Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών*Ασφάλεια Υπολογιστών Και Δικτύων*

Μεταπτυχιακή Διατριβή

ΣΥΣΤΗΜΑΤΑ ΕΛΕΓΧΟΥ ΤΑΥΤΟΤΗΤΑΣ ΓΙΑ ONLINEBANKINGBIOMETRICS-ΠΩΣ ΜΠΟΡΟΥΜΕ ΝΑ ΔΙΑΣΦΑΛΙΣΟΥΜΕ ΜΕΓΑΛΥΤΕΡΗ ΑΣΦΑΛΕΙΑ ΚΑΙ ΑΠΟΔΟΤΙΚΟΤΗΤΑ

Μαρία Τσιμιδάκη

Επιβλέπων Καθηγητής
Αδαμαντίνη Περατικού

Δεκέμβριος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών*Ασφάλεια Υπολογιστών Και Δικτύων*

Μεταπτυχιακή Διατριβή

ΣΥΣΤΗΜΑΤΑ ΕΛΕΓΧΟΥ ΤΑΥΤΟΤΗΤΑΣ ΓΙΑ ONLINEBANKINGBIOMETRICS- ΠΩΣ ΜΠΟΡΟΥΜΕ ΝΑ ΔΙΑΣΦΑΛΙΣΟΥΜΕ ΜΕΓΑΛΥΤΕΡΗ ΑΣΦΑΛΕΙΑ ΚΑΙ ΑΠΟΔΟΤΙΚΟΤΗΤΑ

Μαρία Τσιμιδάκη

Επιβλέπων Καθηγητής
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στηΤσιμιδάκη Μαρία
από τη Σχολή Θετικών Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2019

Περίληψη

Το onlinebanking είναι ένα από τα πιο αξιοσημείωτα επιτεύγματα που επηρέασε τη ζωή του ανθρώπου και εφαρμόζεται σε όλο το κόσμο καθώς οι γρήγοροι ρυθμοί ζωής πλέον καθιστούν αναγκαίο τέτοιες συναλλαγές όπως οι τραπεζικές που γίνονται σε καθημερινή βάση, να απαιτούν ελάχιστο χρόνο, ευκολία και μέγιστη αποδοτικότητα. Ξεκίνησε με την απλή online συναλλαγή μεταξύ τραπεζικών λογαριασμών (καταθέσεις, εμβάσματα) και σιγά σιγά εμφανίστηκαν οι αγορές με πιστωτικές και χρεωστικές κάρτες, οι προπληρωμένες κάρτες, η online εξόφληση λογαριασμών και σήμερα πλέον απαιτείται σε όλα τα καταστήματα χονδρικής και λιανικής πώλησης που διαθέτουν μηχανήματα POS. Σκοπός της έρευνας αυτής είναι να ερευνηθεί κατά πόσο τα συστήματα ελέγχου ταυτότητας για onlinebanking μπορούν να δεχτούν βελτίωση ως προς τη ασφάλεια, αν όχι να εξασφαλιστεί, και ταυτόχρονα να μειωθεί ο χρόνος εκτέλεσης της διαδικασίας αυτής χρησιμοποιώντας βιομετρικές τεχνολογίες όπως δακτυλικό αποτύπωμα.

Λέξεις κλειδιά: online banking, authentication systems, biometrics

Summary

Online banking is one of the most remarkable achievements that has influenced human life and is being implemented all over the world as fast paced life now necessitates such transactions, as day-to-day banking, to require minimum time, convenience and maximum profitability. It started with the simple online transaction between bank accounts (deposits, remittances) and slowly emerged credit and debit card purchases, prepaid cards, online bill payment and is now requires in POS wholesalers and retailers. The purpose of this research is to investigate whether authentication systems for online banking can be improved, if not completely secured, and at the same time to reduce the time required to perform this process using biometrics technologies such as fingerprint.

Keywords: online banking, authentication systems, biometrics

Ευχαριστίες

Ένα μεγάλο ευχαριστώ στην οικογένεια μου για τη πολύτιμη στήριξη και βοήθεια τους χωρίς την οποία δε θα μπορούσα να παρακολουθήσω το μεταπτυχιακό πρόγραμμα Σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων.

Με την ευκαιρία της ολοκλήρωσης της διπλωματικής διατριβής μου, θα ήθελα επίσης να εκφράσω τις ευχαριστίες μου στην καθηγήτρια μου κα. Αδαμαντίνη Περατικού για την καθοδήγηση κατά τη διάρκεια της εκπόνησης της διπλωματικής διατριβής καθώς και για τις συμβουλές της στη στατιστική ανάλυση των δεδομένων της διατριβής μου.

Εισαγωγή

Εισαγωγή

Εδώ και αρκετά χρόνια παρατηρείται συνεχώς μια άνοδο στα τεχνολογικά επιτεύγματα και στην εξέλιξη του διαδικτύου. Αυτό βέβαια μπορεί να πρόσφερε άνεση και εξοικονόμηση χρόνου στη καθημερινότητα μας αλλά ταυτόχρονα αύξησε το κίνδυνο για τυχόν απάτες. Στο χώρο της οικονομίας και των συναλλαγών συναντάμε το onlinebanking. Στην Ελλάδα το onlinebanking εξελίχθηκε τα τελευταία χρόνια. Μέσω της ηλεκτρονικής τραπεζικής ο χρήστης μπορεί να πραγματοποιήσει τις εργασίες του όπως θα έκανε και σε ένα φυσικό κατάστημα με μεγαλύτερη ευκολία και απόδοση. Καθώς το βασικό του αντικείμενο είναι τα χρήματα, πολλοί είναι αυτοί που θέλουν να προκαλέσουν προβλήματα προς δικό τους όφελος κυρίως. Η πλαστοπροσωπία και η κλοπή διαπιστευτηρίων (καρτών, κωδικών) κάνουν τη εμφάνισή τους. Για το λόγο αυτό απαιτείται ολοένα και μεγαλύτερη ασφάλεια στα συστήματα ελέγχου ταυτότητας στο onlinebanking. Είναι φανερό ότι οι δυνατοί κωδικοί (complex), η συχνή ανανέωση των κωδικών, τα πολλά δικαιολογητικά για την απόδειξη της ταυτότητας μας σε περίπτωση ανάληψης μπορεί να μειώνουν το πρόβλημα της ασφάλειας αλλά όχι όσο θα μπορούσαμε εμείς οι νέοι επιστήμονες και ερευνητές. Στο σημείο αυτό έρχεται η έννοια βιομετρικές τεχνολογίες. Στην Ελλάδα τα biometrics προς το παρόν εφαρμόζονται μόνο στην αναγνώριση και ταυτοποίηση σε συστήματα ελέγχου πρόσβασης σε χώρους με περιορισμένη έως αυστηρή προσβασιμότητα όπως σε στρατιωτικές βάσεις ή θυρίδες τραπεζών. Βέβαια το fingerprint είναι το μόνο βιομετρικό σύστημα που μπορούμε να συναντήσουμε στην ταυτοποίηση για την είσοδό μας σε online συναλλαγή μέσω mobile και υπολογιστή.

Σκοπός έρευνας

Η έρευνα θα δείξει κατά πόσο τα συστήματα ελέγχου ταυτότητας για online banking μπορούν να δεχτούν βελτίωση στην ασφάλεια των συναλλαγών και αν μπορεί να συμβάλλουν σε αυτό οι βιομετρικές τεχνολογίες. Ο κύριος στόχος είναι να ερευνηθεί κατά πόσο υπάρχει ανάγκη για βελτίωση των επιπέδων ασφαλείας και ευκολίας των ηλεκτρονικών συναλλαγών στην Ελλάδα και αν αυτή η βελτίωση μπορεί να επιτευχθεί με τη χρήση βιομετρικών τεχνολογιών στην επαλήθευση ταυτότητας.

Βασικά ερευνητικά ερωτήματα

1. Τι συστήματα ελέγχου ταυτότητας είναι διαθέσιμα για online ιστοσελίδες;
2. Τα συστήματα ελέγχου ταυτότητας για online banking διευκολύνουν τη καθημερινότητα μας;
3. Υπάρχουν επί του παρόντος εφαρμογές ή / και εξελίξεις βιομετρικών συστημάτων ελέγχου ταυτότητας στο πλαίσιο της λειτουργίας e banking στην Ελλάδα;
4. Πως λειτουργούν τα τρέχον συστήματα ελέγχου ταυτότητας σε ιστοσελίδες Τραπεζικής στην Ελλάδα και τι ζητήματα ασφαλείας και ευκολίας προκύπτουν από αυτά;
5. Τα biometrics μπορούν να συμβάλλουν στη διατήρηση της ασφάλειας και στην απλοποίηση και μείωση του χρόνου εκτέλεσης του online banking;

Αναγκαιότητα και σπουδαιότητα έρευνας

Η συνεχής εξέλιξη του διαδικτύου και των τεχνολογικών επιτευγμάτων καθιστά αναγκαία τη θωράκιση των συστημάτων για online banking των τραπεζών με πρόσθετη ασφάλεια. Η έρευνα έχει ως αντικείμενο να ψάξει αν οι τραπεζικές online συναλλαγές μπορούν να γίνονται πιο γρήγορα και με ασφάλεια και ασε αυτό θα βοηθήσουν οι βιομετρικές τεχνολογίες.

Περιεχόμενα

Κεφάλαιο 1

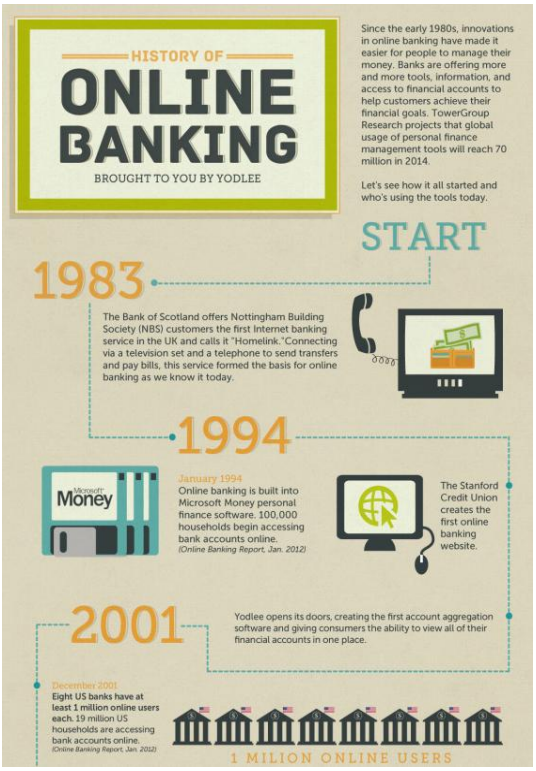
Ηλεκτρονική Τραπεζική

Η Ιστορία του OnlineBanking

Η εξέλιξη της ηλεκτρονικής τραπεζικής ξεκίνησε τη δεκαετία του 1980 όταν ο ορισμός και η πρακτική της τραπεζικής μέσω διαδικτύου ήταν πολύ διαφορετική από αυτό που είναι σήμερα. Παρόλο που υπήρξαν μεγάλες τράπεζες όπως η WellsFargoBank στις Ηνωμένες Πολιτείες που εδραίωσαν την ηλεκτρονική τραπεζική και έλαβαν μέτρα για την υλοποίηση τέτοιων υπηρεσιών στα μέσα της δεκαετίας του 1990, πολλοί ήταν αυτοί που δίστασαν να δοκιμάσουν συναλλαγές μέσω διαδικτύου. Το 1995 εμφανίστηκαν οι λεγόμενες "εικονικές τράπεζες" με πρώτη στη κατηγορία αυτή την "SecurityFirstNetworkBank" οι οποίες δρούσαν μόνο διαδικτυακά. Τον ίδιο χρόνο, εταιρείες σαν την Amazon, το eBay και την AmericaOnline που εμπιστεύτηκαν και άρχισαν να υλοποιούν ηλεκτρονικές συναλλαγές, κατάφεραν να επηρεάσουν τους καταναλωτές. Έτσι, μέχρι και το 2000 το 80% των αμερικανικών τραπεζών πρόσφερε onlinebanking. Βέβαια, αν λάβουμε υπόψη ότι η BankofAmerica, χρειάστηκε δέκα χρόνια για να αποκτήσει δυο εκατομμύρια πελάτες ηλεκτρονικής τραπεζικής, θα καταλάβουμε ότι ο ρυθμός αύξησης των πελατών ήταν πολύ αργός.

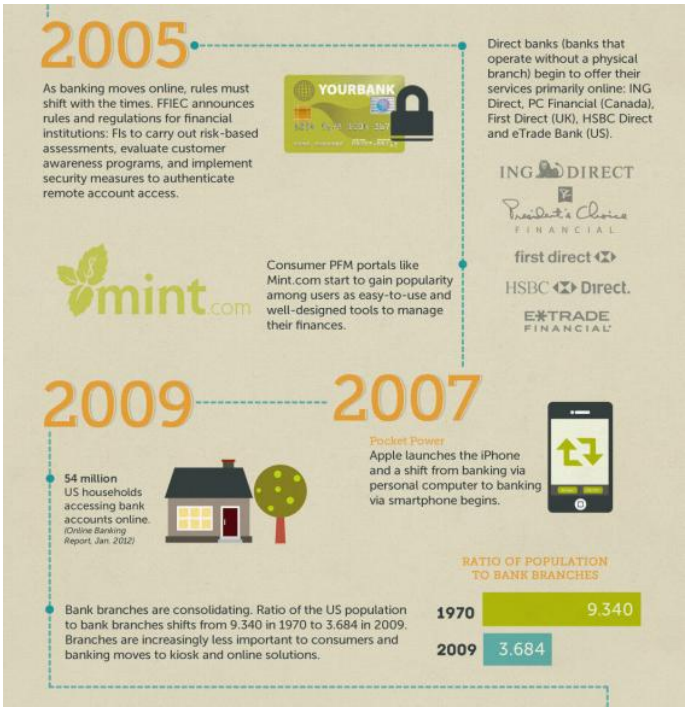
Εντούτοις, σημαντική πολιτισμική αλλαγή επήλθε μετά τη λήξη του προβλήματος Υ2Κ, με τη Τράπεζα της Αμερικής να αυξάνει στα τρία εκατομμύρια τους πελάτες διαδικτυακής τραπεζικής, ξεπερνώντας έτσι και το 20% της πελατειακής της βάσης μέσα σε μόλις ένα χρόνο. Σε σύγκριση, μεγάλες επενδυτικές τράπεζες όπως η CityGroup και η JPMorganChase κατάφεραν να φτάσουν τις 2,2 εκατομμύριαonline συναλλαγές παγκοσμίως και τους 750 χιλιάδες πελάτες με online τραπεζική αντίστοιχα. Τον Οκτώβριο του 2001, στη Τράπεζα της Αμερικής πραγματοποιήθηκαν 2,5 online πληρωμές λογαριασμών ξεπερνώντας το ένα δισεκατομμύριο συνολικά. Τελικά αποδείχθηκε ότι οι καταναλωτές που άρχισαν να χρησιμοποιούν το onlinebanking ήταν πιο κερδοφόροι για τις τράπεζες από ότι οι πελάτες στα καταστήματα.

Η Νέα Υόρκη ήταν η πρώτη στη μέχρι τότε ιστορία της τραπεζικής που το 1981 μέσω των τραπεζών ChaseManhattan, Citibank, Chemical και ManufacturesHanover εξέτασε το πρώτο ηλεκτρονικό τραπεζικό σύστημα μη καταφέρνοντας βέβαια να γίνει αποδεκτό από τους καταναλωτές, μέχρι που το 1994 η Ομοσπονδιακή Ένωση Πιστωτικών Ιδρυμάτων Stanford πρόσφερε για πρώτη φορά Internetbanking ενώ το 1995 η Presidentbank κατάφερε να γίνει η πρώτη τράπεζα που πρόσφερε online πρόσβαση.



Εικόνα 1: Ιστορία του onlinebanking (1)

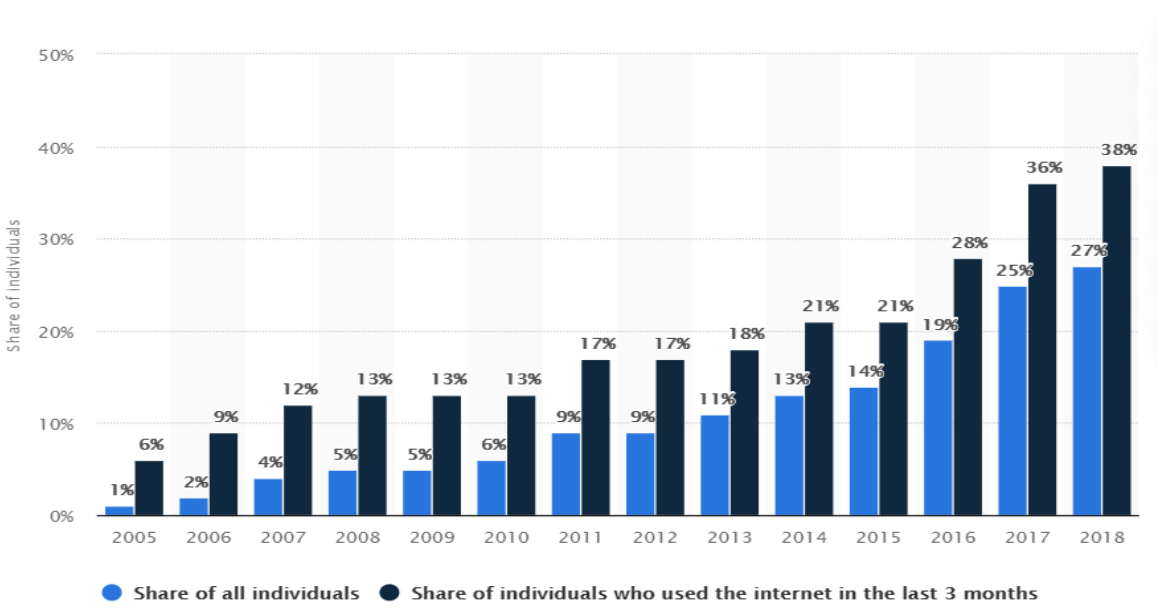
Το 2007, κάνει την εμφάνιση της η iPhone και προωθεί τα νέα Smartphone κινητά τα οποία έρχονται να διευκολύνουν ακόμα περισσότερο τους καταναλωτές καθώς θα μπορούν πλέον να χρησιμοποιούν το onlinebanking μέσω των κινητών αντικαθιστώντας τους ηλεκτρονικούς υπολογιστές.



Εικόνα 2: Ιστορία του onlinebanking (2)

Παρακάτω αυτή η στατιστική δείχνει τη διείσδυση των online συναλλαγών στην Ελλάδα από το 2005 έως το 2018.

Παρατηρείται ότι το 2018, το 27% όλων των ατόμων χρησιμοποίησε το internet για onlinebanking, αλλά η χρήση ήταν υψηλότερη σε όσους είχαν χρησιμοποιήσει το διαδίκτυο μέσα στους τελευταίους μήνες φτάνοντας το 38%.

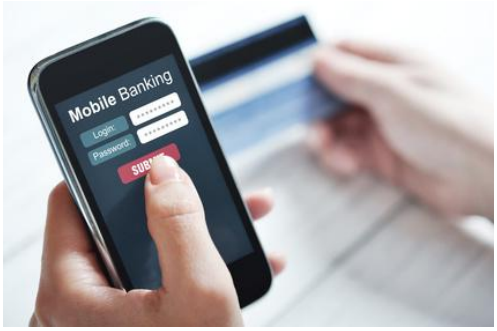


Διάγραμμα 1: Χρήση e-banking στην Ελλάδα 2005-2018

Ορισμός και δυνατότητες του OnlineBanking

Από τα παραπάνω γίνεται κατανοητό ότι το OnlineBanking
αποτελεί ένα γρήγορο εξελισσόμενο πεδίο εφαρμογής, το οποίο έχει εισβάλει σημαντικά στις ζωές των καταναλωτών.

Κάθε τραπεζικό ίδρυμα διαθέτει κάποια μορφή ηλεκτρονικής τραπεζικής τόσο με εφαρμογές σε υπολογιστές όσο και σε κινητά τηλέφωνα.



Εικόνα 3: E-bankingμευπολογιστή Εικόνα 4: E-bankingμε κινητό

Με την ηλεκτρονική τραπεζική, οι καταναλωτές δεν υποχρεούνται να επισκέπτονται ένα υποκατάστημα της τράπεζας για να ολοκληρώσουν τις περισσότερες βασικές τραπεζικές συναλλαγές τους. Μπορούν να κάνουν όλα αυτά με τη δική τους ευκολία, όποτε θέλουν - στο σπίτι, στη δουλειά ή εν κινήσει.Για την ασφαλέστερη αποδοτικότητα οι τράπεζες δημιούργησαν συστήματα ασφαλείας για να διασφαλίσουν ότι οι συναλλαγές που πραγματοποιούνται μέσω διαδικτύου προστατεύονται από απειλές ασφαλείας στο διαδίκτυο με τις περισσότερες τράπεζες να χρησιμοποιούν ένα λογισμικό και πρωτόκολλο SecureTransaction για τη διαχείριση της ασφάλειας στα συστήματά τους.

Η ηλεκτρονική τραπεζική απαιτεί υπολογιστή ή άλλη συσκευή, σύνδεση στο διαδίκτυο και μια χρεωστική κάρτα . Για να έχουν πρόσβαση στην υπηρεσία, οι πελάτες πρέπει να εγγραφούν για την ηλεκτρονική τραπεζική υπηρεσία της τράπεζάς τους. Για να εγγραφούν, πρέπει να δημιουργήσουν έναν κωδικό πρόσβασης. Μόλις γίνει αυτό, μπορούν να χρησιμοποιήσουν την υπηρεσία για να κάνουν όλες τις τραπεζικές εργασίες τους.Προσφέρει στους πελάτες σχεδόν όλες τις υπηρεσίες που είναι διαθέσιμες σε ένα τοπικό κατάστημα τραπέζης.
Βασικές υπηρεσίες που μας παρέχει το onlinebanking είναι η μεταφορά κεφαλαίων, χρημάτων δηλαδή μεταξύ λογαριασμών της ίδιας τράπεζας ή διαφορετικών τραπεζών. Οι περισσότερες τράπεζες προσφέρουν γενικά βασικές υπηρεσίες όπως μεταφορές (εμβάσματα) και πληρωμές λογαριασμών και δανείων. Εκτός βέβαια από τις οικονομικές συναλλαγές, ο καταναλωτής μπορεί

να εκδώσει παράβολα Δημοσίου, να πληρώσει φόρους όπως το Ε.Ν.Φ.Ι.Α και πιο γενικά να διαχειριστεί οικονομικές συναλλαγές του με το Δημόσιο. Τέλος, η ηλεκτρονική τραπεζική παρέχει στο χρήστη πληροφοριακές συναλλαγές όπως το αναλυτικό υπόλοιπο του λογαριασμού του αλλά και διαδικαστικές υπηρεσίες που σε άλλη περίπτωση ένας καταναλωτής θα υποχρεούταν να παραβρεθεί σε ένα φυσικό κατάστημα τραπέζης για να υποβάλει αίτηση για δάνειο, να ανοίξει μια προθεσμιακή κατάθεση, FD, αλλά και να αιτηθεί για νέο PIN χρεωστικής κάρτας.

Ορισμένες τράπεζες επιτρέπουν επίσης στους πελάτες να ανοίξουν νέους λογαριασμούς και να υποβάλουν αίτηση για πίστωση μέσω διαδικτυακών τραπεζικών portal.

Οι έλεγχοι μπορούν πλέον να κατατεθούν στο διαδίκτυο μέσω μιας εφαρμογής για κινητά. Ο πελάτης εισάγει απλά το ποσό πριν πάρει μια φωτογραφία του μπροστινού και του πίσω μέρους της επιταγής για να ολοκληρώσει την κατάθεση.

Η ηλεκτρονική τραπεζική δεν επιτρέπει την αγορά ταξιδιωτικών επιταγών, τραπεζικών σχεδίων, ορισμένων τραπεζικών εμβασμάτων ή την ολοκλήρωση ορισμένων πιστωτικών εφαρμογών όπως οι υποθήκες. Οι συναλλαγές αυτές πρέπει να πραγματοποιηθούν πρόσωπο με πρόσωπο με έναν εκπρόσωπο της τράπεζας.

Κίνδυνοι της Ηλεκτρονικής Τραπεζικής

Σίγουρα το onlinebanking μπορεί να παρέχει στο καταναλωτή όλα αυτά τα οφέλη και τα πλεονεκτήματα που προαναφέρθηκαν παραπάνω αλλά όπως σε κάθε ιστόχωρο, έτσι και ο ιστόχωρος του onlinebanking δέχεται καθημερινά

επιθέσεις από επίδοξους ηλεκτρονικούς εγκληματίες, hackers. Για το λόγο αυτό οι κατασκευαστές και χειριστές των υπολογιστικών συστημάτων δε μπορούν να εγγυηθούν ότι αυτά είναι πλήρως ασφαλή.

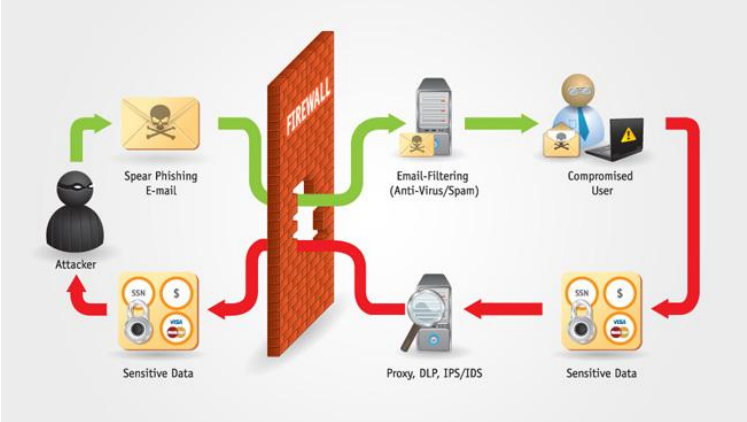
Σύμφωνα με τον QinghuaZhang, σχετικά με την ηλεκτρονική απάτη, πρέπει να γίνονται γνωστές πληροφορίες σε πιθανά μελλοντικά θύματα σχετικά με κακόβουλες πράξεις ενάντια σε χρηματοπιστωτικά ιδρύματα, τις τράπεζες αναφέροντας σα βασικές τεχνικές απάτης τη κλοπή ταυτότητας και το phishingattack.

Οι κυριότεροι στόχοι των hacker είναι μεγάλες τράπεζες. Παρακάτω αναφέρονται δυο περιστατικά ηλεκτρονικής απάτης που έχουν συμβεί.

- Η Citigroup αναφέρει ότι το 2011 περισσότεροι από 360.000 λογαριασμοί της έγιναν ευάλωτοι από επίθεση καταλήγοντας οι 3.400 από αυτούς να υποστούν απώλειες ύψους 2.7 εκατομμυρίων δολαρίων.
- Το 2012 Ιρανοί hacker είχαν ως στόχο λογαριασμούς πελατών της Citigroup, της BankofAmerica και της JPMorganChase. Οι επιθέσεις γνωστοποιήθηκαν ένα χρόνο μετά.

Οι πελάτες και ακόμα περισσότερο οι τράπεζες οφείλουν να είναι γνώστες όλων των μεθόδων ηλεκτρονικών επιθέσεων και να λαμβάνουν τα ανάλογα μέτρα. Παρακάτω αναφέρονται μέθοδοι υποκλοπής δεδομένων μέσω Διαδικτύου:

- **Phishing:** έχοντας ένα λογαριασμό onlinebanking μπορεί ο πελάτης να πέσει θύμα phishingattack. Στη περίπτωση αυτή ο hacker δημιουργεί ιστοσελίδες-ιστότοπους που είναι πανομοιότυπες με τις αυθεντικές ιστοσελίδες των τραπεζών και τις οποίες χρησιμοποιεί για να παραβιάσει την εμπιστοσύνη του θύματος. Τότε το θύμα θεωρώντας ότι πρόκειται για την αυθεντική ιστοσελίδα του ιδρύματος του, προχωρά στην εισαγωγή κωδικών και άλλων ευαίσθητων πληροφοριών τα οποία μέσω κακόβουλου λογισμικού που έχει φορτώσει η ‘’fake’’ιστοσελίδα, συλλέγονται εκεί και γνωστοποιούνται στον υποκλοπέα καταλήγοντας να αποσπώνται μεγάλα χρηματικά ποσά.



Εικόνα 5: Phishing attack

- **Identitytheft:** σίγουρα υπάρχουν και άλλοι τρόποι ένας hacker να συγκεντρώσει τις πληροφορίες που χρειάζεται για να αποσπάσει χρήματα από λογαριασμούς πελατών. Μια απλή κλοπή του πορτοφολιού γεμάτο με πιστωτικές και χρεωστικές κάρτες και άλλα ευαίσθητα δεδομένα, κάνουν το έργο του πιο εύκολο. Οι πελάτες πολλές φορές δημοσιοποιούν στο Internet προσωπικές πληροφορίες όπως αριθμό κοινωνικής ασφάλισης όπως επίσης πολλοί από αυτούς δε καταστρέφουν εξ ολοκλήρου παλιά ευαίσθητα έντυπα θεωρώντας ότι κανένας δε θα ψάξει στα 'σκουπίδια'.

Εικόνα 6: Identity theft

- **Trojanhorses:** πρόκειται για τον πιο γνωστό τρόπο υποκλοπής δεδομένων σύμφωνα με τον οποίο το θύμα εγκαθιστά στον υπολογιστή του ή το κινητό του ένα λογισμικό το οποίο θεωρεί αξιόπιστο αλλά στην ουσία αυτό που κάνει είναι να καταγράφει τις κινήσεις του θύματος και να υποκλέπτει δεδομένα συμπεριλαμβανομένου κωδικούς τραπεζικών λογαριασμών. Θεωρήθηκε η επόμενη γενιά 'phishingattack'.

Εικόνα 7: Trojanhorses

Σύμφωνα με τον ShammiIsharaHewamadduma, το τρίτο τρίμηνο του 2013, το 31,45% όλων των phishingattack ήταν μόνο ενάντια σε χρηματοπιστωτικά ιδρύματα, διπλάσιο ποσοστό από το 2012 ενώ το 22,2% πρόκειται για 'fake' ιστότοπους. Αξιοσημείωτο παράδειγμα που φανερώνει την ανάγκη για ενίσχυση της ασφάλειας στην ηλεκτρονική τραπεζική είναι οι τράπεζες της Σρι Λάνκα οι οποίες δεν έχουν ακόμα αναπτύξει μεθόδους ανίχνευσης μη εξουσιοδοτημένης σύνδεσης σε λογαριασμούς. Αυτό σημαίνει ότι όταν συμβεί μια επίθεση παράνομης πρόσβασης σε λογαριασμό κάποιου πελάτη της, η τράπεζα δεν είναι σε θέση να αντιληφθεί το περιστατικό έως ότου ο πελάτης κάνει τη καταγγελία του.

Καταλήγουμε λοιπόν ότι μπορεί η τεχνολογία να εξελίσσεται και οι τράπεζες συνεχώς να προσπαθούν και πράγματι να βελτιώνουν την ασφάλεια των συστημάτων τους, όμως θα υπάρχουν και οι κακόβουλοι χρήστες που θα είναι ενημερωμένοι πάντα για της καινοτομίες της πληροφορικής και θα συνεχίζουν το έργο τους με επιτυχία. Άρα απαιτείται ενίσχυση στην ασφάλεια των συστημάτων των χρηματοπιστωτικών ιδρυμάτων.

ΚΕΦΑΛΑΙΟ 2

Συστήματα ελέγχου ταυτότητας

Εισαγωγή στηναυθεντικοποίηση στο onlinebanking

Στόχος των χρηματοπιστωτικών ιδρυμάτων είναι να συνδυάσουν όσο καλύτερα γίνεται την ασφάλεια και την ευκολία στις ηλεκτρονικές συναλλαγές. Οφείλουν να εξασφαλίσουν τη πιστοποίηση της ταυτότητας, την ακεραιότητα και τη μη-άρνηση(non-repudiation). Βασική προϋπόθεση για την προσπέλαση μιας οντότητας σε κάθε πόρο του συστήματος είναι ο έλεγχος της ταυτότητας του χρήστη.Κύριο χαρακτηριστικό στο τομέα αυτό είναι η αυθεντικοποίηση. Όπως αναφέρθηκε και στο 1ο κεφάλαιο, τα τελευταία χρόνια πολλές τράπεζες και πελάτες έπεσαν θύματα ηλεκτρονικής απάτης. Τι θα γινόταν άραγε αν ο κάθε πελάτης δεν επαλήθευε τη ταυτότητα του?

Εικόνα 8: Επαλήθευση ταυτότητας με password

Ορισμός της αυθεντικοποίησης και οι τεχνικές της

Κάθε εβδομάδα φαίνεται ότι μια διαφορετική εταιρεία είναι θύμα από hackerπου κλέβει ευαίσθητα δεδομένα. Για αυτό η παροχή ισχυρής ασφάλειας δικτύου για του πελάτες είναι πιο σημαντική από ποτέ. Η πρωταρχική ευθύνη ενός ασφαλούς συστήματος είναι να διασφαλίσει ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο δίκτυο.

Αυθεντικοποίηση είναι η διαδικασία επιβεβαίωσης της ταυτότητας ενός χρήστη. Κατά την αυθεντικοποίηση επεξεργάζονται οι πληροφορίες που απαιτούνται ώστε να ελεγχθεί η εγκυρότητα της ταυτοποίησης.

Υπάρχουν τρεις βασικοί τρόποι για την υλοποίηση ενός συστήματος αυθεντικοποίησης οι οποίοι βασίζονται στα παρακάτω.

- κάτι το οποίο το άτομο γνωρίζει. Όπως ένας κωδικός PIN ή ένα συνθηματικό
- κάτι το οποίο το άτομο κατέχει. Πρόκειται για ένα token ή μια έξυπνη κάρτα
- κάτι που το άτομο το χαρακτηρίζει. Εδώ αφορά ένα βιολογικό χαρακτηριστικό όπως δακτυλικό αποτύπωμα.

Περνώντας από διάφορα στάδια ασφάλειας των πληροφοριακών συστημάτων και ενώ η τεχνολογία του διαδικτύου συνεχώς αναπτύσσεται, εμφανίζονται διάφορα μοντέλα ελέγχου ταυτότητας. Αυτά περιλαμβάνουν τόσο τις γενικές τεχνικές επαλήθευσης ταυτότητας όπως κωδικοί πρόσβασης, 2FA, tokens, βιομετρικά χαρακτηριστικά, έλεγχος ταυτότητας συναλλαγών, SSOκαι αναγνώριση υπολογιστή καθώς και συγκεκριμένα πρωτόκολλα ελέγχου ταυτότητας συμπεριλαμβανομένων των Kerberoskαι SSL/TLS.

Η πιο βασική μορφή ελέγχου ταυτότητας είναι η εισαγωγή κωδικού πρόσβασης που έχει χρησιμοποιηθεί από όλους ανεξαιρέτως χρήστη. Χρησιμοποιείται ένας μοναδικός και μυστικός κωδικός ώστε να έχει ο χρήστης εξουσιοδοτημένη πρόσβαση στα δεδομένα του. Αφού εισάγει ο χρήστης το όνομα χρήστη, πρέπει να πληκτρολογήσει και ένα κωδικό πρόσβασης. Εάν ο κάθε χρήστης διατηρεί το κωδικό του ιδιωτικό, θεωρητικά η μη εξουσιοδοτημένη πρόσβαση θα αποτραπεί. Ωστόσο, η εμπειρία έχει δείξει ότι ακόμα και μυστικοί κωδικοί πρόσβασης είναι ευάλωτοι στην πειρατεία(hacking). Οι hackerχρησιμοποιούν προγράμματα που δοκιμάζουν χιλιάδες κωδικούς αποκτώντας πρόσβαση μόλις βρουν το σωστό.

Για να μειωθεί αυτός ο κίνδυνος, οι χρήστες πρέπει να επιλέξουν ασφαλείς κωδικούς με γράμματα και αριθμούς, με κεφαλαία και πεζά, με ειδικούς χαρακτήρες (-, %, #) και κωδικούς που να μην υπάρχουν σε κάποιο λεξικό. Είναι επίσης σημαντικό να χρησιμοποιεί μεγάλους σε έκταση κωδικούς. Βέβαια, ακόμα και οι πιο ισχυροί κωδικοί πρόσβασης ενδέχεται να είναι ευάλωτοι στο hacking. Για αυτό και οι ειδικοί ασφαλείας έχουν αναπτύξει πιο εξελιγμένες τεχνικές επαλήθευσης ταυτόττητας.

Άλλο μοντέλο αυθεντικοποίησης είναι το 2FactorAuthentication, έλεγχος ταυτότητας δύο παραγόντων. Είναι μια επιπλέον αυθεντικοποίηση. Απαιτείται τόσο κωδικός πρόσβασης όσο και η κατοχή συγκεκριμένου φυσικού αντικειμένου για να επιτραπεί η πρόσβαση. Τα ATM είναι ένα πρώιμο σύστημα που χρησιμοποιεί 2FA.

Αφού ο χρήστης εισάγει το όνομα χρήστη και το κωδικό, πρέπει να εισάγουν επιπλέον έναν κωδικό μιας χρήσης από μια συγκεκριμένη φυσική συσκευή. Ο κωδικός αυτόςείτε του έχει σταλεί μέσω emailστο κινητό του είτε έχει παραχθεί από μια εφαρμογή του κινητού του. Εάν ο hackerμαντέψει το κωδικό πρόσβασης, δε μπορεί να προχωρήσει χωρίς το κινητό του χρήστη. Αν πάλι κλέψουν το κινητό, δε μπορούν να ξέρουν το κωδικό πρόσβασης. Το 2FAεφαρμόζεται σε ένα αυξανόμενο αριθμό τραπεζικών ιδρυμάτων.

Ορισμένες τράπεζες έχουν στραφεί στα συστήματα Tokensπου χρησιμοποιούν μια φυσική συσκευή προοριζόμενη για το 2FA. Αυτό μπορεί να είναι ένα dongleπου εισάγετε στη θύρα usbτου υπολογιστή ή μια έξυπνη κάρτα που περιέχει αναγνώριση ραδιοσυχνοτήτων. Εάν χρησιμοποιείται σύστημα με Token, πρέπει να φυλάσσονται τα dongleskαι οι έξυπνες κάρτες ώστε να μη βρεθούν σε λάθος χέρια. Αυτά τα συστήματα είναι πιο ακριβά καθώς απαιτείται η αγορά συσκευών αλλά παρέχουν ένα επιπλέον επίπεδο ασφάλειας.

Στη συνέχεια αναφέρεται σα μέθοδος αυθεντικοποίησης η πιστοποίηση αναγνώρισης υπολογιστή. Η αναγνώριση υπολογιστή επαληθεύει ότι ο χρήστης είναι αυτός που ισχυρίζεται. Στη περίπτωση αυτή ο χρήστης επιλέγει μια συγκεκριμένη συσκευή από την οποία θα συνδέεται στο λογαριασμό του ηλεκτρονικά. Εισάγεται σε αυτή ένα plug-in λογισμικού με ένα δείκτη κρυπτογραφικής συσκευής κατά τη πρώτη του σύνδεση και έτσι στις επόμενες συνδέσεις ελέγχεται αυτόματα αν η σύνδεση γίνεται από τη συγκεκριμένη συσκευή ή όχι. Το καλό με αυτό το σύστημα είναι ότι ο χρήστης δεν ασχολείται με τίποτα διαδικαστικό για την εγκατάσταση του plug-inεκτός από το να βάλει το όνομα χρήστη και το κωδικό του. Βέβαια το μειονέκτημα εδώ είναι ότι πλέον οι χρήστες αλλάζουν συνεχώς συσκευές. Για αυτό και πρέπει να επιτρέπεται η σύνδεση και σε άλλες συσκευές χρησιμοποιώντας άλλες μεθόδους επαλήθευσης όπως κωδικοποιημένους κωδικούς.
https://www.solarwindsmsp.com/blog/network-authentication-methods

SSO είναι μια υπηρεσία επαλήθευσης σύνδεσης που επιτρέπει σε ένα χρήστη να χρησιμοποιεί ένα όνομα χρήστη και ένα κωδικό για να πρόσβαση σε πολλαπλές εφαρμογές. Το SSO εξοικονομεί χρόνο και διατηρεί τους χρήστες online χωρίς να χρειάζεται να εισάγουν ξανά και ξανά κωδικούς πρόσβασης.

Οι πληροφορίες τοποθεσίας έχουν αρχίσει να χρησιμοποιούνται για σκοπούς πιστοποίησης. Πολλές τράπεζες χρησιμοποιούν ένα είδος εξακρίβωσης της ταυτότητας βάση τη τοποθεσία που χρησιμοποιεί τη γεωγραφική τοποθέτηση IPτου υπολογιστή για τον εντοπισμό τυχόν απάτης με πιστωτικές κάρτες, συγκρίνοντας τη θέση του χρήστη. Υπάρχουν δυο τεχνικές επαλήθευσης. Η

πρώτη ονομάζεται STAIκαι χρησιμοποιεί σύστημα GPSκαι η δεύτερη STAIIχρησιμοποιεί μια τεχνολογία επικοινωνίας IQRFγια το προσδιορισμό της θέσης. Η τοποθεσία προσδιορίζεται με δυο τρόπους. Ο πρώτος τρόπος χρησιμοποιεί την IPτου χρήστη σε πραγματικό χρόνο και η δεύτερη βασίζεται στο γεγονός ότι όλοι οι χρήστες χρησιμοποιούν κινητό τηλέφωνο τα οποία διαθέτουν GPSκαι Wi-Fi.
https://link.springer.com/content/pdf/10.1007%2F978-3-642-25734-6_136.pdf

Τέλος, η βιομετρική επαλήθευση ταυτότητας στο οποίο θα επικεντρωθώ στην εργασία αυτή αποτελεί αξιοσημείωτη μέθοδο ελέγχου ταυτότητας. Βασίζεται στη μέτρηση ενός φυσικού χαρακτηριστικού του χρήστη για τη πρόσβαση του σε ένα υπολογιστικό σύστημα. Τα πιο διαδεδομένα βιομετρικά συστήματα χρησιμοποιούν δακτυλικά αποτυπώματα, σαρώσεις ίριδας, αναγνώριση φωνής και ανίχνευση προσώπου.

Κεφάλαιο 3

Εισαγωγή

Καθώς οι άνθρωποι από όλο τον κόσμο νιώθουν πιο άνετοι χρησιμοποιώντας το διαδίκτυο για μια διευρυμένη σειρά αλληλεπιδράσεων, η εμβέλεια, ο όγκος και η αξία των προσωπικών πληροφοριών αυξάνονται σημαντικά. Συνεπώς, οι τράπεζες καθίστανται ολοένα και περισσότερο αφοσιωμένες στην ανάπτυξη πιο βολικών και ασφαλών μέσων για τη πρόσβαση στις πληροφορίες αυτές, επιτρέποντας στους χρήστες να οργανώνουν τη ζωή τους ψηφιακά χωρίς το φόβο κάποιας εξαπάτησης. Από τους αρχαίους κιόλας χρόνους οι άνθρωποι χρησιμοποίησαν τη βιομετρία ως μέσο ταυτοποίησης. Στην αρχή σα βιομετρικό χαρακτηριστικό χρησιμοποιήθηκε το δακτυλικό αποτύπωμα αλλά όσο πιο πολύ χρήσιμο γινόταν τόσο πιο πολλά χαρακτηριστικά του ανθρώπου ταυτοποιούνταν.
https://www.currencycloud.com/company/blog/the-future-of-biometric-banking/

Ορισμός Βιομετρικού Συστήματος

Βιομετρικό σύστημα είναι αυτό που πιστοποιεί τη ταυτότητα ενός χρήστη λαμβάνοντας υπόψη ένα χαρακτηριστικό του. Επιβεβαιώνει αν ο χρήστης είναι πράγματι αυτός που ισχυρίζεται ότι είναι. Για να υλοποιηθεί ένας τέτοιος τύπος συστήματος ελέγχου πρόσβασης απαιτείται ένα βιομετρικό χαρακτηριστικό του ατόμου το οποίο αρχικά αποθηκεύεται σε μια βάση δεδομένων ως ένα προσδιοριστικό δείγμα και σε κάθε σύνδεση συγκρίνεται με το πρόσφατο χαρακτηριστικό που δηλώνεται εκείνη τη στιγμή.

Η χρησιμότητα των βιομετρικών συστημάτων

Η βιομετρική τεχνολογία παρέχει την ισχυρότερη μέθοδο ελέγχου ταυτότητας που προστατεύει τη πληροφορία από παραβάτες. Λαμβάνοντας υπόψιν τις μαζικές επιθέσεις στο κυβερνοχώρο κατά τις onlineδραστηριότητες, η βιομετρία βοηθά τις τράπεζες να προστατέψει τη ταυτότητα των πελατών τους κατά τη χρήση της υπηρεσίας. Ένα σύστημα βασισμένο σε κάρτες μπορεί να ελέγξει τη πρόσβαση των επιτρεπόμενων πλαστικοποιημένων καρτών αλλά όχι ποιος τις κατέχει. Τα συστήματα που χρησιμοποιούν PINαπαιτούν μόνο ένα άτομο να γνωρίζει το μοναδικό κωδικό. Ο χρήστης όμως ποτέ δε προσδιορίζεται. Αντίθετα, οι βιομετρικές τεχνολογίες επαληθεύουν ποιος είναι το πρόσωπο από το οποίο είναι, είτε το χέρι, είτε το δακτυλικό αποτύπωμα είτε η φωνή. Η βιομετρία μπορεί επίσης να εξαλείψει την ανάγκη για κάρτες. Μια χαμένη κάρτα πρέπει να επανεκδοθεί. Αυτό ισοδυναμεί με κάποιες εργατοώρες μέχρι να ολοκληρωθεί η εργασία ενώ τα βιομετρικά χαρακτηριστικά δε χάνονται ούτε φθείρονται ώστε να αντικατασταθούν.
https://www.academia.edu/1802094/E-
Banking Security Issues Is There A Solution in Biometrics

Τα βιομετρικά συστήματα ελέγχου πρόσβασης παρουσιάζουν πολλά πλεονεκτήματα σε σχέση με τις παραδοσιακές μεθόδους ταυτοποίησης όπως μαγνητικές κάρτες λωρίδων, έξυπνες κάρτες ή κωδικούς πρόσβασης που πιθανό να χαθούν, να ξεχαστούν ή να διαρρεύσουν. Φυσικά δε μπορούμε να πούμε ότι όλοι οι τύποι βιομετρικού συστήματος είναι τέλεια λειτουργικοί και ικανοποιητικοί σε όλες τις ανάγκες. Διαφορετικές τεχνολογίες μπορεί να είναι κατάλληλες για διαφορετικές εφαρμογές, ανάλογα με το προφίλ των χρηστών, την ανάγκη διασύνδεσης με άλλα συστήματα ή βάσεις δεδομένων, τις περιβαλλοντικές συνθήκες και άλλες ειδικές παραμέτρους εφαρμογής. Το βιομετρικό σύστημα καθίσταται χρήσιμο και ασφαλές χάρις στη μοναδικότητα των στοιχείων που χρησιμοποιεί για τη λειτουργία του. Είναι παγκοσμίως γνωστό ότι ο κάθε άνθρωπος έχει μοναδικό δακτυλικό αποτύπωμα. Επομένως είναι δύσκολο έως αδύνατον να κλαπεί, να ξεχαστεί ή να διαρρεύσει. Επίσης,

μπορούμε να τονίσουμε ότι τα συστήματα αυτά έχουν τη δυνατότητα για επικύρωση με γρήγορο και εύκολο τρόπο χωρίς να απαιτεί από το χρήστη περισσότερες πληροφορίες. Σύμφωνα με τη Mastercard, σε περίπτωση πιθανής αγοράς, το ποσοστό εγκατάλειψης της μειώνεται έως και 70% με τη χρήση βιομετρικού ελέγχου πρόσβασης από ότι με άλλες μεθόδους όπως 2FA (two-factor-authentication) μέσω ενός smsστο κινητό.https://m.naftemporiki.gr/story/1314989/asfalesteres-online-sunallages-me-biometrics

Εικόνα 9: Βιομετρικό σύστημα δακτυλικού αποτυπώματος

Τεχνικές μέτρησης και τύποι Βιομετρικού Συστήματος

Οι τεχνικές μέτρησης που χρησιμοποιεί ένα σύστημα ελέγχου πρόσβασης χωρίζονται σε αυτές που βασίζονται σε κάποιο φυσικό χαρακτηριστικό και σε αυτές που εξαρτώνται από τη συμπεριφορά-ψυχολογία του χρήστη.

Στη πρώτη κατηγορία οι τύποι βιομετρικών συστημάτων είναι οι παρακάτω:

- Δακτυλικό αποτύπωμα. Πρόκειται για την αναγνώριση του δακτυλικού αποτυπώματος που είναι μοναδικό σε κάθε χρήστη.Το δακτυλικό αποτύπωμα δεν αλλοιώνεται με το πέρασμα του χρόνου. Η αναγνώρισηδακτυλικών αποτυπωμάτων περιλαμβάνει τη λήψη μιας εικόνας δακτυλικών αποτυπωμάτων ενός ατόμου και καταγράφει τα χαρακτηριστικά του όπως καμάρες, περιγράμματα των άκρων και των αυλάκων. Για να γίνει η συλλογή αποτυπώματος χρησιμοποιούνται οπτικοί αισθητήρες που χρησιμοποιούν αισθητήρα εικόνας CMOSή CCD. Η σάρωση δακτυλικού ίχνους είναι πολύ σταθερή και αξιόπιστη. Προστατεύει τις συσκευές εισόδου και η πρόσβαση στο δίκτυο γίνεται όλο και πιο αμοιβαία. Επί του παρόντος, ένας μικρός αριθμός τραπεζών έχουν αρχίσει να χρησιμοποιούν αναγνώστες δακτυλικού αποτυπώματος στα ΑΤΜ.
- Σχήμα προσώπου. Εδώ συγκρίνεται το σχήμα του προσώπου, της μύτης και άλλων χαρακτηριστικών.Ένα σύστημα αναγνώρισης προσώπου είναι ένας τύπος βιομετρικής εφαρμογής ηλεκτρονικού υπολογιστή που μπορεί να αναγνωρίσει ή να επαληθεύσει ένα άτομο από μια ψηφιακή εικόνα συγκρίνοντας και αναλύοντας τα πρότυπα. Τα υπάρχοντα αναγνωριστικά συστήματα μπορούν να αναγνωρίσουν 80 κομβικά σημεία σε ένα ανθρώπινο πρόσωπο. Τα σημεία αυτά δεν είναι τίποτα άλλο από τα τελικά σημεία που χρησιμοποιούνται για τη μέτρηση των μεταβλητών στο πρόσωπο ενός ατόμου, το οποίο περιλαμβάνει το μήκος και ο πλάτος της μύτης, το βάθος της κοιλότητας των ματιών και το σχήμα των ζυγωματικών. Τα συστήματα αυτά επικεντρώνονται σε εφαρμογές των smartphones. Παράδειγμα μέσα κοινωνικής δικτύωσης όπως το facebookχρησιμοποιούν λογισμικό αναγνώρισης προσώπου για την επισήμανση των χρηστών σε φωτογραφίες. Επίσης, στο τομέα της εμπορίας, οι διαφημιστικές πινακίδες έχουν λογισμικό αναγνώρισης της ηλικίας, του φύλλου και της εθνικότητας ώστε να προσφέρουν στοχευμένο μάρκετινγκ.

Εικόνα 10: Βιομετρικό σύστημα αναγνώρισης προσώπου

- Σάρωση ίριδας του ματιού. Εδώ ελέγχεται η μορφολογία των αγγείων του ματιού που είναι μοναδικό για το καθένα.Η αναγνώριση ίριδας είναι ένας τύπος μεθόδου βιομετρίας που χρησιμοποιείται για την ταυτοποίηση των ανθρώπων βάσει μονών μοτίβων στη δακτυλιοειδή περιοχή που περιβάλλει το μάτι του χρήστη.

Εικόνα 11: Βιομετρικό σύστημα ανάλυσης ίριδας

- Σχήμα χεριού. Εστιάζει στο σχήμα των κλειδώσεων και το μήκος των δαχτύλων.Οι βιομετρίες γεωμετρίες χεριών αναφέρονται στη μέτρηση των χαρακτηριστικών των χεριών όπως το μήκος και το πλάτος των δακτύλων, η καμπυλότητα τους και η σχετική τους θέση με άλλα χαρακτηριστικά του χεριού.
  https://www.ibeta.com/different-types-of-biometrics/
- Ανάλυση DNA. Πολύ αξιόπιστη αλλά χρονοβόρα καθώς το δείγμα δε συγκρίνεται άμεσα.Το DNA έχει χρησιμοποιηθεί από καιρό για σκοπούς αναγνώρισης. Επιπλέον είναι η μόνη μορφή βιομετρικών στοιχείων που μπορεί να ανιχνεύσει οικογενειακούς δεσμούς. Η αντιστοίχιση του DNA είναι ιδιαίτερα χρήσιμηόταν ασχολείται με αγνοούμενα πρόσωπα, τον

εντοπισμό θυμάτων καταστροφών και τη πιθανή εμπορία ανθρώπων. Το DNA που συγκεντρώνεται από τα μαλλιά, το σάλιο, το σπέρμα και ούτω καθεξής περιέχει αλληλουχίες ShortTandemRepeat (STR). Οι STR μπορούν να επιβεβαιώσουν τη ταυτότητα συγκρίνοντας τες με άλλες STR σε μια βάση δεδομένων.
https://www.ibeta.com/different-types-of-biometrics/

- Αγγειακό σχήμα. Βασίζεται στο σχήμα των φλεβών του χεριού.Οι φλέβες είναι πολύ πιο δύσκολο να αποτυπωθούν σε σχέση με άλλες βιομετρικές ανιχνεύσεις επειδή εμφανίζονται βαθιά μέσα στο δέρμα. Τα υπέρυθρα φώτα περνούν από την επιφάνεια του δέρματος όπου απορροφούνται σε αποξυγονωμένο αίμα. Μια ειδική κάμερα καταγράφει την εικόνα που ψηφιοποιεί τα δεδομένα, στη συνέχεια τα αποθηκεύει ή τα χρησιμοποιεί για επιβεβαίωση της ταυτότητας.
https://www.ibeta.com/different-types-of-biometrics/

Στη δεύτερη κατηγορία οι τύποι βιομετρικών συστημάτων είναι:

- Ανάλυση φωνής. Πρόκειται για έλεγχο του τρόπου που το άτομο μιλάει. Η τεχνολογία φωνητικής αναγνώρισης χρησιμοποιείται για την παραγωγή προτύπων ομιλίας συνδυάζοντας φυσιολογικούς παράγοντες και συμπεριφοράς που μπορούν να ληφθούν με την επεξεργασία της τεχνολογίας ομιλίας. Οι πιο σημαντικές ιδιότητες που χρησιμοποιούνται για την ταυτοποίηση ομιλίας είναι ο ρινικός τόνος, η κλίση, ο ρυθμός και η θεμελιώδης συχνότητα. Η αναγνώριση της φωνής μπορεί να χωριστεί σε διαφορετικές κατηγορίες βάσει του είδους του τομέα επαλήθευσης, όπως είναι η μέθοδος σταθερού κειμένου, η μέθοδος που εξαρτάται από το κείμενο και η τεχνική συνομιλίας.
- Αναγνώριση βηματισμού. Βασίζεται στο βηματισμό του καθένα που είναι μοναδικός.
- Αναγνώριση υπογραφής. Ελέγχεται ο τρόπος και η ταχύτητα που κάποιος σχεδιάζει την υπογραφή του.Η αναγνώριση υπογραφών είναι ένας τύπος βιομετρικής μεθόδου που χρησιμοποιείται για την ανάλυση και τη μέτρηση της φυσικής δραστηριότητας της υπογραφής, όπως η

πίεση που εφαρμόστηκε και η ταχύτητα. Μερικά βιομετρικά στοιχεία χρησιμοποιούνται για να συγκρίνουν τις οπτικές εικόνες των υπογραφών. Η αναγνώριση των υπογραφών γίνεται με δύο τρόπους, τη στατική και τη δυναμική.

Σε στατική λειτουργία, οι χρήστες συντάσσουν την υπογραφή τους σε χαρτί και την ψηφιοποιούν μέσω κάμερας ή οπτικού σαρωτή. Αυτό το σύστημα αναγνωρίζει την υπογραφή εξετάζοντας το σχήμα της.
Σε δυναμική υπογραφή, οι χρήστες γράφουν την υπογραφή ψηφιοποιημένη σε ένα tabletto οποίο λαμβάνει την υπογραφή σε πραγματικό χρόνο. Ορισμένα βιομετρικά στοιχεία λειτουργούν επίσης σε smartphonesτα οποία έχουν οθόνη αφής όπου ο χρήστης μπορεί να υπογράψει χρησιμοποιώντας μια πένα ή το δάχτυλό του.

Εικόνα 12: Βιομετρικό σύστημα αναγνώρισης υπογραφής
https://www.ibeta.com/different-types-of-biometrics/

Τα χαρακτηριστικά του Βιομετρικού Συστήματος

Τα χαρακτηριστικά ενός Βιομετρικού συστήματος είναι η αξιοπιστία, η ακρίβεια, η ταχύτητα, οι απαιτήσεις της επεξεργασίας και η διαδικασία αποθήκευσης αυτών σε ένα μέσο, η μοναδικότητα, η αντίσταση παραποίησης στοιχείων και η αποδοχή του χρήστη. Αναφέρονται παρακάτω πιο αναλυτικά.

Αξιοπιστία

Στη περίπτωση αυτή ένα σύστημα θεωρείται αξιόπιστο αν χαρακτηρίζεται από ακριβής, γρήγορη και συνεχή λειτουργία με όσο το δυνατόν λιγότερο έλεγχο λειτουργίας και συντήρησης.

Ακρίβεια

Αφορά τη δυνατότητα του συστήματος να μπορεί να κρίνει αν πρόκειται για το εξουσιοδοτημένο ή μη άτομο. Οι μονάδες μέτρησης που χρησιμοποιούνται είναι είτε το ποσοστό απόρριψης των εξουσιοδοτημένων ατόμων είτε το ποσοστό αποδοχής των μη εξουσιοδοτημένων. Αυτές οι δύο μετρήσεις έχουν σαν σημείο τομής το Ολικό Επίπεδο Σφάλματος. Αυτό σημαίνει ότι όταν σε ένα τέτοιο σύστημα απαιτείται να μην γίνεται αποδοχή ένας μη εξουσιοδοτημένου χρήστη, ο δείκτης ποσοστού του σφάλματος αποδοχής θα είναι περίπου στο 0%.

Ταχύτητα

Σημαντικό ρόλο παίζει η ταχύτητα απόκρισης. Δηλαδή μέσα σε πόσο χρόνο γίνεται η αναγνώριση του χρήστη.

Απαιτήσεις της επεξεργασίας και διαδικασία αποθήκευσης.

Τα χαρακτηριστικά αυτά επηρεάζουν το χρόνο αναγνώρισης ενός χρήστη καθώς αν απαιτείται από το σύστημα να ικανοποιεί όσο το δυνατόν μικρότερο επίπεδο αποδοχής σφάλματος τόσο πιο πολύ χρόνο χρειάζεται για να συγκριθούν τα στοιχεία με αυτά στη βάση δεδομένων. Εκτιμάται ότι ένα αρχείο βιομετρικών στοιχείων είναι περίπου 256 με 1000 bytes.

Μοναδικότητα

Καθώς τα βιομετρικά συστήματα δουλεύουν με βάση κάποιο χαρακτηριστικό του ανθρώπου που είναι μοναδικό, εξασφαλίζεται η αποφυγή λαθών κατά την αναγνώριση.

Αντίσταση παραποίησης στοιχείων

Ακριβώς επειδή στόχος των συστημάτων αυτών είναι να μην έχει πρόσβαση κάποιος μη εξουσιοδοτημένος χρήστης, είναι απαραίτητο το χαρακτηριστικό που θα συλλεχθεί για τη ταυτοποίηση να είναι όσο γίνεται αναλλοίωτο στο χρόνο.

Αποδοχή από το χρήστη

Βέβαια ακριβώς επειδή τα βιομετρικά συστήματα βασίζονται σε προσωπικά χαρακτηριστικά για τα οποία απαιτείται να αποθηκεύονται σε μια βάση δεδομένων, πολλοί είναι αυτοί που αντιδρούν αρνητικά βασιζόμενοι στη καταπάτηση προσωπικών δικαιωμάτων. Επίσης, φοβούνται για τυχόν πρόκληση σωματικής βλάβης όπως τύφλωση από τη κόκκινη δέσμη που σαρώνει την ίριδα του ματιού. Για αυτό είναι αναγκαία η ενημέρωση των χρηστών σχετικά με τη τεχνολογία των βιομετρικών συστημάτων ώστε να γίνει αποδεκτή και επιτυχής η εφαρμογή τους.

Πλεονεκτήματα και μειονεκτήματα βιομετρικής τεχνολογίας

Μπορεί με αυτές τις μεθόδους ασφαλείας να διευκολύνουμε τη ζωή μας απαλλάσσοντας την από το να βρεθούμε σε ένα φυσικό κατάστημα τραπέζης, να θυμόμαστε έναν κωδικό ή να προσέχουμε συνεχώς αν θα κλαπεί η πιστωτική μας κάρτα, αλλά υπάρχει ένα βασικό μειονέκτημα που πολλοί δίνουν έμφαση, η ιδιωτικότητα.

Πλεονεκτήματα

- Δεν απαιτεί κάποιο υλικό μέσο όπως κάρτα.
- Δύσκολο να ξεχαστούν ή να χαθούν.
- Δεν απαιτεί ανανέωση του φυσικού χαρακτηριστικού όπως γίνεταιμε τη λήξη των κωδικών.
- Γρήγορη διαδικασία εξουσιοδότησης.

Μειονεκτήματα

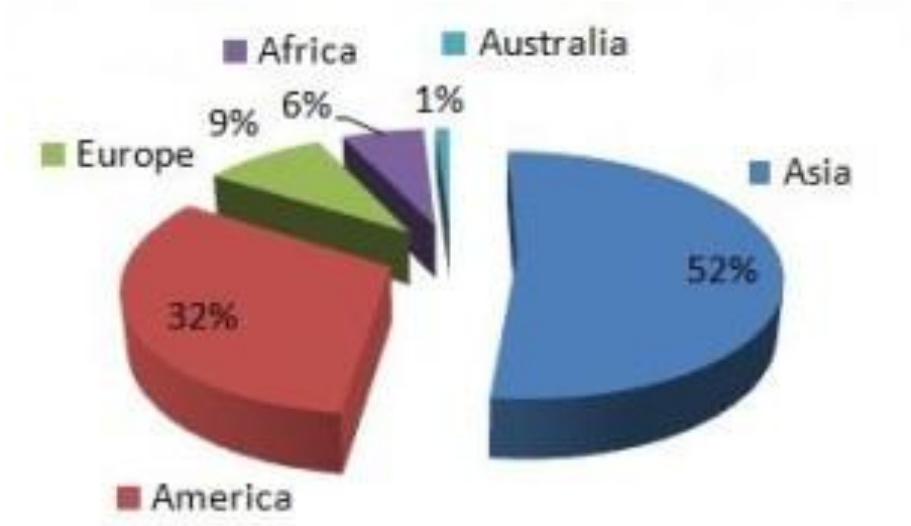
- Απαιτεί μεγάλες βάσεις δεδομένων.
- Χρονοβόρα διαδικασία καταχώρησης των χαρακτηριστικών.
- Υψηλό κόστος κατασκευής και συντήρησης.
- Η κοινωνική άποψη ότι η αποθήκευση προσωπικών χαρακτηριστικών είναι καταπάτηση προσωπικής ιδιωτικότητας.
- Ο φόβος ότι η ακτίνες lazer βλάπτουν την υγεία.

Η επίδραση των Biometrics στις ηλεκτρονικές συναλλαγές

Η γρήγορη ψηφιοποίηση των τραπεζικών υπηρεσιών σε συνδυασμό με τη συνεχή ανάγκη θέσπισης αυστηρότερων πρωτοκόλλων ταυτοποίησης πελατών και εργαζομένων για τη πρόληψη της κλοπής ταυτότητας, έθεσε τη τεχνολογία της βιομετρίας σημαντικό τμήμα των συστημάτων ασφαλείας των τραπεζικών υπηρεσιών. Ενεργώντας ως ισχυρό εργαλείο ελέγχου πρόσβασης για την ασφάλεια ηλεκτρονικών συναλλαγών, η βιομετρική τεχνολογία στο τραπεζικό τομέα συμβάλλει επίσης στην αύξηση της εμπιστοσύνης των πελατών. Λόγω του αυξανόμενου ρυθμού υιοθέτησης των ηλεκτρονικών συναλλαγών αλλά και των παραβιάσεων ασφαλείας, η ανάγκη για μια ισχυρότερη λύση ελέγχου πρόσβασης κατέστη αναπόφευκτη.

Πολλές τράπεζες παγκοσμίως ήδη έχουν εφαρμόσει και χρησιμοποιούν βιομετρική τεχνολογία για την ταυτοποίηση των πελατών τους και μάλιστα το 52% είναι τράπεζες στην Ασία. Στην Ιαπωνία υπάρχουν περίπου 15

εκατομμύρια χρήστες ηλεκτρονικής συναλλαγής που χρησιμοποιούν κάποιο βιομετρικό τους χαρακτηριστικό για την ταυτοποίηση τους.



Διάγραμμα 2: Χώρες που χρησιμοποιούν biometricsσε τραπεζική συναλλαγή

Η αντικατάσταση των παραδοσιακών τρόπων πρόσβασης όπως αριθμός PINή tokenσυσκευήγίνεται με αργούς ρυθμούς. Παρακάτω αναφέρω τρόπους με τους οποίους οι τράπεζες χρησιμοποιούν βιομετρική τεχνολογία για τη βελτίωση της αποδοτικότητας των συναλλαγών και τη προστασία των περιουσιακών στοιχείων των πελατών τους.

- Βιομετρία στα καταστήματα τραπεζών

Το δακτυλικό αποτύπωμα είναι το πιο συχνό χαρακτηριστικό που χρησιμοποιούν οι χρηματοπιστωτικές υπηρεσίες καθώς παρέχει γρήγορα αποτελέσματα ελέγχου και είναι κατάλληλα για τους πιο συχνούς σε χρήση κλάδους της τραπεζικής. Επιπλέον, είναι φιλικά προς το χρήστη, εύκολο στη χρήση και αξιόπιστα όσον αφορά την ασφάλεια. Αφού γίνει σύγκριση και ταυτοποιηθεί το ήδη βιομετρικό πρότυπο που είναι αποθηκευμένο σε μια βάση δεδομένων με το τρέχον δακτυλικό αποτύπωμα που προσφέρεται εκείνη τη στιγμή, ο χρήστης μπορεί να προχωρήσει στις τραπεζικές του συναλλαγές.

- Βιομετρία στα τραπεζικά ATM

Η χρήση βιομετρικών στοιχείων στα ATMείναι δημοφιλής στις ανεπτυγμένες χώρες και το ποσοστό υιοθεσίας αυξάνεται σημαντικά. Υπάρχουν δυο προσεγγίσεις για τον έλεγχο ταυτότητας πελατών σε ATM.

Από τη μια ένας πελάτης χρησιμοποιεί μια κάρτα και ένα βιομετρικό χαρακτηριστικό και από την άλλη έναν αριθμό PIN και ένα βιομετρικό στοιχείο του. Επομένως, το δακτυλικό αποτύπωμα, η αναγνώριση προσώπου και της ίριδας και τα μοτίβα των φλεβών των δακτύλων είναι τα πιο κατάλληλα για ATM συναλλαγές καθώς τα χαρακτηριστικά αυτά είναι εύκολα αναγνωρίσιμα από το περιβάλλον αυτό. Σίγουρα, η ακρίβεια αυτών παίζει σημαντικό ρόλο στην επιβεβαίωση της καταλληλότητα τους.

- Βιομετρία για το Internet Banking

Οι φορητοί υπολογιστές και τα smartτηλέφωνα έχουν ήδη μικρόφωνα, κάμερες και σαρωτή δακτυλικού αποτυπώματος. Αυτό κάνει ακόμα πιο εύκολο το έργο των τραπεζών να υιοθετήσουν τη βιομετρική τεχνολογία στις ηλεκτρονικές συναλλαγές. Υπάρχουν τράπεζες που απαιτούν εκτός από το πληκτρολόγηση του παραδοσιακού κωδικού πρόσβασης και μια βιομετρική ταυτοποίηση για να ενισχύσουν τον έλεγχο ταυτότητας. Αυτό βοηθά στο να αποφεύγονται οι παράνομες προσπάθειες απόκτησης ευαίσθητων πληροφοριών.

- Βιομετρία στο Mobile Banking

Το mobilebankingαυξάνεται ταχύτατα παγκοσμίως. Σύμφωνα με έρευνα της JuniperResearchτο 2013, 400 εκατομμύρια χρήστες πραγματοποίησαν mobilebanking. Παρόλα αυτά πολλοί είναι αυτοί που δεν εμπιστεύονται τις πλατφόρμες για mobilebankingενισχύοντας έτσι ανησυχίες για την ασφάλεια. Ένα παράδειγμα είναι οι πελάτες να χρησιμοποιούν το μικρόφωνο στα κινητά τους τηλέφωνα ώστε μέσα από ένα σύστημα αναγνώρισης της φωνής να επαληθεύουν τη ταυτότητά τους.

- Βιομετρία στο Single Sign On

Σύμφωνα με την ACI, το 44% των τραπεζικών λογαριασμών έχει τεθεί σε κίνδυνο ενώ το 15% των παραβάσεων έχει καταλήξει σε απάτη. Οι τράπεζες

μπορούν εύκολα να υιοθετήσουν λύσεις βιομετρικής SSOστο δίκτυο τους για διαχείριση κωδικών, ταυτότητας, ασφάλειας δεδομένων και έλεγχο 2FA (twofactorauthentication). Έτσι θα εξαλειφθούν τα κενά των συστημάτων ασφαλείας των τραπεζών και θα αποτρέψει μη εξουσιοδοτημένη πρόσβαση και παραβιάσεις δεδομένων.
http://www.m2sys.com/blog/financial-services/impact-biometrics-banking/

Διαφορές Βιομετρικών χαρακτηριστικών συμπεριφοράς με φυσιολογικών

Όσον αφορά τις πιθανές εφαρμογές, η διαφοροποίηση μεταξύ συμπεριφορικής και φυσιολογικής βιομετρίας έχει μεγάλη σημασία για πολλούς λόγους που εξαρτώνται από τη δήλωση προθέσεων, τη ταυτοποίηση και τη βεβαιότητα.

Σενάρια όπου ο έλεγχος ταυτότητας συνδέεται με ρητή συγκατάθεση στη διαδικασία επαλήθευσης, τα συστήματα συμπεριφοράς θεωρούνται πιο κατάλληλα από τα φυσιολογικά. Τέτοια περίπτωση είναι το σύστημα που χρησιμοποιεί την υπογραφή που είναι κοινωνικά αποδεκτό εδώ και πολλούς αιώνες.

Οι εφαρμογές όπου η αυτοματοποιημένη ταυτοποίηση των χρηστών έχει προσδιοριστεί από πριν, τα φυσιολογικά χαρακτηριστικά είναι ιδανικά. Τα χαρακτηριστικά συμπεριφοράς μπορούν πιο εύκολα να απορριφθούν όπως αν δε ταιριάζει ο τρόπος γραφής της υπογραφής. Στη περίπτωση ταυτοποίησης ενός εγκληματία τα φυσιολογικά χαρακτηριστικά όπως η αναγνώριση προσώπου, φαίνονται πιο πρακτικά
Στη Τρίτη περίπτωση

Κεφάλαιο 4

Ανάλυση αποτελεσμάτων

Μεθοδολογία έρευνας

Σύμφωνα με τη βιβλιογραφία, για μια ποσοτική έρευνα οι διάφορες μέθοδοι συλλογής δεδομένων και οι μέθοδοι συλλογής υλικού που χρησιμοποιούνται είναι: οι συνεντεύξεις, τα ερωτηματολόγια, η παρατήρηση, η ανάλυση περιεχομένου, η ανάλυση επίσημων στατιστικών και τα ελεγχόμενα πειράματα. (Λαγουμιντζής, 2015)

Στη παρούσα εργασία, η μέθοδος που επιλέχθηκε για τη διεξαγωγή της έρευνας είναι το ερωτηματολόγιο, το οποίο δομήθηκε κυρίως με ερωτήσεις κλειστού τύπου. Το ερωτηματολόγιο αποτελεί ίσως τη πιο διαδεδομένη ερευνητική μέθοδο κλειστού τύπου για τη συλλογή στοιχείων στη ποσοτική έρευνα. (Ζαφειρόπουλος, 2005). Η αναγνωσιμότητά τους ως αποτελεσματικό εργαλείο οφείλεται κυρίως στο ότι παρουσιάζει μεγάλη ευελιξία και προσαρμοστικότητα ως προς τους τρόπους με τους οποίους μπορούν να εκφραστούν οι ερωτήσεις. Στα πλεονεκτήματα του συγκαταλέγονται η δυνατότητα για άμεση αποδελτίωση, η δυνατότητα συλλογής πολλών δεδομένων, οι συνθήκες διαμόρφωσης των ερωτήσεων που ευνοούν την αντικειμενικότητα της έρευνας, δηλαδή οι ερωτώμενοι μπορούν να εκφραστούν ελεύθερα και ο ερευνητής δε μπορεί να επηρεάσει τις απαντήσεις, είναι οικονομικότερο και θεωρείται

λιγότερο χρονοβόρα μέθοδος. Στα μειονεκτήματα του εντοπίζονται θέματα σχετικά με τον έλεγχο των άγνωστων συνθηκών συμπλήρωσης του ερωτηματολογίου, τις οποίες ο ερευνητής δεν είναι πάντα σε θέση να ελέγξει, υπάρχει και το ενδεχόμενο της μη κατανόησης των ερωτημάτων, ενώ τέλος υποχρεώνει τον ερωτηθέντα να απαντήσει με ένα συγκεκριμένο τρόπο. (Ζαφειρόπουλος, 2005, Λαγουμιντζής, 2015).

Τα ερωτηματολόγια μπορούν να διαμορφωθούν με διαφορετικού τύπου ερωτήσεις, οι οποίες σε γενικές γραμμές έχουν τις εξής μορφές:

- Ερωτήσεις κλειστού τύπου (δομημένες): Πρόκειται για ερωτήσεις που παρέχουν μια σειρά προκαθορισμένων, από τον ερευνητή, απαντήσεων.
- Ερωτήσεις ανοιχτού τύπου (μη δομημένες): Επιτρέπουν στους ερωτώμενους να απαντήσουν με πλήρη ελευθερία, χωρίς να περιορίζονται μέσα από προκαθορισμένες απαντήσεις.

Η συγκεκριμένη έρευνα ξεκινά με πέντε ερωτήσεις:

- Ποια η ηλικία σας;**(ερώτηση 1)**
- Ποιο το επίπεδο σπουδών σας;**(ερώτηση 2)**
- Ποια η κύρια απασχόληση σας;**(ερώτηση 3)**
- Πόσο χρησιμοποιείτε το internetστη ζωή σας;**(ερώτηση 4)**
- Κατά πόσο είστε φιλικός με τις τεχνολογικές καινοτομίες;**(ερώτηση 5)**

Στη συνέχεια, ζητείται να απαντηθούν ερωτήσεις που αφορούν τα εξής:

- Κατά πόσο χρησιμοποιείτε τις παρακάτω μεθόδους για τις τραπεζικές σας συναλλαγές;**(ερώτηση 6)**
- Χρησιμοποιείτε e-banking; **(ερώτηση 7)**
- Αν ναι, πόσο χρονικό διάστημα;**(ερώτηση 8)**
- Κατά πόσο το θεωρείται ασφαλές;**(ερώτηση 9)**

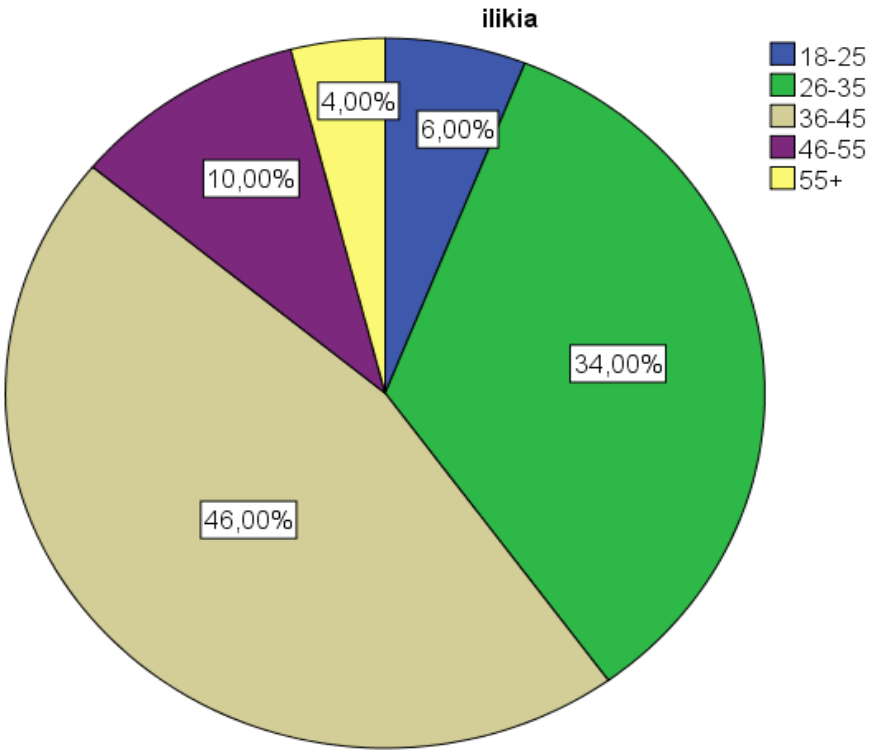
- Έχετε ακούσει να συμβαίνουν στο περίγυρό σας πλαστοπροσωπία και κλοπή διαπιστευτηρίων σε ηλεκτρονικές συναλλαγές ή ακόμα και σε απλές τραπεζικές συναλλαγές;**(ερώτηση 10)**
- Είστε ικανοποιημένος από τη εξυπηρέτηση μέσω ηλεκτρονικής τραπεζικής;**(ερώτηση 11)**
- Τι θεωρείτε πιο σημαντικό στο e-banking;**(ερώτηση 12)**
- Με το e-bankingπιστεύετε αυξάνεται η απόδοση των τραπεζικών συναλλαγών;**(ερώτηση 13)**
- Γνωρίζετε σχετικά με τις βιομετρικές τεχνολογίες;**(ερώτηση 14)**
- Πιστεύετε ότι το πολιτισμικό επίπεδο (π.χ ο τρόπος αντίληψης της ζωής) μιας χώρας καθορίζει τη χρήση ή μη των βιομετρικών τεχνολογιών στο onlinebanking;**(ερώτηση 15)**
- Στη περίπτωση που γνωρίζετε, ποιο από τα παρακάτω βιομετρικά συστήματα θα επιλέγατε για τις onlineσυναλλαγές;**(ερώτηση 16)**
- Εσείς σήμερα χρησιμοποιείτε κάποια βιομετρική τεχνολογία στις τραπεζικές σας συναλλαγές;**(ερώτηση 17)**
- Σε σχέση με την εισαγωγή κωδικού PIN, θεωρείτε τις βιομετρικές τεχνολογίες πιο ασφαλείς;**(ερώτηση 18)**
- Κατά πόσο θα εμπιστευόσασταν σε οργανισμούς όπως τράπεζες τα βιομετρικά σας χαρακτηριστικά;**(ερώτηση 19)**
- Αν τις επόμενες μέρες κιόλας, η τράπεζα που συνεργάζεστε σας πρότεινε να δώσετε κάποιο βιομετρικό στοιχείο για να προχωρήσει σε βιομετρική onlinetραπεζική, κατά πόσο θα ήσασταν θετικοί;**(ερώτηση 20)**
- Για ποιον από τους παρακάτω λόγους, κατά προτεραιότητα, δε θα χρησιμοποιούσατε τα biometricsστο onlinebanking;**(ερώτηση 21)**
- Γνωρίζοντας ότι τα βιομετρικά συστήματα είναι εξαιρετικά ασφαλή, η πιθανόν μικρότερη ταχύτητα ανταπόκρισης σε σχέση με την εισαγωγή PIN θα σας επηρέαζε αρνητικά;**(ερώτηση 22)**
- Έστω ότι προχωρούσατε σε βιομετρική onlinetραπεζική, πως πιστεύετε θα ήταν πιο ασφαλής ο τρόπος αποθήκευσης του βιομετρικού σας χαρακτηριστικού;**(ερώτηση 23**

Ανάλυση αποτελεσμάτων

Περιγραφική στατιστική

Ερώτηση 1: ποια η ηλικία σας;

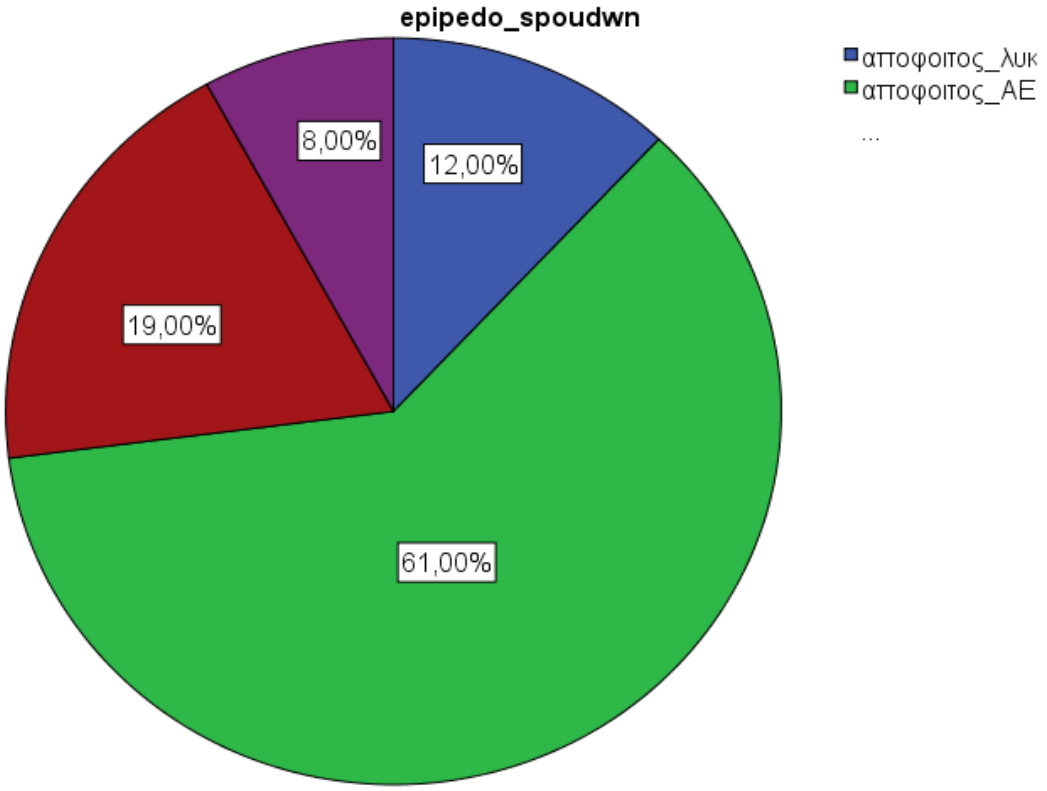
Στη πρώτη ερώτηση του ερωτηματολογίου παρουσιάζονται οι ηλικίες του δείγματος που επέλεξα να απευθυνθώ. Συγκεκριμένα, ηλικίας 36-45 είναι το 46% του δείγματος και 26-35 το 34%. Ακολουθούν οι ηλικίες 45-55 με 10%, 18-25 και 55+ με 6% και 4% αντίστοιχα.



Διάγραμμα 3: Ηλικία δείγματος

Ερώτηση 2: ποιο το επίπεδο σπουδών σας;

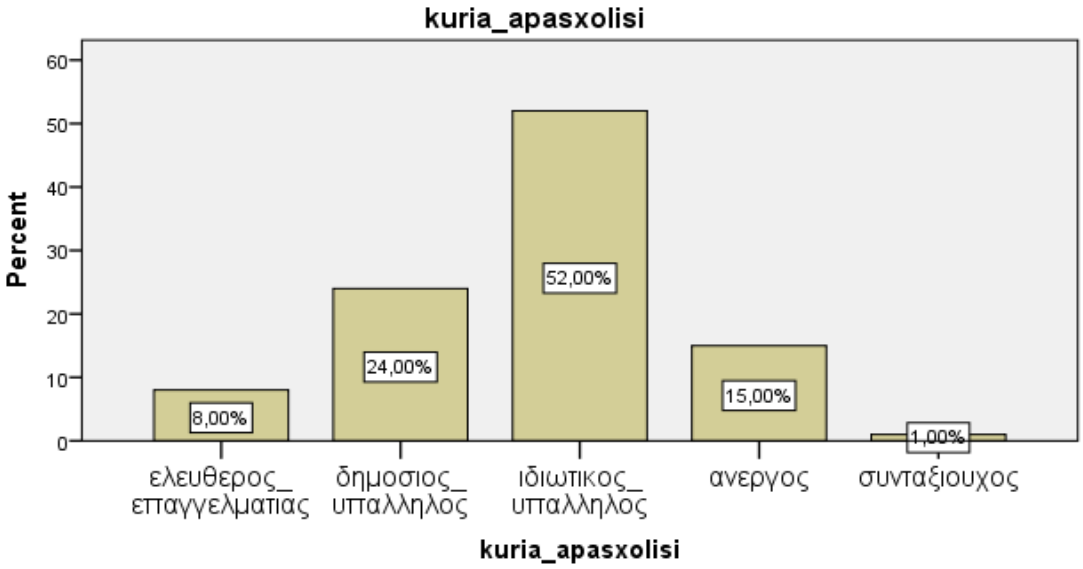
Το μεγαλύτερο ποσοστό με 61% είναι απόφοιτοι ΑΕΙ/ΤΕΙ. Ακολουθούν οι κάτοχοι μεταπτυχιακού τίτλου με 19% και στη συνέχεια έχουμε τους αποφοίτους λυκείου και τους κάτοχους διδακτορικού με 12% και 8% αντίστοιχα.



Διάγραμμα 4: Επίπεδο σπουδών

Ερώτηση 3: ποια η κύρια απασχόλησή σας;

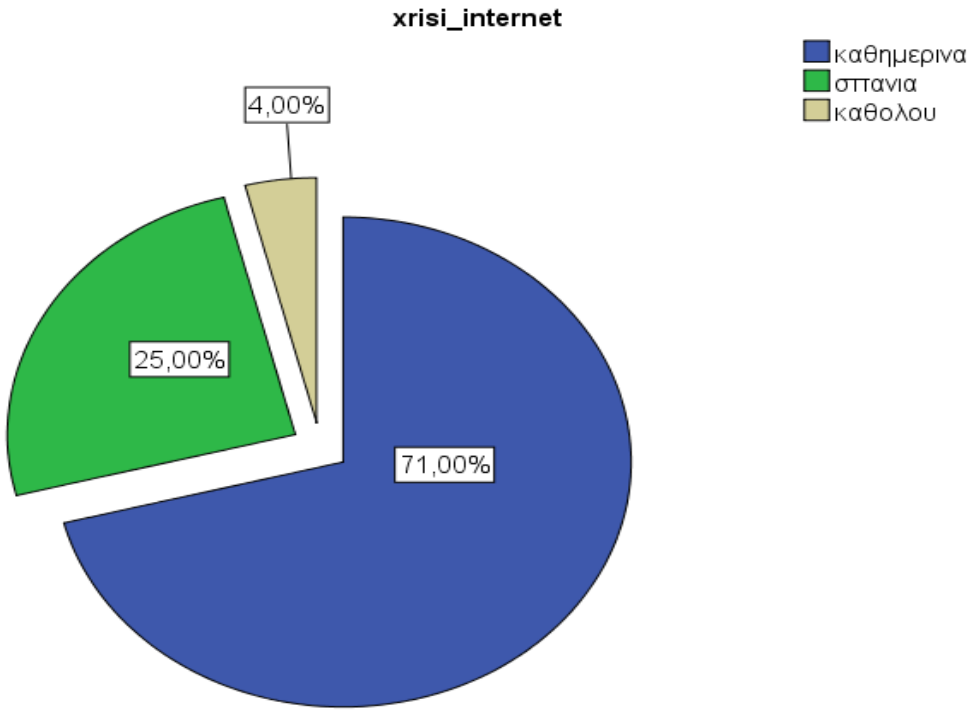
Οι περισσότεροι που ερωτήθηκαν είναι ιδιωτικοί υπάλληλοι, 52%, οι δημόσιοι υπάλληλοι είναι 24%. Επίσης το ποσοστό του 15% αντιστοιχεί στους ανέργους. Ακολουθούν οι ελεύθεροι επαγγελματίες με 8% και οι συνταξιούχοι με 1%



Διάγραμμα 5: Κύρια απασχόληση

Ερώτηση 4: πόσο χρησιμοποιείτε το internet στη ζωή σας;

Το 71% χρησιμοποιεί το internet καθημερινά. Ενώ το 25% σπάνια με ένα ποσοστό 4% για αυτούς που δε το χρησιμοποιούν καθόλου.

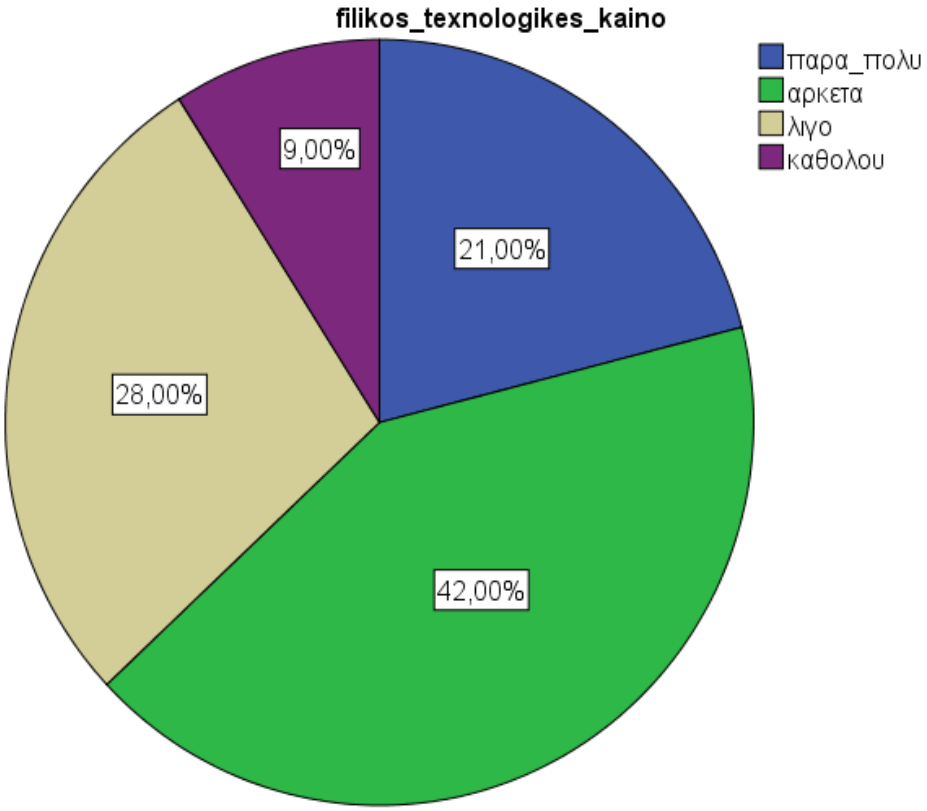


Διάγραμμα 5: Συχνότητα χρήσης internet

Ερώτηση 5: κατά πόσο είστε φιλικός με τις τεχνολογικές καινοτομίες;

Παρατηρούμε ότι υπάρχει ένα καλό ποσοστό, 42%, για αυτούς που προσαρμόζονται αρκετά με τις τεχνολογικές καινοτομίες, ένα 28% που πιθανόν να μην είναι και τόσο φιλικοί ενώ το 21% του δείγματος μου δεν έχουν κανένα

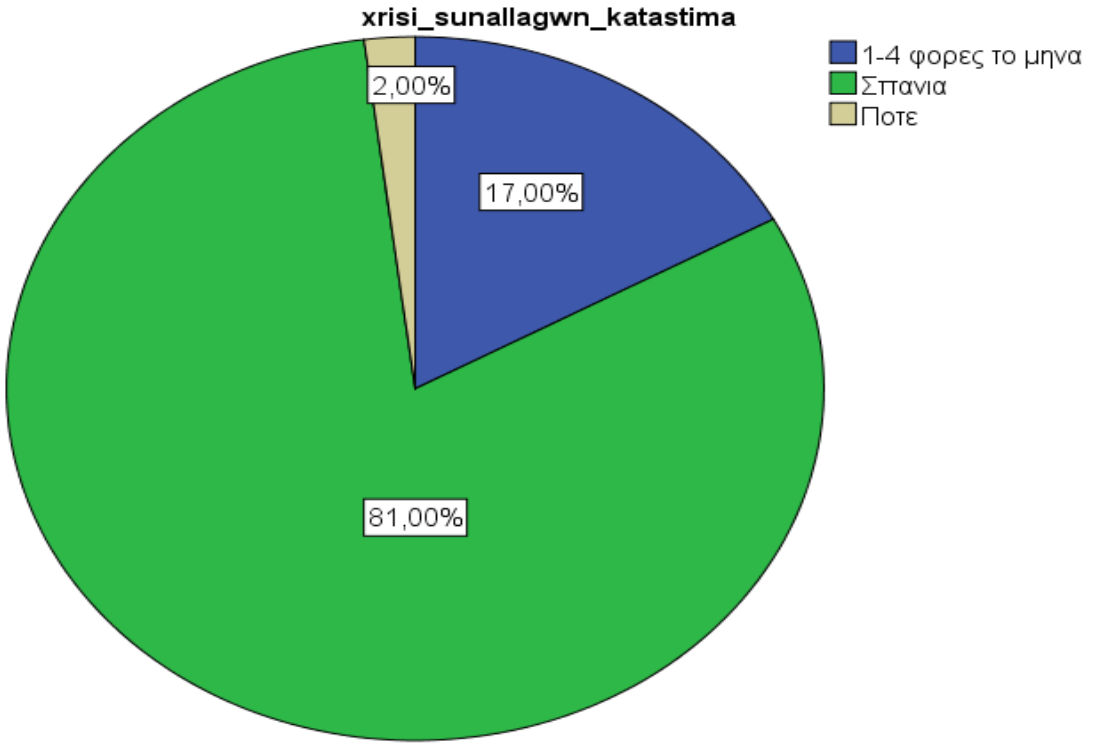
πρόβλημα με τις νέες τεχνολογίες. Τέλος, το 9% δε τα πάει καθόλου καλά με τις τεχνολογικές καινοτομίες.



Διάγραμμα 7: Φιλικός με τεχνολογικές καινοτομίες

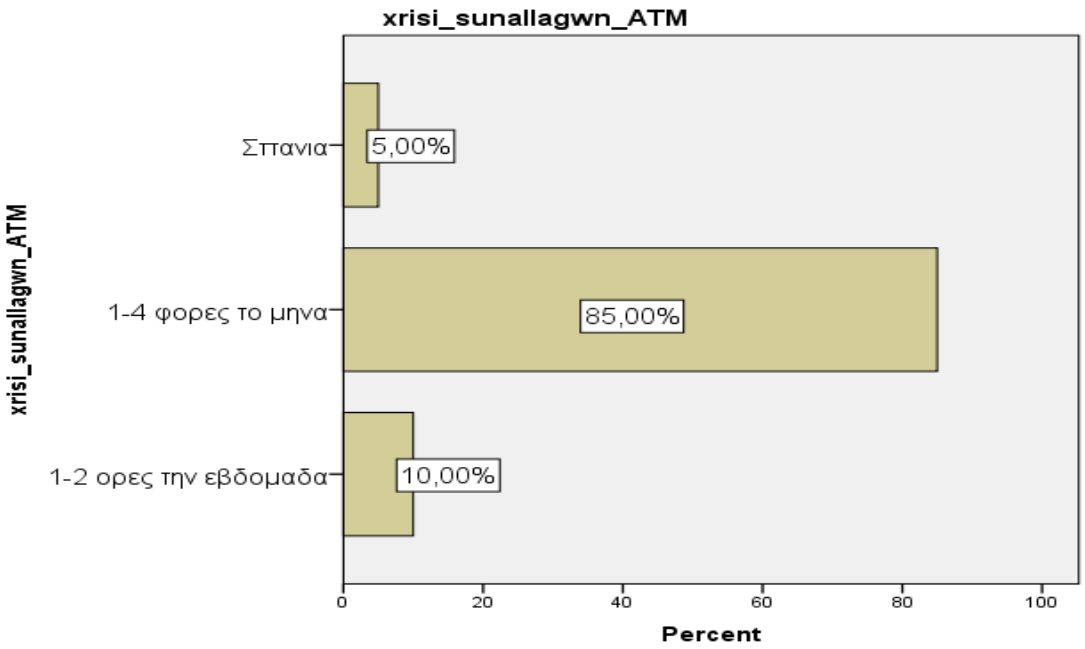
Ερώτηση 6: κατά πόσο χρησιμοποιείτε τις παρακάτω μεθόδους για τις τραπεζικές σας συναλλαγές;

Παρατηρείται ότι στο τραπεζικό κατάστημα το 81% του δείγματος πηγαίνει σπάνια, ενώ 1-4 φορές το μήνα πηγαίνει το 17% και το 2% καθόλου.



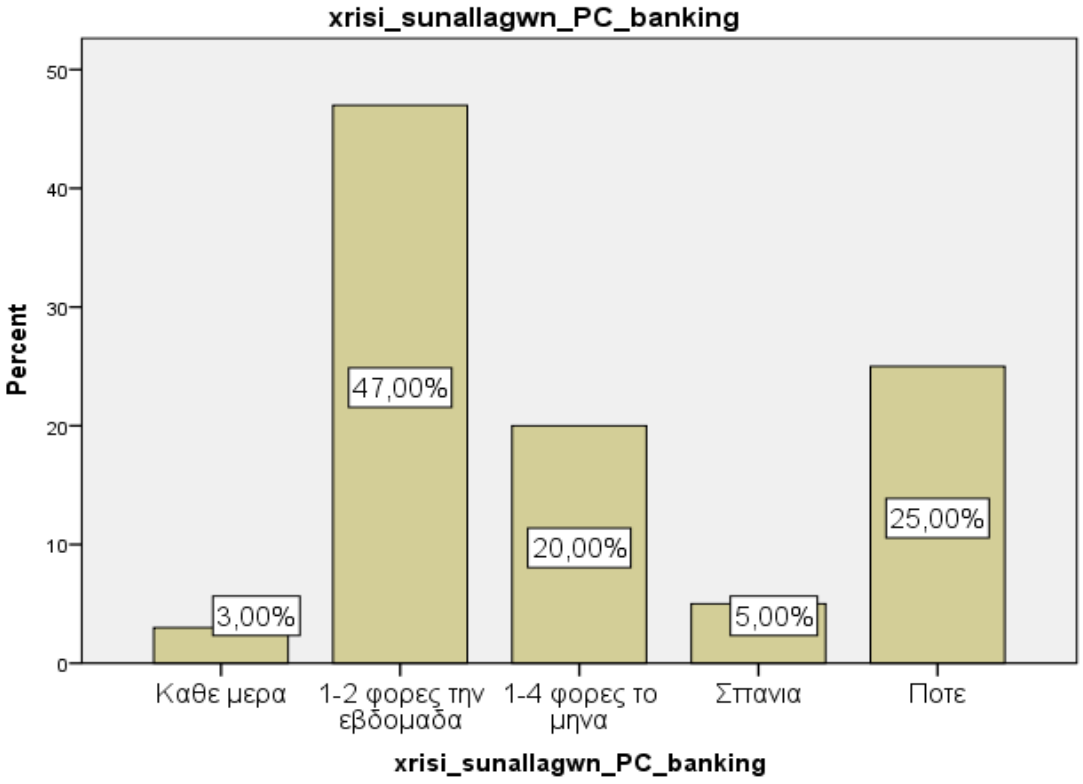
Διάγραμμα 8: Χρήση τραπεζικού καταστήματος

Το 85% του δείγματος χρησιμοποιεί το ΑΤΜ μηχάνημα 1-4 φορές το μήνα. Το 10% αποτελεί αυτούς που βρίσκονται σε κάποιο ΑΤΜ 1-2 φορές την εβδομάδα ενώ σπάνια χρησιμοποιούν το ΑΤΜ το 5%.



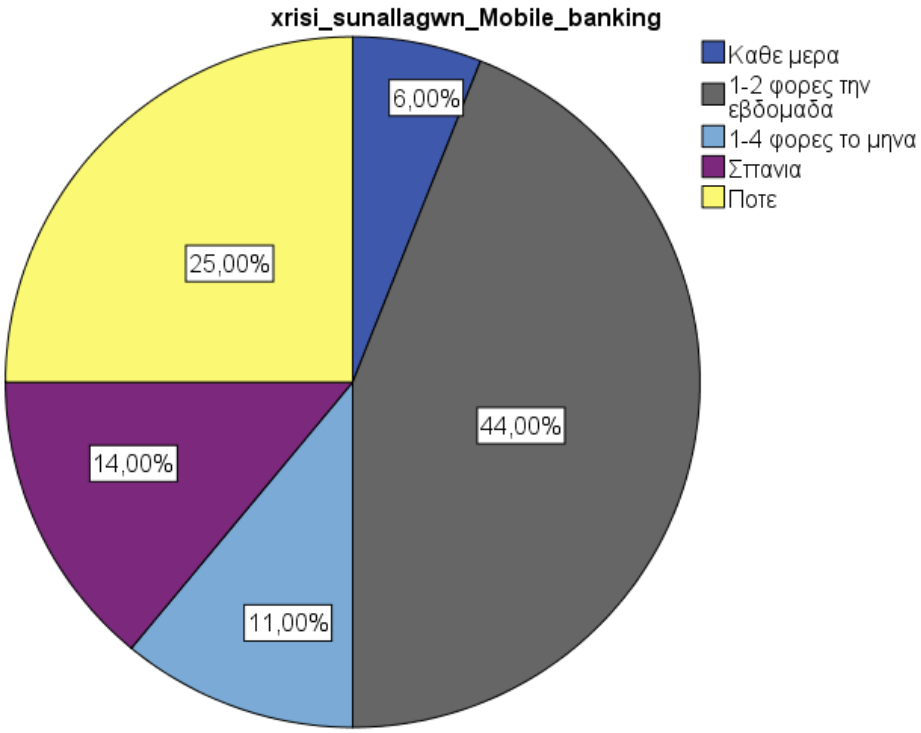
Διάγραμμα 9: Χρήση ATM μηχανήματος

Όσον αφορά τη χρήση PC-banking, ένα ποσοστό, 47%, υλοποιεί συναλλαγές 1-2 φορές την εβδομάδα ενώ το 25% δε χρησιμοποιεί ποτέ υπολογιστή για τραπεζικές του συναλλαγές. Το 20% πραγματοποιεί συναλλαγές μέσω PC, 1-4 φορές το μήνα ενώ τα δυο μικρότερα ποσοστά, 5% και 3%, αντιστοιχούν σε σπάνια χρήση PCbankingκαι κάθε μέρα.



Διάγραμμα 10: Χρήση PCbanking

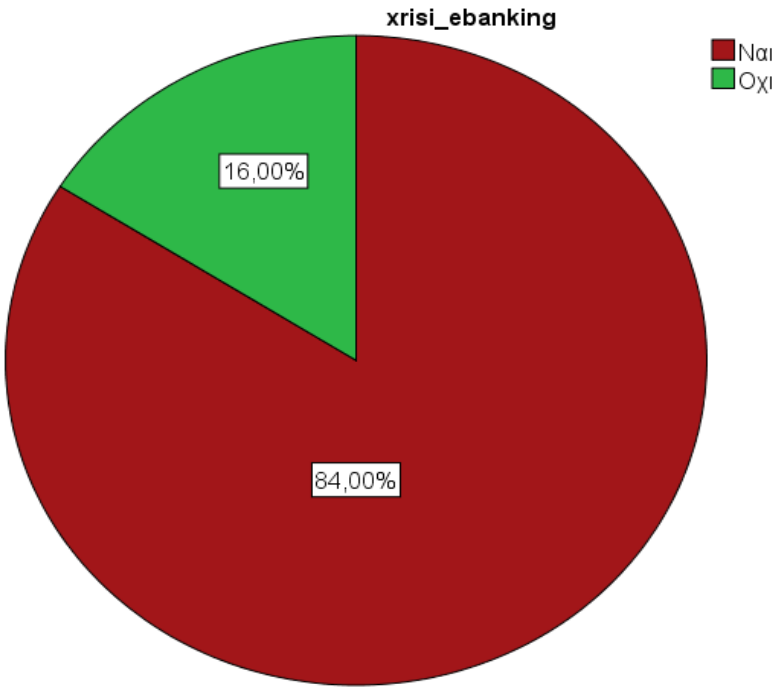
Ερωτήθηκαν βέβαια και για mobilebanking. Το44%, 1-2 φορές την εβδομάδα ενώ το αμέσως επόμενο ποσοστό είναι για αυτούς που δε χρησιμοποιούν ποτέ mobilebanking, 25%. Έχουμε ένα ποσοστό 14% για αυτούς που σπάνια κάνουν τραπεζικές συναλλαγές μέσω κάποιου κινητού και το 11% του δείγματος χρησιμοποιεί mobilebanking1-4 φορές το μήνα. Τέλος, λίγοι είναι αυτοί, 6%, που καθημερινά κάνουν κάποια τραπεζική συναλλαγή με mobilesυσκευή.



Διάγραμμα 11: Χρήση mobilebanking

Ερώτηση 7: χρησιμοποιείτε e-banking;

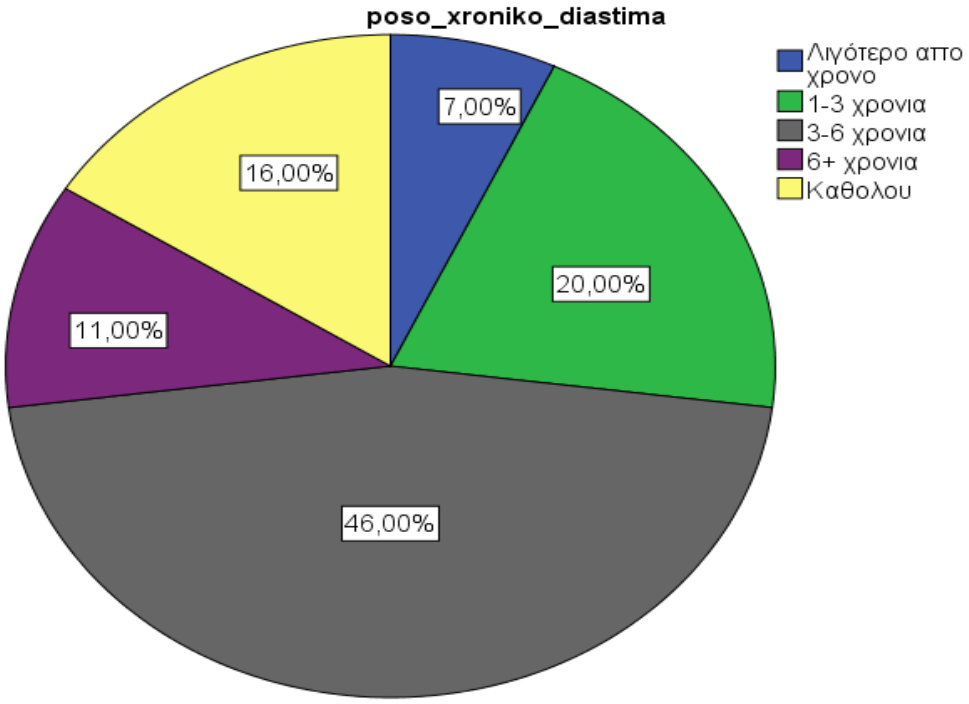
Ένα πολύ μεγάλο ποσοστό, 84%, χρησιμοποιεί e-bankingενώ ένα μικρό ποσοστό, μόλις 16%, δεν επιλέγει να κάνει τις τραπεζικές του συναλλαγές μέσω e-banking



Διάγραμμα 12: Χρήση e-banking

Ερώτηση 8: αν ναι, πόσο χρονικό διάστημα;

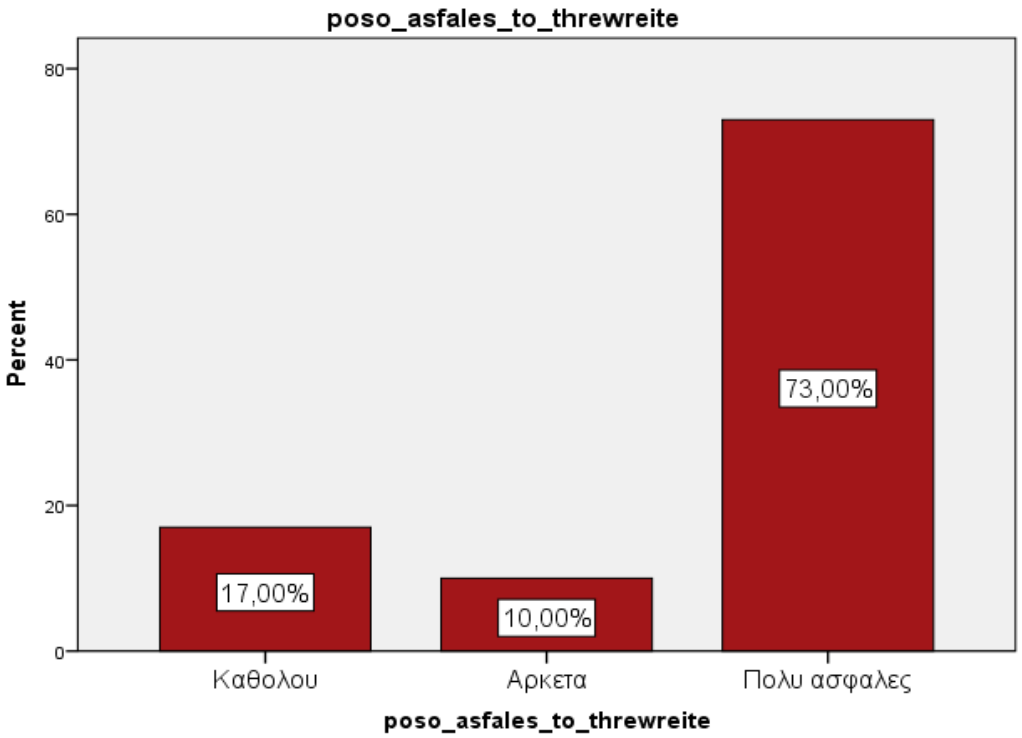
Παρατηρείται ότι το μεγαλύτερο ποσοστό ανήκει σε αυτούς που χρησιμοποιούν e-banking3 έως 6 χρόνια, 46% ενώ το μικρότερο σε αυτούς που το χρησιμοποιούν λιγότερο από χρόνο, 7%. Ενδιάμεσες τιμές έχουν αυτοί που κάνουν ηλεκτρονικές συναλλαγές 1-3 χρόνια, καθόλου και 6+ χρόνια με ποσοστά 20%, 16% και 11% αντίστοιχα.



Διάγραμμα 9: Πόσο χρονικό διάστημα χρησιμοποιούν e-banking

Ερώτηση 9: πόσο ασφαλές το θεωρείτε;

Πολλοί είναι αυτοί, 73%, που θεωρούν το onlinebankingπολύ ασφαλές. Μεγάλη διαφορά στα ποσοστά με τη συγκεκριμένη απάντηση έχουν αυτοί που δε το θεωρούν καθόλου ασφαλές, 17%, και αυτοί που πιστεύουν ότι είναι αρκετά ασφαλές.



Διάγραμμα 10: Πόσο ασφαλές το θεωρείτε

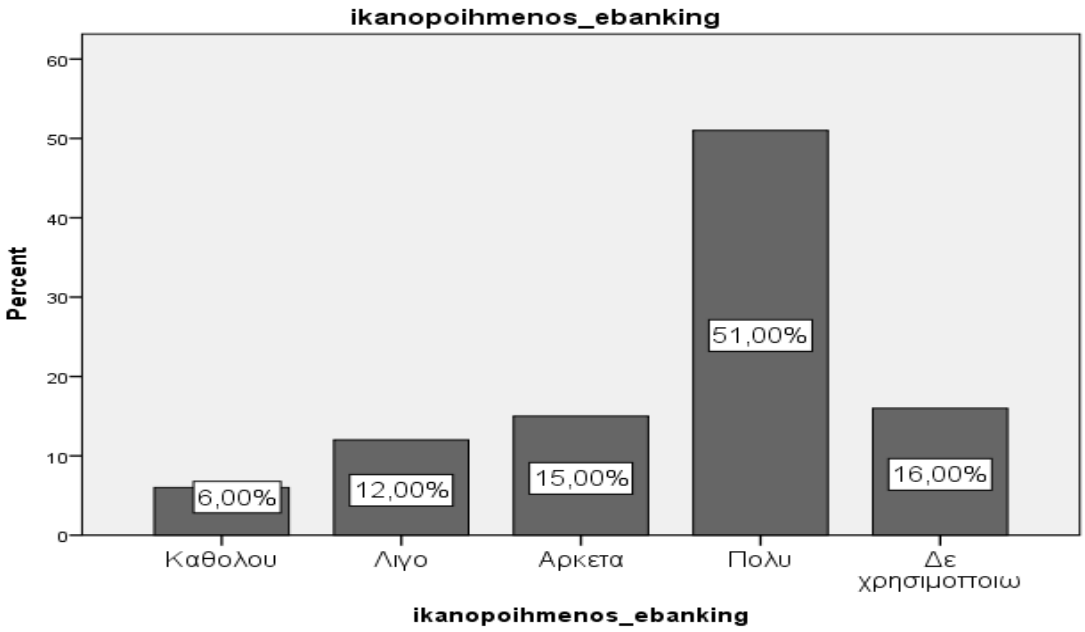
Ερώτηση 10: Έχετε ακούσει να συμβαίνουν στο περίγυρό σας πλαστοπροσωπία και κλοπή διαπιστευτηρίων σε ηλεκτρονικές συναλλαγές ή ακόμα και σε απλές τραπεζικές συναλλαγές;

Η πλειοψηφία των ερωτηθέντων με ποσοστό 88% δε γνωρίζουν κάποιο περιστατικό κλοπής διαπιστευτηρίων ή πλαστοπροσωπίας σε ηλεκτρονικές που να έχει συμβεί στο περίγυρο τους, όσον αφορά ηλεκτρονικές συναλλαγές. Ένα μικρό ποσοστό όμως, 12%, όπως φαίνεται γνωρίζουν.

Διάγραμμα 11: Αν γνωρίζουν κάποιο περιστατικό απάτης

Ερώτηση 11: είστε ικανοποιημένος από την εξυπηρέτηση μέσω ηλεκτρονικής συναλλαγής;

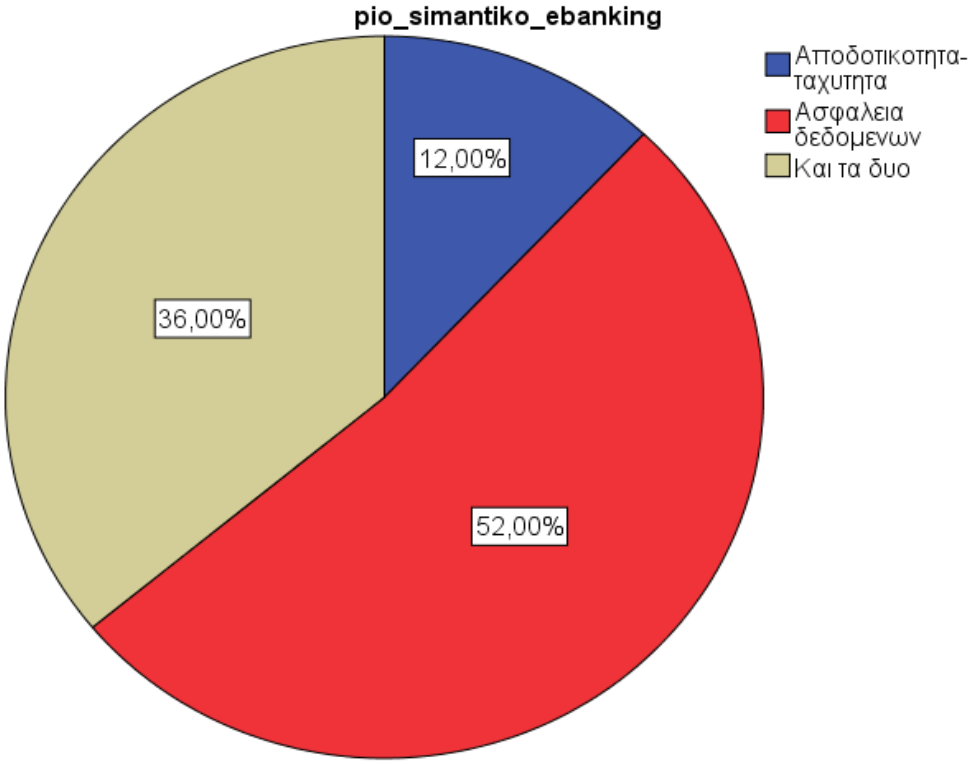
Το 51% του δείγματος είναι ικανοποιημένο από το e-bankingενώto 15%αρκετά, το 12% λίγο και το 6% όπως φαίνεται είναι απογοητευμένο από τις υπηρεσίες του onlinebanking



Διάγραμμα 12: Ικανοποιημένος από το e-banking

Ερώτηση 12: τι θεωρείτε πιο σημαντικό στο e-banking;

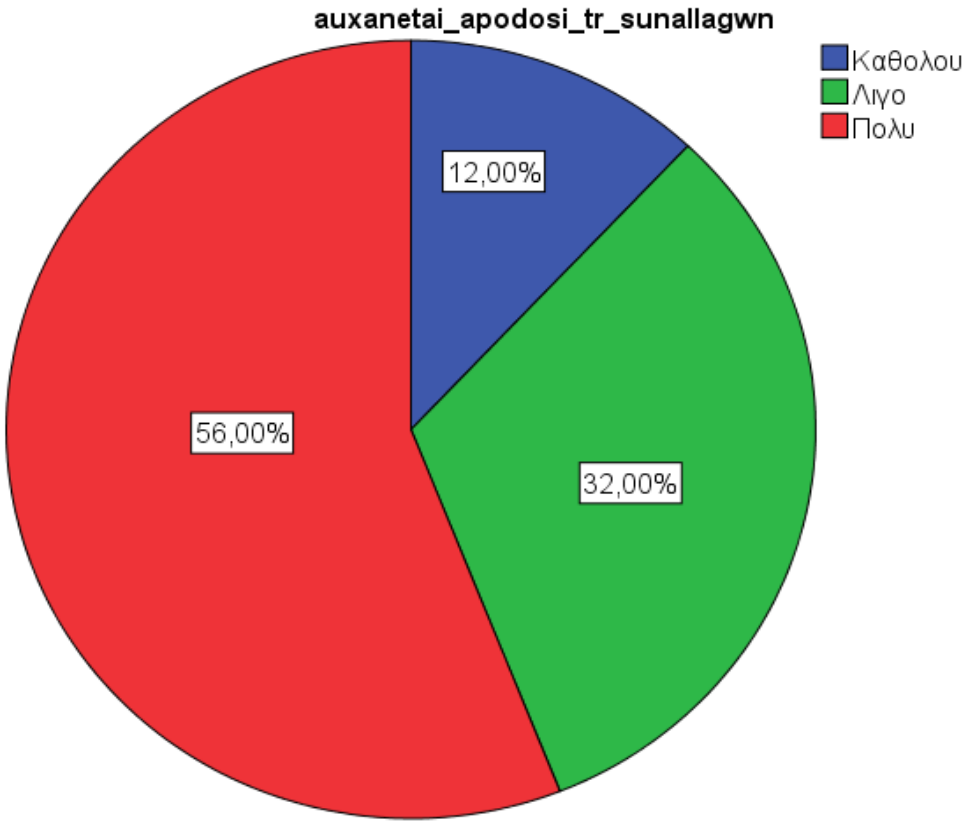
Φαίνεται από το στατιστικό διάγραμμα ότι πολλοί χρήστες θεωρούν πιο σημαντικό την ασφάλεια των δεδομένων, 52%. Ακολουθεί το ποσοστό αυτών δίνουν μεγάλη σημασία και στην αποδοτικότητα-ταχύτητα των συστημάτων και στην ασφάλεια της περιουσίας τους καλύπτοντας το ποσοστό 36% ενώ ένα 12% τους ενδιαφέρει η αποδοτικότητα- ταχύτητα των συναλλαγών τους.



Διάγραμμα 13: Πιο σημαντικό στο e-banking

Ερώτηση 13: με το e-bankingπιστεύετε αυξάνεται η απόδοση των τραπεζικών συναλλαγών;

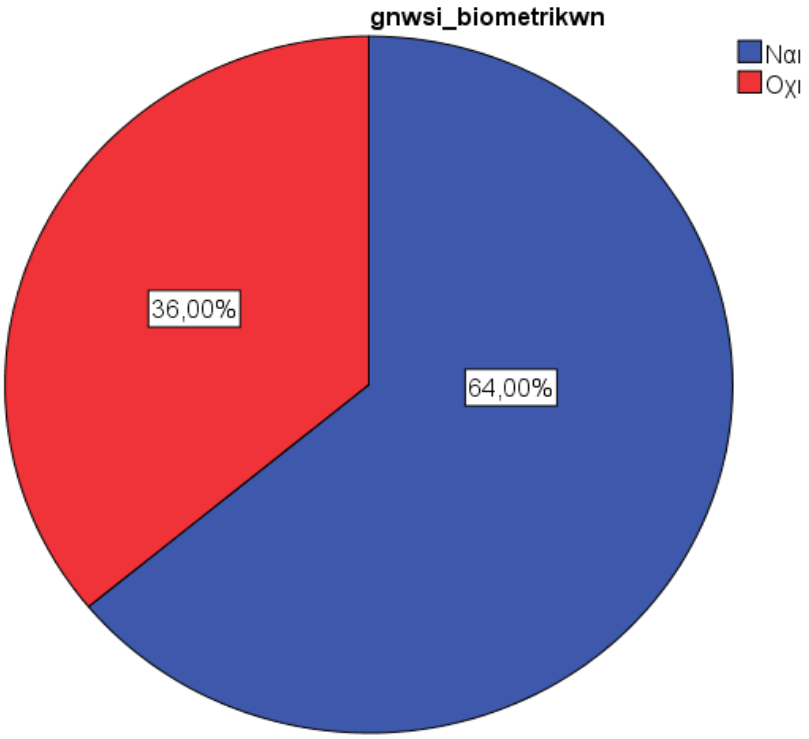
Λίγο πάνω από το μισό δείγμα που επέλεξα, το 56%, θεωρεί ότι με τη χρήση e-bankingέχει βελτιωθεί η απόδοση των τραπεζικών συναλλαγών. Το 12% απάντησε 'καθόλου' ενώ το 32% πιστεύει ότι το e-bankingεπηρέασε ελάχιστα τη απόδοση των συναλλαγών.



Διάγραμμα 14: Αύξηση απόδοσης τραπεζικών συναλλαγών με τη χρήση e-banking

Ερώτηση 14: γνωρίζετε σχετικά με τις βιομετρικές τεχνολογίες;

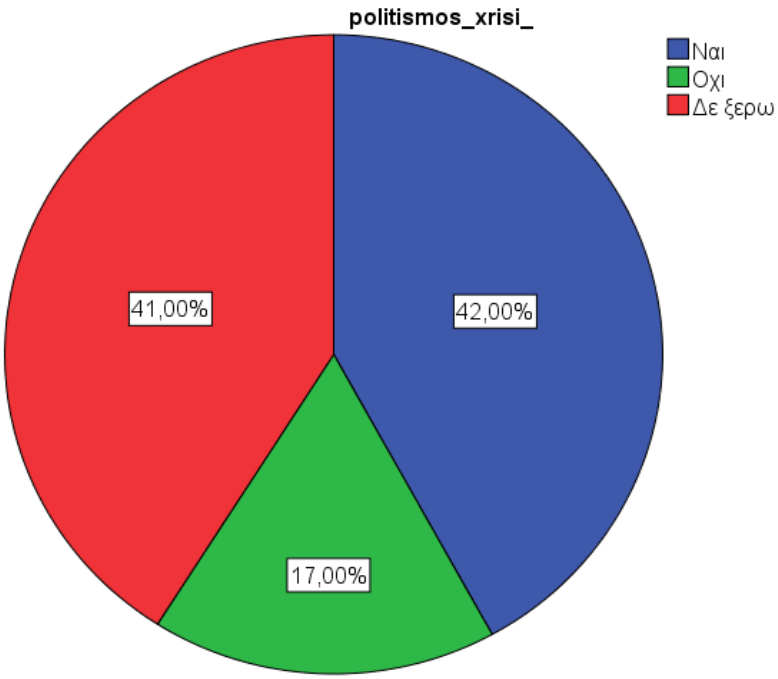
Φαίνεται ότι πολλοί είναι ενήμεροι για τις βιομετρικές τεχνολογίες καλύπτοντας ένα ποσοστό 64% ενώ αυτοί που δε γνωρίζουν πολλά για το θέμα αυτό είναι το 36% του δείγματός μου.



Διάγραμμα 15: Γνώση σχετικά με biometrics

Ερώτηση 15: Πιστεύετε ότι το πολιτισμικό επίπεδο (π.χ ο τρόπος αντίληψης της ζωής) μιας χώρας καθορίζει τη χρήση ή μη των βιομετρικών τεχνολογιών στο onlinebanking;

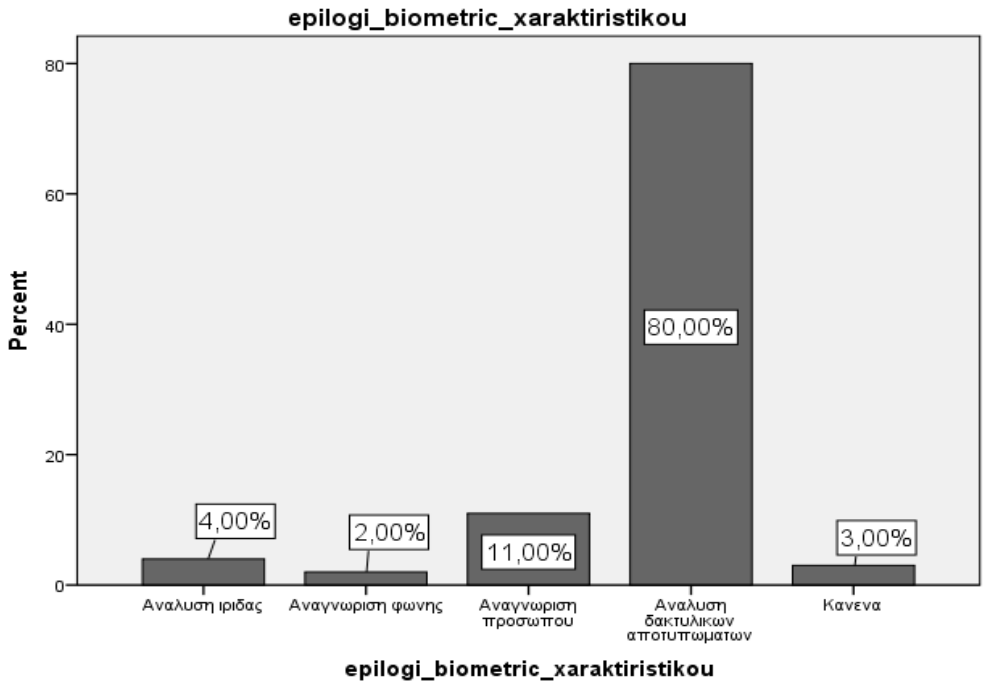
Από το στατιστικό διάγραμμα μπορούμε να καταλάβουμε ότι αυτοί που θεωρούν ότι το πολιτισμικό επίπεδο μιας χώρας επηρεάζει την υιοθέτηση των biometricsστις onlineσυναλλαγές, με ποσοστό 42%, είναι περίπου ίσοι με αυτούς που δε γνωρίζουν, 41%. Βέβαια υπάρχουν και αυτοί, 17%, που απάντησαν ότι δεν υπάρχει καμία σχέση ανάμεσα το πολιτισμικό επίπεδο και τη χρήση των biometrics.



Διάγραμμα 16: Επιρροή πολιτισμού στην υιοθέτηση biometrics

Ερώτηση 16: στη περίπτωση που γνωρίζετε, ποιο από τα παρακάτω βιομετρικά συστήματα θα επιλέγατε για τις onlinesυναλλαγές σας;

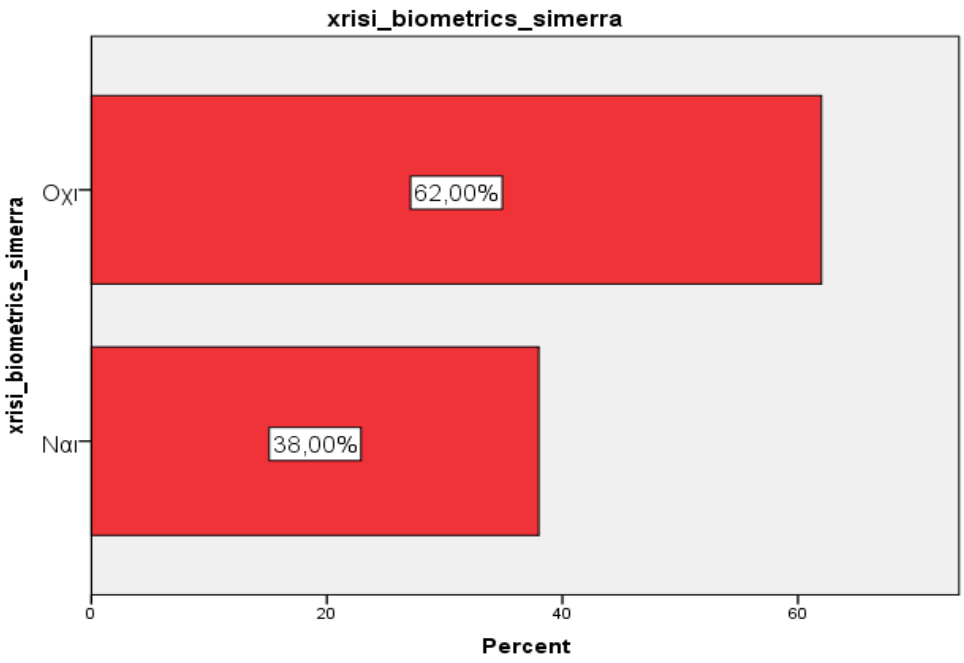
Με διαφορά φαίνεται ότι οι περισσότεροι, 80%, θα επιλέγανε σα πρώτη επιλογή την ανάλυση του δακτυλικού αποτυπώματος. Οι υπόλοιπες κατηγορίες όπως αναγνώριση προσώπου, ανάλυση ίριδας και αναγνώριση φωνής καλύπτουν τα ποσοστά 11%, 4% και 2% αντίστοιχα. Ένα 3% δήλωσαν ότι δε θα επέλεγαν κανένα βιομετρικό χαρακτηριστικό από αυτά που είχα συμπεριλάβει. Βέβαια κανένας δεν επέλεξε την ανάλυση DNA, την ανάλυση πληκτρολόγησης και την ανάλυση βηματισμού.



Διάγραμμα 17: Επιλογή βιομετρικού χαρακτηριστικού

Ερώτηση 17: εσείς χρησιμοποιείτε κάποια βιομετρική τεχνολογία στις τραπεζικές σας συναλλαγές;

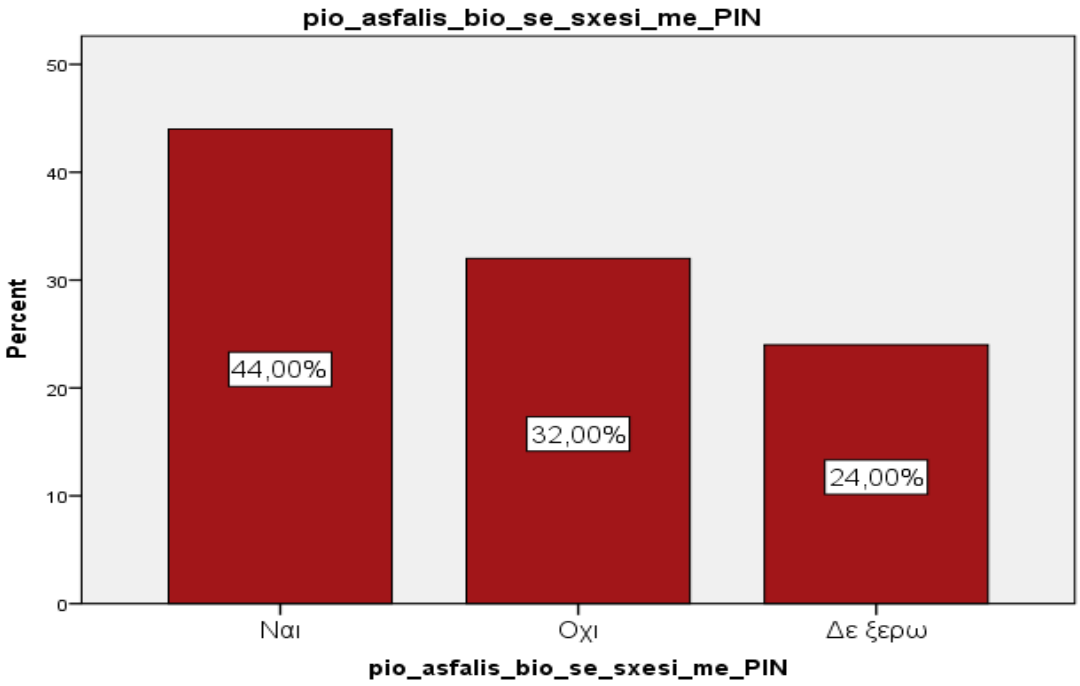
Το 62% των ερωτηθέντων δήλωσε ότι δε χρησιμοποιούν κάποιο είδος βιομετρικής τεχνολογίας στις τραπεζικές τους συναλλαγές ενώ το 38% όπως βλέπουμε κάνει χρήση βιομετρικής τεχνολογίας.



Διάγραμμα 18: Χρήση βιομετρίας σήμερα

Ερώτηση 18: σε σχέση με την εισαγωγή κωδικού PIN θεωρείτε τις βιομετρικές τεχνολογίες πιο ασφαλείς;

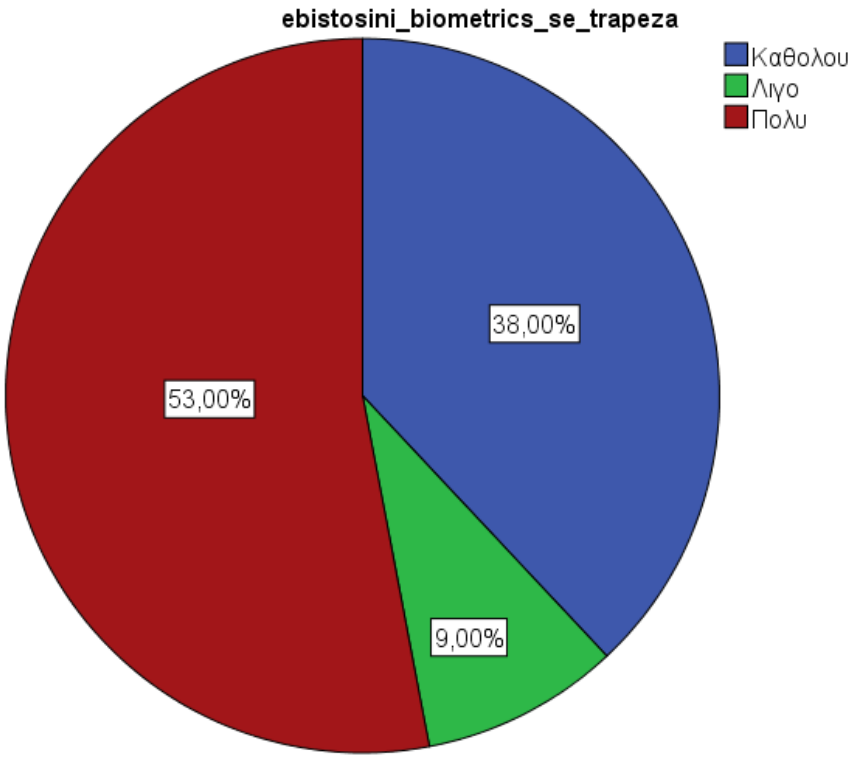
Όπως παρατηρείται αυτοί που πιστεύουν στη μεγαλύτερη ασφάλεια των biometricsαπό το κωδικό PIN, δεν έχουν μεγάλη διαφορά με αυτούς που είναι αντίθετοι στην άποψη αυτή. Τη πρώτη άποψη την υποστηρίζει το 44% του δείγματος ενώ την αντίθετη το 32%. Υπάρχουν και αυτοί που σύμφωνα με την απάντηση τους δε γνωρίζουν σε επίπεδο ασφάλειας τα biometricsκαι τον κωδικό PIN.



Διάγραμμα 19: Ασφάλεια βιομετρικού συστήματος σε σχέση με κωδικό PIN

Ερώτηση 19: Κατά πόσο θα εμπιστευόσασταν σε οργανισμούς όπως τράπεζες τα βιομετρικά σας χαρακτηριστικά;

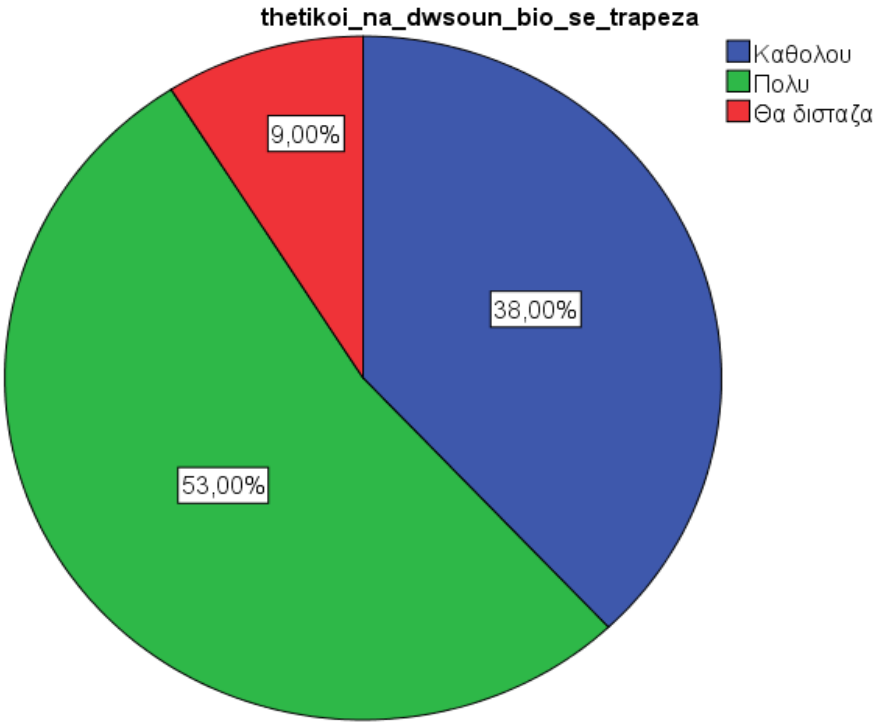
Σχεδόν οι μισοί του δείγματος, 53%, δε θα είχαν κανένα απολύτως πρόβλημα να εμπιστευτούν κάποιο βιομετρικό τους χαρακτηριστικό σε μια τράπεζα. Επίσης, 38% δηλώνουν ότι δε θα το εμπιστευόταν ενώ λίγοι, 9%, με βάση την απάντηση που έδωσαν φαίνεται ότι θα ήθελαν να ξέρουν περισσότερα για να καταλήξουν σε μια ξεκάθαρη απάντηση.



Διάγραμμα 20: Εμπιστοσύνη βιομετρικού χαρακτηριστικού σε μια τράπεζα

Ερώτηση 20: Αν τις επόμενες μέρες κιόλας, η τράπεζα που συνεργάζεστε σας πρότεινε να δώσετε κάποιο βιομετρικό στοιχείο για να προχωρήσει σε βιομετρική online τραπεζική, κατά πόσο θα ήσασταν θετικοί;

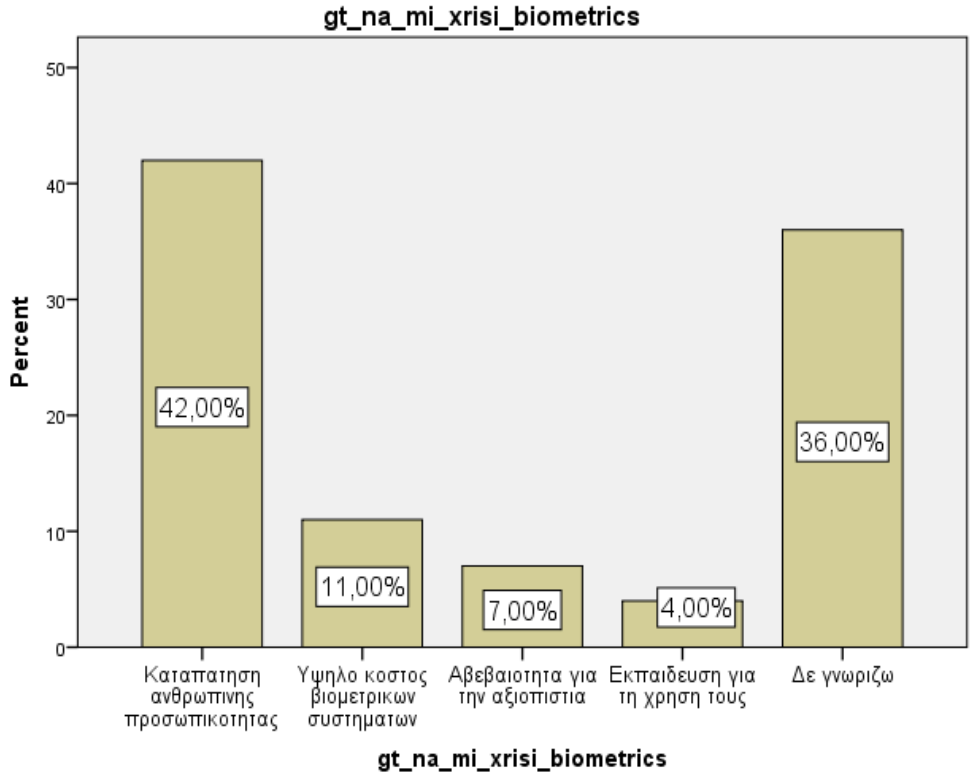
Η πλειοψηφία του εξεταζόμενου δείγματος, 53%, δε θα δίσταζαν καθόλου να ξεκινήσουν άμεσα διαδικασία για τη χρήση βιομετρικού συστήματος ελέγχου πρόσβασης για onlinebanking. Κάποιοι, 9%, προφανώς θα ήθελαν να το σκεφτούν καλύτερα ή να ενημερωθούν περισσότερο ενώ το 38% έχει αποφασίσει ότι δε δώσουν τόσο σύντομα ένα τόσο προσωπικό στοιχείο.



Διάγραμμα 21: Θετικοί στο να δώσουν αύριο κιόλας στη τράπεζα κάποιο βιομετρικό χαρακτηριστικό

Ερώτηση 21: για ποιον από τους παρακάτω λόγους δε θα χρησιμοποιούσατε biometrics;

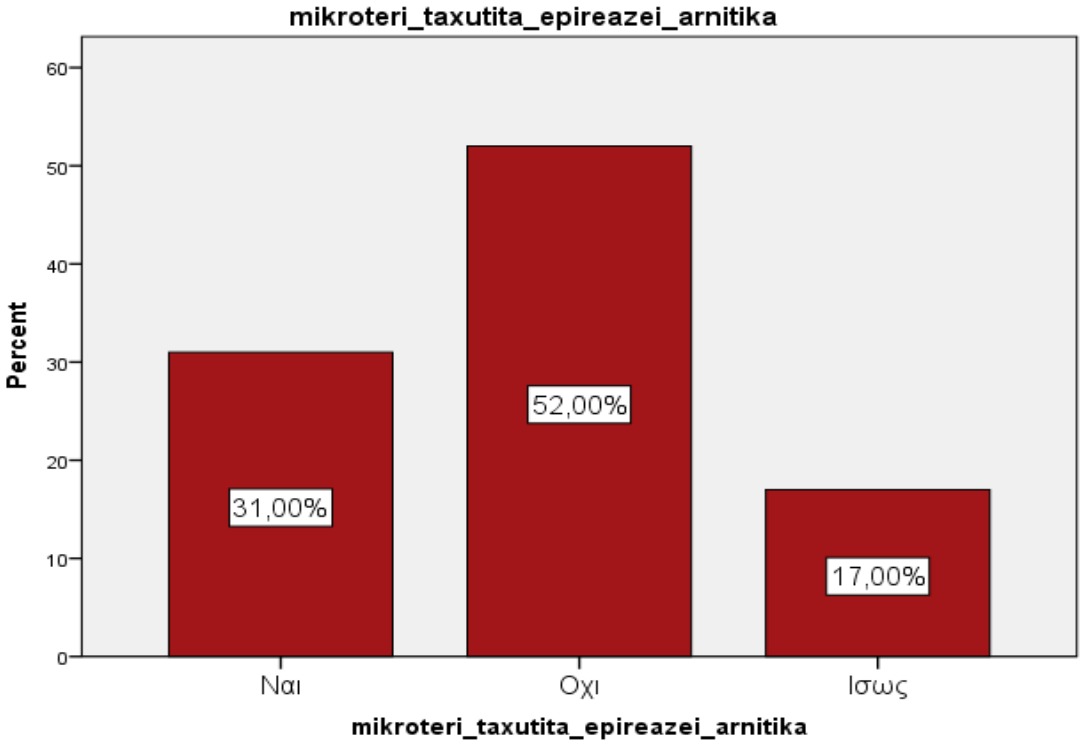
Το 42% του δείγματος δίνει μεγάλη σημασία στη καταπάτηση ανθρώπινης προσωπικότητας. Ακολουθούν αυτοί που δε γνωρίζουν πολλά για τα biometrics, 26%, άρα δε γνωρίζουν. Τέλος, είναι το υψηλό κόστος των συστημάτων, η αβεβαιότητα αυτών και η εκπαίδευση στη χρήση τους με 11%, 7% και 4% αντίστοιχα.



Διάγραμμα 22: Λόγοι μη χρήσης βιομετρικών συστημάτων

Ερώτηση 22: Γνωρίζοντας ότι τα βιομετρικά συστήματα είναι εξαιρετικά ασφαλή, η πιθανόν μικρότερη ταχύτητα ανταπόκρισης σε σχέση με την εισαγωγή PIN θα σας επηρέαζε αρνητικά;

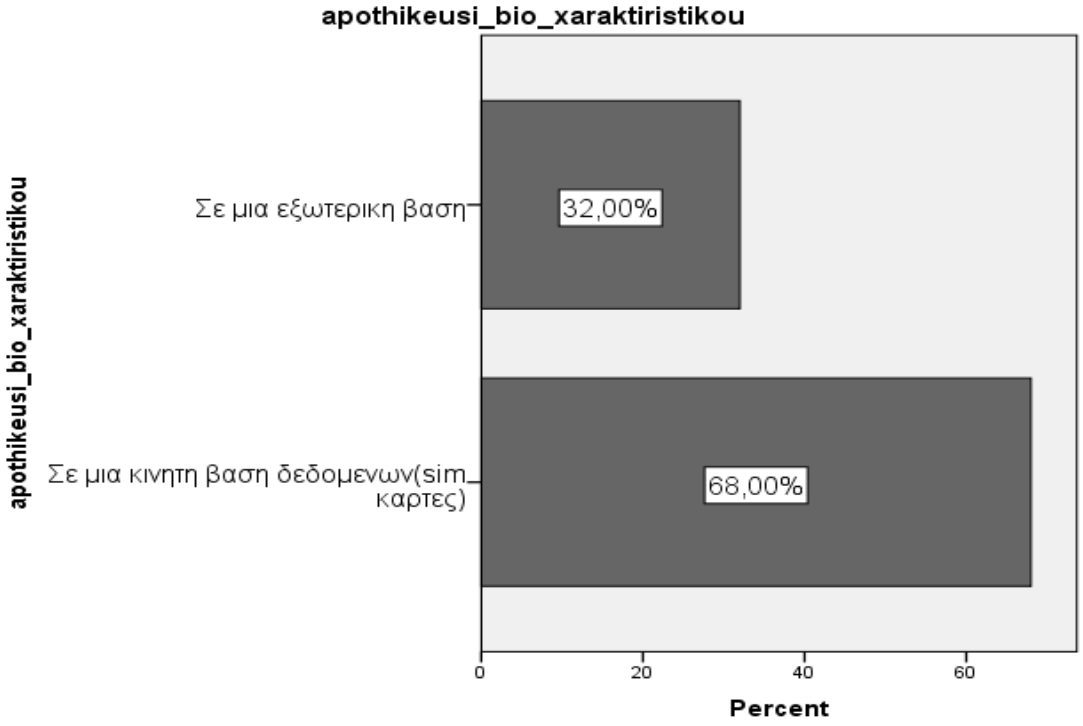
Η πλειοψηφία των ερωτηθέντων, 52%, απάντησε ότι δε θα τους επηρέαζε αρνητικά η σχετικά μικρότερη ανταπόκριση ενός βιομετρικού συστήματος σε σχέση με ένα κωδικό PIN. Το 31% απάντησαν 'Ναι' ενώ ένα μικρό ποσοστό 17% δε μπορούν να είναι σίγουροι.



Διάγραμμα 23: Αρνητική επιρροή η μικρότερη ανταπόκριση ενός βιομετρικού συστήματος

Ερώτηση 23: Έστω ότι προχωρούσατε σε βιομετρική online τραπεζική, πως πιστεύετε θα ήταν πιο ασφαλής ο τρόπος αποθήκευσης του βιομετρικού σας χαρακτηριστικού;

Το 68% του δείγματος επέλεξε ότι θέλει το βιομετρικό του χαρακτηριστικό να είναι αποθηκευμένο σε μια κινητή συσκευή ενώ το 32% σε μια εξωτερική βάση.



Διάγραμμα 24: Αποθήκευση βιομετρικού χαρακτηριστικού

Συσχετίσεις

Συσχέτιση μεταξύ των μεταβλητών 'ηλικία' – 'κατά πόσο χρησιμοποιείτε το internet στη ζωή σας'

H0: οι μεταβλητές είναι ανεξάρτητες

H1: οι μεταβλητές εξαρτώνται

ilikia * xrisi_internetCrosstabulation

Count

		xrisi_internet			
		καθημερινα	σπανια	καθολου	Total
ilikia	18-25	6	0	0	6
	26-35	27	7	0	34
	36-45	32	13	1	46
	46-55	6	3	1	10
	55+	0	2	2	4
Total		71	25	4	100

Πίνακας 1: ηλικία * συχνότητα χρήσης internet

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	31,177[a]	8	,000
LikelihoodRatio	21,881	8	,005
Linear-by-Linear Association	15,981	1	,000
N of ValidCases	100		

a. 10 cells (66,7%) have expected count less than 5. The minimum expected count is ,16.

Πίνακας 2: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. γιατονPearsonChi-Squareείναι 0,000 που είναι μικρότερο από το 0,05. Άρα αποδεχόμαστε την H1. Αυτό

σημαίνει ότι οι απαντήσεις που δόθηκαν στη‘συχνότητα χρήσης internet’**εξαρτάται** από την ‘ηλικία’ του δείγματος.

Συσχέτιση μεταξύ των μεταβλητών ‘ηλικία’ – ‘κατά πόσο φιλικός είσαι με τις τεχνολογικές καινοτομίες’

H0: οι μεταβλητές είναι ανεξάρτητες

H1: οι μεταβλητές εξαρτώνται

ilikia * filikos_texnologikes_kainotomies Crosstabulation

Count

		filikos_texnologikes_kainotomies				
		παρα_πολυ	αρκετα	λιγο	καθολου	Total
ilikia	18-25	4	2	0	0	6
	26-35	9	19	4	2	34
	36-45	7	17	19	3	46
	46-55	1	4	4	1	10
	55+	0	0	1	3	4
Total		21	42	28	9	100

Πίνακας 3: ηλικία * φιλικός με τεχνολογικές καινοτομίες

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	41,135[a]	12	,000
LikelihoodRatio	32,365	12	,001
Linear-by-Linear Association	20,221	1	,000
N of ValidCases	100		

Πίνακας 4: : Chi-Square Tests

a. 14 cells (70,0%) have expected count less than 5. The minimum expected count is ,36.

Από τον πίνακα Chi-SquareTests παρατηρούμε ότι η τιμή Asymp. Sig. για τον PearsonChi-Square είναι 0,000 που είναι μικρότερο από το 0,05. Άρα αποδεχόμαστε την Η1. Αυτό σημαίνει ότι το κατά πόσο είναι κάποιος φιλικός με τις τεχνολογικές καινοτομίες **εξαρτάται** από την ηλικία του δείγματος.

Συσχέτιση μεταξύ των μεταβλητών 'επίπεδο σπουδών' – 'γνώση σχετικά με βιομετρίες'

Η0: οι μεταβλητές είναι ανεξάρτητες

Η1: οι μεταβλητές εξαρτώνται

epipedo_spoudwn * gnwsi_biometrikwn Crosstabulation

Count

		gnwsi_biometrikwn		
		Ναι	Οχι	Total
epipedo_spoudwn	αποφοιτος_λυκειου	7	5	12
	αποφοιτος_AEI/TEI	37	24	61
	κατοχος_μεταπτυχιακου	13	6	19
	κατοχος_διδακτορικου	7	1	8
Total		64	36	100

Πίνακας 5: επίπεδοσπουδών * γνώσησχετικάμεbiometrics

Chi-SquareTests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2,542[a]	3	,468
Likelihood Ratio	2,884	3	,410
Linear-by-Linear Association	2,076	1	,150
N of Valid Cases	100		

a. 2 cells (25,0%) have expected count less than 5. The minimum expected count is 2,88.

Πίνακας 6: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,468 που είναι μεγαλύτερο από το 0,05. Άρα αποδεχόμαστε την H0. Αυτό σημαίνει ότι το αν γνωρίζουν σχετικά με βιομετρίες **δεν εξαρτάται** από το επίπεδο σπουδών.

Συσχέτιση μεταξύ των μεταβλητών 'κύρια απασχόληση' – 'χρήση e-banking'

H0: οι μεταβλητές είναι ανεξάρτητες

H1: οι μεταβλητές εξαρτώνται

kuria_apasxolisi * xrisi_ebanking Crosstabulation

Count

		xrisi_ebanking		
		Ναι	Οχι	Total
kuria_apasxolisi	ελευθερος_επαγγελματιας	6	2	8
	δημοσιος_υπαλληλος	21	3	24
	ιδιωτικος_υπαλληλος	48	4	52
	ανεργος	9	6	15
	συνταξιουχος	0	1	1
Total		84	16	100

Πίνακας 7: κύριααπασχόληση * χρήσηe-banking

Chi-Square Tests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	15,050[a]	4	,005
LikelihoodRatio	12,458	4	,014
Linear-by-Linear Association	2,314	1	,128
N of ValidCases	100		

a. 5 cells (50,0%) have expected count less than 5. The minimum expected count is ,16.

Πίνακας 8: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,005 που είναι μικρότερο από το 0,05. Άρα αποδεχόμαστε την Η1. Αυτό σημαίνει ότι το η χρήση e-banking**εξαρτάται**τη κύρια απασχόληση του δείγματος.

Συσχέτιση μεταξύ των μεταβλητών 'κύρια απασχόληση' – 'χρήση pcbanking'

Η0: οι μεταβλητές είναι ανεξάρτητες

Η1: οι μεταβλητές εξαρτώνται

kuria_apasxolisi * xrisi_sunallagwn_PC_banking Crosstabulation

Count

		xrisi_sunallagwn_PC_banking			
		Καθεμερα	1-2 φορεςτηνεβδομαδα	1-4 φορεςτο μηνα	Σπανια
kuria_apasxolisi	ελευθερος_επαγγελματιας	0	3	3	0
	δημοσιος_υπαλληλος	0	13	4	2
	ιδιωτικος_υπαλληλος	3	24	11	3
	ανεργος	0	7	2	0
	συνταξιουχος	0	0	0	0
Total		3	47	20	5

Πίνακας 9: κύριααπασχόληση * χρήσηPCbanking

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	11,459[a]	16	,780
LikelihoodRatio	13,028	16	,671
Linear-by-Linear Association	,620	1	,431
N of ValidCases	100		

a. 19 cells (76,0%) have expected count less than 5. The minimum expected count is ,03.

Πίνακας 10: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτηντιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,780 που είναι μεγαλύτερο από το 0,05. Άρα αποδεχόμαστε την Η0. Αυτό σημαίνει ότι το η χρήση PCbanking**δενεξαρτάται**από τη κύρια απασχόληση του δείγματος

Συσχέτιση μεταξύ των μεταβλητών 'ηλικία' – 'χρήση mobilebanking'

Η0: οι μεταβλητές είναι ανεξάρτητες

Η1: οι μεταβλητές εξαρτώνται

ilikia * xrisi_sunallagwn_Mobile_banking Crosstabulation

Count

		xrisi_sunallagwn_Mobile_banking					
		Καθεμερα	1-2 φορες την εβδομαδα	1-4 φορες το μηνα	Σπανια	Ποτε	Total
ilikia	18-25	0	4	0	0	2	6
	26-35	1	17	4	3	9	34
	36-45	3	20	6	9	8	46

	46-55	2	2	1	2	3	10
	55+	0	1	0	0	3	4
Total		6	44	11	14	25	100

Πίνακας 11: ηλικία * χρήση mobilebanking

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	17,025[a]	16	,384
LikelihoodRatio	17,931	16	,328
Linear-by-Linear Association	1,074	1	,300
N of ValidCases	100		

a. 19 cells (76,0%) have expected count less than 5. The minimum expected count is ,24.

Πίνακας 12: : Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,384 που είναι μεγαλύτερο από το 0,05. Άρα αποδεχόμαστε την Η0. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για τη χρήση mobilebanking**δενεξαρτάται**από την ηλικία του δείγματος.

Συσχέτιση μεταξύ των μεταβλητών 'χρήση e-banking' – 'τι θερούν πιο σημαντικό στο e-banking'

Η0: οι μεταβλητές είναι ανεξάρτητες

Η1: οι μεταβλητές εξαρτώνται

xrisi_ebanking * pio_simantiko_ebanking Crosstabulation

Count

		pio_simantiko_ebanking			
		Αποδοτικοτητα-ταχυτητα	Ασφαλειαδεδομενων	Και τα δυο	Total
xrisi_ebanking	Ναι	12	43	29	84
	Οχι	0	9	7	16
Total		12	52	36	100

Πίνακας 13: χρήση e-banking * τι θεωρούν πιο σημαντικό στο e-banking

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	2,670[a]	2	,263
LikelihoodRatio	4,550	2	,103
Linear-by-Linear Association	1,741	1	,187
N of ValidCases	100		

a. 1 cells (16,7%) have expected count less than 5. The minimum expected count is 1,92.

Πίνακας 14: : Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτηντιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,263 που είναι μεγαλύτερο από το 0,05. Άρα αποδεχόμαστε την H0. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για το τι θεωρούν πιο σημαντικό στο e-banking**δενεξαρτάται**από το αν χρησιμοποιεί ο ερωτώμενος e-banking.

Συσχέτιση μεταξύ των μεταβλητών 'χρήση internet' – 'χρήση ATM για συναλλαγές'

H0: οι μεταβλητές είναι ανεξάρτητες

H1: οι μεταβλητές εξαρτώνται

xrisi_internet * xrisi_sunallagwn_ATM Crosstabulation

Count

		xrisi_sunallagwn_ATM			
		1-2 ορες την εβδομαδα	1-4 φορες το μηνα	Σπανια	Total
xrisi_internet	καθημερινα	7	63	1	71
	σπανια	1	20	4	25
	καθολου	2	2	0	4
Total		10	85	5	100

Πίνακας 15: χρήση internet * χρήση ATM για συναλλαγές

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	16,149[a]	4	,003
LikelihoodRatio	12,045	4	,017
Linear-by-Linear Association	,094	1	,759
N of ValidCases	100		

a. 6 cells (66,7%) have expected count less than 5. The minimum expected count is ,20.

Πίνακας 16: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,003 που είναι μικρότερο από το 0,05. Άρα αποδεχόμαστε την Η1. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για το κατά πόσο χρησιμοποιούν ένα ΑΤΜ για συναλλαγές **εξαρτάται**από το αν χρησιμοποιούν internetστη ζωή τους.

Συσχέτιση μεταξύ των μεταβλητών 'κύρια απασχόληση' – 'πόσο χρονικό διάστημα χρησιμοποιούν το e-banking'

Η0: οι μεταβλητές είναι ανεξάρτητες

Η1: οι μεταβλητές εξαρτώνται

kuria_apasxolisi * poso_xroniko_diastima Crosstabulation

Count

		poso_xroniko_diastima				
		Λιγότερο αποχρονο	1-3 χρονια	3-6 χρονια	6+ χρονια	Καθολ υ
kuria_apasxolisi	ελευθερος_επαγγελματιας	2	0	3	1	
	δημοσιος_υπαλληλος	1	5	15	0	
	ιδιωτικος_υπαλληλος	3	13	23	9	
	ανεργος	1	2	5	1	
	συνταξιουχος	0	0	0	0	
Total		7	20	46	11	1

Πίνακας 17: κύρια απασχόληση * πόσο χρονικό διάστημα χρησιμοποιούν e-banking

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	27,064[a]	16	,041
LikelihoodRatio	26,848	16	,043
Linear-by-Linear Association	2,301	1	,129
N of ValidCases	100		

a. 19 cells (76,0%) have expected count less than 5. The minimum expected count is ,07.

Πίνακας 18: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιητιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,041 που είναι μικρότερο από το 0,05. Άρα αποδεχόμαστε την Η1. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για το πόσο χρονικό διάστημα χρησιμοποιούν το e-banking**εξαρτάται**από τη κύρια απασχόλησή τους.

Συσχέτιση μεταξύ των μεταβλητών 'ηλικία' – 'πόσο χρονικό διάστημα χρησιμοποιούν το e-banking'

Η0: οι μεταβλητές είναι ανεξάρτητες
Η1: οι μεταβλητές εξαρτώνται

ilikia * poso_xroniko_diastima Crosstabulation

Count

		poso_xroniko_diastima					
		Λιγότερο αποχρονο	1-3 χρονια	3-6 χρονια	6+ χρονια	Καθολου	Total
ilikia	18-25	1	3	1	0	1	6
	26-35	0	6	20	5	3	34
	36-45	3	10	21	6	6	46
	46-55	2	1	4	0	3	10
	55+	1	0	0	0	3	4
Total		7	20	46	11	16	100

Πίνακας 19: ηλικία * πόσο χρονικό διάστημα χρησιμοποιούν e-banking

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	29,957[a]	16	,018
LikelihoodRatio	30,750	16	,014
Linear-by-Linear Association	1,668	1	,197
N of ValidCases	100		

a. 18 cells (72,0%) have expected count less than 5. The minimum expected count is ,28.

Πίνακας 20: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,018 που είναι μικρότερο από το 0,05. Άρα αποδεχόμαστε την H1. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για το πόσο χρονικό διάστημα χρησιμοποιούν το e-banking**εξαρτάται**από την ηλικία του δείγματος.

Συσχέτιση μεταξύ των μεταβλητών 'κατά πόσο είναι ικανοποιημένοι από το e-banking' – 'τι θεωρούν πιο σημαντικό στο e-banking'

H0: οι μεταβλητές είναι ανεξάρτητες

H1: οι μεταβλητές εξαρτώνται

ikanopoihmenos_ebanking * pio_simantiko_ebanking Crosstabulation

Count

		pio_simantiko_ebanking			
		Αποδοτικοτητα-ταχυτητα	Ασφαλειαδεδομενων	Και τα δυο	Total
ikanopoihmenos_ebanking	Καθολου	1	4	1	6
	Λιγο	1	5	6	12
	Αρκετα	0	10	5	15

	Πολυ	10	24	17	51
	Δε χρησιμοποιω	0	9	7	16
Total		12	52	36	100

Πίνακας 21: ικανοποιημένοι από το e-banking * τι θεωρούν πιο σημαντικό στο e-banking

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	9,507[a]	8	,301
LikelihoodRatio	12,856	8	,117
Linear-by-Linear Association	,068	1	,794
N of ValidCases	100		

a. 7 cells (46,7%) have expected count less than 5. The minimum expected count is ,72.

Πίνακας 22: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,301 που είναι μεγαλύτερο από το 0,05. Άρα αποδεχόμαστε την H0. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για τοτι θεωρούν πιο σημαντικό στο e-banking**δενεξαρτάται**από το αν είναι ικανοποιημένοι από αυτό.

Συσχέτιση μεταξύ των μεταβλητών 'ηλικία' – 'γνώση σχετικά με biometrics'

H0: οι μεταβλητές είναι ανεξάρτητες

H1: οι μεταβλητές εξαρτώνται

ilikia * gnwsi_biometrikwnCrosstabulation

Count

		gnwsi_biometrikwn		
		Ναι	Οχι	Total
ilikia	18-25	3	3	6
	26-35	25	9	34
	36-45	31	15	46
	46-55	4	6	10
	55+	1	3	4
Total		64	36	100

Πίνακας 23: ηλικία * γνώση βιομετριών

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	7,221[a]	4	,125
LikelihoodRatio	7,022	4	,135
Linear-by-Linear Association	2,828	1	,093
N of ValidCases	100		

a. 5 cells (50,0%) have expected count less than 5. The minimum expected count is 1,44.

Πίνακας 24: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτηντιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,125 που είναι μεγαλύτερο από το 0,05. Άρα

αποδεχόμαστε την Η0. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για τοαν έχουν γνώση σχετικά με biometrics**δενεξαρτάται**από την ηλικία τους.

Συσχέτιση μεταξύ των μεταβλητών 'ικανοποιημένοι από το e-banking' – 'χρήσηbiometricsσε τραπεζική συναλλαγή σήμερα'

Η0: οι μεταβλητές είναι ανεξάρτητες
Η1: οι μεταβλητές εξαρτώνται

ikanopoihmenos_ebanking * xrisi_biometrics_simerra Crosstabulation

Count

		xrisi_biometrics_simerra		
		Ναι	Οχι	Total
ikanopoihmenos_ebanking	Καθολου	1	5	6
	Λιγο	8	4	12
	Αρκετα	6	9	15
	Πολυ	23	28	51
	Δε χρησιμοποιω	0	16	16
Total		38	62	100

Πίνακας 25: ικανοποιημένοι από το e-banking * χρήση biometricsσε τραπεζική συναλλαγή σήμερα

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	16,267[a]	4	,003
LikelihoodRatio	21,729	4	,000
Linear-by-Linear Association	3,209	1	,073
N of ValidCases	100		

a. 3 cells (30,0%) have expected count less than 5. The minimum expected count is 2,28.

Πίνακας 26: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,003 που είναι μικρότερο από το 0,05. Άρα αποδεχόμαστε την H1. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για τοαν χρησιμοποιούν κάποια βιομετρική τεχνολογία σήμερα σε τραπεζική συναλλαγή**εξαρτάται**από το αν είναι ικανοποιημένοι από το e-banking.

Συσχέτιση μεταξύ των μεταβλητών 'ηλικία' – 'αν θα τους επηρέαζε αρνητικά η μικρότερη ταχύτητα ανταπόκρισης των βιομετρικών συστημάτων'

H0: οι μεταβλητές είναι ανεξάρτητες

H1: οι μεταβλητές εξαρτώνται

ilikia * mikroteri_taxutita_epireazei_arnitika Crosstabulation

Count

		mikroteri_taxutita_epireazei_arnitika			
		Ναι	Οχι	Ισως	Total
ilikia	18-25	2	4	0	6
	26-35	9	21	4	34
	36-45	16	21	9	46

	46-55	2	6	2	10
	55+	2	0	2	4
Total		31	52	17	100

Πίνακας 27: ηλικία * αρνητική επιρροή η μικρότερη ταχύτητα ανταπόκρισης των βιομετρικών συστημάτων

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	9,097[a]	8	,334
LikelihoodRatio	11,305	8	,185
Linear-by-Linear Association	,729	1	,393
N of ValidCases	100		

a. 8 cells (53,3%) have expected count less than 5. The minimum expected count is ,68.

Πίνακας 28: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,334 που είναι μεγαλύτερο από το 0,05. Άρα αποδεχόμαστε την H0. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για τοαν θα τους επηρέαζε αρνητικά η μικρότερη ταχύτητα ανταπόκρισης των βιομετρικών συστημάτων **δενεξαρτάται**από την ηλικία του δείγματος.

Συσχέτιση μεταξύ των μεταβλητών 'ηλικία' – 'γιατί να μη χρησιμοποιήσουν biometrics'

H0: οι μεταβλητές είναι ανεξάρτητες

H1: οι μεταβλητές εξαρτώνται

ilikia * gt_na_mi_xrisi_biometrics Crosstabulation

Count

		gt_na_mi_xrisi_biometrics					
		Καταπατησηανθρωπινηςπροσωπικοτητας	Υψηλοκοστος βιομετρικωνσυστηματων	Αβεβαιοτητα για την αξιοπιστια	Εκπαιδευση για τη χρηση τους	Δε γνωριζω	Total
ilikia	18-25	1	0	2	0	3	6
	26-35	19	6	0	0	9	34
	36-45	20	4	4	3	15	46
	46-55	2	1	1	0	6	10
	55+	0	0	0	1	3	4
Total		42	11	7	4	36	100

Πίνακας 29: ηλικία * γιατί να μη χρησιμοποιήσουν biometrics

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	28,714[a]	16	,026
LikelihoodRatio	30,312	16	,016
Linear-by-Linear Association	4,560	1	,033
N of ValidCases	100		

a. 20 cells (80,0%) have expected count less than 5. The minimum expected count is ,16.

Πίνακας 30: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,026 που είναι μικρότερο από το 0,05. Άρα αποδεχόμαστε την H1. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για το λόγο που δε θα χρησιμοποιούσαν τα biometricsστο onlinebanking**εξαρτάται**από την ηλικία.

Συσχέτιση μεταξύ των μεταβλητών 'επίπεδο σπουδών' – 'χρήση biometrics'

H0: οι μεταβλητές είναι ανεξάρτητες

H1: οι μεταβλητές εξαρτώνται

epipedo_spoudwn * xrisi_biometrics_simerra Crosstabulation

Count

		xrisi_biometrics_simerra		
		Ναι	Οχι	Total
epipedo_spoudwn	αποφοιτος_λυκειου	3	9	12
	αποφοιτος_ΑΕΙ/ΤΕΙ	21	40	61
	κατοχος_μεταπτυχιακου	10	9	19
	κατοχος_διδακτορικου	4	4	8
Total		38	62	100

Πίνακας 32: επίπεδο σπουδών * χρήση biometrics

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	3,407[a]	3	,333
LikelihoodRatio	3,393	3	,335
Linear-by-Linear Association	2,853	1	,091
N of ValidCases	100		

a. 3 cells (37,5%) have expected count less than 5. The minimum expected count is 3,04.

Πίνακας 33: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,333 που είναι μεγαλύτερο από το 0,05. Άρα αποδεχόμαστε την H0. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για το αν χρησιμοποιούν biometricsστο onlinebanking**δενεξαρτάται**από το επίπεδο σπουδών.

Συσχέτιση μεταξύ των μεταβλητών 'γνώση σχετικά με biometrics' – 'πόσο θετικοί θα ήταν αν τους ζητούσε η τράπεζα τους να δώσουμε κάποιο βιομετρικό χαρακτηριστικό'

H0: οι μεταβλητές είναι ανεξάρτητες
H1: οι μεταβλητές εξαρτώνται

gnwsi_biometrikwn * thetikoi_na_dwsoun_bio_se_trapeza Crosstabulation

Count

		thetikoi_na_dwsoun_bio_se_trapeza			
		Καθολου	Πολυ	Θα δισταζα	Total
gnwsi_biometrikwn	Ναι	2	53	9	64
	Οχι	36	0	0	36
Total		38	53	9	100

Πίνακας 34: γνώση σχετικά με biometrics * κατά πόσο θα έδιναν κάποιο βιομετρικό τους χαρακτηριστικό στη τράπεζα τους.

Chi-SquareTests

	Value	df	AsymptoticSignificance (2-sided)
PearsonChi-Square	91,776[a]	2	,000
LikelihoodRatio	115,013	2	,000

Linear-by-Linear Association	72,744	1	,000
N of ValidCases	100		

a. 1 cells (16,7%) have expected count less than 5. The minimum expected count is 3,24.

Πίνακας 35: Chi-Square Tests

ΑπότονπίνακαChi-SquareTestsπαρατηρούμεότιτιμήAsymp. Sig. για τον PearsonChi-Square είναι 0,000 που είναι μικρότερο από το 0,05. Άρα αποδεχόμαστε την Η1. Αυτό σημαίνει ότι οι απαντήσεις που δόθηκαν για το αν θα έδιναν αύριο κιόλας ένα βιομετρικό τους χαρακτηριστικό στη τράπεζα τους **εξαρτάται**από το αν γνωρίζουν σχετικά τα biometrics.

Συμπεράσματα έρευνας

Η πλειοψηφία του εξεταζόμενου δείγματος είναι ηλικίας 36-45 ακολουθούμενο από τους 46-55 με τους περισσότερους απόφοιτους ΑΕΙ/ΤΕΙ. Συμπεραίνεται ότι το 71%, ένα μεγάλο ποσοστό, χρησιμοποιεί το internetσε καθημερινή βάση ενώ μόλις ένα 4% φαίνεται να μη βρίσκει ενδιαφέρον το Διαδίκτυο. Όσον αφορά τώρα την ηλεκτρονική τραπεζική, το 84% του δείγματος έχει επιλέξει να υλοποιεί ηλεκτρονικές του συναλλαγές, εκτός βέβαια από το να βρεθούν επιπλέον σε κάποιο φυσικό κατάστημα, το 17% 1-4 φορές το μήνα, ή σε κάποιο ΑΤΜ, το 10% 1-2 φορές την εβδομάδα, χρησιμοποιώντας τον υπολογιστή του ή κάποια κινητή συσκευή.

Λίγο πάνω από το 50% του δείγματος δηλώνει σα το πιο σημαντικό χαρακτηριστικό του e-bankingτην ασφάλεια των δεδομένων, δηλαδή τη προστασία της περιουσίας τους. Το 36% τους ενδιαφέρει επιπλέον και η αποδοτικότητα-ταχύτητα των συστημάτων. Αυτό σημαίνει ότι είναι αναγκαίο οι τράπεζες να δώσουν έμφαση στη θωράκιση των συστημάτων πρόσβασης σε

ηλεκτρονικές συναλλαγές και έπειτα στο πόσο πιο ‘φιλικά’ μπορούν να γίνουν αυτά τα συστήματα προς τον χρήστη. Στη συνέχεια, παρατηρείται ότι μπορεί η πλειοψηφία να γνωρίζει σχετικά με τις βιομετρικές τεχνολογίες, 64%, αλλά το 1/3 σχεδόν του δείγματος, μεγάλο ποσοστό, δε φαίνεται να είναι ενήμεροι για τις βιομετρικές τεχνολογίες στο τομέα της τραπεζικής. Καταλήγουμε επομένως ότι απαιτείται γνωστοποίηση τις συγκεκριμένης τεχνολογίας από τους χρηματοπιστωτικούς φορείς, όπως τράπεζες και σίγουρα ο καθένας ξεχωριστά καλό θα ήταν να ενημερώνεται. Σημαντικό ρόλο στην ενημέρωση και επιρροή θα παίξουν τα μέσα κοινωνικής δικτύωσης γιατί όλα φυσικά είναι θέμα marketing.

Παρατηρείται ότι για το αν θα έδιναν κάποιο βιομετρικό τους χαρακτηριστικό στη τράπεζα τους για να προχωρήσουν σε βιομετρική τραπεζική, εξαρτάται από το αν γνωρίζουν σχετικά με τα biometrics. Αυτό σημαίνει ότι αν πραγματικά θέλουμε να υιοθετήσουμε τα biometricsστη τραπεζική, είναι αναγκαίο να υπάρχει ενημέρωση για τη τεχνολογία αυτή. Επίσης, στη στατιστική ανάλυση συσχέτισης, φαίνεται ότι το πόσοι χρησιμοποιούν κάποια βιομετρική τεχνολογία σήμερα στις onlinesυναλλαγές τους εξαρτάται από το πόσο ικανοποιημένοι είναι γενικά από το e-banking. Μπορεί το ποσοστό αυτών που χρησιμοποιούν σήμερα biometricsνα είναι μικρό αλλά το σύνολο αυτό είναι όσοι είναι ικανοποιημένοι από το onlinebanking. Επομένως, θα ήταν αρκετά σημαντικό να βελτιώσουμε αρχικά τις υπηρεσίες που προσφέρει το e-bankingώστε να αποκτηθεί ένα είδος εμπιστοσύνης προς τις τράπεζες από τους χρήστες και στη συνέχεια πιο εύκολα να υιοθετηθούν οι βιομετρικές τεχνολογίες.

Βιβλιογραφία

[1] https://www.gobankingrates.com/banking/banks/history-online-banking/

[2] https://thefinancialbrand.com/25380/yodlee-history-of-internet-banking/

[3] https://bizfluent.com/about-5109945-history-ebanking.html

[4]"Fingerprint Technology Speeds School Lunch Lines", http://www.eschoolnews.com/showstory.cfm?ArticleID=2146, eSchool News online, April 26, 2001

[5] Authenticate by Security Force Corp, TactileSense™ White Paper, A Breakthrough in Fingerprint Authentication, http://www.ginvar.com/whitepapers/SFC%20 White%20 Paper%20-%20 TactileSense.pdf

[6] http://www.biometrics.org.

[7] Biometrics Technologies website, Biometric Glossary http://www.biometrica.ru/ glossary a.shtml

[8] Σωκράτης Κ. Κατσίκας Κ. Κατσίκας – Δημήτρης Γκρίτζαλης- Στέφανος Γκρίτζαλης ., ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

[9] Δρ. Ελευθέριος Μπόβιος 'Σημειώσεις Εφαρμοσμένης Ασφάλειας Πληροφοριακών Συστηματών

[10] Tiago Duarte, Joao Paulo Pimentao, Pedro Sousa, Sergio Onofre, Biometric Control Access Systems: A Review on technologies to improve their efficiency, Paper.

[11] ΣφυράκηςΠαναγίωτης (2008), Η Χρήση των Βιομετρικών Συστημάτων ως Μέσο Προστασίας των Πολιτών και των Πληροφοριών. Η Αναγκαιότητα Αποδοχής από τους Πολίτες, pp.8-12 και 22-27

[12] Γεροντίδης Ευγένιος (2012), Βιομετρικά Συστήματα Ασφαλείας. Τεχνικές Υλοποίησης και Εφαρμογές τους, pp.7-29

[13] https://www.solarwindsmsp.com/blog/network-authentication-methods

[14] https://link.springer.com/content/pdf/10.1007%2F978-3-642-25734-6_136.pdf

[15]https://www.currencycloud.com/company/blog/the-future-of-biometric-banking/

]16] https://www.academia.edu/1802094/E

[17] Banking_Security_Issues_Is_There_A_Solution_in_Biometrics

[18] https://m.naftemporiki.gr/story/1314989/asfalesteres-online-sunallages-me-biometrics

[19] https://www.ibeta.com/different-types-of-biometrics/

[20] http://www.m2sys.com/blog/financial-services/impact-biometrics-banking/