



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΣΧΟΛΗ ΕΠΙΣΤΗΜΗΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ
ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΕΞΕΛΙΞΗ
ΜΗΧΑΝΙΣΜΩΝ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ
ΤΡΙΤΩΝ ΣΤΟΝ ΠΑΓΚΟΣΜΙΟ ΙΣΤΟ

Ονοματεπώνυμο Βαλαβάνης Παναγιώτης

A.M. Π2012091

Τριμελής Επιτροπή : Τσώχου Αγγελική, Μάνος Μάγκος,

Βασίλειος Χρυσικόπουλος

Επόπτης Καθηγητής : Τσώχου Αγγελική

Κέρκυρα Μάιος 2019

Contents

Περίληψη	6
Abstract.....	7
Κεφάλαιο 1 ^ο : Προσωπικά δεδομένα και ιδιωτικότητα στο διαδίκτυο	8
Εισαγωγή	9
1.1. Ορισμοί	9
1.1.1. Ιδιωτικότητα	9
1.1.2. Προσωπικά δεδομένα.....	11
1.2. Διαχείριση προσωπικών δεδομένων	11
1.3. Τρόποι συλλογής προσωπικών δεδομένων απο το διαδίκτυο	12
1.3.1. HTTP Cookies	13
1.3.2. Flash cookies.....	15
1.3.3. ETags.....	15
1.3.4. Web-bugs	16
1.3.5. Clickstream Analytics.....	17
1.3.6. Τεχνικές που χρησιμοποιούν το αποτύπωμα.....	17
1.3.6.1. Οι παθητικοί μηχανισμοί αποτυπωμάτων	17
1.3.6.2. Οι ενεργητικοί μηχανισμοί αποτυπωμάτων.....	18
Κεφάλαιο 2 ^ο : Προστασία Προσωπικών Δεδομένων	19
2.1. Προστασία Προσωπικών Δεδομένων	20
2.1.1. Νομικό πλαίσιο.....	20
2.1.2. Προστασία Προσωπικών Δεδομένων στην Ελληνική πραγματικότητα	23
2.2. Μέτρα ασφαλείας για την Προστασία Προσωπικών Δεδομένων	24
2.2.1. Μέθοδοι ενίσχυσης της ιδιωτικότητας	25
2.2.1.1. Firewall	25
2.2.1.2. Κρυπτογράφηση.....	26
2.2.1.3. Πιστοποίηση αυθεντικότητας	27
2.2.1.4. Ψηφιακές Υπογραφές	28
2.2.2. Τρόποι ανίχνευσης των υποκλοπών.....	28
2.2.2.1. Ανίχνευση μέσω Λειτουργικών Συστημάτων	29
2.2.2.2. Χρήση προγραμμάτων ασφαλείας στο διαδίκτυο (Anti-Spyware).....	29
2.2.2.3. Τεχνολογίες ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies, PETs) ..	29
Κεφάλαιο 3 ^ο : Εξέλιξη μηχανισμών παρακολούθησης τρίτων στον Παγκόσμιο Ιστό	31

3.1. Εξέλιξη μηχανισμών παρακολούθησης τρίτων στον Παγκόσμιο Ιστό.....	31
3.1.1. Χρησιμοποιώντας μεταδεδομένα τηλεφώνου.....	32
3.1.2. Η παρακολούθηση μέσω GPS (Global Positioning System)	32
3.1.3. Μη συνειδητή συνεργασία του χρήστη	33
3.2. Ανάλυση τεχνικών προστασίας απο τις νέες μορφές διαδικτυακών υποκλοπών	34
3.2.1. Αποκλεισμός διαφημιστικών υπηρεσιών.....	35
3.2.2. Απόκρυψη της διεύθυνσης IP	36
3.2.3. Τροποποίηση των δεδομένων που αποστέλλονται μέσω του δικτύου.....	37
3.2.4. Αποκλεισμός cookies.....	37
3.2.5. DNT	37
3.2.6. Λειτουργία ιδιωτικής περιήγησης.....	38
3.2.7. Διαγραφή της προσωρινής μνήμης και του ιστορικού του προγράμματος περιήγησης.....	38
3.3. Phishing.....	38
3.3.1. Τύποι phishing40	
3.3.1.1. Phishing με κλώνους.....	40
3.3.1.2. Phishing τύπου Spear.....	40
3.3.1.3. Phishing μέσω τηλεφώνου41	
3.3.2. Τεχνικές ηλεκτρονικού "ψαρέματος" και μέτρα αντιμετώπισης.....	41
3.3.2.1. Πλαστογράφηση Email (Spoofing).....	41
3.3.2.2. Web Spoofing	43
3.3.2.3. Pharming	45
3.3.2.4. Η δηλητηρίαση των DNS και της προσωρινής μνήμης DNS (DNS spoofing).....	45
3.3.2.5. Κακόβουλο λογισμικό	45
3.3.2.6. Phishing μέσω εγγράφων PDF	46
3.3.3. Πρόσθετα προληπτικά μέτρα.....	47
3.3.4. Εκπαίδευση χρηστών.....	47
3.3.5. Ομάδες κατά της απάτης.....	49
3.4. Το μέλλον της παρακολούθησης.....	49
3.4.1. Η Ομάδα Εργασίας Cookie	49
3.4.2. Google AdID	49
3.4.3. Αναγνωριστικό της συσκευής από τη Microsoft51	
3.4.4. Εργαστήριο Διαφάνειας Δεδομένων51	
3.5. Στατιστικά στοιχεία51	

Βιβλιογραφία	56
---------------------------	-----------

Περίληψη

Η ιδιωτικότητα φαίνεται να είναι η Αχίλλειος πτέρνα του σημερινού διαδικτύου. Οι περισσότερες διαδικτυακές υπηρεσίες κάνουν συνεχείς προσπάθειες για να παρακολουθούν τους χρήστες και να λαμβάνουν όσο το δυνατόν περισσότερες προσωπικές πληροφορίες από τα πράγματα που εκείνοι αναζητούν, τους ιστότοπους που επισκέπτονται, τους ανθρώπους που επικοινωνούν και τα προϊόντα που αγοράζουν. Αυτές οι πληροφορίες χρησιμοποιούνται ως επί το πλείστον για εμπορικούς σκοπούς. Παρόλο που πολλοί χρήστες γνωρίζουν ήδη τους κινδύνους για την ιδιωτική τους ζωή που συνδέονται με τη χρήση διαδικτυακών υπηρεσιών, οι συγκεκριμένες μέθοδοι και οι τεχνολογίες που χρησιμοποιούνται για την παρακολούθηση τους είναι πολύ λιγότερο γνωστές. Στην παρούσα εργασία, γίνεται μια ανασκόπηση της υπάρχουσας βιβλιογραφίας σχετικά με τις μεθόδους που χρησιμοποιούν οι διάφορες διαδικτυακές υπηρεσίες για την παρακολούθηση των χρηστών, καθώς και για τους σκοπούς, τις επιπτώσεις τους και τις δυνατότητες άμυνας του χρήστη. Γίνεται αναφορά σε κύριες μεθόδους που χρησιμοποιούνται για την παρακολούθηση των χρηστών, οι οποίες βασίζονται σε δεδομένα αποθήκευσης, σε διαδικτυακά αποτυπώματα και άλλες προσεγγίσεις. Παρουσιάζεται επίσης ο τρόπος με τον οποίο οι χρήστες μπορούν να εντοπιστούν στο διαδίκτυο και να συνδεθούν με τα πραγματικά τους ονόματα, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου, τους αριθμούς τηλεφώνου ή ακόμη και τις διευθύνσεις των οδών που διαμένουν. Γίνεται αναφορά στο λόγο για τον οποίο χρησιμοποιείται η παρακολούθηση και στις πιθανές επιπτώσεις για τους χρήστες. Για κάθε μια από τις μεθόδους παρακολούθησης, παρουσιάζονται πιθανές άμυνες. Τέλος, παρουσιάζονται οι μελλοντικές τάσεις στον εντοπισμό των χρηστών που ενδέχεται να δημιουργήσουν σημαντικές απειλές για το ιδιωτικό τους απόρρητο.

Abstract

The privacy seems to be the weak point of the Internet in our days. Most web services make continuous efforts to track users and take as much personal information of the things they search for, the sites they visit, the people they communicate with and the products they buy. This information is used mostly for commercial purposes. Although many users are already aware of the dangers for their private life associated with the use of web services, the specific methods and technologies used for their tracking is much less known. In this study, we present a review of the existing literature on the methods used by different online services to track users. Also, we try to point out the purpose of web tracking and its impact to the user's private life and we refer to the user's defense capabilities. We refer to web tracking mechanisms, based either on the data stored or in web fingerprints and other approaches. We also present the way in which users can be tracked online and connect with their real names, email addresses, phone numbers or even addresses of the street they live in. For each tracking method, we present possible defenses. Finally, we present the future trends in tracking users which may pose significant threats to their privacy.

Κεφάλαιο 1°. Προσωπικά δεδομένα και ιδιωτικότητα στο διαδίκτυο

Εισαγωγή

Στην σημερινή εποχή, το διαδίκτυο έχει γίνει αναπόσπαστο κομμάτι στις ζωές των ανθρώπων. Η καθημερινότητα απαρτίζεται σε μεγάλο βαθμό από συσκευές και καταναλωτικά αγαθά που προέρχονται από εταιρείες και οργανισμούς πολύ μακριά από τον τόπο διαμονής του εκάστοτε χρήστη. Η άνοδος του βιωτικού επιπέδου των λαών καθώς και η ανάγκη για διευκόλυνση καθημερινών αναγκών, βοήθησε στην ραγδαία εξέλιξη του τρόπου αλληλεπίδρασης των χρηστών του διαδικτύου. Η ανάπτυξη όμως αυτή, εκτός από πολύ ισχυρά πλεονεκτήματα, επέφερε και ορισμένες επιπτώσεις πάνω στο θέμα της ιδιωτικότητας και της ασφάλειας των προσωπικών δεδομένων. Στο κεφάλαιο αυτό δίνονται οι ορισμοί της ιδιωτικότητας και των προσωπικών δεδομένων και στην συνέχεια αναφέρονται και αναλύονται οι τρόποι διαχείρισης και συλλογής των προσωπικών δεδομένων.

1.1. Ορισμοί

Παρακάτω παρατίθενται οι ορισμοί της ιδιωτικότητας και των προσωπικών δεδομένων, δύο σημασίες που θα βοηθήσουν στην καλύτερη κατανόηση της πτυχιακής εργασίας

1.1.1. Ιδιωτικότητα

Η σημασία της λέξης ιδιωτικότητα είναι πολύ δύσκολο να δωθεί απλά με έναν ορισμό. Η κοινωνία και η εποχή στην οποία ανήκει το άτομο που την χρησιμοποιεί, ή ακόμη και το ίδιο το άτομο, αποτελούν παράγοντες που επηρεάζουν την σημασία της λέξης αυτής. Για παράδειγμα, αυτό που θεωρείται ιδιωτικό από ένα άτομο υπάρχει περίπτωση να διαφέρει από αυτό που πρεσβεύει ο νόμος ως ιδιωτικό (Konvitz, 1966). Αρκετοί αναγνωρισμένοι νομικοί προσπάθησαν να δημιουργήσουν έναν ολοκληρωμένο ορισμό της λέξης «ιδιωτικότητα» αλλά λόγω του μεγάλου εύρους της σημασίας της και των αδιάλειπτων αλλαγών στα στοιχεία που ανήκουν στην ιδιωτική σφαίρα του εκάστοτε ατόμου, οι περισσότεροι από αυτούς τους ορισμούς παρουσιάζουν μόνο μια πτυχή της λέξης.

Ο Καναδός δικηγόρος Brian Dickson (1916-1998), επικεφαλής του Ανώτατου Δικαστηρίου του Καναδά (1984-1990), προσπάθησε να προσεγγίσει τον όρο «ιδιωτικότητα» από την νομική σκοπιά. Σύμφωνα με τον Dickson (Duarte, 1990), ιδιωτικότητα μπορεί να οριστεί ως το

δικαίωμα του ατόμου να καθορίσει πότε, πώς και σε ποιό βαθμό θα εκθέσει/δημοσιοποιήσει τα προσωπικά του στοιχεία. Βέβαια, το άτομο πρέπει να γνωρίζει εξ' αρχής ότι το κράτος επιτρέπεται να παραβιάσει αυτό το δικαίωμα και να προβεί σε παρακολούθηση και καταγραφή ιδιωτικών επικοινωνιών, εφόσον κρίνει ότι οι συζητήσεις αυτές συνδέονται με την διάπραξη αδικήματος.

Η ανάγκη για ιδιωτικότητα εκφράστηκε για πρώτη φορά από τον Πλάτωνα (Jowett, 2015) σε μία εποχή όπου όλη η ζωή των ανθρώπων καθοριζόταν αποκλειστικά από το κράτος χωρίς να υπάρχει χώρος για οποιαδήποτε αυτονομία και ατομική ελευθερία. Έτσι, οι ζωές των ατόμων ήταν δομημένες με συγκεκριμένο τρόπο ούτως ώστε να εξυπηρετούνται επαρκώς τα δημόσια συμφέροντα. Έπειτα, κατά τον Μεσαίωνα η ιδιωτικότητα ήταν άρρητα συνδεδεμένη με την έννοια της κοινότητας. Το κάθε άτομο έπρεπε να λειτουργεί σύμφωνα με τους κανόνες της κοινότητας και να παρακολουθείται συνεχώς από τα υπόλοιπα μέλη της. Ριζική αλλαγή στον τρόπο αντιμετώπισης της ιδιωτικής ζωής των ανθρώπων επήλθε τον 19^ο αιώνα με την διανοητική εξέλιξη των ατόμων και την ανάπτυξη της οικονομίας (Solove, 2002). Η εμφάνιση των εφημερίδων και των κουτσομπολίστικων περιοδικών ήταν το εφαλτήριο για τους Samuel Warren και Louis Brandeis για την συγγραφή του *The Right to Privacy* το 1890 (Bratman, 2002), ενός από τα πιο διάσημα άρθρα που αφορά τις απειλές από την παραβίαση της ιδιωτικότητας και την ανάγκη για προστασία της ιδιωτικής ζωής.

Από τα μέσα του 20^{ου} αιώνα πολλές χώρες ξεκίνησαν να αναγνωρίζουν το δικαίωμα στην ιδιωτικότητα ως θεμελιώδες ανθρώπινο δικαίωμα και το καθιέρωσαν με την υιοθέτηση των σχετικών νομικών εγγράφων. Η μη ύπαρξη όμως συγκεκριμένων ευρέως αποδεκτών οδηγιών για τον ακριβή ορισμό της ιδιωτικότητας, είχε ως αποτέλεσμα την διαφοροποίηση της νομολογίας σε κάθε χώρα (Niemietz v. Germany, 1992), με τα δικαστήρια να καθορίζουν τις λεπτομέρειες των νόμων περι ιδιωτικής ζωής.

Με την μεγάλη επανάσταση στην τεχνολογία και την εμφάνιση του διαδικτύου ξεκίνησε να αμφισβητείται εάν το δικαίωμα στην ιδιωτικότητα είναι ικανό να εξασφαλίσει την προστασία της ιδιωτικής ζωής. Η διαπίστωση αυτή οδήγησε στην διεκδίκηση ενός νέου, ξεχωριστού δικαιώματος, του δικαιώματος στην προστασία προσωπικών δεδομένων.

1.1.2. Προσωπικά δεδομένα

Σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία αναφέρεται σε ένα άτομο ή διαφορετικές πληροφορίες που συλλέγονται μαζί και μπορούν να οδηγήσουν στην αναγνώριση ενός συγκεκριμένου ατόμου.

Τέτοια δεδομένα είναι:

- όλα τα στοιχεία αναγνώρισης όπως όνομα, επώνυμο, ηλικία, οικογενειακή κατάσταση κλπ
- τα φυσικά χαρακτηριστικά όπως εκπαίδευση, εργασία, εργασιακή συμπεριφορά κλπ
- οικονομική κατάσταση όπως περιουσιακά στοιχεία και έσοδα καθώς επίσης και
- αγαπημένες δραστηριότητες, συνήθειες, ενδιαφέροντα.

Ευαίσθητα προσωπικά δεδομένα θεωρούνται τα δεδομένα πεποιθήσεων, αξιόποινων πράξεων, δεδομένα που αναφέρονται σε φυλετική ή εθνική προέλευση και προστατεύονται από τους Νόμους κάθε κράτους με αυστηρές ρυθμίσεις σε σχέση με τα προσωπικά δεδομένα που αναφέρθηκαν παραπάνω.

Τα ψευδώνυμα δεδομένα μπορεί να καθιστούν πιο δύσκολη την ταυτοποίηση προσώπων αλλά εξακολουθούν να αποτελούν προσωπικά δεδομένα.

Εδώ πρέπει να τονιστεί ότι οι πληροφορίες σχετικά με έναν αποθανόντα καθώς και οι πληροφορίες για εταιρείες ή δημόσιες αρχές, δεν αποτελούν προσωπικά δεδομένα.

1.2. Διαχείριση προσωπικών δεδομένων

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, για να γίνει επεξεργασία και συλλογή δεδομένων τρίτων, θα πρέπει να υπάρχει η γραπτή συγκατάθεσή τους. Αρχικά θα πρέπει να γίνει ορισμός του σκοπού της συλλογής δεδομένων καθώς και του πεδίου συλλογής (Γενικός Κανονισμός για την Προστασία των Δεδομένων, 2016). Το άτομο που θα διαχειριστεί τα δεδομένα θα πρέπει να είναι πολύ καλός γνώστης της νομοθεσίας και να έχει στην κατοχή του όλα τα αποδεικτικά στοιχεία συμμόρφωσης για να τα προσκομίσει σε περίπτωση ελέγχου από τις εποπτικές αρχές.

Όσον αφορά τις εταιρείες, όταν ένα άτομο επισκέπτεται έναν ιστότοπο για να δει ένα προϊόν ή να κάνει μία αγορά, αυτομάτως θα πρέπει να ενημερώνεται ότι η εταιρεία θέλει να κάνει χρήση κάποιων δεδομένων του και να ζητείται η συγκατάθεσή του. Η φόρμα συγκατάθεσης θα πρέπει να έχει κάποια συγκεκριμένα χαρακτηριστικά σύμφωνα με τον κανονισμό:

- να είναι συνοπτική και συγκεκριμένη, να μπορεί να αναγνωστεί εύκολα και να γίνει κατανοητή
- να εξηγείται πλήρως ποιά δεδομένα συλλέγονται, ο λόγος για τον οποίο συλλέγονται καθώς και το χρονικό πλαίσιο για το οποίο τα δεδομένα θα παραμένουν αποθηκευμένα στα αρχεία της εταιρείας
- να περιγράφει ακριβώς την εταιρεία και τις λειτουργίες της και να συμπεριλαμβάνεται το όνομα της επιχείρησης καθώς και τα ονόματα οποιωνδήποτε σχετικών τρίτων οντοτήτων
- να ενημερώνει τους ενδιαφερόμενους ότι έχουν την δυνατότητα ανα πάσα στιγμή να αποσύρουν την συγκατάθεσή τους.

Αναλυτικότερα, το νομικό πλαίσιο είναι διαθέσιμο στο δεύτερο κεφάλαιο.

Όταν υπάρχει πλήρης ενημέρωση πάνω στον τρόπο με τον οποίο χρησιμοποιούνται τα προσωπικά δεδομένα τότε ο χρήστης/καταναλωτής νοιώθει μεγαλύτερη ασφάλεια όσων αφορά την ιδιωτικότητά του. Αυτό συμβάλει στην οικοδόμηση εμπιστοσύνης με τους διάφορους οργανισμούς που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα (Broad, 2016). Η ανάλυση των δεδομένων επιτρέπει την ανάπτυξη νέων προϊόντων και υπηρεσιών αλλά και την αποτελεσματικότερη χρήση των ήδη υπάρχοντων. Διευκολύνει την περιήγηση των χρηστών του διαδικτύου και δίνει στους καταναλωτές όσο το δυνατόν καλύτερη εξατομικευμένη ενημέρωση.

1.3. Τρόποι συλλογής προσωπικών δεδομένων απο το διαδίκτυο

Ένα απο τα πιο σημαντικά βήματα σε μία έρευνα αγοράς είναι η συλλογή δεδομένων (Ochoa, 2017). Ξεκινάει με τον καθορισμό των ερευνητικών στόχων και τελειώνει εφόσον ολοκληρωθεί η λήψη των δεδομένων που χρειάζονται να αναλυθούν για την εξαγωγή συμπερασμάτων (Ochoa, 2017). Υπάρχουν αρκετοί τρόποι οι οποίοι επιτρέπουν την συλλογή προσωπικών δεδομένων απο το διαδίκτυο (Ochoa, 2017). Οι περισσότερες όμως εταιρείες έχουν δημιουργήσει αρκετά ύπουλες τεχνικές στην προσπάθειά τους να κατανοήσουν καλύτερα την συμπεριφορά των καταναλωτών online και offline.

Ο πιο συνηθισμένος τρόπος παρακολούθησης χρηστών στο διαδίκτυο είναι η αποθήκευση μοναδικών αναγνωριστικών σε κάποιο μη εμφανές σημείο στον υπολογιστή τους (Li et al, 2015). Αυτά μπορούν στη συνέχεια, ακολουθώντας τους χρήστες στην περιήγησή τους στον ιστό, να απαντήσουν σε πιθανά ερωτήματα (queries) οποιασδήποτε οντότητας που θα ζητήσει την πληροφορία αυτή. Η διαφορά με την αποτύπωση δακτυλικών αποτυπωμάτων είναι ότι η

αποτύπωση δακτυλικών αποτυπωμάτων δεν αποθηκεύει ένα αναγνωριστικό τοπικά στον υπολογιστή του χρήστη (Li et al, 2015) και ότι βασίζεται στα χαρακτηριστικά ενός χρήστη (Li et al, 2015) όπως η διεύθυνση IP του. Η παρακολούθηση με χρήση δεδομένων αποθήκευσης λειτουργεί με αναγνωριστικά που έχουν δημιουργηθεί από εκείνον που ενδιαφέρεται να παρακολουθήσει (Li et al, 2015) και δεν έχουν καμία σχέση με τα συγκεκριμένα χαρακτηριστικά του χρήστη.

1.3.1. HTTP Cookies

Ένας από τους πιο διαδεδομένους τρόπους συλλογής δεδομένων και παρακολούθησης των χρηστών είναι η χρήση των cookies HTTP, τα οποία συχνά αναφέρονται μόνο ως "Cookies". Τα προγράμματα περιήγησης βασίζονται στο πρωτόκολλο HTTP (πρωτόκολλο μεταφοράς υπερκειμένου) για τη μεταφορά πληροφοριών (Li et al, 2015). Το HTTP, ωστόσο, είναι ένα πρωτόκολλο κατά τη λειτουργία του οποίου δεν διατηρούνται πληροφορίες σύνδεσης ούτε από τον διακομιστή ούτε από τον πελάτη. Αυτό έκανε αδύνατη την ύπαρξη κάποιων υπηρεσιών την ώρα της περιήγησης στην οποία χρειάζεται να διατηρηθεί μια κατάσταση (όπως ο συνδεδεμένος χρήστης). Ως λύση, έγινε δυνατή η αποθήκευση μικρών αρχείων κειμένου (έως 4KB) στους υπολογιστές των χρηστών, στον οποίο αποθηκεύεται η κατάσταση του προγράμματος περιήγησης (Barth, 2011). Αυτά τα αρχεία κειμένου αποστέλλονται με κάθε μήνυμα αίτησης HTTP. Στην ουσία τα cookies είναι κάποια πολύ μικρά αρχεία τα οποία αποθηκεύονται στον υπολογιστή αυτόματα όταν κάποιος επισκέπτεται μία ιστοσελίδα. Τα Cookies χρησιμοποιούνται κυρίως για την βελτίωση της online εμπειρίας των χρηστών. Λειτουργούν σαν ένα είδος μνήμης που διαφυλλάσει τις προτιμήσεις του χρήστη και παρέχει στοχευμένο περιεχόμενο ή διαφημίσεις σχετικές με τις προηγούμενες επιλογές του (Kristol, 2001). Υπάρχει όμως περίπτωση τα δεδομένα αυτά να χρησιμοποιηθούν και από διαφημιστές που παρέχουν διαφημίσεις στους ιστότοπους τους οποίους επισκέπτεται ο χρήστης με αποτέλεσμα ο χρήστης να παρακολουθείται παθητικά (Hoofnagle et al, 2010) καθώς η πληροφόρησή του πάνω σε τέτοιου είδους ζητήματα είναι πολύ περιορισμένη αν όχι πλήρως ελλιπής.

Τα Cookies με ημερομηνία λήξης αποθηκεύονται στον υπολογιστή των χρηστών μέχρι να περάσει η ημερομηνία λήξης ή μέχρι να διαγραφεί το Cookie. Όταν δεν έχει οριστεί ημερομηνία λήξης κατά τη ρύθμιση του cookie, θεωρείται ως ένα cookie περιόδου σύνδεσης. Αυτό σημαίνει

ότι το Cookie θα διαγραφεί μόλις ολοκληρωθεί η περίοδος λειτουργίας του προγράμματος περιήγησης. Άλλες λέξεις-κλειδιά για τα Cookies είναι Domain, Secure και HttpOnly. Αυτά καθορίζουν τον τομέα στον οποίο ανήκει το cookie (και ως εκ τούτου σε ποιους διακομιστές μπορεί να αποστέλλεται το Cookie), αν το cookie μπορεί να αποσταλεί μόνο μέσω ασφαλούς σύνδεσης και εάν το Cookie μπορεί να συνδεθεί ή όχι με δέσμες ενεργειών που εκτελεί η πλευρά του πελάτη.

Τα HTTP cookies μπορούν να είναι είτε "πρώτου επιπέδου" είτε "τρίτου επιπέδου". Τα Cookies πρώτου επιπέδου είναι Cookies που ορίζονται από την σελίδα που επισκέπτεται απευθείας ο χρήστης, ενώ τα Cookies τρίτου επιπέδου, ορίζονται από σελίδες που επισκέπτεται έμμεσα, για παράδειγμα όταν μια ιστοσελίδα φορτώνει έναν πόρο από μια άλλη.

Η εικόνα που ακολουθεί είναι από το δείχνει με πολύ απλό τρόπο τη βασική ιδέα πίσω από τη λειτουργία των Cookies (Rokitta, 2015).



Rokitta Christian, 2015, APEX & Cookie Monster, Slideshare

Τα Cookies HTTP μπορούν να χρησιμοποιηθούν ως εργαλείο παρακολούθησης με πολλούς τρόπους. Μπορούν να χρησιμοποιηθούν μόνο τους, τοποθετώντας ένα Cookie με ένα αναγνωριστικό στη συσκευή του χρήστη όταν επισκέπτεται μια ιστοσελίδα ή μπορούν να χρησιμοποιηθούν σε συνδυασμό με άλλες τεχνικές, για παράδειγμα τον συγχρονισμό των cookies, την ανάκτηση των cookies και τις ιστοσελίδες συγκέντρωσης δεδομένων παρακολούθησης «aggregators» όπως ονομάζονται στην αγγλική ορολογία (Schmucker, 2011). Ο συγχρονισμός των Cookies σημαίνει ότι τα Cookies από έναν τομέα μεταβιβάζονται σε ένα άλλο. Τα επαναλαμβανόμενα cookies επαναφέρουν τα διαγραφμένα Cookies από άλλη θέση αποθήκευσης, στην οποία αποθηκεύτηκε το ίδιο αναγνωριστικό. Ορισμένες σελίδες παρακολούθησης χρησιμεύουν ως aggregators για άλλες υπηρεσίες παρακολούθησης.

Δεν χρησιμοποιούνται όλα τα cookies HTTP για σκοπούς παρακολούθησης. Οι Li και άλλοι έχουν δείξει ότι τα Cookies εντοπισμού και μη εντοπισμού μπορούν να διακριθούν με πολύ υψηλή ακρίβεια (Li et al, 2015).

1.3.2. Flash cookies

Τα Flash cookies χρησιμοποιούνται συνήθως σε διαφημίσεις ιστότοπων και βίντεο. Όπως τα HTTP cookies, τα Flash cookies αποθηκεύουν πληροφορίες στον υπολογιστή του τελικού χρήστη. Οι πληροφορίες επιτρέπουν σε έναν ιστότοπο να αναγνωρίζει το πρόγραμμα περιήγησης του πελάτη όταν επιστρέφει (Schmucker, 2011). Τα Flash cookies περιέχουν μερικές φορές τις ίδιες πληροφορίες που περιέχουν τα HTTP cookies, αλλά αποθηκεύουν επίσης πληροφορίες, όπως το σημείο στο οποίο σταμάτησε να παίζει το βίντεο του χρήστη ή η διαφήμιση. Τα τοπικά αυτά αρχεία έχουν επέκταση αρχείου .sol.

Σε αντίθεση με τα HTTP cookies που αποθηκεύονται με τα αρχεία του προγράμματος περιήγησης, τα Flash cookies αποθηκεύονται σε ξεχωριστό αρχείο Adobe και ενδέχεται να πρέπει να διαχειρίζονται και να διαγράφονται ξεχωριστά από τις ρυθμίσεις του Adobe Flash player (Schmucker, 2011). Πολλοί τελικοί χρήστες δεν γνωρίζουν ότι υπάρχουν Flash cookies και δεν έχουν ιδέα ότι όταν διαγράφουν τα HTTP cookies του HTTP, τα Flash cookies θα μπορούσαν να παραμείνουν ανεπηρέαστα και να χρησιμοποιηθούν για την αναδημιουργία διαγραμμένων HTTP cookies. Η διαδικασία αυτή, η οποία ονομάζεται respawning, είναι εξαιρετικά αμφιλεγόμενη, διότι διευκολύνει την παρακολούθηση διαδικτυακών περιηγητών και δημιουργεί ανησυχίες για την προστασία της ιδιωτικής ζωής όταν η χρήση των Flash cookies δεν αποκαλύπτεται στην πολιτική απορρήτου ενός ιστοτόπου.

Η Adobe έχει κάνει αλλαγές στο Flash για να αποθαρρύνει το respawning των Flash cookies και έχει ενσωματώσει πληροφορίες στον ιστοχώρο της σχετικά με τη διαχείριση των Flash cookies. Η εταιρεία συνεργάζεται επίσης με μεγάλα προγράμματα περιήγησης για να επιτρέπει στους τελικούς χρήστες να διαχειρίζονται τα cookies μέσω των ρυθμίσεων του προγράμματος περιήγησης, με μια πρόσθετη διεπαφή API (Schmucker, 2011).

Μια άλλη διαφορά μεταξύ των Flash cookies και των αντίστοιχων HTTP είναι ότι τα Flash cookies δεν λήγουν από προεπιλογή. Στην πραγματικότητα, δεν έχουν καθόλου ημερομηνία λήξης. Αυτό σημαίνει ότι τα Flash LSOs (Local Storage Objects) παραμένουν στον υπολογιστή του χρήστη μέχρι να διαγραφούν.

1.3.3. ETags

Τα ETags είναι μια μέθοδος που χρησιμοποιείται από κάποιους ιδιοκτήτες ιστότοπων για την καταστρατήγηση της επιλογής των χρηστών για την παρακολούθηση και αποτελούν μια ενδιαφέρουσα

εικόνα του τρόπου με τον οποίο λειτουργεί η παρακολούθηση. Για να εντοπιστεί ένας χρήστης, ένας ιστότοπος πρέπει να τοποθετήσει μια πληροφορία στο σύστημα του συγκεκριμένου χρήστη για να τα αναγνωρίσει (Davis, 2014). Όταν ο χρήστης επισκέπτεται για πρώτη φορά μια σελίδα, ο διακομιστής στέλνει τα ζητούμενα δεδομένα μαζί με έναν μοναδικό αριθμό ταυτοποίησης - συχνά σε ένα cookie, το οποίο είναι απλά ένα αρχείο κειμένου (Davis, 2014).

Τα ETags αποτελούν μέρος του HTTP, του πρωτοκόλλου με το οποίο οι πληροφορίες μεταδίδονται από το διακομιστή στο πρόγραμμα περιήγησης. Υπάρχουν για να βοηθήσουν τα προγράμματα περιήγησης να αποφεύγουν να φορτώνουν τα ίδια δεδομένα επανειλημμένα (Davis, 2014). Εάν επισκεφτεί ένας χρήστης μια ιστοσελίδα με μια εικόνα, θα γίνει λήψη και αποθήκευση στον υπολογιστή του (Davis, 2014). Εάν η εικόνα αυτή δεν αλλάζει ποτέ, δεν χρειάζεται να την κατεβάσει ξανά, αλλά το πρόγραμμα περιήγησης χρειάζεται κάποιον τρόπο για να καθορίσει εάν η εικόνα έχει αλλάξει πριν τη μεταφορτώσει. Όταν η εικόνα αποστέλλεται για πρώτη φορά, ο διακομιστής μπορεί να στείλει ένα ETag μαζί με αυτό, το οποίο αποθηκεύει το πρόγραμμα περιήγησης (Avenson et al, 2011). Το ETag είναι απλά ένας αριθμός σε ένα πεδίο κεφαλίδας HTTP που αναγνωρίζει μια μοναδική έκδοση της εικόνας. Αν η εικόνα παραμένει η ίδια, το ίδιο ισχύει και για το ETag. Όταν ο επισκέπτης επιστρέψει στη σελίδα, ο περιηγητής μπορεί να στείλει τον αριθμό ETag πίσω με μια ερώτηση που ρωτά εάν το τρέχον ETag στον διακομιστή ταιριάζει με αυτό που έχει αποθηκευτεί. Ο διακομιστής μπορεί στη συνέχεια να απαντήσει με ένα μήνυμα "δεν άλλαξε" και το πρόγραμμα περιήγησης θα χρησιμοποιήσει την εικόνα που είχε λάβει προηγουμένως (Avenson et al, 2011). Αν το ETag είναι διαφορετικό, τότε το πρόγραμμα περιήγησης κατεβάζει τη νέα έκδοση της εικόνας. Χωρίς να χρειαστεί ο χρήστης να κάνει λήψη των ίδιων δεδομένων περισσότερο από μία φορά, εξοικονομεί εύρος ζώνης και καλύτερη ταχύτητα φόρτωσης (Davis, 2014).

Τα ETags είναι ένας μοναδικός αριθμός που μπορεί να αναγνωρίσει ένα πρόγραμμα περιήγησης και στέλνονται αυτόματα σε ένα διακομιστή όταν ζητούν έναν συγκεκριμένο πόρο, ο οποίος μπορεί να είναι μια μικροσκοπική εικόνα. Το ETag μπορεί να πληκτρολογηθεί σε μια καταχώρηση βάσης δεδομένων που περιέχει προηγούμενες συνήθειες περιήγησης με τον ίδιο τρόπο όπως και οι πληροφορίες που περιέχονται σε ένα cookie.

Οι ETags είναι ένα ενδιαφέρον παράδειγμα του τρόπου με τον οποίο η τεχνολογία που εφευρέθηκε με ένα πράγμα στο μυαλό μπορεί να τεθεί σε λειτουργία εντελώς ακούσια.

1.3.4. Web-bugs

Τα Web-bugs γνωστά και ως Web beacon (Gilbert, 2008), είναι πολύ μικρά αρχεία κώδικα που τοποθετούνται σε έναν ιστότοπο ή σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου για να ελέγχουν την συμπεριφορά των χρηστών. Σε αντίθεση με τα "Cookies" δεν αποθηκεύεται στον

υπολογιστή και ούτε ζητείται η συναίνεση του χρήστη για την ύπαρξή του. Είναι αόρατο απο το άτομο που κάνει την περιήγησή του στην ιστοσελίδα και για να το εντοπίσει κάποιος, θα πρέπει να έχει εξειδικευμένες γνώσεις. Αν και τα Web-bugs λειτουργούν ενάντια στους κανονισμούς προστασίας δεδομένων, πολλοί παραδέχονται ότι έχουν άκρως θετική χρήση εντοπίζοντας παραβιάσεις πνευματικών δικαιωμάτων στο διαδίκτυο.

1.3.5. Clickstream Analytics

Τέλος με το Clickstream Analytics (ανάλυση Clickstream) συλλέγονται και αναλύονται δεδομένα σχετικά με τις ιστοσελίδες που επισκέπτεται ο χρήστης και την σειρά που ακολουθεί στην περιήγησή του. Η ανάλυση των δεδομένων αυτών επιτρέπουν στις εταιρείες που δραστηριοποιούνται μέσω του διαδικτύου να διαμορφώνουν κατάλληλα τις ιστοσελίδες τους για να είναι προσίτες και προτιμώμενες απο τους χρήστες (Tucker, 2010).

1.3.6. Τεχνικές που χρησιμοποιούν το αποτύπωμα

Η παρακολούθηση μπορεί επίσης να πραγματοποιηθεί χωρίς να αποθηκεύονται αναγνωριστικά στη συσκευή ενός χρήστη (Eckersley, 2010). Η πιο συνηθισμένη μέθοδος γι' αυτό είναι η αποκαλούμενη αποτύπωση δακτυλικών αποτυπωμάτων (Eckersley, 2010). Αυτό το αποτύπωμα μπορεί να γίνει με δύο τρόπους: ενεργητικό ή παθητικό (Eckersley, 2010). Η παθητική λήψη δακτυλικών αποτυπωμάτων γίνεται με την ανάλυση των πληροφοριών που αποστέλλονται μέσω του δικτύου σε κάθε περίπτωση, χωρίς να ζητούνται ορισμένες πληροφορίες (Eckersley, 2010). Για παράδειγμα, η διεύθυνση IP μιας συσκευής είναι πάντα ορατή εάν αυτή η συσκευή συνδέεται με μια υπηρεσία ιστού (Eckersley, 2010). Το ενεργητικό αποτύπωμα, από την άλλη πλευρά, διερευνά ενεργά τη συσκευή για περισσότερες πληροφορίες. Αυτό περιλαμβάνει το λειτουργικό σύστημα και τις εγκατεστημένες γραμματοσειρές μιας συσκευής (Eckersley, 2010).

1.3.6.1. Οι παθητικοί μηχανισμοί αποτυπωμάτων

Όπως αναφέρθηκε παραπάνω, οι παθητικοί μηχανισμοί αποτυπωμάτων από μια υπηρεσία ιστού παρατηρούν την κίνηση του δικτύου δημιουργώντας ένα μοναδικό αναγνωριστικό για το συνδυασμό χρήστη / συσκευής (Eckersley, 2010). Με αυτό το αποτύπωμα, τα μέρη παρακολούθησης μπορούν στη συνέχεια να ακολουθήσουν τους χρήστες, ακόμη και σε μεγαλύτερες χρονικές περιόδους (Eckersley, 2010). Οι ιδιότητες του χρήστη ή της συσκευής ενδέχεται να αλλάξουν με την πάροδο του χρόνου, αλλά έχει αποδειχθεί από τον Peter Eckersley

ότι μπορεί να διαπιστωθεί τότε ένα αποτύπωμα είναι ένας "διάδοχος" ενός άλλου αποτυπώματος (Eckersley, 2010). Αυτό μπορεί να γίνει με ακρίβεια άνω του 99%.

Οι παθητικοί μηχανισμοί αποτυπωμάτων δεν μπορούν να παρατηρηθούν από τους χρήστες, καθώς μια ιστοσελίδα δεν στέλνει ειδικές απαιτήσεις ή αποθηκεύει πληροφορίες σε συσκευές (Eckersley, 2010). Όλα τα αποτυπώματα και η παρακολούθηση συμβαίνουν στην πλευρά του διακομιστή (Eckersley, 2010). Αυτό την καθιστά μια μορφή παρακολούθησης που είναι πολύ δύσκολο να παρατηρηθεί ή να αντιμετωπιστεί (Eckersley, 2010) και ως εκ τούτου μια εξαιρετικά ενδιαφέρουσα μορφή παρακολούθησης για την παρακολούθηση των κομμάτων.

1.3.6.2. Οι ενεργητικοί μηχανισμοί αποτυπωμάτων

Οι ενεργητικοί μηχανισμοί αποτυπωμάτων λειτουργούν σαν εμπόδιο, μαζί με τους παθητικούς μηχανισμούς αποτυπωμάτων, μεταξύ της δυνατότητας πρόσβασης σε περισσότερες πληροφορίες (Mowery, 2012) -και συνεπώς της δημιουργίας ενός μοναδικού αποτυπώματος- και της δυνατότητας εντοπισμού των χρηστών και κατά συνέπεια της αντιμετώπισης αυτών των δακτυλικών αποτυπωμάτων (Mowery, 2012). Ωστόσο, μερικοί μετρητές για λήψη αποτυπωμάτων μπορούν ακόμη και να διευκολύνουν την αποτύπωση δακτυλικών αποτυπωμάτων. Για παράδειγμα το Adobe Flash μπορεί να δώσει ορισμένες λεπτομέρειες σχετικά με τη συσκευή του χρήστη. Αυτό διευκολύνει τη δημιουργία ενός ακριβούς αποτυπώματος. Αλλά όταν ο χρήστης απενεργοποιεί το Flash Player, αυτό τον καθιστά μέρος ενός πολύ μικρότερου συνόλου χρηστών, γεγονός που κάνει ακόμη πιο εύκολη τη λήψη αποτυπωμάτων στη συσκευή του.

Οι ενεργητικοί μηχανισμοί αποτυπωμάτων μπορούν να θεωρηθούν ως ένα επιπρόσθετο κομμάτι των παθητικών μηχανισμών αποτυπωμάτων (Mowery, 2012). Οι πιο συνηθισμένες τεχνικές χρησιμοποιούν τις πληροφορίες που συλλέγονται με χρήση των παθητικών μηχανισμών αποτυπωμάτων (Mowery, 2012). Οι δημοφιλείς ενεργητικοί μηχανισμοί για τη λήψη αποτυπωμάτων χρησιμοποιούν τη λίστα εγκατεστημένων γραμματοσειρών (Eckersley, 2010) ή κάνουν χρήση αποτυπωμάτων σε καμβά (Mowery, 2012). Σε αυτή την τεχνική, ο τρόπος με τον οποίο μια συσκευή χειρίζεται την σχεδίαση μιας εικόνας κάποιου είδους σε μια ιστοσελίδα,

χρησιμοποιείται ως μοναδικό αποτύπωμα (Mowery, 2012). Πολύ πρόσφατα, οι Cao, Li και Wijmans βρήκαν μια μέθοδο εξαγωγής αποτυπωμάτων που μπορεί να παρακολουθεί τους χρήστες σε διαφορετικούς φυλλομετρητές ιστού σε μία μόνο συσκευή (Cao, Wijmans, 2017). Η μέθοδος λειτουργεί με τη χρήση χαρακτηριστικών του υλικού της συσκευής που έχει αποτυπώματα, όπως η στοίβα GPU και ήχου και προβάλλεται στο uniquemachine.org.

Κάθε τεχνική αποτύπωσης που απαιτεί ενεργό αίτημα σε μια συσκευή, θεωρείται ενεργητικός μηχανισμός αποτυπωμάτων (Cao, Wijmans, 2017).

Κεφάλαιο 2^ο: Προστασία Προσωπικών Δεδομένων

2.1. Προστασία Προσωπικών Δεδομένων

Η προστασία των προσωπικών δεδομένων θεσπίζεται από τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (Ε.Ε. 2016/679) ο οποίος δημοσιεύτηκε το 2016 και αποφασίστηκε να τεθεί σε εφαρμογή από τις 25 Μαΐου 2018, αφήνοντας ένα περιθώριο περίπου 2 ετών στις επιχειρήσεις αλλά και σε όλους τους χρήστες του διαδικτύου να συμμορφωθούν με τα νέα δεδομένα. Οι επικείμενες διατάξεις ισχύουν σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης και δημιουργήθηκαν έπειτα από έντονες διαβουλεύσεις όλων των συνεργαζόμενων κρατών (Lawspot, 2018). Στόχος του Κανονισμού είναι η προστασία της ιδιωτικότητας αλλά και των ηλεκτρονικών επικοινωνιών. Για τον λόγο αυτό, στις ειδικές σημειώσεις που επισυνάπτονται, ορίζεται ένας στόχος που πρέπει να επιτευχθεί από όλα τα κράτη-μέλη. Οι κανόνες που θα χρησιμοποιηθούν για την επίτευξη του στόχου αυτού διαφέρουν από χώρα σε χώρα ανάλογα με την κουλτούρα, την οικονομική της κατάσταση και γενικά τον τρόπο με τον οποίο είναι δομημένη κοινωνικά.

2.1.1. Νομικό πλαίσιο

Το νομικό πλαίσιο για την προστασία προσωπικών δεδομένων (Lawspot, 2018) αποτελείται από τον Γενικό Κανονισμό Προστασίας Δεδομένων/General Data Protection Regulation (GDPR)

(Κανονισμός 2016/679) και από δύο οδηγίες που επισυνάπτονται και επιβάλλεται να τηρηθούν μαζί με τον βασικό κανονισμό (Οδηγία 2016/680 και Οδηγία 2016/681).

Σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 2016), η προστασία και ασφάλεια στην επεξεργασία προσωπικών δεδομένων φυσικών προσώπων, αποτελεί θεμελιώδες δικαίωμα. Απώτερος στόχος του Κανονισμού είναι να επιτευχθεί ατομική και προσωπική ελευθερία και το σύνολο των ατόμων να νοιώθει ότι ζει σε μια κοινωνία δικαιοσύνης και ασφάλειας. Επίσης με την εφαρμογή του κανονισμού ενισχύεται το διεθνές εμπόριο αλλά και το εμπόριο στο εσωτερικό των χωρών με αποτέλεσμα την οικονομική και κοινωνική ευημερία των λαών.

Στα άρθρα που περιλαμβάνονται στον Κανονισμό τονίζεται η ανάγκη για προστασία των φυσικών προσώπων όταν αποστέλουν και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα με φυσικά πρόσωπα άλλων κρατών/μελών.

Προφανώς στον κανονισμό υπάρχουν και περιορισμοί οι οποίοι αφορούν το δικαίωμα που κατέχει η κοινωνία να άρει το απόρρητο των δεδομένων φυσικού χαρακτήρα αν κρίνει ότι κάτι τέτοιο θα εξυπηρετούσε το κοινωνικό συμφέρον. Η άρση της προστασίας προσωπικών δεδομένων φυσικών προσώπων γίνεται για την προστασία άλλων εξίσου σημαντικών θεμελιωδών δικαιωμάτων σύμφωνα με τις Συνθήκες και τους Κανονισμούς των χωρών της Ευρωπαϊκής Ένωσης.

Η ραγδαία ανάπτυξη της τεχνολογίας και της ψηφιακής οικονομίας έχουν ως συνέπεια την απότομη αύξηση του όγκου δεδομένων προσωπικού χαρακτήρα που συλλέγονται και ανταλλάσσονται. Τόσο οι επιχειρήσεις ιδιωτικού τομέα όσο και οι οργανισμοί του δημοσίου εκμεταλεύονται οποιαδήποτε πληροφορία προσωπικού χαρακτήρα μπορούν να προσεγγίσουν, για ιδίον όφελος. Αν και η μετάδοση δεδομένων χωρίς περιορισμούς διευκολύνει τον τρόπο ζωής των ανθρώπων και ανεβάζει το βιοτικό επίπεδο, θα πρέπει να διασφαλίζεται παράλληλα η προστασία της ιδιωτικότητας. Το κάθε άτομο θα πρέπει να μπορεί να ελέγχει ακριβώς ποιός μπορεί να έχει πρόσβαση στα δεδομένα προσωπικού του χαρακτήρα και να μπορεί να θέσει όρια στην επεξεργασία των δεδομένων του από τρίτους.

Δημιουργώντας ένα ισχυρό νομικό πλαίσιο για την προστασία της ιδιωτικότητας, επιτυγχάνεται η οικοδόμηση εμπιστοσύνης και αναπτύσσεται η παγκόσμια ψηφιακή οικονομία. Απαραίτητη προϋπόθεση για έγκυρα αποτελέσματα είναι η αυστηρή εφαρμογή του Κανονισμού Προστασίας

Δεδομένων. Ενδεχόμενη παραβίαση έχει ως αποτέλεσμα την επιβολή υπέρογκων προστίμων στους παραβάτες.

Ανά πάσα στιγμή ο χρήστης μπορεί να ανακαλέσει την συγκατάθεσή του για την επεξεργασία των δεδομένων που τον αφορούν. Κάθε άτομο έχει την δυνατότητα να διορθώσει οποιαδήποτε ανακρίβεια αντιληφθεί σε δεδομένα που τον αφορούν ή και να ζητήσει την διαγραφή τους στην περίπτωση που η συλλογή τους εναντιώνεται στον Κανονισμό. Επίσης μπορεί να θέσει και περιορισμούς στον τρόπο επεξεργασίας των δεδομένων του και να επιλέξει ποιά δεδομένα του θα τεθούν υπο επεξεργασία.

Το κείμενο της πολιτικής απορρήτου της κάθε ιστοσελίδας επιβάλλεται να είναι γραμμένο απλά και κατανοητά με διατύπωση που μπορεί να γίνει αντιληπτή από άτομα όλων των ηλικιών και επιπέδων μόρφωσης.

Σε περίπτωση ποινικών υποθέσεων ή περιπτώσεων που βλάπτουν το κοινωνικό συμφέρον τα δεδομένα καθίστανται διαθέσιμα χωρίς περιορισμό μεταξύ των δικαστικών αρχών των κρατών-μελών.

Η οδηγία 2016/681 αναφέρεται εξ' ολοκλήρου στις αερομεταφορές και περιλαμβάνει όλες τις λεπτομέρειες για τις κατευθυντήριες γραμμές που δόθηκαν στη Διεθνή Οργάνωση Πολιτικής Αεροπορίας πάνω στο θέμα της επεξεργασίας των δεδομένων για την πάταξη των τρομοκρατικών ενεργειών και την καταπολέμηση της διεθνούς εγκληματικότητας. Για την αποφυγή διαβίβασης ψευδών δεδομένων, οι αρμόδιες αρχές θα πρέπει να ανανεώνουν τις βάσεις των δεδομένων τους και να μεταφέρουν στο μέτρο του δυνατού τυχόν διορθώσεις ή αλλαγές στα αρχεία τους.

Σε περίπτωση που παρατηρηθεί παραβίαση στα δεδομένα φυσικού χαρακτήρα, το υποκείμενο που εξαπατήθηκε θα πρέπει να ενημερωθεί άμεσα για να μπορέσει να προστατευτεί απο ενδεχόμενη μεγαλύτερη ζημία. Η ενημέρωση θα πρέπει να γίνεται εγγράφως, να περιγράφει λεπτομερώς την φύση της παραβίασης και να παρέχει συστάσεις για την αποφυγή δυσμενέστερων συνεπειών.

Η κάθε χώρα θα πρέπει να προσαρμόσει το νομικό πλαίσιο για την προστασία προσωπικών δεδομένων για να συνάδει με την εσωτερική πολιτική της χώρας με νόμους ισοδύναμους με αυτούς που επιβάλει η Ευρωπαϊκή Ένωση.

2.1.2. Προστασία Προσωπικών Δεδομένων στην Ελληνική πραγματικότητα

Η προστασία προσωπικών δεδομένων είναι κατοχυρωμένη Συνταγματικά στην Ελλάδα από το 2001 με το Άρθρο 9^A που αναθεωρήθηκε στις 27 Μαΐου 2008. Σύμφωνα με το Σύνταγμα (Βουλή των Ελλήνων, 2008) «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».

Το 2006 τροποποιήθηκε ο Νόμος για να μπορεί να προστατεύει τους πολίτες πίο αποτελεσματικά από υποκλοπές και παραβιάσεις της ιδιωτικότητας μέσω των ηλεκτρονικών επικοινωνιών. Ο Νόμος 3471/2006 θεσπίζει το θεμελιώδες δικαίωμα των φυσικών προσώπων στην προστασία των προσωπικών τους δεδομένων και του απόρρητου των ψηφιακών διαβιβάσεων των δεδομένων τους. Όπως καθίσταται σαφές από τον αρχικό νόμο για την προστασία των προσωπικών δεδομένων (Ν. 2472/1997) που δημοσιεύτηκε στην εφημερίδα της Κυβερνήσεως στις 10 Απριλίου 1997 υπογεγραμμένο από τον τότε Υπουργό Δικαιοσύνης Ευάγγελο Γιαννόπουλο (ΑΑΔΕ, 1997) η προστασία της ιδιωτικότητας είναι δικαίωμα όλων των πολιτών και οι επικείμενοι νόμοι θα πρέπει να επικαιροποιούνται και να εξιχνάζονται για να ανταποκρίνονται στις ανάγκες της εποχής.

Με τον νέο Κανονισμό του 2016, επιβλήθηκε σε όλες τις επιχειρήσεις που βρίσκονται στην Ευρωπαϊκή Ένωση -και κατά συνέπεια και στην Ελλάδα- που συλλέγουν ή/και επεξεργάζονται δεδομένα φυσικών προσώπων, να υιοθετήσουν τις νέες οριοθετήσεις. Σε περίπτωση μη τήρησης των νέων κανόνων, οι κυρώσεις θα ήταν καταστροφικές για την κάθε εταιρεία. Έτσι από τις 25-05-2018 ο δημόσιος τομέας καθώς και όλες οι ιδιωτικές επιχειρήσεις θα έπρεπε να είναι έτοιμες και προετοιμασμένες κατάλληλα για να ακολουθήσουν με συνέπεια τις προϋποθέσεις του Κανονισμού.

Οι περισσότερες επιχειρήσεις δημιούργησαν μία νέα θέση εργασίας, αυτή του Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer, DPO), ο οποίος πρέπει να είναι επιστημονικά καταρτισμένος σε θέματα προστασίας δεδομένων και να γνωρίζει όλο το νομικό πλαίσιο που τα περιβάλλει. Στόχος του DPO είναι να διασφαλίζει την ομαλή τήρηση των διατάξεων του κανονισμού προλαμβάνοντας δυνητικές περιπτώσεις παραβίασης των δεδομένων προσωπικού χαρακτήρα. Είναι επίσης αρμόδιος και για την εκπαίδευση των υπαλλήλων των εταιρειών πάνω

στον τρόπο με τον οποίο θα πρέπει να συλλέγουν, να επεξεργάζονται , να αποθηκεύουν και να διατηρούν τα δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων.

Στον δημόσιο τομέα οι ΕΟΠΥΥ (Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας), ΗΔΙΚΑ (Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης), ΓΓΠΣ (Γενική Γραμματεία Πληροφοριακών Συστημάτων) και ΕΔΕΤ (Εθνικό Δίκτυο Έρευνας και Τεχνολογίας), θα πρέπει να συμμορφωθούν αυστηρά με τις προϋποθέσεις του νέου Κανονισμού λόγω του τεράστιου όγκου προσωπικών δεδομένων που διαθέτουν. Για την προσαρμογή των οργανισμών ορίζεται από τον αρμόδιο της κυβέρνησης ένας Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων ο οποίος καλείται να συντονίσει τους φορείς του δημοσίου.

Έλεγχοι που έγιναν από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έξι μήνες μετά την οριστική εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (Κόλλια, 2019) έδειξαν ότι ο δημόσιος τομέας στερείται διαφάνειας και συμμόρφωσης με τις διατάξεις για τους τρόπους συλλογής και διατήρησης των δεδομένων σε όλο το εύρος του, σε σχέση με τον ιδιωτικό τομέα. Ελλιπής επίσης παρουσιάστηκε και η ενημέρωση των αρμόδιων φυσικών προσώπων για τους τρόπους με τους οποίους μπορούν να ελέγχουν τα προσωπικά τους δεδομένα και να καταγγέλουν δυνητικές παραβιάσεις απορρήτου.

Πιο συγκεκριμένα, Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διεξήγαγε αυτεπάγγελτη έρευνα, σε σύνολο 65 υπευθύνων που δραστηριοποιούνται διαδικτυακά στους τομείς των χρηματοπιστωτικών υπηρεσιών, υπηρεσιών ασφάλισης, ηλεκτρονικού εμπορίου, υπηρεσιών εισιτηρίων και των υπηρεσιών δημοσίου τομέα, για να διαπιστώσει πρωτίστως παντελή έλλειψη συμμόρφωσης με τη νομοθεσία για τα cookies και τις συναφείς τεχνολογίες, στο σύνολο σχεδόν των υπευθύνων επεξεργασίας (Κόλλια, 2019).

Σύμφωνα πάντα με την Αρχή, «παρατηρήθηκε, επίσης, ελλιπής ενημέρωση για τις πράξεις επεξεργασίας και τους αποδέκτες των δεδομένων σε ποσοστό 40% περίπου των υπευθύνων. Αισθητή είναι η υστέρηση του Δημοσίου στη συμμόρφωση, κυρίως στον τομέα της διαφάνειας στο σύνολο σχεδόν των φορέων που ελέγχθηκαν» (Κόλλια, 2019).

Στον αντίποδα, κινούνται τα στοιχεία που αφορούν την ασφάλεια των διαδικτυακών τόπων μέσω ενδεικτικών σημείων ελέγχου, αντιληπτών από τον πολίτη κατά την πλοήγησή του, καθώς το σχετικό ποσοστό υπερβαίνει κατά τι το 80% των υπευθύνων επεξεργασίας δεδομένων. Παρατηρήθηκε επίσης επαρκής βαθμός δημοσιοποίησης στοιχείων υπευθύνου προστασίας

δεδομένων στον ιδιωτικό τομέα, σε ποσοστό άνω του 70% των υπευθύνων επεξεργασίας (Κόλλια, 2019).

Παράλληλα γίνονται μεγάλες προσπάθειες από τους συντονιστές DPO για άμεση εξαμάλυνση των θεμάτων που καθυστερούν την συμμόρφωση των οργανισμών με τον νέο Κανονισμό.

2.2. Μέτρα ασφαλείας για την Προστασία Προσωπικών Δεδομένων

Για την υψηλού επιπέδου ασφάλεια των προσωπικών δεδομένων είναι απαραίτητη η λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων ανάλογα με την επικινδυνότητα που μπορεί να συνεπάγεται απο την επεξεργασία και διαβίβαση των δεδομένων. Πριν απο οποιαδήποτε χρήση προσωπικών δεδομένων φυσικών προσώπων, το αρμόδιο άτομο ή ο φορέας, θα πρέπει να ενημερώει την Αρχή Προστασίας Προσωπικών Δεδομένων και να κατοχυρώνει την άδειά της εγγράφως (ΑΑΔΕ, 1997). Με τον τρόπο αυτό, γίνεται σωστή χρήση των δεδομένων κάτω απο συγκεκριμένους όρους και προϋποθέσεις που θεσπίζει η Αρχή.

Ο Κώδικας Δεοντολογίας αποσκοπεί στην διευκόλυνση της τήρησης των κανόνων του Γενικού Κανονισμού Προστασίας Δεδομένων ρυθμίζοντας τον τρόπο με τον οποίο θα πρέπει να εκτελείται η επεξεργασία δεδομένων.

Είναι εξίσου σημαντικό όλοι οι οργανισμοί που κατέχουν ή/και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα να καθορίσουν ένα Σχέδιο Ασφαλείας (Security Plan) μέσα στο οποίο θα γίνεται λεπτομερής περιγραφή των αρχών και των κανόνων που πρέπει να ακολουθούνται και τον ακριβή τρόπο υλοποίησής τους. Σε περίπτωση φυσικής ή τεχνικής καταστροφής, ο αρμόδιος φορέας είναι υποχρεωμένος να έχει προβλέψει τρόπους ανάκαμψης και αποκατάστασης όλων των δεδομένων, και ο οργανισμός να είναι έτοιμος να κινηθεί σύμφωνα με το ήδη υπάρχων Σχέδιο Ανάκαμψης απο καταστροφές (Disaster Recovery and Contingency Plan).

Τέλος, ο κάθε οργανισμός θα πρέπει να διαθέτει Πολιτική Ασφαλείας (Security Policy) που θα περιγράφει τις πιο σημαντικές αρχές προστασίας προσωπικών δεδομένων που χρησιμοποιούνται. Επίσης θα πρέπει να φαίνεται η πλήρης κατανομή εργασιών των υπαλλήλων που είναι υπεύθυνοι για την Ασφάλεια και γενικά να περιγράφονται λεπτομερώς όλες οι τεχνικές λεπτομέρειες όσων αφορά την διαχείριση και την επεξεργασία δεδομένων φυσικού χαρακτήρα.

2.2.1. Μέθοδοι ενίσχυσης της ιδιωτικότητας

Λόγω της ραγδαίας ανάπτυξης της τεχνολογίας των πληροφοριών και του τεράστιου όγκου δεδομένων που διαβιβάζονται στο ιντερνετ καθημερινά, κρίθηκε απαραίτητο να δημιουργηθούν τρόποι που να προστατεύουν τα δεδομένα προσωπικού χαρακτήρα όλων των οντοτήτων απο κακόβουλες επιθέσεις και υποκλοπές. Παρακάτω παρατίθενται συνοπτικά πληροφορίες σχετικά με τα Firewalls, την Κρυπτογράφηση, την Πιστοποίηση Αυθεντικότητας και τις Ψηφιακές Υπογραφές όπου είναι ευρέως διαδεδομένοι τρόποι προστασίας της ιδιωτικότητας παγκοσμίως και αποτελούν άκρως αποτελεσματικές λύσεις.

2.2.1.1. Firewall

Ένας απο τους πιο διαδεδομένους τρόπους ενίσχυσης της ασφάλειας των δεδομένων είναι τα Firewalls. Το Firewall ελέγχει και ρυθμίζει την ροή των πληροφοριών ανάμεσα σε δύο ή και παραπάνω δίκτυα (Κάτσικας, 2004). Θεωρείται πολύ ισχυρό εργαλείο για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα και αποτελεί την πρώτη γραμμή άμυνας του δικτύου απέναντι στην παραβατικότητα. Η ρύθμιση του εργαλείου πρέπει να γίνεται απο εξειδικευμένα άτομα που να έχουν ολοκληρωμένη γνώση πάνω στο τι απαιτείται απο κάθε οργανισμό και στο ποιά θα πρέπει να είναι τα όρια στην επεξεργασία και την διαβίβαση δεδομένων. Σε περίπτωση που δεν γίνουν οι απαραίτητες ρυθμίσεις, το Firewall αδυνατεί να λειτουργήσει αποτελεσματικά με αποτέλεσμα να υπάρχει διαρροή πληροφοριών. Κάτι τέτοιο θα μπορούσε να αποβεί καταστροφικό σε περιπτώσεις δημοσιοποίησης ευαίσθητων προσωπικών δεδομένων. Τα Firewalls λειτουργούν σαν μία περιμετρική άμυνα που βρίσκεται ανάμεσα στα δίκτυα που ελέγχουν, και επιτρέπουν ή αποτρέπουν την διαβίβαση των δεδομένων σύμφωνα με όσα έχει ορίσει ο υπεύθυνος δικτύου. Η περιγραφή του Firewall γίνεται στα Ελληνικά με τον όρο «τείχος προστασίας». Το τείχος προστασίας δεν μπορεί απο μόνο του να προστατέψει στο έπακρον το δίκτυο του οργανισμού, σε συνδυασμό όμως και με άλλους μηχανισμούς ασφάλειας είναι ένας απο τους καταλληλότερους τρόπους ασφάλειας των προσωπικών δεδομένων φυσικών προσώπων. Εκτός απο τον έλεγχο των πληροφοριών που μεταφέρονται απο το ένα δίκτυο στο άλλο, το εργαλείο καταγράφει και αποθηκεύει όλο το ιστορικό της κινητικότητας των δεδομένων σε ένα αρχείων συμβάντων. Τέλος τα Firewalls παρέχουν την δυνατότητα απόκρυψης των πραγματικών διευθύνσεων (Internet Protocol, IP) των δικτύων των οργανισμών.

Αν και το τείχος προστασίας είναι αρκετά αξιόπιστος τρόπος για την προστασία της ιδιωτικότητας δεν παρέχει προστασία απο απειλές κακόβουλου λογισμικού. Μπορεί να υποδείξει όμως την διεύθυνση του υπολογιστή απο τον οποίο προήλθε το μολυνσμέο πρόγραμμα.

Επίσης σε εσωτερικό επίπεδο ενός οργανισμού το τείχος προστασίας αδυνατεί να καλύψει της ανάγκες ασφάλειας αφήνοντας τα δεδομένα ανοιχτά σε κάθε επιτήδευο υποκλοπέα. Σε αυτή την περίπτωση πρέπει να οριστούν διαφορετικοί μηχανισμοί προστασίας.

Τα firewalls δεν προστατεύουν τα προσωπικά δεδομένα όταν ο χρήστης του δικτύου αποθηκεύσει μόνος του ένα αρχείο που περιέχει ενδεχόμενη μορφή επίθεσης, με κάποιο εξωτερικό σκληρό δίσκο ή κάποιο αρχείο που θα ‘κατεβάσει’ οικειοθελώς. Επίσης δεν μπορούν να αναγνωρίσουν νέες απειλές αλλά μόνο όσες έχουν ήδη αντιμετωπιστεί και είναι αποθηκευμένες στη μνήμη τους.

2.2.1.2. Κρυπτογράφηση

Η κρυπτογράφηση είναι η διαδικασία που απαιτείται για να κωδικοποιηθούν τα δεδομένα προσωπικού χαρακτήρα έτσι ώστε να εμποδίζεται η αναγνώρισή τους από μη εξουσιοδοτημένες οντότητες (ESET, 2019). Με τον τρόπο αυτό προστατεύει τους χρήστες του διαδικτύου και τους οργανισμούς απο κινδύνους παραβίασης της ιδιωτικότητας. Απαραίτητο εργαλείο για να λειτουργήσει η κρυπτογράφηση είναι ο αλγόριθμος κρυπτογράφησης μαζί με μία ακολουθία απο bits που ονομάζεται «κλειδί». Οι κωδικοί αυτοί είναι πολύ δύσκολο έως ακατόρθωτο να παραβιαστούν, με αποτέλεσμα να αποτελεί έναν απο τους πιο λειτουργικούς τρόπους προστασίας της ιδιωτικότητας. Η κρυπτογράφηση γίνεται εκτός από μέσα στα σταθερά κομμάτια (hardware) του υπολογιστή και μέσω λογιστικού που εγκαθίσταται στο σύστημα. Ο πιο αποτελεσματικός τρόπος είναι μέσω hardware αλλά λόγω πολύ υψηλού κόστους όλοι οι αρμόδιοι φορείς προτιμούν την κρυπτογράφηση μέσω προγραμμάτων. Η πιο διαδεδομένη μέθοδος κρυπτογράφησης είναι η Συμμετρική Κρυπτογράφηση (Symmetric Cryptography ή Secret-Key Cryptography) στην οποία χρησιμοποιούνται ίδιοι κωδικοί για την κρυπτογράφηση και την αποκρυπτογράφηση (Κάτσικας, 2004). Υπάρχει επίσης και η Ασύμμετρη Κρυπτογράφηση (Public-Key Cryptography) που διαθέτει ξεχωριστά κλειδιά στην κρυπτογράφηση και την αποκρυπτογράφηση. Ενώ στην Συμμετρική κρυπτογράφηση το «κλειδί» είναι εύκολο να υποκλαπεί κατα την διαδικασία της διαβίβασης, στην Ασύμμετρη

κρυπτογράφηση η υποκλοπή δεν είναι εφικτή. Η Συμμετρική κρυπτογράφηση όμως είναι πολύ ταχύτερη από την Ασύμμετρη. Βέβαια και οι δύο αυτοί τρόποι κρυπτογράφησης μπορούν να συνεργαστούν αρμονικά και να μηδενίσουν το οποιοδήποτε μειονέκτημα του καθενός ξεχωριστά, με αποτέλεσμα την πλήρη προστασία της ιδιωτικότητας.

2.2.1.3. Πιστοποίηση αυθεντικότητας

Η πιστοποίηση αυθεντικότητας είναι ένα από τα πιο σοβαρά ζητήματα που έχουν να κάνουν με το ηλεκτρονικό εμπόριο και τα ευαίσθητα προσωπικά δεδομένα. Όταν κάποιος χρήστης ή φορέας επιλέγει να κάνει μία αγορά στο διαδίκτυο θα πρέπει να είναι απόλυτα σίγουρος ότι τα δεδομένα που αποστέλλει στον ιστότοπο του έμπορου είναι ασφαλή και μη παραβιάσιμα (Brown, 2016). Επίσης θα πρέπει να έχει την δυνατότητα να ελέγξει αν τα στοιχεία του, τα λαμβάνει το επιθυμητό άτομο ή φορέας και παράλληλα ο παραλήπτης των δεδομένων θα πρέπει να έχει πρόσβαση σε ορισμένα στοιχεία του αποστολέα.

Η πιστοποίηση αυθεντικότητας χρήστη ή φορέα γίνεται με τον προσδιορισμό και έπειτα την επιβεβαίωση του ονόματος χρήστη και του κωδικού πρόσβασης ή με την χρήση βιομετρικών στοιχείων όπως τα δακτυλικά αποτυπώματα κλπ ή και συνδυασμό αυτών.

Τα πρωτόκολλα πιστοποίησης αυθεντικότητας χρησιμοποιούνται για να αποδείξουν ότι τα άτομα που επικοινωνούν είναι αυτά τα οποία δηλώνουν και όχι κάποια άλλα. Εδώ υπάρχει κρυπτογράφηση ολόκληρης της ροής των πληροφοριών και ένα κλειδί συνόδου (session key) το οποίο βοηθάει στο να γίνεται επιβεβαίωση της αυθεντικότητας της οντότητας. Γενικότερα στην σημερινή εποχή υπάρχουν πολλά πρωτόκολλα που μπορούν να χρησιμοποιηθούν για να διασφαλίσουν την υψηλού επιπέδου ασφάλειας των προσωπικών δεδομένων φυσικών προσώπων.

2.2.1.4. Ψηφιακές Υπογραφές

Η ψηφιακή υπογραφή λειτουργεί ακριβώς όπως η χειρόγραφη υπογραφή και πιστοποιεί ότι οποιαδήποτε πληροφορία διαβιβάστηκε, ανήκει στο άτομο που έχει υπογράψει. Χρειάζεται δύο κωδικούς κλειδιά για να λειτουργήσει σε αντίθεση με την κρυπτογράφηση που λειτουργεί και με ένα. Τα κλειδιά πρέπει να είναι ένα ιδιωτικό και ένα δημόσιο και είναι σχεδιασμένα με τρόπο ώστε να είναι ακατόρθωτο να προβλέψει κάποιος το ένα γνωρίζοντας το άλλο.

Η ψηφιακή υπογραφή μπορεί να αντικαταστήσει την ιδιόχειρη μόνο αν πληρεί όλες τις προϋποθέσεις επιβεβαίωσης και ταυτοποίησης προσωπικών στοιχείων σύμφωνα με την Αρχή Πιστοποίησης (ΑΠΕΔ, 2017). Χρειάζεται να υπάρχει ένα πιστοποιητικό που να αποδεικνύει την αυθεντικότητα της οντότητας που χρησιμοποιεί την ψηφιακή υπογραφή καθώς και την αυθεντικότητα και γνησιότητα του εγγράφου το οποίο υπογράφεται.

Η ψηφιακή υπογραφή εξυπηρετεί πολύ για την παροχή ακρίβειας στις ηλεκτρονικές συναλλαγές και συμβάλει στην πάταξη της γραφειοκρατείας στην μείωση στις λειτουργικές δαπάνες και προσφέρει ευελιξία τόπου και χρόνου κατά την διάρκεια διεκπεραίωσης των συναλλαγών.

2.2.2. Τρόποι ανίχνευσης των υποκλοπών

Παρόλο που οι μέθοδοι ενίσχυσης της προστασίας των προσωπικών δεδομένων είναι πλέον αποτελεσματικοί σε μεγάλο βαθμό, υπάρχουν ακόμοι επιτήδριοι που καταφέρνουν να σπάσουν το φράγμα όλων των συστημάτων ασφαλείας και να επιτύχουν υποκλοπές και παραβιάσεις απορρήτων επικοινωνιών κατα συρροή κατ' εξακολούθηση. Στην συνέχεια της υποενότητας παρουσιάζονται συνοπτικά ορισμένοι τρόποι ανίχνευσης υποκλοπών.

2.2.2.1. Ανίχνευση μέσω Λειτουργικών Συστημάτων

Το κάθε λειτουργικό σύστημα Mac, Windows, iOS κλπ παρέχει στα ενδιαφερόμενα μέρη τρόπους ανίχνευσης ορισμένων προγραμμάτων υποκλοπών. Εάν γίνεται συνεχής έλεγχος των προγραμμάτων που είναι αποθηκευμένα στο σύστημα, ο χρήστης μπορεί εύκολα να εντοπίσει κάποιο το οποίο δεν του είναι γνώριμο και να κάνει έλεγχο νομιμότητας ψάχνοντας πληροφορίες στο διαδίκτυο. Όταν το λειτουργικό σύστημα λειτουργεί με επιβραδυνμένο ρυθμό και οι ταχύτητες στο ίντερνετ είναι αρκετά χαμηλές, τότε ίσως υπάρχει κάποιο είδος κακόβουλου λογισμικού. Επίσης όταν υπάρχει συνεχής λήψη μηνυμάτων για σφάλματα σε διαδικασίες που λαμβάνουν χώρα στο ίντερνετ θα πρέπει να γίνεται έλεγχος για κατασκοπεία. Τέλος, χρειάζεται να γίνεται έλεγχος της χρήσης των δεδομένων ανά τακτά χρονικά διαστήματα. Όταν ο όγκος των δεδομένων είναι τεράστιος τότε η πιθανότητα να γίνεται υποκλοπή είναι πολύ υψηλή.

2.2.2.2. Χρήση προγραμμάτων ασφαλείας στο διαδίκτυο (Anti-Spyware)

Τα προγράμματα ασφαλείας ανιχνεύουν και αφαιρούν οτιδήποτε κατασκοπεύει τον χρήστη ή τον φορέα διαδικτυακά. Εκτός από το Spyware που έχει μολύνει την συσκευή που περιέχει τα προσωπικά δεδομένα, αφαιρεί όλα τα αρχεία που έχουν μολυνθεί και επισκευάζει όσα έπαθαν ζημιά. Λόγω της ενδεχόμενης μη έγκαιρης ανίχνευσης, θα πρέπει να γίνεται άμεση αλλαγή των κωδικών πρόσβασης και των κλειδιών ασφαλείας και να γίνεται ενημέρωση όλων των χρηματοπιστωτικών ιδρυμάτων για δυνητική υποκλοπή δεδομένων.

2.2.2.3. Τεχνολογίες ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies, PETs)

Υπάρχουν τεχνολογίες που όχι μόνο παρέχουν λύσεις στην ενίσχυση της ιδιωτικής ζωής αλλά και μπορούν να ανιχνεύσουν αν κάποιος υπολογιστής έχει μολυνθεί από κακόβουλο λογισμικό. Οι τεχνολογίες αυτές ονομάζονται PETs και επιτρέπουν στα άτομα ή τους φορείς που χρησιμοποιούν το διαδίκτυο να κρατούν τα προσωπικά τους δεδομένα απόρρητα. Στόχος τους είναι να ελαχιστοποιούν τα δεδομένα προσωπικού χαρακτήρα που μπορεί να συλλέξει και να επεξεργαστεί οποιοσδήποτε ενδιαφερόμενος, δημιουργώντας ανώνυμες άδειες δεδομένων ή ψευδώνυμα.

Οι PETs παρέχουν στον χρήστη την δυνατότητα να επεξεργαστεί τους όρους απορρήτου των προσωπικών του δεδομένων και του επιτρέψει να αποφασίσει αυτός ποιά δεδομένα θα μπορούν να τίθενται υπο επεξεργασία και σε ποιόν βαθμό (Brunton, 2015). Επίσης του δίνεται η δυνατότητα τροποποίησης ή και διαγραφής των προσωπικών του δεδομένων.

Κεφάλαιο 3^ο: Εξέλιξη μηχανισμών παρακολούθησης τρίτων στον Παγκόσμιο Ιστό

3.1. Εξέλιξη μηχανισμών παρακολούθησης τρίτων στον Παγκόσμιο Ιστό

Παρακολούθηση είναι η τάση των διαφημιστικών εταιρειών και των επιχειρήσεων να αναζητούν ακριβείς πληροφορίες για τους χρήστες τους (Λιμνιώτης, 2011). Το κίνητρο για την παρακολούθηση είναι σχεδόν πάντα τόσο ύποπτο όσο θα μπορούσαν να πιστεύουν ορισμένοι υποστηρικτές της ιδιωτικής ζωής (Broad, 2016). Οι εταιρείες χρησιμοποιούν τις πληροφορίες για να παρέχουν καλύτερες υπηρεσίες (Broad, 2016). Ωστόσο, οι χρήστες θα πρέπει να είναι σε θέση να αποφασίζουν οι ίδιοι εάν θα επιτρέψουν την παρακολούθηση της δραστηριότητάς τους στο διαδίκτυο (Λιμνιώτης, 2011). Πολλοί αποφασίζουν να εγκαταστήσουν τους αποκλεισμούς εντοπισμού και να αρνηθούν τη χρήση cookie τρίτου μέρους και αυτό αποτελεί απόδειξη ότι υπάρχει ένα ποσοστό των χρηστών του Διαδικτύου που δεν συμπαθούν την ιδέα της παρακολούθησης. Παρακάτω παρουσιάζονται κάποιες μέθοδοι παρακολούθησης και συλλογής προσωπικών δεδομένων οι οποίοι χρησιμοποιούνται ευρέως στην σημερινή εποχή.

3.1.1. Χρησιμοποιώντας μεταδεδομένα τηλεφώνου

Σύμφωνα με τις μελέτες που παρουσιάζονται στο (Mayer, 2014), τα μεταδεδομένα τηλεφώνου (π.χ., ημερολόγια κλήσεων που έχουν προεπιλεγεί από κυβερνήσεις των περισσότερων χωρών)

είναι εξαιρετικά ευαίσθητα. Οι συγγραφείς ανέπτυξαν μια εφαρμογή Android, η οποία συλλαμβάνει τα μεταδεδομένα του τηλεφώνου. Χρησιμοποιώντας τα αρχεία καταγραφής των κλήσεων οι ερευνητές ήταν σε θέση να προσδιορίσουν την κατάσταση της υγείας (Mayer, 2014) (συμπεριλαμβανομένης της ψυχικής) του ατόμου, τις θρησκευτικές πεποιθήσεις και τους εθισμούς. Καθώς πολλοί χρήστες τοποθετούν τους αριθμούς τηλεφώνου τους σε δημόσιους καταλόγους (π.χ. Google+, Facebook), οι επιστήμονες μπορούσαν να συσχετίσουν περίπου το 18% των ιδιωτικών αριθμών με τις ταυτότητες των πραγματικών χρηστών. Συνοψίζοντας, οι εφαρμογές για κινητά, η χορήγηση αδειών πρόσβασης στα ημερολόγια κλήσεων και άλλα ευαίσθητα δεδομένα αποτελούν σοβαρή απειλή για την προστασία της ιδιωτικής ζωής των χρηστών (Mayer, 2014).

3.1.2. Η παρακολούθηση μέσω GPS (Global Positioning System)

Η παρακολούθηση μέσω GPS είναι πλέον ένας από τους πιο εύκολους και καθιερωμένους τρόπους συλλογής δεδομένων. Κάθε φορά που ο χρήστης γνωστοποιεί την τοποθεσία του σε κάποιο από τα μέσα κοινωνικής δικτύωσης ή εγκαθιστά μία εφαρμογή αυτομάτως αποθηκεύονται τα δεδομένα της τοποθεσίας του (GPS, 2014) από τον ιστότοπο ή/και τους διαφημιστές που χρησιμοποιούν τον ιστότοπο. Αυτό βέβαια μπορεί ίσως να φαίνεται ότι παραβιάζει την ιδιωτικότητα των χρηστών (Broad, 2016), τους βοηθάει όμως στο να εντοπίζουν την τοποθεσία τους (GPS, 2014) και να βρίσκουν συντομότερους τρόπους για να φτάσουν στον προορισμό τους ή και να θυμούνται συγκεκριμένες περιοχές που θα ήθελαν να επισκεφτούν ξανά (GPS, 2014).

3.1.3. Μη συνειδητή συνεργασία του χρήστη

Εκτός από τις αυτόματες λύσεις, το ιστορικό περιήγησης μπορεί να εντοπιστεί και σε συνεργασία με τον χρήστη, ο οποίος δεν γνωρίζει αυτό το γεγονός (Weinberg et al, 2011). Τέσσερις εύκολα εφαρμόσιμες μέθοδοι προτάθηκαν από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Weinberg et al, 2011). Οι ιδέες βασίζονται στην παραγωγή εικόνων που προσποιούνται ότι είναι CAPTCHA, τις οποίες ο χρήστης χρειάζεται να πληκτρολογήσει σε ένα πεδίο κάτω από την εικόνα και να υποβληθεί στην υπηρεσία πριν να είναι δυνατές κάποιες εγκαταστάσεις ή ενέργειες στον ιστότοπο. Οι εικόνες αποτελούνται από λέξεις, γράμματα ή άλλα σύμβολα, τα οποία στην πραγματικότητα συνδέονται με τους προορισμούς (Weinberg et

al, 2011) που πρόκειται να ελεγχθούν ώστε να διαπιστωθεί αν είχαν προηγουμένως τους είχε επισκεφθεί ο χρήστης. Το χρώμα του συγκεκριμένου συμβόλου έχει οριστεί να είναι το ίδιο με το φόντο σε περίπτωση που έχει επισκεφθεί ο χρήστης τον προορισμό πατώντας στον υπερσύνδεσμο (Weinberg et al, 2011), διαφορετικά το χρώμα έχει ρυθμιστεί ώστε να διακρίνεται από το φόντο, έτσι ώστε το σύμβολο να αναγνωρίζεται εύκολα από το χρήστη (Weinberg et al, 2011). Η παραγόμενη εικόνα CAPTCHA καλύπτεται συνήθως από μια διαφανή εικόνα που καθιστά δυσκολότερο για τον χρήστη να αναγνωρίσει ότι αυτό το CAPTCHA αποτελείται από υπερσυνδέσμους.

Επιπλέον έχει κάνει την εμφάνισή της μια μέθοδος που βασίζεται σε μια web camera. Σε αντίθεση με την προηγούμενη, αυτή η μέθοδος περιορίζεται για χρήση σε ιστότοπους όπου οι άνθρωποι χρησιμοποιούν κανονικά τις κάμερές τους (Weinberg et al, 2011). Το χρώμα φόντου της ιστοσελίδας εξαρτάται από το εάν ο χρήστης επισκέφθηκε προηγουμένως τον ιστότοπο ή όχι (Weinberg et al, 2011). Το φως του φόντου ανακλάται από τον χρήστη και συλλαμβάνεται από την κάμερα (Weinberg et al, 2011). Αυτή η μέθοδος περιορίζεται στις εκτιμήσεις της ημέρας και στη δοκιμή ενός συγκεκριμένου ιστότοπου κάθε φορά (Weinberg et al, 2011). Αν και το φόντο μπορεί να αλλάξει για να δοκιμάσει διάφορους ιστοτόπους, δεν μπορεί να αλλάξει πολύ συχνά ώστε να ενοχλεί τον χρήστη (Weinberg et al, 2011).

Πολλές φορές ο χρήστης γνωστοποιεί εθελοντικά τα προσωπικά του δεδομένα ή ακόμη και δεδομένα τρίτων εφόσον του ζητηθούν (Ucros, 2018). Για παράδειγμα σε μία online αγορά ο χρήστης αποκαλύπτει οικειοθελώς τα στοιχεία της πιστωτικής του κάρτας. Επίσης, σε μία εγγραφή σε κάποιο από τα κοινωνικά δίκτυα προϋπόθεση μπορεί να είναι η δημοσίευση ορισμένων πληροφοριών σχετικά με κάποιον φίλο ή συγγενικό πρόσωπο (Ucros, 2018). Εδώ ο χρήστης θα πρέπει να είναι πολύ προσεκτικός για τα δεδομένα που καλείται να αποκαλύψει έτσι ώστε να μην παραβιάζεται η ιδιωτικότητα των τρίτων προσώπων (Ucros, 2018).

Επιπρόσθετα, οι online αγορές δίνουν ακριβείς πληροφορίες στις επιχειρήσεις για τις προτιμήσεις των χρηστών με αποτέλεσμα να μπορούν εύκολα να τους χαρτογραφήσουν. Έτσι την επόμενη φορά που θα επισκευτούν την συγκεκριμένη ιστοσελίδα, οι προσφορές και τα προϊόντα που θα συναντήσουν πρώτα θα είναι αυτά που τους ενδιαφέρουν (Ucros, 2018) ανάλογα με την αγορά που προηγήθηκε.

3.2. Ανάλυση τεχνικών προστασίας απο τις νέες μορφές διαδικτυακών υποκλοπών

Οι νέες μορφές διαδικτυακών υποκλοπών απαιτούν και πίο εξειδικευμένους τρόπους προστασίας των οντοτήτων που κάνουν χρήση του παγκόσμιου ιστού. Παρακάτω παρατίθενται κάποιες απο τις πίο διαδεδομένες τεχνικές για την προστασία διαδικτυακών υποκλοπών.

3.2.1. Αποκλεισμός διαφημιστικών υπηρεσιών

Μέχρι στιγμής, η παρακολούθηση μέσω τρίτων γινόταν κυρίως με τη χρήση μαύρων λιστών, όπως η Λίστα Προστασίας της Παρακολούθησης της Microsoft (TPL), η οποία αποτελεί μέρος του νεότερου Internet Explorer (Microsoft, 2014). Ο κατάλογος αυτός χαρακτηρίζεται από ακρίβεια 96,3% και δυνατότητα ανάκλησης 72,2%. Είναι πιθανό να αποφύγει κανείς την παρακολούθηση μέσω τρίτων, αποκλείοντας τις συνδέσεις σε όλους τους σχετικούς ιστότοπους, ωστόσο μόνο το 37% των αιτήσεων σε ιστότοπους που οδηγείται κανείς μέσω τρίτων, προσανατολίζονται σε έναν ιχνηλάτη (Li et al, 2015).

Τα TPLs έχουν σχεδιαστεί για να αποκλείουν μόνο περιεχόμενο τρίτων. Όταν ο χρήστης πλοηγείται απευθείας σε έναν ιστότοπο από ένα TPL, μπορεί να προσεγγιστεί χωρίς προβλήματα, καθώς θεωρείται ως διαδικτυακός τόπος πρώτου μέρους. Αυτό μπορεί να χρησιμοποιηθεί για τη φόρτωση του περιεχομένου τρίτων ως περιεχόμενο πρώτου μέρους (Li et al, 2015). Είναι επίσης δυνατή η χρήση αναδυόμενων παραθύρων για αυτό το σκοπό - το φορτωμένο περιεχόμενο τρίτου μέρους θα εμφανίζεται επίσης σαν να προέρχεται από το πρώτο μέρος (Fleischer, 2012).

Το Facebook παραδέχεται ότι κατά την περιήγηση σε έναν ιστότοπο που περιέχει το κουμπί Like, οι πληροφορίες σχετικά με το αναγνωριστικό του χρήστη στο Facebook αποστέλλονται στο διακομιστή προκειμένου να του δείξουν ποιοι από τους φίλους του δήλωσαν επίσης ότι τους αρέσει η σελίδα (Facebook, 2019). Ταυτόχρονα, αποστέλλονται στο Facebook ορισμένες πρόσθετες πληροφορίες σχετικά με τον περιηγητή μαζί με τη διεύθυνση του ιστότοπου που

αναζητά (Facebook, 2019). Οι πληροφορίες που συλλέγει ο Atlas (Atals, 2018) (ο υποκείμενος μηχανισμός παρακολούθησης) από διάφορες πηγές (συμπεριλαμβανομένων των προφίλ στο Facebook) χρησιμοποιούνται για την πώληση διαφημίσεων από το Facebook (Kafka, 2014). Το ShareMeNot (EEF, 2014), ενσωματωμένο από τον Ιούλιο του 2014 στο Privacy Badger (EEF, 2014), μπορεί να εντοπίσει και να εμποδίσει επιλεκτικά τα κουμπιά τρίτων (π.χ. Google +1 ή Facebook) να εντοπίζουν τον χρήστη εκτός και αν ο χρήστης τους κάνει κλικ. Με αυτόν τον τρόπο, η λειτουργικότητα των ιστοσελίδων δεν περιορίζεται, αλλά το απόρρητο του χρήστη προστατεύεται από την παρακολούθηση σε όλους τους ιστοτόπους που επισκέφτηκαν (EEF, 2014).

Παρόμοια λειτουργεί και το Adblock Plus. Το Adblock Plus είναι μια δημοφιλής επέκταση προγράμματος ανοιχτού κώδικα που δημιουργήθηκε το 2006, η οποία κατάφερε να κερδίσει από εκείνη την εποχή περισσότερους από 50 εκατομμύρια χρήστες. Αποκλεισμός όλων των ανεπιθύμητων διαφημίσεων από προεπιλογή, π.χ., διαφημίσεις βίντεο στο YouTube, διαφημίσεις Facebook, αναδυόμενα παράθυρα. Το Adblock Plus είναι επίσης σε θέση να προσδιορίσει αποδεκτές διαφημίσεις. Μπορεί να ρυθμιστεί ώστε να αποκλείει τομείς που είναι γνωστοί για την εξάπλωση κακόβουλου λογισμικού ή για την απενεργοποίηση όλων των γνωστών παραμέτρων παρακολούθησης (Adblock Plus, 2014). Επιτρέπει επίσης την κατάργηση όλων των κουμπιών των κοινωνικών μέσων από κάθε ιστότοπο (Adblock Plus, 2014). Τον Δεκέμβριο του 2014, το γαλλικό τμήμα του Γραφείου Διαδραστικής Διαφήμισης IAB (IAB, 2014) αποφάσισε να καταγγείλει στο δικαστήριο το λογισμικό αυτό, που επιτρέπει να κρύβονται οι διαφημίσεις, και ειδικά στην Adblock, η οποία είναι ηγέτης της αγοράς.

3.2.2. Απόκρυψη της διεύθυνσης IP

Η πιο δημοφιλής μέθοδος απόκρυψης της διεύθυνσης IP από μια απομακρυσμένη τοποθεσία είναι η χρήση ανώνυμων διακομιστών proxy, Virtual Private Networks (VPN) ή Tor (Schmucker, 2011).

Οι διακομιστές μεσολάβησης είναι ενδιάμεσες οντότητες σε επικοινωνία μεταξύ δύο μερών (Schmucker, 2011). Μερικοί από τους διακομιστές μεσολάβησης προσφέρουν υπηρεσίες ανωνυμοποίησης, οι οποίες βασίζονται μεταξύ άλλων στην απόκρυψη της διεύθυνσης IP του χρήστη ή / και στην αφαίρεση των cookies από αιτήματα HTTP. Ταυτόχρονα, μερικές από τις υπηρεσίες proxy επιτρέπουν στο χρήστη να παρακάμπτει τη λογοκρισία, καθώς ο χρήστης

συνδέεται με τον διακομιστή μεσολάβησης αντί με τον απαγορευμένο απομακρυσμένο ιστότοπο. Υπάρχουν πολλές ανώνυμες υπηρεσίες μεσολάβησης μέσω διαδικτύου που προσφέρονται δωρεάν, π.χ. Zend2 (Zend2, 2014) και KProxy (KPROXY, 2014).

Τα VPN έχουν σχεδιαστεί για να επεκτείνουν το ιδιωτικό δίκτυο μέσω μιας ασφαλούς σήραγγας. Οι κόμβοι VPN είναι εξυπηρετητές σε ένα δίκτυο που μοιράζεται το ίδιο υποδίκτυο, ανεξάρτητα από το πού βρίσκονται οι κόμβοι. Η σήραγγα που συνδέει τα συγκεκριμένα τμήματα ενός VPN ασφαλίζεται συνήθως με ένα από τα παρακάτω πρωτόκολλα: Πρωτόκολλο σημείου προς σημείο (PPTP), Πρωτόκολλο σήραγγας Layer 2 (L2TP), Πρωτόκολλο Ασφάλειας Διαδικτύου (IPsec), Secure Sockets Layer (SSL) ή OpenVPN (VPNReactor, 2014).

3.2.3. Τροποποίηση των δεδομένων που αποστέλλονται μέσω του δικτύου

Το Privoxy (Privoxy, 2013) είναι ένας διακομιστής μεσολάβησης HTTP και SSL, ο οποίος είναι σε θέση να αλλάξει, να φιλτράρει ή να απομακρύνει τις πληροφορίες που ζητά ο χρήστης. Η κύρια λειτουργία του επικεντρώνεται στην παρεμπόδιση διαφημίσεων, banners και αναδυόμενων παραθύρων και στο φιλτράρισμα της παρακολούθησης καθώς επίσης και στο φιλτράρισμα καταχρηστικού περιεχομένου ή cookies. Το Privoxy μπορεί επίσης να τροποποιήσει τις κεφαλίδες HTTP εν κινήσει.

3.2.4. Αποκλεισμός cookies

Οι χρήστες μπορούν να εξαιρεθούν από τη συμπεριφορική διαφήμιση χρησιμοποιώντας τα cookies εξαίρεσης. Ωστόσο, σύμφωνα με (Booth, 2011), λιγότερο από το 1% των προγραμμάτων περιήγησης ιστού αναφέρουν ότι τα χρησιμοποιούν. Υπάρχουν αρκετοί λόγοι για μια τέτοια κατάσταση. Στην αρχή, για κάθε τρίτο μέρος, πρέπει να οριστεί ένα νέο cookie παρακολούθησης. Δεύτερον, αυτά τα cookies έχουν περιορισμένη διάρκεια ζωής, επομένως πρέπει να ανανεώνονται περιοδικά με το χέρι. Τρίτον, τα cookies χάνονται όταν ο χρήστης καθαρίζει τα cookies από το πρόγραμμα περιήγησης (Mitchell, 2012). Τέταρτον, η εξαίρεση δεν εμποδίζει την ίδια την παρακολούθηση, αλλά παρέχει μόνο τις διαφημίσεις που βασίζονται στην παρακολούθηση (Mayer, 2011).

3.2.5. DNT

Το DNT (Beihang, 2019) είναι ένα νέο είδος κεφαλίδας HTTP, το οποίο μπορεί να προσαρτηθεί σε εξερχόμενες αιτήσεις για την ενημέρωση της υπηρεσίας που ο χρήστης δεν επιθυμεί να παρακολουθεί. Το DNT ορίζει επίσης μια ιδιότητα HTML DOM, η οποία είναι προσβάσιμη από ενέργειες που εκτελούνται στον ιστότοπο, και API για την καταχώριση εξαιρέσεων που αφορούν συγκεκριμένες τοποθεσίες που χορηγεί ο χρήστης. Οι ιστότοποι μπορούν να περιλαμβάνουν την κεφαλίδα για να γνωστοποιήσουν εάν και πώς θα χρησιμοποιήσουν μια ληφθείσα προτίμηση (Beihang, 2019). Το DNT υιοθετήθηκε ευρέως από όλους τους κύριους φυλλομετρητές ιστού. Σκοπός του ήταν να γίνει η συνήθης τεχνική για την εξαίρεση του εντοπισμού ιστοσελίδων από διαφορετικές υπηρεσίες, ωστόσο απαιτεί τη συμμόρφωση του tracker και δεν υπάρχει καμία τεχνική ή νόμιμη δυνατότητα να επιβληθεί αυτό το αίτημα (Roesner, 2012).

3.2.6. Λειτουργία ιδιωτικής περιήγησης

Όλα τα κύρια προγράμματα περιήγησης ανέπτυξαν μια ιδιωτική λειτουργία περιήγησης για να δώσουν στον χρήστη περισσότερη ανωνυμία. Μια ολοκληρωμένη σύγκριση των εφαρμογών ιδιωτικής περιήγησης από διάφορα σύγχρονα προγράμματα περιήγησης εμφανίζεται στο (Bursztein, 2010). Όλα τα κύρια προγράμματα περιήγησης (Firefox, Safari, Chrome και Internet Explorer) παρέχουν αρκετά καλούς αμυντικούς μηχανισμούς ενάντια στον τοπικό «εισβολέα», ο οποίος δεν είναι πλέον σε θέση να καθορίσει ποιους ιστοτόπους επισκέφθηκε ο χρήστης, υπό την προϋπόθεση ότι ο εισβολέας δεν είχε προηγούμενη πρόσβαση στον υπολογιστή (Bursztein, 2010) και ο χρήστης δεν τοποθέτησε σελιδοδείκτη σε οποιονδήποτε ιστότοπο (Bursztein, 2010) ή δεν έσωσε κανένα αρχείο στο σκληρό δίσκο του. Όσον αφορά τον εισβολέα ιστού, η κατάσταση είναι αρκετά διαφορετική (Bursztein, 2010). Το Safari, σε αντίθεση με τα άλλα προγράμματα περιήγησης, αγνοεί αυτήν την απειλή κάνοντας τα παλαιότερα cookies, το ιστορικό και τις αποθήκες HTML5 προσβάσιμα στη λειτουργία της ιδιωτικής περιήγησης.

3.2.7. Διαγραφή της προσωρινής μνήμης και του ιστορικού του προγράμματος περιήγησης

Αυτή η μέθοδος, με την προϋπόθεση ότι ο χρήστης καθαρίζει σωστά κάθε αποθηκευτικό χώρο στον οποίο το πρόγραμμα περιήγησης και τα plugins του μπορούν να διατηρούν πληροφορίες, συμπεριφέρεται σχεδόν με τον ίδιο τρόπο όπως και η ιδιωτική περιήγηση. Η μόνη εξαίρεση είναι

το Safari, το οποίο στη λειτουργία της ιδιωτικής περιήγησης εκτελεί συνεχώς cookies και ιστορικό από τις προηγούμενες δραστηριότητες περιήγησης.

3.3. Phishing

Το "ηλεκτρονικό" ψάρεμα είναι ένα έγκλημα στον κυβερνοχώρο στο οποίο ένας ή περισσότεροι χρήστες στοχοποιούνται μέσω ηλεκτρονικού ταχυδρομείου, τηλεφώνου ή γραπτού μηνύματος από κάποιον που εμφανίζεται ως νόμιμο ίδρυμα για να εκμαιεύσει από τους χρήστες ευαίσθητα δεδομένα, όπως στοιχεία προσωπικής ταυτοποίησης, στοιχεία τραπεζικών και πιστωτικών καρτών και κωδικούς πρόσβασης (Jakobsson, 2007).

Οι πληροφορίες χρησιμοποιούνται στη συνέχεια για πρόσβαση σε σημαντικούς λογαριασμούς των χρηστών και μπορούν να οδηγήσουν σε κλοπή ταυτότητας και οικονομικές απώλειες (Jakobsson, 2007). Η φράση "phishing" εμφανίστηκε γύρω στο 1995, όταν οι απατεώνες στο Διαδίκτυο χρησιμοποιούσαν μηνύματα ηλεκτρονικού ταχυδρομείου για να "ψαρεύουν" κωδικούς πρόσβασης και οικονομικές πληροφορίες από τους χρήστες του Διαδικτύου. Οι πρώτοι phishers αντέγραψαν τον κώδικα από τον ιστότοπο AOL και δημιουργούσαν σελίδες που έμοιαζαν με εκείνες της AOL. Στη συνέχεια έστειλαν ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου ή άμεσα μηνύματα με σύνδεσμο προς αυτήν την ψεύτικη ιστοσελίδα, ζητώντας από τα πιθανά θύματα να αποκαλύψουν τους κωδικούς τους (Shain, 2003).

Μια πλήρης επίθεση phishing περιλαμβάνει τρεις ρόλους phishers. Πρώτον, οι αποστολείς στέλνουν ένα μεγάλο αριθμό ψευδών μηνυμάτων ηλεκτρονικού ταχυδρομείου (συνήθως μέσω των botnet), τα οποία κατευθύνουν τους χρήστες σε δόλιες ιστοσελίδες. Δεύτερον, οι συλλέκτες δημιουργούν ψευδείς ιστότοπους (συνήθως φιλοξενούνται σε κατεστραμμένα μηχανήματα), οι οποίοι παροτρύνουν ενεργά τους χρήστες να παρέχουν εμπιστευτικές πληροφορίες (Shain, 2003). Τέλος, οι phishers χρησιμοποιούν τις εμπιστευτικές πληροφορίες για να κάνουν μια πληρωμή. Οι οικονομικές ανταλλαγές συμβαίνουν συχνά μεταξύ αυτών των phishers.

Στο σημείο αυτό, είναι σημαντικό να γίνει κατανοητό τι δεν είναι phishing. Η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου σε παραλήπτες για την παροχή χρημάτων στον απατεώνα (Lance, 2005) και οι απάτες μέσω δημοπρασιών στο Διαδίκτυο (μη παράδοση, παραπλανητική παρουσίαση ή πώληση κλεμμένων αγαθών) δεν θεωρούνται phishing δεδομένου ότι δεν συνεπάγονται την απόκτηση προσωπικών κωδικών των χρηστών (Lance, 2005).

Τα τελευταία στατιστικά στοιχεία αποκαλύπτουν ότι οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα μαζί με τα social media και τα sites τυχερών παιχνιδιών εξακολουθούν να αποτελούν το επίκεντρο των phishers. Οι ΗΠΑ καλύπτουν το μεγαλύτερο ποσοστό στις επιθέσεις phishing, αντιπροσωπεύοντας το 43% των ιστότοπων ηλεκτρονικού "ψαρέματος" που ανακοινώθηκαν τον Ιανουάριο του 2012. Στη συνέχεια, η Γερμανία ήταν στο 6%, ακολουθούμενη από την Αυστραλία, την Ισπανία, τη Βραζιλία, τον Καναδά, την Ολλανδία, τη Γαλλία, τις Κάτω Χώρες και τη Ρωσία (PhishTank, 2012). Μια μελέτη των δημογραφικών παραγόντων υποδηλώνει ότι οι γυναίκες είναι πιο ευάλωτες στο ηλεκτρονικό ψάρεμα (phishing) από τους άνδρες και ότι οι χρήστες ηλικίας μεταξύ 18 και 25 ετών είναι περισσότερο επιρρεπείς σε phishing από άλλες ηλικιακές ομάδες (Sheng, 2010). Οι επιθέσεις ηλεκτρονικού "ψαρέματος" που αρχικά απευθύνονταν σε γενικούς καταναλωτές εξελίσσονται τώρα ώστε να συμπεριλαμβάνουν υψηλού επιπέδου στόχους, με στόχο την κλοπή πνευματικής ιδιοκτησίας, επιχειρηματικών μυστικών και ευαίσθητων πληροφοριών σχετικά με την εθνική ασφάλεια.

3.3.1. Τύποι phishing

Το phishing έχει εξαπλωθεί πέρα από τα μηνύματα ηλεκτρονικού ταχυδρομείου ώστε να περιλαμβάνει VOIP, SMS, μηνύματα, ιστότοπους κοινωνικής δικτύωσης και ακόμη και παιχνίδια για πολλούς παίκτες. Ακολουθούν ορισμένες σημαντικές κατηγορίες ηλεκτρονικού "ψαρέματος" (phishing).

3.3.1.1. Phishing με κλώνους

Σε αυτόν τον τύπο ο phisher δημιουργείται ένα κλωνοποιημένο μήνυμα ηλεκτρονικού ταχυδρομείου, παίρνοντας πληροφορίες όπως διευθύνσεις περιεχομένου και παραλήπτη από ένα νόμιμο e-mail που είχε παραδοθεί στο παρελθόν. Στη συνέχεια στέλνει το ίδιο email με συνδέσμους που έχουν αντικατασταθεί από κακόβουλους. Χρησιμοποιεί επίσης μια διεύθυνση έτσι ώστε το email φαίνεται να είναι από τον αρχικό αποστολέα (Mutton, 2011).

3.3.1.2. Phishing τύπου Spear

Οι στόχοι του phishing τύπου Spear είναι μια συγκεκριμένη ομάδα. Έτσι, αντί να στέλνουν χιλιάδες μηνύματα ηλεκτρονικού ταχυδρομείου τυχαία, οι phishers στοχεύουν επιλεγμένες ομάδες ανθρώπων με κάτι κοινό, για παράδειγμα άτομα από την ίδια οργάνωση (FBI, 2009).

Το phishing τύπου Spear χρησιμοποιείται επίσης ενάντια σε στόχους υψηλού επιπέδου, σε ένα είδος επίθεσης που ονομάζεται "φαλαιοθηρία". Για παράδειγμα, το 2008, αρκετοί διευθύνοντες σύμβουλοι στις Η.Π.Α. έλαβαν μια ψεύτικη κλήση μαζί με ένα συνημμένο που θα εγκαθιστούσε κακόβουλο λογισμικό κατά την προβολή του (Markoff, 2008). Στα θύματα των επιθέσεων phishing στα τέλη του 2010 και στις αρχές του 2011 περιλαμβάνονται το γραφείο του πρωθυπουργού της Αυστραλίας, η κυβέρνηση του Καναδά, η υπηρεσία ταχυδρομικής λίστας Epsilon, το Εθνικό Εργαστήριο HBGary Federal και το Oak Ridge (Hong, 2011).

3.3.1.3. Phishing μέσω τηλεφώνου

Αυτός ο τύπος ηλεκτρονικού "ψαρέματος" αναφέρεται σε μηνύματα που ισχυρίζονται ότι προέρχονται από μια τράπεζα ζητώντας από τους χρήστες να καλέσουν έναν αριθμό τηλεφώνου σχετικά με προβλήματα με τους τραπεζικούς τους λογαριασμούς. Ο παραδοσιακός τηλεφωνικός εξοπλισμός διαθέτει αποκλειστικές γραμμές, έτσι ώστε η φωνή μέσω IP, γίνεται μια καλή επιλογή για τον phisher. Μόλις καλείται ο αριθμός τηλεφώνου που ανήκει στον phisher, ζητείται από τον καλούντα να εισάγει τους αριθμούς λογαριασμού του και τον κωδικό PIN. Η κωδικοποίηση της ταυτότητας του καλούντος, η οποία δεν απαγορεύεται από το νόμο, μπορεί να χρησιμοποιηθεί μαζί με όλα αυτά, ώστε να φαίνεται ότι η κλήση προέρχεται από αξιόπιστη πηγή (Vignesh, 2013).

3.3.2. Τεχνικές ηλεκτρονικού "ψαρέματος" και μέτρα αντιμετώπισης

Διάφορες τεχνικές αναπτύσσονται σχετικά με τις επιθέσεις phishing με στόχο να τις κάνουν λιγότερο ύποπτες. Για παράδειγμα χρησιμοποιούνται για να φανεί ότι τα ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου προέρχονται από νόμιμους αποστολείς, έτσι ώστε οι παραλήπτες να είναι πιο πιθανό να πιστέψουν το μήνυμα (Webcommand, 2018). Πλαστές ιστοσελίδες μοιάζουν με τις νόμιμες, έτσι ώστε οι χρήστες να εισάγουν εμπιστευτικές πληροφορίες σε αυτές (Webcommand, 2018). Τα κακόβουλα προγράμματα εγκαθίστανται στους υπολογιστές των θυμάτων για να συλλέγουν πληροφορίες απευθείας (Webcommand, 2018) ή με τη βοήθεια άλλων τεχνικών. Τα έγγραφα PDF, τα οποία υποστηρίζουν scripting και φόρμες για συμπλήρωση στοιχείων, χρησιμοποιούνται επίσης για phishing (Webcommand, 2018).

3.3.2.1. Πλαστογράφηση Email (Spoofing)

Η λέξη "spoof" σημαίνει "πλαστογράφηση". Ένα ψευδές μήνυμα ηλεκτρονικού ταχυδρομείου είναι αυτό στο οποίο ο αποστολέας τροποποιεί σκόπιμα τμήματα του μηνύματος για να φαίνεται σαν να γράφτηκε από κάποιον άλλο (Jakobsson, 2007). Συνήθως, το όνομα ή η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα και το σώμα του μηνύματος διαμορφώνονται ώστε να εμφανίζονται σαν να προέρχονται από μια νόμιμη πηγή (Jakobsson, 2007), όπως μια τράπεζα, μια εφημερίδα ή μια νόμιμη εταιρεία στο διαδίκτυο. Μερικές φορές, ο πλαστογράφος κάνει το μήνυμα ηλεκτρονικού ταχυδρομείου να φαίνεται ότι προέρχεται από έναν ιδιώτη πολίτη (Jakobsson, 2007).

Σε πολλές περιπτώσεις, το πλαστογραφημένο μήνυμα ηλεκτρονικού ταχυδρομείου αποτελεί μέρος μιας επίθεσης ηλεκτρονικού "ψαρέματος" – μια απάτη. Σε άλλες περιπτώσεις, ένα πλαστογραφημένο μήνυμα ηλεκτρονικού ταχυδρομείου χρησιμοποιείται για την ανέντιμη προώθηση μιας online υπηρεσίας ή για την πώληση ενός ψεύτικου προϊόντος.

Υπάρχουν μερικοί λόγοι για τους οποίους παραβιάζονται τα μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνουν οι χρήστες.

Ο πλαστογράφος (spoofers) προσπαθεί να καταργήσει τους κωδικούς του χρήστη και τα ονόματα σύνδεσης. Το ηλεκτρονικό "ψάρεμα" (phishing) εμφανίζεται όταν ο ανέντιμος αποστολέας προσπαθεί να παρασύρει το χρήστη. Ένας ψευδής (πλαστογραφημένος) ιστότοπος μπορεί να περιμένει από την πλευρά του, κρυφά μεταμφιεσμένος για να εμφανιστεί ως νόμιμος ιστότοπος ηλεκτρονικής τράπεζας ή πληρωμένης διαδικτυακής υπηρεσίας, όπως το eBay. Πολύ συχνά, τα θύματα πιστεύουν άθελά τους το ψεύτικο ηλεκτρονικό ταχυδρομείο και κάνουν κλικ στο ψεύτικο ιστότοπο (Babu et al, 2010). Εμπιστευόμενοι τον πλαστογραφημένο ιστότοπο, τα θύματα εισάγουν τον κωδικό πρόσβασης και την ταυτότητα σύνδεσης, και λαμβάνουν ένα ψευδές μήνυμα λάθους ότι ο ιστότοπος δεν είναι διαθέσιμος (Babu et al, 2010). Κατά τη διάρκεια αυτού του γεγονότος, ο πλαστογράφος καταγράφει τις εμπιστευτικές πληροφορίες του θύματος και το χρησιμοποιεί για να αποσύρει τα κεφάλαια του θύματος (Babu et al, 2010) ή να εκτελέσει ανέντιμες συναλλαγές.

Ο πλαστογράφος ηλεκτρονικού ταχυδρομείου είναι ένας spammer που προσπαθεί να κρύψει την αληθινή ταυτότητά του ενώ ταυτόχρονα γεμίζει το γραμματοκιβώτιο του χρήστη με διαφημίσεις. Χρησιμοποιώντας ένα λογισμικό μαζικής αλληλογραφίας που ονομάζεται ratware, οι spammers

αλλάζουν τη διεύθυνση ηλεκτρονικού ταχυδρομείου πηγής ώστε να εμφανίζονται από έναν αθώο πολίτη, μια νόμιμη εταιρεία ή μια κρατική οντότητα (Babu et al, 2010).

Η διαχείριση του τρόπου με τον οποίο επιλέγουμε να στέλνουμε μηνύματα ηλεκτρονικού ταχυδρομείου είναι το πρώτο βήμα για την αποτροπή επιθέσεων που σχετίζονται με την πλαστογράφηση. Οι επιθέσεις spam είναι συχνές όταν οι χρήστες χρησιμοποιούν έναν λογαριασμό ηλεκτρονικού ταχυδρομείου ο οποίος μοιράζεται μεταξύ αξιόπιστων και μη αξιόπιστων επαφών (Babu et al, 2010). Η συνέπεια αυτού είναι ότι ένας χρήστης θα πρέπει να προσπαθήσει να αποκτήσει περισσότερους από έναν λογαριασμούς ηλεκτρονικού ταχυδρομείου αν επιλέξει να παραμείνει σε επαφή με χρήστες (Babu et al, 2010) στους οποίους δεν μπορεί να βασιστεί πλήρως. Οι επιθέσεις spam περιέχουν συνήθως ενσωματωμένους «ιούς». Εκτός αυτού, το πρόγραμμα περιήγησης θα πρέπει επίσης να ρυθμιστεί έτσι ώστε να μην επιτρέπει κακόβουλα σενάρια σε μηνύματα ηλεκτρονικού ταχυδρομείου (Babu et al, 2010) και θα πρέπει να κλείνει μετά την αποσύνδεση του ηλεκτρονικού ταχυδρομείου. Σε περίπτωση που ο χρήστης έχει χρησιμοποιήσει ένα δημόσιο τερματικό, η κρυφή μνήμη πρέπει να εκκαθαριστεί, ώστε να αποφευχθεί το ηλεκτρονικό ψάρεμα (Babu et al, 2010).

Πρέπει να διασφαλιστεί ότι ο λογαριασμός ηλεκτρονικού ταχυδρομείου που χρησιμοποιείται δεν είναι μη ασφαλής. Μερικές φορές ο δέκτης πρέπει να είναι προσεκτικός σχετικά με την προέλευση των μηνυμάτων ηλεκτρονικού ταχυδρομείου (Babu et al, 2010) έτσι ώστε να μην κάνει λάθος. Ο αποστολέας μπορεί να χρησιμοποιήσει το πεδίο bcc έτσι ώστε οι χρήστες να μην επικοινωνούν μεταξύ τους. Σε άλλες περιπτώσεις, τα θύματα θα πρέπει να προσέχουν να μην διαβιβάζουν ή να απαντούν σε ύποπτο υλικό (Babu et al, 2010).

Η λήψη αντιγράφων ασφαλείας ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου μπορεί να οδηγήσει στην εξάπλωση κακόβουλων προγραμμάτων (Babu et al, 2010). Επιπρόσθετη φροντίδα απαιτείται όταν η πρόσβαση γίνεται σε κινητές συσκευές (Babu et al, 2010) καθώς υπάρχει κίνδυνος δυσλειτουργίας της συσκευής. Πρέπει να ληφθεί μέριμνα κατά τη διαγραφή ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου (Babu et al, 2010) ώστε να μην μεταφέρονται απλώς στον φάκελο των διαγραμμένων μηνυμάτων από πού μπορούν να γίνουν και πάλι ενεργά. Οι χρήστες του ηλεκτρονικού ταχυδρομείου θα πρέπει επίσης να γνωρίζουν σχετικά με τον τρόπο αντιμετώπισης ψευδών μηνυμάτων ηλεκτρονικού ταχυδρομείου (Babu et al, 2010). Δεν πρέπει να πιστεύει σε ισχυρισμούς όπως «έχετε κερδίσει μια κλήρωση» (Babu et al, 2010) ή παρόμοιους τίτλους. Επίσης, οι χρήστες θα πρέπει να προσπαθήσουν να αναγνωρίσουν τις

επιθέσεις ηλεκτρονικού "ψαρέματος" στα μηνύματα του ηλεκτρονικού τους ταχυδρομείου και να αποφύγουν να ακολουθήσουν τους συνδέσμους τους. Θα πρέπει να αποφεύγεται η αποστολή προσωπικών και οικονομικών πληροφοριών σε μηνύματα ηλεκτρονικού ταχυδρομείου μέσω μη ασφαλών καναλιών (Babu et al, 2010). Ο χρήστης θα πρέπει να αποφύγει να πέσει στις παγίδες όπως να καταργήσει την εγγραφή σε ένα ενημερωτικό δελτίο που δεν έχει ποτέ εγγραφεί (Babu et al, 2010).

3.3.2.2. Web Spoofing

Ένας πλαστογράφος (phisher) θα μπορούσε να δημιουργήσει έναν ιστότοπο που μοιάζει με έναν νόμιμο ιστότοπο, έτσι ώστε τα θύματα να πιστεύουν ότι πρόκειται για τον αυθεντικό ιστότοπο και να εισαγάγουν τους κωδικούς πρόσβασης και τα προσωπικά του στοιχεία, τα οποία συλλέγει ο phisher (Microsoft, 2019).

Τα σύγχρονα προγράμματα περιήγησης έχουν ορισμένους ενσωματωμένους δείκτες ασφαλείας που μπορούν να προστατεύσουν τους χρήστες από απάτες ηλεκτρονικού "ψαρέματος" (phishing scams). Ωστόσο, συχνά αυτά παραμελούνται από απρόσεκτους χρήστες.

Κατά τη δημιουργία ενός πλαστού ιστότοπου είναι σημαντικό να κλωνοποιήσει κανείς την εμφάνιση ενός ιστότοπου, αντιγράφοντας τον κώδικα (Microsoft, 2019). Ένα μικρό κομμάτι προγραμματισμού είναι απαραίτητο για την ανακατεύθυνση της εισόδου του χρήστη σε ένα αρχείο ή μια βάση δεδομένων, και στη συνέχεια μια ειδοποίηση τύπου "ιστοσελίδα υπό συντήρηση"(Microsoft, 2019).

Το λογισμικό μεσολάβησης, όπως το squid (squid-cache, 2013) ή το Fiddler2 (Lawrence, 2013), θα μπορούσε να επεκταθεί για να δημιουργήσει έναν πλήρως λειτουργικό κλώνο ενός ιστότοπου. Οι χρήστες μπορούν να συνδεθούν με επιτυχία και να χρησιμοποιούν όλες τις υπηρεσίες που παρέχονται από τον αρχικό ιστότοπο ενώ όλα τα δεδομένα εισόδου συλλέγονται από το διακομιστή (Microsoft, 2019) και όλες οι σελίδες μπορούν να τροποποιηθούν από το διακομιστή. Μόλις ο πλαστογραφημένος ιστότοπος είναι συνδεδεμένος στο διαδίκτυο, ο phisher πρέπει να κάνει τα υποψήφια θύματα να τον επισκεφθούν. Οι πλαστογράφοι έχουν την τάση να χρησιμοποιούν παραπλανητικές διευθύνσεις, όπως <http://www.paypal.com.cgi-bin.webcr.example.com/>, για να εξαπατήσουν τους χρήστες. Με το όνομα τομέα να επισημαίνεται, οι χρήστες μπορούν εύκολα να ερμηνεύσουν τη διεύθυνση και να εντοπίσουν την τρέχουσα ιστοσελίδα με μια ματιά (Microsoft, 2019).

Οι δείκτες ασφάλειας των προγραμμάτων περιήγησης δεν είναι τόσο αποτελεσματικοί όσο κάποιος μπορεί να σκεφτεί. Μια έρευνα (Dhamija, 2006) αναφέρει ότι το 23% των συμμετεχόντων χρησιμοποίησε μόνο το περιεχόμενο μιας ιστοσελίδας για να προσδιορίσει τη νομιμότητα. Ένας ταυτόσημος κλώνος με οποιοδήποτε όνομα τομέα χωρίς https είναι αρκετό για να τους εξαπατήσει. Η χρήση του HTTPS δεν επαρκεί.

Τα Dynamic Skins Security (Dhamija, Tygar, 2005) φαίνεται να είναι μια καλή μέθοδος. Η ιδέα είναι ότι ο διακομιστής παράγει μια μοναδική αφηρημένη εικόνα για κάθε χρήστη (Dhamija, Tygar, 2005) και το πρόγραμμα περιήγησης υπολογίζει επίσης ανεξάρτητα την ίδια εικόνα. Ο αλγόριθμος εξασφαλίζει ότι ένας phisher δεν μπορεί να προβλέψει αυτήν την εικόνα. Ο χρήστης χρειάζεται μόνο να συγκρίνει αυτές τις δύο εικόνες, αν είναι ταυτόσημες, ο διακομιστής είναι νόμιμος.

3.3.2.3. Pharming

Το Pharming είναι ένας τύπος επίθεσης που αποσκοπεί στην ανακατεύθυνση της επισκεψιμότητας σε έναν ψεύτικο ιστότοπο του Διαδικτύου. Υπάρχουν διάφορες μέθοδοι για επιθέσεις pharming, μεταξύ των οποίων η δηλητηρίαση της της προσωρινής μνήμης DNS είναι η πιο κοινή.

3.3.2.4. Η δηλητηρίαση των DNS και της προσωρινής μνήμης DNS (DNS spoofing)

Το Domain Name System (DNS) είναι ένα κρίσιμο κομμάτι της υποδομής του Internet.

Το DNS είναι κρίσιμο για την ασφάλεια στο Διαδίκτυο. Εάν το DNS παραβιάζεται, τα παραποιημένα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να περάσουν από αυτά τα μέτρα πρόληψης που βασίζονται στην υπογραφή (Zhang, 2007).

Η δηλητηρίαση της προσωρινής μνήμης DNS επιχειρεί να τροφοδοτήσει την προσωρινή μνήμη των τοπικών ανιχνευτών DNS με εσφαλμένες εγγραφές. Αυτό είναι δυνατό επειδή: Το DNS τρέχει μέσω του UDP και είναι εύκολο να παραβιάσει τη διεύθυνση προέλευσης ενός πακέτου UDP. η κεφαλίδα πακέτου DNS περιέχει ένα πεδίο αναγνωριστικού ερωτήματος 16 bit, το οποίο είναι σχετικά σύντομο, έτσι ώστε να είναι εφικτή μια επίθεση (Google Public DNS, 2018).

Ο κώδικας που στοχοποιεί την προσωρινή μνήμη DNS βρίσκεται συχνά σε διευθύνσεις URL που αποστέλλονται μέσω ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου προσπαθούν να τρομάξουν τους χρήστες ώστε να κάνουν

κλικ στη διεύθυνση URL, η οποία με τη σειρά τους μολύνει τον υπολογιστή τους. Οι διαφημίσεις banner και οι εικόνες - τόσο σε μηνύματα ηλεκτρονικού ταχυδρομείου όσο και σε αναξιόπιστους ιστότοπους - μπορούν επίσης να κατευθύνουν τους χρήστες σε αυτόν τον κώδικα. Μόλις μολυνθεί ο υπολογιστής του χρήστη, θα τον οδηγήσει σε ψεύτικες ιστοσελίδες που μοιάζουν με τις πραγματικές, εκθέτοντάς τον σε κινδύνους όπως spyware ή keyloggers.

Η μόλυνση του DNS δημιουργεί αρκετούς κινδύνους, ξεκινώντας από την κλοπή των δεδομένων. Οι τραπεζικοί ιστότοποι και οι δημοφιλείς ιστοσελίδες διαδικτυακών πωλήσεων παραβιάζονται εύκολα, πράγμα που σημαίνει ότι οποιοσδήποτε κωδικός πρόσβασης, πιστωτική κάρτα ή προσωπικές πληροφορίες ενδέχεται να διακυβεύονται.

Η επέκταση ασφαλείας συστήματος ονόματος τομέα (DNSSEC) (Eastlake, 1997) είναι μια επέκταση του DNS που παρέχει τρεις ξεχωριστές υπηρεσίες: διανομή κλειδιών, έλεγχος προέλευσης δεδομένων και έλεγχος ταυτότητας συναλλαγών και αιτημάτων. Κάθε εγγραφή DNS μπορεί να πιστοποιηθεί μέσω μιας αλυσίδας εμπιστοσύνης. Η δηλητηρίαση της μνήμης cache δεν είναι πλέον δυνατή, επειδή ο phisher δεν μπορεί να παράγει μια σωστή υπογραφή χωρίς να γνωρίζει το ιδιωτικό κλειδί του τομέα. Ωστόσο, το DNSSEC δεν χρησιμοποιείται ακόμη ευρέως. Το Δημόσιο DNS της Google, ο μεγαλύτερος δημόσιος αναλυτής DNS στον κόσμο, μετριάξει τις επιθέσεις δηλητηρίασης κρυφής μνήμης (Google Public DNS, 2018).

3.3.2.5. Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό είναι ένα λογισμικό που έχει αναπτυχθεί είτε με σκοπό να βλάψει έναν υπολογιστή είτε να αποκομίσει οφέλη από αυτό σε βάρος του χρήστη (Jakobsson, Myers, 2007). Τα κακόβουλα προγράμματα μπορούν να χρησιμοποιηθούν για τη συλλογή εμπιστευτικών πληροφοριών απευθείας ή για να βοηθήσουν άλλες τεχνικές phishing.

Τα προϊόντα ασφάλειας πελατών είναι σε θέση να ανιχνεύσουν και να καταργήσουν το κακόβουλο λογισμικό και άλλα δυνητικά ανεπιθύμητα προγράμματα, αλλά οι phishers μπορούν να καταστήσουν το malware μη ανιχνεύσιμο. Τα χρηματοπιστωτικά ιδρύματα και οι πωλητές διαδικτυακών παιχνιδιών διανέμουν προγράμματα ασφαλείας για την προστασία των πελατών τους (Jakobsson, Myers, 2007).

Τα κακόβουλα προγράμματα μπορούν να χρησιμοποιηθούν για τη συλλογή εμπιστευτικών πληροφοριών τις οποίες στη συνέχεια θα στείλουν σε phishers. Μπορούν να συλλέξουν πλήκτρα, στιγμιότυπα οθόνης, περιεχόμενα μηνυμάτων και άλλες δραστηριότητες. Το πλαίσιο

εισαγωγής κωδικού πρόσβασης, όπου τα γράμματα εμφανίζονται ως αστερίσκοι, μπορεί να διαβαστεί εύκολα με ένα πρόγραμμα (Jakobsson, Myers, 2007). Το κακόβουλο πρόγραμμα μπορεί επίσης να εμφανίσει ένα ψεύτικο περιβάλλον χρήστη για να συλλέγει ενεργά πληροφορίες (Jakobsson, Myers, 2007). Οι συλλεγμένες πληροφορίες μπορούν να αποστέλλονται αυτόματα στους phishers μέσω ηλεκτρονικού ταχυδρομείου, διακομιστή ftp ή καναλιού IRC (Jakobsson, Myers, 2007).

Τα προϊόντα ασφάλειας των χρηστών αναπτύσσονται ευρέως. Το Microsoft Update αναπτύσσει επίσης μηνιαίως το "Εργαλείο αφαίρεσης κακόβουλου λογισμικού", το οποίο είναι ένας ελαφρύς σαρωτής κακόβουλου λογισμικού.

Ωστόσο, δεν είναι πάντα αποτελεσματικές. Είναι εύκολο να τροποποιηθεί ένα πρόγραμμα έτσι ώστε να μην περιέχει καμία γνωστή υπογραφή, για να παρακάμψει την ανίχνευση που βασίζεται στην υπογραφή. Υπάρχουν επίσης τεχνικές για την παράκαμψη ορισμένων τρόπων ανίχνευσης που βασίζονται στη συμπεριφορά (Jakobsson, Myers, 2007). Τα χρηματοπιστωτικά ιδρύματα, οι πιο συνηθισμένοι στόχοι του phishing, διανέμουν προγράμματα ασφαλείας για την προστασία των πελατών τους (Jakobsson, Myers, 2007).

3.3.2.6. Phishing μέσω εγγράφων PDF

Η μορφή PDF της Adobe είναι η πιο δημοφιλής και αξιόπιστη μορφή εγγράφων. Αυτό καθιστά τα έγγραφα PDF πιο ευαίσθητα στις απειλές ηλεκτρονικού "ψαρέματος", λόγω της φορητότητας τους σε πολλές πλατφόρμες. Το PDF, εκτός από το ότι είναι ένας ιδιαίτερα ισχυρός τύπος εγγράφου είναι μια ολοκληρωμένη γλώσσα προγραμματισμού που είναι αφιερωμένη στη δημιουργία και διαχείριση εγγράφων με ισχυρά χαρακτηριστικά. Ορισμένες κρίσιμες λειτουργίες της γλώσσας αυτής θα μπορούσαν να χρησιμοποιηθούν κατά λάθος από έναν εισβολέα ή έναν χάκερ για να σχεδιάσει ένα έγγραφο PDF προς όφελός του και να εξαγάγει τις επιθυμητές πληροφορίες από το θύμα, δημιουργώντας έτσι μια νέα παγκόσμια απειλή. Αυτές οι δυνητικά επικίνδυνες λειτουργίες περιλαμβάνουν το OpenAction και το SubmitForm (Gundee, 2011).

Παρόλο που η Adobe έχει εφαρμόσει ορισμένους μηχανισμούς ασφαλείας στα Adobe Reader και Adobe Acrobat προκειμένου να ειδοποιήσει τον χρήστη σε περίπτωση (δυνητικά) κακόβουλων προσπαθειών, αυτά τα μέτρα ειδοποίησης είναι μόνο στο πλαίσιο κάποιων μηνυμάτων, ζητώντας από τον χρήστη να επιτρέψει (Gundee, 2011) ή να αποκλείσει μια

ενέργεια. Δυστυχώς, τέτοια μηνύματα συχνά παραμελούνται από τους χρήστες και είναι δυνατό να παρακάμψουν αυτούς τους μηχανισμούς ασφαλείας τροποποιώντας τα αρχεία RdLang32.FRA και AcroRd32.dll με κακόβουλο λογισμικό (Gundeeep, 2011).

3.3.3. Πρόσθετα προληπτικά μέτρα

Δεδομένου του κινδύνου phishing, ποιοι είναι οι τρόποι με τους οποίους τα άτομα και οι οργανώσεις μπορούν να προστατευθούν; Αν και είναι δύσκολο να εφαρμοστεί, η εκπαίδευση του χρήστη είναι ίσως ο καλύτερος μηχανισμός προστασίας. Αναγνωρίζοντας τη σοβαρότητα του θέματος, περισσότεροι μη κερδοσκοπικοί οργανισμοί και ομάδες ενώνουν τα χέρια τους για την καταπολέμηση της απάτης του ηλεκτρονικού "ψαρέματος". Σχετικά με τη νομοθεσία απαιτείται να υπάρξει ιδιαίτερη προσοχή σε αυτό το θέμα για να καθοριστεί ρητά το phishing και να αποδοθούν συγκεκριμένες ποινές για το ηλεκτρονικό ψάρεμα.

3.3.4. Εκπαίδευση χρηστών

Το ηλεκτρονικό "ψάρεμα" εκμεταλλεύεται τα ευάλωτα σημεία του ανθρώπου, έτσι ώστε οι τεχνικές λύσεις να εμποδίζουν μόνο μερικούς από τους ιστότοπους ηλεκτρονικού "ψαρέματος". Δεν έχουν σημασία τα τείχη προστασίας, το λογισμικό κρυπτογράφησης, τα πιστοποιητικά ή οι μηχανισμοί επαλήθευσης ταυτότητας για να αποτραπεί μια επίθεση phishing.

Μια μελέτη σχετικά με την αποτελεσματικότητα πολλών εκπαιδευτικών υλικών κατά του ηλεκτρονικού "ψαρέματος" υποδηλώνει ότι τα εκπαιδευτικά υλικά μείωσαν την τάση των χρηστών να εισάγουν πληροφορίες σε ιστοσελίδες ηλεκτρονικού "ψαρέματος" κατά 40%. Ωστόσο, ορισμένα από τα εκπαιδευτικά υλικά ελάττωσαν επίσης ελαφρώς στην τάση των συμμετεχόντων να κάνουν κλικ σε νόμιμους συνδέσμους (Sheng et al, 2010). Αυτό οδηγεί στην πεποίθηση ότι είναι πρωταρχικής σημασίας να βρεθεί ένας νέος και αποτελεσματικός τρόπος εκπαίδευσης ενός μεγάλου μέρους του πληθυσμού (Wilson, 2011).

Υπάρχουν μερικά ερωτήματα που τίθενται: Πρέπει να εφαρμόσουμε όλους αυτούς τους μηχανισμούς προστασίας που περιπλέκουν το περιβάλλον εργασίας χρήστη (Wilson, 2011); Πρέπει να παρέχουμε καλύτερη εμπειρία χρήστη έχοντας ως κόστος τη μειωμένη ασφάλεια ή να βελτιώσουμε την ασφάλεια πληρώνοντας το κόστος της ενόχλησης του χρήστη (Wilson, 2011); Αρκετές πρόσφατες έρευνες δείχνουν ότι η έλλειψη ασφάλειας οδηγεί σε απώλεια της εμπιστοσύνης των πελατών (Wilson, 2011) στο εμπόριο στο Διαδίκτυο. Αυτό σημαίνει ότι οι

χρήστες επιθυμούν να υπάρχουν οι κατάλληλοι έλεγχοι ασφαλείας ακόμα κι αν σημαίνει ότι πρέπει να έχουν κωδικό πρόσβασης ή ότι λαμβάνουν τους κωδικούς πρόσβασης τους μέσω SMS. Σήμερα, το phishing αναγνωρίζεται από τους χρήστες ως μια πραγματική και δυνητικά επιζήμια απειλή. Εάν δεν υπάρχουν κατάλληλοι έλεγχοι κατά του ηλεκτρονικού "ψαρέματος" (phishing), υπάρχουν μεγάλες πιθανότητες να στραφούν οι πελάτες σε ασφαλέστερο μέρος για να κάνουν επιχειρήσεις.

3.3.5. Ομάδες κατά της απάτης

Το PhishTank, το οποίο ξεκίνησε τον Οκτώβριο του 2006, είναι ένα συνεργατικό κέντρο εκκαθάρισης για δεδομένα και πληροφορίες σχετικά με το ηλεκτρονικό ψάρεμα στο διαδίκτυο. Το PhishTank χρησιμοποιεί ένα εκλεπτυσμένο σύστημα ψηφοφορίας που απαιτεί από την κοινότητα να ψηφίσει "phish" ή "όχι phish", μειώνοντας την πιθανότητα ψευδών θετικών και βελτιώνοντας το συνολικό εύρος και κάλυψη των δεδομένων phishing. Παρέχει επίσης ένα ανοιχτό API για προγραμματιστές και ερευνητές για την ενσωμάτωση δεδομένων κατά του ηλεκτρονικού "ψαρέματος" στις εφαρμογές τους χωρίς χρέωση. Το PhishTank υποστηρίζεται από το OpenDNS, έναν δημόσιο ανιχνευτή DNS. Το OpenDNS χρησιμοποιεί δεδομένα του PhishTank για την πρόληψη των επιθέσεων phishing για τους χρήστες τους.

Το APWG, που δημιουργήθηκε το 2003, είναι μια διεθνής κοινοπραξία που συγκεντρώνει επιχειρήσεις που έχουν πληγεί από επιθέσεις ηλεκτρονικού "ψαρέματος", εταιρείες ασφάλειας προϊόντων και υπηρεσιών, υπηρεσίες επιβολής του νόμου, κυβερνητικές υπηρεσίες, εμπορικές ενώσεις, περιφερειακές διεθνείς συμφωνίες συνθηκών και εταιρείες επικοινωνιών (APWG, 2019).

Η FraudWatch International, μια ιδιωτική εταιρεία ασφάλειας στο Διαδίκτυο που ιδρύθηκε το 2003, παρέχει μια ποικιλία προϊόντων και υπηρεσιών κατά της απάτης (phishing) για την προστασία των οικονομικών υπηρεσιών, του ηλεκτρονικού εμπορίου και των εταιρειών φιλοξενίας μέσω διαδικτύου από phishing.

3.4. Το μέλλον της παρακολούθησης

Όλο και περισσότεροι χρήστες του κυβερνοχώρου έχουν αρχίσει να ενοχλούνται από την υπερβολική έκθεση των προσωπικών τους δεδομένων. Συνεχώς ψάχνουν να βρουν τρόπους που

θα τους προφυλλάσουν εξ ολοκλήρου από επιθέσεις υποκλοπών. Γενικότερα έχει γίνει τεράστια πρόοδος προς την κατεύθυνση αυτή (Donoghue, 2014) και συνεχίζει να γίνεται.

3.4.1. Η Ομάδα Εργασίας Cookie

Η Ομάδα Εργασίας Cookie (Donoghue, 2014) του Γραφείου Διαδραστικής Διαφήμισης IAB (IAB, 2014) σχεδιάζει μια νέα τεχνολογία για την παρακολούθηση χρηστών σε πολλαπλές συνεδρίες και συσκευές. Η ομάδα αποτελείται από 90 εταιρείες-μέλη, συμπεριλαμβανομένων των Adobe, Amazon, AOL, eBay, Google, PayPal, Quantcast, Verizon και Yahoo (Donoghue, 2014). Η IAB, αποτελείται από περισσότερες από 650 κορυφαίες εταιρίες μέσων και τεχνολογίας που είναι υπεύθυνες για την πώληση, την παράδοση και τη βελτιστοποίηση της ψηφιακής διαφήμισης ή εκστρατειών μάρκετινγκ. Ισχυρίζεται ότι αντιπροσωπεύει το 86% της διαδικτυακής διαφήμισης στις ΗΠΑ (IAB, 2014).

Στη λευκή ετικέτα που δημοσιεύθηκε τον Ιανουάριο του 2011 (IAB, 2014), η ομάδα αναφέρει ότι οι τρέχουσες τεχνικές παρακολούθησης δεν επαρκούν. Τα cookies τρίτου μέρους συχνά απενεργοποιούνται από χρήστες που ενδιαφέρονται για την προστασία της ιδιωτικής τους ζωής (και από τον Firefox, από προεπιλογή). Οι χρήστες εξετάζουν προσεγγίσεις στη νομοθεσία, για τη ρύθμιση των τρεχουσών πολιτικών παρακολούθησης. Όλα αυτά προκαλούν απώλεια εσόδων στις διαφημιστικές εταιρείες. Ο στόχος αυτού του νέου προγράμματος παρακολούθησης είναι να προσφέρει πλήρη διαφάνεια στον καταναλωτή (IAB, 2014).

3.4.2. Google AdID

Σύμφωνα με άρθρο του Σεπτεμβρίου 2013 (Barr, 2013), η Google αναπτύσσει το AdID, ένα ανώνυμο αναγνωριστικό, το οποίο μπορεί να χρησιμοποιηθεί για τη διαφήμιση και την αντικατάσταση των cookies μέσω τρίτων. Αυτό το αναγνωριστικό προορίζεται να διαβιβαστεί στα μέρη που συμφωνούν με ορισμένες κατευθυντήριες γραμμές που δίνουν στους χρήστες περισσότερη προστασία της ιδιωτικής τους ζωής (Barr, 2013) και τον έλεγχο της παρακολούθησής τους. Το AdID προγραμματίζεται ώστε να επαναφέρεται κάθε χρόνο. Τα διαφορετικά προφίλ περιήγησης θα συσχετιστούν με διαφορετικούς αναγνωριστικούς κωδικούς πρόσβασης, δίνοντας στους χρήστες τη δυνατότητα να διατηρήσουν τις ιδιωτικές τους περιόδους σύνδεσης (Barr, 2013) αποσυνδεδεμένες από τις συνήθειες δραστηριότητες περιήγησής τους.

Επιπλέον, οι χρήστες θα μπορούν να αποκλείσουν συγκεκριμένους διαφημιζόμενους από τον πίνακα ελέγχου στα προγράμματα περιήγησης (Barr, 2013).

3.4.3. Αναγνωριστικό της συσκευής από τη Microsoft

Ένα άρθρο από τον Οκτώβριο 2013 (Peterson, 2013) αποκαλύπτει ότι η Microsoft εργάζεται για την ανάπτυξη της δικής της τεχνολογίας παρακολούθησης χρησιμοποιώντας ένα αναγνωριστικό συσκευής. Η τεχνολογία έχει σχεδιαστεί για να καλύπτει επιφάνεια εργασίας, κινητά και xbox. Η άδεια χρήσης του αναγνωριστικού θα δίνεται στη Microsoft από τον χρήστη όταν εκείνος δέχεται τη συμφωνία χρήστη ή τους όρους παροχής υπηρεσιών.

3.3.4. Εργαστήριο Διαφάνειας Δεδομένων

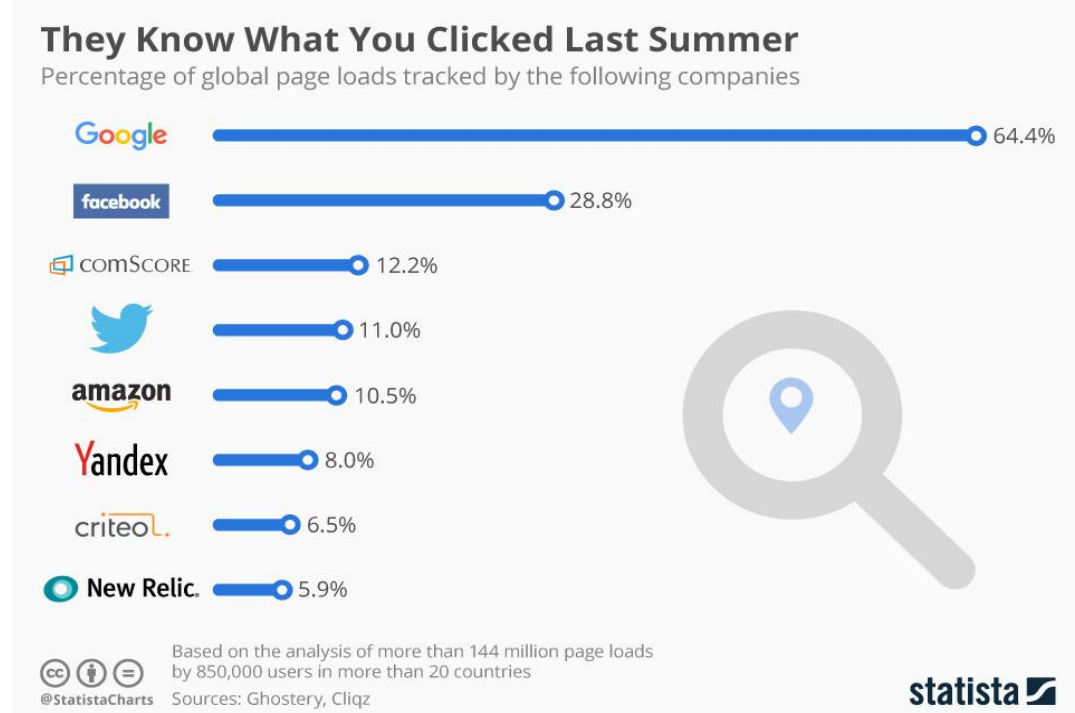
Το Εργαστήριο Διαφάνειας Δεδομένων (Data Transparency Lab, DTL, 2014) είναι μια κοινότητα που στοχεύει στην αποσαφήνιση της χρήσης των προσωπικών δεδομένων στο διαδίκτυο και στη διερεύνηση τρόπων για ένα εμπόριο δεδομένων στο μέλλον το οποίο θα διέπεται από σεβασμό και πλήρη διαφάνεια. Το DTL αποτελείται από πανεπιστήμια, επιχειρήσεις και άλλα ιδρύματα, τα οποία ανακαλύπτουν νέες μεθόδους ανίχνευσης, αναλύουν τον αντίκτυπό τους και εργαλεία σχεδιασμού, ώστε να μπορούν οι χρήστες να ελέγχουν τη χρήση των προσωπικών τους πληροφοριών στον ιστό.

3.5. Στατιστικά στοιχεία

Κάθε άνθρωπος έχει κάποια παρόμοια εμπειρία: βλέπει ένα όμορφο ζευγάρι παπούτσια στο διαδίκτυο, αποφασίζει να μην το αγοράσει και ξαφνικά αυτά τα παπούτσια εμφανίζονται ως διαφημίσεις (IAB, 2014) σε κάθε άλλη ιστοσελίδα που επισκέπτεται. Μετά από δύο ακόμη ημέρες κοιτάζοντας αυτά τα πολύ ωραία παπούτσια, η αντίσταση του κάμπτεται και έτσι τα παραγγέλλει (IAB, 2014).

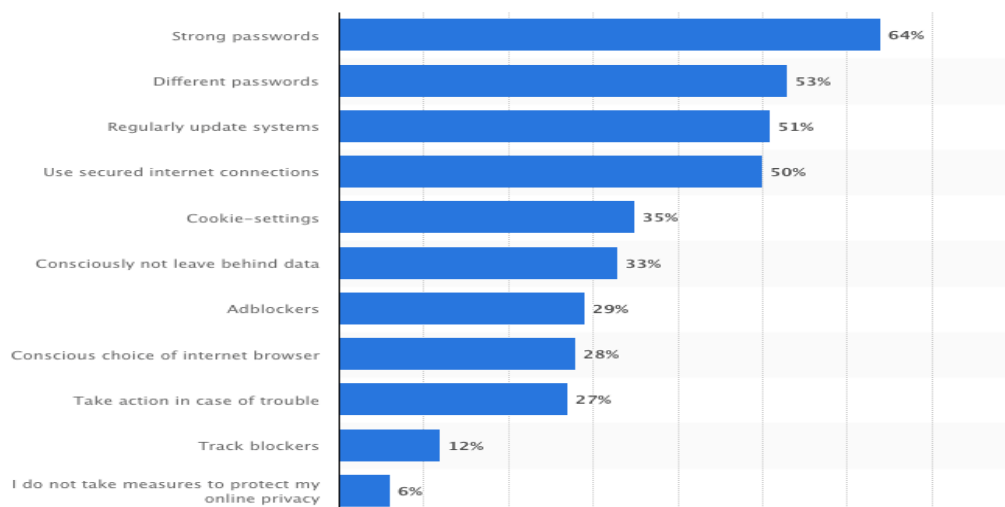
Αυτές οι εξατομικευμένες προσφορές, βασίζονται σε μια πρακτική που ονομάζεται επαναπροσανατολισμός, δηλαδή η στόχευση των καταναλωτών με βάση την προηγούμενη δραστηριότητα τους στο διαδίκτυο (Broad, 2016). Μόλις ο καταναλωτής εξετάσει ένα συγκεκριμένο προϊόν του προστίθεται μια ετικέτα με εικονοστοιχείο παρακολούθησης επιτρέποντας στον διαφημιζόμενο να προβάλλει διαφημίσεις στοχευμένης προβολής (Broad, 2016) σε αυτό το άτομο σε ιστότοπους τρίτων.

Σύμφωνα με μια νέα μελέτη του Ghostery, το 77% όλων των σελίδων περιέχει τουλάχιστον έναν tracker. Είτε πρόκειται για στατιστικούς ή για διαφημιστικούς σκοπούς, οι μηχανισμοί παρακολούθησης επιτρέπουν στις εταιρείες να εισχωρούν σε βάθος και να ελέγχουν την περιήγηση των χρηστών στο διαδίκτυο (Ghostery, 2019). Η Google είναι πρωτοπόρος στην παρακολούθηση όταν πρόκειται για τη συμπεριφορά των χρηστών στο διαδίκτυο. Όπως δείχνει το γράφημα, από την ιστοσελίδα www.statista.com, ο γίγαντας της αναζήτησης και της διαφήμισης παρακολούθησε το 64% όλων των φορτώσεων σελίδων στο υπό μελέτη δείγμα των 144 εκατομμυρίων σελίδων.



Στη συνέχεια παρουσιάζεται το αποτέλεσμα μιας έρευνας σχετικά με τα μέτρα που ελήφθησαν για την προστασία του ιδιωτικού απορρήτου στην Ολλανδία το 2017. Όταν ερωτήθηκαν πώς προστατεύουν το ηλεκτρονικό τους απόρρητο, περίπου το 65% δήλωσαν ότι προστατεύουν την ιδιωτική τους ζωή χρησιμοποιώντας ισχυρούς κωδικούς πρόσβασης. Περίπου πέντε τοις εκατό, από την άλλη πλευρά, δήλωσαν ότι απέχουν από τη λήψη μέτρων για την προστασία του

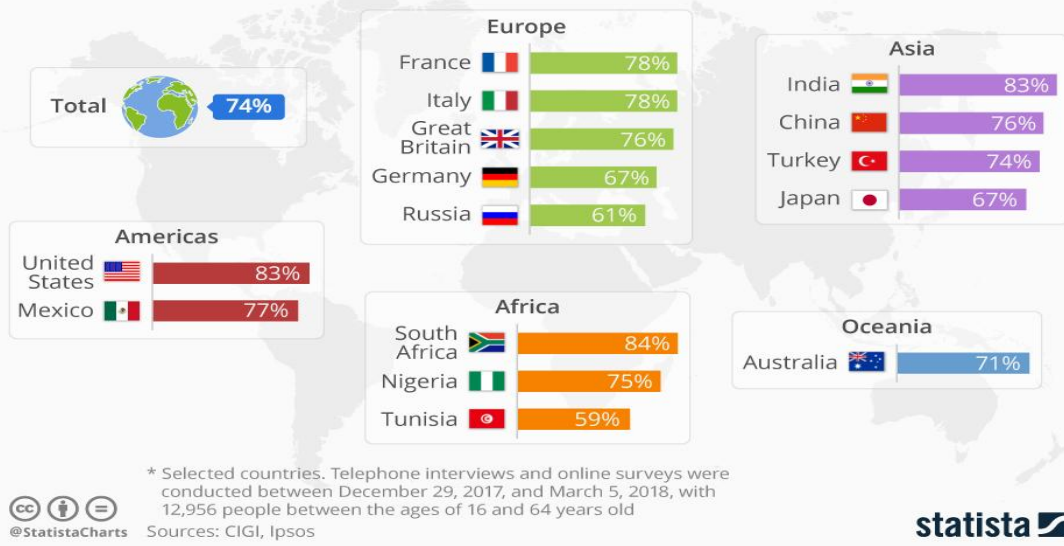
ιδιωτικού τους απορρήτου (statista, 2017). Το διάγραμμα είναι δημιουργία του www.statista.com



Σύμφωνα με τις δημοσκοπήσεις που διεξήγαγαν οι IPSOS και CIGI, οι χρήστες του Διαδικτύου σε όλες τις περιοχές του κόσμου ανησυχούν ολοένα και περισσότερο για την ιδιωτική τους ζωή στο διαδίκτυο. Στις Ηνωμένες Πολιτείες, το 83% των χρηστών του διαδικτύου ανησυχούν ολοένα και περισσότερο για το ηλεκτρονικό τους απόρρητο. Η Γαλλία είχε παρόμοια αποτελέσματα με το 78% των ερωτηθέντων που ανησυχούν για το ηλεκτρονικό τους απόρρητο, ενώ στη Γερμανία το 67% των χρηστών του Διαδικτύου ανησυχεί για το ηλεκτρονικό τους απόρρητο. Στο διάγραμμα που ακολουθεί, από το www.statista.com φαίνονται τα αποτελέσματα αυτών των δημοσκοπήσεων:

Where Are People Concerned About Online Privacy?

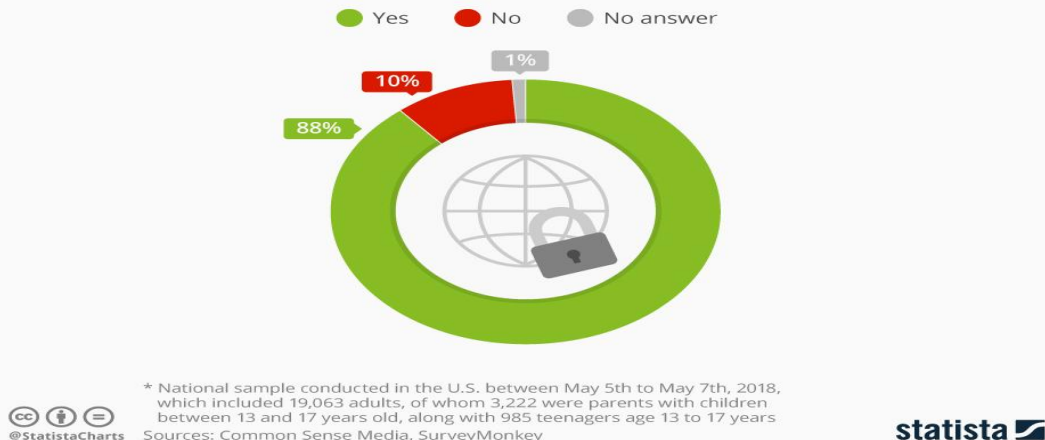
% of internet users increasingly concerned about online privacy to due internet companies*



Σύμφωνα με δημοσκόπηση που διεξήχθη από το Sense Media και την Monkey Survey, το 88% των ερωτηθέντων γονέων συζητά με τους εφήβους τους σχετικά με την προστασία της ιδιωτικής ζωής στο διαδίκτυο το 2018. Μόνο το 10% των γονέων δεν είχε μιλήσει με τα παιδιά τους για το ιδιωτικό απόρρητο στο διαδίκτυο (statista, 2018).

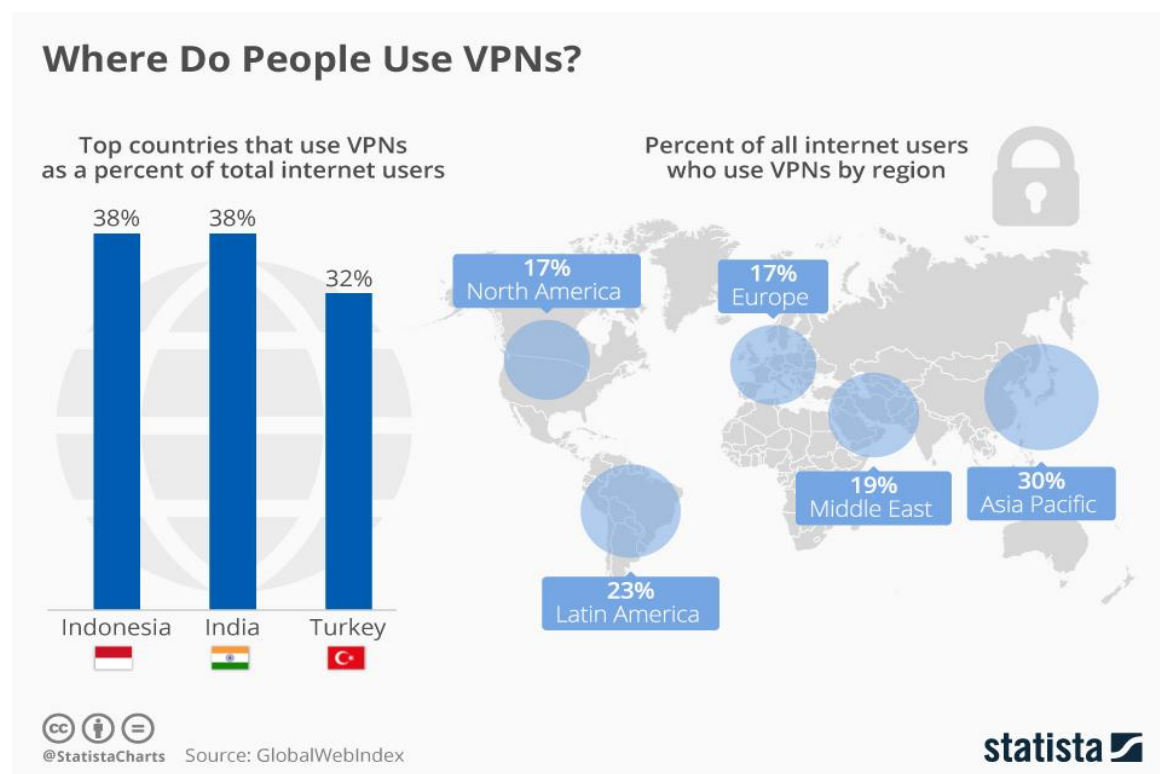
Most Parents Sit Down with Teens About Online Privacy

Share of parents in the U.S. who have spoken to their teenagers about online privacy in 2018*



Σύμφωνα με τον Global Web Index, η Ινδονησία, η Ινδία και η Τουρκία αποτελούν τις κορυφαίες χώρες για χρήση εικονικού ιδιωτικού δικτύου (VPN) σε σύγκριση με τον συνολικό αριθμό χρηστών του Διαδικτύου σε κάθε χώρα. Από όλους τους χρήστες του διαδικτύου παγκοσμίως, η Ασία-Ειρηνικός είναι η περιοχή στην οποία κατοικούν οι χρήστες που χρησιμοποιούν πιο συχνά VPN, ακολουθούμενη από τη Λατινική Αμερική και τη Μέση Ανατολή. Η Ευρώπη και η Βόρεια Αμερική χρησιμοποιούν τα VPN λιγότερο σε σύγκριση με τους χρήστες στις περιοχές αυτές.

Τα εικονικά ιδιωτικά δίκτυα συνδέουν τη συσκευή ενός χρήστη με έναν απομακρυσμένο διακομιστή, αποκρύπτοντας την τοποθεσία στην οποία βρίσκεται ο χρήστης (statista, 2018). Το VPN αναλαμβάνει τη διεύθυνση IP του διακομιστή αντί της τοποθεσίας του ατόμου. Τα VPN δημιουργούν μια ασφαλή, ιδιωτική σύνδεση μεταξύ ενός χρήστη και ενός διακομιστή.



Βιβλιογραφία

Ανεξάρτητη Αρχή Δημοσίων Εσόδων, 1997, Νόμος 2472/1997, Διαθέσιμο από:
<http://www.publicrevenue.gr/elib/view?d=/gr/act/1997/2472> Τελευταία πρόσβαση: 31 Μαρτίου 2019

Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), 2017, Ψηφιακές Υπογραφές, Διαθέσιμο από: <http://www.aped.gov.gr/thesmiko-plaisio/arxi-pistor.html>, Τελευταία πρόσβαση: 05 Απριλίου 2019

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2019, Διαθέσιμο από:
http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL,
Τελευταία πρόσβαση: 16 Μαρτίου 2019

Βουλή των Ελλήνων, 2008, Άρθρο 9Α: (Προστασία προσωπικών δεδομένων), Διαθέσιμο από:
<https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-9a/>
Τελευταία πρόσβαση: 31 Μαρτίου 2019

Γενικός Κανονισμός για την Προστασία των Δεδομένων, 2016, Διαθέσιμο από:

https://www.lawspot.gr/nomikes-plirofories/nomothesia/genikos-kanonismos-gia-tin-prostasia-dedomenon?lspt_context=gdpd , Τελευταία πρόσβαση: 17 Μαρτίου 2019

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης (ΕΕΕΕ), 2016, Διαθέσιμο από: <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016L0680&from=EL> Τελευταία πρόσβαση: 31 Μαρτίου 2019

Κάτσικας Σ., Γκρίτζαλης Στ., Γκρίτζαλης Δ., 2004, Ασφάλεια πληροφοριακών συστημάτων, Εκδόσεις Νέων Τεχνολογιών

Κόλλια Ε., 2019, Προσωπικά δεδομένα: Ανέτοιμο το Δημόσιο – Υστερεί στην προστασία τους, Διαθέσιμο από: <https://www.tovima.gr/2019/01/31/society/to-dimosio-ysterei-stin-prostasia-ton-prosopikon-dedomenon/> Τελευταία πρόσβαση: 31 Μαρτίου 2019

Λιμνιώτης Κ., Μπούρκα Α., Παναγοπούλου Γ., 2011, Προσωπικά δεδομένα και Διαδίκτυο, Διαθέσιμο από: <http://www.log.gr/prosopika-dedomena-ke-diadiktuo/>, Τελευταία Πρόσβαση: 20 Απριλίου 2019

Adblock Plus, Surf the web without annoying ads!, 2014, Διαθέσιμο από: <https://adblockplus.org/>, Τελευταία πρόσβαση: 29 Απριλίου 2019

APWG, 2019, Anti-Phishing working group, Unifying the Global Response to Cybercrime, Διαθέσιμο από: <https://www.antiphishing.org/>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Atlas Solutions Group, 2018, Privacy Policy, Διαθέσιμο από: <https://atlassolutionsgroup.com/privacy-policy/>, Τελευταία πρόσβαση: 29 Απριλίου 2019

Avenson M. D., Wambach J. D., Soltani A., Good N., Hoofnagle C. J., 2011, Flash cookies and privacy ii: Now with html5 and etag respawning, Διαθέσιμο από:

<https://pdfs.semanticscholar.org/42cf/18892910afd15b0d6872f16384a7bb6cf915.pdf>, Τελευταία Πρόσβαση: 23 Απριλίου 2019

Babu P. R., Bhaskari D. L., Satyanarayana C. H., 2010, A Comprehensive Analysis of Spoofing, International Journal of Advanced Computer Science and Applications, Vol. 1, No.6

Barr A., 2013, Google may ditch 'cookies' as online ad tracker, Διαθέσιμο από: <http://www.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183>, Τελευταία πρόσβαση: 29 Απριλίου 2019

Barth A., 2011, RFC 6265: Http state management mechanism, Διαθέσιμο από: <https://tools.ietf.org/html/rfc6265>, Τελευταία πρόσβαση: 29 Απριλίου 2019
Beihang, Keio, MIT, ERCIM, 2019, Tracking Preference Expression (DNT), Διαθέσιμο από: <https://www.w3.org/TR/tracking-dnt/>, Τελευταία πρόσβαση: 27 Απριλίου 2019

Booth D., 2011, Web Tracking and User Privacy Workshop, 29 April 2011, Διαθέσιμο από: <http://w3.org/2011/04/29-w3cdnt-minutes.html>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Bratman B. E., 2002, Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy, Tennessee Law Review Vol. 69. p. 344

Broad E., 2016, Openness principles for organizations handling personal data, Διαθέσιμο από: <https://theodi.org/article/openness-principles-for-organisations-handling-personal-data/>, Τελευταία πρόσβαση: 17 Μαρτίου 2019

Brown L., 2016, Cryptography and Network Security Chapter 15 Fifth Edition by William Stallings Lecture slides, Διαθέσιμο από: <https://slideplayer.com/slide/4517889/>, Τελευταία πρόσβαση: 04 Απριλίου 2019

Brunton F., Nissenbaum H., 2015, Obfuscation a user's guide for privacy and protest, The MIT Press

Bursztein G. A. E., Jackson C. and Boneh D., 2010, An analysis of private browsing modes in modern browsers, in Proceedings of the 19th USENIX Security Symposium

Cao Y., Li S. and Wijmans E., 2017, cross-browser Fingerprinting via os and hardware level features, Lehigh University

Data Transparency Lab, 2014, Διαθέσιμο από: <http://datatransparencylab.org>, Τελευταία πρόσβαση: 29 Απριλίου 2019

Davis M., 2014, Etags Allow Tracking Without Cookies, Διαθέσιμο από: <https://www.futurehosting.com/blog/etags-allow-tracking-without-cookies/> Τελευταία πρόσβαση: 29 Απριλίου 2019

Dhamija R., Tygar J. D. and Hearst M., 2006, Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems, New York, NY, USA, pp. 581–590

Dhamija R. and Tygar J. D., 2005, The battle against phishing: Dynamic security skins, In Proceedings of the 2005 symposium on Usable privacy and security, New York, NY, USA, pp. 77–88

Donoghue C., 2014, The Future of the Cookie Working Group, Διαθέσιμο από: http://www.iab.net/member/center/committees/working_groups/FutureoftheCookieWorkingGroup, Τελευταία πρόσβαση: 29 Απριλίου 2019

Duarte R., 1990 ,1 SCR 30, 1990 CanLII 150 (Supreme Court of Canada), Διαθέσιμο από:
<http://canlii.ca/t/1fszz>, Τελευταία πρόσβαση: 16 Μαρτίου 2019

Eastlake D., 1997, Domain Name System Security Extensions, CyberCash, Διαθέσιμο από:
<https://tools.ietf.org/html/rfc2065>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Eckersley P., 2010, How unique is your web browser? In International Symposium on Privacy Enhancing Technologies Symposium, Springer, pages 1-18

Enjoy Safer Technology, ESET, 2019, Η κρυπτογράφηση ως λύση, Διαθέσιμο από:
<https://encryption.eset.com/gr/what-is-encryption/>, Τελευταία πρόσβαση: 04 Απριλίου 2019

Electronic Frontier Foundation, 2014, Privacy Badger, Διαθέσιμο από:
<https://www EFF.org/privacybadger/faq>, Τελευταία πρόσβαση: 29 Απριλίου 2019

Facebook, 2019, Τι δεδομένα λαμβάνει το Facebook όταν επισκέπτομαι ιστότοπους που διαθέτουν το κουμπί "Μου αρέσει!"; Διαθέσιμο από:
<https://www.facebook.com/help/186325668085084>, Τελευταία πρόσβαση: 27 Απριλίου 2019

Federal Bureau of Investigation (FBI), 2009, Spear phishers, Διαθέσιμο από:

http://www.fbi.gov/news/stories/2009/april/spearphishing_040109, Τελευταία πρόσβαση: 25 Απριλίου 2019

Fleischer G., 2012, "Implementing web tracking," in Black Hat USA 2012 Conference Briefings. Black Hat, pp. 1–37 Διαθέσιμο από:

https://media.blackhat.com/bh-us-12/Briefings/Fleischer/BH_US_12_Fleischer_Implementing_Web_Tracking_gfleischer_WP.pdf, Τελευταία πρόσβαση: 27 Απριλίου 2019

Gilbert, F., 2008, Beacons, Bugs, and Pixel Tags: Do You Comply with the FTC Behavioral Marketing Principles and Foreign Law Requirements?, Journal of Internet Law

Google Public DNS, 2018, Security Benefits, Διαθέσιμο από:

<https://developers.google.com/speed/public-dns/docs/security>, Τελευταία πρόσβαση: 25 Απριλίου 2019

GPS, 2014, Protecting your privacy, What to expect when visiting our website, Διαθέσιμο από: <https://www.noaa.gov/protecting-your-privacy>, Τελευταία πρόσβαση: 27 Απριλίου 2019

Gundeeep S. B., 2011, Masquerading as a trustworthy entity through portable document file, In Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing, pp. 784 –789

Hong J., 2011, Why have there been so many security breaches recently?, Διαθέσιμο από: <https://cacm.acm.org/blogs/blog-cacm/107800-why-have-there-been-so-many-security-breaches-recently/fulltext>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Hoofnagle, Chris Jay and King, Jennifer and Li, Su and Turow, Joseph, 2010, How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? Διαθέσιμο από:

SSRN: <https://ssrn.com/abstract=1589864> or <http://dx.doi.org/10.2139/ssrn.1589864>, Τελευταία πρόσβαση: 17 Μαρτίου 2019

IAB, About the IAB, 2014, Διαθέσιμο από: http://www.iab.net/about_the_iab, Τελευταία πρόσβαση: 26 Απριλίου 2019

IAB, 2014, Privacy and Tracking in a Post-Cookie World, Διαθέσιμο από:
<http://www.iab.net/media/file/IABPostCookieWhitepaper.pdf>, Τελευταία πρόσβαση: 29
Απριλίου 2019

Intersoft Consulting, GDPR Data Protection Officer, 2019, Διαθέσιμο από: [https://gdpr-
info.eu/issues/data-protection-officer/](https://gdpr-info.eu/issues/data-protection-officer/) Τελευταία Πρόσβαση: 14 Απριλίου 2019

Jakobsson M. and Myers S., 2007, Phishing and countermeasures: understanding the in- creasing
problem of electronic identity theft, John Wiley & Sons Inc.

Jowett B, 2015, Plato Laws, The Dialogues of Plato translated by B. Jowett, Aeterna Press

Kafka P., 2014, Facebook Will Use Facebook Data to Sell Ads on Sites That Aren't Facebook,
Διαθέσιμο από: [https://www.recode.net/2014/9/28/11631346/facebook-will-facebook-data-to-
sell-ads-on-sites-that-arent-facebook](https://www.recode.net/2014/9/28/11631346/facebook-will-facebook-data-to-sell-ads-on-sites-that-arent-facebook), Τελευταία πρόσβαση: 29 Απριλίου 2019

Konvitz, M. R., 1966, Privacy and the Law: A Philosophical Prelude. Law and Contemporary
Problems Vol 31, No. 2. p. 272

KPROXY – Free Anonymous Web Proxy – Anonymous Proxy, 2014. Διαθέσιμο από:
<https://www.kproxy.com>, Τελευταία πρόσβαση: 29 Απριλίου 2019

Kristol D. M., 2001, HTTP Cookies: Standards, Privacy, and Politics, ACM Transactions on
Internet Technology, Vol. 1, No. 2, Pages 151–198, Διαθέσιμο από:
<http://www-cs.ccny.cuny.edu/~fazio/S13-csc48000/Kristol01.pdf> , Τελευταία πρόσβαση: 17
Μαρτίου 2019

Lance J., 2005, Phishing Exposed, Rockland, Syngress

Lawrence E., 2013, Fiddler web debugger - a free web debugging tool, Διαθέσιμο από:
<http://www.fiddler2.com/fiddler2/>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Lawspot , 2018, Τι αλλάζει στο νομικό πλαίσιο προστασίας και ασφάλειας δεδομένων στην Ευρωπαϊκή Ένωση;, Διαθέσιμο από: <https://www.lawspot.gr/nomika-nea/ti-allazei-sto-nomiko-plaisio-prostasias-kai-asfaleias-dedomenon-stin-eyropaiki-enosi> , Τελευταία πρόσβαση: 29 Μαρτίου 2019

Li T.-C., Hang H., Faloutsos M., and Efstathopoulos P., 2015, TrackAdvisor: Taking back browsing privacy from Third-Party Trackers, in Proceedings of the 16th Passive and Active Measurement Conference (PAM 2015), Proceedings Series: Lecture Notes in Computer Science 8362. Springer International Publishing Switzerland, New York, USA, pp. 1–12 and 277-289

Markoff J., 2008, Larger Prey Are Targets of Phishing, Διαθέσιμο από:

<https://www.nytimes.com/2008/04/16/technology/16whale.html>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Mayer J., 2014, MetaPhone: The Sensitivity of Telephone Metadata. Διαθέσιμο από: <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>, Τελευταία πρόσβαση: 29 Απριλίου 2019

Mayer J., 2011, Tracking the Trackers: Self-Help Tools – Stanford Center for Internet and Society, Διαθέσιμο από:

<http://cyberlaw.stanford.edu/blog/2011/09/tracking-trackers-self-help-tools>, Τελευταία πρόσβαση: 26 Απριλίου 2019

Microsoft Corporation, 2019, Internet explorer help, Διαθέσιμο από:

<https://support.microsoft.com/en-us/hub/4230784/internet-explorer-help>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Microsoft Corporation, 2014, Internet Explorer 9 Tracking Protection Lists, Διαθέσιμο από: <https://testdrive-archive.azurewebsites.net/browser/trackingprotectionlists/default.html>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Mitchell J. C. and Mayer J. R., 2012, Third-party web tracking: Policy and technology, IEEE Symposium on Security and Privacy (SP). IEEE, pp. 413-427

Mowery K. and Shacham H., 2012, Pixel perfect: Fingerprinting canvaw in html5. Proceedings of W2SP

Mutton P., 2011, FraudWatch International, Phishing, Διαθέσιμο από: <https://fraudwatchinternational.com/category/phishing/>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Niemietz v. Germany, 1992, 72/1991/324/396, Council of Europe: European Court of Human Rights, Διαθέσιμο από: <https://www.refworld.org/cases,ECHR,3f32560b4.html>, Τελευταία πρόσβαση: 16 Μαρτίου 2019

Ochoa C., 2017, 7 steps to follow for online data collection, Διαθέσιμο από: <https://www.netquest.com/blog/en/7-steps-to-follow-for-online-data-collection-0>, Τελευταία πρόσβαση: 17 Μαρτίου 2019

Oliveira R. V., Lad M., Zhang B., Zhang L., 2007, Geographically Informed Inter-Domain Routing, pp. 103-112

Peterson T., 2013, Bye, bye cookie: Microsoft Plots its own Tracking Technology to Span Desktop, Mobile, Xbox, Διαθέσιμο από: <https://adage.com/article/digital/microsoft-cookie-replacement-span-desktop-mobile-xbox/244638>, Τελευταία πρόσβαση: 27 Απριλίου 2019

PhishTank, 2012, Phishtank stats-jan, Διαθέσιμο από:

<http://www.phishtank.com/stats/2012/01/?y=2012&m=01>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Privoxy – Home Page, 2013, Διαθέσιμο από: <http://www.privoxy.org>, Τελευταία πρόσβαση: 29 Απριλίου 2019

Roesner F., Kohno T., and Wetherall D., 2012, Detecting and defending against third-party tracking on the web, in Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation, ser. NSDI'12. Berkeley, CA, USA: USENIX Association, pp. 12–12. Διαθέσιμο από: <http://dl.acm.org/citation.cfm?id=2228298.2228315>, Τελευταία πρόσβαση: 23 Απριλίου 2019

Rokitta C., 2015, APEX & Cookie Monster, Slideshare

Schmucker N., 2011, Web tracking, in SNET2 Seminar Paper. Berlin University of Technology, p. 9

Shain A., 2003, Phishing, Διαθέσιμο από: <https://wordspy.com/index.php?word=phishing>, Τελευταία πρόσβαση: 25 Απριλίου 2019

ShareMeNot, 2014, Διαθέσιμο από: <http://sharemenot.cs.washington.edu>, Τελευταία πρόσβαση: 29 Απριλίου 2019

Sheng S., Holbrook M., Kumaraguru P., Cranorand L. and Downs J., 2010, Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions, In 28th international conference on Human factors in computing systems

Solove, D. J., 2002, Conceptualizing privacy. California Law Review Vol. 90, No. 4. pp. 1132-1140

Tor Project: Anonymity Online, 2014, Διαθέσιμο από: <https://www.torproject.org>, Τελευταία πρόσβαση: 27 Απριλίου 2019

squid-cache, 2013, squid: Optimising Web Delivery, Διαθέσιμο από: <http://www.squid-cache.org/>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Tucker C., 2010, The Economics Value of Online Customer Data, The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, OECD Conference Centre

Ucros M., 2018, 10 Sneaky Ways Companies Are Collecting Data to Understand Customers, Διαθέσιμο από: <https://medium.com/@melodyucros/10-sneaky-ways-companies-are-collecting-data-to-understand-customers-be0b9089d54a>, Τελευταία πρόσβαση: 17 Μαρτίου 2019

Vignesh M., Gokul Ram T., Akhil R., Rajesh Kumar N.S.R, Karthikeyan R., 2013, Analysis of Phishing in Networks, International Journal of Scientific & Engineering Research, Volume 4, Issue 9

VPNReactor.com, 2014, Διαθέσιμο από: <https://www.vpnreactor.com/default.php>, Τελευταία πρόσβαση: 29 Απριλίου 2019

Webcommand, 2018, Διαθέσιμο από:

<https://www.webcommand.net/index.php/2018/02/07/pdf-files-latest-target-phishing-scam/>, Τελευταία πρόσβαση: 25 Απριλίου 2019

Weinberg Z., Chen E. Y., Jayaraman P. R., and Jackson C., 2011, I still know what you visited last summer: Leaking browsing history via user interaction and side channel attacks, in Security and Privacy (SP), 2011 IEEE Symposium on. IEEE, pp. 147–161

Wilson C. and Argles D., 2011, The fight against phishing: Technology, the end user and legislation, In Information Society, 2011 International Conference, pp. 501 –504

Zend2, 2014. Διαθέσιμο από: <https://www.zend2.com>, Τελευταία πρόσβαση: 29 Απριλίου 2019