ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΠΟΛΙΤΙΣΜΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Δεσποτίδη Χαρίκλεια

Α.Μ 1312015027

Παράγοντες αποδοχής, υιοθέτησης και χρήσης των Βιομετρικών Συστημάτων: Η περίπτωση των φοιτητών-τριών του Πανεπιστημίου Αιγαίου

Acceptance, adoption and use of Biometric Systems: The case of the University of the Aegean students

Συμβουλευτική Επιτροπή:

Επιβλέπων:

Χρήστος Καλλονιάτης
Αναπληρωτής Καθηγητής
Πανεπιστημίου Αιγαίου

Εξεταστική Επιτροπή:

Καβακλή Ευαγγελία
Αναπληρώτρια Καθηγήτρια
Πανεπιστημίου Αιγαίου

Σίμου Σταύρος
Εργαστηριακό Διδακτικό
Προσωπικό(Ε.ΔΙ.Π.) Πανεπιστημίου
Αιγαίου

Πίνακας περιεχομένων

1.Εισαγωγή

Η παρατηρούμενη τάση στην αγορά τα τελευταία χρόνια για παροχή εξατομικευμένων υπηρεσιών αλλά και η διαρκώς αυξανόμενη απαίτηση για την ενίσχυση της ασφάλειας σε διάφορους τομείς της ζωής των ανθρώπων, δημιουργούν την ανάγκη για αναζήτηση νέων μηχανισμών, μεθόδων και συστημάτων ταυτοποίησης. Συγκεκριμένα, οι βιομετρικές τεχνολογίες βασιζόμενες σε ανθρώπινα χαρακτηριστικά με ιδιαίτερες εγγενείς ιδιότητες, όπως η μοναδικότητα, η συλλεξιμότητα και η παγκοσμιότητα, οι οποίες συγκροτούν βασικές προϋποθέσεις για την ταυτοποίηση των ανθρώπων, συνιστούν μια συντονισμένη ερευνητική προσπάθεια κάλυψης αυτών των υψηλών αναγκών (Ανδρόνικου, 2009) . Σήμερα, ο όρος βιομετρικά συστήματα αναφέρεται στις τεχνικές εκείνες που αναλύουν τα ανθρώπινα χαρακτηριστικά για λόγους ασφαλείας. Η εφαρμογή συστημάτων βιομετρικής τεχνολογίας, αποτελεί μια ασφαλή μέθοδο ταυτοποίησης που βασίζεται σε μονοσήμαντα στοιχεία του ανθρώπου για την αναγνωσιμότητα του λογικού υποκειμένου από ένα Πληροφοριακό Σύστημα (Van der Ploeg,1999). Στη βιομηχανία των συστημάτων ασφάλειας, τα βιομετρικά συστήματα θεωρείται ότι παρέχουν το υψηλότερο επίπεδο ασφάλειας. Ένα πληροφοριακό σύστημα, χρησιμοποιεί πολλές τεχνικές αυθεντικοποίησης και ταυτοποίησης, οι οποίες αποτελούν βασικό στοιχείο της ασφάλειας των υπολογιστικών συστημάτων (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης, 2004). Οι εφαρμογές της ταυτοποίησης και της αυθεντικοποίησης συνδράμουν στον έλεγχο της πρόσβασης των εξουσιοδοτημένων χρηστών, ώστε τα δεδομένα των χρηστών να βρίσκονται σε έμπιστα περιβάλλοντα ασφαλείας. Τα βιομετρικά συστήματα, αποτελούν κατηγορία της διαδικασίας της αυθεντικοποίησης, αλλά παρουσιάζονται και τα υπόλοιπα συστήματα αυθεντικοποίησης.

Οι τεχνολογίες αυτές και οι δυνατότητες τους, δημιουργούν έντονους προβληματισμούς όσον αφορά το επίπεδο της ακρίβειας και της ασφάλειας που «υπόσχονται», καθώς όπως αναφέρθηκε και προηγουμένως, οι διαρκώς εντεινόμενες απαιτήσεις για την ασφαλέστερη και αποτελεσματικότερη

διαχείριση της ταυτότητας, γίνεται η αφορμή των ερευνών σε παγκόσμιο επίπεδο. Παρόλα αυτά, τα υπάρχοντα βιομετρικά συστήματα(Ανδρόνικου,2009), περιλαμβάνουν πιθανούς κινδύνους για την ιδιωτικότητα. Αυτές οι απειλές προς την ιδιωτικότητα εντείνονται από τις τεχνολογικές αδυναμίες των βιομετρικών συστημάτων, καθώς κανένα βιομετρικό σύστημα δεν μπορεί να προσφέρει 100% επιτυχία στη σωστή ταυτοποίηση ή επιβεβαίωση της ταυτότητας των ατόμων(Ανδρόνικου, 2009).

2. Συστήματα, Πληροφοριακά Συστήματα, Ασφάλεια Πληροφοριακών Συστημάτων

Η Ασφάλεια των Πληροφοριακών Συστημάτων αποτελεί από τις βασικότερες προτεραιότητες στον χώρο της Πληροφορικής και ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους. Ένα μέρος αυτών των συστημάτων έχουν αποθηκευμένα προσωπικά δεδομένα, τα οποία είναι σημαντικά για τους ιδιοκτήτες αυτών των συστημάτων (Καρύδα, π.χ.). Επομένως, η προστασία των προσωπικών δεδομένων χρήζει ιδιαίτερης σημασίας, καθώς επίσης και η διατήρηση ελέγχου σε χώρους περιορισμένης πρόσβασης. Ένα απλός παραλληλισμός της καθημερινής ζωής με αυτό που μπορεί να προκληθεί από τους υπολογιστές είναι η πλαστογραφία των προσωπικών δεδομένων ενός ατόμου είτε πρόκειται για κωδικό πρόσβασης είτε για αστυνομική ταυτότητα. Η αποφυγή ή η πρόληψη τέτοιων περιπτώσεων οδήγησε στη δημιουργία συστημάτων, τα οποία ονομάζονται βιομετρικά(Τζίτζικας, 2010) και θεωρούνται από πολλούς ασφαλέστερα από τα ήδη υπάρχοντα. Τα βιομετρικά συστήματα αναφέρονται σε φυσιολογικά χαρακτηριστικά του ατόμου, αλλά και σε χαρακτηριστικά συμπεριφοράς προκειμένου να γίνει η ταυτοποίηση του (Τζίτζικας, 2010). Πριν γίνει εκτενής αναφορά στον όρο της βιομετρίας και των βιομετρικών χαρακτηριστικών, η προσοχή θα εστιαστεί στην ασφάλεια των πληροφοριακών συστημάτων και τη σημασία της.

2.1 Πληροφοριακά Συστήματα & Ασφάλεια

Το παρόν κεφάλαιο αναφέρεται στις έννοιες του Συστήματος, του Πληροφοριακού Συστήματος, οι οποίες θα αναλυθούν εκτενέστερα στη συνέχεια του κεφαλαίου, καθώς και στο γενικότερο όρο της Ασφάλειας Πληροφοριακών Συστημάτων και Υποδομών. Σε ένα ευρύτερο πλαίσιο, η Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών αφορά σε οντότητες και αντικείμενα, τα οποία χρήζουν προστασίας. Καθετί που αξίζει να προστατευθεί ονομάζεται Αγαθό (Asset). Τα Αγαθά αξίζει να προστατευθούν επειδή έχουν Αξία (Value). Η Αξία τους μπορεί να μειωθεί αν υποστούν Ζημιά. Τα Αγαθά χρειάζονται προστασία μόνον αν υπάρχουν Κίνδυνοι (Dangers) που μπορούν να τους προκαλέσουν Ζημιά. Ο Ιδιοκτήτης (Owner) ενός προστατευόμενου Αγαθού χρησιμοποιεί Μέσα Προστασίας (Safeguards) είτε για να μειώσει τον Κίνδυνο να προξενήσει Ζημιά στο Αγαθό είτε για να μειώσει τις συνέπειες της (Κάτσικας , Γκρίτζαλης & Γκρίτζαλης, 2004). Η χρήση των Μέσων Προστασίας επιφέρει Κόστος. Δεδομένου ότι τα Μέσα Προστασίας δεν μπορούν να εγγυηθούν πλήρη ασφάλεια, το Κόστος τους πρέπει να αναλογεί στην Επισφάλεια (Hazard) του Αγαθού αυτού, καθώς και στις συνέπειες που θα έχει μια Ζημιά στον Ιδιοκτήτη του. Ο ιδιοκτήτης είναι εκείνος που θα κρίνει , όταν θέτει το Στόχο Ασφάλειας (InfoSec Goal), ποια είναι η πιο επωφελής ισορροπία ανάμεσα στο Κόστος, την Επισφάλεια και τις Συνέπειες. Ο Ιδιοκτήτης έχει τη δυνατότητα επιπλέον, να αναζητήσει Εξασφάλιση (Assurance) ότι ο Στόχος του θα επιτευχθεί με τα Μέσα Προστασίας που θα χρησιμοποιήσει (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης, 2004).

Βασισμένοι στο γεγονός ότι τα Αγαθά υπάρχουν για να αξιοποιούνται, ιδιαίτερη σημασία χρήζουν οι έννοιες του Χρήστη και του Ιδιοκτήτη τους. Τα Αγαθά έχουν Ιδιότητες, οι οποίες πρέπει να προστατευθούν. Οι Ζημιές που μπορεί να προκληθούν από Κινδύνους και αφορούν Ζημιές και όχι στα Αγαθά αλλά και στις Ιδιότητές τους. Αξίζει να σημειωθεί ότι οι Ζημιές εκτιμώνται από τον Χρήστη ή Ιδιοκτήτη. Κατά κύριο λόγο ο Ιδιοκτήτης είναι αυτός που θα καθορίσει τους Στόχους, οι οποίοι προσδιορίζουν τη μέγιστη ανεκτή Ζημιά που οι Ιδιοκτήτες

μπορούν να υποστούν. Ο ρόλος των Μέσων Προστασίας έγκειται στο να αντιμετωπίζουν τους Κινδύνους αποτρέποντας τις Ζημιές και προστατεύοντας τα Αγαθά και τις Ιδιότητες.

2.2 Ορισμοί

Οι παρακάτω βασικές έννοιες Σύστημα και Πληροφοριακό Σύστημα θα αναλυθούν συνοπτικά και στη συνέχεια θα επικεντρωθούμε στην Ασφάλεια Πληροφοριακών Συστημάτων.

Με βάση τη γενική θεωρία συστημάτων, ως σύστημα ορίζεται ένας αριθμός αλληλοεπιδρώντων στοιχείων, που οργανικά συναρμολογημένα σε μια ολότητα μπορούν να εκτελούν μια ορισμένη λειτουργία (Μπόζιος, 2004). Τα στοιχεία αυτά αλληλεπιδρούν όχι μόνο μεταξύ τους, αλλά και με το περιβάλλον του συστήματος, δηλαδή με κάθε οντότητα που βρίσκεται έξω από αυτό (Ψάνη & Καμπούρης, 2016).΄Έτσι, ο άνθρωπος μπορεί να κατασκευάσει συστήματα για έναν συγκεκριμένο σκοπό.

Ένα Πληροφοριακό Σύστημα ορίζεται μέσω του Υπολογιστικού Συστήματος και γι' αυτό περιλαμβάνει όλα τα τεχνικά συστατικά του Υπολογιστικού Συστήματος, το περιβάλλον στο οποίο λειτουργεί το σύστημα, το σκοπό αλλά και τις Πληροφορίες. Ουσιαστικά, το Υπολογιστικό Σύστημα είναι εγκατεστημένο σε συγκεκριμένη τοποθεσία, με καθορισμένο λειτουργικό περιβάλλον και ανταποκρίνεται σε συγκεκριμένο σκοπό. Σε κάθε Πληροφοριακό Σύστημα εντοπίζονται πέντε αλληλοεπιδρώντες συνιστώσες με απώτερο σκοπό τη βελτίωση της αποδοτικότητας, της ανταγωνιστικότητας και της επιβίωσης (Ψάνη & Καμπούρης, 2016).

- Υλικό (εξοπλισμός, δίκτυα, μηχανές)
- Λογισμικό (εντολές, προγράμματα)
- Διαδικασίες (κανόνες)
- Δεδομένα
- Άνθρωποι (προγραμματιστές, διευθυντές, χρήστες κ.α.)

Στη διεθνή βιβλιογραφία δεν υπάρχει ένας ορισμός κοινά αποδεκτός για τον ορισμό της Ασφάλειας Πληροφοριακών Συστημάτων. Παρόλα αυτά, αυτός που παρατίθεται περιγράφει όσο πιστότερα γίνεται τον όρο, διότι αποτρέπει την πιθανή σύγκριση ή ταύτιση με τις έννοιες «Ασφάλεια Τεχνολογίας Πληροφορικής» και «Ασφάλεια Πληροφοριών», οι οποίες αναφέρονται στην Ασφάλεια της Τεχνολογικής Υποδομής του Πληροφοριακού Συστήματος και στην Ασφάλεια Δεδομένων αντίστοιχα. Ο ορισμός αυτός συγχρόνως διατυπώνει με σαφήνεια ότι στην Ασφάλεια Πληροφοριακών Συστημάτων, η οπτική του παρατηρητή είναι συστημική. Επομένως, η Ασφάλεια Πληροφοριακών Συστημάτων είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος αλλά και το Σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης , 2004).
Ο παραπάνω ορισμός συγκεντρώνει πέντε βασικά στοιχεία :

- Δίνεται έμφαση όχι μόνο στην έννοια του Πληροφοριακού Συστήματος ως ολότητα αλλά και στα επιμέρους στοιχεία του.
- Η προστασία αφορά κάθε είδους απειλή είτε πρόκειται για τυχαία είτε για σκόπιμη.
- Η Ασφάλεια Πληροφοριακών Συστημάτων δεν αναφέρεται μόνο σε διοικητικά και τεχνικά θέματα αλλά και σε παραδοχές, αρχές και αντιλήψεις.
- Το πλαίσιο αυτό χαρακτηρίζεται από οργάνωση.
- Η οπτική του παρατηρητή είναι συστημική.

2.3 Χαρακτηριστικά Ασφάλειας Πληροφοριακών Συστημάτων

Όπως έχει ήδη αναφερθεί, η Ασφάλεια αφορά στην προστασία της πληροφορίας και των πληροφοριακών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, χρήση, τροποποίηση με στόχο την (Λέκκα, 2002):

- Εμπιστευτικότητα (**C**onfidentiality), η οποία αφορά στη διαφύλαξη της πληροφορίας που είναι αποθηκευμένη σε ένα σύστημα και φανερώνεται

μόνο στους χρήστες που είναι εξουσιοδοτημένοι και έχουν πρόσβαση σε αυτήν, προστατεύοντας έτσι την ιδιωτικότητα.

- Ακεραιότητα (**I**ntegrity), όπου αφορά στην προστασία και διασφάλιση της αυθεντικότητας της πληροφορίας, άρα η πληροφορία μπορεί να μεταβληθεί μόνο από τους χρήστες που διαθέτουν το δικαίωμα να το κάνουν.
- Διαθεσιμότητα (**A**vailability), όπου η διασφάλιση της προσπέλασης της πληροφορίας, από εξουσιοδοτημένους χρήστες πραγματοποιείται στον εύλογα προσδοκώμενο χρόνο.

3. Ταυτοποίηση και Αυθεντικοποίηση

Ένα πληροφοριακό σύστημα χρησιμοποιεί πολλές τεχνικές αυθεντικοποίησης και ταυτοποίησης των χρηστών του. Βασικό στοιχείο της ασφάλειας των υπολογιστικών και επικοινωνιακών συστημάτων αποτελεί η βέλτιστη επιλογή μεταξύ των διαφορετικών τεχνικών (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης , 2004). Το παρόν κεφάλαιο παρουσιάζει τις θεμελιώδεις αρχές ταυτοποίησης και αυθεντικοποίησης, καθώς επίσης και τους τρόπους με τους οποίους μπορούν να εφαρμοστούν σε αυτοματοποιημένα περιβάλλοντα. Επιπλέον, το κεφάλαιο αυτό παρουσιάζει τις κατηγορίες της αυθεντικοποίησης με βάση τις τεχνολογικές επιλογές, καθώς και παραθέτει συνοπτικά τα σημαντικότερα είδη αυθεντικοποίησης όπως: τα συνθηματικά, τις έξυπνες κάρτες, τα ψηφιακά πιστοποιητικά και τα βιομετρικά συστήματα.

3.1 Εννοιολογική Θεμελίωση

Σημαντικός παράγοντας της Ασφάλειας των Πληροφοριακών Συστημάτων αποτελεί ο έλεγχος της ταυτότητας των χρηστών. Αυτή η διαδικασία συντελείται μέσω της ταυτοποίησης και της αυθεντικοποίησης των χρηστών ενός συστήματος. Ο έλεγχος ταυτότητας για την πρόσβαση των χρηστών σε ένα Πληροφοριακό Σύστημα αποτελεί βασική προϋπόθεση για την ομαλή διαδικασία

του ελέγχου προσπέλασης σε κάθε πόρο ενός συστήματος(Guideline for the Use of Advanced Authentication Technology Alternatives,1994).

Οι έννοιες της ταυτοποίησης και της αυθεντικοποίησης σχετίζονται άμεσα με τον έλεγχο προσπέλασης και ορίζονται ως εξής: (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης, 2004)

- Ταυτοποίηση (identification) ενός λογικού υποκειμένου καλείται η διαδικασία εκείνη κατά την οποία το λογικό υποκείμενο παρέχει σε ένα Πληροφοριακό Σύστημα τις πληροφορίες που απαιτούνται προκειμένου να συσχετιστεί με ένα από τα αντικείμενα που δικαιούνται προσπέλασης στους πόρους (resources) του.
- Αυθεντικοποίηση (authentication) ενός λογικού υποκειμένου καλείται η διαδικασία εκείνη κατά την οποία ένα λογικό υποκείμενο παρέχει σε ένα Πληροφοριακό Σύστημα τις πληροφορίες που απαιτούνται προκειμένου να ελεγχθεί η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία της ταυτοποίησης.

Επομένως, η αυθεντικοποίηση αφορά τη διαδικασία κατά την οποία επαληθεύεται η δηλωθείσα ταυτότητα ενός λογικού υποκειμένου. Σε ένα σύστημα, η ανάγκη αυθεντικοποίησης οφείλεται σε δύο λόγους :

- Η ταυτότητα του λογικού υποκειμένου αποτελεί παράμετρο για τον έλεγχο προσπέλασης στους πόρους του συστήματος.
- Η ταυτότητα του λογικού υποκειμένου πρέπει να καταγράφεται σε ημερολόγια ελέγχου κατά τη διαδικασία πρόσβασης.

Η ταυτοποίηση και αυθεντικοποίηση αποτελούν τα δύο σκέλη πρωτοκόλλου επικοινωνίας, που ενεργοποιείται όταν ένα λογικό υποκείμενο αιτείται προσπέλαση στους πόρους ενός Πληροφοριακού Συστήματος. Το πρώτο από τα δύο μέρη της επικοινωνίας αυτής, δηλαδή το λογικό υποκείμενο, αποκαλείται συνήθως «Επικυρωτής» (Prover), δεδομένου ότι είναι επιφορτισμένο με την υποχρέωση να παρέχει εκείνες τις πληροφορίες που απαιτούνται για να ελεγχθεί η ταυτότητα του. Το δεύτερο μέρος, αποκαλείται συνήθως «Σκεπτικιστής» (Skeptic), δεδομένου ότι είναι επιφορτισμένο με τον έλεγχο και παρέχει ο Prover στο δεύτερο μέρος. Κάθε ένα από τα δύο μέρη μπορεί να είναι είτε χρήστης, είτε

υπολογιστικό σύστημα, είτε Πληροφοριακό Σύστημα (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης, 2004). Η διαδικασία ταυτοποίησης περιλαμβάνει την παροχή πληροφοριών, που είναι συνήθως δημόσια γνωστές (π.χ. οι πληροφορίες που σχετίζονται με τα στοιχεία ταυτότητας του λογικού υποκειμένου, οι πόροι τους οποίους επιθυμεί να προσπελάσει ή να αξιοποιήσει το υποκείμενο αυτό.)

3.2 Κατηγορίες Αυθεντικοποίησης

Η διαδικασία της αυθεντικοποίησης περιλαμβάνει την υποβολή πληροφοριών στο σύστημα που είναι εκ των προτέρων γνωστές αποκλειστικά και μόνο στο λογικό υποκείμενο και στο Πληροφοριακό Σύστημα. Ανάλογα με το είδος του συστήματος, κυριαρχούν τέσσερις βασικοί τρόποι για την εφαρμογή ελέγχων αυθεντικοποίησης. Αυτοί βασίζονται σε :

- Τύπος I : Κάτι που το λογικό υποκείμενο γνωρίζει (π.χ. ένα συνθηματικό ή ένα PIN)
- Τύπος II : Κάτι που το λογικό υποκείμενο κατέχει (μαγνητική συσκευή αναγνώρισης π.χ. έξυπνη κάρτα ή ψηφιακό πιστοποιητικό)
- Τύπος III : Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του (σύστημα βιομετρικής τεχνολογίας, π.χ. εφαρμογές δαχτυλικών αποτυπωμάτων, αναγνώριση φωνής και ίριδας ματιού
- Τύπος IV : Κάτι που προσδιορίζει την τοποθεσία που βρίσκεται το λογικό υποκείμενο (π.χ. διεύθυνση IP) (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης , 2004)

Η διαδικασία αυθεντικοποίησης περιλαμβάνει :

i. Την παροχή της πληροφορίας από ένα λογικό υποκείμενο στο σύστημα
ii. Την ανάλυση αυτής της πληροφορίας και
iii. Τον έλεγχο ότι πράγματι αυτή η πληροφορία σχετίζεται με το ίδιο λογικό υποκείμενο.

Το σύστημα, για την πραγματοποίηση των παραπάνω διαδικασιών, αποθηκεύει και διαχειρίζεται, με τους ανάλογους μηχανισμούς, τις σχετικές με τα υποκείμενα

πληροφορίες. Επομένως, ένα σύστημα αυθεντικοποίησης αποτελείται από τα παρακάτω πέντε βασικά μέρη:

- Το σύνολο A που περιέχει τις πληροφορίες με βάση τις οποίες κάθε λογικό υποκείμενο αποδεικνύει την ταυτότητά του.
- Το σύνολο C που περιέχει τις συμπληρωματικές πληροφορίες που αποθηκεύει και χρησιμοποιεί το σύστημα ώστε να επικυρώνει πληροφορίες αυθεντικοποίησης.
- Το σύνολο F των συμπληρωματικών συναρτήσεων που δημιουργούν τις συμπληρωματικές πληροφορίες για την αυθεντικοποίηση. Δηλαδή, για f ε F, τότε: f: Aϋ C.
- Το σύνολο L των συναρτήσεων αυθεντικοποίησης που αναγνωρίζουν ένα λογικό υποκείμενο. Δηλαδή, για l ε L, l: A X C ϋ {true, false}
- Το σύνολο S των λοιπών συναρτήσεων επιλογής που δίνουν τη δυνατότητα σε ένα λογικό υποκείμενο να δημιουργήσει ή να τροποποιήσει τις πληροφορίες της αυθεντικοποίησης ή τις συμπληρωματικές πληροφορίες (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης, 2004).

3.3 Πλεονεκτήματα και Μειονεκτήματα Δεδομένων Αυθεντικοποίησης

Οι παραπάνω τρεις πρώτοι τρόποι αυθεντικοποίησης (τύπος I, τύπος II, τύπος III), έχουν βασικά πλεονεκτήματα και μειονεκτήματα, τα οποία στηρίζονται στην φύση των δεδομένων αυθεντικοποίησης που χρησιμοποιούνται ξεχωριστά. Αυτά παρατίθενται στην συνέχεια (Αγγελινός, 2016) :

- Τύπος I : Κάτι που το λογικό υποκείμενο γνωρίζει

  Πλεονεκτήματα :

  - Εύκολη υλοποίηση και εφαρμογή
  - Τροποποιούνται εύκολα
  - Δεν χάνονται
  - Αν και είναι απλά στην χρήση τους, στην περίπτωση που είναι ένας συνδυασμός αλφαριθμητικών χαρακτήρων, δεν αποκαλύπτονται εύκολα

Μειονεκτήματα:

- Τα τεκμήρια αυθεντικοποίησης εύκολα μπορούν να αντιγραφούν
- Είναι εφικτό να τα μαντέψει κανείς χωρίς ιδιαίτερες τεχνικές γνώσεις
- Συνήθως μπορούν να αποκαλυφθούν με αυτοματοποιημένες μεθόδους
- Μπορούν να ξεχασθούν εύκολα

- Τύπος ΙΙ : Κάτι που το λογικό υποκείμενο κατέχει

  Πλεονεκτήματα:

  - Δεν αντιγράφονται εύκολα καθώς κατασκευάζονται από ειδικά υλικά, τα οποία δεν είναι ευρέως διαθέσιμα

  Μειονεκτήματα:

  - Υψηλό κόστος
  - Μπορούν εύκολα να χαθούν ή να κλαπούν

- Τύπος ΙΙΙ : Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του:

  Πλεονεκτήματα:

  - Παρέχουν μεγαλύτερα ασφάλεια από τον Τύπο Ι και Τύπο ΙΙ

  Μειονεκτήματα:

  - Δεν είναι αλάνθαστα
  - Έχουν εντοπισθεί δυσκολίες στην κατασκευή αξιόπιστων συσκευών αναγνώρισης με χαμηλό κόστος

3.4 Δεδομένα Αυθεντικοποίησης

Στο παρόν υποκεφάλαιο αναλύονται τα τεκμήρια που χρησιμοποιούνται για την εφαρμογή των ελέγχων αυθεντικοποίησης και ανήκουν στις δύο πρώτες κατηγορίες αυθεντικοποίησης. Συγκεκριμένα, θα αναλυθούν τα συνθηματικά, τα ψηφιακά πιστοποιητικά και οι έξυπνες κάρτες, ενώ για τα βιομετρικά συστήματα θα παρατεθεί αναλυτική παρουσίαση στη συνέχεια (O'Gorman,2002).

1. Συνθηματικά (Passwords)

Αξίζει να σημειωθεί πως, τα συνθηματικά θεωρούνται το συνηθέστερο μέσο αυθεντικοποίησης και ανήκουν στον Τύπο Ι, που αναλύσαμε και παραπάνω, δηλαδή στους μηχανισμούς που βασίζονται σε κάτι που τα λογικά υποκείμενα (χρήστες) γνωρίζουν. Συγκεκριμένα, ως συνθηματικό ορίζεται η πληροφορία, η οποία σχετίζεται με ένα λογικό υποκείμενο και η οποία επιβεβαιώνει την ταυτότητα του λογικού υποκειμένου.

Η χρήση συνθηματικών συνδυάζεται συνήθως με τα μοναδιαία αναγνωριστικά του κάθε χρήστη. Για να επιτευχθεί η διαδικασία της αυθεντικοποίησης, ο χρήστης καταχωρεί το αναγνωριστικό του και το αντίστοιχο συνθηματικό του στο σύστημα και ακολουθεί ο μηχανισμός της επαλήθευσης των στοιχείων του χρήστη (O'Gorman,2002). Η επαλήθευση γίνεται με την σύγκριση των εισαχθέντων στοιχείων με αυτά που ήδη έχουν καταχωρηθεί στο αρχείο συνθηματικών (password file) του συστήματος. Με την έγκυρη καταχώρηση των στοιχείων επέρχεται και η πρόσβαση. Λόγω της σπουδαιότητας της ασφάλειας των δεδομένων των χρηστών, ορισμένα συστήματα, τηρούν έναν μετρητή για την καταγραφή των αποτυχημένων προσπαθειών πρόσβασης από το λογικό υποκείμενο και σε περίπτωση που ξεπερασθεί το όριο, τότε αυτόματα κλειδώνει και ο λογαριασμός του χρήστη. Επιπλέον, υπάρχουν και συστήματα, τα οποία εφαρμόζουν έναν μηχανισμό επαναλαμβανόμενης αυθεντικοποίησης, ο οποίος συντελείται και κατά τη διάρκεια της χρήσης του εκάστοτε συστήματος ανά τακτά χρονικά διαστήματα (O'Gorman,2002).

Η διάδοση της χρήσης συνθηματικών βασίζεται στα πλεονεκτήματα που παρουσιάζουν :

- Έχουν χαμηλό κόστος καθώς δεν προϋποθέτουν πρόσθετο εξοπλισμό για την υλοποίηση τους, ούτε και την πρότερη εκπαίδευση των χρηστών ενός Πληροφοριακού Συστήματος.
- Είναι απλά στη χρήση τους και έχουν περιορισμένη σχεδιαστική πολυπλοκότητα.

- Παρέχουν έναν ικανοποιητικό βαθμό προστασίας, εφόσον υπάρχει πολιτική για την ασφαλέστερη εφαρμογή τους όπως θα αναφερθεί στην συνέχεια.

Παρόλα αυτά, η χρήση συνθηματικών ως μηχανισμός αυθεντικοποίησης παρουσιάζει και μειονεκτήματα όπως (O'Gorman, 2002):

- Είναι πιθανή η ανακάλυψη το συνθηματικού με συστηματικό τρόπο
- Θεωρείται πιθανή η τυχαία αποκάλυψη του
- Είναι δυνατή η αποκάλυψη συνθηματικού κατά τη διάρκεια της μετάδοσης του (ειδικά σε κατανεμημένα περιβάλλοντα)

Τα μειονεκτήματα που παραθέσαμε αυτόματα φανερώνουν την αναγκαιότητα της επιλογής συνθηματικών με σκοπό την ασφάλεια των υπολογιστικών συστημάτων. Οι μη εξουσιοδοτημένοι χρήστες μπορούν τυχαία η σκόπιμα να ανακαλύψουν το συνθηματικό των χρηστών με διαφόρους τρόπους. Τα αποτελέσματα μιας έρευνας σχετικά με την ασφάλεια απέδειξε πως το 30% των συνθηματικών που χρησιμοποιούνται από τους χρήστες, μπορεί εύκολα να αποκαλυφθεί από κάποιον που γνωρίζει τα βασικά στοιχεία ενός χρήστη. Η υποκλοπή των συνθηματικών, έχει χαρακτηριστεί από πολλούς ως ο συνηθέστερος τρόπος παραβίασης της ασφάλειας από μη εξουσιοδοτημένους χρήστες και έχουν καταγραφεί δύο μέθοδοι (O'Gorman,2002).

I. Συστηματικό ψάξιμο (brute force) : η δοκιμή όλων των πιθανών συνδυασμών των αλφαριθμητικών χαρακτήρων συγκεκριμένου μεγέθους.
II. Έξυπνο ψάξιμο : η δοκιμή πιθανών συνδυασμών που απορρέουν από πληροφορίες που σχετίζονται με τους χρήστες όπως ημερομηνία γέννησης, όνομα κ.α..

Σύμφωνα με τα παραπάνω, λόγω των πολιτικών ασφαλείας των οργανισμών, η επιλογή του συνθηματικού πρέπει να βασίζεται σε κάποια κριτήρια, τα οποία θα διασφαλίσουν την ασφάλεια του χρήστη και θα αποφύγουν τα ευπαθή συνθηματικά. Ένα σύστημα χρησιμοποιεί τα παρακάτω κριτήρια για την καθοδηγημένη επιλογή του password:

- Μήκος Συνθηματικού: ορίζεται πάντα ένα ελάχιστο μήκος (π.χ. 8 χαρακτήρες).
- Μορφότυπο Συνθηματικού: να αποτελείται από συνδυασμούς γραμμάτων, χαρακτήρων και αριθμών.
- Αποφυγή εύκολων συνθηματικών: εκμάθηση των χρηστών να αποφεύγουν εύκολα συνθηματικά όπως ονόματα.
- Οδηγίες φύλαξης: να φυλάσσονται σε ασφαλή μέρη και να μην ανακοινώνονται σε τρίτους.
- Αλλαγή Συνθηματικών: αυτόματη αλλαγή συνθηματικών από τους χρήστες.

Παρόλα αυτά, είναι δύσκολο να διασφαλίσει κανείς και να εγγυηθεί πως τα παραπάνω κριτήρια προσθέτουν ασφάλεια στο σύστημα. Αυτό συμβαίνει διότι η διαδικασία αυθεντικοποίησης είναι αδιαφανής και αυτό έχει ως αποτέλεσμα, ο χρήστης να μην γνωρίζει αν τα δεδομένα που εισάγει γνωστοποιούνται και σε μη εξουσιοδοτημένους χρήστες. Σε τέτοιες περιπτώσεις, η ενημέρωση του χρήστη κάθε φορά που υπάρχει μια αποτυχημένη προσπάθεια εισόδου στο σύστημα, αντιμετωπίζει το φαινόμενο της ψευδής χρήσης ορισμάτων. Σημαντικοί παράγοντες προστασίας των δεδομένων θεωρείται ο χρόνος αποθήκευσης των στοιχείων από το σύστημα (π.χ. πάνω στην ιστοσελίδα) και ο τόπος αποθήκευσης των φυσικών ενδιάμεσων πόρων (π.χ. cache ,buffer).

2. Ψηφιακά Πιστοποιητικά (digital certificate)

Η εφαρμογή ελέγχων αυθεντικοποίησης γίνεται με την χρήση αντικειμένων από τον χρήστη. Το ψηφιακό πιστοποιητικό αποτελεί μια διαδεδομένη τεχνολογία εφαρμογής της αυθεντικοποίησης που βασίζεται σε κάτι που ο χρήστης κατέχει (Τύπος ΙΙ). Συγκεκριμένα, τα ψηφιακά πιστοποιητικά έχουν τη μορφή δυαδικών αρχείων και η λειτουργία τους στηρίζεται στην κρυπτογραφία του δημόσιου κλειδιού. Είναι δυνατό να χρησιμοποιηθούν για τον περιορισμό της αποκάλυψης της ταυτότητας του χρήστη, ενσωματώνοντας ψευδώνυμα αντί της πραγματικής του ταυτότητας. Υπάρχουν τρία πρότυπα ψηφιακών πιστοποιητικών(Λέκκα, 2002) :

I. PKIX (Internet PKI based on X.509) : Είναι μια σειρά από προσχέδια για το διαδίκτυο που περιγράφουν διάφορα θέματα σχετικά με την ανάπτυξη μιας ιεραρχικής Υποδομής Δημοσίου Κλειδιού (ΥΔΚ). Δεδομένου ότι το Χ.059 είναι ένα γενικό πρότυπο, το οποίο αφήνει πολλά κενά που σχετίζονται με την πραγματική λειτουργία και διαχείριση μιας Έμπιστης Τρίτης Οντότητας, ΕΤΟ, αναπτύχθηκαν τα προσχέδια του PKIX.

II. SPKI (Simple Public Key Infrastructure): Αυτό το πρότυπο, περιγράφει τα πιστοποιητικά, τις απαιτήσεις, τις λειτουργίες και τα παραδείγματα χρήσης για μια ΥΔΚ μη καθολικού χαρακτήρα, για χρήση σε περιορισμένα πεδία εφαρμογής. Το SPKI χρησιμοποιεί πιστοποιητικά που έχουν ως κωδικό αναφοράς το δημόσιο κλειδί αντί για το όνομα και αντιστοιχούν σε ρόλους και όχι σε πρόσωπο. Αντιθέτως, το Χ.059 αντιστοιχεί τα δημόσια κλειδιά με ονόματα.

III. PGP (Pretty Good Privacy) : Χαρακτηρίζεται ως πρότυπο αλλά είναι μια εφαρμογή που χρησιμοποιείται στην ηλεκτρονική αλληλογραφία. Σύμφωνα με αυτό, κάθε χρήστης δημιουργεί το δικό του πιστοποιητικό και το καταχωρεί σε ένα κεντρικό ευρετήριο. Δεν υπάρχει Έμπιστη Τρίτη Οντότητα (ΕΤΟ) και έτσι ο ένας χρήστης υπογράφει το πιστοποιητικό το άλλου, εδραιώνοντας με αυτό τον τρόπο την εμπιστευτικότητα μεταξύ τους. Με αυτό τον τρόπο, σχηματίζεται ένα πλέγμα εμπιστοσύνης (web od trust), καθώς δημιουργούνται Ν προς Ν σχέσεις. Η διεύθυνση ηλεκτρονικής αλληλογραφίας κατέχει το ρόλο του διακριτικού ονόματος , η οποία βέβαια συχνά αλλάζει.

3. Έξυπνες Κάρτες (smart cards)

Οι έξυπνες κάρτες αποτελούν μα διαδεδομένη τεχνολογία εφαρμογής της αυθεντικοποίησης και βασίζεται στον Τύπο ΙΙ. Συγκεκριμένα, παρουσιάζουν ένα υψηλό επίπεδο ασφάλειας για τα δεδομένα που αποθηκεύουν και επεξεργάζονται. Επομένως, η αξιοποίηση τους από τους χρήστες και η πρόοδος που έχει παρατηρηθεί σε αυτόν τον τομέα οφείλεται στην πρόοδο στις τεχνολογίες κατασκευής ολοκληρωμένων κυκλωμάτων, η αποτελεσματικότητα

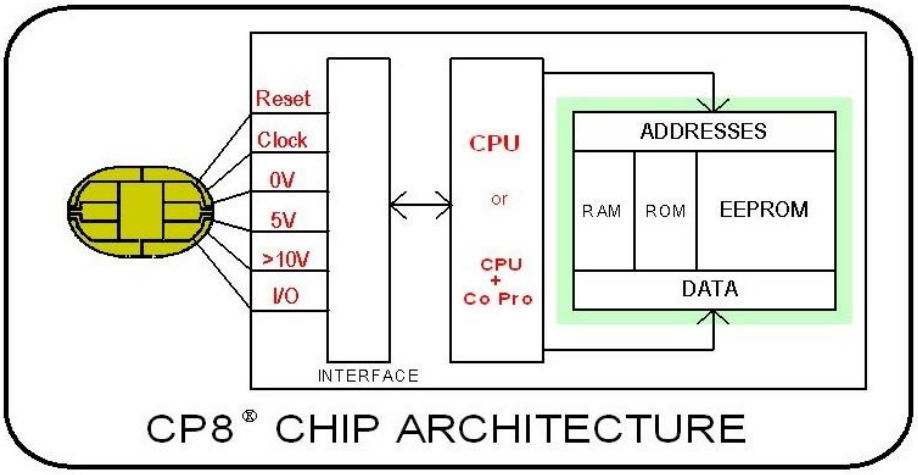
των δραστηριοτήτων προτυποποίησης και η αύξηση των περιστατικών απάτης σε συγκεκριμένους τομείς εφαρμογών. Χαρακτηριστικό των έξυπνων καρτών αποτελεί ο μικροεπεξεργαστής που διαθέτουν, με τον οποίο επιτυγχάνεται σε ένα μεγάλο επίπεδο η ασφάλεια των δεδομένων, σε αντίθεση με τις μαγνητικές κάρτες, οι οποίες διαθέτουν μερικά bytes επαναχρησιμοποιήσιμης μνήμης(Fancher, 1997).

Επιπλέον οι έξυπνες κάρτες προσδιορίζονται στο έπακρο από τρεις λέξεις: ασφάλεια, φορητότητα και ευκολία χρήσης. Είναι γεγονός ότι ο επεξεργαστής, η μνήμη και η υποστήριξη για I/O βρίσκεται σε ένα κύκλωμα, το οποίο είναι ενσωματωμένο σε μια πλαστική κάρτα. Επιπλέον, η ευκολία χρήσης και η φορητότητα τις έχουν καταστήσει σε χώρες όπως οι Ηνωμένες Πολιτείες της Αμερικής και το Μπαχρέιν ως «ηλεκτρονικά πορτοφόλια», καθώς οι χρήστες έχουν την δυνατότητα για ασφαλής αγορές στο ίντερνετ, αφού οι πληροφορίες που απαιτούνται βρίσκονται μόνο στη μνήμη της κάρτας.

Τα πλεονεκτήματα που προαναφέρθηκαν έχουν δημιουργήσει ένα κλίμα ασφάλειας για τους χρήστες με αποτέλεσμα διάφοροι οργανισμοί να υιοθετούν την συγκεκριμένη τεχνολογία και σε άλλες εφαρμογές όπως : κινητά τηλέφωνα, ηλεκτρονικό πορτοφόλι, κάρτα ασθενούς, έλεγχος φυσικής πρόσβασης σε εγκαταστάσεις κ.α. Στην συνέχεια της συγκεκριμένης υποενότητας θα αναφερθούμε στην αρχιτεκτονική των έξυπνων καρτών, καθώς και στη συμβολή τους στις διαδικασίες της ταυτοποίησης και αυθεντικοποίησης.

Το παρακάτω σχήμα που ακολουθεί απεικονίζει τη λειτουργία της έξυπνης κάρτας, η οποία διαθέτει μικροεπεξεργαστή που ελέγχει τη λειτουργία τριών διαφορετικών τύπων μνήμης: (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης , 2004)

- Μνήμη εργασίας (working memory- Random Access Memory)
- Η μη διαγράψιμη μνήμη ROM (Read Only Memory)
- Η μνήμη εφαρμογών (EEPROM)



Εικόνα 1: Αρχιτεκτονική Έξυπνης Κάρτας

Συγκεκριμένα:

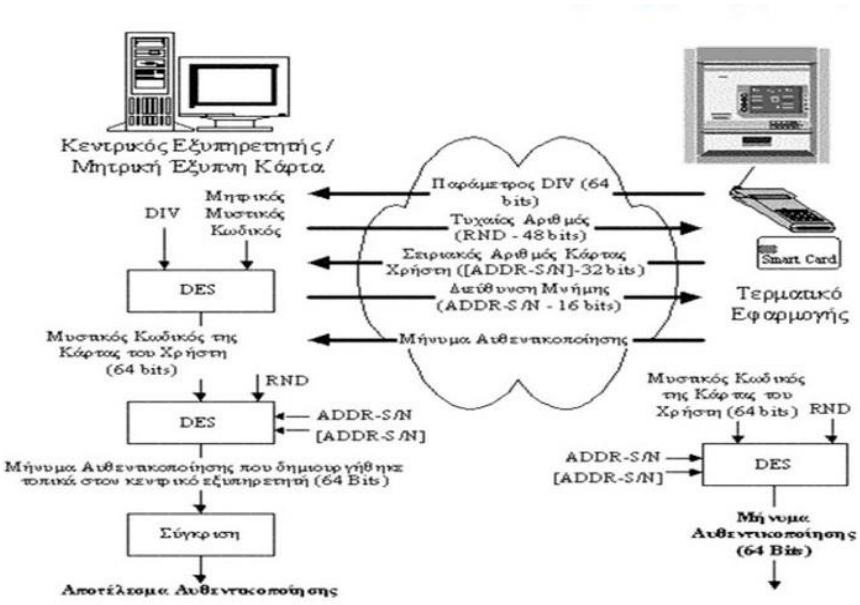
- Η μνήμη εργασίας διατηρεί τα περιεχόμενά της μόνο κατά τη διάρκεια που η έξυπνη κάρτα τροφοδοτείται με ρεύμα και συνεπώς αξιοποιείται αποκλειστικά και μόνο από τον μικροεπεξεργαστή για προσωρινή αποθήκευση δεδομένων.
- Η μη διαγράψιμη μνήμη, η οποία δεν απαιτεί συνεχή τροφοδοσία για τη διατήρηση των δεδομένων που έχουν αποθηκευτεί σ' αυτή. Αυτή η μνήμη αξιοποιείται για την αποθήκευση του λειτουργικού συστήματος της κάρτας μέσω του οποίου υποστηρίζονται οι λειτουργικές προδιαγραφές και οι μηχανισμοί ασφάλειας (διαχείριση μυστικών κλειδιών και κωδικών, εκτέλεση κρυπτογραφικών αλγορίθμων) της κάρτας.
- Η μνήμη εφαρμογών, η οποία αξιοποιείται για την εγγραφή, ενημέρωση και διαγραφή δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής της έξυπνης κάρτας. Συνήθως η συγκεκριμένη μνήμη οργανώνεται σε λέξεις των 32 bit, ενώ η συνολική χωρητικότητα της είναι από 1 έως 64 Kbytes.

Στο σημείο αυτό, όπως αναφέρθηκε και προηγουμένως, θα μιλήσουμε για τη συμβολή των έξυπνων καρτών στις διαδικασίες της αυθεντικοποίησης και της ταυτοποίησης. Πιο συγκεκριμένα, η διαδικασία της ταυτοποίησης του κατόχου της έξυπνης κάρτας γίνεται μέσω του μυστικού προσωπικού κωδικού του (PIN), ο οποίος είναι απαραίτητος ώστε να χρησιμοποιηθεί η κάρτα. Έτσι, αυτός ο κωδικός

συγκρίνεται με τον αντίστοιχο κωδικό που είναι αποθηκευμένος στη μυστική περιοχή της μνήμης της έξυπνης κάρτας, διαδικασία η οποία θεωρείται ασφαλής καθώς εκτελείται εσωτερικά στην έξυπνη κάρτα. Δεδομένου ότι η διαδικασία της ταυτοποίησης γίνεται εσωτερικά, αυτόματα απομακρύνεται ο κίνδυνος να ανακληθεί το PIN από μια μαγνητική κάρτα. Επιπλέον, ως πλεονέκτημα οι έξυπνες κάρτες διαθέτουν μεγάλο αποθηκευτικό χώρο, ο οποίος μπορεί να ανταποκριθεί και σε βιομετρικά χαρακτηριστικά αντί της χρήσης του PIN από τον κάτοχο της. Οι έξυπνες κάρτες έχουν την δυνατότητα να αποθηκεύουν το δακτυλικό αποτύπωμα, το σχήμα της παλάμης αλλά και την ίριδα του ματιού. Σχετικά με τα βιομετρικά συστήματα θα αναφερθούμε εκτενώς στο επόμενο κεφάλαιο.

Αντιστοίχως, η διαδικασία της αυθεντικοποίησης στοχεύει στην διασφάλιση της γνησιότητας της έξυπνης κάρτας, δηλαδή ότι έχει εκδοθεί από εξουσιοδοτημένους φορείς. Η υλοποίηση αυτής της διαδικασίας μπορεί να γίνει είτε με την χρήση ψηφιακών πιστοποιητικών και ασύμμετρων κρυπτογραφικών αλγορίθμων, είτε χρησιμοποιώντας τους συμμετρικούς αλγορίθμους κρυπτογράφησης. Ειδικότερα, οι έξυπνες κάρτες πρέπει πρώτα να προσωποποιηθούν και μετά να δοθούν στους κατόχους. Κατά τη διάρκεια αυτής της διαδικασίας εγγράφονται οι απαραίτητοι μυστικοί κωδικοί και κλειδιά. Η δημιουργία τους έχει ως κεντρικό πυρήνα την εμπιστευτικότητα των κλειδιών και κωδικών των καρτών, επομένως βασίζεται στη διαφοροποίηση ενός μητρικού μυστικού κωδικού που βρίσκεται αποθηκευμένο στη γνωστή ως μητρική έξυπνη κάρτα (Fancher, 1997). Η εσωτερική αυτή διαδικασία περιλαμβάνει το μητρικό μυστικό κωδικό, ο οποίος είναι αποθηκευμένος μέσα στην κάρτα, μια προκαθορισμένη διεύθυνση μνήμης της μητρικής έξυπνης κάρτας, τα περιεχόμενα της συγκεκριμένης θέσης μνήμης και το σειριακό αριθμό της έξυπνης κάρτας που θα προσωποποιηθεί. Αξίζει να σημειωθεί ότι το γεγονός ότι κάθε κάρτα έχει διαφορετικό σειριακό αριθμό, διασφαλίζει την διαφοροποίηση των παραγόμενων κλειδιών για τις κάρτες των χρηστών. Επιπλέον, ο μυστικός αυτός κωδικός δεν είναι γνωστός σε κανέναν.

Αντιστοίχως, κατά τη διαδικασία της αυθεντικοποίησης, όταν κάποιος χρήστης εισάγει την κάρτα του σε ένα τερματικό με στόχο να αποκτήσει πρόσβαση σε υπηρεσίες ή δεδομένα, τότε ο κεντρικός εξυπηρετητής, στον οποίο είναι εγκατεστημένη η μητρική έξυπνη κάρτα, ζητά από την έξυπνη κάρτα τη δημιουργία και αποστολή ενός μηνύματος αυθεντικοποίησης (Fancher, 1997) . Για να δημιουργηθεί αυτό το μήνυμα, χρησιμοποιείται ένας τυχαίος αριθμός και ο σειριακός αριθμός της κάρτας του χρήστη. Το ίδιο ακριβώς μήνυμα υπολογίζεται και από την μητρική κάρτα, ανεξάρτητα από τη κάρτα του χρήστη και τα δύο αυτά μηνύματα συγκρίνονται. Αν είναι τα ίδια τότε η κάρτα θεωρείται γνήσια. Το παρακάτω σχήμα απεικονίζει αυτή τη διαδικασία της αυθεντικοποίησης:



Εικόνα 2: Διαδικασία Αυθεντικοποίησης
Πηγή Δρ. Αγγελινός, Γ. (2016)

Ειδικότερα τα βήματα κατά τη διαδικασία της αυθεντικοποίησης είναι τα εξής (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης , 2004) :

<u>Δημιουργία Μηνύματος Αυθεντικοποίησης από την Κάρτα του Χρήστη</u>

- Ο κεντρικός εξυπηρετητής δημιουργεί και αποστέλλει στην έξυπνη κάρτα του χρήστη ένα τυχαίο αριθμό (RND), μαζί με τη διεύθυνση της θέσης μνήμης που είναι αποθηκευμένος ο σειριακός αριθμός της έξυπνης κάρτας (ADDR-S/N).
- Η έξυπνη κάρτα του χρήστη εκτελεί το κρυπτογραφικό αλγόριθμο DES με παραμέτρους εισόδου τον τυχαίο αριθμό (RND), το μυστικό κωδικό της

κάρτας, τη διεύθυνση της θέσης μνήμης που είναι αποθηκευμένος ο σειριακός αριθμός της (ADDR-S/N) και τον ίδιο τον σειριακό αριθμό της. Ο αλγόριθμός DES εκτελείται δύο φορές όπως και στην προσωποποίηση της κάρτας, όπου αντί του σειριακού αριθμό χρησιμοποιείται ένας τυχαίος αριθμός.

Αναπαραγωγή Μυστικού Κωδικού της Κάρτας Χρήστη από την Μητρική Έξυπνη Κάρτα

- Η έξυπνη κάρτα δημιουργεί και αποστέλλει στον κεντρικό πυρήνα την παράμετρο DIV.
- Η μητρική έξυπνη κάρτα αναπαράγει το μυστικό κωδικό της κάρτας του χρήστη, ακολουθώντας την ίδια ακριβώς διαδικασία που είχε ακολουθηθεί κατά τη διάρκεια της προσωποποίησης της έξυπνης κάρτας.

Δημιουργία Μηνύματος Αυθεντικοποίησης από την Μητρική Έξυπνη Κάρτα

- Η έξυπνη κάρτα αποστέλλει στον κεντρικό εξυπηρετητή τα περιεχόμενα της θέσης μνήμης, που είναι ο σειριακός αριθμός της κάρτας.
- Η μητρική έξυπνη κάρτα αξιοποιεί τον μυστικό κωδικό της κάρτας του χρήστη, τον οποίο αναπαράγει για να υπολογίσει το μήνυμα.

Σύγκριση των Μηνυμάτων Αυθεντικοποίησης

- Η μητρική έξυπνη κάρτα συγκρίνει το μήνυμα αυθεντικοποίησης που υπολογίστηκε με αυτό που έστειλε η έξυπνη κάρτα στον χρήστη. Αν αυτά τα δύο είναι ίδια, τότε η κάρτα του χρήστη θεωρείται γνήσια.

Τέλος, αξίζει να σημειωθεί, ότι κατά τη διαδικασία της αυθεντικοποίησης κανένα μυστικό κλειδί δεν μεταφέρεται μέσω του δικτύου από ή προς την έξυπνη κάρτα του χρήστη. Μόνο το μήνυμα αυθεντικοποίησης που υπολογίζει η έξυπνη κάρτα του χρήστη αποστέλλεται μέσω του δικτύου στο κεντρικό εξυπηρετητή.

4.Βιομετρικά Συστήματα

Το κεφάλαιο αυτό πραγματεύεται τα βιομετρικά συστήματα, τα οποία ανήκουν στην τρίτη κατηγορία αυθεντικοποίησης που χαρακτηρίζουν το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του. Οι μέχρι τώρα

μέθοδοι αναγνώρισης ταυτότητας που βασίζονται σε πιστοποιητικά, δηλαδή κωδικοί πρόσβασης, ταυτότητες κ.α., δεν μπορούν να ανταποκριθούν στις συνεχώς αυξανόμενες απαιτήσεις για την καλύτερη ασφάλεια των λογικών υποκειμένων σε εφαρμογές που αφορούν τον έλεγχο πρόσβασης σε εγκαταστάσεις κρίσιμες για την εθνική ασφάλεια. Τα κυριότερα τεκμήρια της διαδικασίας της αυθεντικοποίησης αποτελούν τα δακτυλικά αποτυπώματα, η ίριδα ματιού, η χροιά φωνής, η γεωμετρία χεριού και το DNA, τα οποία θα αναλύσουμε στην συνέχεια του κεφαλαίου. Επιπλέον, θα παρουσιαστούν και ερευνητικά ευρήματα σε σχέση με την επίγνωση των χρηστών και η αποδοχή των βιομετρικών συστημάτων.

4.1 Βιομετρικά Συστήματα

Η ραγδαία ανάπτυξη των βιομετρικών τεχνολογιών και η αύξηση της εφαρμογής τους σε διάφορους τομείς δημιουργούν ορισμένους προβληματισμούς από την οπτική γωνία της προστασίας των προσωπικών δεδομένων. Η χρήση των βιομετρικών συστημάτων αποσκοπεί στην εφαρμογή ελέγχων ταυτοποίησης και αυθεντικοποίησης. Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται από βιομετρικά συστήματα έχουν ιδιαίτερο χαρακτήρα και προσδιορίζουν τον κάθε άνθρωπο μοναδικά. Τα βιομετρικά συστήματα διαθέτουν αυτοματοποιημένες μεθόδους για τη μέτρηση ενός ανθρώπινου φυσικού ή βιολογικού χαρακτηριστικού. Κατά την εγγραφή του ανθρώπου σε ένα βιομετρικό σύστημα, αποθηκεύεται το χαρακτηριστικό του γνώρισμα με τη χρήση ειδικών τεχνικών μετρήσεων. Οι βιομετρικές τεχνικές διαχωρίζονται σε δύο κατηγορίες: (“Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα”)https://www.dpa.gr/portal/page?_pageid=33,131182&_dad=portal&_schema=PORTAL

1. Φυσικά χαρακτηριστικά ανθρώπων, όπου περιλαμβάνονται τα δακτυλικά αποτυπώματα, η ίριδα ματιού, γεωμετρία χεριού, ανάλυση δείγματος DNA, ανάλυση ιδρώτα και η αναγνώριση αυτιού.
2. Τεχνική μέτρησης της συμπεριφοράς, όπου περιλαμβάνεται η αναγνώριση της υπογραφής, η ανάλυση της πληκτρολόγησης και η ανάλυση της ομιλίας. Η

κατηγορία αυτή ονομάζεται και βιολογικά χαρακτηριστικά, στα οποία προστίθενται η χροιά της φωνής, το βάδισμα, ακόμα και η εφίδρωση. Παράδειγμα όμως συμπεριφοράς αποτελεί και ο τρόπος που θα πιεστεί το δάκτυλο μας πάνω στον αισθητήρα αναγνώρισης δακτυλικού αποτυπώματος.

Έχουν παρατηρηθεί δύο βασικές έννοιες στην μέτρηση των βιομετρικών χαρακτηριστικών, η μέθοδος αποθήκευσης των προτύπων ανάλυσης και η ανοχή στο σφάλμα. Η αποτύπωση της βιομετρικής μέτρησης του γνωρίσματος του χρήστη, αποκαλείται πρότυπο και μπορεί να αποθηκευτεί σε διάφορα μέσα σύμφωνα με τις δυνατότητες της χρησιμοποιούμενης τεχνολογίας και τις απαιτήσεις ασφάλειας της εφαρμογής. Τα πρότυπα μπορούν να αποθηκευτούν είτε στην ίδια βιομετρική συσκευή είτε σε μια κεντρική βάση δεδομένων ή σε μια πλαστική κάρτα. Η ρύθμιση του βαθμού σφάλματος από την άλλη σε αυτά τα συστήματα είναι κρίσιμη, καθώς επηρεάζει την απόδοση του συστήματος. Το επίπεδο ανοχής πρέπει να είναι χαμηλό και να αναφέρεται από τον κατασκευαστή του συστήματος (O'Gorman, 2002).

4.2 Παραδείγματα Βιομετρικών Τεχνικών

Θα αναλύσουμε ενδεικτικά για κάποια από τα είδη συστημάτων της βιομετρικής τεχνολογίας :

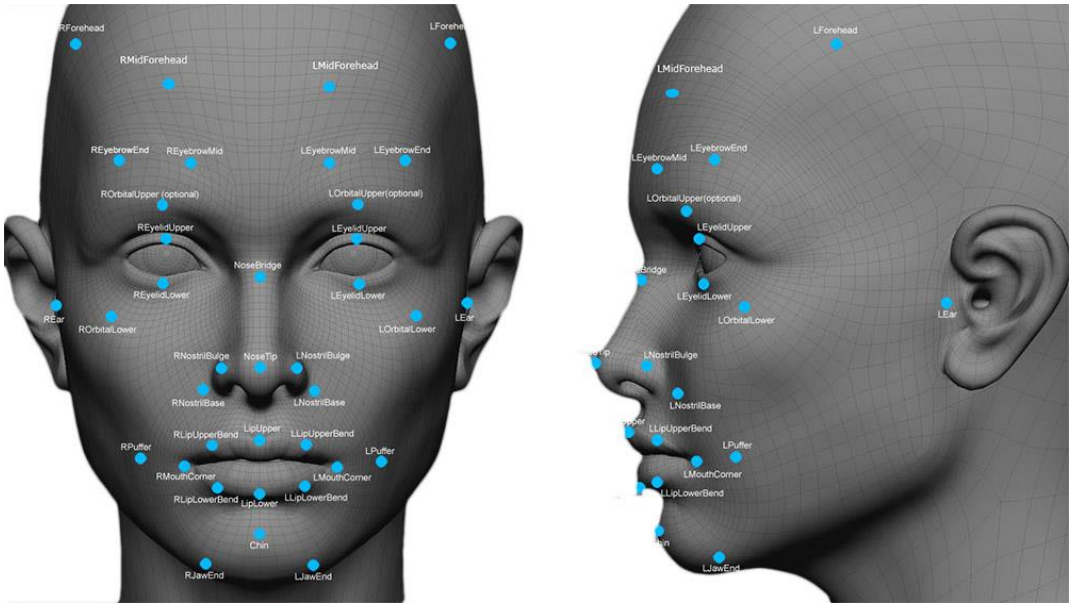
1. <u>Δακτυλικά Αποτυπώματα</u>

Ο τύπος και η γεωμετρία των δακτυλικών αποτυπωμάτων διαφέρει ανά τους ανθρώπους. Τα χαρακτηριστικά αυτά δεν μεταβάλλονται με την γήρανση. Τα πιο χαρακτηριστικά γνωρίσματα είναι οι καμπύλες και οι διαιρέσεις των σπειρών καθώς και η ολική μορφή του δακτυλικού σπειρώματος. Τα συστήματα που χρησιμοποιούνται για την αναγνώριση των δακτυλικών αποτυπωμάτων είναι πολύπλοκα. Η οπτική ανίχνευση των δακτυλικών αποτυπωμάτων γίνεται από ειδικές κάμερες οι οποίες είναι ογκώδης. Μια ικανοποιητική τεχνική χρησιμοποιεί τις διαφορές των ηλεκτρονικών φορτίων στις σπείρες του δακτύλου ώστε να εντοπίσει τα σημεία του δακτύλου που εφαρμόζουν στο τσιπ. Οι συσκευές αυτές λέγονται fingerprints scanners και διαθέτουν έναν αισθητήρα, όπου ο χρήστης τοποθετεί το δάκτυλό του για να καταγραφεί το αποτύπωμά του, βάσει του οποίου

θα ελέγχεται κάθε ένας που θα προσπαθήσει στο μέλλον να μπει στον υπολογιστή. Το αποτύπωμα αποθηκεύεται σε μία βάση δεδομένων και το ειδικευμένο software που συνοδεύει αυτές τις συσκευές αναλαμβάνει να συγκρίνει τα χαρακτηριστικά του αποτυπώματος όποιου εκκινεί το σύστημα με τα αποτυπώματα του χρήστη που έχει αποθηκευμένο(Jain, Pankanti, Ross & Prabhakar,2001). Παρόλα αυτά, υπάρχουν και κάποια μειονεκτήματα από τη χρήση τέτοιου είδους βιομετρικών συστημάτων. Μερικά από αυτά δεν μπορούν να διακρίνουν ένα πραγματικό δακτυλικό αποτύπωμα ενός ανθρώπου από ένα αντίγραφο. Τυχαίες και πρόσκαιρες τροποποιήσεις του δακτυλικού αποτυπώματος (π.χ. τραυματισμός στο μέρος του δακτύλου) αποτελούν παράγοντες που μπορούν να επηρεάσουν την επίδοση των συστημάτων αυτών. Επίσης, υπάρχει κοινωνική αντίδραση στη χρήση της συγκεκριμένης μεθόδου καθώς συνδυάζεται με τη χρήση τους από αστυνομικές υπηρεσίες (π.χ. καταγραφή δακτυλικών αποτυπωμάτων).Συνήθως, προτείνεται το δακτυλικό αποτύπωμα να μην αποθηκεύεται σε κεντρική βάση δεδομένων αλλά σε κάρτα ιδιοκτησίας του χρήστη. Η χρήση των παραπάνω συστημάτων είναι ευρεία σε τομείς της ιατρικής, σε κυβερνητικούς φορείς, σε αεροδρόμια, σε χρηματοοικονομικούς οργανισμούς.

2. <u>Αναγνώριση προσώπου</u>

Η τεχνική αυτή βασίζεται στο ότι τα χαρακτηριστικά γνωρίσματα του προσώπου των ανθρώπων όπως σχήμα ματιών, το στόμα κ.α. είναι μοναδικά για τον καθένα και εύκολα μπορεί να γίνει η ταυτοποίηση. Λόγω της χρήσης εξελιγμένων νευρωτικών δικτύων, καθιστά την τεχνολογία ακριβή. Επιπλέον, η χρήση κάμερας θεωρείται αναγκαία ώστε να εξάγει τα χαρακτηριστικά γνωρίσματα του προσώπου και να τα αποθηκεύσει σε μια μαγνητική κάρτα. Βέβαια, τα συστήματα αυτά έρχονται αντιμέτωπα με αρκετούς περιορισμούς εξαιτίας της θέσης του προσώπου απέναντι στην κάμερα, τον φωτισμό, αλλά και σε περίπτωση μορφασμών. (Μπόζιος 2004)



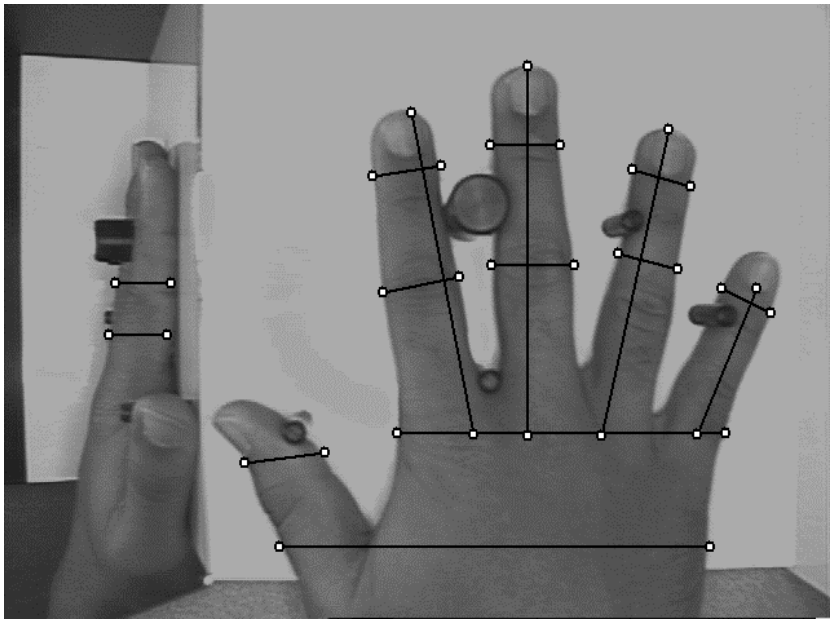
Εικόνα 3: Αναγνώριση Προσώπου

3. <u>Ίριδα ματιού</u>

Η αναγνώριση και ταυτοποίηση της ανθρώπινης ίριδας σύμφωνα με ειδικούς μελετητές αποτελεί μια μοναδική και απαραβίαστη μέθοδο αναγνώρισης κάποιου ατόμου. Αυτό συμβαίνει διότι η ίριδα του ματιού είναι το μοναδικό ανατομικό στοιχείο του, για το οποίο υπάρχει πραγματικά ισχνή πιθανότητα να μοιάζει με κάποιο άλλο. Το σύστημα αυτό ονομάζεται Iris Recognition System (IRIS) και αναγνωρίζει το κατά πόσο ένας άνθρωπος είναι πραγματικά αυτός που ισχυρίζεται ότι είναι. Η διαδικασία έχει ως εξής: όταν το μάτι του ανθρώπου πλησιάσει το φακό της κάμερας 5 με 10 εκατοστά, τότε ο φακός εστιάζει στην ίριδα και τραβάει στιγμιότυπο (snapshot), αφού η ίριδα είναι καθαρή. Μετά την επεξεργασία, το διάγραμμα της ίριδας μετατρέπεται ψηφιακά σε μια μοναδική διάταξη αλγορίθμων, που αποτελεί τον κωδικό πρόσβασης του χρήστη. Η χρήση αυτού του συστήματος δεν έχει θεωρηθεί επιβλαβής για την υγεία των ανθρώπων (Burger & Fustier, 2005)

4. Γεωμετρία χεριού

Η γεωμετρία χεριού είναι γνωστή και ως σάρωση χεριού. Πρόκειται για μια αυτοματοποιημένη μέτρηση πολλών μεγεθών του χεριού και των δαχτύλων. Η τεχνολογία αυτή χρησιμοποιεί το ύψος των δαχτύλων, την απόσταση μεταξύ κλειδώσεων και το σχήμα των αρθρώσεων για να πιστοποιήσει την ταυτότητα του χρήστη. Η τεχνική αυτή δεν θεωρείται από τις πιο δημοφιλής, παρόλα αυτά χρησιμοποιείται μόνο για επαλήθευση και έλεγχο πρόσβασης ασφάλειας χαμηλού επιπέδου. Η μέθοδος απόκτησης του βιομετρικού δείγματος είναι ιδιαίτερα απλή καθώς ο χρήστης τοποθετεί το χέρι του στην ειδική συσκευή ακουμπώντας την παλάμη του σε μια μεταλλική επιφάνεια διαστάσεων 8x10. Στην συνέχεια, ο χρήστης ευθυγραμμίζει το χέρι του σύμφωνα με τα πέντε ειδικά καρφιά, που είναι σχεδιασμένα έτσι ώστε να υποδεικνύουν την κατάλληλη θέση των δακτύλων. Πολλές φορές, η σάρωση χεριού ταυτίζεται με την σάρωση παλάμης, παρ' όλο που πρόκειται για διαφορετικές τεχνολογίες(Burger & Fustier, 2005;Μπόζιος,2004).



Εικόνα 4: Γεωμετρία Χεριού

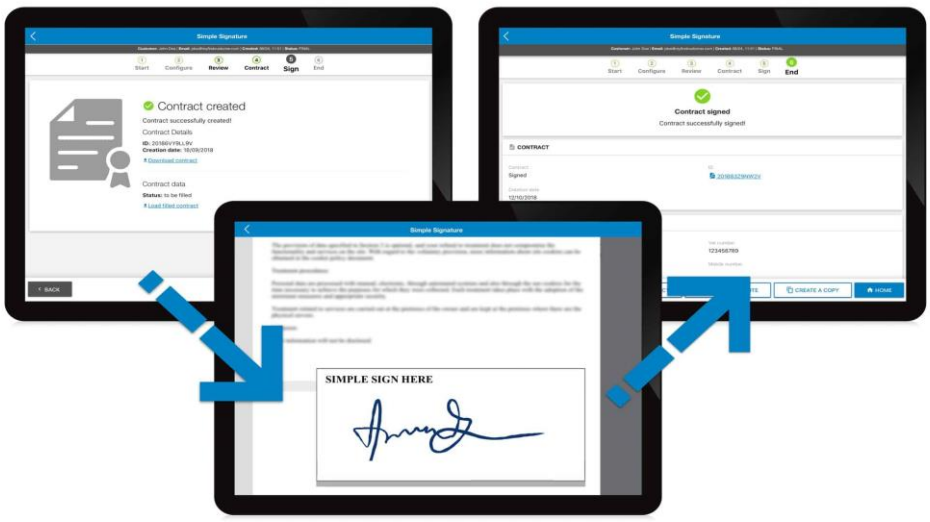
5. DNA

Η μέθοδος βασίζεται σε ανάλυση DNA. Ειδικότερα, για να εκτελεστεί μια ανάλυση DNA, ο χρήστης πρέπει να δώσει μερικά από τα κύτταρα του, για παράδειγμα δίνοντας μαλλιά ή κάποιο δέρμα. Η ανάλυση του DNA απαιτεί πολύ

χρόνο και αυτός είναι ο βασικότερος λόγος για τον οποίο δεν χρησιμοποιείται ως μέθοδος ελέγχου ταυτότητας. Η συμβολή του δείγματος DNA, θα μπορούσε να βοηθήσει τις διαδικασίες αυθεντικοποίησης, καθώς θα παρείχε εξαιρετική πιστοποίηση, διότι όλοι είναι μοναδικοί μέσω του DNA τους. Όμως, μπορεί εύκολα κάποιος να κλέψει μια τρίχα από κάποιον άλλο και να παραπλανήσει το σύστημα. Με βάση αυτήν την εκδοχή, πιθανόν οι ερευνητές να βρουν έναν καλό τρόπο να εφαρμόσουν τέτοιες συσκευές και ίσως να γίνει ο πιο αποτελεσματικός τρόπος ταυτοποίησης των ανθρώπων(Burger & Fustier, 2005).

6. Αναγνώριση της υπογραφής

Η υπογραφή είναι μια συμπεριφοριστική βιομετρική μορφή που χρησιμοποιείται σε καθημερινές συναλλαγές και θεωρείται αξιόπιστη αναγνώριση ατόμων με βάση την υπογραφή τους. Επειδή το κάθε άτομο έχει έναν προσωπικό γραφικό χαρακτήρα, το σύστημα παίρνει τα χαρακτηριστικά του τρόπου γραφής και αναλύει τη δυναμική του χτυπήματος, της ταχύτητας και της πίεσης. Έχουν γίνει πολλές προσπάθειες για τη δημιουργία συστημάτων αναγνώρισης υψηλής ευκρίνειας, όμως ήταν ανεπιτυχής λόγω της πιθανής αλλαγής των υπογραφών μέσα στο πέρασμα του χρόνου (Burger & Fustier, 2005).



Εικόνα 5: Αναγνώριση Υπογραφής

7. Ανάλυση βηματισμού

Η συγκεκριμένη τεχνολογία βρίσκεται ακόμα σε πρώιμο στάδιο, όμως αναμένεται να αποτελέσει ένα ισχυρό όπλο στην προσπάθεια εντοπισμού εγκληματιών. Έχει πλέον διαπιστωθεί ότι ο κάθε άνθρωπος περπατάει διαφορετικά με έναν δικό του τρόπο, καθώς οι κινήσεις που εκτελεί όταν περπατάει είναι μοναδικές. Σκοπός της πλατφόρμας που βρίσκεται σε εξέλιξη είναι, η σύγκριση και αναγνώριση της ταυτότητας προσώπων. Απώτερος σκοπός είναι η δημιουργία συστημάτων επιτήρησης, που θα μπορούν να αναγνωρίσουν και να πιστοποιήσουν ανθρώπινους στόχους από τον τρόπο που περπατάνε σε κρίσιμες περιοχές ασφαλείας όπως αεροδρόμια, τράπεζες (Burger & Fustier, 2005).

8. Ανάλυση Πληκτρολόγησης

Η συγκεκριμένη τεχνική εξετάζει το πώς ένα άτομο δακτυλογραφεί ή πιέζει τα πλήκτρα. Αυτή η τεχνολογία αναλύει χαρακτηριστικά όπως η ταχύτητα, η δύναμη, η συχνότητα λάθους, ο συνολικός χρόνος δακτυλογράφησης ενός συγκεκριμένου συνθηματικού και ο χρόνος που μεσολαβεί από το πάτημα ενός συγκεκριμένου πλήκτρου έως το πάτημα ενός άλλου συγκεκριμένου πλήκτρου. Η παραπάνω τεχνική έχει ως πλεονέκτημα το γεγονός ότι ο τρόπος δακτυλογραφεί ένα άτομο είναι ξεχωριστός, ειδικά ο ρυθμός του. Δηλαδή ακόμα κι αν κάποιος μαντέψει το συνθηματικό, δε θα μπορέσει να το βάλλει με τον κατάλληλο ρυθμό (Burger & Fustier, 2005).

4.3 Χαρακτηριστικά Βιομετρικών Συστημάτων

Τα κύρια χαρακτηριστικά των βιομετρικών συστημάτων παρατίθενται αναλυτικά: (Κάτσικας, Γκρίτζαλης & Γκρίτζαλης , 2004)

1. Ακρίβεια

Ορίζεται το ποσοστό συχνότητας ορθής αναγνώρισης ενός εξουσιοδοτημένου προσώπου από ένα μη εξουσιοδοτημένο. Χρησιμοποιούνται δύο μονάδες μέτρησης της ακρίβειας:

- το ποσοστό απόρριψης εξουσιοδοτημένων ατόμων και (Σφάλμα Απόρριψης)
- το ποσοστό αποδοχής μη εξουσιοδοτημένων ατόμων (Σφάλμα Αποδοχής)

Οι δύο μονάδες μέτρησης ρυθμίζονται ανάλογα με τις απαιτήσεις ασφαλείας του βιομετρικού συστήματος.

2. Ταχύτητα

Ως ταχύτητα απόκρισης θεωρείται το χρονικό όριο αναγνώρισης του ατόμου από το σύστημα, περίπου πέντε δευτερόλεπτα.

3. Αξιοπιστία

Η αξιοπιστία ορίζεται ως η συνεχής, ακριβής και γρήγορη λειτουργία του βιομετρικού συστήματος, χωρίς να απαιτείται υψηλό ποσοστό συντήρησης ή ελέγχου λειτουργίας του.

4. Αποθήκευση Δεδομένων και Απαιτήσεις Επεξεργασίας

Ο χρόνος επεξεργασίας των δεδομένων ενός χρήστη επηρεάζεται από αυτά τα δύο χαρακτηριστικά. Το χαμηλό επίπεδο αποδοχής σφάλματος δημιουργεί περισσότερη αναμονή για την εισαγωγή δεδομένων και τη σύγκριση με τη βάση δεδομένων. Οι απαιτήσεις επεξεργασίας των βιομετρικών συσκευών θεωρούνται ικανοποιητικές από άποψη λειτουργίας, καθώς έχουν ανακαλυφθεί ταχύτατοι επεξεργαστές. Το μέσο μέγεθος ενός αρχείου με βιομετρικά στοιχεία κυμαίνεται μεταξύ 256 και 1000 bytes.

5. Διαδικασία Καταχώρησης

Ορίζεται ως ο χρόνος που απαιτείται για την εισαγωγή των στοιχείων της ταυτότητας και του βιομετρικού χαρακτηριστικού ενός χρήστη. Στα σημερινά συστήματα δεν αποτελεί στοιχείο προς αξιολόγηση, καθώς ο μέσος χρόνος καταχώρησης είναι τα δύο λεπτά.

6. Μοναδικότητα

Τα βιομετρικά συστήματα βασίζονται σε μοναδικά χαρακτηριστικά του ανθρώπινου σώματος ενισχύουν την πιθανότητα της ορθής εφαρμογής της αναγνώρισης. Τα τρία φυσικά χαρακτηριστικά που ικανοποιούν αυτό το κριτήριο είναι το δακτυλικό αποτύπωμα, η ίριδα ματιού και ο αμφιβληστροειδής του ματιού.

7. Παραποίηση Στοιχείων

Στα βιομετρικά συστήματα καθοριστικό ρόλο διαδραματίζει η μη δυνατότητα εισόδου σε μη εξουσιοδοτημένο πρόσωπο. Για την επίτευξη της πρόσβασης χρειάζεται μεγάλη ακρίβεια του βιομετρικού χαρακτηριστικού.

8. Αποδοχή του Χρήστη

Λόγω της ιδιομορφίας που παρουσιάζουν ως προς τα εισαγόμενα δεδομένα, τα βιομετρικά συστήματα, δημιουργούν κάποιες κοινωνικές αντιδράσεις. Οι χρήστες συχνά αντιδρούν, νοιώθοντας ότι πρέπει να καταχωρήσουν ένα γνώρισμα (π.χ. διαστάσεις παλάμης) του σώματος τους σε μια βάση δεδομένων του συστήματος κατά τη διαδικασία της εγγραφής τους. Επιπλέον, κυριαρχεί το συναίσθημα και ο φόβος ότι παρακολουθούνται από το σύστημα και ότι καταγράφονται οι κινήσεις τους. Η πλειοψηφία των χρηστών θεωρεί ότι προκαλεί βλαβερές συνέπειες στην υγεία τους το κόκκινο laser που χρησιμοποιείται στην ίριδα του ματιού. Όμως, όσα αναφέρθηκαν, αποτελούν απλά ανησυχίες των χρηστών, χωρίς να έχει προκληθεί κάποια σωματική βλάβη από τα βιομετρικά συστήματα . Καθίσταται επομένως απαραίτητη η ενημέρωση και εκπαίδευση των χρηστών σχετικά με την χρήση των βιομετρικών συστημάτων, καθώς κρίνεται αναγκαία για την επιτυχημένη εφαρμογή τους.

4.4 Πλεονεκτήματα και Μειονεκτήματα Βιομετρικών Συστημάτων

Η χρήση των βιομετρικών συστημάτων ως μέθοδοι ασφαλείας, διευκολύνουν την καθημερινότητά μας, διότι μας απαλλάσσουν από την απομνημόνευση κωδικών. Χρειαζόμαστε μόνο ένα από τα μονοσήμαντα χαρακτηριστικά μας για να έχουμε πρόσβαση στους επιτρεπόμενους χώρους. Ωστόσο, η τεχνολογία και η εξέλιξη της έχει κατά κύριο λόγο διττή επίδραση στους χρήστες, η οποία θα παρατεθεί στην συνέχεια. Τα ακόλουθα πλεονεκτήματα και μειονεκτήματα των βιομετρικών συστημάτων παρουσιάζονται συνοπτικά (Burger & Fustier, 2005).

Πλεονεκτήματα:

- Δεν απαιτούν την χρήση κάρτας, κωδικού πρόσβασης ή άλλης συσκευής από τον χρήστη.

- Δεν απαιτούν την απομνημόνευση κωδικών από τον χρήστη, αφού η αναγνώριση γίνεται με φυσικά χαρακτηριστικά και δεν απαιτείται η διαρκής ύπαρξη διαχειριστή για την ενημέρωση του συστήματος.
- Δεδομένου ότι αναφερόμαστε σε μοναδικά χαρακτηριστικά τα οποία δεν μεταβάλλονται με το πέρασμα του χρόνου, δεν απαιτείται η ανανέωση με εξαίρεση την αναγνώριση φωνής, την υπογραφή και την αναγνώριση πληκτρολόγησης.
- Χαμηλός χρόνος απόκρισης.
- Σύντομη διαδικασία καταχώρησης.

Μειονεκτήματα:

- Υψηλό ποσοστό απόρριψης, απαίτηση για εφαρμογή τεχνικών λήψης αντιγράφων ασφαλείας για την αυθεντικοποίηση με έμμεσο αποτέλεσμα την δυσαρέσκεια του χρήστη.
- Η κοινωνική αντίληψη ότι η λήψη δακτυλικού αποτυπώματος συνδέεται με την διάπραξη εγκληματικής ενέργειας.
- Η αντίληψη του συνόλου ότι η εκπεμπόμενη ακτινοβολία είναι βλαβερή.
- Η αντίληψη της παραβίασης της ιδιωτικότητας, αφού ο χρήστης εισαγάγει ένα δικό του χαρακτηριστικό στην βάση δεδομένων. Προκύπτουν ερωτήματα κατά πόσο είναι νόμιμο και ποιοι κίνδυνοι εγείρονται από την χρήση αυτή.
- Χαρακτηριστικό παράδειγμα ομοζυγωτικών διδύμων το 201, όπου ξεγέλασαν το Face ID.
- Υψηλό κόστος εφαρμογής βιομετρικών αναγνωστών

4.5 Επίγνωση Ζητημάτων Ιδιωτικότητας στην χρήση Βιομετρικών Συστημάτων

Τα βιομετρικά συστήματα εγείρουν σοβαρές ανησυχίες κατά κύριο λόγο στον τομέα της ιδιωτικής ζωής και της προστασίας δεδομένων, οι οποίες επηρεάζουν την κοινωνική αποδοχή τους και τροφοδοτούν τη συζήτηση περί ασφάλειας και νομιμότητας. Τα αποτελέσματα των ερευνών, ανά τα χρόνια, που θα παρατεθούν ομαδοποιημένα στη συνέχεια, σχετίζονται με την αποδοχή των

βιομετρικών συστημάτων από τους χρήστες, καθώς και με τους τρόπους που τα αντιλαμβάνονται. Τα βιομετρικά δεδομένα έχουν μεγάλη ισχύ, αλλά και αποτελούν ιδιαίτερη απειλή για την ιδιωτικότητα, διότι είναι άρρηκτα συνδεδεμένα με την ταυτότητα των κατόχων τους. Τα βιομετρικά χαρακτηριστικά αποτελούν μόνιμους ταυτοποιητές, σε αντίθεση με έναν κωδικό πρόσβασης ή μια έξυπνη κάρτα, ενώ οι εναλλακτικές επιλογές είναι περιορισμένες. Επομένως, η βιομετρική εξαπάτηση αποτελεί όχι μόνο κίνδυνο αλλά και πρόκληση, την οποία καλούνται τα βιομετρικά συστήματα να αντιμετωπίσουν, διότι τα βιομετρικά χαρακτηριστικά εκτίθενται δημοσίως. Για παράδειγμα, εύκολα μπορούν να ληφθούν εικόνες του προσώπου από κάμερες σε δημόσιους χώρους καθώς και δακτυλικά αποτυπώματα που μπορούν να συλλεγούν από κάθε σημείο, το οποίο ακουμπά το άτομο. Επομένως, μαζί με την ευκολία και το επίπεδο ασφάλειας που παρέχουν, συνυπάρχει μια ανησυχία για την ιδιωτικότητα. Για να λειτουργήσει αποτελεσματικά η βιομετρική τεχνολογία, πρέπει να υπάρχει μια βάση δεδομένων που να περιλαμβάνει τις σχετικές πληροφορίες για κάθε άτομο που έχει εξουσιοδοτηθεί από το σύστημα. Οι διαφορετικές προσεγγίσεις που συγκαταλέγονται στο ζήτημα της ιδιωτικότητας, ενισχύονται μέσα από έρευνες.

Οι έρευνες που θα παρατεθούν, κατά κάποιον τρόπο, διαφοροποιούνται ως προς:

1. <u>Χρήστες που τάσσονται υπέρ των βιομετρικών συστημάτων χωρίς δισταγμούς και τα συνδέουν με την ασφάλεια</u>

Συγκεκριμένα, η πρώτη κατηγορία ερευνών αφορά σε χρήστες που τάσσονται υπέρ της αντικατάστασης των κωδικών πρόσβασης με βιομετρικά χαρακτηριστικά.

Η έρευνα που έγινε τον Αύγουστο του 2015 (Technologies & Sentiments, 2016: 3) δείχνει ότι το 61% των χρηστών προτιμάει τα δακτυλικά αποτυπώματα, καθώς αισθάνονται κουρασμένοι από τη χρήση κωδικών, ειδικότερα σε σχέση με τις τράπεζες και την ασφάλεια των δεδομένων τους. Ένα χρόνο πριν, δηλαδή τον Νοέμβριο του 2014, έρευνα προς τους χρήστες κινητής τηλεφωνίας δείχνει ότι οι χρήστες προτιμούν την επαλήθευση δακτυλικών αποτυπωμάτων, η οποία έχει καίρια σημασία για την Apple και τη Samsung, οι οποίες έχουν αφοσιωθεί στην όσο ευκολότερη και χρηστικότερη δημιουργία του fingerprint(Cranor, 2015). Τα

αποτελέσματα της ίδιας έρευνας παρουσιάζουν ένα 10% των χρηστών να απέχει από τις τεχνικές βιομετρικής ευκολίας που έχουν τα κινητά τηλέφωνα, χωρίς να γίνονται φανεροί οι λόγοι. Επιπλέον, η πλειοψηφία των ερωτηθέντων από την Accenture (Doyle, 2014) σε έξι χώρες (ΗΠΑ, Ηνωμένο Βασίλειο, Γαλλία, Γερμανία, Ιαπωνία και Αυστραλία 89% δηλώνει ότι είναι διατεθειμένη να μοιραστεί τις βιομετρικές λεπτομέρειες - τα μοναδικά φυσικά χαρακτηριστικά, όπως δακτυλικά αποτυπώματα, και την αυτοματοποίηση της αναγνώρισης όταν ταξιδεύει στα διεθνή σύνορα. Ο διευθύνων σύμβουλος της Accenture Border and Identity Services, αναφέρει ότι «*οι άνθρωποι είναι ιδιαίτερα πρόθυμοι να μοιράζονται βιομετρικά στοιχεία όταν πρόκειται για τη βελτίωση της ασφάλειας*».(Doyle,2014). Χρειάζεται να σημειωθεί πως καθοριστικό ρόλο στην άνεση των χρηστών να ταυτοποιούνται με βάση τα βιομετρικά τους χαρακτηριστικά, είχε η ένταξη του δακτυλικού αποτυπώματος στο Iphone 5, καθώς οι χρήστες εξοικειώθηκαν με αυτό. Οι ερωτηθέντες των ΗΠΑ είναι πολύ δεκτικοί στη χρήση βιομετρικών στοιχείων ως μέσο βελτίωσης της συνολικής ασφάλειας των συνόρων : το 65% αναφέρει ότι θα μοιραζόταν βιομετρικά στοιχεία εάν αυτό σήμαινε μεγαλύτερη ασφάλεια των συνόρων της χώρας. Περισσότεροι από τους μισούς (61%) δηλώνουν ότι είναι πιθανό να μοιραστούν τα βιομετρικά στοιχεία τους για να εξασφαλίσουν ταχύτερη επεξεργασία μέσω των τελωνείων και του ελέγχου των συνόρων και το 59% θα είναι πρόθυμο να επιτύχει πιο βολικό ταξίδι. Σχεδόν το ένα τέταρτο των ερωτηθέντων από τη Γερμανία (23%) λένε ότι έχουν μοιραστεί βιομετρικά στοιχεία με τρίτους, το υψηλότερο ποσοστό ερωτηθέντων και στις 6 χώρες που συμμετείχαν στην έρευνα. Αντίθετα, μόνο το 17% των ερωτηθέντων της Ιαπωνίας και του Ηνωμένου Βασιλείου αναφέρουν ότι έχουν μοιραστεί βιομετρικές πληροφορίες στο παρελθόν. Ένα χρόνο αργότερα και συγκεκριμένα τον Μάρτιο του 2016, έρευνα που διεξάχθηκε στις ΗΠΑ (Santa, 2016), αναφέρει ότι ποσοστό γύρω στο 62% αισθάνεται άνετα να χρησιμοποιεί βιομετρικές τεχνολογίες. Η έρευνα απευθύνεται σε ενήλικες καταναλωτές και χωρίζεται σε τρεις ενότητες, την υιοθέτηση των βιομετρικών από τους καταναλωτές, τα επίπεδα άνεσης τω καταναλωτών και τα επίπεδα εμπιστοσύνης. Διαπιστώνεται επίσης ότι σχεδόν τα 2/3 όλων των καταναλωτών υποστηρίζουν τις βιομετρικές τεχνολογίες για

αλτρουιστικούς σκοπούς στην ιατρική έρευνα 58% και στην υποστηρικτική τεχνολογία 67%. Βέβαια, σύμφωνα με τα αποτελέσματα της έρευνας, οι χρήστες έχουν περισσότερη εμπιστοσύνη στις υπηρεσίες με σημαντικές λειτουργίες όπως τα νοσοκομεία και οι τράπεζες με ποσοστό 64%. Επιπλέον, έχει παρατηρηθεί από τους χρήστες μια ανησυχία όσον αφορά στις τραπεζικές τους συναλλαγές, πιστεύοντας πως η ισχύουσα κατάσταση εντείνει τη πιθανότητα της κλοπής και απαιτείται περισσότερη ασφάλεια. Οι λόγοι αυτής της εύκολης αποδοχής έγκεινται στον φόβο πιθανής κλοπής της ταυτότητας και στις αντιλήψεις περί ασφάλειας. Συγκεκριμένα μεταξύ 23-25 Σεπτεμβρίου του 2015 σε μια πόλη της Αγγλίας, στο Nottingham, έλαβε χώρα η συγκεκριμένη έρευνα από την Opinium Research με αντιπροσωπευτικό δείγμα 2002 άτομα σε εθνικό επίπεδο. Από την έρευνα, διαπιστώθηκε ότι οι περισσότεροι ενήλικες είναι πλέον πρόθυμοι να αγκαλιάσουν τη βιομετρική ταυτότητα στις τράπεζες (Keough, 2016). Αυτό που αξίζει να σημειωθεί στην συγκεκριμένη έρευνα και είναι αναπάντεχο, είναι πως οι ηλικιακές ομάδες άνω των 55 χρονών προτιμούν και εμπιστεύονται κατά 22% την σάρωση της ίριδας από τους νεότερους χρήστες ηλικίας 18-34, με ποσοστό 14%. Όταν πρόκειται για τη διαχείριση ηλεκτρονικών λογαριασμών, τρεις στους πέντε ανθρώπους, δηλαδή το 61%, πιστεύουν ότι η βιομετρική αναγνώριση είναι εξίσου ασφαλής ή πιο ασφαλής από το σημερινό σύστημα κωδικών πρόσβασης. Επομένως, οι ενήλικες του Ηνωμένου Βασιλείου είναι πιο άνετοι να χρησιμοποιούν τη βιομετρική τεχνολογία για να έχουν πρόσβαση στην ηλεκτρονική τράπεζα τους απ' ότι στους λογαριασμούς των κοινωνικών μέσων - διπλάσια, 64% σε σύγκριση με 32%. Όσο λιγότερα είναι τα επίπεδα ασφάλειας, τόσο πιο ευάλωτα είναι όσον αφορά στην κλοπή αυτών των συστημάτων. Φυσικά πρέπει να υπάρχει ισορροπία μεταξύ της πρόληψης των κινδύνων και της εμπειρίας του ατόμου που προσπαθεί να συνδεθεί.
Δεν αποτελεί έκπληξη το γεγονός ότι η σάρωση δακτυλικών αποτυπωμάτων είναι η βιομετρική αναγνώριση που οι περισσότεροι ενήλικες από το Ηνωμένο Βασίλειο αισθάνονται άνετα. Δύο πέμπτα (40%) δηλώνουν ότι θα είναι ευχαριστημένοι με τη χρήση σάρωσης δακτυλικών αποτυπωμάτων για την πρόσβαση σε ηλεκτρονικούς λογαριασμούς. Παρόλο που φαίνεται ότι υπάρχουν κάποιες

επιφυλάξεις σχετικά με τη σάρωση του αμφιβληστροειδούς, σχεδόν ένας στους πέντε (19%) θα εξακολουθεί να είναι άνετος έχοντας επαληθεύσει την ταυτότητά του με αυτόν τον τρόπο. Ομοίως, σχεδόν ένας στους δέκα ανθρώπους (9%) θα ήταν άνετος με την αναγνώριση προσώπου της κάμερας ως μια μορφή αναγνώρισης, ενώ ένας στους είκοσι (5%) δηλώνει ότι θα ήταν ευχαριστημένος χρησιμοποιώντας την τεχνολογία αναγνώρισης φωνής για να ξεκλειδώσουν τους λογαριασμούς τους στο διαδίκτυο. Την ίδια χρονολογική περίοδο στο Ηνωμένο Βασίλειο, έρευνα που διεξάγεται προς τους πελάτες της MasterCard, παρουσιάζει πως το 53% των χρηστών της ξεχνούν τους κωδικούς πρόσβασης τους τουλάχιστον μια φορά την εβδομάδα, με αποτέλεσμα να χάνουν περισσότερο από 10 λεπτά για την επαναφορά τους στους λογαριασμούς τους (Graham, 2016). Με έναυσμα αυτή την έρευνα, η εταιρία δηλώνει πως οι πελάτες της θα μπορούν να αντικαταστήσουν τους κωδικούς πρόσβασης τους με «selfie» ή με το δακτυλικό τους αποτύπωμα, προκειμένου η διαδικασία της ταυτοποίησης να γίνεται πιο γρήγορα και με περισσότερη ασφάλεια αλλά ταυτόχρονα οι online αγορές θα αυξηθούν καθώς αυτός ο τρόπος είναι πιο βολικός. Η επικεφαλής των διεθνών αγορών της MasterCard, Ann Cairns, δήλωσε πως οι βιομετρικοί έλεγχοι δοκιμάστηκαν στις ΗΠΑ και τις Κάτω Χώρες και σύντομα θα ξεκινήσουν και στο Ηνωμένο Βασίλειο. Αντιστοίχως, η τραπεζική εταιρία Citi Group, το 2016 ξεκίνησε στις Η.Π.Α ένα πρόγραμμα πιστοποίησης μέσω της φωνής, όπου επιτρέπει στους πελάτες της να χρησιμοποιούν τη φωνή τους για να επαληθεύσουν τον εαυτό τους όταν καλούν την τράπεζα. Όπως αναφέρει και ο επικεφαλής της Ash Khan : «*Θέλουμε να προσφέρουμε στους πελάτες μας επιλογές όσον αφορά τον έλεγχο ταυτότητας και πάντα εξετάζουμε καινοτόμους και ασφαλείς τρόπους για να το κάνουμε αυτό*» (Yurcan, 2016). Το ίδιο άρθρο αναφέρει πως η Citi Group συνεργάζεται με την NICE Systems για την τεχνολογία, η οποία μπορεί να αναγνωρίσει περίπου 130 διαφορετικά φυσικά και συμπεριφορικά χαρακτηριστικά στο φωνητικό πρότυπο ενός ατόμου. Όταν οι πελάτες για παράδειγμα, καλούν, οι φωνές τους ταιριάζουν με τα προκαταχωρημένα δεδομένα τους. Με βάση αυτό, αναφέρει πάλι ο Khan «*Η εγκατάσταση της φωνητικής αποτύπωσης διαρκεί λιγότερο από ένα λεπτό. Αρχίζω να μιλάω στον εκπρόσωπο, ζητούν τον αριθμό της κάρτας μου και αυτό είναι. Στη*

συνέχεια, αρχίζουν να μου μιλούν για το λογαριασμό μου, μου απευθύνονται με το όνομα μου και είναι μια εντελώς διαφορετική εμπειρία» (Yurcan ,2016). Εκτός από την αναγνώριση φωνής, η Citi Group εξετάζει και άλλες βιομετρικές τεχνολογίες, συμπεριλαμβανομένης της συνεργασίας με την Diebold για τα ATMs, για την ανίχνευση ίριδας. Αξίζει να σημειωθεί πως η Citi Group δεν είναι μοναδική στην εστίασή της σε αυτή την τεχνολογία. Η Ανατολική Τράπεζα ξεκίνησε νωρίτερα φέτος μια παρόμοια πρωτοβουλία ελέγχου ταυτότητας φωνής, ενώ η USAA επιτρέπει στους πελάτες της να παίρνουν "selfies" για να συνδεθούν με την κινητή τραπεζική. Με τους ίδιους ρυθμούς κινείται και η HSBC στο Ηνωμένο Βασίλειο όπου έθεσε σε λειτουργία το Voice ID για μεγαλύτερη ασφάλεια. Σύμφωνα με την εταιρία, η τεχνολογία αυτή θα προσφέρει ανώτερη και ασφαλέστερη τραπεζική εμπειρία, καθώς μέσω αυτής της βιομετρικής τεχνολογίας, θα δίνεται στον χρήστη η δυνατότητα για γρηγορότερη πρόσβαση στον λογαριασμό του (Sherman, 2016). Επομένως, *«όπως ένα δακτυλικό αποτύπωμα, η φωνή μας είναι μοναδική. Η τεχνολογία βιομετρικών στοιχείων πίσω από το Voice ID επικεντρώνεται στο πώς μιλάμε, όχι σε αυτό που λέμε. Δεν έχει σημασία ποια γλώσσα ο πελάτης μιλάει, αν έχει κρύο ή πονόλαιμο, το Voice ID θα μπορεί να επιβεβαιώσει την ταυτότητά του. Η ανάμνηση του σωστού κωδικού πρόσβασης και του PIN είναι προκλητική και οι πελάτες απογοητεύονται όταν αποτυγχάνουν στη διαδικασία ταυτοποίησης και πρέπει να επαναφέρουν τα στοιχεία τους. Έχοντας έναν μικρότερο αριθμό τηλεφωνικής ασφάλειας ή PIN που θα θυμάστε, θα επιταχύνει τη διαδικασία επαλήθευσης και θα δώσει στον πελάτη περισσότερο χρόνο για να μιλήσει για τις οικονομικές ανάγκες του»* (Sherman, 2016).

Από την παρούσα έρευνα προκύπτει πως οι χρήστες αισθάνονται άνετα με τις βιομετρικές τεχνολογίες και με το γεγονός ότι χρησιμοποιούνται σε χώρους που θεωρούνται ιδιαίτερα ασφαλείς όπως αεροδρόμια, τραπεζικές συναλλαγές, διαδικτυακές αγορές ή χρειάζονται μεγαλύτερη προστασία (Ponemon Institute, 2013). Το δείγμα της συγκεκριμένης έρευνας είναι 1.924 καταναλωτές ηλικίας από 18 έως 65 ετών στις Ηνωμένες Πολιτείες, το Ηνωμένο Βασίλειο και τη Γερμανία, όπου όλοι οι ερωτηθέντες ανέφεραν ότι ξοδεύουν τουλάχιστον 10 ώρες κάθε εβδομάδα χρησιμοποιώντας το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης και

ασχολούνται με δραστηριότητες όπως διαδικτυακές αγορές, διαδικτυακές τραπεζικές συναλλαγές, blogging και απόκτηση κρατικών υπηρεσιών. Όμως, αυτό που καταδεικνύει η έρευνα και στο οποίο θα αναφερθούμε και στην συνέχεια, είναι ότι η βιομηχανία πρέπει να κάνει περισσότερα για να εκπαιδεύσει τους χρήστες σχετικά με τα οφέλη της βιομετρίας και των χρήσεων της. Το 1/3 των καταναλωτών είναι ουδέτερο στην χρήση αυτών των τεχνολογιών εξαιτίας της έλλειψης κατανόησης σχετικά με την εμπειρία των χρηστών και των υπαλλήλων στις υπηρεσίες και την ασφάλεια των δεδομένων.

Παρόμοια έρευνα σχετικά με την κλοπή στο εργασιακό περιβάλλον, πραγματοποιήθηκε μεταξύ 27 Ιανουαρίου και 16 Φεβρουαρίου 2015, μεταξύ ενός δείγματος 461 άτομα στις ΗΠΑ με ενήλικες ηλικίας 18 ετών και άνω (Lee, 2016). Το Pew Research Center διαπίστωσε ότι πάνω από το ήμισυ (54%) των ερωτηθέντων σκέφτηκε ότι η χρήση φωτογραφικών μηχανών αναγνώρισης προσώπου είναι αποδεκτή στο χώρο εργασίας για να πιάσει τους κλέφτες των προσωπικών αντικειμένων των εργαζομένων, ενώ το 1/5 (21%) των ενηλίκων λέει ότι η εκτίμησή τους θα εξαρτηθεί από τις περιστάσεις. Οι απόψεις των εργαζόμενων διίστανται καθώς θεωρούν πως ο κύριος λόγος της τοποθέτησης των καμερών δεν είναι ο εντοπισμός του κλέφτη, αλλά η παρακολούθηση των εργαζόμενων κατά τη διάρκεια της δουλειάς τους και οι επιδόσεις τους.

2. <u>Χρήστες που αισθάνονται ότι καταπατάται η ιδιωτικότητα τους και θεωρούν πως τα βιομετρικά συστήματα δεν είναι τόσο ασφαλή όσο φαίνονται ή όσο τα προωθούν</u>

Στην δεύτερη κατηγορία ερευνών, το κοινό εκφράζει τους φόβους και τις ανησυχίες του σχετικά με την ιδιωτικότητα του και το κατά πόσο ασφαλή μπορούν να θεωρηθούν αυτές οι τεχνικές. Μια έρευνα που διεξήχθη στην Γαλλία με αντιπροσωπευτικό δείγμα 100 άτομα, στο Université de Caen Basse-Normandie, είχε θέμα την «Evaluation of biometric systems: a study of users' acceptance and satisfaction» (El-abed, Giot, Hemery & Rosenberger, 2014) δηλαδή πρόκειται για μια αξιολόγηση των βιομετρικών συστημάτων με βάση το κατά πόσο οι χρήστες τα αποδέχονται και είναι ευχαριστημένοι απ' αυτά. Τα αποτελέσματα της έρευνας αναφέρουν ότι υπάρχει δυνητική ανησυχία για την κατάχρηση δεδομένων

προσωπικού χαρακτήρα, τα οποία θεωρούνται ότι παραβιάζουν το απόρρητο των χρηστών και τις πολιτικές ελευθερίες. Μια άλλη σημαντική ανησυχία είναι η πιθανότητα οι εγκληματίες να διαπράξουν σφοδρές πράξεις για να αποκτήσουν πρόσβαση(π.χ. κόψιμο των δαχτύλων). Επιπλέον, έχουν διαπιστωθεί φόβοι σχετικά με την υγιεινή που αγγίζει τέτοιες συσκευές και τους κινδύνους για την υγεία για πιο προηγμένες τεχνολογίες όπως η ίριδα ή ο αμφιβληστροειδής. Όμως, μέχρι στιγμής δεν έχει παρατηρηθεί κάποια σωματική βλάβη στους χρήστες αυτών των συστημάτων. Υπάρχει ένα ποσοστό ανθρώπων όπου παραπονιούνται ότι αν το βιομετρικό πρότυπο κλαπεί, τίθεται σε κίνδυνο για πάντα (El-abed, Giot, Hemery & Rosenberger, 2014). Επιπλέον, στην έρευνα των El-abed,Giot,Hemery&Rosenberger (2014), επισημάνθηκε από τους χρήστες πως τα βιομετρικά στοιχεία δεν είναι μυστικά όπως ένας κωδικός πρόσβασης ή ιδιωτικό κλειδί κρυπτογράφησης. Τα βιομετρικά στοιχεία «αφήνονται» παντού (π.χ. δακτυλικά αποτυπώματα ή πρόσωπο) ή μπορούν να ληφθούν από οποιονδήποτε. Δεν υπάρχει άλλος τύπος ταυτοποίησης που είναι τόσο εύκολα ορατός και προσβάσιμος. Το μεγαλύτερο πρόβλημα με έναν μη κρυφό παράγοντα επαλήθευσης είναι ότι είναι εύκολο να αντιγραφούν για κακόβουλη επαναχρησιμοποίηση. Τα δακτυλικά αποτυπώματα και το πρόσωπό σας είναι κυριολεκτικά παντού και μπορούν εύκολα να ληφθούν, να αντιγραφούν και να επαναχρησιμοποιηθούν. Αφού έχουν συλληφθεί από κάποιον άλλο, πώς μπορεί κάποιο σύστημα που βασίζεται σε αυτά τα βιομετρικά χαρακτηριστικά να έχει εμπιστοσύνη ότι είστε εσείς που λέτε ότι είστε (Muir & Keough, 2016). Σε μια πιο πρόσφατη έρευνα που έγινε στην Αμερική το 2018, το 43% των ερωτηθέντων επέλεξε πως τα βιομετρικά δεδομένα εισβάλλουν στην ιδιωτική τους ζωή, ενώ το 24% δήλωσε ότι από την κυβέρνηση. Η αποθήκευση των βιομετρικών μας σε βάσεις δεδομένων εξυπηρετεί κυβερνητικές και εταιρικές σκοπιμότητες Σχεδόν το 20% ανησυχούσε για κλοπή ταυτότητάς τους αλλά μόνο το 4% ανησυχούσε περισσότερο για το στοχευμένο μάρκετινγκ από τους διαφημιζόμενους.

3. Χρήστες που εντοπίζουν προβλήματα ως προς την χρηστικότητα τους και θεωρούν πως απαιτείται η κατάλληλη εκπαίδευση

Η τρίτη και τελευταία κατηγορία αναφέρεται σε ανησυχίες χρηστικότητας των βιομετρικών συστημάτων. Ειδικότερα, η ακρίβεια πολλών βιομετρικών συστημάτων εξακολουθεί να μην είναι αρκετά υψηλή για κάποιες εφαρμογές δηλαδή αρνητική ταυτοποίηση ή αντιστοίχιση με μια πολύ μεγάλη βάση δεδομένων (Levine , Reiter, Wang & Wright, 2004). Χαρακτηριστικό παράδειγμα αποτελεί ότι οι χρήστες με ειδικά φυσικά χαρακτηριστικά, όπως τα ξεθωριασμένα δακτυλικά αποτυπώματα, οδηγώντας σε υψηλά ποσοστά «μη εγγραφής» και κατ' επέκταση σε συνεχιζόμενα προβλήματα των βιομετρικών συσκευών. Σε μια δοκιμή πεδίου των συσκευών ανάγνωσης δακτυλικών αποτυπωμάτων ραδιοσυχνοτήτων στις τραπεζικές μηχανές ATM, σημειώθηκε ποσοστό αποτυχίας εγγραφής 13%, κυρίως λόγω των φτωχών εικόνων δακτυλικών αποτυπωμάτων από ηλικιωμένες γυναίκες. Επίσης, επειδή παρατηρήθηκε κάποιο ποσοστό αποτυχίας στην προσπάθεια των χρηστών να τοποθετήσουν σωστά τα δάχτυλά τους στους αισθητήρες, πλέον οι καλύτεροι αναγνώστες τείνουν να έχουν κανάλια ή οδηγούς για να βοηθήσουν την σωστή τοποθέτηση των δαχτύλων (Chau, Stephens & Jamieson, 2004). Παρόμοια περιστατικά έχουν παρατηρηθεί και με τους σαρωτές Iris, σχετικά με την ευθυγράμμιση του οφθαλμού στο φακό της κάμερας. Έτσι, θεωρείται πλέον αναγκαία η εκπαίδευση των χρηστών ώστε να αντιληφθούν με διαφορετικό τρόπο τα βιομετρικά συστήματα και την χρήση τους. Όσον αφορά στην αποδοχή των βιομετρικών συστημάτων ασφαλείας, οι παράγοντες που καθιστούν τα συστήματα περισσότερο αποδεκτά περιλαμβάνουν το τεχνικό ενδιαφέρον, τις ανησυχίες για κλοπή ταυτότητας, κυβερνητικές πρωτοβουλίες ελέγχου των συνόρων, διασφάλιση βασικών υποδομών και την ευκαιρία να μειωθούν οι απαιτήσεις μνήμης αντικαθιστώντας αποθηκευμένους κωδικούς πρόσβασης (Levine , Reiter, Wang & Wright, 2004). Ωστόσο, η έρευνα έχει δείξει ότι παρόλο που η αποδοχή αυξάνεται, οι χρήστες παραμένουν επιφυλακτικοί επειδή τα οφέλη δεν είναι πάντα εμφανή. Όπως αναφέρθηκε και προηγουμένως, ένα από τα φλέγοντα ζητήματα που απασχολεί τους χρήστες είναι η ιδιωτικότητα, καθώς από την

στιγμή που η βιομετρική τεχνολογία είναι ευρέως διαδεδομένη στην καθημερινή ζωή και όλες οι δραστηριότητές των χρηστών αποθηκεύονται στη βάση δεδομένων, τότε δεν τίθεται θέμα περί ιδιωτικού απορρήτου. Οι προσωπικές πληροφορίες που λαμβάνονται με βιομετρική συσκευή μπορούν να χρησιμοποιηθούν κατά παράβαση. Η χρήση βιομετρικού ελέγχου ταυτότητας πρέπει να είναι επιλογή για τον χρήστη και όχι υποχρέωση (Chau, Stephens & Jamieson, 2004).

5. Η ταυτότητα της Έρευνας

5.1 Μέθοδος

Για την πραγματοποίηση της έρευνας, η μέθοδος συλλογής υλικού που χρησιμοποιήθηκαν είναι οι ποσοτικές μέθοδοι, αξιοποιώντας ως εργαλείο το ερωτηματολόγιο. Η χρήση ποσοτικών μεθόδων κρίθηκε καταλληλότερη, γιατί πρόκειται για μια έρευνα που απαιτεί μετρήσεις σε ένα μεγάλο αριθμό πληθυσμού, σε αντίθεση με την ποιοτική προσέγγιση που στοχεύει στην διερεύνηση και κατανόηση σε βάθος των κοινωνικών φαινομένων (Χαλικιάς,Λάλου & Μανωλέσου, 2015). Στην ποσοτική έρευνα ο στόχος είναι η γενίκευση, δηλαδή η περιγραφή μιας ή περισσοτέρων μεταβλητών του πληθυσμού, καθώς και την εξήγηση των σχέσεων μεταξύ μεταβλητών του πληθυσμού. Συνεπώς χρειάζεται να συγκεντρωθούν και να αναλυθούν πληροφορίες για τις διάφορες μεταβλητές του πληθυσμού. Οι ποσοτικές μέθοδοι που βασίζονται σε δειγματοληπτική έρευνα με ερωτηματολόγιο, προσφέρουν τη δυνατότητα στον ερευνητή να προσεγγίσει μεγάλο μέρος του πληθυσμού για τον έλεγχο των συγκεκριμένων υποθέσεων ή ερωτημάτων. Το αντιπροσωπευτικό δείγμα είναι απαραίτητο για να μπορέσει να οδηγηθεί σε έγκυρα αποτελέσματα και επιτρέπει στον ερευνητή να γενικεύσει τα συμπεράσματα του με περισσότερη ακρίβεια. Με τα ερωτηματολόγια συλλέγονται δεδομένα ζητώντας από ανθρώπους να απαντήσουν στο ίδιο ακριβώς σύνολο ερωτήσεων(Iseris,2016). Αξίζει να σημειωθεί πως, απευθύνεται ομοιόμορφα στα υποκείμενα της έρευνας για την συλλογή ερευνητικών πληροφοριών που σχετίζονται με την άποψη και

αντίληψη τους στο θέμα που τίθεται. Αυτός είναι και ο σκοπός της διεξαγωγής του.

5.2 Εργαλείο της έρευνας

Για τη συγκεκριμένη έρευνα χρησιμοποιήθηκε η τεχνική του ερωτηματολογίου . Πρόκειται για ένα μέσο καταγραφής που περιλαμβάνει μια σειρά δομημένων ερωτήσεων, στις οποίες ο ερωτώμενος καλείται να απαντήσει γραπτά και με μια συγκεκριμένη σειρά. Επιλέχθηκε επομένως το ερωτηματολόγιο, διότι συγκριτικά με άλλες μεθόδους συλλογής πληροφοριών, αφενός είναι σχετικά πιο εύκολο στην ανάλυση του, αφετέρου είναι εύκολο και γρήγορο στην συμπλήρωση του, ενώ οι συμμετέχοντες έχουν τον απαραίτητο χρόνο να επεξεργαστούν και να απαντήσουν στις ερωτήσεις (Menexes, 2008). Για τη συγκεκριμένη έρευνα κατασκευάστηκε καινούριο ερωτηματολόγιο, το οποίο βασίστηκε σε προηγούμενες έρευνες. Απώτερος σκοπός είναι μέσα από την συμπλήρωση του να εξετάσουμε τους παράγοντες αποδοχής, υιοθέτησης και χρήσης των Βιομετρικών Συστημάτων από τους χρήστες και συγκεκριμένα εξετάζεται η περίπτωση των φοιτητών του Πανεπιστημίου Αιγαίου. Στην αρχή του ερωτηματολογίου θεωρήθηκε σημαντικό να προστεθεί ένα εισαγωγικό σημείωμα γιατί με βάση πιλοτική προκαταρκτική έρευνα, πριν την δημιουργία του ερωτηματολογίου, διαπιστώθηκε πως αρκετοί φοιτητές/φοιτήτριες δεν γνώριζαν τι ονομάζουμε βιομετρικά συστήματα. Επομένως κρίθηκε σκόπιμο να τεθεί ως ερώτημα στην αρχή του ερωτηματολογίου, ώστε να διερευνηθεί το ποσοστό αυτών που τα γνωρίζουν και αυτών που δεν τα γνωρίζουν.

Το ερωτηματολόγιο αυτό είχε την κατάλληλη δομή, τον κατάλληλο σχεδιασμό και ερωτήσεις που θα έφερναν σε πέρας τους στόχους της έρευνας και την συλλογή των κατάλληλων πληροφοριών. Σχετικά με τις ερωτήσεις, αυτές που αναφέρονται στο ίδιο θέμα είναι συγκεντρωμένες σε διακριτές ενότητες, ώστε το ερωτηματολόγιο να έχει συνάφεια και λογική ροή. Έτσι λοιπόν, το ερωτηματολόγιο είναι χωρισμένο σε 8 ενότητες. Συνολικά, πρόκειται για 38 ερωτήσεις, δύο ειδών: είτε ανοιχτού τύπου, είτε κλειστού τύπου, όπου ο

ερωτώμενος έχει να επιλέξει μεταξύ συγκεκριμένων απαντήσεων. Οι υποκατηγορίες των κλειστών ερωτήσεων είναι οι ακόλουθες:

- Διχοτομικές Ερωτήσεις , όπου επιτρέπουν στον ερωτώμενο να επιλέξει μόνο τη μια από τις δύο απαντήσεις [Ναι/ Όχι]
- Ερωτήσεις Βαθμονόμησης , όπου μπορεί να απαντήσει σε μια από τις υπάρχουσες κατηγορίες [Καθόλου-Πάρα πολύ]
- Ερωτήσεις Διαβαθμισμένης Κλίμακας [από το 1 έως το 5]
- Πολλαπλής επιλογής, μπορεί να διαλέξει περισσότερες από μια

Το ερωτηματολόγιο ελέγχθηκε ως προς τη μορφή του, τη γλώσσα του, τη σαφήνεια του, τη δυσκολία και την αξιοπιστία του σε μια πιλοτική έρευνα που προηγήθηκε της κύριας δειγματοληψίας.

5.3 Η διαδικασία συλλογής δεδομένων

Στη προκειμένη περίπτωση, ο τρόπος συλλογής των δεδομένων έγινε ηλεκτρονικά.

Το ερωτηματολόγιο δόθηκε σε φοιτητές και φοιτήτριες του Πανεπιστημίου Αιγαίου σε όλα τα τμήματα του, σε προπτυχιακούς, μεταπτυχιακούς και διδακτορικούς.

Τα δεδομένα συλλέχθηκαν σε διάστημα ενός (1) μήνα περίπου με ερωτηματολόγιο που δημιουργήθηκε μέσω δωρεάν ηλεκτρονικής πλατφόρμας «Google Forms». Η συγκεκριμένη πλατφόρμα επιτρέπει γρήγορη και εύκολη δημιουργία ερωτηματολογίων, καθώς και άμεση διανομή τους μέσω ηλεκτρονικού ταχυδρομείου. Η διανομή του ανώνυμου ερωτηματολογίου έγινε είτε σε εργαστήρια μαθημάτων είτε μέσω του ακαδημαϊκού ταχυδρομείου και συλλέχθηκαν 768 ερωτηματολόγια πλήρως συμπληρωμένα από τους συμμετέχοντες.

5.4 Ανάλυση δεδομένων

Με την συλλογή των συμπληρωμένων ερωτηματολογίων, τα δεδομένα που συλλέχθηκαν εξήχθησαν και αποθηκεύτηκαν σε βιβλίο εργασίας του Microsoft

Excel. Η στατιστική επεξεργασία έγινε με χρήση του πακέτου λογισμικού στατιστικής IBM SPSS.

5.5 Αξιοπιστία και εγκυρότητα

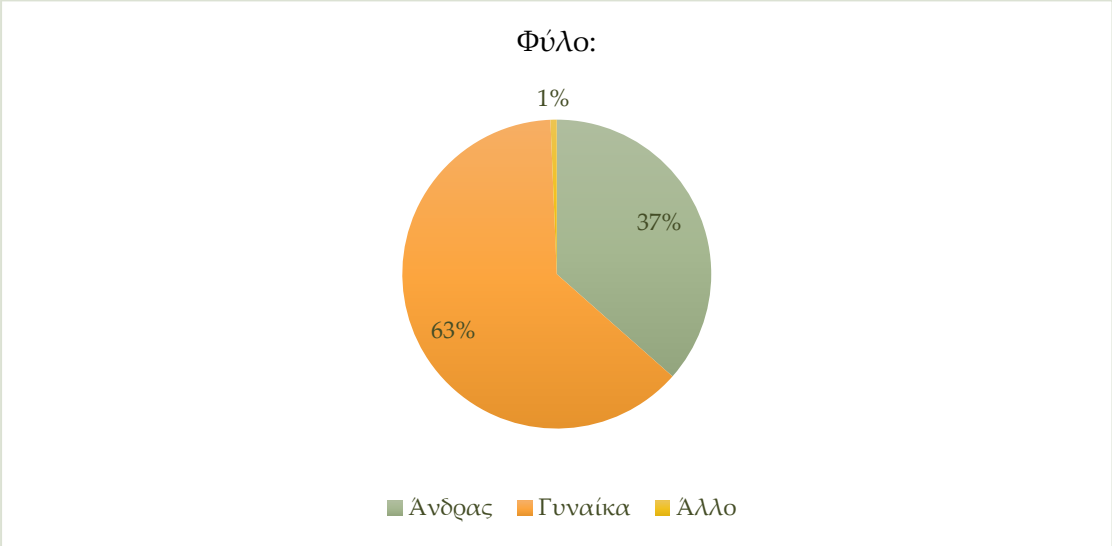
Το ερωτηματολόγιο συμπληρώθηκε αρχικά από ένα δείγμα 150 φοιτητών, όπου τα δεδομένα αναλύθηκαν στατιστικά από το στατιστικό πρόγραμμα IBM SPSS Statistics Data Editor με τους ελέγχους αξιοπιστίας και εγκυρότητας σε σχέση με το υπό εξέταση πρόβλημα. Όσον αφορά την εγκυρότητα όλων των διχοτομικών ερωτήσεων, εφαρμόστηκε ο δείκτης Kuder-Richardson Reliability Coefficients KR20 για τον υπολογισμό της αξιοπιστίας με μοναδική διαφορά τη μη χρήση συσχετίσεων μεταξύ των ερωτημάτων διχοτομικού τύπου ενός ερωτηματολογίου. Ο δείκτης αξιοπιστίας εσωτερικής συνέπειας προκύπτει είτε από τον τύπο KR-20, όταν τα ερωτήματα επιδέχονται μόνο δύο απαντήσεις, τα στοιχεία δηλαδή που αναλύονται είναι διωνυμικού τύπου, είτε μέσω του τύπου Cronbach A, όταν το A είναι ο δείκτης αξιοπιστίας, όταν τα ερωτήματα μιας κλίμακας επιδέχονται βαθμολόγηση με περισσότερες από δύο βαθμίδες (Iseris, 2016).

5.6 Αποτελέσματα

Στην έρευνα συμμετείχαν 279 άνδρες φοιτητές, 480 γυναίκες και 6 άτομα που δήλωσαν άλλο φύλο από το σύνολο των 16.000 φοιτητών-τριων του Πανεπιστημίου Αιγαίου. Τα αποτελέσματα παρουσιάζονται μέσα από τα ακόλουθα γραφήματα, τα οποία προέκυψαν από την ανάλυση των απαντήσεων των φοιτητών-τριών και συσχετίσθηκαν με τα δημογραφικά στοιχεία τους. Για τη διερεύνηση των τυχόν συσχετίσεων συλλέχτηκαν τα ακόλουθα δημογραφικά στοιχεία, τα οποία θα παρατεθούν σε γραφήματα και είναι: φύλο, ηλικιακή ομάδα, επίπεδο και έτος σπουδών, τμήμα φοίτησης, εργασία φοιτητή και κατηγοριοποίηση τους επαγγέλματος του, το επάγγελμα του πατέρα και της μητέρας και το ετήσιο εισόδημα. Συγκεκριμένα, όπως διαφαίνεται από το

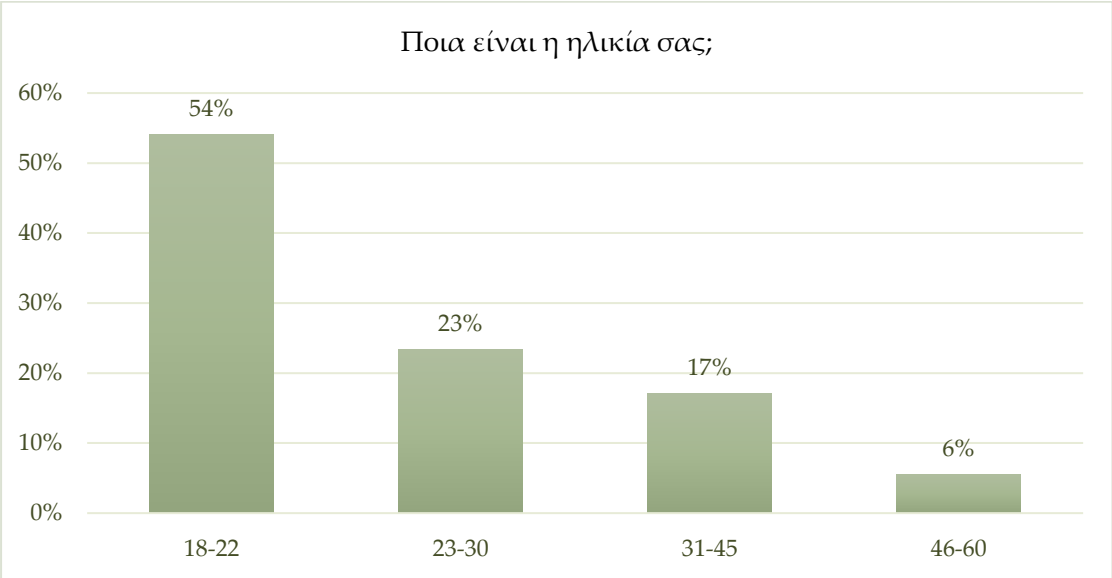
γράφημα το μεγαλύτερο ποσοστό είναι αυτό των γυναικών, το οποίο ανέρχεται στο 63%, το 37% είναι άνδρες, ενώ το 1% δηλώνει άλλο φύλο.

Γράφημα 1. Δημογραφικά Στοιχεία-Φύλο



Στο ακόλουθο γράφημα αποτυπώνεται ποσοστιαία το σύνολο των συμμετεχόντων-ουσών φοιτητών-τριών ανά ηλικιακή ομάδα. Όπως διαφαίνεται από το γράφημα 2, το μεγαλύτερο ποσοστό ανήκει στην ηλικιακή ομάδα 18-22, το οποίο ανέρχεται στο 54%, το 23% ανήκει στην ομάδα 23-30, ενώ το 17% στην ομάδα 31-45 και το 6% στην ομάδα 46-60.

Γράφημα 2. Δημογραφικά Στοιχεία-Ηλικιακή Ομάδα



Το ακόλουθο γράφημα απεικονίζει ποσοστιαία το επίπεδο σπουδών των φοιτητών-τριών, το οποίο χωρίζεται στους προπτυχιακούς, τους μεταπτυχιακούς και τους διδακτορικούς φοιτητές. Από τα ποσοστά προκύπτει πως το μεγαλύτερο ποσοστό ανήκει στους προπτυχιακούς φοιτητές, το οποίο ανέρχεται στο 68%, το 24% σε μεταπτυχιακούς ενώ το 9% σε διδακτορικούς φοιτητές.

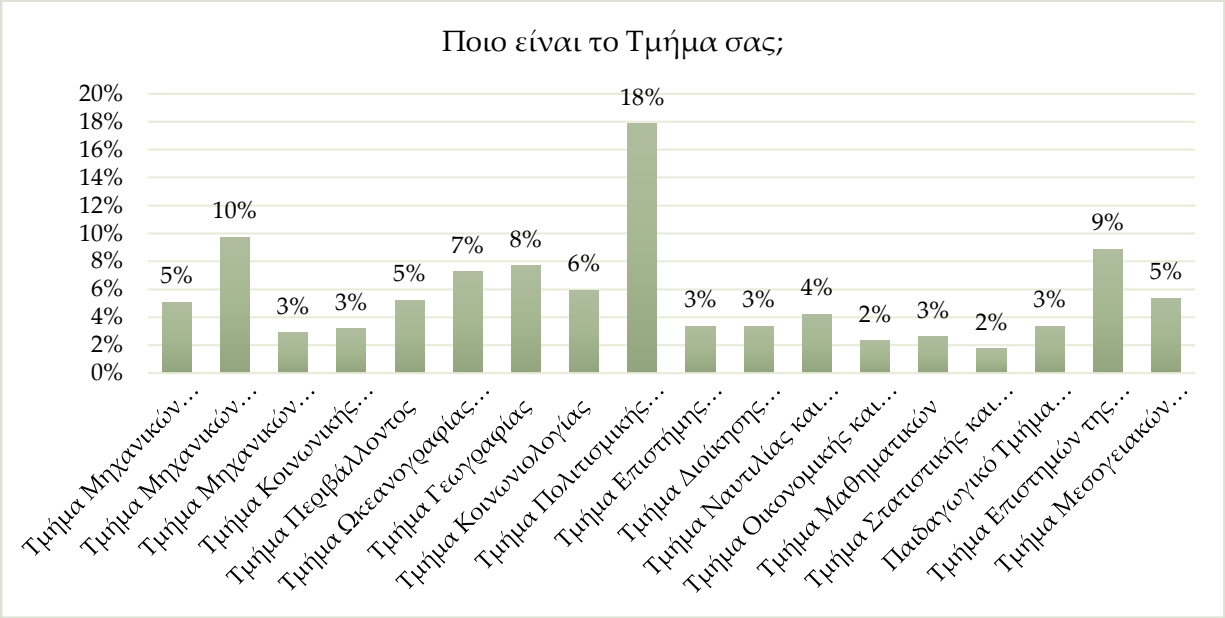
Γράφημα 3. Δημογραφικά Στοιχεία-Επίπεδο Σπουδών

Στο ακόλουθο γράφημα αποτυπώνεται ποσοστιαία το σύνολο των προπτυχιακών φοιτητών, προκειμένου να καταγραφεί με περισσότερη ακρίβεια το έτος τους ώστε να διαφανεί εκτός από το επίπεδο σπουδών, εάν και το έτος των προπτυχιακών φοιτητών διαδραματίζει σημαντικό ρόλο στην αντίληψη τους για τα Βιομετρικά Συστήματα. Όπως διαφαίνεται, το μεγαλύτερο ποσοστό προέρχεται από τους φοιτητές που διανύουν το πρώτο έτος της φοίτησης τους, το οποίο ανέρχεται στο 28%, το 20% από φοιτητές δεύτερου έτους, το 17% από τεταρτοετείς φοιτητές ενώ στο 12% καταγράφηκαν φοιτητές από το τρίτο και πέμπτο έτος αντίστοιχα και μόλις το 10% από φοιτητές που διανύουν μεγαλύτερο από το πέμπτο έτος σπουδών τους.

Γράφημα 4. Δημογραφικά Στοιχεία-Έτος Προπτυχιακών Φοιτητών

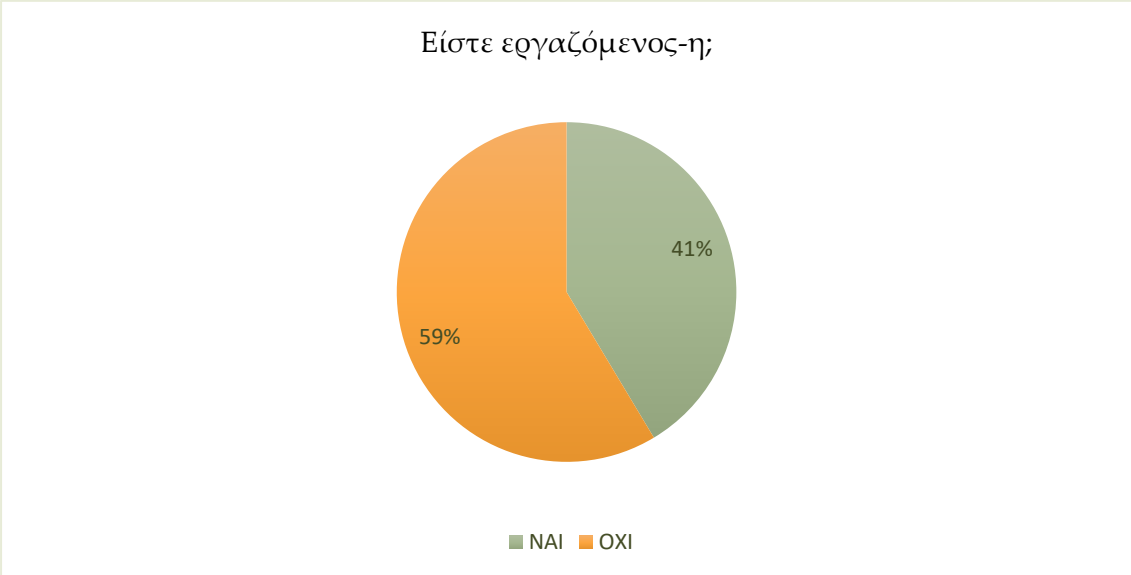
Από το παρακάτω γράφημα φαίνεται το Τμήμα φοίτησης των συμμετεχόντων-ουσών φοιτητών-τριών από τα συνολικά 18 τμήματα του Πανεπιστημίου Αιγαίου. Το μεγαλύτερο ποσοστό καταγράφεται από τους φοιτητές του Τμήματος Πολιτισμικής Τεχνολογίας και Επικοινωνίας, το οποίο ανέρχεται στο 18%, το 10% ανήκει σε φοιτητές του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, το 9% σε φοιτητές του Τμήματος Επιστημών της Προσχολικής Αγωγής και του Εκπαιδευτικού Σχεδιασμού, ενώ τα μικρότερα ποσοστά καταγράφηκαν από τους φοιτητές του Τμήματος Οικονομικής και Διοίκησης Τουρισμού και του Τμήματος Στατιστικής και Αναλογιστικών-Χρηματοοικονομικών Μαθηματικών με ποσοστό 2%.

Γράφημα 5. Δημογραφικά Στοιχεία-Τμήμα Φοίτησης



Το γράφημα 6 σκιαγραφεί τα ποσοστά των φοιτητών-τριών που εργάζονται. Όπως διαφαίνεται από το γράφημα, το 59% των συμμετεχόντων-ουσών φοιτητών-τριών δηλώνει πως δεν εργάζεται ενώ το 41% φαίνεται πως εργάζεται παράλληλα με τις ακαδημαϊκές το σπουδές.

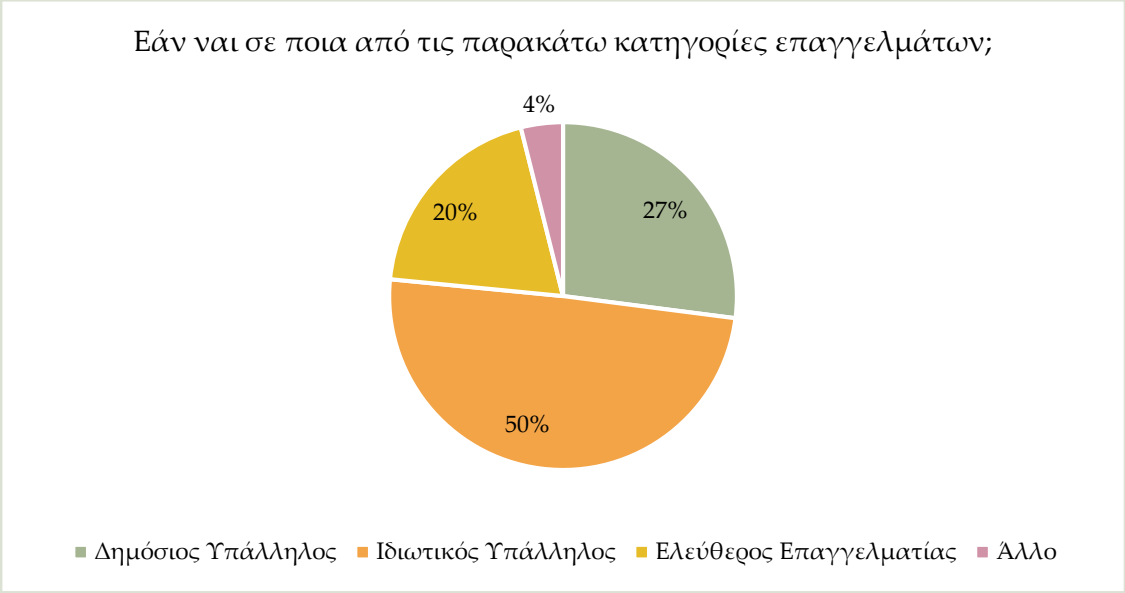
Γράφημα 6. Δημογραφικά Στοιχεία- Είστε εργαζόμενος-η;



Το παρακάτω γράφημα αποτελεί συνέχεια του γραφήματος 6 και ουσιαστικά επικεντρώνεται στο 41% των φοιτητών, οι οποίοι δηλώνουν πως εργάζονται, επομένως χωρίζει τις κατηγορίες επαγγέλματος τους. Συγκεκριμένα, από τους

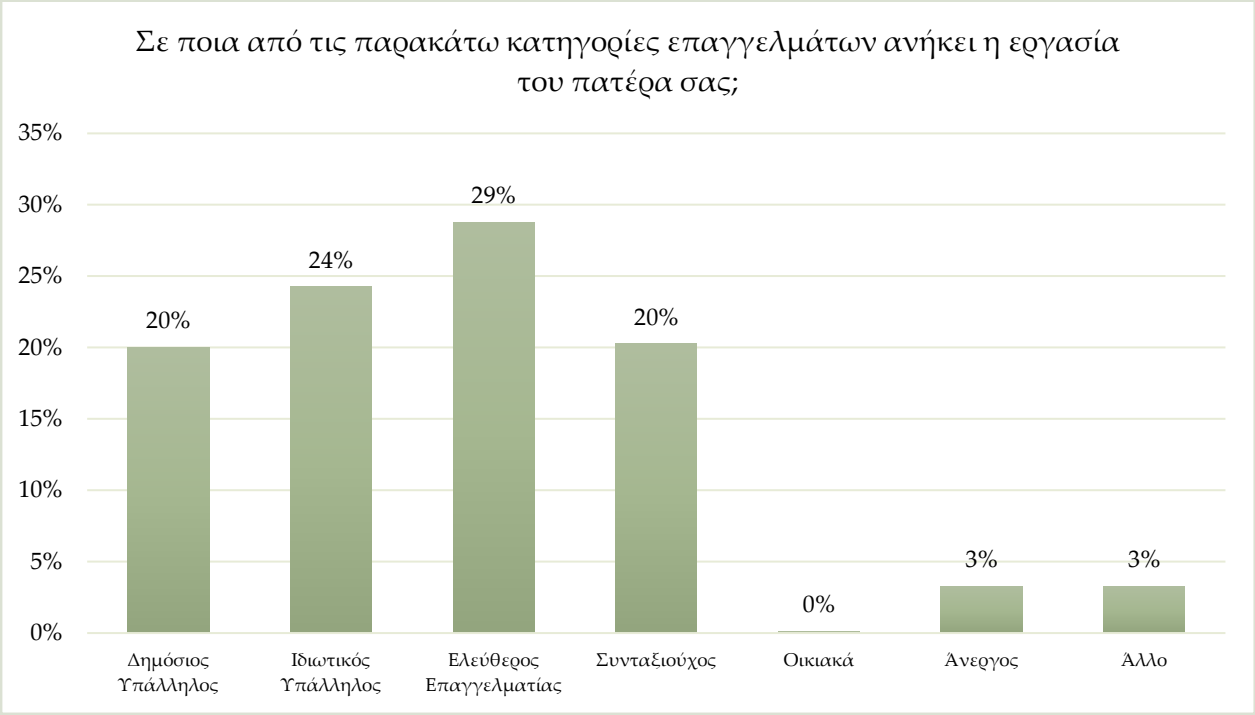
φοιτητές που απάντησαν πως εργάζονται, σημειώνεται πως το 50% εργάζεται ως ιδιωτικοί υπάλληλοι, το 27% ως δημόσιοι υπάλληλοι, ενώ το 20% ως ελεύθεροι επαγγελματίες και μόλις το 4% δηλώνει ως επάγγελμα άλλο.

Γράφημα 7. Δημογραφικά Στοιχεία- Εάν ναι, σε ποια κατηγορία επαγγέλματος;



Το ακόλουθο γράφημα αποτυπώνει ποσοστιαία την κατηγορία επαγγέλματος του πατέρα των φοιτητών-τριών που συμμετείχαν στην έρευνα. Το μεγαλύτερο ποσοστό του γραφήματος προκύπτει από τους ελεύθερους επαγγελματίες, το οποίο ανέρχεται στο 29%, το 24% προέρχεται από τους ιδιωτικούς υπαλλήλους, ενώ στο 20% ανήκουν και οι δημόσιοι υπάλληλοι και συνταξιούχοι και με ποσοστό μόλις 3% ανήκουν οι άνεργοι και οι φοιτητές που δήλωσαν άλλο ως κατηγορία επαγγέλματος του πατέρα τους. Εντύπωση προκαλεί το ποσοστό 0% που προέρχεται από την επιλογή οικιακά, παρουσιάζοντας έτσι πως το ανδρικό φύλο δεν ασχολείται με την «κατηγορία» αυτή.

Γράφημα 8. Δημογραφικά Στοιχεία- Κατηγορία Επαγγέλματος Πατέρα



Παρατηρώντας το παρακρατώ γράφημα, από το οποίο διαφαίνεται η κατηγορία επαγγέλματος της μητέρας των συμμετεχόντων-ουσών στην έρευνα, τα ποσοστά που προκύπτουν δεν παρουσιάζουν κάποια ιδιαίτερη διαφοροποίηση μεταξύ τους όπως στο επάγγελμα του πατέρα. Σύμφωνα με τα ποσοστά, το μεγαλύτερο παρατηρείται στους ιδιωτικούς και δημόσιους υπαλλήλους αλλά και στην επιλογή οικιακά, το οποίο ανέρχεται στο 21%. Τα επόμενα ποσοστά που παρουσιάζουν μια

Γράφημα 9. Δημογραφικά Στοιχεία- Κατηγορία Επαγγέλματος Μητέρας

ποσοστιαία διαφορά ανήκουν στις κατηγορίες ελεύθερος επαγγελματίας, συνταξιούχος, άνεργος και την επιλογή άλλο, τα οποία ανέρχονται στο 14%, 13%, 8% και 1% αντίστοιχα.

Από την τελευταία ερώτηση που κλήθηκαν να απαντήσουν οι συμμετέχοντες-ουσες, η οποία αναφέρεται στο ετήσιο εισόδημα τους, διαφαίνονται τα παρακάτω ποσοστά. Προκύπτει πως το μεγαλύτερο ποσοστό με όχι και τόσο μεγάλη διαφορά, ανήκει στους φοιτητές-τριες με ετήσιο εισόδημα μικρότερο από 10.000€, το οποίο ανέρχεται στο 44%, ενώ με 42% να επιλέγουν όσοι έχουν 10.001€-25.000€. Το ποσοστό 13% ανήκει στους φοιτητές-τριες με εισόδημα 25.001€- 55.000€, ενώ μικρό είναι το ποσοστό όσων έχουν ετήσιο εισόδημα μεγαλύτερο από 55.0001€.

Γράφημα 10. Δημογραφικά Στοιχεία- Ετήσιο Εισόδημα

Αναλυτικότερα, από το πλήθος των δημογραφικών στοιχείων που παρατέθηκαν παραπάνω, οκτώ κατηγορίες εξ' αυτών αναδεικνύουν σημαντικότητα μια τάση των χρηστών απέναντι στα Βιομετρικά Συστήματα, βασισμένα πάντα στα αποτελέσματα των ερωτήσεων. Αξίζει να σημειωθεί πως μορφολογικά το ερωτηματολόγιο είναι χωρισμένο σε ενότητες, προκειμένου οι ερωτήσεις να είναι δομημένες και να έχουν μια λογική συνάφεια ώστε οι συμμετέχοντες να έχουν συγκεντρωτικά τις ερωτήσεις. Σύμφωνα με αυτή τη λογική, η ανάλυση των αποτελεσμάτων θα παρατεθεί με βάση τις ενότητες του ερωτηματολογίου.

Ενότητα Α

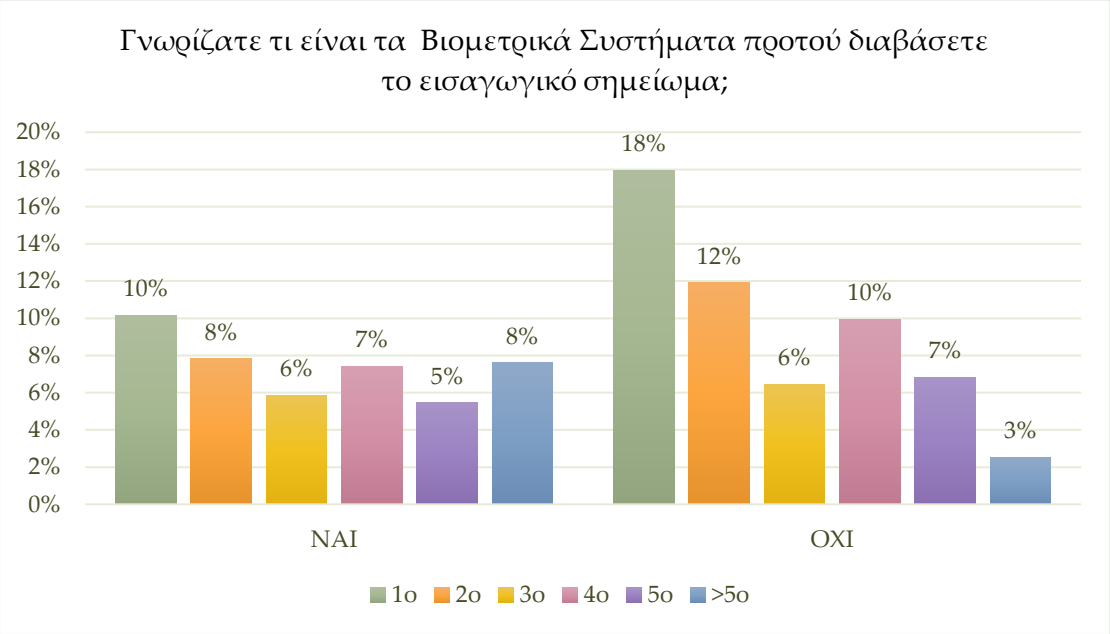
Η ενότητα αυτή αποτελείται από δύο ερωτήσεις και προκύπτουν τα αποτελέσματα που σχετίζονται με την γνώση των Βιομετρικών Συστημάτων από τους χρήστες. Αρχικά, κρίθηκε αναγκαίο να αναλυθεί το ποσοστό των συμμετεχόντων που γνώριζαν και δεν γνώριζαν τα Βιομετρικά Συστήματα προτού διαβάσουν το εισαγωγικό σημείωμα. Ουσιαστικά, αυτή είναι και η πρώτη ερώτηση της ενότητας και παρακάτω διαφαίνονται τα αποτελέσματα της.

Γράφημα 11. Ενότητα Α- Ερώτηση Α

Από το παραπάνω γράφημα διαφαίνεται ποσοστιαία μια μικρή διαφορά ανάμεσα στους συμμετέχοντες-ουσες που γνώριζαν και δεν γνώριζαν τα Βιομετρικά Συστήματα. Το μεγαλύτερο ποσοστό ανήκει στους χρήστες που γνώριζαν τον ορισμό τους, το οποίο ανέρχεται στο 51%, ενώ με 49% είναι οι χρήστες που έμαθαν τι είναι τα Βιομετρικά Συστήματα λόγω του εισαγωγικού σημειώματος της έρευνας. Αν και τα αποτελέσματα της συγκεκριμένης ερώτησης δεν παρουσιάζουν καμία διαφοροποίηση στην ανάλυση τους με βάση τα δημογραφικά στοιχεία, καθώς δεν υπήρχε κάποιος παράγοντας που να συντελεί στη γνώση η μη των βιομετρικών συστημάτων αλλά και στην ποσοστιαία διαφορά μεταξύ του «ΝΑΙ» και του «ΟΧΙ», παρατηρήθηκε μια σημαντική διαφορά από το έτος σπουδών των προπτυχιακών φοιτητών.

Όπως διαφαίνεται από το παρακάτω γράφημα το ποσοστό των φοιτητών που δεν γνωρίζουν τα βιομετρικά συστήματα είναι μεγαλύτερο από αυτό που τα γνωρίζει. Συγκεκριμένα, το 44% των φοιτητών απαντάει «ΝΑΙ», ενώ το 56% «ΟΧΙ». Αυτό που προκύπτει από το γράφημα και αξίζει να αναλυθεί είναι ότι το μεγαλύτερο ποσοστό ανήκει στους πρωτοετείς φοιτητές, το οποίο ανέρχεται στο 18% και δηλώνουν πως δεν γνώριζαν τον ορισμό τους. Ανεξάρτητα από τους δευτεροετείς φοιτητές με ποσοστό 12%, διαφαίνεται πως οι φοιτητές που διανύουν το τέταρτο έτος των σπουδών τους έχουν ποσοστό μεγαλύτερο από τους φοιτητές του τρίτου έτους, τα οποία ανέρχονται στο 10% και το 6% αντίστοιχα.

Γράφημα 12. Ενότητα Α- Ερώτηση Α- Ανά Έτος Σπουδών Προπτυχιακών Φοιτητών



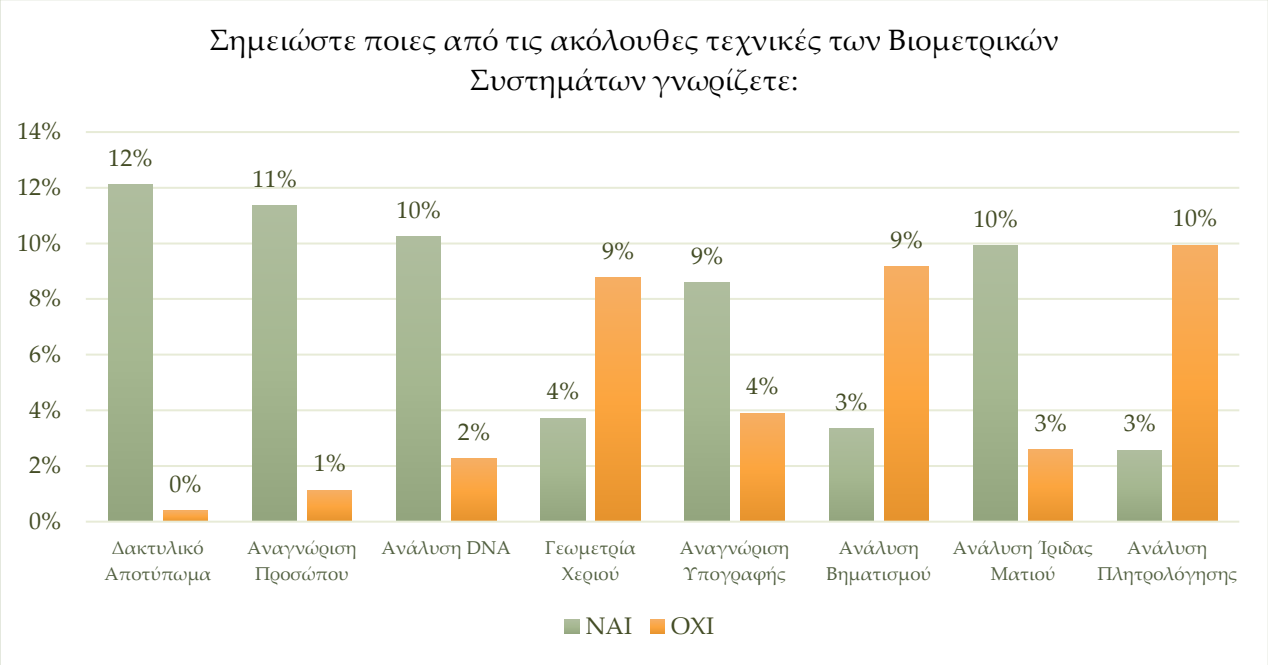
Παρατηρείται λοιπόν, πως η γνώση δεν συνάδει πάντα με το επίπεδο των σπουδών και αυτό γίνεται αντιληπτό από το χαμηλότερο ποσοστό που ανέρχεται στο 3% και προέρχεται από τους φοιτητές που διανύουν μεγαλύτερο από το πέμπτο έτος και απαντούν «ΟΧΙ», ενώ το ίδιο πάλι έτος σπουδών με ποσοστό 8% έχει από τα υψηλότερα ποσοστά των φοιτητών που δηλώνουν ότι γνώριζαν εξαρχής των ορισμό των Βιομετρικών Συστημάτων. Επιπλέον, από τις υπόλοιπες τιμές συγκριτικά και στις δύο επιλογές, τα αντίστοιχα έτη δεν παρουσιάζουν ιδιαίτερες διαφοροποιήσεις.

Το παρακάτω γράφημα αποτυπώνει τα αποτελέσματα που προέκυψαν από την δεύτερη ερώτηση της ίδιας ενότητας «Σημειώστε ποιες από τις ακόλουθες τεχνικές των Βιομετρικών Συστημάτων γνωρίζετε:»

Όπως διαφαίνεται από το γράφημα, η πιο δημοφιλής βιομετρική τεχνική είναι το δακτυλικό αποτύπωμα με το συνολικό ποσοστό των συμμετεχόντων-ουσών να ανέρχεται στο 12%. Κατά κύριο λόγο οι περισσότερες βιομετρικές τεχνικές καταγράφουν υψηλά ποσοστά, εκτός από την γεωμετρία χεριού, την ανάλυση βηματισμού και την ανάλυση πληκτρολόγησης, οι οποίες έχουν υψηλότερα ποσοστά από τους χρήστες που δεν τις γνωρίζουν, τα οποία ανέρχονται στο 9% για τις δύο πρώτες, ενώ στο 10% για την ανάλυση πληκτρολόγησης.

Αξίζει να σημειωθεί πως αναφορικά με το δακτυλικό αποτύπωμα και την αναγνώριση προσώπου, τα ποσοστά των χρηστών που δε τις γνωρίζουν είναι μικρότερα του 1%, αποτελέσματα που δείχνουν ότι πρόκειται με διαφορά για τις πιο δημοφιλείς βιομετρικές τεχνικές. Ιδιαίτερα, η ηλικιακή ομάδα 18-22 καταγράφει τα μεγαλύτερα ποσοστά των φοιτητών-τριών που γνωρίζουν το δακτυλικό αποτύπωμα και την αναγνώριση προσώπου. Ο παράγοντας ηλικία,

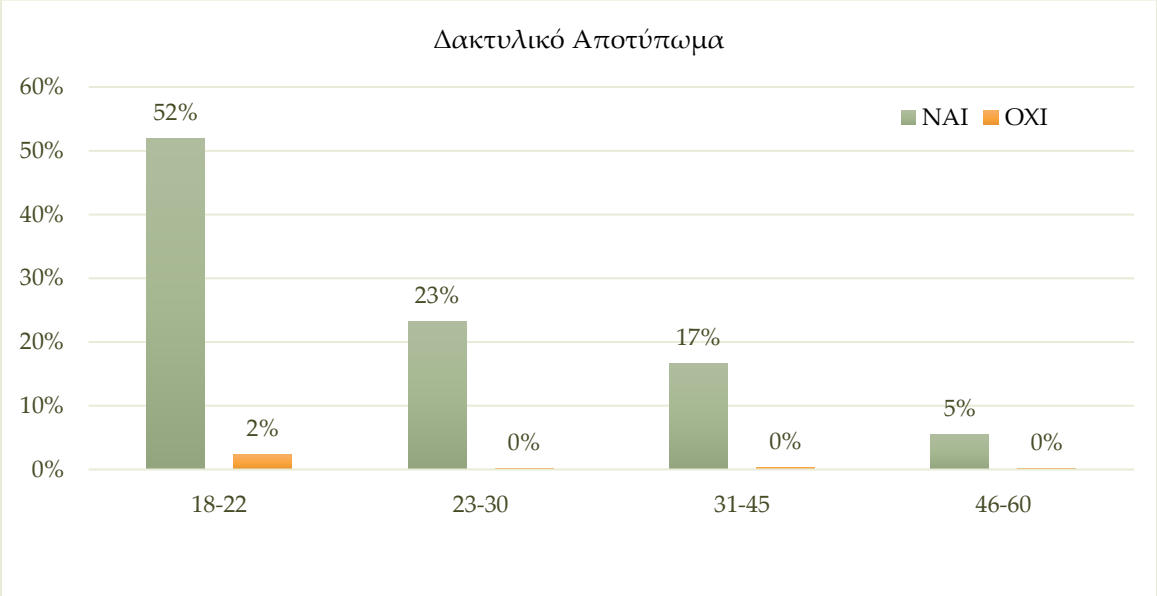
Γράφημα 13. Ενότητα Α- Ερώτηση Β



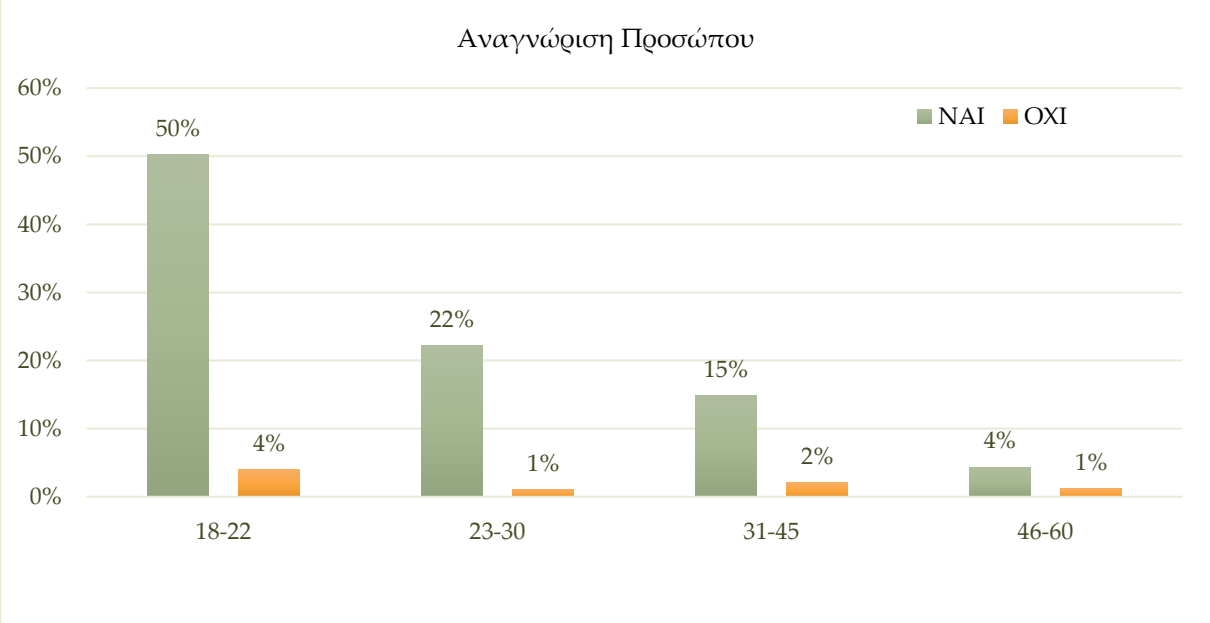
όπως φαίνεται στα γραφήματα 13 και 14, διαδραματίζει σημαντικό ρόλο στην γνώση των τεχνικών αυτών. Η ποσοστιαία διαφορά που προκύπτει από το γράφημα με τα δακτυλικά αποτυπώματα, δημιουργεί μια ξεκάθαρη εικόνα,

καθώς το 52% των συμμετεχόντων-ουσών, δηλαδή πάνω από το ήμισυ γνωρίζει την βιομετρική αυτή τεχνική και μόλις το 2% αυτής της ηλικίας δεν την γνωρίζει. Παράλληλα, φαίνεται πως τα υπόλοιπα ποσοστά των άλλων ηλικιακών ομάδων είναι εξίσου υψηλά, το οποίο δεν παρατηρήθηκες σε κάποιο άλλο δημογραφικό στοιχείο. Εκτός απ' αυτό, μπορεί το δακτυλικό αποτύπωμα στην ηλικία 18-22 να καταγράφει υψηλά ποσοστά, όμως εξίσου σημαντικό είναι πως στις υπόλοιπες ηλικιακές ομάδες δεν καταγράφεται κανένα ποσοστό των χρηστών που να μην το γνωρίζουν. Παρόμοια αποτελέσματα προέκυψαν και από την ανάλυση της ανα-

Γράφημα 13. Ενότητα Α- Ερώτηση Β -Ανά Ηλικιακή Ομάδα



Γράφημα 14. Ενότητα Α- Ερώτηση Β -Ανά Ηλικιακή Ομάδα



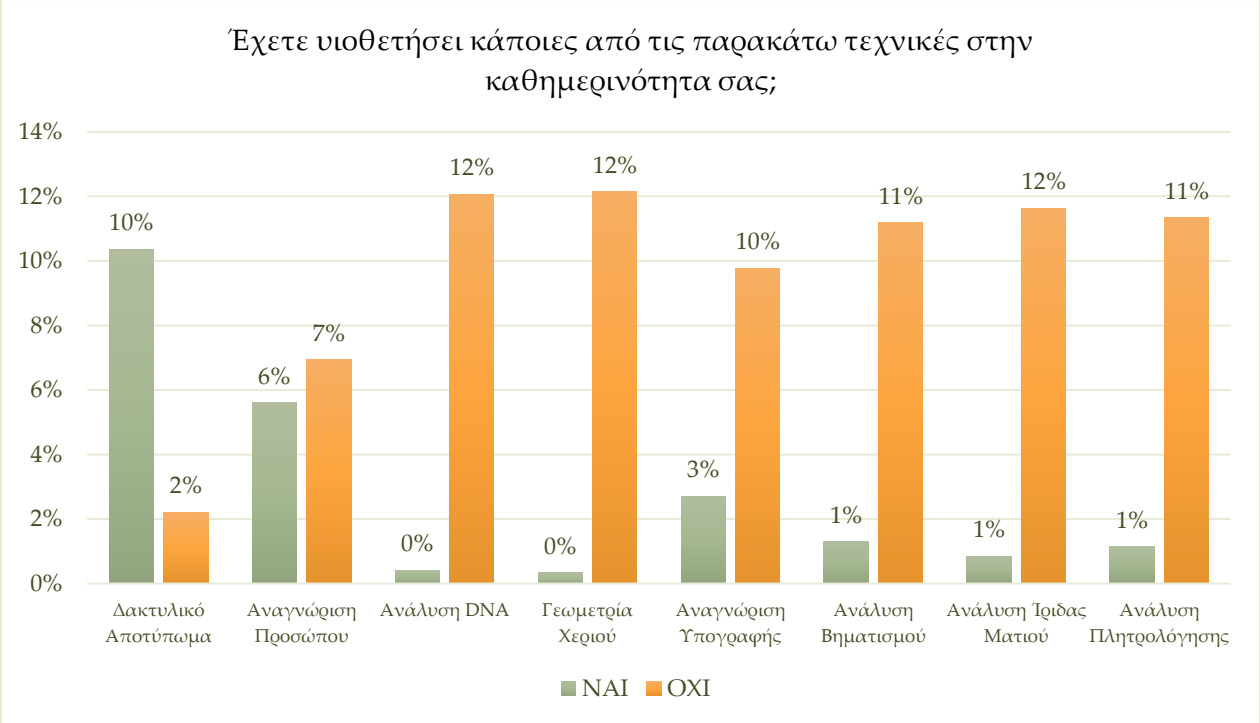
γνώρισης προσώπου. Όπως και στο δακτυλικό αποτύπωμα η ηλικιακή ομάδα 18-22 κατέγραψε τα υψηλότερα ποσοστά, έτσι και στην αναγνώριση προσώπου με 50% συμβαίνει το ίδιο. Ειδικότερα, το 22% των 23-30 γνωρίζει την τεχνική αυτή, όπως επίσης και το 15% των 31-45 αλλά και το 4% των 46-60. Από την τεχνική της αναγνώρισης προσώπου, τα ποσοστά των χρηστών που δεν τις γνωρίζουν παρουσιάζουν μια αυξητική τάση σε σχέση με αυτά του δακτυλικού αποτυπώματος, δείχνοντας που η αναγνώριση προσώπου καταγράφει υψηλότερα ποσοστά των χρηστών που δεν την γνωρίζουν με αποτέλεσμα να μην είναι τόσο δημοφιλές όσο το δακτυλικό αποτύπωμα.

Ενότητα Β

Η ενότητα αυτή σκιαγραφεί την εμπειρία που δημιουργείται από την χρήση των βιομετρικών συστημάτων. Αναλυτικότερα, οι παρακάτω ερωτήσεις που αποτελούν την ενότητα αυτή, δημιουργούν μια σαφή εικόνα σχετικά με τη χρήση των τεχνικών αυτών στην καθημερινότητα των χρηστών.

Η πρώτη ερώτηση της ενότητας αυτής είναι «Έχετε υιοθετήσει κάποιες από τις παρακάτω τεχνικές στην καθημερινότητα σας;» Από το παρακάτω γράφημα

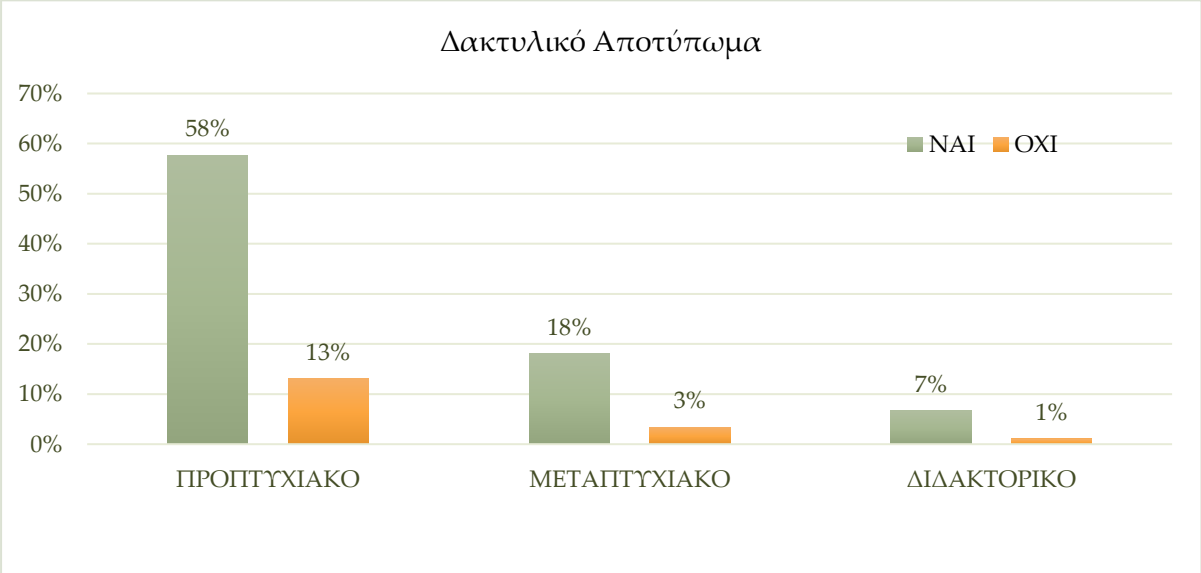
Γράφημα 15. Ενότητα Β- Ερώτηση C



εξάγεται το ίδιο συμπέρασμα με τα προηγούμενα γραφήματα. Αναλυτικότερα, διαμορφώνεται ένα 10% των χρηστών που υιοθετούν το δακτυλικό αποτύπωμα στην καθημερινότητα τους, το οποίο εξηγεί τα αποτελέσματα της προηγούμενης ερώτησης. Αυτό όπως παρατηρείται δεν συμβαίνει με την αναγνώριση προσώπου, καθώς φάνηκε να είναι από τις πιο δημοφιλείς τεχνικές όμως αυτό δεν συνεπάγεται πως οι χρήστες την χρησιμοποιούν στην καθημερινότητα τους. Το ποσοστό 7% αναδιαμορφώνει την κατάσταση αυτή. Επιπλέον, σχετικά με τις τεχνικές που οι χρήστες υιοθετούν εντύπωση δημιουργεί το 0% από την ανάλυση DNA και την γεωμετρία χεριού, ποσοστό που δείχνει πως δεν πρόκειται για τεχνικές που μπορεί εύκολα να χρησιμοποιηθούν στην καθημερινότητα των χρηστών. Παράλληλα, παρατηρούνται υψηλά ποσοστά σε όλες τις υπόλοιπες βιομετρικές τεχνικές. Εκτός από το δακτυλικό αποτύπωμα δεν διαφαίνεται καμία άλλη βιομετρική τεχνική που να έχει υιοθετηθεί από τους χρήστες σε καθημερινή χρήση με ποσοστά να κυμαίνονται από 10%-12%.

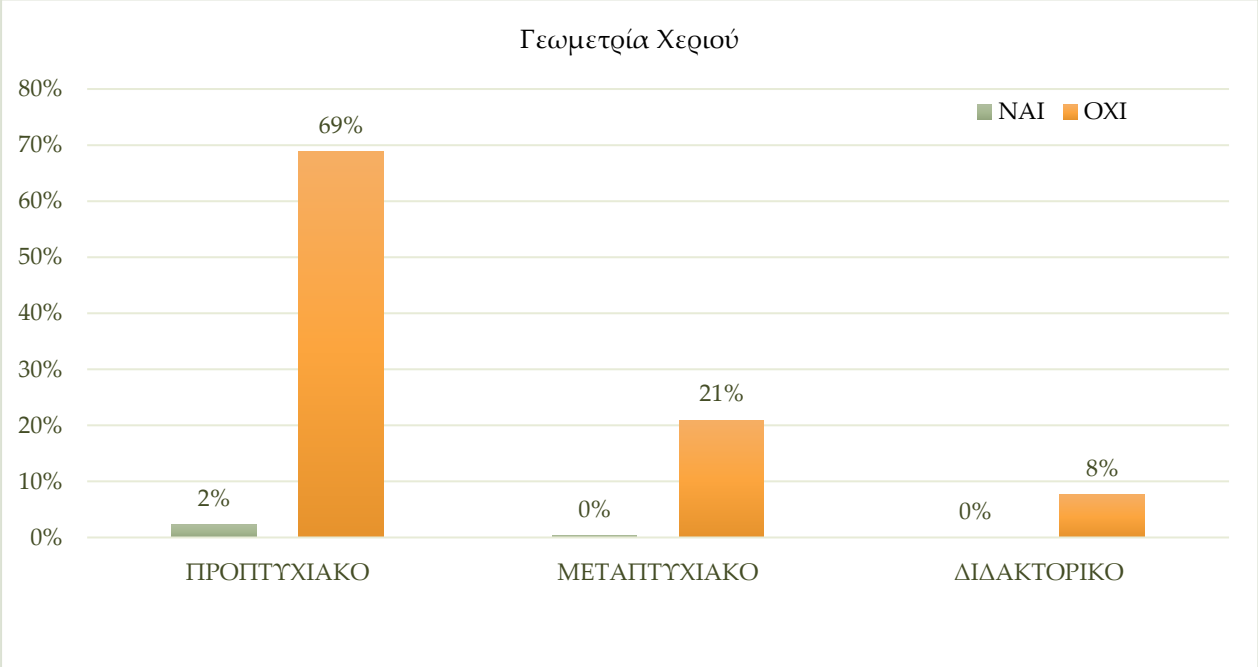
Τα συνολικά αυτά αποτελέσματα έρχεται να ενισχύσει το επίπεδο σπουδών των συμμετεχόντων-ουσών. Το επίπεδο σπουδών διαφαίνεται να λειτουργεί ως παράγοντας διαφοροποίησης, καθώς σύμφωνα με τα παρακάτω γραφήματα στο προπτυχιακό επίπεδο επιβεβαιώνονται με σαφήνεια τα συνολικά αποτελέσματα σχετικά με την υιοθέτηση των βιομετρικών τεχνικών στην καθημερινότητα των χρηστών. Αρχικά από το γράφημα 16 φαίνεται πως επιβεβαιώνεται το υψηλό πο-

Γράφημα 16. Ενότητα Β- Ερώτηση C-Ανά Επίπεδο Σπουδών



σοστό των συμμετεχόντων που υιοθετούν το δακτυλικό αποτύπωμα στην καθημερινότητα τους. Το μεγαλύτερο ποσοστό καταγράφεται από τους προπτυχιακούς φοιτητές, το οποίο ανέρχεται στο 58%, το 18% από τους μεταπτυχιακούς ενώ το 7% από τους διδακτορικούς φοιτητές. Τα ποσοστά των χρηστών που δεν έχουν υιοθετήσει τη παρούσα τεχνική, ενώ δεν είναι υψηλά συγκριτικά όμως με τα υπόλοιπα δείχνουν κι αυτά μια τάση. Για παράδειγμα, ενώ το 1% των διδακτορικών φοιτητών που δεν υιοθετεί το αποτύπωμα δεν είναι σημαντικό, εάν συγκριθεί με το 7% των ίδιων, η διαφορά τους δεν είναι μεγάλη. Αντιθέτως, αναφορικά με την γεωμετρία χεριού τα αποτελέσματα δείχνουν πως μόνο το 2% των χρηστών συνολικά την υιοθετεί και προέρχεται από τους προπτυχιακούς φοιτητές. Επιπλέον, από το γράφημα προκύπτει πως το 69% των προπτυχιακών φοιτητών δεν την υιοθετεί, όπως επίσης και οι μεταπτυχιακοί με 21% και οι διδακτορικοί με 8%.

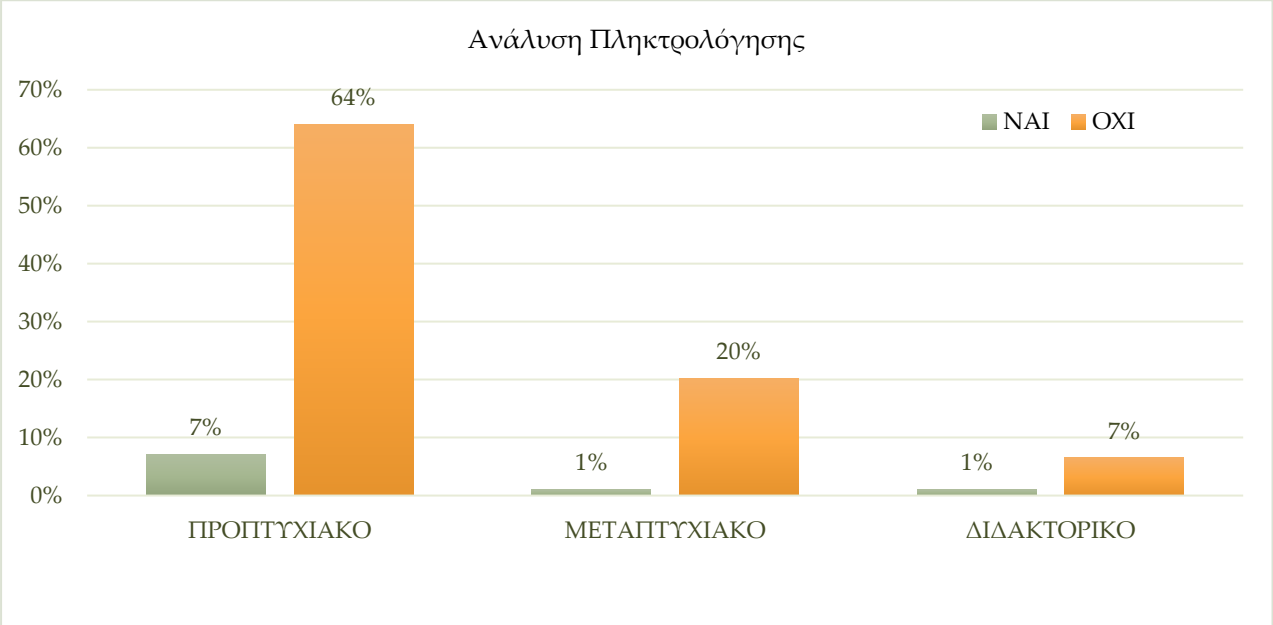
Γράφημα 17. Ενότητα Β- Ερώτηση C-Ανά Επίπεδο Σπουδών



Στο ίδιο πλαίσιο κυμαίνονται και τα ποσοστά της ανάλυσης πληκτρολόγησης. Ιδιαίτερα, συγκριτικά με την γεωμετρία χεριού, παρατηρείται μια συνολική αύξηση των ποσοστών των χρηστών που υιοθετούν την ανάλυση πληκτρολόγησης, τα οποία ανέρχονται στο 9%, τα οποία μοιράζονται από 7% στους προπτυχιακούς και από 1% σε μεταπτυχιακούς και διδακτορικούς φοιτητές. Αντιθέτως, το μεγαλύτερο ποσοστό ανήκει στους προπτυχιακούς φοιτητές, το

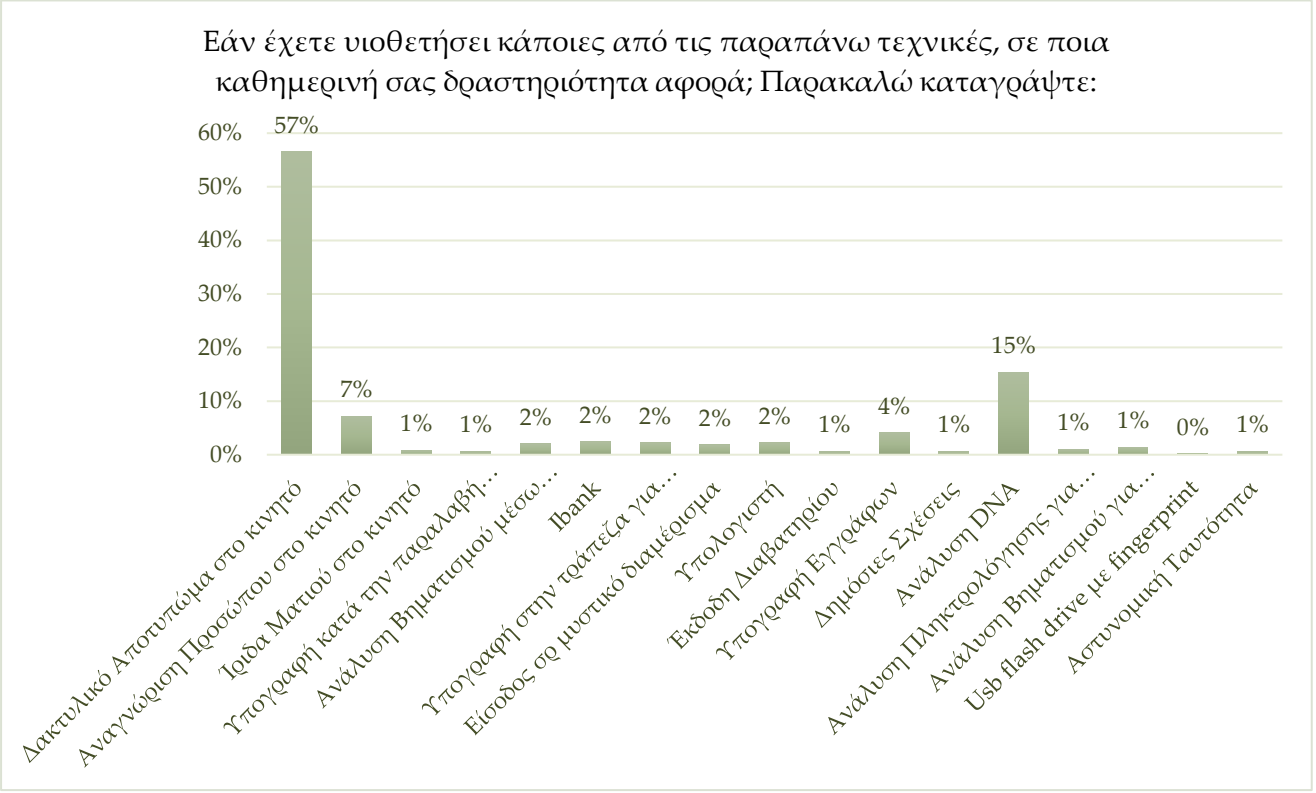
οποίο ανέρχεται στο 64%, ενώ το 20% στους μεταπτυχιακούς και το 7% σε διδακτορικούς.

Γράφημα 18. Ενότητα Β- Ερώτηση C-Ανά Επίπεδο Σπουδών



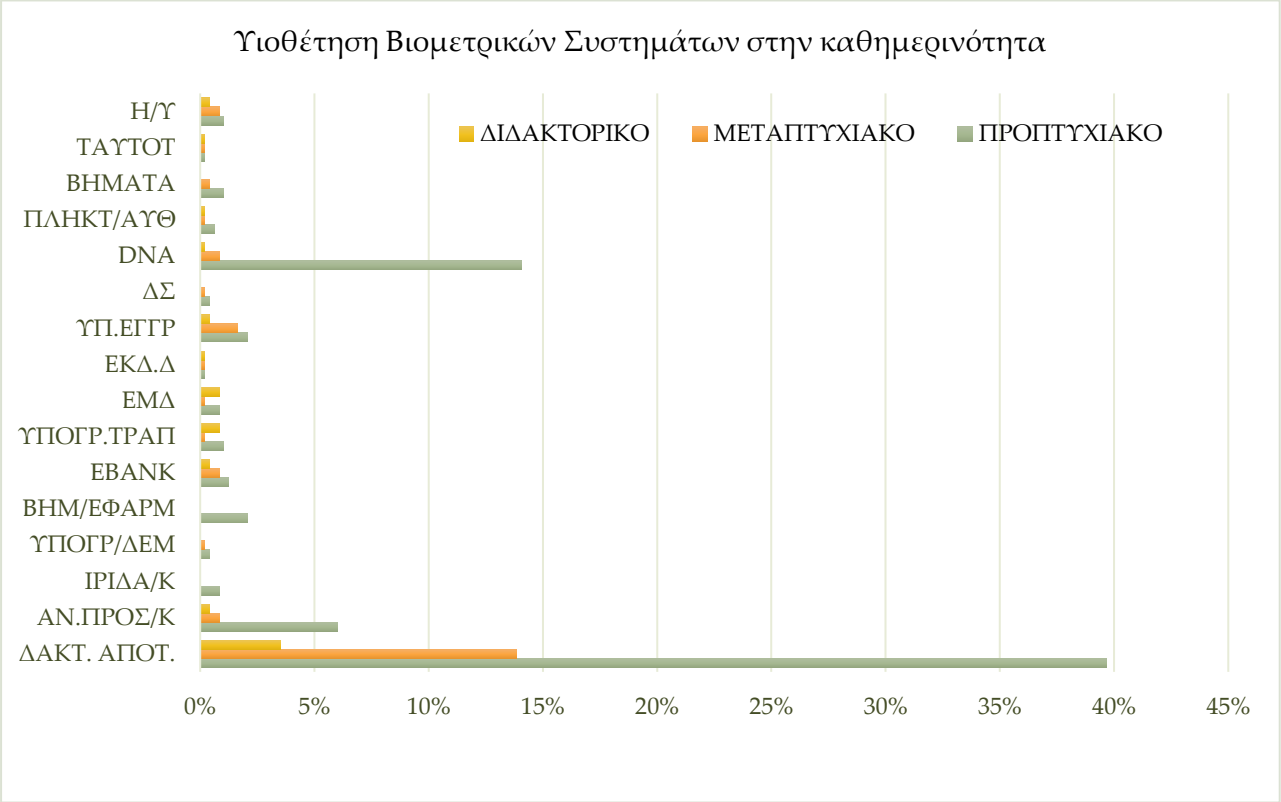
Όπως επισημάνθηκε στη αρχή της υποενότητας αυτής, οι ενότητες του ερωτηματολογίου είναι χωρισμένες έτσι ώστε μέσα στην ενότητα πιθανά οι ερωτήσεις να μπορούν να συνδεθούν. Η λογική αυτή παρατηρείται και στην συγκεκριμένη ερώτηση «Εάν έχετε υιοθετήσει κάποιες από τις παραπάνω τεχνικές, σε ποια καθημερινή σας δραστηριότητα αφορά; Παρακαλώ καταγράψτε:», η οποία αποτελεί συνέχεια της προηγούμενης», η οποία είναι άρρηκτα συνδεδεμένη με την προηγούμενη. Συγκεκριμένα, πρόκειται για μια ερώτηση ανοικτού τύπου, επομένως οι συμμετέχοντες κλήθηκαν να καταγράψουν σε ποιες καθημερινές τους δραστηριότητες χρησιμοποιούν τις βιομετρικές τεχνικές που υιοθετούν. Παρατηρώντας το παρακάτω γράφημα διαφαίνεται η μεγάλη διαφορά μεταξύ των επιλογών των χρηστών. Το μεγαλύτερο ποσοστό προέρχεται από τους χρήστες που χρησιμοποιούν το δακτυλικό τους αποτύπωμα για να ξεκλειδώσουν το κινητό τους τηλέφωνο, το οποίο ανέρχεται στο 57%, το 15% ανήκει στους χρήστες που υιοθετούν την ανάλυση DNA και το 7% που χρησιμοποιεί την αναγνώριση προσώπου στο κινητό. Τα υπόλοιπα ποσοστά είναι αισθητά μικρότερα και ισάξια στο 1%-2%.

Γράφημα 19. Ενότητα Β- Ερώτηση D



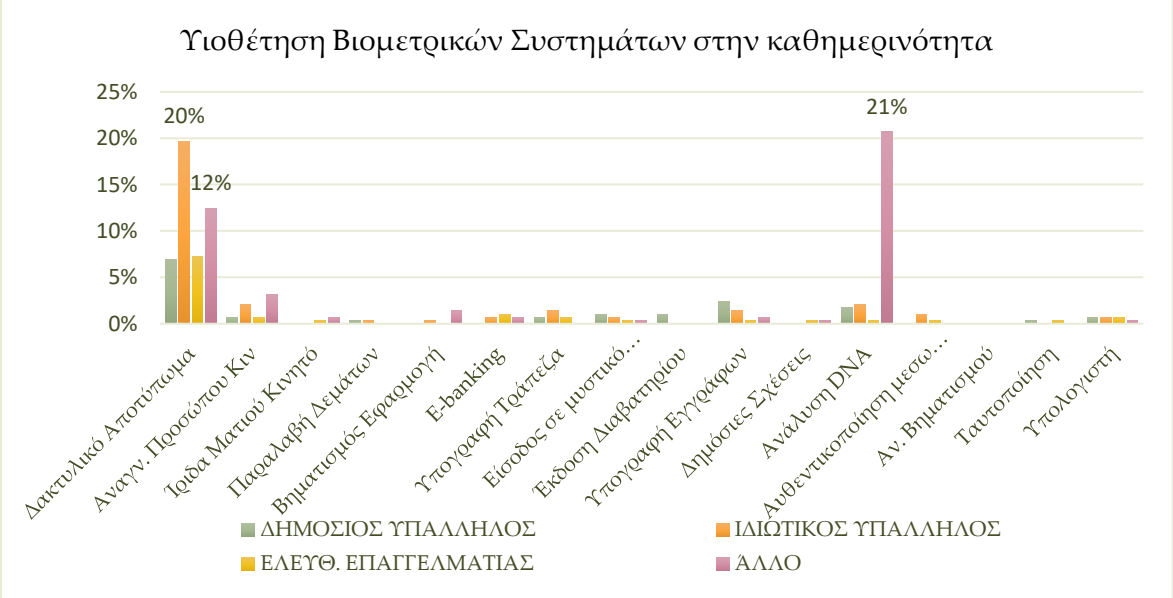
Επιπλέον, το επίπεδο σπουδών και η κατηγορία επαγγέλματος των φοιτητών φαίνεται να λειτουργεί ως παράγοντας διαφοροποίησης. Αρχικά, από το δημογραφικό στοιχείο επίπεδο σπουδών καταγράφηκε συγκριτικά με τα υπόλοιπα δημογραφικά το μεγαλύτερο ποσοστό των χρηστών που υιοθετεί το δακτυλικό αποτύπωμα για να ξεκλειδώσει το κινητό του τηλέφωνο. Το ποσοστό αυτό ανέρχεται στο 40% και ανήκει στους προπτυχιακούς φοιτητές, οι οποίοι σε αντίθεση με τα άλλα επίπεδα σπουδών φαίνεται να τα χρησιμοποιούν σε μεγαλύτερο βαθμό. Αυτό που προκαλεί εντύπωση είναι πως συνολικά η ανάλυση DNA δεν ήταν από τις τεχνικές που οι χρήστες χρησιμοποιούν με μεγαλύτερη ευκολία στην καθημερινότητα τους. Παρόλα αυτά, οι δύο αυτοί παράγοντες, το επίπεδο σπουδών και το επάγγελμα των φοιτητών-τριών, σημειώνουν υψηλά ποσοστά στην τεχνική αυτή. Σχετικά με το επίπεδο σπουδών όπως φαίνεται και στο ακόλουθο γράφημα, το ποσοστό τω προπτυχιακών φοιτητών που την υιοθετούν ανέρχεται στο 15%.

Γράφημα 20. Ενότητα Β- Ερώτηση D- Ανά Επίπεδο Σπουδών



Ομοιογενή αποτελέσματα προκύπτουν και από τις κατηγορίες επαγγελμάτων των φοιτητών-τριών. Ειδικότερα, το μεγαλύτερο ποσοστό καταγράφεται από τους φοιτητές που δηλώνουν ως κατηγορία επαγγέλματος την επιλογή άλλο και ανήκει στην ανάλυση DNA, η οποία ανέρχεται στο 21%. Το 20% των φοιτητών που εργάζονται ως ιδιωτικοί υπάλληλοι χρησιμοποιούν το δακτυλικό τους αποτύπωμα για να ξεκλειδώσουν το κινητό τους τηλέφωνο. Η δραστηριότητα αυτή συνολικά

Γράφημα 21. Ενότητα Β- Ερώτηση D- Ανά Κατηγορία Επαγγελμάτων Φοιτητή-τριας



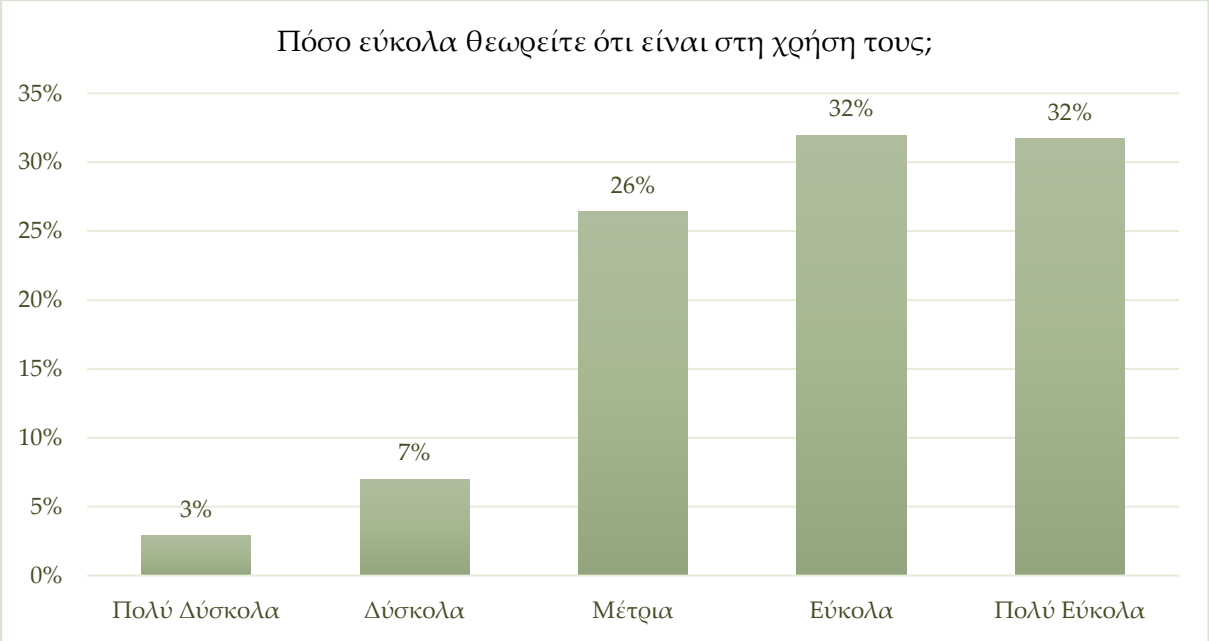
καταγράφει τα περισσότερα ποσοστά καθώς επίσης το 12% όσων εργάζεται ως άλλο επιλέγει αυτή την τεχνική μαζί με το 7% που προέρχεται από δημόσιους υπάλληλους και ελεύθερους επαγγελματίες.

Ενότητα Γ

Η ενότητα αυτή σκιαγραφεί την ευχρηστία των βιομετρικών συστημάτων. Αναλυτικότερα, οι παρακάτω ερωτήσεις που αποτελούν την ενότητα αυτή, δημιουργούν μια σαφή εικόνα σχετικά με την αντίληψη των χρηστών απέναντι στα βιομετρικά συστήματα.

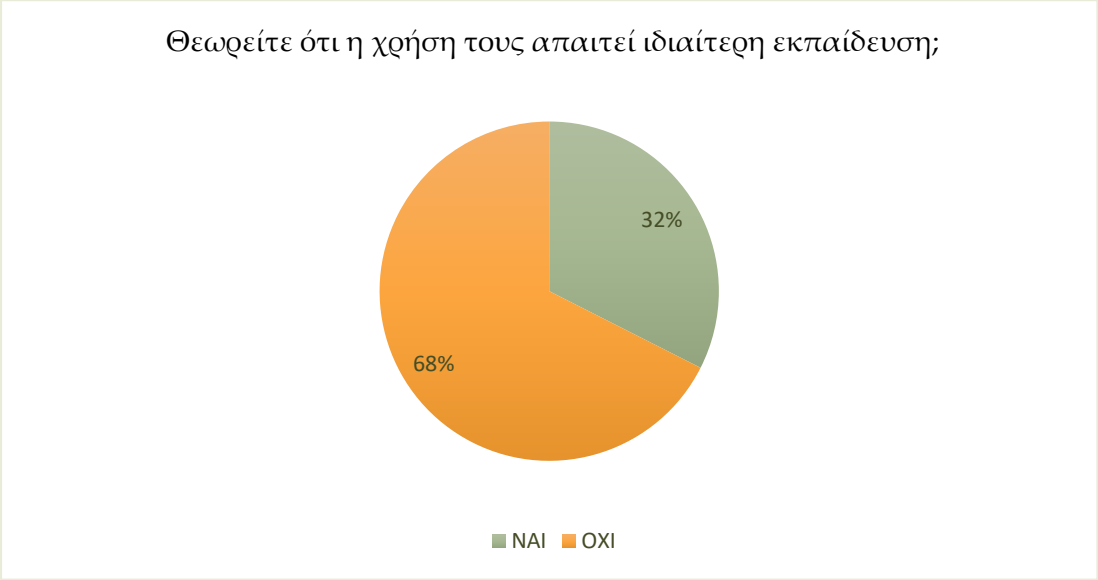
Η πρώτη ερώτηση της ενότητας αυτής είναι : «Πόσο εύκολα θεωρείτε ότι είναι στη χρήση τους;». Οι συμμετέχοντες κλήθηκαν να επιλέξουν από το 1 έως το 5, κατά πόσο θεωρούν τα βιομετρικά συστήματα εύκολα στην χρήση τους. Από το παρακάτω γράφημα δεν προκύπτει κάποια ιδιαίτερη δυσκολία από τους χρήστες. Το μεγαλύτερο ποσοστό ανέρχεται στο 32%, όπου οι χρήστες επιλέγουν το νούμερο 4 και 5 όπου αντιστοιχούν στο «Εύκολα» και «Πολύ Εύκολα». Χωρίς μεγάλη διαφορά, το 26% των συμμετεχόντων δηλώνει «Μέτρια» την χρήση τους, ενώ το 7% αντιμετωπίζει δυσκολίες όπως και το 3% που τα θεωρεί «Πολύ Δύσκολα» στη χρήση τους.

Γράφημα 22. Ενότητα Γ- Ερώτηση Ε



Ίδιου τύπου είναι και η επόμενη ερώτηση «Θεωρείτε ότι η χρήση τους απαιτεί ιδιαίτερη εκπαίδευση;», αυτή τη φορά όμως όχι να «τα βαθμολογήσουν» αλλά να απαντήσουν σχετικά με το εάν απαιτούν συγκεκριμένη εκπαίδευση ώστε να χρησιμοποιηθούν με σωστό τρόπο. Από το γράφημα προκύπτει με ποσοστιαία διαφορά πως το 68% των χρηστών δεν θεωρεί πως απαιτούν ιδιαίτερη εκπαίδευση, ενώ υψηλό είναι το ποσοστό αυτών που θεωρεί πως απαιτεί, το οποίο ανέρχεται στο 32%.

Γράφημα 23. Ενότητα Γ- Ερώτηση F



Στην παρακάτω ερώτηση ζητήθηκε από τους χρήστες να επιλέξουν ή και να συμπληρώσουν αυτό που θεωρούν το σημαντικότερο πλεονέκτημα των Βιομετρικών Συστημάτων «Ποιο από τα παρακάτω θεωρείτε το σημαντικότερο πλεονέκτημα για τη χρήση των βιομετρικών συστημάτων;». Επομένως, στο ακόλουθο γράφημα το μεγαλύτερο ποσοστό ανέρχεται στο 41% όπου θεωρεί πως το βασικότερο πλεονέκτημα των βιομετρικών συστημάτων είναι πως η πιθανότητα ορθής αναγνώρισης βασίζεται σε μοναδικά χαρακτηριστικά, το 26% θεωρεί σημαντικότερο την ταχύτητα με την οποία γίνεται η επαλήθευση, ενώ το 19% ότι δεν απαιτούν απομνημόνευση όπως οι κωδικού πρόσβασης. Το 11% των συμμετεχόντων θεωρεί σημαντικότερο πλεονέκτημα ότι δεν απαιτούν την χρήση κλειδιού, κάρτας ή άλλης συσκευής από τον χρήστη, ενώ το 4% την ευκολία εκμάθησης τους, Οι επιλογές που καταγράφηκαν από τους χρήστες χωρίς όμως κάποιο ιδιαίτερο ποσοστό είναι πως υπάρχει μεγαλύτερη ασφάλεια καθώς δεν

μπορεί ο καθένας να ξεκλειδώσει το κινητό του άλλου, ενώ αναφέρθηκε και η δυσκολία πρόσβασης ως σημαντικότερο πλεονέκτημα των βιομετρικών συστημάτων. Ιδιαίτερα οι γυναίκες όπως διαφαίνεται από το γράφημα 25 θεωρούν την ορθή αναγνώριση ως το σημαντικότερο πλεονέκτημα τους. Συγκεκριμένα, το

Γράφημα 24. Ενότητα Γ- Ερώτηση G

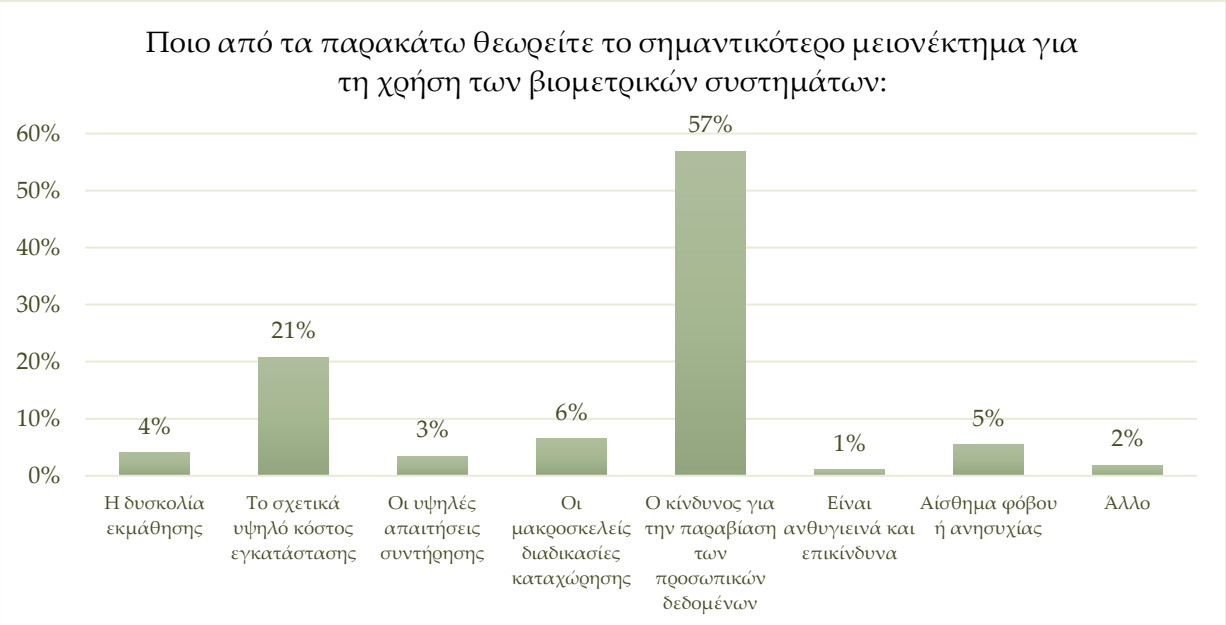
μεγαλύτερο ποσοστό ανήκει όπως αναφέρθηκε και προηγουμένως στις γυναίκες, το οποίο ανέρχεται στο 26% και θεωρούν ως σημαντικότερο πλεονέκτημα τους

Γράφημα 25. Ενότητα Γ- Ερώτηση G- Ανά Φύλο

πως η ταυτοποίηση τους από τις συσκευές βασίζεται στα μοναδικά χαρακτηριστικά του εκάστοτε ανθρώπου. Αντιστοίχως, με μικρότερο ποσοστό αλλά υψηλότερο για τους άνδρες να ανέρχεται στο 14%, θεωρούν πως η μοναδικότητα επαλήθευσης των βιομετρικών συστημάτων είναι το σημαντικότερο απ' όλα. Το 16% των γυναικών τα συγκρίνει με τους κωδικούς πρόσβασης και θεωρεί πως η ταχύτητα επαλήθευσης τους είναι σημαντική, αντίληψη που αποτυπώνεται και από το 12% των ιδίων που θεωρού πως δεν απαιτείται η απομνημόνευση του κωδικού όπως γινόταν. Τις ίδιες αντιλήψεις έχει και το ανδρικό φύλο με ποσοστά 9% και 7% αντίστοιχα με τις επιλογές των γυναικών.

Στην επόμενη ερώτηση ζητήθηκε να προσδιοριστεί το σημαντικότερο μειονέκτημα των βιομετρικών συστημάτων «Ποιο από τα παρακάτω θεωρείτε το σημαντικότερο μειονέκτημα για τη χρήση των βιομετρικών συστημάτων:».

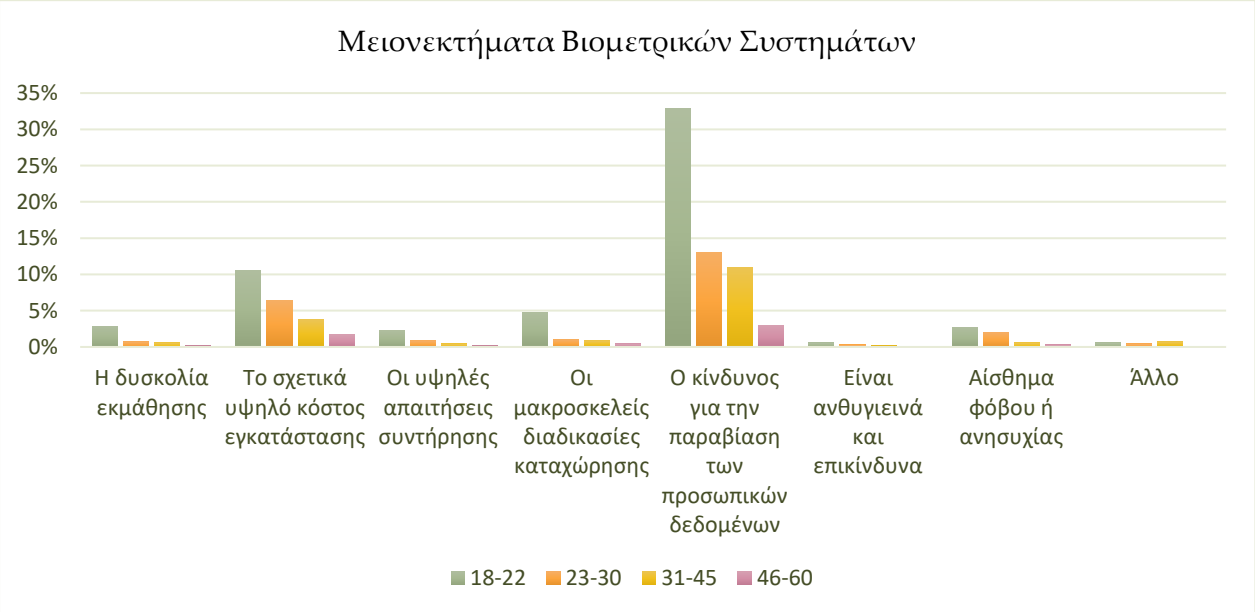
Γράφημα 26. Ενότητα Γ- Ερώτηση Η



Όπως διαφαίνεται από το παραπάνω γράφημα, το μεγαλύτερο ποσοστό ανήκει στην επιλογή «ο κίνδυνος για την παραβίαση των προσωπικών δεδομένων», το οποίο ανέρχεται στο 57%, το 21% στην επιλογή «το σχετικά υψηλό κόστος εγκατάστασης», ενώ το 6% θεωρεί σημαντικότερο μειονέκτημα τους «τις μακροσκελείς διαδικασίες καταχώρησης». Αυτό που προκαλεί εντύπωση είναι

πως ναι μεν το υψηλότερο ποσοστό τω συμμετεχόντων θεωρεί πως μέσω αυτών υπάρχει ο κίνδυνος να παραβιαστούν τα προσωπικά του δεδομένα, αλλά μόνο το 5% των χρηστών ανησυχεί και αισθάνεται φόβο. Αναλογικά με το πλήθος των υπόλοιπων επιλογών, το ποσοστό 4% αν και μικρό είναι σημαντικό γιατί θεωρεί δύσκολη την εκμάθηση των βιομετρικών συστημάτων, το 3% τις υψηλές απαιτήσεις συντήρησης, το 2% των χρηστών δηλώνει πως άλλα ως σημαντικότερα μειονεκτήματα των συστημάτων, ενώ μόλις το 1% τα βρίσκει ανθυγιεινά και επικίνδυνα για τον χρήστη. Ιδιαίτερα, όπως διαφαίνεται από το γράφημα 27, η ηλικιακή ομάδα 18-22 δηλώνει εντονότερη ανησυχία σχετικά με τον κίνδυνο της παραβίασης των προσωπικών τους δεδομένων με ποσοστό να ανέρχεται στο 33%, ενώ και οι άλλες ηλικιακές ομάδες καταγράφουν τα μεγαλύτερα ποσοστά στην επιλογή αυτή, με 13% από τους 23-30, 11% από τους 31-45 και 3% από τους 46-60. Εξίσου έντονη σε όλες τις ηλικιακές ομάδες είναι το μειονέκτημα σχετικά με τι υψηλό κόστος που απαιτούν τα βιομετρικά συστήματα για να εγκατασταθούν με ποσοστό 10% για τους 18-22, με 6% από τους 23-30, 4% από τους 31-45 και 2% από τους 46-60. Αν και δεν πρόκειται για μεγάλο ποσοστό αξίζει όμως να τονιστεί πως το 1% των χρηστών που δήλωσε άλλο ως σημαντικότερο μειονέκτημα των βιομετρικών συστημάτων, θεωρεί η μοναδικότητα του κάθε ανθρώπου είναι ένα προνόμιο που επιφέρει εφησυχασμό στους χρήστες, ενώ ταυτόχρονα υπάρχει πάντα η ανησυχία της υποκλοπής δεδομένων.

Γράφημα 27. Ενότητα Γ- Ερώτηση Η- Ανά Ηλικιακή Ομάδα

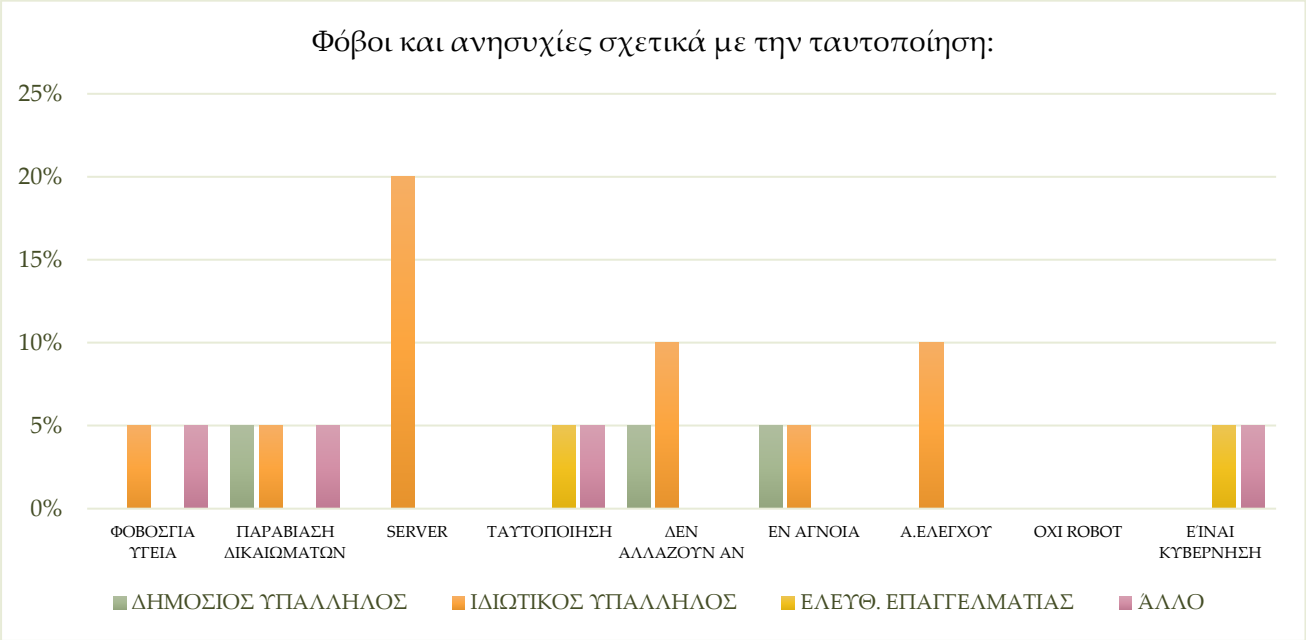


Η τελευταία ερώτηση της ενότητας αυτής αποτελεί συνέχεια της προηγούμενης: «Εάν έχετε επιλέξει στην παραπάνω ερώτηση ότι αισθάνεστε φόβο ή ανησυχία όταν ταυτοποιήστε με βάση τα βιομετρικά σας δεδομένα, παρακαλώ αιτιολογείστε.». Επί της ουσίας, η ερώτηση αυτή έπρεπε να απαντηθεί μόνο από τους χρήστες που δήλωσαν στην παραπάνω ερώτηση πως κατά τη γνώμη τους το σημαντικότερο μειονέκτημα των βιομετρικών συστημάτων είναι το αίσθημα φόβου ή ανησυχίας, καθώς κλήθηκαν να απαντήσουν σε μια ερώτηση ανοικτού τύπου για να καταγράψουν τις ανησυχίες τους αυτές. Αναλυτικότερα, από το παρακάτω γράφημα προκύπτει το μεγαλύτερο ποσοστό , το οποίο ανέρχεται στο 22% και ανήκει σε δύο επιλογές των χρηστών «καταχωρούνται σε server και εύκολα αποκτούν πρόσβαση τρίτοι» και «αποκτώνται πληροφορίες εν αγνοία των χρηστών». Πρόκειται για δύο επιλογές με το υψηλότερο ποσοστό, όπου στην πρώτη οι άνθρωποι ανησυχούν πως πιθανά τα βιομετρικά τους δεδομένα να αποθηκεύονται σε βάσεις δεδομένων στις οποίες έχουν πρόσβαση τρίτοι, επομένως κλονίζεται το κατά πόσο είναι ασφαλείς. Παρόμοια είναι και η δεύτερη υψηλότερη σε ποσοστό ανησυχία των χρηστών πως κανείς δεν τους διασφαλίζει πως δεν αποκτώνται πληροφορίες εν αγνοία τους, οι οποίες δύναται να χρησιμοποιηθούν εναντίον τους και να τους στοχοποιήσουν. Ιδιαίτερα σημαντικός είναι και ο φόβος που αποτυπώνεται μέσα από το 12% των χρηστών, που δηλώνουν πως σε αντίθεση με τους κωδικούς πρόσβασης, το αρνητικό με τα βιομετρικά συστήματα είναι πως σε περίπτωση που παραβιαστούν δεν μπορούν να αλλάξουν, ενώ το 10% των χρηστών αισθάνεται πως ανά πάσα στιγμή και ώρα ελέγχεται και πως το ίδιο πάλι ποσοστό ανησυχεί για το κατά πόσο παραμένουν στην πραγματικότητα ιδιωτικά. Υψηλό βέβαια είναι και το 6% των χρηστών, το οποίο ανησυχεί πως οι βιομετρικές τεχνικές είναι ανθυγιεινές και επικίνδυνα για τους χρήστες. Εντύπωση προκαλεί πως το 4% των χρηστών φαίνεται να εμπιστεύεται την εκάστοτε κυβέρνηση με «κλειστά» μάτια, διότι δηλώνει πως αν ελέγχεται από αυτήν δεν του δημιουργείται κανένας φόβος αφού πρόκειται για την ασφάλεια των πολιτών.

Γράφημα 28. Ενότητα Γ- Ερώτηση Ι

Ιδιαίτερα κάποια δημογραφικά στοιχεία φαίνεται να λειτουργούν ως παράγοντες διαφοροποίησης και ειδικότερά οι κατηγορίες επαγγελμάτων των φοιτητών, το επάγγελμα του πατέρα και το τμήμα φοίτησης των συμμετεχόντων-ουσών στην έρευνα. Αναλυτικότερα, από το γράφημα 29, το μεγαλύτερο ποσοστό των συμμετεχόντων-ουσών, το οποίο ανέρχεται στο 20% και προέρχεται από τους φοιτητές που εργάζονται ως ιδιωτικοί υπάλληλοι, ανησυχεί πως τα δεδομένα τους καταχωρούνται σε server και εύκολα αποκτούν πρόσβαση τρίτοι. Το πιο εντυπωσιακό είναι πως αυτή την ανησυχία την έχουν μόνο αυτοί οι φοιτητές, καθώς σκιαγραφείται ένα 0% από τα υπόλοιπα επαγγέλματα των φοιτητών. Πάλι οι ιδιωτικοί υπάλληλοι με ποσοστό 10% ανησυχούν πως σε αντίθεση με τα passwords, τα βιομετρικά δεν αλλάζουν αν παραβιαστούν, ενώ αισθάνονται πως ελέγχονται. Παρατηρώντας το γράφημα, φαίνεται πως οι φοιτητές που εργάζονται ως ελεύθεροι επαγγελματίες ανησυχούν μόνο για δύο λόγους με ποσοστό 5%, όπου ανησυχούν σχετικά με την ταυτοποίηση και μένουν ήσυχοι αν γνωρίζουν πως ελέγχονται από την εκάστοτε κυβέρνηση.

Γράφημα 29. Ενότητα Γ- Ερώτηση Ι- Ανά Κατηγορία Επαγγελμάτων Φοιτητή-τριας

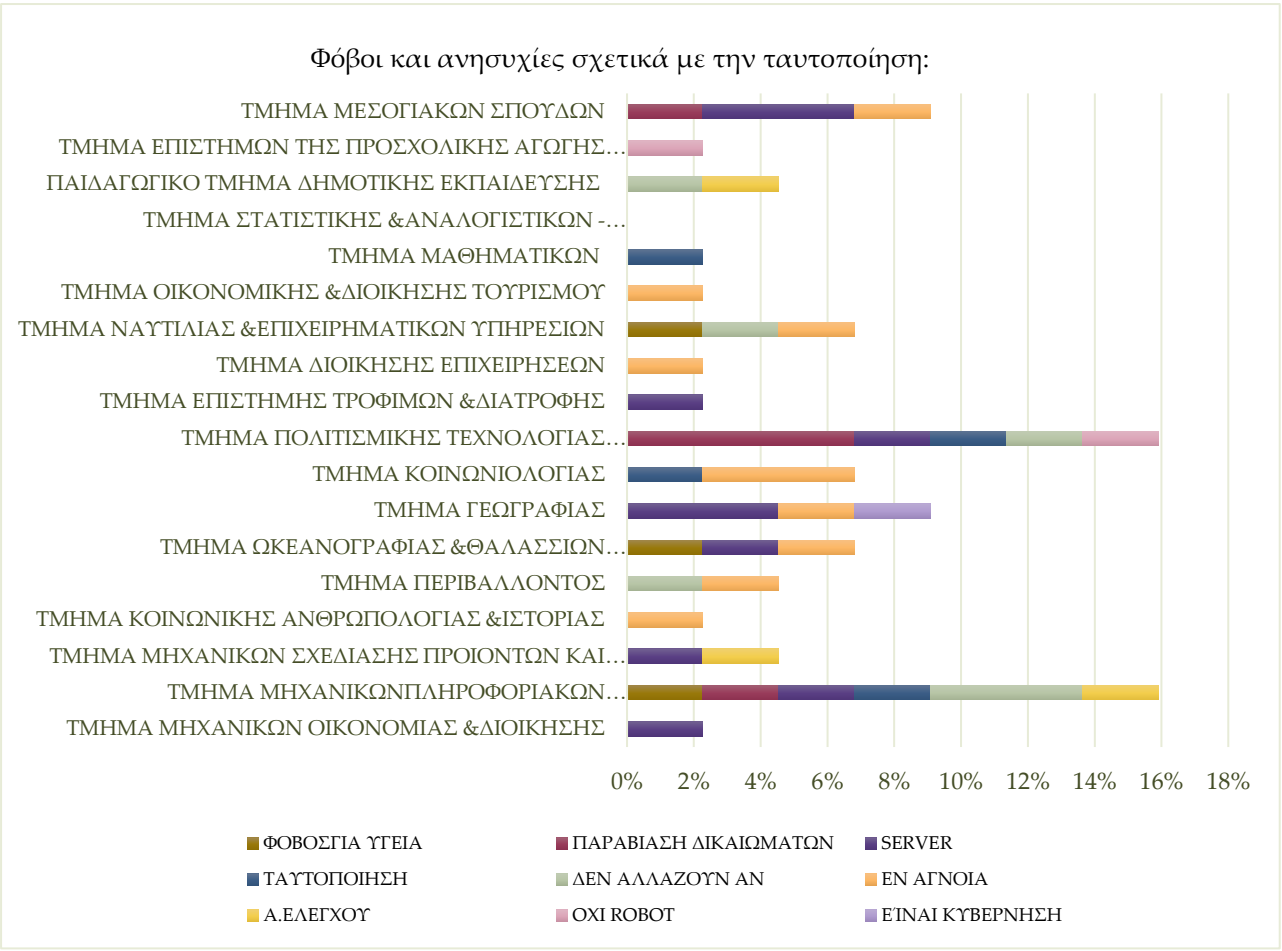


Οι φόβοι που αποτυπώνονται από τους χρήστες σχετικά με την ταυτοποίηση τους διαφέρουν από αυτούς που παρατηρήθηκαν από τους φοιτητές που εργάζονται. Ουσιαστικά, το 9% των ερωτηθέντων που ο πατέρας τους εργάζεται ως ελεύθερος επαγγελματίας δηλώνει πως ανησυχεί περισσότερο για την πιθανότητα να αποκτώνται πληροφορίες εν αγνοία των χρηστών, οι οποίοι να χρησιμοποιηθούν εις βάρος τους. Κατά κύριο λόγο οι φόβο και οι ανησυχίες που διαφαίνονται στο γράφημα δεν παρουσιάζουν ιδιαίτερες διαφορές, εκτός από το ποσοστό 7% που παρατηρείται στους φοιτητές που ο πατέρας τους εργάζεται ως δημόσιος υπάλληλος κα δηλώνουν πως ανησυχούν για την περίπτωση πως αν κάποιος κωδικός κλαπεί, μπορεί να αλλαχθεί, όμως αυτό δεν συμβαίνει και με τις βιομετρικές πληροφορίες. Το ίδιο ποσοστό από τους φοιτητές που ο πατέρας τους εργάζεται ως ελεύθερος επαγγελματίας ανησυχεί πως τα δεδομένα που καταχωρούνται σε server.

Γράφημα 30. Ενότητα Γ- Ερώτηση Ι- Ανά Επάγγελμα Πατέρα

Αναφορικά με το Τμήμα φοίτησης των συμμετεχόντων-ουσών στην έρευνα, αυτό που παρουσιάζει μεγαλύτερη σημασία για να λεχθεί είναι πως κανείς θα περίμενε τα τεχνολογικά τμήματα να ανησυχούν περισσότερο για την πιθανότητα παραβίασης των δικαιωμάτων τους. Μόνο τρία τμήματα φοβούνται πως μια τέτοια οπτική είναι πιθανό να συμβεί και συγκεκριμένα το μεγαλύτερο ποσοστό που ανησυχεί σχετικά με αυτό, ανέρχεται στο 7% και είναι φοιτητές-τριες που προέρχονται από το Τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας. Το 2% των συμμετεχόντων-ουσών προέρχεται από το Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων και από το Τμήμα Μεσογειακών Σπουδών.

Γράφημα 31. Ενότητα Γ- Ερώτηση Ι- . Ανά Τμήμα Σπουδών



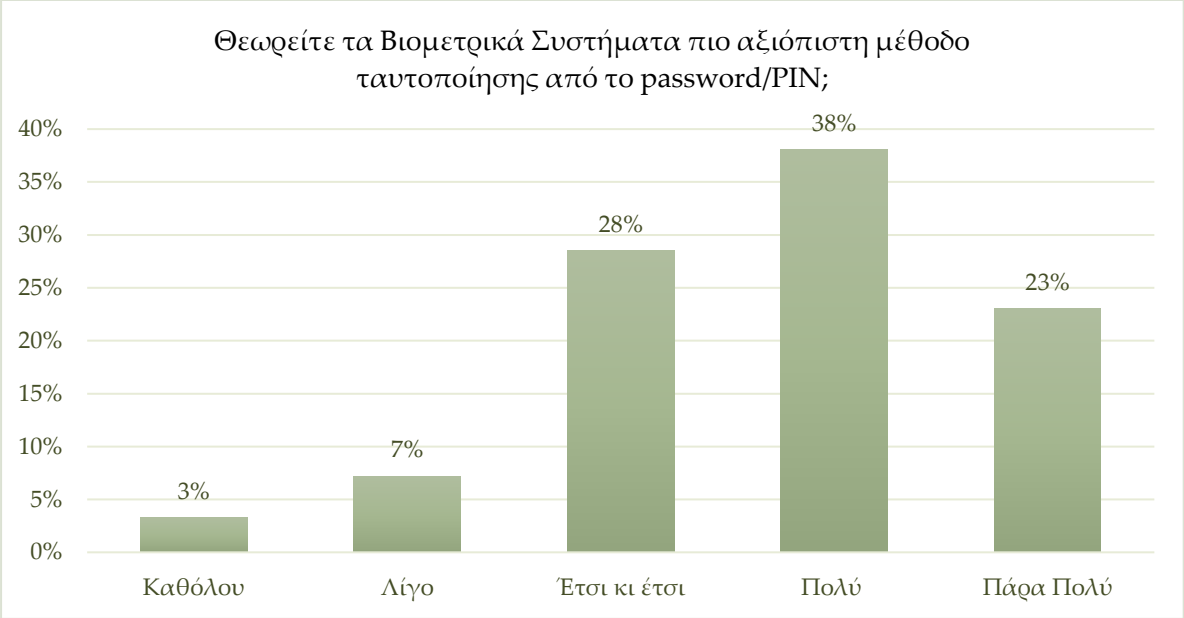
Ενότητα Δ

Η ενότητα αυτή σκιαγραφεί το κατά πόσο τα βιομετρικά συστήματα είναι αξιόπιστα. Αναλυτικότερα, οι παρακάτω ερωτήσεις που αποτελούν την ενότητα αυτή, δημιουργούν μια σαφή εικόνα αναφορικά με την εμπιστοσύνη που προάγουν τα βιομετρικά συστήματα στους χρήστες σχέση με το password ή PIN.

Η πρώτη ερώτηση της ενότητας αυτής είναι «Θεωρείτε τα Βιομετρικά Συστήματα πιο αξιόπιστη μέθοδο ταυτοποίησης από το password/PIN;». Οι συμμετέχοντες-ουσες στην προκείμενη ερώτηση κλήθηκαν να βαθμολογήσουν από το 1 έως το 5 που αντιστοιχεί από το Καθόλου έως το Πάρα Πολύ πόσο αξιόπιστα τα θεωρούν. Όπως διαφαίνεται από το παρακάτω γράφημα το μεγαλύτερο ποσοστό ανήκει στην επιλογή «Πολύ», το οποίο ανέρχεται στο 38% και δείχνει πως συγκριτικά με τους κωδικούς πρόσβασης τα θεωρούν πιο αξιόπιστη μέθοδο. Το 28% των

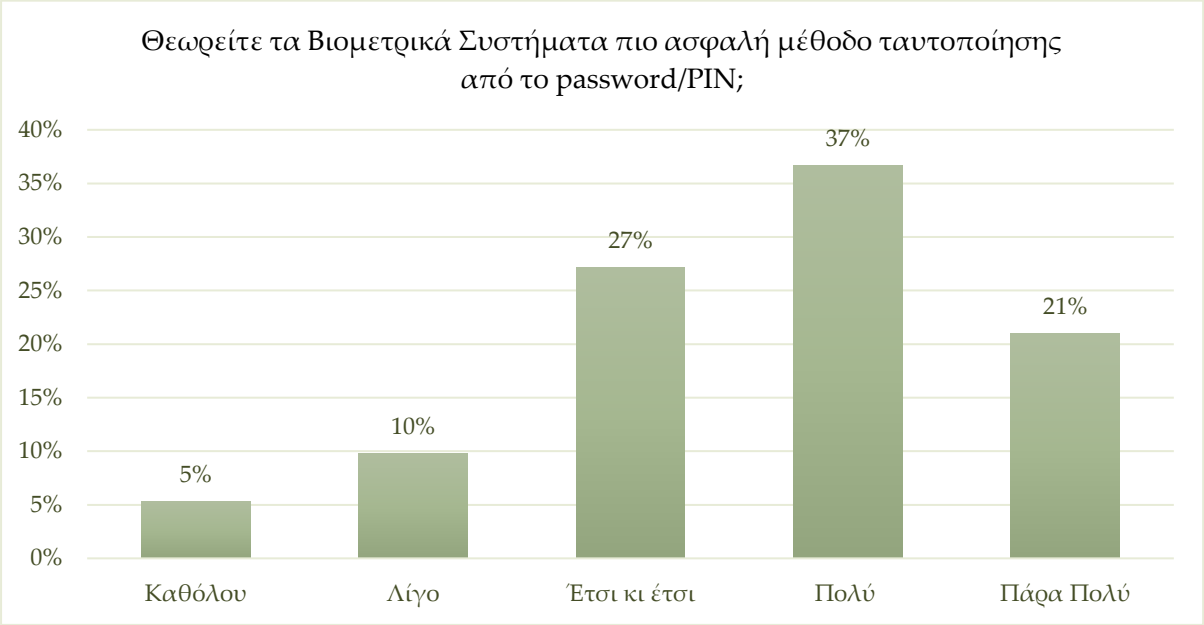
φοιτητών βρίσκεται στην μέση αυτή της ερώτησης, ενώ το 23% των συμμετεχόντων-ουσών δηλώνει «Πάρα Πολύ». Σημαντικά είναι τα χαμηλά ποσοστά των χρηστών, τα οποία δείχνουν πως οι χρήστες δεν εμπιστεύονται τόσο τους κωδικούς πρόσβασης όσο τις βιομετρικές τεχνικές και αυτό σκιαγραφείται από το 7% των φοιτητών που δηλώνει «Λίγο» και το 3% που δηλώνει «Καθόλου».

Γράφημα 32. Ενότητα Δ- Ερώτηση J



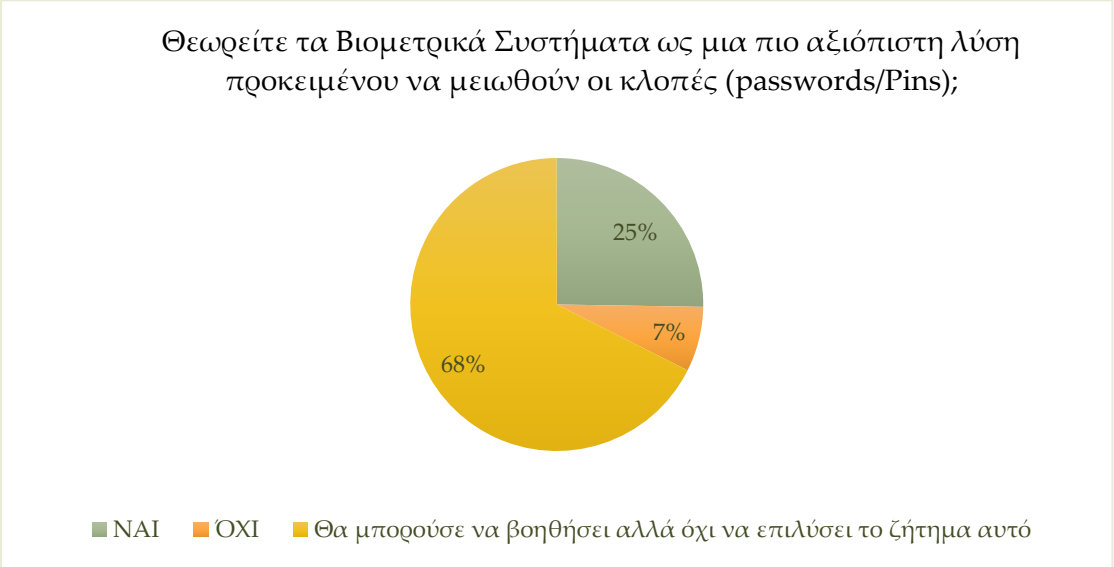
Ίδιου τύπου είναι και η επόμενη ερώτηση αλλά με διαφορετικό περιεχόμενο «Θεωρείτε τα Βιομετρικά Συστήματα πιο ασφαλή μέθοδο ταυτοποίησης από το password/PIN;», καθώς εδώ η σύγκριση αφορά την ασφάλεια και όχι την αξιοπιστία ανάμεσα τους. Με βάση και το παρακάτω γράφημα, διαφαίνεται πως τα αποτελέσματα είναι σχεδόν ίδια με την προηγούμενη ερώτηση. Αναλυτικότερα, το μεγαλύτερο ποσοστό ανήκει στην επιλογή «Πολύ», το οποίο ανέρχεται στο 37%, το 27% βρίσκεται στην μέση και δεν προσανατολίζεται περισσότερο από κάποια κατεύθυνση, το 21% δηλώνει «Πάρα Πολύ», ενώ και πάλι μικρά είναι τα ποσοστά που κατά κάποιον τρόπο «υπερασπίζονται» τους κωδικούς πρόσβασης σε σχέση με τις βιομετρικές τεχνικές, με ποσοστό 10% να δηλώνει «Λίγο» και 5% να δηλώνει «Καθόλου».

Γράφημα 33. Ενότητα Δ- Ερώτηση Κ



Η τελευταία ερώτηση της ενότητας αυτής αναφέρεται στο αν «Θεωρείτε τα Βιομετρικά Συστήματα ως μια πιο αξιόπιστη λύση προκειμένου να μειωθούν οι κλοπές (passwords/Pins);». Όπως διαφαίνεται από το παρακάτω γράφημα, το μεγαλύτερο ποσοστό των χρηστών, το οποίο ανέρχεται στο 68% δεν μπορεί να πάρει ξεκάθαρη θέση στο ερώτημα αυτό, καθώς δηλώνει πως ναι μεν θα μπορούσαν οι βιομετρικές τεχνικές να βοηθήσουν την κατάσταση αυτή, αλλά δεν γνωρίζουν αν είναι ικανές να την επιλύσουν κιόλας. Παρόλα αυτά, το 25% των χρηστών θεωρούν τα βιομετρικά συστήματα μια αξιόπιστη λύση ώστε να αποφευχθούν οι κλοπές, ενώ το 7% διαφωνεί με την προοπτική αυτή.

Γράφημα 34. Ενότητα Δ- Ερώτηση L



Ιδιαίτερα, η ηλικιακή ομάδα 18-22 με ποσοστό 40% δηλώνει πως μια τέτοια λύση μπορεί να βελτιώσει την κατάσταση αλλά δεν αρκεί για να επιλυθεί. Την άποψη αυτή φαίνεται πως υιοθετεί το μεγαλύτερο ποσοστό όλων των ηλικιακών ομάδων, με ποσοστό 23% να ανήκει στους 23-30, 9% στους 31-45 και 3% στους 46-60. Παρατηρείται από το γράφημα, πως επικρατούν χαμηλά ποσοστά των χρηστών που είναι αντίθετοι σε μια τέτοια οπτική, με χαρακτηριστικό το 0% που προέρχεται από την ηλικιακή ομάδα 46-60.

Γράφημα 35. Ενότητα Δ- Ερώτηση L- Ανά Ηλικιακή Ομάδα

Ενότητα Ε

Η ενότητα αυτή σκιαγραφεί την πρόθεση χρήσης των βιομετρικών συστημάτων. Αναλυτικότερα, οι παρακάτω ερωτήσεις που αποτελούν την ενότητα αυτή, δημιουργούν μια σαφή εικόνα αναφορικά με τις αντιλήψεις των χρηστών απέναντι σε κάποιες καίριες ερωτήσεις σχετικά με τα βιομετρικά συστήματα.

Η πρώτη ερώτηση αυτής της ενότητας είναι: «Πιστεύετε πως η χρήση των Βιομετρικών Συστημάτων μπορεί να κάνει πιο εύκολη τη καθημερινότητα σας;». Όπως διαφαίνεται από το ακόλουθο γράφημα, το 85% των συμμετεχόντων-ουσών δηλώνει πως τα βιομετρικά συστήματα έχουν καταστήσει την καθημερινότητα τους αρκετά πιο εύκολη με πριν. Αντιθέτως, το 15% βρίσκεται αντίθετο στην άποψη αυτή.

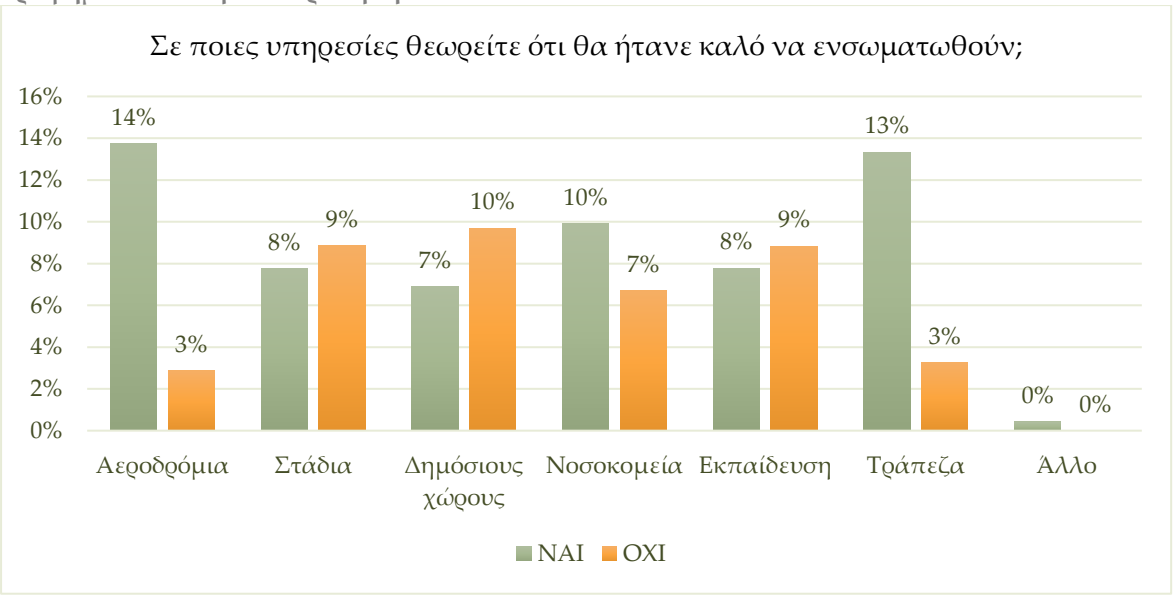
Γράφημα 36. Ενότητα Ε- Ερώτηση Μ

Το δημογραφικό στοιχείο της ηλικιακής ομάδας είναι αυτό που στην συγκεκριμένη ερώτηση αποτυπώνει μια διαφοροποίηση σε σχέση με τις υπόλοιπα δημογραφικά στοιχεία. Ουσιαστικά, όπως φαίνεται από το γράφημα, το μεγαλύτερο ποσοστό ανήκει στην ηλιακή ομάδα 18-22, το οποίο ανέρχεται στο 49%, το 19% στους 23-30, το 13% στους 31-45 και το 4% στους 46-60. Τα χαμηλά αποτελέσματα που προκύπτουν από τους χρήστες που απάντησαν «ΟΧΙ» είναι εξίσου σημαντικά με διαφορά το 2% από τους 46-60.

Γράφημα 37. Ενότητα Ε- Ερώτηση Μ- Ανά Ηλικιακή Ομάδα

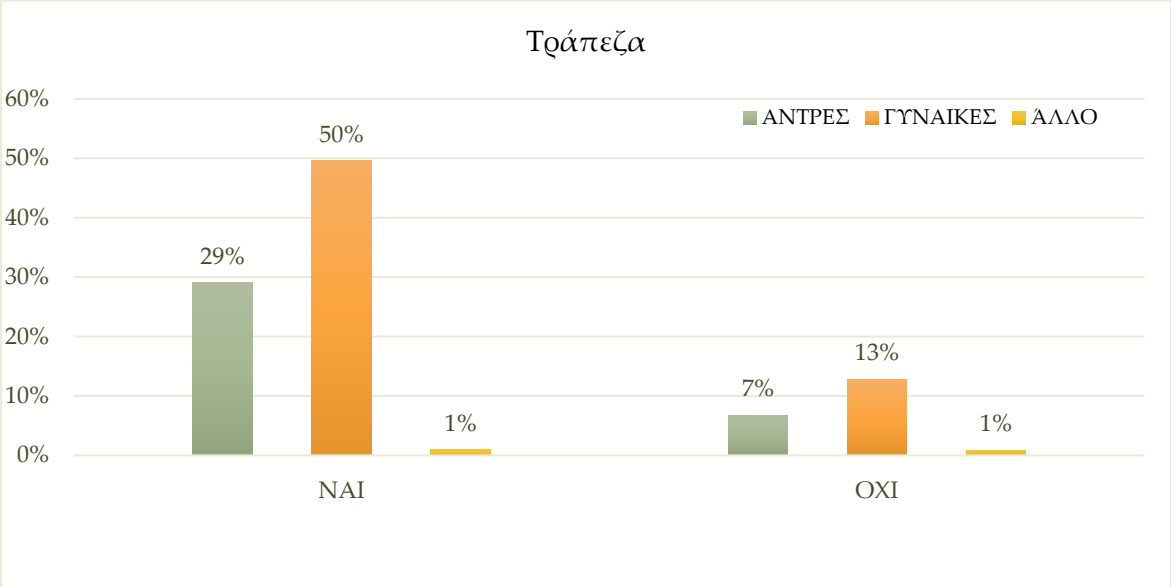
Η επόμενη ερώτηση είναι «Σε ποιες υπηρεσίες θεωρείτε ότι θα ήτανε καλό να ενσωματωθούν;». Οι χρήστες ανεξάρτητα από κάποιες συγκεκριμένες υπηρεσίες που είχαν παρατεθεί, μπορούσαν να καταγράψουν οποιαδήποτε άλλη υπηρεσία κρίνουν πως απαιτεί ενσωμάτωση των βιομετρικών συστημάτων. Αναλυτικότερα, όπως διαφαίνεται από το ακόλουθο γράφημα, τα μεγαλύτερα ποσοστά υπέρ της ενσωμάτωσης τους καταγράφονται στο αεροδρόμιο και στην τράπεζα με 14% και 13% αντίστοιχα. Το επόμενο ποσοστό είναι το 10% το οποίο δεν παρατηρείται μόνο υπέρ της ενσωμάτωσης των βιομετρικών τεχνικών στα νοσοκομεία αλλά το ίδιο ποσοστό θεωρεί πως δεν θα ήτανε καλό να ενσωματωθούν σε δημόσιους χώρους όπως και σα στάδια, με ποσοστό 9%. Κατά γενική ομολογία, οι απόψεις διίστανται ανάμεσα στους χρήστες σχετικά με το εάν είναι αναγκαία ή όχι μια τέτοια ενσωμάτωση και κατά πόσο θα μπορούσε να αλλάξει την υπάρχουσα κατάσταση.

Γράφημα 38. Ενότητα Ε- Ερώτηση Ν



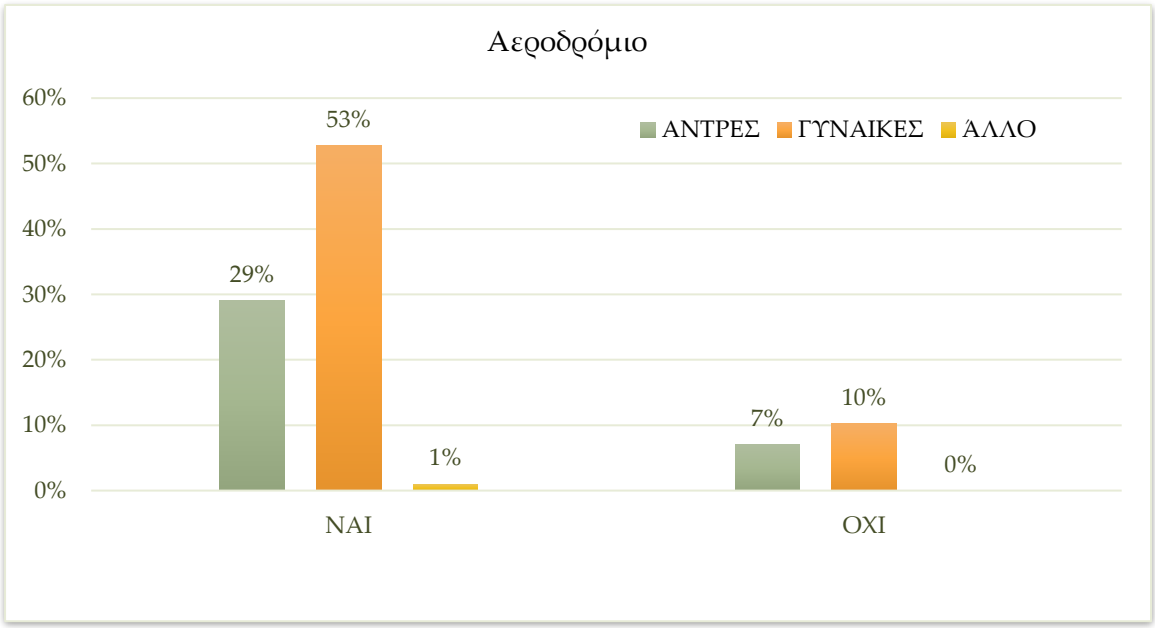
Ιδιαίτερα οι γυναίκες όπως διαφαίνεται από το ακόλουθο γράφημα, με μεγαλύτερο ποσοστό να ανέρχεται στο 50% δίνουν περισσότερη έμφαση σε μια τέτοιου είδους ενσωμάτωση, διότι πρόκειται για ασφάλεια. Θεωρούν πως μια τέτοια ενσωμάτωση απαιτείται στην τράπεζα, όπως επίσης και το ανδρικό φύλο με ποσοστό 29%. Υψηλά βέβαια είναι και τα ποσοστά όσων διαφωνούν με μια τέτοια ενσωμάτωση στην τράπεζα με 13% από τους γυναίκες και 7% από τους άνδρες, Οι χρήστες που δήλωσαν ως φύλο την επιλογή άλλο, είναι χωρισμένοι καθώς το 1% είναι υπέρ και το άλλο είναι κατά ως προς την τράπεζα.

Γράφημα 39. Ενότητα Ε- Ερώτηση Ν-Ανά Φύλο



Παράλληλα, σχεδόν ίδιες ποσοστιαίες διαφορές προκύπτουν σχετικά με την αναγκαιότητα ενσωμάτωσης τους στο αεροδρόμιο. Διαφαίνεται από το γράφημα 40 πως το 53% των γυναικών κρίνει αναγκαία μια τέτοια ενσωμάτωση καθώς τίθεται θέμα ασφάλειας λόγω του πληθυσμού που συνωστίζεται στο αεροδρόμιο. Υπέρ της ενσωμάτωσης στο αεροδρόμιο είναι και το ανδρικό φύλο με ποσοστό 29%

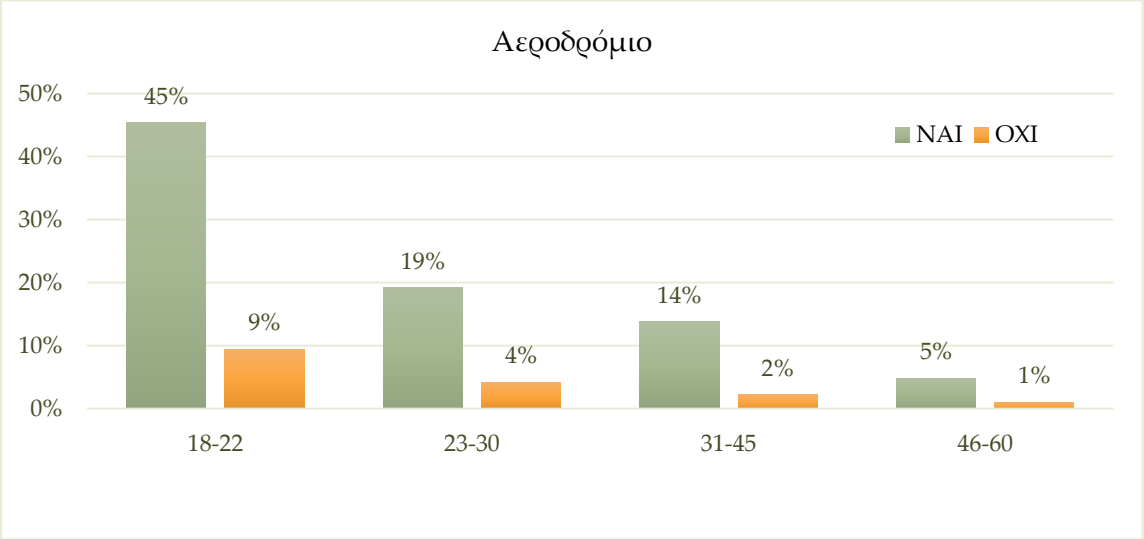
Γράφημα 40. Ενότητα Ε- Ερώτηση Ν-Ανά Φύλο



και όσοι δήλωσαν άλλο με ποσοστό 1%. Ταυτόχρονα, δεν παύουν τα ποσοστά που είναι κατά αυτή της αναγκαιότητας να είναι υψηλά με ποσοστό 10% στις γυναίκες και 7% στους άνδρες. Ανεξάρτητα από το φύλο, παρατηρείται πως και η ηλικιακή

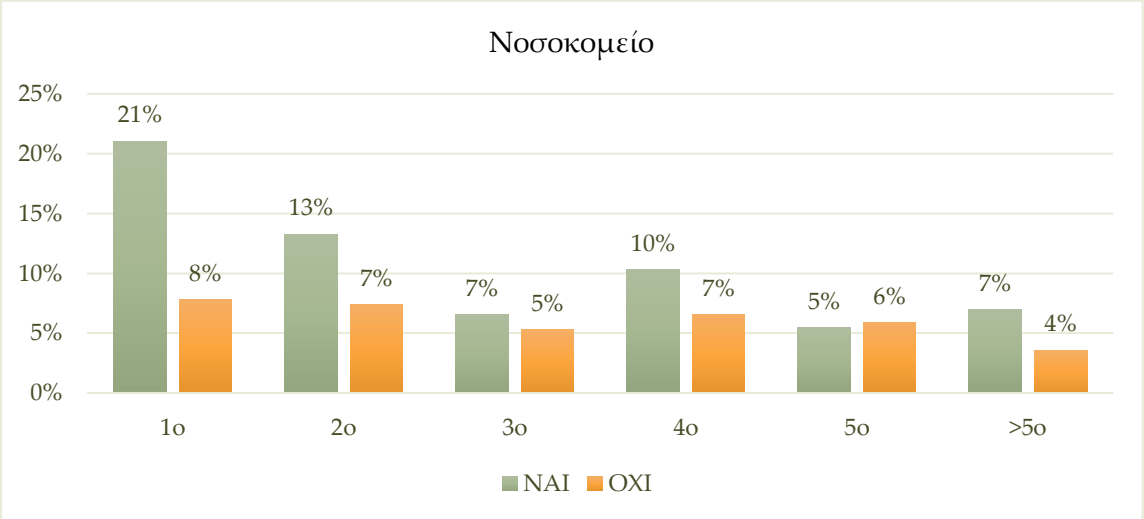
ομάδα των 18-22, με ποσοστό 45%,κρίνει αναγκαία την ενσωμάτωση τους από τις υπηρεσίες του αεροδρομίου προκειμένου να αυξηθούν τα μέτρα ασφαλείας προς τους επιβάτες και το προσωπικό. Σύμφωνοι στην οπτική αυτή με 19% είναι και ηλικιακή ομάδα 23-30, με 14% και οι 31-45 όπως και οι 46-60 με ποσοστό 5%.

Γράφημα 41. Ενότητα Ε- Ερώτηση Ν-Ανά Ηλικιακή Ομάδα



Τέλος, την σπουδαιότητας της ενσωμάτωσης τους έρχεται να υπογραμμίσει και οι φοιτητές του πρώτου έτους με ποσοστό να ανέρχεται στο 21% κρίνοντας απαραίτητο το νοσοκομείο να υιοθετήσει τις βιομετρικές τεχνικές. Με ποσοστό 13% οι φοιτητές του δεύτερου έτους τάσσονται υπέρ της ενσωμάτωσης αυτής στις

Γράφημα 42. Ενότητα Ε- Ερώτηση Ν- Ανά Έτος Σπουδών Προπτυχιακών Φοιτητών



υπηρεσίες υγείας. Αρκετά ποσοστά αντιδρούν σε μια τέτοια μελλοντική ενσωμάτωση.

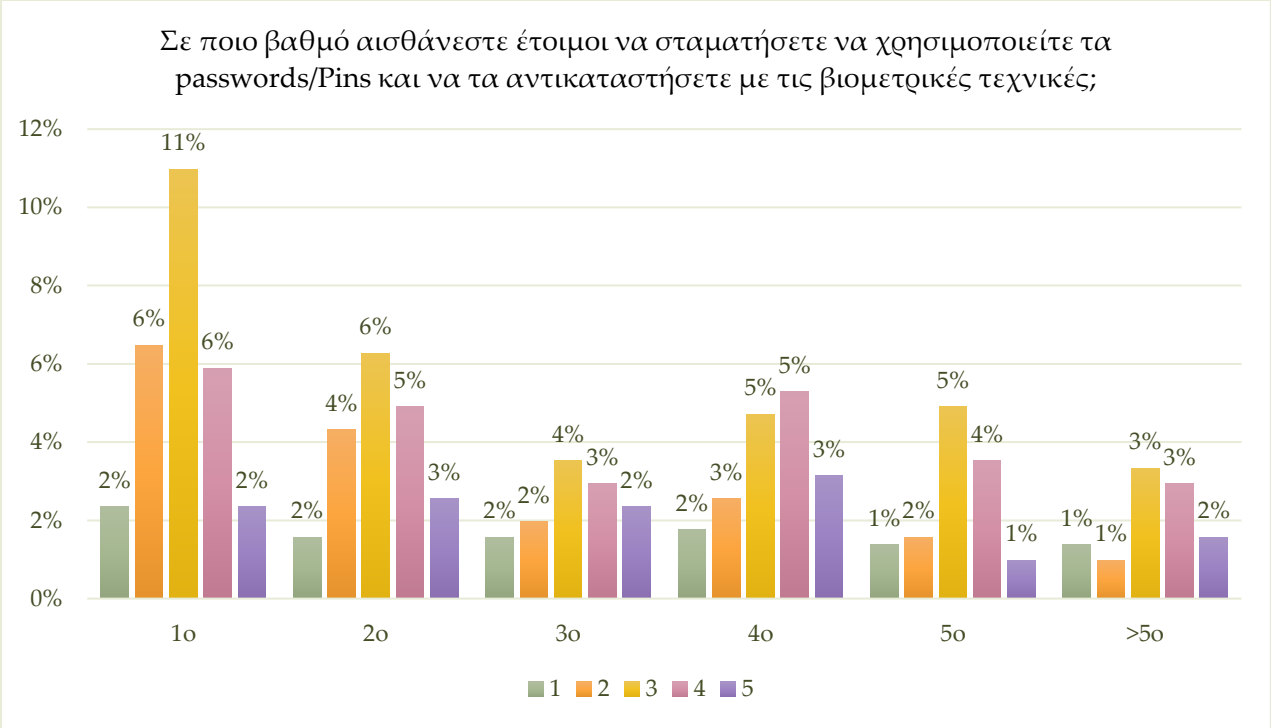
Μορφολογικά, η επόμενη ερώτηση «Σε ποιο βαθμό αισθάνεστε έτοιμοι να σταματήσετε να χρησιμοποιείτε τα passwords/Pins και να τα αντικαταστήσετε με τις βιομετρικές τεχνικές;» έχει παρουσιαστεί και παραπάνω, καθώς οι συμμετέχοντες-ουσες καλούνται να «βαθμολογήσουν» την άποψη τους. Επομένως, από το παρακάτω γράφημα διαφαίνεται πως το μεγαλύτερο ποσοστό των χρηστών δεν τάσσεται ούτε υπέρ αλλά ούτε και κατά μιας τέτοιας αντικατάστασης. Βρίσκεται ουσιαστικά στην μέση, με ποσοστό 31%, ενώ το 24% των χρηστών αισθάνεται αρκετά έτοιμο σε μια πιθανή αντικατάσταση. Παρόλα αυτά, η άγνοια των χρηστών αποτυπώνεται καλύτερα στα δύο αυτά ποσοστά, όπου αν και κοντά, το 17% δεν αισθάνεται σχεδόν καθόλου έτοιμο για μια τέτοια ανταλλαγή, ενώ το 16% δηλώνει «Πάρα Πολύ» έτοιμο για την μόνιμη αντικατάσταση τους. Την σύνθετη αυτή κατάσταση έρχεται να συμπληρώσει το 12% των χρηστών το οποίο είναι ενάντια σε μια τέτοια διαφοροποίηση.

Γράφημα 43. Ενότητα Ε- Ερώτηση Ο

Την περίπλοκη αυτή ερώτηση συμπληρώνει το έτος σπουδών των προπτυχιακών φοιτητών-τριών. Συγκεκριμένα, αν και απ' όλα τα έτη σκιαγραφείται μια ενδιάμεση άποψη επί του θέματος, με μεγαλύτερο ποσοστό το 11% από τους πρωτοετείς φοιτητές. Μια ίσως πιο ξεκάθαρη αντίληψη σχετικά με την αντικατάσταση αυτή φαίνεται να έχουν οι φοιτητές που διανύουν το πέμπτο έτος

σπουδών τους, όπου με ποσοστό 5% το οποίο αντιστοιχεί στην επιλογή «Πολύ», να δηλώνει μια θετική διάθεση απέναντι στην ανανέωση αυτή. Βέβαια, υπάρχει το 5% που βρίσκονται σε μια ενδιάμεση κατάσταση σχετικά με το θέμα αυτό.

Γράφημα 43. Ενότητα Ε- Ερώτηση Ο-Ανά Έτος Σπουδών Προπτυχιακών Φοιτητών

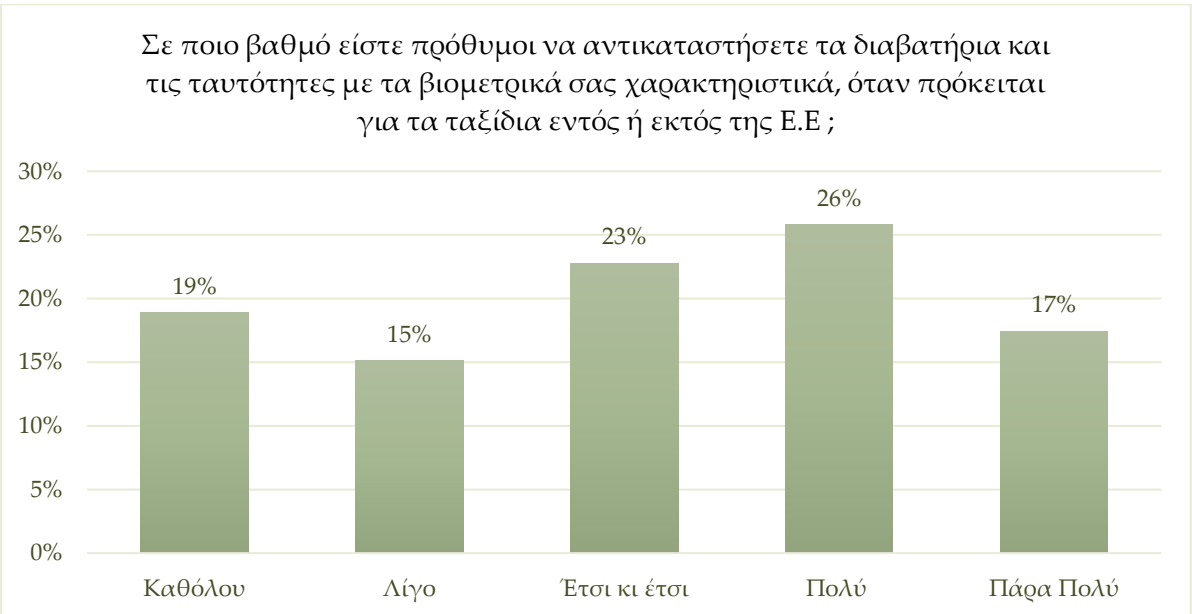


Η επόμενη ερώτηση «Σε ποιο βαθμό είστε πρόθυμοι να υιοθετήσετε τη βιομετρική ταυτότητα για τις ηλεκτρονικές τραπεζικές σας συναλλαγές;» βρίσκει τους χρήστες πάλι μπερδεμένους. Συγκεκριμένα, το μεγαλύτερο ποσοστό ανέρχεται στο 24% και ανήκει στους συμμετέχοντες που δηλώνουν «Έτσι κι Έτσι» και «Πολύ». Το θετικό πρόσημο προς την υιοθέτηση της βιομετρικής ταυτότητας για τις ηλεκτρονικές τραπεζικές συναλλαγές, έρχεται να συμπληρώσει το 20% των χρηστών που δηλώνουν «Πάρα Πολύ» πρόθυμοι-ες μπροστά σε μια τέτοια υιοθέτηση. Αντιθέτως, στο 16% ανήκουν δύο επιλογές των χρηστών «Λίγο» και «Καθόλου», ποσοστά εξίσου υψηλά που εναντιώνονται σε μια τέτοια υιοθέτηση.

Γράφημα 44. Ενότητα Ε- Ερώτηση P

Παρόμοια ως προς την μορφή είναι και η ακόλουθη ερώτηση «Σε ποιο βαθμό είστε πρόθυμοι να αντικαταστήσετε τα διαβατήρια και τις ταυτότητες με τα βιομετρικά σας χαρακτηριστικά, όταν πρόκειται για τα ταξίδια εντός ή εκτός της Ε.Ε ;». Σε αντίθεση με τα δύο προηγούμενα γραφήματα, στο παρακάτω διαφαίνεται μια πιο ξεκάθαρη κατεύθυνση των χρηστών. Ιδιαίτερα, το μεγαλύτερο ποσοστό καταγράφεται για την επιλογή «Πολύ», το οποίο ανέρχεται στο 26%, ενώ το 23% των χρηστών φαίνεται να αμφιταλαντεύεται για το αν είναι διατεθειμένο να μοιραστεί τα βιομετρικά του δεδομένα για ταξίδια εντός ή εκτός της Ε.Ε. Το 19%

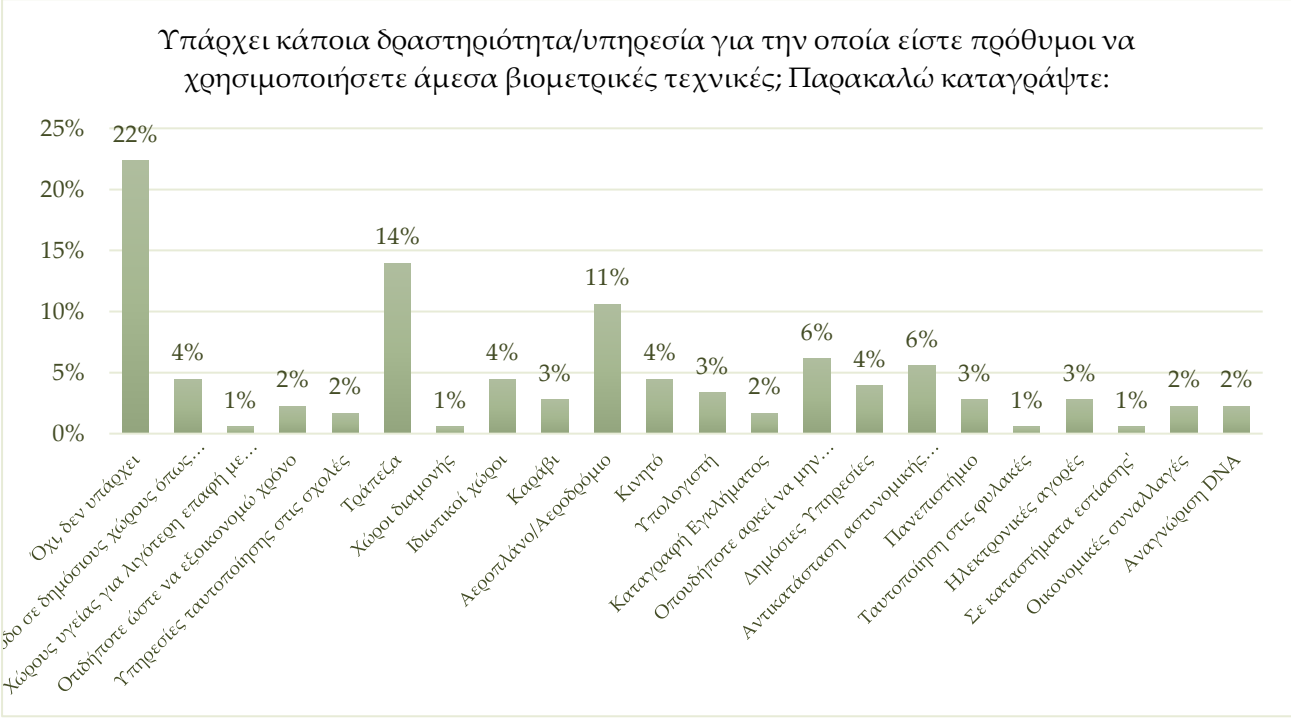
Γράφημα 45. Ενότητα Ε- Ερώτηση Q



των χρηστών δηλώνει πως δεν είναι «Καθόλου» πρόθυμο να μοιραστεί τις βιομετρικές τους πληροφορίες προκειμένου να αυξηθεί το επίπεδο ασφάλειας του στο αεροδρόμιο, ενώ το 17% δηλώνει «Πάρα Πολύ» έτοιμο ώστε να διασφαλιστεί σε μεγαλύτερο βαθμό η ασφάλεια του κατά το ταξίδι.

Η τελευταία ερώτηση της παρούσας ενότητας, αποτελεί συνέχεια της προηγούμενη, καθώς ζητείται από τους χρήστες εάν «Υπάρχει κάποια δραστηριότητα/υπηρεσία για την οποία είστε πρόθυμοι να χρησιμοποιήσετε άμεσα βιομετρικές τεχνικές; Παρακαλώ καταγράψτε:». Όπως προκύπτει από το παρακάτω γράφημα το μεγαλύτερο ποσοστό των συμμετεχόντων, το οποίο ανέρχεται στο 22%, δηλώνει πως δεν υπάρχει κάποια δραστηριότητα για την οποία θα ήταν πρόθυμοι να χρησιμοποιήσουν άμεσα τις βιομετρικές τεχνικές. Το 14% των χρηστών δηλώνει πως στις υπηρεσίες της τράπεζας θα ήτανε πρόθυμο να τις υιοθετήσει άμεσα όπως ακριβώς και στο αεροδρόμιο/αεροπλάνο με ποσοστό 11%. Σημαντικό είναι και το 6% των χρηστών που δηλώνει πως θα ήτανε πρόθυμο να το υιοθετήσει οπουδήποτε αρκεί να εξοικονομεί χρόνο, ενώ πάλι το 6% είναι πρόθυμο να αντικαταστήσει άμεσα την αστυνομική του ταυτότητα ή τις πιστωτικές του κάρτες.

Γράφημα 46. Ενότητα Ε- Ερώτηση R



Ενότητα ΣΤ

Η ενότητα αυτή σκιαγραφεί την προστασία της ιδιωτικότητας (privacy) και της ασφάλειας (security).Αναλυτικότερα, οι παρακάτω ερωτήσεις που αποτελούν την ενότητα αυτή, δημιουργούν μια σαφή εικόνα αναφορικά με τις αντιλήψεις των χρηστών περί ασφάλειας, απειλών και διασφάλισης της.

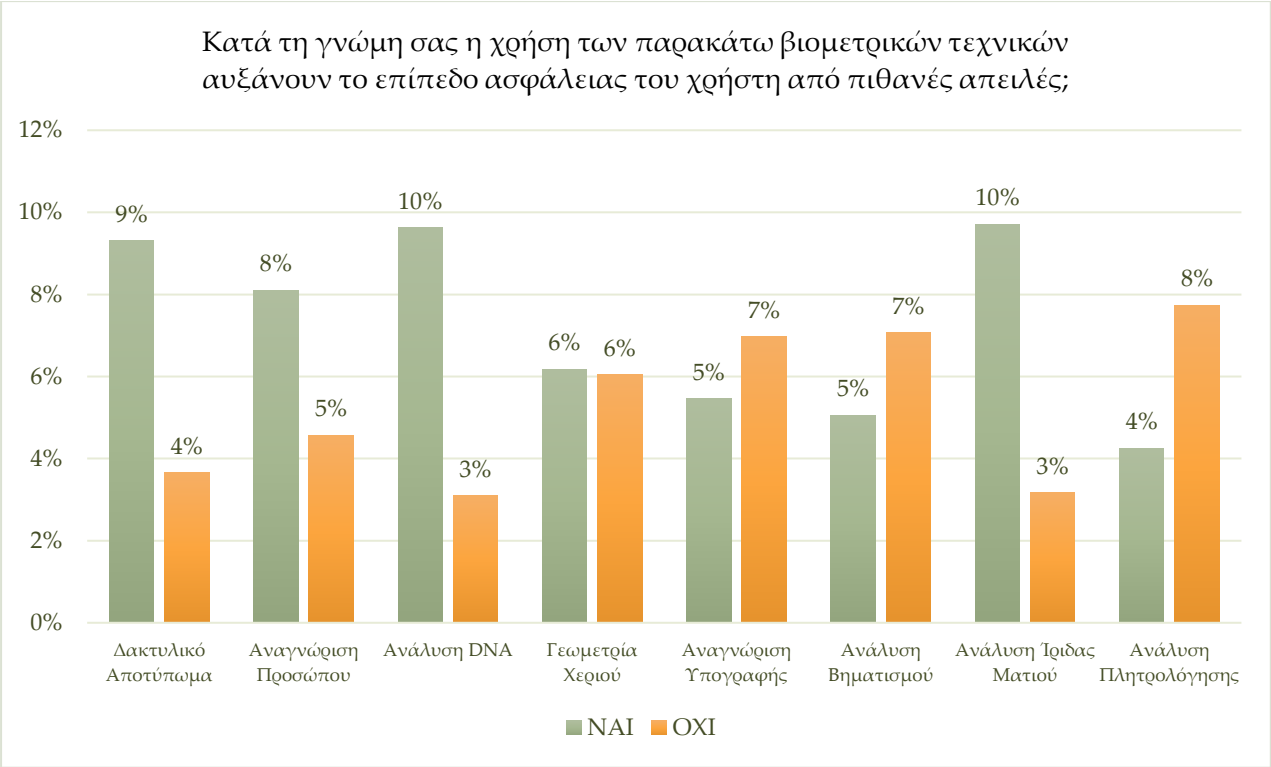
Η πρώτη ερώτηση αυτής της ενότητας είναι: «Κατά τη γνώμη σας η χρήση των παρακάτω βιομετρικών τεχνικών δεν αυξάνουν τον κίνδυνο παραβίασης της ιδιωτικότητας;». Όπως διαφαίνεται από το παρακάτω γράφημα, τα ποσοστά και στην επιλογή του «ΝΑΙ» και του «ΟΧΙ» είναι ακριβώς τα ίδια. Μεγαλύτερο είναι το ποσοστό 7%, το οποίο επί της ουσίας σύμφωνα με τους χρήστες όλες οι βιομετρικές τεχνικές αυξάνουν τον κίνδυνο παραβίασης της ιδιωτικότητας, ενώ το 6% όλων των βιομετρικών τεχνικών αντιτάσσεται στην οπτική αυτή.

Γράφημα 47. Ενότητα ΣΤ- Ερώτηση S

Ίδια ως προς την μορφή αλλά με διαφορετικό περιεχόμενο είναι και η ακόλουθη ερώτηση «Κατά τη γνώμη σας η χρήση των παρακάτω βιομετρικών τεχνικών αυξάνουν το επίπεδο ασφάλειας του χρήστη από πιθανές απειλές;». Σε αντίθεση με την αύξηση των κινδύνων της παραβίασης της ιδιωτικότητας, τα ποσοστά της

παρούσας ερώτησης είναι πιο ξεκάθαρα. Αναλυτικότερα, το μεγαλύτερο ποσοστό ανέρχεται στο 10% και ανήκει στην ανάλυση DNA και την ανάλυση της ίριδας του ματιού, όπου κατά τη γνώμη των χρηστών οι τεχνικές αυτές αυξάνουν το επίπεδο ασφάλειας περισσότερο συγκριτικά με τις υπόλοιπες, ενώ το 9% θεωρεί πως και το δακτυλικό αποτύπωμα συγκαταλέγεται στις τεχνικές αυτές που προασπίζουν την ασφάλεια των δεδομένων από πιθανές απειλές. Αντιθέτως, από τις βιομετρικές τεχνικές που δεν αυξάνουν το επίπεδο ασφάλειας απέναντι στις απειλές, με ποσοστό 8% είναι η ανάλυση πληκτρολόγησης και μ 7% η αναγνώριση υπογραφής και η ανάλυση βηματισμού.

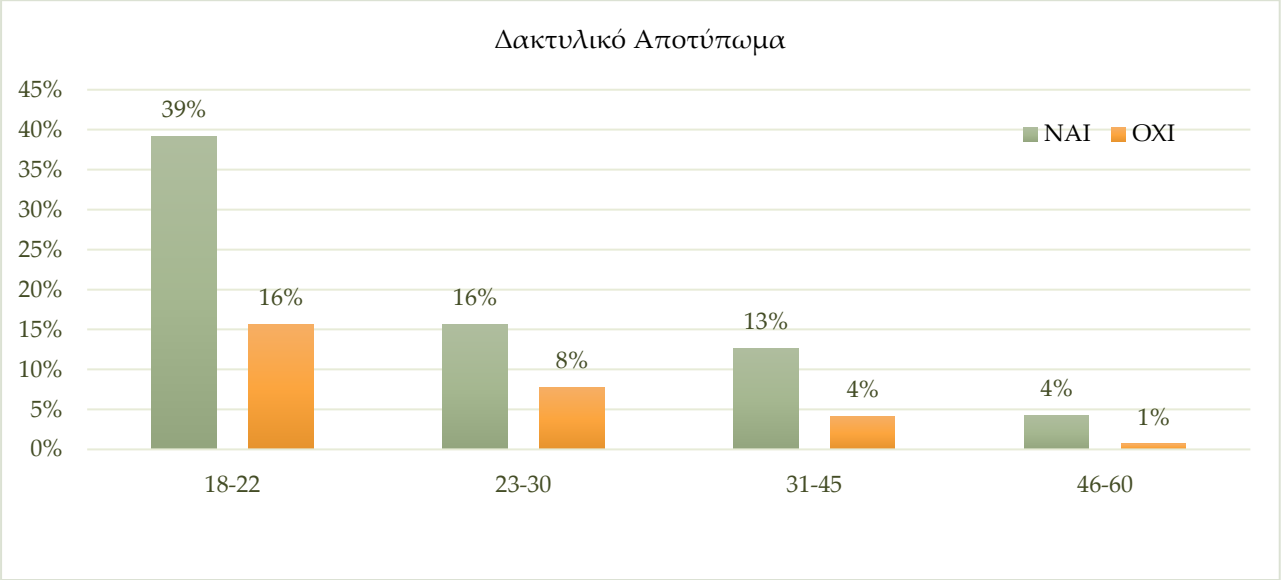
Γράφημα 48. Ενότητα ΣΤ- Ερώτηση Τ



Ιδιαίτερα, η ηλικιακή ομάδα 18-22 με ποσοστό 39% θεωρεί πως η χρήση της βιομετρικής τεχνικής του δακτυλικού αποτυπώματος, δημιουργεί στους χρήστες την πεποίθηση ότι αυξάνεται το επίπεδο ασφαλείας από πιθανές απειλές, σε αντίθεση με τις υπόλοιπες τεχνικές των βιομετρικών συστημάτων. Οι υπόλοιπες ηλικιακές ομάδες έχουν ακριβώς την ίδια αντίληψη σχετικά με το δακτυλικό αποτύπωμα, με ποσοστό 16% να ανήκει στους 23-30, 13% στους 31-45 και 4% στους 46-60. Ταυτόχρονα, παρατηρούνται και υψηλά ποσοστά που θωρούν πως το

δακτυλικό αποτύπωμα δεν αποτρέπει τις απειλές, με μεγαλύτερο ποσοστό να καταγράφεται από την ηλικιακή ομάδα 18-22 και να ανέρχεται στο 16%. Αξίζει να σημειωθεί πως από το πλήθος των δημογραφικών στοιχείων, μόνο από την ηλικιακή ομάδα δύναται να προκύψουν τέτοιες διαφοροποιήσεις.

Γράφημα 49. Ενότητα ΣΤ- Ερώτηση Τ-Ανά Ηλικιακή Ομάδα

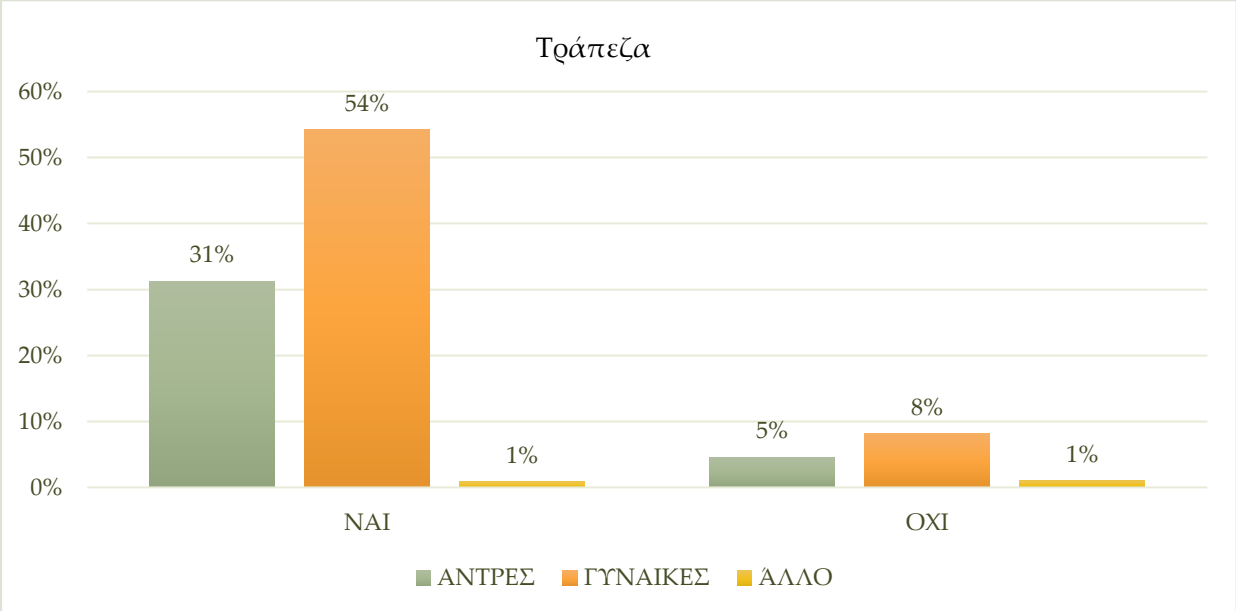


Η τελευταία ερώτηση της ενότητας αυτής ζητά από τους χρήστες με βάση την γνώμη τους να αναφέρουν «Ποιες υπηρεσίες/οργανισμοί πιστεύετε ότι χρησιμοποιούν ισχυρές μεθόδους ασφάλειας και προστασίας της ταυτότητας σας:». Ουσιαστικά, το μεγαλύτερο ποσοστό προέρχεται από τους δημόσιους χώρους, το οποίο ανέρχεται στο 16% και πρόκειται με βάση τους χρήστες για την υπηρεσία που δεν χρησιμοποιούνται ισχυρές μέθοδοι προστασίας της ταυτότητας. Η πλειοψηφία των υψηλότερων ποσοστών δεν δημιουργεί ασφάλεια στους χρήστες, με ποσοστό 12% να ανήκει στις εταιρίες κινητής τηλεφωνίας, στις υπηρεσίες υγείας και 11% στις αεροπορικές εταιρίες. Αντιθέτως, το 14% των ερωτηθέντων βρίσκει τις τράπεζες να χρησιμοποιούν ισχυρές μεθόδους ασφάλειας και προστασίας της ταυτότητας των χρηστών της. Μόλις το 2% πιστεύει πως η τράπεζα δεν χρησιμοποιεί ισχυρές μεθόδους προστασίας.

Γράφημα 50. Ενότητα ΣΤ- Ερώτηση U

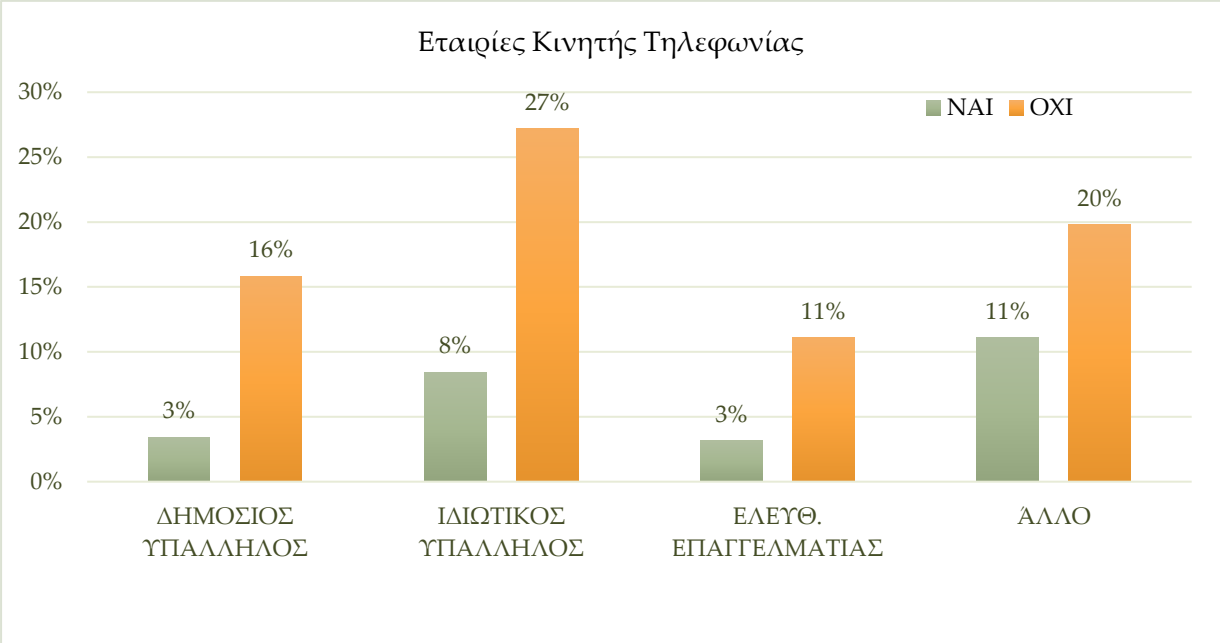
Ιδιαίτερα οι γυναίκες με υψηλότερο ποσοστό να ανέρχεται στο 54%, θεωρούν πως οι τράπεζες έχουν συγκριτικά με τις υπόλοιπες βιομετρικές τεχνικές πιο ισχυρές μεθόδους ασφάλειας και προστασίας της ταυτότητας του χρήστη. Υψηλό είναι και το ποσοστό των ανδρών, το οποίο ανέρχεται στο 31%, ενώ οι χρήστες που δηλώνουν άλλο βρίσκονται στη μέση καθώς το 1% θεωρεί πως χρησιμοποιούν ενώ το άλλο πως δεν είναι τόσο ισχυρές μέθοδοι.

Γράφημα 51. Ενότητα ΣΤ- Ερώτηση U-Ανά Φύλο



Η ερώτηση αυτή περί ισχυρών μεθόδων δημιουργεί περισσότερους χρήστες αντίθετους, όπως ακριβώς και στο παρακάτω γράφημα. Η εταιρίες κινητής τηλεφωνίας όπως είδαμε από το συνολικό γράφημα, ανήκουν στις υπηρεσίες που οι χρήστες θεωρούν πως δεν χρησιμοποιούνται ισχυρές μέθοδοι ασφάλειας και προστασίας της ταυτότητας του χρήστη. Ειδικότερα, το υψηλότερο ποσοστό ανέρχεται στο 27% και προέρχεται από τους φοιτητές που εργάζονται ως ιδιωτικοί υπάλληλοι και απαντούν «ΟΧΙ». Όλες οι κατηγορίες επαγγελμάτων φοιτητών δεν θεωρούν πως διασφαλίζεται η ασφάλεια τους και συγκεκριμένα, οι δημόσιοι υπάλληλοι με ποσοστό 16%, οι ελεύθεροι επαγγελματίες με 11% και όσοι δηλώνουν άλλο με 20%. Ταυτόχρονα, παρατηρείται και ένα ποσοστό 11% από τους φοιτητές που εργάζονται ως άλλο, οι οποίοι θεωρούν πως οι εταιρίες κινητής τηλεφωνίας χρησιμοποιούν ισχυρές μεθόδους ασφαλείας και προστασίας της ιδιωτικότητας των πελατών τους.

Γράφημα 52. Ενότητα ΣΤ- Ερώτηση U-Ανά Κατηγορία Επαγγελμάτων Φοιτητή-τριας



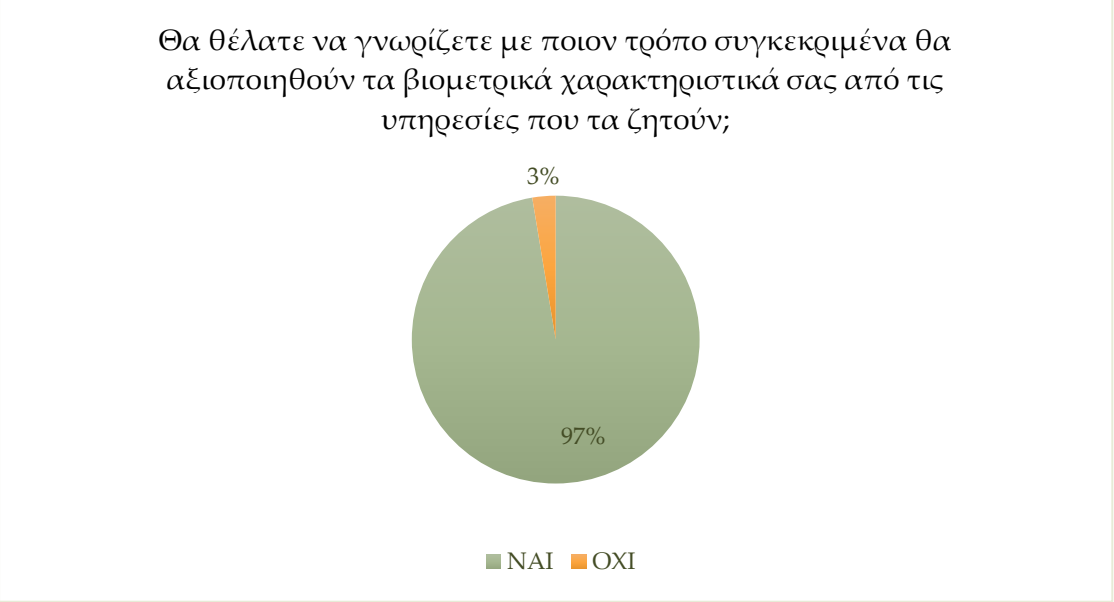
<u>Ενότητα Ζ</u>

Η ενότητα αυτή σκιαγραφεί την εμπιστοσύνη και τον κοινωνικό έλεγχο των βιομετρικών συστημάτων στους χρήστες.

Η πρώτη ερώτηση αυτής της ενότητας είναι: «Θα θέλατε να γνωρίζετε με ποιον τρόπο συγκεκριμένα θα αξιοποιηθούν τα βιομετρικά χαρακτηριστικά σας από τις υπηρεσίες που τα ζητούν;». Παρατηρώντας το παρακάτω γράφημα, διαφαίνεται

ίσως η μεγαλύτερη ποσοστιαία διαφορά σε μια ερώτηση, όπου το 97% των χρηστών δηλώνει να θα ήθελε να γνωρίζει πως θα αξιοποιηθούν οι βιομετρικές του πληροφορίες, ενώ μόνο το 3% αδιαφορεί σχετικά με αυτό. Ιδιαίτερα, η ανάγκη

Γράφημα 53. Ενότητα Z- Ερώτηση V

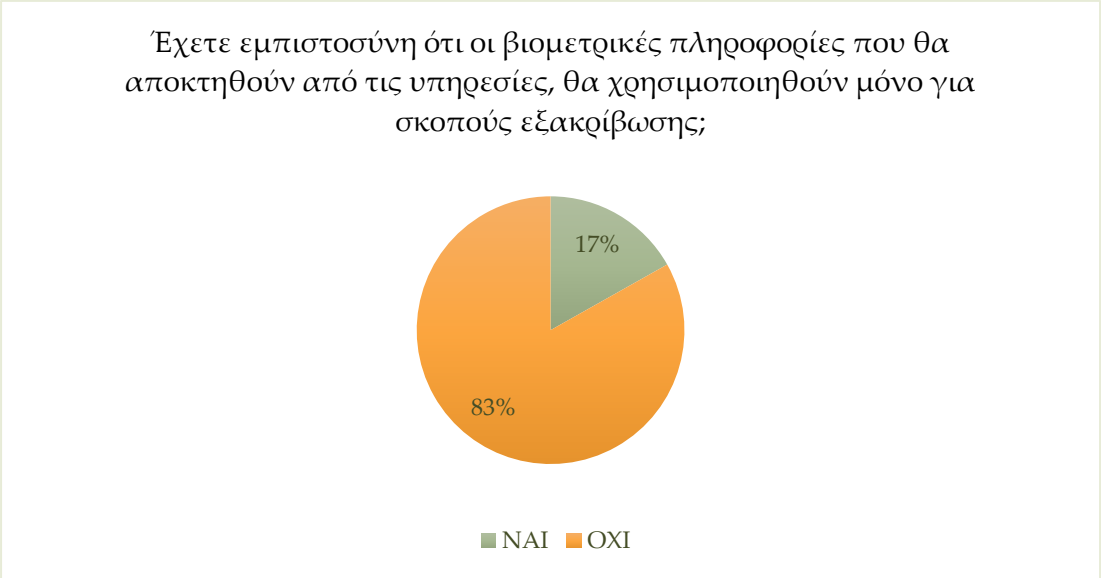


αυτή αποτυπώνεται πιο έντονα στο γυναικείο φύλο, όπου το 61% των γυναικών δηλώνει πως θα ήθελε οπωσδήποτε να γνωρίζει τις περαιτέρω διαδικασίες μετά την απόκτηση των βιομετρικών τους πληροφοριών από τις υπηρεσίες, ενώ το 34% παρουσιάζει την ανάγκη αυτή. Όπως και στο συνολικό γράφημα, έτσι και εδώ μόνο το 4% του φύλου αμεροληπτεί για την μετέπειτα αποθήκευση των βιομετρικών του πληροφοριών.

Γράφημα 54. Ενότητα Z- Ερώτηση V-Ανά Φύλο

Το ακόλουθο γράφημα απαντά στην επόμενη ερώτηση σχετικά με το αν «Έχετε εμπιστοσύνη ότι οι βιομετρικές πληροφορίες που θα αποκτηθούν από τις υπηρεσίες, θα χρησιμοποιηθούν μόνο για σκοπούς εξακρίβωσης;». Παρατηρείται όπως και προηγουμένως μια εξαιρετικά μεγάλη διαφορά ανάμεσα στους χρήστες που εμπιστεύονται και δεν εμπιστεύονται ότι οι βιομετρικές τους πληροφορίες δεν θα χρησιμοποιηθούν ξανά για κάποιες άλλους σκοπούς ανεξάρτητα από την εξακρίβωση των στοιχείων τους. Το 83% των χρηστών δεν εμπιστεύεται τις εκάστοτε υπηρεσίες, φαίνεται καχύποπτο και αβέβαιο απέναντι στις προθέσεις των υπηρεσιών, αντίθετα με το 17% των συμμετεχόντων-ουσών που εμπιστεύονται απόλυτα τις υπηρεσίες που δίνουν τα βιομετρικά τους δεδομένα, αφού πρόκειται μόνο για εξακρίβωση στοιχείων. Ιδιαίτερα, οι γυναίκες δίνουν

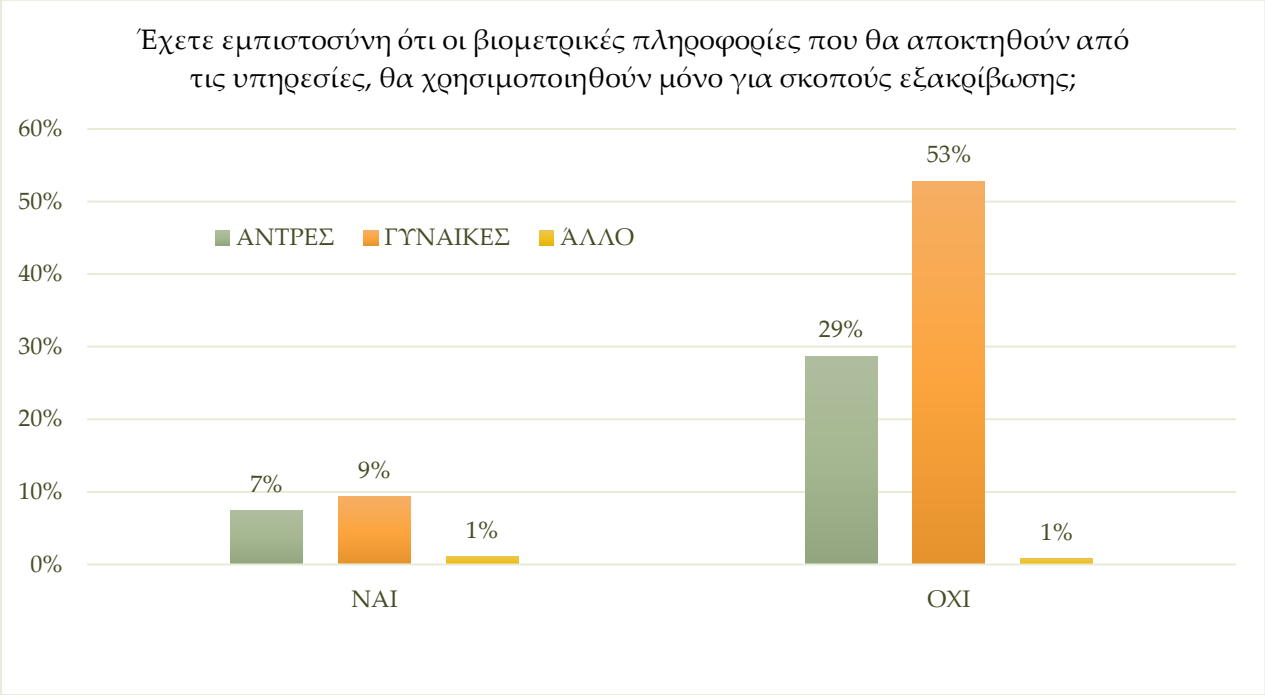
Γράφημα 55. Ενότητα Z- Ερώτηση W



εξαιρετική σημασία σε μια πιθανή κατάσταση, γεγονός που διαφαίνεται από το 53% αυτών, το οποίο φανερώνει πως δεν εμπιστεύεται ότι οι υπηρεσίες θα χρησιμοποιήσουν τις βιομετρικές τους πληροφορίες μόνο για σκοπούς εξακρίβωσης και ταυτοποίησης τους, επομένως καθίσταται κατανοητό πως οι γυναίκες ανησυχούν περισσότερο όχι μόνο για το που κι αν αποθηκεύονται τα δεδομένα τους αλλά και για ποιος σκοπούς δύναται να χρησιμοποιηθούν. Μεγάλο βέβαια είναι και το ποσοστό των ανδρών στο 29% να φανερώνει την ανησυχία του σχετικά με το πιθανό αυτό σενάριο, που αυτομάτως καταστεί τον άνθρωπο έρμαιο ελέγχου. Ενώ υπάρχουν αυτά τα μεγάλα ποσοστά δυσπιστίας απέναντι στις

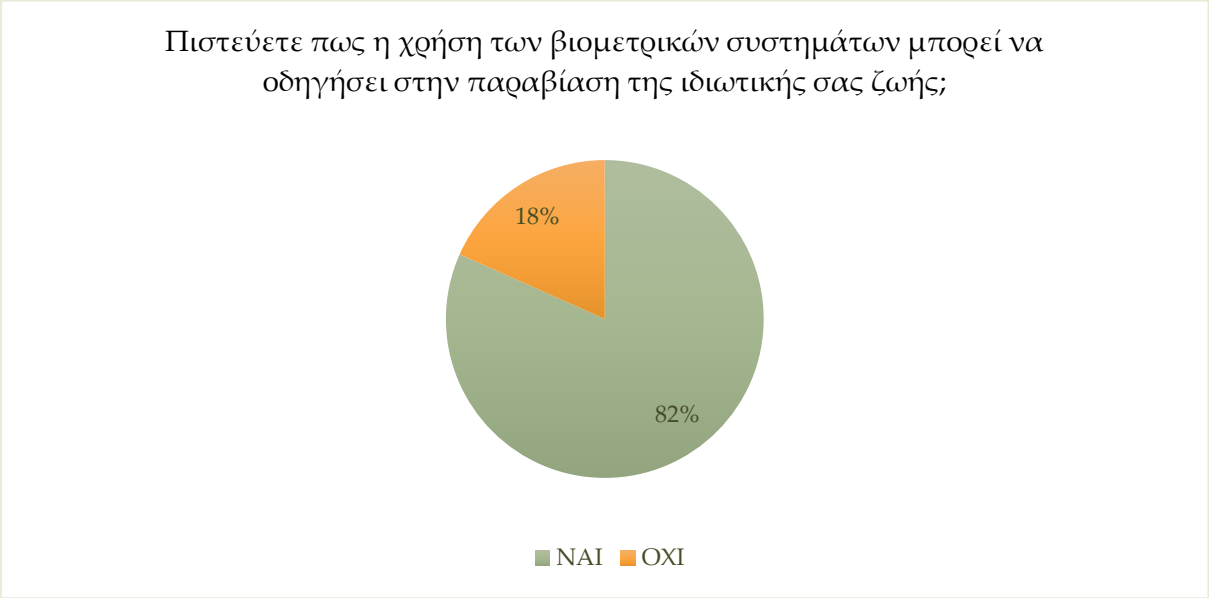
προθέσεις των υπηρεσιών, το φύλο άλλο είναι χωρισμένο στην μέση, με τους μισούς χρήστες να φοβούνται πως αυτό δεν συμβαίνει στην πραγματικότητα και με τους υπόλοιπους να ανησυχούν για το ενδεχόμενο αυτό. Υψηλά ποσοστά δημιουργούνται από τους χρήστες που διαφωνούν με τη οπτική αυτή. Αξίζει να σημειωθεί πως μόνο στο δημογραφικό στοιχείο «Φύλο» παρατηρήθηκε μια τόσο μεγάλη διαφορά μεταξύ των ερωτηθέντων.

Γράφημα 56. Ενότητα Z- Ερώτηση W- Ανά Φύλο



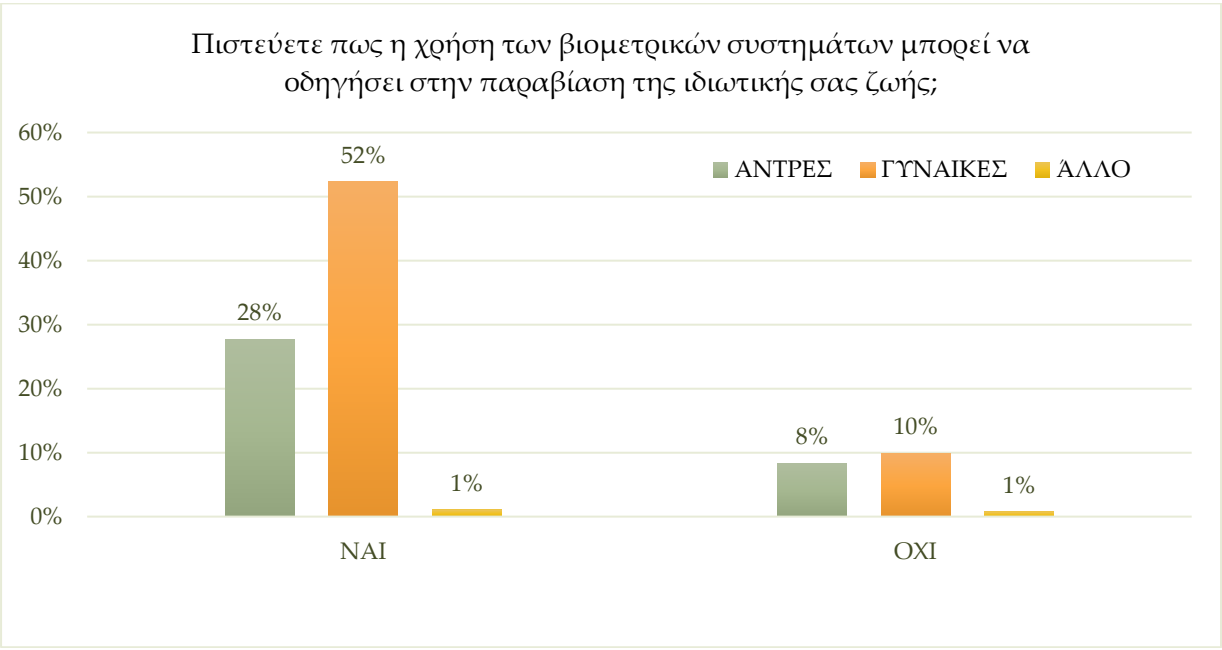
Η επόμενη ερώτηση της ενότητας αυτής σχετίζεται με το αν «Πιστεύετε πως η χρήση των βιομετρικών συστημάτων μπορεί να οδηγήσει στην παραβίαση της ιδιωτικής σας ζωής;». Γίνεται αντιληπτό πως η εκάστοτε ερώτηση της ενότητας αυτής χαρακτηρίζεται από το αν και κατά πόσο οι χρήστες δίνουν εμπιστοσύνη ή καχυποψία απέναντι στα βιομετρικά συστήματα. Συγκεκριμένα, από το γράφημα 57 προκύπτει μια από τις μεγαλύτερες ανησυχίες των συμμετεχόντων αναφορικά με την παραβίαση της ιδιωτικής τους ζωής, όπου διαφαίνεται ξεκάθαρα το 82% των χρηστών να αισθάνεται πως μπορεί από την χρήση τους να καταπατηθεί η ανωνυμία και ελευθερία των χρηστών. Η ανησυχία αυτή αποτυπώνεται σε μεγαλύτερο επίπεδο συγκριτικά με τα υπόλοιπα δημογραφικά στοιχεία, από το φύλο. Όπου φαίνεται πως αν και το φύλο συνολικά θεωρεί πως ναι από την χρήση τους δύναται η παραβιαστεί η ιδιωτικότητα τους, οι γυναίκες ανησυχούν

Γράφημα 57. Ενότητα Ζ- Ερώτηση Χ



περισσότερο. Η ανησυχία αυτή διαγράφεται από το 52% αυτών να από την χρήση τους απορρέει το αίσθημα της καταπάτησης της ιδιωτικότητας των χρηστών, ενώ οι άνδρες αν και συμφωνούν με τις γυναίκες, δεν φαίνεται να ανησυχούν σε τόσο μεγάλο βαθμό, με ποσοστό 28%. Μπορεί η πλειονοψηφία των γυναικών να ανησυχεί, όμως εξαιρετικά σημαντικό είναι και το 10% αυτών που έχει αντίθετη άποψη, καθώς δεν θεωρεί πως από την χρήση τους μπορεί να προκύψει τέτοιο αποτέλεσμα.

Γράφημα 58. Ενότητα Ζ- Ερώτηση Χ-Ανά Φύλο

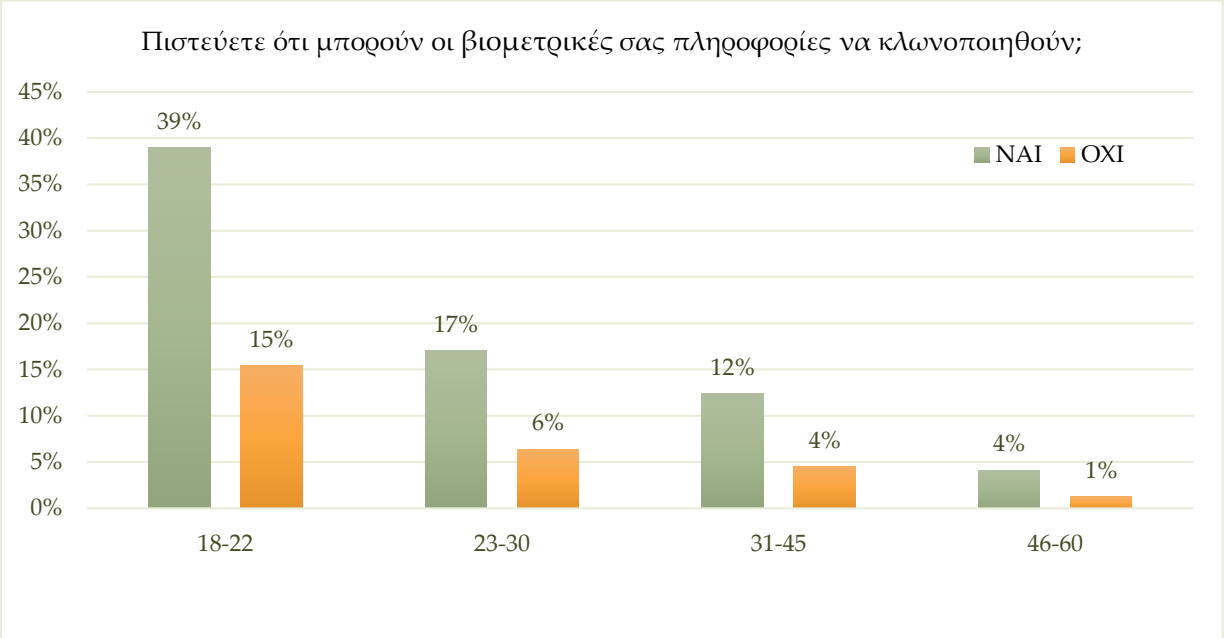


Τα αποτελέσματα που αποτυπώνονται παρακάτω απαντούν στην ερώτηση «Πιστεύετε ότι μπορούν οι βιομετρικές σας πληροφορίες να κλωνοποιηθούν;», με την πλειοψηφία των χρηστών να θεωρεί πως οι βιομετρικές πληροφορίες μπορούν εύκολα να κλωνοποιηθούν, με απόρροια να παραβιαστεί η ακεραιότητα του εκάστοτε χρήστη. Το μεγαλύτερο ποσοστό θεωρεί πως μπορούν να κλωνοποιηθούν, το οποίο ανέρχεται στο 73%, ενώ υψηλό είναι και το ποσοστό αυτών που δεν πιστεύουν ότι δύναται να κλωνοποιηθούν. Σημαντικά και εξίσου

Γράφημα 59. Ενότητα Z- Ερώτηση Y

ανατρεπτικά από το πλήθος των δημογραφικών στοιχείων, είναι τα υψηλά ποσοστά της ηλικιακής ομάδας 18-22, όπου το 39% θεωρεί πως μπορούν να κλωνοποιηθούν, σε αντίθεση με το υψηλό ποσοστό του 15% που πιστεύει πως δεν μπορούν. Αξίζει να σημειωθεί πως το ποσοστό αυτό βρίσκεται αρκετά κοντά στην άποψη των χρηστών της ηλικιακής ομάδας 23-30, το 17% αυτών να θεωρεί πως μπορούν να κλωνοποιηθούν. Τα ποσοστά των άλλων ομάδων είναι αρκετά κοντά μεταξύ τους, σκιαγραφώντας μια εικόνα ενός αβέβαιου στην πλειονότητα του πληθυσμού, όπου το 12% των 31-45 πιστεύει πως μπορούν ενώ το 4% δεν μπορούν, αντιστοίχως και για την ηλικιακή ομάδα 46-60.

Γράφημα 60. Ενότητα Ζ- Ερώτηση Υ- Ανά Ηλικιακή Ομάδα

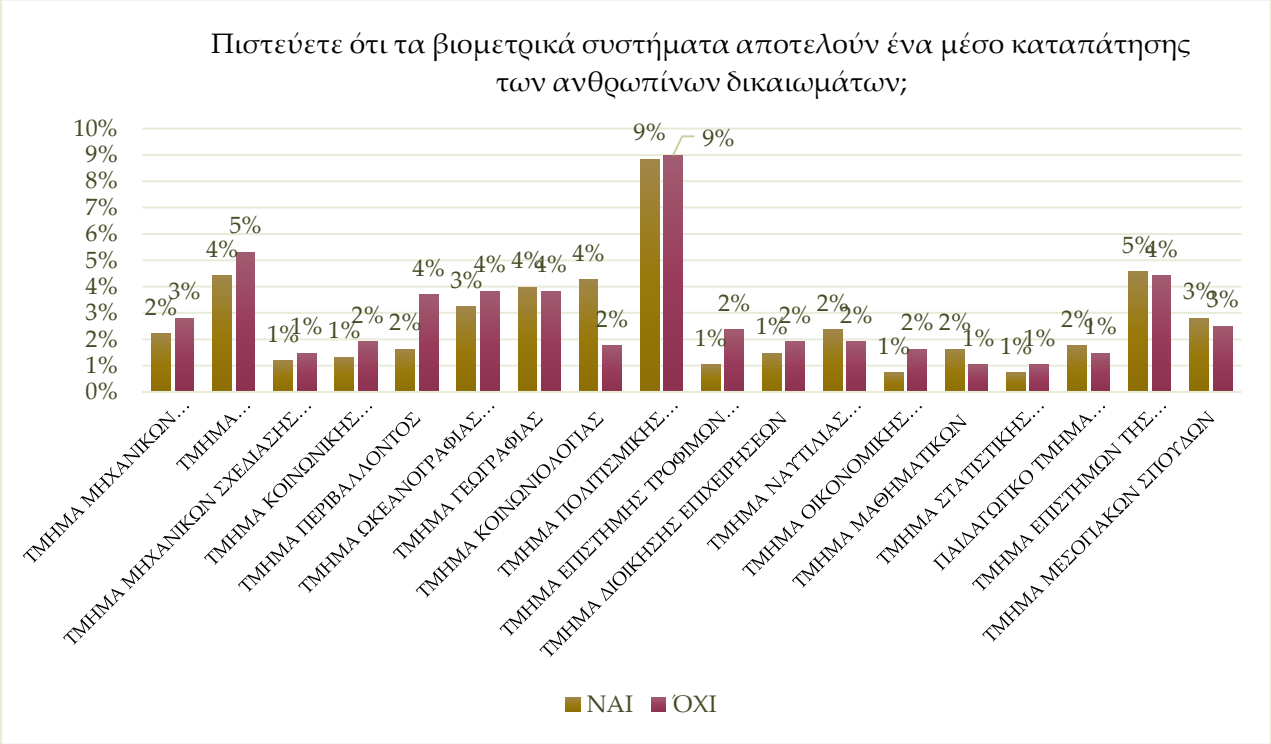


Η τελευταία ερώτηση από το πλήθος αυτών που είναι μορφολογικά ίδιες και αναλύεται στα παρακάτω γραφήματα είναι: «Πιστεύετε ότι τα βιομετρικά συστήματα αποτελούν ένα μέσο καταπάτησης των ανθρωπίνων δικαιωμάτων;». Ενώ από τα παραπάνω αποτελέσματα φάνηκε μεγάλη διαφορά ως προς τον φόβο της καταπάτησης της ιδιωτικής ζωής, στο παρόν γράφημα παρατηρείται μια εντελώς διαφορετική αντίληψη των χρηστών. Συγκεκριμένα, το 52% των συμμετεχόντων-ουσών δηλώνει πως τα βιομετρικά συστήματα δεν αποτελούν ένα μέσο καταπάτησης των ανθρωπίνων δικαιωμάτων, σε αντίθεση με το 48% που

Γράφημα 61. Ενότητα Ζ- Ερώτηση Ζ

δηλώνει πως έχουν αυτή την δυνατότητα. Η ποσοστιαία διαφορά του 4% ανάμεσα τους, υπογραμμίζεται και από το Τμήμα Φοίτησης των φοιτητών-τριών. Όπως διαφαίνεται στο γράφημα, ανεξάρτητα από το τμήμα φοίτησης των ερωτηθέντων, τα μεγαλύτερα ποσοστά δείχνουν πως οι χρήστες φοβούνται ότι μέσω των βιομετρικών τους πληροφορίων είναι πιο εύκολο να παραβιαστούν τα ανθρώπινα δικαιώματα τους. Παρόλα αυτά τα μεγαλύτερα ποσοστά προκύπτουν από το τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας με 9% και στην επιλογή ναι και στην επιλογή όχι. Τα περισσότερα ποσοστά είναι ισόποσα, γεγονός που δείχνει την έντονη διαφοροποίηση των απόψεων του δείγματος, αν και σε προηγούμενη σχετική ερώτηση, υπήρχε μια διαφορετική κατεύθυνση των χρηστών.

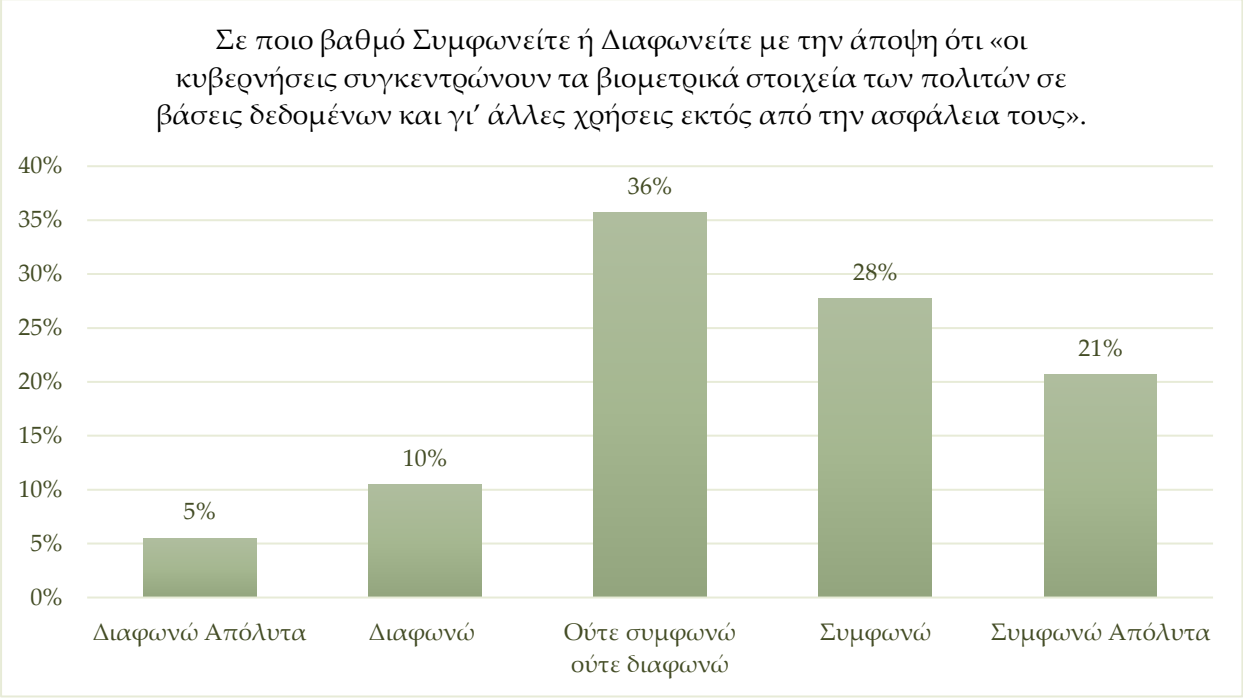
Γράφημα 62. Ενότητα Z- Ερώτηση Z-Ανά Τμήμα Σπουδών



Οι δύο παρακάτω ερωτήσεις με τις οποίες ολοκληρώνεται το ερωτηματολόγιο σε πρώτο επίπεδο και η παράθεση των αποτελεσμάτων σε δεύτερο, συνδέονται καθώς η μια αποτελεί συνέχεια της άλλης. Η πρώτο στη σειρά γράφημα απαντάται στην ερώτηση «Σε ποιο βαθμό Συμφωνείτε ή Διαφωνείτε με την άποψη

ότι «οι κυβερνήσεις συγκεντρώνουν τα βιομετρικά στοιχεία των πολιτών σε βάσεις δεδομένων και γι' άλλες χρήσεις εκτός από την ασφάλεια τους»». Πρόκειται μια ερώτηση βαθμονόμησης από το 1 έως το 5 και όπως παρατηρείται στο γράφημα 63, το υψηλότερο ποσοστό δεν μπορεί να διατυπώσει μια ξεκάθαρη γνώμη σχετικά με την ερώτηση, το οποίο ανέρχεται στο 36%, Ηχηρά όμως είναι τα ποσοστά του 28% αρχικά όπου φαίνεται πως ένα μεγάλος αριθμός των χρηστών συμφωνεί με την παραπάνω διαπίστωση, ενώ παράλληλα το 21% των ερωτηθέντων-ουσών συμμερίζεται την άποψη αυτή. Εξίσου καθοριστικά ως προς την κατανόηση του δείγματος είναι και το 10% των χρηστών που φαίνεται να διαφωνεί με την παρούσα άποψη, όπως επίσης και το 5% των χρηστών που δηλώνει πως «Διαφωνώ Απόλυτα» με την διαπίστωση αυτή.

Γράφημα 63. Ενότητα Z- Ερώτηση ΑΑ



Τα αποτελέσματα που προκύπτουν από τα ακόλουθα γραφήματα αποτελούν συνέχεια της προηγούμενης ερώτησης, αφού η συγκεκριμένη είναι μια ανοικτού τύπου ερώτηση ώστε οι χρήστες να αιτιολογήσουν την 'άποψη τους αναφορικά με την προηγούμενη άποψη. Το μεγαλύτερο ποσοστό ανήκει στην παραδοχή πως οι υπηρεσίες από την στιγμή που συγκεντρώνουν τις βιομετρικές πληροφορίες των

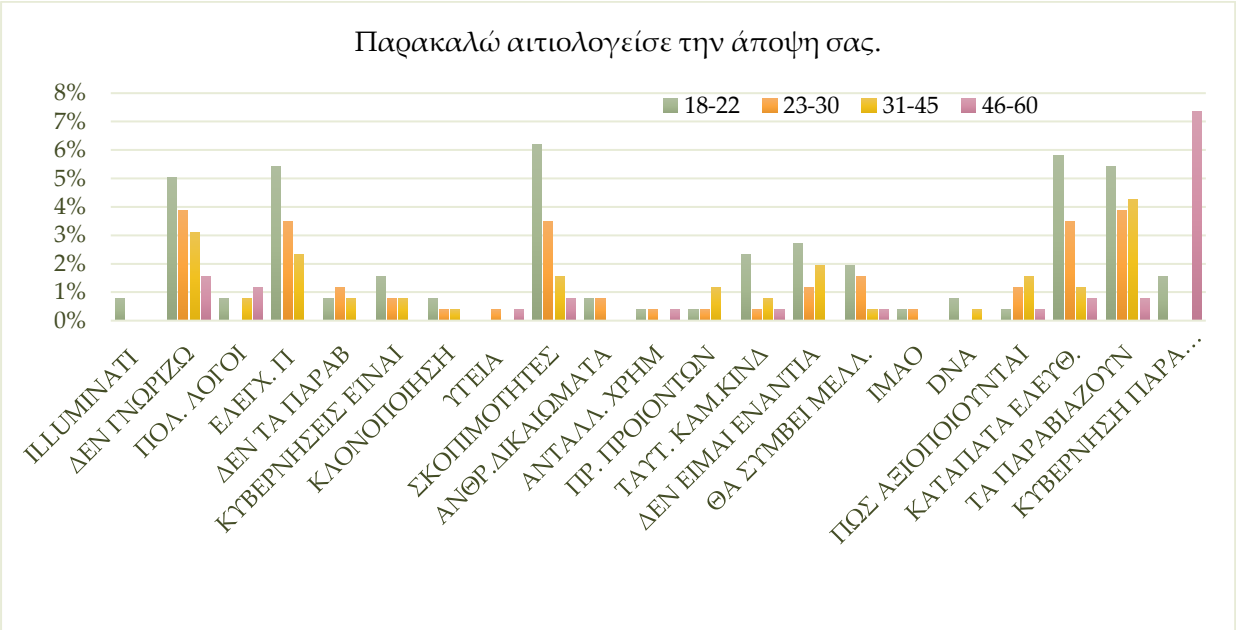
χρηστών, αυτομάτως παραβιάζεται η ιδιωτικότητα τους. Η έντονη αυτή ανησυχία ισορροπείται με το 14% των χρηστών να δηλώνει πως από την στιγμή πως δεν γνωρίζει κανείς με ακρίβεια δεν γίνεται να υπάρχει μια κατεύθυνση στην άποψη αυτή. Ουσιαστικά, το ποσοστό αυτό θεωρεί πως αφενός υπάρχουν υποψίες αλλά τίποτα δεν είναι συγκεντρωτικό αν δεν επιβεβαιωθούν. Το 12% σκιαγραφεί το ποσοστό των χρηστών που θεωρεί πως «πίσω» απ' όλα αυτά κρύβονται πολιτικοί λόγοι και επιτελούνται συμφέροντα και σκοπιμότητες εις βάρος των πολιτών.

Γράφημα 64. Ενότητα Z- Ερώτηση ΑΒ

Το ακόλουθο γράφημα, παρουσιάζει τις αντιλήψεις των χρηστών ανά ηλικιακή ομάδα. Το μεγαλύτερο ποσοστό ανήκει στην ηλικιακή ομάδα 46-60, το οποίο ανέρχεται στο 7%. Συγκεκριμένα, οι χρήστες δηλώνουν πως προτιμούν να παρακολουθούνται από την εκάστοτε κυβέρνηση, παρά από τρίτους. Ουσιαστικά, το ποσοστό αυτό φαίνεται να συμφωνεί και να προτιμά με την άποψη που λέει ότι «οι κυβερνήσεις συγκεντρώνουν τα βιομετρικά στοιχεία των πολιτών σε βάσεις δεδομένων και γι' άλλες χρήσεις εκτός από την ασφάλεια τους». Παρόλα αυτά υπάρχουν και άλλες δυο απαντήσεις με ποσοστό 6% και ανήκουν στην ηλικιακή ομάδα 18-22, όπου από την πρώτη προκύπτει πως η κατάσταση αυτή συμβαίνει διότι υπάρχουν συμφέροντα και σκοπιμότητες, ενώ οι χρήστες δηλώνουν πως αν

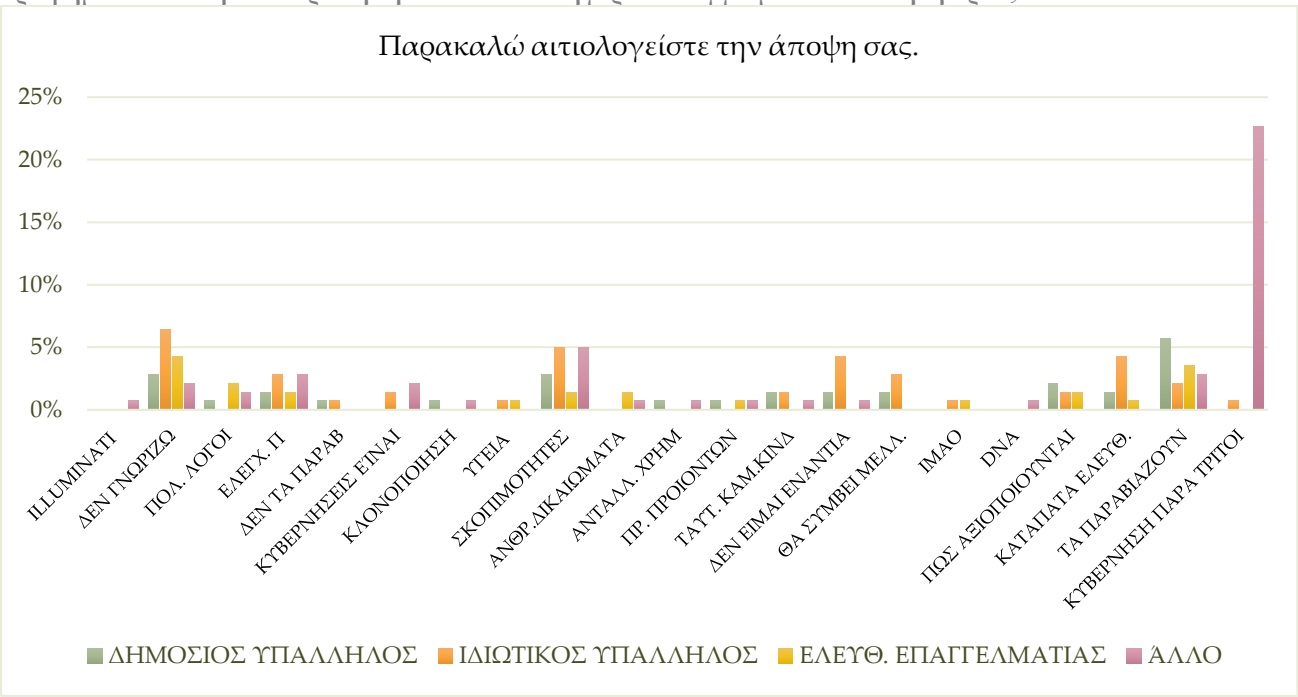
αυτό είναι πραγματικότητα, τότε καταπατάται η ελευθερία και η ανωνυμία καθώς πάντα κάποιος «ξέρει» τις κινήσεις μας.

Γράφημα 65. Ενότητα Z- Ερώτηση AB- Ανά Ηλικιακή Ομάδα



Τέλος, εξίσου σημαντική είναι και η τάση που προέρχεται από την κατηγορία επαγγέλματος των φοιτητών-τριών. Το μεγαλύτερο ποσοστό ανήκει στους φοιτητές που έχουν επιλέξει την επιλογή άλλο ως επάγγελμα, το οποίο ανέρχεται στο 23%. Συγκεκριμένα, οι χρήστες δηλώνουν πως προτιμούν να παρακολουθούνται από την εκάστοτε κυβέρνηση, παρά από τρίτους. Ουσιαστικά, οι χρήστες φαίνεται να συμφωνούν και να προτιμούν την άποψη που λέει ότι «οι κυβερνήσεις συγκεντρώνουν τα βιομετρικά στοιχεία των πολιτών σε βάσεις δεδομένων και γι' άλλες χρήσεις εκτός από την ασφάλεια τους». Επιπλέον, το 6% των ερωτηθέντων που εργάζονται ως ιδιωτικοί υπάλληλοι δηλώνει πως δεν γνωρίζει ξεκάθαρα την κατάσταση αρά δεν μπορεί να πάρει ξεκάθαρη θέση στην άποψη αυτή, ενώ το ίδιο ποσοστό που εργάζεται ως δημόσιος υπάλληλος, θεωρεί πως παραβιάζονται τα ανθρώπινα δικαιώματα από την στιγμή που η εκάστοτε υπηρεσία/κυβέρνηση ζητά τις βιομετρικές πληροφορίες για να προβεί σε ταυτοποίηση.

Γράφημα 65. Ενότητα Ζ- Ερώτηση ΑΒ- Ανά Κατηγορία Επαγγελμάτων Φοιτητή-τριας



5.7 Συζήτηση-Συμπεράσματα

Μορφολογικά, το παρόν υποκεφάλαιο δομείται με τις αντίστοιχες ενότητες του ερωτηματολογίου, όπως και στο προηγούμενο υποκεφάλαιο, ώστε τα συμπεράσματα να έχουν μια λογική σειρά και μια συνέχεια στην ερμηνεία τους. Τα ποσοστά της πρώτης ενότητας, τα οποία στο ερωτηματολόγιο ζητήθηκαν από τους χρήστες τελευταία είναι τα δημογραφικά στοιχεία. Παρατίθενται στην αρχή των αποτελεσμάτων για να παρουσιάζουν τους συμμετέχοντες-ουσες στην έρευνα. Στο ερωτηματολόγιο έλαβαν μέρος 279 άνδρες, 480 γυναίκες και 6 άτομα που δήλωσαν άλλο φύλο από το σύνολο των 16.000 φοιτητών-τριων του Πανεπιστημίου Αιγαίου. Οι ηλικίες των χρηστών χωρίστηκαν σε τέσσερις ομάδες, από τις οποίες σημειώθηκε μεγαλύτερο ποσοστό συμμετοχής από την ηλικιακή ομάδα 18-22 με ποσοστό στο 54%, από την ομάδα 23-30 το ποσοστό ανήλθε στο 23%, ενώ από την ομάδα 31-45 στο 17% και τέλος από την ομάδα 46-60 στο 6%. Να σημειωθεί πως το ερωτηματολόγιο δημιουργήθηκε μόνο για φοιτητές του

Πανεπιστήμιου Αιγαίου και συγκεκριμένα για προπτυχιακούς, μεταπτυχιακούς και διδακτορικούς φοιτητές, με απώτερο σκοπό να διαφανεί αν η αντίληψη των χρηστών αναφορικά με τα Βιομετρικά Συστήματα σχετίζεται. Από τα γραφήματα προέκυψε μικρότερος αριθμός συμμετοχής από τους διδακτορικούς φοιτητές με ποσοστό 9%, αισθητά μεγαλύτερη απήχηση είχε στους μεταπτυχιακούς φοιτητές με ποσοστό 24% και τέλος το μεγαλύτερο ποσοστό καταγράφηκε από τους προπτυχιακούς φοιτητές με ποσοστό στο 68%. Προκειμένου να αποσαφηνιστεί το επίπεδο σπουδών των προπτυχιακών φοιτητών, ζητήθηκε μόνο από αυτούς να καταγράψουν το έτος σπουδών που διανύουν. Το μεγαλύτερο ποσοστό καταγράφηκε από πρωτοετείς φοιτητές με ποσοστό στο 28%, 20% των φοιτητών διανύουν το δεύτερο έτος τους, 12% το τρίτο, 17% το τέταρτο ενώ 12% και 10% διανύει αντίστοιχα το πέμπτο και μεγαλύτερο αυτού έτος σπουδών. Όπως αναφέρθηκε προηγουμένως, πρόκειται για έρευνα που αφορά πλήρως τα δεκαοχτώ Τμήματα του Πανεπιστήμιο Αιγαίου. Από αυτά, το μεγαλύτερο ποσοστό των απαντήσεων προήλθε από τους φοιτητές του Τμήματος Πολιτισμικής Τεχνολογίας και Επικοινωνίας, το οποίο ανέρχεται στο 18%, 10% των απαντήσεων από το Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, 9% από το Τμήμα Επιστημών της Προσχολικής Αγωγής και του Εκπαιδευτικού Σχεδιασμού, ενώ μικρότερα ποσοστά προήλθαν από το Τμήμα Οικονομικής και Διοίκησης Τουρισμού και Στατιστικής και Αναλογιστικών-Χρηματοοικονομικών Μαθηματικών με ποσοστό 2%. Προκειμένου να σκιαγραφηθούν με μεγαλύτερη ακρίβεια οι συμμετέχοντες-ουσες, ρωτήθηκαν εάν παράλληλα με τις σπουδές τους εργάζονται κι όσοι απάντησαν «ναι» κλήθηκαν να συμπληρώσουν την κατηγορία του επαγγέλματος τους. Αρχικά, οι περισσότεροι φοιτητές δεν εργάζονται παράλληλα με τις σπουδές τους με ποσοστό 59%, ενώ από το υπόλοιπο 41%, το οποίο εργάζεται, οι μισοί (50%) εξ' αυτών εργάζονται ως ιδιωτικοί υπάλληλοι, το 27% ως δημόσιοι υπάλληλοι, ενώ 20% ως ελεύθεροι επαγγελματίες και 4% δηλώνει ως κατηγορία επαγγέλματος άλλο. Σκιαγραφώντας τα χαρακτηριστικά των φοιτητών-τριών κρίθηκε σκόπιμο να προσδιοριστούν η κατηγορία επαγγέλματος του πατέρα και της μητέρα των συμμετεχόντων-ουσών στην έρευνα, καθώς και το ετήσιο εισόδημα τους,

προκειμένου να δημιουργεί μια σφαιρική εικόνα για τους χρήστες. Από το επάγγελμα του πατέρα, παρατηρήθηκε πως η πλειοψηφία αυτών εργάζεται ως ελεύθερος επαγγελματίας με ποσοστό 29%, 24% ως ιδιωτικός υπάλληλος, ενώ 20% είναι δημόσιοι υπάλληλοι και συνταξιούχοι. Από την ανάλυση αυτή φαίνεται το ποσοστό 0% των ανδρών που ασχολούνται με τα οικιακά, σε αντίθεση με των γυναικών που θα παρατεθεί στην συνέχεια. Σχετικά με την εργασία της μητέρας των χρηστών, τα υψηλότερα ποσοστά είναι χωρισμένα σε τρία επαγγέλματα, όπου το 22% εργάζεται ως ιδιωτικοί υπάλληλοι, ενώ το 21% ως δημόσιοι υπάλληλοι και ασχολούνται με τα οικιακά. Σχετικά υψηλό είναι το ποσοστών των μητέρων που είναι άνεργες, το οποίο ανέρχεται στο 8%, ενώ μόλις το 1% δηλώνει ως επάγγελμα άλλο. Τέλος, το υψηλότερο ποσοστό των φοιτητών, το οποίο ανέρχεται στο 44% δηλώνει ως ετήσιο εισόδημα τους <10.000€, το 42% κυμαίνεται από 10.001€-25.000€, ενώ αισθητά διαφοροποιούνται τα ποσοστά στην κατηγορία 25.001€- 55.000€ με ποσοστό στο 13% και μόλις 1% στην κατηγορία με ετήσιο εισόδημα >55.0001€.

Η ενότητα Α, με τίτλο «Γνώση Βιομετρικών Συστημάτων» εισάγει τους συμμετέχοντες-ουσες στο βασικό θέμα της έρευνας, που είναι τα Βιομετρικά Συστήματα. Κρίθηκε αναγκαίο για στατιστικούς λόγους, να καταγραφεί στο εισαγωγικό σημείωμα ο ορισμός των Βιομετρικών Συστημάτων, ώστε να προκύψει το ποσοστό των χρηστών που γνώριζαν και αυτών που δεν γνώριζαν γι' αυτά. Κατά τη διαδικασία της περιγραφικής ανάλυσης, παρατηρήθηκε πως το ποσοστό των χρηστών που απάντησαν «ναι» ή «όχι» δεν είναι μεγάλο. Συγκεκριμένα, το μεγαλύτερο ποσοστό ανήκει στους χρήστες που γνώριζαν τον ορισμό τους, το οποίο ανέρχεται στο 51%, ενώ με 49% είναι οι χρήστες που έμαθαν τι είναι τα Βιομετρικά Συστήματα λόγω του εισαγωγικού σημειώματος. Επιπλέον, το έτος σπουδών διαφαίνεται να λειτουργεί ως παράγοντας διαφοροποίησης, καθώς το 18% των πρωτοετών φοιτητών δεν γνώριζε τον ορισμό τους προτού διαβάσει το εισαγωγικό σημείωμα. Το ποσοστό που χρήζει μεγαλύτερης σημασίας από την ερώτηση αυτή είναι πως οι φοιτητές που διανύουν το τέταρτο έτος των σπουδών τους έχουν μεγαλύτερο ποσοστό άγνοιας του ορισμού των Βιομετρικών Συστημάτων, με ποσοστό στο 10% συγκριτικά με μικρότερους τριτοετείς φοιτητές.

Ανατρέχοντας από στατιστικής πλευράς στα αποτελέσματα, παρατηρείται κατά γενική ομολογία πως κατά τη διάρκεια των σπουδών, οι γνώσεις των φοιτητών-τριών εξελίσσονται. Αυτό όμως δεν παρατηρείται στην προκείμενη, καθώς θα έπρεπε όσο μεγαλώνουν τα έτη σπουδών να μειώνεται ο αριθμός των φοιτητών που δεν γνωρίζει τα βιομετρικά συστήματα, διαφαίνεται πως συμβαίνει το αντίθετο. Η δεύτερη ερώτηση της ενότητας αυτής «Σημειώστε ποιες από τις ακόλουθες τεχνικές των Βιομετρικών Συστημάτων γνωρίζετε:», αποτυπώνει τα αποτελέσματα που προέκυψαν. Συγκεκριμένα, φαίνεται πως οι πιο γνωστές βιομετρικές τεχνικές είναι το δακτυλικό αποτύπωμα με ποσοστό 12%, η αναγνώριση προσώπου με 11%, η ανάλυση DNA με 10% καθώς και η ανάλυση της ίριδας του ματιού. Οι τεχνικές αυτές συγκεντρώνουν χαμηλά ποσοστά από χρήστες που δεν τα γνωρίζουν, δείχνοντας έτσι πως έχουν μεγαλύτερη φήμη, σε αντίθεση με την γεωμετρία χεριού, την ανάλυση βηματισμού και την αναγνώριση της πληκτρολόγησης, τεχνικές που με ποσοστό 9% και 10%, η τελευταία, δεν είναι σε μεγάλο βαθμό γνωστές προς τους χρήστες. Συνολικά, καταγράφονται υψηλότερα ποσοστά γνώσης παρά άγνοιας των βιομετρικών τεχνικών που παρατέθηκαν. Ιδιαίτερα, η ηλικία διαφαίνεται να λειτουργεί ως παράγοντας διαφοροποίησης, καθώς η ηλικιακή ομάδα 18-22 σημειώνει τα υψηλότερα ποσοστά των χρηστών που γνωρίζουν τις βιομετρικές τεχνικές. Εντύπωση δημιουργεί πως μόνο στο δακτυλικό αποτύπωμα, καταγράφηκε το χαμηλότερο ποσοστό χρηστών που δεν το γνώριζαν με ποσοστό μόλις 2%, ενώ οι υπόλοιπες ηλικιακές ομάδες καταγράφουν 0%. Χαρακτηριστικό παράδειγμα αποτελούν τα ποσοστά της αναγνώρισης προσώπου, στην οποία αν και παρατηρούνται μικρά ποσοστά, ξεπερνούν αυτά του αποτυπώματος αναφορικά με τους χρήστες που δεν την γνωρίζουν. Ανεξάρτητα από την τάση αυτή, το μεγαλύτερο ποσοστό καταγράφεται για άλλη μια φορά στην ηλικιακή ομάδα 18-22, γεγονός που φανερώνει πως οι νεότερες γενιές αισθάνονται περισσότερη οικειότητα με τους ορισμούς αυτούς. Τα ευρήματα της έρευνας του Πανεπιστημίου Αιγαίου ενισχύονται από τα αποτελέσματα έρευνας που διεξήχθη στο Ηνωμένο Βασίλειο, από την οποία προέκυψε πως η σάρωση δακτυλικών αποτυπωμάτων είναι η βιομετρική τεχνική που οι περισσότεροι ενήλικες γνωρίζουν και αισθάνονται

άνετα να χρησιμοποιούν με ποσοστό 40% (Keough, 2016). Παρατηρείται επομένως πως η ηλικιακή ομάδα 18-22 γνωρίζει την τεχνική του δακτυλικού αποτυπώματος και της αναγνώρισης προσώπου με υψηλότερα ποσοστά απ' ότι τις υπόλοιπες βιομετρικές τεχνικές, ενώ στην περίπτωση του δακτυλικού αποτυπώματος παρατηρείται καθολική γνώση ανεξαρτήτου ηλικίας. Ένα καθοριστικό σχόλιο που προήλθε από τους συμμετέχοντες είναι «*Δεν υπάρχει πλέον κινητό τηλέφωνο χωρίς δακτυλικό αποτύπωμα*», επομένως είναι επόμενο να καταγράφονται τόσο υψηλά ποσοστά στην ηλικιακή ομάδα 18-22.

Η ενότητα Β, με τίτλο «Εμπειρία στη χρήση Βιομετρικών Συστημάτων» επιδιώκει να περιγράψει με σαφήνεια αν και κατά πόσο οι βιομετρικές τεχνικές διαδραματίζουν καθοριστικό ρόλο στην καθημερινότητα των χρηστών. Από την ερώτηση «Έχετε υιοθετήσει κάποιες από τις παρακάτω τεχνικές στην καθημερινότητα σας;», προκύπτει ένα συνολικό ποσοστό όλων των συμμετεχόντων, το οποίο δηλώνει πως η πιο δημοφιλής βιομετρική τεχνική είναι το δακτυλικό, όπου το 10% των ερωτηθέντων υιοθετεί την συγκεκριμένη τεχνική στην καθημερινότητα του. Ιδιαίτερα, οι προπτυχιακοί φοιτητές με ποσοστό 58% δίνουν ιδιαίτερη έμφαση στην υιοθέτησης της τεχνικής αυτής, διότι όπως θα αναλυθεί και στην συνέχεια, η τεχνική του δακτυλικού αποτυπώματος χρησιμοποιείται καθημερινά από τους χρήστες για να ξεκλειδώσουν το κινητό τους τηλέφωνο. Η προώθηση του δακτυλικού αποτυπώματος από τις εταιρίες κινητής τηλεφωνίας το καθιστά την πιο δημοφιλή βιομετρική τεχνική. Το πόρισμα αυτό έρχεται να επιβεβαιωθεί από την ακόλουθη έρευνα. Αναλυτικότερα, η καινοτομία αυτή σύμφωνα με έρευνα που έγινε το 2015 στην Σιγκαπούρη σε χρήστες Android 4.0+ και Iphone 5s, έδειξε την ανάγκη των χρηστών για ευκολία και ευχρηστία κατά το άνοιγμα του κινητού τους τηλεφώνου, με ποσοστό 69% (Cranor 2015). Διαπιστώνουμε λοιπόν, πως θα ήτανε «περίεργο» να μην υιοθετηθεί ευρέως το δακτυλικό αποτύπωμα αφού προσφέρει ευκολία, ταχύτητα και μείωση αποτυχίας εισόδου σε σύγκριση με τους κωδικούς πρόσβασης.
Από τα συνολικά αποτελέσματα, προέκυψε πως οι βιομετρικές τεχνικές που δεν υιοθετούνται στην καθημερινότητα είναι περισσότερες απ' αυτές που υιοθετούνται από τους χρήστες. Συγκεκριμένα, η γεωμετρία χεριού καταγράφει

συνολικά ποσοστό 0% των χρηστών που την υιοθετούν και 12% αυτών που δεν την υιοθετούν, αντιστοίχως παρόμοια αποτελέσματα προκύπτουν και από την ανάλυση DNA, την ανάλυση πληκτρολόγησης και την ανάλυση βηματισμού. Επιπλέον, το επίπεδο σπουδών διαφαίνεται να λειτουργεί ως παράγοντας διαφοροποίησης, καθώς οι προπτυχιακοί φοιτητές δεν υιοθετούν την τεχνική της γεωμετρίας χεριού στην καθημερινότητα τους με ποσοστό 69%. Ταυτόχρονα, ένα υψηλό ποσοστό, το οποίο ανέρχεται στο 64% και ανήκει στο ίδιο επίπεδο σπουδών, δεν υιοθετεί την ανάλυση της πληκτρολόγησης, αν και σε σχέση με τις υπόλοιπες βιομετρικές τεχνικές, παρατηρείται ένα 7% των προπτυχιακών που χρησιμοποιούν στην καθημερινότητα τους την τεχνική αυτή.
Τα αποτελέσματα που προκύπτουν από τις ερωτήσεις είναι βοηθητικά, διότι είναι ικανά να αιτιολογήσουν πιθανές τάσεις και απόψεις των χρηστών. Αναλυτικότερα, τα ποσοστά που προέκυψαν από την ερώτηση «Εάν έχετε υιοθετήσει κάποιες από τις παραπάνω τεχνικές, σε ποια καθημερινή σας δραστηριότητα αφορά; Παρακαλώ καταγράψτε:», διαδραματίζουν καθοριστικό ρόλο στην κατανόηση της τάσης των χρηστών να υιοθετούν το δακτυλικό αποτύπωμα. Πρόκειται για μια ερώτηση ανοικτού τύπου, στην οποία οι χρήστες είχαν την δυνατότητα να καταγράψουν χωρίς κάποιο προβλεπόμενο πλαίσιο, τις δραστηριότητες που υιοθετούν τις βιομετρικές τεχνικές. Διαφαίνεται από το συνολικό γράφημα πως η πιο συνηθισμένη καθημερινή δραστηριότητα των χρηστών είναι το ξεκλείδωμα του κινητού τους τηλεφώνου με την χρήση του δακτυλικού αποτυπώματος. Αυτό αποτυπώνεται με το πρώτο μεγαλύτερο ποσοστό στο 57%, ενώ στο 15% οι χρήστες υιοθετούν την ανάλυση DNA. Ιδιαίτερα, οι προπτυχιακοί φοιτητές με ποσοστό 40% δίνουν ιδιαίτερη έμφαση στην υιοθέτηση του ξεκλειδώματος του κινητού τηλεφώνου με το αποτύπωμά τους, καθώς επίσης δίνουν αυξημένη βαρύτητα που αποτυπώνεται από το δεύτερο μεγαλύτερο ποσοστό στο 14%. Επιπλέον, η κατηγορία επαγγέλματος των φοιτητών-τριών που εργάζονται, διαφαίνεται να λειτουργεί ως παράγοντας διαφοροποίησης, καθώς οι φοιτητές-τριες που εργάζονται ως άλλο υιοθετούν με μεγαλύτερο ποσοστό το 21% την ανάλυση DNA. Από τους ιδιωτικούς υπαλλήλους παρατηρείται το μεγαλύτερο ποσοστό των χρηστών που χρησιμοποιούν το

δακτυλικό αποτύπωμα για να ξεκλειδώσουν το κινητό τους. Παρατηρείται επομένως, πως οι χρήστες που υιοθετούν το αποτύπωμα για να ξεκλειδώσουν το κινητό τους προέρχονται από το προπτυχιακό επίπεδο σπουδών και από όσους εργάζονται ως ιδιωτικοί υπάλληλοι.

Η ενότητα Γ με τίτλο «Ευχρηστία Βιομετρικών Συστημάτων» επιδιώκει να περιγράψει σε πρώτο στάδιο την άποψη που δημιουργούν τα βιομετρικά συστήματα στους συμμετέχοντες-ουσες. Αρωγός της επίτευξης του σκοπού αποτελούν οι ερωτήσεις της ενότητας αυτής. Συγκεκριμένα, οι χρήστες «βαθμολόγησαν» από το 1 έως το 5, που αντιστοιχεί από το Πολύ Δύσκολα έως το Πολύ Εύκολα την ερώτηση «Πόσο εύκολα θεωρείτε ότι είναι στη χρήση τους;». Από τα συνολικά αποτελέσματα προκύπτει πως οι χρήστες θεωρούν τα βιομετρικά συστήματα «Πολύ Εύκολα» και «Εύκολα» στην χρήση τους. Το ποσοστό που αποτυπώνει την άποψη αυτή είναι το μεγαλύτερο και ανέρχεται στο 32%. Την αντίληψη αυτή, έρχεται να συμπληρώσουν τα υπόλοιπα ποσοστά της ερώτησης αυτής, τα οποία σε δεύτερο βαθμό αναδεικνύουν το υψηλό ποσοστό των χρηστών που δεν έχει κάποια ξεκάθαρη γνώμη απέναντι στα αυτά, δηλώνοντας πως είναι «Μέτρια» στην χρήση τους, ενώ τα ποσοστά 7% και 3% παρουσιάζουν ένα μικρό ποσοστό το πληθυσμού που τα θεωρεί δύσκολα. Σκόπιμο θα ήταν οι πολιτικές που προωθούν τα Βιομετρικά Συστήματα, να επικεντρωθούν ώστε οι βιομετρικές τεχνικές να είναι απλούστερες για μεγαλύτερο ποσοστό του πληθυσμού. Εκτός από την ευχρηστία τους, σημαντικό είναι το ποσοστό των συμμετεχόντων που κρίνει αν «Θεωρείτε ότι η χρήση τους απαιτεί ιδιαίτερη εκπαίδευση;». Η ερώτηση αυτή αποσαφηνίζεται μέσα από τα παρακάτω ποσοστά, όπου το 68% των ερωτηθέντων υποστηρίζει πως δεν απαιτείται ιδιαίτερη εκπαίδευση τους. Αν και η διαφορά των αντιλήψεων είναι μεγάλη, αυτό δεν σημαίνει πως το 32% που θεωρεί πως θα ήτανε βοηθητικό να εκπαιδεύονται, τίθενται σε δεύτερη μοίρα. Αντιθέτως, πρώτιστό μέλημα των πολιτικών θα πρέπει να είναι η εξισορρόπηση του πληθυσμού. Στην προκείμενη, για να επιτευχθεί πιο μαζικά ο στόχος, θα πρέπει να μειωθεί αισθητά το ποσοστό των χρηστών που θα θεωρεί αναγκαία την εκπαίδευση τους.

Οι δύο ερωτήσεις που ακολουθούν αναφέρονται στα πλεονεκτήματα και τα

μειονεκτήματα των βιομετρικών συστημάτων σύμφωνα με την άποψη των συμμετεχόντων-ουσών. Συγκεκριμένα, από την πρώτη ερώτηση «Ποιο από τα παρακάτω θεωρείτε το σημαντικότερο πλεονέκτημα για τη χρήση των βιομετρικών συστημάτων;», αποτυπώνεται συνολικά πως το 41% των χρηστών υποστηρίζει ότι η πιθανότητα ορθής αναγνώρισης, η οποία βασίζεται σε μοναδικά χαρακτηριστικά του εκάστοτε ανθρώπου, είναι το σημαντικότερο πλεονέκτημα των βιομετρικών συστημάτων. Ιδιαίτερα, οι γυναίκες με ποσοστό 26% έρχεται να ενισχύσει το πλεονέκτημα αυτό. Στην αντίστοιχη επιλογή, το ποσοστό των ανδρών φαίνεται να είναι αισθητά μικρότερο, με 14%. Παρατηρείται επομένως πως το γυναικείο φύλο θεωρεί ότι η διαδικασία της αναγνώρισης της ταυτότητας του βασίζεται κατά κύριο λόγο στην μοναδικότητα των βιομετρικών δεδομένων του, γεγονός που τα κάνει να υπερτερούν σε σύγκριση με τους κωδικούς πρόσβασης, οι οποίοι εύκολα μπορούν να χαθούν, να κλαπούν ή να παραβιαστούν. Την αντίληψη αυτή έρχονται να συμπληρώσουν τα υπόλοιπα ποσοστά της ερώτησης αυτής, τα οποία σε δεύτερο βέβαιο επίπεδο, αναδεικνύουν πως η επαλήθευση των δεδομένων από τα συστήματα γίνεται με ταχείς διαδικασίες με ποσοστό 16%, καθώς επίσης φαίνεται πως το γυναικείο φύλο αισθανόταν κουρασμένο από την απομνημόνευση των κωδικών. Αυτό αποτυπώνεται με το τρίτο μεγαλύτερο ποσοστό στο 12%. Εύκολα μπορεί να ειπωθεί πως οι γυναίκες εκλαμβάνουν τα πλεονεκτήματα των βιομετρικών συστημάτων με περισσότερη ευκολία απ' ότι οι άνδρες, γεγονός που παρουσιάζει μια μεγαλύτερη ανάγκη των γυναικών για προστασία και ευκολία επαλήθευσης. Αντιθέτως, η επόμενη ερώτηση υποδεικνύει «Ποιο από τα παρακάτω θεωρείτε το σημαντικότερο μειονέκτημα για τη χρήση των βιομετρικών συστημάτων:». Από το ποσοστό των αποτελεσμάτων προέκυψε πως το σημαντικότερο μειονέκτημα τους είναι ο κίνδυνος της παραβίασης των προσωπικών δεδομένων με ποσοστό στο 57%. Ιδιαίτερα, η ηλικιακή ομάδα 18-22 με ποσοστό 33% θεωρεί ως σημαντικότερο μειονέκτημα των βιομετρικών συστημάτων τον κίνδυνο για την παραβίαση των προσωπικών τους δεδομένων. Στην αντίστοιχη επιλογή, το ποσοστό των υπόλοιπων ηλικιακών ομάδων φαίνεται να είναι αισθητά μικρότερο με 13% να ανήκει στους 23-30, 11% στους 31-45 και μόλις 3% στους 46-60.

Παρατηρείται επομένως, πως η ηλικιακή ομάδα 18-22 ανησυχεί για την πιθανότητα να πραγματοποιηθεί ο κίνδυνος, σε σύγκριση με κάποιο άλλο μειονέκτημα, όπως το υψηλό κόστος εγκατάστασης τους με ποσοστό 10%. Την αντίληψη αυτή έρχονται να συμπληρώσουν τα υπόλοιπα ποσοστά της ερώτησης αυτής, τα οποία σε δεύτερο βέβαιο επίπεδο, αναδεικνύουν τις μακροσκελείς διαδικασίες καταχώρησης τους, την δυσκολία εκμάθησης αλλά και το αίσθημα φόβου ή ανησυχίας που τους δημιουργείται. Γίνεται αντιληπτό, πως η ηλικιακή ομάδα 18-22 εκλαμβάνει τα μειονεκτήματα των βιομετρικών συστημάτων με την πιθανότητα παραβίασης των προσωπικών τους δεδομένων.
Η τελευταία ερώτηση της ενότητας αυτής αποτελεί συνέχεια της προηγούμενης, καθώς ζητήθηκε μόνο από τους χρήστες που επέλεξαν πως το σημαντικότερο μειονέκτημα των βιομετρικών συστημάτων είναι το αίσθημα φόβου ή ανησυχίας, να αιτιολογήσουν την άποψη τους. Το 22% των ερωτηθέντων αισθάνεται φόβο πως κατά την διαδικασία της ταυτοποίησης, τα δεδομένα τους καταχωρούνται σε βάσεις δεδομένων και εύκολα αποκτούν πρόσβαση τρίτοι, ενώ το ίδιο πάλι ποσοστό ανησυχεί πως είναι εύκολο να αποκτηθούν πληροφορίες από τις εκάστοτε υπηρεσίες εν αγνοία των χρηστών. Ιδιαίτερα, οι φοιτητές που εργάζονται ως ιδιωτικοί υπάλληλοι, ανησυχούν περισσότερο με ποσοστό 20% πως τα βιομετρικά τους δεδομένα καταχωρούνται σε βάσεις δεδομένων, στις οποίες εύκολα μπορεί να έχει πρόσβαση κάποιος τρίτος. Στην αντίστοιχη επιλογή, παρατηρείται πως καμία άλλη κατηγορία επαγγέλματος δεν ανησυχεί σχετικά με το αυτό, με ποσοστό 0%. Έτσι, διαφαίνεται πως οι ιδιωτικοί υπάλληλοι, εκτός από τις βάσεις δεδομένων, παρουσιάζουν έντονη ανησυχία, με μικρότερο ποσοστό στο 10%, σχετικά με το αίσθημα ελέγχου που τους δημιουργείται όταν ταυτοποιούνται με τα βιομετρικά τους δεδομένα, την άγνοια των χρηστών, διότι θεωρούν πως ανά πάσα στιγμή μπορεί να αποκτώνται πληροφορίες χωρίς την συγκατάθεση του και τέλος πως σε αντίθεση με τους κωδικούς πρόσβασης, τα βιομετρικά δεδομένα εάν παραβιαστούν δεν μπορούν να αλλάξουν. Συνεπώς, οι φοιτητές αυτοί αισθάνονται περισσότερο εκτεθειμένοι όταν ταυτοποιούνται με βάση τα βιομετρικά τους δεδομένα, γι' αυτό και παρουσιάζουν μεγαλύτερη ανησυχία. Τα αυξημένα ποσοστά ανησυχίας των χρηστών παρατηρούνται και στις κατηγορίες

επαγγέλματος του πατέρα αλλά και στο Τμήμα φοίτησης των χρηστών. Αρχικά, από τα διαγράμματα του επαγγέλματος του πατέρα, διαφαίνεται πως, από τους ελεύθερους επαγγελματίες προέρχονται οι περισσότερες ανησυχίες με ποσοστό 9% σχετικά με τις πληροφορίες που μπορούν να αποκτηθούν εν αγνοία των χρηστών και πιθανά αυτές μπορούν να τους στοχοποιήσουν και να χρησιμοποιηθούν εις βάρος τους, το 7% πως καταχωρούνται σε βάσεις δεδομένων, ενώ το 5% ανησυχεί για το πόσο παραμένουν ιδιωτικά καθώς και για την διαδικασία της ταυτοποίησης. Μερικοί χρήστες σχολιάζουν πως *«πάντα υπάρχει μια ανησυχία σε περίπτωση που κάποιος τα χρησιμοποιήσει για να στραφεί εναντίον σου»* και *«μπορεί κάποιος να χρησιμοποιήσει χωρίς την θέλησή μου.»*. Θεωρούν επομένως πως από την στιγμή που κάτι ψηφιοποιείται μπορεί ανά πάσα στιγμή να χρησιμοποιηθεί για οποιονδήποτε σκοπό από τον οποιονδήποτε. Αρκετά κοντά στο 9% βρίσκεται το ποσοστό 5% που προέρχεται από τους φοιτητές που ο πατέρας τους εργάζεται ως ιδιωτικός υπάλληλος. Το ποσοστό αυτό σκιαγραφεί μια ανησυχία των χρηστών πως οι βιομετρικές τεχνικές προξενούν προβλήματα στην υγεία. Η έντονη αυτή ανησυχία των χρηστών δεν παρατηρείται μόνο στην Ελλάδα αλλά και σε σχετική έρευνα που έλαβε χώρα στην Γαλλία. Συγκεκριμένα, το 14% των χρηστών σε έρευνα που διεξήχθη από το Université de Caen Basse-Normandie, ανησυχεί σχετικά με την υγιεινή των τεχνικών αυτών και συγκεκριμένα για τεχνικές όπως η ανάλυση της ίριδας του ματιού. Σύμφωνα με την έρευνα αυτή, δεν έχει παρατηρηθεί κάποια σωματική βλάβη ή κάποιο πρόβλημα υγείας των χρηστών που χρησιμοποιούν τις τεχνικές αυτές (El-abed, Giot, Hemery & Rosenberger, 2014). Επιπλέον, με το Τμήμα φοίτησης των συμμετεχόντων-ουσών στην έρευνα, αυτό που παρουσιάζει μεγαλύτερη σημασία για να λεχθεί είναι πως κανείς θα περίμενε τα τεχνολογικά τμήματα να ανησυχούν περισσότερο για την πιθανότητα παραβίασης των δικαιωμάτων τους. Αντιθέτως, μόνο δύο τεχνολογικά και ένα θεωρητικό με όχι και τόσο υψηλά ποσοστά, εκφράζουν τις ανησυχίες τους για την παραβίαση των δικαιωμάτων τους. Τα ποσοστά αυτά ενισχύονται από τα σχόλια των χρηστών στην συγκεκριμένη ερώτηση όπως : *«Από την στιγμή που είναι κατοχυρωμένα τα προσωπικά σου δεδομένα σε μια βάση δεδομένων, πάντα υπάρχει μια ανησυχία σε περίπτωση που κάποιος τα*

χρησιμοποιήσει για να στραφεί εναντίον σου.», «Καταχωρούνται προσωπικές μου πληροφορίες που δεν ξέρω πως μπορούν να χρησιμοποιηθούν». Τα ευρήματα της έρευνας μας επιβεβαιώνονται από την έρευνα που διεξήχθη από τους (Muir & Keough, 2016), η οποία συμπληρώνει τους φόβους των φοιτητών-τριών. Αναλυτικότερα, το 24% των χρηστών δήλωσε ότι η αποθήκευση των βιομετρικών τους σε βάσεις δεδομένων εξυπηρετεί κυβερνητικές και εταιρικές σκοπιμότητες. Ουσιαστικά ο φόβος των χρηστών στην Ελλάδα επιβεβαιώνεται από τις αντίστοιχες έρευνες στο εξωτερικό, που δείχνουν πως τα δεδομένα των χρηστών αποθηκεύονται σε βάσεις δεδομένων και είναι στην διάθεση την εκάστοτε κυβέρνησης για τα «αξιοποιήσει» ανάλογα με τις ανάγκες της. Το δεύτερο μεγαλύτερο ποσοστό στην ερώτηση αυτή καταγράφηκε πάλι από τους φοιτητές που εργάζονται ως ιδιωτικοί υπάλληλοι, με το 10% να θεωρεί πως οι βιομετρικές τεχνικές δίνουν την αίσθηση του μόνιμου ελέγχου από τρίτους *«Ψηφιοποιώ τα δικά μου χαρακτηριστικά, δημιουργώντας data τα οποία μπορεί κάποιος να χρησιμοποιήσει χωρίς την θέλησή μου.».* Ένα χαρακτηριστικό παράδειγμα που ανέφερε χρήστης είναι μια εφαρμογή, η οποία αποκαλύφθηκε πως αποθήκευε τις φωτογραφίες των χρηστών σε βάσεις δεδομένων και μπορούν να τις χρησιμοποιούν για επίτευξη δικών τους σκοπών χωρίς να το γνωρίζουν οι χρήστες. Τέτοια περιστατικά μπορεί να συμβαίνουν σε οποιαδήποτε εφαρμογή και η πιθανότητα αυτή δημιουργεί περαιτέρω ανησυχία στους χρήστες. Άλλη μια ανησυχία που προέρχεται από τους ίδιους τους φοιτητές-τριες με ποσοστό 10% είναι πως σε αντίθεση με τους κωδικούς πρόσβασης, τα βιομετρικά δεδομένα αν παραβιαστούν δεν αλλάζουν, επομένως ο χρήστης είναι περισσότερο εκτεθειμένος στον κίνδυνο της παραβίασης της ιδιωτικότητας του. Συνοπτικά, όσα έρχονται στην διαφάνεια που αλλοιώνουν την υψηλή προστασία που «υπόσχονται» τα βιομετρικά συστήματα, διότι πρόκειται για μοναδικά χαρακτηριστικά του κάθε ανθρώπου, ο φόβος και η ανησυχία των χρηστών θα μεγεθύνεται.

Η <u>ενότητα Δ</u> με τίτλο «Αξιοπιστία των Βιομετρικών Συστημάτων» αποβλέπει στο αν και κατά πόσοι οι χρήστες τα θεωρούν αξιόπιστα και βοηθητικά. Από την πρώτη ερώτηση της ενότητας «Θεωρείτε τα Βιομετρικά Συστήματα πιο αξιόπιστη

μέθοδο ταυτοποίησης από το password/PIN;», διαφαίνεται πως το 38% των ερωτηθέντων τα θεωρεί μια αξιόπιστη μέθοδο ταυτοποίησης. Αντίστοιχα, το επόμενο ποσοστό δηλώνει «έτσι κι έτσι» με ποσοστό 28%, ενώ το 23% τα θεωρεί «την πιο αξιόπιστη» διαδικασία συγκριτικά με τους κωδικούς. Ταυτόχρονα, υπάρχουν και τα ποσοστά που εναντιώνονται στο θετικό τους πρόσημα, τα οποία με ποσοστό 7% και 3% τα θεωρούν «λιγότερο» και «καθόλου» αξιόπιστα αντίστοιχα. Παρατηρείται επομένως πως το μεγαλύτερο ποσοστό των χρηστών φαίνεται να είναι κουρασμένο από την πληθώρα των κωδικών πρόσβασης, με αποτελέσματα να αναζητά πιο γρήγορες και αξιόπιστες μεθόδους ταυτοποίησης. Η επόμενη ερώτηση μορφολογικά δεν διαφέρει από αυτή, αλλά αποζητά μια κατεύθυνση του κοινού σχετικά με το αν «Θεωρείτε τα Βιομετρικά Συστήματα πιο ασφαλή μέθοδο ταυτοποίησης από το password/PIN». Όπως προηγουμένως, έτσι και τώρα, το 37% των ερωτηθέντων δηλώνει πως τα θεωρεί ασφαλή μέθοδο ταυτοποίησης. Την αντίληψη αυτή έρχονται να συμπληρώσουν, το 27% που δηλώνει «έτσι κι έτσι», το 21% που τα θεωρεί «πάρα πολύ» ασφαλείς μεθόδους, ενώ το 10% τα βρίσκει «λιγότερο» ασφαλή και το 5% που δεν τα εμπιστεύεται καθόλου. Συνεπώς, γίνεται αντιληπτό, πως το υψηλότερο ποσοστό των χρηστών φαίνεται να βασίζεται στην μοναδικότητα των βιομετρικών δεδομένων τους όπου σε σύγκριση με τους κωδικούς πρόσβασης υπερτερούν, καθώς είναι πιο δύσκολο να χαθούν, να κλαπούν ή να παραβιαστούν.
Τέλος, η ενότητα ολοκληρώνεται με την ερώτηση «Θεωρείτε τα Βιομετρικά Συστήματα ως μια πιο αξιόπιστη λύση προκειμένου να μειωθούν οι κλοπές (passwords/Pins);». Το 68% των ερωτηθέντων θεωρεί πως τα βιομετρικά συστήματα μπορούν να βοηθήσουν στην επίλυση του προβλήματος αλλά δεν μπορούν να είναι η λύση στο ζήτημα. Αντίστοιχα, το 25% δηλώνει πως τα βιομετρικά συστήματα μπορούν να διαδραματίζουν καθοριστικό ρόλο στο ζήτημα αυτό, ενώ το 7% εναντιώνεται με την θέση αυτή. Ιδιαίτερα, η ηλικιακή ομάδα 18-22, δίνει περισσότερη έμφαση στο γεγονός πως τα βιομετρικά συστήματα δεν είναι ικανά να εξαλείψουν τις κλοπές, αλλά σε πρώτο επίπεδο θεωρούνται ένα επιπρόσθετο μέτρο προστασίας. Στην αντίστοιχη επιλογή, το 11% θεωρεί πως μπορούν να επιλύσουν το ζήτημα αυτό, ενώ το 3% διαφωνεί πλήρως.

Παρατηρείται επομένως, πως η ηλικιακή ομάδα υποστηρίζει εντονότερα πως έτσι όπως τα γνωρίζουν δεν μπορούν τα βιομετρικά συστήματα να απαλείψουν τις κλοπές, μπορούν όμως να τις μειώσουν. Την αντίληψη αυτή υποστηρίζουν και οι υπόλοιπες ηλικιακές ομάδες. Τα ποσοστά που προέκυψαν από την έρευνα φαίνεται να επιβεβαιώνονται από μια έρευνα που έλαβε χώρα το 2015 στην Αμερική. Αναλυτικότερα, το 54% των Αμερικανών πολιτών δήλωσε πως η χρήση μηχανών για αναγνώριση προσώπου στα εργασιακά περιβάλλοντα είναι ικανή να μειώσει τις κλοπές, αρκεί να τηρεί τις κατάλληλες προϋποθέσεις και να μην αποτελεί μέσο ελέγχου της δουλειάς των υπαλλήλων (Lee, 2016). Βλέπουμε λοιπόν πως οι χρήστες είναι πρόθυμοι να μοιραστούν τα βιομετρικά τους δεδομένα προκειμένου να μειωθούν οι κλοπές, αυτό όμως προϋποθέτει πως οι κάμερες δεν θα χρησιμοποιούν εναντίον τους για να επιβλέπονται κατά την εργασία τους και να κρίνονται εξ αυτών. Αυτό σημαίνει πως σε τέτοιες περιπτώσεις δεν πρέπει τα βιομετρικά συστήματα να λειτουργούν ως εύκολο μέσο κάτω από το οποίο θα υποκινούνται περαιτέρω σκοπιμότητες. Η ανάγκη των χρηστών για περισσότερη ασφάλεια, είναι κάτι που θα πρέπει να δρομολογηθεί από τους εκάστοτε υπεύθυνους.

Η ενότητα Ε με τίτλο «Πρόθεση χρήσης των Βιομετρικών Συστημάτων» σκιαγραφεί σε τι επίπεδο βρίσκονται οι χρήστες απέναντι στα βιομετρικά συστήματα. Από την πρώτη ερώτηση «Πιστεύετε πως η χρήση των Βιομετρικών Συστημάτων μπορεί να κάνει πιο εύκολη τη καθημερινότητα σας;», παρατηρείται πως το 85% των ερωτηθέντων υποστηρίζει πω τα βιομετρικά συστήματα απλοποιούν την καθημερινότητα, ενώ το 15% έχει αντίθετη άποψη. Ιδιαίτερα, η ηλικιακή ομάδα 18-22 υποστηρίζει εντονότερα την άποψη αυτή, με ποσοστό 49%. Στην αντίστοιχη επιλογή, φαίνεται να είναι αισθητά μικρότερο το ποσοστό των χρηστών που θεωρούν πως δεν απλοποιείται η καθημερινότητα του, με ποσοστό 5%. Παρατηρείται επομένως, πως οι βιομετρικές τεχνικές επειδή είναι εύχρηστες έχουν απλοποιήσει την καθημερινότητα των χρηστών μεταξύ 18-22. Την αντίληψη αυτή έρχονται να συμπληρώσουν οι υπόλοιπες ηλικιακές ομάδες, όπου το 19% ανήκει στους 23-30, το 13% στους 31-45 και το 4% στους 46-60. Τα περισσότερα ποσοστά που προέκυψαν από την παρακάτω ερώτηση σχετικά με

το «Σε ποιες υπηρεσίες θεωρείτε ότι θα ήτανε καλό να ενσωματωθούν;», αφορούν τις υπηρεσίες στις οποίες δεν είναι αναγκαία η ενσωμάτωση τους. Ουσιαστικά, το 14% των ερωτηθέντων υποστηρίζει ότι τα αεροδρόμια χρειάζεται να αξιοποιούν τα βιομετρικά συστήματα, επομένως κρίνεται αναγκαίο να ενσωματωθούν εκεί. Παράλληλα με τα αεροδρόμια, το 13% των ερωτηθέντων κρίνει απαραίτητη την ενσωμάτωσή τους στις τράπεζες. Ιδιαίτερα, οι γυναίκες με ποσοστό 50% και 53% δίνουν περισσότερη έμφαση στην ενσωμάτωση τους στις τράπεζες και στο αεροδρόμιο αντίστοιχα προκειμένου να διαφυλαχθεί η ασφάλεια τους. Στην αντίστοιχη επιλογή, το ποσοστό των ανδρών φαίνεται να είναι αισθητά μικρότερο, με 29% στις τράπεζες και το αεροδρόμιο. Και από τα δύο γραφήματα που απαντούν στο ίδιο ερώτημα, παρατηρείται πως το ανδρικό φύλο αντιμετωπίζει την προοπτική αυτή με επιφύλαξη αν και είναι θετικό στην ένταξη αυτή, παρόλα αυτά αρκετοί δήλωσαν πως δεν είναι σε μεγάλο βαθμό υπέρμαχοι καθώς τέτοιες δυνατότητες παραβιάζουν την ιδιωτικότητα τους και θα είναι προτιμότερο να χρησιμοποιούνται μόνο σε συσκευές του εκάστοτε ανθρώπου. Συνεπώς από τις δύο περιπτώσεις προκύπτει πως το γυναικείο φύλο υποστηρίζει σε μεγαλύτερο βαθμό την ενσωμάτωση στις υπηρεσίες αυτές, διότι ανησυχεί περισσότερο για το επίπεδο ασφάλειας αυτών και των δεδομένων τους. Σύμφωνα και με την έρευνα του (Ponemon, 2013), παρουσιάζει ένα μεγάλο ποσοστό των ενηλίκων στην Ευρωπαϊκή Ένωση, να αισθάνεται άνετα με τις βιομετρικές τεχνολογίες και με το γεγονός ότι χρησιμοποιούνται σε χώρους που θεωρούνται ιδιαίτερα ασφαλείς όπως αεροδρόμια ή χρειάζονται μεγαλύτερη προστασία. Διαφαίνεται λοιπόν η ανάγκη των χρηστών για διασφάλιση της προστασίας τους σε τέτοιους χώρους. Δεδομένου αυτής της «ανάγκης» των χρηστών για διεύρυνση της ασφάλειας τους μέσω των βιομετρικών τους δεδομένων, καλό θα ήτανε οι αρμόδιοι της κάθε υπηρεσίες, να λαμβάνουν υπόψη τους τις σκέψεις των χρηστών για τη μεγαλύτερη ασφάλεια τους. Επιπλέον, η ηλικία διαφαίνεται να λειτουργεί ως παράγοντας διαφοροποίησης, καθώς η ηλικιακή ομάδα 18-22 κρίνει αναγκαία την ενσωμάτωση τους στο αεροδρόμιο με ποσοστό 45%, ενώ στην αντίστοιχη θέση το 9% δεν το κρίνει αναγκαίο. Την αντίληψη αυτή συμμερίζονται και οι υπόλοιπες ηλικιακές ομάδες όπου το 19% ανήκει στους 23-30, το 14% στους 31-45 και το 5%

στους 46-60. Παρατηρείται επομένως πως η ηλικιακή ομάδα 18-22 θεωρεί αναγκαία την ενσωμάτωση αυτή, γεγονός που παρουσιάζει εντονότερα την επιθυμία τους για περισσότερη ασφάλεια στο αεροδρόμιο, καθώς πρόκειται για μια υπηρεσία στην οποία αλληλεπιδρούν ταυτόχρονα πολλοί άνθρωποι και συχνά είναι στόχος επιθέσεων. Από τα σχόλια των χρηστών στην εν λόγο ερώτηση συμπεραίνεται πως υπάρχουν άνθρωποι που θεωρούν ότι μπορεί μέσω της ενσωμάτωσης τους να αυξηθεί το επίπεδο ασφάλεια και ταυτοποίησης των επιβατών, όμως και πάλι τα βιομετρικά συστήματα παραβιάζουν την ιδιωτικότητα καθώς δεν μπορεί να διασφαλιστεί πως αυτά θα χρησιμοποιηθούν εξ' ολοκλήρου για σκοπούς εξακρίβωσης στοιχείων. Μια διαφορετική προσέγγιση σχετικά με την ενσωμάτωση των βιομετρικών συστημάτων σε ορισμένες υπηρεσίες, προκύπτει από το έτος σπουδών των φοιτητών. Το 21% των φοιτητών που διανύουν το πρώτο έτος κρίνει αναγκαία την ενσωμάτωση τους στα νοσοκομεία, γεγονός που φανερώνει την ανησυχία τους σχετικά με την ασφάλεια των αρρώστων. Τα ευρήματα της έρευνας μας απορρίπτονται σε έρευνα που διεξήχθη τον Μάρτιο του 2016 στο Ηνωμένο Βασίλειο. Από την ανάλυση αυτή προέκυψε πως σχεδόν τα 2/3 όλων των καταναλωτών υποστηρίζουν τις βιομετρικές τεχνολογίες για αλτρουιστικούς σκοπούς στην ιατρική έρευνα 58%, ενώ με ποσοστό 64% οι χρήστες έχουν περισσότερη εμπιστοσύνη στις υπηρεσίας με σημαντικές λειτουργίες όπως τα νοσοκομεία. Παρατηρείται λοιπόν πως στην Ελλάδα μια τέτοια ενσωμάτωση βρίσκεται σε διαδικασίες έρευνας με πολλές αντίθετες απόψεις σχετικά με την αναγκαιότητα της αφού υπάρχουν και πιο σημαντικές υπηρεσίες. Βλέπουμε πως κάτι τέτοιο δεν συμβαίνει στο Ηνωμένο Βασίλειο καθώς εκεί οι χρήστες και ειδικότερα ένα ποσοστό μεγαλύτερο από το μισό, θεωρεί πως τα νοσοκομεία διαθέτουν ένα ασφαλέστερο σύστημα προστασίας των βιομετρικών τους δεδομένων. Κάτι που σε μια χώρα έχει προαχθεί και κερδίσει την εμπιστοσύνη των χρηστών, σε μια άλλη παρατηρείται μια θετική στάση σε μια πιθανή ένταξη μόνο από τους πρωτοετείς φοιτητές. Συνεπώς, οι πρωτοετείς φοιτητές στέκονται με περισσότερη θετικότητα απέναντι σε πιθανή βελτίωση ορισμένων υπηρεσιών μέσω της χρήσης βιομετρικών τεχνικών.

Από την παρακάτω ερώτηση «Σε ποιο βαθμό αισθάνεστε έτοιμοι να σταματήσετε να χρησιμοποιείτε τα passwords/Pins και να τα αντικαταστήσετε με τις βιομετρικές τεχνικές;», το 31% των συμμετεχόντων βρίσκεται σε μια ενδιάμεση κατάσταση, το 24% των χρηστών αισθάνεται αρκετά έτοιμο σε μια πιθανή αντικατάσταση, ενώ το 17% δεν αισθάνεται σχεδόν καθόλου έτοιμο για μια τέτοια ανταλλαγή και το 16% δηλώνει «Πάρα Πολύ» έτοιμο για την μόνιμη αντικατάσταση τους. Ιδιαίτερα, οι πρωτοετείς φοιτητές υποστηρίζουν με ποσοστό 11% να βρίσκονται στην μέση. Παρατηρείται επομένως, πως οι πρωτοετείς φοιτητές δεν έχουν πεισθεί πως τα βιομετρικά συστήματα θα αλλάξουν την καθημερινότητα τους, αλλά δεν είναι και αντίθετη σε μια πιθανή αντικατάσταση. Συνεπώς, οι πολιτικές που προάγουν θα πρέπει να στραφούν στους χρήστες που είναι δύσπιστοι ή βρίσκονται σε μια ενδιάμεση κατάσταση. Τα ποσοστά των χρηστών που «πιστεύουν» στα βιομετρικά συστήματα είναι ικανοποιητικά αλλά όχι δυναμικά και χρειάζονται ενίσχυση. Μια παρόμοια κατάσταση φαίνεται πως είναι πιο ξεκάθαρη στην Αγγλία. Συγκεκριμένα, το 61% των χρηστών προτιμάει τα δακτυλικά αποτυπώματα, καθώς αισθάνονται κουρασμένοι από τη χρήση κωδικών, ειδικότερα σε σχέση με τις τράπεζες και την ασφάλεια των δεδομένων τους. Ουσιαστικά, οι χρήστε είναι κουρασμένοι από την απομνημόνευση των κωδικών για να ταυτοποιηθούν και είναι πρόθυμοι να τους αντικαταστήσουν για λόγους ευχρηστίας, ασφάλειας και ευκολίας (Technologies & Sentiments, 2016). Παρατηρείται πως στην Ελλάδα εν έτη 2020, υπάρχει μια αβεβαιότητα και ένας φόβος των χρηστών να αντικαταστήσουν τα passwords/Pins τους με τις βιομετρικές τεχνικές, ενώ στην Αγγλία ήδη οι χρήστες πριν από 4 χρόνια ήτανε πρόθυμοι να απαλλαγούν από την απομνημόνευση των κωδικών και να διευκολύνουν την καθημερινότητα τους. Υπάρχει μια μεγάλη διαφοροποίηση της νοοτροπίας και των συνθηκών μεταξύ των χωρών, οι οποίοι απεικονίζεται μέσα από τα βιομετρικά συστήματα. Στην Ελλάδα κατά κύριο λόγο η αντίληψη των βιομετρικών συστημάτων δεν γίνεται κατανοητή, καθώς οι επιλογές πολλών χρηστών δείχνουν ένα αίσθημα φόβου για την προστασία της ιδιωτικότητας τους που συνδυάζεται με ευκολία πρόσβασης στο κινητό (ξεκλείδωμα κινητού τηλεφώνου με δακτυλικό αποτύπωμα). Οι πολιτικές που θα προάγουν τα

Βιομετρικά Συστήματα πρέπει να απευθυνθούν με μεγαλύτερη ακρίβεια και σαφήνεια απέναντι στους χρήστες ανεξάρτητα των δημογραφικών στοιχείων. Από τα παρακάτω αποτελέσματα, παρατηρείται πως «Σε ποιο βαθμό είστε πρόθυμοι να υιοθετήσετε τη βιομετρική ταυτότητα για τις ηλεκτρονικές τραπεζικές σας συναλλαγές;» οι ερωτηθέντες είναι περισσότερο σκεπτικοί σε μια πιθανή ενσωμάτωση, με ποσοστό 24%, το οποίο είναι το ίδιο με τους χρήστες που δηλώνουν «Πολύ» σε μια τέτοια υιοθέτηση. Αξίζει να σημειωθεί πως τα ποσοστά που δείχνουν μια αρνητική τάση στην υιοθέτηση αυτή είναι εξίσου σημαντικά και υψηλά, αφού ανέρχονται στο 16%. Πρόκειται για μια υιοθέτηση που απαιτεί μια ολόκληρη διαδικασία για να επιτευχθεί. Το σημαντικότερο είναι η αντίληψη των χρηστών, στην οποία πρέπει οι πολιτικές που προάγουν τα βιομετρικά συστήματα να επικεντρωθούν για να καταστήσουν σαφές τι σημαίνει επί της ουσίας μια τέτοια υιοθέτηση, ώστε να μπορούν να κρίνουν.
‘Άλλη μια ερώτηση σχετικά με αντικατάσταση της υπάρχουσας κατάστασης, φαίνεται να διαφοροποιεί την μέχρι τώρα άποψη των χρηστών. Η ερώτηση είναι «Σε ποιο βαθμό είστε πρόθυμοι να αντικαταστήσετε τα διαβατήρια και τις ταυτότητες με τα βιομετρικά σας χαρακτηριστικά, όταν πρόκειται για τα ταξίδια εντός ή εκτός της Ε.Ε ;» Παρόλο που πρόκειται για μια ολιστική αλλαγή του τρόπου ταυτοποίησης των επιβατών, το 26% των ερωτηθέντων δηλώνει «πολύ», υποστηρίζοντας μια τέτοια αλλαγή. Την αντίληψη αυτή έρχονται να συμπληρώσουν τα υπόλοιπα ποσοστά της ερώτησης , όπου το 23% είναι ιδιαίτερα σκεπτικό σε μια τέτοια αλλαγή, το 19% διαφωνεί κάθετα στην αντικατάσταση του διαβατηρίου, ενώ 17% των χρηστών πιστεύει πως αποτελεί καινοτομία, η οποία προασπίζει την ασφάλεια των επιβατών και των δεδομένων τους και το 15% πως είναι «λίγο» πρόθυμο σε μια τέτοια διαφοροποίηση. Κρίνεται απαραίτητη η ενημέρωση των χρηστών, διότι πρόκειται για μια τεχνολογία που στην Ελλάδα δεν εδραιώνεται αρκετά χρόνια, όπως σε άλλες χώρες, επομένως απαιτεί μια στοιχειώδη ενημέρωση για τις δυνατότητες και τις ανησυχίες των βιομετρικών συστημάτων, προκειμένου οι χρήστες να δρουν εν γνώσει τους.
Η τελευταία ερώτηση με την οποία ολοκληρώνεται η ενότητα αυτή ζητά από τους χρήστες να καταγράψουν αν «Υπάρχει κάποια δραστηριότητα/υπηρεσία για την

οποία είστε πρόθυμοι να χρησιμοποιήσετε άμεσα βιομετρικές τεχνικές;». Το 22% των ερωτηθέντων δηλώνουν πως δεν υπάρχει κάποια δραστηριότητα για την οποία είναι διατιθέμενοι να απαλλαχθούν από τους κωδικούς πρόσβασης και να ταυτοποιούνται μόνο με τα βιομετρικά τους δεδομένα. Οι πολιτικές που ασχολούνται με τα βιομετρικά συστήματα οφείλουν να αντιστρέψουν το ποσοστό αυτό, καθώς υποδηλώνει αβεβαιότητα για το καινούργιο. Αντιθέτως, το 14% των ερωτηθέντων δηλώνει ιδιαίτερα πρόθυμο να ταυτοποιείται μόνο με βάση τα βιομετρικά του δεδομένα στις υπηρεσίες της τράπεζες, καθώς έτσι θεωρεί πως αυξάνεται το επίπεδο ασφάλειας του. Εξίσου σημαντική είναι η τάση των χρηστών για απαλλαγή των διαβατηρίων στο αεροδρόμιο και κατ' επέκταση η ταυτοποίηση στο αεροπλάνο να γίνεται αποκλειστικά με τις βιομετρικά δεδομένα του εκάστοτε επιβάτη. Η επιλογή αυτή βέβαια έρχεται σε αντίθεση με τα αποτελέσματα της προηγούμενης ερώτησης. Εντύπωση δημιουργεί το 6% των χρηστών που δηλώνουν πως προκειμένου να εξοικονομήσουν χρόνο, αισθάνονται πρόθυμοι να χρησιμοποιήσουν άμεσα τις βιομετρικές τεχνικές.

Η ενότητα ΣΤ με τίτλο «Προστασία της ιδιωτικότητας(privacy) και Ασφάλεια (security)» αποτελείται από ερωτήσεις, οι οποίες περιγράφουν την υπάρχουσα κατάσταση των χρηστών απέναντι στα βιομετρικά συστήματα σχετικά με την προστασία των δεδομένων τους. Συγκεκριμένα, από την πρώτη ερώτηση της ενότητας «Κατά τη γνώμη σας η χρήση των παρακάτω βιομετρικών τεχνικών δεν αυξάνουν τον κίνδυνο παραβίασης της ιδιωτικότητας;», δεν προκύπτει κάποια ξεκάθαρη κατάσταση. Παρατηρείται πως η απάντηση «ναι» καταγράφει ποσοστά 7%, ενώ το «όχι» 6%. Παρατηρείται πως όλες οι βιομετρικές τεχνικές δεν αυξάνουν τον κίνδυνο παραβίασης της ιδιωτικότητας των δεδομένων των χρηστών.

Η επόμενη ερώτηση σχετίζεται με την ασφάλεια των χρηστών και συγκεκριμένα «Κατά τη γνώμη σας η χρήση των παρακάτω βιομετρικών τεχνικών αυξάνουν το επίπεδο ασφάλειας του χρήστη από πιθανές απειλές;». Το 10% των ερωτηθέντων θεωρεί πως η ανάλυση DNA και η ανάλυση της ίριδας ματιού αυξάνουν το επίπεδο ασφάλειας συγκριτικά με τις υπόλοιπες τεχνικές. Επιπλέον, το δακτυλικό αποτύπωμα και η αναγνώριση συγκαταλέγονται στις τεχνικές με το υψηλότερο

επίπεδο ασφάλειας από πιθανές απειλές, με ποσοστό 9% και 8% αντίστοιχα. Ιδιαίτερα, η ηλικιακή ομάδα 18-22 υποστηρίζει πως το δακτυλικό αποτύπωμα σε σχέση με τις άλλες βιομετρικές τεχνικές, δημιουργεί αίσθημα ασφάλειας απέναντι σε μια πιθανή απειλή. Στην αντίστοιχη επιλογή, το ποσοστό που δηλώνει όχι φαίνεται να είναι αισθητά μικρότερο, με 16%. Παρατηρείται επομένως πως η ηλικιακή ομάδα 18-22 λειτουργεί ως παράγοντας διαφοροποίησης, μήπως επειδή τα θεωρούν εύκολα στη χρήση τους και τα έχουν υιοθετήσει με μεγαλύτερη ευκολία στην καθημερινότητα τους, επομένως γιατί να μην είναι και ασφαλή;

Τέλος, με βάση την εμπειρία και την αντίληψη τους, οι συμμετέχοντες ρωτήθηκαν «Ποιες υπηρεσίες/οργανισμοί πιστεύετε ότι χρησιμοποιούν ισχυρές μεθόδους ασφάλειας και προστασίας της ταυτότητας σας:» και προέκυψε από το σύνολο των ερωτηθέντων με ποσοστό 16% πως αδιαμφισβήτητα οι δημόσιοι χώροι δεν χρησιμοποιούν καμία μέθοδο ασφάλειας της ταυτότητας των πολιτών. Στην αντίστοιχη επιλογή, το ποσοστό που θεωρεί πως χρησιμοποιούνται φαίνεται να είναι αισθητά μικρότερο, με 1%. Αντιθέτως, η τράπεζα σύμφωνα με το 14% των ερωτηθέντων είναι η υπηρεσία με το μεγαλύτερο ποσοστό, στην οποία οι χρήστες θεωρούν πως χρησιμοποιούνται ισχυρές μέθοδοι προστασίας της ταυτότητας. Ιδιαίτερα, οι γυναίκες με ποσοστό 54% υποστηρίζουν πως η τράπεζα αποτελεί την υπηρεσία που οι χρήστες θεωρούν πως οι μέθοδοι ασφαλείας είναι ισχυρότεροι από κάθε άλλη υπηρεσία. Στην αντίστοιχη επιλογή, το ποσοστό των ανδρών φαίνεται να είναι μικρότερο, με 31%. Παρατηρείται επομένως πως για το γυναικείο φύλο, φαίνεται πως έχει ιδιαίτερη σημασία η ασφάλεια της εκάστοτε υπηρεσίες για να εμπιστευτούν τα δεδομένα τους σε μεγαλύτερο βαθμό. Σε αντίθεση με τους άνδρες, που φαίνονται να μην ανησυχούν για το κατά πόσο είναι ή δεν είναι ασφαλές το σύστημα της τράπεζας και η στάση τους δικαιολογείται από τα σχόλια τους στην συγκεκριμένη ερώτηση: *Αν κάποιος χρησιμοποιεί ισχυρές μεθόδους όπως π.χ. ισχυρούς αλγόριθμους κρυπτογράφησης, δεν σημαίνει ότι μας παρέχει και την απαραίτητη ασφάλεια.*»

- «*Κανείς από αυτούς τους φορείς. Αυτό έχει αποδειχθεί πολλές φορές στο παρελθόν*»

- *«Κανένας οργανισμός δεν μπορεί να προστατευτεί από δόλιες ενέργειες, που θα είχαν ως αποτέλεσμα την υποκλοπή των στοιχείων αυτών. Δεν υπάρχει ισχυρή μέθοδος ασφαλείας με την παρούσα δομή του παγκόσμιου ιστού.»*
- *«Δε θεωρώ πως προστατεύεται εξολοκλήρου η ταυτότητα μου. Κράτος, τράπεζα, τηλεφωνικές εταιρίες θεωρώ πως έχουν πλήρη εικόνα της ταυτότητάς μου.»*

Τα ευρήματα αυτά εν μέρει επιβεβαιώνονται από την έρευνα του Santa (2016)που διεξήχθη στην Αμερική το 2016, στην οποία οι χρήστες δήλωσαν πως δεδομένου του υψηλού κινδύνου για κλοπή δεδομένων από τα τραπεζικά συστήματα, οι υπηρεσίες αυτές καλούνται να «δυναμώνουν» τα συστήματα τους ώστε να αποτρέπουν τις πιθανές απειλές και να καταστούν ασφαλέστερη την ταυτοποίηση με τα βιομετρικά τους χαρακτηριστικά. Ουσιαστικά, οι χρήστες εστιάζουν την προσοχή τους στις τράπεζες και στην ενδυνάμωση τους μέσω των βιομετρικών συστημάτων. Οι απόψεις τους συνάδουν ως προς τις τραπεζικές υπηρεσίες, όμως είναι ενδεικτικό ότι στην Αμερική θεωρούν πως το σύστημα της τράπεζας δεν παρέχει την ύψιστη ασφάλεια των δεδομένων τους, σε αντίθεση με το γυναικείο φύλο στην Ελλάδα που θεωρεί πως οι τράπεζες έχουν ισχυρότερα συστήματα ασφαλείας σε σχέση με άλλες υπηρεσίες. Επιπλέον, οι φοιτητές που εργάζονται και συγκεκριμένα ως ιδιωτικοί υπάλληλοι, φαίνεται να υποστηρίζουν με ποσοστό 27% πως οι εταιρίες κινητής τηλεφωνίας δεν χρησιμοποιούν ισχυρές μεθόδους ασφάλειας των δεδομένων των πελατών τους, ενώ θα ήτανε απαραίτητο καθώς πολλές φορές οι λόγοι επικοινωνίας είναι για διαφημιστικούς σκοπούς και προώθησης προϊόντων. Την αντίληψη αυτή έρχονται να συμπληρώσουν τα υπόλοιπα ποσοστά της ερώτησης αυτής, τα οποία σε δεύτερο βέβαιο επίπεδο, αναδεικνύουν πως καμία κατηγορία επαγγέλματος δεν θεωρεί πως οι εταιρίες κινητής τηλεφωνίας προασπίζουν την ασφάλεια των πελατών τους. Μόνο το 11% αυτών που εργάζονται ως άλλο, διατυπώνει μια αντίθετη γνώμη υπέρ των εταιριών κινητής τηλεφωνίας.

Από την τελευταία ενότητα Ζ, με τίτλο «Εμπιστοσύνη και Κοινωνικός

Έλεγχος» προκύπτουν τα ακόλουθα αποτελέσματα. Από την ερώτηση «Θα θέλατε να γνωρίζετε με ποιον τρόπο συγκεκριμένα θα αξιοποιηθούν τα βιομετρικά χαρακτηριστικά σας από τις υπηρεσίες που τα ζητούν;», το 97% των ερωτηθέντων υποστηρίζει πως θα ήθελε να γνωρίζει την μετέπειτα εξέλιξη των βιομετρικών του πληροφοριών. Ιδιαίτερα, οι γυναίκες με ποσοστό 61% δηλώνουν πως θέλουν να γνωρίζουν πως θα αξιοποιηθούν τα δεδομένα τους στην συνέχεια. Στην αντίστοιχη επιλογή, το ποσοστό των ανδρών φαίνεται να είναι αισθητά μικρότερο, με 34%. Παρατηρείται επομένως ότι η ανάγκη των γυναικών προέρχεται από την ανησυχία μήπως τα δεδομένα τους καταγραφούν σε άλλες βάσεις για μετέπειτα χρήση τους, όπως θα δούμε στην συνέχεια από τα γραφήματα. Συνεπώς, δικαιολογημένα, θέλουν να γνωρίζουν με ακρίβεια, αν τα δεδομένα που χρησιμοποιεί η εκάστοτε υπηρεσία, μετά την χρήση τους παραμένουν στις βάσεις δεδομένων τους. Εξίσου σημαντικά είναι τα χαμηλά ποσοστά των συμμετεχόντων που φαίνεται να έχουν καθολική εμπιστοσύνη στις υπηρεσίες και δεν ανησυχούν για τα βιομετρικά τους δεδομένα. Αυτό αποτυπώνεται από το 2% των ανδρών, το 1% των γυναικών και το 1% των άλλο, που δεν θέλουν να γνωρίζουν πως θα αξιοποιηθούν τα δεδομένα τους. Η επόμενη ερώτηση σχετικά με το αν «Έχετε εμπιστοσύνη ότι οι βιομετρικές πληροφορίες που θα αποκτηθούν από τις υπηρεσίες, θα χρησιμοποιηθούν μόνο για σκοπούς εξακρίβωσης» συμπληρώνει την προηγούμενη ερώτηση. Το 83% των ερωτηθέντων δεν εμπιστεύεται τις υπηρεσίες που αποκτούν τα βιομετρικά τους δεδομένα. Υπάρχει πάντα ο φόβος πως οι βιομετρικές πληροφορίες δεν θα χρησιμοποιηθούν μόνο για σκοπούς εξακρίβωσης. Αντιθέτως, το 17% των συμμετεχόντων εμπιστεύονται καθολικά την εκάστοτε υπηρεσία. Ιδιαίτερα, οι γυναίκες με ποσοστό 53% υποστηρίζουν που δεν εμπιστεύονται τις υπηρεσίες ότι θα χρησιμοποιήσουν τα βιομετρικά τους δεδομένα μόνο για σκοπούς ταυτοποίησης. Στην αντίστοιχη επιλογή, το ποσοστό των ανδρών φαίνεται να είναι αισθητά μικρότερο, με 29%. Εύκολα μπορεί να ειπωθεί πως οι γυναίκες εκλαμβάνουν τον κίνδυνο των βιομετρικών συστημάτων με περισσότερη ευκολία απ' ότι οι άνδρες, γεγονός που παρουσιάζει μια μεγαλύτερη ανάγκη των γυναικών για προστασία και διασφάλιση του απορρήτου. Παράλληλα με την

δυσπιστία που προέρχεται από τις υπηρεσίες που χρησιμοποιούν τα βιομετρικά δεδομένα των χρηστών, τίθεται το ερώτημα αν «Πιστεύετε πως η χρήση των βιομετρικών συστημάτων μπορεί να οδηγήσει στην παραβίαση της ιδιωτικής σας ζωής;». Αδιαμφισβήτητα, το 82% των ερωτηθέντων θεωρεί πως η χρήση των βιομετρικών συστημάτων μπορεί να οδηγήσει στην παραβίαση της ιδιωτικότητας των χρηστών, ενώ υψηλό είναι το ποσοστό των συμμετεχόντων που δεν ανησυχούν, το οποίο ανέρχεται στο 18%. Το γυναικείο φύλο με ποσοστό 52% ανησυχεί μήπως καταπατηθεί η ιδιωτικότητα τους. Στην αντίστοιχη επιλογή, το ποσοστό των ανδρών φαίνεται να είναι αισθητά μικρότερο, με 28%. Παρατηρείται επομένως πως το γυναικείο φύλο, παρατηρεί με περισσότερη καχυποψία την κατάσταση και πιθανότητα δύναται να αντιστέκεται σε υπηρεσίες που δεν εμπιστεύεται όσο τις υπόλοιπες, σε αντίθεση με τους άνδρες, που το επίπεδο ανησυχίας τους κυμαίνεται σε χαμηλότερα επίπεδα απ' ότι των γυναικών. Τα αποτελέσματα που αποτυπώνονται παρακάτω απαντούν στην ερώτηση «Πιστεύετε ότι μπορούν οι βιομετρικές σας πληροφορίες να κλωνοποιηθούν;», με το 73% των χρηστών να θεωρεί πως οι βιομετρικές πληροφορίες μπορούν εύκολα να κλωνοποιηθούν, με απόρροια να παραβιαστεί η ακεραιότητα του εκάστοτε χρήστη, ενώ το 27% αντιτίθεται στην άποψη αυτή. Ιδιαίτερα, η ηλικιακή ομάδα 18-22 υποστηρίζει με ποσοστό 39% πως τα βιομετρικά τους δεδομένα μπορούν να κλωνοποιηθούν, κατ' επέκταση να παραβιαστούν. Παρατηρείται πως συγκριτικά με τις υπόλοιπες ηλικιακές ομάδες, το υψηλό ποσοστό των 18-22 σκιαγραφεί την εντονότερη ανησυχία τους πως μπορούν να κλωνοποιηθούν οι πληροφορίες τους, επομένως η ασφάλεια τους κλονίζεται, όλα είναι ρευστά, όπως ακριβώς και στους κωδικούς πρόσβασης. Επιπλέον, η ποσοστιαία διαφορά με τις υπόλοιπες ηλικιακές ομάδες, αποτυπώνει την καχυποψία που έχουν οι νέοι απέναντι σε οτιδήποτε καινούργιο προσφέρει πληθώρα πλεονεκτημάτων, υποβόσκουν όμως και μειονεκτήματα, όπως άλλωστε σε κάθε τεχνολογία.
Η τελευταία ερώτηση από το πλήθος αυτών που είναι μορφολογικά ίδιες και αναλύεται στα παρακάτω γραφήματα είναι: «Πιστεύετε ότι τα βιομετρικά συστήματα αποτελούν ένα μέσο καταπάτησης των ανθρωπίνων δικαιωμάτων;». Το 52% των συμμετεχόντων-ουσών δηλώνει πως τα βιομετρικά συστήματα δεν

καταπατούν τα ανθρώπινα δικαιώματα. Ιδιαίτερα, τα ποσοστά που προκύπτουν από το Τμήμα φοίτησης των φοιτητών-τριών είναι σημαντικά. Συγκεκριμένα, το μεγαλύτερο ποσοστό ανέρχεται στο 9% και ανήκει στους φοιτητές του Τμήματος Πολιτισμικής Τεχνολογίας και Επικοινωνίας, οι οποίοι είναι χωρισμένοι στην μέση. Αξιοσημείωτη είναι η διαφοροποίηση που παρουσιάζεται στην παρούσα ανάλυση, καθώς διαφαίνεται από τα ποσοστά πως ανεξάρτητα από το τμήμα φοίτησης των φοιτητών, τα ποσοστά δεν διαφοροποιούνται. Τα ευρήματα της έρευνας μας διαφοροποιούνται με την σχετική έρευνα στην Γαλλία. Τα αποτελέσματα της έρευνας αυτής αναφέρουν ότι υπάρχει δυνητική ανησυχία για την κατάχρηση δεδομένων προσωπικού χαρακτήρα, τα οποία θεωρούνται ότι παραβιάζουν το απόρρητο των χρηστών και τις πολιτικές ελευθερίες (El-abed, Giot, Hemery & Rosenberger, 2014). Αντιθέτως, η πλειοψηφία των ποσοστών της ανάλυσης από την περίπτωση της Ελλάδας θεωρεί πως τα βιομετρικά συστήματα δεν αποτελούν ένα μέσο καταπάτησης των ανθρωπίνων δικαιωμάτων. Οι δύο τελευταίες ερωτήσεις που ολοκληρώνουν την ενότητα αυτή, συνδέονται. Αναλυτικότερα, η μία σχετίζεται «Σε ποιο βαθμό Συμφωνείτε ή Διαφωνείτε με την άποψη ότι «οι κυβερνήσεις συγκεντρώνουν τα βιομετρικά στοιχεία των πολιτών σε βάσεις δεδομένων και γι' άλλες χρήσεις εκτός από την ασφάλεια τους». Το 36% των συμμετεχόντων κρατάει ουδέτερη στάση, ενώ το επόμενο ποσοστό στο 28% φαίνεται να συμφωνεί με την παραπάνω άποψη. Προκειμένου να καταγραφούν όλες οι απόψεις, η τελευταία ερώτηση είναι ανοικτού τύπου και επί της ουσίας «ζητάει» από τους συμμετέχοντες να αιτιολογήσουν την άποψη τους αναφορικά με την άποψη που παρατέθηκε. Συνολικά, το 15% των ερωτηθέντων υποστηρίζει πως από την στιγμή που οι υπηρεσίες από την στιγμή που συγκεντρώνουν τις βιομετρικές πληροφορίες των χρηστών, αυτομάτως παραβιάζεται η ιδιωτικότητα τους. Ιδιαίτερα είναι τα ποσοστά που προκύπτουν από τα δημογραφικά στοιχεία. Συγκεκριμένα, από την ηλικιακή ομάδα διαφαίνεται πως οι απόψεις των φοιτητών ποικίλουν και διαφέρουν μεταξύ τους. Το μεγαλύτερο ποσοστό με 7% προέρχεται από την ηλικιακή ομάδα 46-60, η οποία δηλώνει πως είναι προτιμότερο να παρακολουθείτε από την εκάστοτε κυβέρνηση παρά από τρίτες, κακόβουλες εταιρίες. Βλέπουμε λοιπόν στην Ελλάδα πως ένα ποσοστό ανθρώπων δεν είναι

ενάντια στην παρακολούθηση του από την εκάστοτε κυβέρνηση με την αιτιολογία «*τι όφελος μπορούν έχουν από εμάς;*» ή «*δεν έχουν απώτερο σκοπό να βλάψουν απλώς να διασφαλίσουν τα δεδομένα μας σε αντίθεση με κακόβουλες εταιρίες που έχουν κέρδος*». Δεν μπορούν να λείπουν και οι χρήστες που συμφωνούν με ποσοστό 6% να δηλώνει πως πίσω από τέτοιες πολιτικές κυβερνήσεις «παραμονεύουν» τα συμφέρονται και οι σκοπιμότητες των λίγων. Στον βωμό του κέρδους, οι άνθρωποι δεν δρουν με κανόνες αλλά με αίσθημα απόκτησης. Ένας φοιτητής-τρια αναφέρει χαρακτηριστικά ότι «*Οι «δυνατοί» σε βάθος χρόνου θα προσπαθήσουν να το εκμεταλλευτούν έτσι ώστε να καταφέρουν να πετύχουν απώτερους σκοπούς, που εξυπηρετούν παρασκηνιακά «παιχνίδια» τα οποία ο απλός κόσμος ούτε που μπορεί να συλλάβει ότι συμβαίνουν. Η πρόοδος και η ανάπτυξη της τεχνολογίας συμβαίνει για καλό… στο βωμό του χρήματος και της δόξας, πλέον, την εκμεταλλεύονται εις βάρος της ανθρωπότητας και όχι για καλό της ανθρωπότητας.*» Μια τέτοιου είδους ερώτηση είναι επόμενο να εγείρει διαφόρων σχολιασμών περί της επικρατούσας κατάστασης όπως οι ακόλουθοι:

- «*Δεν μπορώ να γνωρίζω και δεν θα προβώ σε εικασίες. Είμαι απολύτως υπέρ των βιομετρικών συστημάτων για χρήσεις σχετικές με την ασφάλεια και τα θεωρώ τόσο αξιόπιστα στον τομέα αυτό που προθυμοποιούμαι να πάρω το (μικρό) ρίσκο τα δεδομένα αυτά να χρησιμοποιούνται για άλλους σκοπούς.*»
- «*Μιλώντας για την Ελλάδα δεν έχουν βάσεις δεδομένων ούτε για τα βασικά. Πόσο μάλλον να κάνει κάτι τέτοιο. Σε άλλες χώρες ίσως αλλά κάτι τέτοιο θεωρώ ότι μπορεί να υπάρχει και χωρίς βιομετρικά.*»
- «*Θεωρία συνωμοσίας, αυτά τα βλέπουμε μόνο σε ταινίες. Η πραγματικότητα διαφέρει κατά πολύ*» ή «*μόνο σε ταινίες του Hollywood*»

Παρατηρείται από τους χρήστες μια απάθεια για το ζήτημα αυτό. Η σιγουριά των ανθρώπων πως κάτι αρνητικό δε μπορεί να συμβεί σε μας, δημιουργεί αντιδράσεις που δε αφήνουν βήμα σε διαφορετικές προσεγγίσεις. Τα παραπάνω παραδείγματα μπορούν να περιγράψουν τα λεγόμενα που παρατέθηκαν, όμως αξίζει να τονιστεί πως ορισμένες τέτοιες περιπτώσεις έχουν λάβει χώρα σε χώρες του εξωτερικού που συντελούν στην δημιουργία μιας κατακλείδας που ενώνει την παραβίαση των προσωπικών δεδομένων με την επιλογή αξιοποίησης των

βιομετρικών δεδομένων. Η πρόθεση και ο απώτερος σκοπός δύναται να μεταποιήσουν την εικόνα που προάγουν τα βιομετρικά συστήματα περί προστασία της ασφάλεια και ταυτοποίησης «*Ποιος ορίζει τα όρια της ασφάλειας;*».

Συμπεραίνοντας, η κατάσταση που επικρατεί στην Ελλάδα συγκριτικά με τις υπόλοιπες χώρες, θα μπορούσε να χαρακτηριστεί ως μια διαδικασία, η οποία απαιτεί αρκετό χρόνο και κατάλληλο έδαφος για να μπορέσει να προσαρμοστεί με τις συνήθειες των χρηστών ή πρέπει οι χρήστες να συμβαδίσουν με τα βιομετρικά συστήματα. Ανατρέχοντας στην έρευνα, παρατηρείται πως ο κυριότερος φόβος των χρηστών απέναντί στα βιομετρικά συστήματα σχετίζεται αφενός με την άγνοια τους, αφετέρου με τις πολιτικές που προωθούν τα βιομετρικά συστήματα, οι οποίες βλέποντας πως οι βιομετρικές τεχνικές εισβάλλουν στην καθημερινότητα των χρηστών, δεν απευθύνονται στους χρήστες που πραγματικά είναι δύσπιστοι ή και φοβούνται τα βιομετρικά συστήματα για οποιονδήποτε λόγο. Οι πολιτικές αυτές, πρέπει να «παραγκωνίσουν» τους χρήστες που αντιμετωπίζουν τις βιομετρικές τεχνικές με μεγαλύτερη προθυμία και να εστιάσουν στους χρήστες που αδιαφορούν ή θεωρούν πως δεν χρειάζεται να μάθουν. Πρωταρχικό μέλημα να γίνει η εξισορρόπηση των ποσοστών των χρηστών και στην συνέχεια η περαιτέρω αποδοχή θα είναι πιο εύκολη, αν οι χρήστες βρίσκονται στο ίδιο επίπεδο.

6. Βιβλιογραφία

Bhagavatula, R., Ur, B., Iacovino, K., Kywe, S. M., Cranor, L. F., & Savvides, M. (2015). Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption.

Chau, A., Stephens, G., & Jamieson, R. (2004). Biometrics acceptance-perceptions of use of biometrics. *ACIS 2004 Proceedings*, 28.

Doyle Joe. (2014). Accenture Research Shows Citizen Support for Biometrics to Facilitate Travel and Secure Borders | Accenture Newsroom. Retrieved from https://newsroom.accenture.com/industries/health-public-service/accenture-research-shows-citizen-support-for-use-of-biometrics-to-facilitate-travel-and-secure-borders.htm

Duggan, M., & Rainie, L. (2016). Scenario: Workplace security and tracking. *Pew Research Center*.

El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2012). Evaluation of biometric systems: a study of users' acceptance and satisfaction.

Fancher, C. H. (1997). In your pocket: smartcards. *IEEE spectrum*, *34*(2), 47-53.

Graham, L. (2016). MasterCard to replace passwords with selfies. Retrieved from https://www.cnbc.com/2016/02/24/mastercard-to-replace-passwords-with-selfies.html

Guideline for the Use of Advanced Authentication Technology Alternatives, Federal Information Processing Standards Publication 190, National Institute of Standards and Technology, Gaithersburg, September 1994.

Iseris, G. (2016). Στατιστικές μέθοδοι ελέγχου εγκυρότητας και αξιοπιστίας ερωτηματολογίων. Η περίπτωση του CiGreece. *International Journal of Language, Translation and Intercultural Communication*, *5*, 175-189.

Izzy Santa. (2016). Biometric Technology Enjoys Strong Support from Consumers, Says CTA | Business Wire. Retrieved from https://www.businesswire.com/news/home/20160330006149/en/Biometric-?-Technology-?-Enjoys-?-Strong-?-Support-?-Consumers-?-CTA

Jain, A. K., Pankanti, S., Prabhakar, S., & Ross, A. (2001, June). Recent advances in fingerprint verification. In *International conference on audio-and video-based biometric person authentication* (pp. 182-190). Springer, Berlin, Heidelberg.

Keough, E. & Muir S. (2016, January 13). Experian. *UK now ready for biometric banking.* Διαθέσιμο σε https://www.experianplc.com/media/news/2016/uk-now-ready-for-biometric-banking/ [ανακτήθηκε 25 Οκτωβρίου 2019]

Le, C., & Jain, R. (2009). A survey of biometrics security systems. *EEUU. Washington University in St. Louis*.

Levine, B. N., Reiter, M. K., Wang, C., & Wright, M. (2004, February). Timing attacks in low-latency mix systems. In *International Conference on Financial Cryptography* (pp. 251-265). Springer, Berlin, Heidelberg.

O'Gorman, L. (2002). Securing Business's Front Door–Password, Token, and Biometric Authentication. *Ghosh, S.; Malek, M.; Stohr, EA (Hg.): Guarding Your Business. A Management Approach to Security, S*, 119-149.

Professor: Johan Montelius Autumn Semester 2005 Assignment 1, Biometric authentication, Internet Security and Privacy. 2G1704 Alexandre Fustier Vincent Burger Internet Security and Privacy. 2G1704 Professor: Johan Montelius Autumn. Internet Security and Privacy , 2G1704, September 2005

Sherman, R. (2016, February 19). Business Wire. *HSBC Launches Biometric Banking* Διαθέσιμο σε https://www.businesswire.com/news/home/20160219005825/en/HSBC-Launches-Biometric-Banking [ανακτήθηκε 25 Οκτωβρίου 2019]

Yurcan B. (2016). American Banker. *Banks Embrace Biometrics, But Will Customers?* Διαθέσιμο σε https://www.americanbanker.com/news/banks-embrace-biometrics-but-will-customers [ανακτήθηκε 24 Οκτωβρίου 2019]

Κάτσικας, Κ. Σ & Γκρίτζαλης, Δ., & Γκρίτζαλης, Σ. (2004).*Ασφάλεια Πληροφοριακών Συστημάτων.* Αθήνα: Εκδόσεις Νέων Τεχνολογιών

Ανδρόνικου, Β. (2009). *Καινοτόμοι Μηχανισμοί Βελτίωσης Απόδοσης Και Αποτελεσματικότητας Των Βιομετρικών Συστημάτων.* Διδακτορική Διατριβή, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Διαθέσιμο σε https://www.sbs-studies.gr/apa-style [ανακτήθηκε 24 Οκτωβρίου 2019]

Δρ. Αγγελινός, Γ. (2016) *Ασφάλεια Πληροφοριακών Συστημάτων- Ταυτοποίηση Και Αυθεντικοποίηση.* Διαθέσιμο σε https://slideplayer.gr/slide/11329048/ [ανακτήθηκε 18 Ιουλίου 2019]

Καρύδα, Μ. Ηλεκτρονικές σημειώσεις, Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων, Διαθέσιμο: http://www.icsd.aegean.gr/website_files/metaptyxiako/315624416.ppt bro

Λέκκα, Δ. Π.(2002). Ασφάλεια Πληροφοριακών Και Επικοινωνιακών Συστημάτων Με Χρήση Υπηρεσιών Έμπιστης Τρίτης Οντότητας: Λειτουργικά, Αρχιτεκτονικά Και Οργανωτικά Ζητήματα. Διδακτορική Διατριβή, Πανεπιστήμιο Αιγαίου, Σάμος

Menexes, George. 2008. "Η Έρευνα Με Ερωτηματολόγιο," 1–49.

Δρ. Μπόζιος, Ε. (2004). *ΣΗΜΕΙΩΣΕΙΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ* Διαθέσιμο σε https://docplayer.gr/3552572-Simeioseis-efarmosmenis-asfaleias-pliroforiakon-systimaton.html [ανακτήθηκε 18 Ιουλίου 2019]

Τζίτζικας, Γ. (2010). *Εισαγωγή στα Πληροφοριακά Συστήματα*. Παρουσίαση μαθήματος Ανάλυση και Σχεδίαση Πληροφοριακών Συστημάτων, Πανεπιστήμιο Κρήτης

Χαλικιάς, Μ. & Λάλου, Π. & Μανωλέσου, Α. *Μεθοδολογία έρευνας και εισαγωγή στη Στατιστική Ανάλυση Δεδομένων με το IBM SPSS STATISTICS* [eBook version] διαθέσιμο σε https://repository.kallipos.gr/handle/11419/5075 , [ανακτήθηκε 18 Ιουλίου 2019]

Ψάνη, Α. & Καμπούρης, Α.(2016) Πληροφοριακά Συστήματα Στην Εκπαίδευση. Μελέτη Περίπτωσης: Αξιολόγηση Του Συστήματος Ηλεκτρονικής Διακυβέρνησης http://okeanis.lib.puas.gr/xmlui/bitstream/handle/123456789/3241/%CE%A0%CE%A4%CE%A5%CE%A7%CE%99%CE%91%CE%9A%CE%97%20%CE%95%CE%A1%CE%93%CE%91%CE%A3%CE%99A%20MYSCHOOL%202016.pdf?sequence=1.