περιλαμβάνει τα παρακάτω βασικά στοιχεία:

- **Δεδομένα - Έγγραφα:** Αυτά είναι πληροφορίες που έχουν κάποια αξία για την επιχείρηση. Οι εικονικοί χρήστες έχουν πρόσβαση σε αυτά για να πετύχουν τους στόχους τους. Παραδείγματα τέτοιων δεδομένων μπορεί να είναι λογιστικά της επιχείρησης, επιχειρηματικά σχέδια, υλικό marketing κ.α.

  Μερικά δεδομένα είναι μεγάλης αξίας ενώ άλλα είναι ασήμαντα. Γι’ αυτό υπάρχει ένα κόστος στον οργανισμό όταν μία πληροφορία τεθεί σε κίνδυνο. Κάθε πληροφορία έχει διαφορετική αξία και για τον επιτιθέμενο. Άλλες πληροφορίες έχουν αξία γιατί είναι μυστικές και άλλες γιατί είναι ακέραιες.

Μπορεί να υπάρχουν κατηγορίες που ομαδοποιούν χαρακτηριστικά και τα κληρονομούν διάφοροι τύποι πληροφοριών.

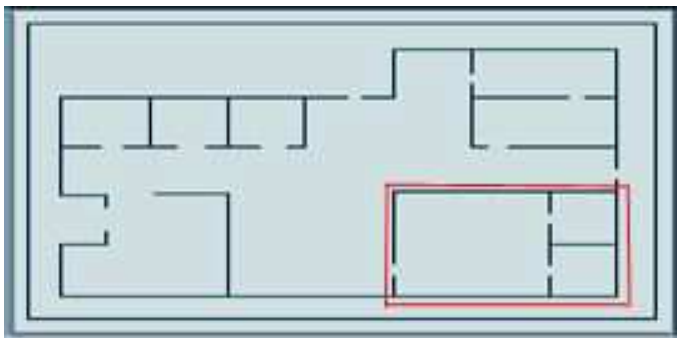
- **Χρήστες:** Κάθε σενάριο του CyberCIEGE περιλαμβάνει ένα σετ από εικονικούς χρήστες των οποίων η δουλεία παράγει χρήμα για την επιχείρηση και τον οργανισμό. Οι χρήστες έχουν εργασιακούς στόχους που πρέπει να επιτευχθούν για να παραμείνουν παραγωγικοί και ευτυχισμένοι. Είναι ευθύνη του παίκτη να παρέχει στους χρήστες τα μέσα για να επιτύχουν τους στόχους τους.

  Κάθε χρήστης έχει έναν ή περισσότερους στόχους που εκφράζονται ως ανάγκη να έχει πρόσβαση σε συγκεκριμένα δεδομένα. Μερικοί στόχοι μπορεί να συσχετίζονται με την παραγωγικότητα του χρήστη και άλλοι με την ευτυχία.

  Αν ο χρήστης δεν πετύχει παραγωγικούς στόχους, επηρεάζεται η κατάσταση της επιχείρησης ή του οργανισμού. Αν δεν πετύχει ένα στόχο ευτυχίας δεν επηρεάζεται η επιχείρηση άμεσα αλλά ένας απογοητευμένος υπάλληλος μπορεί να θέσει σε κίνδυνο την ασφάλεια του οργανισμού.

- **Ζώνες:** Κάθε σενάριο περιλαμβάνει μία ή περισσότερες ζώνες (περιοχές), (***βλ. εικ.21***), που χρησιμοποιούνται για τη φυσική κίνηση των χρηστών. Παράδειγμα τέτοιας ζώνης είναι ένα κλειδωμένο γραφείο του οποίου το κλειδί το έχουν επιλεγμένοι χρήστες.

  Όταν αγοράζονται νέα μηχανήματα τοποθετούνται σε μία συγκεκριμένη ζώνη. Φυσική πρόσβαση σε αυτά τα μηχανήματα, απαιτεί και πρόσβαση στη ζώνη που είναι τοποθετημένα. Μια ζώνη μπορεί να περιλαμβάνει μικρότερες ζώνες με διαφορετικούς κανονισμούς ασφαλείας.



Εικόνα 21 CyberCIEGE: Επισήμανση μίας ζώνης στον όροφο

- **Συνθήκες ενεργοποίησης:** Ο σχεδιαστής του σεναρίου καθορίζει τις συνθήκες που θα υπάρξουν κατά την διάρκεια του παιχνιδιού, και καθορίζει επίσης το αποτέλεσμα ενός συγκεκριμένου συνδυασμού συνθηκών. Για παράδειγμα, σε κάποιο σημείο ο εικονικός χρήστης μπορεί να λάβει ένα νέο στόχο, και πρέπει ο παίκτης να κάνει κάποιες ενέργειες για να του επιτρέψει να τον πετύχει.

Ακόμα, ο σχεδιαστής του σεναρίου, μπορεί να καθορίσει συγκεκριμένους τύπους επιθέσεων που θα υπάρξουν και θα εξαρτώνται από διαφορετικές συνθήκες, όπως για παράδειγμα ο χρόνος παιχνιδιού και η πρόοδος των εικονικών χρηστών.

Η πρόοδος του παίκτη, συμβουλές αλλά και παράπονα από δυσαρεστημένους εικονικούς χρήστες εμφανίζονται χρησιμοποιώντας αναδυόμενα παράθυρα (***βλ. εικ.22***) και μία κινούμενη μπάρα στο κάτω μέρος της οθόνης.

Εικόνα 22 CyberCIEGE: Ένας εικονικός χρήστης μιλάει

Η νίκη ή η ήττα καθορίζονται επίσης με χρήση συνθηκών και σκανδαλισμών. Αυτό επιτρέπει στο σχεδιαστή σεναρίου, να παρουσιάσει στο παίκτη διαφορετικές οθόνες αποτελέσματος ανάλογα με την αιτία λόγω της οποίας επήλθε η ήττα.

- **Στόχοι και φάσεις:** Τα σενάρια μπορούν να χωριστούν σε πολλές φάσεις και κάθε φάση αποτελείται από έναν ή περισσότερους στόχους. Οι στόχοι περιγράφονται με βάση κάποιες συνθήκες όπως είπαμε και παραπάνω.

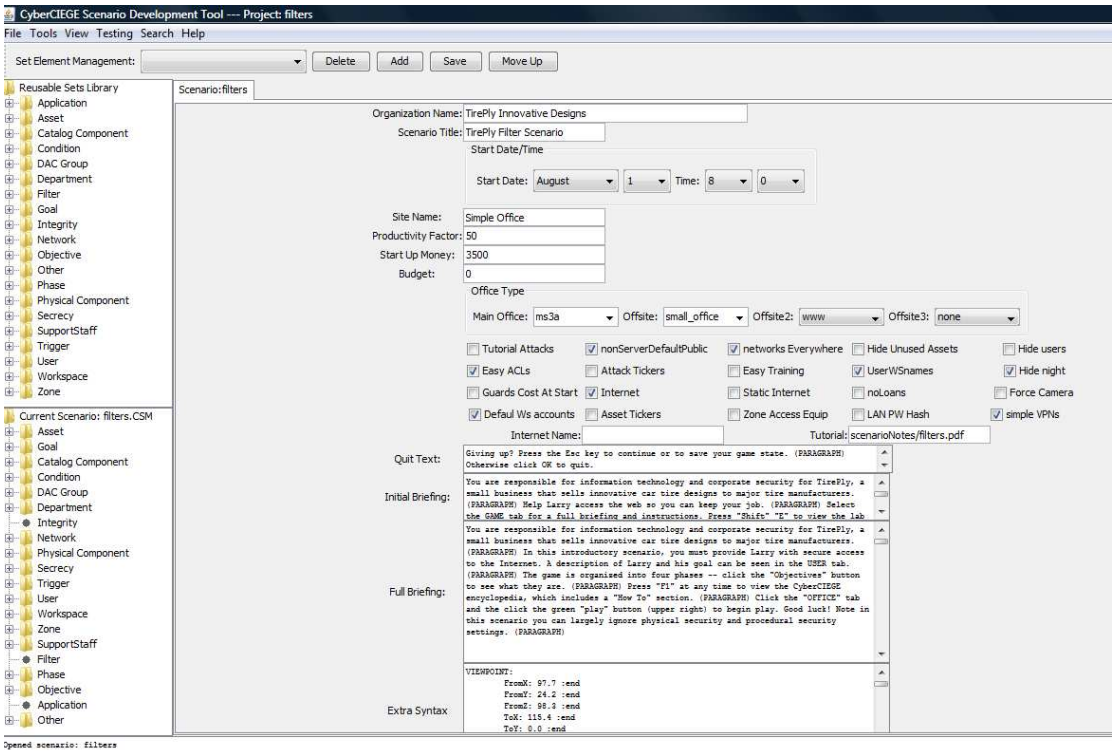
  Ο παίκτης πρέπει να πετύχει κάθε στόχο σε μία συγκεκριμένη φάση, πριν η εξομοίωση μεταβεί στην επόμενη φάση. Αυτό επιτρέπει στο σχεδιαστή να καθοδηγήσει το παίκτη και δίνει στο παίκτη μία αίσθηση σταδιακής προόδου.

7.4.3 Εργαλείο Περιγραφής Σεναρίων (Scenario Development Tool)

Το εργαλείο περιγραφής σεναρίων είναι πολύπλοκο και απαιτητικό όσον αφορά τη σύνταξη, αφού χρειάζονται χιλιάδες γραμμές κειμένου για να εκφραστεί ένα πλήρες σενάριο. Οι σχεδιαστές μπορούν να χρησιμοποιήσουν ένα εργαλείο βασισμένο σε φόρμες, για να κατασκευάσουν σενάρια χωρίς να παλεύουν με τη σύνταξη της γλώσσας.

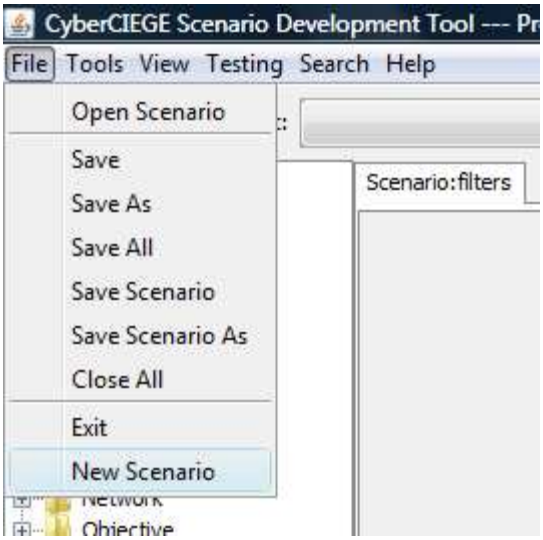
Το εργαλείο αυτό παρέχει ένα περιβάλλον ανάπτυξης, όπου οι σχεδιαστές μπορούν κατασκευάσουν σενάρια που εκμεταλλεύονται επαναχρησιμοποιήσιμες βιβλιοθήκες στοιχείων σεναρίου. Αυτό επιτρέπει την εύκολη κατασκευή οικογενειών σεναρίων με ελάχιστες αλλαγές.

Το περιβάλλον ανάπτυξης περιλαμβάνει εργαλεία για την αξιολόγηση και την εκτέλεση νέων σεναρίων. Στην παρακάτω εικόνα φαίνεται ένα στιγμιότυπο από το εργαλείο περιγραφής σεναρίων:



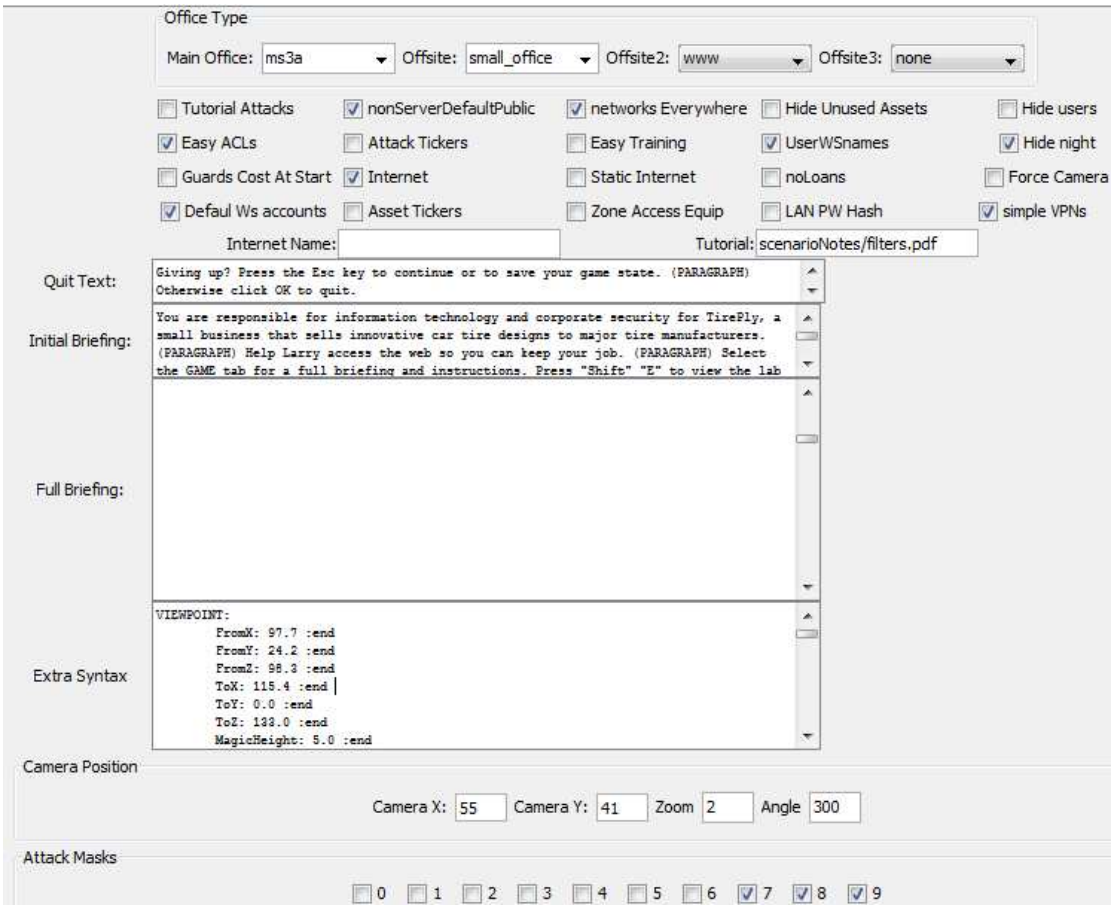
Εικόνα 23 CyberCIEGE: Εργαλείο Περιγραφής Σεναρίων

Για να δημιουργήσουμε ένα νέο σενάριο, πάμε στο μενού **File -> New Scenario**. Στο πεδίο κειμένου, που θα αναδυθεί, πληκτρολογούμε το επιθυμητό όνομα του σεναρίου.



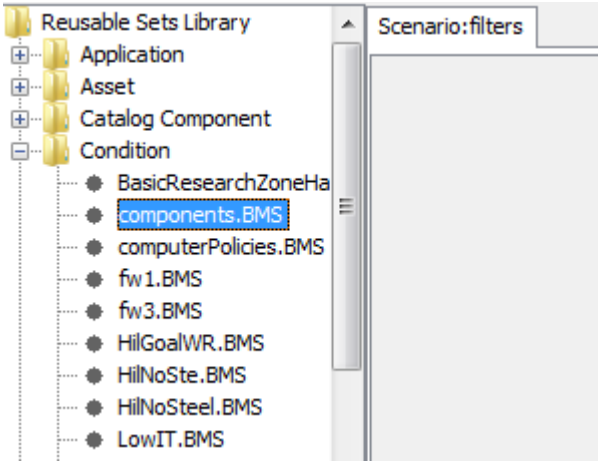
Εικόνα 24 CyberCIEGE: Δημιουργία νέου σεναρίου

Στην κεντρική οθόνη κάνουμε τις βασικές ρυθμίσεις που επιθυμούμε. Στο πεδίο **Quit Text**, γράφουμε το μήνυμα που θα εμφανιστεί στο παίχτη όταν επιχειρήσει να βγει από το παιχνίδι. Στο πεδίο **Initial Briefing** γράφουμε την σύντομη περιγραφή του σεναρίου, που θα εμφανιστεί αμέσως μόλις το ξεκινήσουμε. Και στο πεδίο **Full Briefing**, γράφουμε την πλήρη περιγραφή του σεναρίου. Τέλος, στο **Camera position**, κάνουμε τις αρχικές ρυθμίσεις της οπτικής γωνίας.



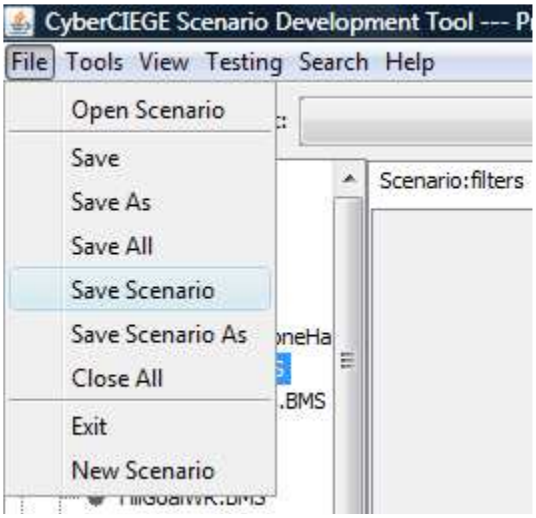
Εικόνα 25 CyberCIEGE: Οι βασικές ρυθμίσεις νέου σεναρίου

Για να παραμετροποιήσουμε κάθε λεπτομέρεια του σεναρίου, χρειάζεται να πάμε στο μενού **Reusable Sets Library** που βρίσκεται πάνω αριστερά. Κάνοντας διπλό κλικ σε κάθε ενότητα, εμφανίζονται τα στοιχεία της ενότητας. Για να επεξεργαστούμε κάποιο συγκεκριμένο στοιχείο, κάνουμε διπλό κλικ πάνω του.



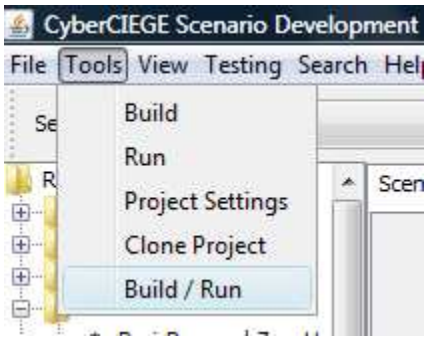
Εικόνα 26 CyberCIEGE: Αναλυτικές ρυθμίσεις

Όταν τελειώσουμε από τις ρυθμίσεις, μπορούμε να σώσουμε το σενάριο, μέσα από το μενού **File -> Save Scenario As.** Αν αργότερα θέλουμε να ανοίξουμε το σενάριο, για να το επεξεργαστούμε ή να το παίξουμε, πάμε στο μενού **File -> Open Scenario.**



Εικόνα 27 CyberCIEGE: Σώζουμε το σενάριο

Τέλος, για να τρέξουμε το σενάριο, πάμε στο μενού **Build / Run**. Το σενάριο θα κατασκευαστεί αυτόματα και θα τρέξει σε μερικά δευτερόλεπτα.



Εικόνα 28 CyberCIEGE:Τρέχουμε το σενάριο

Το CyberCIEGE έχει σχεδιαστεί με τέτοιο τρόπο ώστε κάθε σενάριο να είναι μία καλά ορισμένη διδακτική μονάδα για την ασφάλεια των πληροφοριών.

Χρησιμοποιώντας την ιδέα της καμπάνιας, αυτές οι διδακτικές μονάδες μπορούν να συνδυαστούν για να παρέχουν είτε μία αλληλουχία από σενάρια κλιμακούμενης δυσκολίας είτε μία εστιασμένη εκπαιδευτική μονάδα που καλύπτει πολλά ζητήματα.

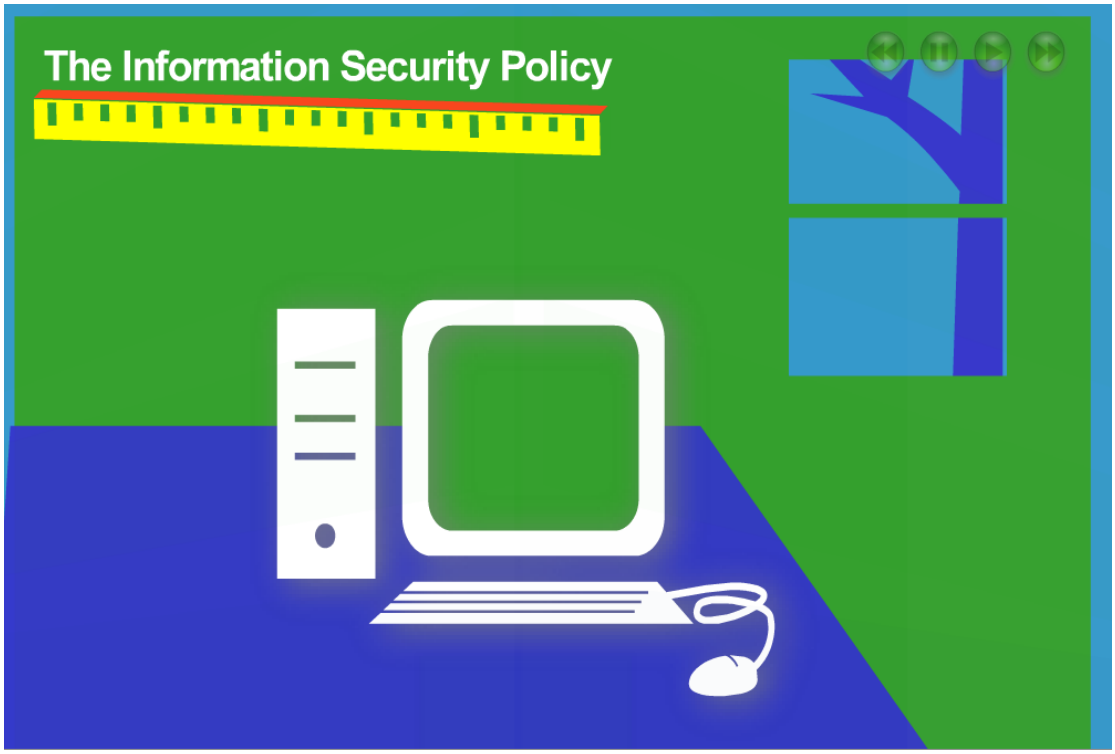
7.4.4 Εγκυκλοπαίδεια

Για να βελτιώσει την εμπειρία του διαδραστικού περιβάλλοντος, το CyberCIEGE περιέχει μία εγκυκλοπαίδεια. Οποιαδήποτε στιγμή μέσα στο σενάριο ο παίκτης μπορείς να πατήσει το πλήκτρο ‘e’ ή ‘E’ για να καλέσει την εγκυκλοπαίδεια. Εδώ, παρουσιάζεται στον παίκτη ένα μενού το οποίο οδηγεί σε μια πληθώρα θεμάτων.

Υπάρχουν στην εγκυκλοπαίδεια θέματα που σκοπό έχουν να μάθουν στο παίκτη πώς παίζεται το παιχνίδι. Περιγράφουν δηλαδή τα στοιχεία του σεναρίου και μαθαίνουν στο χρήστη να καταλαβαίνει πότε κερδίζει και πότε χάνει.

Άλλη θεματική ενότητα της εγκυκλοπαίδειας περιγράφει μία μεγάλη γκάμα από θέματα ασφάλειας πληροφοριών. Αυτά περιλαμβάνουν περιγραφές πολιτικών ασφαλείας, κωδικών, συσκευών δικτύου, κακόβουλου λογισμικού κ.α.

Επειδή υπάρχει περίπτωση πολλοί χρήστες να μην θέλουν να διαβάσουν ούτε μία σελίδα της εγκυκλοπαίδειας, υπάρχουν βίντεο που κάνουν περίπου την ίδια δουλεία με την εγκυκλοπαίδεια. Τα βίντεο είναι κινούμενα σχέδια που περιγράφουν θέματα ασφαλείας. Στιγμιότυπο ενός βίντεο φαίνεται στην παρακάτω εικόνα:



Εικόνα 29 CyberCIEGE: Στιγμιότυπο ενός βίντεο

Είναι σχεδιασμένα για να είναι κατανοητά ακόμα και από παιδιά και να είναι διασκεδαστικά σε όλες τις ηλικιακές ομάδες.

Η αρχική κυκλοφορία του CyberCIEGE, περιλαμβάνει βίντεο για τις πολιτικές ασφαλείας, το κακόβουλο λογισμικό, τα τείχη προστασίας και τη διασφάλιση της πληροφορίας. Ακόμα, περιλαμβάνεται ένα βίντεο που περιγράφει την χρήση του CyberCIEGE.

7.5 Οδηγίες εγκατάστασης του CyberCIEGE

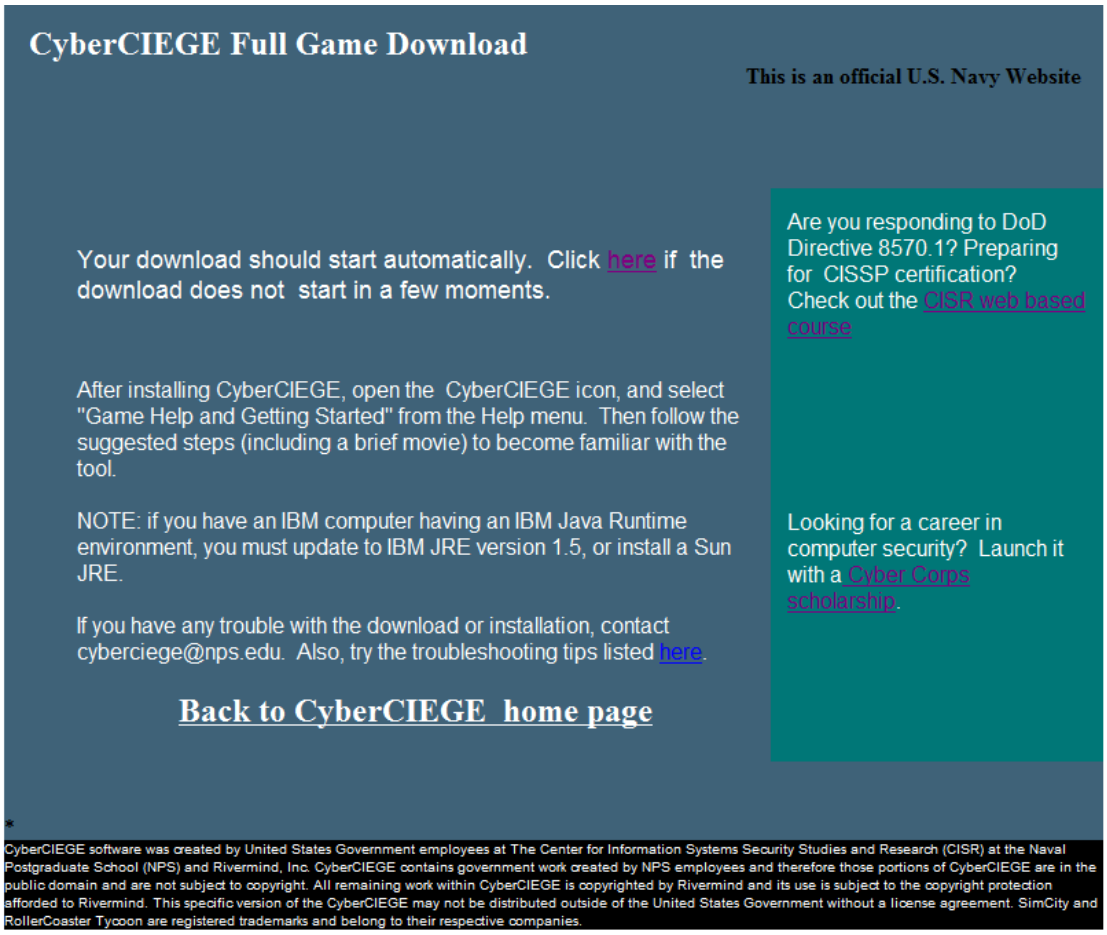
Η τελική έκδοση του CyberCIEGE είναι διαθέσιμη για όλους όσους επιθυμούν να το παίξουν, από την ιστοσελίδα: *http://cisr.nps.edu/cyberciege/latestv.html*. Μπαίνοντας στην ιστοσελίδα αυτή, εμφανίζεται το παρακάτω παράθυρο ***(βλ. εικ.30)***.

Τα βήματα εγκατάστασης φαίνονται αναλυτικά παρακάτω και πραγματοποιήθηκαν σε **Microsoft Windows Vista 32 bit Home Edition.**

1^{ο} βήμα: Όπως φαίνεται και στην εικόνα, δίπλα από το Organization Name πληκτρολογούμε την φράση: *Cyberciege academic license request* και στο Contact Email Address βάζουμε το εξής e-mail: *mfthomps@nps.edu*.

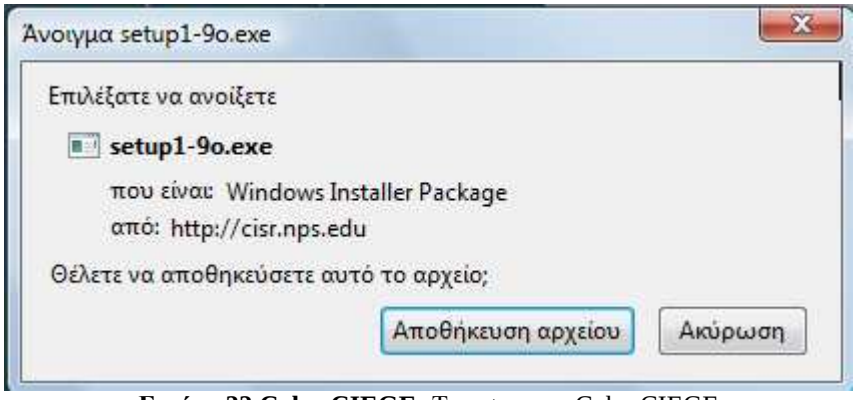
Εικόνα 30 CyberCIEGE: Φόρμα συμπλήρωσης για εγκατάσταση του παιχνιδιού

2^{ο} βήμα: Τέλος, αφού συμπληρωθούν τα πεδία, πατάμε το Get CyberCIEGE και θα εμφανιστεί το παρακάτω παράθυρο ***(βλ. εικ.31)***, το οποίο δίνει οδηγίες σχετικά με το CyberCIEGE, οι οποίες πρέπει να τηρηθούν, μετά την εγκατάστασή του καθώς περιλαμβάνει και κάποια άλλα links, σε περίπτωση που περάσει το χρονικό περιθώριο και δεν μπορέσει κάποιος να εγκαταστήσει τελικά το παιχνίδι.



Εικόνα 31 CyberCIEGE: Η τελική έκδοση είναι έτοιμη για εγκατάσταση

3ο βήμα: Στο βήμα αυτό, βλέπουμε το setup του αρχείου του CyberCIEGE, που είναι απαραίτητο για την εγκατάσταση. Και θα πατήσουμε την επιλογή: **Αποθήκευση αρχείου.**



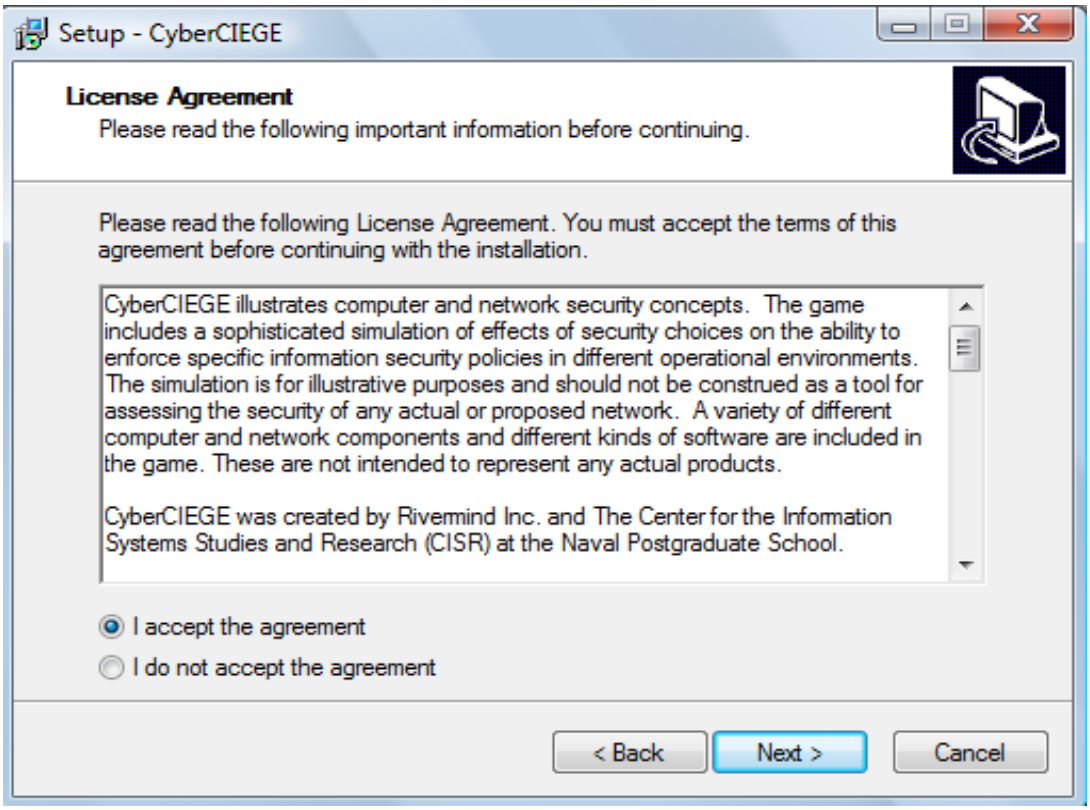
Εικόνα 32 CyberCIEGE: Το setup του CyberCIEGE

4ο βήμα: Στην συνέχεια, θα επιλέξουμε την επιλογή: **Αποδοχή (Εμπιστεύομαι το πρόγραμμα)** και όχι την λέξη: Άκυρο, γιατί έτσι θα διακοπεί η διαδικασία.

5ο βήμα: Στο βήμα αυτό, εμφανίζεται το αμέσως παρακάτω παράθυρο και πρέπει να πατήσουμε το **Next>** για να προχωρήσει παρακάτω. Σε διαφορετική περίπτωση, θα διακοπεί η διαδικασία της εγκατάστασης:

Εικόνα 33 CyberCIEGE: CyberCIEGE Setup Wizard

6ο βήμα: Εδώ, πρέπει να επιλέξουμε την επιλογή: **I accept the agreement**, δηλαδή ότι συμφωνούμε με τους όρους και τις προϋποθέσεις του κατασκευαστή του παιχνιδιού, Αν συμφωνούμε πατάμε **Next>** και προχωράμε. Αν διαφωνήσουμε πατάμε την επιλογή: **I do not accept the agreement** και δεν μπορούμε όμως να προχωρήσουμε στο επόμενο βήμα:

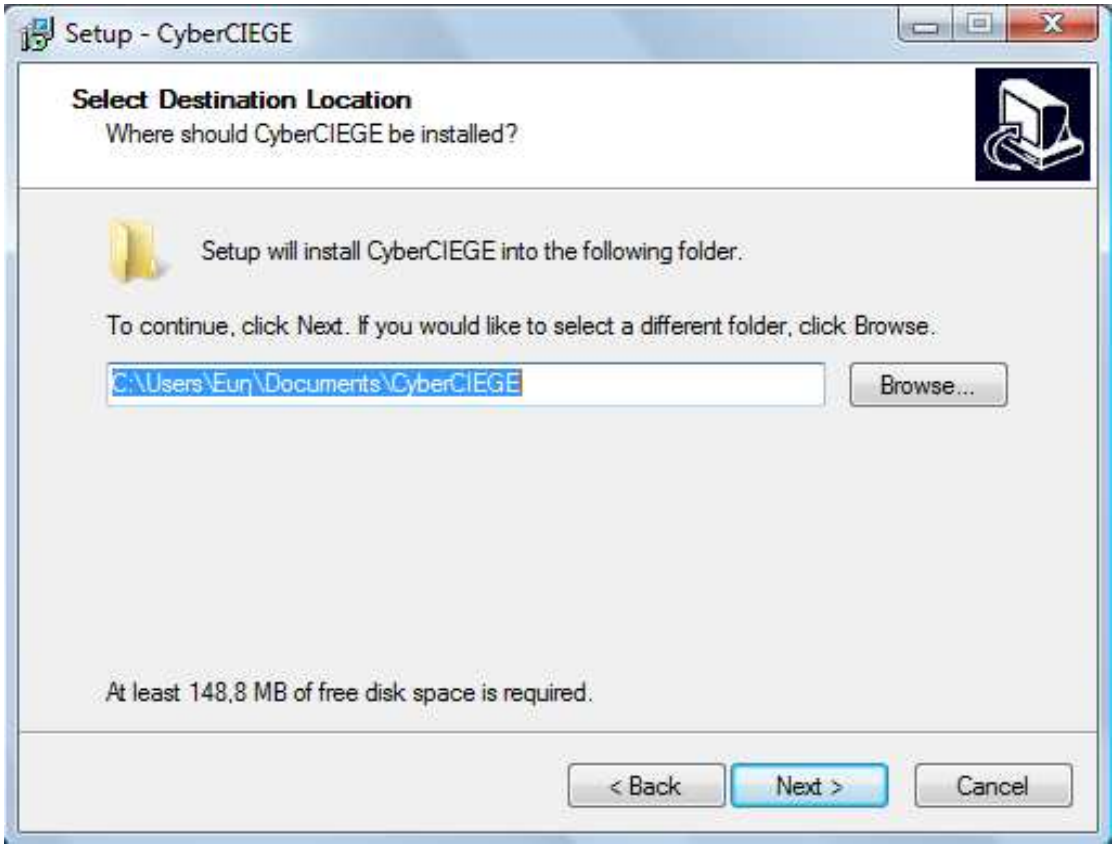


Εικόνα 34 CyberCIEGE: Όροι και προϋποθέσεις του κατασκευαστή

7ο βήμα: Για να μπορέσουμε να προχωρήσουμε επιτυχώς στο επόμενο βήμα, πρέπει να δώσουμε ένα password που είναι το **grostolis** και πατάμε **Next> :**

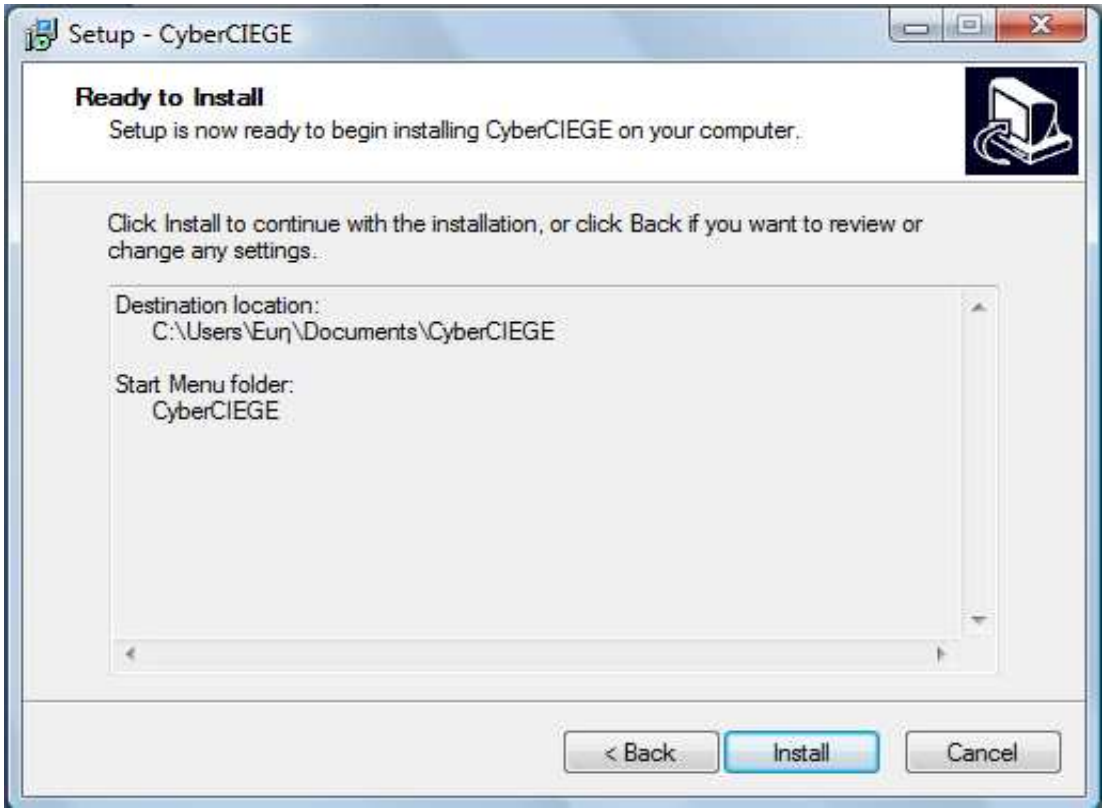
Εικόνα 35 CyberCIEGE: Απαιτείται η εισαγωγή password

8ο βήμα: Στο βήμα αυτό, επιλέγουμε σε ποιο φάκελο επιθυμούμε να αποθηκευτεί το παιχνίδι, μέσω της επιλογής Browse. Αν δεν επιθυμούμε την αλλαγή το αφήνουμε όπως το βγάζει και πατάμε **Next> :**



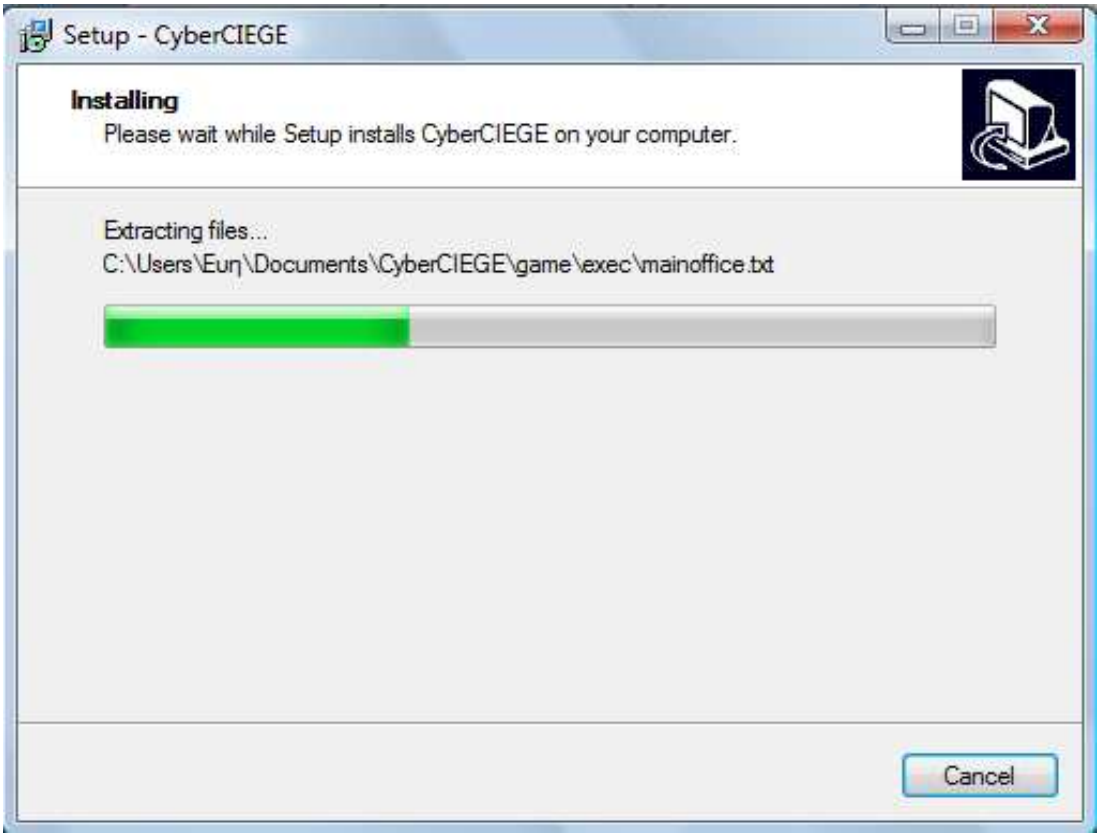
Εικόνα 36 CyberCIEGE: Επιλογή φακέλου για αποθήκευση του παιχνιδιού

9^{ο} βήμα: Το screenshot αυτό δείχνει ότι το πρόγραμμα είναι έτοιμο για να εγκατασταθεί. Για να ξεκινήσει η εγκατάσταση πρέπει να πατήσουμε την επιλογή **Install**:



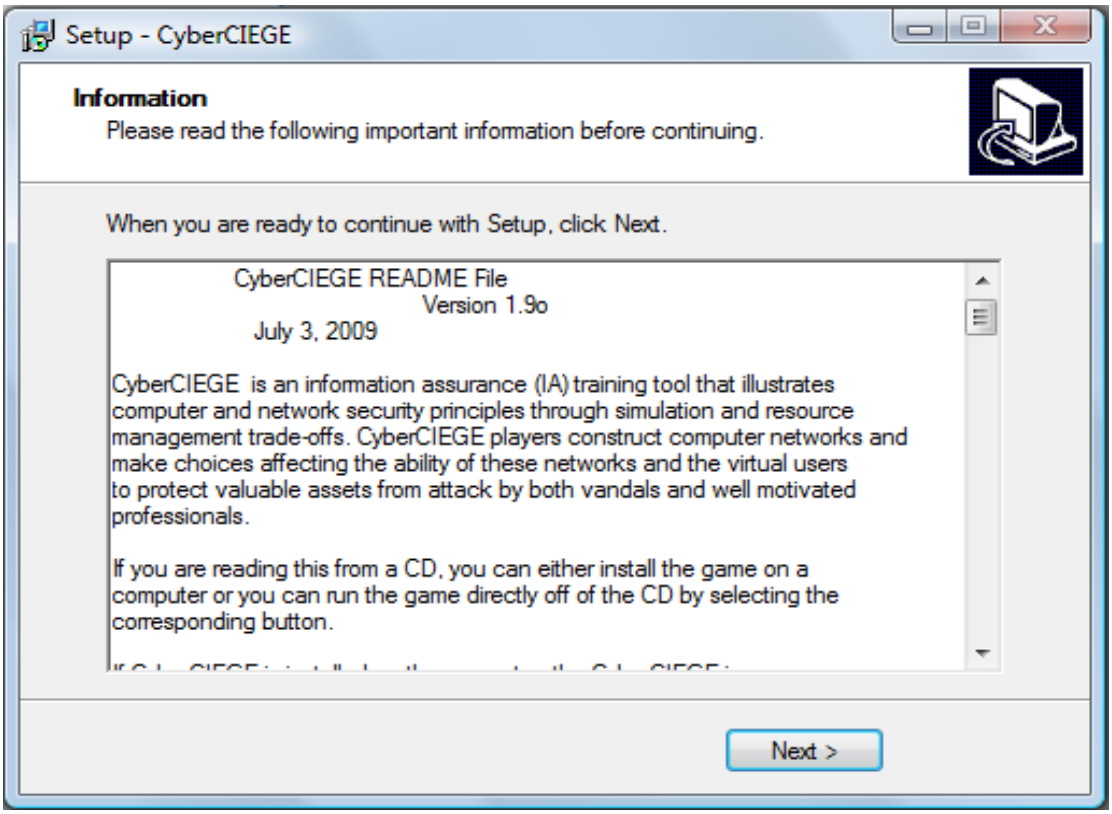
Εικόνα 37 CyberCIEGE: Το παιχνίδι είναι έτοιμο για εγκατάσταση

10^{ο} βήμα: Στο βήμα αυτό, γίνεται η εγκατάσταση των αρχείων του παιχνιδιού. Πρέπει να περιμένουμε μέχρι όλη η μπάρα να γίνει πράσινη, για να προχωρήσουμε παρακάτω:



Εικόνα 38 CyberCIEGE: Εγκατάσταση των αρχείων του παιχνιδιού

11^{ο} βήμα: Στο βήμα αυτό, το μόνο που πρέπει να κάνουμε είναι να διαβάσουμε αυτά που μας γράφει, και πατάμε **Next> :**



Εικόνα 39 CyberCIEGE: Πληροφορίες σχετικές με το παιχνίδι

12^{ο} βήμα: Και με αυτό το βήμα, ολοκληρώθηκε επιτυχώς η εγκατάσταση του παιχνιδιού. Τέλος, πατάμε **Finish:**

Εικόνα 40 CyberCIEGE: Παράθυρο ολοκλήρωσης της εγκατάστασης

7.6 Χρήση του CyberCIEGE

Στην αρχή του κάθε σεναρίου παρουσιάζεται στο παίκτη μία οθόνη ενημέρωσης που περιγράφει το σενάριο και την επιχείρηση, για την οποία πρέπει να γίνει διαχείριση υπολογιστικών πόρων[66].

Σε μερικά σενάρια, ο παίκτης είναι υπεύθυνος για τη ρύθμιση υπαρχόντων υπολογιστικών συστημάτων συμπεριλαμβανομένης της σύνδεσής τους στο δίκτυο. Ακόμα, ο παίκτης είναι υπεύθυνος για να κάνει επιλογές φυσικής και διαδικαστικής ασφάλειας και για να προσλαμβάνει προσωπικό.

Σε άλλου τύπου σενάρια, ο παίκτης αγοράζει υπολογιστικά συστήματα και τα συνδέει στο δίκτυο. Υπάρχει ενημέρωση για το ποσό που διατίθεται για αγορά και συντήρηση εξοπλισμού και για πρόσληψη προσωπικού υποστήριξης.

Ο στόχος του παίκτη είναι να παράγει χρήματα για την επιχείρηση, μέσω αποτελεσματικής και ασφαλούς διαχείρισης των υπολογιστικών δικτύων της επιχείρησης.

[66] http://cisr.nps.edu/cyberciege/downloads/FISSEA_CyberCIEGE_PreConf.pdf

Προστασία από κλοπή προσωπικών στοιχείων

Για να πετύχει σε ένα συγκεκριμένο σενάριο ο παίκτης, πρέπει να κατανοήσει την ανάγκη του κάθε εικονικού χρήστη να έχει πρόσβαση σε διαφορετικά δεδομένα (δηλαδή τους στόχους του). Πρέπει στη συνέχεια να εξασφαλιστεί ο κατάλληλος εξοπλισμός και ο κατάλληλες διασυνδέσεις, για να μπορούν οι χρήστες να πετύχουν τους στόχους τους.

Ο παίκτης πρέπει να δημιουργήσει και να διατηρήσει ένα περιβάλλον όπου οι πληροφορίες προστατεύονται σύμφωνα με την πολιτική ασφαλείας της επιχείρησης. Η πολιτική αυτή ουσιαστικά σημαίνει ποιοι χρήστες επιτρέπεται να έχουν πρόσβαση σε ποια δεδομένα. Αποτυχία να προστατευτούν τα πολύτιμα δεδομένα, οδηγεί είτε σε άμεσες απώλειες της επιχείρησης είτε σε χαμένη παραγωγικότητα των εικονικών χρηστών.

Τα ακόλουθα είδη επιλογών επηρεάζουν την προστασία των δεδομένων με βάση την πολιτική ασφαλείας:

- Επιλογή στοιχείων που επιβάλουν επιλεγμένες πολιτικές ασφαλείας και εφαρμογή των στοιχείων σε κατάλληλες τοπολογίες.

- Ρύθμιση των στοιχείων για να βοηθήσουν στην επιβολή των πολιτικών (π.χ. αυτόματη αποσύνδεση μετά από κάποιο χρόνο αδράνειας).

- Διασύνδεση των στοιχείων με χρήση δικτύων (και η επιλογή να μην συνδεθούν ορισμένα στοιχεία).

- Καθοδήγηση των χρηστών να ακολουθούν συγκεκριμένες διαδικασίες (π.χ. να μην επιλέγουν ανόητα password) καθώς και επαρκής εκπαίδευσή τους.

- Επιβολή φυσικής ασφάλειας περιορίζοντας τους χρήστες που μπορούν να εισέλθουν σε μία ζώνη και επιβάλλοντας αυτούς τους περιορισμούς (π.χ. μέσω καμερών ασφαλείας, φρουρών κ.α.).

- Έλεγχος ιστορικού (π.χ. ποινικού και εργασιακού μητρώου) σε διαφορετικούς εικονικούς χρήστες.

Αυτές οι επιλογές ασφαλείας, επηρεάζουν τη προστασία των δεδομένων που μπορούν να δεχτούν επίθεση από βανδάλους, δυσαρεστημένους εργαζόμενους, επαγγελματίες επιτιθέμενους και ανεπαρκείς χρήστες.

Ο πιο δύσκολος τύπος επίθεσης, είναι αυτός των επαγγελματιών που στοχοποιούν συγκεκριμένα δεδομένα. Τα μέσα που χρησιμοποιούν οι επιτιθέμενοι, εξαρτώνται από την αξία που έχουν τα δεδομένα γι αυτούς.

Οι παίκτες μπορούν ξεκινήσουν και να κάνουν παύση της εξομοίωσης όποτε θέλουν. Είναι καλό να κατασκευάζονται τα δίκτυα και να αποφασίζονται οι πολιτικές ασφαλείας πριν ξεκινήσει η εξομοίωση. Όταν αυτή ξεκινήσει, οι εικονικοί χρήστες μπορούν να αρχίσουν να δημιουργούν και να έχουν πρόσβαση στα δεδομένα τους, τα οποία χωρίς την απαιτούμενη προσοχή κινδυνεύουν από επιθέσεις.

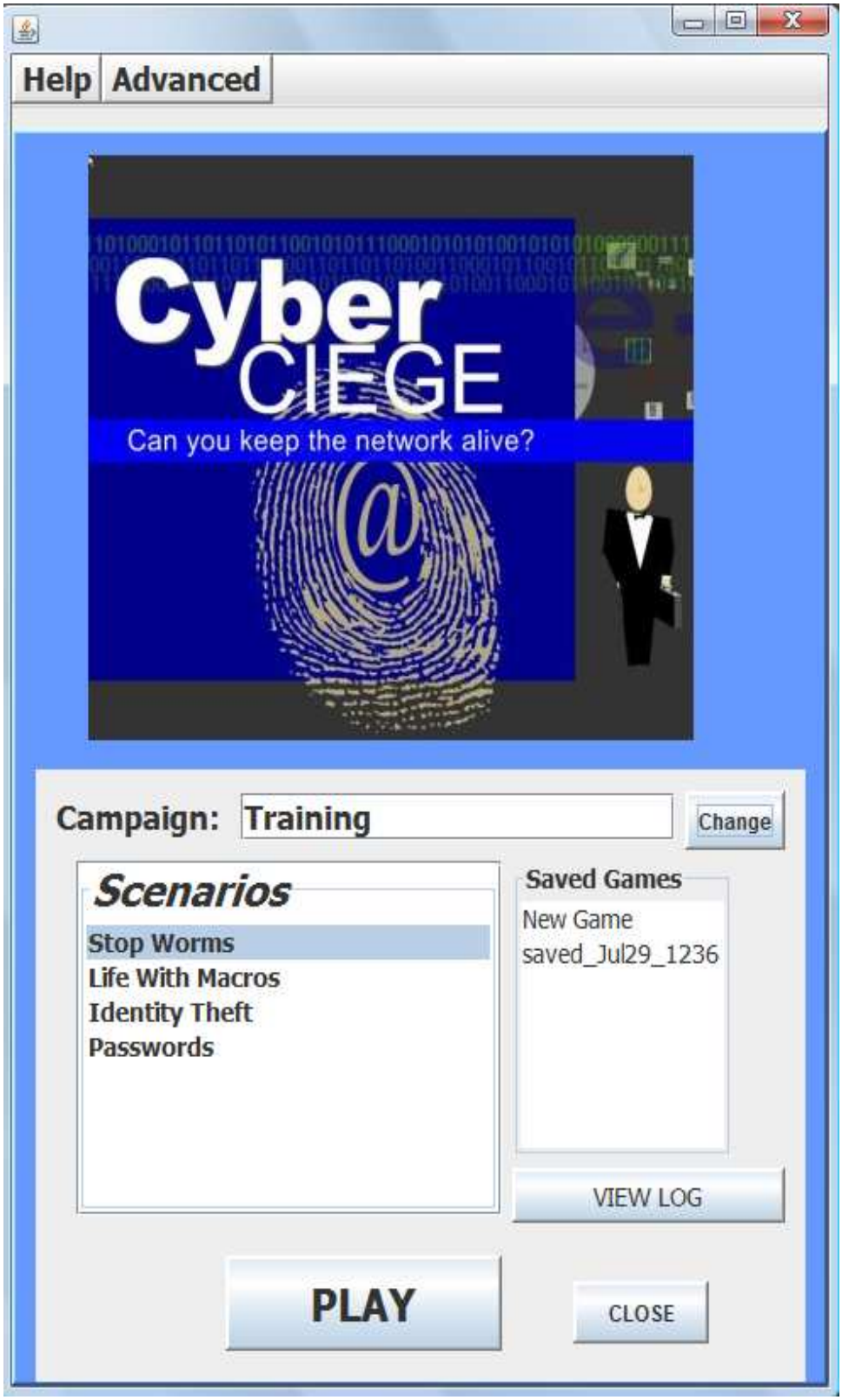
Κατά την διάρκεια της εξομοίωσης, οι παίκτες μπορούν να επιλέξουν και να παρατηρήσουν την κατάσταση της παραγωγικότητας και της ευτυχίας ενός χρήστη. Οι εικονικοί χρήστες που δεν μπορούν να πετύχουν τους στόχους τους, γίνονται νευρικοί και κτυπούν το πληκτρολόγιο.

Μία μπάρα μηνυμάτων στο κάτω μέρος της οθόνης και αναδυόμενα μηνύματα, χρησιμοποιούνται από τους σχεδιαστές του σεναρίου και για να ενημερώσουν τους φοιτητές για την πρόοδό τους.

7.7 Campaigns και σενάρια

Το CyberCIEGE περιλαμβάνει διάφορα Campaigns με τα σενάρια τους. Τα Campaigns αυτά είναι τα εξής: **Training**, **Staring Scenarios**, **Encryption**, **Identity Management** και τα **Extras**.

Για να τα δούμε πατάμε την επιλογή **Change** του Campaign **(*βλ. εικ.41*)**. Επιλέγοντας τα, εμφανίζεται μια σύντομη περιγραφή στο κάτω μέρος για τα σενάρια που περιλαμβάνει κάθε ένα από αυτά τα Campaigns **(*βλ. εικ.42*).**

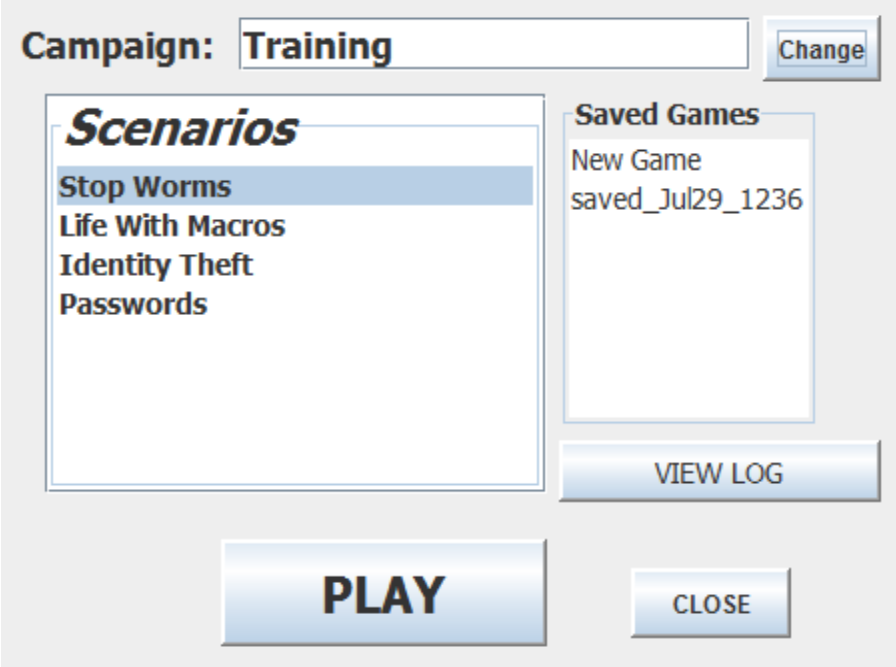


Εικόνα 41 CyberCIEGE: Αρχική οθόνη του CyberCIEGE

Εικόνα 42 CyberCIEGE: Campaigns

Στο σημείο αυτό θα δοθεί η περιγραφή των σεναρίων και με την βοήθεια των screenshots που ακολουθούν, θα δούμε ποια είναι τα σενάρια αυτά:

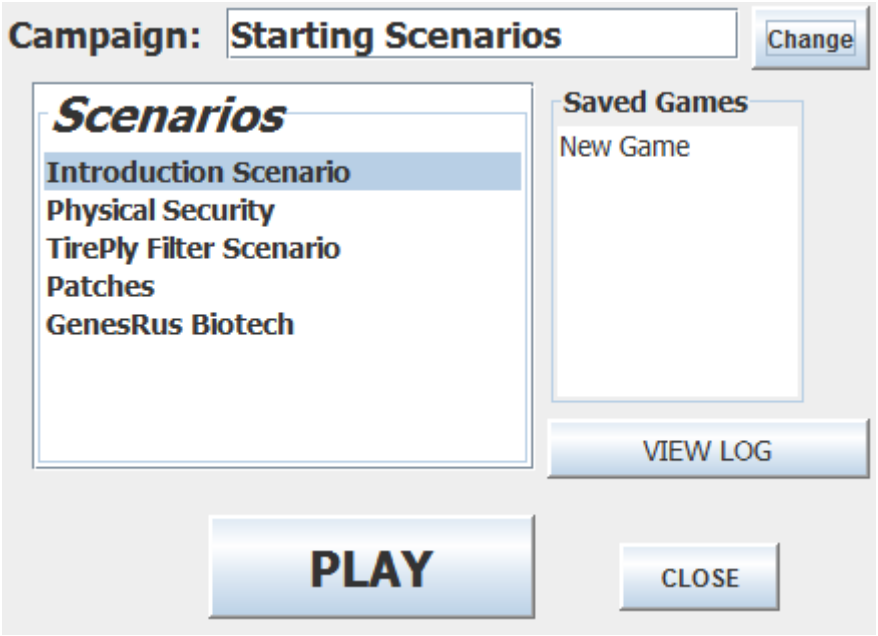
- **Training**
  Τα σενάρια του CyberCIEGE που αφορούν βασικά θέματα ασφαλείας υπολογιστών ***(βλ. εικ.43)***, απευθύνονται στο γενικό πληθυσμό των χρηστών υπολογιστών. Οι παίκτες ενθαρρύνονται να εξερευνήσουν τις συνέπειες διαφορετικών επιλογών ακόμα και αυτών που είναι λάθος.



Εικόνα 43 CyberCIEGE: Τα σενάρια του Training

- **Staring Scenarios**
  Τα σενάρια αυτά, ασχολούνται με θέματα ασφάλειας δικτύου (***βλ. εικ.44***). Είναι κλιμακούμενης δυσκολίας και έχουν σαν σκοπό να ενισχύσουν την εκπαίδευση για την ασφάλεια των πληροφοριών.

  Το 1ο σενάριο περιλαμβάνει συμβουλές βοήθειας ώστε να εξοικειωθούν οι παίκτες με την μηχανική του παιχνιδιού. Οι χρήστες ενθαρρύνονται να κάνουν λάθη και να εξερευνήσουν τις συνέπειες διαφορετικών επιλογών.



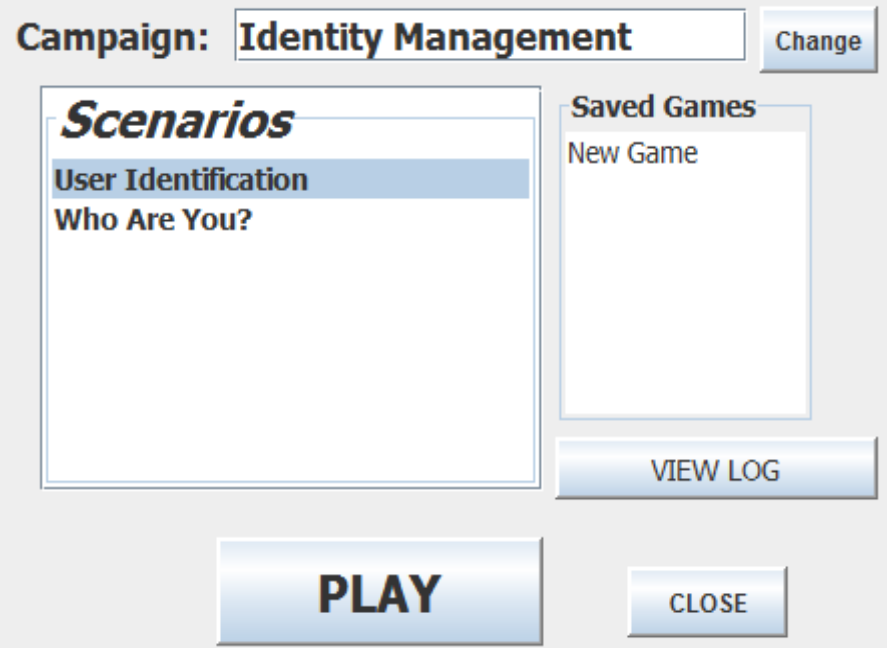
Εικόνα 44 CyberCIEGE: Τα σενάρια του Starting

- **Encryption**
  Στο σενάριο αυτό επιχειρείται η εισαγωγή στη χρήση της κρυπτογραφίας για την προστασία επικοινωνιών από διαρροή και παραποίηση **(*βλ. εικ.45*)**.

  Η ενότητα αυτή περιλαμβάνει επίσης τεχνικές για την διαχείριση της ταυτότητας των δεδομένων π.χ. πιστοποίηση της προέλευσης των δεδομένων.

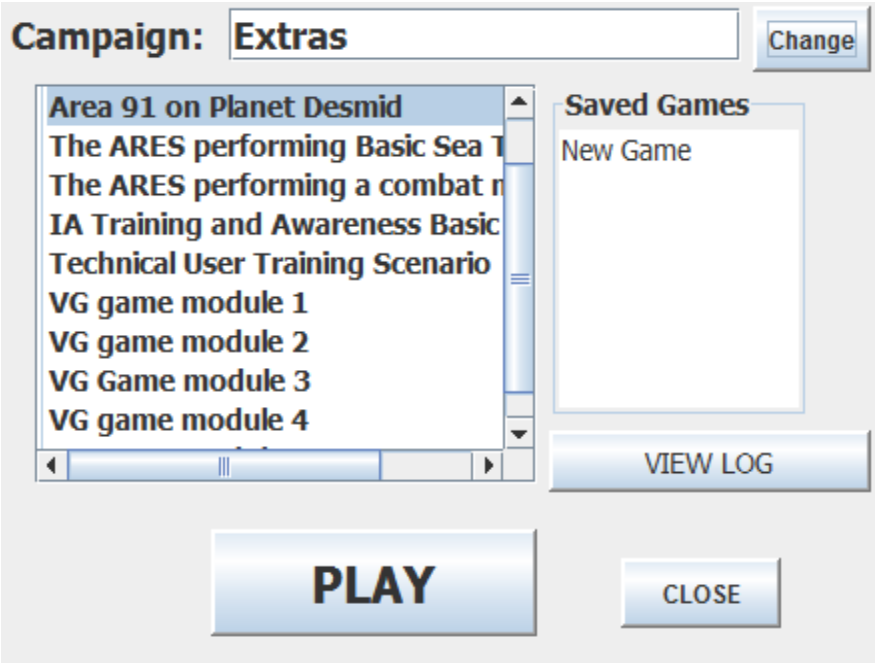
Εικόνα 45 CyberCIEGE: Τα σενάρια του Encryption

- **Identity Management**
  Στην ενότητα αυτή μελετάται η χρήση βιομετρικών scanners και συσκευών ανάγνωσης καρτών, με σκοπό την επιβεβαίωση της ταυτότητας των χρηστών (***βλ. εικ.46***):



Εικόνα 46 CyberCIEGE: Τα σενάρια του Identity Management

- **Extras**
  Τα σενάρια αυτά δεν είναι πλήρως αποσφαλματωμένα. Ακόμα η ενότητα αυτή περιλαμβάνει νέα σενάρια που μπορεί να μην είναι ολοκληρωμένα
  (***βλ. εικ.47***):



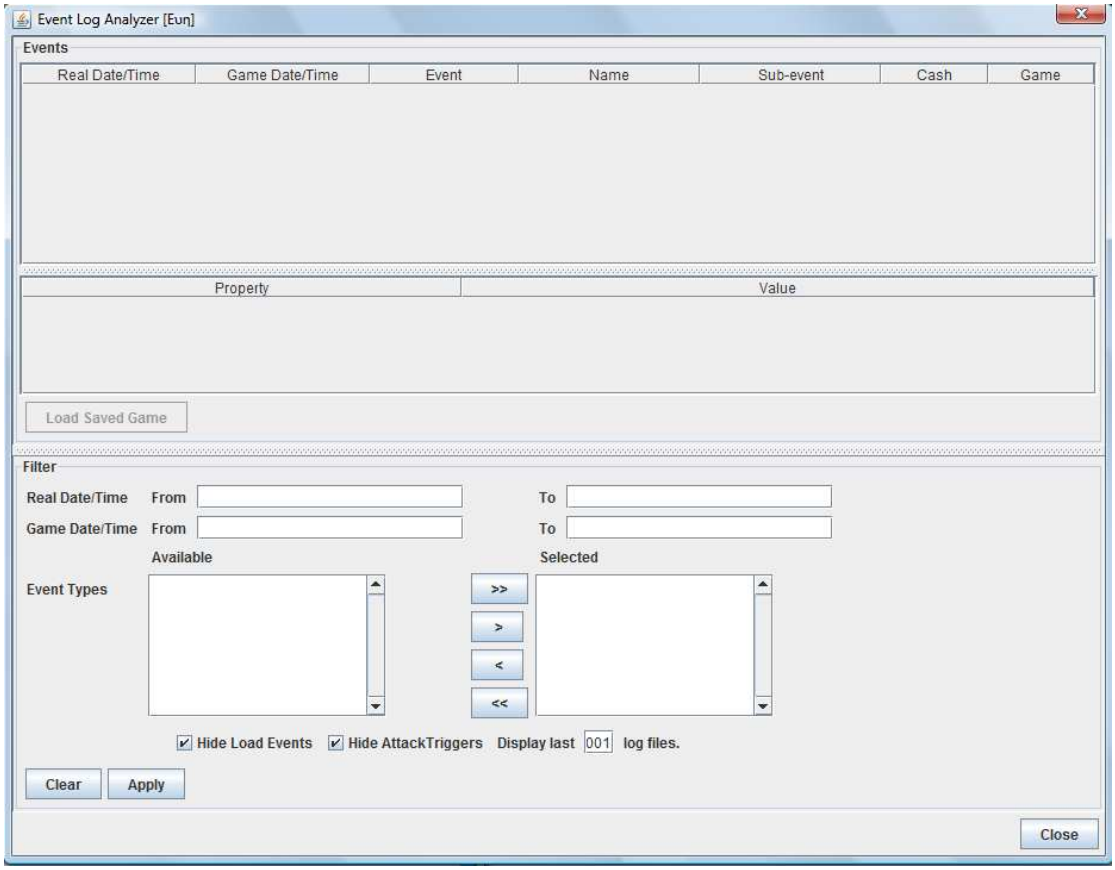
Εικόνα 47 CyberCIEGE: Τα σενάρια των Extras

7.7.1 Λίγα λόγια για το LOG

Το View Log είναι ένα μητρώο που αποθηκεύονται τα γεγονότα που έχουν λάβει χώρα στο παιχνίδι (***βλ. εικ.48***).

Στο πάνω μέρος υπάρχει ο πίνακας Events. Αυτός περιλαμβάνει επτά στήλες και αυτές κατά σειρά είναι:

- **Real Date/Time** όπου αποθηκεύεται η ημερομηνία και ώρα στην πραγματική ζωή,
- **Game Date/Time** όπου αποθηκεύεται η ημερομηνία και ώρα στο κόσμο του παιχνιδιού,
- **Event** όπου αποθηκεύεται ο τύπος του γεγονότος που λαμβάνει χώρα,
- **Name** όπου αποθηκεύεται το όνομα του γεγονότος που λαμβάνει χώρα.
- **Sub-event** όπου αποθηκεύεται ο τύπος δευτερευόντων γεγονότων που ακολουθούν τα κύρια και
- **Cash** όπου αποθηκεύεται το ποσό των χρημάτων που διαθέτει ο παίκτης στην εκτέλεση κάθε γεγονότος. Η τελευταία στήλη μας δείχνει τον αριθμό παιχνιδιού στον οποίο λαμβάνουν χώρα τα γεγονότα.



Εικόνα 48 CyberCIEGE: View Log

Όταν επιλέξουμε ένα γεγονός, κάτω από τον πίνακα, εμφανίζονται λεπτομέρειες για το γεγονός.

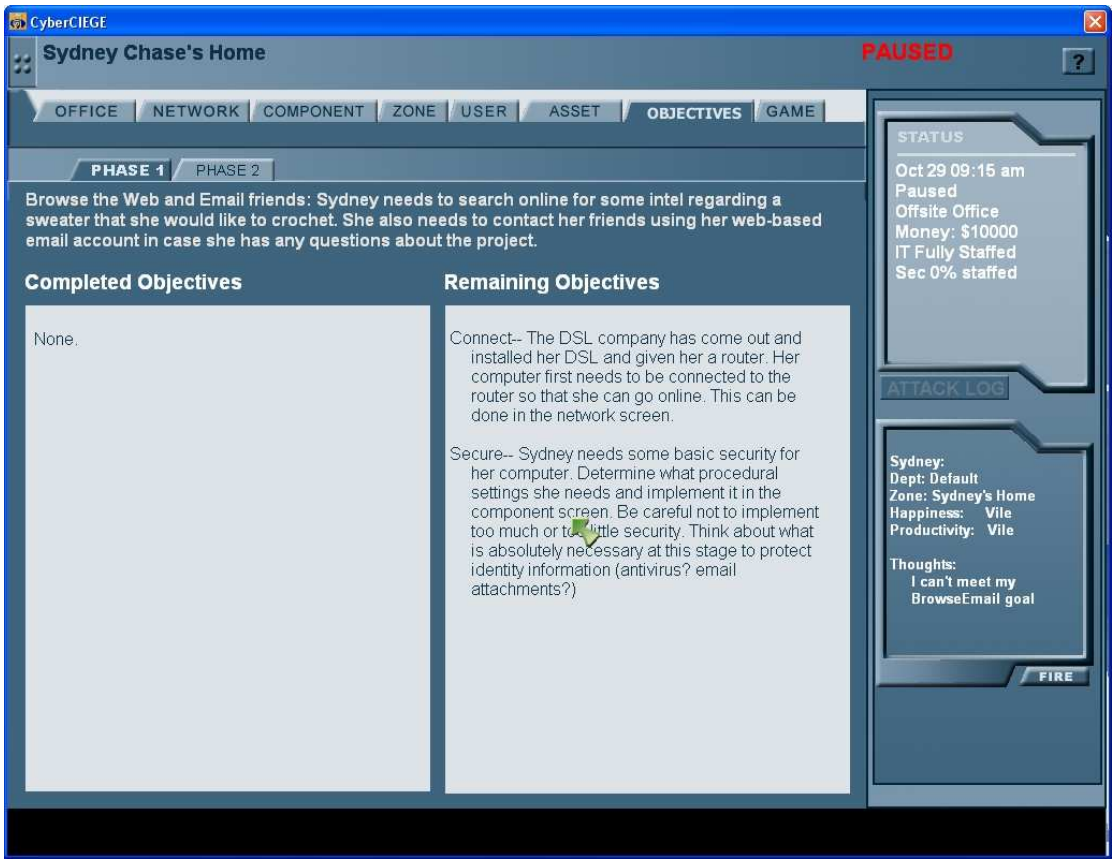
Και στο κομμάτι **Filter** μπορούμε να εφαρμόσουμε διάφορες παραμέτρους και να περιορίσουμε ποια γεγονότα εμφανίζονται στο παραπάνω πίνακα.

7.7.2 Σενάριο Identity Theft – Εκτέλεση σεναρίου σε επίπεδο Training

Στο έτοιμο αυτό σενάριο του CyberCIEGE, πρωταγωνιστεί μια κοπέλα, η Sydney, η οποία θέλει να πραγματοποιήσει μια on-line αγορά και να στείλει e-mail σε φίλους. Παρακάτω περιγράφονται αναλυτικά τα βήματα του σεναρίου:

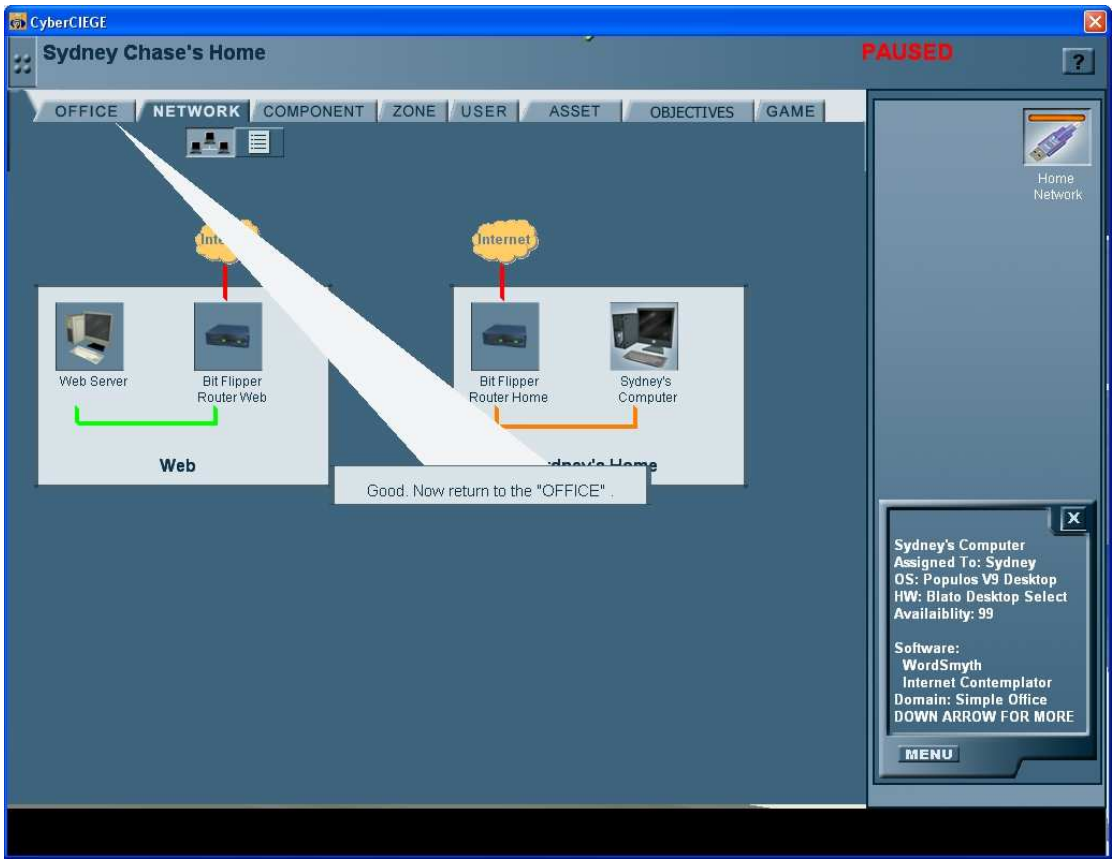
Στην πρώτη οθόνη του CyberCIEGE και αφού σιγουρευτούμε ότι βρισκόμαστε στο Campaign **Training** επιλέγουμε το σενάριο Identity Theft.

Μπαίνοντας στο σενάριο, πρέπει να δούμε πρώτα την καρτέλα “**OBJECTIVES**” (στόχους):



Εικόνα 49 CyberCIEGE: Φάση1 - Objectives

Βρισκόμαστε στη **φάση 1**: Το πρώτο πράγμα που πρέπει να γίνει είναι να συνδεθεί η Sydney στο διαδίκτυο. Αυτό ρυθμίζεται από την καρτέλα “**NETWORK**”.

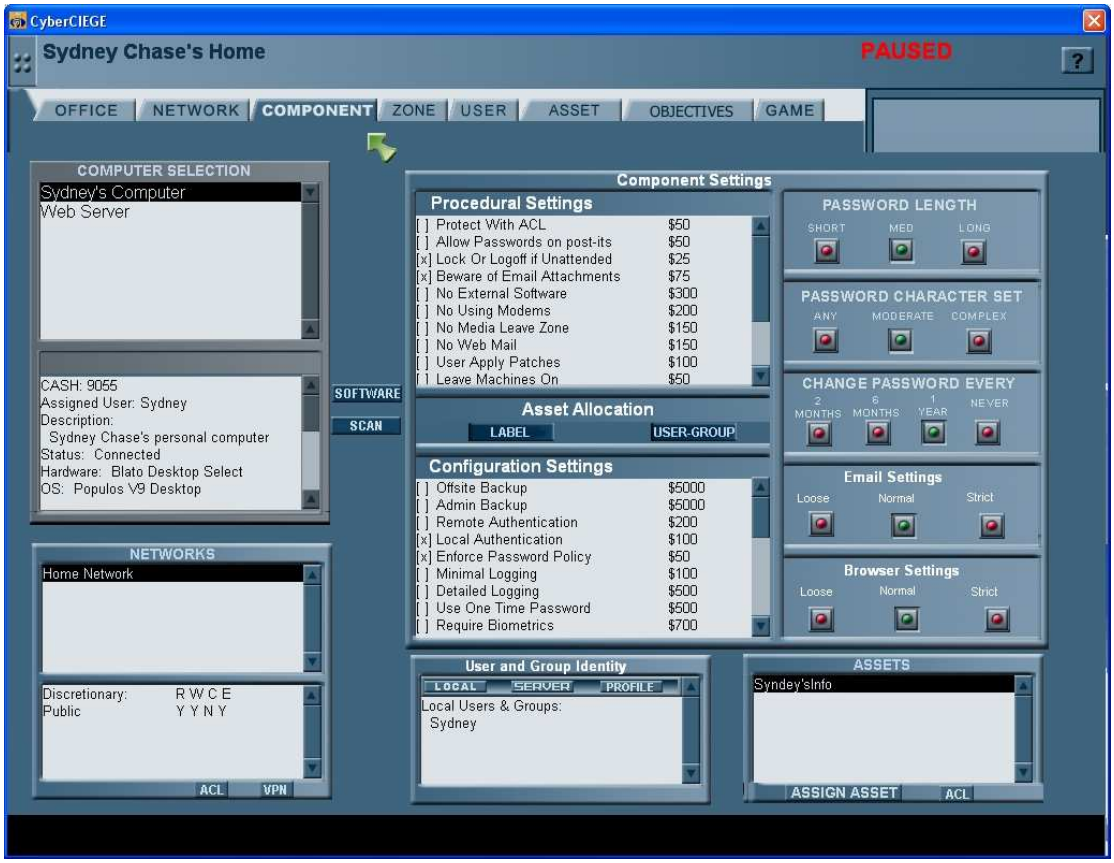


Εικόνα 50 CyberCIEGE: Ρύθμιση σύνδεσης δικτύου

Πηγαίνουμε στην καρτέλα “**OFFICE**” και πατάμε το **play**. Ο πρώτος στόχος έχει επιτευχθεί.

Εικόνα 51 CyberCIEGE: Το πρόγραμμα τρέχει

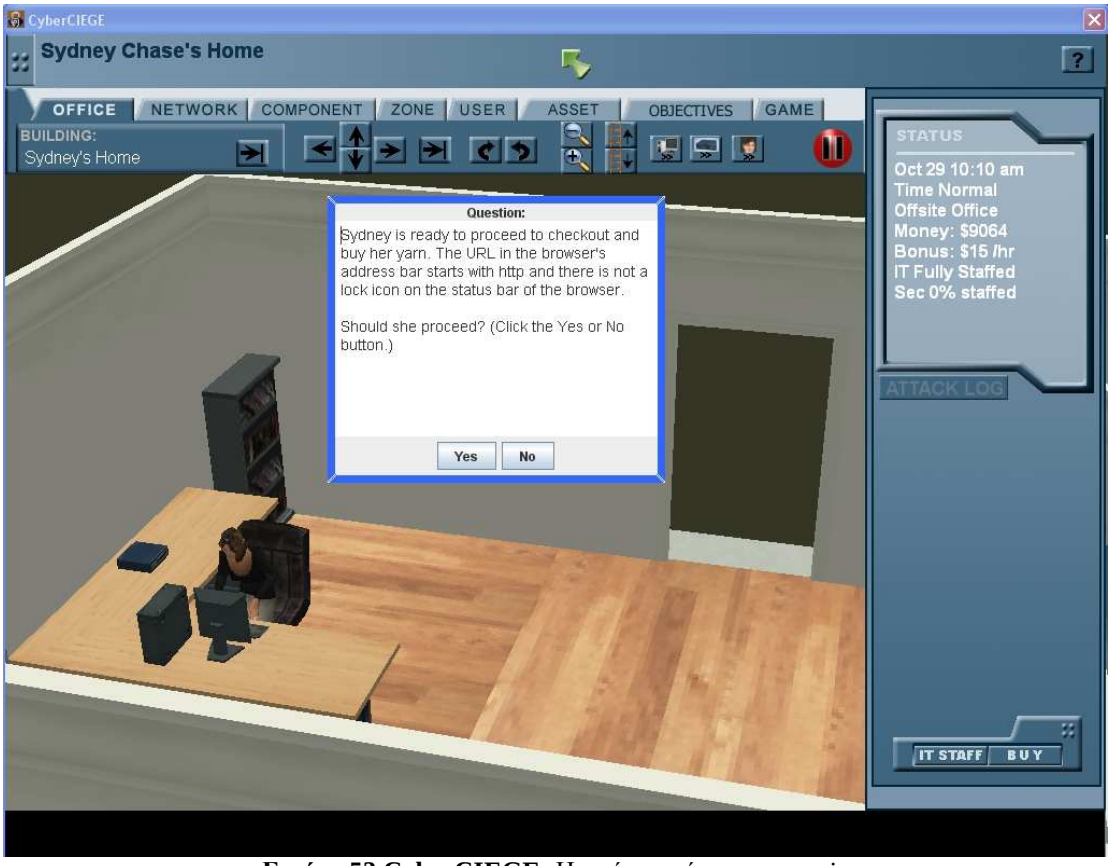
Σε λίγο θα δούμε ένα μήνυμα που μας λέει ότι πρέπει να γίνουν οι απαραίτητες ρυθμίσεις για να είναι ασφαλής η πλοήγηση στο διαδίκτυο. Αυτό γίνεται μέσα από την καρτέλα "**COMPONENT**". Πατάμε πρώτα **pause** και μετά επιλέγουμε την καρτέλα αυτή.



Εικόνα 52 CyberCIEGE: Ρυθμίσεις ασφαλείας υπολογιστή

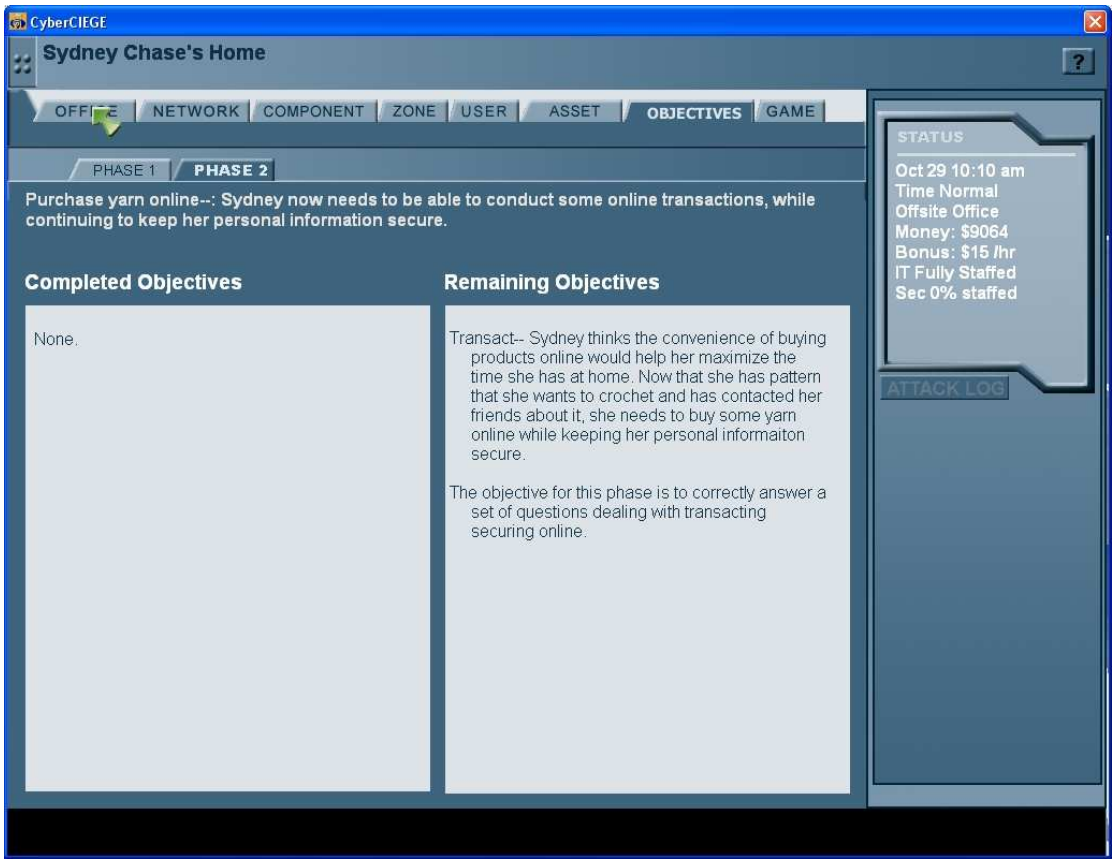
Αφού γίνουν οι απαραίτητες ρυθμίσεις επιστρέφουμε στη καρτέλα "**OFFICE**" και πατάμε πάλι το **Play**. Έχει επιτευχθεί και ο δεύτερος στόχος. Τέλος, με τις ρυθμίσεις γι αυτό το σενάριο.

Τώρα το CyberCIEGE θα μας κάνει μια ερώτηση την οποία αν απαντήσουμε σωστά θα προχωρήσουμε στη φάση 2.



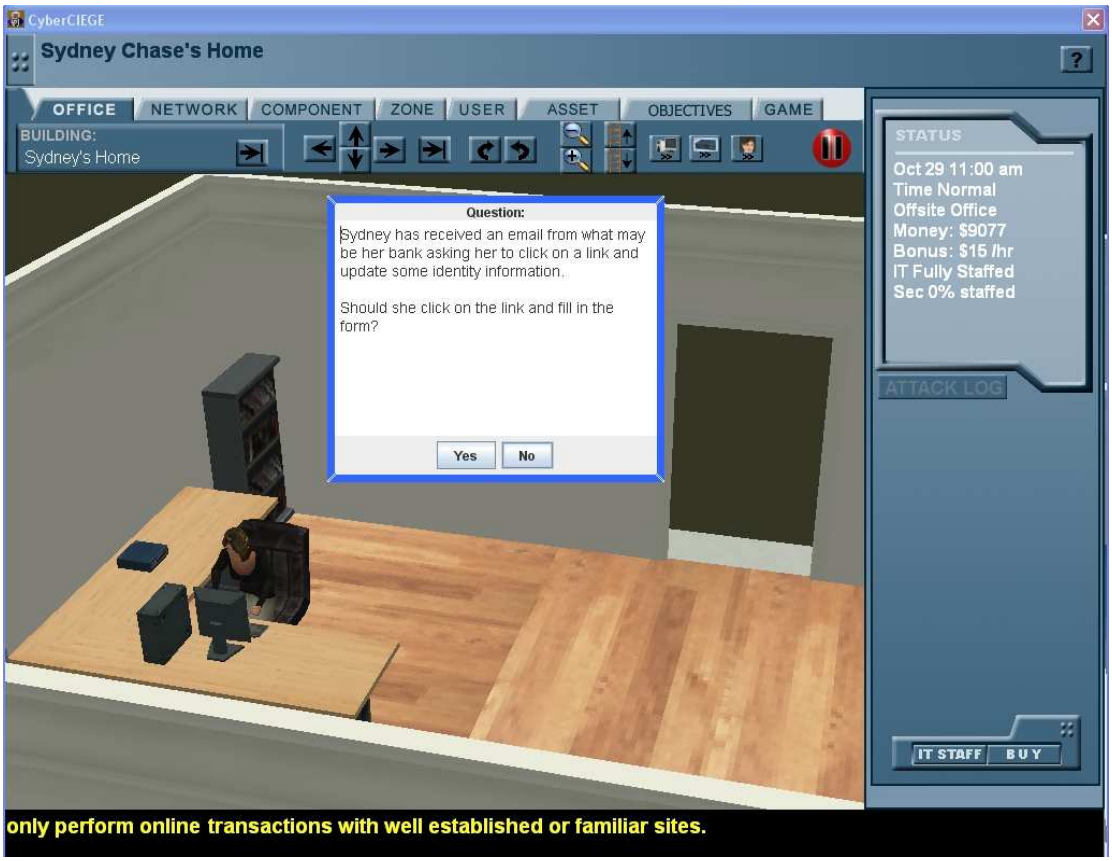
Εικόνα 53 CyberCIEGE: Η πρώτη ερώτηση του quiz

Αφού απαντηθεί σωστά η ερώτηση ξεκλειδώνει η **φάση 2**. Μπορούμε να δούμε τους στόχους της φάσης στην καρτέλα "**OBJECTIVES**".



Εικόνα 54 CyberCIEGE: Φάση2 - Objectives

Όπως φαίνεται και στην εικόνα, στη φάση αυτή δε χρειάζεται κάποια ρύθμιση. Ο παίκτης πρέπει να απαντήσει σε μια σειρά ερωτήσεων.



Εικόνα 55 CyberCIEGE: Μία από τις ερωτήσεις της φάσης2

Οι ερωτήσεις αυτές προϋποθέτουν βασικές γνώσεις ασφάλειας ηλεκτρονικού ταχυδρομείου και συναλλαγών. Εφόσον απαντηθούν σωστά, ολοκληρώνεται επιτυχώς το σενάριο και ξεκλειδώνεται το επόμενο.

7.8 Κατάσταση του CyberCIEGE

Οι φοιτητές στη σχολή του Ναυτικού των Η.Π.Α., ανέπτυξαν ένα αριθμό σεναρίων κατά την δημιουργία του προγράμματος. Στην τελική έκδοση προστέθηκαν παραπάνω σενάρια[67].

Μία έκδοση περιορισμένης διάθεσης του CyberCIEGE, δημιουργήθηκε και τον Φεβρουάριο του 2005 έγινε διαθέσιμη δωρεάν στις κυβερνητικές υπηρεσίες των Η.Π.Α.. Στην συνέχεια, μία δοκιμαστική έκδοση του εμπορικού προϊόντος έγινε διαθέσιμη από την εταιρεία Rivermind. Το CyberCIEGE κυκλοφόρησε επίσημα την άνοιξη του 2005.

[67] http://cisr.nps.edu/cyberciege/downloads/FISSEA_CyberCIEGE_PreConf.pdf

Η επεκτασιμότητα του CyberCIEGE προσφέρει μία μοναδική ευκαιρία στους εκπαιδευτές θεμάτων ασφαλείας να συμβάλλουν στην περαιτέρω ανάπτυξή του. Υπάρχει μία online κοινότητα για το CyberCIEGE, όπου οι εκπαιδευτές μπορούν να μοιραστούν σενάρια με άλλους. Ακόμα, μπορεί κάποιος εκπαιδευτής να πάρει το σενάριο κάποιου άλλου και να το τροποποιήσει. Το μοντέλο αυτό θυμίζει αυτό της Open Source κοινότητας.

7.9 Σύγκριση του CyberCIEGE με παρόμοια εργαλεία

Το **CyberProject** είναι ένα παιχνίδι που σχετίζεται με την ασφάλεια των πληροφοριών[68]. Δημιουργήθηκε με την χρηματοδότηση του γραφείου του υφυπουργού άμυνας των Η.Π.Α.. Είναι μία εξομοίωση διαχείρισης πόρων ενός μικρού οργανισμού με απλή δικτύωση. Παρέχει στο παίκτη μερικά χρήματα, τα οποία ανεπαρκούν, ώστε να αγοράσει εξοπλισμό για να αντιμετωπίσει διάφορες απειλές.

Τα μειονεκτήματά του είναι τα παρακάτω:

- Δεν υπάρχει η έννοια της πολιτικής ασφαλείας στον οργανισμό.
- Δεν είναι άμεσα επεκτάσιμο από τους χρήστες, αντίθετα διαθέτει ένα προκαθορισμένο αριθμό δραστηριοτήτων.
- Δεν διαθέτει εικονικό κόσμο με εικονικούς ανθρώπους και προσωπικούς στόχους για τον καθένα.

Άλλος ανταγωνιστής του CyberCIEGE είναι το **Information Security system (ISWS)**[69]. Αυτό δημιουργήθηκε για το πανεπιστήμιο άμυνας των Η.Π.Α. και είναι μία εξομοίωση που ασχολείται εκτενώς με συγκεκριμένες επιθέσεις και μέτρα άμυνας. Η εξομοίωση αυτή είναι ουσιαστικά ένα tutorial, για την αντιμετώπιση επιθέσεων μέσω δικτύου.

Κάθε άσκηση ασχολείται με ένα τύπο επίθεσης ξεχωριστά. Στους παίκτες παρουσιάζεται η πολιτική του οργανισμού και αυτοί πρέπει να επιλέξουν τα κατάλληλα αμυντικά εργαλεία, για να αντιμετωπίσουν τις επιθέσεις.
Σε αντίθεση με το CyberCIEGE, η εξομοίωση αυτή, είναι αφηρημένη και στατική. Δεν υπάρχει εικονικός κόσμος και επιπλέον δεν υπάρχει δυνατότητα επεκτασιμότητας.

Τέλος, υπάρχει το **AI Wars: The Awakening**[70]**,** που είναι ένα τρισδιάστατο παιχνίδι, που απαιτεί στρατηγική και δράσεις. Αυτό το παιχνίδι είναι καθαρά για διασκέδαση και δεν παρέχει ρεαλιστικές πληροφορίες για τις διάφορες επιθέσεις.

[68] http://cisr.nps.edu/cyberciege/downloads/FISSEA_CyberCIEGE_PreConf.pdf
[69] http://www.johnsaunders.com/papers/securitysimulation.htm
[70] http://pc.ign.com/objects/014/014949.html

Παράρτημα Α

e-SHOP.gr ----ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ----

*"Η **e-shop.gr AE** και το **www.e-shop.gr**, δημιούργησαν την παρούσα ιστοσελίδα με μοναδικό σκοπό την εξυπηρέτηση των πελατών τους. Η ιστοσελίδα e-shop.gr είναι απλή και φιλική στη χρήση της ενώ έχει σχεδιαστεί για να ανταποκρίνεται στις συγκεκριμένες ανάγκες του κάθε χρήστη. Για να επιτευχθεί η καλύτερη εξυπηρέτησή σας, είναι σημαντικό εσείς, ο πελάτης μας, να καταλάβετε ότι πρέπει να μας παρέχετε συγκεκριμένες πληροφορίες που αφορούν την διεκπεραίωση της παραγγελίας σας και οι οποίες διαφυλάσσονται από εμάς.*

Η παρούσα Δήλωση Προστασίας Προσωπικών Δεδομένων και οι επισυναπτόμενοι σε αυτήν Όροι και Προϋποθέσεις Χρήσης της παρούσας ιστοσελίδας περιγράφουν τη μέθοδο συλλογής δεδομένων από την ιστοσελίδα e-shop.gr, τη χρήση αυτών των δεδομένων από εμάς και τους όρους και προϋποθέσεις χρήσεως της παρούσας ιστοσελίδας. Η παρούσα Δήλωση Προστασίας Προσωπικών Δεδομένων αναφέρεται αποκλειστικά και μόνο στα προσωπικά σας δεδομένα, τα οποία εσείς μας παρέχετε κατά τη διάρκεια των παραγγελιών σας στην παρούσα ιστοσελίδα.

Γενικά

Οι πληροφορίες που έχουν δοθεί εκούσια από τους χρήστες της αναφερόμενης ιστοσελίδας, χρησιμοποιούνται από το e-shop.gr, προκειμένου οι χρήστες του να έχουν άμεση και ουσιαστική επικοινωνία με το κατάστημα, να τους παρέχονται απαντήσεις σε συγκεκριμένα ερωτήματα που θέτουν και τέλος να εξυπηρετούνται και να εκτελούνται οι παραγγελίες τους. Οι πληροφορίες που συλλέγει το e-shop.gr μέσω της ιστοσελίδας έχουν ως σκοπό να μετρήσουν το αριθμό επισκεψιμότητας της, να καθορίσουν τις απαιτήσεις των πελατών για περισσότερα προϊόντα και να διευκολύνουν στις συνναλαγές με την εταιρεία. Το e-shop.gr δεν διανέμει σε κανένα άλλο οργανισμό ή συνεργάτη που δεν συνδέεται με το e-shop.gr τις ηλεκτρονικές διευθύνσεις, ή οποιαδήποτε άλλη πληροφορία που αφορά τους χρήστες και πελάτες του.

Συγκέντρωση πληροφοριών

Το e-shop.gr σχεδίασε την ιστοσελίδα του έτσι ώστε οι χρήστες του να μπορούν να την επισκέπτονται χωρίς να χρειάζεται να αποκαλύπτουν τη ταυτότητα τους εκτός και αν το επιθυμούν. Ζητείται από τους επισκέπτες της ιστοσελίδας μας, να μας παρέχουν με προσωπικά τους δεδομένα μόνο στη περίπτωση που θέλουν να παραγγείλουν προϊόν(τα), να εγγραφούν στην ιστοσελίδα μας και/ή να στείλουν email στο e-shop.gr.

<u>Χρήση των Πληροφοριών.</u> Το e-shop.gr συλλέγει τέσσερις τύπους πληροφοριών σχετικά με τους χρήστες: (1) στοιχεία που ο χρήστης μας δίνει κατά την εγγραφή του ως πελάτης, (2) στοιχεία που ο χρήστης μας δίνει προκειμένου να εκτελεστεί η παραγγελία του από το e-shop.gr, (3) στοιχεία που ο χρήστης μας δίνει σε συμμετοχές διαγωνισμών που πραγματοποιούνται κατα καιρούς, (4) στοιχεία που ο χρήστης μας δίνει για ενεργοποιήσεις υπηρεσιών τηλεφωνίας και internet.

Προστασία από κλοπή προσωπικών στοιχείων

Κατά την συμπλήρωση οποιασδήποτε φόρμας παραγγελίας στην ιστοσελίδα μας, θα σας ζητηθεί το ονοματεπώνυμο, η διεύθυνση, ο ταχυδρομικός κωδικός της περιοχής σας, η ηλεκτρονική σας διεύθυνση, το τηλέφωνο σας, στοιχεία πιστωτικής κάρτας, ο τρόπος πληρωμής της παραγγελίας. Συμπληρωματικά μπορεί να σας ζητηθούν και πιο συγκεκριμένες πληροφορίες, όπως στοιχεία αποστολής - παράδοσης μιας παραγγελίας, στοιχεία τιμολόγησης ή λεπτομέρειες σχετικά με προσφορά που έχετε ζητήσει. Το e-shop.gr κάνει χρήση των πληροφοριών που μας δίνετε κατά τη διάρκεια της ηλεκτρονικής αποστολής της φόρμας, προκειμένου να επικοινωνήσουμε μαζί σας σχετικά με (i) την παράδοση της παραγγελίας στο χώρο σας, (ii) για επιβεβαίωση και ταυτοποίηση του πελάτη σε κάθε αναγκαία περίπτωση, (iii) για νέα ή εναλλακτικά προϊόντα που προσφέρονται από το e-shop.gr, (iv) ειδικές προσφορές του e-shop.gr, (v) ενεργοποίηση υπηρεσίας τηλεφωνίας ή internet, (vi) παραλαβή δώρων μετά από κλήρωση διαγωνισμού. Έχετε τη δυνατότητα να επιλέξετε αν θέλετε ή όχι να λαμβάνετε τέτοιου είδους επικοινωνίες από το e-shop.gr στέλνοντας το αίτημα σας μέσω e-mail στην ηλεκτρονική διεύθυνση sales@e-shop.gr

Πρόσβαση στις Πληροφορίες. Κάθε διεκπαιρέωση παραγγελίας απαιτεί την συλλογή προσωπικών στοιχείων, για παράδοση ή κράτηση μιας παραγγελίας. Επίσης η χρήση πιστωτικής κάρτας, για την χρέωση της οποίας χρειάζονται δικαιολογητικά ταυτοποίησης στοιχείων νόμιμου κατόχου την πρώτη και μόνο φορά διασφαλίζεται σε κάθε περίπτωση. Οποιοδήποτε δικαιολογητικό και έγγραφο πιστοποιεί και δηλώνει την ταυτότητα του πελάτη παραμένει αυστηρά απόρρητο και ελέγχεται μόνο από το αρμόδιο υπεύθυνο τμήμα του e-shop.gr. Η εκ μέρους σας προσκόμιση των προσωπικών σας δεδομένων, σημαίνει ότι συναινείτε τα δεδομένα αυτά να χρησιμοποιούνται από τους υπαλλήλους του e-shop.gr για τους λόγους που αναφέρθηκαν παραπάνω. Το e-shop.gr απαιτεί από τους υπαλλήλους του και τους συντηρητές της ιστοσελίδας του να παρέχουν στους χρήστες-πελάτες του το επίπεδο ασφαλείας που αναφέρεται στη παρούσα Δήλωση Προστασίας Προσωπικών Δεδομένων. Σε καμία άλλη περίπτωση το e-shop.gr δεν μπορεί να μοιραστεί με άλλους τα προσωπικά σας στοιχεία χωρίς πρότερη δική σας συναίνεση, εκτός και αν αυτό απαιτηθεί μέσω της νομίμου οδού. Παρακαλούμε όπως λάβετε υπόψη σας ότι κάτω από συγκεκριμένες προϋποθέσεις που επιτρέπεται ή επιβάλλεται από το νόμο ή βάση δικαστικής απόφασης, η συλλογή, χρήση και η αποκάλυψη των προσωπικών δεδομένων σας, τα οποία έχουν συλλεχθεί online χωρίς την εκ μέρους σας πρότερη συναίνεση (για παράδειγμα σε περίπτωση δικαστικής απόφασης).

Cookies

Το e-shop.gr έχει τη δυνατότητα να χρησιμοποιεί cookies ως μέρος της διευκόλυνσης αλλά και λειτουργίας των υπηρεσιών μέσω της ιστοσελίδας του. Τα Cookies είναι μικρά αρχεία (text files), τα οποία αποστέλλονται και φυλάσσονται στον ηλεκτρονικό υπολογιστή του χρήστη, επιτρέποντας σε ιστοσελίδες όπως το e-shop.gr, να λειτουργούν απρόσκοπτα και χωρίς τεχνικές ανωμαλίες, να συλλέγονται πολλαπλές επιλογές του χρήστη, να αναγνωρίζουν τους συχνούς χρήστες, να διευκολύνουν την πρόσβαση τους σε αυτή, και για τη συλλογή δεδομένων για τη βελτίωση του περιεχομένου της ιστοσελίδας.

Προστασία από κλοπή προσωπικών στοιχείων

Τα Cookies δεν προκαλούν βλάβες στους ηλεκτρονικούς υπολογιστές των χρηστών αλλά και στα αρχεία που φυλάσσονται σε αυτούς. Χρησιμοποιούμε τα cookies για να σας παρέχουμε πληροφορίες και να διεκπεραιώνονται οι παραγγελίες σας ενώ σε κάθε έξοδό σας από το site διαγράφονται αυτόματα. Πρέπει να έχετε υπόψη σας ότι τα cookies είναι απόλυτα αναγκαία προκειμένου να λειτουργεί σωστά και απρόσκοπτα η ιστοσελίδα www.e-shop.gr.

Διόρθωση, Τροποποίηση ή Διαγραφή Πληροφοριών

Το e-shop.gr επιτρέπει στους χρήστες του να διορθώνουν, αλλάζουν, συμπληρώνουν ή να διαγράφουν δεδομένα και πληροφορίες που έχουν προσκομιστεί στο e-shop.gr. Εάν επιλέξετε να διαγράψετε μια πληροφορία, το e-shop.gr θα ενεργήσει έτσι ώστε να διαγραφεί αυτή η πληροφορία από τα αρχεία του άμεσα. Για τη προστασία και την ασφάλεια του χρήστη το e-shop.gr θα προσπαθήσει να βεβαιωθεί ότι το πρόσωπο που κάνει τις αλλαγές είναι όντως το ίδιο πρόσωπο με το χρήστη. Για να έχετε πρόσβαση, να αλλάξετε ή να διαγράψετε τα προσωπικά σας δεδομένα, για να αναφέρετε προβλήματα σχετικά με τη λειτουργία της ιστοσελίδας ή για να κάνετε οποιοδήποτε ερώτημα επικοινωνήστε με το e-shop.gr μέσω www.e-shop.gr ή μέσω e-mail στην ηλεκτρονική διεύθυνση sales@e-shop.gr. Η αλλαγή ή η διόρθωση των προσωπικών σας δεδομένων μπορεί να γίνει επίσης μέσω του σελίδας εγγραφής του e-shop.gr. Παρακαλούμε όπως λάβετε υπόψη σας ότι θα κάνουμε ότι είναι δυνατό προκειμένου να προστατεύσουμε τα προσωπικά σας δεδομένα, αλλά η προστασία τους κωδικού πρόσβασης σας στην ιστοσελίδα μας εξαρτάται και από εσάς.

Ασφάλεια συναλλαγών

Το e-shop.gr δεσμεύεται όσον αφορά στην εξασφάλιση της ασφάλειας και της ακεραιότητας των δεδομένων που συλλέγει σχετικά με τους χρήστες της ιστοσελίδας του. Το e-shop.gr έχει υιοθετήσει διαδικασίες, οι οποίες προφυλάσσουν τα προσωπικά δεδομένα που οι χρήστες προσκομίζουν στην ιστοσελίδα του ή του παρέχουν με οποιοδήποτε άλλο μέσο (πχ. τηλεφωνικά). Αυτές οι διαδικασίες προστατεύουν τα δεδομένα των χρηστών από οποιαδήποτε μη επιτρεπόμενη πρόσβαση ή αποκάλυψη, απώλεια ή κακή χρήση, και αλλαγή ή καταστροφή. Βοηθούν επίσης στο να πιστοποιείται ότι τα στοιχεία αυτά είναι ακριβή και χρησιμοποιούνται σωστά. Η σύνδεσή σας σε αυτό είναι ασφαλής διότι χρησιμοποιεί τεχνολογία SSL (Secure Socket Layer). Η τεχνολογία SSL στηρίζεται σε ένα κωδικό κλειδί για κρυπτογράφηση των δεδομένων πριν αποσταλούν μέσω της (SSL) σύνδεσης.

Ο έλεγχος ασφαλείας μεταξύ των δεδομένων και του Server γίνεται με βάση το μοναδικό κωδικό κλειδί διασφαλίζοντας στο ακέραιο την επικοινωνία. Οι φυλλομετρητές (browsers) Netscape Navigator, Internet Explorer, Mozilla Firefox, Opera, Safari υποστηρίζουν το πρωτόκολλο SSL και προτείνεται η χρήση τους για τήν σύνδεση στην ιστοσελίδα του e-shop.gr.

Περιοδικές Αλλαγές

Συνεχώς το e-shop.gr επεκτείνει, ενημερώνει και βελτιώνει την ιστοσελίδα του, και τα σχετικά με αυτή προϊόντα και υπηρεσίες, θα ανανεώνει και τη παρούσα πολιτική.

Σας συστήνουμε να διαβάζετε τη διαδικασία αυτή σε τακτά χρονικά διαστήματα, προκειμένου να ενημερώνεστε για τυχόν αλλαγές στο περιεχόμενο της παρούσας πολιτικής προστασίας προσωπικών δεδομένων. Η πολιτική αυτή θα τροποποιείται από καιρό σε καιρό χωρίς προηγούμενη προειδοποίηση προς τους χρήστες.

Αποδοχή των Διαδικασιών Προστασίας τους Απορρήτου που εφαρμόζει το e-shop.gr

Εάν χρησιμοποιείτε την παρούσα ιστοσελίδα αποδέχεσθε και συναινείτε με τη παρούσα Δήλωση Προστασίας Προσωπικών Δεδομένων καθώς επίσης και με τους όρους και τις Προϋποθέσεις χρήσης της ιστοσελίδας που έχουν ανακοινωθεί μέσω αυτής.

ΟΡΟΙ ΚΑΙ ΠΡΟΥΠΟΘΕΣΕΙΣ ΧΡΗΣΗΣ

Περιορισμένη άδεια

Το e-shop.gr, υπό τους όρους και τις προϋποθέσεις που τίθενται στο παρόν και όλους τους εφαρμοστέους νόμους και κανονισμούς, σας χορηγεί ένα μη αποκλειστικό, αμεταβίβαστο, προσωπικό, περιορισμένο δικαίωμα πρόσβασης, χρήσης και παρουσίασης αυτής της ιστοσελίδας και των περιεχομένων στοιχείων της. Αυτή η άδεια δεν αποτελεί μεταβίβαση τίτλου στην ιστοσελίδα και στα στοιχεία της και υπόκειται στους ακόλουθους περιορισμούς: (1) πρέπει να διατηρείτε σε όλα τα αντίγραφα της ιστοσελίδας και των στοιχείων της, όλες τις επισημειώσεις που αφορούν πνευματικά δικαιώματα και άλλα ιδιοκτησιακά δικαιώματα και (2) δεν μπορείτε να τροποποιήσετε την ιστοσελίδα και τα στοιχεία της με κανένα τρόπο ή να αναπαράγετε ή να παρουσιάσετε δημοσίως, ή να διανείμετε ή με άλλο τρόπο να χρησιμοποιήσετε την ιστοσελίδα και τα στοιχεία της για οποιοδήποτε δημόσιο ή εμπορικό σκοπό, εκτός εάν άλλως επιτρέπεται με το παρόν.

Μεταβολές

Το e-shop.gr διατηρεί το δικαίωμα να μεταβάλει ή να τροποποιεί τους εφαρμοστέους όρους και προϋποθέσεις για τη χρήση της ιστοσελίδας σε οποιαδήποτε χρονική στιγμή. Τέτοιες αλλαγές, τροποποιήσεις, προσθήκες ή διαγραφές στους όρους και τις προϋποθέσεις της χρήσης θα τίθενται σε ισχύ άμεσα από την γνωστοποίησή τους, η οποία μπορεί να δοθεί με κάθε μέσο συμπεριλαμβανομένης, αλλά όχι περιοριστικά, της θέσης καινούργιων όρων και προϋποθέσεων στην ιστοσελίδα. Κάθε χρήση της ιστοσελίδας κατόπιν τέτοιας αλλαγής ή τροποποίησης θα θεωρείται ότι αποτελεί αποδοχή εκ μέρους σας τέτοιων αλλαγών, τροποποιήσεων, προσθηκών ή διαγραφών.

Το e-shop.gr μπορεί, σε οποιαδήποτε χρονική στιγμή, να καταγγείλει, αλλάξει, αναστείλει ή διακόψει οποιαδήποτε επιμέρους λειτουργία αυτής της ιστοσελίδας συμπεριλαμβανομένης της διαθεσιμότητας, της φωτογραφία παρουσίασης ή περιγραφής οποιουδήποτε προϊόντος ή υπηρεσίας.

Περιορισμός Ευθύνης

Το e-shop.gr, οι υπάλληλοί του, ή άλλοι αντιπρόσωποί του, δεν έχει καμία ευθύνη, υπό οποιεσδήποτε συνθήκες, για όποιες επακόλουθες, παρεμπίπτουσες, έμμεσες, ειδικές αποζημιώσεις ή έξοδα ή χρηματικές ποινές, συμπεριλαμβανομένων, αλλά όχι

περιοριστικά, διαφυγόντων κερδών, διακοπής λειτουργίας της επιχείρησης, απώλειας πληροφοριών ή δεδομένων, ή απώλειας πελατείας, απώλειας ή ζημίας περιουσίας, και οποιωνδήποτε αξιώσεων τρίτων μερών προκύψουν από ή σε σχέση με την χρήση, την αντιγραφή, ή την παρουσίαση αυτής της ιστοσελίδας ή των περιεχομένων της ή οποιασδήποτε άλλης συνδεδεμένης ιστοσελίδας, ανεξαρτήτως εάν το e-shop.gr είχε ενημερωθεί, γνώριζε ή έπρεπε να γνωρίζει αυτή την πιθανότητα.

Δικαιώματα Πνευματικής Ιδιοκτησίας και Σήμα

Όλος ο σχεδιασμός της ιστοσελίδας, το κείμενο, τα γραφικά η επιλογή και οι ρυθμίσεις αυτής, είναι ιδιοκτησία της e-shop.gr ΑΕ και είναι Δικαίωμα Πνευματικής Ιδιοκτησίας © 2000, 2005 E-SHOP.GR A.E. Επιφυλασσομένων όλων των δικαιωμάτων. Κάθε κείμενο ή εικόνα που φέρει τα σύμβολα TM, SM ή © είναι σήματα ή καταχωρημένα σήματα και χρησιμοποιούνται στο παρόν κατόπιν αδείας των αντίστοιχων ιδιοκτητών τους."

Συμπεράσματα

Στην παρούσα πτυχιακή εργασία συναντήσαμε πολλά και διάφορα θέματα που σχετίζονται με την κλοπή των προσωπικών μας δεδομένων. Συγκεκριμένα, στην αρχή της εργασίας έγινε μια περιγραφή για το πώς ξεκίνησε το φαινόμενο της κλοπής και πώς εξαπλώθηκε αργότερα με την χρήση των υπολογιστών και του Internet.

Στην συνέχεια, είδαμε διάφορες έρευνες σχετικές με απάτες που έχουν να κάνουν με την κλοπή ταυτότητας. Ένα παράδειγμα έρευνας είναι αυτό που περιγράφει πώς τα θύματα ανακάλυψαν την απάτη.

Επιπλέον, συναντήσαμε πολλούς τρόπους που χρησιμοποιούν οι απατεώνες με σκοπό να κλέψουν τα προσωπικά στοιχεία των θυμάτων στην καθημερινή ζωή αλλά και μέσω του διαδικτύου. Επιπροσθέτως, στο ίδιο κεφάλαιο είδαμε τρεις διάσημους κλέφτες ταυτοτήτων, τον Radovan Karadzic, την Jocelyn S. Kirsch και τον Edward Kyle Anderton. Ο πρώτος κατηγορήθηκε όχι μόνο για κλοπή ταυτότητας αλλά και για πολλά εγκλήματα πολέμου. Όσον αφορά τους άλλους δύο που ήταν ζευγάρι, κατηγορήθηκαν για απάτες βασισμένες μόνο σε κλοπή ταυτότητας.

Επιπλέον, άλλο ένα σημαντικό κεφάλαιο είναι αυτό στο οποίο αναφέραμε τρόπους άμυνας, προκειμένου τα θύματα να προστατευθούν σε περίπτωση που τους κλαπεί για παράδειγμα η πιστωτικής τους κάρτα κ.τ.λ.

Στην συνέχεια της εργασίας αυτής, είδαμε κάποιες αρχές όπως για παράδειγμα την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, που εποπτεύουν την επεξεργασία των προσωπικών δεδομένων καθώς επίσης και ποιο είναι το νομικό καθεστώς σε σχέση με την προστασία των δεδομένων σε Ελλάδα αλλά και εξωτερικό.

Τέλος, συναντήσαμε το παιχνίδι-εξομοιωτή CyberCIEGE, που σαν σκοπό έχει να διδάξει τρόπους ασφαλείας υπολογιστών και δικτύων. Έτσι, λοιπόν, δώσαμε μια αναλυτική περιγραφή, περιγράψαμε βήμα-βήμα πως εγκαθίσταται σε έναν υπολογιστή καθώς και παίξαμε με αυτό και παρατηρήσαμε ότι είναι αρκετά ενδιαφέρον.

Βιβλιογραφία

- **Identity Theft and Identity Fraud**
  http://www.usdoj.gov/criminal/fraud/websites/idtheft.html#whatdoing

- **The History of Identity Theft**
  http://www.idtheft-prevent-and-restore.com/history-of-identity-theft.html

- **Ghosting (identity theft)**
  http://en.wikipedia.org/wiki/Ghosting_(identity_theft)#General_description

- **Identity theft**
  http://en.wikipedia.org/wiki/Identity_theft#Spread_and_impact

- **Federal Trade Commission – 2006 Identity theft Survey Report**
  Federal Trade Commission: 2006 Identity Theft Survey Report: Prepared for the Commission by Synovate (November 2007)

- **Naval Postgraduate school – Identity theft prevention in CyberCIEGE**
  http://theses.nps.navy.mil/05Dec_Ruppar.pdf

- **Arrest made in Berkeley laptop theft case**
  https://www.securityfocus.com/news/11319

- **Checking Account Fraud Is Increasing**
  http://www.washingtonpost.com/wp-dyn/articles/A60345-2004Jul18.html

- **Bank insider guilty of £1.3m fraud scam**
  http://www.thisismoney.co.uk/news/article.html?in_article_id=417505&in_page_id=2

- **Απάτη με πιστωτικές κάρτες - 105.000$ φέσι**
  http://www.hotstation.gr/article-print-1702.html

- **Ύποπτες εμπορικές σελίδες**
  http://www.saferinternet.gr/%CE%98%CE%AD%CE%BC%CE%B1%CF%84%CE%B1/%CE%95%CE%95%CF%80%CE%B9%CF%87%CE%B5%CE%B9%CF%81%CE%B5%CE%AF%CE%BD/%CE%8E%CF%80%CE%BF%CF%80%CF%84%CE%B5%CF%82%CE%B5%CE%BC%CF%80%CE%BF%CF%81%CE%B9%CE%BA%CE%AD%CF%82%CF%83%CE%B5%CE%BB%CE%AF%CE%B4%CE%B5%CF%82/tabid/58/Default.aspx

- **Phishing**
  http://en.wikipedia.org/wiki/Phishing#Social_engineering

- **Κλοπή δεδομένων από το μεγαλύτερο site εύρεσης εργασίας**
  http://new.ego.gr/tech/article.asp?catid=6424&subid=2&tag=4885&pubid=1693751

- **Identity Cloning Case Shocks Woman**
  http://www.myidfix.com/identity-theft-stories3.php

- **PHISHING: Νέες μέθοδοι σε ένα γνωστό ηλεκτρονικό έγκλημα**
  http://www.securitymanager.gr/it_security/contents_article.php?id=21&category=REFERENCE&month=%CE%A3%CE%95%CE%A0%CE%A4%CE%95%CE%9C%CE%92%CE%A1%CE%99%CE%9F%CE%A3-%CE%9F%CE%9A%CE%A4%CE%A9%CE%92%CE%A1%CE%99%CE%9F%CE%A3&year=2008&issue=6

- **Fake job offers from Nigeria**
  http://www.exportbureau.com/fraud_report.html?story=21&news=fake_job_offers_from_nigeria

- **Mail Theft and Identity Theft**
  http://www.privacymatters.com/identity-theft-information/mail-theft.aspx

- **Dumpster diving**
  http://en.wikipedia.org/wiki/Dumpster_diving

- **Ευαίσθητα κρατικά και προσωπικά δεδομένα ανακτώνται από παλιούς υπολογιστές**
  http://www.in.gr/news/article.asp?lngEntityID=1011508&lngDtrID=252

- **Identity theft prevention & Recovery**
  http://idsafeguards.blogspot.com/2007/10/synthetic-id-theft.html

- **Securities fraud**
  http://en.wikipedia.org/wiki/Investment_fraud

- **Bernard Madoff**
  http://en.wikipedia.org/wiki/Bernie_Madoff

- **Ponzi scheme**
  http://en.wikipedia.org/wiki/Ponzi_scheme

- **UK Ponzi scheme: GFX Capital Markets Ltd director Terry Freeman was arrested in an alleged £40 investment fraud**
  http://wallstfolly.typepad.com/wallstfolly/2009/02/uk-ponzi-scheme-gfx-capital-markets-ltd-director-terry-freeman-was-arrested-in-an-alleged-40-investm.html

- **Stock manipulation**
  http://en.wikipedia.org/wiki/Stock_manipulation

- **Three charged in alleged 'pump and dump' scheme**
  http://findarticles.com/p/articles/mi_hb5247/is_19_28/ai_n29351033/?tag=content;col

- **Spanish police smash €35m dialer scam**
  http://www.theregister.co.uk/2004/06/23/spain_dial_scam/

- **Alleged ID theft victim has been battling problems for nearly a decade**
  http://www.eagletribune.com/punewsnh/local_story_080093930

- **What Is Medical Identity Theft?**
  http://crime.suite101.com/article.cfm/what_is_medical_identity_theft

- **Ράντοβαν Κάρατζιτς**
  http://el.wikipedia.org/wiki/%CE%A1%CE%AC%CE%BD%CF%84%CE%BF%CE%B2%CE%B1%CE%BD_%CE%9A%CE%AC%CF%81%CE%B1%CF%84%CE%B6%CE%B9%CF%84%CF%82#.CE.A3.CF.8D.CE.BB.CE.BB.CE.B7.CF.88.CE.B7

- **In pictures: Karadzic detained**
  http://news.bbc.co.uk/2/hi/in_pictures/7518646.stm

- **Jocelyn Kirsch and Edward K.Anderton**
  http://pysih.com/2007/12/07/jocelyn-kirsch-and-edward-k-anderton/

- **Οι ανησυχίες των Καταναλωτών**
  http://kepka.org/index.php?option=com_content&task=view&id=294&Itemid=50

- **Τα προσωπικά δεδομένα των Καταναλωτών απειλούνται στο internet**
  http://kepka.org/index.php?option=com_content&task=view&id=793&Itemid=61

- **Laptop Security Guidelines**
  http://labmice.techtarget.com/articles/laptopsecurity.htm

- **Paper shredder**
  http://en.wikipedia.org/wiki/Paper_shredder

- **Citibank Greece**
  http://www.citibank.com/greece/homepage/index.htm

- **The Twenty Minute Guide to PC Security: 20 Tips to Secure your Box**
  http://www.itsecurity.com/features/20-minute-guide-pc-security-021307

- **Καλώς ήλθατε στην ιστοσελίδα της Αρχής Προστασίας Δεδομένων προσωπικού Χαρακτήρα!**
  http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL

- **Identity theft**
  http://en.wikipedia.org/wiki/Identity_theft#Regional_Legal_responses

- **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**
  http://el.wikipedia.org/wiki/%CE%91%CF%81%CF%87%CE%AE_%CE%A0%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD_%CE%A0%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%BF%CF%8D_%CE%A7%CE%B1%CF%81%CE%B1%CE%BA%CF%84%CE%AE%CF%81%CE%B1#.CE.97.CE.BC.CE.AD.CF.81.CE.B1_.CE.A0.CF.81.CE.BF.CF.83.CF.84.CE.B1.CF.83.CE.AF.CE.B1.CF.82_.CE.A0.CF.81.CE.BF.CF.83.CF.89.CF.80.CE.B9.CE.BA.CF.8E.CE.BD_.CE.94.CE.B5.CE.B4.CE.BF.CE.BC.CE.AD.CE.BD.CF.89.CE.BD

- **Α.Δ.Α.Ε.**
  http://www.adae.gr/adae/viewarticle.html?langid=el&articleid=129

- **Privacy policy**
  http://en.wikipedia.org/wiki/Privacy_policy

- **Sample Privacy Notice**
  http://www.bbbonline.org/privacy/sample_privacy.asp

- **Data loss prevention products**
  http://en.wikipedia.org/wiki/Data_Loss_Prevention

- **Criticism of Facebook**
  http://en.wikipedia.org/wiki/Criticism_of_Facebook#Privacy_concerns

- **Criticism of Google**
  http://en.wikipedia.org/wiki/Criticism_of_Google#Privacy

- **Information privacy**
  http://en.wikipedia.org/wiki/Data_protection

- **Θεσμικό πλαίσιο για την προστασία των προσωπικών δεδομένων**
  http://www.dpa.gr/portal/page?_pageid=33,23367&_dad=portal&_schema=PORTAL

- **CyberCIEGE**
  http://en.wikipedia.org/wiki/CyberCIEGE

- **CyberCIEGE brochure**
  http://cisr.nps.edu/cyberciege/downloads/CCIEGEbrochure.pdf

- **CyberCIEGE: An Information Assurance Teaching Tool for Training and Awareness**
  http://cisr.nps.edu/cyberciege/downloads/FISSEA_CyberCIEGE_PreConf.pdf

- **The Case for Modeling and Simulation of Information Security**
  http://www.johnsaunders.com/papers/securitysimulation.htm

Προστασία από κλοπή προσωπικών στοιχείων

- **AI Wars: The Awakening**
  http://pc.ign.com/objects/014/014949.html

- **Προστασία Προσωπικών Δεδομένων**
  http://www.e-shop.gr/protection.phtml