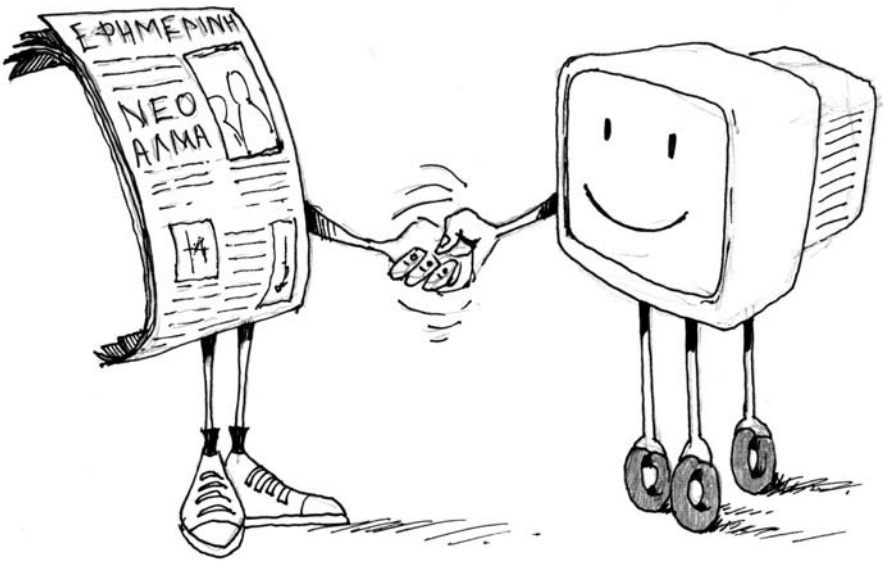

Σύγχρονες Μορφές Ηλεκτρονικής Εγκληματικότητας

της **Χριστίνας Κρέτση** // Φοιτήτριας Νομικής ΑΠΘ

Η έλευση της ψηφιακής εποχής προκάλεσε την εμφάνιση σύγχρονων μορφών εγκληματικότητας, όπως της Νιγηριανής επιστολής (Nigerian letter), των ηλεκτρονικών μηνύματων-δολωμάτων (phishing), της μαζικής υποκλοπής στοιχείων (pharming) και των προγραμμάτων κρυφών κλήσεων (dialers). Η ραγδαία ανάπτυξη της νέας ηλεκτρονικής εγκληματικότητας δεν δημιουργεί μόνο πολλά προβλήματα στην καθημερινή χρήση του διαδικτύου, δεδομένου ότι ο εντοπισμός των δραστών είναι συχνά δυσχερής, αλλά καθιστά συνάμα επιτακτική την ανάγκη της ενημέρωσης των πολιτών.

Η εξέλιξη της τεχνολογίας και η ανάπτυξη του διαδικτύου έχουν επιφέρει μεγάλες αλλαγές στην καθημερινότητα των ανθρώπων. Αυτές οι αλλαγές, οι οποίες είναι κατά ένα μεγάλο μέρος θετικές, δημιούργησαν παράλληλα πρόσφορο έδαφος για την ανάπτυξη νέων μορφών εγκληματικότητας. Έχουν κάνει την εμφάνισή τους, λοιπόν, πολλά νέα εγκλήματα τα οποία δεν υπήρχαν με αυτή τη μορφή πριν την ραγδαία ανάπτυξη του διαδικτύου. Στο παρόν άρθρο θα εξετάσουμε έναν αριθμό ηλεκτρονικών εγκλημάτων και ειδικότερα θα αναφερθούμε στη Νιγηριανή επιστολή (Nigerian letter), στα ηλεκτρονικά μηνύματα-δολώματα (phishing), στη μαζική υποκλοπή στοιχείων (pharming) και στα προγράμματα κρυφών κλήσεων (dialers).

Η Νιγηριανή Επιστολή

Ο όρος Νιγηριανή επιστολή αναφέρεται σε μια διαδικτυακή απάτη, που ξεκίνησε από τη Νιγηρία[1] και συνήθως πραγματοποιείται με μηνύματα ανεπιθύμητης αλληλογραφίας(spam e-mails), τα οποία αποστέλλονται μαζικά. Ο αποστολέας υποτίθεται ότι είναι μέλος της κυβέρνησης ή μιας εταιρίας ή τράπεζας και για κάποιους λόγους επιθυμεί να βγάλει χρήματα από την χώρα του. Για να το πετύχει αυτό είναι αναγκαίο να χρησιμοποιήσει τον τραπεζικό λογαριασμό κάποιου άλλου

Ένα ηλεκτρονικό μήνυμα-δόλωμα μπορεί να φαίνεται ίδιο με ένα νόμιμο ηλεκτρονικό μήνυμα από την τράπεζα του αποδέκτη και να χρησιμοποιεί μάλιστα και το λογότυπό της.

γιατί οι δικοί του είτε παρακολουθούνται είτε δε θέλει να κινήσει υποψίες, ενώ ως; αντάλλαγμα στις υπηρεσίες του θύματος υπόσχεται να προσφέρει ένα μέρος των χρημάτων σ' αυτό. Σε όλα τα στάδια της απάτης οι δράστες προσπαθούν να αποσπάσουν χρήματα και προσωπικά στοιχεία των θυμάτων λέγοντας ότι είναι απαραίτητα για τη μεταφορά των χρημάτων.[2] Στην πραγματικότητα κρατούν τα χρήματα που απέσπασαν και χρησιμοποιούν τα στοιχεία του θύματος και για άλλες απάτες. Σημειώθηκαν μάλιστα περιπτώσεις θυμάτων που δέχτηκαν ή πρότειναν τα ίδια να ταξιδέψουν στο εξωτερικό και εκεί κρατήθηκαν ως όμηροι ή δολοφονήθηκαν.[3]

Στο ελληνικό δίκαιο αυτή η απάτη θα μπορούσε να θεωρηθεί ότι εμπίπτει στην αντικειμενική υπόσταση του άρθρου 386ΠΚ αφού πρόκειται για μια μορφή απάτης που τελείται μέσω υπολογιστή[4]. Εδώ, δηλαδή, ο υπολογιστής είναι το μέσο τέλεσης της κοινής απάτης, οπότε έχουμε πλάνη φυσικού προσώπου δηλαδή του λήπτη του ηλεκτρονικού μηνύματος και όχι πλάνη μηχανής.

Συνοψίζοντας, ο θύτης πείθει το θύμα μέσω ηλεκτρονικού ταχυδρομείου να κάνει μια πράξη, είτε αυτή είναι η αποστολή χρημάτων είτε η παράδοση του αριθμού του τραπεζικού του λογαριασμού με σκοπό να βλάψει την περιουσία του. Αυτό το επιτυγχάνει παρουσιάζοντας ψευδή γεγονότα ως αληθινά, υποστηρίζοντας δηλαδή ότι είναι κάποιος άλλος και έχει κάποια χρήματα στη διάθεσή του που είναι διατεθειμένος να μοιραστεί. Επομένως πληρείται η αντικειμενική υπόσταση του εγκλήματος του άρθρου 386 §1 ΠΚ. Τέλος , πρέπει να σημειώσουμε ότι η πράξη της αποστολής του ηλεκτρονικού μηνύματος γίνεται με σκοπό να αποκομίσει ο δράστης ή κάποιος τρίτος παράνομο περιουσιακό όφελος, έχοντας δόλο για την βλάβη της περιουσίας του θύματος.

Ηλεκτρονικά Μηνύματα-Δολώματα (phishing)

Τα ηλεκτρονικά μηνύματα-δολώματα (phishing e-mails) φαίνεται να αποστέλλονται από μια νόμιμη εταιρία και προτρέπουν τους αποδέκτες να επισκεφτούν μια ψεύτικη ιστοσελίδα, με σκοπό να συγκεντρωθούν προσωπικές ή οικονομικές πληροφορίες γι' αυτούς από τους δράστες.[5] Αυτή η ιστοσελίδα είναι ένα πιστό αντίγραφο της αυθεντικής ιστοσελίδας της εταιρίας και το θύμα σπάνια έχει τη δυνατότητα να διακρίνει τις διαφορές.[6]

Για παράδειγμα, ένα ηλεκτρονικό μήνυμα-δόλωμα (phishing e-mail) μπορεί να φαίνεται ίδιο με ένα νόμιμο ηλεκτρονικό μήνυμα από την τράπεζα του αποδέκτη και να χρησιμοποιεί μάλιστα και το λογότυπό της.[7] Με αυτό ζητείται από τον παραλήπτη να επιβεβαιώσει κάποιες προσωπικές πληροφορίες ή πληροφορίες κίνησης του λογαριασμού του, πατώντας ένα σύνδεσμο (link)[8] που εμφανίζεται σ' αυτό. Μόλις ο παραλήπτης πατήσει το σύνδεσμο (link) θα κατευθυνθεί στον ψεύτικο διαδικτυακό τόπο (phishing site) όπου ό,τι πληροφορίες εισάγει θα συλλεχθούν για να χρησιμοποιηθούν στη συνέχεια εις βάρος του.[9]

Η απάτη αυτή θα μπορούσε να αντιμετωπιστεί με βάση τη διάταξη του άρθρου 386 ΠΚ, καθώς εδώ το θύμα λαμβάνει ένα ηλεκτρονικό μήνυμα που παρουσιάζει ψευδή στοιχεία ως αληθινά, δηλαδή αναφέρει ότι το πρόσωπο που το στέλνει είναι το αρμόδιο να ζητήσει τις αναγραφόμενες πληροφορίες. Με αυτά τα ψευδή στοιχεία το θύμα πείθεται να τελέσει μια πράξη, δηλαδή να δώσει τα ζητούμενα στοιχεία στον αποστολέα, ο οποίος τα χρησιμοποιεί για να βλάψει την περιουσία του. Επειδή ο σκοπός του δράστη είναι να αποκομίσει ο ίδιος ή κάποιος τρίτος παράνομο περιουσιακό όφελος, πραγματώνεται η νομοτυπική μορφή του 386 ΠΚ.[10]

Μαζική Υποκλοπή Στοιχείων (pharming)

Όπως στα ηλεκτρονικά μηνύματα-δολώματα έτσι και στη μαζική υποκλοπή στοιχείων (pharming) έχουμε απόπειρα κλοπής προσωπικών στοιχείων και κωδικών. Η διαφορά είναι ότι στη μαζική υποκλοπή στοιχείων δεν αποστέλλονται ηλεκτρονικά μηνύματα στα θύματα αλλά τα ίδια τα θύματα πληκτρολογώντας τη διεύθυνση μιας ιστοσελίδας ανακατευθύνονται αυτόματα σε μια άλλη επειδή έχει προηγηθεί παρέμβαση στο λογισμικό του υπολογιστή τους.[11]

Η ιστοσελίδα όπου ανακατευθύνονται εν αγνοία τους είναι φαινομενικά ίδια με αυτή που επιθυμούσαν αλλά κάθε πληροφορία που εισάγουν παρακολουθείται και στη συνέχεια χρησιμοποιείται εις βάρος τους.[12] Αυτό που συμβαίνει, είναι ότι στέλνονται ψευδείς πληροφορίες στους DNS servers (συστήματα ονομασίας πεδίων)[13] οι οποίοι παρέχουν πληροφορίες για τις διαδικτυακές τοποθεσίες μεταφράζοντας τη διεύθυνση που πληκτρολογούμε σε αριθμούς. Πρόκειται επομένως για μια μορφή απάτης της ηλεκτρονικής διεύθυνσης (απάτη του domain name).[14]

Αυτή η μορφή απάτης υπάγεται στη διάταξη του άρθρου 386Α ΠΚ αφού πρόκειται για το έγκλημα της απάτης με υπολογιστή.[15] Ο δράστης επηρεάζει στοιχεία του υπολογιστή με επέμβαση κατά την εφαρμογή του προγράμματος και ανακατευθύνει το θύμα σε μια λανθασμένη διεύθυνση. Αυτό που κάνει είναι να επεμβαίνει μεταβάλλοντας τη λειτουργία του προγράμματος και τη διαδικασία επεξεργασίας των δεδομένων[16] με επέμβαση στο λογισμικό του υπολογιστή.[17] Η ιστοσελίδα όπου ανακατευθύνεται το θύμα είναι πανομοιότυπη με την αληθινή και έτσι αυτό δεν έχει την δυνατότητα ελέγχου ώστε να αντιληφθεί τα δεδομένα που έχουν αλλαχθεί. Στη συνέχεια ο δράστης χρησιμοποιεί τα στοιχεία του θύματος για να προσποριστεί ο ίδιος ή κάποιος τρίτος παράνομο περιουσιακό όφελος ζημιώνοντάς το εκ προθέσεως. Σ' αυτό το σημείο πρέπει να σημειωθεί ότι πριν από την τέλεση της απάτης με υπολογιστή, ο δράστης τελεί όλες ή κάποια από τις παρακάτω αξιόποινες πράξεις: πλαστογραφία του άρθρου 216ΠΚ, παραβίαση απορρήτου του άρθρου 370Β, αθέμιτη πρόσβαση σε δεδομένα του άρθρου 370Γ ΠΚ και παραβίαση απορρήτου επικοινωνιών του άρθρου 10 Ν.3115/2003.[18]

Μη χρήση των κωδικών

Τόσο στη μαζική υποκλοπή στοιχείων όσο και στα παράνομα μηνύματα-δολώματα ανακύπτει η προβληματική του τι ισχύει όταν ο δράστης καταφέρει να αποκτήσει τους κωδικούς και τα στοιχεία του θύματος χωρίς στη συνέχεια να τα χρησιμοποιήσει.

Σ' αυτό το θέμα υπάρχουν αντικρουόμενες απόψεις. Αρχικά, υποστηρίζεται η άποψη ότι δεν έχουμε καν απόπειρα απάτης ή απάτης με υπολογιστή, αφού το θύμα δεν προβαίνει σε άμεση διάθεση της περιούσιάς του συνεπεία της οποίας να επέρχεται άμεση μείωσή της. Πρέπει δηλαδή ο ίδιος ο δράστης να προβεί σε μια πράξη, αυτή της χρήσης των κωδικών. Λείπει επομένως το στοιχείο της αμεσότητας που είναι απαραίτητο για την πλήρωση της αντικειμενικής υπόστασης της απάτης, αφού η απόκτηση των κωδικών ως προπαρασκευαστική πράξη είναι μη τιμωρητέα.[19]

Στη μαζική υποκλοπή στοιχείων και στα παράνομα μηνύματα-δολώματα ανακύπτει η προβληματική του τι ισχύει όταν ο δράστης αποκτήσει τους κωδικούς και τα στοιχεία του θύματος χωρίς στη συνέχεια να τα χρησιμοποιήσει.

Η άλλη άποψη υποστηρίζει ότι υφίσταται ολοκληρωμένο έγκλημα γιατί ο δράστης ανά πάσα στιγμή μπορεί να προβεί στην χρήση των κωδικών αυτών. Έχει προχωρήσει σε σημαντικό βαθμό η προσβολή της περιουσίας του θύματος, η οποία είναι άμεσα εξαρτημένη από τη συμπεριφορά του θύματος, οπότε υπάρχει και η αμεσότητα που είναι απαραίτητη για το έγκλημα της απάτης. Υπάρχει, δηλαδή, ενεστώσα βλάβη της περιουσίας του θύματος.[20]

Τέλος, υποστηρίζεται και μια ενδιάμεση άποψη σύμφωνα με την οποία σ' αυτή την περίπτωση έχουμε απλώς απόπειρα απάτης ή απάτης με υπολογιστή.

Προγράμματα Κρυφών Κλήσεων (Dialers)

Τα προγράμματα κρυφών κλήσεων (dialers) είναι μικρά προγράμματα[21] που δημιουργούν μια τηλεφωνική σύνδεση μέσω του modem (τηλεπικοινωνιακός διαμορφωτής-αποδιαμορφωτής ηλεκτρονικού υπολογιστή) και εγκαθίστανται στον υπολογιστή είτε εν αγνοία του χρήστη, είτε ενώ αυτός το έχει μερικώς πληροφορηθεί,[22] είτε εν γνώσει του. Στην τελευταία περίπτωση εγκατάστασης των dialers στον υπολογιστή εν γνώσει του χρήστη, αυτός αποδέχεται την χρήση τους συνεπώς δεν παρατηρείται κάποια παραβατική συμπεριφορά.[23] Κατά συνέπεια θα εξετάσουμε μόνο τις δύο πρώτες περιπτώσεις.

Η διαδικασία που ακολουθείται συνήθως για την εγκατάσταση του dialer ξεκινάει με την είσοδο του χρήστη σε μια ιστοσελίδα ή με το άνοιγμα ενός προσβεβλημένου ηλεκτρονικού μηνύματος. Τότε το πρόγραμμα κρυφών κλήσεων dialer αρχίζει να εγκαθίσταται στον υπολογιστή είτε απευθείας, χωρίς τη συναίνεση του χρήστη, είτε όταν αυτός εγκαθιστά ένα άλλο πρόγραμμα στο οποίο είναι μυστικά ενσωματωμένος ο dialer με τη μορφή «δούρειου ίππου».

Από τη στιγμή, λοιπόν, που εγκαθίσταται στον υπολογιστή το πρόγραμμα κρυφών κλήσεων, αλλάζει τις ρυθμίσεις του modem από μια συγκεκριμένη σύνδεση στο διαδίκτυο σε μία άλλη. Αποσυνδέει, δηλαδή, την υπάρχουσα κλήση της τηλεφωνικής γραμμής που συνδέει τον χρήστη με τον τοπικό παροχέα υπηρεσιών διαδικτύου και πραγματοποιεί κλήσεις υψηλής χρέωσης.[24]

Στο ελληνικό ποινικό δίκαιο διαφοροποιείται η αντιμετώπιση της απάτης ανάλογα με τον τρόπο που έγινε η εγκατάσταση του προγράμματος στον υπολογιστή του θύματος. Στην περίπτωση που ο δράστης πείσει το θύμα να κάνει την εγκατάσταση του προγράμματος στον υπολογιστή του, παρουσιάζοντάς του το αναληθές γεγονός ότι πρόκειται για ένα άλλο πρόγραμμα και αποκρύπτοντας το γεγονός ότι εγκαθίσταται στον υπολογιστή του και ένας -κρυμμένος- dialer που θα επιφέρει βλάβη στην περιουσία του, έχουμε απάτη της μορφής του 386 ΠΚ.

Στην περίπτωση που το πρόγραμμα κρυφών κλήσεων εγκαθίσταται εν αγνοία του θύματος έχουμε απάτη με υπολογιστή του άρθρου 386Α ΠΚ. Εδώ ο δράστης με επέμβαση κατά την εφαρμογή του προγράμματος και χωρίς τη μεσολάβηση πλάνης φυσικού προσώπου, επηρεάζει τα στοιχεία του υπολογιστή που αφορούν τις παραμέτρους σύνδεσης στο διαδίκτυο και έτσι βλάπτει την περιουσία του θύματος. Επεμβαίνει δηλαδή στο λογισμικό του υπολογιστή[25] μεταβάλλοντας τη λειτουργία του προγράμματος και την διαδικασία επεξεργασίας των δεδομένων της σύνδεσης στο διαδίκτυο, έχοντας σκοπό το δικό του περιουσιακό όφελος.

Στο ελληνικό ποινικό δίκαιο διαφοροποιείται η αντιμετώπιση της απάτης ανάλογα με τον τρόπο που έγινε η εγκατάσταση του προγράμματος στον υπολογιστή του θύματος.

Σ' αυτό το σημείο πρέπει να σημειωθεί πως το πρόβλημα των προγραμμάτων κρυφών κλήσεων έχει λυθεί σε ένα μεγάλο βαθμό και θεωρείται ξεπερασμένο έπειτα από την γενικευμένη χρήση των γρήγορων γραμμών τύπου DSL, οι οποίες δεν επιτρέπουν την χρήση τους.

Επίλογος

Απ' όλα τα παραπάνω γίνεται κατανοητό ότι η ραγδαία ανάπτυξη της ηλεκτρονικής εγκληματικότητας δημιουργεί πολλά προβλήματα στην καθημερινή χρήση του διαδικτύου. Επιπλέον, η συνεχής βελτίωση των ηλεκτρονικών μέσων και η πρόοδος της τεχνολογίας καθιστούν όλο και πιο δύσκολο τον εντοπισμό και την αντιμετώπιση των συνεχώς αυξανόμενων ηλεκτρονικών εγκλημάτων που δημιουργούνται. Γι' αυτό και είναι τόσο σημαντική η ενημέρωση των χρηστών του διαδικτύου για την ηλεκτρονική εγκληματικότητα και για τους τρόπους προστασίας τους.

1. http://www.consumeraffairs.govt.nz/scamwatch/nigerian.html, (ημερομηνία ανάκτησης περιεχομένου 5 Ιουνίου 2008).
2. http://en.wikipedia.org/wiki/419_fraud (ημερομηνία ανάκτησης περιεχομένου 5 Ιουνίου 2008).
3. Περιπτώσεις ομηρίας αναφέρονται στην ιστοσελίδα: http://www.fbi.gov/majcases/fraud/fraudschemes.htm (05/06/2008).
4. Άρθρο 386 §1 Ποινικού Κώδικα: Όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. και αν η ζημιά που προξενήθηκε είναι ιδιαίτερα μεγάλη με φυλάκιση τουλάχιστον δύο ετών.
5. http://www.antiphishing.org/ (06/06/2008)
6. Το θύμα δεν έχει τη δυνατότητα να διακρίνει τις διαφορές που υπάρχουν μεταξύ της αυθεντικής και της πλαστής ιστοσελίδας επειδή συνήθως οι πλαστές ιστοσελίδες δημιουργούνται με αντιγραφή των κωδικών HTML των αυθεντικών ιστοσελίδων οπότε είναι πανομοιότυπες με τις αυθεντικές. Βλ: http://www.forthnet.gr/templates/viewcontentTmCh.aspx?c=10009043 όπου η εταιρία forthnet στην προσπάθειά της να προστατέψει τους χρήστες της τους ενημερώνει, δίνοντας μεγάλη σημασίας στην ενημέρωση αυτή. Ανάλογη πολιτική ενημέρωσης ακολουθούν και άλλες εταιρίες.
7. Ν Κουράκη Τα οικονομικά εγκλήματα ΙΙ- ειδικό μέρος, 2007, Δ. Κιούπης Ηλεκτρονικά οικονομικά εγκλήματα σελ. 416.
8. Ο σύνδεσμος παραπέμπει τον χρήστη σε μια άλλη ιστοσελίδα αν τον επιλέξει με τον δείκτη.
9. http://www.fdic.gov/consumers/consumer/alerts/phishing.html, (06/06/2008).
10. Ε. Βασιλακάκη Ποινικά Χρονικά, ΝΖ/2007, Τα φαινόμενα "Phishing", "Pharming" και η ποινική τους αξιολόγηση, σελ. 860-862.
11. Βλ http://www.microsoft.com/hellas/athome/security/privacy/pharming.mspx όπου η microsoft, η εταιρία που παρέχει το λειτουργικό σύστημα που χρησιμοποιούν οι περισσότεροι χρήστες στους προσωπικούς τους Η/Υ στον κόσμο, ενημερώνει τους πελάτες της στην προσπάθειά της να τους προστατεύσει, πολιτική που ακολουθούν επίσης πολλές ακόμη εταιρίες. (ανάκτηση περιεχομένου στις 6/6/2008).
12. Οι δράστες αναζητούν προσωπικές και οικονομικές πληροφορίες από τα θύματά τους, όπως κωδικούς πιστωτικών καρτών και αριθμούς κοινωνικής ασφάλισης για να τις χρησιμοποιήσουν εν συνεχεία για δικό τους περιουσιακό όφελος.
13. Το Domain Name System ή DNS μεταφράζει διευθύνσεις URL (π.χ. τη διεύθυνση www.google.gr) σε μια διεύθυνση η οποία αποτελείται από αριθμούς (π.χ. 66.102.9.99).
14. http://en.wikipedia.org/wiki/Pharming (06/06/2008).
15. Άρθρο 368Α ΠΚ: «Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.»
16. Ν. Κουράκη, παρατηρήσεις σε Νομολογία ,Ποιν.Λόγος 2001, σελ.2592- Γ. Νούσκαλης , σελ.180. Χ. Μυλωνόπουλος, Ποινικό Δίκαιο Ειδικό Μέρος :Τα εγκλήματα κατά της περιουσίας σελ.599.
17. Χ. Μυλωνόπουλος, ό.π ,σελ.599.
18. Ν. Κουράκη, Τα οικονομικά εγκλήματα ΙΙ- ειδικό μέρος 2007, Δ. Κιούπης Ηλεκτρονικά οικονομικά εγκλήματα, σελ 418.
19. Ν. Κουράκη, Τα οικονομικά εγκλήματα ΙΙ- ειδικό μέρος 2007, Δ. Κιούπης Ηλεκτρονικά οικονομικά εγκλήματα, σελ 417.
20. Βλ. σχετικά Ε. Βασιλακάκη, Ποινικά Χρονικά, ΝΖ/2007, Τα φαινόμενα "Phishing", "Pharming" και η ποινική τους αξιολόγηση, σελ. 862,
21. Βλ. http://www.forthnet.gr/templates/viewcontentTmArt.aspx?p=102396. όπου η εταιρία forthnet ενημερώνει τους χρήστες της για τους dialers με σκοπό να τους προστατέψει. Ανάλογη πολιτική ενημέρωσης ακολουθούν και άλλες εταιρίες. (ανάκτηση περιεχομένου στις 6/6/2008).
22. Ν. Κουράκη, Τα οικονομικά εγκλήματα ΙΙ- ειδικό μέρος 2007, Δ. Κιούπης Ηλεκτρονικά οικονομικά εγκλήματα, σελ 415.
23. http://research.sunbelt -software.com/threatdisplay.aspx?name=DialerPlatform & threatid = 15015, (ανάκτηση περιεχομένου στις 7/6/2008).
24. http://www.pandasecurity.com/homeusers/security-info/glossary/#DIALER (ανάκτηση περιεχομένου στις 7/6/2008).
25. Ν. Κουράκη, Τα οικονομικά εγκλήματα ΙΙ- ειδικό μέρος, 2007, Δ. Κιούπης, Ηλεκτρονικά οικονομικά εγκλήματα σελ 415.