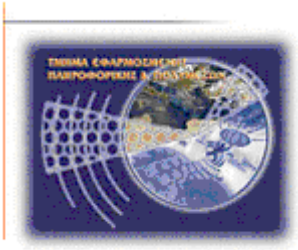
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Τηλεπικοινωνιακή Απάτη

Εμμανουήλ Χουστουλάκης (ΑΜ: 1613)
E-mail: epp1613@epp.teicrete.gr

Ηράκλειο – 13-11-10

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

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

Ευχαριστίες

Θα ήθελα να ευχαριστήσω κυρίως τον επόπτη καθηγητή μου κύριο Μανιφάβα Χαράλαμπο που μου έδωσε την ευκαιρία να αναπτύξω την παρούσα πτυχιακή εργασία και για την πολύτιμη βοήθειά του στην διεκπεραίωση αυτής.

Ακόμα, θα ήθελα να ευχαριστήσω τους υπόλοιπους καθηγητές μου καθώς και όλους όσους με στήριξαν κατά τη διάρκεια της φοίτησής μου στο ΤΕΙ Κρήτης και κυρίως τους γονείς μου.

Ιστορικό εκδόσεων

Ημερομηνία	Έκδοση	Λεπτομέρειες
13/11/2010	Τελική	Διορθώσεις και προσθήκη λεπτομερειών στο σύνολο της πτυχιακής εργασίας.
23/09/2010	1.2	Ολοκληρωμένα τα κεφάλαια 4 και 5
12/05/2010	1.1	Ολοκληρωμένη εισαγωγή και ιστορική αναδρομή
27/04/2010	1.0	Εισαγωγή και μέρος ιστορικής αναδρομής

Περίληψη

Η τηλεπικοινωνιακή απάτη είναι τόσο παλιά, όσο το ίδιο το τηλεφωνικό σύστημα. Μπορεί να πάρει διάφορες μορφές και να εξελίσσεται με την πάροδο του χρόνου. Έτσι, οι απατεώνες πάντα καταφέρνουν να προσαρμόζονται στα δεδομένα κάθε εποχής και να αποφεύγουν τη σύλληψη.

Η τηλεπικοινωνιακή απάτη χωρίζεται κατά βάση σε δύο μεγάλες κατηγορίες ανάλογα με το θύμα το οποίο στοχεύει. Έτσι υπάρχει απάτη εναντίον καταναλωτών και εναντίον εταιριών. Σε κάθε περίπτωση, θύτης μπορεί να είναι μία άλλη εταιρία ή κάποιος τρίτος. Φυσικά υπάρχει πάντα και η περίπτωση των διεφθαρμένων υπαλλήλων στους τηλεπικοινωνιακούς οργανισμούς

Η οικονομική ζημιά που προκαλείται ετησίως στα θύματα από την τηλεπικοινωνιακή απάτη είναι σχεδόν ανυπολόγιστη. Τα θύματα προέρχονται από όλες τις ηλικιακές ομάδες αλλά η πλειοψηφία τους ανήκει σε ηλικίες άνω των 45 ετών. Η οικονομική απώλεια για κάθε θύμα ποικίλει από μικρά ποσά έως όλη τους την περιουσία (στις χειρότερες περιπτώσεις). Οι εγκληματίες εκμεταλλεύονται την ανωνυμία τους και γλιτώνουν τις νομικές συνέπειες. Στη συγκεκριμένη μορφή απάτης υπάρχουν ελάχιστες συλλήψεις. Δυστυχώς, το πρόβλημα στο μέλλον αναμένεται να αυξηθεί αντί να συρρικνωθεί.

Abstract

Telecom fraud is as old as the telephone system. It can take many forms and evolve as the time goes by. That way, the crooks manage to adjust to each era and situation and avoid being arrested.

Telecom fraud can be divided in two basic categories, depending on the intended victim. There is fraud against consumers and against companies. In all the cases, the scammer could be another company or a third party. Of course, there are always corrupted employees in phone companies.

The financial damage caused each year by telecom fraud is great and cannot easily be calculated. The victims belong to all age groups, but the majority of them are aged 45 and above. The financial damage for every victim can vary from small sums to their whole fortune (in the worst cases). The criminals use their anonymity and avoid legal consequences. In this particular fraud type, very few suspects are arrested. And the problem is expected to grow in the future.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Κεφάλαιο 1 Εισαγωγή

1.1 Γενικά

Η παρούσα πτυχιακή, όπως προαναφέρθηκε στην εισαγωγή, ασχολείται με τις τηλεφωνικές απάτες. Το τηλέφωνο, αποτελεί πλέον αναπόσπαστο κομμάτι της προσωπικής και επαγγελματικής ζωής κάθε ανθρώπου. Είναι απαραίτητο στη βιομηχανία, στις επιχειρήσεις και στις κυβερνητικές υπηρεσίες και υπάρχει σχεδόν σε κάθε σπίτι του ανεπτυγμένου κόσμου.

Η τηλεφωνία πέρασε από διάφορα στάδια μέχρι να φτάσει στη σημερινή της μορφή. Δυστυχώς όμως, από το ξεκίνημα της μέχρι και σήμερα έχει χρησιμοποιηθεί όχι μόνο ως μέσο επικοινωνίας, αλλά και ως μέσο εξαπάτησης.

Υπάρχουν πολλές μορφές απάτης που σχετίζονται με τη χρήση τηλεφωνικών συστημάτων. Στην πιο απλή και συνηθισμένη περίπτωση, οι απατεώνες εκμεταλλεύονται την έλλειψη προσωπικής επαφής και παριστάνουν άλλους, προσπαθώντας να αποσπάσουν από τα θύματά τους πληροφορίες και εντέλλει χρήματα. Αν οι απατεώνες έχουν τις απαραίτητες γνώσεις, αλλά και τεχνικά μέσα, μπορούν να εξαπατήσουν και τις ίδιες τις εταιρίες παροχής τηλεφωνικών υπηρεσιών.

Φυσικά, οι εταιρίες δεν είναι πάντα αθώες. Πολλές φορές, με δόλιους τρόπους προσπαθούν να αποσπάσουν επιπλέον χρήματα από τους πελάτες τους ή από ανταγωνιστές τους. Σε πολλές περιπτώσεις, κάποιος διεφθαρμένος υπάλληλος μπορεί να χρησιμοποιήσει την εξουσία του για να εξαπατήσει πελάτες της εταιρίας, ή ακόμα και τους εργοδότες του.

Το συμπέρασμα που βγαίνει είναι ότι η τηλεφωνική απάτη, είναι ιδιαίτερα διαδεδομένη και έχει ως αποτέλεσμα απώλεια χρημάτων από τις εταιρίες και τους καταναλωτές.

1.2 Σκοπός

Η εργασία αυτή έχει ως σκοπό να ενημερώσει τον αναγνώστη σχετικά με τα είδη της τηλεπικοινωνιακής απάτης που σχετίζονται με σταθερή και κινητή τηλεφωνία. Πιο συγκεκριμένα, αναλύονται τα παρακάτω θέματα:

1. Πώς ξεκίνησε η τηλεφωνική απάτη και ποιοι ήταν οι πρώτοι απατεώνες και ποια ήταν τα πρώτα εργαλεία που χρησιμοποιούνταν για το σκοπό αυτό.

2. Ποια είναι η κατάσταση τη σημερινή εποχή, ποιο είναι το πραγματικό οικονομικό αντίκτυπο βάσει στατιστικών και παρουσίαση πραγματικών περιστατικών.

3. Ποιοι είναι οι τύποι της τηλεπικοινωνιακής απάτης στο χώρο της σταθερής και κινητής τηλεφωνίας.

4. Δίνεται έμφαση στην απάτη με τηλεφωνικές πωλήσεις που είναι η πιο συχνή μορφή τηλεφωνικής απάτης.

5. Παρατίθεται ένα κεφάλαιο με συμπεράσματα και βιβλιογραφία.

1.3 Συνοπτική Περιγραφή

Στο κεφάλαιο 2 γίνεται μια ιστορική αναδρομή όπου παρουσιάζεται πως και πότε ξεκίνησε η τηλεφωνική απάτη σε τεχνικό επίπεδο. Αναλύεται δηλαδή η τεχνική του phreaking που είναι ο πρόγονος του computer hacking. Ακόμα υπάρχουν οι βιογραφίες των δύο πρώτων και πιο γνωστών ανθρώπων που ασχολήθηκαν με τη μελέτη του τηλεπικοινωνιακού συστήματος για προσωπικό τους όφελος, καθώς και τα εργαλεία που χρησιμοποιούσαν.

Στο κεφάλαιο 3 παρουσιάζεται η κατάσταση σήμερα που το τηλεφωνικό σύστημα έχει αλλάξει και βασίζεται στη χρήση υπολογιστών. Ακόμα, παρουσιάζονται τα Fraud Management Systems που είναι κατασκευασμένα για να προλαμβάνουν και να εντοπίζουν την απάτη. Ακόμα παρουσιάζονται ορισμένα στατιστικά στοιχεία που προέρχονται από τον Καναδά και τις ΗΠΑ και αφορούν την τηλεφωνική απάτη καθώς και πλήθος πραγματικών περιστατικών.

Στο κεφάλαιο 4 αναλύονται όλα τα είδη της τηλεφωνικής που έχουν καταγραφεί. Αφορούν την κινητή και σταθερή τηλεφωνία. Είναι χωρισμένα σε κατηγορίες ανάλογα με το ποιοι είναι οι θύτες και ποια τα θύματα. Όπου υπάρχουν, αναλύονται και τυχόν παραλλαγές του κάθε είδους.

Στο κεφάλαιο 5 αναλύεται η απάτη με τηλεφωνικές πωλήσεις ή τηλεαγορές. Αυτή είναι η πιο συχνά εμφανιζόμενη μορφή τηλεπικοινωνιακής απάτης και μάλλον δεν υπάρχει καταναλωτής που να μην έχει βρεθεί στη θέση του υποψήφιου θύματος. Παρουσιάζονται όλες οι παραλλαγές αυτού του τύπου απάτης καθώς και μερικά πραγματικά περιστατικά.

Στο κεφάλαιο 6 υπάρχει μια ενότητα με συμπεράσματα που μπορεί κάποιος να εξάγει διαβάζοντας την παρούσα πτυχιακή. Ακόμα υπάρχουν συγκεντρωμένες όλες οι πηγές που χρησιμοποιήθηκαν στη συγγραφή της.

1.4 Σχεδιάγραμμα Αναφοράς

Αριθμός κεφαλαίου	Τίτλος
1	Εισαγωγή
2	Phreaking
3	Σημερινή κατάσταση

Κεφάλαιο 2 Phreaking

2.1 Η ιστορία του phreaking

Ένα χαρακτηριστικό της τηλεφωνικής απάτης είναι η διαχρονικότητά της. Από την αρχή, οι απατεώνες είτε θα προσπαθούσαν να ξεγελάσουν τους συνδρομητές, είτε τις εταιρίες με σκοπό να αποσπάσουν χρήματα ή προσωπικά στοιχεία. Και πάντα με παρόμοιους τρόπους, δηλαδή είτε παριστάνοντας κάποιο αξιόπιστο πρόσωπο, είτε χρησιμοποιώντας εξελιγμένα τεχνικά μέσα.

Στο κεφάλαιο αυτό, δεν θα αναφερθούν τα είδη της απάτης (πράγμα το οποίο θα γίνει αναλυτικά σε επόμενο κεφάλαιο), αλλά το πώς ξεκίνησε η κακή εκμετάλλευση του τηλεφωνικού δικτύου σε τεχνικό επίπεδο. Θα αναλυθεί δηλαδή το φαινόμενο του phreaking[1], που άνθισε στα μέσα μέχρι τα τέλη του προηγούμενου αιώνα καθώς και οι βιογραφίες των πρωτεργατών του είδους.

2.1.1 Τι είναι το Phreaking

Το "Phreaking" είναι ένας άτυπος όρος που χρησιμοποιείται για να περιγράψει τη δραστηριότητα κάποιων ανθρώπων, οι οποίοι μελετούν τα τηλεπικοινωνιακά συστήματα και πειραματίζονται με αυτά. Ασχολούνται κυρίως με εξοπλισμό που σχετίζεται με δημόσια τηλεφωνικά δίκτυα. Τα τελευταία χρόνια, που τα τηλεπικοινωνιακά συστήματα βασίζονται σε ηλεκτρονικούς υπολογιστές, ο όρος "Phreaking" έχει συνδεθεί με τον όρο "Computer Hacking".

Τα άτομα που ασχολούνται με την παραπάνω δραστηριότητα αποκαλούνται "Phreaks". Ο όρος "Phreak" είναι παράγωγο των λέξεων phone και freak και μπορεί ακόμα να αναφέρεται στη χρήση διαφόρων συχνοτήτων ήχου για το χειρισμό ενός τηλεπικοινωνιακού συστήματος. Αξίζει να σημειωθεί ότι ένα μεγάλο μέρος των phreaks ήταν τυφλοί.

2.1.2 Πως ξεκίνησε το Phreaking

Η ακριβής προέλευση του phreaking είναι άγνωστη. Πιστεύεται, ότι ξεκίνησε μετά τη μαζική χρησιμοποίηση αυτόματων διακοπτών στα τηλεφωνικά δίκτυα. Στις ΗΠΑ, η εταιρία AT&T χρησιμοποίησε για πρώτη φορά αυτόματους διακόπτες για υπεραστικές κλήσεις, στα μέσα της δεκαετίας του 1950. Τότε, ήταν η πρώτη φορά που το ευρύ κοινό ερχόταν σε επαφή με υπολογιστική δύναμη σε ευρεία κλίμακα.

Την εποχή εκείνη ήταν δύσκολο, για διάφορους λόγους, να ασχοληθεί κάποιος άμεσα με τους ηλεκτρονικούς υπολογιστές. Έτσι, όσοι είχαν ανησυχίες και ήθελαν να εξερευνήσουν περεταίρω την τεχνολογία των υπολογιστών, στράφηκαν στην μοναδική διαθέσιμη επιλογή που είχαν: το ελεγχόμενο από υπολογιστές τηλεφωνικό δίκτυο.

[1] http://en.wikipedia.org/wiki/Phreaking

2.1.3 Ο τόνος των 2600Hz

Οι αυτόματοι διακόπτες της εταιρίας AT&T χρησιμοποιούσαν τονική κλήση και περιελάμβαναν μερικούς τόνους που ήταν για εσωτερική εταιρική χρήση. Ένας εσωτερικός τόνος χρήσης ήταν ένας με συχνότητα 2600Hz. Ο τόνος αυτός αποτελούσε το σήμα τερματισμού κλήσης ενός αυτόματου διακόπτη. Αυτό το χαρακτηριστικό μπορούσε να χρησιμοποιηθεί για την πραγματοποίηση δωρεάν υπεραστικών και διεθνών κλήσεων.

Ο τόνος αυτός ανακαλύφθηκε το 1957 από τον Joe Engressia, ένα τυφλό επτάχρονο αγόρι. Ο Engressia, είχε την ικανότητα να αναπαράγει ακριβώς με σφύριγμα ήχους συγκεκριμένης συχνότητας. Τυχαία, ανακάλυψε ότι μία νότα που σφύριζε (ένας τόνος συχνότητας 2600Hz) σταματούσε την καταγραφή μιας κλήσης. Χωρίς αρχικά να γνωρίζει τι είχε κάνει, κάλεσε την εταιρεία τηλεπικοινωνιών και ρώτησε γιατί σταταματούσε η καταγραφή. Αυτή ήταν η αρχή του ενδιαφέροντός του Egressia για την μελέτη του τηλεπικοινωνιακού συστήματος.

Άλλοι phreaks της εποχής ήταν ο "Bill από τη Νέα Υόρκη" και ο John Draper. Ο Bill ανακάλυψε ότι ένα καταγραφικό φωνής που διέθετε, μπορούσε να αναπαράγει τον τόνο των 2600Hz με τα ίδια αποτελέσματα με αυτά του Engressia. Ο John Draper ήταν φίλος του Engressia. Με τη βοήθεια του δεύτερου, ο Draper ανακάλυψε ότι η σφυρίχτρα που ήταν δώρο στη συσκευασία των δημητριακών "Cap'n Crunch", παρήγαγε έναν ήχο συχνότητας 2600Hz. Από το όνομα των δημητριακών, πήρε ο Draper το ψευδώνυμο "Captain Crunch".

2.1.4 Πολλαπλή συχνότητα

Παρόλο που η μοναδική συχνότητα δούλευε σε συγκεκριμένες τηλεφωνικές γραμμές, για μεγαλύτερες αποστάσεις απαιτούνταν πολλαπλή συχνότητα. Οι συγκεκριμένες συχνότητες που απαιτούνταν ήταν άγνωστες μέχρι το 1964. Τότε η εταιρία "Bell Systems" δημιούργησε ένα εγχειρίδιο που περιέγραφε τις μεθόδους και τις συχνότητες που χρησιμοποιούνταν για την εσωτερική επικοινωνία της εταιρίας. Το εγχειρίδιο αυτό προοριζόταν για τους τεχνικούς της εταιρίας, αλλά με κάποιο τρόπο διέρρευσε στη φοιτητική κοινότητα. Με αυτό τον τρόπο, η Bell Systems αποκάλυψε κατά λάθος τα μυστικά του τηλεφωνικού συστήματος και όσοι είχαν βασικές γνώσεις ηλεκτρονικής, μπορούσαν να το εκμεταλλευτούν.

Εκείνη τη εποχή, εμφανίστηκε η δεύτερη γενιά από phreaks. Μερικοί από αυτούς ήταν οι: "Evan Doorbell", "Ben Decibel" και Neil R. Bell από τη Νέα Υόρκη, και οι Mark Bernay, Chris Bernay, και "Alan από τον Καναδά" από την Καλιφόρνια. Καθένας από αυτούς έκανε τους δικούς του πειραματισμούς πάνω στο τηλεφωνικό δίκτυο ξεχωριστά, αλλά ανακάλυψαν ο ένας τον άλλο στα ταξίδια τους. Αργότερα σχημάτισαν δύο ομάδες, οι τρεις πρώτοι την " Group Bell" και οι τρεις δεύτεροι την "Mark Bernay Society". Η δράση των ομάδων αυτών είναι δημοφιλής μεταξύ των phreaks όλων των εποχών.

2.1.5 Δημοσιοποίηση του Phreaking

Τον Οκτώβριο του 1971, το phreaking έγινε γνωστό στο ευρύ κοινό, μετά τη δημοσίευση ενός άρθρου στο περιοδικό Esquire. Ο τίτλος του άρθρου ήταν "Τα μυστικά του μικρού μπλε κουτιού" και περιέγραφε τη δραστηριότητα των Draper και Engressia, ταυτίζοντας το όνομά τους με το phreaking. Το άρθρο αυτό τράβηξε το ενδιαφέρον μελλοντικών phreaks, όπως των Steve Wosniak και Steve Jobs, των ιδρυτών της εταιρίας Apple.

Το 1971, ήταν η χρονιά που ξεκίνησε από τους Abbie Hoffman και Al Bell το YIPL (Youth International Party Line), ένα περιοδικό που αναφερόταν σε αντιεξουσιαστές νέους και είχε ως θεματολογία τα τηλέφωνα. Το 1973, ο Bell πρόσθεσε στο YIPL το TAP (Technology Assistance Program). Το TAP εξελίχθηκε σε κύρια πηγή τεχνικών πληροφοριών για τους phreaks και τους hackers παγκοσμίως. Το TAP προχώρησε μέχρι το 1984. Το 1983 ο Bell παρέδωσε την έκδοση του περιοδικού στον Tom Edison. Μετά από διάρρηξη και εμπρησμό στο σπίτι του Edison τον ίδιο χρόνο, το περιοδικό το ανέλαβε ο οίκος Cheshire Catalyst, αλλά σταμάτησε την έκδοσή του το 1984.

Πριν τα γεγονότα αυτά, το έτος 1972, δημοσιεύτηκε στο περιοδικό "Ramparts" ένα άρθρο που περιέγραφε τη διαδικασία κατασκευής ενός κουτιού για phreaking. Το κουτί αυτό μπορούσε να χρησιμοποιηθεί για πραγματοποίηση δωρεάν υπεραστικών κλήσεων και η κατασκευή του ήταν πολύ απλή. Μετά από μήνυση του Bell, το Ramparts αναγκάστηκε να αποσύρει τα αντίτυπα από την κυκλοφορία αλλά ήταν ήδη αργά, αφού πολλοί είχαν ήδη προμηθευτεί το περιοδικό.

2.1.6 Απάτη με τηλεφωνικές κάρτες

Το 1984 μετά τη διαίρεση της AT&T, εμφανίστηκαν πολλές μικρές τηλεφωνικές εταιρίες που ανταγωνίζονταν στον τομέα των φτηνών υπεραστικών κλήσεων. Μεταξύ αυτών ήταν και οι πρωτοεμφανιζόμενες Sprint και MCI. Εκείνη την εποχή, δεν υπήρχε τρόπος οι μικρές εταιρίες να χρησιμοποιήσουν τις γραμμές της AT&T αυτόματα. Οι πελάτες των μικρών εταιριών έπρεπε πρώτα να καλέσουν ένα τοπικό κέντρο παροχής υπηρεσιών και να πληκτρολογήσουν τον αριθμό της τηλεφωνικής τους κάρτας και στη συνέχεια το νούμερο με το οποίο ήθελαν να επικοινωνήσουν. Καθότι η όλη διαδικασία ήταν αρκετά χρονοβόρος, οι εταιρίες παρείχαν σύντομους αριθμούς τηλεφωνικών καρτών(6-7 ψηφία). Το γεγονός αυτό διευκόλυνε την δουλειά των phreaks που διέθεταν υπολογιστή.

Οι εξαψήφιες κάρτες είχαν 1 εκατομμύριο συνδυασμούς, ενώ οι επταψήφιες 10 εκατομμύρια. Αυτό σημαίνει, ότι σε μια εταιρία με 10000 πελάτες, η πιθανότητα για ένα phreak να μαντέψει τον αριθμό μιας κάρτας, ήταν 1 στις 100 για τους εξαψήφιους και μία στις 1000 για τους επταψήφιους. Η διαδικασία αυτή μπορούσε σχετικά εύκολα να γίνει χειροκίνητα, πόσο μάλλον με τη χρήση υπολογιστή. Αναπτύχθηκαν από hackers σχετικά προγράμματα για τους υπολογιστές που διέθεταν μόντεμ. Το μόντεμ καλούσε το τοπικό κέντρο παροχής και δοκίμαζε ένα τυχαίο αριθμό τηλεφωνικής κάρτας. Αν ήταν σωστός τον αποθήκευε στο δίσκο. Αν ήταν λάθος, διέκοπτε τη κλήση και ξαναδοκίμαζε. Με τον τρόπο αυτό, τα προγράμματα τέτοιου τύπου έβρισκαν εκατοντάδες ενεργούς αριθμούς τηλεφωνικών καρτών σε μια μέρα, οι οποίοι μοιράζονταν μεταξύ των phreaks.

Τότε ήταν δύσκολο για τις μικρές εταιρίες να εντοπίσουν τις επιθέσεις αυτές, αφού δεν είχαν πρόσβαση στα αρχεία της κεντρικής εταιρίας τηλεπικοινωνιών. Κάτι τέτοιο ήταν ακριβό και χρονοβόρο. Παρόλο που υπήρξε κάποια πρόοδος στον εντοπισμό των απατεώνων στις αρχές του 1990, το πρόβλημα δεν εξαλείφθηκε έως ότου οι μικρές εταιρίες μπορούσαν να χρησιμοποιήσουν αυτόματα τις γραμμές της κεντρικής τηλεπικοινωνιακής εταιρίας.

2.1.7 Συσκευές εκτροπής κλήσεων

Μία άλλη μέθοδος που χρησιμοποιούνταν για πραγματοποίηση δωρεάν κλήσεων ήταν οι εκτροπείς. Τη δεκαετία του 80 και στις αρχές της δεκαετίας του 90, η προώθηση κλήσεων δεν παρέχονταν σε πολλούς εταιρικούς πελάτες. Έτσι, πολλές επιχειρήσεις αναγκάζονταν να αγοράσουν εξοπλισμό που έκανε εκτροπή από μία γραμμή σε άλλη. Όταν η επιχείρηση έκλεινε, προγραμμάτιζαν τους εκτροπείς να απαντούν τις κλήσεις, να συνδέονται με μια δεύτερη γραμμή η οποία καλούσε τον αυτόματο τηλεφωνητή και να συνδέουν τις δύο γραμμές. Ο καλών, είχε την εντύπωση ότι συνδεόταν απευθείας με τον αυτόματο τηλεφωνητή. Οι περισσότεροι όμως εκτροπείς, μετά το τέλος της κλήσης έκαναν επανεκκίνηση. Αν ο καλών περίμενε λίγο, έπαιρνε σήμα από τη δεύτερη γραμμή και μπορούσε να πραγματοποιήσει κλήση. Φυσικά οι phreaks το είδαν αυτό σαν τεράστια ευκαιρία και ξόδευαν ώρες εφαρμόζοντάς το. Με τον τρόπο αυτό, έκαναν τηλεφωνήματα οπουδήποτε στο κόσμο και καλούσαν ροζ τηλέφωνα σε βάρος της εταιρίας. Οι εταιρίες ήταν υποχρεωμένες να πληρώσουν το λογαριασμό, αφού υπαίτιος ήταν ο δικός τους εξοπλισμός και δεν ευθυνόταν ο παροχέας. Μέχρι το 1993, η προώθηση κλήσεων προσφερόταν σε όλους σχεδόν τους εταιρικούς πελάτες, καθιστώντας τους εκτροπείς άχρηστους. Οι phreaks σταμάτησαν να ασχολούνται και η μέθοδος αυτή πέθανε.

2.1.8 Το τέλος της πολλαπλής συχνότητας

Στις 15 Ιουνίου του 2006 στις ΗΠΑ, αντικαταστάθηκαν οι παλαιάς τεχνολογίας γραμμές με νέες που δεν υποστήριζαν την πολλαπλή συχνότητα. Κατά συνέπεια, σταμάτησε να υπάρχει και η δυνατότητα του "παραδοσιακού" phreaking. Η τελευταία γραμμή που υποστήριζε πολλαπλή συχνότητα λειτουργούσε στην Wawina Township της πολιτείας Minnesota. Τις τελευταίες μέρες πριν τη διακοπή phreaks από όλο τον κόσμο, μεταξύ αυτών και οι διάσημοι Engressia και Draper, τηλεφωνούσαν στην εναπομείνασα αυτή γραμμή. Τις μέρες 7-12 Ιουνίου του 2006, ξεκίνησαν να υπάρχουν παρεμβολές στην γραμμή και οι phreaks αποκτούσαν δύσκολα πρόσβαση. Στις 15 Ιουνίου ήταν αδύνατη η πρόσβαση στην γραμμή. Μέχρι τις 29 Ιουλίου, το μόνο που ακουγόταν απλά ένα μήνυμα που ενημέρωνε για την ώρα και τη θερμοκρασία στη συγκεκριμένη πολιτεία.

2.2 Τα πρώτα εργαλεία των απατεώνων

Τα κουτιά phreaking[2] ήταν συσκευές που κατασκευαζόταν από τους ίδιους τους phreaks για διευκόλυνση του έργου τους. Μέσω αυτών, οι απατεώνες είχαν πρόσβαση σε λειτουργίες που κανονικά ήταν διαθέσιμες μόνο σε υπαλλήλους τηλεφωνικών εταιριών. Υπήρχαν πολλοί τύποι τέτοιων συσκευών, καθένας με διαφορετικές ιδιότητες και κάθε τύπος ονομαζόταν σύμφωνα με ένα χρώμα.

Η πλήρης λίστα των χρωμάτων που χρησιμοποιούνταν για την ονοματολογία των κουτιών είναι η παρακάτω: μωβ, κόκκινο, πορτοκαλί, πράσινο, μπλε, μπεζ, μαύρο, ζωηρό ερυθρό, χρυσαφί, διαφανές και ασημί. Από αυτά, τα πιο γνωστά και περισσότερο χρησιμοποιούμενα ήταν το μαύρο, το μπεζ, το μπλε και το κόκκινο.

2.2.1 Το Μαύρο κουτί

Τα μαύρα[3] phreaking κουτιά κατασκευάζονταν μεταξύ των δεκαετιών 1960 και 1980 και παρείχαν στους κατασκευαστές-κατόχους τη δυνατότητα να πραγματοποιούν δωρεάν κλήσεις. Λειτουργούσαν σε τηλεφωνικές γραμμές που χρέωναν ανάλογα με το χρόνο που το ακουστικό ήταν σηκωμένο. Το μαύρο κουτί έκανε το σηκωμένο ακουστικό του τηλεφώνου να φαίνεται κατεβασμένο, με αποτέλεσμα να σταματάει η χρέωση της κλήσης. Για να λειτουργήσει αυτή η απάτη, έπρεπε να υπάρχει ένα μαύρο κουτί και στις δύο συσκευές που βρισκόταν σε επικοινωνία. Για το λόγο αυτό έγινε δημοφιλές κυρίως μεταξύ φίλων, οι οποίοι πραγματοποιούσαν πολύωρες συζητήσεις χωρίς να χρεώνονται.

Ένα απλό μαύρο κουτί, αποτελούνταν από ένα πυκνωτή και μια αντίσταση, συνδεδεμένα παράλληλα. Το σύστημα αυτό συνδεόταν σε σειρά με το τηλέφωνο και η εγκατάστασή του ήταν σχετικά εύκολη. Με χρήση της αντίστασης, μειωνόταν η ποσότητα του παρεχόμενου συνεχούς ρεύματος στη συσκευή. Έτσι, υπήρχε αρκετό ρεύμα για να λειτουργήσει το μικρόφωνο, αλλά όχι και ο μηχανισμός του διακόπτη. Με τον τρόπο αυτό, μπορούσε να χρησιμοποιηθεί το τηλέφωνο, ενώ η εταιρία το "έβλεπε" κατεβασμένο.

2.2.2 Το Μπεζ κουτί

Τα μπεζ[4] κουτιά ήταν συσκευές υποκλοπής. Εκτελούσαν την ίδια λειτουργία με τις συσκευές που είχαν οι τεχνικοί των εταιριών για διάγνωση κατάστασης της γραμμής. Για την κατασκευή τους απαιτούνταν 3 απλά πράγματα: μια τηλεφωνική συσκευή, ένα κολλητήρι και δύο ηλεκτρόδια σε μορφή κλιπ. Μπορούσε να χρησιμοποιηθεί και ένας διακόπτης για απενεργοποίηση του μικροφώνου, ώστε να μην μεταφέρεται στη γραμμή ο θόρυβος του περιβάλλοντος.

Το μπεζ κουτί, έχει συνδεθεί σαν έννοια, με την παράνομη παρακολούθηση τηλεφώνων. Παρόλο που στις περισσότερες περιπτώσεις είναι νόμιμη η κατασκευή

[2] http://en.wikipedia.org/wiki/Phreaking_boxes
[3] http://en.wikipedia.org/wiki/Black_box_(phreaking)
[4] http://en.wikipedia.org/wiki/Beige_box_(phreaking)

και κατοχή μιας τέτοιας συσκευής, απαγορεύεται αυστηρά η χρήση του πάνω σε τηλεφωνικές γραμμές.

2.2.3 Το μπλε κουτί

Το μπλε[5] κουτί, ένα από τα πιο παλιά και χρήσιμα εργαλεία phreaking, ήταν ουσιαστικά ένας εξομοιωτής της κονσόλας που χρησιμοποιούσαν οι χειριστές τηλεφωνικών κέντρων. Βασιζόταν στην ανακάλυψη του γνωστού πλέον Engressia, τον τόνο των 2600Hz. Η υλοποίησή του βέβαια, έγινε δυνατή όταν η εταιρία Bell Systems δημοσίευσε δύο άρθρα με λεπτομέρειες γύρω από τη λειτουργία του υπεραστικού τηλεφωνικού συστήματος. Τα μπλε κουτιά δεν τα χρησιμοποιούσαν μόνο οι phreaks για πραγματοποίηση δωρεάν προσωπικών υπεραστικών κλήσεων, αλλά και η μαφία για εγκληματικούς σκοπούς.

Το μπλε κουτί λειτουργούσε με τον παρακάτω τρόπο: Πρώτα, ο χρήστης πραγματοποιούσε μια κλήση σε ένα απομακρυσμένο αριθμό. Στη συνέχεια με το μπλε κουτί αναπαρήγαγε τον τόνο των 2600Hz. Το άλλο άκρο, νόμιζε ότι ο καλών είχε κλείσει το τηλέφωνο. Όταν σταματούσε ο τόνος, γινόταν επανεκκίνηση του διακόπτη της γραμμής, με ένα χαρακτηριστικό ήχο. Ο ήχος αυτός, αποτελούσε σήμα ότι το απομακρυσμένο τηλέφωνο περιμένει να δρομολογήσει μια κλήση. Χρησιμοποιώντας πάλι το μπλε κουτί, ο phreak καλούσε τον επιθυμητό αριθμό χωρίς δική του χρέωση.

Εικόνα 1: Το μπλε κουτί του Steve Wosniak

[5] http://en.wikipedia.org/wiki/Blue_box_(phreaking)

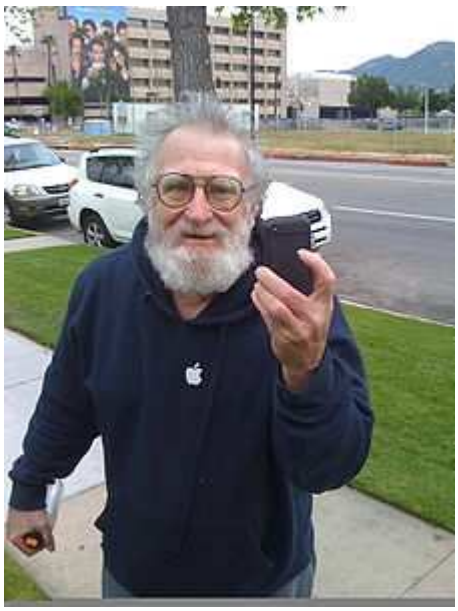
2.2.4 Το κόκκινο κουτί

Το κόκκινο κουτί[6], χρησιμοποιούνταν σε δημόσια τηλέφωνα που λειτουργούσαν με κέρματα. Εξομοίωνε τον ήχο που έκαναν τα κέρματα όταν έπεφταν στη συσκευή. Ήταν ίσως η πιο απλή μέθοδος phreaking, αφού ως κόκκινο κουτί μπορούσε να χρησιμοποιηθεί οποιαδήποτε συσκευή με ικανότητα αναπαραγωγής ηχογραφημένων ήχων. Για κάθε τύπο κέρματος που δεχόταν τα τηλέφωνα, απαιτούνταν διαφορετικός ήχος. Παρόλο που η τεχνολογία έχει προχωρήσει και στα δημόσια τηλέφωνα, η μέθοδος αυτή μπορεί ακόμα να χρησιμοποιηθεί σε ελάχιστες περιοχές των ΗΠΑ.

2.3 Οι πιο γνωστοί Phreaks

2.3.1 Ο John Draper

Ο John Thomas Draper[7] (γεννήθηκε το 1944) γνωστός με τα ψευδώνυμα Captain Crunch, Crunch, Crunchman και Mr. Crunshtastic είναι ένας τέως phreak. Είναι γνωστός για την κακή του υγιεινή και το οδοντιατρικό του ιστορικό.

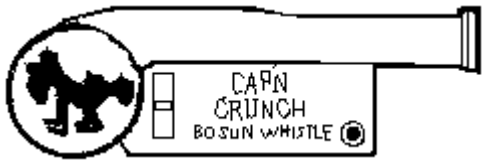


Εικόνα 2: Ο John Draper (Captain Crunch)

Ο πατέρας του ήταν μηχανικός στην πολεμική αεροπορία των ΗΠΑ. Και ο ίδιος ο Draper υπηρέτησε στην πολεμική αεροπορία την περίοδο 1964-1968. Εκεί, και ενώ βρισκόταν στην Αλάσκα, κατάφερε με κάποιο τρόπο που επινόησε, να αποκτήσει πρόσβαση σε ένα τοπικό τηλεφωνικό κέντρο. Έτσι, αυτός και οι συνάδελφοί του έκαναν δωρεάν τηλεφωνήματα στα σπίτια τους.

[6] http://en.wikipedia.org/wiki/Red_box_(phreaking)
[7] http://en.wikipedia.org/wiki/John_Draper

Η ενασχόλησή του με το phreaking ξεκίνησε όταν, με τη βοήθεια του φίλου του Joe Engressia, ανακάλυψε τις "μαγικές" ιδιότητες της σφυρίχτρας που ήταν δώρο στη συσκευασία των δημητριακών Cap'n Crunch. Ο τόνος της σφυρίχτρας, συχνότητας ακριβώς 2600Hz, ξεγελούσε τον διακόπτη της τηλεφωνικής εταιρίας και σταματούσε την καταγραφή μιας κλήσης. Ο καλών όμως, που δεν είχε κατεβάσει το ακουστικό, είχε πλέον πρόσβαση στο τηλεφωνικό κέντρο, και μπορούσε μέσω αυτού να καλέσει όπου ήθελε, χωρίς να χρεώνεται ο ίδιος. Μετά από πολλούς πειραματισμούς, ο Draper κατασκεύασε το μπλε κουτί, μια ηλεκτρονική συσκευή η οποία μπορούσε να αναπαράγει τόνους που χρησιμοποιούνταν από τους διακόπτες τηλεφωνικών εταιριών. Οι σφυρίχτρες αυτές θεωρούνται συλλεκτικό αντικείμενο, παρόλο που πλέον είναι άχρηστες.



Εικόνα 3: Η περίφημη σφυρίχτρα των 2600Hz

Το 1971, δημοσιεύτηκε στο περιοδικό Esquire ένα άρθρο σχετικό με το phreaking που περιείχε μια συνέντευξη του Draper και που τελικά τον έβαλε σε μπελάδες. Το 1972, συνελήφθη και καταδικάστηκε σε 5 χρόνια επιτήρησης. Το άρθρο όμως αυτό, τράβηξε την προσοχή του Steve Wozniak, ο οποίος ήρθε σε επαφή με τον Draper. Στα μέσα της δεκαετίας του 70, ο τελευταίος δίδαξε την "τέχνη" του phreaking στους Steve Wozniak και Steve Jobs, τους μελλοντικούς ιδρυτές της εταιρίας Apple. Ο Draper δούλεψε στην Apple για ένα σύντομο διάστημα, αναπτύσσοντας λογισμικό για τον τότε υπολογιστή της εταιρίας, τον Apple II. Ο Draper συνελήφθη ξανά το 1977 για τηλεφωνική απάτη και μπήκε στη φυλακή.

Ο Draper, εκτός από phreak ήταν και ικανός προγραμματιστής. Έγραψε το EasyWriter, τον πρώτο επεξεργαστή κειμένου για τον υπολογιστή Apple II το 1979. Πολλοί λένε ότι έγραψε τον κώδικα σε χαρτί, την περίοδο που βρισκόταν στη φυλακή και αργότερα τον πέρασε σε υπολογιστή. Ο ίδιος όμως επιβεβαιώνει ότι, σύμφωνα με τους όρους της ποινής του, περνούσε τις ημέρες έξω από τη φυλακή δουλεύοντας σε ένα μουσικό studio και μόνο τις νύχτες έμενε στη φυλακή. Στο studio, είχε πρόσβαση σε υπολογιστή και εκεί έγραφε τον κώδικα. Τα βράδια, στο κελί του έπαιρνε αντίγραφα του κώδικα και τον επεξεργαζόταν.

Αργότερα, το λογισμικό του μεταφέρθηκε και σε υπολογιστές της IBM. Ο Draper ίδρυσε μια μικρή επιχείρηση, αλλά χρεοκόπησε λόγω απάτης από το διανομέα του λογισμικού του. Στη συνέχεια προσελήφθη στην εταιρία Autodesk, αλλά απολύθηκε σύντομα. Η εκκεντρική του συμπεριφορά δεν βοηθούσε την επικοινωνία του με πιθανούς πελάτες. Όταν η Apple κυκλοφόρησε τους υπολογιστές Macintoch, δίδαξε μια σειρά online μαθημάτων για προγραμματισμό του Mac. Τώρα πλέον, ο Draper είναι προϊστάμενος τεχνικού τμήματος της εταιρίας En2go, που ασχολείται με τη διανομή πολυμεσικού περιεχομένου.

2.3.2 Ο Joe Engressia

Ο Josef Carl Engressia Jr[8] (25 Μαΐου 1949- 8 Αυγούστου 2007), γνωστός με το ψευδώνυμο Joybubbles, ήταν ένας από τους πρώτους phreaks. Γεννήθηκε τυφλός και το ενδιαφέρον του για τα τηλέφωνα ξεκίνησε όταν ήταν 4 ετών. Είχε το χάρισμα να καταλαβαίνει την ακριβή συχνότητα ενός ήχου που άκουγε και μπορούσε επίσης να τον αναπαράγει με σφύριγμα.

Σε ηλικία 5 ετών ανακάλυψε ότι μπορούσε να καλέσει ένα αριθμό με διαδοχικά χτυπήματα του διακόπτη της συσκευής(το λεγόμενο tapping). Όταν ήταν 7 ανακάλυψε ότι το σφύριγμα σε συγκεκριμένες συχνότητες μπορούσε να απενεργοποιήσει τους τηλεφωνικούς διακόπτες.

Όταν ήταν φοιτητής στο πανεπιστήμιο της νότιας Florida είχε αποκτήσει το παρατσούκλι "Whistler", λόγω της ικανότητας που είχε να κάνει δωρεάν τηλεφωνήματα με το σφύριγμα. Όταν ανακάλυψαν ότι εμπορευόταν την ικανότητά του αυτή, τον έδιωξαν προσωρινά από το πανεπιστήμιο, αλλά αργότερα επέστρεψε και αποφοίτησε.

Ένας υπάλληλος της εταιρίας Bell Telephone Company παρακολουθούσε παράνομα τις τηλεφωνικές του συζητήσεις και τις παρέδωσε στο FBI. Τελικά ο Engressia συνελήφθη το 1971, μετά από επιδρομή της αστυνομίας στο σπίτι του. Κατηγορήθηκε μόνο για πλημμέλημα και η ποινή του ήταν με αναστολή. Παρόλα αυτά, εγκατέλειψε το phreaking για πάντα.

Το 1982, μετακόμισε στην πολιτεία της Minnesota. Ζούσε με την αναπηρική του σύνταξη και μια δουλειά ως πειραματόζωο για μία έρευνα σχετικά με αρώματα. Όταν ήταν παιδί, είχε κακοποιηθεί σεξουαλικά από μία καλόγρια δασκάλα του. Θέλοντας να ξεχάσει το παρελθόν του, το 1988 δήλωσε ότι έγινε ξανά παιδί και ότι είχε αφήσει πίσω του την κακοποίηση που υπέστη. Άλλαξε επίσημα το όνομά του σε Joybubbles και μέχρι το τέλος της ζωής του ισχυριζόταν ότι ήταν 5 ετών.

Εικόνα 4: Ο Joe Engressia

[8] http://en.wikipedia.org/wiki/Joybubbles

Κεφάλαιο 3 Σημερινή Κατάσταση

3.1 Ύφεση της τηλεπικοινωνιακής απάτης

Παρόλο που έχουμε περάσει πλέον στην ψηφιακή εποχή και οι παραδοσιακές μέθοδοι phreaking δεν δουλεύουν στην πλειοψηφία τους, οι απατεώνες βρίσκονται πάντα ένα βήμα μπροστά[9]. Δυστυχώς όμως, μερικοί από τους απατεώνες δεν είναι πια έφηβοι και νεαροί που απλά ικανοποιούν την περιέργειά τους και κάνουν δωρεάν τηλεφωνήματα. Είναι εγκληματίες που σκοπό έχουν να αποσπάσουν τεράστια ποσά χρημάτων και προσωπικά στοιχεία από ανυποψίαστους χρήστες του τηλεφωνικού δικτύου, αλλά και από τις εταιρίες.

3.1.1 Ασφάλεια βάσεων δεδομένων

Όπως όλοι γνωρίζουν, οι εταιρίες τηλεπικοινωνιών διατηρούν βάσεις δεδομένων με τα πλήρη στοιχεία των πελατών, καθώς και τις υπηρεσίες που αντιστοιχούν στον καθένα. Αυτές οι βάσεις, με ανεπαρκή προστασία και διαχείριση, αποτελούν εύκολους στόχους.

Λόγω του ότι οι βάσεις δεδομένων δεν είναι ομοιόμορφες στην χρήση των πεδίων τους, το όνομα του ίδιου πελάτη μπορεί να γράφεται διαφορετικά σε κάθε βάση, δημιουργώντας έτσι μπέρδεμα και κατά συνέπεια κενά ασφαλείας. Αυτό, σε συνδυασμό με ένα ανεπαρκές ή ανύπαρκτο τείχος προστασίας, ανοίγει την πόρτα σε εισβολείς οι οποίοι σίγουρα θα εκμεταλλευτούν στο έπακρο τις αδυναμίες της βάσης δεδομένων.

Σύμφωνα με τον Bob Bender, στέλεχος της εταιρίας τηλεπικοινωνιών Teradata, όσο πιο αυστηρή είναι η ασφάλεια μιας βάσης δεδομένων, τόσο πιο εύκολα θα πιαστεί ο πιθανός εισβολέας. Η εταιρία του, για παράδειγμα, διατηρεί ξεχωριστή βάση για κάθε υπηρεσία. Μια διαρροή στοιχείων πελατών, είναι ικανή να καταστρέψει τη δημόσια εικόνα μιας τηλεπικοινωνιακής εταιρίας.

3.1.2 Τα λάθη των εταιριών και το παράδειγμα Singular

Η αμερικανική εταιρία τηλεπικοινωνιών Singular Wireless ξεκίνησε δοκιμαστικά το 2004 μια online υπηρεσία, όπου οι συνδρομητές μπορούσαν να δουν τον υπολειπόμενο χρόνο ομιλίας τους και αν τυχόν όφειλαν χρήματα εισάγοντας τον αριθμό τηλεφώνου και τον ταχυδρομικό κώδικά τους. Μετά από πολλά παράπονα των πελατών για την απλότητα και την ευκολία παραβίασης του συστήματος, η λειτουργία της υπηρεσίας σταμάτησε.

Η προαναφερθείσα υπηρεσία, επέτρεπε ακόμα στους πελάτες να πληρώσουν το τυχόν οφειλόμενο ποσό με την πιστωτική τους κάρτα. Σύμφωνα βέβαια με τη δομή της πλατφόρμας, το μόνο που μπορούσε να κάνει ένας απατεώνας ήταν να πληρώσει το ποσό που χρωστούσε ο πελάτης, χωρίς αυτός να το γνωρίζει. Μετά το κλείσιμο της υπηρεσίας, ακολούθησαν αρνητικά δημοσιεύματα, τα οποία κατηγορούσαν το

[9] http://www.billingworld.com/articles/feature/Telecom-Fraud-on-the-Rise.html

σύστημα της εταιρίας για την έκθεση των ευαίσθητων προσωπικών στοιχείων των πελατών. Στην πραγματικότητα, το μόνο που μπορούσαν να δουν οι επίδοξοι εισβολείς, ήταν ο υπολειπόμενος χρόνος ομιλίας και το ποσό που χρωστούσε ο πελάτης.

Στο παραπάνω περιστατικό, ευτυχώς δεν υπήρξαν θύματα. Δεν συμβαίνει όμως πάντα το ίδιο. Η αλήθεια είναι ότι, οι περισσότεροι τηλεπικοινωνιακοί πάροχοι διαχειρίζονται τα δεδομένα των πελατών με ελαστικό τρόπο. Υπολογίζεται, ότι για το 70% περίπου της τηλεφωνικής απάτης ευθύνονται αδυναμίες που υπάρχουν στις διαδικασίες προώθησης προϊόντων και υπηρεσιών του οργανισμού.

Το μόνο που χρειάζεται να κάνει ο επίδοξος απατεώνας, είναι να βρει τα στοιχεία ενός πελάτη με καλό όνομα και ιστορικό. Πράγμα που είναι σχετικά εύκολο. Κλέβοντας την αλληλογραφία που του στέλνει ο πάροχος για παράδειγμα (ή ακόμα και να τη βρει στα σκουπίδια). Η αλληλογραφία μπορεί να περιέχει είτε λογαριασμούς, είτε διαφημιστικό υλικό, που αποτελεί πλούσια πηγή πληροφοριών γύρω από τον πελάτη. Φυσικά, ο κλέφτης μπορεί πάντα να κατασκοπεύσει τον ανυποψίαστο συνδρομητή για να δει τον αριθμό PIN του ή άλλα στοιχεία (εκεί βέβαια δεν ευθύνεται ο πάροχος).

Όταν λοιπόν με κάποιο δόλιο τρόπο ο απατεώνας αποσπάσει τα στοιχεία του πελάτη, μπορεί να καλέσει την εταιρία παριστάνοντας το θύμα του, για να επεξεργαστεί στοιχεία του λογαριασμού. Ακόμα, μπορεί να χρησιμοποιήσει το καλό όνομα του συνδρομητή για να λάβει υπηρεσίες και προϊόντα.

3.1.3 Πρόοδος στην παρακολούθηση δικτύων

Τα τελευταία χρόνια, υπάρχει μεγάλη βελτίωση στις τεχνικές παρακολούθησης δικτύων. Ο Peder Jungck είναι ιδρυτής της εταιρίας CloudShield, η οποία εδρεύει στην California των ΗΠΑ και ειδικεύεται στην κατασκευή εξειδικευμένου λογισμικού για παρακολούθηση και ασφάλεια δικτύων. Σύμφωνα με αυτόν, υπάρχουν πολλές φορές κενά ασφαλείας σε λειτουργίες του δικτύων μετάδοσης πακέτων. Υπάρχουν επίσης και πολλές καινούριες τεχνικές για τον περιορισμό των επιθέσεων, που δεν απαιτούν διακοπή της κανονικής λειτουργίας του δικτύου.

Μία από τις δυνατότητες του λογισμικού ασφαλείας, είναι να "πιάνει" τους hackers που κλέβουν δεδομένα από τις βάσεις μιας εταιρίας. Στην περίπτωση ενός τηλεπικοινωνιακού παρόχου, τα δεδομένα αυτά θα μπορούσαν να είναι αριθμοί τηλεφωνικών καρτών. Για παράδειγμα, το λογισμικό της CloudShield, μπορεί να τοποθετήσει ένα ηλεκτρονικό υδατόσημο στα δεδομένα που κατεβάζει ο κλέφτης, την ώρα που τα κατεβάζει χωρίς αυτός να το αντιληφθεί. Με τον τρόπο αυτό, η αστυνομία μπορεί να εντοπίσει και να παρακολουθεί τη χρήση κλεμμένων αριθμών τηλεφωνικών καρτών, ανακαλύπτοντας έτσι όχι μόνο τον κλέφτη, αλλά και πιθανούς "συναδέλφους" του (ολόκληρη δηλαδή σπείρα από hackers).

Μια άλλη δυνατότητα που έχει το λογισμικό, είναι να παρακολουθεί τις οικονομικές συναλλαγές από την αρχή, μέχρι το τέλος τους. Μπορεί να εντοπίσει την προσπάθεια τρίτων να παραβιάσουν τη συναλλαγή, hackers που προσπαθούν να μαντέψουν κωδικούς πρόσβασης καθώς και οποιαδήποτε απόκλιση της λειτουργίας του δικτύου από την προβλεπόμενη.

3.1.4 Τι πρέπει να κάνουν οι τηλεπικοινωνιακοί πάροχοι

Το επίπεδο της αυτοματοποίησης και της προστασίας που χρησιμοποιεί κάθε πάροχος, εξαρτάται από τον ίδιο. Αναμφίβολα όμως, τη σημερινή εποχή χρειάζονται υψηλά επίπεδα προστασίας. Τα ασταθή διεθνή δίκτυα, οι καινούριοι και αναξιόπιστοι πελάτες καθώς και όλοι οι επίδοξοι απατεώνες, βεβαιώνουν ότι θα υπάρξει απώλεια χρημάτων.

Χρειάζεται μεγάλη προσοχή από τους παρόχους τηλεπικοινωνιακών υπηρεσιών, ώστε να εντοπίσουν τους πραγματικούς απατεώνες. Η κατάχρηση εύρους ζώνης από κάποιο συνδρομητή αντιμετωπίζεται πολλές φορές σαν έγκλημα, χωρίς απαραίτητα να είναι. Απάτη υπάρχει όταν επιχειρείται απόκρυψη ταυτότητας. Όταν κάποιος συνδρομητής κάνει κακή χρήση του εύρους ζώνης, απλά παραβιάζει τους όρους του συμβολαίου του με την εταιρία. Ο τηλεπικοινωνιακός πάροχος, θα μπορούσε να χρεώσει επιπλέον τη κατάχρηση αυτή και να κυνηγήσει τους πραγματικούς απατεώνες.

Το σημαντικότερο βήμα για την προστασία των χρημάτων των συνδρομητών και των παρόχων είναι η εξαντλητική δοκιμή κάθε νέας υπηρεσίας, πριν αυτή ξεκινήσει να λειτουργεί. Πιο συγκεκριμένα, πρέπει να γίνει μια αξιολόγηση ασφαλείας σε όλους τους τομείς τη υπηρεσίας για να εντοπιστούν τυχόν κενά απ'όπου θα μπορούσαν να χαθούν χρήματα. Οι τεχνικοί ασφαλείας, θα πρέπει να εμπλέκονται σε όλα τα στάδια της ανάπτυξης νέων υπηρεσιών, ώστε να έχουν αφαιρέσει όλα τα πιθανά προβλήματα πριν την έναρξή τους.

Τη σημερινή εποχή, που οι τηλεπικοινωνιακές υπηρεσίες τρέχουν πάνω σε πολλές διαφορετικές πλατφόρμες, είναι δύσκολο να αντιμετωπιστεί η απάτη. Τα δεδομένα "ταξιδεύουν" ασύρματα, μέσα από modem και μέσα από τηλεφωνικές γραμμές. Δεν αρκεί απλά η προστασία των switch από παραβίαση. Χρειάζεται να δημιουργηθεί μια ενιαία πολιτική ασφαλείας που να καλύπτει όλους τους τηλεπικοινωνιακούς παρόχους της αγοράς. Η επιτυχία των τηλεπικοινωνιακών υπηρεσιών εξαρτάται από το πόσο εμπιστεύονται οι πελάτες τα στοιχεία τους στους παρόχους.

3.1.5 Οι απατεώνες μπορούν να βοηθήσουν

Αρκετοί από τους σύγχρονους hackers, βρίσκουν δουλειά[10] ως σύμβουλοι ασφαλείας σε εταιρίες που διαχειρίζονται ευαίσθητα δεδομένα πελατών (κυρίως δηλαδή τηλεπικοινωνιακούς οργανισμούς). Ένα πρόσφατο παράδειγμα προέρχεται από την Νέα Ζηλανδία. Ο δεύτερος μεγαλύτερος τηλεπικοινωνιακός οργανισμός της χώρας, η εταιρία TelstraClear, προσέλαβε το 2009 τον Owen Thor Walker ένα ικανό νεαρό hacker.

Ο Walker, διαχειριζόταν ένα ρομποτικό δίκτυο (botnet) αποτελούμενο από περίπου 1,3 εκατομμύρια υπολογιστές. Ακόμα, απέκτησε παράνομα πρόσβαση σε ένα server του πανεπιστημίου της Πενσυλβάνια και τον χρησιμοποιούσε για να εγκαθιστά ενημερωμένες εκδόσεις του κακόβουλου λογισμικού στα μολυσμένα μηχανήματα

[10] http://www.theregister.co.uk/2009/03/24/telstraclear_hires_convicted_hacker/

που είχε υπό τον έλεγχό του. Το ψευδώνυμο που χρησιμοποιούσε ήταν "Akill". Συνελήφθη κατά τη διάρκεια μιας επιχείρησης του FBI εναντίον hackers που χειρίζονταν botnets.

Ο Walker ομολόγησε τις πράξεις του και θα μπορούσε να έχει καταδικαστεί σε 5 χρόνια φυλάκισης ή επιτήρησης. Αντί αυτού όμως, έλαβε ένα συμβόλαιο με την TelstraClear, θυγατρική της εταιρίας Telstra που εδρεύει στην Αυστραλία. Η δουλειά του εκεί είναι εκπαιδευτική. Μέσα από μια σειρά σεμιναρίων, θα βοηθήσει τους τεχνικούς ασφαλείας της εταιρίας να αντιμετωπίσουν πιο αποτελεσματικά μελλοντικές επιθέσεις.

Το παραπάνω φαινόμενο (να προσλαμβάνονται δηλαδή καταδικασμένοι hackers), τείνει να γίνει μόδα μεταξύ των μεγάλων εταιριών. Φυσικά, οι πρώην hackers εκτός από νόμιμη δουλειά, αποκτούν και πρόσβαση στο δίκτυο της εταιρίας. Υπάρχουν όμως ερωτηματικά για την αξιοπιστία τους. Πολλοί το παρομοιάζουν με το να ανατεθεί σε κάποιο διαρρήκτη και κλέφτη έργων τέχνης η φύλαξη ενός μουσείου.

3.1.6 Fraud Management System

Η ραγδαία ανάπτυξη του κλάδου των τηλεπικοινωνιών, έχει σαν συνέπεια και την εμφάνιση νέων τύπων απάτης. Οι απατεώνες εκμεταλλεύονται κάθε αδυναμία που μπορούν να βρουν στα τηλεπικοινωνιακά συστήματα. Στις περιπτώσεις αυτές, στόχος είναι οι εταιρίες παροχής τηλεπικοινωνιακών υπηρεσιών. Το αποτέλεσμα είναι μεγάλη απώλεια κερδών για τους παρόχους που αυξάνεται χρόνο με το χρόνο. Εδώ έρχονται να βοηθήσουν τα FMS[11], ή Fraud Management Systems. Όπως μαρτυρά το όνομά τους, είναι συστήματα (κυρίως λογισμικό) που έχουν σαν σκοπό τον εντοπισμό κάθε ύποπτης συμπεριφοράς στο σύνολο του δικτύου που μπορεί να συνιστά απάτη. Βασίζονται σε κανόνες σωστής χρήσης του δικτύου και στη δημιουργία προφίλ για κάθε συνδρομητή.

Ένα σύγχρονο FMS, λειτουργεί σε δύο επίπεδα, διαχωρίζοντας τη βάση δεδομένων με τους κανόνες από την παρακολούθηση του δικτύου. Μπορεί δηλαδή να ενημερώνει τα στοιχεία του τη στιγμή που επιβλέπει και προστατεύει. Αυτό είναι ιδιαίτερα χρήσιμο κατά την προώθηση νέων προϊόντων και υπηρεσιών όπου ανακαλύπτονται συνεχώς αδυναμίες και το FMS πρέπει να ενημερώνεται δυναμικά. Αυτό αποτρέπει την εκμετάλλευση από τους απατεώνες και βελτιστοποιεί την ποιότητα των υπηρεσιών που παρέχεται στους χρήστες.

Όπως προαναφέρθηκε, η λειτουργία του FMS βασίζεται σε κανόνες συμπεριφοράς. Ένα FMS, παρακολουθεί συνεχώς τη συμπεριφορά των συνδρομητών και μπορεί να καταλάβει πότε κάτι αποκλίνει του φυσιολογικού. Δημιουργεί δηλαδή για κάθε χρήστη ένα προφίλ, ανάλογα με το ποιες υπηρεσίες χρησιμοποιεί και για πόσο χρόνο. Για παράδειγμα, κάποιος συνδρομητής πραγματοποιεί κάθε μέρα μόνο κλήσεις λίγων λεπτών. Αν ξαφνικά ξεκινήσει να χρησιμοποιεί υπηρεσίες που βασίζονται σε πακέτα GPRS ή να στέλνει ασύστολα SMS και MMS, το FMS θα τον επισημάνει ως ύποπτο. Κάποιος απατεώνας θα μπορούσε να έχει κλωνοποιήσει την κάρτα SIM και να

---

11 http://www.ztesoft.com/ztesoft_en/download/pdf/bss/products/Fraud%20Management%20Product.pdf

εκμεταλλεύεται τον ανυποψίαστο συνδρομητή. Το σύστημα έχει τη δυνατότητα να παρακολουθεί το δίκτυο σε πραγματικό χρόνο(την ώρα που χρησιμοποιείται), αλλά και σε μη πραγματικό(κάθε επόμενη μέρα αναλύει τη δραστηριότητα της προηγούμενης).

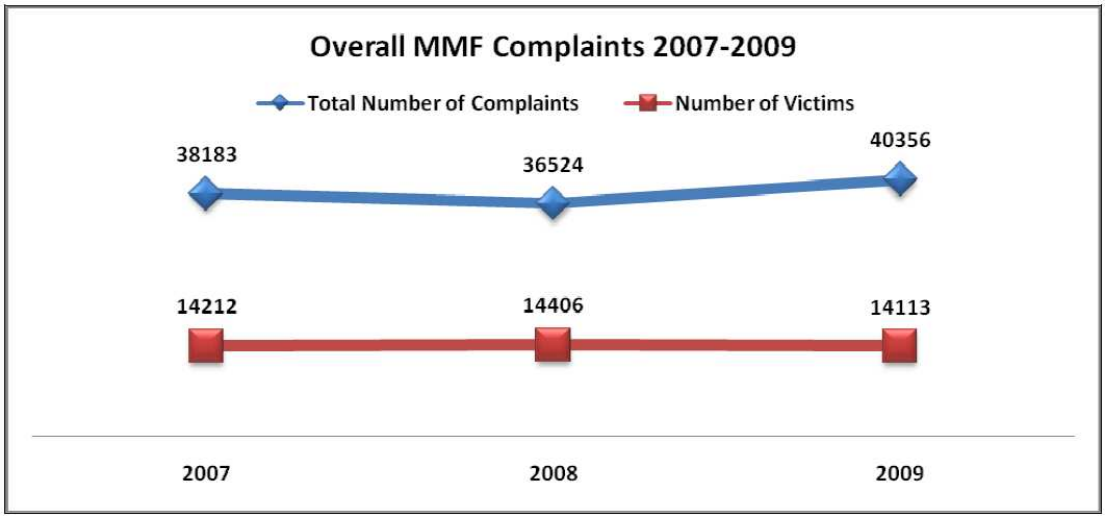
Όταν εντοπίσει κάποια περίπτωση ύποπτη για απάτη, το FMS ειδοποιεί τους αρμόδιους τεχνικούς ασφαλείας της εταιρίας, προτείνοντάς πιθανές λύσεις που έχει αποθηκευμένες στη βάση δεδομένων του. Φυσικά, ένα σύγχρονο σύστημα αποτροπής απάτης είναι πλήρως προγραμματιζόμενο. Οι τεχνικοί μπορούν, με κατάλληλες ρυθμίσεις, να δώσουν στο FMS τη δυνατότητα να αναλύσει και να διαχειριστεί μόνο του την απάτη. Μπορούν ανά πάσα στιγμή να ενσωματώσουν νέους κανόνες και λύσεις στο σύστημα. Τέλος, υπάρχει η δυνατότητα ανάλυσης της απάτης και παρουσίασης στατιστικών στοιχείων, ώστε ο πάροχος να βρει τις αδυναμίες που υπάρχουν στο δίκτυό του.

3.2 Μερικά στοιχεία για την απάτη

3.2.1 Στατιστικές από τον Καναδά

Τα παρακάτω στατιστικά στοιχεία[12] προέρχονται από τον Καναδά και συγκεκριμένα από το Κέντρο Αντιμετώπισης Απάτης (Canadian Anti Fraud Centre). Αφορούν το έτος 2009 και πραγματοποιείται σύγκριση με τα δύο προηγούμενα χρόνια.

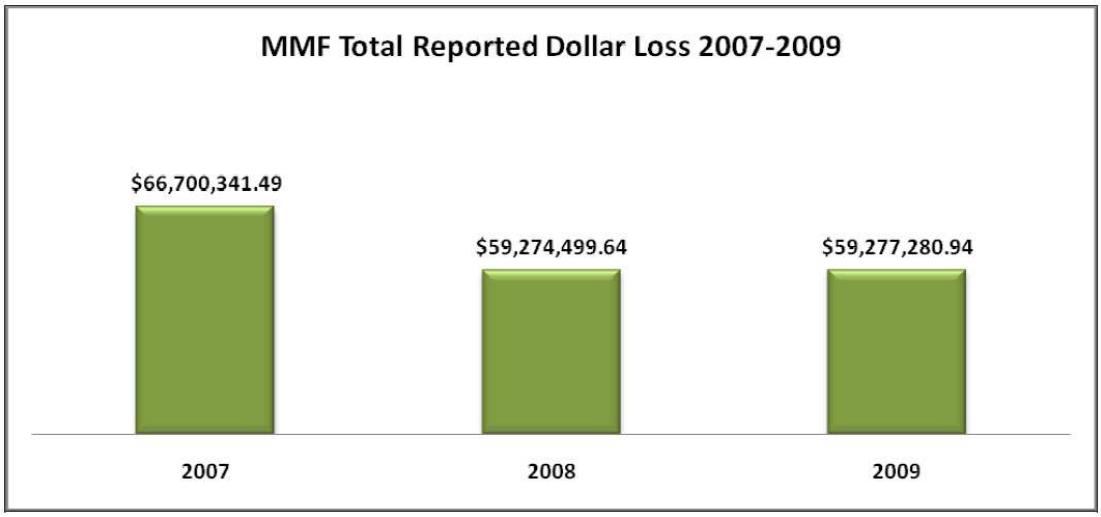
Στην παρακάτω εικόνα φαίνονται δύο διαγράμματα, ένα με το συνολικό αριθμό καταγγελιών και άλλο ένα με το συνολικό αριθμό των θυμάτων την περίοδο 2007-2009. Παρόλο που παρατηρείται μείωση των καταγγελιών το 2008 και απότομη αύξηση το 2009, ο συνολικός αριθμός θυμάτων παραμένει σχεδόν σταθερός.



Εικόνα 5: Αριθμός καταγγελιών-θυμάτων

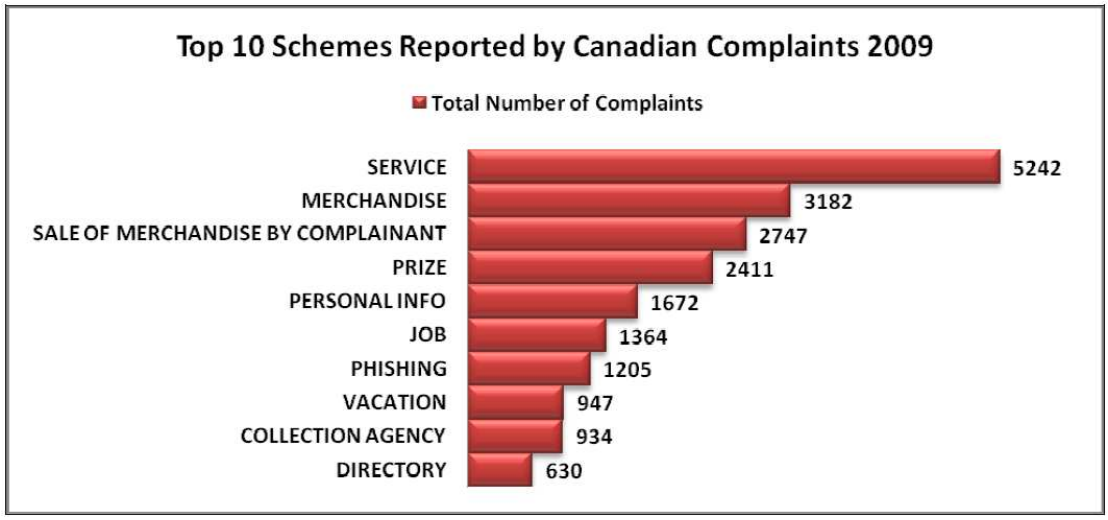
[12] http://www.phonebusters.com/english/statistics.html

Στην επόμενη εικόνα φαίνονται οι οικονομικές απώλειες σε δολάρια της περιόδου που εξετάζεται. Παρόλο που τα ποσά που χάνονται είναι τεράστια, είναι θετικό το γεγονός ότι παρατηρείται σημαντική μείωση το 2008 σε σχέση με το 2007.



Εικόνα 6: Οικονομικές απώλειες τηλεφωνικής απάτης

Παρακάτω φαίνεται ένα διάγραμμα με τις 10 μορφές τηλεφωνικής απάτης που συναντώνται πιο συχνά. Οι περισσότεροι απατεώνες, προσποιούνται ότι προσφέρουν κάποια υπηρεσία-προϊόν ή προσπαθούν να πείσουν το υποψήφιο θύμα ότι έχει κερδίσει βραβείο. Σε πιο σπάνιες περιπτώσεις παριστάνουν φοροεισπράκτορες ή υπαλλήλους υπηρεσίας τηλεφωνικού καταλόγου.



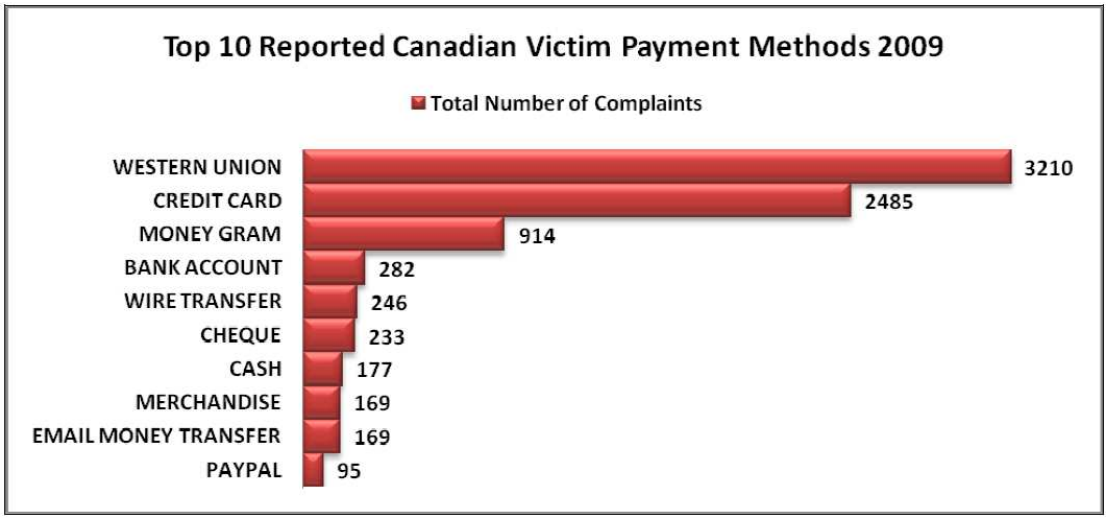
Εικόνα 7: Οι 10 κυρίαρχες μορφές τηλεφωνικής απάτης.

Στον επόμενο πίνακα, φαίνεται κάτι πολύ ενδιαφέρον και πιο συγκεκριμένα η ηλικιακή κατανομή των θυμάτων. Η ομάδα που πλήττεται περισσότερο είναι αυτή μεταξύ 50-59 ετών, αφού δέχονται το μεγαλύτερο αριθμό επιθέσεων και έχουν τη μεγαλύτερη απώλεια χρημάτων. Παρόλα αυτά, ο μεγαλύτερος αριθμός θυμάτων βρίσκεται στην ομάδα 40-49.

Canadian Complainant Age Range Breakdown on MMF 2009				
Age Range	No. of Attempts	No. of Victims	Total Number of Complaints	Total Reported Dollar Loss
1 - 9	2	1	3	$0.00
10 - 19	200	199	399	$185,107.75
20 - 29	1654	1065	2719	$1,559,635.57
30 - 39	2151	1052	3203	$2,230,658.50
40 - 49	2732	1279	4011	$4,256,304.86
50 - 59	2864	1109	3973	$6,201,911.34
60 - 69	2556	851	3407	$3,843,559.76
70 - 79	1364	416	1780	$2,206,696.69
80 - 89	581	238	819	$691,298.22
90 - 99	71	33	104	$141,536.93
BUSINESS	1568	444	2012	$2,069,661.98
DECEASED	39	2	41	$63,000.00
UNKNOWN	2665	1093	3758	$2,965,663.88

Εικόνα 8: Ηλικιακή κατανομή των θυμάτων.

Το διάγραμμα που ακολουθεί, απεικονίζει τους 10 προτιμώμενους τρόπους με τους οποίους τα θύματα πλήρωσαν τους απατεώνες. Ενώ θα περίμενε κανείς την πρώτη θέση να την κατέχει η πιστωτική κάρτα, κάτι τέτοιο δεν ισχύει. Σύμφωνα με το διάγραμμα, η κατεξοχήν χρησιμοποιούμενη μέθοδος είναι η Western Union, ενώ η λιγότερο χρησιμοποιούμενη το PayPal (και οι δύο είναι εταιρίες που δραστηριοποιούνται στη διακίνηση χρημάτων).



Εικόνα 9: Οι τρόποι πληρωμής των θυμάτων.

3.2.2 Στοιχεία για τις Η.Π.Α

Ο Dr. Lynne Russell, καθηγητής στο πανεπιστήμιο του Arkansas πραγματοποίησε μια ενδιαφέρουσα έρευνα σχετικά με την απάτη γενικά. Από την έρευνα αυτή έχουν απομονωθεί τα στοιχεία που αφορούν την τηλεπικοινωνιακή απάτη και παρουσιάζονται παρακάτω. Τα στοιχεία προέρχονται φυσικά από τον πληθυσμό των ΗΠΑ.

Πρώτα απ' όλα, πρέπει να σημειωθεί ότι ένας στους έξι αμερικανούς δηλώνει θύμα απάτης, οποιασδήποτε μορφής. Περίπου 30% των Αμερικανών, λαμβάνουν μέρος σε πλαστούς διαγωνισμούς. Από αυτούς που εξαπατούνται, μόνο το 10% καταγγέλλει το περιστατικό στις αρχές. Μόνο το 31% ανέφερε το περιστατικό σε κάποιον (συγγενή, φίλο ή τις αρχές). Περίπου το 51% αυτών που εξαπατήθηκαν, προσπάθησαν να επικοινωνήσουν με την εταιρία που τους εξαπάτησε. Μόλις το 9% του συνόλου των εξαπατημένων, κατάφερε να ανακτήσει τα χρήματά του. Τα άτομα ηλικίας άνω των 65, αποτελούν το 12% του πληθυσμού των ΗΠΑ, αλλά και περίπου το 30% των εξαπατημένων. Σύμφωνα με το FBI κάθε χρόνο χάνονται πάνω από 40 δισεκατομμύρια δολάρια εξαιτίας της τηλεφωνικής απάτης.

Στις ΗΠΑ, υπάρχουν κατ' εκτίμηση 700 εταιρίες τηλεφωνικών πωλήσεων οι οποίες πραγματοποιούν 18 εκατομμύρια κλήσεις ημερησίως και απασχολούν 3 με 5 εκατομμύρια εργαζόμενους. Το 10% αυτών των εταιριών δεν είναι νόμιμες. Το 54% των ενήλικων Αμερικανών, δήλωσε ότι θα έκλεινε το τηλέφωνο αν κάποιος άγνωστος τους έκανε μια προσφορά ή πρόταση για επένδυση που ακουγόταν υπερβολικά δελεαστική. Το 17% των Αμερικανών δήλωσαν ότι δυσκολεύονται να αντισταθούν σε ένα προϊόν που τους προσφέρεται τηλεφωνικά σε καλή τιμή. Οι έγχρωμοι και οι Ισπανόφωνοι Αμερικανοί εξαπατώνται ευκολότερα από τους λευκούς, σύμφωνα με την έρευνα. Επίσης ευκολότερα θύματα αποτελούν οι άνθρωποι με χαμηλό μορφωτικό επίπεδο όπως και τα νοικοκυριά με εισόδημα κάτω των $15000 το χρόνο.

Τα στατιστικά που παρατίθενται στη συνέχεια, προέρχονται από το CFCA (Communications Fraud Control Assosiation)[13], που είναι ένας μη κερδοσκοπικός οργανισμός με έδρα τις ΗΠΑ και ασχολείται με την μελέτη και πρόληψη τηλεπικοινωνιακής απάτης(εναντίον κυρίως των εταιριών). Αφορούν μια έρευνα που πραγματοποίησε ο οργανισμός την περίοδο 2005-2008 και δημοσιεύτηκε το 2009. Αντικείμενο της έρευνας είναι το αντίκτυπο της εξαπάτησης των τηλεπικοινωνιακών παρόχων. Μελετώνται οι περιπτώσεις όπου οι απατεώνες χρησιμοποιούν τις υπηρεσίες και τα προϊόντα των παρόχων χωρίς να σκοπεύουν να πληρώσουν (δηλαδή πλαστές συνδρομές και κλωνοποίηση τηλεφώνων και οι παραλλαγές τους για τα οποία υπάρχει περιγραφή στο επόμενο κεφάλαιο).

Σύμφωνα με την έρευνα, την περίοδο 2005-2008 αυξήθηκε το εισόδημα των τηλεπικοινωνιακών εταιριών παγκοσμίως κατά 52% αλλά ταυτόχρονα αυξήθηκε και η απάτη κατά 34%. Οι οικονομικοί αναλυτές εκτιμούν ότι οι χρηματικές απώλειες λόγω της απάτης ανέρχονται περίπου σε $72-$80 δισεκατομμύρια το χρόνο σε παγκόσμιο επίπεδο. Τα χρήματα αυτά αποτελούν περίπου το 4,5% του εισοδήματος του κλάδου των τηλεπικοινωνιών. Αξίζει να σημειωθεί ότι παρά την αύξηση των περιπτώσεων απάτης, οι χρηματικές απώλειες μειώθηκαν κατά 0,6% λόγω της απότομης αύξησης του εισοδήματος.

Οι πρώτες πέντε χώρες στις οποίες διαπράττεται κατά κόρον τέτοια μορφή απάτης είναι κατά σειρά: Κούβα, Φιλιππίνες, Λίχνενσταϊν, Ινδία και Ηνωμένο Βασίλειο. Το 91% των παρόχων που συμμετείχαν στη έρευνα δήλωσαν ότι οι οικονομικές απώλειες από την απάτη έχουν αυξηθεί ελαφρώς ή έχουν μείνει το ίδιο. Το 78% των

[13] http://www.cfca.org/pdf/survey/2009%20Global%20Fraud%20Loss%20Survey-Press%20Release.pdf

συμμετεχόντων δήλωσαν ότι οι εσωτερικές απώλειες του οργανισμού τους έχουν αυξηθεί ή έχουν μείνει το ίδιο. Οι απώλειες σε μορφή ποσοστού ποικίλουν ανάλογα με τον οργανισμό. Το 23% των συμμετεχόντων δήλωσαν απώλειες της τάξης του 1% του εισοδήματος, ενώ το 27% από αυτούς δήλωσαν απώλειες της τάξης του 5%. Όπως είναι φυσικό εταιρίες που είχαν πάρει μέτρα περιορισμού της απάτης έχασαν λιγότερα χρήματα. Οι τρεις κατηγορίες απάτης που προκάλεσαν τη μεγαλύτερη ζημιά είναι: 1)πλαστές συνδρομές (29% των απωλειών αντιστοιχούν σε $22 δις), 2)Παραβίαση τηλεφωνικών κέντρων (20% των απωλειών αντιστοιχούν σε $15 δις), 3)απάτη με αριθμούς υψηλής χρέωσης (6% των απωλειών αντιστοιχούν σε $4,5 δις).

3.2.3 Αυξανόμενη απάτη εναντίον επιχειρήσεων στις ΗΠΑ

Το πρώτο τρίμηνο του 2010, η τηλεπικοινωνιακή απάτη σε βάρος εταιριών στις ΗΠΑ αυξήθηκε κατά 400%. Αυτό προκύπτει από στοιχεία[14] του TIG (Telecommunications Industry Group) που είναι μια κοινοπραξία τηλεπικοινωνιακών παρόχων και τα οποία δημοσιεύτηκαν στην ιστοσελίδα National Business Review. Σύμφωνα με την TIG, δέκα εταιρίες την εβδομάδα πέφτουν θύματα hacker. Αυτοί, επιτίθενται στα συστήματα PBX, πραγματοποιούν κλήσεις σε αριθμούς υψηλής χρέωσης που έχουν στήσει οι ίδιοι σε χώρες με χαλαρό νομικό καθεστώς (κυρίως στην Αφρική και σε ορισμένα μέρη της Ευρώπης. Οι απατεώνες μπορεί να βρίσκονται οπουδήποτε στον κόσμο. Οι χρεώσεις στις περιπτώσεις αυτές ανέρχονται περίπου σε $15 ανά λεπτό. Το χειρότερο είναι ότι οι επιθέσεις γίνονται απογεύματα και Κυριακές (όταν δηλαδή είναι κλειστές οι επιχειρήσεις), με αποτέλεσμα να μην καταλάβει κανένας κάτι. Έτσι, οι απατεώνες μπορούν να κερδίσουν χιλιάδες δολάρια εύκολα και γρήγορα και οι επιχειρήσεις θα το αντιληφθούν όταν θα είναι αργά.

Ο Rob Spray, στέλεχος της TIG, δηλώνει ότι κατά μέσο όρο κάθε εταιρία που εξαπατάται με τέτοιο τρόπο, χάνει περίπου $10000. Υπάρχουν όμως και πολλές περιπτώσεις που οι απώλειες είναι μεταξύ $20000 και $50000. Σύμφωνα με τον κύριο Spray, η ευκολία απόκτησης συστήματος PBX από τις μικρές εταιρίες έχει οδηγήσει στην αύξηση των επιθέσεων. Παλιότερα, μόνο οι μεγάλες εταιρίες μπορούσαν να αποκτήσουν το δικό τους PBX, αφού το τελευταίο είχε απαγορευτικό κόστος. Όμως, τα τελευταία πέντε χρόνια έχουν εμφανιστεί ψηφιακά PBX που βασίζονται στο πρωτόκολλο IP. κατά συνέπεια οι περισσότερες μικρές επιχειρήσεις μπορούν να εγκαταστήσουν το δικό τους. Ένας ιδιοκτήτης χωρίς γνώσεις γύρω από το VoIP(Voice over IP) μπορεί να στήσει ένα IP PBX σε λιγότερο από μια ώρα.

Εκεί ακριβώς βρίσκεται το πρόβλημα. Ένας άνθρωπος χωρίς γνώσεις μπορεί να στήσει ένα σύστημα που λειτουργεί αλλά δεν έχουν γίνει οι απαραίτητες ρυθμίσεις ασφαλείας. Έτσι τα συστήματα IP PBX είναι ευάλωτα σε επιθέσεις από hackers. Μια τυπική παράλειψη είναι να αφήνουν οι ιδιοκτήτες το εργοστασιακό password στο σύστημά τους, ή να επιλέγουν κάποιο εύκολο(1234, 0000, κλπ). Κάτι άλλο που παραλείπεται συχνά στις περιπτώσεις αυτές είναι η ρύθμιση του τείχους προστασίας, ώστε να επιτρέπεται πρόσβαση μόνο στον τηλεπικοινωνιακό πάροχο. Φυσικά, υπάρχουν και αρκετοί που ισχυρίζονται πως είναι ειδικοί σε τέτοια συστήματα αλλά έχουν στην πραγματικότητα μόνο βασικές γνώσεις. Όπως θα περιγραφεί σε επόμενο

[14] http://www.nbr.co.nz/article/companies-hit-400-increase-phone-fraud-128569

κεφάλαιο, οι hackers αποκτούν πρόσβαση διαχειριστή μέσω της θύρας συντήρησης του PBX και από εκεί μπορούν να κάνουν πραγματικά ότι θέλουν.

Η μόνη λύση στο πρόβλημα είναι η σωστή πρόληψη κατά το στήσιμο του συστήματος. Οι απατεώνες δρουν από μεγάλη απόσταση, ίσως και από άλλη χώρα. Υπάρχουν μερικά περιστατικά συλλήψεων αλλά ο κανόνας είναι ότι οι απατεώνες δεν θα συλληφθούν ποτέ. Τελικά, υπεύθυνος γι' αυτό που συμβαίνει είναι ο ιδιοκτήτης του PBX και όχι ο πάροχος και το χρέος δεν παραγράφεται με κανένα τρόπο.

3.2.4 Ποιοι είναι πιθανοί προδότες του οργανισμού τους

Η παρακάτω έρευνα[15] προσπαθεί να κάνει γνωστό στο ευρύ κοινό ποιοι υπάλληλοι είναι πιθανό να προδώσουν τον οργανισμό τους. Πραγματοποιήθηκε από τον οργανισμό ACFE (Association of Certified Fraud Examiners). Ο οργανισμός αυτός αποτελείται από ανθρώπους ειδικούς στην αντιμετώπιση της απάτης κάθε μορφής από όλο τον κόσμο. Παρέχει κυρίως ενημέρωση και συμβουλές προστασίας και οικονομική υποστήριξη στους ενδιαφερόμενους μέσω ερευνών και επιχορηγήσεων. Ακόμα, χρηματοδοτεί υποτροφίες υποψήφιων μελών του.

Σύμφωνα με την έρευνα, βασικοί ένοχοι είναι οι άντρες. Η πιθανότητα να διαπράξει ένας άντρας απάτη είναι δύο φορές μεγαλύτερη από μια γυναίκα συνάδελφό του. Ακόμα, οι απώλειες στις περιπτώσεις απάτης των αρρένων είναι διπλάσιες ή και περισσότερες. Αυτό μπορεί να οφείλεται στο γεγονός ότι οι άνδρες κατέχουν τις περισσότερες υψηλόβαθμες θέσεις στις επιχειρήσεις και κατά συνέπεια μπορούν να προκαλέσουν μεγαλύτερη οικονομική ζημιά. Η ηλικία των απατεώνων είναι τα 40 χρόνια κατά μέσο όρο. Γενικά, οι κάτοχοι των θέσεων εξουσίας είναι από 50 ετών και άνω και αυτοί είναι που προκαλούν τις μεγαλύτερες απώλειες (το διπλάσιο από αυτό που προκαλεί το σύνολο των ηλικιακών ομάδων κάτω των 50). Στα περισσότερα περιστατικά απάτης, οι ένοχοι δρουν μόνοι τους. Αν υπάρχει συνεργασία δύο ή περισσότερων ατόμων, έχει αποδειχτεί ότι η οικονομική ζημιά είναι μέχρι και τέσσερις φορές μεγαλύτερη. Τέλος, η έρευνα έδειξε ότι όσο υψηλότερο είναι το μορφωτικό επίπεδο του απατεώνα, τόσο μεγαλύτερη είναι η οικονομική ζημιά. Το τμήμα των επιχειρήσεων με τους περισσότερους προδότες είναι το λογιστήριο, αφού οι εργαζόμενοι του έχουν πρόσβαση στα περιουσιακά στοιχεία του οργανισμού και μπορούν πιο εύκολα να κρύψουν την απάτη.

3.3 Πραγματικά περιστατικά

3.3.1 Το κύκλωμα με τα iPhone

Αυτό το πρόσφατο περιστατικό[16] δείχνει πόσο καλά οργανωμένοι μπορεί να είναι οι απατεώνες. Η αστυνομία του Λονδίνου έκανε τον Αύγουστο του 2010 επιδρομή σε διάφορα σημεία της πόλης και κατάφερε να συλλάβει εννέα υπόπτους. Αυτοί συμμετείχαν σε ένα διεθνές κύκλωμα τηλεπικοινωνιακής απάτης, που έκανε ζημιά εκατομμυρίων λιρών σε παρόχους της Μεγάλης Βρετανίας.

[15] http://www.scribd.com/doc/13885875/Interesting-Facts-about-Fraud
[16] http://news.softpedia.com/news/UK-Police-Dismantles-International-Telecom-Fraud-Ring-153123.shtml

Οι ύποπτοι του Λονδίνου ήταν μόνο μία από τις πολλές ομάδες απ' όλο τον κόσμο που συμμετείχαν στο κύκλωμα. Η απάτη ξεκινούσε από μια συμμορία απατεώνων στη δυτική Αφρική. Αυτοί, χρησιμοποιώντας κλωνοποιημένες πιστωτικές κάρτες και κλεμμένες ταυτότητες αγόραζαν συνδρομές κινητής τηλεφωνίας και συσκευές IPhone μέσω διαδικτύου. Στη συνέχεια, διεφθαρμένοι οδηγοί (τους είχε χρηματίσει το κύκλωμα) αναλάμβαναν να παραδώσουν τις συσκευές και τις κάρτες SIM σε ένα συγκεκριμένο άτομο και όχι στην διεύθυνση που είχε δηλωθεί κατά την παραγγελία. Το πρόσωπο αυτό υπολογίζεται ότι έλαβε σχεδόν 1000 IPhone με τον παραπάνω τρόπο.

Και αυτή ήταν μόνο η αρχή. Οι κάρτες SIM αφαιρούνταν από τις συσκευές από τον τύπο που αναφέρθηκε πριν. Στη συνέχεια, πωλούνταν (οι SIM) σε μια άλλη συμμορία αποτελούμενη από υπηκόους του Πακιστάν. Η ομάδα αυτή, έστελνε τις κάρτες σε συνεργάτες που είχε στη μέση Ανατολή, την Ασία και την Ευρώπη. οι κάρτες τοποθετούνταν σε φυσικούς αυτόματους dialers (συσκευές) και καλούσαν τοπικούς αριθμούς υψηλής χρέωσης ασταμάτητα. Με τη μέθοδο αυτή, οι απατεώνες κατάφεραν να κλέψουν από τη Βρετανική εταιρία τηλεπικοινωνιών O2 $1,800,000 μόνο τον Ιούλιο. Η O2 πλήρωνε τους ξένους παρόχους για τους αριθμούς υψηλής χρέωσης, αλλά η ίδια δεν έπαιρνε ποτέ τα χρήματα από τους "πελάτες" της.

Όσο αφορά τα IPhone, αυτά πωλούνταν από άλλη συμμορία σε χώρες που οι πάροχοι δεν μπλοκάρουν τις κλεμμένες συσκευές. Το ενδιαφέρον είναι ότι συνήθως πωλούνταν στην κανονική τιμή λιανικής. Μετά την επιδρομή, η αστυνομία βρήκε και κατέσχεσε εκατοντάδες κάρτες SIM, καινούρια IPhone στα κουτιά τους, κλωνοποιημένες πιστωτικές κάρτες και πλαστά διαβατήρια.

3.3.2 Μαζική σύλληψη υπόπτων στην Κίνα

Η τηλεπικοινωνιακή απάτη χτυπάει σε μεγάλο και τις χώρες της ανατολικής Ασίας. οι αστυνομικές δυνάμεις της Κίνας και της Ταιβάν ξεκίνησαν τον Ιούνιο του 2010 μια κοινή επιχείρηση[17] για να εξαρθρώσουν κυκλώματα που δραστηριοποιούνταν σε αυτό τον τομέα απάτης. Μέχρι τον Αύγουστο του ιδίου έτους, είχαν συλλάβει 1,282 υπόπτους, καταστρέφοντας 150 συμμορίες.

Τον Αύγουστο του ίδιου έτους, οι αστυνομικές δυνάμεις των δύο χωρών, κατέστρεψαν ένα μεγάλο κύκλωμα τηλεπικοινωνιακής απάτης με έδρα την Κίνα. Συνολικά συνελήφθησαν 451 άτομα. Από αυτούς, οι 186 προέρχονταν από την Ταιβάν, ένας από το Χονγκ-Κογκ και οι υπόλοιποι από την Κίνα. Τον Μάιο εντοπίστηκε ένας τύπος ονόματι Jiang (υπήκοος Ταιβάν), ο οποίος είχε νοικιάσει ένα server στην επαρχία Fujian της Κίνας. Χρησιμοποιώντας τον server αυτόν, στήθηκε το προαναφερθέν δίκτυο εξαπάτησης. Οι απατεώνες παρείχαν τηλεφωνικές υπηρεσίες σε ανυποψίαστους καταναλωτές. Ουσιαστικά, είχαν στήσει μια παράνομη εταιρία τηλεπικοινωνιών. Η συμμορία των απατεώνων αποτελούνταν από τρία μέρη. Υπήρχε ομάδα τεχνικής υποστήριξης, υπεύθυνη για τη λειτουργία του δικτύου. Στη συνέχεια, υπήρχε η ομάδα η οποία μάζευε πελάτες. Το τρίτο μέρος ήταν μια παράνομη τράπεζα

[17] http://english.cri.cn/6909/2010/08/25/45s591016.htm

η οποία ασχολούνταν φυσικά με τη διαχείριση και το ξέπλυμα των χρημάτων που έκλεβαν οι απατεώνες.

3.3.3 Η συμμορία της Ταιβάν

Την ίδια περίοδο και συγκεκριμένα στις 18 Αυγούστου, εξαρθρώθηκε άλλο ενα παρόμοιο (αλλά πολύ μικρότερο) κύκλωμα[18] από την αστυνομία. Αυτή η δεύτερη συμμορία αποτελούνταν από 17 μέλη και είχε σαν έδρα την Ταϊβάν. Λειτουργούσε πίσω από την κάλυψη ενός νόμιμου καταστήματος λατρευτικών ειδών. Η ιδιαιτερότητα αυτής της συμμορίας, ήταν ότι στρατολογούσε ανήλικα εγκληματικά στοιχεία για την πραγματοποίηση των κλήσεων. Τα θύματα προερχόταν στο σύνολό τους από την Κίνα.

Οι απατεώνες δρούσαν σε δύο στάδια. Πρώτα επέλεγαν (τυχαία) τα θύματά τους. Στη συνέχεια καλούσαν παριστάνοντας εκπροσώπους της εταιρίας China Telecom (η μεγαλύτερη εταιρία σταθερής τηλεφωνίας στην Κίνα). Μία γυναίκα, υποτιθέμενη υπάλληλος τους τμήματος εξυπηρέτησης πελατών, καλούσε το θύμα λέγοντάς του ότι υπάρχει κάποιο πρόβλημα με το λογαριασμό του και ότι υπάρχει πιθανότητα να τον εκμεταλλεύεται κάποιος απατεώνας. Στη συνέχεια, η κλήση προωθούνταν στην (υποτιθέμενη) αστυνομία. Φυσικά, οι αστυνομικοί δεν ήταν πραγματικοί αλλά μέλη του κυκλώματος. Αυτοί συμβούλευαν το θύμα να αλλάξει το pin στην κάρτα του ATM του, για περισσότερη ασφάλεια (ακολουθώντας φυσικά τις δικές τους οδηγίες).

Στο δεύτερο στάδιο, οι απατεώνες επικοινωνούσαν με τα θύματα παριστάνοντας υπαλλήλους της εισαγγελίας ή κάποιου οικονομικού οργανισμού. Συμβούλευαν τους συνδρομητές να μεταφέρουν τις καταθέσεις τους σε ένα λογαριασμό που τους υποδείκνυαν. Η δικαιολογία ήταν ότι υπήρχε πιθανόν διαρροή των στοιχείων τους (που συνδεόταν με τη υποτιθέμενη διαρροή του προηγούμενου τηλεφωνήματος) και έπρεπε να εξασφαλίσουν τα χρήματά τους. Αν το θύμα έκανε το λάθος να τους πιστέψει και πραγματοποιούσε τη μεταφορά, αυτοί στη συνέχεια πραγματοποιούσαν ανάληψη από τον πλαστό λογαριασμό.

Τα μέλη της ομάδας ήταν μέλη μιας τοπικής θρησκευτικής οργάνωσης της Ταιβάν και όπως προαναφέρθηκε, κέντρο των επιχειρήσεών τους ήταν ένα κατάστημα λατρευτικών ειδών. Το κτίριο αποτελούνταν από πολλά κρυφά δωμάτια και είχε πολλές κρυφές εξόδους. Μέσα στα δωμάτια αυτά πραγματοποιούσαν τις κλήσεις οι ανήλικοι απατεώνες μέσω voip τηλεφώνων. Στην είσοδο και τον κεντρικό διάδρομο του κτιρίου, υπήρχαν κάμερες παρακολούθησης που ειδοποιούσαν αυτούς που βρισκόταν στα ενδότερα για πιθανή έλευση της αστυνομίας.

Οι αστυνομικοί είχαν πληροφορηθεί για την ύπαρξη της ομάδας από τον Ιανουάριο του 2010. Τους επόμενους οκτώ μήνες μάζευαν στοιχεία εναντίον τους. Όταν πραγματοποιήθηκε η επιδρομή τον Αύγουστο, η ομάδα πιάστηκε εν ώρα εργασίας. Όταν οι απατεώνες είδαν τους αστυνομικούς μέσα από τις κάμερες και προσπάθησαν να καταστρέψουν όσα στοιχεία μπορούσαν, φυσικά και ψηφιακά. Μερικοί, δοκίμασαν να ξεφύγουν από τις διάφορες εξόδους που διέθετε το κτίριο. Ήταν όμως

[18] http://www.free-press-release.com/news-fraud-crime-gang-busted-1282542064.html

αργά για όλους, αφού συνελήφθησαν στο σύνολό τους. Στιγμιότυπα της σύλληψης φαίνονται στις παρακάτω εικόνες. Στην αρχή αρνήθηκαν τις κατηγορίες, αλλά αφού τους παρουσιάστηκαν αποδεικτικά στοιχεία (κυρίως ηχογραφημένες συνομιλίες) ομολόγησαν όλοι. Η παρακολούθηση των υπόπτων έγινε με σύστημα e-detective (σύστημα διαδικτυακής παρακολούθησης αποτελούμενο από υλικό και λογισμικό αποκλειστικά για χρήση από τις υπηρεσίες επιβολής του νόμου) από την εταιρία Decision Group[19]. Το ακριβές ποσό που απέσπασαν από τα θύματά τους οι απατεώνες είναι δύσκολο να εκτιμηθεί. Οι πλαστοί λογαριασμοί που χρησιμοποιούνταν βρισκόταν στην Κίνα. Εκεί συνεργάτες του κυκλώματος τα έβγαζαν από τους πλαστούς λογαριασμούς και τα τοποθετούσαν κανονικούς. Ένα μεγάλο μέρος τους χρησιμοποιούνταν για την πληρωμή μισθού σε αυτούς που βρισκόταν στην Ταιβάν.

Εικόνα 10: Στιγμιότυπα από τη σύλληψη

[19] http://www.edecision4u.com

Κεφάλαιο 4 Οι Τύποι της απάτης

Οι τύποι της απάτης[20] μπορούν να χωριστούν σε δύο μεγάλες κατηγορίες: εναντίον χρηστών και εναντίον εταιριών. Οι χρήστες μπορούν να εξαπατηθούν είτε από εταιρίες (όχι απαραίτητα τηλεπικοινωνιακές), είτε (κυρίως) από τρίτους. Οι εταιρίες γίνονται στόχος είτε άλλων εταιριών, είτε κακόβουλων τρίτων (σε μερικές περιπτώσεις και των ίδιων των συνδρομητών).

4.1 Απάτες εταιριών εναντίον των χρηστών από εταιρίες

4.1.1 Cramming

Το cramming[21] είναι μια μορφή απάτης κατά την οποία μικρές χρεώσεις προστίθενται στο λογαριασμό του συνδρομητή, χωρίς ο ίδιος να το έχει εγκρίνει ή να το γνωρίζει. Σε πολλές περιπτώσεις, η χρεώσεις αυτές μπορεί να είναι μεταμφιεσμένες σαν τηλεφωνικά τέλη που χρεώνονται φυσιολογικά. Ο σκοπός του cramming είναι, να μην δώσει ο συνδρομητής σημασία στη μικρή αυτή χρέωση και να την πληρώσει. Σύμφωνα με την Ένωση Δικηγόρων της Αμερικής, το cramming ήταν 4η συχνή απάτη το 2007.

Ο μόνος τρόπος να εντοπιστεί[22] το cramming είναι η ανάγνωση του μηνιαίου τηλεφωνικού λογαριασμού. Ανάγνωση βέβαια, δεν σημαίνει να κοιτάξει κάποιος μόνο το σύνολο, αλλά να διαβάσει αναλυτικά κάθε γραμμή του λογαριασμού και να καταλάβει από που προέρχεται η κάθε χρέωση. Με την πάροδο του χρόνου ο συνδρομητής μπορεί να καταλάβει ποιές χρεώσεις υπάρχουν πάγιες στον λογαριασμό του και ποιές προέρχονται από κάποια άγνωστη πηγή.

Υπάρχουν πολλά παραδείγματα τέτοιων χρεώσεων. Το πιο συνηθισμένο είναι να υπάρχουν περισσότερα τέλη τηλεφωνίας από το κανονικό. Εάν τα τέλη αυτά δεν περιλαμβάνονται στο συμβόλαιο που έχει υπογράψει ο συνδρομητής με την εταιρεία τότε κατά πάσα πιθανότητα είναι παράνομα. Ακόμα, θα μπορούσαν στο λογαριασμό να περιλαμβάνονται κλήσεις προς αριθμούς υψηλής χρέωσης, τις οποίες ο συνδρομητής δεν πραγματοποίησε ποτέ. Άλλο επίσης συχνό παράδειγμα είναι η χρέωση υπηρεσιών τηλεφωνίας τις οποίες δεν έχει ζητήσει και δεν λαμβάνει ο συνδρομητής (κατέβασμα ήχων κλήσης για παράδειγμα), ή παράλογη χρέωση για υπηρεσίες που έχει ζητήσει.

Σε περίπτωση που ο συνδρομητής εντοπίσει κάποια χρέωση της οποίας την υπηρεσία δεν έχει λάβει ποτέ ή του φαίνεται γενικά παράξενη, το πρώτο πράγμα που πρέπει να κάνει είναι να καλέσει την εταιρεία από την οποία προέρχεται η χρέωση. Στην συνέχεια πρέπει να επικοινωνήσει με τον τηλεπικοινωνιακό πάροχο και να τον ενημερώσει για την λανθασμένη χρέωση. Εάν το πρόβλημα δεν διορθωθεί τότε ο συνδρομητής θα πρέπει να κάνει κάποια διαμαρτυρία σε ένωση καταναλωτών ή στις τοπικές αρχές.

---

[20] http://en.wikipedia.org/wiki/Phone_fraud
[21] http://en.wikipedia.org/wiki/Cramming_(fraud)
[22] http://www.ucan.org/telenforcers/consumers/pursueandresolve/strategic_guides/cramming

4.1.2 Slamming

Το slamming[23] είναι μια ανορθόδοξη πρακτική (αλλά όχι απαραίτητα παράνομη), κατά την οποία οι τηλεφωνικές υπηρεσίες ενός συνδρομητή μεταφέρονται από μία εταιρία σε άλλη, χωρίς ο ίδιος να το γνωρίζει ή να το εγκρίνει. Στη Μεγάλη Βρετανία, το slamming χτυπάει περίπου 15000 καταναλωτές το μήνα. Οι slammers εκμεταλλεύονται συνήθως κενά που υπάρχουν στο νόμο. Τα μόνα πράγματα που χρειάζονται για να εγγράψουν το θύμα σε άλλο δίκτυο, είναι το όνομα, ο ταχυδρομικός κώδικας και το νούμερο τηλεφώνου. Δε χρειάζονται κάποια υπογραφή ή γραπτή συναίνεση από το συνδρομητή. Για να κινούνται στο πλαίσιο της νομιμότητας, οι slammers είναι υποχρεωμένοι να του στείλουν ένα γράμμα, όπου τον ενημερώνουν για την αλλαγή που έχει γίνει και του δίνουν δέκα μέρες για να ακυρώσει τη μεταφορά. Πολλά από τα θύματα, πετούν τα γράμματα νομίζοντας ότι πρόκειται για διαφημιστικό υλικό και περνούν εβδομάδες ή μήνες μέχρι να καταλάβουν τι έχει συμβεί.

Αξίζει να εξεταστεί μια τυπική περίπτωση slamming. Ένας πωλητής μιας τηλεφωνικής εταιρίας τηλεφωνεί στον πελάτη μιας ανταγωνιστικής εταιρίας. Ο πωλητής υπόσχεται χαμηλότερες χρεώσεις και προσπαθεί να πείσει τον πελάτη να αλλάξει πάροχο. Αυτός αρνείται να κάνει τη αλλαγή, αλλά συμφωνεί να του σταλούν ενημερωτικά έντυπα με το ταχυδρομείο δίνοντας τη διεύθυνση και τον ταχυδρομικό κώδικά του. Τότε ο πωλητής, έχοντας όνομα, διεύθυνση και ταχυδρομικό κώδικα, εγγράφει το θύμα στην εταιρία του και στέλνει αίτηση στον αρχικό πάροχο ζητώντας μεταφορά των υπηρεσιών(χωρίς φυσικά το θύμα να γνωρίζει κάτι). Μόλις η μεταφορά έχει πραγματοποιηθεί, το θύμα λαμβάνει δύο γράμματα. Ένα από τον αρχικό πάροχο που τον ενημερώνει ότι η συνεργασία τους λήγει μια δεδομένη ημερομηνία και ένα από το slammer που τον ενημερώνει πότε ενεργοποιείται ο νέος του λογαριασμός. Ακόμα, ο slammer δίνει τη δυνατότητα στο θύμα να ακυρώσει τη μεταφορά μέσα σε δέκα μέρες. Αν δεν γίνει ακύρωση στο διάστημα αυτό, η μεταφορά πραγματοποιείται αυτόματα και ο slammer ξεκινά να στέλνει τους δικούς του λογαριασμούς ή να χρεώνει τον τραπεζικό λογαριασμό του πελάτη, αν αυτός του έχει δώσει τις κατάλληλες πληροφορίες. Αφού δίνεται η δυνατότητα στο θύμα να ακυρώσει τη μεταφορά, η όλη διαδικασία είναι νόμιμη.

Σε πολλές περιπτώσεις, οι πωλητές αυτοί δουλεύουν για πρακτορεία στα οποία οι εταιρίες έχουν αναθέσει τη συσσώρευση πελατείας. Μπορεί να παριστάνουν και υπαλλήλους του παρόχου του θύματος, για να αποσπάσουν τις πληροφορίες που χρειάζονται. Ακόμα, μπορεί να δοκιμάσουν να πουλήσουν στον πελάτη νέες υπηρεσίες και στα ψιλά γράμματα να περιλαμβάνεται η αλλαγή παρόχου.

[23] http://www.thisismoney.co.uk/news/article.html?in_article_id=399990&in_page_id=2

4.2 Απάτες εναντίον των χρηστών από τρίτους

4.2.2 Αυτόματοι dialers

Οι αυτόματοι dialers[24] είναι ηλεκτρονικές συσκευές που μπορούν να καλέσουν τηλεφωνικούς αριθμούς και χρησιμοποιούνται συνήθως για κακόβουλες ενέργειες. Όταν η πλευρά που καλούν απαντήσει, αναπαράγουν κάποιο φωνητικό μήνυμα ή στέλνουν ψηφιακά δεδομένα (πχ SMS σε κινητά τηλέφωνα).

Οι αυτόματοι dialers έχουν τη δυνατότητα να ξεχωρίζουν τους ανθρώπους από τους αυτόματους τηλεφωνητές. Αυτό το πετυχαίνουν με κάποιο αλγόριθμο ανάλυσης φωνής που περιέχουν. Οποιοσδήποτε υπολογιστής μπορεί να μετατραπεί σε αυτόματο dialer με τη χρήση τηλεφωνικού πίνακα ή μόντεμ σε συνεργασία με το κατάλληλο λογισμικό. Υπάρχουν και οι λεγόμενοι έξυπνοι autodialers που μπορούν να αποθηκεύουν και να αναγνωρίζουν φωνή, καθώς και να μετατρέπουν κείμενο σε ομιλία. Τέλος, υπάρχουν και ημιαυτόματοι dialers στους οποίους κάθε ενέργεια που γίνεται ξεκινάει με ανθρώπινη παρέμβαση. Οι τελευταίοι χρησιμοποιούνται κυρίως στο telemarketing.

Βασική χρήση των autodialers είναι το λεγόμενο "Wangiri"[25] που προέρχεται από την Ιαπωνία. Στην απάτη αυτή, ένας υπολογιστής με μόντεμ, που λειτουργεί ως αυτόματος dialer, καλεί τυχαία εκατοντάδες αριθμούς κινητών τηλεφώνων και διακόπτει αμέσως την κλήση, με αποτέλεσμα να φαίνεται σαν αναπάντητη. Ο ιδιοκτήτης του τηλεφώνου, όντας ανυποψίαστος, καλεί τον αριθμό που βλέπει. Το νούμερο αυτό στην καλύτερη περίπτωση περιέχει διαφημιστικά μηνύματα, στην χειρότερη αντιστοιχεί σε γραμμές υψηλής χρέωσης.

Οι dialers υπάρχουν και σε μορφή software. Είναι προγράμματα που περιέχουν κακόβουλο κώδικα και εγκαθίστανται στον υπολογιστή χωρίς να το γνωρίζει ο χρήστης. Προκαλούν διακοπή της σύνδεσης του υπολογιστή από τον επίσημο πάροχο και πραγματοποιούν κλήση σε αριθμό υψηλής χρέωσης, συνήθως στο εξωτερικό. Οι πρώτοι dialers χρησιμοποιούσαν αριθμούς στη Μολδαβία.

4.2.3 Απάτη με τηλεφωνικές πωλήσεις

Η απάτη με τηλεφωνικές πωλήσεις, είναι η πιο συχνή μορφή απάτης και χρησιμοποιείται όχι μόνο για να αποσπάσουν οι απατεώνες χρήματα, αλλά και για να διαπράξουν κλοπή ταυτότητας. Πιθανόν να μην υπάρχει συνδρομητής εναντίον του οποίου να μην έχει επιχειρηθεί έστω και μια φορά τέτοιος τύπος απάτης. Ο όρος "τηλεφωνικές πωλήσεις", δεν σημαίνει απαραίτητα προσφορά εικονικών προϊόντων, αλλά καλύπτει ένα ευρύτατο φάσμα καλοστημένων τηλεφωνικών παγίδων εναντίον ανυποψίαστων καταναλωτών. Πολύ συχνά, στόχος γίνονται άνθρωποι μεγαλύτερης ηλικίας με προβλήματα υγείας ή μικρές και μεσαίες επιχειρήσεις. Ουσιαστικά, η απάτη τηλεφωνικών πωλήσεων έχει γίνει συνώνυμη της ίδιας της τηλεφωνικής απάτης. Για το λόγο αυτό, θα αφιερωθεί ολόκληρο το επόμενο κεφάλαιο στην ανάλυσή της.

---

[24] http://en.wikipedia.org/wiki/Autodialer
[25] http://en.wikipedia.org/wiki/Wangiri

4.2.4 Απάτη με τηλεφωνικές κάρτες

Οι τηλεφωνικές κάρτες είναι επίσης ευάλωτες στην κακή χρήση. Πάνω τους αναγράφεται κάποιο νούμερο ή κωδικός, τον οποίο πληκτρολογεί ο κάτοχός τους για να χρεώσει τις κλήσεις του στην κάρτα. Αν ο κωδικός πέσει στα χέρια κάποιου απατεώνα, μπορεί να κάνει κατάχρηση της κάρτας με το να πραγματοποιεί προσωπικά τηλεφωνήματα ή ακόμα και να πουλήσει τον κωδικό.

4.2.5 Απάτη από χώρες τρίτου κόσμου

Οι απάτες με το πρόθεμα 809[26], πλήττουν κυρίως τους κατοίκους των ΗΠΑ και του Καναδά. Οι απατεώνες προσπαθούν με δόλιους τρόπους να πείσουν τους συνδρομητές ότι πρέπει να καλέσουν έναν αριθμό, ο οποίος φυσικά είναι υψηλής χρέωσης. Ο κωδικός 809 δουλεύει καλύτερα απ' όλους γιατί πολλοί τον συγχέουν με τον κωδικό 800 (που αντιστοιχεί σε κλήσεις χωρίς χρέωση), αλλά χρησιμοποιούνται και άλλοι πέραν αυτού. Φυσικά, δεν σημαίνει ότι ένα νούμερο με κωδικό περιοχής 809 εμπλέκεται απαραίτητα σε απάτη. Τα περισσότερα τέτοια νούμερα ανήκουν σε νόμιμους συνδρομητές των χωρών που καλύπτει αυτός ο κωδικός.

Αυτή η πλεκτάνη, στοχεύει τους ανθρώπους που δεν είναι εξοικειωμένοι με την πολυπλοκότητα του τηλεφωνικού συστήματος (την πλειοψηφία των ανθρώπων δηλαδή). Οι κάτοικοι των ΗΠΑ και του Καναδά, για να τηλεφωνήσουν σε κάποιον που βρίσκεται στο εξωτερικό, καλούν έναν αριθμό με διαφορετική μορφή από αυτό που έχουν συνηθίσει (xxx-xxx-xxxx). Μερικές χώρες όμως (όπως η Δομινικανή Δημοκρατία και οι Μπαχάμες), έχουν κωδικούς περιοχής και νούμερα όμοια με αυτά της βόρειας Αμερικής.

Οι απατεώνες δρουν κυρίως στις παραπάνω χώρες. Πρώτα αφήνουν μηνύματα στους τηλεφωνητές των υποψήφιων θυμάτων τους. Τους λένε είτε ότι έχουν κερδίσει κάποιο βραβείο ή ότι ένα μέλος της οικογένειάς τους έχει αρρωστήσει/τραυματιστεί σοβαρά. Ακόμα, μπορεί να ισχυρίζονται ότι προσφέρουν εργασία ή να εμφανίζονται ως υπάλληλοι εισπρακτικής εταιρίας. Μετά τη δικαιολογία, ζητούν από το θύμα να καλέσει ένα αριθμό για να μάθει επιπλέον πληροφορίες. Αν το θύμα καλέσει τον αριθμό που του υποδεικνύουν, απαντάει ένας αυτόματος τηλεφωνητής με ένα μακροσκελές ηχογραφημένο μήνυμα ή σε πολλές περιπτώσεις και κάποιος άνθρωπος που συμμετέχει στην απάτη. Ο σκοπός είναι να κρατήσουν το θύμα όσο περισσότερο μπορούν στο τηλέφωνο και οι χρέωση να παίρνει τη μορφή χιονοστιβάδας. Στη συνέχεια, η τηλεφωνική εταιρία του εξωτερικού που χρησιμοποιούν οι απατεώνες χρεώνει το θύμα μέσω της δικής του εταιρίας. Τέλος, ο διεφθαρμένος αυτός πάροχος μοιράζεται τα κέρδη με τους απατεώνες. Σύμφωνα με τη νομοθεσία των ΗΠΑ, αν κάποιος συνδρομητής καλεί μια γραμμή υψηλής χρέωσης εντός της χώρας, η τηλεφωνική εταιρία είναι υποχρεωμένη να τον ενημερώνει για τη χρέωση στην αρχή της κλήσης. Επειδή οι διεφθαρμένες αυτές εταιρίες δραστηριοποιούνται στο εξωτερικό, δεν υπόκεινται στη συγκεκριμένη νομοθεσία.

[26] http://www.snopes.com/fraud/telephone/809.asp

Υπάρχουν πολλές λανθασμένες πληροφορίες στο διαδίκτυο, που μιλούν για χιλιάδες δολάρια χρεώσεων ανά λεπτό. Στην πραγματικότητα, το οικονομικό αντίκτυπο της απάτης δεν είναι ιδιαίτερα μεγάλο. Οι συνήθεις χρεώσεις είναι 25-100 δολάρια ανά λεπτό. Στις περισσότερες περιπτώσεις, οι χρεώσεις αυτές μπορούν να αφαιρεθούν από το λογαριασμό του θύματος αν επικοινωνήσει με τον τοπικό του πάροχο. Γενικά, η απάτη με το πρόθεμα 809 είναι σπάνια. Καλό βέβαια θα ήταν, αν κάποιος δει ένα άγνωστο αριθμό με το πρόθεμα αυτό, να μην τον καλέσει, αλλά να τον αγνοήσει.

4.2.6 Τροποποίηση ταυτότητας καλούντος

Είναι δυνατό κάποιος που πραγματοποιεί μια κλήση να αλλάξει τον μεταδιδόμενο αριθμό[27], με αποτέλεσμα στη οθόνη του καλουμένου να εμφανίζεται κάποιος διαφορετικός και όχι ο πραγματικός. Κάτι τέτοιο μπορεί να γίνει τόσο σε σταθερά, όσο και σε κινητά τηλέφωνα και δε συνιστά απαραίτητα απάτη.

Η τροποποίηση ταυτότητας καλούντος, υπάρχει από την αρχή λειτουργίας της υπηρεσίας (δέκα χρόνια περίπου). Η ανάγκη για την τροποποίηση αυτή γεννήθηκε από τις επιχειρήσεις που χρησιμοποιούσαν πολλές τηλεφωνικές γραμμές και κάθε μία είχε ξεχωριστό νούμερο. Οι επιχειρήσεις ήθελαν όταν καλούν κάποιον να εμφανίζεται ένα νούμερο για όλες τις γραμμές.

Σύντομα, η δυνατότητα αυτή έπεσε στην αντίληψη των ιδιωτικών αστυνομικών. Η αλλαγή του αριθμού που εμφανιζόταν στις εξερχόμενες κλήσεις τους, τους εξασφάλιζε ότι το πραγματικό τους νούμερο θα παρέμενε απόρρητο και ότι θα προστατευόταν η ανωνυμία τους. Η τροποποίηση του αριθμού, εξυπηρετούσε περισσότερο από την απόκρυψη γιατί η τελευταία δεν δούλευε πάντα. Οι αριθμοί χωρίς χρέωση (800-) μπορούσαν να δουν ποιός τους καλεί, ακόμα και αν χρησιμοποιούσε απόκρυψη.

Φυσικά, οι σύγχρονοι phreaks δεν θα μπορούσαν να μην ασχοληθούν με το θέμα. Κατασκεύασαν τα πορτοκαλί κουτιά, τα οποία μπορούσαν να αλλάξουν την ταυτότητα καλούντος. Αυτά ήταν συνήθως εξειδικευμένο λογισμικό υπολογιστή. Δούλευαν στέλνοντας μία σειρά από τόνους στη γραμμή τα πρώτα δευτερόλεπτα της κλήσης εξομοιώνοντας έτσι το σήμα που στέλνει ο πάροχος για να γίνει αναγνώριση του αριθμού. Το πορτοκαλί κουτί όμως δεν είχε μεγάλη επιτυχία γιατί χρειαζόταν σωστό συγχρονισμό για την αποστολή του σήματος και γενικά ήταν αναξιόπιστο.

4.2.7 Κλοπή ταυτότητας

Μερικοί εγκληματίες βασίζονται στο τηλέφωνο για να αποσπάσουν προσωπικές πληροφορίες[28] από τους καταναλωτές. Καλούν το υποψήφιο θύμα τους και ψεύδονται για το ποιοι είναι. Συνήθως παριστάνουν εκπροσώπους εταιριών (με τις οποίες συναλλάσσεται το θύμα) ή κυβερνητικών οργανισμών. Προσπαθούν να πείσουν το θύμα ότι υπάρχει πρόβλημα με τα οικονομικά του θέματα και για να το διορθώσουν χρειάζονται επιβεβαίωση ορισμένων προσωπικών και οικονομικών στοιχείων. Αν πάρουν τα στοιχεία που θέλουν, μπορούν να πραγματοποιήσουν αγορές, να

[27] http://www.calleridspoofing.info/
[28] http://www.ftc.gov/bcp/edu/microsites/phonefraud/identity.shtml

συνάψουν δάνεια, να εκδώσουν πιστωτικές κάρτες, ακόμα και να διαπράξουν εγκλήματα και όλα αυτά σε βάρος του θύματος.

Αυτοί που έχουν εξαπατηθεί, συνήθως το μαθαίνουν όταν πλέον έχει γίνει ζημιά. Για το λόγο αυτό, όταν κάποιος υποπτεύεται ότι τα προσωπικά του στοιχεία έχουν παραβιαστεί, πρέπει να δρα άμεσα ενημερώνοντας τις τράπεζες με τις οποίες συναλλάσσεται καθώς και την αστυνομία. Κάτι άλλο που πρέπει να θυμούνται οι καταναλωτές, είναι ότι δεν πρόκειται κάποιος νόμιμος οικονομικός ή κυβερνητικός οργανισμός να τους ζητήσει ευαίσθητα προσωπικά στοιχεία μέσω τηλεφώνου.

4.2.8 Ψεύτικες απειλές για βόμβα

Ο συγκεκριμένος τρόπος απάτης δεν αποτελεί απαραίτητα καλοσχεδιασμένη πλεκτάνη, αλλά είναι ξεκάθαρος εκβιασμός. Κάποιος απατεώνας τηλεφωνεί σε ένα μεγάλο κτίριο που είναι μόνιμα γεμάτο με κόσμο (συνήθως πολυκατάστημα ή συγκρότημα με γραφεία) και απειλεί πως θα εκραγεί βόμβα[29] αν η διοίκηση του κτιρίου δεν ακολουθήσει τις οδηγίες του. Συνήθως ο επιτήδειος τους προειδοποιεί ότι παρακολουθεί το κτίριο, αν και σύμφωνα με την αστυνομία οι κλήσεις γίνονται πάντα από διαφορετική πολιτεία ή χώρα. Υπάρχουν στοιχεία που καταδεικνύουν ότι οι απατεώνες απέκτησαν σε ορισμένες περιπτώσεις πρόσβαση στο σύστημα παρακολούθησης της εταιρίας, αλλά δεν έχει επιβεβαιωθεί ποτέ. Οι "οδηγίες" που δίνει ο εγκληματίας, δεν είναι τίποτα άλλο από την απαίτηση για αποστολή χρημάτων. Μερικές φορές μάλιστα, ζητούν και άλλα πράγματα άκρως εξευτελιστικά, όπως το να βγάλουν όλοι οι παραβρισκόμενοι στο κτίριο τα ρούχα τους.

Επειδή στη μορφή αυτή απάτης εμπλέκεται απειλή για βόμβα (και κατά συνέπεια κίνδυνος για την ανθρώπινη ζωή), η κινητοποίηση της αστυνομίας είναι άμεση. Ο απατεώνας λόγω της μεγάλης απόστασης στην οποία συνήθως βρίσκεται δεν ανησυχεί για το ενδεχόμενο σύλληψης. Όταν πλέον έχει λάβει τα χρήματα, τότε μόνο οι αρχές και οι απειλούμενοι καταλαβαίνουν ότι επρόκειτο για απάτη.

Σε μια παραλλαγή του παραπάνω, ο εκβιαστής δεν παριστάνει το βομβιστή, αλλά τον επαγγελματία εκτελεστή. Λέει συγκεκριμένα στο θύμα ότι τον έχει προσλάβει κάποιος άνθρωπος του κοντινού του περιβάλλοντος για να τον/την δολοφονήσει. Ο "εκτελεστής" όμως, δηλώνει ότι μπορεί να μην ολοκληρώσει την αποστολή του αν το θύμα του δώσει αρκετά χρήματα. Σε ορισμένες περιπτώσεις μάλιστα, προσφέρεται να σκοτώσει και τον αρχικό εντολέα του. Φυσικά, κάθε τέτοιο τηλεφώνημα συνοδεύεται από προειδοποίηση προς το θύμα να μην επικοινωνήσει με τις αρχές.

4.2.10 Παρακολούθηση τηλεφωνικών συνομιλιών

Η παρακολούθηση τηλεφωνικών συνομιλιών[30] είναι αυτό που δηλώνει το όνομά της. Κάποιος τρίτος, ακούει και (πιθανόν) καταγράφει τις τηλεφωνικές συνομιλίες μεταξύ δύο άλλων προσώπων, χωρίς να γίνεται αντιληπτός. Ανάλογα με το σκοπό της μπορεί να είναι να είναι νόμιμη, οπότε δε συνιστά απαραίτητα απάτη. Χρησιμοποιείται κυρίως από την αστυνομία και τις μυστικές υπηρεσίες για παρακολούθηση υπόπτων

[29] http://en.wikipedia.org/wiki/Advance_fee_fraud
[30] http://en.wikipedia.org/wiki/Telephone_tapping

και τρομοκρατών. Ακόμα, μπορεί να χρησιμοποιηθεί από ιδιωτικούς αστυνομικούς για την παρακολούθηση του στόχου τους (κυρίως "άτακτων" συζύγων) ή από επιχειρηματίες για παρακολούθηση της χρήσης των τηλεφώνων της εταιρίας τους.

Δυστυχώς, δεν παρακολουθούν τα τηλέφωνα μόνο οι εκπρόσωποι του νόμου. Η πρακτική αυτή χρησιμοποιείται και από πολλούς απατεώνες που θέλουν να υποκλέψουν στοιχεία για να εξαπατήσουν τα θύματά τους. Αν κάποιος δίνει προσωπικά του στοιχεία σε κάποιο έμπιστο συνομιλητή και η γραμμή παρακολουθείται, τότε άθελά του δίνει στοιχεία και στους απατεώνες.

Η παρακολούθηση μπορεί να γίνει με διάφορους τρόπους[31]. Απαιτούνται ειδικές συσκευές που κάποιος μπορεί να αγοράσει έτοιμες ή να κατασκευάσει μόνος του χρησιμοποιώντας απλά στοιχεία κυκλωμάτων. Μια διαδεδομένη συσκευή είναι αυτή που παρεμβάλλεται μεταξύ της πρίζας και του τηλεφώνου και διαθέτει έξοδο ήχου προς κάποια συσκευή καταγραφής. Το μειονέκτημά της είναι ότι πρέπει να βρίσκεται κοντά στο τηλέφωνο και πολλές φορές σε εμφανές σημείο και κατά συνέπεια εντοπίζεται εύκολα. Είναι περισσότερο κατάλληλη για ανθρώπους που θέλουν να ηχογραφούν τις δικές τους κλήσεις και όχι να παρακολουθούν άλλους. Για παρακολουθήσεις επαγγελματικού επιπέδου, συνιστάται η χρήση ενός πομπού(στα ελληνικά αποκαλείται "κοριός"). Μια σύγχρονη συσκευή τέτοιου τύπου είναι αρκετά μικρή ώστε να μπορεί να τοποθετηθεί μέσα στο ακουστικό ενός σταθερού τηλεφώνου ή να είναι μεταμφιεσμένη ως duplex splitter αντάπτορας. Μπορεί να εκπέμπει σε συχνότητες FM, UHF ή να χρησιμοποιεί κάρτα SIM. Η συσκευή καταγραφής μπορεί να βρίσκεται δεκάδες μέτρα μακριά, ενώ στις περιπτώσεις που χρησιμοποιείται SIM μπορεί να γίνεται παρακολούθηση ενός τηλεφώνου από οποιοδήποτε μέρος του κόσμου(αρκεί να υπάρχει κάλυψη δικτύου GSM).

4.2.11 Παρακολούθηση συνομιλιών τηλεφώνων GSM

Όπως είναι γνωστό, το GSM είναι ο πιο δημοφιλής τύπος δικτύου κινητής τηλεφωνίας στον κόσμο. Η ασφάλειά του βασίζεται σε διάφορους αλγορίθμους κρυπτογράφησης των μεταφερόμενων δεδομένων. Στην Ευρώπη και τις ΗΠΑ, χρησιμοποιείται ο A5/1 που θεωρείται ο πιο ισχυρός. Στον υπόλοιπο κόσμο χρησιμοποιείται ο A5/2 που είναι λιγότερο αποτελεσματικός. Έχουν βρεθεί σοβαρές αδυναμίες και στους δύο αλγορίθμους. Ειδικά ο A5/2 αποκρυπτογραφείται πολύ εύκολα και γρήγορα.

Τον Δεκέμβριο του 2009, ένας μηχανικός πληροφορικής ονόματι Karsten Nohl δήλωσε ότι η ομάδα του κατάφερε να αποκρυπτογραφήσει και τον αλγόριθμο A5/1[32]. Ο συγκεκριμένος αλγόριθμος χρησιμοποιείται από το 1988. Το αποτέλεσμα της έρευνάς του, που είναι ένα code book μεγέθους 2 terabyte, κυκλοφορεί μέσω του πρωτοκόλλου ανταλλαγής αρχείων bittorrent. Το code book αυτό περιέχει όλους τους πιθανούς αλγορίθμους που μπορεί να χρησιμοποιηθούν για την αποκρυπτογράφηση των κλήσεων στο GSM δίκτυο. Ο Nohl ισχυρίστηκε ότι το λογισμικό που χρησιμοποίησε είναι στο σύνολό του ανοικτού κώδικα και κατά συνέπεια διατίθεται ελεύθερα στο διαδίκτυο. Αυτό σημαίνει ότι κάθε ενδιαφερόμενος μπορεί να

[31] http://www.spy.th.com/audio.html#!au046
[32] http://www.blackberrycool.com/2009/12/29/gsm-algorithm-cracked-leaving-voice-calls-unsecure/

κατεβάσει το λογισμικό και το code book και να αποκρυπτογραφήσει τον αλγόριθμο του GSM.

Μετά την ανακοίνωση εξαπλώθηκε κύμα ανησυχίας στους χρήστες του GSM που ενημερώθηκαν για το γεγονός. Στην πραγματικότητα όμως τα πράγματα δεν είναι τόσο σοβαρά. Αυτό που κατάφερε η ομάδα του Nohl είναι να αποκρυπτογραφήσει τον A5/1. Αυτό από μόνο του δεν σημαίνει τίποτα. Για να ακούσει κάποιος τις συνομιλίες άλλων χρειάζεται να κάνει πολύ περισσότερα. Πρέπει πρώτα απ' όλα να συλλάβει το σήμα για να το αποκωδικοποιήσει και πάρει τα κρυπτογραφημένα δεδομένα. Στη συνέχεια θα ακολουθήσει η αποκρυπτογράφηση. Τέλος, χρειάζονται επιπλέον ενέργειες για να μετατραπούν τα δεδομένα σε φωνή και να ακούσει ο ενδιαφερόμενος την αρχική συνομιλία. Για την πραγματοποίηση των παραπάνω χρειάζεται ειδικός εξοπλισμός και υπηρεσίες που χρειάζονται αδειοδότηση και δεν μπορούν εύκολα να πέσουν στα χέρια του απλού καθημερινού ανθρώπου. Ακόμα και αν μπορούσαν, το κόστος αγοράς θα ήταν απαγορευτικό.

Οι περισσότερες εταιρίες κινητής τηλεφωνίας παραδέχονται ότι ο A5/1 είναι ξεπερασμένος. Μερικές προτίθενται να τον αντικαταστήσουν με τον A5/3(γνωστό και ως Kasumi) που αποτελείται από 128 bit έναντι 64 του A5/1 και προς το παρόν χρησιμοποιείται για την ασφάλεια των δικτύων τρίτης γενιάς(3G). Το 2010 αναφέρθηκε σε διάφορους ιστότοπους ότι μια ομάδα από ειδικούς στην κρυπτογράφηση δεδομένων κατάφερε να αποκρυπτογραφήσει και τον A5/3. Οι ειδικοί όμως υποστηρίζουν ότι αυτό δε σημαίνει κάτι και ο αλγόριθμος είναι αρκετά ασφαλής για να συνεχίσει να χρησιμοποιείται. Δυστυχώς οι περισσότερες εταιρίες κινητής τηλεφωνίας δεν κάνουν βήματα προς την αντικατάσταση του απαρχαιωμένου A5/1, κυρίως λόγω του υψηλού κόστους μετάβασης από τον ένα αλγόριθμο στον άλλο.

4.2.12 Ψεύτικα εγγόνια

Στη συγκεκριμένη μορφή απάτης, οι απατεώνες παριστάνουν τα εγγόνια[33] των θυμάτων και ζητούν χρήματα. Όπως είναι φυσικό, στοχεύει ηλικιωμένους ανθρώπους, οι οποίοι δεν έχουν καθημερινή επαφή με τα εγγόνια τους. Μια τυπική περίπτωση περιγράφεται παρακάτω. Ο απατεώνας τηλεφωνεί και ισχυρίζεται πως είναι εγγονός/εγγονή του θύματος και βρίσκεται σε μπελάδες. Πιο συγκεκριμένα, έχει συλληφθεί για κάποιο ασήμαντο αδίκημα (συνήθως πρόκληση ζημιάς σε σταθμευμένο όχημα) και χρειάζεται άμεσα χρήματα για να πληρώσει την εγγύηση και να αποφυλακιστεί. Σε διαφορετική περίπτωση, θα παραμείνει έγκλειστος για αρκετές μέρες. Πάντα υπόσχεται ότι θα επιστρέψει τα χρήματα. Σε περίπτωση που το θύμα πειστεί, σύντομα θα καλέσει κάποιος που ισχυρίζεται ότι είναι εκπρόσωπος του νόμου και θα δώσει οδηγίες στο θύμα για την πληρωμή (η οποία γίνεται πάντα σε μετρητά με υπηρεσίες μεταφοράς χρημάτων).

Οι ηλικιωμένοι άνθρωποι αποτελούν εύκολα θύματα, αφού είναι από τη φύση τους περισσότερο αφελείς από τους νεότερους. Ακόμα, η αγωνία που έχουν για τα εγγόνια τους, τους κάνει περισσότερο ευάλωτους. Αυτό το φαινόμενο εμφανίζεται, όπως είναι φυσικό στις ΗΠΑ και τον Καναδά, αλλά και στην Ιαπωνία σε μεγάλο βαθμό. Το

[33] http://www.crimes-of-persuasion.com/Crimes/Telemarketing/Outbound/Minor/assistance.htm

οικονομικό αντίκτυπο μπορεί να φτάσει από μερικές εκατοντάδες έως πολλές χιλιάδες δολάρια. Καλό είναι, όταν κάποιος λάβει ένα τέτοιου είδους τηλεφώνημα, να επιβεβαιώνει αν υπάρχει πράγματι πρόβλημα, καλώντας το άτομο που υποτίθεται ότι έχει συλληφθεί. Αν αυτό δεν είναι δυνατό, μπορεί να επικοινωνήσει με άλλους συγγενείς ή την αστυνομία.

Αυτή η μορφή απάτης έχει και άλλες παραλλαγές. Δηλαδή ο απατεώνας μπορεί να παριστάνει τον γιο ή την κόρη του θύματος ή κάποιο άλλο κοντινό συγγενή. Υπάρχει και μια άλλη παραλλαγή που δεν στοχεύει συγγενείς αλλά ανθρώπους του κλήρου. Ο απατεώνας ισχυρίζεται ότι ανήκει στο ποίμνιο της εκκλησίας-στόχου και παρουσιάζεται να έχει ανάγκη από χρήματα αφού (συνήθως) του χάλασε το αυτοκίνητο πηγαίνοντας σε μια κηδεία συγγενικού του προσώπου (ή σε κάποιο άλλο μυστήριο και φυσικά σε άλλη πολιτεία).

4.2.13 Τηλεφωνικές Φάρσες

Η τηλεφωνική φάρσα[34] είναι ίσως η πιο απλή μορφή τηλεφωνικής απάτης. Γίνεται καθαρά για διασκέδαση αυτών που την πραγματοποιούν. Είναι αθώα από τη φύση της, αλλά αν ο φαρσέρ είναι κακόβουλος μπορεί να προκαλέσει μεγάλη αναστάτωση, ακόμα και οικονομική ζημιά στα θύματά του.

Οι τηλεφωνικές φάρσες ξεκίνησαν να γίνονται γνωστές στην Αμερική από τη δεκαετία του 1960. Κωμικοί ηθοποιοί της εποχής, μέσα από ραδιοφωνικές εκπομπές τηλεφωνούσαν σε διασημότητες αλλά και στο ευρύ κοινό παριστάνοντας κάποιους άλλους. Οι φάρσες συνήθως ηχογραφούνταν και κυκλοφορούσαν σε κασέτες. Αργότερα δημιουργήθηκαν και τηλεοπτικές εκπομπές ψυχαγωγικού χαρακτήρα με τέτοια θεματολογία. Μερικά από τα διάσημα θύματα αυτής της απάτης είναι η βασίλισσα της Αγγλίας, ο πρόεδρος της Βενεζουέλας Hugo Chavez και της Κούβας Fidel Castro. Αξίζει να σημειωθεί ότι ο πρόεδρος Castro, εξύβρισε δημοσίως τους ηθοποιούς που του έκαναν τη φάρσα.

Φυσικά, οι τηλεφωνικές φάρσες έγιναν αγαπημένη ασχολία πολλών παιδιών(μικρών και μεγάλων) ανά τον κόσμο. Καλούσαν συγγενείς και φίλους αλλά και αγνώστους από τον τηλεφωνικό κατάλογο. Το φαινόμενο περιορίστηκε από τη δεκαετία του 1990 και μετά, αφού σχεδόν όλοι οι συνδρομητές είχαν πλέον αναγνώριση κλήσεων. Τη σημερινή εποχή αν κάποιος δεν θέλει να αποκαλύψει την ταυτότητά του πρέπει να χρησιμοποιήσει απόκρυψη αριθμού, να καλέσει από δημόσιο τηλέφωνο ή μέσω υπηρεσίας voip ή να τροποποιήσει την ταυτότητα καλούντος.

Σε γενικές γραμμές, οι αθώες τηλεφωνικές φάρσες δεν είναι παράνομες. Όταν όμως κάνει ζημιά σε δημόσια ή ιδιωτικά συμφέροντα τότε υπάρχει αδίκημα. Όταν για παράδειγμα κάποιος αναφέρει ένα ψεύτικο περιστατικό στην αστυνομία ή σε κέντρο άμεσης βοήθειας με μόνο σκοπό να σπαταλήσει το χρόνο των εργαζομένων. Ακόμα αδίκημα υπάρχει όταν γίνονται ψεύτικες απειλές για βόμβα σε μεγάλα δημόσια κτίρια, όπου η αστυνομία είναι υποχρεωμένη να ψάχνει για ώρες μια απειλή που δεν υφίσταται. Η ποινή στις ΗΠΑ για τις περιπτώσεις αυτές μπορεί να φτάσει μέχρι δύο χρόνια φυλάκιση και χρηματικό πρόστιμο, αλλά σπάνια εφαρμόζεται.

---

[34] http://en.wikipedia.org/wiki/Prank_call

Υπάρχει μια κοινότητα που οργανώνει τέτοιου είδους κακόβουλες και παράνομες φάρσες με έδρα τον Καναδά. Το όνομά της είναι Pranknet[35] και ιδρύθηκε το 2000. Θεωρείται υπεύθυνη για 60 περίπου αδικήματα εναντίον ξενοδοχείων και εστιατορίων fast food. Τα μέλη τηλεφωνούν παριστάνοντας άτομα που έχουν εξουσία (πχ υψηλόβαθμα στελέχη των επιχειρήσεων) και προσπαθούν να πείσουν τους εργαζομένους να κάνουν διάφορα παράδοξα πράγματα. Στις πιο απλές περιπτώσεις να χτυπήσουν συναγερμό φωτιάς ή σε πιο σοβαρές να επιτεθούν σε συναδέλφους. Βασικό στοιχείο είναι η ανωνυμία των μελών της. Χρησιμοποιούν την υπηρεσία skype η οποία δεν απαιτεί κάποιο αποδεικτικό ταυτότητας. Μεταξύ τους συζητούν με την υπηρεσία Beyluxe messenger που έχει έδρα έξω από τη βόρεια Αμερική. Το 2009, αποκαλύφθηκε η ταυτότητα του αρχηγού και μερικών ιδρυτικών μελών μετά από έρευνα των υπευθύνων της ιστοσελίδας Smoking Guns. Τα ονόματα, ψευδώνυμα και ηλικίες (το 2009) ακολουθούν: Tariq Malik("Dex", 25), William Marquis("Hempster", 51), James Tyler Markle("Prankster", 19), Shawn Powell("Slipknotpsycho", 24), LeeAnn Jordan(" Veruca", 28). Στη συνέχεια τα ονόματα παραδόθηκαν στο FBI και μερικά από τα μέλη συνελήφθησαν. Σήμερα, υπολογίζεται ότι η κοινότητα έχει περίπου 250 μέλη.

4.2.14 Επίθεση στα PBX εταιριών

Μια μεγάλη απειλή για τις επιχειρήσεις είναι η εκμετάλλευση από τους απατεώνες του PBX που διαθέτουν. PBX[36] είναι τα αρχικά των λέξεων Private Branch Exchange (ιδιωτικό κέντρο), δηλαδή ιδιωτικό τηλεφωνικό σύστημα που χρησιμοποιείται μέσα σε μια εταιρεία. Οι χρήστες του τηλεφωνικού συστήματος PBX τηλεφωνούν εκτός εταιρείας με κοινή χρήση μιας σειράς εξωτερικών γραμμών. Το PBX συνδέει τα εσωτερικά τηλέφωνα μέσα σε μια επιχείρηση μεταξύ τους αλλά και με το δημόσιο τηλεφωνικό δίκτυο μεταγωγής (public switched telephone network (PSTN)). Μία από τις τελευταίες τάσεις στην εξέλιξη των τηλεφωνικών συστημάτων PBX είναι το VoIP PBX, επίσης γνωστό ως IP PBX, που χρησιμοποιεί το πρωτόκολλο Ίντερνετ για τη μετάδοση κλήσεων.

Αν κάποιος απατεώνας[37] αποκτήσει πρόσβαση στο PBX μπορεί να πραγματοποιήσει κλήσεις οπουδήποτε θέλει σε βάρος της εταιρίας. Βάσει νόμου κάθε οργανισμός είναι υποχρεωμένος να λαμβάνει μέτρα για την προστασία του τηλεφωνικού του κέντρου. Κατά συνέπεια τα χρέη προς τον πάροχο πρέπει να πληρωθούν από τον εξαπατημένο οργανισμό και η διαγραφή τους αποκλείεται σε κάθε περίπτωση. Οι τηλεπικοινωνιακές εταιρίες δεν έχουν πρόσβαση στο PBX κάθε οργανισμού και κατά συνέπεια δεν μπορούν να σταματήσουν τις επιθέσεις. Το καλύτερο που έχουν να κάνουν οι οργανισμοί είναι να προστατέψουν όλα τα αδύναμα σημεία του τηλεφωνικού τους συστήματος και να εκπαιδεύσουν κατάλληλα το προσωπικό. Μικρότερες εταιρίες χρειάζεται να ανησυχούν περισσότερο γιατί η οικονομική ζημιά αυτού του τύπου απάτης είναι συνήθως μεγάλη.

[35] http://en.wikipedia.org/wiki/Pranknet
[36] http://www.3cx.gr/voip-sip/tilefoniko-systima-pbx.php
[37] http://www.tsips.com/PBX_Fraud_Facts.htm

Οι απατεώνες αποκτούν πρόσβαση συνήθως απομακρυσμένα χρησιμοποιώντας αυτόματους dialers σε συνδυασμό με λογισμικό ανίχνευσης password. Προσπαθούν να αποκτήσουν πρόσβαση στη θύρα συντήρησης του PBX μέσω της οποίας στη συνέχεια ελέγχουν ουσιαστικά όλο το σύστημα. Κάνουν τις κατάλληλες αλλαγές στο λογισμικό ώστε να μπορουν να πραγματοποιούν παράνομες κλήσεις. Πολλές φορές αποκτούν πρόσβαση με τη βοήθεια ενός διεφθαρμένου υπαλλήλου. Στη συνέχεια πουλάνε την υπηρεσία αυτή και σε άλλους. Οι hackers είναι μέλη διεθνών κυκλωμάτων και πολύ σπάνια εντοπίζονται και συλλαμβάνονται. Το οικονομικό αντίκτυπο σε μια τυπική περίπτωση μπορεί να φτάσει τα $80000.

4.3 Απάτες εναντίον εταιριών

4.3.1 Απάτη διαμεσολάβησης-από μία εταιρία εναντίον άλλης

Υπάρχουν περιπτώσεις που μια κλήση, καθώς προωθείται από την προέλευση προς τον προορισμό της, χρειάζεται να περάσει από το δίκτυο κάποιου δεύτερου παρόχου. Όποτε συμβαίνει κάτι τέτοιο, ο πάροχος του πελάτη, είναι υποχρεωμένος να πληρώσει κάποιο ποσό στον δεύτερο πάροχο που "φιλοξενεί την κλήση. Όταν λοιπόν το δεύτερο δίκτυο ζητήσει περισσότερα χρήματα από όσα πρέπει κανονικά να πάρει, τότε υπάρχει απάτη διαμεσολάβησης από την πλευρά του δεύτερου παρόχου.

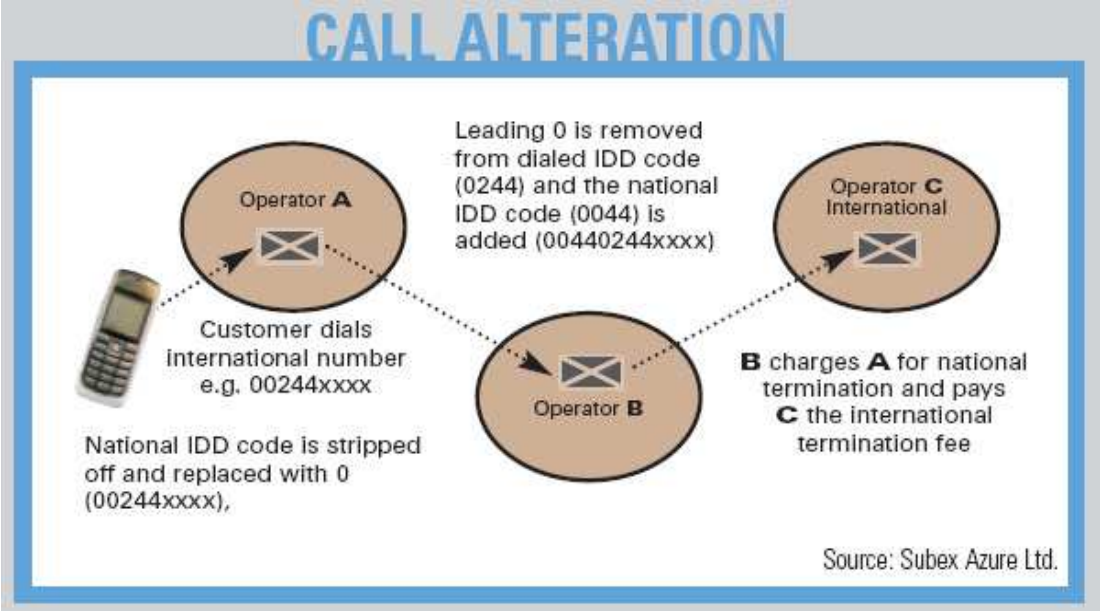
Βέβαια, μπορεί να γίνει και το αντίθετο, δηλαδή ο πάροχος που εξυπηρετεί την προέλευση να εξαπατήσει αυτόν που εξυπηρετεί τον προορισμό. Η χρέωση για την "φιλοξενία" της κλήσης από ένα δίκτυο υπολογίζεται βάσει του ποσοστού της συνολικής απόστασης που καλύπτει ο δεύτερος πάροχος. Ο πρώτος πάροχος λοιπόν, που εξυπηρετεί την προέλευση, μπορεί να αλλάξει το νούμερο της προέλευσης με ένα άλλο που εμφανίζεται πιο απομακρυσμένο. Έτσι φαίνεται ότι ο δεύτερος πάροχος εξυπηρετεί μικρότερο ποσοστό απόστασης και κατά συνέπεια, ο πρώτος του χρωστάει λιγότερα χρήματα.

Η απάτη διαμεσολάβησης είναι αρκετά δύσκολο να εντοπιστεί[38]. Αυτό συμβαίνει γιατί υπάρχουν εκατοντάδες πάροχοι που εξυπηρετούν ο ένας τον άλλο κάτω από διαφορετικά φορολογικά καθεστώτα και τιμολογιακές πολιτικές. Κάθε εταιρία συνάπτει συμβόλαια διαμεσολάβησης με εκατοντάδες άλλες και δεν μπορεί να εντοπίσει εύκολα ποιος τιμά τη συμφωνία και ποιος όχι. Για να το πετύχει αυτό, θα πρέπει να έχει επενδύσει πολλά χρήματα σε κατάλληλο εξοπλισμό και να συνάπτει κάθε τέτοια συμφωνία παρουσία νομικών προσώπων. Σε ορισμένες περιπτώσεις, ένας πάροχος είναι δυνατόν να χάσει εκατομμύρια λόγω της απάτης διαμεσολάβησης.

Στην παρακάτω εικόνα, φαίνεται ένα τυπικό σχήμα τέτοιας απάτης. Ο πελάτης του Α καλεί κάποιο πελάτη του C που βρίσκεται σε άλλη χώρα. Ο Β θα μεσολαβήσει για να πραγματοποιηθεί η κλήση. Θα κάνει όμως και κάτι άλλο: θα αλλάξει το νούμερο, βάζοντας μπροστά το πρόθεμα της χώρας προορισμού. Έτσι, ο C ενώ λαμβάνει μια διεθνή κλήση, θα βλέπει ότι αυτή προέρχεται από τη χώρα του. Το αποτέλεσμα είναι

[38] http://www.teralight.com/fraud.php

ότι Β θα πάρει από τον Α τα χρήματα που του αναλογούν, αλλά θα πληρώσει στο C λιγότερα από αυτά που πρέπει.



Εικόνα 11: Παράδειγμα απάτης διαμεσολάβησης

4.3.2 Phreaking

Το phreaking δεν χρειάζεται συστάσεις, αφού γι' αυτό έγινε εκτενέστατη αναφορά στο δεύτερο κεφάλαιο. Είναι ο πρόγονος του computer hacking και πλέον είναι ξεπερασμένο, αφού το τηλεφωνικό δίκτυο στο σύνολο του σχεδόν βασίζεται στη χρήση υπολογιστών.

Μια πιο σύγχρονη εκδοχή του phreaking είναι ο επαναπρογραμματισμός των switch. Στην περίπτωση αυτή, ο hacker ανοίγει μια "πίσω πόρτα" και αποκτά πρόσβαση στο δίκτυο της εταιρίας. Από εκεί και πέρα, μπορεί να πραγματοποιεί δωρεάν τηλεφωνήματα, ακόμα και να πουλήσει τη δυνατότητα αυτή σε άλλους.

4.3.3 Κλωνοποίηση κινητών τηλεφώνων

Κλωνοποίηση[39] είναι η μεταφορά/αντιγραφή της ταυτότητας ενός κινητού τηλεφώνου με σκοπό την πραγματοποίηση παράνομων κλήσεων με χρέωση κάποιου συνδρομητή. Στα δίκτυα CDMA, η ταυτοποίηση κάθε χρήστη γίνεται μέσω του ηλεκτρονικού σειριακού αριθμού (ESN) και του αριθμού κλήσης (MIN) που υπάρχουν αποθηκευμένα σε κάθε συσκευή κινητού τηλεφώνου. Ο απατεώνας απλά αλλάζει τα ESN και MIN στο τηλέφωνό του με αυτά που αντιστοιχούν σε κάποιο νόμιμο συνδρομητή. Για να βρει τα νούμερα αυτά, χρειάζεται είτε να αποκτήσει πρόσβαση στη συσκευή του θύματος, είτε να εισβάλει στη βάση δεδομένων μιας τηλεφωνικής εταιρίας.

[39] http://en.wikipedia.org/wiki/Cloning_(telephony)

Η κλωνοποίηση είναι ιδιαίτερα εύκολο να πραγματοποιηθεί και δεν απαιτεί τεχνικές γνώσεις. Χρειάζονται δύο συσκευές, μία που διαθέτει σύνδεση και μία χωρίς. Δεν πρέπει απαραίτητα να είναι το ίδιο μοντέλο. Όλα τα κινητά τηλέφωνα, διαθέτουν κάποιο κρυφό μενού με εξειδικευμένες ρυθμίσεις και διαγνωστικά, που γίνεται προσβάσιμο με την πληκτρολόγηση ενός κωδικού στην οθόνη αναμονής. Το πρώτο που πρέπει να κάνει ο ενδιαφερόμενος, είναι να μπει στο κρυφό μενού της συσκευής που διαθέτει σύνδεση, να βρει το ESN και να το σημειώσει κάπου. Στη συνέχεια, μπαίνει στο ίδιο μενού της συσκευής που δεν διαθέτει σύνδεση και αλλάζει το ESN και τον αριθμό τηλεφώνου, ώστε να είναι ίδια με αυτά της πρώτης. Τώρα υπάρχουν δύο πλήρως λειτουργικά τηλέφωνα που το ένα είναι αντίγραφο του άλλου. Να σημειωθεί ότι οι κωδικοί πρόσβασης στο κρυφό μενού είναι διαφορετικοί για κάθε μάρκα κινητού τηλεφώνου και τους βρίσκει κάποιος εύκολα με τη βοήθεια μιας μηχανής αναζήτησης.

Εικόνα 12:Τηλέφωνα που μπορούν να κλωνοποιηθούν

Στα δίκτυα GSM η παραπάνω μέθοδος σπάνια εφαρμόζεται. Μπορεί να κλωνοποιηθεί η κάρτα SIM, χωρίς να αλλαχθούν τα στοιχεία της συσκευής, αφού στο GSM δεν υπάρχουν αριθμοί ESN και MIN παρά μόνο το IMEI.

Ο μόνος αποτελεσματικός τρόπος για να εντοπιστούν[40] τα κλωνοποιημένα τηλέφωνα είναι η χρήση ειδικού λογισμικού από τον πάροχο. Το λογισμικό συλλέγει στοιχεία για τη "συμπεριφορά"(τη χρήση δηλαδή του τηλεφωνικού δικτύου) κάθε νόμιμου χρήστη. Τα στοιχεία αυτά αφορούν κυρίως τον αριθμό, την διάρκεια και τους παραλήπτες των κλήσεων που πραγματοποιεί ο συνδρομητής. Έτσι για κάθε χρήστη δημιουργείται ένα προφίλ το οποίο συγκρίνεται με την καθημερινή του δραστηριότητα. Αν εντοπιστούν σημαντικές αποκλίσεις το σύστημα θα ειδοποιήσει τους τεχνικούς ασφαλείας της εταιρίας που θα ερευνήσουν για παράνομη δραστηριότητα. Μια άλλη μέθοδος είναι η χρήση κανόνων συμπεριφοράς από το λογισμικό με βάση κάποια πρωτότυπα μοντέλα. Έτσι η χρήση των υπηρεσιών του συνδρομητή συγκρίνεται με γνωστές παράνομες συμπεριφορές. Το μειονέκτημα των παραπάνω μεθόδων είναι ότι δεν ανακαλύπτουν την απάτη, απλά ειδοποιούν για τυχόν ύποπτες δραστηριότητες που δεν είναι απαραίτητα παράνομες.

[40] http://icta05.teithe.gr/papers/69.pdf

4.3.4 Απάτη με δημόσια τηλέφωνα

Οι απατεώνες, προσπαθούσαν πάντα να εκμεταλλευτούν τα δημόσια τηλέφωνα[41] που λειτουργούν με κέρματα. Στο δεύτερο κεφάλαιο της παρούσας εργασίας, έγινε αναφορά στα κόκκινα κουτιά που χρησιμοποιούσαν οι phreaks για να αναπαράγουν τον ήχο των κερμάτων. Η μέθοδος αυτή δουλεύει ακόμα και σήμερα σε μερικά μέρη του κόσμου όπου υπάρχουν τέτοια τηλέφωνα.

Στην Αυστραλία, κάποιος ανακάλυψε μια άλλη μέθοδο να ξεγελάει τα δημόσια τηλέφωνα με ένα απλό καλαμάκι και έχει ανεβάσει τις οδηγίες σε κάποιο forum. Σύμφωνα με τον τύπο αυτό, η καλύτερη μέθοδος είναι να χρησιμοποιηθούν καλαμάκια από τα εστιατόρια McDonalds στα τηλέφωνα της εταιρίας Telstra. Ο καλών πρέπει πρώτα απ' όλα να διπλώσει το καλαμάκι. Στη συνέχεια το τοποθετεί στην υποδοχή των νομισμάτων και το σπρώχνει μέσα περίπου 5 πόντους, όπου θα πρέπει να ακουμπήσει κάποιο διακόπτη αν περιστρέψει ελαφρώς το καλαμάκι προς τα αριστερά. Σπρώχνοντας το διακόπτη 1-2 πόντους προς τα μέσα και ταυτόχρονα καλώντας τον επιθυμητό αριθμό, το τηλέφωνο "νομίζει" ότι έχουν μπει κέρματα. Αν η άλλη πλευρά απαντήσει, η θυρίδα θα κάνει ένα θόρυβο που δείχνει ότι προσπαθεί να ρίξει τα κέρματα μέσα στην αποθήκη. Η κλήση πραγματοποιήθηκε με επιτυχία και προπάντων δωρεάν.

Η μέθοδος αυτή είναι πιθανό να δουλεύει και σε δημόσια τηλέφωνα στον υπόλοιπο κόσμο. Ο εμπνευστής της μεθόδου αυτής δεν γνωρίζει τεχνικές λεπτομέρειες και τονίζει ότι χρειάζεται να προσπαθήσει κάποιος μερικές φορές μέχρι να το καταφέρει.

4.3.5 Απάτη με πλαστές συνδρομές

Πλαστή συνδρομή[42] είναι μια μορφή απάτης που συμβαίνει κυρίως στα κινητά τηλέφωνα. Ένας νέος συνδρομητής, υπογράφει ένα συμβόλαιο τηλεφωνίας χρησιμοποιώντας πλαστή ή κλεμμένη ταυτότητα. Οι εταιρίες συνήθως δίνουν μια περίοδο χάριτος 1-3 μηνών, πριν ο λογαριασμός ακυρωθεί. Στο διάστημα αυτό, οι απατεώνες προλαβαίνουν να πραγματοποιήσουν κλήσεις αξίας χιλιάδων ευρώ(ή δολαρίων αν μιλάμε για τις ΗΠΑ).

Σε περίπτωση που ο απατεώνας έχει χρησιμοποιήσει κλεμμένα στοιχεία, είναι δύσκολο να διαφοροποιηθεί η απάτη από την ασυνέπεια στην πληρωμή. Εκτιμάται, ότι πάνω από 30% του χρέους των ασυνεπών συνδρομητών, είναι στην πραγματικότητα πλαστές συνδρομές.

Έχουν προταθεί διάφορες λύσεις για την αντιμετώπιση του προβλήματος, όπως η παρακολούθηση της μεθόδου που χρησιμοποιούν οι απατεώνες, ή η σύγκριση κάθε μελλοντικού συνδρομητή με γνωστούς εγκληματίες. Δυστυχώς, ότι και να γίνει, οι

---

41 http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=481&mode=thread&order=0&thold=0

42 http://identityresolutiondaily.com/727/attacking-subscription-fraud-with-identity-resolution/

απατεώνες είναι πάντα ένα βήμα μπροστά και προσαρμόζονται σε κάθε βελτίωση του συστήματος αντιμετώπισής τους.
Η απάτη roaming[43] είναι προέκταση της πλαστής συνδρομής. Όπως είναι γνωστό, κατά το roaming ο συνδρομητής χρησιμοποιεί το δίκτυο μιας διαφορετικής εταιρίας σε σημείο που η δική του δεν έχει κάλυψη. Ο συνδρομητής δεν πληρώνει άμεσα την τρίτη αυτή εταιρία για το roaming. Πληρώνει το δικό του πάροχο, ο οποίος με τη σειρά του πληρώνει το άλλο δίκτυο. Όταν λοιπόν κάποιος έχει πραγματοποιήσει πλαστή συνδρομή, κάποια στιγμή θα διακοπεί η σύνδεσή του αφού δεν πληρώνει. Αν όμως ξεκινήσει να χρησιμοποιεί υπηρεσίες roaming πριν τη διακοπή, μπορεί να συνεχίσει να πραγματοποιεί κλήσεις μέσω του άλλου παρόχου. Κατά συνέπεια ο εξαπατημένος τηλεπικοινωνιακός οργανισμός καταλήγει να έχει χάσει ακόμα περισσότερα χρήματα.

4.3.6 Διεφθαρμένοι υπάλληλοι

Δυστυχώς μια εταιρία δεν μπορεί πάντα να βασιστεί σε όλους τους υπαλλήλους[44] της. Υπάρχουν αρκετοί που είναι διατεθειμένοι να θέσουν σε μεγάλο κίνδυνο τον οργανισμό στον οποίο δουλεύουν αλλά και τους πελάτες του. Και όλα αυτά για να αποκτήσουν κάποιο προσωπικό όφελος.

Οι διεφθαρμένοι αυτοί υπάλληλοι μπορεί να βρίσκονται σε οποιαδήποτε βαθμίδα της ιεραρχίας του οργανισμού τους. Η ζημιά που κάνουν μπορεί να έχει διάφορες διαστάσεις. Σε μικρότερες επιχειρήσεις(π.χ εμπορικά καταστήματα) συνήθως διαπράττουν κλοπή χρημάτων άμεσα(κατευθείαν από το ταμείο) ή έμμεσα(επιπλέον χρέωση προϊόντων σε πελάτες κλπ). Σε μεγάλες επιχειρήσεις, οι προδότες συνήθως συνεργάζονται με ανταγωνιστές του εργοδότη τους για να τον καταστρέψουν. Το αντάλλαγμα είναι συνήθως χρήματα και κάποια καλύτερη θέση εργασίας στην ανταγωνιστική επιχείρηση. Στις περιπτώσεις τώρα των τηλεπικοινωνιακών οργανισμών που διαχειρίζονται ευαίσθητα προσωπικά στοιχεία χιλιάδων πελατών, το πρόβλημα παίρνει μεγαλύτερες διαστάσεις. Τα στοιχεία των πελατών πολλές φορές πωλούνται σε κακόβουλους τρίτους. Έτσι, διαπράττονται απάτες σε βάρος των πελατών και πλήττεται ανεπανόρθωτα το κύρος του οργανισμού.

Οι διεφθαρμένοι υπάλληλοι ήταν, είναι και θα είναι αναπόσπαστο κομμάτι των επιχειρήσεων και των οργανισμών. Για το λόγο αυτό, οι διευθυντές των τμημάτων θα πρέπει να ψάχνουν συνεχώς για στοιχεία που προδίδουν ένα τέτοιο υπάλληλο. Το πρώτο πράγμα που χρειάζεται να παρατηρήσουν είναι η συμπεριφορά των εργαζομένων. Αν κάποιο από τα μέλη του προσωπικού έχει αδικαιολόγητο άγχος ή απότομη αλλαγή προσωπικότητας, δουλεύει σχεδόν πάντα μέχρι αργά και αρνείται πεισματικά να πάρει άδεια, τότε το θέμα χρειάζεται διερεύνηση. Αν πάλι κάποιος υπάλληλος έχει ανεξήγητα μεγάλη οικονομική δυνατότητα και απότομη αλλαγή τρόπου ζωής κάτι μπορεί να κρύβεται από πίσω. Νεοπροσληφθέντες υπάλληλοι που παραιτούνται γρήγορα θα πρέπει επίσης να κινήσουν υποψίες. Ακόμα, πρέπει να παρακολουθούνται τυχόν στενές σχέσεις μελών του προσωπικού με εξωτερικούς συνεργάτες. Τέλος, άλλα δύο φαινόμενα που θα πρέπει να σημάνει συναγερμό, είναι η απότομη και αδικαιολόγητη αύξηση του κόστους λειτουργίας της επιχείρησης και

[43] http://www.thefreelibrary.com/Telecommunications+fraud-a020794166
[44] http://www.cifas.org.uk/default.asp?edit_id=579-57

παράπονα πελατών για μη αναγνωρισμένες συναλλαγές. Καλό είναι, όλοι οι υπάλληλοι ενός οργανισμού (ανεξαρτήτως βαθμού) να γνωρίζουν ότι βρίσκονται συνεχώς υπό παρακολούθηση, ακόμα και αν δεν συμβαίνει κάτι τέτοιο. Αυτό από μόνο του μπορεί να αποτρέψει πολλούς επίδοξους απατεώνες.

Η οικονομική ζημιά που προκαλούν οι προδότες στις τηλεπικοινωνιακές εταιρίες είναι σίγουρα μεγάλη. Το πόσο μεγάλη όμως δεν είναι δυνατό να διαπιστωθεί, αφού δεν υπάρχουν αρκετά στοιχεία. Καμία εταιρία δεν παραδέχεται ότι έχει διεφθαρμένα άτομα στο δυναμικό της, αφού κάτι τέτοιο θα έκανε μεγαλύτερη ζημιά στην εικόνα της

4.3.7 Απάτη με τηλεκάρτες

Στην Ελλάδα, πάντα υπήρχε μια επιθυμία του κοινού να ξαναγεμίζει τις τηλεκάρτες ή να κατασκευάζει δικές του αποσκοπώντας(φυσικά) σε δωρεάν τηλεφωνήματα. Πριν από 10-15 χρόνια αυτό ήταν δυνατό, αφού δεν υπήρχε κάποια ουσιαστική δικλείδα ασφαλείας στα καρτοτηλέφωνα. Ο έλεγχος εγκυρότητας γινόταν επιτόπου στη συσκευή και αν όλα απλά φαινόταν να είναι εντάξει, ο απατεώνας μπορούσε να πραγματοποιήσει κλήση. Με κατάλληλα μηχανήματα ανάγνωσης τέτοιων καρτών και λογισμικό υπολογιστή, οι απατεώνες άλλαζαν το υπόλοιπο των μονάδων και έκαναν τις κάρτες να φαίνονται γεμάτες ακόμα και αν είχαν ελάχιστες μονάδες.

Τη σύγχρονη εποχή, τα πράγματα έχουν αλλάξει[45]. Όταν η τηλεκάρτα εισάγεται στο καρτοτηλέφωνο για πρώτη φορά, ο σειριακός της αριθμός καταγράφεται στο server του ΟΤΕ και το υπόλοιπο μονάδων παρακολουθείται, οπότε αποκλείεται το ενδεχόμενο ξαναγεμίσματος. Αν η ίδια κάρτα την επόμενη φορά που θα εισαχθεί περιέχει παραπάνω μονάδες, αυτόματα ακυρώνεται. Οπότε η μόνη λύση φαντάζει αυτή της κατασκευής μιας καινούριας.

Ακόμα όμως και μια πλαστή τηλεκάρτα βάζει σε κίνδυνο τον κάτοχό της. Η κατανάλωση του ρεύματος πρέπει να είναι σωστή, αλλιώς θα ειδοποιηθούν τα κεντρικά του ΟΤΕ και στη συνέχεια κάποιο κοντινό περιπολικό για να ελέγξει την κατάσταση. Αν ξεπεραστεί και αυτό το πρόβλημα, ο επίδοξος απατεώνας δεν θα πρέπει να ξεχάσει την τελευταία δικλείδα ασφαλείας. Κάθε βράδυ, το εσωτερικό modem κάθε καρτοτηλεφώνου, στέλνει στο server του ΟΤΕ μια λίστα με τις κάρτες που χρησιμοποιήθηκαν, καθώς και τις κλήσεις που πραγματοποιήθηκαν. Αν υπάρχει κάποια υποψία (και κάποιος σοβαρός λόγος), μπορούν οι αρχές μέσω των κλήσεων που έχουν πραγματοποιηθεί να εντοπίσουν τον ιδιοκτήτη μιας πλαστής τηλεκάρτας.

[45] http://www.techteam.gr/forum/topic/44821-sxetika-me-fake-thlekartes-/

Κεφάλαιο 5 Telemarketing Fraud

5.1 Τι είναι η απάτη με τηλεφωνικές πωλήσεις

Η απάτη με τηλεφωνικές πωλήσεις(ή τηλεαγορές)[46] αναφέρεται γενικά σε κάθε μορφή πλεκτάνης στην οποία οι απατεώνες χρησιμοποιούν το τηλέφωνο για να επικοινωνήσουν με τα υποψήφια θύματά τους. Συνήθως, οι επιτήδειοι, μέσα από υποσχέσεις, ψευδείς πληροφορίες και πλαστοπροσωπία προσπαθούν να πείσουν τα θύματα τους να στείλουν χρήματα. Μπορεί να εμφανίζονται ως πωλητές προϊόντων ή ως εκπρόσωποι φιλανθρωπικών/κυβερνητικών οργανισμών και να ζητούν από το θύμα χρήματα για διάφορους λόγους. Για να πετύχουν το σκοπό τους, πρέπει να προσέξουν τρία βασικά πράγματα, τα οποία θα αναλυθούν αμέσως παρακάτω.

Πρώτα απ' όλα, οι απατεώνες πρέπει να εμφανίσουν το προϊόν ή την υπηρεσία που προσφέρουν ως κάτι που αξίζει τα χρήματα που ζητούν. Οι ψεύτικοι τηλεπωλητές προσπαθούν να μεγιστοποιήσουν τα κέρδη τους με δύο τρόπους. Ο ένας είναι να πάρουν τα χρήματα του θύματος και να μην προσφέρουν τίποτα ως αντάλλαγμα. Ο δεύτερος, είναι να προσφέρουν κάτι αρκετά μικρότερης αξίας από τα χρήματα που έχουν λάβει. Ενώ για παράδειγμα ο καταναλωτής έχει αγοράσει ένα ρολόι που νομίζει ότι κοστίζει χιλιάδες ευρώ, λαμβάνει ένα με χαμηλή ποιότητα κατασκευής και υλικών που κοστίζει λίγες δεκάδες ευρώ.

Είναι επίσης σημαντικό για τους απατεώνες να λάβουν την πληρωμή τους, πριν το θύμα προλάβει να δει ποια είναι η πραγματική αξία του αγαθού που πλήρωσε. Ένας ψεύτικος τηλεπωλητής, θα επιμείνει να λάβει την πληρωμή του εκ των προτέρων χωρίς να δίνει την ευκαιρία στον καταναλωτή να ελέγξει την ποιότητα του αγαθού και κατά συνέπεια να ακυρώσει την αγορά. Για να ξεγελάσουν τα θύματά τους, συνήθως ασκούν πίεση λέγοντας ότι το αγαθό είναι σε περιορισμένη ποσότητα για περιορισμένο χρόνο. Ακόμα, ζητούν να πληρωθούν με κάποια μέθοδο που θα τους επιτρέψει να πάρουν τα χρήματα όσο πιο γρήγορα γίνεται.

Το σημαντικότερο ίσως που πρέπει να προσέξουν οι απατεώνες είναι να δημιουργούν μια εικόνα νομιμότητας γύρω από τη δραστηριότητά τους, αντιγράφοντας τον τρόπο επικοινωνίας νόμιμων επιχειρήσεων ή κυβερνητικών οργανισμών. Πολλές φορές προσποιούνται ότι είναι κυβερνητικοί πράκτορες ή αξιωματούχοι για να δώσουν αξιοπιστία στην απαίτησή τους για χρήματα.

Ένας βασικός παράγοντας που διαχωρίζει μια νόμιμη από μία παράνομη επιχείρηση τηλεαγορών, είναι το γεγονός ότι η δεύτερη συχνά ξαναχτυπά. Οι απατεώνες δηλαδή που έπεισαν κάποιο θύμα να τους στείλει χρήματα, μπορεί να ξανακαλέσουν και να εμφανίσουν ποικίλες δικαιολογίες για να ζητήσουν ακόμη περισσότερα. Για παράδειγμα, ένα θύμα έχει πληρώσει εκ των προτέρων τα έξοδα μεταφοράς για ένα εικονικό βραβείο που έχει κερδίσει. Ο απατεώνας μπορεί να καλέσει ξανά και να προσφέρει ακόμα πιο δελεαστικά δώρα με αντάλλαγμα την πληρωμή επιπλέον εξόδων μεταφοράς ή φόρων. Αυτή η πρακτική μπορεί να κλιμακωθεί σε τέτοιο σημείο που θα κάνει μεγάλη οικονομική ζημιά στο θύμα.

---

[46] http://www.justice.gov/criminal/fraud/telemarket/ask/whatis.html

Μία τακτική που ακολουθούν οι ψεύτικοι τηλεπωλητές, είναι να επικοινωνούν με καταναλωτές που βρίσκονται σε άλλη πόλη ή πολιτεία, ώστε να δυσκολέψουν τα θύματά τους και τις αρχές σε περίπτωση που προσπαθήσουν να τους κυνηγήσουν. Το θύμα πιθανόν να μη γνωρίζει που πρέπει να απευθυνθεί στην περίπτωση αυτή (στις τοπικές του δηλαδή αρχές ή του απατεώνα) και η συνεργασία των αρχών για τη δίωξη των επιτήδειων μπορεί να μην είναι επιτυχής.

5.2 Τύποι απάτης με τηλεφωνικές πωλήσεις

Διαβάζοντας κάποιος αυτή την ενότητα, θα διαπιστώσει ότι όλοι σχεδόν οι τύποι[47] αυτής της απάτης, αποσκοπούν στο να αποσπάσουν όσα περισσότερα χρήματα γίνεται από τα θύματα. Αξίζει να παρατηρήσει κανείς την εφευρετικότητα των απατεώνων σε πολλές περιπτώσεις.

5.2.1 Εικονικές φιλανθρωπίες

Πολλοί άνθρωποι έχουν την επιθυμία να βοηθήσουν οικονομικά αυτούς που έχουν ανάγκη. Οι ψεύτικοι τηλεπωλητές συχνά εκμεταλλεύονται τα φιλανθρωπικά συναισθήματα των άλλων, οργανώνοντας απάτες που ισχυρίζονται δια τηλεφώνου ότι μαζεύουν χρήματα για κοινωφελείς σκοπούς. Οι σκοποί τώρα αυτοί ποικίλουν. Μπορεί να είναι βοήθεια σε "κλασσικές" ομάδες που έχουν ανάγκη, όπως ορφανά, άπορους ηλικιωμένους, ανθρώπους του τρίτου κόσμου ή άτομα που προσπαθούν να απεξαρτηθούν από τα ναρκωτικά. Πολλές φορές, οι απατεώνες εκμεταλλεύονται και την επικαιρότητα και ισχυρίζονται ότι μαζεύουν χρήματα για τους εκάστοτε σεισμόπληκτους, πυρόπληκτους ή πλημμυροπαθείς. Σε ορισμένες περιπτώσεις, εμφανίζονται να μαζεύουν χρήματα για την ενίσχυση του τοπικού αστυνομικού ή πυροσβεστικού σώματος.

Μερικοί από αυτούς τους εγκληματικούς οργανισμούς, απλά παίρνουν τα χρήματα των θυμάτων και δεν δίνουν κάποιο ποσό για φιλανθρωπικούς σκοπούς. Κάποιοι άλλοι, για να διατηρήσουν μια εικόνα νομιμότητας, δωρίζουν ένα ελάχιστο ποσό από τα χρήματα που μαζεύουν (συνήθως 10% ή λιγότερο) σε κάποιο φιλανθρωπικό οργανισμό. Έτσι, έχουν αποδεικτικά στοιχεία ότι βοηθούν σε περίπτωση που τους ασκηθεί δίωξη από τις αρχές. Μία τέτοια εγκληματική οργάνωση μάλιστα (η οποία εξαρθρώθηκε και τα μέλη της καταδικάστηκαν), έστελνε και στα θύματα κάποια δώρα, ασήμαντης φυσικά αξίας, ως αναγνώριση της βοήθειας που έδιναν σε ένα φιλανθρωπικό "ίδρυμα". Το ίδρυμα αυτό, στην πραγματικότητα ήταν μία οργάνωση από πρώην ψεύτικους τηλεπωλητές που δεν έδινε κάποια βοήθεια για κοινωφελείς σκοπούς.

5.2.2 Πιστωτικές κάρτες-δάνεια

Μερικές από τις μηχανορραφίες των απατεώνων στοχεύουν ανθρώπους με κακό οικονομικό ιστορικό και χαμηλό εισόδημα. Οι επιτήδειοι τηλεφωνούν στα υποψήφια θύματα, δήθεν ως εκπρόσωποι χρηματοοικονομικών οργανισμών. Τους βεβαιώνουν ότι μπορεί να εκδοθεί πιστωτική κάρτα στο όνομά τους αν και δεν πληρούν τις προϋποθέσεις με κάποιο μικρό οικονομικό αντάλλαγμα. Τα θύματα που πληρώνουν

[47] http://www.justice.gov/criminal/fraud/telemarket/ask/schemes.html

αυτό το ποσό, συνήθως δεν λαμβάνουν τίποτα. Αν οι απατεώνες στείλουν κάτι, αυτό θα είναι είτε διαφημιστικά φυλλάδια είτε κάποια φόρμα αίτησης για την έκδοση κάρτας. Σε μια παραλλαγή της πλεκτάνης αυτής, τα θύματα θα λάβουν μια πιστωτική κάρτα, αλλά για να την ενεργοποιήσουν θα πρέπει να πληρώσουν επιπλέον χρήματα σε κάποια εταιρία που βρίσκεται στο εξωτερικό.

Στις περιπτώσεις των δανείων, οι απατεώνες υπόσχονται σε ανθρώπους με βεβαρυμμένο τραπεζικό ιστορικό ότι μπορούν να τους δώσουν δάνειο, με μια μικρή οικονομική επιβάρυνση που πρέπει να πληρωθεί εκ των προτέρων. Τα θύματα που πληρώνουν τα ζητούμενα χρήματα γράφονται σε κάποια λίστα που διατηρούν οι απατεώνες, για να ειδοποιηθούν αργότερα ότι η αίτησή τους για δάνειο απορρίφθηκε.

Οι ψεύτικοι τηλεπωλητές, δεν θα προσπαθήσουν πάντα να εκδώσουν δάνειο ή πιστωτική κάρτα στα θύματά τους. Σε ορισμένες πλεκτάνες, οι απατεώνες υπόσχονται "επιδιόρθωση" του κακού οικονομικού ιστορικού των υποψήφιων θυμάτων. Αφαίρεση δηλαδή χρεών, ενταλμάτων σύλληψης, καταδικαστικών αποφάσεων, υποθηκών χρεοκοπιών κλπ. Φυσικά, στις περισσότερες χώρες δεν υπάρχει η δυνατότητα να αφαιρεθούν στοιχεία από το οικονομικό ιστορικό κάποιου, εκτός αν αποδειχθεί ότι υπάρχει σφάλμα. Οπότε αν κάποια εταιρία ισχυρίζεται ότι μπορεί να βελτιώσει την οικονομική εικόνα ενός καταναλωτή, απλά ψεύδεται.

5.2.3 Επενδύσεις

Από τη δεκαετία του '70, πολλοί ψεύτικοι τηλεπωλητές προσφέρουν "ευκαιρίες" για επενδύσεις σε διάφορους τομείς. Στοχεύουν κυρίως τους άπειρους επενδυτές, με προσφορές που φαίνονται ιδιαίτερα δελεαστικές. Τη δεκαετία του '80 για παράδειγμα, οι απατεώνες πρόβαλλαν στα υποψήφια θύματά ευκαιρίες επενδύσεις σε σπάνια νομίσματα και πολύτιμα μέταλλα. Τη δεκαετία του ΄90, οι περισσότερες τέτοιες πλεκτάνες περιστρεφόταν γύρω από πολύτιμους λίθους, φάρμες με πουλερικά και τηλεοπτικά συστήματα.

Στις περιπτώσεις που το προϊόν πάνω στο οποίο το θύμα έχει επενδύσει είναι μικρό σε (φυσικό) μέγεθος (π.χ. κάποιο σπάνιο νόμισμα ή πολύτιμος λίθος), οι απατεώνες συνήθως του το αποστέλλουν σε ένα σφραγισμένο πλαστικό κουτί. Ο (ανυποψίαστος) επενδυτής προειδοποιείται να μην ανοίξει το κουτί, γιατί το προϊόν πιθανόν να χάσει τη συλλεκτική του αξία ή κάποια εγγύηση που υποτίθεται πως διαθέτει. Στην πραγματικότητα, οι απατεώνες απλά δε θέλουν να επιτρέψουν στο θύμα να εκτιμήσει την αξία του προϊόντος, ή να συμβουλευτεί κάποιον ειδικό. Αν τώρα το θύμα έχει επενδύσει σε κάτι που δεν μεταφέρεται (π.χ. πετρελαιοπηγές, τηλεοπτικά συστήματα κλπ), οι απατεώνες απλά ισχυρίζονται ότι τα προϊόντα βρίσκονται ακόμα σε φάση ανάπτυξης και δεν μπορούν να αποφέρουν κέρδος.

Σε μερικές από τις πλεκτάνες, οι απατεώνες καταφέρνουν να αποσπάσουν επιπλέον χρήματα ξεγελώντας για δεύτερη φορά τον ίδιο "επενδυτή". Τον ενημερώνουν δηλαδή ότι υπάρχει υποψήφιος αγοραστής για την επένδυση που έχει κάνει και τον "συμβουλεύουν" να επενδύσει ακόμα μεγαλύτερο ποσό στο ίδιο προϊόν για να έχει μεγαλύτερο κέρδος. Αν το θύμα ξεγελαστεί (ξανά), μετά από σύντομο χρονικό διάστημα τον ενημερώνουν ότι ο υποτιθέμενος αγοραστής δεν ενδιαφέρεται πλέον για την επένδυση.

Οι πλεκτάνες με νέες επιχειρήσεις, είναι μια παραλλαγή του παραπάνω σχεδίου. Στοχεύουν τους ανθρώπους που επιθυμούν να ξεκινήσουν δική τους επιχείρηση. Οι τηλεπωλητές, υπόσχονται να αναλάβουν το στήσιμο της επιχείρησης, χρησιμοποιώντας μεθόδους με εγγυημένη επιτυχία. Τέτοιου τύπου επιχειρήσεις έχουν να κάνουν με μηχανήματα αναψυκτικών, τηλεφωνικούς θαλάμους ή ηλεκτρονικά παιχνίδια. Το κόστος των επενδύσεων αυτών ανέχεται συνήθως σε χιλιάδες ευρώ/δολάρια, αλλά το μόνο που καταφέρνει τελικά ο επενδυτής είναι να αγοράσει άχρηστα μηχανήματα που δεν μπορεί στη συνέχεια να τα μεταπωλήσει.

Οι πλεκτάνες αυτές χρησιμοποιούν συνήθως μια συγκεκριμένη μέθοδο. Οι απατεώνες βάζουν αγγελία ή διαφήμιση στις τοπικές εφημερίδες και το τηλέφωνο που δίνουν είναι συνήθως αριθμός χωρίς χρέωση (800-). Στη διαφήμιση υπόσχονται τεράστια κέρδη με σχετικά απλές διαδικασίες. Οι καταναλωτές που θα ξεγελαστούν και θα καλέσουν, ακούν γενικολογίες για μεγάλα προβλεπόμενα κέρδη και πολλές υποσχέσεις για την επιτυχία της επιχείρησης. Δυστυχώς για το πως θα γίνει αυτό, συνήθως δεν τους λέει κανένας, γιατί απλά δεν θα γίνει.

Ένας νόμιμος πωλητής franchise, θα δώσει στον υποψήφιο επενδυτή αναλυτικές πληροφορίες για τον τρόπο οργάνωσης και λειτουργίας της επιχείρησης, καθώς και στατιστικά πωλήσεων και κερδών από άλλους που έχουν ήδη επενδύσει. Ακόμα, ο ενδιαφερόμενος αν θέλει μπορεί να μιλήσει και με ιδιοκτήτες τέτοιων επιχειρήσεων και να μάθει ότι επιπλέον χρειάζεται. Το συμπέρασμα είναι ότι, οι υποσχέσεις για πολλά χρήματα με λίγη προσπάθεια, περιγράφουν αυτό που θα κερδίσει ο απατεώνας και όχι ο καταναλωτής.

5.2.4 Απάτες εκτός συνόρων

Στη συγκεκριμένη μορφή απάτης, οι θύτες χτυπούν θύματα που βρίσκονται σε διαφορετική χώρα. Οι προφάσεις που χρησιμοποιούνται από τους απατεώνες είναι συνήθως επενδύσεις, τζόγος και βραβεία. Οι ψεύτικοι τηλεπωλητές προτιμούν αυτή τη μέθοδο γιατί σε περίπτωση που τα θύματα τους καταγγείλουν θα είναι πιο δύσκολος ο εντοπισμός τους. Αυτό συμβαίνει γιατί υπάρχει καθυστέρηση στη συνεργασία των αρχών των δύο χωρών.

Οι τοπικές αρχές του θύματος θα πρέπει να ακολουθήσουν κάποια συγκεκριμένη νομική διαδικασία για να πετύχουν την έκδοση του καταζητούμενου από την άλλη χώρα. Οι διαδικασίες αυτές είναι ιδιαίτερα μακροσκελείς και δίνουν τη ευκαιρία στους απατεώνες να αποφύγουν τη σύλληψη. Τη σημερινή εποχή, η καθυστέρηση αυτή είναι τόσο μεγάλη ώστε ακόμα και αν συλληφθούν τελικά οι απατεώνες, το θύμα μάλλον θα πεθάνει πριν προλάβει να γίνει η εκδίκαση της υπόθεσης (δεδομένου ότι στόχος των απατεώνων είναι συνήθως άνθρωποι μεγαλύτερης ηλικίας).

5.2.5 Κληρώσεις του εξωτερικού

Οι ψεύτικοι τηλεπωλητές συχνά προσπαθούν να πουλήσουν στους καταναλωτές λαχνούς ή λαχεία από κληρώσεις του εξωτερικού. Στις ΗΠΑ και αλλού , είναι παράνομη η εισαγωγή λαχνών από διαφορετικές χώρες. Παρόλα αυτά οι απατεώνες συνεχίζουν τη συγκεκριμένη πρακτική, επικοινωνώντας με τα υποψήφια θύματά τους μέσω αλληλογραφίας, τηλεφώνου και ηλεκτρονικού ταχυδρομείου. Τα θύματα που πέφτουν στην παγίδα ξεκινούν συνήθως με μικρά ποσά της τάξης των 5-10 δολαρίων

ή ευρώ. Αργότερα επικοινωνεί μαζί κάποιος που παριστάνει τον "ειδικό" στις επενδύσεις σε τυχερά παιχνίδια και προσπαθεί να τους πείσει να επενδύσουν σταδιακά ακόμα περισσότερα χρήματα. Δεν είναι λίγες οι φορές, που τα θύματα έστειλαν δεκάδες ή εκατοντάδες χιλιάδες δολάρια στους απατεώνες με την ελπίδα να κερδίσουν πολλαπλάσια ποσά.

Στην πραγματικότητα, οι επιτήδειοι τηλεπωλητές επενδύουν ελάχιστα (ή καθόλου) από τα χρήματα των ανυποψίαστων καταναλωτών σε τυχερά παιχνίδια, κρατώντας το μεγαλύτερο ποσοστό για τη συντήρηση του εαυτού τους και της παράνομης επιχείρησής τους. Δεν είναι λίγες οι φορές που τα θύματα από μόνα τους ανακάλυψαν ότι ο αριθμός του λαχείου που είχαν αγοράσει κέρδισε. Όταν επικοινώνησαν με τους απατεώνες η δικαιολογία που άκουσαν ήταν ότι τα κέρδη "επενδύθηκαν" στην αγορά περισσότερων λαχνών αντί να δοθούν άμεσα σε αυτούς.

5.2.6 Συνδρομές περιοδικών

Τα τελευταία χρόνια, υπάρχουν πολλές απάτες τηλεαγορών που προσφέρουν υποτιθέμενες συνδρομές σε περιοδικά. Οι απατεώνες βασίζονται στη δημοτικότητα των πολυδιαφημισμένων εταιριών προώθησης περιοδικών, που μαζί με κάθε συνδρομή κάνουν δώρο τη συμμετοχή σε κάποιο μεγάλο διαγωνισμό. Μία τέτοια πλεκτάνη, έχει συνήθως τη μορφή που θα περιγραφεί αμέσως παρακάτω.

Ο ψεύτικος τηλεπωλητής, τηλεφωνεί στο υποψήφιο θύμα. Του λέει ότι έχει κερδίσει ένα δώρο μεγάλης αξίας, αλλά για να το παραλάβει θα πρέπει να αγοράσει συνδρομή σε ένα ή περισσότερα περιοδικά. Η τιμή του πακέτου των συνδρομών μπορεί να κυμαίνεται μεταξύ εκατοντάδων, ακόμα και χιλιάδων δολαρίων/ευρώ. Το θύμα όμως, δεν ενημερώνεται για τους τίτλους των περιοδικών που θα λάβει. Αν τελικά συμφωνήσει να πληρώσει τα χρήματα, του αποστέλλεται ταχυδρομικώς μια λίστα με τα διαθέσιμα περιοδικά την οποία συμπληρώνει και στέλνει πίσω στον απατεώνα. Το τί γίνεται στη συνέχεια, ποικίλει. Το θύμα μπορεί θα λάβει τα προσυμφωνηθέντα περιοδικά, αλλά θα διαπιστώσει ότι τα έχει πληρώσει πολύ πιο ακριβά από το κανονικό. Σε άλλες περιπτώσεις, είτε θα λάβει ένα μέρος τους ή ακόμα και τίποτα. Σε ορισμένες ακραίες περιπτώσεις, θα του αποσταλούν τεύχη περιοδικού το οποίο κανονικά διανέμεται δωρεάν.

Αυτή η μορφή απάτης, είναι ίσως η πιο εύκολη στην αναγνώριση. Υπάρχουν έντονες διαφορές στον τρόπου προσέγγισης των πελατών μεταξύ μιας νόμιμης εταιρίας και των απατεώνων. Πρώτα απ' όλα, οι καταναλωτές θα πρέπει να γνωρίζουν ότι μια νόμιμη εταιρία δεν θα αποκρύψει ποτέ την πραγματική τιμή των περιοδικών. Θα τους ενημερώσει αναλυτικά για το κέρδος που θα έχουν αν πληρώσουν τη συνδρομή, αντί να αγοράσουν τα περιοδικά από το περίπτερο. Ο απατεώνας σπάνια θα κάνει κάτι τέτοιο, γιατί μπορεί να αποκαλυφθεί. Δεύτερον, οι νόμιμες επιχειρήσεις, θα ενημερώσουν από την αρχή (πριν γίνει οποιαδήποτε συναλλαγή) για το ποιοι τίτλοι περιοδικών είναι διαθέσιμοι. Οι απατεώνες θα απαιτήσουν από τον πελάτη να στείλει πρώτα χρήματα και μετά θα μάθει για τη διαθεσιμότητα των τίτλων. Τρίτον, μια νόμιμη επιχείρηση θα στείλει όλα τα τεύχη της συνδρομής για όλη τη διάρκεια αυτής. Οι απατεώνες αρκετές φορές, θα στείλουν μόνο ένα μέρος των τευχών στο θύμα και θα ισχυριστούν ότι τα υπόλοιπα τα δώρισαν σε άπορες ομάδες του πληθυσμού.

5.2.7 Εξοπλισμός γραφείου

Ακόμα ένας συνηθισμένος τύπος πλεκτάνης που οργανώνουν οι ψεύτικοι τηλεπωλητές και στοχεύει τις επιχειρήσεις, είναι η απάτη με εξοπλισμό γραφείου (ή αλλιώς απάτη toner). Στις άπατες αυτές, ένας εργαζόμενος του οργανισμού των απατεώνων τηλεφωνεί στην επιχείρηση και με διάφορες δικαιολογίες προσπαθεί να μάθει κατασκευαστή και μοντέλο του φωτοτυπικού μηχανήματος που χρησιμοποιούν. Μετά από μερικές μέρες, ο απατεώνας τηλεφωνεί ξανά και αυτή τη φορά ισχυρίζεται πως δουλεύει για τον κατασκευαστή του φωτοτυπικού. Ενημερώνει τον αρμόδιο υπάλληλο της επιχείρησης ότι τα toner που χρησιμοποιεί το φωτοτυπικό θα πάρουν αύξηση. Στη συνέχεια, προτείνει στον υπάλληλο να αγοράσει η εταιρία του μια μεγάλη ποσότητα toner με την τρέχουσα τιμή. Αν ο υπεύθυνος συμφωνήσει, αυτό που θα λάβει τελικά θα είναι μια απόδειξη χωρίς εμπόρευμα, ή ένα φορτίο το οποίο με την πρώτη ματιά μοιάζει να είναι εντάξει.

Τελικά όμως, δεν είναι. Αυτός που παραλαμβάνει τα toner, γρήγορα θα διαπιστώσει ότι δεν είναι καινούρια αλλά αναγομωμένα και ίσως σε κακή κατάσταση. Ακόμα χειρότερα, μπορεί να είναι τρίτου κατασκευαστή και χαμηλής ποιότητας. Και στις δύο περιπτώσεις, η εταιρία τα έχει πληρώσει πολύ ακριβότερα απ' ότι αξίζουν. Αυτά τα χαμηλής ποιότητας αναλώσιμα προκαλούν κατά κανόνα βλάβες και μπλοκαρίσματα στα φωτοτυπικά μηχανήματα, οι οποίες απαιτούν επισκευή από τεχνικό. Κατά την επίσκεψη του τεχνικού, οι υπεύθυνοι της εταιρίας συνήθως μαθαίνουν ότι τα toner δεν επρόκειτο να πάρουν αύξηση και ότι έχουν εξαπατηθεί.

5.2.8 Επιδόματα από την κυβέρνηση

Αυτή η μορφή απάτης συναντάται κυρίως στις ΗΠΑ. Ο απατεώνας καλεί το υποψήφιο θύμα και ισχυρίζεται ότι είναι αντιπρόσωπος ενός κυβερνητικού οργανισμού που χορηγεί οικονομικά επιδόματα[48]. Προσφέρεται να βοηθήσει τον καταναλωτή να λάβει ένα τέτοιο κυβερνητικό επίδομα, συνήθως της τάξης των 5000 δολαρίων. Για την εξυπηρέτηση αυτή, ο καταναλωτής χρειάζεται να πληρώσει ένα μικρό χρηματικό ποσό, το οποίο είναι ελάχιστο σε σχέση με την υποτιθέμενη απολαβή. Ακόμα, ο απατεώνας ζητά μερικά προσωπικά και οικονομικά στοιχεία από το θύμα, υποτίθεται για να προχωρήσει τη διαδικασία της χορήγησης του επιδόματος.

Στη συγκεκριμένη μορφή πλεκτάνης, οι απατεώνες χρησιμοποιούν ονόματα κυβερνητικών οργανισμών που ακούγονται αξιόπιστα (ακόμα και αληθινά ονόματα σε ορισμένες περιπτώσεις). Για να γίνουν πιο πιστευτοί, πολλές φορές παραπέμπουν τους καταναλωτές σε ιστοσελίδες, τις οποίες έχουν κατασκευάσει οι ίδιοι. Αυτές έχουν επίσημη και καλά οργανωμένη εμφάνιση. Εκεί ο καταναλωτής μπορεί να λάβει περισσότερες πληροφορίες και να συμπληρώσει μια φόρμα με τα προσωπικά του στοιχεία, πράγμα που τον κάνει να αισθάνεται μεγαλύτερη ασφάλεια. Όμως υπάρχει μια σημαντική παρατήρηση. Η διεύθυνση της ιστοσελίδας ενός επίσημου κυβερνητικού οργανισμού, τελειώνει σχεδόν πάντα σε .gov. Οι απατεώνες είναι σχεδόν αδύνατο να κάνουν τη διεύθυνση της δικής τους σελίδας να τελειώνει σε κάτι τέτοιο.

---

[48] http://www.fraudguides.com/federal_grant_scam.asp

Οι καταναλωτές, για να αποφύγουν αυτό τον τύπο απάτης, πρέπει πρώτα απ' όλα να γνωρίζουν ότι τα κυβερνητικά επιδόματα δεν έρχονται ποτέ από μόνα τους. Πρέπει να έχει προηγηθεί αίτηση του ενδιαφερομένου στην αρμόδια υπηρεσία. Και φυσικά, δεν υπάρχει κάποια χρέωση για το δικαιούχο σε περίπτωση που το επίδομα εγκριθεί, αφού θα ήταν παράνομη. Τέλος, οι καταναλωτές θα πρέπει να θυμούνται το γενικό κανόνα. Να μη δίνουν δηλαδή τα προσωπικά τους στοιχεία σε άγνωστους συνομιλητές, όσο αξιόπιστοι και αν ακούγονται. Πρέπει να ζητούν το όνομά τους, το όνομα της υπηρεσίας που εκπροσωπούν, καθώς και ένα τηλέφωνο για να μπορέσουν να επιβεβαιώσουν τους ισχυρισμούς.

5.2.9 Τηλεφωνικά βραβεία

Καθημερινά γίνονται χιλιάδες τηλεφωνήματα από ψεύτικους τηλεπωλητές σε ανυποψίαστα θύματα. Οι απατεώνες ισχυρίζονται ότι το θύμα έχει κερδίσει κάποιο βραβείο[49] μεγάλης χρηματικής αξίας. Επειδή μάλλον το θύμα δεν έχει πάρει μέρος σε κάποιο διαγωνισμό, του λένε ότι έχει επιλεγεί τυχαία από τον τηλεφωνικό κατάλογο ή βάσει στοιχείων που έχουν λάβει από μια αξιόπιστη (στο υποψήφιο θύμα) πηγή. Τα υποτιθέμενα δώρα, είναι συνήθως ιδιαίτερα δελεαστικά. Μπορεί να είναι κάποιο αυτοκίνητο, ακριβά κοσμήματα ή ρολόγια ή ακόμα και ολιγοήμερες διακοπές σε ένα εξωτικό προορισμό με διαμονή σε πολυτελές ξενοδοχείο. Το μόνο που χρειάζεται να κάνει ο "τυχερός" για να αποκτήσει το δώρο του, είναι να πληρώσει κάποιο μικρό χρηματικό ποσό (συνήθως για φόρους) ή ακόμα χειρότερα να αποκαλύψει λεπτομέρειες γύρω από τον τραπεζικό του λογαριασμό.

Το υποτιθέμενο δώρο μπορεί να μη φτάσει ποτέ στα χέρια του θύματος. Αν είναι κάτι μικρό και χειροπιαστό (π.χ. ρολόι-κόσμημα), μάλλον θα του αποσταλεί. Ο "τυχερός" όμως, θα διαπιστώσει ότι το ακριβό προϊόν του γνωστού κατασκευαστή που περίμενε, δεν είναι τίποτε άλλο από μια φτηνή απομίμηση που δεν άξιζε την προσοχή του. Στην παρακάτω εικόνα, φαίνεται το αντίγραφο ενός ακριβού ρολογιού (αξία περίπου 3500 ευρώ). Το θύμα που το "κέρδισε", μπορεί να πλήρωσε ακόμα και 100 ευρώ ή παραπάνω για τον υποτιθέμενο φόρο. Αυτό που λαμβάνει όμως, είναι η φτηνή απομίμηση της εικόνας που δεν αξίζει πάνω από 30 ευρώ.

Εικόνα 13:Μια απομίμηση του Rolex Submariner

[49] http://www.spamlaws.com/prize-scam.html

Κατά κανόνα, αν κάτι είναι πολύ καλό, τότε μάλλον δεν είναι αληθινό. Παρόλο όμως που οι απάτες αυτές είναι γνωστές εδώ και αρκετά χρόνια, υπάρχει ένας μεγάλος αριθμός ανθρώπων που συνεχίζουν να στέλνουν χρήματα ή να διακυβεύουν τους τραπεζικούς τους λογαριασμούς, με την πεποίθηση ότι θα αποκτήσουν αγαθά πολλαπλάσιας αξίας. Μετά από μια σχετικά πρόσφατη επιδρομή των αρχών του Καναδά σε μια μία τέτοια παράνομη εταιρία τηλεπωλήσεων, ανακαλύφθηκαν επιταγές συνολικής αξίας $350.000. Οι επιταγές αυτές προερχόταν από θύματα στη Μεγάλη Βρετανία και ήταν μόνο μία εβδομάδα δουλειάς.

Δυστυχώς, τα προβλήματα του θύματος δεν τελειώνουν στο γεγονός ότι έχει εξαπατηθεί. Όποιος άνθρωπος υποκύψει σε μια τέτοια πλεκτάνη, μπαίνει αυτόματα σε μια λίστα από "κορόιδα". Η λίστα αυτή περιέχει τα προσωπικά του στοιχεία και πωλείται από τον απατεώνα (που εξαπατά πρώτος το θύμα) σε "συναδέλφους" του σε όλο τον κόσμο. Έτσι, αν το θύμα κάνει μία φορά το λάθος, μπορεί να μην ησυχάσει ποτέ από τα τηλεφωνήματα των ψεύτικων τηλεπωλητών.

Μία άλλη συνέπεια είναι η δυσφήμηση των νόμιμων εταιριών που διεξάγουν διαγωνισμούς. Η αύξηση των περιστατικών ψεύτικων διαγωνισμών και εικονικών βραβείων έχει δημιουργήσει ένα κλίμα δυσπιστίας εναντίον κάθε μορφής διαγωνισμού, ακόμα και αυτών που διεξάγονται νόμιμα από αξιόπιστες εταιρίες. Σύμφωνα με τις προειδοποιήσεις πολλών κυβερνήσεων, οι καταναλωτές θα πρέπει να είναι προσεκτικοί όταν λαμβάνουν μέρους σε διαγωνισμούς ή όταν τους προσφέρονται βραβεία. Καλό είναι να επιβεβαιώνουν πάντα ποια εταιρία βρίσκεται πίσω από το διαγωνισμό και να μη στέλνουν σε καμία περίπτωση χρήματα εκ των προτέρων.

5.2.10 Απάτη εν κινήσει

Συνήθως, οι εγκληματίες που διαπράττουν απάτη με τηλεφωνικές πωλήσεις βρίσκονται σταθερά σε κάποιο σημείο. Ενοικιάζουν δηλαδή κάποιο κτίριο αρκετά μεγάλο (γνωστό στη γλώσσα τους ως "λεβητοστάσιο") ώστε να φιλοξενήσει αυτούς και τους δεκάδες ή εκατοντάδες εργαζομένους τους. Το "κέντρο των επιχειρήσεών" τους βρίσκεται τις περισσότερες φορές σε μεγάλη χιλιομετρική απόσταση από τα υποψήφια θύματα.

Τα τελευταία όμως χρόνια, οι αρχές έχουν σημειώσει μεγάλη πρόοδο στον εντοπισμό και τη σύλληψη των απατεώνων. Φυσικά και αυτοί δεν έχουν μείνει με σταυρωμένα χέρια. οι περισσότεροι στρέφονται στις απάτες εν κινήσει[50]. Δεν δρουν δηλαδή από ένα σταθερό σημείο, αλλά από πολλά διαφορετικά και ανώνυμα. Χρησιμοποιούν δηλαδή δωμάτια ξενοδοχείων, δημόσια τηλέφωνα και καρτοκινητά. Όλα αυτά έχουν το κοινό ότι δεν εντοπίζονται εύκολα. Ο πιο συχνός τύπος απάτης που εφαρμόζεται εκ κινήσει είναι τα "δωμάτια αποκατάστασης" που περιγράφονται παρακάτω.

Όπως είναι φυσικό, σε αυτές τις πλεκτάνες οι απατεώνες ζητούν από τα θύματα να τους στείλουν χρήματα σε ταχυδρομικές θυρίδες ή μέσω κάποιας υπηρεσίας μεταφοράς χρημάτων. Πάντα δηλαδή μετρητά, τα οποία επίσης εντοπίζονται δύσκολα

[50] http://www.fraudguides.com/telemarketing-rip-and-tear.asp

και μπορούν να ξοδευτούν οπουδήποτε. Μια άλλη τεχνική που χρησιμοποιούν, είναι να αναθέτουν την παραλαβή των χρημάτων σε εταιρίες ταχυμεταφορών (courier). Αν η αστυνομία συλλάβει τον ανυποψίαστο μεταφορέα και τον οδηγήσει σε ανάκριση, δεν θα πάρει πληροφορίες αφού και ο ίδιος δεν γνωρίζει τίποτα για την πλεκτάνη και γίνεται άθελά του πιόνι στα χέρια των απατεώνων.

5.2.11 Δωμάτια αποκατάστασης

Ίσως η πιο ανήθικη μορφή απάτης τηλεφωνικών πωλήσεων, είναι τα λεγόμενα "δωμάτια αποκατάστασης[51]". Ένας απατεώνας τηλεφωνεί σε κάποιον άνθρωπο που έχει πέσει ήδη θύμα απάτης (πιθανόν και του ιδίου) και παριστάνει τον υπάλληλο σε κάποιο κυβερνητικό οργανισμό, την αστυνομία ή το γραφείο του εισαγγελέα. Ισχυρίζεται ότι η υπηρεσία του μπορεί να βοηθήσει τον παθόντα να ανακτήσει μέρος των χρημάτων που έχασε. Εμφανίζεται πλήρως ενημερωμένος για την ιστορία και τα στοιχεία του θύματος, πράγμα που του προσδίδει κάποια αξιοπιστία. Για να προχωρήσει τη διαδικασία ανάκτησης των χρημάτων, το θύμα μαθαίνει ότι πρέπει να πληρώσει κάποιο φόρο. Αμέσως μετά τα χρήματα θα αποδεσμευτούν και το δικαστήριο θα εγκρίνει την επιστροφή στον παθόντα. Το αποτέλεσμα: το θύμα έχει χάσει ακόμα περισσότερα χρήματα και ο τηλεπωλητής-αντιπρόσωπος του νόμου, εξαφανίζεται για πάντα.

Αυτή η πλεκτάνη, στοχεύει ανθρώπους που έχουν χάσει μεγάλο μέρος των χρημάτων τους και είναι απελπισμένοι να τα πάρουν πίσω. Η ψυχολογία τους είναι σε κακή κατάσταση γιατί από τη μία έχουν χάσει τα χρήματά τους και από την άλλη αισθάνονται ανόητοι και ντρέπονται να καταγγείλουν το περιστατικό στις αρχές. Οι υποτιθέμενοι εκπρόσωποι του νόμου, προσφέρουν κατανόηση, ανωνυμία και πάνω απ' όλα την ελπίδα που το θύμα έχει πραγματικά ανάγκη. Και όλα αυτά για να του κάνουν τελικά μεγαλύτερο κακό από αυτό που έχουν ήδη κάνει.

5.3 Πέντε πραγματικά περιστατικά

5.3.1 Η περίπτωση του Juan Llamas

Στις 8 Δεκεμβρίου 2008, ο Juan Llamas[52] καταδικάστηκε σε 11 χρόνια φυλάκιση και πληρωμή 4 εκατομμυρίων δολαρίων για τη συμμετοχή του σε διεθνές κύκλωμα απάτης με τηλεαγορές. Το υπουργείο εμπορίου των ΗΠΑ, διερευνούσε την υπόθεση για 5 χρόνια. Οι απατεώνες είχαν ως έδρα την Κόστα Ρίκα και ο Llamas ήταν ο τελευταίος που καταδικάστηκε μετά την ομολογία για συμμετοχή του σε 63 περιπτώσεις απάτης. Στη συγκεκριμένη πλεκτάνη, οι απατεώνες στην επικοινωνία τους με τα θύματα, παρίσταναν αντιπροσώπους κυβερνητικών υπηρεσιών των ΗΠΑ. Ισχυρίζονταν ότι το θύμα έχει κερδίσει βραβεία μεγάλης αξίας σε κάποιο διαγωνισμό και για να τα αποκτήσει έπρεπε φυσικά να πληρώσει κάποιο μικρό ποσό για φόρους και έξοδα αποστολής.

Οι απατεώνες με τον τρόπο αυτό κατάφεραν να αποσπάσουν από κατοίκους των ΗΠΑ δεκάδες εκατομμύρια δολάρια. Τελικά, συνελήφθησαν 37 άτομα, τα οποία

[51] http://www.fraudguides.com/telemarketing-recovery-room.asp
[52] http://www.oig.doc.gov/oig/investigations/000603.html

καταδικάστηκαν σε φυλάκιση και πλήρωσαν πάνω από 200 εκατομμύρια δολάρια σε αποζημιώσεις.

5.3.2 Τα αδέρφια John και Ray Lin

Το Μάρτιο του 2010, το FTC (Federal trade Commission) των ΗΠΑ κατάφερε να φέρει ενώπιον της δικαιοσύνης δύο αδέλφια[53] με κατηγορίες για cramming και απάτης με τηλεαγορές. Οι John και Ray Lin, κατάφεραν μέσα σε διάστημα πέντε ετών να αποσπάσουν 19 εκατομμύρια δολάρια από ιδιώτες και επιχειρήσεις. Η ιδιαιτερότητα της περίπτωσης αυτής, είναι ότι τα αδέλφια εμφανίστηκαν στο δικαστήριο και υπερασπίστηκαν μέχρι τέλους τους εαυτούς τους. Προσπάθησαν δηλαδή να πολεμήσουν το FTC και να αποδείξουν ότι λειτουργούσαν μια νόμιμη επιχείρηση. Τελικά καταδικάστηκαν, μεταξύ άλλων και για πλαστογράφηση της υπογραφής της μητέρας τους, μετά το θάνατό της.

5.3.3 Η ομάδα των 9

Στις 9 Ιουλίου 2009, ένας ομοσπονδιακός εισαγγελέας στις ΗΠΑ άσκησε δίωξη σε εννέα άτομα[54] που συμμετείχαν σε τηλεφωνική απάτη. Πιο συγκεκριμένα, οι κατηγορούμενοι φαίνεται να δρούσαν σε ένα "λεβητοστάσιο"(κάθε κτίριο στο οποίο όπως είπαμε δραστηριοποιούνται οι ψεύτικοι τηλεπωλητές) στο Ισραήλ. Στόχος τους ήταν ηλικιωμένα άτομα στις ΗΠΑ. Προσπαθούσαν να πείσουν τους ηλικιωμένους να συμμετέχουν σε εικονικές κληρώσεις στέλνοντας μεγάλα χρηματικά ποσά.

Η περίπτωση αυτή ήταν μια ξεκάθαρη μορφή πλεκτάνης εκτός συνόρων. Λειτουργούσε σε δύο στάδια. Στο πρώτο στάδιο, οι απατεώνες είχαν στα χέρια τους μια λίστα από υποψήφια θύματα. Επικοινωνούσαν μαζί τους παριστάνοντας τους εργαζόμενους σε εταιρία στοιχημάτων και ισχυρίζονταν ότι το θύμα έχει κερδίσει κάποιο μεγάλο χρηματικό βραβείο. Κρατούσαν τα προσωπικά στοιχεία όσων έπεφταν στην παγίδα και στη συνέχεια τα προωθούσαν σε συναδέλφους τους. Αυτοί προχωρούσαν στο δεύτερο στάδιο. Επικοινωνούσαν δηλαδή με τα θύματα και παρίσταναν τους δικηγόρους των εταιριών αυτών, με υποτιθέμενη πάντα έδρα τις ΗΠΑ. Υπαγόρευαν στα θύματα το γνωστό παραμύθι, ότι δηλαδή για να παραλάβουν το βραβείο τους έπρεπε να στείλουν χρήματα για την πληρωμή φόρων και τη μεταφορά των χρημάτων.

Μέχρι τη στιγμή που γράφτηκε το άρθρο, οι αρχές των ΗΠΑ δεν είχαν ζητήσει ακόμα την έκδοση των κατηγορουμένων. Κατά συνέπεια, δεν υπάρχει ακριβής αναφορά της οικονομικής ζημιάς που έκαναν, αν και εκτιμάται να είναι αρκετά εκατομμύρια δολάρια.

[53] http://arstechnica.com/tech-policy/news/2010/03/ftc-crams-a-major-crammer.ars
[54] http://blogs.findlaw.com/courtside/2009/07/ring-ring-boiler-room-telemarketing-lottery-fraud-calling.html

5.3.4 Η συμμορία της Φλόριντα

Τον Ιανουάριο του 2010, συνελήφθη ένας άντρας στην Φλόριντα των ΗΠΑ κατηγορούμενος για απάτη με πλαστές επενδύσεις[55]. Συμμετείχε σε δύο διαφορετικά κυκλώματα απάτης που εξαρθρώθηκαν. Κατηγορείται ότι απέσπασε εκατοντάδες χιλιάδες δολάρια από κατοίκους χωρών εκτός ΗΠΑ.

Ο άνθρωπος αυτός ονομαζόταν John A. Reece και ήταν τότε 57 ετών. Στο πρώτο κύκλωμα συμμετείχε μαζί με τον Patrick Soltis, ο οποίος είχε ήδη συλληφθεί και είχε δηλώσει ένοχος. Ξεκίνησαν να ψάχνουν για επενδυτές-θύματα το 2002. Είχαν προσλάβει τηλεπωλητές και προσπαθούσαν να πουλήσουν σε επενδυτές μετοχές μιας εταιρίας που υπήρχε μόνο στη φαντασία τους. Ισχυρίζονταν πως η (φανταστική) εταιρία τους, η "Wolf & Soltis Holdings LLc", είχε έντονη επιχειρηματική δραστηριότητα και επρόκειτο να επεκταθεί σε διάφορες περιοχές. Οι απατεώνες ισχυρίζονταν ότι η προαναφερθείσα εταιρία είχε και πολλές θυγατρικές. Μεταξύ αυτών, ήταν μια επιχείρηση που ασχολούνταν με καλλυντικά και μια άλλη που δραστηριοποιούνταν στην εμφιάλωση νερού. Ακόμα, υποτίθεται ότι συνεργάζονταν με το πανεπιστήμιο της Μινεσότα για να αναπτύξουν ένα νέο είδος δέντρου που αναπτυσσόταν πιο γρήγορα. Στην πραγματικότητα, όπως είναι φυσικό, η εταιρία δεν διέθετε καμία περιουσία, δραστηριότητα, κέρδος και προσωπικό εκτός από τους τηλεπωλητές. Οι δύο απατεώνες κρατούσαν το μεγαλύτερο μέρος από τα χρήματα των θυμάτων. Τα υπόλοιπα τα χρησιμοποιούσαν για να πληρώσουν τους τηλεπωλητές, τους λογαριασμούς του τηλεφώνου και τα λοιπά έξοδα της οργάνωσής τους.

Σε κάποιο σημείο υπήρξε διαφωνία μεταξύ των δύο συνεργατών. Ο Reece εγκατέλειψε τον Soltis και ξεκίνησε μια δική του συμμορία εξαπάτησης επενδυτών. Ίδρυσε πάλι μια εικονική εταιρία, την "Wellington Group" που υποτίθεται ότι ασχολούνταν με βιολογικά προϊόντα. Προσέλαβε τηλεπωλητές και αγόρασε λίστες με υποψήφια θύματα από άλλους απατεώνες. Έδωσε στους υπαλλήλους του οδηγίες για να μπορούν να προωθήσουν αποτελεσματικά τις ανύπαρκτες μετοχές σε ανυποψίαστους επενδυτές. Ο Reece, επέλεγε να εξαπατά ανθρώπους που βρισκόταν στο εξωτερικό σε αγγλόφωνες χώρες. Αυτό γινόταν φυσικά, για να αποφύγει ή τουλάχιστον να καθυστερήσει τη δίωξή του από τις αρχές των ΗΠΑ σε περίπτωση που γινόταν καταγγελία σε βάρος του. Η πλειοψηφία των θυμάτων προερχόταν από τον Καναδά και την Αυστραλία. Η οικονομική ζημιά που έκανε ο Reece στα θύματά του ξεπερνά τις 500000 δολάρια. Παραδέχτηκε την ενοχή του ενώπιον του δικαστηρίου και τιμωρήθηκε με φυλάκιση και χρηματικό πρόστιμο.

5.3.5 Το κύκλωμα του Καναδά

Τον Δεκέμβριο του 2006, η αστυνομία του Μόντρεαλ ξεσκέπασε ένα κύκλωμα τηλεπικοινωνιακής απάτης[56] που στόχευε ηλικιωμένους ανθρώπους κυρίως στις ΗΠΑ, αλλά και τον Καναδά. Μετά την διεξαγωγή ερευνών σε 50 περίπου σημεία, έγινε μεγάλος αριθμός συλλήψεων και κατασχέθηκαν περίπου 20000 δολάρια σε μετρητά.

---

[55] http://atlanta.bizjournals.com/atlanta/stories/2010/01/11/daily20.html
[56] http://www.ctv.ca/CTVNews/TopStories/20061219/fraud_mtl_061219/

Η απάτη αυτή ξεκίνησε το 2003 και χτυπούσε περίπου 500 άτομα την εβδομάδα, αποδίδοντας κέρδος μεταξύ 8 και 13 εκατομμυρίων δολλαρίων το χρόνο. Τα ποσά που πλήρωναν τα θύματα ποικίλουν. Περίπου 1500 δολάρια στις καλύτερες περιπτώσεις και 65000 στις χειρότερες. Οι απατεώνες δεν χρησιμοποιούσαν την ίδια δικαιολογία σε όλα τα θύματα. Συνήθως έλεγαν στο θύμα το γνωστό παραμύθι με τον υποτιθέμενο διαγωνισμό και μεγάλο χρηματικό έπαθλο. Ότι δηλαδή το θύμα είναι νικητής σε ένα διαγωνισμό(στον οποίο δεν έλαβε μέρος) και το βραβείο είναι κάποιο μεγάλο χρηματικό ποσό. Για να παραλάβει όμως τα χρήματα, ο νικητής έπρεπε να πληρώσει κάποιο ποσο(για φόρους ή διαδικαστικά έξοδα) που στη συγκεκριμένη απάτη ανερχόταν μεταξύ 1500 και 60000 δολαρίων. Άλλη δικαολογία που χρησιμοποιούνταν ήταν η αγορά υπηρεσιών υγείας. Τα χρήματα μεταφέρονταν μέσω της υπηρεσίας Western Union.

Η μεγάλη επιτυχία της απάτης οφείλεται κυρίως στο μέσο όρο ηλικίας των θυμάτων. Πάνω από το 90% αυτών ήταν πάνω από 60 ετών. Στην ηλικία αυτή οι άνθρωποι τείνουν να είναι ευαίσθητοι και να πιστεύουν ευκολότερα. Στις πιο τραγικές περιπτώσεις, οι άνθρωποι έβαλαν υποθήκη το σπίτι τους για να πληρώσουν τους απατεώνες. Η πλειοψηφία των θυμάτων, βρισκόταν στις ΗΠΑ αλλά υπήρχε ένας μικρός αριθμός και στον Καναδά.

Οι εγκληματίες προερχόταν όλοι από τον Καναδά και δρούσαν εκεί. Αξίζει να σημειωθεί ότι οι περισσότεροι συλληφθέντες ήταν σεσημασμένοι εγκληματίες και είχαν απασχολήσει ξανά τις αρχές με περιστατικά βίας και εμπορίας ναρκωτικών. Ακόμα, η εταιρία Western Union έκλεισε εθελοντικά επτά υποκαταστήματά της στο Μόντρεαλ, μέσω των οποίων γινόταν η παραλαβή των χρημάτων από τους απατεώνες. Εκπρόσωπος της εταιρίας δήλωσε ότι υπάρχουν υποψίες για πιθανή συνεργασία των καταστημάτων με τους κατηγορούμενους.

Αυτή η συμμορία ήταν μόνο μία από τις πολλές που δρούσαν και δρουν στον Καναδά. Ο οργανισμός Phonebusters(που ασχολείται με την αντιμετώπιση της τηλεπικοινωνιακής απάτης) εκτιμά ότι καθημερινά δρουν 500 με 1000 συμμορίες που διαπράττουν τηλεφωνική απάτη, κερδίζοντας περίπου ένα δισεκατομμύριο δολάρια το χρόνο.

Κεφάλαιο 6 Επίλογος

6.1 Συμπεράσματα

Στην παρούσα πτυχιακή εργασία, παρουσιάστηκε αναλυτικά το πρόβλημα της τηλεπικοινωνιακής απάτης, κυρίως σε επίπεδο τηλεφωνίας σταθερής και κινητής. Όπως διαπιστώθηκε, η τηλεπικοινωνιακή απάτη δεν είναι ένα ασήμαντο είδος απάτης, αλλά μια παράνομη επιχείρηση εκατομμυρίων. Θα μπορούσε κανείς να πει ότι μοιάζει με το εμπόριο ναρκωτικών αλλά χωρίς τις τόσες κοινωνικές επιπτώσεις. Οι απατεώνες που διαπράττουν αυτό το είδος απάτης είναι πραγματικοί εγκληματίες και πρέπει να αντιμετωπίζονται ως τέτοιοι.

Τη σημερινή εποχή, η τηλεπικοινωνιακή απάτη εναντίον των καταναλωτών τουλάχιστον(η οποία βασίζεται κυρίως στο social engineering) θα έπρεπε να έχει εξαλειφτεί. Τα μέσα μαζικής ενημέρωσης σε συνεργασία με τις ενώσεις καταναλωτών πραγματοποιούν εκστρατείες για την ενημέρωση του κοινού και την πρόληψη της απάτης. Παρόλα αυτά, το πρόβλημα δείχνει να εντείνεται αντί να συρρικνώνεται. Δυστυχώς μαζί με τους καταναλωτές προσαρμόζονται και οι απατεώνες. Προσπαθούν πάντα να παραστήσουν μια έμπιστη οντότητα και συνήθως το καταφέρνουν. Εμφανίζονται ενημερωμένοι για το ιστορικό και τη ζωή του υποψήφιου θύματος και τα σημεία που μπορούν να τους ξεχωρίσουν από ένα έμπιστο πρόσωπο είναι λεπτά και δύσκολο να εντοπιστούν από τον μέσο άνθρωπο. Δεν είναι όμως αδύνατο. Αν οι καταναλωτές μάθουν να μην εμπιστεύονται κανένα και να επιβεβαιώνουν αυτά που ακούν, το φαινόμενο θα περιοριστεί σημαντικά.

Το άλλο μεγάλο πρόβλημα που χτυπά τις επιχειρήσεις είναι η εκμετάλλευση των PBX. Δυστυχώς, όσο οι επιχειρηματίες προσπαθούν να εξοικονομήσουν ελάχιστα χρήματα στήνοντας μόνοι τους τα PBX, το πρόβλημα θα συνεχίσει να υφίσταται. Ένα τέτοιο σύστημα με κατάλληλες ρυθμίσεις δεν κινδυνεύει, τουλάχιστον όχι άμεσα. Οι επιχειρηματίες σε κάθε περίπτωση θα πρέπει να εμπιστεύονται την εγκατάσταση συστημάτων PBX σε εξειδικευμένους επαγγελματίες.

Το τρίτο σημαντικό πρόβλημα που μαστίζει τους τηλεπικοινωνιακούς παρόχους ανά τον κόσμο, είναι η πραγματοποίηση συνδρομών με πλαστά στοιχεία. Αυτό το είδος απάτης είναι πραγματικά δύσκολο να αντιμετωπιστεί. Και γίνεται ακόμα πιο δύσκολο τη σύγχρονη εποχή που πολλές νέες συνδέσεις πραγματοποιούνται μέσω διαδικτύου και η επιβεβαίωση στοιχείων είναι πρακτικά αδύνατη. Τα FMS που υπάρχουν, εφαρμόζουν πολιτικές ελέγχου των στοιχείων αλλά είναι από τη φύση τους ανεπαρκείς.

Διαπιστώνεται λοιπόν, ότι η τηλεπικοινωνιακή απάτη δεν είναι κάτι ασήμαντο ή αμελητέο. Συμβαίνει σε κάθε γωνιά του κόσμου και έχει τεράστιο οικονομικό αλλά και κοινωνικό αντίκτυπο. Δεν είναι λίγες οι περιπτώσεις που άνθρωποι έχουν καταστραφεί οικονομικά ή έχουν εγκληματήσει για να ικανοποιήσουν τις απαιτήσεις των απατεώνων. Και φυσικά δεν πρόκειται να εξαλειφθεί ποτέ. Οι εγκληματίες εκμεταλλευόμενοι την ανωνυμία τους και υπάρχοντα νομικά καθεστώτα γλιτώνουν τις περισσότερες φορές τη σύλληψη και είναι ελεύθεροι να ξεκινήσουν από την αρχή τις παράνομες ενέργειές τους.

6.2 Βιβλιογραφία

Εδώ παρατίθενται όλες οι πηγές που χρησιμοποιήθηκαν για την πραγματοποίηση της παρούσας πτυχιακής εργασίας με τη σειρά εμφάνισής τους:

1. http://en.wikipedia.org/wiki/Phreaking
2. http://en.wikipedia.org/wiki/Phreaking_boxes
3. http://en.wikipedia.org/wiki/Black_box_(phreaking)
4. http://en.wikipedia.org/wiki/Beige_box_(phreaking)
5. http://en.wikipedia.org/wiki/Blue_box_(phreaking)
6. http://en.wikipedia.org/wiki/Red_box_(phreaking)
7. http://en.wikipedia.org/wiki/John_Draper
8. http://en.wikipedia.org/wiki/Joybubbles
9. http://www.billingworld.com/articles/feature/Telecom-Fraud-on-the-Rise.html
10. http://www.theregister.co.uk/2009/03/24/telstraclear_hires_convicted_hacker/
11. http://www.ztesoft.com/ztesoft_en/download/pdf/bss/products/Fraud%20Management%20Product.pdf
12. http://www.phonebusters.com/english/statistics.html
13. http://www.cfca.org/pdf/survey/2009%20Global%20Fraud%20Loss%20Survey-Press%20Release.pdf
14. http://www.nbr.co.nz/article/companies-hit-400-increase-phone-fraud-128569
15. http://www.scribd.com/doc/13885875/Interesting-Facts-about-Fraud
16. http://news.softpedia.com/news/UK-Police-Dismantles-International-Telecom-Fraud-Ring-153123.shtml
17. http://english.cri.cn/6909/2010/08/25/45s591016.htm
18. http://www.free-press-release.com/news-fraud-crime-gang-busted-1282542064.html
19. http://en.wikipedia.org/wiki/Phone_fraud
20. http://en.wikipedia.org/wiki/Cramming_(fraud)

21. http://www.ucan.org/telenforcers/consumers/pursueandresolve/strategic_guides/cramming

22. http://www.thisismoney.co.uk/news/article.html?in_article_id=399990&in_page_id=2

23. http://en.wikipedia.org/wiki/Autodialer

24. http://en.wikipedia.org/wiki/Wangiri

25. http://www.snopes.com/fraud/telephone/809.asp

26. http://www.calleridspoofing.info/

27. http://www.ftc.gov/bcp/edu/microsites/phonefraud/identity.shtml

28. http://en.wikipedia.org/wiki/Advance_fee_fraud

29. http://en.wikipedia.org/wiki/Telephone_tapping

30. http://www.spy.th.com/audio.html#!au046

31. http://www.blackberrycool.com/2009/12/29/gsm-algorithm-cracked-leaving-voice-calls-unsecure/

32. http://www.techteam.gr/forum/topic/44821-sxetika-me-fake-thlekartes-/

33. http://www.crimes-of-persuasion.com/Crimes/Telemarketing/Outbound/Minor/assistance.htm

34. http://en.wikipedia.org/wiki/Prank_call

35. http://en.wikipedia.org/wiki/Pranknet

36. http://www.3cx.gr/voip-sip/tilefoniko-systima-pbx.php

37. http://www.tsips.com/PBX_Fraud_Facts.htm

38. http://www.teralight.com/fraud.php

39. http://en.wikipedia.org/wiki/Cloning_(telephony)

40. http://icta05.teithe.gr/papers/69.pdf

41. http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=481&mode=thread&order=0&thold=0

42. http://identityresolutiondaily.com/727/attacking-subscription-fraud-with-identity-resolution/

43. http://www.thefreelibrary.com/Telecommunications+fraud-a020794166

44. http://www.cifas.org.uk/default.asp?edit_id=579-57

45. http://www.justice.gov/criminal/fraud/telemarket/ask/whatis.html

46. http://www.justice.gov/criminal/fraud/telemarket/ask/schemes.html

47. http://www.fraudguides.com/federal_grant_scam.asp

48. http://www.spamlaws.com/prize-scam.html

49. http://www.fraudguides.com/telemarketing-rip-and-tear.asp

50. http://www.fraudguides.com/telemarketing-recovery-room.asp

51. http://www.oig.doc.gov/oig/investigations/000603.html

52. http://arstechnica.com/tech-policy/news/2010/03/ftc-crams-a-major-crammer.ars

53. http://blogs.findlaw.com/courtside/2009/07/ring-ring-boiler-room-telemarketing-lottery-fraud-calling.html

54. http://atlanta.bizjournals.com/atlanta/stories/2010/01/11/daily20.html

55. http://www.ctv.ca/CTVNews/TopStories/20061219/fraud_mtl_061219/