



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής

Πτυχιακή Εργασία
“Αυτόματη Παρακολούθηση στο Διαδίκτυο: Τεχνολογίες, Μέθοδοι
Προστασίας και Επίγνωση των Χρηστών”

Φοιτητής:
Νικόλαος Μπαλάτος

Επιβλέπουσα Καθηγήτρια:
Δρ. Αγγελική Τσώχου

Σεπτέμβριος, 2025

Τριμελής Επιτροπή:

Δρ. Αγγελική Τσώχου

Δρ. Χριστόφορος Νταντογιάν

Δρ. Σπυρίδων Δουκάκης

Περιεχόμενα

Τριμελής Επιτροπή:	2
1. Εισαγωγή	4
1.1. Το ερευνητικό πρόβλημα και κίνητρο για την έρευνα.....	4
1.2. Ερευνητικά ερωτήματα.....	5
1.3. Σύνοψη της μεθοδολογίας, των αποτελεσμάτων και της συνεισφοράς της εργασίας.....	5
2. Θεωρητικό Υπόβαθρο	6
2.1. Τεχνολογίες και μέθοδοι Παρακολούθησης	6
2.2. Σκοποί αυτόματης παρακολούθησης χρηστών διαδικτύου	11
2.3. Τρόποι προστασίας	13
2.4. Επίγνωση των Χρηστών	15
3. Εισαγωγή στην Μεθοδολογία και Σχεδιασμός της Έρευνας	20
3.1 Μεθοδολογία.....	20
3.2 Ανάπτυξη του ερωτηματολογίου.....	21
3.3 Πιλοτική φάση	24
3.4 Αποτελέσματα πιλοτικής φάσης και προσαρμογές του ερωτηματολογίου	25
3.5 Διανομή του ερωτηματολογίου.....	25
4. Αποτελέσματα	27
4.1. Κατανόηση και επίγνωση σχετικά με tracking μηχανισμούς	27
4.2. Συμπεριφορά των χρηστών απέναντι στους μηχανισμούς αυτόματης παρακολούθησης	35
4.3. Επίγνωση των χρηστών σχετικά με τον βαθμό παρακολούθησης.....	38
4.4. Η στάση των χρηστών απέναντι στα εργαλεία και τις τεχνικές ενίσχυσης της ιδιωτικότητας	42
5. Συζήτηση και Συμπεράσματα	48
5.1. Περιορισμοί της έρευνας	50
5.2. Ιδέες για Περαιτέρω Έρευνα	50
5.3. Ιδέες για την Αξιοποίηση των Αποτελεσμάτων	51
Βιβλιογραφία	52

1. Εισαγωγή

Στην εποχή μας η χρήση του διαδικτύου αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας μας καθώς μας διευκολύνει σε διάφορους τομείς όπως η επικοινωνία, η αναζήτηση πληροφοριών, η εκπαίδευση και η ψυχαγωγία. Ωστόσο η χρήση του διαδικτύου σε όλους αυτούς τους τομείς συνοδεύεται από πολυάριθμες προκλήσεις στον τομέα της προστασίας της ιδιωτικότητας του χρήστη. Μέσω της παρακολούθησης στο διαδίκτυο εκτελούνται αυτοματοποιημένες ενέργειες όπως η συλλογή, καταγραφή, αποθήκευση και ανάλυση προσωπικών δεδομένων από διάφορους παρόχους διαδικτυακών υπηρεσιών, πολλές φορές χωρίς την επίγνωση και την συγκατάθεση του χρήστη. Το πρόβλημα αυτό είναι πολυδιάστατο και θα πρέπει οι χρήστες να ενημερώνονται για τις προκλήσεις και τους κινδύνους σχετικά με την ιδιωτικότητα των δεδομένων τους στο διαδίκτυο καθώς οι περισσότεροι αγνοούν τα ζητήματα της ιδιωτικότητας τους και δεν λαμβάνουν μέτρα προστασίας, με αποτέλεσμα να εκτίθενται σε πολυάριθμους κινδύνους καθημερινά.

1.1. Το ερευνητικό πρόβλημα και κίνητρο για την έρευνα

Είναι σημαντικό να είμαστε σε θέση να ορίσουμε ποιος χρήστης θεωρείται πως έχει επαρκή επίγνωση της αυτόματης παρακολούθησης και γνωρίζει πως να προστατέψει και να διαχειριστεί τα προσωπικά του δεδομένα. Για τον σκοπό αυτό στην παρούσα εργασία θα αναλυθεί το προφίλ του επαρκώς ενήμερου χρήστη και θα διερευνηθούν οι παράγοντες που επηρεάζουν το επίπεδο επίγνωσης όπως η τεχνολογική κατάρτιση, η εξοικείωσή του με τις πολιτικές απορρήτου και η χρήση εργαλείων προστασίας της ιδιωτικότητας.

Για την ενίσχυση της επίγνωσης των χρηστών είναι επίσης σημαντικό να εξετάσουμε τους σκοπούς συλλογής δεδομένων καθώς και τους τρόπους και τις τεχνολογίες που χρησιμοποιούνται από διάφορους παρόχους για την συλλογή προσωπικών δεδομένων καθώς με αυτό τον τρόπο θα γίνουν πιο εύκολα αντιληπτοί οι κίνδυνοι. Τέλος θα εξετάσουμε τα αντίμετρα που μπορεί να εφαρμόσει ο χρήστης για την προστασία της ιδιωτικότητας του και την ασφάλεια των δεδομένων του προκειμένου να ενισχυθεί η κριτική σκέψη των χρηστών του διαδικτύου σχετικά με το θέμα.

1.2. Ερευνητικά ερωτήματα

1. Ποιες είναι οι κυριότερες τεχνολογίες και μέθοδοι που συναντώνται στο διαδίκτυο σχετικά με την αυτοματοποιημένη παρακολούθηση των χρηστών και ποια τα αντίμετρα που μπορεί να λάβει ο χρήστης;
2. Ποια χαρακτηριστικά διέπουν τον επαρκώς ενήμερο χρήστη;
3. Ποιο είναι το επίπεδο επίγνωσης των χρηστών σχετικά με την παρακολούθηση στο διαδίκτυο στις μέρες μας και ποιοι παράγοντες επηρεάζουν την ικανότητα ή την αδυναμία των χρηστών να προστατευτούν;

1.3. Σύνοψη της μεθοδολογίας, των αποτελεσμάτων και της συνεισφοράς της εργασίας

Η παρούσα εργασία βασίζεται σε δύο βασικές μεθοδολογικές προσεγγίσεις. Αρχικά, πραγματοποιήθηκε βιβλιογραφική ανασκόπηση με βάση τρεις διαφορετικούς άξονες, με τον πρώτο να επικεντρώνεται στους τρόπους και τις τεχνολογίες παρακολούθησης στο διαδίκτυο. Το δεύτερο μέρος της βιβλιογραφικής ανασκόπησης αφορά στους τρόπους με τους οποίους ο χρήστης μπορεί να ενισχύσει την προστασία της ιδιωτικότητας του και να προστατευτεί από τους μηχανισμούς παρακολούθησης και ο τελικός άξονας της βιβλιογραφικής ανασκόπησης αφορά στην επίγνωση των χρηστών σχετικά με την προστασία της ιδιωτικότητας τους και τους κινδύνους που σε μεγάλο βαθμό αγνοούν. Στην συνέχεια, σχεδιάστηκε και διανεμήθηκε ερωτηματολόγιο καθώς έγιναν και πιλοτικές συνεντεύξεις, με στόχο τη διερεύνηση της επίγνωσης των χρηστών σχετικά με την παρακολούθηση και τις πρακτικές προστασίας της ιδιωτικότητάς τους.

2. Θεωρητικό Υπόβαθρο

Υπάρχουν πολλοί τρόποι με τους οποίους πραγματοποιείται αυτόματη παρακολούθηση των χρηστών στο διαδίκτυο με σκοπό τη συλλογή δεδομένων. Από τους τρόπους αυτούς άλλοι είναι απλοί και εύκολα κατανοητοί και άλλοι πολύ πιο σύνθετοι με αρκετά μεγάλη πολυπλοκότητα με αποτέλεσμα να γίνεται πιο δυσνόητη η έννοια της προστασίας της ιδιωτικότητας. Επίλυση πολλών ζητημάτων μας προσφέρουν διάφορα διαθέσιμα εργαλεία και τεχνικές που αποτελούν αντίμετρα στην παρακολούθηση των χρηστών προσφέροντας έτσι μεγαλύτερη ασφάλεια και εμπιστοσύνη στην διαδικασία πλοήγησης του χρήστη στο παγκόσμιο ιστό. Ταυτόχρονα είναι πολύ σημαντικό να μελετήσουμε το επίπεδο της επίγνωσης των χρηστών σχετικά με τους κινδύνους της ιδιωτικότητας τους, η οποία μπορεί να παραβιάζεται με διάφορους τρόπους τους οποίους οι χρήστες αγνοούν.

Οι λόγοι για τους οποίους είναι πολύ σημαντικό να εξετάσουμε τα παραπάνω είναι πολλοί και είναι αρκετά σημαντικοί γιατί μας αφορούν όλους μας, καθώς όλοι μας είμαστε υποκείμενα διαδικτυακής παρακολούθησης και συλλογής δεδομένων. Ένας από τους σημαντικότερους λόγους είναι η διαφήμιση στο διαδίκτυο η οποία για να είναι αποτελεσματική απαιτεί την συλλογή τεράστιου όγκου δεδομένων για τον κάθε χρήστη ώστε να δημιουργηθεί ένα προφίλ προτιμήσεων και να αξιοποιηθεί από διαφημιστικά δίκτυα. Με αυτό τον τρόπο τα δεδομένα υπόκεινται σε τεράστια εμπορευματοποίηση η οποία τα έχει μετατρέψει σε πολύτιμο πόρο και ως επακόλουθο έχουμε την αυτοματοποιημένη παρακολούθηση στο διαδίκτυο ως μια ευρέως διαδεδομένη πρακτική η οποία εφαρμόζεται από πλατφόρμες, επιχειρήσεις και διαφημιστικά δίκτυα.

2.1. Τεχνολογίες και μέθοδοι Παρακολούθησης

Είναι σημαντικό όλοι οι χρήστες του διαδικτύου ασχέτως της συχνότητας με την οποία περιηγούνται σε αυτό να γνωρίζουν τους τρόπους με τους οποίους μπορεί να παρακολουθούνται και πως μπορεί να συλλέγονται και να αξιοποιούνται τα ευαίσθητα αλλά και μη δεδομένα από τους διάφορους παρόχους υπηρεσιών. Υπάρχουν αρκετοί τρόποι συλλογής δεδομένων οι οποίοι είναι αρκετά διαδεδομένοι όπως τα Cookies και το Scripting (Κρυφός κώδικας στο παρασκήνιο της ιστοσελίδας) καθώς και πιο σύνθετοι όπως το Fingerprinting και Client Identification.

2.1.1. Cookies & Cross site tracking

Τα Cookies είναι μια τριπλέτα που περιέχει τα δεδομένα key, domain, value και αποθηκεύεται στον browser του χρήστη (Roesner et al. 2012). Domain είναι η ιστοσελίδα που επισκέπτεται ο χρήστης ενώ Key & Value είναι αφανείς μεταβλητές που συσχετίζονται με τον χρήστη. Υπάρχουν δύο ειδών cookies τα First-Party & Third-Party Cookies.

- First-Party Cookies: Είναι τα cookies που καθορίζονται απευθείας από τον πάροχο της ιστοσελίδας και αφορούν αποκλειστικά στο αντίστοιχο domain που επισκέφθηκε ο χρήστης. Το αρχείο που δημιουργούν τα cookies αποθηκεύεται στον σκληρό δίσκο του υπολογιστή χωρίς να γνωστοποιείται η ενέργεια αυτή στον χρήστη.
- Third-Party Cookies: Αφορούν στα Cookies που δημιουργούνται από τρίτους παρόχους (διαφημιστές, παρόχους plug-in κτλ.). Τα third-party cookies συμβάλλουν στο third-party tracking, δηλαδή την διαδικασία κατά την οποία ο χρήστης επισκέπτεται έναν ιστότοπο ο οποίος περιλαμβάνει περιεχόμενο τρίτων παρόχων όπως για παράδειγμα μια διαφήμιση και κατά την φόρτωση της διαφήμισης δημιουργούνται cookies τα οποία αποθηκεύονται στον browser του χρήστη. Τα cookies που μόλις δημιουργήθηκαν όμως ανήκουν στον τρίτο πάροχο, του οποίου το domain ο χρήστης δεν έχει επισκεφτεί ποτέ, με τον τρόπο αυτό τα third-party cookies, αυτόματα εντοπίζουν μια σειρά ιστοσελίδων που επισκέπτεται ο χρήστης και έτσι δημιουργούν ένα προφίλ προτιμήσεων, χωρίς ο χρήστης να δει ποτέ τον μηχανισμό που λειτουργεί στο παρασκήνιο. (Roesner et al. 2012).

Σε πολλές περιπτώσεις ο αρχικός πάροχος της ιστοσελίδας (First Party) συνεργάζεται με τρίτους παρόχους (Third Party) και λόγω αυτής της συνεργασίας μεταφέρονται τα δεδομένα των χρηστών και στους τρίτους παρόχους χωρίς ο χρήστης να δίνει την συγκατάθεση του ή να έχει άμεσα αναζητήσει τις υπηρεσίες τρίτων. (Mitchell 2013) Τεχνικά η παραπάνω διαδικασία γίνεται εφικτή με διάφορες βιβλιοθήκες JavaScript οι οποίες εκτελούνται στο παρασκήνιο του browser και όταν τα Third Party Cookies ενός παρόχου διαφήμισης για παράδειγμα χρησιμοποιούνται σε διάφορα sites τότε επιτυγχάνεται το Cross-Site Tracking (Quan Chen et al. 2021).

Κατά το Cross-Site Tracking έχουμε την ταυτοποίηση ενός χρήστη, μέσω της συλλογής δεδομένων του από Cookies, και μπορούμε να τον ταυτοποιούμε όσο εκείνος συνεχίζει την πλοήγησή του σε διαφορετικές ιστοσελίδες. Είναι σημαντικό σε αυτό το σημείο να σημειωθεί πως οι τεχνικές

third-party tracking παραμένουν στο διαδίκτυο αλλά, μετά την εφαρμογή διάφορων νομοθεσιών περί ιδιωτικότητας των χρηστών – GDPR στην Ευρώπη και CCPA στην Αμερική – Το third-party tracking έχει μειωθεί κατά περίπου 40% από τους παρόχους ενώ οι εύκολα ανιχνεύσιμοι χρήστες έχουν μειωθεί κατά 12% (Alexander Bleier, 2021) με βάση την έρευνα που έγινε σε δεδομένα ταξιδιωτών ανάμεσα σε 40 διαφορετικές χώρες στην Ευρώπη (Aridor, Che, and Salz 2020).

Παράλληλα είναι σημαντικό να γνωρίζουμε πως δεν συμβάλλουν όλα τα cookies στην αυτοματοποιημένη παρακολούθηση, καθώς υπάρχει και μια κατηγορία τους που ονομάζεται λειτουργικά cookies και πολλές φορές βοηθούν στην πιο ομαλή λειτουργία της εκάστοτε ιστοσελίδας και προσφέρουν την πιο ποιοτική περιήγηση του χρήστη. Παραδείγματα των λειτουργικών cookies είναι τα ονομαζόμενα από τις ιστοσελίδες «Αυστηρά απαραίτητα» τα οποία συνεισφέρουν σε λειτουργίες όπως την προσθήκη προϊόντων σε ένα διαδικτυακό καλάθι αγορών για παράδειγμα και για τα συγκεκριμένα δεν απαιτείται συγκατάθεση του χρήστη απαραίτητα. Ένα ακόμη παράδειγμα των λειτουργικών cookies είναι τα session cookies τα οποία βοηθούν στην συνεχή επικοινωνία server-client και με την λήξη της πλοήγησης του χρήστη αυτά διαγράφονται.

Πέρα από τις πιο διαδεδομένες τεχνικές Cookies που αναφέρθηκαν τελευταία όλο και περισσότερο συναντώνται τεχνικές όπως τα Zombie Cookies ή Super Cookies. Η διαγραφή των απλών Cookies είναι σχετικά εύκολη μέσω των ρυθμίσεων του browser, τα Zombie Cookies όμως δεν είναι απλή υπόθεση καθώς χρησιμοποιούν κώδικα JS μέσω του οποίου όταν ο χρήστης διαγράφει τα απλά Cookies του τα Zombie Cookies δημιουργούν αυτόματα εκ νέου τις πληροφορίες που μόλις διαγράφηκαν και τις αποθηκεύουν σε σημεία δύσκολα προσπελάσιμα από τον χρήστη. Καθιστώντας έτσι πολύ δύσκολη την δραστηριότητα διαγραφής των δεδομένων που αποθηκεύονται σε οποιασδήποτε μορφής Cookies (Niklas Schmucker 2011).

2.1.2. Fingerprinting και αναγνώριση χρηστών

Ένας ακόμη όρος σημαντικός για την κατανόηση της αυτόματης παρακολούθησης στο διαδίκτυο είναι το Fingerprinting μέσω του οποίου επιτυγχάνεται η αναγνώριση χρηστών, δραστηριότητα παρόμοια με το Cross-Site Tracking. Κατά το Fingerprinting συλλέγονται πληροφορίες του χρήστη από τον browser όπως:

- ανάλυση της οθόνης,

- η ζώνη ώρας,
- τα εγκατεστημένα plug-ins,
- οι εγκατεστημένες γραμματοσειρές,
- το λογισμικό σύστημα,
- η γλώσσα του browser κ.α.

Οι παραπάνω πληροφορίες πολλές φορές εμπεριέχονται στα HTTP Headers, διαφορετικά συλλέγονται από JS Scripts που εκτελούνται στον browser και στην συνέχεια αποθηκεύονται στους servers του browser, χωρίς την συγκατάθεση ή την επίγνωση του χρήστη. Οι παραπάνω πληροφορίες μπορεί αρχικά να φαίνονται ασήμαντες αλλά στην πραγματικότητα όταν συνδυαστούν μειώνουν σε σημαντικό βαθμό την εντροπία της ταυτότητας του browser του χρήστη, με αποτέλεσμα την διάκριση ενός συγκεκριμένου χρήστη ανάμεσα σε πολλούς. (Niklas Schmucker 2011). Κατά την διαδικασία μελέτης των περιπτώσεων αναγνώρισης χρηστών παρατηρήθηκε το εξής παράδοξο, όταν χρησιμοποιήθηκε το Flash Blocker plug-in το οποίο αποτρέπει την λειτουργία των fingerprinting μηχανισμών άρα κατά συνέπεια και την αναγνώριση του χρήστη, τα αποτελέσματα ήταν αντίθετα από τα επιθυμητά καθώς γινόταν ανιχνεύσιμο από τον browser το Plug-in και αυτό παρήγαγε περισσότερες πληροφορίες από ότι θα παράγονταν χωρίς το Plug-in, ενισχύοντας έτσι την αναγνώριση του συγκεκριμένου χρήστη αντί να την μειώνει.

2.1.3. Ορατότητα Τεχνολογιών Tracking

Είναι πολύ σημαντικό να κατανοήσουμε πως οι τεχνολογίες που χρησιμοποιούνται μπορούν να κατηγοριοποιηθούν και με βάση την ορατότητα τους στον χρήστη. Συνήθως στην κατηγορία των μη ορατών έχουμε της πιο τεχνικά περίπλοκες και επίμονες γεγονός αρκετά ανησυχητικό που σίγουρα δεν βοηθά στην ενίσχυση της επίγνωσης της ιδιωτικότητας.

Ορατές από τον χρήστη:

- First Party Cookies: Μηχανισμός που αφορά στην ιστοσελίδα στην οποία περιηγείται ο χρήστης. Εμφανίζονται με banners όταν ο χρήστης ξεκινά να περιηγείται στην ιστοσελίδα και μπορεί να τα απορρίψει ή να τα αποδεχτεί.
- Silverlight Isolated Storage: Τεχνολογία web-storage που απαιτεί το κατάλληλο plug-in της Microsoft οποτεδήποτε ο χρήστης επιλέγει να το χρησιμοποιήσει.

- URL Query Strings: Μια τεχνική όπου κατά την περιήγηση του χρήστη στην ιστοσελίδα αλλάζει το URL και προστίθεται στο τέλος του ένα ID για την εκάστοτε συνεδρία. Με τον τρόπο αυτό κάθε συνεδρία του χρήστη αποθηκεύεται στον server τις ιστοσελίδας και έτσι μπορεί διάφορες ενέργειες που περιλαμβάνουν προσωπικά δεδομένα του χρήστη να κοινοποιηθούν σε τρίτους.
- Google Gears: Τεχνολογία που αποθηκεύει δεδομένα του χρήστη στον browser αλλά απαιτεί την έγκριση του χρήστη για κάθε ξεχωριστό site. Τήρηση του Same-Origin Policy.

Μη ορατές από τον χρήστη:

- Click Stream Analysis: Η τεχνική κατά την οποία η ιστοσελίδα μέσω κώδικα tracking καταγράφει τα click του χρήστη και αξιολογεί κατά πόσο μια διαφήμιση ήταν αποτελεσματική, κερδίζοντας το ενδιαφέρον του χρήστη.
- Client Identification: Κατά κανόνα το πρωτόκολλο HTTPS δεν αποθηκεύει δεδομένα από μια συνεδρία προς μια άλλη, οι σύγχρονες όμως διαδικτυακές εφαρμογές καταγράφουν τα αιτήματα χρηστών ακόμη και μεταξύ διαφορετικών ιστοσελίδων δημιουργώντας έτσι προφίλ για τις προτιμήσεις του χρήστη ο οποίος τακτοποιείται μέσω της διεύθυνσης IP του υπολογιστή του.
- Hidden Form Fields: Υπάρχουν σε διάφορες ιστοσελίδες κρυμμένες φόρμες HTML στις οποίες αποθηκεύεται ένα ID για τον εκάστοτε χρήστη το οποίο με τις προγραμματιστικές μεθόδους POST και GET κοινοποιείται μεταξύ ιστοτόπων με αποτέλεσμα να γίνεται tracking του χρήστη μεταξύ διάφορων ιστοσελίδων.
- Deep Packet Inspection: Η τεχνική με την οποία οι πάροχοι Internet μπορούν να προσπελάσουν ολόκληρη τη δραστηριότητα ενός χρήστη, αναλύοντας σε βάθος τα πακέτα του δικτύου που δημιουργούνται κατά την περιήγηση.
- Web-Bugs & Third Party Cookies: Είναι η τεχνική κατά την οποία ο δημιουργός της ιστοσελίδας τοποθετεί εικόνες στην ιστοσελίδα οι οποίες φαινομενικά δεν έχουν κάποια λειτουργικότητα αλλά ουσιαστικά κρύβουν τεχνολογίες Third Party Cookies, όπου συλλέγονται δεδομένα για της ενέργειες του χρήστη εντός της ιστοσελίδας και ενημερώνουν τον δημιουργό κάθε φορά που ένας χρήστης επιστρέφει σε αυτή.
- Zombie-Cookies: Καθώς οι χρήστες αρχίζουν να ευαισθητοποιούνται σχετικά με το tracking μέσω cookies οι εταιρίες βρίσκουν παρόμοιες τεχνολογίες, όπως τα Zombie

Cookies ή Super Cookies, τα οποία αποθηκεύονται σε τοποθεσίες δύσκολα προσπελάσιμες από τον χρήστη γεγονός που καθιστά την διαγραφή τους πολύ δύσκολη. Με τον τρόπο αυτό ακόμη και αν ένας χρήστης διαγράψει τα cookies του, τα Super Cookies θα δημιουργήσουν εκ νέου το προφίλ του χρήστη με τα δεδομένα που παρέμειναν και μετά την εκκαθάριση των Flash Cookies.

2.2. Σκοποί αυτόματης παρακολούθησης χρηστών διαδικτύου

Εφόσον αναλύθηκαν οι τεχνολογίες με τις οποίες εκτελείται η αυτόματη παρακολούθηση των χρηστών είναι σημαντικό να αναλυθούν και οι σκοποί παρακολούθησης από τους διάφορους παρόχους υπηρεσιών. Υπάρχουν διάφορες κατηγορίες που μπορούμε να ταξινομήσουμε τις προθέσεις των παροχών, κάποιες έχουν σημαντική επίπτωση στην ιδιωτικότητα των χρηστών ενώ άλλες έχουν χαμηλό βαθμό επικινδυνότητας. Συνήθως trackers περιέχονται στο περιεχόμενο των διαφημιστών εντός τις ιστοσελίδας και όσο πιο καλύτερα στοχευμένες είναι οι διαφημίσεις τόσο περισσότερες αλληλεπιδράσεις θα συλλέξουν και με αυτό τον τρόπο αυξάνεται το κέρδος του διαφημιζόμενου αλλά και του παρόχου της ιστοσελίδας. Τα τελευταία χρόνια έχει μειωθεί το κόστος της απαιτούμενης υπολογιστικής ισχύος για την συλλογή, επεξεργασία και αξιοποίηση των δεδομένων των χρηστών με αποτέλεσμα οι απλές πλέον διεργασίες που χρειάζονται για την στοχευμένη διαφήμιση να είναι πολύ αποτελεσματικές (Alexander Bleier, 2021). Για τους παραπάνω λόγους είναι σημαντικό να μελετηθούν οι τεχνικές με τις οποίες η διαφήμιση γίνεται στοχευμένα.

2.2.1. Contextual Advertising

Ένας πιο κλασσικός όρος του Contextual Advertising θα αφορούσε στον τύπο διαφημίσεων όπου η βάση τους είναι το περιεχόμενο της ιστοσελίδας, δηλαδή με βάση διάφορα key-words τα οποία είναι αντιπροσωπευτικά για το περιεχόμενο της ιστοσελίδας αποφασίζεται αυτόματα από τον διαφημιστή ποια διαφήμιση θα εμφανίσει στον εκάστοτε επισκέπτη (Niklas Schmucker, 2011). Τα τελευταία όμως χρόνια έχει αλλάξει ο τρόπος με τον οποίο λειτουργεί το Contextual Advertising καθώς πλέον αξιοποιούνται και δεδομένα τα οποία πιθανώς παράγει ένας χρήστης κατά την περιήγηση του στην ιστοσελίδα για τα του προταθούν προϊόντα ή υπηρεσίες που είναι πολύ πιθανό να τον αφορούν (Alexander Bleier, 2021). Η προσθήκη πιο περίπλοκων τεχνικών στην στοχευμένη διαφήμιση αυξάνει τους επικείμενους κινδύνους για την ιδιωτικότητα του χρήστη, την ασφάλεια των δεδομένων του και κάνει δυσμενή την ηθική των μεθόδων διαφήμισης (Riabova et al. 2024). Παρά της προκλήσεις που προαναφέρθηκαν, σε σύγκριση με άλλες τεχνικές στοχευμένης

διαφήμισης -όπως το Behavioral Tracking- το contextual advertising είναι ο πιο privacy-friendly τρόπος επίτευξης της (Alexander Bleier, 2021).

2.2.2. Behavioral Tracking

Ως Behavioral Tracking ορίζουμε τις τεχνικές με τις οποίες πάροχοι υπηρεσιών δημιουργούν ένα προφίλ για τον εκάστοτε χρήστη μέσω δεδομένων που συλλέγονται για αυτόν, κατά την περιήγηση του σε διάφορους ιστοτόπους (Niklas Schmucker, 2011). Σύμφωνα με την βιβλιογραφία (Kaan Varnali, 2019) περιέχονται τα εξής στοιχεία στα εξατομικευμένα προφίλ των χρηστών:

1. Έμφυτα χαρακτηριστικά του χρήστη όπως, δημογραφικά δεδομένα, ψυχολογικά χαρακτηριστικά και προδιαθέσεις
2. Αντιλήψεις και πεποιθήσεις σε συνδυασμό με προηγούμενες εμπειρίες
3. Στοιχεία προσαρμοσμένα στην κατάσταση του χρηστή σχετικά με τις άμεσες συνθήκες στις οποίες βρίσκεται την στιγμή που του προτείνεται μια συγκεκριμένη διαφήμιση

Όσο αφορά στον τεχνικό τομέα του Behavioral Tracking αυτό επιτυγχάνεται μέσω των τεχνικών Click-Stream analysis και Client Identification οι οποίες αναλύθηκαν παραπάνω και καθιστούν εφικτή την δημιουργία των εξατομικευμένων προφίλ συλλέγοντας στοιχεία ανάμεσα σε πολυάριθμους ιστοτόπους.

Η σύγχρονη βιβλιογραφία, μας δείχνει πώς οι χρήστες αποδέχονται περισσότερο τις τεχνικές του Behavioral Advertising όταν αυτό γίνεται με διαφάνεια και γνωρίζουν πως γίνεται χρήση των δεδομένων τους για την επίτευξη αυτού (Tucker, 2014; Aguirre et al., 2015; Bleier and Eisenbeiss, 2015a; Boerman et al., 2017). Ενώ είναι εντελώς διαφορετική η κατάσταση όταν οι χρήστες έχουν άγνοια για την συλλογή και επεξεργασία των δεδομένων τους, τότε παρατηρείται πως οι χρήστες αποφεύγουν οποιαδήποτε δραστηριότητα γύρω από τις διαφημίσεις που τους προτείνονται και τις αντιμετωπίζουν με ανησυχία (Aguirre et al., 2015; Boerman et al., 2017). Ένας τρόπος μελέτης των παραπάνω αποτελεσμάτων είναι η παρατήρηση των click των χρηστών όπου οι χρήστες που γνώριζαν τον τρόπο λειτουργίας της στοχευμένης διαφήμισης είχαν μεγαλύτερη πρόθεση για κλικ, ενώ όσοι είχαν άγνοια είχαν και πολύ χαμηλή αλληλεπίδραση με της διαφημίσεις που τους προτάθηκαν (Aiolfi et al. 2021).

2.2.3. Usability Tests & Analytics

Ένας από τους λιγότερο απειλητικούς για την ιδιωτικότητα του χρήστη σκοπούς παρακολούθησης είναι τα Analytics, που χρησιμοποιούνται για τον έλεγχο χρησιμότητας της ιστοσελίδας. Στον τομέα αυτό μέσω scripts JS καταγράφεται το input του χρήστη (ποντίκι & πληκτρολόγιο) εντός μίας ιστοσελίδας με στόχο τον έλεγχο της χρησιμότητας διάφορων elements στην ιστοσελίδα καθώς και το κατά πόσο είναι κατανοητό το περιεχόμενο ανάλογα με την ταχύτητα της περιήγησης του χρήστη.

2.3. Τρόποι προστασίας

Λόγω της πολυπλοκότητας των μεθόδων παρακολούθησης αλλά και της συχνότητας με την οποία συναντώνται δεν είναι πάντα εύκολο οι χρήστες να προστατευτούν πλήρως. Έστω ότι ο χρήστης είναι διατεθειμένος να λάβει αντίμετρα, αλλά δεν είναι πάντοτε εφικτό να χρησιμοποιεί πολλαπλά εργαλεία ασφάλειας μόνο για την πλοήγησή του στο διαδίκτυο, τουλάχιστον όχι μακροχρόνια ή κάθε φορά. Όταν όμως οι χρήστες αποφασίσουν να ενισχύσουν την ιδιωτικότητα τους έχουν μια πληθώρα εργαλείων στην διάθεσή τους τα οποία μπορούν να χρησιμοποιούν με ελάχιστο ή μηδενικό κόστος όπως, IP address protection, End-to-end encryption, Browser Plug ins και τέλος Private Browsing (Sim et al. 2024).

2.3.1. IP address protection

Πολλές φορές η δραστηριότητα του χρήστη παρακολουθείται μέσω tracking της IP διεύθυνσης η οποία αντιστοιχεί στην ταυτότητα του υπολογιστή που χρησιμοποιεί ο χρήστης (Supriyandi et al. 2017). Είναι σημαντικό να σημειωθεί πως μέσω της IP διεύθυνσης μπορούν να ταυτοποιηθούν στοιχεία του χρήστη όπως η φυσική τοποθεσία του, ο πάροχος δικτύου του καθώς και να πραγματοποιηθεί η συλλογή δεδομένων του. Είναι λοιπόν για τους λόγους που προαναφέρθηκαν πολύ σημαντικό να μπορεί να προστατευτεί η διεύθυνση IP. Υπάρχουν τα εξής εργαλεία για την επίτευξη της απόκρυψης και προστασίας μιας IP διεύθυνσης.

- TOR browser: Ένα δίκτυο με υποδομές ανωνυμοποίησης που συντηρείται από εθελοντές και μέσω της τεχνολογίας onion routing προσθέτει στην σύνδεση του χρήστη ένα encryption layer αποφεύγοντας έτσι την ανίχνευση του διακομιστή (Niklas Schmucker 2011).

- Proxies: Τα proxies λειτουργούν ως ενδιάμεσος μεταξύ χρήστη – server και έτσι δεν αποκρύπτεται η IP του χρήστη σε τρίτους παρόχους καθώς αυτοί «βλέπουν» μόνο την IP του proxy provider (Niklas Schmucker 2011).
- Firewalls: Τα Firewalls είναι εργαλεία που επιτρέπουν στον χρήστη να τα τροποποιούν ανάλογα με τις ανάγκες τους και να ορίζουν τους κανόνες επικοινωνίας μεταξύ του προσωπικού τους δικτύου και κάποιου τρίτου (Perez 2014).

2.3.2. End to end encryption technologies

Τεχνολογίες end-to-end encryption είναι αυτές που έχουν την δυνατότητα κατά την επικοινωνία χρήστη – διακομιστή να κρυπτογραφούν τα δεδομένα την στιγμή που τα αποστέλλει ο χρήστης και αυτά να παραμείνουν κρυπτογραφημένα σε ολόκληρη την διάρκεια της μεταφοράς τους μέσω του δικτύου. Όταν τα αρχεία καταλήξουν στον τελικό χρήστη τότε αυτά αποκρυπτογραφούνται και είναι πλέον διαθέσιμα για χρήση στον τελικό τους προορισμό. Με αυτό τον τρόπο ακόμη και αν μέσω κακόβουλων δραστηριοτήτων τρίτων χρηστών, διαρρεύσουν δεδομένα, αυτά θα είναι σε κρυπτογραφημένη μορφή, με τον τρόπο αυτό τα end-to-end encryption tools κρατούν ασφαλή τα δεδομένα του χρήστη.

2.3.3. Browser Plugins & Private Browsing

Υπάρχουν πολλά plug-ins τα οποία οι χρήστες μπορούν χωρίς κόστος να εγκαταστήσουν στον browser που χρησιμοποιούν και να έχουν στην διάθεση τους επιπρόσθετες τεχνικές για την διασφάλιση της ιδιωτικότητάς τους. Τα plug-in προσφέρουν προστασία στους χρήστες μέσω τεχνικών όπως αποκλεισμός ανάγνωσης ιστορικού από τον browser, καθαρισμός HTTP Cookies, αποκλεισμός πρόσβασης στην μνήμη cache της συσκευής του χρήστη και έλεγχος των HTTP requests για προστασία από ανεπιθύμητα redirections.

- Ad-Block: Ίσως το πιο συχνό plug-in που συναντάμε είναι το Ad-block το οποίο προσφέρεται από διάφορους παρόχους και έχει ως σκοπό τον αποκλεισμό διαφημίσεων εντός του browser στον οποίο χρησιμοποιείται. Τα ad-blockers έχουν το θετικό ότι πέρα από τον αποκλεισμό της εμφάνισης διαφημίσεων αποκλείουν και την εκτέλεση διάφορων tracking scripts τα οποία μπορεί να περιέχονται κρυφά στις διαφημίσεις (Lopez et al. 2024).

- Ghostery: Εργαλείο το οποίο εντοπίζει τους trackers που περιέχει η κάθε ιστοσελίδα και στην συνέχεια επιτρέπει στον χρήστη να αποφασίζει ξεχωριστά για κάθε domain το οποίο επισκέπτεται, μέσω ενός toggle, αν θα επιτραπεί η εκτέλεση τους (Lopez et al. 2024).
- NoScript: Περιορίζει πολύ αποτελεσματικά την εκτέλεση scripts στο παρασκήνιο του ιστότοπου τα οποία έχουν δημιουργηθεί για την συλλογή δεδομένων των χρηστών και την παρακολούθηση της δραστηριότητάς τους.
- uBlockOrigin: Αποκλείει trackers και διαφημίσεις με υψηλή ακρίβεια, είναι δημοφιλές γιατί προσφέρει ευελιξία χάρη στις ρυθμίσεις φίλτρων που διαθέτει.

2.4. Επίγνωση των Χρηστών

Λόγω των αυξανόμενων κινδύνων που εντοπίζονται στο διαδίκτυο αναφορικά με την ιδιωτικότητα των δεδομένων, καθίσταται επιτακτική η συζήτηση για την επίγνωση (awareness) των χρηστών. Η φύση των τεχνολογιών παρακολούθησης, οι οποίες λειτουργούν συχνά κρυφά στο παρασκήνιο των browsers και χαρακτηρίζονται από τεχνική πολυπλοκότητα, δυσχεραίνει σημαντικά την ικανότητα των χρηστών να αντιληφθούν τις διαδικασίες αυτές, καθιστώντας την επίγνωσή τους ολοένα και πιο δύσκολη.

2.4.1. Ορισμός της επίγνωσης ιδιωτικότητας

Ο όρος «Επίγνωση της Ιδιωτικότητας των Πληροφοριών» (Information Privacy Awareness - IPA) είναι πολυδιάστατος και δεν διαθέτει έναν καθολικά αποδεκτό ορισμό στη βιβλιογραφία. Οι πρόσφατες μελέτες, αναδεικνύουν την απουσία ενιαίας προσέγγισης του ορισμού του IPA (Tsohou et al., 2021), υπογραμμίζοντας την ανάγκη για περαιτέρω έρευνα και ενοποίηση των διαφορετικών οπτικών. Αρχικά πολλοί ερευνητές ορίζουν το IPA ως την επίγνωση των κινδύνων και των συνεπειών που ενέχει η αποκάλυψη των προσωπικών τους δεδομένων (Deuker, 2010; Konings et al., 2013). Αντιθέτως άλλοι την ορίζουν ως την επίγνωση του περιεχομένου των πολιτικών απορρήτου των υπηρεσιών που χρησιμοποιούν καθώς και των νόμων που προστατεύουν τα δικαιώματα της ιδιωτικότητας (Bergman, 2009; Li et al., 2011). Ταυτόχρονα υπάρχει και μια τρίτη κατηγορία στην οποία έχουμε τους επιστήμονες που την ορίζουν ως την δυνατότητα των χρηστών να προστατεύουν την ιδιωτικότητά τους (Avgerou & Stamatiou, 2015; Omoronyia et al., 2013).

Ποιο συγκεκριμένα η πρώτη προσέγγιση αναλύει απόψεις ερευνητών σχετικά με την επίγνωση των κινδύνων και των απειλών που μπορεί ο χρήστης να συναντήσει καθώς και κατανόηση και

αποδοχή των συνεπειών που ίσως χρειαστεί να αντιμετωπίσει ο χρήστης αφού εκείνος παρέχει τα προσωπικά του δεδομένα (Deuker, 2010). Κατά την οπτική αυτή, είναι επίσης σημαντικό οι χρήστες να κατανοούν πως κατά την εγγραφή τους σε κάποιο κοινωνικό δίκτυο για παράδειγμα τα δεδομένα τους θα κοινοποιηθούν και σε τρίτους με σκοπό την στοχευμένη διαφήμιση (Kuo & Talley, 2014). Όταν οι χρήστες κατανοούν αυτούς τους μηχανισμούς είναι σε μια πολύ καλή θέση ώστε να εκφράζουν ενημερωμένες προσωπικές απόψεις σχετικά με το τι γνωρίζουν οι πάροχοι για αυτούς (Wills & Zeljkovic, 2011).

Σχετικά με την δεύτερη προσέγγιση του ορισμού του IPA συναντάμε μελέτες που υποστηρίζουν ότι ως IPA ορίζουμε την επίγνωση των χρηστών σχετικά με το περιεχόμενο των πολιτικών απορρήτου ή των νόμων οι οποίοι υπερασπίζονται τα δικαιώματα απορρήτου (Li et al., 2011). Ένα παράδειγμα ορισμού που ταυτίζεται με αυτή την προσέγγιση είναι το εξής “Θα μπορούσαμε να ορίζουμε το IPA ως την ικανότητα του χρήστη να αντικατοπτρίζει τις δηλώσεις της πολιτικής απορρήτου σχετικά με τον σκοπό επεξεργασίας, την διαβεβαίωση του τρόπου μεταφοράς και την περίοδο διατήρησης των δεδομένων” (Bergman, 2009, p. 239).

Η τρίτη προσέγγιση ορισμών του IPA αφορά στην ικανότητα των χρηστών να διαχειρίζονται με αυτοπεποίθηση και να προστατεύουν το διαδικτυακό τους απόρρητο (Omoronyia et al., 2013). Ένα παράδειγμα ορισμού που ταυτίζεται με αυτή την προσέγγιση είναι το εξής “Η άμεση αξία της επίγνωσης για το απόρρητο είναι ότι δίνει τη δυνατότητα στους ανθρώπους να προστατεύσουν τα προσωπικά τους δεδομένα. Αλλά η επίγνωση για το απόρρητο σχετίζεται επίσης με την ταχέως εξελισσόμενη αγορά πληροφοριών, της οποίας ο κύριος στόχος είναι τα προσωπικά δεδομένα, συμπεριλαμβανομένων των συνηθειών και των προτύπων ζωής και κινητικότητας των ανθρώπων” (Avgerou & Stamatiou, 2015, p. 44). Αντίστοιχα άλλοι ερευνητές (Omoronyia et al., 2013) δηλώνουν πως IPA είναι το μέσο με το οποίο οι χρήστες γνωρίζουν τον τρόπο με τον οποίο θα πρέπει να χειρίζονται καταστάσεις ευαίσθητες για το προσωπικό απόρρητο καθώς και να βρίσκονται σε θέση να αντιλαμβάνονται της επιπτώσεις ενός συμβάντος και να βρίσκονται σε θέση να μετριά-ζουν τις επιπτώσεις του.

2.4.2. Επίπεδα του IPA

Είναι αρκετά σύνηθες να συναντάμε χρήστες οι οποίοι δεν είναι έγκνηωση καθώς και δεν βρίσκονται σε θέση να κατανοήσουν πλήρως τα θέματα ιδιωτικότητας των δεδομένων τους και με τον τρόπο αυτό οδηγούνται σε λανθασμένες αποφάσεις εκθέτοντας έτσι τα προσωπικά τους δεδομένα κατά την διάρκεια πλοήγησης τους στο διαδίκτυο (Pilton et al. 2021). Στον τομέα της έγκνηωσης των πληροφοριών παρατηρούμε το εξής παράδοξο (Spyros Kokolakis et al. 2015), ενώ έρευνες δείχνουν πως οι χρήστες τιμολογούν το ιστορικό του browser τους στην πολλή χαμηλή τιμή των 7\$, ταυτόχρονα άλλες έρευνες, που μελετούν την διάθεση των χρηστών, μας δείχνουν πως οι χρήστες του διαδικτύου ανησυχούν πολύ για την προστασία της ιδιωτικότητας τους καθώς και την συλλογή των προσωπικών τους δεδομένων. Αυτή η αντίθεση είναι το λεγόμενο παράδοξο της ιδιωτικότητας των δεδομένων.

Σε έρευνα που πραγματοποιήθηκε (Norberg et al. 2007) με τους συμμετέχοντες να είναι φοιτητές αποδείχθηκε πως οι χρήστες στην πραγματικότητα παρέχουν πολύ περισσότερα δεδομένα από ότι είναι διατεθειμένοι να μοιραστούν. Η έρευνα διεξήχθη σε δύο φάσεις: στην πρώτη φάση αξιολογήθηκε η πρόθεση των συμμετεχόντων σχετικά με το εύρος των προσωπικών δεδομένων που ήταν διατεθειμένοι να αποκαλύψουν, ενώ στη δεύτερη φάση, η οποία πραγματοποιήθηκε εβδομάδες αργότερα, οι ίδιοι συμμετέχοντες παρείχαν οικειοθελώς σημαντικά περισσότερες πληροφορίες σε σύγκριση με αυτές που είχαν αρχικά δηλώσει ότι θα κοινοποιούσαν.

Σε διαφορετική έρευνα (Acquisti and Grossklags, 2005) φάνηκε πως το 89% των συμμετεχόντων εξέφρασαν ανησυχίες σχετικά με την προστασία της ιδιωτικότητας τους αλλά στην συνέχεια φάνηκε πως το 21% διαμοιράστηκαν τον προσωπικό τους Αριθμό Μητρώου Κοινωνικής Ασφάλισης, για να λάβουν προσφορές σε προϊόντα, ενώ το 28% διαμοιράστηκαν τους αριθμούς τηλεφώνων τους σε ηλεκτρονικούς εμπόρους κτλ.

Όλα τα παραπάνω παραδείγματα αποδεικνύουν με σαφήνεια ότι, ενώ οι χρήστες εκφράζουν ανησυχίες για την ιδιωτικότητα τους στο διαδίκτυο, στην πράξη αποκαλύπτουν ευαίσθητες προσωπικές πληροφορίες έναντι ελάχιστων ανταμοιβών, χωρίς να λαμβάνουν υπόψη τις πιθανές συνέπειες, γεγονός που υποδηλώνει περιορισμένο επίπεδο έγκνηωσης για το ζήτημα της ιδιωτικότητας.

2.4.3. Τρόποι ενίσχυσης της επίγνωσης της ιδιωτικότητας

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί να αυξηθεί το επίπεδο της επίγνωσης των χρηστών σχετικά με τα θέματα της ιδιωτικότητας των πληροφοριών τους. Ένας από αυτούς τους τρόπους είναι η χρήση διάφορων εργαλείων, όπως για παράδειγμα το Privacy Badge, το οποίο όσο εκτελείται παρουσιάζει στον χρήστη στοιχεία σχετικά με την ιδιωτικότητα του όσο εκείνος αλληλοεπιδρά με υπηρεσίες παρόχων στο διαδίκτυο. Παράλληλα το εν λόγω εργαλείο ενημερώνει τον χρήστη μέσω εικονιδίων και διαφορετικών χρωμάτων ανάλογα με την κατάσταση στην οποία βρίσκονται τα δεδομένα του. Ένα ακόμη εργαλείο που έχει τον ίδιο σκοπό είναι το NoTrace το οποίο εντοπίζει όλα τα δεδομένα του χρήστη που κοινοποιούνται σε τρίτους παρόχους και διαφημιστές και ενημερώνει τον χρήστη ενισχύοντας έτσι την επίγνωση του (Malandrino et al. 2013). Ένας ακόμη τύπος εργαλείου για την ενίσχυση της επίγνωσης των χρηστών είναι τα browser plugins, όπως τα Ghostery, Disconnect και DoNotTrackMe τα οποία σύμφωνα με (Schaub et al. 2016), σχεδιάστηκαν για τον εντοπισμό και τον αποκλεισμό των third-party trackers, ενώ παράλληλα ενημερώνουν τους χρήστες σχετικά με τον αριθμό των trackers που εντοπίστηκαν και αποκλείστηκαν, προσφέροντας επιπλέον τη δυνατότητα διαχείρισης αυτών.

2.4.4. Προφίλ του Aware χρήστη

Είναι σύνηθες φαινόμενο στις επιστημονικές έρευνες να δημιουργούνται από τους ερευνητές διάφορα προφίλ, με στόχο, την προώθηση των θετικών ενεργειών και την αποφυγή των αρνητικών. Παρότι δεν είναι ξεκάθαρος στην βιβλιογραφία ο ορισμός της IPA βασισμένοι στις δύο προσεγγίσεις που προαναφέρθηκαν α. επίγνωση των κινδύνων και των επιπτώσεων απώλειας της ιδιωτικότητας και β. επίγνωση των πολιτικών και νόμων προστασίας της ιδιωτικότητας οι (Tsohou & Soumelidou, 2021) προτείνουν ένα προφίλ χρήστη ο οποίος κατέχει ένα αξιολογικό επίπεδο επίγνωσης εφόσον έχει τα εξής χαρακτηριστικά. Πρωταρχικό χαρακτηριστικό είναι η επίγνωση του χρήστη σχετικά με τις απειλές και τις συνέπειες που σχετίζονται με την αποκάλυψη προσωπικών δεδομένων, γνωρίζει το περιεχόμενο των πολιτικών και νόμων απορρήτου, καθώς και τη διαχείριση καταστάσεων που αφορούν την ιδιωτικότητα. Στην συνέχεια θα πρέπει είναι σε θέση να εκδηλώνει επιφυλακτικότητα και τυχόν ανησυχία που τον καταβάλλει σε σχέση με τον διαμοιρασμό προσωπικών του πληροφοριών. Τρίτο απαραίτητο χαρακτηριστικό του ενήμερου χρήστη η χαμηλή εκδήλωση επικινδυνότητας στην συμπεριφορά του, προσαρμόζοντας τις ρυθμίσεις απορρήτου του

και ελαχιστοποιώντας τις πληροφορίες που κοινοποιεί. Τέλος ο επαρκώς ενήμερος χρήστης είναι εξοικειωμένος με τεχνολογίες ενίσχυσης της ιδιωτικότητας και ενημερώνεται συνεχώς για τις εξελίξεις στον τομέα της προστασίας δεδομένων.

3. Εισαγωγή στην Μεθοδολογία και Σχεδιασμός της Έρευνας

Η παρούσα έρευνα υιοθετεί μικτή μεθοδολογία συνδυάζοντας την ποσοτική αλλά και την ποιοτική προσέγγιση. Κύριος σκοπός της έρευνας είναι η κατανόηση του επιπέδου επίγνωσης των χρηστών σχετικά με την αυτοματοποιημένη παρακολούθηση τους στο διαδίκτυο, την στάση τους απέναντι στις πολιτικές ιδιωτικότητας και τους όρους χρήσης ενώ τέλος εξετάζεται και η χρήση εργαλείων προστασίας των δεδομένων των χρηστών καθώς και η διάθεση τους σχετικά με την μελλοντική τους προστασία. Αρχικά αναπτύχθηκε ένα δομημένο ερωτηματολόγιο 21 ερωτήσεων, οι οποίες βασίζονται στην προ υπάρχουσα βιβλιογραφία και έχουν προσαρμοστεί για να εξυπηρετούν τους σκοπούς της παρούσας έρευνας καλύπτοντας τις θεματικές περιοχές που προαναφέρθηκαν. Για την εξασφάλιση της ποιότητας των ερωτήσεων του ερωτηματολογίου και την εύκολη κατανόηση από τους συμμετέχοντες, διεξήχθη πιλοτική φάση του ερωτηματολογίου με την μορφή συνεντεύξεων όπου 7 συμμετέχοντες, αντιπροσωπευτικοί του δείγματος, απάντησαν σε ανοιχτού τύπου ερωτήσεις βασισμένες στο ερωτηματολόγιο.

3.1 Μεθοδολογία

Για την απάντηση των πρώτων δύο ερευνητικών ερωτημάτων της εργασίας, εκπονήθηκε βιβλιογραφική ανασκόπηση των τελευταίων 15 ετών με στόχο την ολοκληρωτική κατανόηση της αυτόματης παρακολούθησης στο διαδίκτυο, μέσω την συστηματικής μελέτης επιστημονικών πηγών, άρθρων και ερευνών. Η προσέγγιση αφορά σε τρεις θεματικούς άξονες **α)** Τις τεχνολογίες και τις μεθόδους παρακολούθησης των χρηστών, όπως cookies, fingerprinting και behavioral tracking **β)** Τα αντίμετρα και τις τεχνολογίες προστασίας της ιδιωτικότητας που μπορούν να αξιοποιήσουν οι χρήστες όπως plug-ins και privacy browsers **γ)** Την επίγνωση των χρηστών σχετικά με τις τεχνολογίες παρακολούθησης τις απειλές της ιδιωτικότητας τους που προκύπτουν από αυτές. Η επιλογή των πηγών πραγματοποιήθηκε εντός των παρακάτω βιβλιογραφικών βάσεων δεδομένων: Google Scholar, IEEE, ResearchGate, ScienceDirect και PubMed. Ιδιαίτερη έμφαση δόθηκε σε σύγχρονες μελέτες που εξετάζουν τις στάσεις, τις αντιλήψεις και τη συμπεριφορά των χρηστών απέναντι στις πρακτικές παρακολούθησης.

Για την απάντηση του τρίτου αλλά και την ενίσχυση της συνεισφοράς σχετικά με το δεύτερο ερευνητικό ερώτημα, σχεδιάστηκε και υλοποιήθηκε ποσοτική έρευνα με στόχο την αποτύπωση της επίγνωσης των χρηστών σχετικά με την αυτόματη παρακολούθηση στο διαδίκτυο. Το ερωτηματολόγιο αναπτύχθηκε βάσει υπάρχουσών ερευνητικών έργων τα οποία μελετούν σε διεθνές

επίπεδο την επίγνωση των χρηστών για διάφορα θέματα, στα οποία έγιναν προσαρμογές ώστε να ανταποκρίνονται στο πλαίσιο και τους στόχους της παρούσας εργασίας. Αποτελείται από 21 ερωτήσεις και 4 διαφορετικές θεματικές ενότητες που θα αναλυθούν στην συνέχεια. Πριν την διανομή του ερωτηματολογίου εκπονήθηκε πιλοτική φάση, σε μορφή συνεντεύξεων, σε μικρό αντιπροσωπευτικό δείγμα συμμετεχόντων με στόχο την ποιοτική αξιολόγηση των ερωτήσεων καθώς και των θεματικών ενότητων.

3.2 Ανάπτυξη του ερωτηματολογίου

Ο σκοπός για την ανάπτυξη του ερωτηματολογίου της εργασίας είναι η εις βάθος διερεύνηση του επιπέδου επίγνωσης των χρηστών σχετικά με την αυτόματη παρακολούθηση στο διαδίκτυο, τις γνώσεις τους σχετικά με τον τρόπο λειτουργίας των μηχανισμών παρακολούθησης καθώς και της διάθεσης τους σχετικά με την χρήση μέτρων προστασίας, συνιστώντας το βασικό εργαλείο για την ανάλυση των ερευνητικών στόχων της παρούσας εργασίας. Το ερωτηματολόγιο που αναπτύχθηκε αποτελείται από συνολικά 21 ερωτήσεις οι οποίες μπορούν να ταξινομηθούν σε 2 διακριτές κατηγορίες: Α) Ερωτήσεις που έχουν αξιοποιηθεί στο παρελθόν, στην προϋπάρχουσα, διεθνή και εγχώρια βιβλιογραφία. Με προσαρμογές στο θέμα ή την απλοποίηση τους για λόγους κατανόησης, όπου αυτό ήταν απαραίτητο. Β) Ερωτήσεις που σχεδιάστηκαν ειδικά για να ανταποκριθούν στο θεματικό πλαίσιο και τις τεχνολογίες που περιέχονται στην παρούσα εργασία.

Για την ανάπτυξη του ερωτηματολογίου αξιοποιήθηκαν 4 θεματικές ενότητες, οι οποίες θα μας βοηθήσουν να κατανοήσουμε πολυεπίπεδα την επίγνωση των χρηστών σχετικά με την αυτοματοποιημένη παρακολούθηση στο διαδίκτυο. Οι θεματικές ενότητες είναι οι εξής: α) Κατανόηση και επίγνωση σχετικά με tracking μηχανισμούς β) Συμπεριφορά των χρηστών απέναντι στους μηχανισμούς γ) Επίγνωση σχετικά με τον βαθμό παρακολούθησης δ) Στάση απέναντι στα εργαλεία και τις τεχνικές ενίσχυσης της ιδιωτικότητας

Πιο συγκεκριμένα στις πρώτες 8 ερωτήσεις, μελετήθηκε η επίγνωση των χρηστών σχετικά με μηχανισμούς παρακολούθησης όπως τα Web Cookies (Niklas Schmucker, 2011) και το fingerprinting, καθώς και τον τρόπο με τον οποίο τα παραπάνω ενισχύουν την στοχευμένη διαφήμιση. Οι ερωτήσεις αυτές επιχειρούν να εντοπίσουν κατά πόσο οι χρήστες αντιλαμβάνονται τις τεχνολογίες που χρησιμοποιούνται για την παρακολούθηση τους τέλος, αν μπορούν να αναγνωρίσουν αυτές τις τεχνολογίες κατά την πλοήγηση τους (Ruhwanya, 2015). Στην συνέχεια, η δεύτερη ομάδα ερωτήσεων εστιάζει στην συμπεριφορά των χρηστών όταν αυτοί καλούνται να

αλληλοεπιδράσουν με tracking μηχανισμούς όπως για παράδειγμα τα cookies, αποτυπώνοντας την πρόθεση τους να προστατευτούν ή την αδιαφορία τους ώστε να έχουν απλά την πιο γρήγορη πιθανή πρόσβαση στο περιεχόμενο μιας ιστοσελίδας (Bibi, et al. 2017). Στην Τρίτη θεματική ενότητα οι ερωτήσεις επικεντρώνονται στην επίγνωση των χρηστών σχετικά με το επίπεδο της παρακολούθησης στους ιστοτόπους τους οποίους επισκέπτονται καθώς και την αξιοποίηση των δεδομένων που συλλέγονται από trackers (Auxier, et al. 2019). Ενώ τέλος, στην τέταρτη θεματική ενότητα του ερωτηματολογίου εξετάζεται η αντίληψη των χρηστών και η γενικότερη στάση τους απέναντι σε εργαλεία και ενέργειες οι οποίες θα ενισχύσουν την ιδιωτικότητα τους και θα τους βοηθήσουν να παραμένουν πιο ασφαλής κατά την περιήγηση τους στο διαδίκτυο.

Για την αξιολόγηση των απαντήσεων θα αξιοποιηθεί η κλίμακα Likert 5 βαθμών η οποία είναι επιτρέπει στους συμμετέχοντες να εκφράσουν με λεπτομέρεια τον βαθμό συμφωνίας ή διαφωνίας τους με κάποια δήλωση ενώ παράλληλα είναι ευρέως διαδεδομένη στην κοινωνική έρευνα για την μέτρηση στάσεων και αντιλήψεων καθώς μας παρέχει την δυνατότητα ποσοτικοποίησης των ποιοτικών δεδομένων. Η συγκεκριμένη μεθοδολογία περιέχει απαντήσεις που εντάσσονται στην εξής κλίμακα, 1 = Διαφωνώ πλήρως μέχρι και 5 = Συμφωνώ πλήρως, δίνοντας στους συμμετέχοντες ποικιλία επιλογών ανάλογα με την κάθε δήλωση (Likert, 1932; Jamieson, 2005). Ενώ παράλληλα θα υπάρχουν και ερωτήσεις πολλαπλής επιλογής οι οποίες εξετάζουν την συχνότητα των ενεργειών των χρηστών και θα μας βοηθήσουν να κατανοήσουμε καλύτερα την στάση τους, καθώς και ερωτήσεις που μπορούν να απαντηθούν με ναι ή όχι.

Το δείγμα στο οποίο απευθύνεται η παρούσα έρευνα είναι ευρύ και απευθύνεται σε κάθε ενήλικο χρήστη του διαδικτύου, ανεξαρτήτως φύλου, ηλικίας, μορφωτικού επιπέδου ή επαγγελματικής ιδιότητας, έχοντας ως στόχο να εξεταστεί το επίπεδο επίγνωσης, οι στάσεις και οι πρακτικές των συμμετεχόντων σε σχέση με την ιδιωτικότητα τους καθώς και με τις τεχνολογίες παρακολούθησης. Το δείγμα εμπεριέχει τακτικούς χρήστες του διαδικτύου για διάφορους σκοπούς όπως πλοήγηση, κοινωνικά δίκτυα, ηλεκτρονικές αγορές και εφαρμογές επικοινωνίας ώστε να εξασφαλιστεί ποικιλία και η εκπροσώπηση διάφορων ειδών χρήσης του διαδικτύου. Η παραπάνω προσέγγιση ακολουθεί προηγούμενες προσεγγίσεις (Norberg et al., 2007; Boerman et al., 2016) οι οποίες τονίζουν την σημασία της ποικιλίας που πρέπει να υπάρχει στο δείγμα καθώς αυτή συμβάλλει στην κατανόηση της επίγνωσης των χρηστών.

	Το ερωτηματολόγιο της εργασίας
1	Γνωρίζετε τι είναι τα Web Cookies;
2	Διαβάζετε τις πολιτικές Cookies των ιστοσελίδων που επισκέπτεστε;
3	Με ανησυχούν τα cookies των ιστοσελίδων που επισκέπτομαι.
4	Πιστεύω πως οι ιστότοποι με ενημερώνουν επαρκώς για τα στοιχεία που συλλέγουν με την χρήση Web Cookies
5	Γνωρίζετε την διαφορά μεταξύ First-Party και Third-Party cookies?
6	Μπορείτε να αναγνωρίσετε πότε μια ιστοσελίδα χρησιμοποιεί τεχνολογίες παρακολούθησης κατά την περιήγησή σας;
7	Αντιλαμβάνομαι τον μηχανισμό με τον οποίο λειτουργεί η στοχευμένη διαφήμιση
8	Γνωρίζετε πως οι ιστοσελίδες που επισκέπτεστε, δημιουργούν ένα προφίλ προτιμήσεων μου μέσω τεχνολογιών fingerprinting.
9	Αποφεύγετε τη χρήση πιστωτικών καρτών για αγορές στο διαδίκτυο επειδή πιστεύετε πως τα στοιχεία σας αποθηκεύονται από trackers;
10	Αποφεύγετε να κάνετε κλικ σε pop-up διαφημίσεις ώστε να περιορίσετε την παρακολούθηση που αποσκοπεί σε στοχευμένη διαφήμιση;
11	Έχετε αποφύγει τη χρήση κάποιας ιστοσελίδας επειδή απαιτούσε την αποδοχή cookies με τα οποία δεν συμφωνούσατε;
12	Αποδέχεστε τα cookies ακόμη και χωρίς να διαβάσετε τους όρους, ώστε να έχετε εύκολη πρόσβαση στις ιστοσελίδες;
13	Σε τι επίπεδο κατανοείτε πως αξιοποιούν οι trackers τα δεδομένα που συλλέγουν όσο περιηγείστε στο διαδίκτυο
14	Πιστεύετε πως έχετε επαρκή έλεγχο των δεδομένων που συλλέγουν μηχανισμοί όπως cookies και fingerprinting κατά την περιήγησή σας στο διαδίκτυο
15	Πιστεύετε πως οι ιστοσελίδες σας ενημερώνουν επαρκώς για τους μηχανισμούς συλλογής και διαμοιρασμού δεδομένων, όπως τα cookies;
16	Χρησιμοποιείτε εργαλεία anti-tracking για την προστασία από cookies ή από behavioral tracking;
17	Έχετε προσπαθήσει να διαγράψετε ή να μπλοκάρετε trackers από τον browser που χρησιμοποιείτε;
18	Χρησιμοποιείτε συχνά εργαλεία όπως privacy browsers και VPN για την προστασία της ιδιωτικότητάς σας;
19	Έχετε παραμετροποιήσει τις ρυθμίσεις του browser σας ώστε να μειώσετε το αποτύπωμά σας;
20	Έχετε αποφύγει τη χρήση κάποιας ιστοσελίδας στο παρελθόν επειδή ανησυχήσατε για την ιδιωτικότητα σας;
21	Σε κλίμακα 1-5, πώς θα αξιολογούσατε τις γνώσεις σας σχετικά με την αυτοματοποιημένη παρακολούθηση στο διαδίκτυο;

	Πηγές του ερωτηματολογίου
1-8	Ruhwanya, Zainab Said. <i>Attitudes toward, and awareness of, online privacy and security: a quantitative comparison of East Africa and US internet users</i> . Diss. Kansas State University, 2015.
9-13	Bibi, A., Hussain, Z., Khan, F., & Maqsood, A. (2017). <i>Quantitative evaluation of Security and Privacy perceptions in online social networks: A case study</i> . 2017 14th International Bhurban Conference on Applied Sciences and Technology
14-16	Pew Research Center, November 2019, “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information”
16-21	Fortes, Nuno & Rita, Paulo & Pagani, Margherita. (2017). The effects of privacy concerns, perceived risk and trust on online purchasing behaviour. <i>International Journal of Internet Marketing and Advertising</i> . 11. 10.1504/IJIMA.2017.10007887.

3.3 Πιλοτική φάση

Μετά την ανάπτυξη του ερωτηματολογίου εκπονήθηκε πιλοτική φάση δοκιμών των ερωτήσεων σε ένα μικρό αντιπροσωπευτικό δείγμα παρόμοιο με το δείγμα που στοχεύει το ερωτηματολόγιο της εργασίας, με στόχο να εντοπιστούν τυχόν σημεία ασάφειας ή κωλύματα στην κατανόηση των ερωτήσεων ώστε να εξασφαλιστεί πως το ερωτηματολόγιο που αναπτύχθηκε είναι κατάλληλο για το δείγμα - στόχο. Κατά την διάρκεια της πιλοτικής φάσης 10 από τις 23 ερωτήσεις μετατράπηκαν σε ανοιχτού τύπου ώστε να υλοποιηθεί σε κάθε περίπτωση μια σύντομη συζήτηση σχετική με τις θεματικές περιοχές της εργασίας και η καταγραφή της στάσης των συμμετεχόντων. Οι ερωτήσεις που συμπεριλήφθηκαν στην πιλοτική φάση είναι αντιπροσωπευτικές των θεματικών περιοχών του αρχικού ερωτηματολογίου, καθώς βασίζονται στις ίδιες ερωτήσεις, ενώ έγινε παραλλαγή τους ώστε να δίνουν το έναυσμα στον συνεντευξιαζόμενο να εκφράσει τις ειλικρινείς του σκέψεις. Ένα παράδειγμα των παραλλαγών που έγιναν στις ερωτήσεις της πιλοτικής φάσης είναι το εξής.

- **Ερώτηση του ερωτηματολογίου:** Διαβάζετε τις πολιτικές Cookies των ιστοσελίδων που επισκέπτεστε;
- **Ερώτηση 1 των πιλοτικών συνεντεύξεων:** Έχετε διαβάσει κάποια πολιτική Cookies; Αν ναι πόσο συχνά και πως σας φάνηκε; Αν όχι γιατί επιλέγετε να μην τις διαβάσετε

Με την αξιοποίηση ερωτήσεων ανοικτού τύπου, σε σύγκριση με τις ερωτήσεις κλίμακας Likert, γίνεται μια συζήτηση με τον συνεντευξιαζόμενο βοηθώντας μας να αντιληφθούμε την στάση του καθώς και τις γνώσεις του σχετικά με το θέμα συζήτησης, ανάλογα την εκάστοτε ερώτηση. Κατά την εκπόνηση της πιλοτικής φάσης καταγράφηκαν λεπτομερώς μέσω σημειώσεων οι απαντήσεις κάθε συμμετέχοντα βοηθώντας στην διεξαγωγή συμπερασμάτων καθώς και την παραμετροποίηση

του αρχικού ερωτηματολογίου, για την βέλτιστη κατανόηση και γενικότερη εμπειρία του συμμετέχοντα.

3.4 Αποτελέσματα πιλοτικής φάσης και προσαρμογές του ερωτηματολογίου

Η εκπόνηση της πιλοτικής φάσης αποδείχθηκε εξαιρετικά χρήσιμη καθώς συνέβαλε στην παραμετροποίηση του ερωτηματολογίου καθώς και στην δημιουργία αρχικών συμπερασμάτων σχετικά με την επιλογή του δείγματος καθώς και των ερευνητικών υποθέσεων που αναπτύχθηκαν με βάση προηγούμενη βιβλιογραφία. Σχετικά με την θεματική ενότητα που αφορά στην στάση των συμμετεχόντων απέναντι στις πολιτικές cookies, και τον μηχανισμό ως σύνολο, όλοι οι είχαν ακούσει για αυτά ενώ η συντριπτική πλειοψηφία είχε διαβάσει τουλάχιστον μία από πολιτική, ταυτόχρονα όμως όλοι τις θεώρησαν υπερβολικά εκτενή και κουραστικά κείμενα, με αποτέλεσμα να μην αποκτούν την ανάγνωση των πολιτικών ως συνήθεια. Η πλειονότητα των συμμετεχόντων έδειξε να έχει ανησυχίες για τα προσωπικά στοιχεία που συλλέγονται από μη ορατούς μηχανισμούς χωρίς όμως να γνωρίζουν τρόπους με τους οποίους μπορούν να προστατευτούν από αυτούς. Παράλληλα σε σχέση με την ερώτηση που αφορά στην στοχευμένη διαφήμιση υπήρξε ποικιλία απαντήσεων. Μια μερίδα των χρηστών φάνηκε να αδιαφορεί για τις στοχευμένες διαφημίσεις και να απολαμβάνει απλώς την διευκόλυνση που τους παρέχουν τα στοχευμένα προϊόντα ενώ άλλοι νιώθουν άβολα με αυτές και προσπαθούν να μειώσουν την έκθεσή τους σε παρόμοιες διαφημίσεις. Κοινό στοιχείο και των δύο ομάδων όμως ήταν πως δεν γνώριζαν τον τρόπο με τον οποίο γίνονται υποκείμενα στοχευμένης διαφήμισης, δηλαδή τις τεχνολογίες και τους μηχανισμούς πίσω από αυτή. Μόνο 2 από τους 7 συμμετέχοντες φάνηκαν να χρησιμοποιούν εργαλεία ιδιωτικότητας όπως privacy browsers και plug-ins.

Οι προσαρμογές που αφορούν στο ερωτηματολόγιο αφορούν στην αφαίρεση κάποιων ερωτήσεων καθώς αποτελούσαν επανάληψη και θα μείωναν το επίπεδο της ποιότητας εμπειρίας τους χρήστη, κάποιες άλλες απλοποιήθηκαν είτε μειώνοντας την έκταση των προτάσεων είτε απλοποιώντας τους όρους που χρησιμοποιήθηκαν, μετατρέποντας τους σε πιο απλούς με τους οποίους οι συμμετέχοντες θα ήταν πιο εξοικειωμένοι.

3.5 Διανομή του ερωτηματολογίου

Το ερωτηματολόγιο διανεμήθηκε διαδικτυακά μέσω Google Forms και κοινοποιήθηκε σε κοινωνικά δίκτυα όπως Facebook και Instagram. Η χρήση αυτών των καναλιών έκανε εφικτή την

συλλογή απαντήσεων από άτομα κάθε ηλικιακής ομάδας, μορφωτικού επιπέδου και βαθμού εξοικείωσης με την τεχνολογία. Το ερωτηματολόγιο της έρευνας παρέμεινε διαθέσιμο Online για 10 ημέρες ενώ διασφαλίστηκε η ανωνυμία και η εθελοντική συμμετοχή όλων των συμμετεχόντων. Συνολικά συγκεντρώθηκαν 68 απαντήσεις, οι οποίες αποτέλεσαν το δείγμα της έρευνας και το βασικό αντικείμενο της ανάλυσης της παρούσας εργασίας.

4. Αποτελέσματα

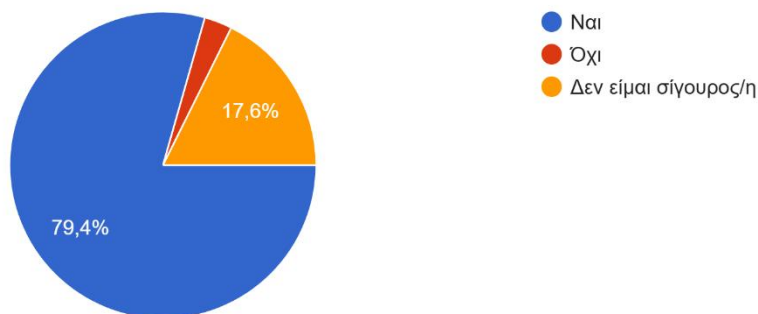
Στο παρόν κεφάλαιο παρουσιάζονται και αναλύονται τα αποτελέσματα που προέκυψαν από την διανομή του ερωτηματολογίου με στόχο την διερεύνηση του επιπέδου επίγνωσης των χρηστών σχετικά με την αυτόματη παρακολούθηση στο διαδίκτυο, την στάση τους απέναντι στους μηχανισμούς συλλογής δεδομένων καθώς και την χρήση εργαλείων προστασίας της ιδιωτικότητάς. Η ανάλυση των αποτελεσμάτων βασίζεται στους τέσσερις άξονες που προαναφέρθηκαν και η ερμηνεία των αποτελεσμάτων γίνεται σε συνάρτηση με την βιβλιογραφία που αναλύθηκε σε προηγούμενα κεφάλαια της παρούσας εργασίας, ώστε να εντοπιστούν ταυτίσεις, αποκλείσεις και οποιεσδήποτε ενδιαφέρουσες τάσεις θα συνεισφέρουν στην συνολική κατανόηση του φαινομένου. Σχετικά με τα δημογραφικά στοιχεία της έρευνας, από τους 68 συμμετέχοντες το 57.4% ήταν γυναίκες και το 42.6% ήταν άνδρες ενώ η πλειοψηφία άνηκε στην ηλικιακή ομάδα 18-24 και τέλος το 66.2% είχαν ως εκπαιδευτικό επίπεδο το πανεπιστήμιο και το 19.1% κατείχαν μεταπτυχιακό.

4.1. Κατανόηση και επίγνωση σχετικά με tracking μηχανισμούς

Η πρώτη θεματική ενότητα που εξετάζει το ερωτηματολόγιο της παρούσας εργασίας αφορά στην κατανόηση των χρηστών σχετικά με tracking μηχανισμούς. Όπως φαίνεται στα παρακάτω γραφήματα τα οποία μας προσφέρουν ένα αντιπροσωπευτικό στιγμιότυπο της συμπεριφοράς των χρηστών του διαδικτύου. Η πλειοψηφία των χρηστών (79.4%) γνωρίζει σαν όρο τα web cookies, ενώ το 17.6% των συμμετεχόντων δηλώνει αβεβαιότητα. Παρότι όμως φαίνεται να υπάρχει υψηλή επίγνωση του μηχανισμού, αυτή φαίνεται να είναι επιφανειακή καθώς μόνο 2.9% των συμμετεχόντων δήλωσαν πως πάντοτε διαβάζουν τις πολιτικές cookies των ιστοσελίδων που επισκέπτονται, ενώ ταυτόχρονα το 54.4% των συμμετεχόντων δεν τις διαβάζουν ποτέ και το 27.9% δήλωσαν σπάνια. Τα παραπάνω ευρήματα μας αποδεικνύουν πως παρότι οι χρήστες γνωρίζουν την ύπαρξη μηχανισμών που συλλέγουν δεδομένα τους, παραμένουν αδιάφοροι.

1. Γνωρίζετε τι είναι τα Web Cookies;

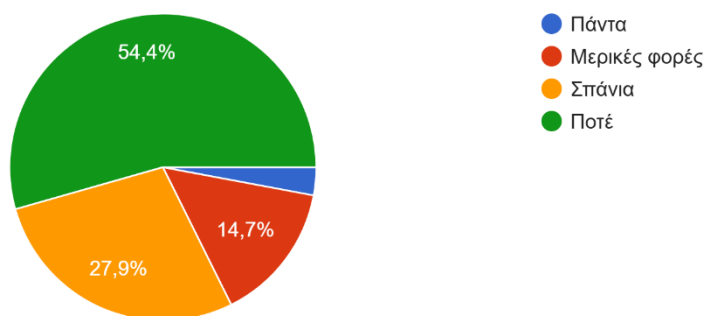
68 απαντήσεις



Γράφημα 1: Η επίγνωση των χρηστών σχετικά με την τεχνολογία cookies.

2. Διαβάζετε τις πολιτικές Cookies των ιστοσελίδων που επισκέπτεστε

68 απαντήσεις



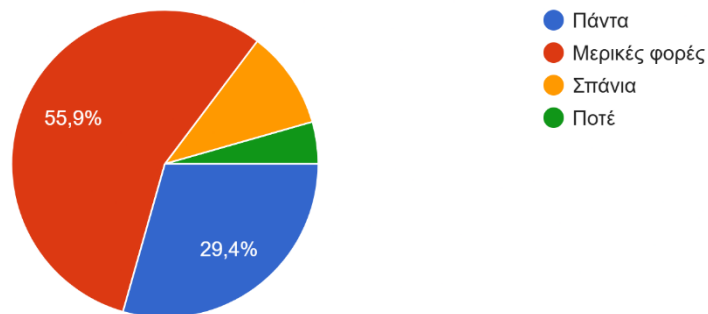
Γράφημα 2: Διάθεση των χρηστών απέναντι στις πολιτικές Cookies.

Το παραπάνω φαινόμενο της απάθειας των χρηστών απέναντι σε μηχανισμούς παρακολούθησης ενισχύεται και από τα ευρήματα που θα συζητήσουμε στην συνέχεια. Η συντριπτική πλειοψηφία των χρηστών φαίνεται πως αποδέχονται αμέσως τις πολιτικές cookies των ιστοτόπων που επισκέπτονται, χωρίς να διαβάσουν τους όρους των πολιτικών, με στόχο την αμεσότερη και απλούστερη πρόσβαση τους σε μια ιστοσελίδα. Πιο συγκεκριμένα το 29.4% των χρηστών δήλωσαν πως πάντοτε αποδέχονται τα cookies χωρίς να διαβάσουν τις πολιτικές ενώ το 55.9% δήλωσε μερικές φορές, 10,3% δήλωσαν σπάνια ενώ μόνο το 4.4% των συμμετεχόντων δήλωσαν πως ποτέ δεν

αποδέχονται τα cookies μόνο για την αμεσότερη πρόσβαση σε κάποιον ιστότοπο. Παράλληλα είναι σημαντικό να σημειωθεί πως η πλειοψηφία των χρηστών δήλωσε πως δεν γνωρίζουν την διαφοροποίηση μεταξύ των όρων First-Party και Third-Party cookies, το 61.8% δήλωσαν πως δεν γνωρίζουν, το 20.6% δήλωσαν την επιλογή Δεν είμαι σίγουρος/η και μόνο το 17.6% δήλωσαν πως γνωρίζουν την διαφοροποίηση. Με τον τρόπο αυτό αρχίζουμε να κατανοούμε πως η επίγνωση των χρηστών σχετικά με τον μηχανισμό των cookies είναι αρκετά επιφανειακή και περιορίζεται ίσως στην επίγνωση του όρου και όχι της λειτουργικότητας ή των χαρακτηριστικών του μηχανισμού.

Αποδέχεστε τα cookies ακόμη και χωρίς να διαβάσετε τους όρους, ώστε να έχετε εύκολη πρόσβαση στις ιστοσελίδες;

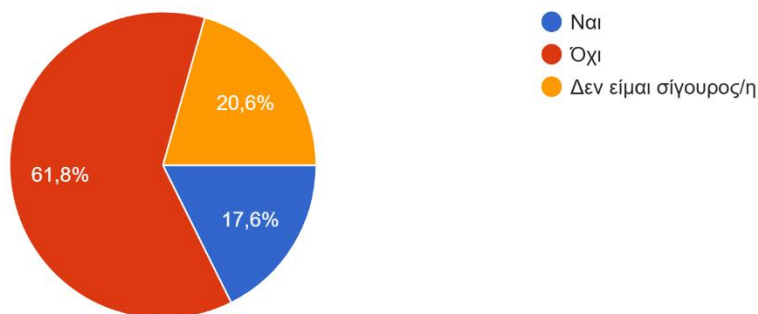
68 απαντήσεις



Γράφημα 3: Αποδοχή των cookies από τους χρήστες για πιο άμεση πλοήγηση.

Γνωρίζεται την διαφορά μεταξύ First-Party και Third-Party Cookies;

68 απαντήσεις

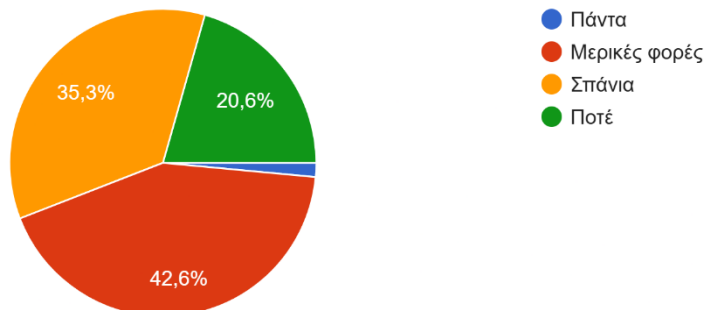


Γράφημα 4: Επίγνωση των χρηστών σχετικά με την διαφοροποίηση First / Third Party cookies.

Επίσης οι χρήστες ερωτήθηκαν, για το αν μπορούν να αναγνωρίσουν πότε μια ιστοσελίδα χρησιμοποιεί τεχνολογίες παρακολούθησης κατά την περιήγηση σε αυτή. Προφανώς αυτή η ερώτηση στοχεύει στον έλεγχο της επίγνωσης των χρηστών σχετικά με τους εμφανείς τρόπους tracking, όπως τα pop-up banners, τις ανακατευθύνσεις ιστοσελίδας και τις στοχευμένες διαφημίσεις, χωρίς την χρήση εξωτερικών εργαλείων και add-ons καθώς θεωρούμε πως έχουμε εύρη κοινό και όχι χρήστες με εξειδικευμένες γνώσεις. Τα αποτελέσματα στην συγκεκριμένη ερώτηση δεν είναι αποθαρρυντικά, αντιθέτως δείχνουν πως οι χρήστες έχουν μια στοιχειώδη τουλάχιστον εικόνα για τον τρόπο που μπορεί να γίνεται tracking. Πιο συγκεκριμένα το 20.6% των χρηστών δήλωσαν πως ποτέ δεν μπορούν να αναγνωρίσουν πότε μια ιστοσελίδα χρησιμοποιεί tracking μηχανισμούς, αντιθέτως όμως την επιλογή σπάνια επέλεξε το 35.3% και την επιλογή μερικές φορές επέλεξε το 42.6%. Τα δύο τελευταία ποσοστά, συνδυαστικά, μας δίνουν την εικόνα πως οι περισσότεροι χρήστες μπορούν να κατανοήσουν πότε συλλέγονται δεδομένα τους, ασχέτως της συχνότητας ή του επιπέδου της βεβαιότητας τους για το συμβάν.

Μπορείτε να αναγνωρίσετε πότε μια ιστοσελίδα χρησιμοποιεί τεχνολογίες παρακολούθησης κατά την περιήγησή σας;

68 απαντήσεις

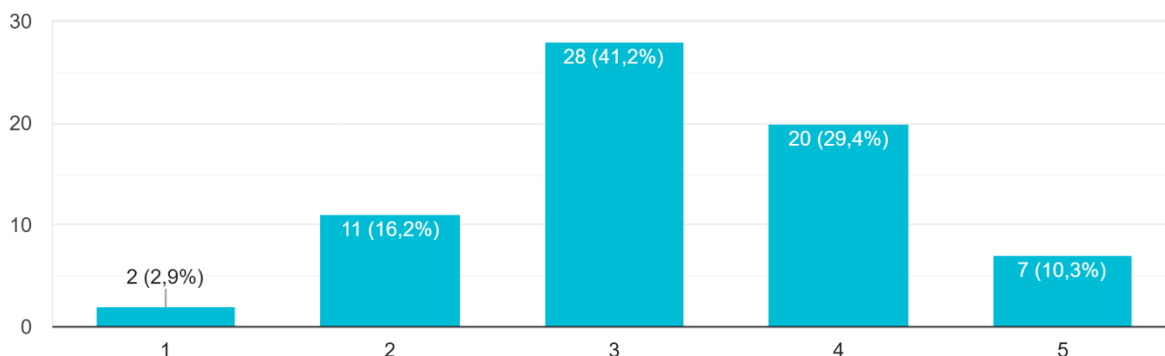


Γράφημα 5: Κατανόηση των χρηστών σχετικά με την συχνότητα χρήσης τεχνολογιών παρακολούθησης από τις ιστοσελίδες.

Το παρακάτω γράφημα απεικονίζει τον βαθμό ανησυχίας των χρηστών του διαδικτύου σε σχέση με τα cookies των ιστότοπων που επισκέπτονται και γενικότερα μας φανερώνει μια μέτρια στάση. Πιο συγκεκριμένα το 41.2% ανήκουν στο επίπεδο 3, ακριβώς στην μέση της κλίμακας ενώ το 29.4% επιλέγει τον βαθμό 4. Το ποσοστό που δηλώνει έντονη ανησυχία, επιλέγοντας το επίπεδο 5, είναι μόλις το 10.3% των συμμετεχόντων ενώ το 19.1% κατατάσσονται στα χαμηλότερα επίπεδα ανησυχίας επιλέγοντας τα επίπεδα 1 και 2. Εν μέρει τα παραπάνω στοιχεία ενισχύουν την μετριοπάθεια των χρηστών καθώς οι περισσότεροι ανήκουν στο τρίτο επίπεδο της κλίμακας, είναι όμως ενθαρρυντικό πως το ποσοστό στα υψηλότερα επίπεδα είναι μεγαλύτερο από αυτό που βρίσκεται στα χαμηλότερα.

Με ανησυχούν τα cookies των ιστοσελίδων που επισκέπτομαι

68 απαντήσεις

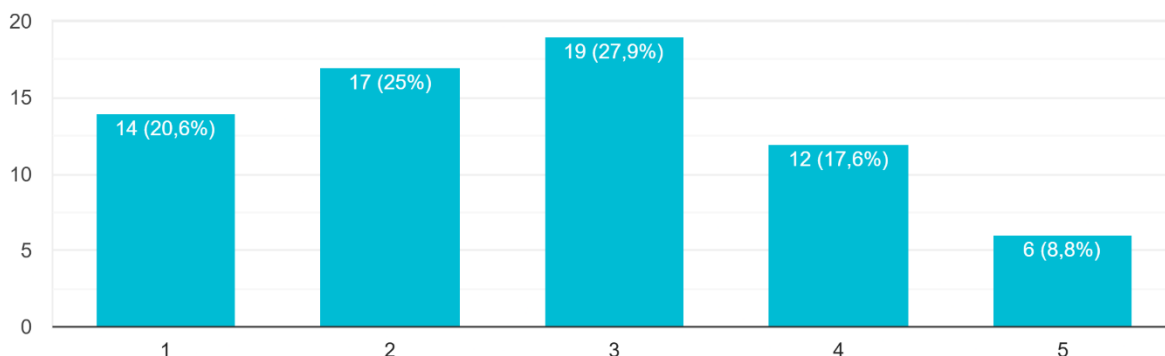


Γράφημα 6: Επίπεδο ανησυχίας των χρηστών σε σχέση με τα cookies.

Μια πολύ σημαντική λειτουργία των cookies είναι η διαφήμιση και για αυτόν τον λόγο είναι σημαντικό ο διαχωρισμός μεταξύ First και Third Party cookies. Στο γράφημα που ακολουθεί θα εξετάσουμε το επίπεδο της επίγνωσης των χρηστών σχετικά με τον τρόπο λειτουργίας της στοχευμένης διαφήμισης. Από τις απαντήσεις προκύπτει πως η γενική κατανόηση των χρηστών είναι περιορισμένη. Πιο συγκεκριμένα σχεδόν οι μισοί συμμετέχοντες κατατάσσονται στα πρώτα δύο επίπεδα της κλίμακας με το 20.6% να δηλώνει πως δεν αντιλαμβάνονται καθόλου τον μηχανισμό (επίπεδο 1) και το 25% βρίσκεται στο επίπεδο 2. Δηλαδή συνδυαστικά το 45.6% των συμμετεχόντων δηλώνει ουσιαστική άγνοια ή ένα πολύ χαμηλό επίπεδο κατανόησης. Το μεγαλύτερο ποσοστό συγκέντρωσε το τρίτο επίπεδο με 27.9% εκφράζοντας μερική κατανόηση χωρίς να φαίνεται να υπάρχει επίγνωση σχετικά με τους μηχανισμούς και τις τεχνικές που εμπλέκονται στην στοχευμένη διαφήμιση. Μόνο ένα μικρό ποσοστό βρίσκεται στο πέμπτο επίπεδο με 8.8% δηλώνοντας πως κατανοούν πλήρως τον τρόπο με τον οποίο λειτουργεί η στοχευμένη διαφήμιση, γεγονός που φανερώνει το χάσμα ανάμεσα στον βαθμό έκθεσης των χρηστών σε στοχευμένο περιεχόμενο και την κατανόηση του τρόπου με τον οποίο αυτό λειτουργεί.

Αντιλαμβάνομαι τον μηχανισμό με τον οποίο λειτουργεί η στοχευμένη διαφήμιση

68 απαντήσεις

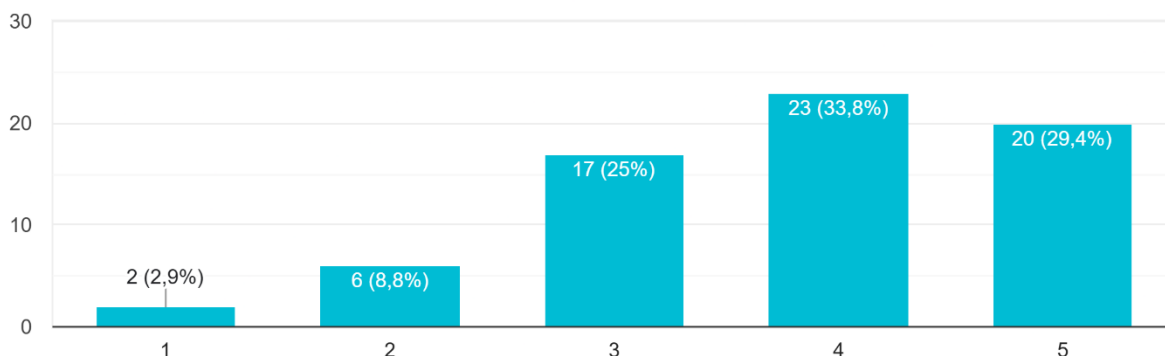


Γράφημα 7: Επίπεδο επίγνωσης σχετικά με τον μηχανισμό της στοχευμένης διαφήμισης.

Στην συνέχεια ζητήθηκε από τους χρήστες να δηλώσουν τον βαθμό ενόχλησης τους από τις διαφημίσεις οι οποίες είναι στοχευμένες στα ενδιαφέροντα τους. Οι διαφημίσεις αυτού του τύπου είναι ξεκάθαρα παρεμβατικές και επακόλουθο της χρήσης μηχανισμών cookies από τις διάφορες ιστοσελίδες που τους αξιοποιούν. Τα αποτελέσματα στην συγκεκριμένη περίπτωση είναι ξεκάθαρα και κατά κύριο λόγο αναμενόμενα. Στην κλίμακα 5 επιπέδων μόνο το 2.9% επέλεξε το επίπεδο 1 και το 8.8% επέλεξε το επίπεδο 2 δείχνοντας καμία έως χαμηλή ενόχληση. Στην συνέχεια έχουμε 25% των χρηστών στο επίπεδο 3, ακριβώς στην μέση της κλίμακας ενώ η πλειοψηφία των χρηστών συγκεντρώνεται στα 2 υψηλότερα επίπεδα με το τέταρτο να συγκεντρώνει 33.8% και το πέμπτο και υψηλότερο 29.4%. Είναι σαφές πλέον πως οι χρήστες θεωρούν τις διαφημίσεις αυτές παρεμβατικές και κατανοούν πως αξιοποιούνται δεδομένα προηγούμενης πλοήγησης τους. Είναι θετικό πως οι χρήστες κατανοούν τον επιβαρυντικό τρόπο με τον οποίο αυτές οι διαφημίσεις λειτουργούν και αποφεύγουν να της ακολουθούν.

Βρίσκετε ενοχλητικές τις διαφημίσεις που είναι σχετικές με τα ενδιαφέροντά σας;

68 απαντήσεις

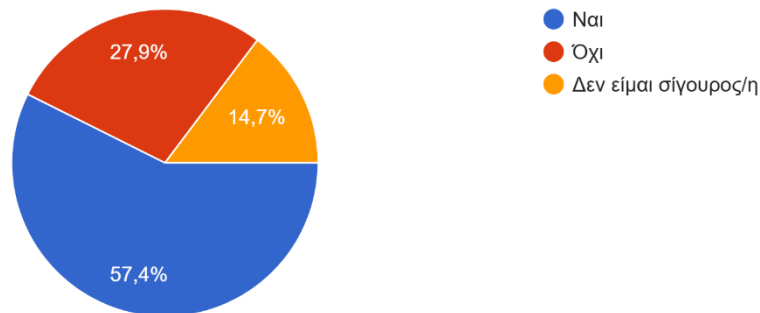


Γράφημα 8: Επίπεδο ανησυχίας των χρηστών αναφορικά με διαφημίσεις που στοχεύουν στα ενδιαφέροντα τους.

Στο τέλος αυτής της θεματικής ενότητας του ερωτηματολογίου, η οποία αφορά στην κατανόηση και επίγνωση των tracking μηχανισμών εξετάσαμε κατά πόσο οι χρήστες είναι εξοικειωμένοι με τον όρο fingerprinting. Είναι σημαντικό να σημειωθεί πως το browser fingerprinting, σαν μηχανισμός, αποτελεί μια πιο προηγμένη τεχνολογία από τα cookies, είναι πολύ πιο σύνθετο από και κυρίως εκτελείται στο παρασκήνιο. Δεν υπάρχει κάποια πολιτική που πρέπει ο χρήστης να αποδεχτεί ή κάποιο pop up banner όταν εκτελούνται fingerprinting μηχανισμοί. Αρχικά έχουμε ένα μεγάλο ποσοστό συμμετεχόντων, το 57.4% να δηλώνουν πως γνωρίζουν για την δημιουργία ψηφιακών προφίλ προτιμήσεων μέσω τεχνολογιών fingerprinting, με το 27.9% να δηλώνει άγνοια ενώ τέλος το 14.7% των συμμετεχόντων δήλωσαν πως δεν είναι σίγουροι. Είναι φανερό πως οι χρήστες του διαδικτύου είναι περισσότερο εξοικειωμένοι με τεχνολογίες όπως τα cookies και λιγότερο με άλλες όπως το fingerprinting. Επίσης είναι πολύ πιθανό οι χρήστες να είναι περισσότερο εξοικειωμένοι με την ιδέα πως δημιουργούνται προφίλ των προτιμήσεων τους όσο εκείνοι εκτελούν ενέργειες στο διαδίκτυο, αλλά να αγνοούν τον τρόπο με τον οποίο δημιουργούνται αυτά τα προφίλ.

Γνωρίζετε πως οι ιστοσελίδες που επισκέπτεστε, δημιουργούν ένα προφίλ προτιμήσεων μέσω τεχνολογιών fingerprinting;

68 απαντήσεις



Γράφημα 9: Επίπεδο επίγνωσης σχετικά με τον μηχανισμό fingerprinting.

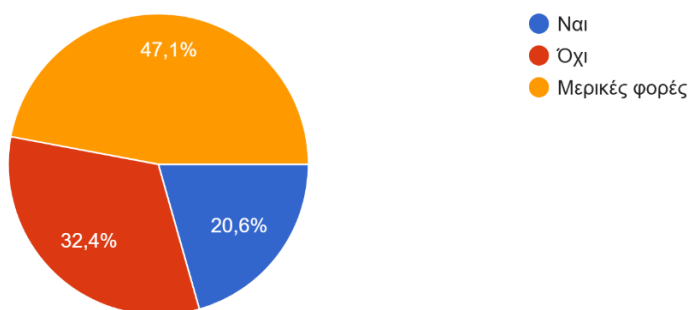
4.2. Συμπεριφορά των χρηστών απέναντι στους μηχανισμούς αυτόματης παρακολούθησης

Εφόσον εξετάσαμε την επίγνωση των χρηστών σχετικά με τους μηχανισμούς αυτόματης παρακολούθησης στο διαδίκτυο και κατά πόσο αυτή είναι επιφανειακή, είναι χρήσιμο να κατανοήσουμε και την στάση τους απέναντι σε αυτούς τους μηχανισμούς σε μεγαλύτερο βάθος. Παραπάνω αναφέρθηκε πως οι χρήστες, σε μεγάλο βαθμό δεν διαβάζουν τις πολιτικές cookies πριν τις αποδεχτούν, είναι σημαντικό να κατανοήσουμε αν η συμπεριφορά τους είναι παρόμοια απέναντι σε άλλους μηχανισμούς και πως αντιδρούν σε ορισμένες καταστάσεις για να προστατευτούν. Πιο συγκεκριμένα αυτές οι καταστάσεις αφορούν ηλεκτρονικές αγορές και την χρήση πιστωτικών καρτών, την αντίδραση των χρηστών σε pop-up banners και την πιθανή αποφυγή κάποιας ιστοσελίδας λόγω της πολιτικής της cookies.

Με το παρακάτω γράφημα εξετάζουμε τον βαθμό ανησυχίας των χρηστών ως προς την προστασία ευαίσθητων στοιχείων όπως αυτά μιας πιστωτικής κάρτας από μηχανισμούς παρακολούθησης, κατά την διαδικασία ψηφιακών αγορών. Αρχικά το ποσοστό των χρηστών που δήλωσαν πως αποφεύγουν τις αγορές με πιστωτική / χρεωστική κάρτα στο διαδίκτυο ήταν 20.6% ενώ ένα σημαντικά μεγαλύτερο ποσοστό των χρηστών, το 47.1% δήλωσαν πως αποφεύγουν τις εν λόγω συναλλαγές μόνο σε ορισμένες περιπτώσεις. Αντιθέτως το 32.4% των συμμετεχόντων δηλώνουν πως δεν

αποφεύγουν την χρήση καρτών στο διαδίκτυο γεγονός που δηλώνει είτε την εμπιστοσύνη αυτών των χρηστών προς τις διαδικτυακές πλατφόρμες, είτε την έλλειψη ανησυχίας σχετικά με την παρακολούθηση προσωπικών οικονομικών δεδομένων.

Αποφεύγετε τη χρήση πιστωτικών / χρεωστικών καρτών για αγορές στο διαδίκτυο επειδή πιστεύετε πως τα στοιχεία σας αποθηκεύονται από trackers;
68 απαντήσεις

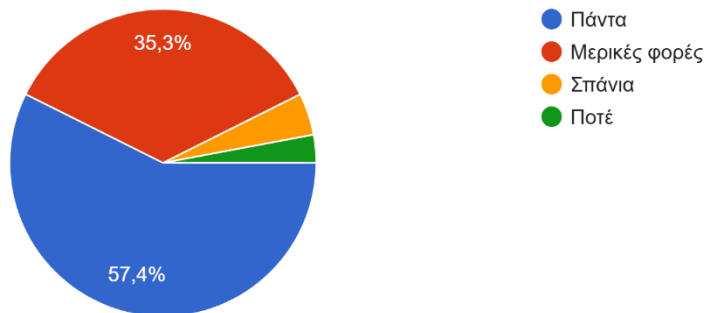


Γράφημα 10: Διάθεση των χρηστών σχετικά με τις ηλεκτρονικές αγορές και την χρήση πιστωτικών καρτών.

Μια αρκετά διαδεδομένη τεχνική από παρόχους ιστοσελίδων για να συλλέξουν δεδομένα των χρηστών τους αλλά και να προωθήσουν συγκεκριμένα προϊόντα που θα ταιριάζουν στο προφίλ του εκάστοτε καταναλωτή είναι τα pop-ups. Καθώς η τεχνική αυτή έχει ως σκοπό να κερδίσει το κλικ του χρήστη με διάφορους τρόπους, είναι ξεκάθαρη και φανερή και όπως φαίνεται και από τα αποτελέσματα του γραφήματος οι χρήστες γνωρίζουν τον τρόπο λειτουργίας των pop-up και τα αποφεύγουν. Το 57.4% των χρηστών δήλωσαν πως πάντα αποφεύγουν τις εν λόγω διαφημίσεις και το 35.3% χρηστών δήλωσαν πως το κάνουν μερικές φορές.

Αποφεύγετε να κάνετε κλικ σε pop-up διαφημίσεις ώστε να περιορίσετε την παρακολούθηση που αποσκοπεί σε στοχευμένη διαφήμιση;

68 απαντήσεις

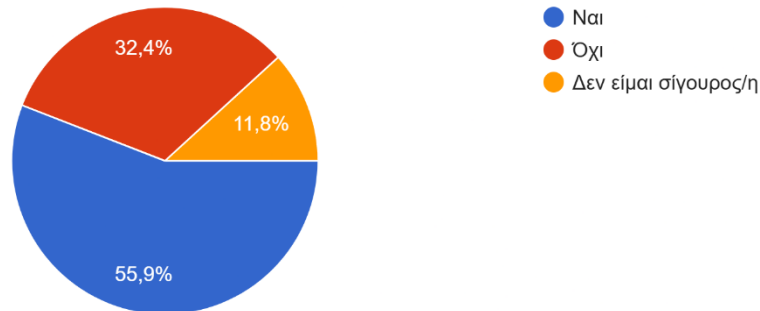


Γράφημα 11: Αντίδραση των χρηστών απέναντι στα pop up banners.

Στο τελευταίο μέρος αυτής της θεματικής ενότητας τους ερωτηματολογίου εξετάζουμε κατά πόσο οι χρήστες έχουν αποφύγει την χρήση κάποιας ιστοσελίδας λόγω των όρων που περιείχε η πολιτική των cookies. Φαίνεται πως η πλειοψηφία των χρηστών, πιο συγκεκριμένα το 55.9% έχουν αποφύγει κάποια ιστοσελίδα λόγω των όρων των cookies, με το 32.4% να δηλώνει το αντίθετο και το 11.8% να διαλέγει την επιλογή δεν είμαι σίγουρος/η. Δεν μπορούμε να εξάγουμε με βεβαιότητα το συμπέρασμα πως στην πραγματικότητα οι χρήστες διάβασαν κάποια πολιτική και την θεώρησαν παρεμβατική ή ενοχλητική, κρίνοντας από προηγούμενα αποτελέσματα, (βλ. γραφήματα 2 & 3) τα οποία φανερώνουν πως οι χρήστες είτε δεν διαβάζουν ποτέ τις πολιτικές είτε αποδέχονται αμέσως τα cookies για την αμεσότερη πλοήγηση τους. Αυτό που μπορούμε όμως να συμπεράνουμε από το παρακάτω γράφημα είναι πως η πλειοψηφία των χρηστών κάποια στιγμή κατά την περιήγηση τους έχουν νιώσει ανασφάλεια ή έχουν ενοχληθεί από τα cookies των ιστοτόπων που επισκέπτονται που απέφυγαν ολοκληρωτικά την χρήση κάποιας ιστοσελίδας ώστε να μην αποδεχθούν τα cookies αυτής. Γεγονός που μπορεί να οφείλεται είτε στον αναγκαστικό τρόπο παρουσί-ασης των cookies σε ορισμένες ιστοσελίδες, κατά τον οποίο έμμεσα η αποδοχή των όρων είναι η μόνη επιλογή, είτε στην γενικότερη επίγνωση των χρηστών όπου γνωρίζουν πως τα cookies είναι μηχανισμοί συλλογής δεδομένων και απλώς απέφυγαν την χρήση κάποιας ιστοσελίδας για τον λόγο αυτό.

Έχετε αποφύγει τη χρήση κάποιας ιστοσελίδας επειδή απαιτούσε την αποδοχή cookies με τα οποία δεν συμφωνούσατε;

68 απαντήσεις



Γράφημα 12: Αποφυγή της χρήσης ιστοσελίδας από τους συμμετέχοντες λόγω πολιτικής cookies.

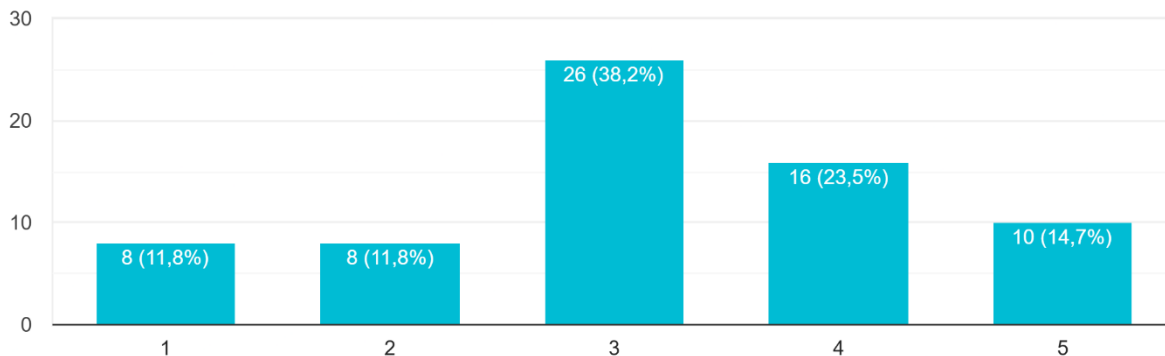
4.3. Επίγνωση των χρηστών σχετικά με τον βαθμό παρακολούθησης

Στην παρούσα θεματική ενότητα της έρευνας θα εξετάσουμε την επίγνωση των χρηστών σχετικά με τον βαθμό της αυτοματοποιημένης παρακολούθησης στο διαδίκτυο. Σκοπός είναι να αναλυθεί το επίπεδο της κατανόησης που έχουν οι χρήστες σχετικά με το πως συλλέγονται, αποθηκεύονται και αξιοποιούνται τα δεδομένα τους από tracking μηχανισμούς.

Στο γράφημα που ακολουθεί φαίνεται πως οι χρήστες αξιολογούν την αντίληψη τους ως προς τους τρόπους αξιοποίησης των δεδομένων που συλλέγουν οι trackers κυρίως στο μεσαίο επίπεδο, πιο συγκεκριμένα το 38.2% επέλεξε το τρίτο επίπεδο ενώ τα επίπεδα 4 και 5 αθροιστικά ξεπέρασαν τα επίπεδα 1 και 2. Φαίνεται πως οι χρήστες που επέλεξαν τα επίπεδα 4 και 5 με ποσοστά 23.5% και 14.7% αντίστοιχα γνωρίζουν τρόπους με τους οποίους πιθανώς να αξιοποιούν οι trackers τα δεδομένα τους. Δυστυχώς όμως η πλειοψηφία των χρηστών φαίνεται να είναι απλώς παθητικοί αποδέκτες της παρακολούθησης.

Σε τι επίπεδο κατανοείτε πως αξιοποιούν οι trackers τα δεδομένα που συλλέγουν όσο περιηγείστε στο διαδίκτυο;

68 απαντήσεις

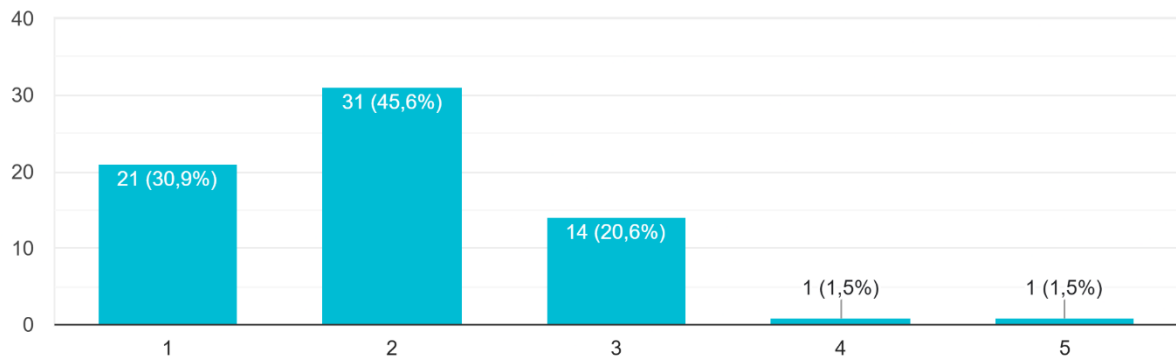


Γράφημα 13: Αποφυγή της χρήσης ιστοσελίδας από τους συμμετέχοντες λόγω πολιτικής cookies.

Στην συνέχεια ζητήθηκε από τους συμμετέχοντες να επιλέξουν το επίπεδο ελέγχου που θεωρούν ότι κατέχουν, στα δεδομένα που συλλέγονται από μηχανισμούς tracking όπως τα cookies και το fingerprinting. Τα αποτελέσματα που μας παρέχει το γράφημα είναι αρκετά αποκαλυπτικά καθώς η συντριπτική πλειοψηφία των συμμετεχόντων, συγκεκριμένα το 45.6% δήλωσαν πως έχουν χαμηλό αίσθημα ελέγχου επιλέγοντας την τιμή 2 ενώ επιπλέον 30.9% δήλωσαν ακόμη χαμηλότερη αίσθηση ελέγχου στο επίπεδο 1. Αυτό σημαίνει πως τουλάχιστον 3 στους 4 χρήστες νιώθουν πως δεν έχουν επαρκή έλεγχο στα δεδομένα τους. Τα παραπάνω ευρήματα φανερώνουν ένα πολύ σημαντικό έλλειμμα στην αίσθηση διαφάνειας και της δυνατότητας παρέμβασης από την πλευρά των χρηστών. Σε συνδυασμό με προηγούμενα ευρήματα που αποδεικνύουν περιορισμένη κατανόηση του τρόπου λειτουργίας του tracking, η έλλειψη ελέγχου που δηλώνουν οι χρήστες ενισχύει την εικόνα του ξεκάθαρα παθητικού χρήστη ο οποίος βιώνει την αυτοματοποιημένη παρακολούθηση ως ένα αναπόφευκτο πλέον φαινόμενο.

Πιστεύετε πως έχετε επαρκή έλεγχο των δεδομένων που συλλέγουν μηχανισμοί όπως cookies και fingerprinting κατά την περιήγησή σας στο διαδίκτυο;

68 απαντήσεις

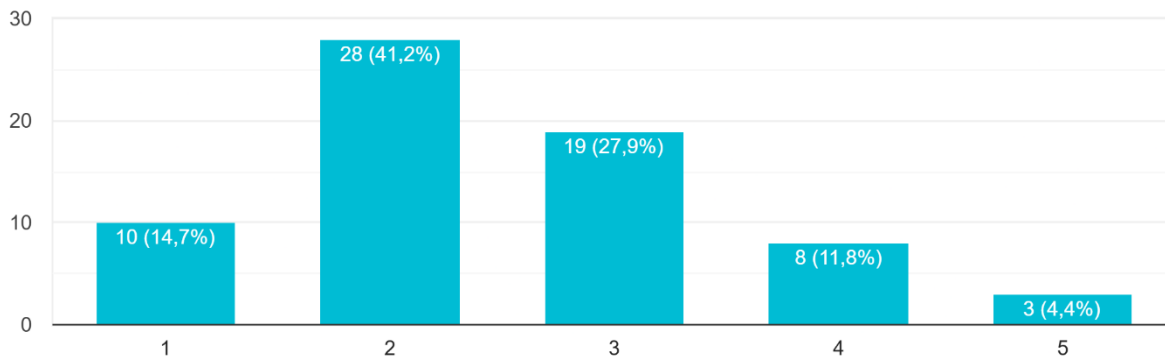


Γράφημα 14: Επίπεδο ελέγχου των δεδομένων που συλλέγονται.

Στην συνέχεια θα αναλύσουμε το επίπεδο της ενημέρωσης που θεωρούν πως έχουν οι χρήστες από παρόχους ιστοσελίδων σχετικά με τους μηχανισμούς συλλογής δεδομένων. Το παρακάτω γράφημα αποτυπώνει με ξεκάθαρο τρόπο της απόψεις των χρηστών αναφορικά με το επίπεδο το οποίο θεωρούν πως τους ενημερώνουν οι πάροχοι ιστοσελίδων σχετικά με τους μηχανισμούς συλλογής και διαμοιρασμού δεδομένων όπως τα cookies. Όπως και για τις προηγούμενες ερωτήσεις της παρούσας θεματικής ενότητας, έχουμε και για αυτή την ερώτηση κλίμακα 5 επιπέδων. Η γενικότερη κατανομή των απαντήσεων των συμμετεχόντων αποκαλύπτει δυσπιστία ως προς την πληροφόρηση των παρόχων των ιστοσελίδων με το 41.2% των συμμετεχόντων να επιλέγουν το δεύτερο επίπεδο και το 14.7% δήλωσαν πως δεν υπάρχει καμία επάρκεια στην ενημέρωση επιλέγοντας το πρώτο επίπεδο. Στην μέση της κλίμακας έχουμε 27.9% των χρηστών, να επιλέγουν το τρίτο επίπεδο. Συνολικά τα παραπάνω αποτελέσματα δείχνουν πως το 83.8% των χρηστών δεν νιώθουν καλά πληροφορημένοι. Αντιθέτως μόνο το 15.2% δηλώνουν πως θεωρούν ότι έχουν επαρκή ενημέρωση σχετικά με τους tracking μηχανισμούς από τους παρόχους ιστοσελίδων που επισκέπτονται.

Πιστεύετε πως οι ιστοσελίδες σας ενημερώνουν επαρκώς για τους μηχανισμούς συλλογής και διαμοιρασμού δεδομένων, όπως τα cookies;

68 απαντήσεις

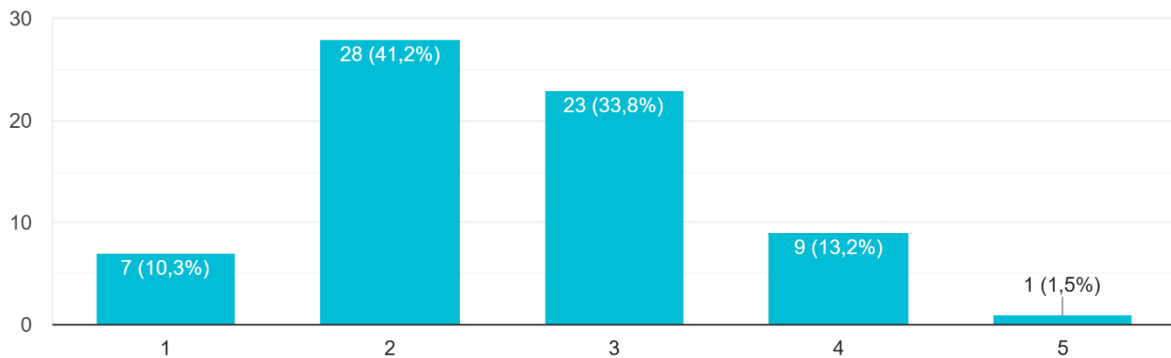


Γράφημα 15: Επίπεδο ενημέρωσης από ιστοσελίδες για τους μηχανισμούς tracking.

Στο τελευταίο μέρος της παρούσας θεματικής ενότητας θα αναλύσουμε το επίπεδο των γνώσεων που θεωρούν πως έχουν οι χρήστες σχετικά με τις γενικότερες γνώσεις τους στο θέμα της αυτοματοποιημένης παρακολούθησης στο διαδίκτυο. Στην αυτοαξιολόγηση τους οι χρήστες επέλεξαν σε πολύ μεγάλο βαθμό της επιλογές στην μέση της κλίμακας και χαμηλότερα. Πιο συγκεκριμένα το 33.8% επέλεξε το επίπεδο 3 ενώ το 42.2% το επίπεδο 2 με το 10.3% να επιλέγει το επίπεδο 1 δηλαδή το χαμηλότερο από όλα. Μόνο το 14.7% των συμμετεχόντων επέλεξε τα δύο υψηλότερα επίπεδα με το 13.2% να δηλώνουν το επίπεδο 4 και μόλις 1.5% να δηλώνει το επίπεδο 5. Τα παραπάνω αποτελέσματα φανερώνουν πως οι χρήστες κατανοούν το χαμηλό επίπεδο των γνώσεων τους για το θέμα, έχοντας μεγάλη έλλειψη επίγνωσης και κατανόησης του.

Σε κλίμακα 1-5 πως θα αξιολογούσατε τις γνώσεις σας σχετικά με την αυτοματοποιημένη παρακολούθηση στο διαδίκτυο;

68 απαντήσεις



Γράφημα 16: Αυτοαξιολόγηση των χρηστών σχετικά με τις γνώσεις τους στο θέμα της αυτοματοποιημένης παρακολούθησης στο διαδίκτυο.

4.4. Η στάση των χρηστών απέναντι στα εργαλεία και τις τεχνικές ενίσχυσης της ιδιωτικότητας

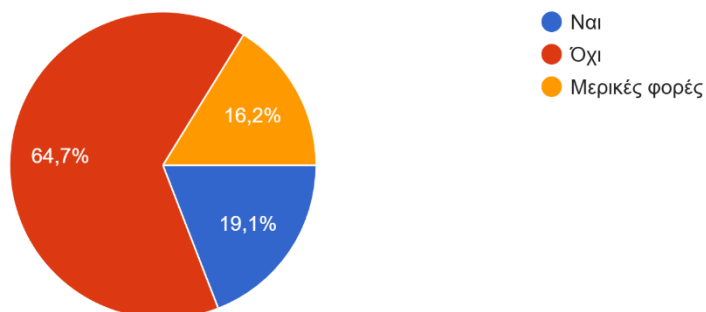
Εφόσον αναλύθηκαν λεπτομερώς στις προηγούμενες θεματικές ενότητες του ερωτηματολογίου, η επίγνωση των χρηστών σχετικά με tracking μηχανισμούς, η συμπεριφορά τους απέναντι σε αυτούς και η γενικότερη επίγνωση τους σχετικά με θέματα αυτοματοποιημένης παρακολούθησης, στην παρούσα θεματική ενότητα είναι σημαντικό να αναλύσουμε την στάση τους απέναντι σε εργαλεία και τεχνικές για την αντιμετώπιση της παρακολούθησης και κατά συνέπεια να εντοπίσουμε τα χαρακτηριστικά που διέπουν τον επαρκώς ενημερωμένο χρήστη σε συνέχεια των προηγούμενων ευρημάτων.

Αρχικά ζητήθηκε από τους συμμετέχοντες να δηλώσουν αν χρησιμοποιούν εργαλεία anti tracking ώστε να προστατευτούν από cookies ή behavioral tracking τεχνικές. Η πλειοψηφία των χρηστών δήλωσαν πως δεν το κάνουν με την επιλογή όχι να συγκεντρώνει το 64.7% και την επιλογή μερικές φορές να συγκεντρώνει το 16.2%. Μόνο το 19.1% δήλωσαν πως αξιοποιούν anti-tracking

εργαλεία για να αποφύγουν τις τεχνικές που εφαρμόζουν τα cookies και άλλοι μηχανισμοί στο διαδίκτυο.

Χρησιμοποιείτε εργαλεία anti-tracking για την προστασία από cookies ή behavioral tracking;

68 απαντήσεις

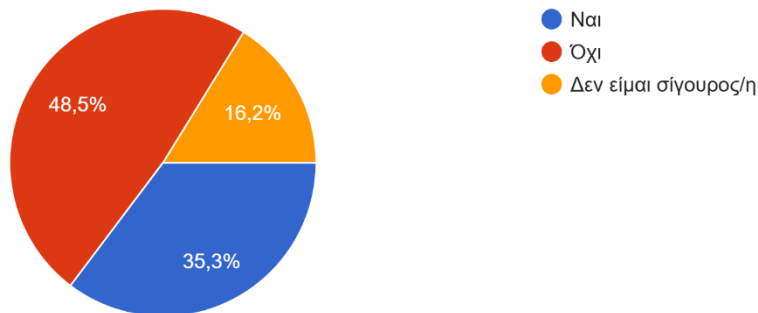


Γράφημα 17: Τα ποσοστά χρήσης εργαλείων anti-tracking από τους συμμετέχοντες.

Το παρακάτω γράφημα απεικονίζει το ποσοστά των χρηστών που έχουν προβεί σε ενέργειες διαγραφής ή αποκλεισμού των trackers μέσω του browser που χρησιμοποιούν. Από τα αποτελέσματα που φανερώνει το γράφημα κατανοούμε πως ένα αρκετά μεγάλο ποσοστό των χρηστών, πιο συγκεκριμένα το 48.5% δεν έχουν προβεί ποτέ σε κάποια ενέργεια ή προσπάθεια αποκλεισμού trackers ενώ συμπληρωματικά ένα ποσοστό 16.2% δήλωσαν αβεβαιότητα. Συνδυαστικά τα παραπάνω αποτελέσματα δείχνουν την εικόνα χρηστών που είτε έχουν άγνοια για τον τρόπο με τον οποίο μπορούν να αποκλείσουν trackers από τον browser που χρησιμοποιούν ή περιπτώσεις που ίσως προσπάθησαν αλλά δεν είναι σίγουροι για τα αποτελέσματα των ενεργειών τους. Παράλληλα όμως είναι ενθαρρυντικό πως υπάρχει ένα ποσοστό 35.3% που δήλωσαν πως διαγράφουν ή αποκλείουν trackers από τους browsers που χρησιμοποιούν, το παραπάνω ποσοστό δεν είναι επαρκές, δηλώνει όμως την πρόθεση και προσπάθεια των χρηστών να προστατεύονται.

Έχετε προσπαθήσει να διαγράψετε ή να μπλοκάρετε trackers από τον browser που χρησιμοποιείτε;

68 απαντήσεις

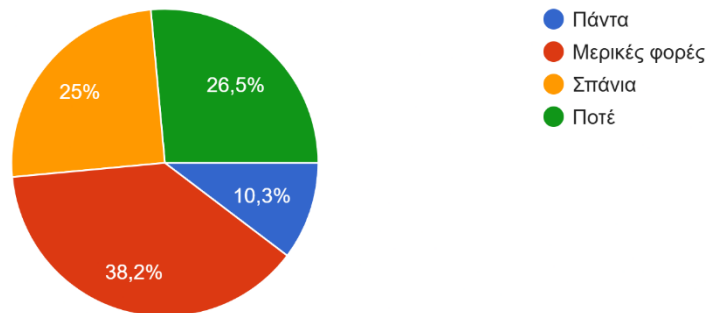


Γράφημα 18: Τα ποσοστά των χρηστών που έχουν προσπαθήσει να διαγράψουν ή να αποκλείσουν tracking μηχανισμούς από τον browser της επιλογής τους.

Στην συνέχεια ζητήθηκε από στους χρήστες να δηλώσουν την συχνότητα κατά την οποία χρησιμοποιούν ψηφιακά εργαλεία με στόχο την προστασία της ιδιωτικότητας τους στο διαδίκτυο, ενδεικτικά τα εργαλεία που αναφέρθηκαν ήταν privacy browsers και οι τεχνολογίες VPN. Από τα αποτελέσματα φαίνεται πως το μεγαλύτερο μέρος των χρηστών δεν τα αξιοποιούν ή το κάνουν μόνο μερικές φορές. Πιο συγκεκριμένα το 26.5% δήλωσαν πως δεν χρησιμοποιούν ποτέ privacy enhancing tools ενώ το 25% δήλωσαν πως τα χρησιμοποιούν σπάνια. Στην συνέχεια το 38.2% δήλωσαν πως τα χρησιμοποιούν μόνο μερικές φορές και μόνο το 10.3% επέλεξαν την επιλογή «Πάντα». Τα δεδομένα μας δείχνουν πως μόνο ένα μικρό ποσοστό του πληθυσμού έχει ενσωματώσει ενεργά πρακτικές προστασίας της ιδιωτικότητας στην καθημερινή του περιήγηση, με το μεγαλύτερο ποσοστό του πληθυσμού να απέχει πλήρως ή να χρησιμοποιεί τα εργαλεία αυτά μόνο περιστασιακά. Φαίνεται λοιπόν πως η χρήση αυτών των εργαλείων είναι περιστασιακή και δεν έχει γίνει μια σταθερή συνήθεια των χρηστών παρότι φαίνεται να γνωρίζουν πως υπάρχουν κίνδυνοι που αφορούν στην ιδιωτικότητα τους κατά την πλοήγηση τους στο διαδίκτυο.

Χρησιμοποιείτε συχνά εργαλεία όπως privacy browsers και VPN για την προστασία της ιδιωτικότητάς σας;

68 απαντήσεις

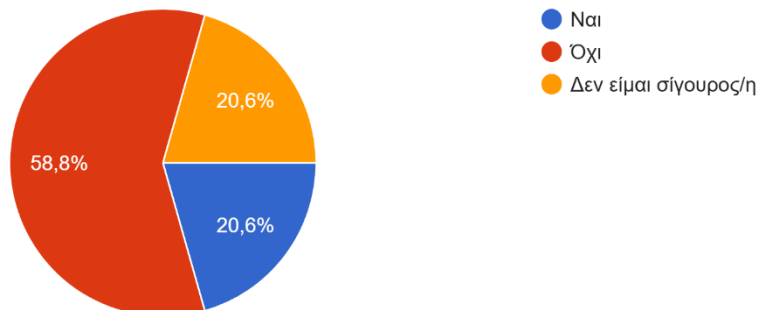


Γράφημα 19: Η συχνότητα κατά την οποία οι χρήστες αξιοποιούν εργαλεία ενίσχυσης της ιδιωτικότητας.

Σε συνέχεια της προηγούμενης ερώτησης οι οποία αφορούσε την χρήση εργαλείων ενίσχυσης της ιδιωτικότητας, ακολουθεί μια ερώτηση πιο απλή, που απαιτεί την ευαισθητοποίηση του χρήστη αλλά όχι την δυνατότητα του να χειριστεί κάποιο πρόσθετο εργαλείο. Όλοι οι χρήστες του διαδικτύου χρησιμοποιούν browsers για την πρόσβαση τους σε ιστοσελίδες και κάποιοι browsers έχουν περισσότερες επιλογές σχετικά με την ιδιωτικότητα του χρήστη από άλλους, όλοι όμως έχουν ρυθμίσεις με τις οποίες ο χρήστης μπορεί να πειραματιστεί για να μειώσει το αποτύπωμα του. Στην ερώτηση λοιπόν για το αν οι χρήστες γνώριζαν τον τρόπο με τον οποίο μπορούν να αλλάξουν ρυθμίσεις στον browser της επιλογής τους με στόχο να μειώσουν το αποτύπωμα τους, λάβαμε τις εξής απαντήσεις. Το 58.5% δήλωσαν πως δεν γνωρίζουν το τρόπο με τον οποίο μπορούν να αλλάξουν ρυθμίσεις στον browser τους με στόχο την ενίσχυση της ιδιωτικότητας τους. Το 20.6% επέλεξαν «Δεν είμαι σίγουρος» και τέλος το υπόλοιπο 30.6% δήλωσαν πως γνωρίζουν. Από τα δεδομένα κατανοούμε πως οι χρήστες έχουν μια εικόνα σχετικά με την παρακολούθηση της οποία υπόκεινται αλλά δεν γνωρίζουν το πως μπορούν να την περιορίσουν, γεγονός που αποδεικνύει πως οι γνώσεις των χρηστών, άσχετα με το επίπεδο τους, είναι ξεκάθαρα θεωρητικές και δεν έχουν την δυνατότητα να τις εφαρμόσουν στην πράξη.

Γνωρίζετε τον τρόπο με τον οποίο μπορείτε να αλλάξετε τις ρυθμίσεις του browser σας ώστε να μειώσετε το αποτύπωμά σας;

68 απαντήσεις

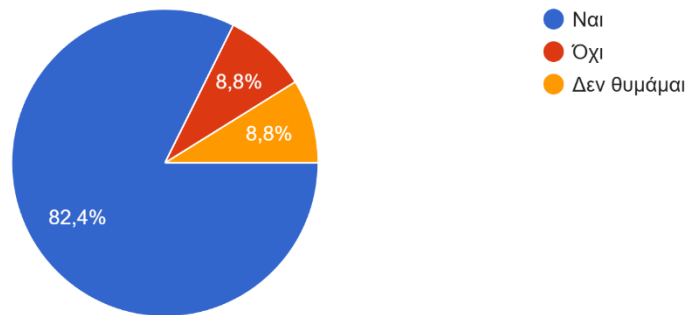


Γράφημα 20: Επίγνωση των χρηστών σχετικά με τις ρυθμίσεις ιδιωτικότητας των browser που χρησιμοποιούν.

Στο τελευταίο μέρος της τελευταίας θεματικής ενότητας του ερωτηματολογίου, ζητήθηκε από τους χρήστες να δηλώσουν εάν έχουν ποτέ αποχωρήσει από κάποια ιστοσελίδα επειδή ανησύχησαν για την ιδιωτικότητα τους. Η συγκεκριμένη ερώτηση εξετάζει μια ενέργεια των χρηστών η οποία δεν απαιτεί κάποια τεχνική γνώση ή κατάρτιση όπως την χρήση εργαλείων ή την παραμετροποίηση σύνθετων ρυθμίσεων, πάρα μόνο την αποφυγή της χρήσης της ιστοσελίδας από τον χρήστη. Τα αποτελέσματα ήταν αρκετά ενθαρρυντικά στην συγκεκριμένη ερώτηση. Το 82.4% δήλωσαν πως έχουν αποχωρήσει στο παρελθόν από κάποιον ιστότοπο έχοντας ανησυχία για την ιδιωτικότητα τους, ενώ οι άλλες δυο επιλογές ήταν «Ναι» και «Όχι» όπου και οι δύο συγκέντρωσαν 8.8% αντίστοιχα. Η ολοκληρωτική αποφυγή ενός ιστότοπου από τους χρήστες δείχνει πως κατανοούν τα σημάδια μια δόλιας ιστοσελίδας, ή κάποιας που ήταν παρεμβατική για παράδειγμα, αλλά και την έλλειψη της δυνατότητας να προστατευτούν με τεχνικά μέσα. Αντιθέτως η ενστικτώδης αντίδραση των χρηστών είναι η αποφυγή ολόκληρης της ιστοσελίδας.

Έχετε αποφύγει τη χρήση κάποιας ιστοσελίδας στο παρελθόν επειδή ανησυχήσατε για την ιδιωτικότητά σας;

68 απαντήσεις



Γράφημα 21: Το ποσοστό των χρηστών που έχουν αποχωρήσει από κάποιον ιστότοπο επειδή ανησύχησαν για την ιδιωτικότητα τους.

5. Συζήτηση και Συμπεράσματα

Στο παρόν κεφάλαιο της εργασίας, στόχος είναι να εκτελεστεί η συνολική ανάλυση των αποτελεσμάτων σε σχέση με την προ υπάρχουσα βιβλιογραφία καθώς και η εξαγωγή συμπερασμάτων σχετικά με τα ερευνητικά ερωτήματα της εργασίας.

Η προ υπάρχουσα βιβλιογραφία περιγράφει τα cookies που χρησιμοποιούν οι διάφορες ιστοσελίδες ως έναν βασικό μηχανισμό ταυτοποίησης και συλλογής δεδομένων του χρήστη τα οποία θέτουν τα θεμέλια για την εκτέλεση του third-party tracking από τους παρόχους των ιστοσελίδων καθώς και την εμπορευματοποίηση των δεδομένων από διαφημιστικά δίκτυα. Το πείραμα της εργασίας, μας φανερώνει πως ένα μεγάλο τμήμα των χρηστών αποδέχονται τους όρους των πολιτικών cookies χωρίς να τις διαβάζουν στην πράξη (Γράφημα 3) μόνο για να έχουν ευκολότερη και πιο άμεση πρόσβαση στο περιεχόμενο των ιστοσελίδων, γεγονός που επιβεβαιώνει πως η επίγνωση του όρου δεν μεταφράζεται απαραίτητα σε συστηματική και ενημερωμένη επιλογή του χρήστη στην πράξη. Παράλληλα φαίνεται πως οι χρήστες δεν είναι σε θέση να διαχωρίσουν τους όρους first / third party cookies, η ασυνεπής διάκριση των όρων αποτελεί κρίσιμο στοιχείο καθώς η κατανόηση της διάκρισης αποτελεί προϋπόθεση για την συνειδητή διαχείριση της παρακολούθησης (Γράφημα 4). Ταυτόχρονα οι χρήστες δείχνουν μέτριο προς υψηλό βαθμό ανησυχίας για την τεχνολογία των cookies (Γράφημα 6) με την πλειοψηφία των χρηστών να έχουν αποφύγει ολοκληρωτικά την χρήση κάποιας ιστοσελίδας λόγω των παρεμβατικών τεχνικών με τις οποίες παρουσιάζονται πολιτικές cookies. Τα παραπάνω μοτίβα που μας δείχνουν την αποδοχή όρων cookies χωρίς την ανάγνωση των πολιτικών, αλλά παράλληλα την γενικότερη ανησυχία απέναντι στους μηχανισμούς και αποφυγή αυτών. Γεγονός που επιβεβαιώνει σε μεγάλο βαθμό το φαινόμενο του privacy paradox (Norberg et al., 2007) κατά το οποίο οι χρήστες γνωρίζουν ή αντιλαμβάνονται τους κινδύνους αλλά τους αποδέχονται για την ευκολότερη ή αμεσότερη πλοήγησή τους. Τα παραπάνω ευρήματα υπογραμμίζουν την ανάγκη για απλούστερες και λιγότερο τεχνικά περίπλοκες πολιτικές απορρήτου καθώς και ενημερωτικές πρωτοβουλίες για την ενημέρωση των χρηστών σχετικά με τους μη ορατούς μηχανισμούς παρακολούθησης ώστε εκείνοι να μπορούν να λάβουν πιο εμπεριστατωμένες επιλογές που θα αφορούν στην ιδιωτικότητα τους.

Όπως προ αναφέρθηκε ένας από τους κυριότερους λόγους για τους οποίους έχουμε την αυτοματοποιημένη συλλογή δεδομένων των χρηστών είναι η στοχευμένη διαφήμιση, προς τα ενδιαφέροντα του εκάστοτε χρήστη. Στην βιβλιογραφία αναφέρεται πως όταν οι χρήστες γνωρίζουν τους

μηχανισμούς με τους οποίους λειτουργεί η στοχευμένη διαφήμιση και πως μέρος των δεδομένων τους συλλέγεται για αυτούς τους σκοπούς τότε είναι περισσότερο πρόθυμοι να δώσουν στοιχεία τους και να αλληλοεπιδράσουν με τέτοιου τύπου διαφημίσεις ενώ αντίθετα, όταν υπάρχει άγνοια από τους χρήστες εκείνοι αποφεύγουν να αλληλοεπιδρούν με αυτούς τους μηχανισμούς (Aguirre et al., 2015; Boerman et al., 2017).

Στο δείγμα της εργασίας, τα παραπάνω επιβεβαιώνονται, πιο συγκεκριμένα οι χρήστες έδειξαν μέτρια προς χαμηλή κατανόηση σχετικά με τους μηχανισμούς λειτουργίας της στοχευμένης διαφήμισης (Γράφημα 7) και ταυτόχρονα ενοχλούνται από αυτές σε πολύ μεγάλο βαθμό (Γράφημα 8). Παράλληλα φαίνεται πως η συντριπτική πλειοψηφία των χρηστών αποφεύγουν να αλληλοεπιδρούν με αυτού του τύπου διαφημίσεις όπως pop-ups (Γράφημα 11) ενώ συγχρόνως γίνεται και αποφυγή χρήσης πιστωτικών καρτών από τους χρήστες για ψηφιακές αγορές (Γράφημα 10) λόγω των trackers. Εξάγουμε λοιπόν το συμπέρασμα πως οι χρήστες απορρίπτουν τα «φαινόμενα» που είναι η παρεμβατικότητα των στοχευμένων διαφημίσεων χωρίς να γνωρίζουν πλήρως τα αίτια πίσω από αυτά, που είναι το behavioral tracking, επιβεβαιώνοντας την θέση που υποστηρίζει ότι η έλλειψη διαφάνειας υπονομεύει την αποδοχή από τους χρήστες.

Στην συνέχεια όσων αφορά στα αντίμετρα τα οποία μπορούν οι χρήστες να χρησιμοποιήσουν, τα οποία είναι πολυάριθμα και έχουν διαφορετικά επίπεδα πολυπλοκότητας στην χρήση τους, οι χρήστες φαίνεται πως δεν τα αξιοποιούν στην πραγματικότητα. Μια συμπεριφορά ξεκάθαρα αντιφατική καθώς φαίνεται πως κατανοούν την παρακολούθηση στην οποία υπόκεινται και νιώθουν παράλληλα πως έχουν χαμηλό επίπεδο ελέγχου επι των δεδομένων τους τα οποία συλλέγονται (Γράφημα 14). Τα αποτελέσματα της έρευνας μας δείχνουν πολύ χαμηλά ποσοστά συστηματικής χρήσης anti-tracking εργαλείων (Γράφημα 17) ενώ ταυτόχρονα σχεδόν οι μισοί χρήστες δεν έχουν προσπαθήσει ποτέ να παραμετροποιήσουν ρυθμίσεις του browser που χρησιμοποιούν με στόχο την μείωση των tracking μηχανισμός ή την διαγραφή τους (Γράφημα 18). Είναι επίσης σημαντικό να σημειωθεί πως οι χρήστες σε μεγάλο ποσοστό εγκαταλείπουν ολοκληρωτικά κάποια ιστοσελίδα όταν ανησυχούν για την ιδιωτικότητα τους, δρουν δηλαδή εκ των υστέρων και όχι προληπτικά όταν νιώθουν πως απειλούνται (Γράφημα 21).

Τα παραπάνω δεδομένα μας παρέχουν μια αρκετά ξεκάθαρη εικόνα της κατάστασης, και μας βοηθούν να προσδιορίσουμε με ακρίβεια πως διαφέρει ή συγκλίνει η συμπεριφορά της πλειοψηφίας των χρηστών σε σχέση με το προφίλ ενός ενήμερου χρήστη, για θέματα ιδιωτικότητας. Όπως

προκύπτει από την βιβλιογραφία ο ενήμερος χρήστης χαρακτηρίζεται από την επίγνωση των απειλών και των συνεπειών που συνεπάγεται η αποκάλυψη προσωπικών δεδομένων, η κριτική στάση απέναντι σε πολιτικές απορρήτου καθώς και η ενεργή χρήση αντιμέτρων (Tsohou & Soumelidou, 2021). Τα αποτελέσματα της παρούσας έρευνας δυστυχώς αποκλίνουν από το συγκεκριμένο προφίλ, μας δείχνουν χαμηλό επίπεδο επίγνωσης, αλλά και όταν αυτή υπάρχει, οι χρήστες τείνουν να παραμένουν παθητικοί δέκτες της αυτόματης παρακολούθησης στο διαδίκτυο. Κύριοι παράγοντες που συμβάλουν στην παθητική στάση των χρηστών, από τα αποτελέσματα της έρευνας φαίνεται να είναι η έλλειψη ψηφιακής κατάρτισης, την αδυναμία κατανόησης των πολιτικών αλλά και η απάθεια απέναντι σε αυτές και σαφώς η απουσία σταθερών συνηθειών εφαρμογής αντιμέτρων.

5.1. Περιορισμοί της έρευνας

Κατά την εκτέλεση της παρούσας έρευνας αξιοποιήθηκε δείγμα 68 ατόμων, το οποίο παρέχει μια εικόνα για τις τάσεις που επικρατούν ανάμεσα στους χρήστες σχετικά με την επίγνωση τους απέναντι στην αυτόματη παρακολούθηση, δεν θα μπορούσε όμως να θεωρηθεί αντιπροσωπευτικό ολόκληρου του πληθυσμού. Παράλληλα η διανομή του ερωτηματολογίου έγινε σε μεγάλο βαθμό μέσω κοινωνικών δικτύων γεγονός που ενδέχεται να οδηγήσει σε ελαφρώς μεγαλύτερη συμμετοχή ατόμων με υψηλότερο επίπεδο εξοικείωσης με την τεχνολογία και τις τεχνικές παρακολούθησης γενικότερα.

5.2. Ιδέες για Περαιτέρω Έρευνα

Μελλοντικές έρευνες σχετικές με το θέμα τις αυτοματοποιημένης παρακολούθησης στο διαδίκτυο θα μπορούσαν να αξιοποιήσουν μεγαλύτερο δείγμα χρηστών που θα παρείχε μεγαλύτερη ποικιλία σε διαφορετικές ηλικιακές, επαγγελματικές και κοινωνικές ομάδες. Ενώ ταυτόχρονα θα ήταν χρήσιμη η διενέργεια συγκριτικών μελετών ανάμεσα σε διαφορετικές χώρες ώστε να εντοπιστεί το πιθανώς διαφορετικό επίπεδο της επίγνωσης ανάμεσα σε κάτοικους χωρών με διαφοροποιήσεις σε πολιτισμικό επίπεδο και νομοθετικό πλαίσιο.

5.3. Ιδέες για την Αξιοποίηση των Αποτελεσμάτων

Τα αποτελέσματα τις παρούσας έρευνας θα μπορούσαν να αξιοποιηθούν σε πολλαπλά επίπεδα. Αρχικά θα μπορούσαν να αποτελέσουν οδηγό για την δημιουργία εκπαιδευτικών προγραμμάτων και εκστρατειών ενημέρωσης τα οποία θα ενημερώνουν τους χρήστες και θα ενισχύουν την επίγνωση τους σχετικά με τα ζητήματα ιδιωτικότητας. Ενώ τέλος, φορείς χάραξης πολιτικών καθώς και πάροχοι ψηφιακών υπηρεσιών θα μπορούσαν να αξιοποιήσουν τα συμπεράσματα της έρευνας στην προσπάθεια τους να δημιουργήσουν πιο διαφανείς και κατανοητές πολιτικές cookies και χρήσης των ιστοσελίδων.

Βιβλιογραφία

- [1] Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014, November). The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security* (pp. 674-689).
- [2] Aiolfi, S., Bellini, S., & Pellegrini, D. (2021). Data-driven digital advertising: benefits and risks of online behavioral advertising. *International Journal of Retail & Distribution Management*, 49(7), 1089-1110.
- [3] Bai, W., Pearson, M., Kelley, P. G., & Mazurek, M. L. (2020, September). Improving non-experts' understanding of end-to-end encryption: An exploratory study. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 210-219). IEEE.
- [4] Bibi, A., Hussain, Z., Khan, F., & Maqsood, A. (2017, January). Quantitative evaluation of security and privacy perceptions in online social networks: a case study. In *2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST)* (pp. 425-433). IEEE.
- [5] Bielova, N. (2017, October). Web tracking technologies and protection mechanisms. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2607-2609).
- [6] Binns, R., & Bietti, E. (2020). Dissolving privacy, one merger at a time: Competition, data and third party tracking. *Computer Law & Security Review*, 36, 105369.
- [7] Bleier, A. (2021). On the viability of contextual advertising as a privacy-preserving alternative to behavioral advertising on the web. *Available at SSRN 3980001*.
- [8] Bujlow, T., Carela-Español, V., Sole-Pareta, J., & Barlet-Ros, P. (2017). A survey on web tracking: Mechanisms, implications, and defenses. *Proceedings of the IEEE*, 105(8), 1476-1510.
- [9] Chen, Q., Ilia, P., Polychronakis, M., & Kapravelos, A. (2021, April). Cookie swap party: Abusing first-party cookies for web tracking. In *Proceedings of the Web Conference 2021* (pp. 2117-2129).

- [10] Chignell, M. H., Quan-Haase, A., & Gwizdka, J. (2003, October). The privacy attitudes questionnaire (paq): initial development and validation. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 47, No. 11, pp. 1326-1330). Sage CA: Los Angeles, CA: SAGE Publications.
- [11] Correia, P. F. L. (2024). Web browser fingerprinting and client defense techniques via web browser plugin (Master's thesis, Universidade do Porto (Portugal)).
- [12] Hale, B., & Komlo, C. (2022). On end-to-end encryption. *Cryptology ePrint Archive*.
- [13] Jamieson, S. (2004). Likert scales: How to (ab) use them?. *Medical Education*, 38(12), 1217-1218.
- [14] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122-134.
- [15] Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R., & Krishnamurthy, B. (2013, November). Privacy awareness about information leakage: Who knows what about me?. In *Proceedings of the 12th ACM workshop on privacy in the electronic society* (pp. 279-284).
- [16] Mitchell, I. D. (2012). Third-party tracking cookies and data privacy.
- [17] Pilton, C., Faily, S., & Henriksen-Bulmer, J. (2021). Evaluating privacy-determining user privacy expectations on the web. *Computers & Security*, 105, 102241.
- [18] Roesner, F., Kohno, T., & Wetherall, D. (2012). Detecting and defending against {Third-Party} tracking on the web. In *9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12)* (pp. 155-168).
- [19] Ruhwanya, Z. S. (2015). Attitudes toward, and awareness of, online privacy and security: a quantitative comparison of East Africa and US internet users (Doctoral dissertation, Kansas State University).
- [20] Schmucker, N. (2011). Web tracking. In *SNET2 Seminar Paper-Summer Term* (Vol. 2011). Princeton, NJ, USA: Citeseer.
- [21] Sim, K., Heo, H., & Cho, H. (2024). Combating web tracking: analyzing web tracking technologies for user privacy. *Future Internet*, 16(10), 363.

[22] Soumelidou, A., & Tsohou, A. (2021). Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness. *Telematics and Informatics*, 61, 101592.

[23] Soumelidou, A., & Tsohou, A. (2023). Development and Validation of Two Domain-Specific Information Privacy Competency Models.