# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων***


## Μεταπτυχιακή Διατριβή

**Συστήματα ελέγχου ταυτότητας για online banking: biometrics - πως μπορούν να χρησιμοποιηθούν για περισσότερη ασφάλεια στις συναλλαγές**


**Χρυστάλλα Σάββα**

**Επιβλέπων Καθηγητής**
**Αδαμαντίνη Περατικού**



**Μάιος 2020**

# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων***


# Μεταπτυχιακή Διατριβή

## Συστήματα ελέγχου ταυτότητας για online banking: biometrics - πως μπορούν να χρησιμοποιηθούν για περισσότερη ασφάλεια στις συναλλαγές


**Χρυστάλλα Σάββα**

**Επιβλέπων Καθηγητής**
**Αδαμαντίνη Περατικού**



Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
Στην Ασφάλεια Υπολογιστών και Δικτύων
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

**Μάιος 2020**

## Περίληψη

Τα τελευταία χρόνια η βιομετρική τεχνολογία εισέβαλε στην καθημερινότητά μας. Ολοένα και περισσότεροι άνθρωποι κάνουν χρήση βιομετρικών μεθόδων για να προστατεύσουν τις συσκευές τους και να επαληθεύσουν την ταυτότητά τους. Οι βιομετρικές μέθοδοι έχουν την ιδιότητα της ανάλυσης και αναγνώρισης των μοναδικών χαρακτηριστικών και των ανθρωπίνων συμπεριφορών. Τα χαρακτηριστικά που συνήθως αναλύονται είναι: τα δακτυλικά αποτυπώματα, η ίριδα, το πρόσωπο και η φωνή. Αυτό που κάνει τις βιομετρικές μεθόδους να ξεχωρίζουν σε σχέση με άλλες μεθόδους επαλήθευσης είναι το γεγονός πως βασίζονται σε κάτι μοναδικό και μη μεταβιβάσιμο. Η τεχνολογία της βιομετρίας έγινε ευρέως διαδεδομένη καθώς συνδυάζει συγχρόνως ασφάλεια και ευχρηστία. Χάρη σε αυτές τις ιδιότητες κατάφερε να εισβάλει σε διάφορους τομείς της καθημερινότητας. Πέραν από την επαλήθευση της ταυτότητας, εφαρμόζεται για έλεγχο πρόσβασης, έλεγχο παρουσίας καθώς και σε ηλεκτρονικές πληρωμές.

Στην παρούσα μεταπτυχιακή διατριβή παρουσιάζονται τα βιομετρικά συστήματα δίνοντας ιδιαίτερη έμφαση στο πώς μπορούν να αξιοποιηθούν ώστε να παρέχουν μεγαλύτερη ασφάλεια στις online συναλλαγές. Σκοπός είναι να διερευνηθεί αν τα συστήματα ελέγχου ταυτότητας για online banking χρήζουν βελτίωσης σε θέμα ασφάλειας καθώς και αν ο χρόνος εκτέλεσης της διαδικασίας αναγνώρισης μπορεί να βελτιωθεί.

Πιο συγκεκριμένα στο 1ο κεφάλαιο γίνεται μία εισαγωγή, παρουσιάζεται ο σκοπός, η συνεισφορά της διατριβής και τα κυριότερα ερευνητικά ερωτήματα. Ακολουθεί το 2ο κεφάλαιο όπου προσδιορίζεται η έννοια του online banking, παρουσιάζονται τα οφέλη και οι κίνδυνοι τόσο για τις τράπεζες όσο και για τους πελάτες.

Στο 3ο κεφάλαιο μελετάται το ζήτημα της ασφάλειας, η διαδικασία ταυτοποίησης και οι κατηγορίες αυθεντικοποίησης. Στο 4ο κεφάλαιο ορίζεται η βιομετρία, αναλύονται τα είδη βιομετρικών χαρακτηριστικών και οι παράγοντες αποδοχής των μεθόδων από τους χρήστες. Έπειτα στο 5ο κεφάλαιο παρουσιάζεται η ερευνητική διαδικασία μαζί με τη μεθοδολογία που έχει ακολουθηθεί και στο 6ο κεφάλαιο γίνεται η παρουσίαση των αποτελεσμάτων της έρευνας και η ανάλυση των δεδομένων που έχουν προκύψει.

Τέλος στο 7ο κεφάλαιο παρουσιάζεται η υιοθέτηση βιομετρικών συστημάτων σε παρόν και μέλλον ενώ η διατριβή ολοκληρώνεται στο 8ο κεφάλαιο με την αποτίμηση της βιομετρικής τεχνολογίας και ανοικτά ερευνητικά θέματα.

## Summary

During the last few years, biometrics has invaded our daily lives. Most people use biometric authentication methods to protect their devices. Biometrics have the intelligence to analyze and identify the behaviors or the unique characteristics of each person. The most commonly analyzed features are: fingerprints, iris, facial, and voice patterns. What makes biometrics to stand out from other verification methods is that the former is based on something unique and non-transferable. Biometric technology has become popular because it combines usability and safety. For that reason, it manages to be adopted by many sectors since it is applied for access control, authentication, application authentication, and, online payments.

This thesis aims to analyze the security and the sufficient ability that banking systems provide, as well as the ability to improve these systems using biometric technology. More specifically, the 1st chapter is an introduction of the study, presents the purpose contribution to the study and provides the research questions. The 2nd chapter defines the benefits and the risks for both banks and customer side. The 3rd chapter examines the security, identification process, and the categories of authentication. The 4th chapter defines biometrics, analyze the types of biometric features and factors used by customers. Then, the 5th chapter presents the research process and the methodology has been followed. In the 6th chapter, research findings and data analysis presenting. The 7th chapter includes the current use and the expected in the future use of biometric systems. Finally, the 8th chapter describes the evaluation of biometrics and open research topics.

**Keywords:** biometrics for online banking, biometric technology in banking, mobile and biometric payments replace cards, user acceptance of biometrics, e-banking security with biometrics, adoption of biometrics technologies, GDPR, biometrics and disability rights

## Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια κα. Αδαμαντίνη Περατικού για την υποστήριξή της καθ' όλη τη διάρκεια εκπόνησης της παρούσας μεταπτυχιακής διατριβής.

Ιδιαίτερες ευχαριστίες σε όσους συνέβαλαν και βοήθησαν στην συλλογή στοιχείων σχετικά με την έρευνα και στήριξαν με κάθε τρόπο αυτή την προσπάθεια. Τέλος, ένα μεγάλο ευχαριστώ στην οικογένεια και τους φίλους που με στηρίζουν με κάθε δυνατό τρόπο και σε κάθε μου βήμα.

# Περιεχόμενα

# Κεφάλαιο 1
# Εισαγωγή

Στη σημερινή εποχή, όλοι σχεδόν οι τραπεζικοί οργανισμοί έχουν κάνει τεράστιες προσπάθειες ώστε οι τραπεζικές συναλλαγές να γίνουν πιο βολικές και πιο ασφαλείς, κερδίζοντας την έγκριση και την εκτίμηση πολλών πελατών.
Οι διαχειριστές των τραπεζικών ιδρυμάτων μελετούν διάφορες μεθόδους για τη βελτίωση της ασφάλειας των συναλλαγών. Ορισμένες από αυτές περιλαμβάνουν φράσεις πρόσβασης, πολλαπλές συσκευές ή και πιστοποιήσεις πολλαπλών παραγόντων που ενδεχομένως να περιλαμβάνουν και διαφόρους συνδυασμούς αυτών μαζί με ένα κωδικό πρόσβασης, για μεγαλύτερη ασφάλεια.
Παρόλο το πλήθος των μεθόδων αυτών, δεν υπάρχει κάποια επικρατέστερη από θέμα υψηλότερης ασφάλειας των συναλλαγών, οπόταν όλοι σχεδόν οι τραπεζικοί οργανισμοί συμβιβάζονται σε κάποιο βαθμό στην ασφάλεια βάση της εμπειρίας του χρήστη.
Έχοντας ως δεδομένο ότι οι παραδοσιακές μέθοδοι πιστοποίησης έχουν αποδείξει ότι εγκυμονούν κίνδυνους στην ασφάλεια τόσο των χρηστών όσο και των συναλλαγών, οι υπεύθυνοι για τη λήψη αποφάσεων στις χρηματοπιστωτικές υπηρεσίες άρχισαν να συνειδητοποιούν ότι μια εντελώς νέα μέθοδος ίσως να μην γινόταν αποδεκτή στα πρώτα στάδια του σχεδιασμού των πολυαναμενόμενων νέων προτύπων πιστοποίησης. Ως εκ τούτου, πραγματοποιήθηκαν αρκετές έρευνες για να μεταφερθεί ο τραπεζικός κόσμος σε ένα νέο κόσμο πέρα από τη χρήση των παραδοσιακών κωδικών πρόσβασης.

Την τελευταία δεκαετία, η βιομετρία αποτελεί μακράν την πιο ελπιδοφόρα και παραγωγική κατεύθυνση στην οποία κινείται η πρόοδος στην αυθεντικοποίηση των χρηστών. Η βιομετρία είναι η μελέτη των διακριτικών και των μετρήσιμων ανθρωπίνων χαρακτηριστικών που μπορούν να χρησιμοποιηθούν για την επισήμανση και την περιγραφή κάθε ατόμου. Τέτοια χαρακτηριστικά ή τα βιομετρικά αναγνωριστικά, μπορεί να είναι οτιδήποτε από φλέβες, δακτυλικά αποτυπώματα, αναγνώριση της ίριδας ή του αμφιβληστροειδούς, αναγνώριση φωνής, προσώπου, ή ακόμη και η χειρόγραφη υπογραφή, τα οποία αποτελούν μοναδικά αναγνωριστικά για τον καθένα μας.

Ωστόσο, η εύρεση ενός βιομετρικού αναγνωριστικού είναι απλώς το πρώτο βήμα για να καταστεί μία εφικτή τεχνολογία στον τραπεζικό τομέα, δεδομένου ότι μόνο ορισμένες τεχνολογίες έχουν δοκιμαστεί και χρησιμοποιούνται στα συστήματα των τραπεζών. Αυτό συμβαίνει διότι κάθε μέθοδος πρέπει να είναι απόλυτα ασφαλείς ώστε να παρέχει όσο το δυνατό μεγαλύτερη προστασία από τυχόν κακόβουλες ενέργειες. Συνάμα, θα πρέπει να είναι καθολική, απλή και πρακτική στο χρήστη γιατί μόνο έτσι θα καταστεί κοινωνικά αποδεκτή.

## 1.1 Σκοπός

Η συνεχής ανάπτυξη του Διαδικτύου καθώς και ο χρόνος που απαιτείται για την ταυτοποίηση ολοένα και αυξάνεται. Ταυτόχρονα, υφίσταται η ανάγκη παροχής επιπρόσθετης ασφάλειας στα συστήματα ταυτοποίησης στις ηλεκτρονικές συναλλαγές. Σκοπός της διατριβής είναι η διερεύνηση της ασφάλειας και της επαρκής ευχέρειας που παρέχουν τα τραπεζικά συστήματα ταυτοποίησης καθώς και η δυνατότητα βελτίωσης μέσω της βιομετρικής τεχνολογίας των συστημάτων αυτών. Τα αποτελέσματα θα πρέπει να δείξουν κατά πόσο χρήζουν βελτίωσης τα συστήματα ελέγχου ταυτότητας στο online banking και αν υπάρχει δυνατότητα επίτευξης της βελτίωσης με τη χρήση βιομετρικής τεχνολογίας.

## 1.2 Συνεισφορά της Έρευνας

Οι συνεχείς εξελίξεις σε τεχνολογικό επίπεδο, καθιστούν την ανάπτυξη βιομετρικής τεχνολογίας σε τραπεζικούς αλλά και σε ευρύτερους τομείς, κερδίζοντας την έγκριση και την εκτίμηση όλο και περισσότερων χρηστών. Δεδομένου ότι δεν υπάρχει κάποια επικρατέστερη βιομετρική μέθοδος στην παρούσα φάση, απώτερος στόχος είναι να εξασφαλιστεί το υψηλό επίπεδο ασφάλειας με όσο το δυνατόν χαμηλότερο κόστος για τους τελικούς χρήστες. Για να καταστεί όμως αυτό, θα πρέπει να δοκιμάζονται συνεχώς νέες βιομετρικές μέθοδοι και τεχνολογίες για την ανεύρεση ενός τρόπου όπου θα ισοσταθμίζεται η πιθανότητα επικύρωσης ενός λάθους του χρήστη, με την μέτρηση της πιθανότητας να μην δοθεί πρόσβαση σε ένα νόμιμο χρήστη.

Επομένως, θα διερευνηθεί η επάρκεια της ευκολίας και της ασφάλειας που παρέχουν τα συστήματα ταυτοποίησης των τραπεζών και πώς μπορούν να βελτιωθούν με την ενίσχυση της βιομετρικής τεχνολογίας.

## 1.3 Βασικά Ερευνητικά Ερωτήματα

Ένα από τα βασικότερα ερευνητικά ερωτήματα που θα εξεταστεί είναι κατά πόσο οι χρήστες επιλέγουν τη χρήση βιομετρικών μεθόδων συγκριτικά με τη χρήση κωδικών πρόσβασης κατά την εκτέλεση πληρωμών ή άλλων χρηματοπιστωτικών υπηρεσιών για την εξακρίβωση της ταυτότητάς τους. Επίσης, η ακεραιότητα και η ασφάλεια των καταναλωτών όταν συλλέγονται και φυλάσσονται τα βιομετρικά τους δεδομένα, αποτελεί ακόμη ένα ερώτημα κατά πόσο λαμβάνονται όλες οι απαραίτητες προφυλάξεις ώστε να βεβαιωθεί η προστασία μη εξουσιοδοτημένης πρόσβασης ή απάτης. Ακόμη, η αίσθηση απόλυτης ασφάλειας των χρηστών είναι κάτι που τους προβληματίζει διότι τους καθιστά πιο επιρρεπείς σε πράξεις και κινήσεις που κάνουν ευκολότερη την παραβίαση της ιδιωτικότητάς τους.

# Κεφάλαιο 2
# Ηλεκτρονική Τραπεζική, Οφέλη και Κίνδυνοι του Online Banking

## 2.1 Ορισμός και Χαρακτηριστικά Ηλεκτρονικής Τραπεζικής (e-banking)

Η ολοένα αυξανόμενη διείσδυση των τεχνολογιών Πληροφορικής και του Διαδικτύου, αποτελεί εδώ και αρκετές δεκαετίες πρόκληση για την ανταγωνιστικότητα των χρηματοπιστωτικών ιδρυμάτων. Πλέον, όλοι κάνουν λόγο για τη «νέα παγκόσμια οικονομία» η οποία έχει καταφέρει να στρέψει τα βλέμματα των επιχειρήσεων και των τραπεζών στην παρακολούθηση των αλλαγών που συντελούνται στο εξωτερικό τους περιβάλλον και να προσαρμόζονται στο νέο σκηνικό.

Η παγκοσμιοποίηση των αγορών μαζί με τις διεθνείς εξελίξεις έχουν αναγκάσει τις τράπεζες να υιοθετήσουν νέα εναλλακτικά εικονικά κανάλια διανομής όπως την ηλεκτρονική τραπεζική (e-banking) για την προώθηση των υπηρεσιών τους μέσω Διαδικτύου [1].

Στην ουσία η ηλεκτρονική τραπεζική παρέχει ένα μεγάλο εύρος τραπεζικών υπηρεσιών το οποίο αναπτύσσεται διαδικτυακά. Οι βασικότερες υπηρεσίες που προσφέρονται μέσω της ηλεκτρονικής τραπεζικής πέραν από τη δυνατότητα των πελατών να έχουν πρόσβαση στους λογαριασμούς τους, είναι η δυνατότητα μεταφοράς χρημάτων τόσο μεταξύ ιδιωτών όσο και μεταξύ επιχειρήσεων [2].

Πολλοί μάλιστα είναι οι χρηματοπιστωτικοί οργανισμοί που αντικατέστησαν αρκετά υποκαταστήματά τους με ηλεκτρονικά κανάλια. Λειτουργούν αποκλειστικά μέσω του Διαδικτύου, καταφέρνοντας να ελαχιστοποιήσουν το κόστος των υπηρεσιών που παρέχουν και να μεγιστοποιήσουν τα κέρδη τους.

Αυτό αποτελεί εξέλιξη στο κλάδο της τραπεζικής αφού η ηλεκτρονική τραπεζική δεν αποτελεί απλά ένα τραπεζικό δημιούργημα που λειτουργεί χωρίς να είναι απαραίτητη η φυσική παρουσία του πελάτη, αλλά επεκτείνει τις δυνατότητές της και συνάμα βοηθά στις επαφές και τις συναλλαγές.

### 2.1.1 Έννοια και ιστορική αναδρομή ηλεκτρονικής τραπεζικής (e-banking)

Με τον όρο ηλεκτρονική τραπεζική εννοούμε ένα σύστημα εναλλακτικών πληρωμών που επιτρέπει μέσω αυτού τη διεκπεραίωση όλων σχεδόν των τύπων συναλλαγών από τους πελάτες των τραπεζών, χωρίς την απαραίτητη φυσική παρουσία τους στις τράπεζες [37]. Όλες οι δυνατές συναλλαγές μπορούν να διενεργηθούν από του πελάτες μέσω της πρόσβασης που παρέχεται από την χρήση ηλεκτρονικών μέσων, κυρίως διαδικτυακά από διάφορους χώρους εκτός τραπεζών. Η πρόσβαση παρέχεται διαμέσου άλλων καναλιών, όπως για παράδειγμα με τη χρήση διαφόρων συσκευών σύνδεσης στα τραπεζικά συστήματα. Τέτοιες συσκευές είναι το σταθερό τηλέφωνο (phone banking) και το κινητό τηλέφωνο (mobile banking). Έτσι, όλες οι παραδοσιακές συναλλαγές που θα μπορούσαν να γίνουν σε ένα υποκατάστημα, πλέον μπορούν να πραγματοποιηθούν μέσω της ηλεκτρονικής τραπεζικής εφόσον πελάτης μπορεί να φέρνει την τράπεζα στο δικό του χώρο οποιαδήποτε χρονική στιγμή επιθυμεί.

Κάνοντας μία ιστορική αναδρομή στο παρελθόν, θα διαπιστώσουμε πως η χρήση των εναλλακτικών καναλιών για την διανομή τραπεζικών προϊόντων δεν αποτελεί σημερινό φαινόμενο αλλά άρχισε να πρωτοεμφανίζεται στις αρχές της δεκαετίας του ’70. Η λειτουργία των εναλλακτικών δικτύων ταυτίζεται με την εξέλιξη των Υπολογιστών και της τεχνολογίας αφού με την εισαγωγή των Ηλεκτρονικών Υπολογιστών στις τράπεζες εμφανίστηκαν οι πρώτες αυτόματες ταμειολογιστικές μηχανές ATM (Automated Teller Machine), όπου διευκόλυναν τις συναλλαγές εκτός του ωραρίου των τραπεζικών υποκαταστημάτων [3].

Από τα μέσα της δεκαετίας του ’80, τα τραπεζικά ιδρύματα άρχισαν να μελετούν το ζήτημα της εξ αποστάσεως υλοποίησης των τραπεζικών συναλλαγών. Έναυσμα για την ιδέα αυτή, ήταν η ολοένα και μεγαλύτερη διάσταση που είχαν οι ηλεκτρονικές αγορές μέσω Διαδικτύου[4]. Σταθμός λοιπόν στην ιστορία της ηλεκτρονικής τραπεζικής, κατέστη η ανάπτυξη των τηλεφωνικών δικτύων μιας και έκανε γνωστό τον όρο «σε απευθείας σύνδεση».

Το «Home banking» όπως αρχικά ονομαζόταν, αναφέρεται στην χρήση τερματικού, όπως οθόνης και πληκτρολογίου για την αποστολή τόνων σε μία τηλεφωνική γραμμή στο τραπεζικό σύστημα. Πιο συγκεκριμένα, εμφανίστηκε για πρώτη φορά στη Νέα Υόρκη όπου τέσσερεις μεγάλες τράπεζες εκείνης της εποχής (Chase Bank, Chemical Bank, Citibank και Manufactures Hanover) πρόσφεραν ένα εξειδικευμένο σύστημα (videotex) το οποίο προωθούσαν στους πελάτες τους ώστε να χρησιμοποιούν τις υπηρεσίες τους από το σπίτι [5].

Στην Ευρώπη, οι πρώτες απομακρυσμένες υπηρεσίες εμφανίστηκαν το 1983 στο Ηνωμένο Βασίλειο, όπου δημιουργήθηκαν από την τράπεζα της Σκωτίας για τους πελάτες της Nottingham Building Society (NBS). Η ιδέα αυτή έθεσε τα θεμέλια επί των οποίων όλα τα υπόλοιπα συστήματα ηλεκτρονικής τραπεζικής έχουν βασιστεί για να προσφέρουν υπηρεσίες online banking. Λόγω της εμπορικής αποτυχίας του videotext, οι τράπεζες στην Νέα Υόρκη και στην υπόλοιπη Ευρώπη δεν έγιναν αρκετά δημοφιλείς εκτός από τη Γαλλία. Όσον αφορά το e-banking στη Γαλλία, λόγω της χρήστη τερματικών Minitel που επιδοτήθηκε από τον πάροχο τηλεπικοινωνιών και δοκιμάστηκε σε μεγάλη μερίδα χρηστών, κατάφερε να αρχίσει την προσφορά των υπηρεσιών της το 1998 [5].

Μέχρι τα τέλη της δεκαετίας του ’90, είχαν εγκατασταθεί εκατομμύρια τερματικά Minitel στα σπίτια καταφέρνοντας να είναι η πιο δημοφιλής υπηρεσία αφού πολλές τράπεζες άρχισαν και έβλεπαν τις τραπεζικές υπηρεσίες ως στρατηγική επιταγή [36]. Μη έχοντας άλλη επιλογή, οι τράπεζες επένδυσαν στο κανάλι της διαδικτυακής τραπεζικής για να παραμείνουν ανταγωνιστικές παρόλο που απαιτεί πολύ υψηλές δαπάνες τόσο στη λειτουργία όσο και στη δημιουργία της.

Στην Ελλάδα, πρωτοεμφανίστηκε το 1997 η πρώτη διαδικτυακή εφαρμογή e-banking από την Εγνατία Τράπεζα. Για τη χρήση της υπηρεσίας WebTeller, οι πελάτες είχαν την δυνατότητα μέσω Internet να διεκπεραιώσουν τις συναλλαγές τους. Έτσι, συνεχίστηκε η τάση και το ενδιαφέρον για την ανάπτυξη της διαδικτυακής τραπεζικής.

Επίσης, οι κυπριακές τράπεζες δεν έμειναν θεατές στην εξελικτική αυτή πορεία. Κατάφεραν να αναπτύξουν και αυτές τις δικές τους ηλεκτρονικές πλατφόρμες παρέχοντας στο πελατολόγιό τους ένα ευρύ φάσμα υπηρεσιών από απλή πληροφόρηση για την ίδια την τράπεζα ως οργανισμό έως ολοκληρωμένες τραπεζικές συναλλαγές.

### 2.1.2 Είδη ηλεκτρονικής τραπεζικής

Οι τράπεζες προσφέρουν στους πελάτες τους υπηρεσίες όπου λαμβάνουν χώρα από απόσταση, το λεγόμενο «Remote Banking». Πρόκειται για τις υπηρεσίες όπου οι ηλεκτρονικές συσκευές είναι συνδεδεμένες με τα πληροφοριακά τους συστήματα [6]. Ανάλογα με τον εξοπλισμό και τα λογισμικά προγράμματα που διαθέτουν διακρίνονται σε τέσσερεις κύριες κατηγορίες. Αυτές είναι: η τραπεζική μέσω Υπολογιστή (PC Banking), η τραπεζική μέσω Διαδικτύου (Internet Banking), μέσω κινητών συσκευών (Mobile Banking) και μέσω τηλεφώνου (Phone Banking). Το e-Banking μπορεί να θεωρηθεί ότι περικλείει όλες τις πιο πάνω κατηγορίες, περιγράφει δηλαδή όλες τις δυνατότητες και τους τρόπους που μπορεί ο πελάτης να έρθει σε επαφή ηλεκτρονικά με την τράπεζά του.

**PC Banking**

Περιγράφει τις συναλλαγές που διεκπεραιώνονται από τους πελάτες των τραπεζών μέσω ενός Υπολογιστή και ενός modem. Μιας και οι τράπεζες προσφέρουν ένα χρηματοοικονομικό λογισμικό που επιτρέπει την εκτέλεση οικονομικών συναλλαγών, η μεταφορά των δεδομένων στις συναλλαγές πραγματοποιείται μέσω αναλογικών ή ψηφιακών τηλεφωνικών γραμμών από τον Υπολογιστή.

**Internet Banking**

Συχνά αναφέρετε και ως Online Banking, αποτελεί το πιο βασικό κομμάτι του e-banking λόγω του ότι χρησιμοποιεί το Internet ως κύριο μέσω διεξαγωγής των τραπεζικών δραστηριοτήτων. Μπορεί όμως να χρησιμοποιηθεί και μέσω άλλων είτε εσωτερικών είτε εξωτερικών δικτύων. Οι χρήστες για να μπορούν να το αξιοποιούν θα πρέπει να έχουν σίγουρα ένα Ηλεκτρονικό Υπολογιστή με σύνδεση στο Διαδίκτυο και παράλληλα εάν επιθυμούν, μπορούν να διαθέτουν για περισσότερη ασφάλεια ένα ειδικό λογισμικό ή ψηφιακό πιστοποιητικό. Μέσω του Internet Banking, οι τράπεζες εκμεταλλευόμενες των δυνατοτήτων που προσφέρει το Διαδίκτυο παρέχουν μία ποικιλία τραπεζικών δυνατοτήτων στους πελάτες τους.

Ένα από τα πρώτα είδη ηλεκτρονικής τραπεζικής είναι το λογισμικό για εξ αποστάσεως τραπεζική συναλλαγή (Remote Banking Software) το όποιο αναπτύσσει η εκάστοτε τράπεζα και το διανέμει στους πελάτες της χωρίς κάποια επιπλέον επιβάρυνση.

Οπόταν οι πελάτες από την μεριά τους, μέσω κωδικών ασφαλείας που τους παρέχονται μπορούν να προβούν στην ενημέρωση σχετικά με τους λογαριασμούς και τις κινήσεις τους [3].

Μία επίσης διαδεδομένη παρουσία των τραπεζών μέσω Διαδικτύου είναι με τη μορφή ιστοσελίδων. Τα τραπεζικά ιδρύματα δημιουργώντας μία φιλική προς τους χρήστες ιστοσελίδα, καταφέρνουν να πληροφορούν τους πελάτες τους για τις υπηρεσίες που παρέχουν. Πλέον έχουν εξελιχθεί σε αυτό τον τομέα, οι ιστοχώροι γίνονται ολοένα και πιο διαδραστικοί παρέχοντας τη δυνατότητα αλληλεπίδρασης μεταξύ τράπεζας και πελατών σε πραγματικό χρόνο [7].

Το πιο ίσως ολοκληρωμένο είδος ηλεκτρονικής τραπεζικής είναι μέσω πλατφόρμας, όπου αποτελεί άλλη μία μορφή Internet Banking. Ο χρήστης μέσω Διαδικτύου, με τη χρήση ενός browser μπορεί να μεταφέρει χρηματικά ποσά μεταξύ των λογαριασμών του, να δέχεται πληροφορίες και να υποβάλλει ερωτήματα χωρίς να απαιτείται η φυσική του παρουσία στο τραπεζικό υποκατάστημα με το οποίο συνεργάζεται.

**Mobile- banking**

Δεδομένης της μεγάλης ανάπτυξης της κινητής τηλεφωνίας, το mobile banking αποτελεί ένα ευρέως χρησιμοποιούμενο κανάλι πραγματοποίησης συναλλαγών. Οι τράπεζες θέλησαν να εκμεταλλευτούν τις εξελίξεις μαζί με την πρόοδο στις κινητές συσκευές που αναπτύσσονται και είναι σε θέση ώστε να μπορούν να προσφέρουν στους πελάτες τους σε υψηλό ποσοστό ποιότητας, τόσο υπηρεσίες όσο και εξυπηρέτηση.

Το mobile banking είναι ισοδύναμο με το Internet banking αλλά παρέχει ευκολότερη πρόσβαση στους χρήστες για να το χρησιμοποιούν από που και αν βρίσκονται χωρίς κάποιο περιορισμό, μέσω ενός συγκεκριμένου προγράμματος που έχει δημιουργηθεί από τα τραπεζικά ιδρύματα.

Παρόλη την ευκολία που παρέχει, σε ορισμένες περιπτώσεις οι χρηματιστηριακές συναλλαγές εκτελούνται σε πιο περιορισμένο φάσμα σε σχέση με το Internet baking [3]. Η ταχύτητα με την οποία διαδίδονται οι φορητές συσκευές έχει κάνει την διάδοση του mobile banking πιο εντατική. Ο κόσμος έχει αρχίσει να το υιοθετεί και είναι εντονότερη η προτίμηση του λόγω της πολύ πιο άμεσης πρόσβασής του στο Διαδίκτυο από την κινητή τους συσκευή .

**Phone- banking**

Είναι το είδος της ηλεκτρονικής τραπεζικής όπου οι τραπεζικές συναλλαγές εκτελούνται μέσω μίας τηλεφωνικής συσκευής. Η συγκεκριμένη υπηρεσία απομακρυσμένης εξυπηρέτησης απευθύνεται στο ευρύτερο τραπεζικό κοινό και βασίζεται σε μία αλληλουχία ηχογραφημένων μνημάτων [3].

Είναι εύχρηστο καθώς απευθύνεται και σε πελάτες που μπορεί να μην είναι εξοικειωμένοι με τη χρήση Ηλεκτρονικών Υπολογιστών ή με το Διαδίκτυο. Ο χρήστης καλώντας την υπηρεσία ακολουθεί τις οδηγίες για την εκπλήρωση της ενέργεια που τον ενδιαφέρει για να εξυπηρετηθεί. Από την άλλη μεριά, ο τραπεζικός σύμβουλος που τον εξυπηρετεί, προχωρά στην ταυτοποίηση των στοιχείων του πελάτη για να εξασφαλιστεί η ασφάλεια και η εμπιστευτικότητα των συναλλαγών και των αιτημάτων του. Η διαφάνεια στις συναλλαγές διασφαλίζεται λόγω του ότι καταγράφονται και ηχογραφούνται όλες οι τηλεφωνικές επικοινωνίες.

Επίσης, προσφέρει άμεση πρόσβαση ολόκληρο το 24ωρο και είναι αρκετά οικονομικό μέσο. Το μόνο που απαιτείται είναι μία τηλεφωνική σύνδεση μαζί με μία τηλεφωνική συσκευή. Έτσι, περιορίζεται σημαντικά ο χρόνος αναμονής των πελατών στα ταμεία εξυπηρέτησης των τραπεζών και γίνεται πιο άμεση η εξυπηρέτησή του από το χώρο του χρήστη.

## 2.2 Οφέλη και Κίνδυνοι του Online Banking

Η ανοδική πορεία της ηλεκτρονικής τραπεζικής αποτελεί τη βάση για την αύξηση των πελατών στις τράπεζες. Η εξυπηρέτηση μέσω νέων καναλιών, όπως το κινητό τηλέφωνο ή το Διαδίκτυο προσφέρει στις τράπεζες τη δυνατότητα να αυξήσουν την αποδοτικότητά τους εισάγοντας νέες καινοτομίες στους πελάτες τους.

### 2.2.1 Πλεονεκτήματα για τις τράπεζες

Οι τράπεζες εκμεταλλεύονται το γεγονός ότι μεγάλη μερίδα των χρηστών αποτελείται από άτομα με υψηλό βιοτικό και μορφωτικό επίπεδο, καθώς οι χρήστες έχουν τη δυνατότητα να κατανοήσουν με μεγαλύτερη ευκολία τα νέα είδη προσφερόμενων προϊόντων και συναλλαγών.

Με τη χρήση στοιχειώδη εργαλείων προώθησης των υπηρεσιών τους μπορούν να προσεγγίσουν μεγαλύτερο εύρος πελατών. Καταφέρνουν να ξεπερνούν τους γεωγραφικούς περιορισμούς σε αντίθεση με παλιότερα και ο αριθμός των υποψηφίων πελατών τείνει να είναι απεριόριστος [38].

Το κόστος για προβολή και διαφήμιση δια μέσου της σελίδας ηλεκτρονικής τραπεζικής περιορίζεται, οπόταν οι τράπεζες προβάλλονται ολοένα και πιο πολύ, κυρίως όταν εφαρμόζουν τις βασικές αρχές του ηλεκτρονικού μάρκετινγκ (e-marketing).

Ακόμη ένα πλεονέκτημα είναι πως ανεξάρτητα από τον τόπο κατοικίας του, ο οποιοσδήποτε έχει τη δυνατότητα να γίνει πελάτης οποιασδήποτε τράπεζας χωρίς να περιορίζεται από το τρόπο εξυπηρέτησης του εκάστοτε υποκαταστήματος. Συνεπώς, το κοινό που πρέπει να εξυπηρετηθεί σε ένα φυσικό κατάστημα μειώνεται και παράλληλα το τραπεζικό προσωπικό δεν αναλώνεται με την εκτέλεση βασικών διαδικασιών. Αντιθέτως, με αυτή την αποσυμφόρηση εκμεταλλεύονται το χρόνο αυτό για την ανάλυση περιπλοκότερων διεργασιών όσον αφορά τα προωθητικά τραπεζικά προϊόντα.

Ταυτόχρονα, μειώνεται το μέσο κόστος για μία συναλλαγή και αυξάνεται η κερδοφορία των τραπεζών δίνοντάς τους μία νέα ώθηση για τη βελτίωση των υπηρεσιών που προσφέρουν. Οι τράπεζες μπορούν πια να επικεντρωθούν στο τι πραγματικά θα ενδιέφερε τους πελάτες τους και πώς να καταφέρουν να συνθέσουν πιο ανταγωνιστικά πλεονεκτήματα τόσο για τη φήμη τους όσο και για την αξιοπιστία των συναλλαγών [8].

### 2.2.2 Πλεονεκτήματα για τους πελάτες

Το βασικότερο πλεονέκτημα για τους πελάτες είναι η εξοικονόμηση χρόνου, αφού όλο το 24ωρο μπορούν να εξυπηρετούνται εκτελώντας όλες τις συναλλαγές τους γρήγορα και απλά από τον Υπολογιστή ή το κινητό τους τηλέφωνο [4].

Επιπλέον, μειώνεται η ανάγκη μετακίνησης στην τράπεζα αφότου δεν απαιτείται η φυσική τους παρουσία στο υποκατάστημα, με αποτέλεσμα να περιορίζονται τα κόστη για τη μετάβασή τους αλλά και ο χρόνος αναμονής στην ουρά για να εξυπηρετηθούν [9].

Το πλεονέκτημα αυτό, είναι εξίσου σημαντικό για τα άτομα που αντιμετωπίζουν κάποιες κινητικές δυσκολίες ως προς τη μετακίνησή τους. Προηγουμένως η μετακίνηση τους θα έπρεπε να γίνει με τη βοήθεια ενός τρίτου ατόμου για να πραγματοποιήσουν τις συναλλαγές τους σε ένα υποκατάστημα. Τώρα, μπορεί εύκολα και αυτή η μερίδα ατόμων να εξυπηρετηθεί αυτόνομα από το χώρο τους χωρίς κανένα περιορισμό [10].

Ένα άλλο προνόμιο που έχουν οι πελάτες, είναι το γεγονός πως μπορούν να αποφασίζουν αβίαστα το τι επενδύσεις θέλουν να κάνουν συλλέγοντας όποια πληροφορία κρίνουν ως σημαντική για να επιλέξουν με ποια τράπεζα θα συνεργαστούν. Επομένως δεν θα έχουν ως μόνο κριτήριο την απόστασή τους από την τράπεζα, αλλά η τελική τους επιλογή γίνεται ανάλογα με το κόστος π.χ. των προμηθειών που θα τους παρέχονται ή τη φήμη της τράπεζας [11].

Επιπρόσθετα, η ηλεκτρονική τραπεζική δίνει τη δυνατότητα στους πελάτες να ελέγχουν τις οικονομικές τους συναλλαγές την ίδια χρονική στιγμή σε πολλές τράπεζες και να μεταφέρουν χρήματα μεταξύ λογαριασμών. Επίσης, μπορούν να πληρώνουν τους

λογαριασμούς τους μέσω e-banking προστατεύοντας έτσι το πορτοφόλι τους από επιπλέον χρεώσεις που τυχόν να είχαν εάν εκτελούσαν τα πιο πάνω με την παρουσία τους σε ένα υποκατάστημα.

### 2.2.3 Μειονεκτήματα για τις τράπεζες

Προκειμένου οι τράπεζες να γίνουν πιο ανταγωνιστικές επενδύουν τεράστια κεφάλαια στην εγκατάσταση και τη συντήρηση των δικτύων τους. Ως αποτέλεσμα αυτού, είναι το υψηλό κόστος για τη δημιουργία και τη λειτουργία της ηλεκτρονικής τραπεζικής και η δαπάνη για την ενίσχυση της ασφάλειας των συστημάτων και των συναλλαγών. Ένα επιπλέον κόστος, είναι η επένδυση στην εκπαίδευση του προσωπικού ώστε να μπορούν να αποκτήσουν τις απαραίτητες γνώσεις για τη χρήση του συγκεκριμένου λογισμικού και να ενημερώνονται συνεχώς για τις αλλαγές που ενδεχομένως να πραγματοποιούνται στη χρήση του e-banking. Απαραίτητη όμως είναι η ανάγκη μίας ομάδας ή ενός τμήματος από προσωπικό που να διακατέχει την απαιτούμενη τεχνογνωσία ώστε να παρέχει λειτουργική υποστήριξη των υπηρεσιών και των νέων τεχνολογιών.

Λόγω του ότι οι υπηρεσίες της ηλεκτρονικής τραπεζικής συνδέονται με τους κινδύνους που επιφυλάσσει το Διαδίκτυο, κύριο μέλημα των τραπεζών είναι η διασφάλιση των συναλλαγών και των προσωπικών δεδομένων των πελατών. Άλλωστε, ο νέος κανονισμός που τέθηκε σε ισχύ τον Μάιο του 2018 από την Ευρωπαϊκή Ένωση περί προστασίας των προσωπικών δεδομένων, ορίζει αποζημιώσεις που μπορεί να φτάσουν μέχρι και το 4% των παγκόσμιων εσόδων της απερχόμενης χρονιάς.

Η ενίσχυση των συστημάτων για περισσότερη ασφάλεια των συναλλαγών όπως η αγορά ενός διακομιστή που επιφέρει επιπλέον κόστος, μπορεί να προβεί επιζήμιο για την ίδια την τράπεζα. Επιπρόσθετα, σε περίπτωση οποιουδήποτε σφάλματος ή κάποιου πιθανού προβλήματος δια-λειτουργικότητας σε ένα Λειτουργικό Σύστημα, μπορεί να επιφέρει σημαντική επίπτωση στην εικόνα των τραπεζών με αντίκτυπο το ενδεχόμενο του κλονισμού της φήμης τους [12].

Ο συνεχής ανταγωνισμός μπορεί επίσης να στραφεί εναντίον των τραπεζικών ιδρυμάτων, διότι προσπαθούν να επιδείξουν ολοένα και πιο πολύ τα καινοτόμα συστήματα και τις υπηρεσίες τους, για να προσελκύουν περισσότερους πελάτες.

Ο πιο σημαντικός ίσως κίνδυνος στον οποίο εκτίθεται μία τράπεζα είναι όταν ενώ έχει προβεί στην ανάπτυξη ενός συστήματος, αργότερα να μην αναλαμβάνει νέες τεχνολογικές επενδύσεις για να κρατά σταθερή την ασφάλειά του, με επακόλουθο να χάνει την προτίμηση των χρηστών.

### 2.2.4 Μειονεκτήματα για τους πελάτες

Μπορεί η πλειοψηφία των χρηστών του online banking να είναι αρκετά εξοικειωμένη με το πώς να χειρίζονται τις καθημερινές τους συναλλαγές, εντούτοις υπάρχει ένα μεγάλο ποσοστό πελατών που ανήκουν σε μία γενιά που δεν κατέχουν τις γνώσεις για τη χρήση του Διαδικτύου και των νέων τεχνολογιών. Αυτό έχει ως αποτέλεσμα, τη μη προσαρμογή τους στην νέα τάξη πραγμάτων εξαιτίας του φόβου και της άγνοιας που τους διακατέχει, αδυνατώντας να προβούν στην εκτέλεση των ηλεκτρονικών τους συναλλαγών. Οπόταν οι πελάτες που δυσκολεύονται με το χειρισμό αυτό, εξακολουθούν να επισκέπτονται τα υποκαταστήματα για να εξυπηρετηθούν χάνοντας χρόνο και χρήμα εξαιτίας των προμηθειών που τους επιβάλλονται.

Ένας ακόμη σημαντικός παράγοντας που δημιουργεί δυσπιστία στο κοινό, είναι η αύξηση στα φαινόμενα ηλεκτρονικής απάτης. Αποτέλεσμα αυτού, είναι η αποτροπή των χρηστών από τις ηλεκτρονικές υπηρεσίες λόγω αβεβαιότητας για την ασφάλεια των συναλλαγών και της προστασίας των προσωπικών τους δεδομένων. Πολλές φορές λόγω λανθασμένων κινήσεων των πελατών, όπως η κοινοποίηση του κωδικού πρόσβασης σε τρίτους ή η μη αποσύνδεση από το σύστημα κατά τη χρήση ενός δημόσιου Υπολογιστή για την εκτέλεση συναλλαγών, τους καθιστά έρμαιους σε κακόβουλες επιθέσεις.

Επιπρόσθετα, η συνεχείς ανάπτυξη του e-banking απαιτεί από τους πελάτες να μένουν διαρκώς ενημερωμένοι για τις αλλαγές των υπηρεσιών που προσφέρονται από τις τράπεζές τους. Πρέπει συνεχώς να εκπαιδεύονται ακολουθώντας όλες τις νέες τεχνολογικές εξελίξεις.

Τέλος, η έλλειψη επαφής με κάποιο τραπεζικό στέλεχος σε περίπτωση άμεσης βοήθειας συμβάλλει στη μείωση των ανθρωπίνων σχέσεων και στη στέρηση της προσωπικής επαφής μεταξύ πελατών και υπαλλήλων.

### 2.2.5 Κίνδυνοι του online banking

Παρόλο που οι τράπεζες επενδύουν συνεχώς στο τομέα της ασφάλειας των ηλεκτρονικών συστημάτων τους, εντούτοις εμφανίζουν τρωτά σημεία που εγκυμονούν κινδύνους τόσο για τις ίδιες τις τράπεζες όσο και για τους πελάτες τους.

Η βασικότερη απειλή που έχει παρατηρηθεί είναι μέσω κακόβουλων λογισμικών που αναπτύσσονται από **εισβολείς** (hackers) με σκοπό να εκμεταλλεύονται είτε την άγνοια των χρηστών, είτε τις αδυναμίες των ίδιων των συστημάτων ώστε να υποκλέψουν προσωπικά δεδομένα προς οικονομικό τους όφελος.

Ο πιο διαδεδομένος κίνδυνος που μπορεί να έρθει αντιμέτωπος ο χρήστης είναι οι **Ιοί** (virus). Τα κακόβουλα αυτά προγράμματα μπορεί να μολύνουν τον Υπολογιστή όπως για παράδειγμα να γίνει διαγραφή κάποιων προσωπικών του αρχείων, χωρίς την γνώση ή την άδεια του ίδιου του χρήστη.

Παρόμοιο με τον ιό είναι ο **Δούρειος Ίππος** (Trojan Horse), όπου φαινομενικά παρουσιάζεται ως ένα χρήσιμο λογισμικό στον Υπολογιστή και τρέχει στο παρασκήνιο μέσω καμουφλαρισμένων εντολών ανοίγοντας την πρόσβαση σε τρίτους. Η πρόσβαση αυτή, μπορεί να είναι η παρακολούθηση δραστηριοτήτων στον Υπολογιστή του χρήση ή ακόμα και ο πλήρης έλεγχος σε αυτόν με σκοπό την διαγραφή ή την υποκλοπή δεδομένων[13].

Μία άλλη μέθοδος που χρησιμοποιούν οι χάκερς είναι τα λεγόμενα **λαγωνικά** (sniffers) όπου και σε αυτή την περίπτωση μπορεί να μην γίνουν αντιληπτά από το χρήστη. Πρόκειται για κρυφά προγράμματα που παρακολουθούν την κίνηση στο δίκτυο και έχουν την δυνατότητα υποκλοπής δεδομένων εάν αυτά δεν είναι κρυπτογραφημένα. Τέτοια δεδομένα μπορεί να είναι αριθμοί των πιστωτικών καρτών είτε κωδικοί πρόσβασης στα τραπεζικά συστήματα τα οποία μπορούν να διαβαστούν από έναν εισβολέα αναλύοντας το πακέτο στο δίκτυο.

Μία ακόμη σοβαρή απειλή για τη διαρροή στοιχείων και ευαίσθητων δεδομένων αποτελεί η **καταγραφή πληκτρολόγησης** (key logging). Ανάλογα με τη μέθοδο του προγραμματιστή και το τι θέλει να επιδιώξει, το κακόβουλο αυτό πρόγραμμα καταγράφει και αποθηκεύει οτιδήποτε πληκτρολογεί ο χρήστης. Έπειτα, το αρχείο με τα δεδομένα καταγραφής λειτουργεί και μπορεί να εγκατασταθεί σε διαφορετικά αρχεία ενός Υπολογιστή, για να μην μπορεί να γίνει αντιληπτό από το χρήστη [3].

Η πιο διαδεδομένη τεχνική που παραπλανά καθημερινά αρκετούς χρήστες είναι το **ψάρεμα** (phishing) κυρίως μέσω ανεπιθύμητων (spam) email. Συνήθως τέτοιου είδους μηνύματα προέρχονται με την επωνυμία μίας νόμιμης επιχείρησης, οργανισμού ή τράπεζας όπου προτρέπουν το χρήστη να επισκεφθεί μέσω ενός συνδέσμου – url μία ιστοσελίδα παρόμοια με αυτή του οργανισμού. Το πλαστό αυτό site ζητά επιβεβαίωση των στοιχείων του χρήστη (π.χ. κωδικούς πρόσβασης, αριθμό πιστωτικών καρτών και τραπεζικών λογαριασμών), πείθοντάς τον ότι πρόκειται για την ασφάλειά του. Μοναδικός φυσικά σκοπός είναι η εξαπάτηση των «θυμάτων» τους και η εκμετάλλευση των προσωπικών τους δεδομένων ενεργώντας κακόβουλα, εκμεταλλευόμενοι την ανυποψία των χρηστών [13].

# Κεφάλαιο 3
# Ασφάλεια, Ταυτοποίηση και Αυθεντικοποίηση

## 3.1 Ασφάλεια

Καθημερινά όλο και περισσότεροι χρήστες του Διαδικτύου στρέφουν το ενδιαφέρον τους στο online banking. Η διασφάλιση του απορρήτου των προσωπικών δεδομένων των χρηστών και οι πρόσθετοι κίνδυνοι που παραμονεύουν λόγω της διακίνησης μέσω Διαδικτύου, αναγκάζουν τις τράπεζες να επενδύουν συνεχώς στο θέμα της ασφάλειας.

Οι τράπεζες καταβάλλουν κάθε δυνατή προσπάθεια από μεριάς τους να διατηρούν το ζήτημα της ασφάλειας σε υψηλά επίπεδα κάνοντας εκτεταμένες επενδύσεις προς αυτή την κατεύθυνση. Πέραν όμως αυτού, έχουν να διευθετήσουν το γεγονός ότι πολλοί χρήστες είναι διστακτικοί και κρατούν τις επιφυλάξεις τους σχετικά με τη χρήση του online banking, εφόσον η μεγαλύτερη τους ανησυχία είναι η ασφάλεια των ευαίσθητων δεδομένων και των συναλλαγών τους [14].

Η συνεργασία τραπεζών και χρηστών είναι απαραίτητη για να καταφέρουν να επιτύχουν το στόχο για την αποτροπή οποιονδήποτε πιθανών απειλών. Για να καταφέρουν να κερδίσουν το κοινό, καλούνται να διασφαλίσουν τα συστήματά τους με συνεχείς αναβαθμίσεις ενώ παράλληλα να ενημερώνουν τους χρήστες ώστε να κατανοήσουν την αξιοπιστία των συστημάτων αυτών. Πρέπει δηλαδή, να εξηγήσουν στους χρήστες εφιστώντας τους την προσοχή πως υπάρχει και από μεριάς τους μερίδιο υπευθυνότητας. Παρόλο που παραμονεύουν αρκετοί κίνδυνοι, επιβάλλεται να καταβάλλουν ότι είναι δυνατό ώστε να θεωρούνται ασφαλές.

Οι χρήστες από πλευράς τους, απαιτούν ακεραιότητα, εμπιστευτικότητα, διαθεσιμότητα και αυθεντικότητα όσον αφορά τις συναλλαγές τους για να εξασφαλίζεται ότι τα δεδομένα τους δεν δύναται να διαρρεύσουν. Για να καταστεί ένα υψηλό επίπεδο ασφάλειας από μεριάς των τραπεζών, δεν απαιτείται απλά η χρήση κατάλληλης τεχνολογίας αλλά είναι θέμα κατάλληλης στρατηγικής.

Άρα τα συστήματα θα πρέπει να διαθέτουν ουσιαστικά ότι απαιτούν και οι χρήστες για την ασφάλεια του online banking.

Το πρώτο και βασικότερο είναι η **εμπιστευτικότητα** (confidentiality), η ικανότητα δηλαδή αποτροπής πρόσβασης και αποκάλυψης ευαίσθητων δεδομένων από μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες. Έτσι με την εφαρμογή κατάλληλων αλγορίθμων, τα δεδομένα που διακινούνται μεταξύ Υπολογιστών στο δίκτυο μπορούν να τροποποιηθούν και να καταστούν μη αναγνώσιμα σε περίπτωση που πέσουν στα χέρια τρίτων.

Επακόλουθο της εγκυρότητας των δεδομένων είναι η **ακεραιότητα** (integrity) αυτών, δηλαδή η πρόληψη μη εξουσιοδοτημένης μεταβολής ή αλλοίωσης πληροφοριών (π.χ. δημιουργία δεδομένων, εγγραφή ή διαγραφή δεδομένων).

Υπάρχουν βέβαια και περιπτώσεις όπου η ανάκτηση των δεδομένων ανά πάσα στιγμή από τους χρήστες είναι απαραίτητη αν συμβεί οποιαδήποτε διακοπή στη λειτουργία του τραπεζικού συστήματος ή προσωρινή διακοπή της λειτουργίας τους. Η **διαθεσιμότητα** (availability) σ ’αυτή την περίπτωση είναι αναγκαία και θα πρέπει να είναι προσπελάσιμη όταν χρειάζεται να ανακτηθεί, χωρίς την αδικαιολόγητη καθυστέρηση των υπηρεσιών ενός δικτύου Υπολογιστών. Αυτό που πρέπει να απασχολεί τις τράπεζες για σκοπούς ασφάλειας, είναι η παρεμπόδιση κακόβουλων επιθέσεων άρνησης παροχής υπηρεσιών για την αποτροπή της μη προσπέλασης στα αγαθά των νόμιμων χρηστών.

Σε κάθε περίπτωση η υποχρέωση ύπαρξης ασφαλιστικών δικλίδων για την επικύρωση της **αυθεντικότητας** (authentication) είναι αναγκαία για την αναγνώριση της γνησιότητας της ταυτότητας του χρήστη που εμφανίζεται στη συναλλαγή. Εφόσον εξακριβωθεί και αποδειχθεί ποιος θα διενεργήσει την συναλλαγή διασφαλίζεται παράλληλα και η νομιμότητά της.

Επομένως για το σκοπό αυτό, υπάρχει η ανάγκη για ανάπτυξη και συνεχής αναβάθμιση μηχανισμών για ταυτοποίηση και αυθεντικοποίηση των χρηστών για την εξασφάλιση της μη αποποίησης της ευθύνης των εμπλεκόμενων μερών σε κάθε συναλλαγή.

## 3.2 Ταυτοποίηση και Αυθεντικοποίηση

Η ταυτοποίηση και η αυθεντικοποίηση του χρήστη είναι οι κύριοι παράγοντες για τον έλεγχο της ασφάλειας ενός συστήματος και αποτελούν βασική προϋπόθεση για τη διαδικασία ελέγχου προσπέλασης στους πόρους που το απαρτίζουν. Αποτελούν στην ουσία τα δύο μέρη ενεργοποίησης του πρωτοκόλλου επικοινωνίας, το πρώτο είναι αυτό

που παρέχει τις πληροφορίες για την απόδειξη της ταυτότητας και το δεύτερο είναι για την επιβεβαίωση ή την απόρριψη της ορθότητας των πληροφοριών.

Σύμφωνα με τους Κάτσικα και Γκρίτζαλη «οι έννοιες ταυτοποίηση και αυθεντικοποίηση ορίζονται ως εξής»:

Με τον όρο **ταυτοποίηση** (identification), εννοούμε τη διαδικασία κατά την οποία σε ένα Πληροφοριακό Σύστημα παρέχονται από το λογικό υποκείμενο οι πληροφορίες που απαιτούνται για να γίνει η συσχέτιση με ένα από τα αντικείμενα που δικαιούνται προσπέλασης στους πόρους (resources) του.

Με τον όρο **αυθεντικοποίηση** (authentication), εννοούμε τη διαδικασία 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.

### 3.2.1Κατηγορίες αυθεντικοποίησης

Η αυθεντικοποίηση είναι αναγκαία σε ένα Πληροφοριακό Σύστημα διότι η ταυτότητα που έχει δηλωθεί σε αυτό, αποτελεί παράμετρο για την προσπέλαση στους πόρους και στην καταγραφή του ελέγχου που γίνεται κατά τη διαδικασία πρόσβασης ενός υποκειμένου στο σύστημα.

Για την ολοκλήρωση της διαδικασίας αυθεντικοποίησης θα πρέπει να περιλαμβάνει την παροχή πληροφοριών από ένα λογικό υποκείμενο στο σύστημα. Ακολούθως θα αναλύεται αυτή η πληροφορία και έπειτα να ελέγχεται ότι πράγματι η πληροφορία έχει σχέση με το ίδιο λογικό αντικείμενο [15].

Λόγω του ότι υπάρχουν διάφορα είδη συστημάτων που πραγματοποιούν τις παραπάνω διαδικασίες με τους ανάλογους μηχανισμούς, έχουν κατηγοριοποιηθεί οι τεχνικές για την εφαρμογή ελέγχων αυθεντικοποίησης και διακρίνονται σε τέσσερεις κύριους τύπους:

**Τύπος Ι:** Κάτι που γνωρίζει το λογικό υποκείμενο (π.χ. ένα PIN, ένα συνθηματικό, όνομα χρήστη)

**Τύπος ΙΙ:** Κάτι που κατέχει το λογικό υποκείμενο (π.χ. ψηφιακό πιστοποιητικό, έξυπνη κάρτα)

**Τύπος ΙΙΙ:** Κάτι που χαρακτηρίζει το λογικό υποκείμενο βάση μονοσήμαντων βιομετρικών χαρακτηριστικών του (π.χ. αναγνώριση φωνής και ίριδας, δακτυλικά αποτυπώματα)

**Τύπος IV:** Κάτι που προσδιορίζει το που βρίσκεται, σε ποια τοποθεσία είναι το λογικό υποκείμενο (π.χ. IP διεύθυνση, αναγνωριστικό Υπολογιστή)

### 3.2.2 Δεδομένα Αυθεντικοποίησης

Τα βασικότερα τεκμήρια που αναλύονται και χρησιμοποιούνται για τον έλεγχο αυθεντικοποίησης και ανήκουν στους τρεις πρώτους τύπους εφαρμογής ελέγχων είναι τα συνθηματικά, οι έξυπνες κάρτες, τα ψηφιακά πιστοποιητικά και τα βιομετρικά συστήματα.

Τα **συνθηματικά** (passwords) ανήκουν στον **Τύπο Ι** τρόπο αυθεντικοποίησης. Χαρακτηρίζεται ως η πληροφορία που σχετίζεται με τους χρήστες και επιβεβαιώνει την ταυτότητά τους. Είναι στην ουσία κάτι που οι ίδιοι οι χρήστες γνωρίζουν.

Ορισμένα κριτήρια που πρέπει να τηρούνται για την επιλογή των συνθηματικών είναι αρχικά η αποφυγή εύκολων κωδικών πρόσβασης. Οι χρήστες έχουν την επιλογή να επιλέγουν οι ίδιοι τα συνθηματικά, παράλληλα όμως πρέπει να υπάρχει ένας περιορισμός στην επιλογή τους, όπως το να αποφεύγουν την εισαγωγή ονομάτων, ημερομηνιών και λέξεων που θα μπορεί εύκολα κάποιος τρίτος να τα μαντέψει. Το μήκος των συνθηματικών πρέπει να είναι αρκετά σύνθετο και να αποτελείται από συνδυασμό γραμμάτων, ειδικών χαρακτήρων και αριθμών. Τα συνθηματικά θα πρέπει να φυλάσσονται και να μην καταγράφονται σε εμφανή σημεία. Καλό θα ήταν να αλλάζονται τακτικά ή να εφαρμόζεται ένας έλεγχος όπου να προτρέπει τους χρήστες να προβούν στην αλλαγή τους.

Για τη δημιουργία των συνθηματικών δεν απαιτείται υψηλό κόστος για το σχεδιασμό τους ούτε κάποιος ιδιαίτερος εξοπλισμός για την υλοποίηση τους. Η απλότητα όσον αφορά τη λειτουργία τους δεν απαιτεί εξειδικευμένη γνώση και εμπειρία για να αναγκάζονται οι χρήστες να τύχουν εκπαίδευσης. Προσφέρουν ένα ικανοποιητικό επίπεδο προστασίας εάν φυσικά υφίσταται μία πολιτική για την ασφαλέστερη εφαρμογή τους στα τραπεζικά συστήματα.

Από την άλλη τυγχάνουν φορές που ένα συνθηματικό μπορεί να αποκαλυφθεί κατά τη διάρκεια της μετάδοσής του σε ένα κατανεμημένο περιβάλλον. Επομένως, οι τραπεζικοί οργανισμοί συσχετίζουν τα συνθηματικά με μοναδικά αναγνωριστικά ώστε να προσδιορίζουν την ταυτότητα του κάθε χρήστη. Για να καταφέρει ο χρήστης την είσοδό του στο σύστημα, θα πρέπει να καταχωρήσει το αναγνωριστικό του και μετά το συνθηματικό του για να πετύχει την αυθεντικοποίησή του. Μετά την εισαγωγή των

δεδομένων στο σύστημα, λειτουργεί ο μηχανισμός για την επαλήθευση της εγκυρότητας των στοιχείων που είναι είδη καταχωρημένα στο αρχείο συνθηματικών. Εφόσον και τα δύο στοιχεία είναι έγκυρα τότε επιτυγχάνεται η πρόσβαση στο σύστημα.
Μιας και η συχνότερη αιτία παραβίασης της ασφάλειας γίνεται με την υποκλοπή των συνθηματικών, ορισμένα συστήματα έχουν εφαρμόσει ακόμη ένα μηχανισμό για την αποφυγή μη εξουσιοδοτημένης πρόσβασης. Έχουν προσθέσει μετρητές που καταγράφουν τον αριθμό των αποτυχημένων προσπαθειών σύνδεσης και εάν το επιτρεπτό όριο ξεπεραστεί αποτρέπεται η είσοδος στο σύστημα. Επιπλέον, τα συστήματα έχουν ενισχυθεί με μηχανισμούς επαναλαμβανόμενης αυθεντικοποίησης όπου ζητείται σε τακτά χρονικά διαστήματα η αυθεντικοποίηση των χρηστών για μεγαλύτερη ασφάλεια των συστημάτων.

Στο **Τύπο ΙΙ** συναντάμε τις **έξυπνες κάρτες** όπου αποτελούν μία αρκετά διαδεδομένη εφαρμογή αυθεντικοποίησης και ταυτοποίησης. Πολλοί οργανισμοί έχουν συμπεριλάβει αυτή την τεχνολογία σε εφαρμογές όπως στο ηλεκτρονικό πορτοφόλι και στα έξυπνα κινητά τηλέφωνα.
Χάρη στην τεχνολογία που διαθέτουν κατάφεραν να αποκτήσουν μεγάλη δυναμική κερδίζοντας αρκετό κοινό. Τα δεδομένα αποθηκεύονται και επεξεργάζονται με τη βοήθεια του μικροεπεξεργαστή που διαθέτουν, ενώ την ίδια στιγμή γίνεται εγγραφή και ενημέρωση των δεδομένων στην κάρτα. Η διαδικασία ταυτοποίησης πραγματοποιείται με την πληκτρολόγηση του μυστικού κωδικού (PIN) του κάθε κατόχου.
Έπειτα εκτελείται εσωτερικά για μεγαλύτερη ασφάλεια, μία διαδικασία ώστε να συγκριθεί ο κωδικός που έχει πληκτρολογηθεί με τον αντίστοιχο κωδικό που βρίσκεται στη μυστική μνήμη της κάρτας. Στόχος αυτής της διαδικασίας είναι η διασφάλιση της γνησιότητας της κάρτας, ότι έχει εξασφαλιστεί δηλαδή από εξουσιοδοτημένο φορέα και κατά συνέπεια επιτρέπει την πρόσβαση του κατόχου της σε δεδομένα και υπηρεσίες.

Πέραν από τις έξυπνες κάρτες στον **Τύπο ΙΙ** ακόμη μία εφαρμογή που συναντάμε είναι τα **ψηφιακά πιστοποιητικά**. Στηρίζουν τη λειτουργεία τους στην Κρυπτογραφία Δημοσίου Κλειδιού με τη μορφή δυαδικών αρχείων. Η ιδιαιτερότητά τους, είναι ότι μπορούν να χρησιμοποιηθούν ενσωματώνοντας ψευδώνυμα στη θέση της πραγματικής ταυτότητας του χρήστη για να περιοριστεί η αποκάλυψη της ταυτότητάς του.

Άλλη μία τεχνική εφαρμογής ελέγχου αυθεντικοποίησης που παρέχει μεγαλύτερη ασφάλεια και ανήκει στην **Τύπου ΙΙΙ** κατηγορία είναι η ταυτοποίηση με **βιομετρικά χαρακτηριστικά**. Τα βιομετρικά χαρακτηριστικά όπως το δακτυλικό αποτύπωμα, η αναγνώριση της ίριδας και άλλα τα οποία θα αναλυθούν περαιτέρω στο επόμενο κεφάλαιο, βασίζονται στα φυσικά χαρακτηριστικά του ανθρωπίνου σώματος. Χρησιμοποιούνται σαν αποδεικτικά στοιχεία για την αναγνώριση και επαλήθευση ενός λογικού υποκειμένου που ζητά προσπέλαση στο Πληροφοριακό Σύστημα.

Συνεπώς, η χρήση βιομετρικών συστημάτων μαζί με την σωστή αξιοποίηση των συνθηματικών και των έξυπνων καρτών θα βοηθήσουν στην επίτευξη ασφάλειας των Πληροφοριακών Συστημάτων και θα καταφέρουν σημαντική βελτίωση στον τεχνολογικό κόσμο.

# Κεφάλαιο 4
# Βιομετρία

## 4.1 Εισαγωγή

Από αρχαιοτάτων χρόνων η χρήση βιομετρίας ήταν αναγκαία για την πιστοποίηση της ταυτότητας των ατόμων ούτως ώστε να αποφευχθεί η απάτη σε συστήματα πληρωμών. Όσα άτομα είχαν εμπλακεί σε εγκλήματα ή παράνομες ενέργειες χρησιμοποιείτο η μέθοδος ταυτοποίησης των αποτυπωμάτων τους ως τρόπος εξιχνίασης. Η μοναδικότητα των αποτυπωμάτων οδηγούσε στο συμπέρασμα ότι το εν λόγω άτομο είχε διαπράξει το έγκλημα και μπορούσε να κατηγορηθεί. Μέσα από την ανακάλυψη αυτή έγινε αντιληπτή η μοναδικότητα των αποτυπωμάτων και συνάμα ξεκίνησε να διευρύνεται η χρήση των βιομετρικών συστημάτων.

## 4.2 Ορισμός Βιομετρίας

Η βιομετρία ορίζεται ως η στατιστική ανάλυση των μοναδικών φυσικών ή βιολογικών χαρακτηριστικών του ανθρώπου. Σήμερα, χαρακτηρίζεται ως η επιστήμη που συλλέγει και αναλύει τα ανθρώπινα χαρακτηριστικά με τη χρήση ψηφιακής τεχνολογίας με σκοπό τον έλεγχο πρόσβασης και ασφάλειας στους πόρους του συστήματος [16].

Βασισμένη στο γεγονός ότι οι παραδοσιακές μέθοδοι ταυτοποίησης (κωδικοί πρόσβασης, PIN) δεν θεωρούνται αξιόπιστες, η βιομετρική έχει εξελιχθεί χάρη στην διαρκώς αυξανόμενη ανάγκη για περισσότερη ασφάλεια. Αρχικά, αναπτύχθηκε από κυβερνητικούς οργανισμούς για τον έλεγχο πρόσβασης σταθμών που θεωρούνταν κρίσιμοι για την εθνική ασφάλεια. Η βελτίωση των βιομετρικών τεχνολογιών, στηρίχθηκε αρκετά από την εξέλιξη στον επιστημονικό χώρο. Ήδη πολλοί οργανισμοί όπου απαιτείται υψηλό επίπεδο ασφάλειας, όπως σε κρατικές υπηρεσίες και σε τράπεζες, ενσωμάτωσαν και εφαρμόζουν βιομετρικές μεθόδους αναγνώρισης στα συστήματά τους.

## 4.3 Χαρακτηριστικά Βιομετρικών Συστημάτων

Όλες οι βιομετρικές μέθοδοι αξιολογούνται με βάση κάποιων παραγόντων και χαρακτηριστικών που διαθέτουν. Τα κυριότερα χαρακτηριστικά των βιομετρικών συστημάτων είναι: [15,17]

**Ακρίβεια**

Τα βιομετρικά συστήματα έχουν ως γνώριμο χαρακτηριστικό τους την ακρίβεια.
Η ακρίβεια ορίζεται ως το ποσοστό της ορθής αναγνώριση ενός εξουσιοδοτημένου προσώπου από ένα μη εξουσιοδοτημένο και έχει δύο μονάδες μέτρησης. Η πρώτη σχετίζεται με το ποσοστό της απόρριψης των εξουσιοδοτημένων ατόμων και η δεύτερη με το ποσοστό αποδοχής μη εξουσιοδοτημένων ατόμων σε ένα σύστημα. Σε περίπτωση πιθανότητας πρόσβασης σε μη εξουσιοδοτημένο άτομο, το σύστημα θα πρέπει να προσαρμοστεί ώστε ο δείκτης του ποσοστού σφάλματος αποδοχής να πλησιάζει το 0%. Οι δύο μονάδες μέτρησης ανάλογα με τις απαιτήσεις ασφαλείας, ρυθμίζονται για να επικρατήσει το σημείο τομής τους στο Ολικό Επίπεδο Σφάλματος (Crossover Error Rate-CER).

**Αξιοπιστία**

Έχοντας όσο το δυνατό λιγότερα έξοδα για τη συντήρηση και τον έλεγχο του συστήματος, η αξιοπιστία μπορεί να οριστεί ως ακριβής, γρήγορη και συνεχής για την ομαλή λειτουργία ενός βιομετρικού συστήματος.

**Μοναδικότητα**

Τα βιομετρικά συστήματα λειτουργούν έχοντας ως άξονα τα μοναδικά είτε φυσικά είτε συμπεριφορικά ανθρώπινα χαρακτηριστικά. Αυτό είναι κάτι που συμβάλλει στην ορθή λειτουργία της διαδικασίας αναγνώρισης αποφεύγοντας την ίδια στιγμή πιθανά λάθη.

**Ταχύτητα**

Η ταχύτητα ελέγχου προσπέλασης κατά τη συλλογή των δεδομένων του βιομετρικού χαρακτηριστικού μέσα από τη Βάση Δεδομένων ενός συστήματος, αποτελεί το βασικότερο χαρακτηριστικό. Η διαδικασία αναγνώρισης πρέπει να γίνεται σε τέτοιο χρόνο που να είναι αποδεκτός από το χρήστη και να διαρκεί όσο το δυνατόν λιγότερα δευτερόλεπτα [15].

**Συλλογή, αποθήκευση και απαιτήσεις επεξεργασίας δεδομένων**

Η συλλογή και η αποθήκευση των δεδομένων απαιτεί τον αντίστοιχο χρόνο που θα χρειαστεί το σύστημα ώστε να μπορέσει να τα επεξεργαστεί. Το επίπεδο αποδοχής σφάλματος επηρεάζει το χρόνο για την εισαγωγή των δεδομένων. Όσο πιο χαμηλό είναι, τόσο περισσότερος χρόνος θα χρειάζεται για να συγκριθούν με τα δεδομένα της βάσης. Σήμερα, μιας και η αγορά διαθέτει ταχύτατους επεξεργαστές και το κόστος είναι συγκριτικά μειωμένο για τις συσκευές που μπορούν να φιλοξενήσουν δεδομένα, είναι σίγουρα πιο αποδεκτός ο χρόνος της επεξεργασίας των αρχείων με βιομετρικά στοιχεία.

**Καταχώρηση**

Ο χρόνος διάθεσης του χρήστη για την εισαγωγή των βιομετρικών στοιχείων του στο σύστημα ορίζεται ως διαδικασία καταχώρησης. Η καταχώρηση θα πρέπει να συνάδει με τις απαιτήσεις του συστήματος προκειμένου να γίνει εφικτή η ταυτοποίηση.

**Παραποίηση στοιχείων**

Η ψευδής εισαγωγή στοιχείων από μία μη εξουσιοδοτημένη οντότητα για την είσοδο στο σύστημα, παίζει καθοριστικό ρόλο στην ασφάλεια των βιομετρικών συστημάτων. Για την αποτροπή της εισόδου απαιτείται ένα αξιόλογο ποσοστό ακρίβειας του βιομετρικού χαρακτηριστικού.

**Αποδοχή από τους χρήστες**

Η καταχώρηση ατομικών γνωρισμάτων προκαλεί κοινωνικές αντιδράσεις στους χρήστες νομίζοντας ότι παρακολουθούνται από κάποιο σύστημα. Ένας άλλος υποθετικός κίνδυνος είναι η δημιουργία κάποιας πάθησης στο οργανισμό των χρηστών από το ίδιο το σύστημα γεγονός που σχετίζεται με την μη αποδοχή τους.

## 4.4 Είδη Βιομετρικών Χαρακτηριστικών

Ως βιομετρικά χαρακτηριστικά ορίζονται όλα τα γνωρίσματα ή οι συμπεριφορές που χρησιμεύουν στη διαδικασία ταυτοποίησης ενός ατόμου και ταξινομούνται σε δύο κατηγορίες. Η πρώτη κατηγορία έχει να κάνει με τη φυσική βιομετρία, όπου μετρά και εξάγει δεδομένα από διάφορα μέλη του σώματος όπου θεωρούνται μοναδικά για κάθε άτομο [15,17].

Τέτοια χαρακτηριστικά είναι:

- Η αναγνώριση του προσώπου (facial recognition)
- Τα δακτυλικά αποτυπώματα (fingerprint)
- Τα αποτυπώματα της παλάμης (palm print)
- Η γεωμετρία του χεριού (hand geometry)
- Η αναγνώριση της ίριδας (iris recognition)
- Η σάρωση του αμφιβληστροειδούς (retinal scan)
- Αγγειακά σχέδια (vascular patterns)
- Ανάλυση γενετικού υλικού (DNA analysis)
- Ανάλυση αυτιού (ear recognition)

Η δεύτερη κατηγορία αφορά την τεχνική μέτρησης της συμπεριφοράς του ατόμου μέσω των βιολογικών χαρακτηριστικών του. Παραδείγματα αποτελούν:

- Η ανάλυση της φωνής (voice recognition)
- Η αναγνώριση της υπογραφής (signature recognition)
- Η ανάλυση της πληκτρολόγησης (keystroke analysis)

### 4.4.1 Φυσικά Βιομετρικά

Όπως αναφέρθηκε προηγουμένως, τα βιολογικά χαρακτηριστικά διακρίνονται σε φυσικά και συμπεριφορικά. Τα φυσικά βιομετρικά χαρακτηριστικά αφορούν την απευθείας μέτρηση των ανθρωπίνων χαρακτηριστικών. Πιο κάτω αναλύονται τα εξής:

**Δακτυλικά αποτυπώματα**

Κάνοντας αρχή από τα φυσικά χαρακτηριστικά, τα δακτυλικά αποτυπώματα αποτελούν μία από τις πιο αξιόπιστες μεθόδους εξακρίβωσης ταυτότητας. Η χρήση δακτυλικών αποτυπωμάτων έχει συνδεθεί όλα αυτά τα χρόνια αποκλειστικά για ποινικούς σκοπούς και ταυτίζεται με την αναγνώριση εγκληματιών. Λόγω της ταύτισης αυτής, αρκετός κόσμος έχει επηρεαστεί και αντιστέκεται σε ένα σύστημα που ζητά την ταυτοποίηση με αναγνώριση αποτυπωμάτων, πιστεύοντας πως αντιμετωπίζονται ως εγκληματίες. Όπως θα διαπιστωθεί και αργότερα στην έρευνα μας, θα δούμε ότι πρόκειται για το σημαντικότερο λόγο που η αποδοχή του κοινού βρίσκεται σε μεσαία επίπεδα παρά την πληθώρα των πλεονεκτημάτων που έχουν τα βιομετρικά συστήματα.

Για την αναγνώριση των αποτυπωμάτων, χρησιμοποιούνται συστήματα με ιδιαίτερη πολυπλοκότητα λόγω του ότι ο τύπος και η γεωμετρία των δακτυλικών αποτυπωμάτων είναι διαφορετικός σε κάθε άτομο χωρίς να μεταβάλλεται με την πάροδο του χρόνου.
Οι καμπύλες μαζί με τις διαιρέσεις των σπειρών αλλά και η μορφή ολόκληρου του δακτυλικού σπειρώματος, είναι τα πιο διαδεδομένα χαρακτηριστικά τα οποία χρησιμοποιούνται στη διαδικασία ανίχνευσης. Τα δακτυλικά αποτυπώματα ανιχνεύονται μέσω ειδικών συσκευών-κάμερες χρησιμοποιώντας τις διαφορές των ηλεκτρονικών φορτίων στις σπείρες των δακτύλων για να εντοπιστεί το σημείο που εφαρμόζουν στο τσιπ. Με τη βοήθεια των συσκευών σάρωσης δακτυλικών αποτυπωμάτων (fingerprint scanners) τα δεδομένα που συλλέγονται και αποθηκεύονται σε μία Βάση Δεδομένων μετατρέπονται σε γραφήματα. Όταν ο χρήστης τοποθετήσει το δάκτυλό του πάνω στη συσκευή, ο αισθητήρας καταγράφει τα αποτυπώματά του και το ειδικό λογισμικό που είναι συνδεδεμένο με τη συσκευή αναλαμβάνει τη σύγκριση των χαρακτηριστικών. Αν τα αποτυπώματα που πάρθηκαν βρεθούν στη βάση, τότε το σύστημα παρέχει την πρόσβαση στο χρήστη, αλλιώς σε περίπτωση μη ταυτοποίησης δεν του επιτρέπεται η είσοδος. Υπάρχουν βέβαια περιπτώσεις όπου οι τροποποιήσεις των δακτυλικών αποτυπωμάτων από εγκαύματα, δερματικές ασθένειες ή τραυματισμούς μπορεί να επηρεάσουν την επίδοση του συστήματος και κατά συνέπεια δεν μπορούν να διακρίνουν εάν πρόκειται για πραγματικό αποτύπωμα για να μπορέσει να ταυτοποιηθεί.

**Αναγνώριση προσώπου**

Ανέκαθεν τα χαρακτηριστικά του προσώπου ήταν κάτι που χρησιμοποιούσαν οι άνθρωποι για να αναγνωρίζουν και να θυμούνται ό ένας τον άλλο. Η μέθοδος της αναγνώρισης του προσώπου κατάφερε να προσομοιώσει τον τρόπο αυτό μέσα από την τεχνική της μοναδικότητας του κάθε ανθρώπου. Τα χαρακτηριστικά γνωρίσματα όπως το σχήμα των ματιών, το πηγούνι, το μέγεθος της μύτης και το στόμα υποδεικνύουν την ταυτότητα ενός ατόμου. Με τη χρήση μίας κάμερας εντοπίζονται τα κύρια σημεία του προσώπου και αποθηκεύονται σε μία μαγνητική κάρτα. Στην συνέχεια μέσω ενός λογισμικού, τα χαρακτηριστικά που λήφθηκαν από τη χαρτογράφηση της γεωγραφίας του ανθρωπίνου κρανίου και από τις γωνίες που έχει, μεταφράζονται σε ένα σετ ψηφιακών δεδομένων και στη συνέχεια διαμορφώνεται το ηλεκτρονικό αποτύπωμα του προσώπου. Κατά τη διαδικασία ταυτοποίησης συγκρίνονται σε πραγματικό χρόνο ένα προς ένα το πρόσωπο που έχει ληφθεί με τα πρόσωπα που είναι αποθηκευμένα στη Βάση Δεδομένων και έτσι επιβεβαιώνεται η ταυτότητά του [19].

Είδη σε ορισμένα ΑΤΜ άρχισε να εφαρμόζεται μία τέτοια μέθοδος ως ένα σύστημα πιστοποίησης. Το βασικό πλεονέκτημα αυτής της τεχνολογίας, είναι ότι το σύστημα μπορεί να κάνει καταγραφή των αποτυπωμάτων των προσώπων με διακριτικότητα χωρίς να γίνει αντιληπτό από το εν λόγω άτομο και να αρνηθεί την καταγραφή του.
Επιπρόσθετα, σε μεγάλες χώρες είναι πολύτιμη η ταυτοποίηση σε πραγματικό χρόνο ύποπτων ή ανεπιθύμητων ατόμων κυρίως σε αεροδρόμια, γήπεδα και σε άλλους τέτοιους αντίστοιχους χώρους όπου συγκεντρώνεται μεγάλη μερίδα ατόμων ούτος ώστε να μπορεί να γίνει ο εντοπισμός ανάμεσά τους [21]. Σε αντίθεση με άλλα βιομετρικά συστήματα, υπάρχουν ορισμένοι περιορισμοί όσον αφορά την ταυτοποίηση, όπως κάποιες μεταβολές του προσώπου (π.χ. μορφασμοί, αλλοίωση προσώπου μετά από ατύχημα). Ένας άλλος περιορισμός είναι ο φωτισμός απέναντι στην κάμερα όπου μπορεί να επιφέρει δυσκολία στην αναγνώριση.

**Γεωμετρία χεριού και παλάμης**

Η τεχνολογία της αυτοματοποιημένης μέτρησης της γεωμετρικής μορφής του χεριού για την επικύρωση της ταυτότητας αποτελεί άλλη μία προσέγγιση βιομετρικού συστήματος. Σε αυτή τη διαδικασία μετράμε το ύψος των δακτύλων, το σχήμα των αρθρώσεων και την απόσταση μεταξύ των κλειδώσεων του χεριού αφού πρώτα ο χρήστης τοποθετήσει την παλάμη του πάνω στην επιφάνεια του συστήματος [18]. Ευθυγραμμίζοντας το χέρι του στην κατάλληλη θέση όπως υποδεικνύεται στο σχεδιάγραμμα πάνω στη συσκευή, η κάμερα αρχίζει τις μετρήσεις για το πάχος, το πλάτος και το μήκος της επιφάνειας του χεριού στις διάφορες θέσεις. Οι μετρήσεις καθορίζουν το διάνυσμα χαρακτηριστικών γνωρισμάτων του χεριού και γίνεται ο υπολογισμός στις διάφορες θέσεις βάση της εικόνας που έχει ληφθεί.
Σε αντίθεση με άλλες τεχνολογίες, είναι πολύ πιο απλή διαδικασία και γίνεται αποδεκτή από τους χρήστες. Αν συμπεριλάβουμε τα άτομα μεγαλύτερης ηλικίας που πιθανώς να αντιμετωπίζουν αρθριτικά προβλήματα στα χέρια, θα μπορούν και αυτοί με την κατάλληλη εκπαίδευση να καταφέρουν να τοποθετήσουν το χέρι τους στη συσκευή.
Όπως και στα υπόλοιπα είδη βιομετρίας, η ακρίβεια και η αξιοπιστία των συστημάτων ενδέχεται να προκαλέσουν την απόρριψη του χρήστη εάν προκληθούν κακώσεις ή μεταβολές στα χέρια τους. Είναι αρκετά ανθεκτική στην απάτη παρόλο που δεν μπορεί να πραγματοποιήσει αναζητήσεις ένα-προς-πολλά, παραμένει εντούτοις αμετάβλητη λόγω του κόστους των σαρωτών.

Η σάρωση χεριού ενίοτε συγχέεται με την μέθοδο του συστήματος που έχει να κάνει με τη σάρωση του αποτυπώματος της παλάμης. Τα αποτυπώματα της παλάμης είναι μια εντελώς διαφορετική τεχνολογία. Σε αυτή τη μέθοδο γίνεται ανάλυση της υφής, των πτυχώσεων και της επιφάνειας της παλάμης.

**Αναγνώριση ίριδας και αμφιβληστροειδούς**

Το πιο ασφαλέστερο ίσως password είναι το μάτι, όπου η μοναδικότητα τις ίριδας και του αμφιβληστροειδούς χιτώνα μαζί με ορισμένες άλλες ιδιότητες τα καθιστούν ως τα πιο ακριβέστερα και ασφαλείς βιομετρικά συστήματα. Αυτό συμβαίνει διότι θεωρούνται μοναδικά ανατομικά στοιχεία του ανθρώπου ενώ παράλληλα αποτελούν μία μοναδική κα απαραβίαστη μέθοδο αναγνώρισης. Μάλιστα, η σάρωση του αμφιβληστροειδούς θεωρείται πιο ασφαλής μέθοδος έχοντας μηδενικές πιθανότητες σφάλματος και παραβίασης. Εντούτοις, απαιτείται από μεριάς του χρήστη μεγαλύτερη εμπλοκή στη διαδικασία και δυστυχώς θεωρείται πιο δύσχρηστη. Το μάτι και κυρίως το εσωτερικό του, είναι πολύ ευαίσθητο έχοντας ως αποτέλεσμα την αποτροπή των χρηστών στη διαδικασία της σάρωσης.

Κατά τη σάρωση του αμφιβληστροειδούς αδένα, ο χρήστης καλείτε να εστιάσει μπροστά από ένα προσοφθάλμιο ώστε ο σαρωτής να συλλέξει τα μοτίβα των αιμοφόρων αγγείων που βρίσκονται στο κέντρο του αμφιβληστροειδούς. Ακολούθως, το σύστημα συγκρίνει το βιομετρικό πρότυπο με την εικόνα που έχει μετατραπεί σε μαθηματική αναπαράσταση και ελέγχει στη Βάση Δεδομένων για την επιβεβαίωση του χρήστη.

Η εξέταση τη οπτικής αναγνώρισης παρουσιάζει πολλές ομοιότητες με την εξέταση της ίριδας. Όταν το άτομο πλησιάσει το φακό της οπτικής κάμερας αυτός εστιάζει στην περιοχή της ίριδάς του. Στη πορεία αφού εστιάσει στην ίριδα, ο φακός τραβάει μία φωτογραφία και μετατρέπει τα διακριτά μοτίβα σε μία ψηφιακή διάταξη αλγορίθμων. Η διαδικασία ολοκληρώνεται όταν ελεγχθεί από το σύστημα η εν λόγω διάταξη και βρεθεί καταχωρημένη στη βάση η ταυτότητα του χρήστη.

Σε σύγκριση με τις υπόλοιπες μεθόδους φυσικών χαρακτηριστικών, η σταθερότητα που παρουσιάζεται στο βιομετρικό δείγμα κάνει τις μεθόδους αυτές πιο ανθεκτικές σε τυχόν απάτες και μειώνει την πιθανότητα κάποιος χρήστης να γίνει αποδεκτός από το σύστημα χρησιμοποιώντας λανθασμένη ταυτότητα. Η ενδεχόμενη απάτη με τυχόν δημιουργία ενός ψεύτικου δείγματος αμφιβληστροειδούς θα ήταν χρονοβόρα και συνάμα δύσκολη διαδικασία. Σε αντίθεση με άλλες τεχνολογίες η σάρωση είναι περιορισμένη και βασίζεται σε συγκεκριμένους μηχανισμούς και πρωτόκολλα.

Οπόταν εάν κάποιοι εκμεταλλεύονταν το πλεονέκτημα μίας πιο αξιόπιστης κάμερας ή ενός ισχυρότερου σαρωτή, η λήψη του δείγματος δεν θα οδηγούσε στο επιθυμητό αποτέλεσμα. Μπορεί να έχει υψηλό κόστος όσον αφορά την εγκατάσταση των συστημάτων αυτών αλλά ήδη χρησιμοποιείται κυρίως σε αεροδρόμια, όπου αντί για τον έλεγχο των διαβατηρίων των επιβατών εξετάζεται η ίριδα των ματιών τους.

**Αγγειακά σχέδια**

Μία ακόμη μέθοδος που βασίζεται στην μελέτη των αιμοφόρων αγγείων είναι αυτή της αναγνώρισης της φλεβικής δομής. Αποτελεί αξιόπιστη διαδικασία μιας και οι φλέβες δεν είναι επιφανειακό χαρακτηριστικό και μπορούν να παράξουν μοναδικά μοτίβα για ταυτοποίηση. Στο πάνω μέρος της παλάμης η φλεβική δομή είναι εντονότερη και μπορεί να διαβαστεί μέσω υπέρυθρης ακτινοβολίας. Σε ορισμένες περιπτώσεις, οι χρήστες καλούνται να σφίξουν τη γροθιά τους κατά τη διάρκεια της μελέτης για να τονιστούν περισσότερο οι φλέβες τους. Η πρακτική εφαρμογή μπορεί να μην έχει ακόμη τεθεί σε ισχύ σε πολλά συστήματα, δεν παύει όμως να αποτελεί μία αξιόπιστη διαδικασία που σύντομα θα εφαρμοστεί σε μελλοντικά συστήματα.

**Ανάλυση αυτιού**

Η ανάλυση της γεωμετρίας του αυτιού ως μέσω αναγνώρισης έχει όλες τις ικανότητες ενός βιομετρικού γνωρίσματος και λειτουργεί παρόμοια με την μέθοδο αναγνώρισης του προσώπου και των χεριών. Μπορεί να θεωρείται ως μία ασυνήθιστη μέθοδος όμως είναι αξιόπιστη καθώς τα μοτίβα του εξωτερικού αυτιού είναι μοναδικά για κάθε άτομο. Δεν είναι ευρέως διαδομένη μέθοδος, παρόλα αυτά εφαρμόζεται σε αστυνομικές υποθέσεις ως μέσο αναγνώρισης.

**Ανάλυση DNA**

Η ανάλυση γενετικού υλικού δεν μπορεί να χαρακτηριστεί εξ ολοκλήρου ως βιομετρική μέθοδος γιατί απαιτεί κάποιο χειροπιαστό φυσικό δείγμα που θα μπορεί να αναλυθεί αυτόματα. Παρόλο που το DNA παραμένει αναλλοίωτο καθ' όλη την διάρκεια ζωής ενός ατόμου και αποτελεί την πιο ακριβής μορφή ταυτοποίησης, δεν παύει να είναι μία χρονοβόρα μορφή αναγνώρισης επειδή δεν μπορεί να μελετηθεί σε πραγματικό χρόνο.
Η συλλογή του δείγματος γίνεται κυρίως μέσω σάλιου ή μέσω ιστού από τα προσωπικά αντικείμενα. Στη συνέχεια το δείγμα αναλύεται για να παραχθεί το προφίλ του DNA που χρησιμοποιείται ως φυσικό χαρακτηριστικό για την επαλήθευση [19].

### 4.4.2 Συμπεριφορικά Βιομετρικά

Τα συμπεριφορικά χαρακτηριστικά βασίζονται σε δεδομένα και μετρήσεις που προέρχονται από τη δράση των ανθρωπίνων χαρακτηριστικών. Πιο κάτω αναλύονται τα εξής:

**Αναγνώριση της φωνής**

Η αναγνώριση φωνής έχει να κάνει με το άτομο που μιλάει και η σάρωση γίνεται με τη χρήση φωνητικών χαρακτηριστικών του. Για τη λήψη των μετρήσεων φωνητικού δείγματος δεν είναι απαραίτητο ο ομιλητής να βρίσκεται μπροστά από κάποια συσκευή. Απεναντίας, υπάρχει η δυνατότητα να είναι πολύ πιο μακριά και διαμέσου του τηλεφώνου ή ενός μικροφώνου να γίνει η εξ αποστάσεως πιστοποίηση. Τα συστήματα μπορούν να αναγνωρίσουν συνήθως επαναλαμβανόμενες φράσεις ή συνδυασμούς λέξεων ή αριθμών και η διάρκεια τους πρέπει να είναι μεταξύ των τριών δευτερολέπτων. Οι μετρήσεις σε διάφορους χρόνους χτίζουν το προφίλ της φωνής διαμέσου ενός κατάλληλου λογισμικού και το συγκρίνει με τα είδη προηγούμενα καταγραμμένα δείγματα. Οι συσκευές προσπαθούν να εστιάζουν σε διαφορετικά χαρακτηριστικά της ομιλίας διότι ένας εξωγενείς παράγοντας όπως είναι ο θόρυβος, ενδεχομένως να επηρεάσει την ακρίβεια αναγνώρισης.

**Αναγνώριση της υπογραφής**

Η υπογραφή είναι ενδεχομένως το πιο αναγνωρισμένο χαρακτηριστικό του καθενός για την επαλήθευση της ταυτότητάς μας. Η σάρωση της υπογραφής μετρά τον τρόπο που ένας χρήστης μπορεί να γράψει το όνομα του, μία φράση ή ένα συνθηματικό και βάση της συμπεριφοράς του κατά τη διαδικασία της υπογραφής, μπορεί να εξακριβωθεί η ταυτότητά του. Είναι βασισμένη στο μοτίβο της υπογραφής, στο πώς δηλαδή ο χρήστης κρατά το στυλό και πώς το πιέζει επάνω στο χαρτί η στην επιφάνεια που παίρνεται το δείγμα. Παράλληλα, λαμβάνεται υπόψη ο χρόνος και η επιτάχυνση που απαιτείται για την ολοκλήρωση της υπογραφής όπου και αναλύονται οι διαστάσεις σε τρεις άξονες. Οι θέσεις αυτές χρησιμοποιούνται για να υποδείξουν τις εναλλαγές στην ταχύτητα ως προς το χρόνο σε μορφή μαθηματικού κώδικα ώστε να χαρακτηρίσει το συγκεκριμένο χρήστη.

**Ανάλυση της πληκτρολόγησης**

Η μέθοδος της ανάλυσης πληκτρολόγησης εξετάζει το ρυθμό και τον τρόπο που ένας χρήστης δακτυλογραφεί στο πληκτρολόγιο. Στην περίπτωση που ένας επιτιθέμενος μαντέψει το συνθηματικό για την πρόσβαση σε ένα σύστημα, σίγουρα δεν θα είναι σε θέση να πληκτρολογεί με τον ίδιο ρυθμό του πραγματικού χρήστη. Όπως εξυπονοεί, η μέθοδος αναλύει τη δύναμη με την οποία πατάει τα πλήκτρα ο χρήστης, την ταχύτητα και το συνολικό χρόνο πληκτρολόγησης. Είναι επίσης ουσιαστικός ο χρόνος που μεσολαβεί μεταξύ του πατήματος ενός συγκεκριμένου πλήκτρου έως το πάτημα ενός άλλου πλήκτρου.

Τα συστήματα ανίχνευσης διαθέτουν μία Βάση Δεδομένων όπου είναι καταχωρημένα για κάθε άτομο όλα τα στοιχεία από την δακτυλογράφησή του. Έτσι όταν ο χρήστης πληκτρολογήσει για παράδειγμα τον κωδικό του για να εισέλθει στο σύστημα, συγκρίνονται τα στοιχεία που είναι αποθηκευμένα στη βάση με αυτά που προέκυψαν από την συγκεκριμένη πληκτρολόγηση και τότε μπορεί να αποκτήσει την αντίστοιχη πρόσβαση. Η κυριότερη ίσως δυσκολία της μεθόδου αυτής, είναι το γεγονός πως η συμπεριφορά του χρήστη κατά τη διάρκεια της ημέρας ενδεχομένως να εναλλάσσεται με αποτέλεσμα να διαφέρει και ο ρυθμός πληκτρολόγησης.

## 4.5 Αποδοχή των Βιομετρικών Μεθόδων από τους Χρήστες

Η ιδιαιτερότητα των βιομετρικών συστημάτων όσο αφορά την ανάγκη εισαγωγής ενός σωματικού αναγνωριστικού από τους χρήστες διεγείρει ανησυχία και αντιδράσεις. Η φύση του ανθρώπου είναι τέτοια που δεν του επιτρέπει να εμπιστευτεί μία νέα τεχνολογία που δεν έχει εξοικειωθεί. Με το άκουσμα βιομετρικών συστημάτων και τεχνολογιών είναι εύλογο να μην μπορεί να αντιληφθεί την έννοια αυτή, πόσο μάλλον να την εφαρμόσει στην καθημερινότητά του. Επιπλέον, υπάρχουν χρήστες που ενδεχομένως να λένε πως ένα σύστημα που δεν εφαρμόζει βιομετρικές μεθόδους είναι και λιγότερο επιρρεπείς σε εισβολείς. Για να καταστεί επομένως κατορθωτή η αποδοχή των βιομετρικών συστημάτων θα πρέπει να πειστούν πως δεν πρόκειται να απειληθούν τα βιομετρικά τους στοιχεία [20].

### 4.5.1 Παράγοντες για την αποδοχή των χρηστών

Οι εφαρμογές των βιομετρικών μεθόδων ολοένα και πληθαίνουν οπόταν η επίτευξη της αποδοχής τους από τους χρήστες τείνει να καταστεί μονόδρομος. Για να καταφέρουν να συμβαδίσουν με τη βιομετρική τεχνολογία, οι χρήστες καλούνται να συνεργαστούν και να είναι πρόθυμοι να αποδεχθούν τη χρήση και την εφαρμογή των βιομετρικών αναγνωριστικών [17].

Η εμπιστοσύνη θα πρέπει να κερδηθεί από τους εξής παράγοντες:

- Το αίσθημα ότι τα συστήματα κρατούν ασφαλή και κάτω από άκρα μυστικότητα τα δεδομένα τους και πως δεν πρόκειται χρησιμοποιούνται για οποιοδήποτε άλλο σκοπό πέραν από την ταυτοποίησή τους.
- Τα νέα βιομετρικά συστήματα συγκρίνονται με τα ευρέως χρησιμοποιούμενα συστήματα και η αξιολόγηση τους, κατά πόσο είναι καταλληλότερα προς χρήση.
- Η ανάγκη αυξημένης προστασίας των δεδομένων των χρηστών μπορεί να ενισχύσει την ασφάλεια των βιομετρικών συστημάτων.
- Ο χρόνος αναμονής κατά τη διαδικασία αναγνώρισης.

### 4.5.2 Παράγοντες που καθιστούν μη αποδεκτές τις βιομετρικές μεθόδους από τους χρήστες

Μεγάλη μερίδα χρηστών θέτει το ερώτημα σε τι διαφέρουν τα βιομετρικά συστήματα από τα ευρέως χρησιμοποιούμενα. Αυτό που θα πρέπει να έχουν υπόψιν, είναι πως τα βιομετρικά έχουν σκοπό την αναγνώριση αλλά χρησιμοποιούν διαφορετικά μέσα και πιο συγκεκριμένα τα ανθρώπινα χαρακτηριστικά. Οι βασικότεροι παράγοντες που απασχολούν και επηρεάζουν τους χρήστες ώστε να μην αποδέχονται τις μεθόδους είναι οι εξής:

- Οι χρήστες ανησυχούν εάν μακροπρόθεσμα η ασφάλεια τους θα γίνεται έρμαιο των εγκληματιών διότι θεωρούν πως θα τους «κόψουν το δάκτυλο» για να έχουν πρόσβαση στο σύστημα με τα δικά τους διαπιστευτήρια.
- Αρκετοί είναι οι χρήστες που πιστεύουν πως η χρήση των βιομετρικών τους χαρακτηριστικών θα επιφέρει ζημιά στα μάτια ή στα δάκτυλά τους.
- Η παραβίαση της ιδιωτικότητας γεννάει το ερώτημα κατά πόσο είναι ασφαλές να έχουν τα συστήματα στις Βάσεις Δεδομένων τους τα στοιχεία τους και πως δεν θα χρησιμοποιηθούν για οποιαδήποτε άλλο σκοπό πέραν από αυτό της ταυτοποίησή τους.

- Ο κίνδυνος παραβίασης του συστήματος από μία μη εξουσιοδοτημένη οντότητα και η απόρριψη πρόσβασης ενός νόμιμου δικαιούχου ανησυχεί τους χρήστες κατά πόσο είναι αξιόπιστη η διαδικασία αναγνώρισης.

### 4.5.3 Επιδράσεις στην αποδοχή των χρηστών

Η αποδοχή από τους χρήστες επηρεάζεται από μία γκάμα ζητημάτων όπως το κόστος, την εκπαίδευση που ενδεχομένως να χρειαστεί, τις νέες τεχνολογικές απαιτήσεις για τις μονάδες διαφύλαξης των δεδομένων αλλά και το τι μπορεί να επέλθει από τη χρήση της βιομετρικής τεχνολογίας. Έχοντας ως δεδομένο ότι οι χρήστες καλούνται να παρουσιάσουν ως αποδεικτικά κάποια μέρη του σώματός τους, προκαλεί ανησυχίες για το που αποθηκεύονται και ποιοι έχουν πρόσβαση στις Βάσεις Δεδομένων που βρίσκονται οι ψηφιοποιημένες εικόνες με τα βιομετρικά δείγματά τους.

Στην περίπτωση που τα δείγματα αποθηκεύονται σε εξωτερικές Βάσεις Δεδομένων και καλείται το σύστημα να εξετάσει την ταυτότητα του χρήστη, οι πληροφορίες στέλνονται εκτός του τοπικού δικτύου. Παρόλο που κρυπτογραφούνται τα δείγματα με όλες τις πληροφορίες που απαιτούνται, παραμονεύει ο κίνδυνος της κλοπής από εισβολείς και η ενδεχόμενη τροποποίηση ή χρήση αυτών με ψευδή και παράνομο τρόπο.

Ένας ακόμη προβληματισμός, έχει να κάνει με το πόσος χρόνος απαιτείται από το σύστημα για την αναγνώριση και την επαλήθευση των στοιχείων του χρήστη. Για να γίνει ο απαραίτητος έλεγχος στη βάση, το σύστημα ψάχνει όλα τα αποθηκευμένα δεδομένα και δημιουργεί σημαντικές καθυστερήσεις.

Εξάλλου, υπάρχουν περιπτώσεις που τα βιομετρικά δεδομένα αποθηκεύονται σε κινητές μονάδες όπως για παράδειγμα σε μία έξυπνη κάρτα για να έχει ο χρήστης τη δυνατότητα του ελέγχου των στοιχείων του. Οι χρήστες όταν θα θέλουν να συνδεθούν στην κινητή μονάδα για να διεκπεραιώσουν μία τραπεζική συναλλαγή, θα πρέπει να δώσουν την ψηφιακή τους υπογραφή ώστε να γίνει η επαλήθευση για να τους δοθεί πρόσβαση στις ασφαλείς υπηρεσίες.

Ένα άλλο πολύ σημαντικό στοιχείο που προκύπτει, είναι το ζήτημα της εκπαίδευσης πάνω στη χρήση των βιομετρικών συστημάτων για να μην παρατηρούνται άσκοπες καθυστερήσεις ή απορρίψεις από μεριάς των συστημάτων. Σίγουρα μία νέα βιομετρική μέθοδος θα πρέπει να συνοδεύεται από τα κατάλληλα εγχειρίδια που να είναι εύκολο προς το χρήστη να κατανοήσει την λειτουργία τους και να μην τον αποθαρρύνει από την προσπάθειά του να μάθει τη νέα αυτή μέθοδο.

Εάν δεν καταφέρει να έχει την απαραίτητη προσέλκυση, ο χρήστης πιθανότατα να παρατήσει τις προσπάθειες εκμάθησης και θα πιστεύει πως οι μέθοδοι δεν είναι οι αρμόζουσες γι' αυτόν. Συνήθως οι χρήστες που είναι πρόθυμοι στο να κάνουν χρήση μίας νέας μεθόδου και ενδιαφέρονται να την μάθουν, είναι αυτοί που χαρακτηρίζονται ως πιο «προχωρημένοι» και μπορούν να διαχειριστούν μία νέα εφαρμογή.
Αξιοσημείωτο είναι βέβαια το κόστος μίας εφαρμογής βιομετρικής τεχνολογίας, το οποίο δεν μπορεί να αγνοηθεί ως μία επίδραση στην αποδοχή του χρήστη. Δεν προχωρούν εύκολα στην απόφαση να πληρώσουν για μία νέα τεχνολογία εάν δεν είναι απολύτως σίγουροι ότι θα τους είναι χρήσιμη, κυρίως στις μέρες μας που διανύουμε μία περίοδο παγκόσμιας οικονομικής ύφεσης.

## 4.6 Είδη Σφαλμάτων Βιομετρικών Συστημάτων

Για να καθοριστεί η αποδοτικότητα και η ποιότητα των βιομετρικών συστημάτων έχουν οριστεί ορισμένα μέτρα που αφορούν τα είδη σφαλμάτων. Η σύγκριση των βιομετρικών χαρακτηριστικών κατά τη διαδικασία καταμέτρησης των στατιστικών σφαλμάτων καθορίζεται από τα όρια της εφαρμογής των βιομετρικών συστημάτων και από το πώς καταφέρνουν το διαχωρισμό των ατόμων αναλόγως των χαρακτηριστικών τους [21].
Τα είδη των μέτρων που έχουν οριστεί ως μετρητές της απόδοσης είναι τα εξής:

- **Δείκτης Λανθασμένης Αποδοχής- False Acceptance Rate (FAR)**

Ο δείκτης FAR μετρά το ποσοστό συχνότητας αποδοχής μη έγκυρων χρηστών σε ένα σύστημα ελέγχου ταυτότητας. Μετρά δηλαδή, το πόσο συχνά ένας χρήστης αναγνωρίζεται λανθασμένα από το σύστημα ωσάν να ήταν ο νόμιμος χρήστης. Υπάρχει ενδεχόμενο να συμβεί μία τέτοια περίπτωση κυρίως σε συστήματα που χρησιμοποιούν βιομετρικά στοιχεία συμπεριφοράς.

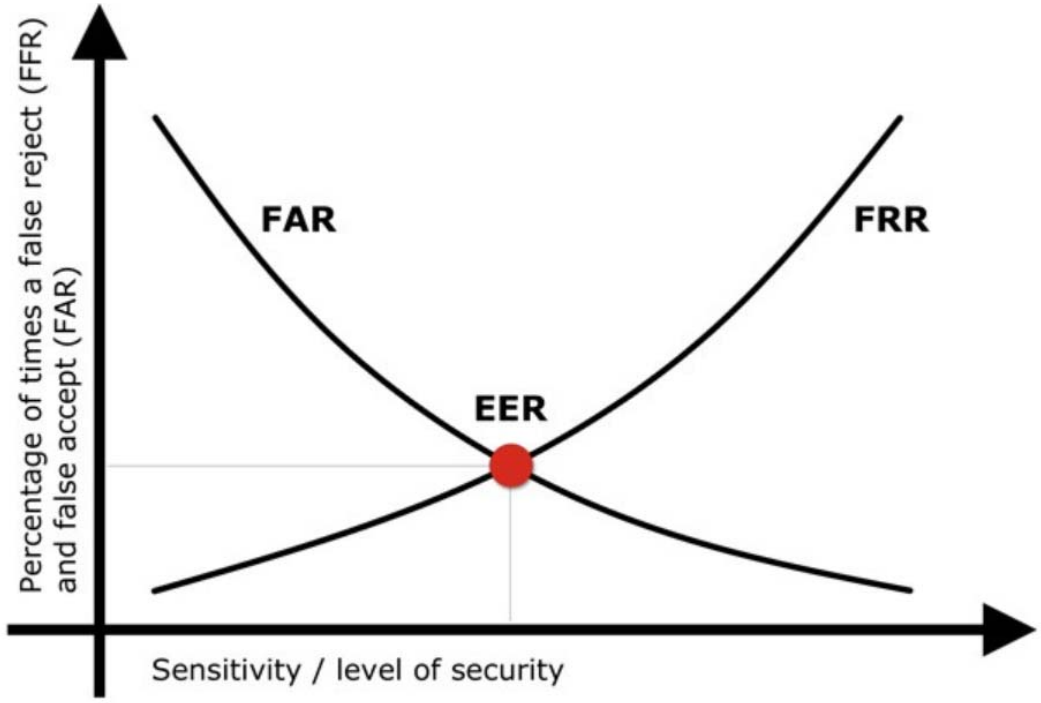
- **Δείκτης Λανθασμένης Απόρριψης - False Rejection Rate (FRR)**

Ο δείκτης FRR μετρά το ποσοστό συχνότητας μη αποδοχής έγκυρων χρηστών σε ένα σύστημα ελέγχου ταυτότητας. Μετρά πόσο συχνά ένας νόμιμος χρήστης δοκιμάζει τον έλεγχο ταυτότητας και δεν του παρέχεται η εξουσιοδοτημένη πρόσβαση.

- **Δείκτης Ίσου Σφάλματος - Equal Error Rate (EER)**

Ο δείκτης EER έχει την ιδιότητα να προκαθορίζει το όριο των αποδεκτών τιμών για το ποσοστό συχνότητας αποδοχής και το ποσοστό συχνότητας μη αποδοχής έγκυρων χρηστών από ένα σύστημα ελέγχου ταυτότητας. Είναι ουσιαστικά το σημείο τομής FAR και FRR.

Στο παρακάτω σχήμα έχουμε σε μορφή γραφήματος τις σχέσεις μεταξύ των τριών δεικτών σε σχέση με την τιμή τους και το όριο σφάλματος. Όπως αναφέρθηκε και φαίνεται στην τομή στο σχήμα, όταν οι τιμές των δεικτών είναι ισότιμες τότε η κοινή τιμή τους αναφέρεται ως ο δείκτης ισοδύναμου ποσοστού σφάλματος [22].




**Διάγραμμα 4.1:** FAR,FRR και EER σε σχέση με επίπεδο ασφάλειας[13]

# Κεφάλαιο 5
# Ερευνητική Διαδικασία

## 5.1 Σκοπός της Έρευνας

Στην παρούσα ερευνητική μελέτη γίνεται μία προσπάθεια ώστε να παρθούν σημαντικά συμπεράσματα σχετικά με το αν οι χρήστες αποδέχονται τη χρήση βιομετρικών μεθόδων στο online banking για περισσότερη ασφάλεια στις συναλλαγές τους. Όπως αναφέρθηκε, υπάρχουν αρκετοί λόγοι που τα βιομετρικά συστήματα δεν είναι απολύτως αποδεκτά. Οπόταν τα συμπεράσματα θα δείξουν κατά πόσο η κατανόηση της ασφάλειας των βιομετρικών μεθόδων από τους χρήστες μπορεί να επηρεάσει θετικά τη στάση τους και την αποδοχή τους για τη χρήση βιομετρικού συστήματος ελέγχου ταυτότητας.
Θα γίνει ανάλυση των ζητημάτων που προκύπτουν από τη χρήση βιομετρικών μεθόδων καθώς και οι προβληματισμοί που αποτυπώνονται από τους χρήστες σχετικά με την προστασία τους.

## 5.2 Μεθοδολογία

Στην παρούσα μελέτη, έχει επιλεγεί η διεξαγωγή δειγματοληπτικής έρευνας μια και θεωρείται ο καταλληλότερος σχεδιασμός ποσοτικής έρευνας. Για την απάντηση των ερευνητικών ερωτημάτων σχεδιάστηκε ηλεκτρονική έρευνα μέσω ερωτηματολογίων (online survey). Χρησιμοποιήθηκε ένα μέρος – δείγμα του πληθυσμού ώστε να εξοικονομηθεί κυρίως χρόνος μιας και οι μετρήσεις σε ολόκληρο τον πληθυσμό ήταν αδύνατο να γίνουν. Στην συγκεκριμένη περίπτωση, επιλέχθηκε ένα δείγμα πέραν των 100 ατόμων το οποίο είναι αντιπροσωπευτικό και συνάμα αξιόπιστο επειδή εκφράζει τις διαφοροποιήσεις του πληθυσμού βάσει του σκοπού της μελέτης [24].
Η δειγματοληψία για τη συλλογή ποσοτικών δεδομένων έγινε μέσω ηλεκτρονικών ερωτηματολογίων. Το ερωτηματολόγιο, αποτελεί ίσως την πιο διαδεδομένη ερευνητική μέθοδο κλειστού τύπου για τη συλλογή ποσοτικών δεδομένων [35].

Οι συμμετέχοντες έχουν τη δυνατότητα να απαντήσουν πολύ πιο γρήγορα στο ερωτηματολόγιο καθώς δεν έχουν χρονικό περιορισμό. Λόγω της ανωνυμίας του δείγματος οι απαντήσεις που λαμβάνονται είναι πιο ειλικρινείς και αυθόρμητες ώστε να διασφαλιστεί η εγκυρότητα των αποτελεσμάτων.

Το online ερωτηματολόγιο χωρίστηκε σε τρία κύρια μέρη. Το πρώτο μέρος αναφέρεται σε γενικές πληροφορίες, το δεύτερο αφορά την γνώση-αντίληψη των χρηστών για τις βιομετρικές μεθόδους και το τρίτο επικεντρώνεται στην αντίληψη των χρηστών για τη χρήση των βιομετρικών μεθόδων όσον αφορά την ασφάλεια και την ιδιωτικότητά τους.

## 5.3 Ερωτηματολόγιο

Έχει επιλεγεί το ερωτηματολόγιο ως ερευνητική μέθοδος λόγω του ότι η συλλογή των πληροφοριών παρέχει ευκολότερη ανάλυση σε σύγκριση με άλλες μεθόδους. Επιλέχθηκε η δημιουργία ηλεκτρονικού ερωτηματολογίου μέσω της δωρεάν πλατφόρμας «Google Forms» για τη συλλογή των ανώνυμων δεδομένων ούτος ώστε να είναι πιο άμεση η διανομή τους μέσω ηλεκτρονικού ταχυδρομείου ή άλλων κοινωνικών μέσω δικτύωσης. Η συγκεκριμένη πλατφόρμα δίνει τη δυνατότητα σχεδιασμού ερωτηματολογίων για πιο άμεση συλλογή των απαντήσεων, ενώ δίνεται η ευχέρεια για άμεση εξαγωγή των αποτελεσμάτων σε υπολογιστικό φύλλο MS excel.

Το ερωτηματολόγιο αποτελείται από 21 κλειστού τύπου ερωτήσεις. Η δομή του χτίστηκε με τέτοιο τρόπο ώστε να μην αποθαρρύνει τον ερωτηθέντα. Αρχικά παρουσιάστηκαν πιο απλές ερωτήσεις, ενώ στη μέση τοποθετήθηκαν οι πιο καθοριστικές και σημαντικές ερωτήσεις.

Χρησιμοποιήθηκαν οι παρακάτω τύποι ερωτήσεων :

- Ερωτήσεις μίας επιλογής (ερωτήσεις: 1-11, 14,17,18,19,21)
- Ερωτήσεις πολλαπλών επιλογών (ερωτήσεις: 12,15,16,20)
- Ερωτήσεις κλίμακας (ερωτήσεις: 13,19)

Οι ερωτήσεις κλίμακας έγιναν με τη μέθοδο Likert όπου στα άκρα της κλίμακας είχαμε τους αριθμούς 1 και 5 ενώ στο ενδιάμεσο είχαμε μία ουδέτερη στάση. Στη δική μας περίπτωση που το δείγμα ρωτήθηκε πόσο συμφωνούν με τις μεθόδους ταυτοποίησης, ο αριθμός 1 αντιστοιχούσε στο διαφωνώ απόλυτα ενώ το 5 στο συμφωνώ απόλυτα και στο ενδιάμεσο της κλίμακας είχαμε μία ουδέτερη στάση.

Η έρευνα πραγματοποιήθηκε στην Κύπρο σε διάστημα δύο εβδομάδων τον Ιανουάριο του 2020 και ο υπολογιζόμενος χρόνος για να απαντηθεί ήταν περίπου 10 λεπτά. Πάρθηκαν 106 πλήρης απαντήσεις αφού όλοι όσοι πήραν μέρος στην έρευνα είχαν συμφωνήσει με τους προκαθορισμένους όρους που είχαν τεθεί. Η μέθοδος αυτή διευκόλυνε κατά πολύ τη στατιστική μελέτη και συνάμα την εξαγωγή ρεαλιστικών συμπερασμάτων. Τα άτομα που χρησιμοποιήθηκαν ως δείγμα στην παρούσα μελέτη ήταν άνδρες και γυναίκες άνω των 18 ετών, οι πλείστοι υψηλού μορφωτικού επιπέδου από διάφορες επαγγελματικές καταστάσεις.

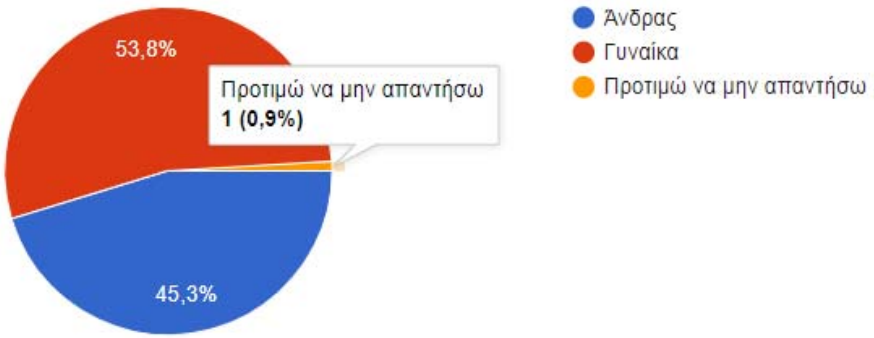
Στην εισαγωγή του ερωτηματολογίου υπάρχει μία εισαγωγική παράγραφος στην οποία παρουσιάζεται ο σκοπός της έρευνας, οι όροι που καλούνται να συμφωνήσουν και σε ποια πλαίσια διεξάγεται (Παράρτημα Α).

# Κεφάλαιο 6
# Συγκέντρωση, Ανάλυση και Ερμηνεία Δεδομένων

## 6.1 Απαντήσεις Ερωτηματολογίου

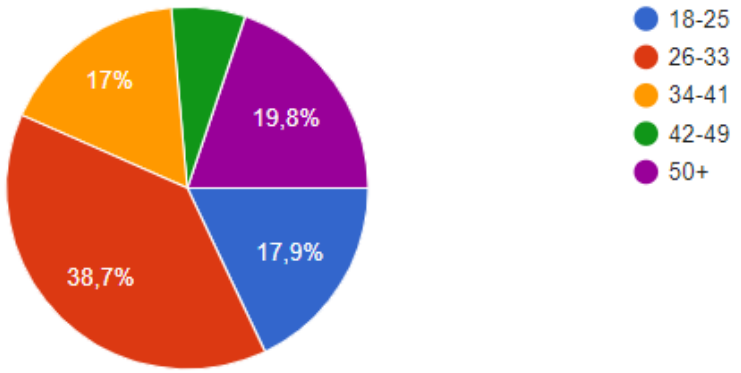
Παρακάτω παρουσιάζονται οι απαντήσεις μαζί με το σχετικό διάγραμμα για κάθε μία από τις ερωτήσεις.

**Ερώτηση 1:** Στο δείγμα των 106 ερωτηθέντων οι 57 απαντήσεις δόθηκαν από γυναίκες σε ποσοστό 53,8%, οι 48 δόθηκαν από άνδρες σε ποσοστό 45,3% και 1 από αυτές απαντήθηκε χωρίς προσδιορισμό του φύλου με ποσοστό 0.9%.



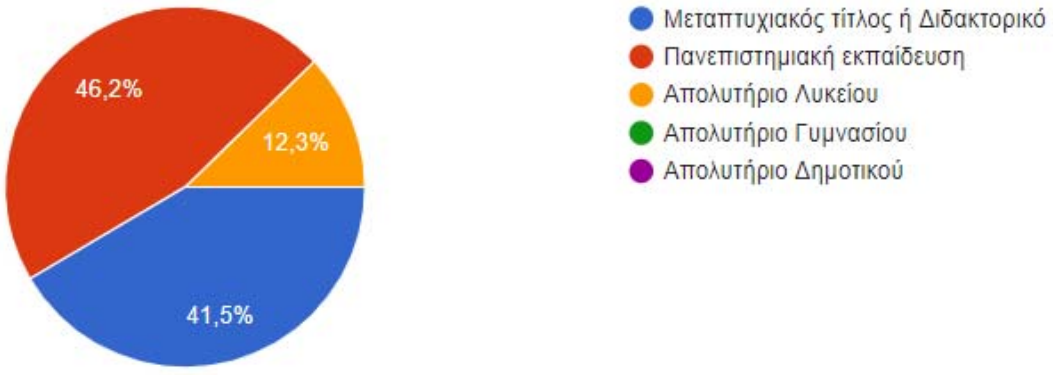

**Διάγραμμα 6.1:** Ποσοστό συμμετοχής κατά φύλο

**Ερώτηση 2:** Στο δείγμα των 106 ερωτηθέντων 19 άτομα ήταν ηλικίας 18-25 ετών σε ποσοστό 17,9%, 41 άτομα ήταν ηλικίας 26-33 ετών σε ποσοστό 38,7%, 18 άτομα ήταν ηλικίας 34-41 ετών σε ποσοστό 17,%, 7 άτομα ήταν ηλικίας 42-49 ετών σε ποσοστό 6,6% και οι υπόλοιποι 21 ήταν πάνω από 50 ετών σε ποσοστό 19,8%.



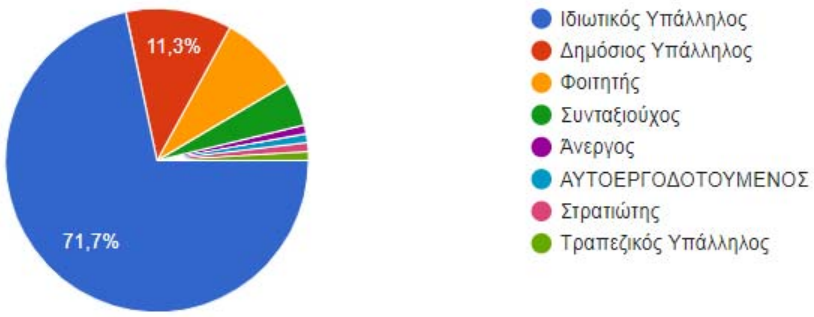

**Διάγραμμα 6.2:** Ποσοστό συμμετοχής κατά ηλικία

**Ερώτηση 3:** Στο δείγμα 106 ερωτηθέντων σχετικά με το επίπεδο εκπαίδευσης οι 44 ήταν κάτοχοι μεταπτυχιακού ή διδακτορικού τίτλου σε ποσοστό 41,5%, οι 49 είχαν πανεπιστημιακή εκπαίδευση σε ποσοστό 46,2% και οι υπόλοιποι 13 ήταν άτομα που κατείχαν απολυτήριο λυκείου σε ποσοστό 12,3%.



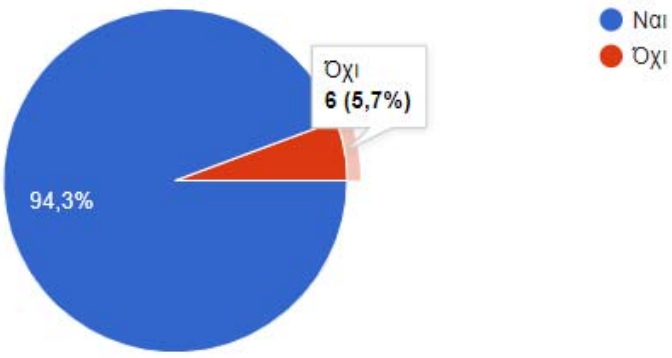

**Διάγραμμα 6.3:** Ποσοστό συμμετοχής κατά επίπεδο εκπαίδευσης

**Ερώτηση 4:** Στο δείγμα 106 ερωτηθέντων σχετικά με το επάγγελμά τους οι 76 ήταν ιδιωτικοί υπάλληλοι σε ποσοστό 71,7%, οι 12 ήταν δημόσιοι υπάλληλοι σε ποσοστό 11,3%, 9 ήταν φοιτητές σε ποσοστό 8,5%, 5 ήταν συνταξιούχοι σε ποσοστό 4,7%, 1 άτομο ήταν άνεργος, 1 άτομο αυτοεργοδοτούμενος, 1 ήταν στρατιώτης και 1 άτομο ήταν τραπεζικός υπάλληλος σε ποσοστά 0,9% έκαστος.



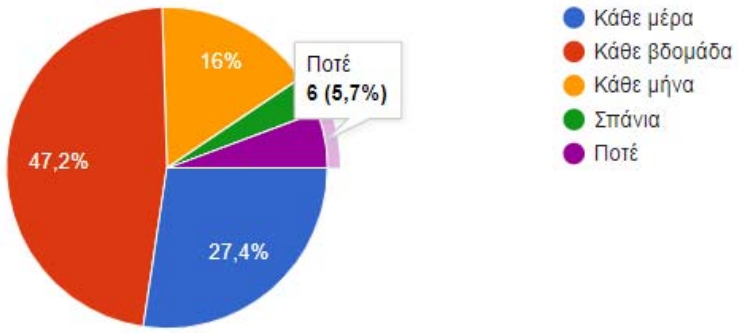

**Διάγραμμα 4.1:** Ποσοστό συμμετοχής βάση επαγγέλματος

**Ερώτηση 5:** Στην ερώτηση κατά πόσο χρησιμοποιούν οι ερωτηθέντες υπηρεσίες του online banking οι 100 απάντησαν Ναι σε ποσοστό 94,3% και οι υπόλοιποι 6 απάντησαν Όχι σε ποσοστό 5,7%.



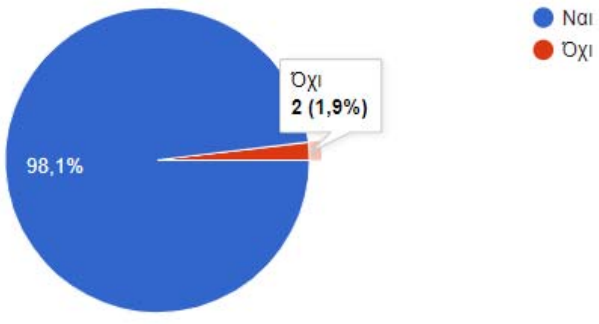

**Διάγραμμα 5.5:** Ποσοστό χρήσης online banking υπηρεσιών

**Ερώτηση 6:** Στην ερώτηση πόσο συχνά οι ερωτηθέντες χρησιμοποιούν το online banking 29 άτομα απάντησαν ότι κάνουν χρήση κάθε μέρα σε ποσοστό 27,4%, 50 άτομα απάντησαν κάθε βδομάδα σε ποσοστό 47,2%, 17 άτομα απάντησαν κάθε μήνα σε ποσοστό 16%, 4 άτομα απάντησαν σπάνια σε ποσοστό 3,8% και οι υπόλοιποι 6 απάντησαν ότι δεν κάνουν ποτέ χρήση σε ποσοστό 5,7%.



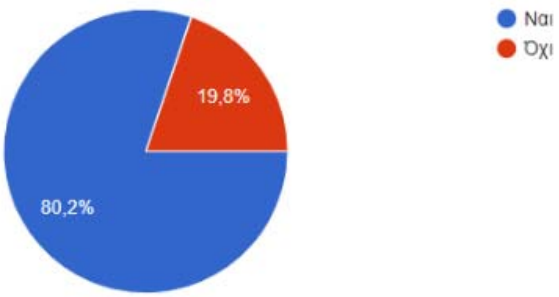

**Διάγραμμα 6.6:** Ποσοστό συχνότητας χρήσης online banking

**Ερώτηση 7:** Στην ερώτηση εάν παρέχει η τράπεζα σας ασφαλείς μεθόδους online banking 104 άτομα απάντησαν Ναι σε ποσοστό 98,1% και 2 άτομα απάντησαν Όχι σε ποσοστό 1.9%.




**Διάγραμμα 6.7:** Ποσοστό ασφαλών μεθόδων online banking από την τράπεζα

**Ερώτηση 8:** Στην ερώτηση εάν οι ερωτηθέντες πιστεύουν ότι το online banking είναι ασφαλές 85 απάντησαν Ναι σε ποσοστό 80,2% και οι υπόλοιποι 21 απάντησαν Όχι σε ποσοστό 19,8%.

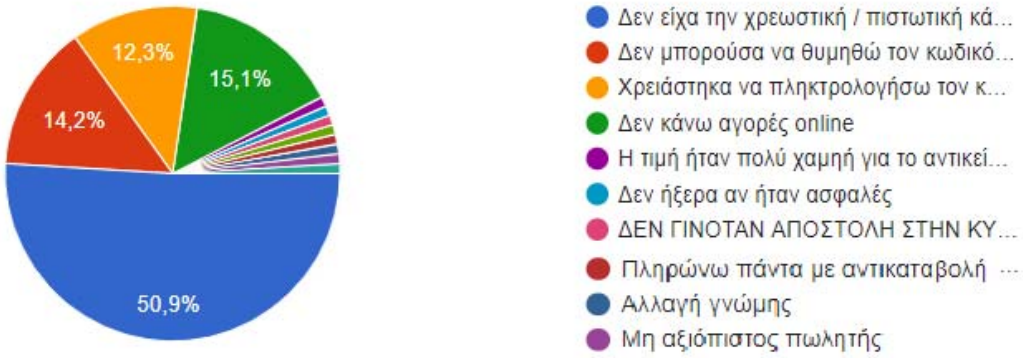



**Διάγραμμα 6.8:** Ποσοστό ασφάλειας online banking

**Ερώτηση 9:** Στην ερώτηση αν γίνεται χρήση ξεχωριστών κωδικών για κάθε τραπεζικό λογαριασμό 43 από τους ερωτηθέντες απάντησαν ότι χρησιμοποιούν έναν μοναδικό κωδικό πρόσβασης/PIN για κάθε λογαριασμό σε ποσοστό 40,6%, 23 απάντησαν ότι χρησιμοποιούν πολλούς κωδικούς πρόσβασης /PIN αλλά δεν είναι μοναδικοί για κάθε λογαριασμό σε ποσοστό 21,7%, 15 απάντησαν ότι χρησιμοποιούν τον ίδιο κωδικό πρόσβασης /PIN για όλους τους λογαριασμούς τους και οι υπόλοιποι 25 ερωτηθέντες απάντησαν πως έχουν μόνο μία χρεωστική ή πιστωτική κάρτα σε ποσοστό 23,6%.

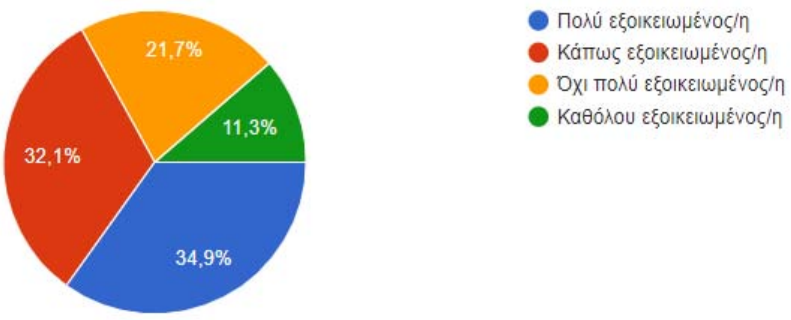

**Διάγραμμα 6.9:** Ποσοστό χρήσης μοναδικών κωδικών πρόσβασης/PIN για κάθε λογαριασμό

**Ερώτηση 10:** Στην ερώτηση ποιος ήταν ο λόγος που είχαν εγκαταλείψει οι ερωτηθέντες κάποια online αγορά οι 54 απάντησαν ότι δεν είχαν μαζί τους την χρεωστική/ πιστωτική τους κάρτα σε ποσοστό 50,9%, 15 απάντησαν πως δεν μπορούσαν να θυμηθούν τον κωδικό τους σε ποσοστό 14,2%, 13 απάντησαν πως χρειάστηκαν να πληκτρολογήσουν τον κωδικό τους σε ποσοστό 12,3%, 16 απάντησαν ότι δεν κάνουν online αγορές σε ποσοστό 15,1%, και οι υπόλοιπες 8 απαντήσεις με ποσοστό 0,9% έκαστος ήταν λόγο άλλων παραγόντων (π.χ. η τιμή του αντικειμένου ήταν πολύ χαμηλή και μπορεί να ήταν κάποιας μορφής απάτη, δεν ήξεραν αν είναι ασφαλές, δεν γινόταν αποστολή του αντικειμένου, αλλαγή γνώμης, μη αξιόπιστος πωλητής).



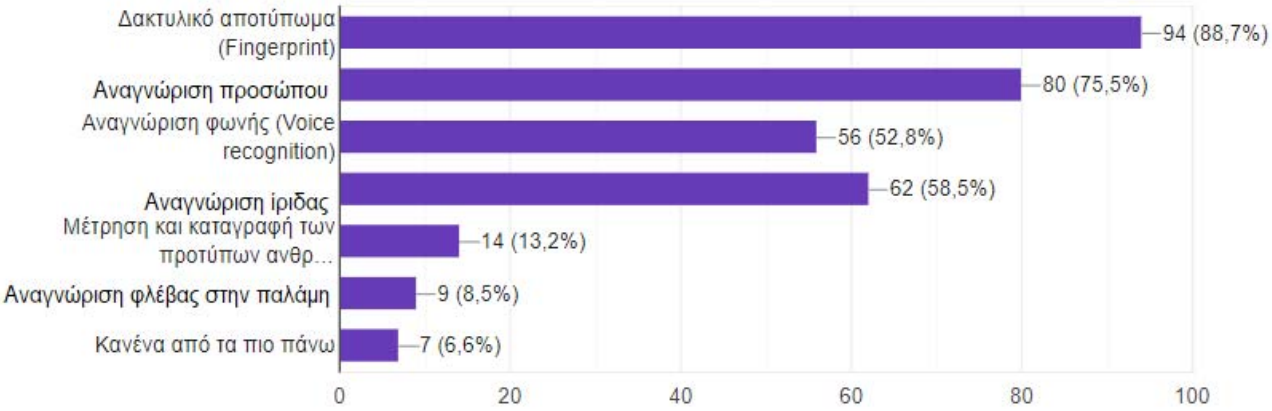

**Διάγραμμα 6.10:** Ποσοστό για λόγους εγκατάλειψης online αγοράς

**Ερώτηση 11:** Στην ερώτηση αν είναι εξοικειωμένοι οι ερωτηθέντες με τη χρήση βιομετρικών στοιχείων 37 άτομα απάντησαν ότι είναι πολύ εξοικειωμένοι με ποσοστό 34,9%, 34 άτομα απάντησαν ότι είναι κάπως εξοικειωμένοι με ποσοστό 32,1%, 23 άτομα απάντησαν ότι δεν είναι πολύ εξοικειωμένοι με ποσοστό 21,7% και 12 άτομα απάντησαν ότι δεν είναι καθόλου εξοικειωμένοι με ποσοστό 11,3%.




**Διάγραμμα 6.11:** Ποσοστό εξοικείωσης χρήσης βιομετρικών μεθόδων

**Ερώτηση 12:** Στην ερώτηση ποιους από τους βιομετρικούς τύπους ελέγχου ταυτότητας γνωρίζεται είχαμε 94 απαντήσεις ότι γνωρίζουν το δακτυλικό αποτύπωμα με ποσοστό 88,7%, 80 απαντήσεις ότι γνωρίζουν την αναγνώριση προσώπου με ποσοστό 75,5%, 56 απαντήσεις ότι γνωρίζουν την αναγνώριση φωνής με ποσοστό 52,8%, 62 απαντήσεις ότι γνωρίζουν τη μέθοδο αναγνώρισης ίριδας με ποσοστό 58,5%, 14 απαντήσεις ότι γνωρίζουν την καταγραφή των προτύπων ανθρώπινης συμπεριφοράς με ποσοστό 13,2%, 9 απαντήσεις ότι γνωρίζουν την αναγνώριση φλέβας στην παλάμη με ποσοστό 8,5% και 7 απαντήσεις ότι δεν γνωρίζουν καμία μέθοδο με ποσοστό 6,6%.

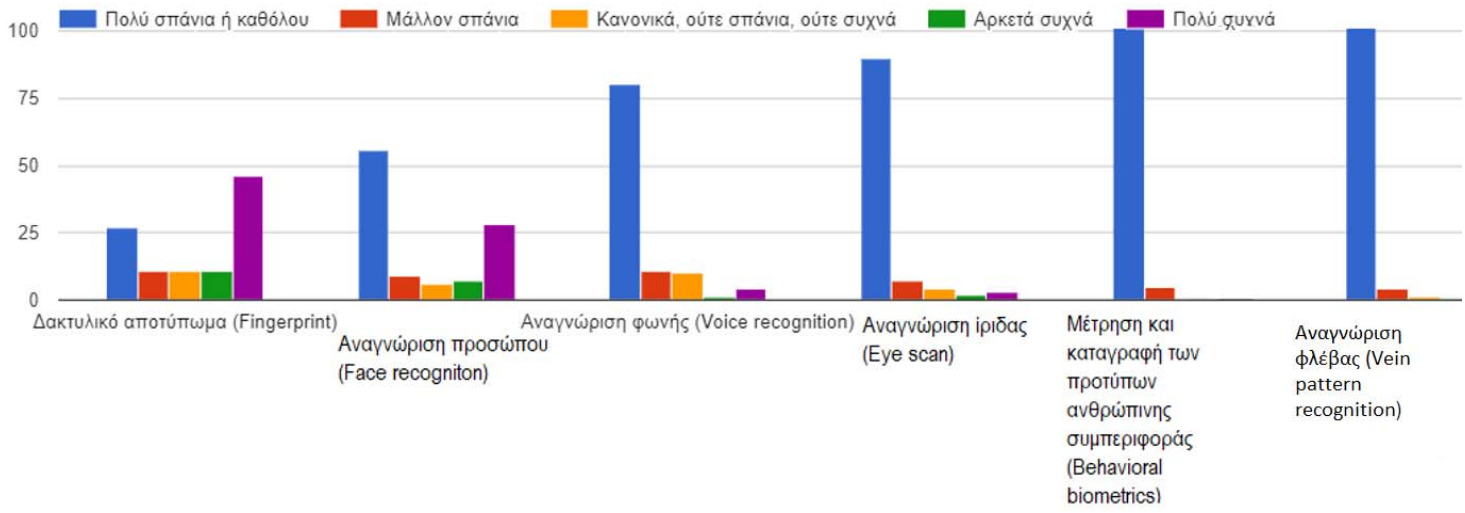



**Διάγραμμα 6.12:** Ποσοστό γνώσης βιομετρικών τύπων ελέγχου ταυτότητας

**Ερώτηση 13:** Στην ερώτηση πόσο συχνά χρησιμοποιούν τις βιομετρικές μεθόδους πήραμε τις εξής απαντήσεις:

- **Για το δακτυλικό αποτύπωμα** 27 άτομα απάντησαν πολύ σπάνια ή καθόλου, 11 άτομα μάλλον σπάνια, 11 άτομα κανονικά ούτε σπάνια ούτε συχνά, 11 άτομα αρκετά συχνά και 46 άτομα πολύ συχνά.
- **Για την αναγνώριση προσώπου** 56 άτομα απάντησαν πολύ σπάνια ή καθόλου, 9 άτομα απάντησαν μάλλον σπάνια, 6 άτομα απάντησαν κανονικά ούτε σπάνια ούτε συχνά, 7 άτομα απάντησαν αρκετά συχνά και 28 άτομα πολύ συχνά.
- **Για την αναγνώριση φωνής** 80 άτομα απάντησαν πολύ σπάνια ή καθόλου, 11 άτομα απάντησαν μάλλον σπάνια, 10 άτομα απάντησαν κανονικά ούτε σπάνια ούτε συχνά, 1 άτομο απάντησε αρκετά συχνά και 4 άτομα απάντησαν πολύ συχνά.
- **Για την αναγνώριση της ίριδας** 90 άτομα απάντησαν πολύ σπάνια ή καθόλου, 7άτομα μάλλον σπάνια, 4 άτομα απάντησαν κανονικά ούτε σπάνια ούτε συχνά, 2 άτομα απάντησε αρκετά συχνά και 3 άτομα απάντησαν πολύ συχνά.

- **Για τη μέτρηση και καταγραφή των προτύπων ανθρώπινης συμπεριφοράς** 101 άτομα απάντησαν πολύ σπάνια ή καθόλου και 5 άτομα απάντησαν μάλλον σπάνια.
- **Για την αναγνώριση φλέβας στην παλάμη** 101 άτομα απάντησαν πολύ σπάνια ή καθόλου , 4 άτομα απάντησαν μάλλον σπάνια και 1 άτομο απάντησε κανονικά ούτε σπάνια ούτε συχνά.

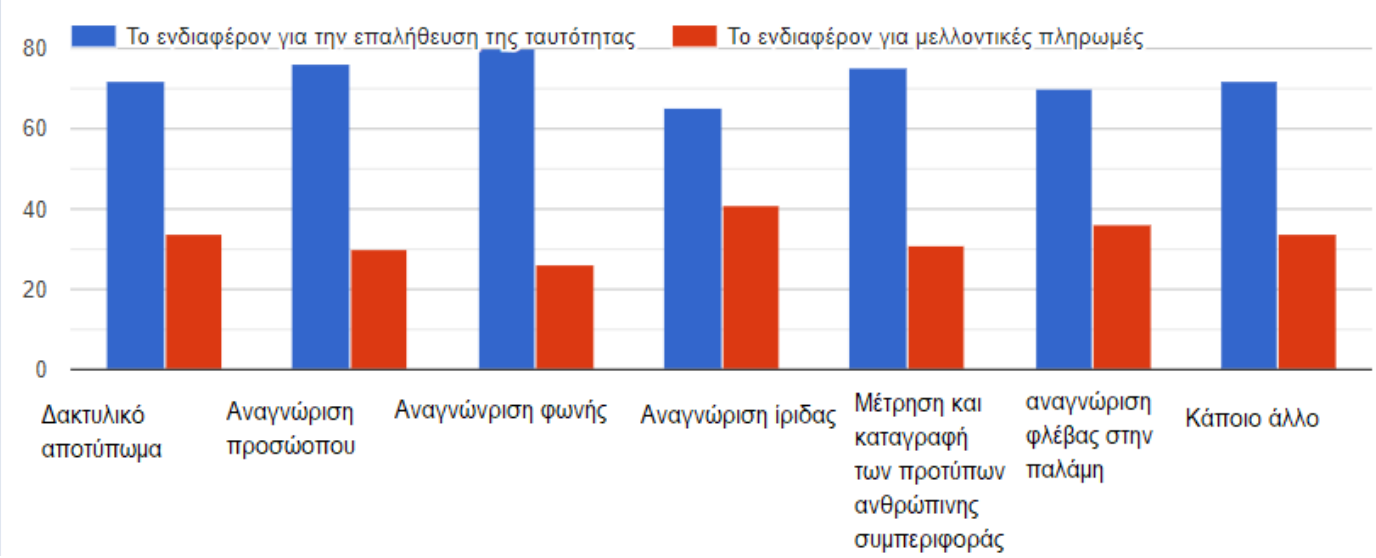



**Διάγραμμα 6.13:** Ποσοστό συχνότητας χρήσης βιομετρικών μεθόδων

**Ερώτηση 14:** Στην ερώτηση ποιο το ενδιαφέρον για τη χρήση βιομετρικών μεθόδων για την επαλήθευση της ταυτότητας των ερωτηθέντων πήραμε τις εξής απαντήσεις:

- **Για το δακτυλικό αποτύπωμα** 72 άτομα απάντησαν το ενδιαφέρον για την επαλήθευση της ταυτότητάς τους και 34 άτομα απάντησαν το ενδιαφέρον για μελλοντικές πληρωμές.
- **Για την αναγνώριση προσώπου** 76 άτομα απάντησαν το ενδιαφέρον για την επαλήθευση της ταυτότητάς τους και 30 άτομα απάντησαν το ενδιαφέρον για μελλοντικές πληρωμές.
- **Για την αναγνώριση φωνής** 80 άτομα απάντησαν το ενδιαφέρον για την επαλήθευση της ταυτότητάς τους και 26 άτομα απάντησαν το ενδιαφέρον για μελλοντικές πληρωμές.
- **Για την αναγνώριση της ίριδας** 65 άτομα απάντησαν το ενδιαφέρον για την επαλήθευση της ταυτότητάς τους και 41 άτομα απάντησαν το ενδιαφέρον για μελλοντικές πληρωμές.

- **Για τη μέτρηση και καταγραφή των προτύπων ανθρώπινης συμπεριφοράς** 75 άτομα απάντησαν το ενδιαφέρον για την επαλήθευση της ταυτότητάς τους και 31 άτομα απάντησαν το ενδιαφέρον για μελλοντικές πληρωμές.
- **Για την αναγνώριση φλέβας στην παλάμη** 70 άτομα απάντησαν το ενδιαφέρον για την επαλήθευση της ταυτότητάς τους και 36 άτομα απάντησαν το ενδιαφέρον για μελλοντικές πληρωμές.
- **Κάποιο άλλο** 72 άτομα απάντησαν το ενδιαφέρον για την επαλήθευση της ταυτότητάς τους και 34 άτομα απάντησαν το ενδιαφέρον για μελλοντικές πληρωμές.



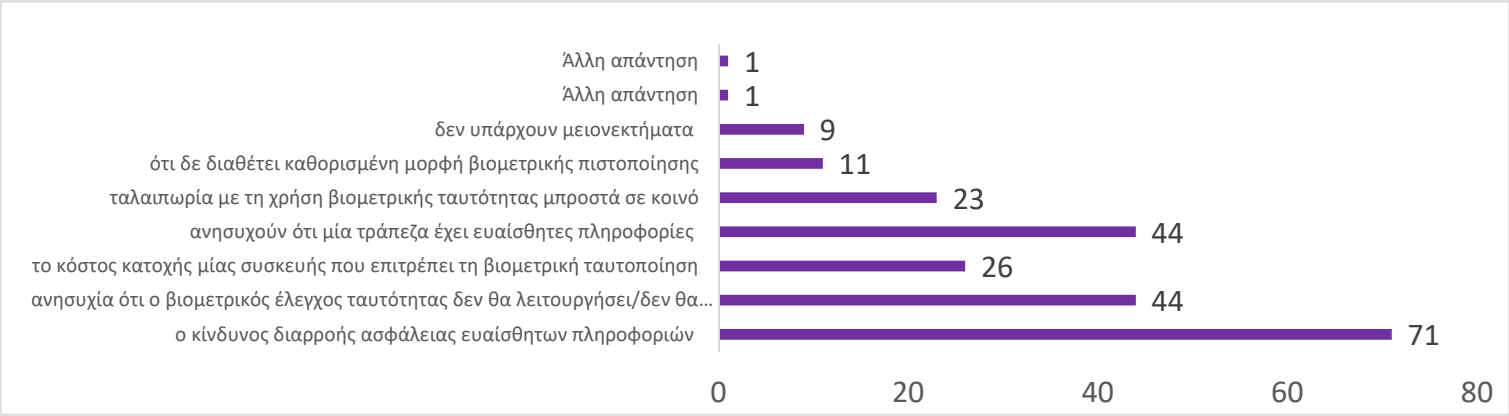

**Διάγραμμα 6.14:** Ενδιαφέρον χρήσης βιομετρικών μεθόδων για επαλήθευση ταυτότητας ή μελλοντικές πληρωμές

**Ερώτηση 15:** Στην ερώτηση ποια τα οφέλη από τη χρήση βιομετρικού ελέγχου ταυτότητας στις συναλλαγές πήραμε 71 απαντήσεις ότι θα εξαλείψει την ανάγκη να θυμόμαστε πολλούς κωδικούς πρόσβασης και PIN σε ποσοστό 67%, 69 απαντήσεις ότι είναι πιο ασφαλείς από τους κωδικούς πρόσβασης και τους αριθμούς PIN επειδή επιβεβαιώνουν την ταυτότητά του σε ποσοστό 65,1%, 36 απαντήσεις δεν ξεχνώ/δεν χάνω τη μέθοδο ταυτότητας σε ποσοστό 34%, 58 απαντήσεις ότι οι λογαριασμοί και τα στοιχεία τους είναι ασφαλές ακόμη και αν κλαπεί το smartphone ή ο Υπολογιστής τους σε ποσοστό 54,7%, 51 απαντήσεις ότι μπορώ να πληρώσω οπουδήποτε/οτιδήποτε επειδή η μέθοδος ελέγχου ταυτότητας αποτελεί μέρος του σε ποσοστό 48,1%, 46 απαντήσεις ότι ο βιομετρικός έλεγχος ταυτότητας είναι ευκολότερος από την εισαγωγή κωδικού πρόσβασης ή PIN σε ποσοστό 43,4%, 34 απαντήσεις ότι η χρήση της

βιομετρικής ταυτότητας θα έδινε την σιγουριά ότι η πληρωμή τους προστατεύεται με ποσοστό 32,1%, 6 απάντησαν ότι δεν υπάρχουν οφέλη σε ποσοστό 5,7%, και άλλες 2 απαντήσεις με ποσοστό 0,9% η κάθε μία.


**Διάγραμμα 6.15:** Οφέλη χρήσης βιομετρικού ελέγχου ταυτότητας στις συναλλαγές

**Ερώτηση 16:** Στην ερώτηση ποιες οι κύριες ανησυχίες των ερωτηθέντων όσο αφορά τη χρήση βιομετρικών στοιχείων αυθεντικοποίησης για τις πληρωμές τους πήραμε 71 απαντήσεις ότι υπάρχει ο κίνδυνος διαρροής ασφάλειας ευαίσθητων πληροφοριών σε ποσοστό 67%, 44 απαντήσεις πως υπάρχει ανησυχία ότι ο βιομετρικός έλεγχος ταυτότητας δεν θα λειτουργήσει / δεν θα λάβει πολλές προσπάθειες σε ποσοστό 41,5%, 26 απαντήσεις για το κόστος κατοχής μίας συσκευής που επιτρέπει τη βιομετρική ταυτοποίηση σε ποσοστό 24,5%, 44 απαντήσεις για την προστασία προσωπικών δεδομένων – ανησυχούν ότι μία τράπεζα έχει ευαίσθητες πληροφορίες σε ποσοστό 41,5%, 23 απαντήσεις ότι υπάρχει ταλαιπωρία με τη χρήση βιομετρικής ταυτότητας μπροστά σε κοινό σε ποσοστό 21,7%, 11 απαντήσεις ότι δεν διαθέτει καθορισμένη μορφή βιομετρικής πιστοποίησης σε ποσοστό 10,4%, 9 απάντησαν ότι δεν υπάρχουν μειονεκτήματα και 2 άλλες απαντήσεις με ποσοστό 0,9% έκαστος.




**Διάγραμμα 6.16:** Ανησυχίες χρήσης βιομετρικών στοιχείων αυθεντικοποίησης στις πληρωμές

**Ερώτηση 17:** Στην ερώτηση εάν τα βιομετρικά στοιχεία είναι ταχύτερα ή πιο αργά από τους κωδικούς πρόσβασης 58 άτομα απάντησαν ότι είναι πολύ πιο γρήγορα από τους κωδικούς πρόσβασης με ποσοστό 54,7%, 19 άτομα απάντησαν ότι είναι λίγο πιο γρήγορα από τους κωδικούς πρόσβασης με ποσοστό 17,9%, 8 άτομα απάντησαν ότι δεν έχουν καμία αλλαγή με ποσοστό 7,5%, 7 άτομα απάντησαν ότι είναι λίγο πιο αργά από τους κωδικούς πρόσβασης με ποσοστό 6,6%, 2 άτομα απάντησαν ότι είναι πολύ πιο αργά από τους κωδικούς πρόσβασης με ποσοστό 1,9% και 12 άτομα απάντησαν ότι δεν γνωρίζουν/ δεν είναι σίγουροι με ποσοστό 11,3%.


**Διάγραμμα 6.17:** Ποσοστό κατά πόσο τα βιομετρικά στοιχεία είναι ταχύτερα ή πιο αργά από τους κωδικούς πρόσβασης

**Ερώτηση 18:** Στην ερώτηση εάν η χρήση βιομετρικών στοιχείων είναι πιο εύκολη ή πιο δύσκολη από τους κωδικούς πρόσβασης 55 άτομα απάντησαν ότι είναι πολύ ευκολότερη από τους κωδικούς πρόσβασης με ποσοστό 51,9%, 29 άτομα απάντησαν ότι είναι λίγο πιο εύκολη από τους κωδικούς πρόσβασης, 7 άτομα απάντησαν ότι δεν παρατηρούν

καμία αλλαγή με ποσοστό 6,6%, 4 άτομα απάντησαν ότι είναι λίγο πιο δύσκολη από τους κωδικούς πρόσβασης με ποσοστό 3,8%, 1 άτομο απάντησε ότι είναι πολύ πιο δύσκολη από τους κωδικούς πρόσβασης με ποσοστό 0,9% και τα υπόλοιπα 10 άτομα απάντησαν ότι δε γνωρίζουν / δεν είναι σίγουροι με ποσοστό 9,4%.

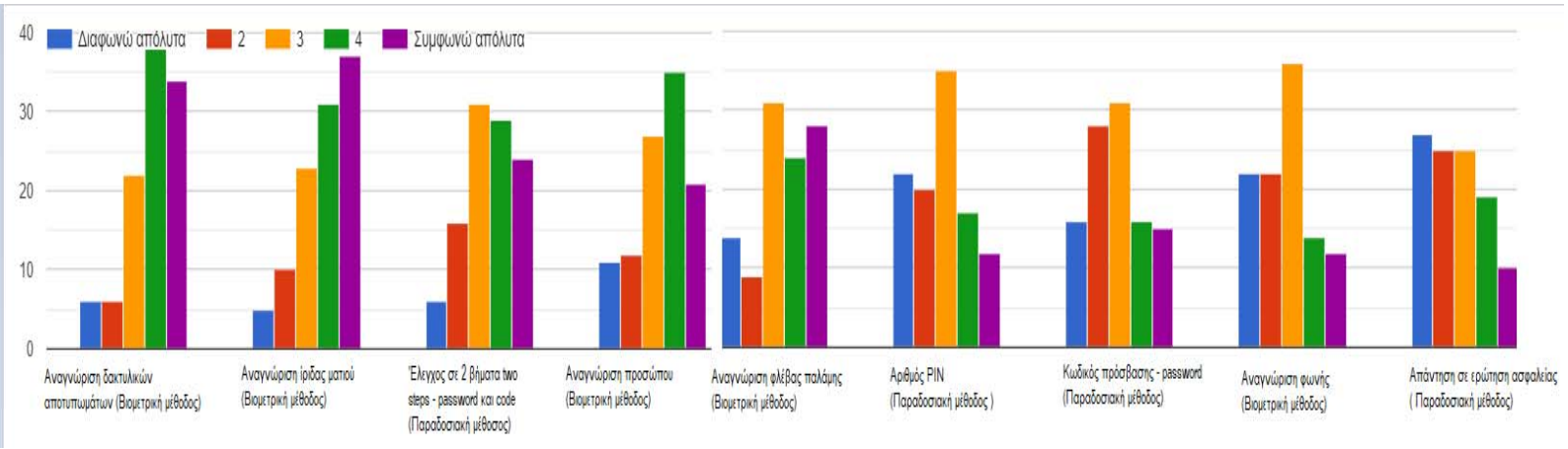

**Διάγραμμα 6.18:** Ποσοστό κατά πόσο τα βιομετρικά στοιχεία είναι ευκολότερα ή δυσκολότερα από τους κωδικούς πρόσβασης

**Ερώτηση 19:** Στην ερώτηση εάν οι βιομετρικές μέθοδοι είναι πιο ασφαλείς από τις παραδοσιακές μεθόδους ταυτοποίησης οι ερωτηθέντες απάντησαν ως εξής:

- **Για την αναγνώριση δακτυλικών αποτυπωμάτων (Βιομετρική μέθοδος)** 6 άτομα απάντησαν ότι διαφωνούν απόλυτα, 6 άτομα διαφωνούν, 22 άτομα ούτε διαφωνούν ούτε συμφωνούν, 38 άτομα συμφωνούν και 34 άτομα συμφωνούν απόλυτα.
- **Για την αναγνώριση της ίριδας (Βιομετρική μέθοδος)** 5 άτομα απάντησαν ότι διαφωνούν απόλυτα, 10 άτομα διαφωνούν, 20 άτομα ούτε διαφωνούν ούτε συμφωνούν, 31 άτομα συμφωνούν και 37 άτομα συμφωνούν απόλυτα.
- **Για τον έλεγχο σε 2 βήματα two steps – password και code (Παραδοσιακή μέθοδος)** 6 άτομα απάντησαν ότι διαφωνούν απόλυτα, 16 άτομα διαφωνούν, 31 άτομα ούτε διαφωνούν ούτε συμφωνούν, 29 άτομα συμφωνούν και 24 άτομα συμφωνούν απόλυτα.
- **Για την αναγνώριση προσώπου (Βιομετρική μέθοδος)** 11 άτομα απάντησαν ότι διαφωνούν απόλυτα, 12 άτομα διαφωνούν, 27 άτομα ούτε διαφωνούν ούτε συμφωνούν, 35 άτομα συμφωνούν και 21 άτομα συμφωνούν απόλυτα.
- **Για την αναγνώριση φλέβας παλάμης (Βιομετρική μέθοδος)** 14 άτομα απάντησαν ότι διαφωνούν απόλυτα, 9 άτομα διαφωνούν, 31 άτομα ούτε

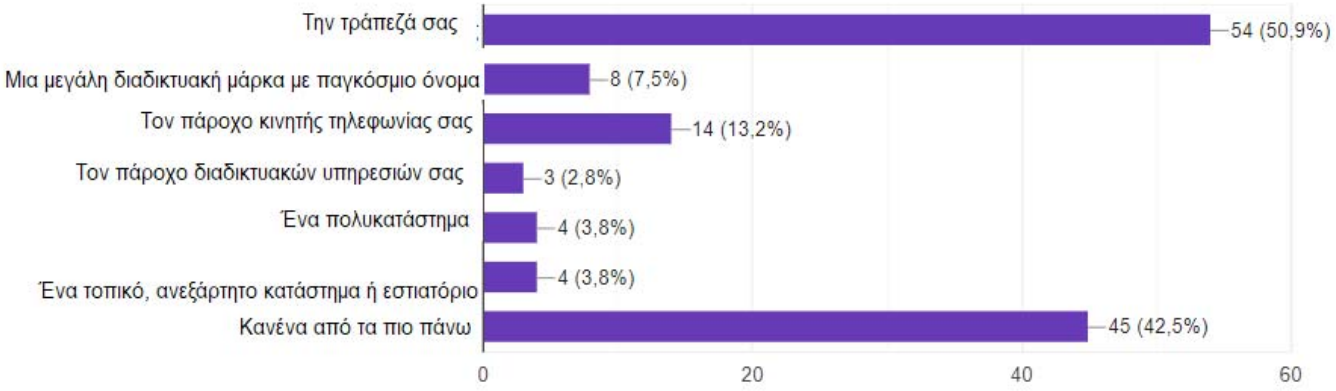
διαφωνούν ούτε συμφωνούν, 24 άτομα συμφωνούν και 28 άτομα συμφωνούν απόλυτα.

- **Για τον αριθμό PIN (Παραδοσιακή μέθοδος)** 22 άτομα απάντησαν ότι διαφωνούν απόλυτα, 20 άτομα διαφωνούν, 35 άτομα ούτε διαφωνούν ούτε συμφωνούν, 17 άτομα συμφωνούν και 12 άτομα συμφωνούν απόλυτα.
- **Για τους κωδικούς πρόσβασης – password(Παραδοσιακή μέθοδος)** 16 άτομα απάντησαν ότι διαφωνούν απόλυτα, 28 άτομα διαφωνούν, 31 άτομα ούτε διαφωνούν ούτε συμφωνούν, 16 άτομα συμφωνούν και 15 άτομα συμφωνούν απόλυτα.
- **Για την αναγνώριση φωνής (Βιομετρική μέθοδος)** 22 άτομα απάντησαν ότι διαφωνούν απόλυτα, 22 άτομα διαφωνούν, 36 άτομα ούτε διαφωνούν ούτε συμφωνούν, 14 άτομα συμφωνούν και 12 άτομα συμφωνούν απόλυτα.
- **Για την απάντηση σε ερώτηση ασφαλείας (Παραδοσιακή μέθοδος)** 27 άτομα απάντησαν ότι διαφωνούν απόλυτα, 25 άτομα διαφωνούν, 25 άτομα ούτε διαφωνούν ούτε συμφωνούν, 19 άτομα συμφωνούν και 10 άτομα συμφωνούν απόλυτα.




**Διάγραμμα 6.19:** Ποσοστό συμφωνίας ασφάλειας βιομετρικών μεθόδων έναντι παραδοσιακών μεθόδων ταυτοποίησης

**Ερώτηση 20:** Στην ερώτηση σε ποιο θα εμπιστεύονταν οι ερωτηθέντες την αποθήκευση βιομετρικών πληροφοριών 54 άτομα απάντησαν την τράπεζα τους με ποσοστό 50,9%, 8 άτομα απάντησαν μια μεγάλη διαδικτυακή μάρκα με παγκόσμιο όνομα με ποσοστό 7,5%, 14 άτομα απάντησαν τον πάροχο κινητής τους τηλεφωνίας σε ποσοστό 13,2%, 3 άτομα απάντησαν τον πάροχο διαδικτυακών υπηρεσιών τους με ποσοστό 2,8%, 4 άτομα απάντησαν ένα πολυκατάστημα με ποσοστό 3,8%, 4 άτομα απάντησαν ένα τοπικό, ανεξάρτητο κατάστημα ή εστιατόριο με ποσοστό 3,8% και οι υπόλοιποι 45 απάντησαν κανένα από τα πιο πάνω με ποσοστό 42,5%.




**Διάγραμμα 6.20:** Ποσοστό εμπιστοσύνης αποθήκευσης βιομετρικών πληροφοριών

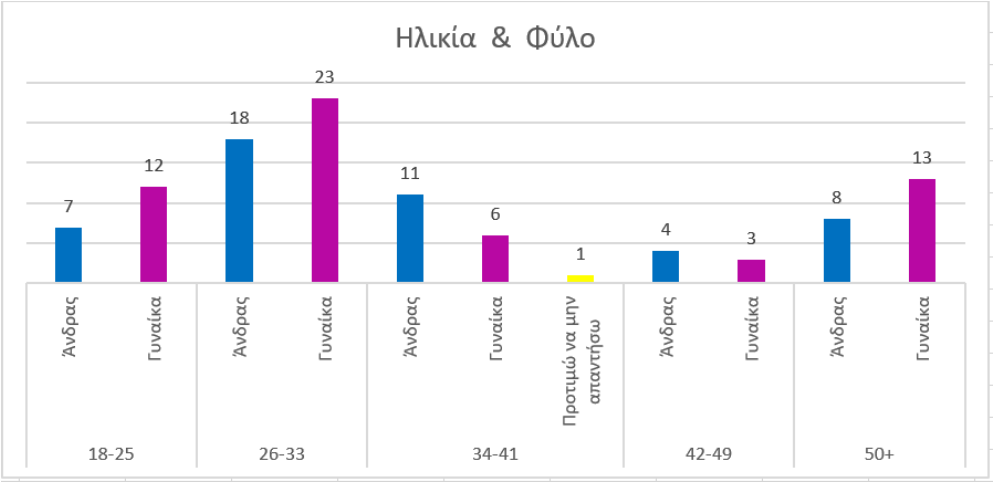
**Ερώτηση 21:** Στην ερώτηση εάν υπήρχε περίπτωση ένας παροχέας να μην σας προσφέρει βιομετρική ταυτοποίηση στο μέλλον από τι θα απομακρυνόσασταν 13 άτομα απάντησαν την πιστωτική τους κάρτα με ποσοστό 12,3%, 33 άτομα απάντησαν την τράπεζά τους με ποσοστό 31,1%, 29 άτομα απάντησαν τον κινητό φορέα τηλεφωνίας τους με ποσοστό 27,4%, 23 άτομα απάντησαν την χρεωστική τους κάρτα με ποσοστό 21,7%, 2 άτομα απάντησαν από κανένα με ποσοστό 1,9% και οι υπόλοιποι 6 έδωσαν άλλες απαντήσεις με συνολικό ποσοστό 5.4%.


**Διάγραμμα 6.21:** Ποσοστό απομάκρυνσης εάν ένας παροχέας δεν προσφέρει βιομετρική ταυτοποίηση

## 6.2 Ανάλυση και Ερμηνεία Δεδομένων

Η ανάλυση και η ερμηνεία των αποτελεσμάτων της έρευνας παρουσιάζει τα δημογραφικά χαρακτηριστικά του δείγματος και ακολούθως υπολογίζονται οι συσχετίσεις μεταξύ των μεταβλητών.

Αναλύοντας τους δημογραφικούς παράγοντες, παρατηρούμε ότι σε δείγμα 106 ατόμων πήραμε περισσότερες απαντήσεις από γυναίκες μεταξύ των ηλικιών 18-25, 26-33 και πάνω από 50+. Ενώ πήραμε περισσότερες απαντήσεις από άνδρες στις ηλικίες 34-41 και 42-49 ετών και είχαμε και μία απάντηση από ένα άτομο που δεν ήθελε να διευκρινιστεί το φύλο του ηλικίας 34-41 ετών.

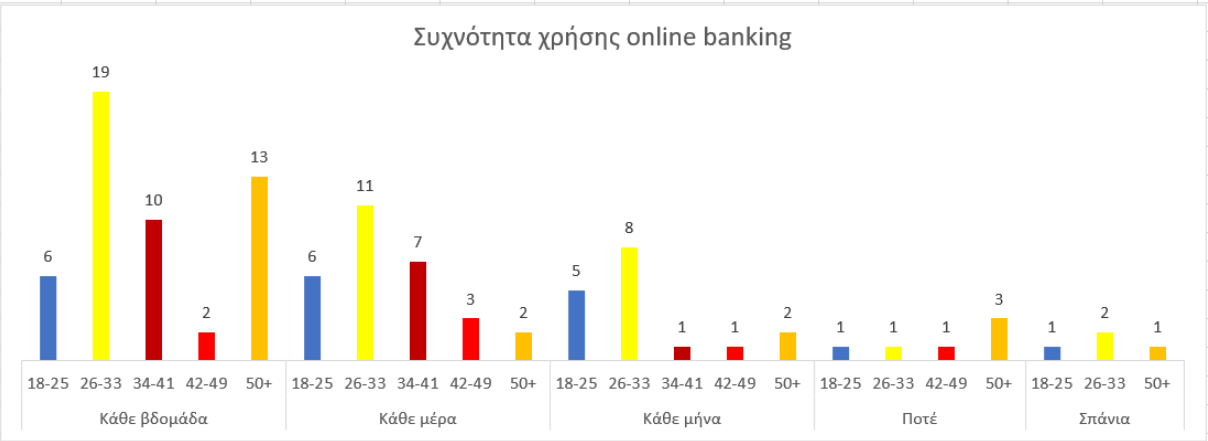



**Διάγραμμα 6.22:** Ποσοστό ηλικίας σε σχέση με το φύλο

Από το σύνολο του δείγματος διακρίνεται ότι το μορφωτικό επίπεδο είναι αρκετά υψηλό μιας και το ποσοστό αποφοίτων πανεπιστημίου ήταν 46,2%, το 41,5% κατέχουν μεταπτυχιακό ή διδακτορικό τίτλο και το υπόλοιπο 12,3% είναι απόφοιτοι λυκείου.

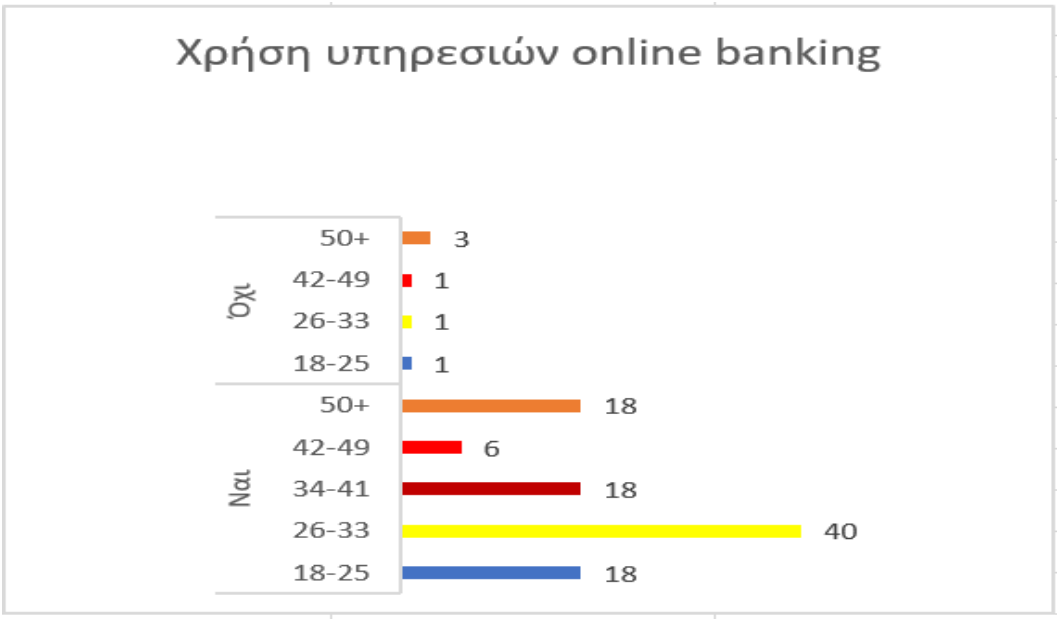
Οι πλείστοι ερωτηθέντες είναι ιδιωτικοί υπάλληλοι με μια μικρή μερίδα να είναι δημόσιοι υπάλληλοι. Οι υπόλοιποι είναι είτε φοιτητές είτε συνταξιούχοι κυρίως τα άτομα πέραν των 50 ετών.

Σχετικά με την συχνότητα χρήσης του online banking αναλόγως της ηλικίας των ερωτηθέντων, παρατηρούμε ότι τα άτομα μεταξύ 26-33 ετών χρησιμοποιούν κάθε μέρα ή κάθε βδομάδα το online banking σε αντίθεση με τα άτομα μεταξύ 34-41 ετών και πάνω των 50+ που το χρησιμοποιούν σχεδόν κάθε βδομάδα. Ορισμένοι είναι αυτοί που το χρησιμοποιούν σπάνια ή ποτέ και τα άτομα μεταξύ 42-49 ετών χρησιμοποιούν το online banking ελάχιστα κάθε μέρα ή κάθε εβδομάδα.



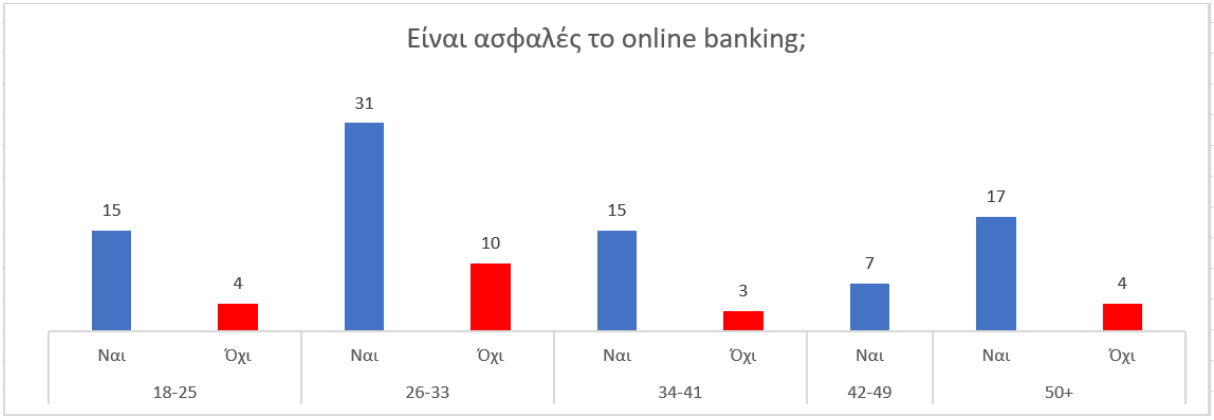

**Διάγραμμα 6.23:** Συχνότητα χρήσης online banking σε σχέση με την ηλικία

Όσον αφορά την χρήση υπηρεσιών online banking παρατηρούμε ότι χρησιμοποιείται σχεδόν από όλες τις ηλικιακές βαθμίδες και κυρίως από τις ηλικίες μεταξύ 26-33 ετών. Ενώ στις ηλικίες 34-41 ετών δεν είχαμε απαντήσεις που να μην χρησιμοποιούν τις υπηρεσίες online banking.



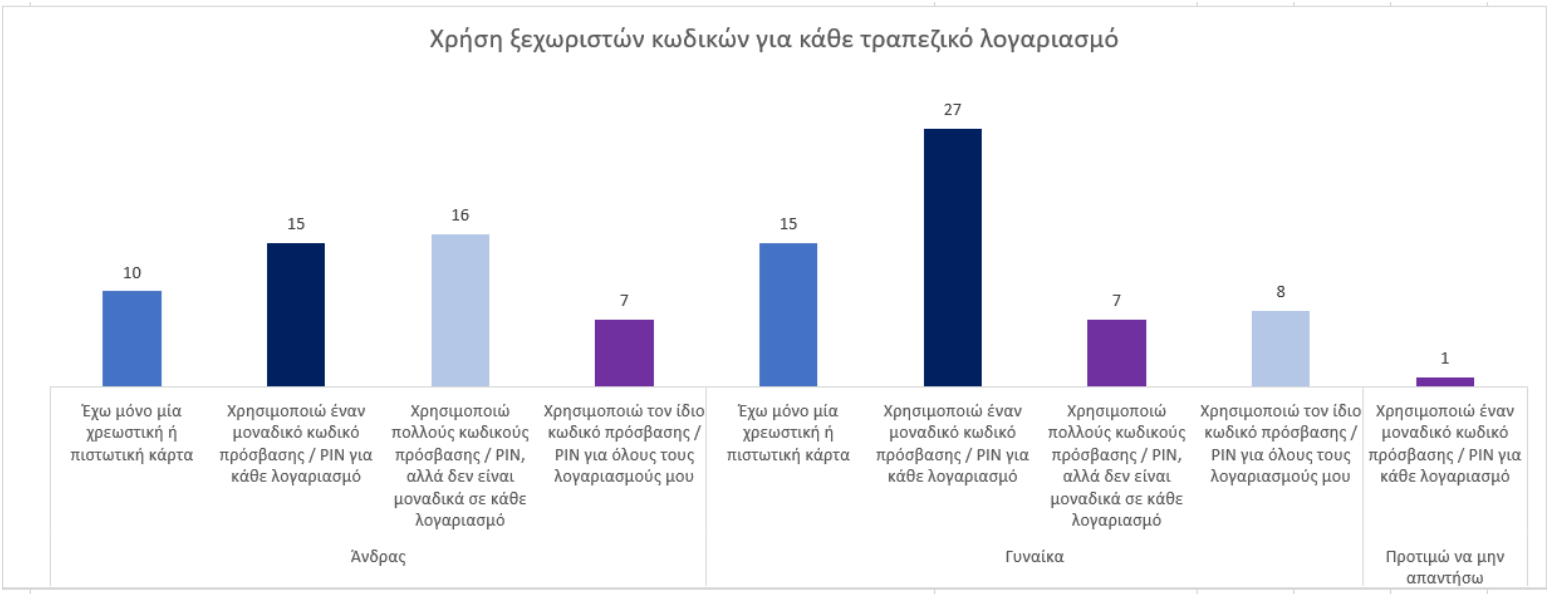

**Διάγραμμα 6.24:** Χρήση υπηρεσιών online banking σε σχέση με την ηλικία

Επίσης, τα περισσότερα άτομα όλων των ηλικιών πιστεύουν πως είναι ασφαλές το online banking ενώ περίπου το 1/5 ολόκληρου του δείγματος (21 άτομα) πιστεύουν πως δεν είναι ασφαλές.




**Διάγραμμα 6.25:** Ασφάλεια online banking σε σχέση με το τι πιστεύει κάθε ηλικία

Στο πιο κάτω διάγραμμα διακρίνουμε ότι οι περισσότερες γυναίκες χρησιμοποιούν ένα μοναδικό κωδικό πρόσβασης/PIN για κάθε λογαριασμό σε αντίθεση με τους άνδρες που οι περισσότεροι χρησιμοποιούν πολλούς κωδικούς πρόσβασης/PIN αλλά δεν είναι μοναδικά για κάθε τους λογαριασμό. Επίσης, είναι περισσότερες οι γυναίκες που έχουν μόνο μία χρεωστική ή πιστωτική κάρτα σε σχέση με τους άνδρες, ενώ και στα δύο φύλα είναι ίδιο το ποσοστό που χρησιμοποιεί τον ίδιο κωδικό πρόσβασης/PIN για όλους τους λογαριασμούς τους.




**Διάγραμμα 6.26:** Χρήση κωδικών για κάθε τραπεζικό λογαριασμό σε σχέση με το φύλο

Οι λόγοι για τους οποίους εγκαταλείπουν οι περισσότεροι ερωτηθέντες κάποια online αγορά και στα δύο φύλα αλλά και το άτομο που προτίμησε να μην προσδιορίσει το φύλο του είναι γιατί δεν είχαν την χρεωστική/ πιστωτική κάρτα μαζί τους. Συνήθως λιγότερες γυναίκες φαίνεται να μην κάνουν αγορές online ενώ περισσότεροι άνδρες εγκατέλειψαν την αγορά τους είτε γιατί δεν μπορούσαν να θυμηθούν τον κωδικό τους είτε διότι χρειάστηκε να τον πληκτρολογήσουν.

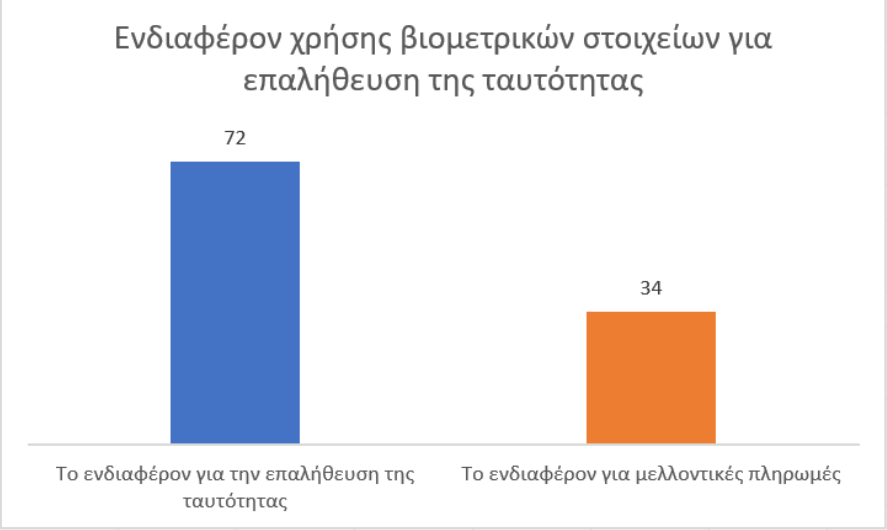

**Διάγραμμα 6.27:** Λόγοι εγκατάλειψης online αγοράς σε σχέση με το φύλο

Οι περισσότεροι χρήστες φαίνεται να είναι αρκετά εξοικειωμένοι με τη χρήση βιομετρικών στοιχείων και πιο συγκεκριμένα οι άνδρες φαίνεται να είναι πολύ εξοικειωμένη σε αντίθεση με τις γυναίκες που είναι κάπως εξοικειωμένες. Πολύ μικρό δείγμα ανδρών δεν είναι καθόλου εξοικειωμένοι και αρκετές γυναίκες είναι όχι και τόσο πολύ εξοικειωμένες.


**Διάγραμμα 6.28:** Ποσοστό εξοικείωσης χρήσης βιομετρικών στοιχείων σε σχέση με το φύλο

Από τα δεδομένα που συλλέχθηκαν αρκετοί ερωτηθέντες, συγκεκριμένα 28 άτομα γνωρίζουν τέσσερεις από τους πιο σημαντικούς βιομετρικούς ελέγχους ταυτότητας τα δακτυλικά αποτυπώματα, την αναγνώριση προσώπου, φωνής και ίριδας. Το 1/8 του δείγματος δηλαδή 13 άτομα γνώριζε μόνο τη μέθοδο αναγνώρισης μέσω δακτυλικού αποτυπώματος ενώ το ένα 1/7 του δείγματος δηλαδή 15 άτομα γνώριζαν τρεις μόνο μεθόδους και αυτές ήταν τα δακτυλικά αποτυπώματα, η αναγνώριση προσώπου και ίριδας. Επιπλέον, 7 άτομα δεν γνώριζαν κανέναν απολύτως βιομετρικό έλεγχο και μόνο 6 άτομα γνώριζαν όλους τους βιομετρικούς ελέγχους ταυτότητας. Σχεδόν το μισό δείγμα χρησιμοποιεί πολύ συχνά μία από τις βιομετρικές μεθόδους και περίπου το 1/3 του δείγματος, 27 άτομα κάνουν πολύ σπάνια ή καθόλου χρήση των βιομετρικών ελέγχων.

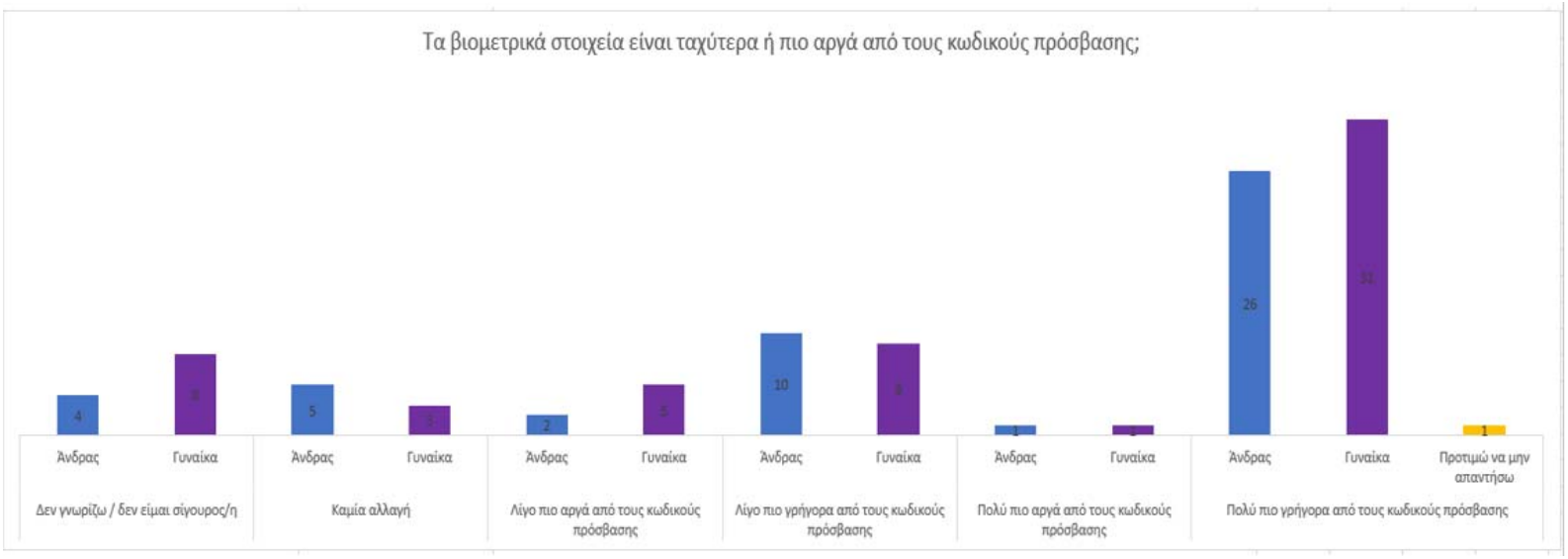
Σχετικά με το ενδιαφέρον των ερωτηθέντων για τη χρήση των βιομετρικών στοιχείων περισσότεροι από τους μισούς 72 άτομα απάντησαν ότι ενδιαφέρονται για την επαλήθευση της ταυτότητάς τους αντί για το ενδιαφέρον μελλοντικών πληρωμών.




**Διάγραμμα 6.29:** Ποσοστό ενδιαφέροντος για χρήσης βιομετρικών στοιχείων

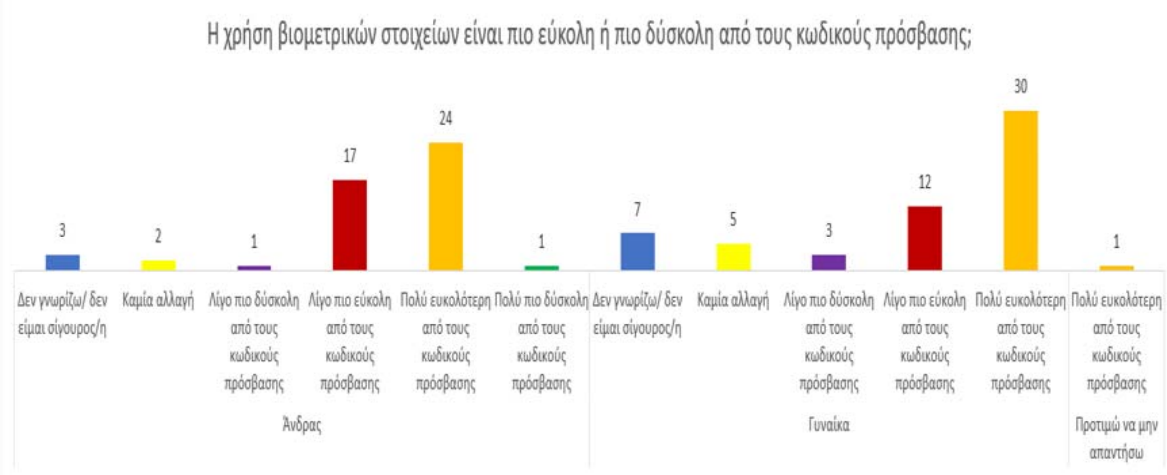
Σχεδόν όλοι οι ερωτηθέντες φαίνεται να γνωρίζουν ποια είναι τα οφέλη από τη χρήση βιομετρικού ελέγχου ταυτότητας στις συναλλαγές τους ενώ μόλις 5 άτομα πιστεύουν πως δεν υπάρχουν καθόλου οφέλη. Πέραν όμως από τα οφέλη, υπάρχουν και ορισμένες ανησυχίες όπως είναι ο κίνδυνος διαρροής ευαίσθητων πληροφοριών και η ανησυχία πως μία τράπεζα έχει τις ευαίσθητες προσωπικές πληροφορίες στην κατοχή της. Παράλληλα υπάρχει και ένα μικρό δείγμα μόλις 9 ατόμων που θεωρεί πως δεν υπάρχουν μειονεκτήματα και δεν ανησυχούν.

Περισσότεροι από το μισό δείγμα και από τα δύο φύλα καθώς και το άτομο που δεν προσδιόρισε το φύλο του, σύνολο 58 άτομα πιστεύουν πως τα βιομετρικά στοιχεία είναι πολύ πιο γρήγορα από τους κωδικούς πρόσβασης και μόλις 2 άτομα ένας άνδρας και μία γυναίκα πιστεύουν το αντίθετο.




**Διάγραμμα 6.30:** Ποσοστό αναγνώρισης ταχύτητας βιομετρικών στοιχείων σε σχέση με τα δύο φύλα

Επιπλέον το περισσότερο δείγμα και στα δύο φύλα δηλαδή 55 άτομα πιστεύει πως η χρήση βιομετρικών στοιχείων είναι πολύ πιο εύκολη από τους κωδικούς πρόσβασης και 29 άτομα πιστεύουν πως είναι λίγο πιο εύκολη από τους κωδικούς πρόσβασης. Μόνο 1 άτομο πιστεύει ότι είναι πολύ πιο δύσκολη από τους κωδικούς πρόσβασης ενώ οι υπόλοιποι ερωτηθέντες και από τα δύο φύλα δεν γνωρίζουν ή δεν βλέπουν ότι υπάρχει κάποια αλλαγή.




**Διάγραμμα 6.31:** Ποσοστό αναγνώρισης ευκολίας βιομετρικών στοιχείων σε σχέση με τα δύο φύλα

Έχοντας ως δεδομένο πως η ασφάλεια παίζει καθοριστικό ρόλο στη χρήση μεθόδων ταυτοποίησης, παρατηρούμε ότι περισσότεροι από το μισό δείγμα, 38 άτομα συμφωνούν μαζί με 34 ακόμη άτομα που συμφωνούν απόλυτα πως οι βιομετρικές μέθοδοι είναι πιο ασφαλείς από τις παραδοσιακές μεθόδους.
Αρκετοί είναι αυτοί (22 άτομα) που απάντησαν πως ούτε συμφωνούν ούτε διαφωνούν σχετικά με το αν οι παραδοσιακές μέθοδοι είναι πιο ασφαλείς ενώ οι υπόλοιποι διαφωνούν και θεωρούν τις παραδοσιακές μεθόδους ως πιο ασφαλείς. Έτσι στην ερώτηση αν θα εμπιστεύονταν την αποθήκευση των βιομετρικών τους πληροφοριών 45 άτομα δήλωσαν ότι δεν εμπιστεύονται σε κανέναν τα στοιχεία τους και 39 άτομα θα εμπιστεύονταν μόνο την τράπεζά τους.
Τέλος, στην περίπτωση που ο παροχέας δεν πρόσφερε βιομετρική ταυτοποίηση στο μέλλον σχεδόν το 1/3 του δείγματος και συγκεκριμένα 33 άτομα απάντησαν ότι θα απομακρύνονταν από την τράπεζά τους, περισσότεροι από το ¼ 29 άτομα δήλωσαν πως θα απομακρύνονταν από τον κινητό φορέα τηλεφωνίας τους, άλλο 1/3 ακόμη 36 άτομα θα έμεναν μακριά από την πιστωτική ή την χρεωστική τους κάρτα και το υπόλοιπο δείγμα δεν θα έκανε κάτι για να κρατηθεί μακριά.

## 6.3 Συσχετίσεις

Για να εξάγουμε τις συσχετίσεις μεταξύ των μεταβλητών έγινε χρήση του στατιστικού εργαλείου SPSS και ο υπολογισμός έγινε μέσω Crosstabulation από το μενού Analyze -> Descriptive Statistics -> Crosstabs

Για τη πρώτη συσχέτιση μεταξύ των μεταβλητών **ηλικία** και **συχνότητας χρήσης του online banking** ορίστηκαν οι εξής υποθέσεις:

**α=** 0.005
**H0:** Η ηλικία δεν σχετίζεται με τη συχνότητα χρήσης του online banking
**H1:** Η ηλικία σχετίζεται με τη συχνότητα χρήσης του online banking

**Ερώτηση 2: Ηλικία * Ερώτηση 6: Πόσο συχνά γίνεται χρήση του online banking; Crosstabulation**

Count

| | | Ερώτηση 6: Πόσο συχνά γίνεται χρήση του online banking; | | | | | |
|---|---|---|---|---|---|---|---|
| | | Κάθε μέρα | Κάθε βδομάδα | Κάθε μήνα | Σπάνια | Ποτέ | Total |
| Ερώτηση 2: Ηλικία | 18-25 | 6 | 6 | 5 | 1 | 1 | 19 |
| | 26-33 | 11 | 19 | 8 | 2 | 1 | 41 |
| | 34-41 | 7 | 10 | 1 | 0 | 0 | 18 |
| | 42-49 | 3 | 2 | 1 | 0 | 1 | 7 |
| | 50 | 2 | 13 | 2 | 1 | 3 | 21 |
| Total | | 29 | 50 | 17 | 4 | 6 | 106 |

**Πίνακας 6.1:** Ηλικία * Συχνότητα χρήσης online banking

**Chi-Square Tests**

| | Value | df | Asymptotic Significance (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 16.852[a] | 16 | .395 |
| Likelihood Ratio | 18.922 | 16 | .273 |
| Linear-by-Linear Association | 1.032 | 1 | .310 |
| N of Valid Cases | 106 | | |

a. 17 cells (68.0%) have expected count less than 5. The minimum expected count is .26.

**Πίνακας 6.2:** Chi- Square Tests ηλικία-συχνότητα χρήσης online banking

Από τον πιο πάνω **πίνακα 6.2** παρατηρούμε ότι για το Pearson Chi-Square το **sig=.395>0.005** άρα ισχύει η Η0 υπόθεση. Καταλήγουμε στο γεγονός ότι η ηλικία δεν εξαρτάται από τη συχνότητα χρήσης του online banking και δεν υπάρχει σημαντική στατιστική συσχέτιση μεταξύ των δύο μεταβλητών.

Η επόμενη συσχέτιση έχει να κάνει με το **επίπεδο εκπαίδευσης** και το πόσο οι χρήστες είναι **εξοικειωμένοι με τη χρήση βιομετρικών στοιχείων** έτσι ορίστηκαν οι πιο κάτω υποθέσεις:

**α=**0.005

**H0:** Το επίπεδο εκπαίδευσης δεν σχετίζεται με την εξοικείωση της χρήσης βιομετρικών στοιχείων

**H1:** Το επίπεδο εκπαίδευσης σχετίζεται με την εξοικείωση της χρήσης βιομετρικών στοιχείων

**Ερώτηση 3: Επίπεδο εκπαίδευσης * Ερώτηση 11: Πόσο εξοικειωμένοι είστε με τη χρήση βιομετρικών στοιχείων; Crosstabulation**

Count

| | | Ερώτηση 11: Πόσο εξοικειωμένοι είστε με τη χρήση βιομετρικών στοιχείων; | | | | |
|---|---|---|---|---|---|---|
| | | Πολύ εξοικειωμένος/η | Κάπως εξοικειωμένος/η | Όχι πολύ εξοικειωμένος/η | Καθόλου εξοικειωμένος/η | Total |
| Ερώτηση 3: Επίπεδο εκπαίδευσης | Μεταπτυχιακός τίτλος ή Διδακτορικό | 23 | 14 | 6 | 1 | 44 |
| | Πανεπιστημιακή εκπαίδευση | 14 | 18 | 12 | 5 | 49 |
| | Απολυτήριο Λυκείου | 0 | 2 | 5 | 6 | 13 |
| Total | | 37 | 34 | 23 | 12 | 106 |

**Πίνακας 6.3:** Επίπεδο εκπαίδευσης * εξοικείωση χρήσης βιομετρικών στοιχείων

**Chi-Square Tests**

| | Value | df | Asymptotic Significance (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 30.711[a] | 6 | .000 |
| Likelihood Ratio | 30.357 | 6 | .000 |
| Linear-by-Linear Association | 24.957 | 1 | .000 |
| N of Valid Cases | 106 | | |

a. 5 cells (41.7%) have expected count less than 5. The minimum expected count is 1.47.

**Πίνακας 6.4:** Chi- Square Tests επίπεδο εκπαίδευσης – εξοικείωση χρήσης βιομετρικών στοιχείων

Από τον πιο πάνω **πίνακα 6.4** παρατηρούμε ότι για το Pearson Chi-Square το **sig=.000<0.005**, άρα ισχύει η Η1 υπόθεση ότι δηλαδή οι δύο μεταβλητές είναι εξαρτημένες. Έτσι το επίπεδο εκπαίδευσης εξαρτάται από το πόσο εξοικειωμένοι μπορεί να είναι οι χρήστες με τη χρήση βιομετρικών στοιχείων οπόταν υπάρχει σημαντικά στατιστική συσχέτιση.

Όσον αφορά εάν συσχετίζεται το **επίπεδο εκπαίδευσης** με το αν θεωρείτε **ασφαλές το online banking** ορίστηκαν οι πιο κάτω υποθέσεις:

**α=**0.005

**H0:** Το επίπεδο εκπαίδευσης δεν εξαρτάται από το αν πιστεύουν ότι είναι ασφαλές το online banking

**H1:** Το επίπεδο εκπαίδευσης εξαρτάται από το αν πιστεύουν ότι είναι ασφαλές το online banking

**Ερώτηση 3: Επίπεδο εκπαίδευσης * Ερώτηση 8: Πιστεύετε ότι το online banking είναι ασφαλές; Crosstabulation**

Count

| | | Ερώτηση 8: Πιστεύετε ότι το online banking είναι ασφαλές; | | |
|---|---|---|---|---|
| | | Ναι | Όχι | Total |
| Ερώτηση 3: Επίπεδο εκπαίδευσης | Μεταπτυχιακός τίτλος ή Διδακτορικό | 38 | 6 | 44 |
| | Πανεπιστημιακή εκπαίδευση | 37 | 12 | 49 |
| | Απολυτήριο Λυκείου | 10 | 3 | 13 |
| Total | | 85 | 21 | 106 |

**Πίνακας 6.5:** Επίπεδο εκπαίδευσης * ασφαλές online banking

**Chi-Square Tests**

| | Value | df | Asymptotic Significance (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 1.818[a] | 2 | .403 |
| Likelihood Ratio | 1.879 | 2 | .391 |
| Linear-by-Linear Association | 1.284 | 1 | .257 |
| N of Valid Cases | 106 | | |

a. 1 cells (16.7%) have expected count less than 5. The minimum expected count is 2.58.

**Πίνακας 6.6:** Chi- Square Tests επίπεδο εκπαίδευσης – ασφαλές online banking

Σύμφωνα με τα αποτελέσματα του πιο πάνω **πίνακα 6.6** στο Pearson Chi- Square το **sig=.403 > 0.005** άρα αποδεχόμαστε τη Η0 υπόθεση ότι δηλαδή το επίπεδο εκπαίδευσης δεν εξαρτάται από το εάν θεωρείται πιο ασφαλές το online banking.

## 6.4 Συμπεράσματα

Με βάση την πιο πάνω δειγματοληπτική έρευνα και τις συσχετίσεις, μπορούμε να εξάγουμε κάποια βασικά συμπεράσματα σχετικά με τη γνώση των χρηστών όσον αφορά τις βιομετρικές μεθόδους, το πόσο συχνά χρησιμοποιούν το online banking και κατά πόσο πιστεύουν ότι είναι ασφαλές. Λόγω του μικρού δείγματος της έρευνας τα συμπεράσματα που προκύπτουν αφορούν τα μέλη του δείγματος που έχουν εξεταστεί και δεν αντανακλούν τη γενική γνώμη ολόκληρου του πληθυσμού.

Κάνοντας αρχή από τα δημογραφικά στοιχεία, το ποσοστό των ερωτηθέντων ήταν μεταξύ 26-33 ετών, γεγονός που υποδηλώνει ότι είναι ώριμοι χρήστες του online banking. Όσο αφορά το εκπαιδευτικό τους υπόβαθρο, οι πλείστοι είναι απόφοιτοι τριτοβάθμιας εκπαίδευσης και είναι ιδιαίτερα εξοικειωμένοι με τη χρήση βιομετρικών μεθόδων.

Έπειτα, ρωτήθηκαν κατά πόσο γνωρίζουν τους εφτά τρόπους συμπεριφορικής και φυσιολογικής βιομετρικής αναγνώρισης που τους είχαν τεθεί στο ερωτηματολόγιο. Στο σημείο αυτό, παρατηρούμε πως οι κλασσικοί φυσιολογικοί μέθοδοι όπως τα δακτυλικά αποτυπώματα, η αναγνώριση προσώπου, ίριδας και φωνής είναι τα δημοφιλέστερα. Χρησιμοποιούνται πολύ πιο συχνά σε αντίθεση με τη μέτρηση και καταγραφή των προτύπων ανθρώπινης συμπεριφοράς και την αναγνώριση φλέβας που δεν τα χρησιμοποιούν καθόλου. Ως πιο φιλικά προς τους χρήστες παρατηρούνται τα δακτυλικά αποτυπώματα και η αναγνώριση προσώπου λόγω της υποσυνείδητης χρήσης τους για μεγαλύτερη αξιοπιστία και επαλήθευση από τις κρατικές αρχές. Παράλληλα, βλέπουμε να επικρατεί αρκετό ενδιαφέρον από το κοινό προς τα συμπεριφορικά βιομετρικά ιδιαίτερα γιατί γνωρίζουν ορισμένα από αυτά. Με τη σωστή ενημέρωση πάνω στη χρήση και την εφαρμογή τους θα κερδίσουν το ενδιαφέρον και θα στραφεί περαιτέρω κοινό προς το μέρος τους.

Εντούτοις, στην επόμενη ερώτηση παρατηρούμε ότι για όλες τις βιομετρικές μεθόδους επικρατεί μεγάλο ενδιαφέρον για την επαλήθευση της ταυτότητας. Μάλιστα τα αποτελέσματα έδειξαν πως η χρήση βιομετρικών μεθόδων στις συναλλαγές είναι πιο ασφαλείς από τους κωδικούς πρόσβασης αφού θα εξαλείψουν την ανάγκη να θυμούνται πολλαπλούς κωδικούς πρόσβασης και PIN. Γενικά οι ερωτηθέντες αντιλαμβάνονται ότι το βιομετρικά συστήματα είναι ταχύτερα και ευκολότερα από τους κωδικούς πρόσβασης. Αντίθετα, μεγάλη ανησυχία επικρατεί για το αν θα διαρρεύσουν ευαίσθητα προσωπικά δεδομένα και αν ο βιομετρικός έλεγχος ταυτότητας δεν θα λειτουργήσει.

Στην ερώτηση για το που θα εμπιστεύονταν την αποθήκευση των βιομετρικών τους στοιχείων, οι πλείστοι απάντησαν σε κανέναν, ενώ στην ερώτηση από τι θα απομακρύνονταν εάν δεν τους προσφερόταν στο μέλλον βιομετρική ταυτοποίηση οι περισσότεροι απάντησαν την τράπεζά τους. Αυτό υποδηλώνει πως οι τράπεζες θεωρούνται αναξιόπιστοι οργανισμοί. Συνεπώς αν δεν βελτιώνουν συνεχώς τις υπηρεσίες τους για περισσότερη ασφάλεια το κοινό θα απομακρύνεται από αυτές.

Εντύπωση αποτελεί το γεγονός ότι μία πολύ μικρή μερίδα των ερωτηθέντων δεν γνώριζε και δεν χρησιμοποιεί κανένα από τα βιομετρικά στοιχεία. Αυτό είναι κάτι που μας προβληματίζει καθώς επικρατεί μία δυσπιστία ως προς την αποδοχή των βιομετρικών μεθόδων. Καταλήγουμε επομένως, ότι εκτός από γνωστοποίηση απαιτείται και ενημέρωση του κοινού για τις νέες τεχνολογίες αν πραγματικά θέλουμε να υιοθετηθούν στις τραπεζικές συναλλαγές. Αν βελτιωθούν οι υπηρεσίες που προσφέρει το online banking θα αποκτηθεί η εμπιστοσύνη προς τις τράπεζες και θα υιοθετηθούν ευκολότερα οι βιομετρικές τεχνολογίες.

# Κεφάλαιο 7
# Βιομετρικά Συστήματα Παρόν και Μέλλον

## 7.1 Υιοθέτηση των Βιομετρικών Μεθόδων στις Τραπεζικές Υπηρεσίες

Μολονότι παρατηρείται καθημερινά αύξηση στις ηλεκτρονικές τραπεζικές συναλλαγές, η υιοθέτηση βιομετρικών μεθόδων για σκοπούς ταυτοποίησης των τελικών χρηστών από διάφορες τραπεζικές υπηρεσίες βρίσκεται ακόμη σε πρώιμο στάδιο [25]. Η ηλεκτρονική τραπεζική έχει στρέψει όλο και περισσότερο κοινό στις ψηφιακές πληρωμές χάριν στην ευκολία μέσω των έξυπνων μεθόδων που διαθέτει. Οι πελάτες ανεξαρτήτως του που βρίσκονται έχουν τη δυνατότητα μέσω διαφόρων εφαρμογών, να έχουν πρόσβαση στους τραπεζικούς τους λογαριασμούς και να εκτελούν τις τραπεζικές τους συναλλαγές από οποιαδήποτε φορητή συσκευή (π.χ. κινητά τηλέφωνα, tablets) με μεγαλύτερη άνεση. Η εμπιστοσύνη των πελατών ως προς τη διάπραξη των συναλλαγών τους από την οθόνη της ψηφιακής συσκευής τους, δίνει στις τράπεζες το κίνητρο να βελτιώσουν τις διάφορες υπηρεσίες τους. Αυτό είναι κάτι που βοηθά ώστε να παρέχουν ανταγωνιστικά πλεονεκτήματα στην εξυπηρέτηση των πελατών, καλύπτοντας παράλληλα και τις ανάγκες των χρηστών.

Ωστόσο, η τάση αυτή έχει πολλαπλασιάσει την ευπάθεια των τραπεζικών συστημάτων και έχει προσελκύσει την απειλή των επιθέσεων στο κυβερνοχώρο. Πλέον οι εγκληματίες δεν ακολουθούν τις παραδοσιακές τεχνικές για τις επιθέσεις τους αλλά κάνουν χρήση πολύ πιο εξελιγμένων τεχνολογιών για να χτυπήσουν ευάλωτα συστήματα και δίκτυα. Στόχος τους είναι η διάπραξη απάτης για υποκλοπή της ταυτότητας μέσα από τις πλατφόρμες ηλεκτρονικής τραπεζικής. Τα μέτρα ασφαλείας που διαθέτουν τα τραπεζικά συστήματα παρόλο που βελτιώνονται συνεχώς, τα αρχικά πρωτόκολλα που εξαρτώνταν

από τους κωδικούς πρόσβασης καθιστούσαν τα συστήματα πιο εύθραυστα και δεν μείωναν την ευπάθεια των τραπεζικών λογαριασμών. Παλιότερα για την ταυτοποίηση ενός προσώπου οι τράπεζες απαιτούσαν από τους πελάτες να παρουσιάζουν την ταυτότητά τους, όπου βάση της φωτογραφίας τους θα πραγματοποιούσαν την πιστοποίηση των πελάτων. Όπως έχει φανεί με τη πάροδο του χρόνου, η μέθοδος αυτή έχει σφυρηλατηθεί από κακόβουλους εγκληματίες λόγω του ότι μπορούσαν να εκτυπώσουν ταυτότητες και έγγραφα ως αποδεικτικά ταυτοποίησης. Δεδομένου ότι οι τράπεζες έχουν μεγάλη βαρύτητα στη σταθερότητα μίας χώρας, η επιτυχία έγκειται στο θεσμό αυστηρότερων μέτρων για εξασφάλιση εμπιστοσύνης των πελατών ηλεκτρονικής τραπεζικής, για να μπορεί να ανιχνεύεται η απάτη και να αποτρέπονται οι εγκληματίες από πιθανές επιθέσεις στους λογαριασμούς των χρηστών.

Η ανάγκη λοιπόν για πιο αξιόπιστους ελέγχους και αναδιάρθρωση των τεχνικών ταυτοποίησης προσελκύει την αξιοποίηση βιομετρικών μεθόδων στην ασφάλεια του online banking. Τα βιομετρικά στοιχεία είναι μοναδικά και δύσκολα μπορούν να αναπαραχθούν. Σε αντίθεση με τους κωδικούς πρόσβασης ή τους αριθμούς PIN, μπορούν να επαληθεύσουν τις συναλλαγές με κάτι που είναι έμφυτο στο χρήστη. Ως εκ τούτου, οι βιομετρικές μέθοδοι επιτρέπουν στα τραπεζικά ιδρύματα την ανάπτυξη ταχύτερων και αποτελεσματικότερων μεθόδων παρέχοντας έτσι ασφαλέστερους και απλούστερους μεθόδους για την σύνδεση και την πραγματοποίηση των online συναλλαγών τους.

### 7.1.1 Η χρήση βιομετρίας προσθέτει αξία στο online banking

Μιας και οι κινητές συσκευές αποτελούν πλέον προέκταση του χεριού μας, ωθούν τις τράπεζες στο να βρίσκουν ολοένα και περισσότερες καινοτόμες εφαρμογές για την πρόσβαση στα τραπεζικά τους συστήματα μέσω των κινητών συσκευών. Ταυτόχρονα, παραμονεύουν οι εγκληματίες που στοχεύουν στις πλατφόρμες online banking και εδώ είναι το σημείο στο οποίο θα πρέπει η βιομετρία να προσθέσει αξία στην ηλεκτρονική τραπεζική. Γνωρίζοντας πως τα βιομετρικά δεδομένα δύσκολα μπορούν να ξεχαστούν ή να μοιραστούν, μειώνεται ο κίνδυνος να κλαπούν δεδομένου ότι εφαρμόζονται οι κατάλληλες μέθοδοι ασφάλειας στα τραπεζικά συστήματα. Κάνοντας τις απαραίτητες τροποποιήσεις τους, οι τραπεζικοί οργανισμοί μπαίνουν σιγά σιγά σε ψηφιακούς ρυθμούς. Αν αυτό συνδυαστεί με βιομετρικές μεθόδους, τότε μπορούν να βοηθήσουν τους πελάτες ώστε να τους παρέχουν περισσότερη ασφάλεια στις ηλεκτρονικές τους συναλλαγές.

Αρκετοί οργανισμοί άρχισαν να αξιοποιούν τις βιομετρικές τεχνολογίες μαζί με τις έξυπνες συσκευές που έχον ενσωματωμένη υποστήριξη βιομετρικών μεθόδων. Είδη οι μεγαλύτεροι κατασκευαστές έξυπνων κινητών συσκευών, έχουν ενσωματώσει στις συσκευές αισθητήρες που ενεργοποιούνται με το δακτυλικό αποτύπωμα ή με την αναγνώριση προσώπου για την επαλήθευση της ταυτότητας των χρηστών [26].
Η βιομετρία είναι ο προσωπικός κωδικός πρόσβασης ενός ατόμου που δεν δύναται να ξεχαστεί ή να χαθεί. Έτσι κάνοντας χρήση των βιομετρικών χαρακτηριστικών ενός πελάτη, τα συστήματα online banking απλοποιούν τη διαδικασία εκτέλεσης ηλεκτρονικών πληρωμών και το έλεγχο ταυτότητας των online αγορών. Η ταχύτητα και η ευελιξία των συναλλαγών είναι ένας σημαντικός παράγοντας ως προς στην εμπιστοσύνη των πελατών προς την τράπεζα, καθώς δεν απαιτείτε από τους χρήστες να θυμούνται κωδικούς πρόσβασης και ερωτήσεις ασφαλείας.

Επιπλέον, οι τραπεζικοί οργανισμοί έχουν εισάγει νέες έξυπνες βιομετρικές κάρτες εφαρμόζοντας τα ίδια πρότυπα που διαθέτουν οι κλασσικές κάρτες, με τη διαφορά ότι έχουν ενσωματωμένους αισθητήρες. Όταν ένας πελάτης έχει στην κατοχή του μία τέτοια κάρτα, έχει τη δυνατότητα να χρησιμοποιήσει το δακτυλικό του αποτύπωμα για να την ενεργοποιήσει και να εκτελέσει την ηλεκτρονική του συναλλαγή. Η συναλλαγή που έχει πιστοποιηθεί με τη χρήση βιομετρικών στοιχείων συμβάλει στο να επιβεβαιωθεί ότι είναι ο ίδιος ο πελάτης που έχει ζητήσει την εκτέλεση της εκάστοτε συναλλαγής.
Σε διάφορες χώρες όπως στην Ιαπωνία, την Βραζιλία αλλά και στην Ευρώπη όπως είδη τίθεται στην Πολωνία, έχουν εισαχθεί ΑΤΜ με βιομετρική πιστοποίηση διαθέτοντας τις ίδιες λειτουργίες για ανάληψη ή κατάθεση μετρητών [27]. Πρόκειται για συστήματα που η ταυτοποίηση λειτουργεί με την τεχνολογία αναγνώρισης φλέβας δακτύλου, δηλαδή ανιχνεύεται το πρότυπο των φλεβών που διέρχονται κάτω από την επιφάνεια του δέρματος και μετά διασταυρώνεται με το καταχωρημένο προφίλ για την πιστοποίηση της ταυτότητας του ατόμου.
Η μετάβαση σε βιομετρικά συστήματα όπως φαίνεται απλοποιεί την εμπορεία των πελατών. Ως εκ τούτου, είναι αναγκαία η υιοθέτηση αυτού του είδους τεχνολογίας για την έγκριση συναλλαγών, δεδομένου πως στην παρούσα φάση τίποτα δεν θα μπορούσε να είναι ασφαλέστερο πέρα από τη χρήση σωματικών χαρακτηριστικών.

### 7.1.2 Η χρήση βιομετρίας ως θετικό πρόσημο στο online banking

Καθώς προχωράμε σε ένα πιο συνδεδεμένο και online κόσμο, η βιομετρική τεχνολογία γίνεται ολοένα και πιο δημοφιλής. Για να αποδειχθεί με βεβαιότητα η ταυτότητά μας στις ηλεκτρονικές πληρωμές χρειάζονται πιο αποτελεσματικοί τρόποι που να έχουν εφαρμογές και στο μέλλον.
Εκτός από τις γνωστές μεθόδους πιστοποίησης υπάρχει μία πληθώρα μεθόδων που μπορούν να εφαρμοστούν από τα τραπεζικά συστήματα. Μία από αυτές είναι η βιομετρία πληκτρολόγησης (keystroke biometrics) η οποία μπορεί να αναπτυχθεί για την επαλήθευση ενός ατόμου στο online banking. Ο ρυθμός δακτυλογράφησης αποτελεί ένα μοναδικό πρότυπο βιομετρικής πιστοποίησης δεύτερης γενιάς. Είναι ουσιαστικά μία μέθοδος όπου εύκολα μπορεί να αναπτυχθεί και να χρησιμοποιηθεί για εξακρίβωση στοιχείων. Τα δεδομένα από την πληκτρολόγηση καταγράφονται, αποθηκεύονται και στην πορεία όταν ζητηθεί διασταυρώνονται και γίνεται η σύγκρισή τους με τα δεδομένα που είναι είδη στη βάση του κάθε συστήματος.

Επιπλέον, υπάρχει ένα ποσοστό πελατών όπου αδυνατεί είτε γιατί δεν πληροί τις απαιτήσεις αναγνώρισης των τραπεζικών συστημάτων είτε γιατί δεν έχουν τύχει της απαραίτητης εκπαίδευσης στο να διεκπεραιώνουν online τις συναλλαγές τους. Σε τέτοιες περιπτώσεις, με τη βιομετρική αναγνώριση φωνής (voice recognition) δίνεται η δυνατότητα απλοποίησης της διαδικασίας ταυτοποίησης. Μέσω των κινητών τους τηλεφώνων, οι χρήστες μπορούν να χρησιμοποιούν το μικρόφωνο της συσκευής τους και να μιλάνε στο σύστημα αναγνώρισης. Το σύστημα όταν τους αναγνωρίσει και επαληθευτεί η ταυτότητά τους, τους επιτρέπει να εκτελέσουν τις συναλλαγές τους και να αυτοεξυπηρετηθούν.

Συνεπώς, η υιοθέτηση βιομετρικών μεθόδων σε συνδυασμό με την αποδοχή από τους πελάτες επιταχύνει και βελτιώνει τη λειτουργία των υπηρεσιών. Ταυτόχρονα προσφέρει μεγαλύτερα οφέλη και ανώτερη τραπεζική εμπειρία μέσω εξατομικευμένης και απαιτούμενης δέσμευσης.

## 7.2 Το σώμα μας- η Ταυτότητά μας

Τα βιομετρικά συστήματα έχουν μετατρέψει το ανθρώπινο σώμα σε κωδικό πρόσβασης για να «ξεκλειδώνει» διάφορα δημόσια και ιδιωτικά συστήματα [28]. Η ζωή μας σύντομα θα μετατραπεί και θα συμβαδίζει με την εξέλιξη της πρωτοποριακής βιομετρικής τεχνολογίας.

Είδη εκατομμύρια από εμάς χρησιμοποιούν ως μοναδικά αναγνωριστικά τα δακτυλικά τους αποτυπώματα ή την αναγνώριση προσώπου για την πρόσβαση είτε στο κινητό μας τηλέφωνο είτε κατά τον έλεγχο των διαβατηρίων σε κάποιο αεροδρόμιο. Οι χιλιάδες επιβάτες που καθημερινά ταξιδεύουν στο εξωτερικό, περνούν από έλεγχο αναγνώρισης προσώπου, ειδάλλως σε περίπτωση που το σύστημα δεν μπορεί να τους αναγνωρίσει εξετάζονται από τους υπαλλήλους του αερολιμένα.

Επιπλέον, η παρακολούθηση μέσω βίντεο (κλειστών κυκλωμάτων παρακολούθησης-cctv) έχει αυξηθεί τα τελευταία χρόνια. Τόσο σε τράπεζες και αεροδρόμια όσο και σε διάφορους άλλους δημόσιους χώρους, εφαρμόζονται για την ανίχνευση εγκληματιών μέσα από τις εικόνες που συλλέγουν και την αντιστοίχισή τους με τις είδη αποθηκευμένες ψηφιακές φωτογραφίες στη Βάση Δεδομένων.

Ορισμένα συστήματα έχουν είδη αποτελέσει εμπορικές επιτυχίες χάρη στην ασφάλεια που παρέχουν προς τους καταναλωτές. Οι εργαζόμενοι σε ορισμένες εταιρίες ιδιωτικού τομέα σαρώνουν αντί για τις κάρτες ωραρίου την παλάμη τους κατά την είσοδο ή την έξοδό τους στο κτίριο της εταιρείας. Η γεωμετρία του χεριού τους, αποτρέπει την εξαπάτηση στις περιπτώσεις που ένας εργαζόμενος μπορούσε να κτυπήσει την κάρτα ενός άλλου συναδέλφου του για να ξεγελάσει το σύστημα αλλά και τον εργοδότη του. Στον εργασιακό χώρο, η επιτήρηση έχει αυξηθεί εξαιτίας του ότι πολλοί εργοδότες παρακολουθούν την κάθε κίνηση των υπαλλήλων τους. Για να διαπιστώσουν εάν οι εργαζόμενοι εκτελούν τα καθήκοντά τους, παρακολουθούν τα emails, τα τηλέφωνα ακόμη και το τι πληκτρολογούν ώστε να δημιουργήσουν ένα προφίλ για τη συμπεριφορά του καθενός. Κάθε τους ενέργεια για συλλογή βιομετρικών δεδομένων είναι απαραίτητη όπως ισχυρίζονται για την προώθηση της επιτυχίας της επιχείρησής τους. Βέβαια, πολλοί ειδικοί δεν συμφωνούν με την γνώμη των εταιρειών που θεωρούν ότι είναι αδύνατο να ξεγελαστούν τα συστήματα τους και τα βιομετρικά δεδομένα δεν θα χρησιμοποιηθούν από τους χάκερς για να εισβάλουν στα «ασφαλή» κατά αυτούς δίκτυα.

Ίσως η βιομετρική τεχνολογία να είναι πολύ πιο διαδεδομένη στο εξωτερικό, εντούτοις στη χώρα μας δεν έχει ακόμη τεθεί σε ισχύ και εξακολουθεί να συνδυάζεται με τις παραδοσιακές μεθόδους λόγω της δυσπιστίας των χρηστών. Για παράδειγμα, η αναγνώριση δακτυλικού αποτυπώματος μπορεί να έχει αρνητική προδιάθεση εξαιτίας του ότι πολλοίς κόσμος την συσχετίζει με τους εγκληματίες και την επιβολή του νόμου. Το βιομετρικό χαρακτηριστικό που ενδέχεται να προσφέρει πιο ακριβή στοιχεία ταυτοποίησης είναι η μέθοδος DNA, όπου δίνει πληροφορίες σχετικά με την κατάσταση υγείας ή ακόμη και την εθνικότητα ενός ατόμου. Το ενδεχόμενο αυτό, πιθανόν να έφερνε σε δύσκολη θέση ορισμένα άτομα διότι θα μπορούσαν να πέσουν θύματα φυλετικών διακρίσεων αλλά και να διέρρεαν ευαίσθητες πληροφορίες που το άτομο δεν θα ενέκρινε, λόγου χάρη το ιατρικό του ιστορικό.

Αξίζει να σημειωθεί πως ότι συμβαίνει με τις υπόλοιπες τεχνολογίες έτσι και στις βιομετρικές, επικρατούν ανησυχίες όπου εστιάζονται κυρίως στην παραβίαση της ιδιωτικής ζωής των χρηστών. Η μη ελεγχόμενη χρήση της τεχνολογίας ενδέχεται να χρησιμοποιηθεί ως μορφή κοινωνικού ελέγχου κυρίως σε δημόσιους χώρους λόγω του ότι αποτελεί σοβαρή απειλή για την ιδιωτικότητα. Με δεδομένο ότι τα βιομετρικά στοιχεία είναι αναγνωριστικά υψηλής ακεραιότητας, αποτελούν απειλή για τη προστασία της ιδιωτικής ζωής. Ο μεγαλύτερος ίσως κίνδυνος που έχει να κάνει με την ιδιωτική ζωή εγκυμονεί όταν το βιομετρικό δείγμα δίνει περισσότερα στοιχεία από την ταυτότητα του ίδιου του ατόμου.

### 7.2.1 Εξαπάτηση συσκευών αναγνώρισης βιομετρίας

Η τεχνολογία προχωράει, το ίδιο και όσοι επιθυμούν να εισβάλλουν στις προσωπικές πληροφορίες και να εξαπατήσουν τα βιομετρικά συστήματα αναγνώρισης. Είτε πρόκειται για την αναγνώριση δακτυλικών αποτυπωμάτων, είτε για την αναγνώριση φωνής, ίριδας ή αμφιβληστροειδούς είναι αποδεδειγμένο πως η βιομετρική ταυτοποίηση μπορεί να «ξεγελαστεί». Πολλές μελέτες έχουν δήξει πως με ορισμένες απλές δοκιμές και με χρήση εργαλείων που διατίθενται στην αγορά κάτι τέτοιο είναι σίγουρα εφικτό.

Κάνοντας αρχή με τα δακτυλικά αποτυπώματα, θα μπορούσαν να αναπαραχθούν με τη χρήση σιλικόνης κάτι που έχει αποδειχθεί από τη μελέτη που έγινε το 2002 από τον Ιάπωνα καθηγητή κρυπτογραφίας και μαθηματικών κ. Tsutomu Matsumoto μαζί με τους φοιτητές του στο πανεπιστήμιο της Γιοκοχάμα [29].
Η ομάδα πραγματοποίησε δύο πειράματα αποδεικνύοντας τη δυνατότητα εξαπάτησης χρησιμοποιώντας ένα αντίγραφο δακτυλικού αποτυπώματος. Στο πρώτο πείραμα δημιούργησαν ένα καλούπι από ζελατίνη και πίεσαν το δάκτυλο τους πάνω στο πλαστικό. Μετά από τις δοκιμές που έγιναν χρησιμοποιώντας το πλαστό δάκτυλο κατάφεραν να εξαπατήσουν τον ανιχνευτή σε ποσοστό 80%.
Στο δεύτερο πείραμα αντέγραψαν ένα δακτυλικό αποτύπωμα από την επιφάνεια ενός ποτηριού για να αποδείξουν το σενάριο πως δεν είναι απαραίτητη η συγκατάθεση του κατόχου του αποτυπώματος για να αναγνωριστεί η ταυτότητά του.
Το δακτυλικό αποτύπωμα για να μπορέσει να μελετηθεί έπρεπε να ενισχυθεί μέσω μίας ειδικής κόλλας ώστε να κολληθεί πάνω στα νεκρά κύτταρα και ακολούθως να φωτογραφηθεί με ψηφιακή μηχανή. Η εικόνα στην συνέχεια βελτιώθηκε μέσω ενός ειδικού προγράμματος επεξεργασίας εικόνας και εκτυπώθηκε σε μία διαφάνεια ώστε να δημιουργηθεί το αντίγραφο για τη δοκιμή. Όπως και στο πρώτο πείραμα έτσι και σε αυτό το σύστημα εξαπατήθηκε μετά από ένα αριθμό δοκιμών με το ίδιο ποσοστό 80% επιτυχίας.

Επίσης, στην περίπτωση των συστημάτων σαρωτών ίριδας, οι εισβολείς έχουν τη δυνατότητα να τραβήξουν μία φωτογραφία τις ίριδας του ματιού με τη χρήση φωτογραφικής μηχανής σε λειτουργία νυχτερινής λήψης. Για να πετύχουν την παραπλάνηση, εκτυπώνουν τη φωτογραφία σε χαρτί και τοποθετούν έναν υγρό φακό επαφής πάνω στη θέση της ίριδας για να καταφέρει να μιμηθεί την στρογγυλότητα του ματιού. Σε άλλες περιπτώσεις, οι πιο εξειδικευμένοι εισβολείς, μέσω ενός εργαλείου αναγνώρισης βασισμένο σε ένα λογισμικό θα παρήγαγαν ένα κώδικα ίριδας. Ο κώδικας θα μεταβαλλόταν χρησιμοποιώντας ένα γενετικό αλγόριθμο για να δημιουργηθεί ένα ίδιο πρότυπο ίριδας και στη συνέχεια θα εκτυπωνόταν σε ένα φακό επαφής για να σκαναριστεί ώστε να ταυτοποιηθεί από το σύστημα.

## 7.3 Απόρρητο και Καταπάτηση Ανθρωπίνων Δικαιωμάτων-GDPR

Για να είναι μία πληροφορία απόρρητη ή εμπιστευτική επιβάλλεται να είναι σε μία κατάσταση περιορισμένης προσβασιμότητα από πρόσωπα, ομάδες κ.α. [30]. Η έννοια του απορρήτου αποτελεί καθήκον των προσώπων ή των οργανισμών, όπως επίσης η φύλαξη και η μη προσπέλαση ορισμένων πληροφοριών που τους έχουν εμπιστευτεί ή κατέχουν λόγω της αρμοδιότητάς τους. Ουσιαστικά, τοποθετεί φραγμούς σε τρίτους από το να μην γνωρίζουν, ή να επεξεργάζονται δεδομένα εάν δεν προσδιορίζεται ο λόγος χρήσης τους ή εφόσον δεν προβλέπεται κάποιος νόμος που να επιτρέπει την παύση του απορρήτου ιδιωτικότητας. Γνωρίζοντας ότι τα βιομετρικά στοιχεία είναι εκ φύσεως ιδιαίτερα ευαίσθητα, χρήζουν ειδικής διαφύλαξης καθότι η επεξεργασία τους θα δημιουργούσε σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και την ελευθερία του ατόμου.

Από τις 25 Μαΐου 2018 που έχει τεθεί σε ισχύ ο Ευρωπαϊκός γενικός κανονισμός ΕΕ/2016/679 περί προστασίας προσωπικών δεδομένων γνωστός ως General Data Protection Regulation (GDPR) επιβλήθηκαν αλλαγές ως προς τον τρόπο που οι οργανισμοί συλλέγουν, επεξεργάζονται και αποθηκεύουν κάθε μορφής προσωπικά δεδομένα [31]. Βάση του νέου κανονισμού, απαγορεύεται η επεξεργασία βιομετρικών δεδομένων με σκοπό την ταυτοποίηση προσώπου. Η οποιαδήποτε επεξεργασία επιτρέπεται κατ' εξαίρεση βάσει του άρθρου 9 παράγραφος 2 του γενικού κανονισμού για χρήση βιομετρικών δεδομένων κατόπιν συναίνεσης του υποκειμένου των δεδομένων. Ο γενικός κανόνας προσωπικών δεδομένων ορίζει αυστηρούς κανονισμούς με σκοπό τη διασφάλιση του υποκειμένου των δεδομένων, δηλαδή το αν κατανοεί το λόγο που έχει δώσει την συγκατάθεσή του. Εφόσον έχει δοθεί η συγκατάθεση τότε μπορούν τα δεδομένα να τύχουν επεξεργασίας μόνο για το σκοπό τον οποίο δόθηκε η άδεια.

Ο περί της προστασίας των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και της ελεύθερης κυκλοφορίας των δεδομένων νόμος (Ν.125(Ι)/2018), κατοχυρώνει τα δικαιώματα των ατόμων περί της επεξεργασίας των προσωπικών τους δεδομένων και θέτει συγκεκριμένες υποχρεώσεις σε όσους διαχειρίζονται τις προσωπικές πληροφορίες [32].

Η κυριότερη ίσως υποχρέωση είναι η λήψη των καταλληλότερων τεχνικών αλλά και οργανωτικών μέτρων για τη διαφύλαξη της ασφάλειας των δεδομένων που τυγχάνουν επεξεργασίας. Βάσει του νόμου, τα μέτρα πρέπει να εξασφαλίζουν ένα υψηλό επίπεδο ασφάλειας έναντι των κινδύνων που συνεπάγονται από την επεξεργασία των δεδομένων. Θα πρέπει να διασφαλίζεται η μη εξουσιοδοτημένη πρόσβαση στις Βάσεις Δεδομένων όπου αποθηκεύονται τα προσωπικά στοιχεία και σε όσους έχουν πρόσβαση να διασφαλίζεται ότι δεν θα διαρρεύσουν σε τρίτους. Όσον αφορά την επεξεργασία βιομετρικών δεδομένων, πρέπει να επιλέγεται ο λιγότερο παρεμβατικός τρόπος επεξεργασίας που να σέβεται την ιδιωτικότητα και την προσωπικότητα των ατόμων.

Σε συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων για παράδειγμα, που χρησιμοποιούνται από εργοδότες για να ελέγχουν την ώρα προέλευσης στο χώρο εργασίας, θεωρείται υπερβολικό μιας και μπορεί να επιτευχθεί με λιγότερο παρεμβατικά μέσα. Σε αντίθεση περίπτωση τέτοια συστήματα μπορούν να επιτραπούν σε χώρους όπου η είσοδος θεωρείται υψίστης ασφαλείας.
Από μεριάς τους οι χρήστες διατηρούν το δικαίωμα να λαμβάνουν πληροφορίες για το ποιος και γιατί τυγχάνουν επεξεργασίας τα προσωπικά τους δεδομένα. Με εφαρμογή το GDPR επιτρέπεται να ζητούν οι ίδιοι να τους δίνεται πρόσβαση και να γνωρίζουν ποια στοιχεία τους διατηρούνται στα συστήματα του εκάστοτε οργανισμού ενώ έχουν το δικαίωμα να απαιτούν τη διαγραφή τους.

Παράλληλα να σημειωθεί πως οι νόμοι δεν σημαίνουν το τέλος των βιομετρικών μεθόδων, αλλά υφίστανται για να δίνουν οι οργανισμοί την απαραίτητη προσοχή τους στο νομοθετικό πλαίσιο. Εν κατακλείδι, κρίνεται αναγκαία η δημιουργία κατάλληλων προοπτικών και μέτρων ασφάλειας, τόσο σε Ευρωπαϊκό όσο και σε κρατικό επίπεδο ώστε τα δεδομένα να προστατεύονται και να διαφυλάσσονται από αθέμιτη καταστροφή, απώλεια, απαγορευμένη διάδοση ή πρόσβαση και από κάθε μορφή παράνομης επεξεργασίας [15].

# Κεφάλαιο 8
# Επίλογος

## 8.1 Αποτίμηση Βιομετρικής Τεχνολογίας

Αναλύοντας τις κυριότερες βιομετρικές μεθόδους καθώς και τις εφαρμογές τους στα προηγούμενα κεφάλαια είναι αναπόφευκτο το γεγονός της αποτίμησής τους. Τα μεγαλύτερα ίσως θέματα που απασχολούν το ευρύ κοινό, είναι κατά πόσο μπορούν να επηρεάσουν την καθημερινότητά μας και ποιο ή ποια από αυτά μπορεί να θεωρηθεί ως το καταλληλότερο βιομετρικό σύστημα. Η βιομετρική τεχνολογία έχει μπει για τα καλά στη ζωή μας. Χρησιμοποιείται καθημερινά από μία μεγάλη μερίδα του πληθυσμού για τον έλεγχο πρόσβασης, τις ηλεκτρονικές πληρωμές και την επαλήθευση της ταυτότητας. Έχει κερδίσει έδαφος καθώς συνδυάζει την ευκολία με την ασφάλεια οπόταν όλο και περισσότεροι τομείς προσπαθούν να την υιοθετήσουν. Τα περισσότερα συστήματα βιομετρικής αναγνώρισης διευκολύνουν το χρήστη από το να θυμάται κωδικούς πρόσβασης και ταυτόχρονα εξοικονομά χρόνο και χρήμα.

Είναι φανερό πως παρά τις τεράστιες δυνατότητες που προσφέρει, η βιομετρία εκφράζει και ανησυχίες για το ποιο σύστημα είναι το καλύτερο βάση κριτηρίων ώστε να γίνει αποδεκτό από το κοινό. Για να απαντηθεί αυτό το ερώτημα καταρχάς θα πρέπει να καθοριστεί η εφαρμογή της βιομετρικής μεθόδου που θα χρησιμοποιηθεί, μετά να εξακριβωθούν οι προτεραιότητές της και έπειτα να προσαρμόζεται βάσει το κόστος, το επίπεδο ακρίβειας, την διακριτικότητα και την προσπάθεια που καταβάλλει ο χρήστης.

Τα βιομετρικά στοιχεία εγείρουν διάφορα ερωτήματα και γεννούν αρκετές αμφιβολίες σε όλους μας. Τα επόμενα χρόνια σίγουρα θα δημιουργηθούν ανησυχίες γύρω από την ιδιωτική μας ζωή ή την αποτυχία των συστημάτων και είναι αδιαμφισβήτητο ότι θα προκληθεί μεγάλη συζήτηση για την πρόοδο της βιομετρικής τεχνολογίας.

Για τους λόγους αυτούς δεν έχει υιοθετηθεί εξ ολοκλήρου το online-banking από όλο το μέγεθος των πελατών, όμως είναι σχεδόν σίγουρο ότι με το πέρασμα του χρόνου και με τη συνεχής τεχνολογική εξέλιξη η χρήση του θα εδραιωθεί καθολικά. Αυτό το οποίο δυνάμεθα να ελπίζουμε είναι κατά πόσο θα μπορέσουμε να αναγνωρίσουμε τους περιορισμούς αλλά και τη δύναμη της τόσο συναρπαστικής τεχνολογίας βιομετρικών στοιχείων.

## 8.2 Ανοικτά Ερευνητικά Ερωτήματα και Θέματα

Εάν αναλογιστούμε το μέγεθος των πραγμάτων που καθημερινά χρησιμοποιούνται για τον έλεγχο πρόσβασης σε οτιδήποτε, η βιομετρία μπορεί να χαρακτηριστεί ως το κλειδί για έναν κόσμο χωρίς κλειδιά. Ουσιαστικά η συσκευή πρόσβασης και ο κωδικός είναι ο ίδιος μας ο εαυτός. Ενώ ήδη έχει αναπτυχθεί σε ορισμένες περιοχές όπως στα έξυπνα τηλέφωνα, η ευρεία υιοθέτηση της βιομετρικής τεχνολογίας εξακολουθεί να αντιμετωπίζει ενστάσεις. Όπως συμβαίνει με κάθε νέα τεχνολογία, το ίδιο και στη βιομετρία αντιμετωπίζονται προκλήσεις μαζί με ορισμένες ανησυχίες.

Η πρόληψη απάτης με μεθόδους ταυτοποίησης κυρίως στις συναλλαγές, είναι κάτι που μελετάται διαρκώς. Οι εκτιμήσεις δείχνουν πως η βιομετρική αναγνώριση είναι το μέλλον των πληρωμών. Τα αποτελέσματα μίας πρόσφατης έρευνας της Visa που έλαβε χώρα το στις 12-19 Σεπτεμβρίου 2017 από την AYTM Market Research, μεταξύ 1000 Αμερικανών καταναλωτών, επιβεβαιώνει ότι οι καταναλωτές ενδιαφέρονται για νέες βιομετρικές μεθόδους που κάνουν τη ζωή τους ευκολότερη [33]. Συγκεκριμένα το 86% του δείγματος ενδιαφέρονται να κάνουν χρήση βιομετρίας για επαλήθευση της ταυτότητάς τους ή για πληρωμές, και το 65% είναι είδη εξοικειωμένο με τα βιομετρικά στοιχεία. Πέραν από το 70% πιστεύει ότι η βιομετρία είναι ευκολότερη και το 46% πιστεύουν ότι είναι πιο ασφαλείς από τη χρήση κωδικών πρόσβασης και PIN. Τα αποτελέσματα δείχνουν ότι ο βιομετρικός έλεγχος ανταποκρίνεται στην ανάγκη των πλείστων καταναλωτών εφόσον οι ίδιοι είναι αυτοί που επιλέγουν τη μορφή πληρωμής που θεωρούν πιο βολική και ασφαλείς. Για το λόγο αυτό οι έρευνες για διασφάλιση μαζί με την απλοποίηση των πληρωμών συνεχίζονται και πάνω σε αυτό θα βασιστεί η περαιτέρω εξάπλωσή τους. Όταν η εμπορική τους αποδοχή γίνει μεγαλύτερη, το κόστος παραγωγής τους θα μειωθεί και η χρήση τους θα είναι εντονότερη.

Δεδομένου ότι η συλλογή σε συνδυασμό με την επεξεργασία βιολογικών προτύπων είναι τόσο ακριβείς και μοναδική προκαλεί κοινωνικό σκεπτικισμό. Πολλοί πιστεύουν ότι η καθιέρωση της βιομετρικής τεχνολογίας αποτελεί παραβίαση των πολιτικών ελευθεριών και των συνταγματικών δικαιωμάτων. Η μαζική αποθήκευση βιομετρικών στοιχείων ελλοχεύει τον κίνδυνο και αυξάνει το κόστος παραβίασης των προσωπικών δεδομένων.

Ένα σημαντικό θέμα προς περαιτέρω έρευνα είναι η χρήση βιομετρικών μεθόδων σε μεγάλο εύρος εφαρμογών από άτομα με αναπηρίες. Αποτελεί μοναδική πρόκληση καθώς μελέτες που αξιολογούν τον αντίκτυπο των βιομετρικών μεθόδων σχετικά με την κοινότητα ατόμων με αναπηρία είναι περιορισμένη [34]. Εντούτοις τείνουν να δείχνουν ότι αρκετά άτομα θα βρεθούν αντιμέτωπα με δυσκολίες πρόσβασης στα βιομετρικά συστήματα. Αυτό εγείρει την ανησυχία ότι ενδέχεται να αντιμετωπίσουν αυξημένη δυσκολία πρόσβασης σε υπηρεσίες που απαιτούν την παραγωγή βιομετρικών δεδομένων. Έτσι, καθίσταται απαραίτητο να εφαρμοστούν νομοθετικές δικλείδες για την εξασφάλιση των δικαιωμάτων των ανθρώπων με αναπηρίες, καθώς ολοένα και περισσότερα προγράμματα αρχίζουν να εφαρμόζονται σε ευρεία βάση.

Παρά τις όποιες ενστάσεις, η βιομετρική τεχνολογία είναι ήδη πολύ κοντά. Ζωντανό παράδειγμα αποτελεί ένας Υπολογιστή όπου καταφέρνει να αναγνωρίσει την φωνή του ομιλητή εκτελώντας τις εντολές που του έχουν ειπωθεί. Η βιομετρική φαίνεται πως έχει όλες τις προϋποθέσεις, το ίδιο και τα βιομετρικά συστήματα να εισχωρήσουν στις καθημερινές μας δραστηριότητες. Οι εταιρίες και οι οργανισμοί έχουν επικεντρωθεί σε έρευνες και μεθόδους προκειμένου να είναι σε θέση να ανταπεξέλθουν άμεσα στις οποιεσδήποτε μελλοντικές προκλήσεις. Είναι πανέτοιμες να βοηθήσουν στο να οργανωθούμε και να προστατευθούμε από διάφορες απειλές που ελλοχεύουν. Έπεται να αναμένουμε υψηλότερα ποσοστά υιοθέτησης μαζί με βελτιωμένες τεχνολογίες αναγνώρισης όχι μόνο για πρόσβαση στις προσωπικές συσκευές αλλά και για εξατομίκευση. Το τι θα επικρατήσει είναι αβέβαιο, είναι κάτι που σίγουρα θα φανεί στο άμεσο μέλλον.

# Βιβλιογραφία


[01] Χ. Γκότσης, "Τεχνολογικές εφαρμογές στη λειτουργία των τραπεζών", Αθήνα, Εκδόσεις Σταμούλη, 2007

[02] M. Shah, "E-banking management: Issues, solutions, and strategies: Issues, Solutions, and Strategies", IGI Global, May 2009

[03] Β. Αγγέλης, "Η βίβλος του e-banking", Εκδόσεις Νέων Τεχνολογιών 2005

[04] M. Dixon, B. Nixon, "E-banking: Managing your money and transactions online", Sams, 2000

[05] RK Miryala, "Trends, challenges & innovations in management", Zenon Academic Publishing, vol.3, Mar 2015

[06] Α. Αρχοντάκης, Γ. Κυριακόπουλος, "Οργανωτικός και τεχνολογικός εκσυγχρονισμός του ελληνικού τραπεζικού συστήματος", Αθήνα ΙΝΑ/ ΟΤΟΕ, 1995

[07] J. Chavan, "Internet banking-benefits and challenges in an emerging economy", International Journal of Research in Business Management, vol 1, no. 1, p.p.19-26, June 2013

[08] P. Malhotra, B. Singh, "The impact of internet banking on bank performance and risk: The Indian experience", Eurasian Journal of Business and Economics, vol 2, no. 4, pp.43-62, 2009

[09] Π. Καρεκλής, "Επιπτώσεις του Internet στη λειτουργία και κερδοφορία των επιχειρήσεων, Οφέλη από τη χρήση υπηρεσιών ηλεκτρονικής τραπεζικής", Δελτίο ΕΕΤ, Γ'Τριμηνία, pp.41-52, 2003

[10] J. Gorst-Williams, "Do banks take disability issues seriously", Our consumer expert looks, 2013

[11] Z. Liao, M.T. Cheung, "Internet-based e-banking and consumer attitudes: an empirical study", Information & management, vol. 39, no. 4, pp.283-295, 2002

[12] V.S. Solanki, "Risks in e-banking and their management", International Journal of Marketing, Financial Services & Management Research,vol 1, no. 9, pp.2277-3622, 2012

[13] "FAR and FRR: security level versus users convenience" https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience

[14] Δ. Μαυρογιάννης, "Ασφάλεια ηλεκτρονικών συναλλαγών", Δελτίο ΕΕΤ, Γ' Τριμηνιαία, 2003

[15] Σ.Κάτσικας, Δ.Γκρίτζαλης, Σ.Γκρίτζαλης "Ασφάλεια Πληροφοριακών Συστημάτων", Εκδόσεις Νέων Τεχνολογιών, 2004

[16] A.K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, vol.14, no. 1, pp. 4-20, Jan 2004

[17] Π. Σφυράκης, "Η χρήση των βιομετρικών συστημάτων ως μέσο προστασίας των πολιτών και των πληροφοριών. Η αναγκαιότητα της αποδοχής τους από τους πολίτες", 2008

[18] T. Duarte, J.P. Pimentão, P. Sousa, and S. Onofre. "Biometric access control systems: A review on technologies to improve their efficiency" IEEE International Power Electronics and Motion Control Conference (PEMC), pp. 795-800, Sept 2016

[19] Ε. Μπόβιος, "Σημειώσεις εφαρμοσμένης ασφάλειας πληροφοριακών συστημάτων, για τις διδακτικές ανάγκες του μαθήματος ασφάλεια πληροφοριακών συστημάτων", ΑΤΕΙ Θεσσαλονίκης, 2004

[20] Z. Mirza, E. Alsalem, F. Mohsin, and W.M. Elmedany, "Users Acceptance of Using Biometric Authentication System for Bahrain Mobile Banking", KnE Engineering, pp.102-121, Oct 2018

[21] R.Saini, N.Rana, "Comparison of various Biometric Methods", International Journal of Advances in Science and Technology (IJAST), vol 2, pp. 24-30, Mar 2014

[22] R. Tassabehji, M. A. Kamala, "Evaluating biometrics for online banking: The case of usability", International Journal of Information Management: The Journal for Information Professionals, vol 32, no. 5, pp 489-494, Oct 2012

[23] NL. Clarke , SM Furnell, PL Reynolds, "Biometric authentication for mobile devices", InProceeding of the 3rd Australian information warfare and security conference, pp. 61-69, Nov 2002

[24] Χ. Λιώλης, "Εργαλεία δειγματοληπτικής έρευνας", Πτυχιακή Εργασία, ΤΕΙ Πειραιά, Σχολή Διοίκησης και Οικονομίας, Τμήμα Διοίκησης Επιχειρήσεων, Αθήνα, 2014

[25] R. Ahluwalia, "Banking's Biometric future", Biometric Technology Today, vol 2016, no. 10, pp 7-9, Oct 2016

[26] D. Thakkar, "Biometrics to Improve Customer Service in Online banking", Bayometric, Mar 2017

[27] D. Thakkar, "Adoption of Biometrics in Banking and Financial Service Industry", Bayometric, Aug 2017

[28] Δ. Καρτσακλής, "Computer για όλους, Βιομετρικά συστήματα αναγνώρισης", Τεύχος 182, 1999

[29] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial" gummy" fingers on fingerprint systems." In Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, pp. 275-289. International Society for Optics and Photonics, April 2002

[30] D.J. Solove, "Identity theft, privacy, and the architecture of vulnerability", Hastings Lj, vol 54, p.1227, 2002

[31] R. Sanchez-Reillo, I. Ortega-Fernandez, W. Ponce-Hernandez and HC. Quiros-Sandoval, "How to implement EU data protection regulation for R&D in biometrics", Computer Standards & Interfaces, vol 61, pp.89-96, Jan 2019

[32] http://www.cylaw.org/nomoi/indexes/2018_1_125.html Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018 (Ν. 125(Ι)/2018) Ε.Ε., Παρ.Ι(Ι), Αρ.4670, Ιούλιος 2018

[33] https://usa.visa.com/visa-everywhere/security/how-fingerprint-authentication-works.html - Research conducted by AYTM Market Research, Sept 2017

[34] T. Lee, "Biometrics and disability rights: legal compliance in biometric identification programs." U. Ill. JL Tech. & Pol'y ,page 209, 2016

[35] Κ. Ζαφειρόπουλος, "Πώς γίνεται μια επιστημονική εργασία. Επιστημονική έρευνα και συγγραφή εργασιών", Αθήνα: Εκδόσεις Κριτική, 2005

[36] Γ. Αθανασίου, "Η χρήση των ηλεκτρονικών καναλιών στην νέα τραπεζική εποχή", Ελληνικό Ανοικτό Πανεπιστήμιο, Σχολή Κοινωνικών Επιστημών, Διπλωματική εργασία, Σεπτέμβριος 2018

[37] Κ. Παπαδοπούλου, "Η ηλεκτρονική Τραπεζική στην Ελλάδα και η αποτελεσματική εφαρμογή της σε επιχειρήσεις", ΑΤΕΙ Θεσσαλονίκης, Σχολή Διοίκησης και Οικονομίας, Τμήμα Λογιστικής, Διπλωματική εργασία, Ιούνιος 2011

[38] SH Sumra, MK Manzoor, HH. Sumra, and M Abbas, "The impact of e-banking on the profitability of banks: A study of Pakistani banks", Journal of Public Administration and Governance, vol 1, no. 1, pp 31-38, 2011

# Παράρτημα Α
# Ερωτηματολόγιο

## Α.1 Τίτλος Ερωτηματολογίου

Συστήματα ελέγχου ταυτότητας για online banking – biometrics: πως μπορούν να χρησιμοποιηθούν για περισσότερη ασφάλεια στις συναλλαγές".

**Εισαγωγικό σημείωμα**

Η παρούσα έρευνα πραγματοποιείται στο πλαίσιο της Μεταπτυχιακής μου Διατριβής με τίτλο «Συστήματα ελέγχου ταυτότητας για online banking: biometrics- πως μπορούν να χρησιμοποιηθούν για περισσότερη ασφάλεια στις συναλλαγές». Σκοπός είναι η μελέτη της ασφάλειας και της επαρκής ευχέρειας που παρέχουν τα τραπεζικά συστήματα ταυτοποίησης καθώς και η δυνατότητα βελτίωσης των συστημάτων με τη χρήση βιομετρικής τεχνολογίας. Δικαίωμα συμμετοχής σε αυτή την έρευνα έχουν άτομα άνω των 18 ετών. Παρακαλώ απαντήστε όλες τις ερωτήσεις όσο το δυνατόν πιο ειλικρινά ώστε να προσφέρετε την καλύτερη δυνατή πληροφορία. Σας διαβεβαιώνω ότι οι απαντήσεις σας θα χρησιμοποιηθούν αποκλειστικά για στατιστική ανάλυση και τα προσωπικά σας στοιχεία θα παραμείνουν απολύτως εμπιστευτικά.

Μετά την εισαγωγή καλούνται να απαντήσουν στο ερωτηματολόγιο κάνοντας αρχή με την αποδοχή όρων: Έχω διαβάσει και αποδεκτεί τους πιο πάνω όρους και δέχομαι να συμμετέχω στην παρούσα έρευνα.

○Ναι

○ Όχι

**Ερώτηση 1:** Φύλο

○ Άνδρας

○ Γυναίκα

○ Προτιμώ να μην απαντήσω

**Ερώτηση 2:** Ηλικία

○ 18-25

○ 26-33

○ 34-41

○ 42-49

○ 50+

**Ερώτηση 3:** Επίπεδο εκπαίδευσης

○ Μεταπτυχιακός τίτλος ή Διδακτορικό

○ Πανεπιστημιακή Εκπαίδευση

○ Απολυτήριο Λυκείου

○ Απολυτήριο Γυμνασίου

○ Απολυτήριο Δημοτικού

**Ερώτηση 4:** Επάγγελμα

○ Ιδιωτικός Υπάλληλος

○ Δημόσιος Υπάλληλος

○ Φοιτητής

○ Συνταξιούχος

○ Άνεργος

○ Άλλο:

**Ερώτηση 5:** Χρησιμοποιείτε υπηρεσίες online banking;

○Ναι

○ Όχι

**Ερώτηση 6:** Πόσο συχνά γίνεται χρήση του online banking;

○ Κάθε μέρα

○ Κάθε βδομάδα

○ Κάθε μήνα

○ Σπάνια

○ Ποτέ

**Ερώτηση 7:** Η τράπεζά σας, παρέχει ασφαλείς μεθόδους online banking;

○Ναι

○ Όχι

**Ερώτηση 8:** Πιστεύετε ότι το online banking είναι ασφαλές ;

○Ναι

○ Όχι

**Ερώτηση 9:** Γίνεται χρήση ξεχωριστών κωδικών για κάθε σας λογαριασμό;

○ Χρησιμοποιώ έναν μοναδικό κωδικό πρόσβασης/PIN για κάθε λογαριασμό

○ Χρησιμοποιώ πολλούς κωδικούς πρόσβασης/PIN αλλά δεν είναι μοναδικά σε κάθε λογαριασμό

○ Χρησιμοποιώ τον ίδιο κωδικό πρόσβασης/PIN για όλους τους λογαριασμούς μου

○ Έχω μόνο μία χρεωστική ή πιστωτική κάρτα

**Ερώτηση 10:** Ποιος ήταν ο λόγος που είχατε εγκαταλείψει ποτέ κάποια online αγορά;

○ Δεν είχα τη χρεωστική/πιστωτική κάρτα μαζί μου

○ Δεν μπορούσα να θυμηθώ των κωδικό μου

○ Χρειάστηκα να πληκτρολογήσω τον κωδικό μου

○ Δεν κάνω αγορέςonline

○ Άλλο:

**Ερώτηση 11:** Πόσο εξοικειωμένοι είστε με τη χρήση βιομετρικών στοιχείων ;

○ Πολύ εξοικειωμένος/η

○ Κάπως εξοικειωμένος/η

○ Όχι πολύ εξοικειωμένος/η

○ Καθόλου εξοικειωμένος/η

**Ερώτηση 12:** Ποιους από τους παρακάτω βιομετρικούς τύπους ελέγχου ταυτότητας γνωρίζετε;

☐ Δακτυλικό αποτύπωμα (Fingerprint)

☐ Αναγνώριση προσώπου (Face recognition)

☐ Αναγνώριση φωνής (Voice recognition)

☐ Αναγνώριση ίριδας ματιού (Eye scan)

☐ Μέτρηση και καταγραφή των προτύπων ανθρώπινης συμπεριφοράς (Behavioral biometrics)

☐ Αναγνώριση φλέβας στην παλάμη (Vein pattern recognition)

☐ Κανένα από τα πιο πάνω

**Ερώτηση 13:** Πόσο συχνά χρησιμοποιείτε τις πιο κάτω βιομετρικές μεθόδους; Επιλέξτε από τις παρακάτω περιπτώσεις την συχνότητα της δραστηριότητας επιλέγοντας 1= Πολύ σπάνια ή καθόλου /2= Μάλλον σπάνια 3/= Κανονικά, ούτε σπάνια ούτε συχνά /4= Αρκετά συχνά /5= Πολύ συχνά

| | Πολύ σπάνια ή καθόλου | Μάλλον σπάνια | Κανονικά, ούτε σπάνια ούτε συχνά | Αρκετά συχνά | Πολύ συχνά |
|---|---|---|---|---|---|
| Δακτυλικό αποτύπωμα (Fingerprint) | ○ | ○ | ○ | ○ | ○ |
| Αναγνώριση προσώπου (Face recognition) | ○ | ○ | ○ | ○ | ○ |
| Αναγνώριση φωνής (Voice recognition) | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| Αναγνώριση ίριδας ματιού (Eye scan) | ○ | ○ | ○ | ○ | ○ |
| Μέτρηση και καταγραφή των προτύπων ανθρώπινης συμπεριφοράς (Behavioral biometrics) | ○ | ○ | ○ | ○ | ○ |
| Αναγνώριση φλέβας στην παλάμη (Vein pattern recognition) | ○ | ○ | ○ | ○ | ○ |

**Ερώτηση 14:** Ποιο το ενδιαφέρον σας για τη χρήση των πιο κάτω βιομετρικών στοιχείων για την επαλήθευση της ταυτότητάς σας;

| | Το ενδιαφέρον μου για την επαλήθευση της ταυτότητας | Το ενδιαφέρον για μελλοντικές πληρωμές |
|---|---|---|
| Δακτυλικό αποτύπωμα (Fingerprint) | ○ | ○ |
| Αναγνώριση προσώπου (Face recognition) | ○ | ○ |
| Αναγνώριση φωνής (Voice recognition) | ○ | ○ |
| Αναγνώριση ίριδας ματιού (Eye scan) | ○ | ○ |
| Μέτρηση και καταγραφή των προτύπων ανθρώπινης συμπεριφοράς (Behavioral biometrics) | ○ | ○ |
| Αναγνώριση φλέβας στην παλάμη (Vein pattern recognition) | ○ | ○ |
| Κάποιο άλλο | ○ | ○ |

**Ερώτηση 15:** Ποια τα οφέλη από τη χρήση βιομετρικού ελέγχου ταυτότητας στις συναλλαγές σας;

☐ Θα εξαλείψει την ανάγκη να θυμόμαστε πολλούς κωδικούς πρόσβασης και PIN

☐ Είναι πιο ασφαλής από τους κωδικούς πρόσβασης και τους αριθμούς PIN επειδή επιβεβαιώνουν την ταυτότητά μου

☐ Δεν ξεχνώ/ χάνω τη μέθοδο ταυτότητάς μου

☐ Οι λογαριασμοί και τα στοιχεία μου είναι ασφαλείς ακόμη και αν κλαπεί το smartphone μου ή ο Υπολογιστής μου

☐ Μπορώ να πληρώσω οπουδήποτε/ οτιδήποτε, επειδή η μέθοδος ελέγχου ταυτότητας αποτελεί μέρος μου

☐ Ο βιομετρικός έλεγχος ταυτότητας είναι ευκολότερος από την εισαγωγή κωδικού πρόσβασης η PIN

☐ Η χρήση της βιομετρικής ταυτότητας θα μου έδινε τη σιγουριά ότι η πληρωμή μου προστατεύεται

☐ Δεν υπάρχουν οφέλη

☐ Άλλο

**Ερώτηση16:** Ποιες οι κύριες ανησυχίες χρήσης βιομετρικών στοιχείων αυθεντικοποίησης για τις πληρωμές σας;

☐ Ο κίνδυνος διαρροής ασφαλείας ευαίσθητων πληροφοριών

☐ Η ανησυχία ότι ο βιομετρικός έλεγχος ταυτότητας δεν θα λειτουργήσει / θα λάβει πολλές προσπάθειες

☐ Το κόστος της κατοχής μία συσκευής που επιτρέπει τη βιομετρική ταυτοποίηση

☐ Προστασία προσωπικών δεδομένων – ανησυχείτε ότι μία τράπεζα έχει ευαίσθητες προσωπικές πληροφορίες για εσάς

☐ Ταλαιπωρία με τη χρήση βιομετρικής ταυτότητας μπροστά σε κοινό

☐ Δε διαθέτει καθορισμένη μορφή βιομετρικής πιστοποίησης

☐ Δεν υπάρχουν μειονεκτήματα

☐ Άλλο

**Ερώτηση 17:** Τα βιομετρικά στοιχεία είναι ταχύτερα ή πιο αργά από τους κωδικούς πρόσβασης;

○ Πολύ πιο γρήγορα από τους κωδικούς πρόσβασης

○ Λίγο πιο γρήγορα από τους κωδικούς πρόσβασης

○ Καμία αλλαγή

○ Λίγο πιο αργά από τους κωδικούς πρόσβασης

○ Πολύ πιο αργά από τους κωδικούς πρόσβασης

○ Δεν γνωρίζω / δεν είμαι σίγουρος/η

**Ερώτηση 18:** Η χρήση βιομετρικών στοιχείων είναι πιο εύκολη ή πιο δύσκολη από τους κωδικούς πρόσβασης;

○ Πολύ ευκολότερη από τους κωδικούς πρόσβασης

○ Λίγο πιο εύκολη από τους κωδικούς πρόσβασης

○ Καμία αλλαγή

○ Λίγο πιο δύσκολη από τους κωδικούς πρόσβασης

○ Πολύ πιο δύσκολη από τους κωδικούς πρόσβασης

○ Δεν γνωρίζω / δεν είμαι σίγουρος/η

**Ερώτηση 19:** Οι βιομετρικές μέθοδοι είναι πιο ασφαλείς από τις παραδοσιακές μεθόδους ταυτοποίησης; 1= Διαφωνώ απόλυτα /2=Διαφωνώ /3=Ούτε διαφωνώ ούτε συμφωνώ /4=Συμφωνώ /5=Συμφωνώ απόλυτα

| | Διαφωνώ απόλυτα | 2 | 3 | 4 | Συμφωνώ απόλυτα |
|---|---|---|---|---|---|
| Αναγνώριση δακτυλικών αποτυπωμάτων (Βιομετρική μέθοδος) | ○ | ○ | ○ | ○ | ○ |
| Αναγνώριση ίριδας ματιού (Βιομετρική μέθοδος) | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| Έλεγχος σε δύο βήματα two steps password και code (Παραδοσιακή μέθοδος) | ○ | ○ | ○ | ○ | ○ |
| Αναγνώριση προσώπου (Βιομετρική μέθοδος) | ○ | ○ | ○ | ○ | ○ |
| Αναγνώριση φλέβας παλάμης (Βιομετρική μέθοδος) | ○ | ○ | ○ | ○ | ○ |
| Αριθμός PIN (Παραδοσιακή μέθοδος) | ○ | ○ | ○ | ○ | ○ |
| Κωδικός πρόσβασης (Παραδοσιακή μέθοδος) | ○ | ○ | ○ | ○ | ○ |
| Αναγνώριση φωνής (Βιομετρική μέθοδος) | ○ | ○ | ○ | ○ | ○ |
| Απάντηση σε ερώτηση ασφαλείας (Παραδοσιακή μέθοδος) | ○ | ○ | ○ | ○ | ○ |

**Ερώτηση 20:** Σε πιο από τα παρακάτω θα εμπιστευόσασταν την αποθήκευση βιομετρικών πληροφοριών;

☐ Την τράπεζά σας

☐ Μια μεγάλη διαδικτυακή μάρκα με παγκόσμιο όνομα

☐ Τον πάροχο κινητής τηλεφωνίας σας

☐ Τον πάροχο διαδικτυακών υπηρεσιών σας

☐ Ένα πολυκατάστημα

☐ Ένα τοπικό, ανεξάρτητο κατάστημα ή εστιατόριο

☐ Κανένα από τα πιο πάνω

**Ερώτηση 21:** Στην περίπτωση που ένας παροχέας δεν σας προσφέρει βιομετρική ταυτοποίηση στο μέλλον, από τι θα απομακρυνόσασταν;

○ Την πιστωτική / χρεωστική σας κάρτα

○ Την τράπεζα σας

○ Τον κινητό φορέα τηλεφωνίας (π.χ. Samsung, Apple)

○ Άλλο: