ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΟ ΜΕΛΛΟΝ ΤΩΝ ΑΝΕΠΑΦΩΝ ΣΥΝΑΛΛΑΓΩΝ ΚΑΙ Η ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Διπλωματική Εργασία

της

Δήμητρας Καραντώνη

Θεσσαλονίκη, Αύγουστος 2023

ΤΟ ΜΕΛΛΟΝ ΤΩΝ ΑΝΕΠΑΦΩΝ ΣΥΝΑΛΛΑΓΩΝ ΚΑΙ Η ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Δήμητρα Καραντώνη

Πτυχίο Οικονομικών Επιστημών, Πανεπιστήμιο Μακεδονίας, 2020

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπουσα Καθηγήτρια
Μαρία Μυλώση

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 1/11/2023

Ευγενία Αλεξανδροπούλου	Φώτιος Κίτσιος	Μαρία Μυλώση
.....	.....	.....

Δήμητρα Καραντώνη

.....

Πίνακας περιεχομένων

Περίληψη

Η εξέλιξη της τεχνολογίας και η ανάπτυξη των ψηφιακών συστημάτων, άλλαξε άρδην τις ψηφιακές υπηρεσίες σε πολλούς κλάδους. Πράγματι, η τραπεζική μέσω κινητού έχει φέρει επανάσταση στον τρόπο με τον οποίο οι άνθρωποι διαχειρίζονται τα οικονομικά τους καθημερινά. Με την άνοδο του mobile banking, οι καταναλωτές μπορούν πλέον να έχουν πρόσβαση στους τραπεζικούς τους λογαριασμούς ανά πάσα ώρα και στιγμή αλλά και να πραγματοποιούν πληρωμές και συναλλαγές με την χρήση βιομετρικών δεδομένων. Ενώ αυτό έχει φέρει απαράμιλλη ευκολία, έχει επίσης επιφέρει νέους κινδύνους ασφαλείας. Οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται τα τρωτά σημεία στις κινητές συσκευές για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε τραπεζικούς λογαριασμούς, να υποκλέψουν προσωπικές πληροφορίες και να πραγματοποιήσουν δόλιες συναλλαγές. Ως αποτέλεσμα, η απειλή της πρόσβασης σε κινητά τηλέφωνα για τραπεζικές συναλλαγές και η ασφάλεια των προσωπικών δεδομένων έχει προκαλέσει μια σημαντική ανησυχία τόσο για τις τράπεζες όσο και για τους πελάτες τους. Στόχος της παρούσας διπλωματικής εργασίας είναι να αναλύσει τις καινοτόμες μορφές βιομετρικών δεδομένων, τους κινδύνους και τις πιθανές επιθέσεις που απορρέουν μέσα από τα σύγχρονα μέσα συναλλαγών αλλά και την ασφάλεια των προσωπικών δεδομένων, η οποία είναι ιδιαιτέρως σημαντική στα συστήματα συναλλαγών.

Λέξεις-Κλειδιά

Ανέπαφες συναλλαγές, μορφές επιθέσεων, ψηφιακή τραπεζική, προσωπικά δεδομένα, ασφάλεια

Abstract

The new of technologies and the development of digital systems, drastically changed the electronic services in many sectors. With the rise of mobile banking, consumers can now access their bank accounts, make payments, and conduct transactions from biometric identification systems. While this has brought unparalleled convenience, it has also brought new security risks. Cybercriminals are exploiting vulnerabilities in mobile devices to gain unauthorized access to bank accounts, intercept personal information, and carry out fraudulent transactions. As a result, the threat in mobile phones from banking transactions and the security of personal data has caused an important concern both from banks and customers. The aim of this work is to analyze the innovative forms of biometric data, the risks and possible attacks arising from modern means of transactions and the security of personal data, which particularly important in transactions systems.

Keywords

Contactless transactions, forms of attacks, digital banking, personal data, security

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες προς τους καθηγητές μου, που με βοήθησαν να ολοκληρώσω τις μεταπτυχιακές μου σπουδές στο πρόγραμμα της Επιχειρηματικής Πληροφορικής του Πανεπιστημίου Μακεδονίας. Θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτρια μου, κ. Μαρία Μυλώση, για την στήριξή της και τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου και τον Γιάννη για την ανεκτίμητη συμπαράσταση που μου προσέφεραν.

ΕΙΣΑΓΩΓΗ

Τα τελευταία χρόνια η άνθιση της τεχνολογικής προόδου και του ψηφιακού μετασχηματισμού έχουν επηρεάσει θετικά σε μεγάλο βαθμό τόσο το καταναλωτικό κοινό όσο και τις επιχειρήσεις. Πολλές τράπεζες, προσπαθούν να επενδύσουν σε νέες μορφές καινοτομίας για να αναδείξουν ευκαιρίες ανάπτυξης. Συχνά δίνουν προτεραιότητα στους πελάτες, προσφέροντάς τους μορφές αξιοποίησης των ψηφιακών εργαλείων που διαθέτουν, για να τους κρατούν διαρκώς ευχαριστημένους και να αυξάνουν το κέρδος τους. Αδιαμφισβήτητα, και οι μικρομεσαίες επιχειρήσεις επωφελούνται από τα ψηφιακά προνόμια που προβάλουν οι τράπεζες.

Ωστόσο, έχει παρατηρηθεί ότι πολλές φορές, ενώ οι τράπεζες καταβάλλουν την μέγιστη δυνατή προσπάθεια για να είναι πρωτοπόρες και καινοτόμες με τα ψηφιακά προϊόντα που αναδεικνύουν, συχνά εμφανίζονται εμπόδια, δημιουργώντας ανασφάλεια, δυσπιστία και φόβο στους χρήστες σχετικά με την χρήση των εύχρηστων εφαρμογών. Το πιο σύνηθες εμπόδιο είναι μέχρι στιγμής οι τραπεζικές επιθέσεις από επιτήδειους που στοχεύουν στην υποκλοπή υπέρογκων χρηματικών ποσών για να αποκομίσουν παράνομα κέρδη εις βάρος των χρηστών. Γι’ αυτό τον λόγο, οι χρήστες οφείλουν να τηρούν τους κανόνες ασφαλείας και να είναι ιδιαιτέρως προσεκτικοί σε τέτοιου είδους επιθέσεις.

Κύριο και αρχικό μέλημα της παρούσας διπλωματικής εργασίας είναι να τεκμηριώσει πλήρως τις νέες ψηφιακές διαδικασίες, τα καινοτόμα βιομετρικά δεδομένα και έπειτα, τη σημαντικότητα και την σπουδαιότητα της ασφάλειας των προσωπικών δεδομένων. Στο τελευταίο μέρος, θα παρατεθούν οι πιθανοί κίνδυνοι που εγκυμονούν από την χρήση ψηφιακών συστημάτων που συνήθως, εμποδίζουν την επιθυμία των χρηστών να χρησιμοποιούν ελεύθερα τις ψηφιακές εφαρμογές, χωρίς φόβο, δυσαρέσκεια και αμφισβήτηση.

ΚΕΦΑΛΑΙΟ 1: ΨΗΦΙΑΚΗ ΤΡΑΠΕΖΙΚΗ

Η ψηφιακή τραπεζική θεωρείται μια καινοτόμος ιδέα για τις τραπεζικές υπηρεσίες αλλά ακόμη και για τους ίδιους τους χρήστες, γιατί μπορούν να εκτελούν άνετα από το κινητό τους τηλέφωνο ή από τον υπολογιστή όλες τις τραπεζικές συναλλαγές. Αυτό το κεφάλαιο έχει ως στόχο να αναδείξει τα πλεονεκτήματα και τα μειονεκτήματα της ψηφιακής τραπεζικής και συγχρόνως, αρκετές πρωτοποριακές υπηρεσίες αλλά και προϊόντα τόσο για τους καταναλωτές όσο και για τις επιχειρήσεις που προσφέρονται στην Εθνική Τράπεζα και στην Τράπεζα Πειραιώς. Παρουσιάζουν ιδιαίτερο ενδιαφέρον, διότι οι υπηρεσίες που παρατίθενται είναι αρκετά εύχρηστες, χωρίς να απαιτείται κάποιο κόστος κατά την χρήση τους.

1.1. Η χρησιμότητα της Ψηφιακής Τραπεζικής

Με τη ραγδαία εξέλιξη της τεχνολογίας οι επιχειρηματικοί κλάδοι έχουν αλλάξει τα επιχειρηματικά τους μοντέλα και έχουν υιοθετήσει μια πιο εξελιγμένη τεχνολογική συνείδηση. Η χρηματοοικονομική τεχνολογία σε συνδυασμό με την τεχνολογική καινοτομία έχουν καταφέρει να δημιουργήσουν ένα αναδυόμενο μετασχηματισμό της τραπεζικής αγοράς (Galvin et al., 2018). Η ψηφιακή τραπεζική είναι μια νέα ηλεκτρονική μορφή τράπεζας, όπου όλες οι τραπεζικές συναλλαγές πραγματοποιούνται μέσα από το διαδίκτυο, με αποτέλεσμα να αυτοματοποιούνται οι διαδικασίες. Αξίζει να σημειωθεί ότι η ψηφιακή τραπεζική εξελίσσεται με ραγδαίους ρυθμούς και υιοθετεί τις πιο σύγχρονες τεχνολογίες σε όλα τα λειτουργικά επίπεδα και σε όλες τις πλατφόρμες παροχής υπηρεσιών. Με τις νέες τεχνολογίες, τα χρηματοπιστωτικά ιδρύματα δεν θα παρέχουν μόνο τις βασικές λειτουργίες, όπως την αίτηση δανείου ή την έκδοση μιας κάρτας, αλλά θα διαθέτουν και πιο σύνθετες συναλλαγές, οι οποίες σχετίζονται με χρηματιστηριακά προϊόντα και επενδύσεις.

Οι πελάτες χρησιμοποιώντας το διαδίκτυο και τα διάφορα ηλεκτρονικά μέσα από τα κλειστά δίκτυα τραπεζών, όπως είναι τα ATMS, APS, POS, αλλά και από τα ανοιχτά δίκτυα, όπως το e-banking, phone Banking και mobile Banking έχουν τη δυνατότητα να πραγματοποιήσουν τις συναλλαγές τους εύκολα και γρήγορα, χωρίς να απαιτείται η φυσική τους παρουσία στο κατάστημα. Ακόμη, μπορούν να

επικοινωνήσουν άμεσα μέσα από μια ψηφιακή πλατφόρμα, σε περίπτωση που αντιμετωπίσουν κάποια δυσκολία κατά τη διάρκεια μιας συναλλαγής.

Αναντίρρητα, παρατηρείται ότι η χρησιμότητα της ψηφιακής τραπεζικής είναι πολύ μεγάλη και γι' αυτό τον λόγο οι τράπεζες οδεύουν ολοένα και περισσότερο στην εφαρμογή αποτελεσματικών και εύχρηστων ψηφιακών συστημάτων, ώστε να διευκολύνουν την καθημερινότητα των πελατών. Ιδιαίτερα σημαντικό είναι το γεγονός ότι οι τράπεζες προκειμένου να ανταπεξέλθουν στις ραγδαίες προκλήσεις του ανταγωνισμού οφείλουν να αναπτύξουν κατάλληλες στρατηγικές και να λάβουν έγκαιρα αποφάσεις, ώστε να διασφαλιστεί η βιωσιμότητά τους και ταυτόχρονα, η ομαλή εξυπηρέτηση των πελατών.

1.2. Η βελτίωση των επιχειρηματικών δραστηριοτήτων μέσω της Ψηφιακής Τραπεζικής

Πράγματι, ο 21^{ος} αιώνας έχει επιφέρει επανάσταση και την ανάπτυξη στην ψηφιακή τεχνολογίας (Norov, 2022). Με την ταχεία άνοδο των ψηφιακών τεχνολογιών και κατ' επέκταση του διαδικτύου ένα μέρος του πληθυσμού παρατηρείται ότι είναι αρκετά πρόθυμο να εμπιστευτεί και να χρησιμοποιήσει τη νέα τεχνολογία που προσφέρεται. Οι τράπεζες λόγω της αυξημένης χρήσης των ψηφιακών μέσων που χρησιμοποιούν οι πελάτες, προσπαθούν να βελτιώνουν σημαντικά τις υπηρεσίες που προσφέρουν. Χαρακτηριστικό παράδειγμα αποτελεί το mobile banking και το online banking που έχουν δημιουργήσει οι εμπορικές τράπεζες για να διευκολύνουν τις τραπεζικές συναλλαγές των πελατών. Επίσης, η απομακρυσμένη πρόσβαση στις τραπεζικές υπηρεσίες μέσω ενός τηλεφώνου ή υπολογιστή δίνει το δικαίωμα στις επιχειρήσεις να κάνουν πληρωμές όλο το εικοσιτετράωρο και να εξοικονομούν χρόνο αλλά και κόστος. Εν κατακλείδι, ιδιαίτερα σημαντική βελτίωση μπορεί να θεωρηθεί η διαδικτυακή συμβουλευτική υπηρεσία που προσφέρεται από τις τράπεζες, όπου οι πελάτες μπορούν να πληροφορούνται και να ενημερώνονται καλύτερα για τυχόν πρόβλημα που αντιμετωπίζουν ή για κάποια ηλεκτρονική ενέργεια που θέλουν να πραγματοποιήσουν (Norov,2022).

1.3. Πλεονεκτήματα και μειονεκτήματα της Ψηφιακής Τραπεζικής

Η χρήση της ψηφιακής τραπεζικής έχει προκαλέσει σημαντικές αλλαγές στις τραπεζικές συναλλαγές, δρώντας σημαντικά στη λειτουργία των ιδρυμάτων και δημιουργώντας οφέλη καθώς και πιθανούς κινδύνους τόσο στους πελάτες όσο και στις τράπεζες. Τα οφέλη από τη χρήση της ψηφιακής τραπεζικής για τους πελάτες είναι τα εξής:

1. Ο πελάτης μπορεί να εξυπηρετηθεί ανά πάσα ώρα και στιγμή και χωρίς καθυστέρηση. Ακόμη, μπορεί να διεκπεραιώσει τις συναλλαγές του άμεσα, χωρίς να μεταβεί σε κάποιο ATM ή να περιμένει έξω από το κατάστημα. Συγκριτικά με τα παραδοσιακά τραπεζικά συστήματα που απαιτούν την φυσική παρουσία των ατόμων υποχρεωτικά, οι ψηφιακές πλατφόρμες έχουν κατασκευαστεί ώστε να προσφέρουν άνεση στους πελάτες, εξοικονομώντας χρόνο.
2. Εξίσου σημαντικό πλεονέκτημα είναι το γεγονός ότι ο πελάτης εξοικονομεί χρήμα, αφού το κόστος για τις περισσότερες συναλλαγές είναι δωρεάν. Βέβαια, υπάρχει μια μικρή χρέωση όταν διενεργείται μια συναλλαγή με μια άλλη τράπεζα, αλλά το κόστος είναι πολύ μικρό, σε σχέση με αυτό που απαιτείται για να προσέλθει κανείς σε ένα τραπεζικό υποκατάστημα.
3. Ιδιαίτερο ενδιαφέρον παρουσιάζει το γεγονός ότι ο πελάτης έχει τη δυνατότητα να ελέγχει οποιαδήποτε στιγμή τη κίνηση των λογαριασμών, το ιστορικό, να ενημερώνεται για την τιμή των μετοχών, να μεταφέρει κεφάλαια εντός της τράπεζας, ακόμη και να πληρώνει οφειλές σε διάφορους οργανισμούς.
4. Οι τράπεζες επενδύουν πολλά χρήματα ώστε να καταφέρουν να εξασφαλίσουν στους πελάτες τους την ασφάλεια των συναλλαγών αλλά και την ταχύτερη εξυπηρέτηση σε ποικίλα θέματα που αναφέρθηκαν παραπάνω.

Βέβαια, και οι τράπεζες μπορούν να επωφεληθούν από τη ψηφιακή τραπεζική με τους εξής τρόπους:

1. Με την ανάπτυξη της τεχνολογίας και τις εξελιγμένες υπηρεσίες που παρέχονται, ενισχύεται η ανταγωνιστικότητα μεταξύ των τραπεζών,

επεκτείνοντας τη θέση τους στην αγορά με την προσέλκυση περισσότερων πελατών (Ding et al., 2022). Το ανταγωνιστικό πλεονέκτημα που αποκτά μια τράπεζα λόγω της υιοθέτησης εξελιγμένων τεχνολογιών είναι άρρηκτα συνδεδεμένο με την ψηφιακή κουλτούρα, δηλαδή το εταιρικό περιβάλλον το οποίο ενθαρρύνει και στηρίζει τη χρήση της τεχνολογίας ώστε οι εργαζόμενοι να δουλεύουν καινοτόμα και αποτελεσματικά.

2. Οι τράπεζες μέσω της ψηφιακής τραπεζικής μπορούν να εξυπηρετήσουν τους πελάτες όπου και αν βρίσκονται, καθώς με τις ηλεκτρονικές της υπηρεσίες καταρρίπτει τα γεωγραφικά όρια προσφέροντας καινοτόμες υπηρεσίες και λύσεις. Με αυτό τον τρόπο αυξάνεται η αποτελεσματικότητα των τραπεζικών εργασιών, η αποδοτικότητα αλλά και το πελατολόγιο της εν λόγω τράπεζας (Livishko, 2020).
3. Ένα ακόμη σημαντικό πλεονέκτημα είναι το γεγονός ότι χρησιμοποιώντας τα σύγχρονα συστήματα πληροφορικής, οι τράπεζες δημιουργούν μια ισχυρή βάση δεδομένων για κάθε πελάτη, ικανοποιώντας όλες τις ανάγκες που μπορεί να δημιουργηθούν.
4. Οι τράπεζες μειώνουν τα λειτουργικά τους έξοδα μέσω των αυτοματοποιημένων ψηφιακών συναλλαγών και παράλληλα, αντικαθιστούν την περιττή χειρωνακτική εργασία με στόχο τη δημιουργία νέων επενδύσεων (Livishko, 2020).

Παρά το σημαντικά πλεονεκτήματα που προσφέρει η ψηφιακή τραπεζική στους πελάτες, υπάρχουν ασφαλώς και ορισμένα μειονεκτήματα τα οποία λειτουργούν ανασταλτικά στην καθιέρωσή της.

1. Υπάρχουν άτομα μεγάλης ηλικίας τα οποία δυσκολεύονται να εξοικειωθούν και να προσαρμοστούν με τις νέες τεχνολογίες και το διαδίκτυο. Επιπρόσθετα, η μη επαρκής γνώση για τη λειτουργία των νέων τεχνολογιών προκαλεί περισσότερες αμφιβολίες για τη χρησιμότητά της, δημιουργώντας την αίσθηση κινδύνου σχετικά με το πόσο ασφαλής είναι η ψηφιακή τραπεζική.
2. Επιπλέον, με την εφαρμογή της ψηφιακής τραπεζικής υπάρχει έλλειψη φυσικής επικοινωνίας με τους υπαλλήλους, αφού καμία συναλλαγή δεν απαιτεί την παρουσία των ατόμων σε κάποιο κατάστημα. Αναμφίβολα, αρκετοί πελάτες όταν μεταβαίνουν σε κάποιο φυσικό κατάστημα, νιώθουν μεγαλύτερη εμπιστοσύνη και ασφάλεια με την ανθρώπινη σχέση που

δημιουργείται με τους υπαλλήλους της τράπεζας και πιστεύουν ότι θα εξυπηρετηθούν καλύτερα.

3. Ένα πολύ σημαντικό μειονέκτημα είναι ότι η ελλιπής ασφάλεια συναλλαγών που αντιμετωπίζει καθημερινά η ψηφιακή τραπεζική, καθώς πολλές φορές πραγματοποιούνται διάφορες επιθέσεις με στόχο την υποκλοπή προσωπικών πληροφοριών, κωδικών και χρημάτων. Με διάφορες εφαρμογές και ιστοσελίδες ψαρέματος, οι εγκληματίες καταφέρνουν και αποκτούν πρόσβαση σε ιδιωτικούς λογαριασμούς.

Η ύπαρξη ορισμένων μειονεκτημάτων μπροστά στα πολύ σημαντικά πλεονεκτήματα που προσφέρει η χρήση της ψηφιακής τραπεζικής στις τράπεζες δεν αποτελούν ανασταλτικό παράγοντα για τη χρήση της. Τα σημαντικότερα μειονεκτήματα είναι τα εξής:

1. Απαιτείται ένα τεράστιο κόστος επένδυσης από τις τράπεζες, οι οποίες χρησιμοποιούν κεφάλαια για την ανάπτυξη, την εξυπηρέτηση και την ασφάλεια των ψηφιακών τεχνολογιών που προσφέρουν στους πελάτες.
2. Αναμφίβολα, η ψηφιακή τραπεζική έχει προκαλέσει ριζικές αλλαγές κυρίως στο τραπεζικό προσωπικό, διότι λόγω του ραγδαίου ρυθμού ψηφιοποίησης και αυτοματοποίησης των διαδικασιών, απαιτούνται εξειδικευμένοι υπάλληλοι στα τραπεζικά συστήματα με υψηλό κόστος, με αποτέλεσμα οι ανειδίκευτοι εργαζόμενοι να οδηγηθούν ακουσίως στην ανεργία (Cao 2021, Li et al., 2020, Sartori & Theodorou 2022).
3. Η αδυναμία ορισμένων πελατών να προσαρμοστούν στις νέες τεχνολογίες και στη νέα ψηφιακή εποχή έχει ως αποτέλεσμα τη μείωση του πελατολογίου των τραπεζών. Οι πελάτες με βάση την ηλικία και το μορφωτικό επίπεδο έχουν διαφορετική εξοικείωση με τα νέα συστήματα και γι’ αυτό οι τράπεζες θα πρέπει να προσπαθήσουν να κερδίσουν την εμπιστοσύνη των καταναλωτών για τη μέγιστη ικανοποίησή τους.
4. Η ασφάλεια των συναλλαγών λόγω κακόβουλων και συχνών επιθέσεων από διάφορους εισβολείς είναι ένα πολύ σοβαρό μειονέκτημα, το οποίο οι τράπεζες θα πρέπει να αντιμετωπίσουν, καθώς μπορεί να επηρεάσει αρνητικά το κύρος και τη φήμη της αλλά και την εμπιστοσύνη των πελατών.

1.4. Μελέτη περίπτωσης: Εθνική Τράπεζα

Η ψηφιακή αλλαγή έχει επηρεάσει θετικά τον τραπεζικό τομέα. Ως επακόλουθο αυτού, οι τράπεζες από τις οποίες αποτελείται ο χρηματοπιστωτικός τομέας, προωθούν διαρκώς το τελευταίο καιρό διάφορα ψηφιακά προϊόντα και υπηρεσίες, με απώτερο στόχο την εξέλιξη των οργανισμών γύρω από τις ψηφιακές τεχνολογίες και ταυτόχρονα, επιθυμούν ολοένα και περισσότερο να παραμένουν ανταγωνιστικές αυξάνοντας συνεχώς τα κέρδη τους. Επίκεντρο σε κάθε ενέργεια ή προϊόν παραμένει ο καταναλωτής, εφόσον ο καταναλωτής είναι αυτός που θα επιλέξει να χρησιμοποιήσει ή όχι ένα ψηφιακό προϊόν. Επομένως, για να υπάρχει μεγαλύτερη ψηφιακή πρόοδος και καινοτομία στα προϊόντα και στις υπηρεσίες, οι τράπεζες οφείλουν να τα διαμορφώσουν με τέτοιο τρόπο ώστε να είναι όσο το δυνατόν περισσότερο φιλικά και συγχρόνως πρακτικά ως προς τον «ψηφιακό πελάτη».

Σ' αυτό το κεφάλαιο θα τεκμηριωθεί πλήρως η μελέτη περίπτωσης της Εθνικής Τράπεζας της Ελλάδος, η οποία διατηρεί μεγάλο ποσοστό αγοράς του χρηματοπιστωτικού τομέα στη χώρα μας. Πρώτον, ακολουθεί μια συνοπτική παρουσίαση του οράματος και της στρατηγικής της τράπεζας και στη συνέχεια, αναλύονται τα ψηφιακά προϊόντα και οι υπηρεσίες που προσφέρονται στους πελάτες, τα οποία θα είναι ιδιαιτέρως πρακτικά στην χρήση τους. Παρακάτω, αναφέρονται τα προϊόντα που προσφέρει η τράπεζα στα μέσα κοινωνικής δικτύωσης, με σκοπό την προώθησή και την διαφήμισή τους για την προσέλκυση περισσότερου κοινού. Τέλος, ακολουθεί η μελέτη της Τράπεζας Πειραιώς, η οποία παρέχει ένα πλήρες φάσμα τραπεζικών συναλλαγών, δίνοντας έμφαση στους ιδιώτες και στις μικρομεσαίες επιχειρήσεις και αναλύονται ορισμένα ψηφιακά προϊόντα και υπηρεσίες που διευκολύνουν αρκετά τους καταναλωτές.

1.5. Το όραμα της «Εθνικής Τράπεζας της Ελλάδος»

Η Εθνική Τράπεζα της Ελλάδος (ΕΤΕ) ιδρύθηκε το 1841 και θεωρείται μια από τις μεγαλύτερες χρηματοοικονομικές υπηρεσίες. Όραμά της είναι να βρίσκεται στην πρώτη επιλογή των καταναλωτών και των επενδυτών, να είναι αξιόπιστη, αποτελεσματική και ταυτόχρονα αναπτυξιακή, παρέχοντας συνεχώς νέες προοπτικές εξέλιξης στους ανθρώπους αλλά και στις επιχειρήσεις. Τηρώντας αυτές τις αξίες, η

Εθνική Τράπεζα προσπαθεί να βελτιώνεται διαρκώς παρά τις προκλήσεις που ενδεχομένως να δέχεται και να προσφέρει ένα καλύτερο και βιώσιμο μέλλον. Ακόμη, είναι σημαντικό ότι, η συγκεκριμένη τράπεζα παρουσιάζεται ως ηγέτης της πράσινης οικονομίας και εφαρμόζει πρακτικές, οι οποίες είναι φιλικές προς το περιβάλλον. Θέτοντας λοιπόν, ως κεντρικό άξονα τον άνθρωπο και το περιβάλλον, η Εθνική Τράπεζα καταβάλλει κάθε δυνατή προσπάθεια για να εξασφαλίσει ένα αποτελεσματικό πλαίσιο επιχειρηματικής ηθικής (www.nbg.gr).

1.6. Ψηφιακές μορφές πληρωμής για τον καταναλωτή

Η Εθνική Τράπεζα της Ελλάδος έχει καταφέρει τα τελευταία χρόνια να αναδειχθεί εξαιτίας της κατασκευής ενός σύγχρονου ηλεκτρονικού σχεδίου παροχής υπηρεσιών και καινοτόμων προϊόντων για τον καταναλωτή, με σκοπό να διευκολύνει τις καθημερινές του συναλλαγές. Προσφέρει λοιπόν, ποικίλες τεχνικές και εργαλεία σε καταναλωτές και σε μικρομεσαίες επιχειρήσεις.

Σ' αυτή την ενότητα, προβάλλονται αναλυτικά τα νέα ψηφιακά μέσα που υλοποίησε η Εθνική Τράπεζα, με σκοπό την γρήγορη και αποτελεσματική εξέλιξη του πελάτη, εφόσον έχουν εισχωρήσει σημαντικά τα τελευταία χρόνια στην καθημερινότητα πολλών ατόμων.

1.6.1 Digital Banking

Η Εθνική Τράπεζα με την εφαρμογή του digital banking προσφέρει την ευκαιρία στους χρήστες να πραγματοποιούν άμεσες και αξιόπιστες συναλλαγές από το κινητό τους τηλέφωνο αλλά και μέσα από τις ανανεωμένες εφαρμογές κοινωνικής δικτύωσης, όπως είναι το Facebook ή το Viber. Η διαδικασία είναι απλή, γιατί ο πελάτης μπορεί να συνδεθεί στην εφαρμογή, χρησιμοποιώντας τον κωδικό που του παραχώρησε η τράπεζα για την υπηρεσία i-bank Digital Banking. Με μία κίνηση ο πελάτης έχει πολλά πλεονεκτήματα, όπως η παρακολούθηση και ο έλεγχος των κινήσεων του λογαριασμού του, ο συγκεντρωτικός έλεγχος των εσόδων και εξόδων και η διαχείριση των οικονομικών του. Αναντίρρητα, διασφαλίζεται το απόρρητο των κινήσεων, η προστασία και ο έλεγχος των ηλεκτρονικών συναλλαγών από προσπάθειες υποκλοπής στοιχείων. Παρακάτω, θα αναφερθούν ορισμένα σύγχρονα

συστήματα πληρωμών που έχουν υιοθετήσει οι τράπεζες για την καλύτερη εξυπηρέτηση των καταναλωτών. Αυτά τα συστήματα είναι τα εξής:

1. **Πληρωμή με QR code**

Ένας κωδικός QR είναι μία από τις πιο γνωστές μεθόδους πληρωμής. Βασική και αναγκαία προϋπόθεση χρήσης του συγκεκριμένου εργαλείου είναι η εταιρία με την οποία συναλλάσσεται ο πελάτης να διαθέτει τερματικό POS. Πιο αναλυτικά, η τράπεζα διανέμει σήματα στις συγκεκριμένες εταιρίες και επιχειρήσεις, τα οποία τοποθετούνται σε φανερά σημεία, έτσι ώστε οι καταναλωτές να μπορούν να τα αντιληφθούν, όταν θέλουν να χρησιμοποιήσουν την υπηρεσία. Όλες οι συναλλαγές γίνονται με άμεσο τρόπο, αρκεί ο καταναλωτής να πλησιάσει την κάμερα της κινητής συσκευής που διαθέτει και να φωτογραφίσει τον κωδικό QR που εκτυπώνεται από τη συσκευή του εμπόρου. Επίσης, ο κωδικός QR είναι αρκετά βολικός και δημοφιλής τρόπος πληρωμής ακόμη και για ανθρώπους που δεν διαθέτουν υψηλές γνώσεις τεχνολογίας. Βέβαια, το πιο σημαντικό είναι ότι μέσω αυτής της μεθόδου οι πληρωμές είναι ασφαλείς και προστατευμένες, διότι δεν απαιτείται να εισαχθεί κάποιος προσωπικός κωδικός στο μηχάνημα της επιχείρησης, το οποίο ασφαλώς μειώνει σημαντικά τον κίνδυνο απάτης (Smith, 2019).

2. **Ανέπαφη πληρωμή**

Η υπηρεσία ανέπαφης πληρωμής της Εθνικής Τράπεζας, δίνει την ευελιξία σε πολλούς χρήστες να ολοκληρώνουν τις ανέπαφες συναλλαγές μέσω του κινητού τηλεφώνου τους. Ο χρήστης σε αυτή την εφαρμογή, χρειάζεται μόνο να πατήσει την επιλογή «Contactless Payment» της κινητής συσκευής του. Αυτομάτως, μπορεί να ελέγξει από το κινητό του τηλέφωνο το χρηματικό ποσό της συναλλαγής που δόθηκε. Συγχρόνως, η εφαρμογή ενημερώνεται με αποτέλεσμα ο χρήστης να γνωρίζει το διαθέσιμο ποσό που του έχει απομείνει. Ασφαλώς, η πληρωμή γίνεται με απόλυτη εχεμύθεια και σε ελάχιστα δευτερόλεπτα. Αναφορικά με την τράπεζα, οι ανέπαφες συναλλαγές προσφέρουν ταχύτητα και ευκολία, κάτι που είναι ιδιαιτέρως σημαντικό όχι μόνο για τους πελάτες αλλά και για τις ίδιες τις τράπεζες.

3. **Συναλλαγή με την χρήση IRIS**

Ο καταναλωτής μπορεί να αξιοποιήσει την σύγχρονη και χρήσιμη υπηρεσία IRIS Payments για να εξοφλήσει τις ηλεκτρονικές του αγορές ή συναλλαγές, μέσα σε ένα

ασφαλές και σίγουρο περιβάλλον ή να αποστείλει χρήματα οπουδήποτε στην Ελλάδα. Η διαδικασία διαρκεί μερικά μόνο λεπτά και εκτελείται με αρκετά εύκολο και γρήγορο τρόπο. Επιπλέον, μπορεί ο χρήστης να ενημερώνεται με μήνυμα κάθε φορά που κάποιος ζητάει να λάβει ένα ποσό, να διατηρεί ένα πλήρες ιστορικό συναλλαγών και να εκτελεί συνολικά δεκαπέντε συναλλαγές ημερησίως. Με την ψηφιακή τεχνολογία όλες οι οικονομικές διαδικασίες γίνονται απευθείας, χωρίς την παραμικρή καθυστέρηση.

4. **Εξόφληση ηλεκτρονικών παραγγελιών**

Η συγκεκριμένη διαδικασία είναι ίσως πιο γνώριμη από τις προηγούμενες που αναφέρθηκαν. Μετά την επιλογή των προϊόντων που θα αποφασίσει να παραγγείλει ο καταναλωτής, θα χρειαστεί να πληρώσει το ανάλογο ποσό. Το μόνο που χρειάζεται είναι απλώς να φωτογραφίσει τον κωδικό QR που εμφανίζεται στην οθόνη του υπολογιστή ή του κινητού τηλεφώνου και η διαδικασία πληρωμής έχει ολοκληρωθεί σε δευτερόλεπτα. Φυσικά, μπορεί να εγκρίνει την πληρωμή μέσω του push notification, όπου αποστέλλεται ένα μήνυμα από την τράπεζα στο κινητό τηλέφωνο του χρήστη και αυτός από την πλευρά του πατάει αποδοχή πληρωμής. Τέλος, είναι ιδιαίτερα βασικό να σημειωθεί ότι η τράπεζα εκτός από τις σύγχρονες υπηρεσίες που παρέχει, αναδεικνύει και τον φιλανθρωπικό της χαρακτήρα δεδομένου ότι διαθέτει μια ειδική επιλογή σύμφωνα με την οποία ο καταναλωτής μπορεί, αν επιθυμεί, να συμβάλλει οικονομικά μεταφέροντας ένα επαρκές ποσό σε διάφορα φιλανθρωπικά ιδρύματα, φορείς και οργανισμούς. Γίνεται αντιληπτό ότι σε κάθε σχεδιασμό μιας ηλεκτρονικής εφαρμογής, η Εθνική Τράπεζα μεριμνά πάντοτε για το κοινωνικό σύνολο.

1.6.2 Ηλεκτρονικό πορτοφόλι

Η Εθνική Τράπεζα, ουραγός του ελληνικού τραπεζικού κλάδου κυκλοφόρησε το 2017 την πρώτη wearable υπηρεσία ανέπαφων πληρωμών, όπου είναι βασισμένη στην τεχνολογία Near Field Communication. Πρόκειται για τη δημιουργία και την εφαρμογή ενός αξεσουάρ, το οποίο από την πρώτη στιγμή εντυπωσίασε το κοινό και θεωρήθηκε έξυπνο προϊόν στη χρήση του και μοναδικό σε παγκόσμιο επίπεδο. Ουσιαστικά, φτιάχτηκαν λαμπερά και όμορφα κοσμήματα, δαχτυλίδια και βραχιόλια, για άντρες και γυναίκες με ενσωματωμένη την ψηφιακή τεχνολογία ανέπαφων

συναλλαγών. Τα κυριότερα πλεονεκτήματα που προσφέρει το εξάρτημα είναι η άνεση και οι τακτικές αναβαθμίσεις. Στην πρώτη περίπτωση, το κόσμημα έχει το ρόλο της πιστωτικής κάρτας και του τραπεζικού λογαριασμού και στην δεύτερη περίπτωση, οι τράπεζες προχωρούν πολύ συχνά σε αναβαθμίσεις και βελτιώσεις των εφαρμογών, διότι βρίσκονται σε διαρκή ανταγωνισμό με άλλες υπηρεσίες. Γι' αυτό, δημιούργησαν με μεγάλη έμπνευση και επιτυχία την εφαρμογή αυτού του κοσμήματος, ώστε ο πελάτης ακόμη και αν ξεχάσει την πιστωτική του κάρτα να μπορεί με αυτό τον τρόπο να προβεί σε ηλεκτρονική συναλλαγή.

1.6.3 i-bank Pass

Το i-bank pass είναι μια αρκετά ενδιαφέρουσα και χρήσιμη υπηρεσία της Εθνικής Τράπεζας που έχει ως στόχο την διευκόλυνση τον καταναλωτή όταν αποφασίσει να παραβρεθεί στο φυσικό κατάστημα. Αυτή η εφαρμογή ενημερώνει το καταναλωτικό κοινό που βρίσκονται τα πιο κοντινά καταστήματα της ΕΤΕ και ποιο είναι το ωράριο λειτουργίας τους για να εξυπηρετηθούν. Ειδικότερα, οι χρήστες όταν εισέλθουν σε κάποιο φυσικό κατάστημα, μπορούν να εκδώσουν δωρεάν ένα ηλεκτρονικό αριθμό προτεραιότητας για να εξυπηρετηθούν από τα ταμεία της τράπεζας, δίχως να περιμένουν άσκοπα αρκετές ώρες. Όταν έρθει η σειρά του καταναλωτή, η τράπεζα τον ενημερώνει με γραπτό μήνυμα στο κινητό του τηλέφωνο προκειμένου να προβεί εγκαίρως στο κατάστημα. Με την υπηρεσία αυτή, αφενός η Εθνική Τράπεζα προσπαθεί να μειώσει την αναμονή των πελατών μπροστά από τα ταμεία της και αφετέρου, ο πελάτης μπορεί να ολοκληρώσει όλες τις προγραμματισμένες εξωτερικές δουλειές που ενδεχομένως να έχει. Έτσι, η τράπεζα καταφέρνει να δημιουργεί ολοένα και περισσότερους χαρούμενους πελάτες, που είναι πρόθυμοι να χρησιμοποιούν τακτικά αυτή την εύχρηστη και βολική εφαρμογή. Φυσικά, λόγω της ευκολίας της, η εν λόγω υπηρεσία προσφέρεται στα περισσότερα καταστήματα της Εθνικής Τράπεζας. Τέλος, ο πελάτης ιδίως αν είναι ηλικιωμένος, μπορεί να κλείσει ηλεκτρονικό ραντεβού, ώστε να μην χρειαστεί να παραμείνει στην ουρά αναμονής και να βοηθηθεί γρήγορα από τους αρμόδιους υπαλλήλους.

1.6.4 i-bank Statements

Η εν λόγω υπηρεσία παραχωρεί το δικαίωμα απόκτησης ηλεκτρονικών ειδοποιήσεων για την έκδοση των αντιγράφων των λογαριασμών τους. Οι λογαριασμοί αυτοί μπορεί να είναι διάφοροι, για παράδειγμα να αφορούν την αποπληρωμή μιας πιστωτικής κάρτας ή ενός δανείου. Ασφαλώς, παρέχεται ένα πλήρες ηλεκτρονικό αρχείο με τους λογαριασμούς και η ενημέρωση γίνεται άμεσα, αφού η τράπεζα αποστέλλει ένα ηλεκτρονικό e-mail, με μηδενικό κόστος. Η πρόσβαση μπορεί να γίνει με την χρήση των προσωπικών κωδικών κάθε πελάτη προκειμένου να προστατευθούν τα προσωπικά δεδομένα και να αποφευχθούν τυχόν κίνδυνοι διαρροής τους. Επιπρόσθετα, σε αυτή την εφαρμογή οι πελάτες έχουν την ευκολία να εκτυπώσουν ή να αποθηκεύσουν τα αντίγραφα στον υπολογιστή ή στο κινητό τηλέφωνο. Τα αντίγραφα είναι διαθέσιμα για 18 μήνες αλλά ακόμη και αν ένας πελάτης χρειαστεί έναν παλαιότερο λογαριασμό, μπορεί να επικοινωνήσει με το κατάστημα για να τον βοηθήσει να το ανακτήσει.

Αξίζει να σημειωθεί ότι, η συγκεκριμένη εφαρμογή συμβάλλει στην προστασία του περιβάλλοντος, διότι μειώνεται σημαντικά η χρήση χαρτιού, μελανιού και ενέργειας, που είναι απαραίτητα για την αποστολή έντυπων ενημερώσεων. Καταλήγοντας, η τράπεζα έχει δημιουργήσει έναν απλό τρόπο ενεργοποίησης της υπηρεσίας για μέγιστη ευκολία, ενώ παράλληλα, δίνει το δικαίωμα στους πελάτες να σταματήσουν οποιαδήποτε στιγμή θελήσουν τον συγκεκριμένο τρόπο ηλεκτρονικής μορφής και να επαναφέρουν όπως πριν, έντυπους τους λογαριασμούς για να εξοφλήσουν τις οφειλές τους.

1.7 Ψηφιακές μορφές πληρωμής για τις επιχειρήσεις: i-bank e-Enterprise

Η Εθνική Τράπεζα της Ελλάδος παρέχει ένα πλήρες σύστημα πληρωμών προς τους επαγγελματίες σε οποιαδήποτε κλάδο και αν αυτοί δραστηριοποιούνται. Με την συγκεκριμένη εφαρμογή δίνεται μια αναβαθμισμένη ψηφιακή εξυπηρέτηση και τα πλεονεκτήματα είναι πολλαπλά και είναι τα εξής:

- Παρακολούθηση συναλλαγών ανά πάσα ώρα και στιγμή, δεδομένου ότι υπάρχει η δυνατότητα ελέγχου των κινήσεων σε πραγματικό χρόνο.

- Απόλυτη αυτονομία στη διαχείριση συναλλαγών, δεδομένου ότι είναι εφικτή η πλήρης εικόνα των κινήσεων από την πλευρά των επαγγελματιών που διαθέτουν επιχειρήσεις.
- Έλεγχος της διαδικασίας checkout των πελατών τους.
- Virtual POS, αφού με την ψηφιακή λειτουργία του τερματικού POS απλοποιούνται σημαντικά οι δραστηριότητες, όπως για παράδειγμα οι επιστροφές χρημάτων.
- Εξόφληση με οποιοδήποτε τρόπο, όπως με e-mail κάνοντας την χρήση εικονικού POS ή με χρήση της κάρτας. Και στις δύο περιπτώσεις οι πελάτες έχουν δικαίωμα επιλογής για την ολοκλήρωση της αγοράς τους.

1.7.1 i-bank B2B

Η συγκεκριμένη εφαρμογή μπορεί να προβεί σε αυτόματες εισπράξεις και να ενημερώνονται απευθείας τα εσωτερικά συστήματα της επιχείρησης. Ορισμένα πλεονεκτήματα αυτής της εφαρμογής είναι τα εξής:

- Εύκολη διαδικασία εκκαθάρισης, εφόσον οι συναλλαγές μπορούν να ολοκληρωθούν όπου και αν βρίσκεται ο επιχειρηματίας.
- Εξάλειψη κινδύνου, διότι φαίνονται οι κινήσεις των επιχειρηματικών λογαριασμών ανά πάσα ώρα και στιγμή.
- Γρήγορη και άμεση λήψη αρχείων με εύκολο τρόπο.
- Προνομιακή χρηματοδότηση, γιατί μπορούν να φανούν συγκεντρωτικά τα έσοδα και τα έξοδα της επιχείρησης.
- Αυτόματη ενημέρωση εσωτερικών συστημάτων, με αποτέλεσμα να μην χάνεται πολύτιμος και άσκοπος χρόνος στα φυσικά καταστήματα της τράπεζας.

Αν παρατηρήσει και μελετήσει κανείς τις παραπάνω εφαρμογές, θα διαπιστώσει ότι με μία απλή κίνηση τα οφέλη για την επιχείρηση είναι πολλαπλά. Με την πάροδο του χρόνου η τράπεζα προσπαθεί να αναπτύξει κι άλλες εφαρμογές για να προσελκύσει περισσότερους επαγγελματίες και να τους γλιτώσει από περιττό χρόνο και κόστος. Σε αυτή την περίπτωση επωφελείται όχι μόνο ο επαγγελματίας αλλά και η ίδια η τράπεζα.

1.7.2 key2Pay

Η νέα υπηρεσία key2pay της Εθνικής Τράπεζας επιτρέπει στις επιχειρήσεις ακόμη και αν δεν διαθέτουν τερματικό POS να πραγματοποιήσουν εξ' αποστάσεως πωλήσεις και να διεκπεραιώσουν τις πληρωμές των πελατών. Τα θετικά σημεία αυτής της εφαρμογής είναι αρκετά, διότι οι επιχειρηματίες μπορούν να παρουσιάσουν τα προϊόντα τους επικοινωνώντας ηλεκτρονικά με τους πελάτες τους ώστε να ενημερωθούν πλήρως και ορθά για τη δυνατότητα πληρωμής ενός προϊόντος σε άτοκες δόσεις με την χρήση κάρτας. Επιπλέον, επιτρέπεται να διαχειρίζονται παραγγελίες όλες τις ώρες μιας και με την συγκεκριμένη υπηρεσία μπορούν με απλό και εύκολο τρόπο οι επιχειρήσεις να παρακολουθούν ηλεκτρονικά όλες τις εντολές πληρωμής. Τέλος, είναι σημαντικό να τονιστεί ότι εξασφαλίζεται η μέγιστη δυνατή ασφάλεια με την υπηρεσία Key2pay, διότι η Εθνική Τράπεζα υποστηρίζει πλήρως το πρωτόκολλο ασφαλείας EMV 3DS για τους εμπόρους και συμμορφώνεται με τις απαιτήσεις ταυτοποίησης πελάτη για τους κατόχους καρτών.

1.8. Μελέτη Περίπτωσης: Τράπεζα Πειραιώς

Η Τράπεζα Πειραιώς, 100% θυγατρική εταιρία της Πειραιώς Financial Holdings, ιδρύθηκε το 1916 και αποτελεί την κορυφαία τράπεζα στην Ελλάδα με βάση τα μερίδια αγοράς δανείων, και παρουσία δικτύου. Η Τράπεζα Πειραιώς παρέχει πλήρες φάσμα τραπεζικών εργασιών, με ιδιαίτερη τεχνογνωσία στις υπηρεσίες προς μεσαίες και μικρές επιχειρήσεις και προς ιδιώτες, στην ηλεκτρονική τραπεζική, καθώς και στην κεφαλαιαγορά. Όπως η Εθνική Τράπεζα της Ελλάδος έχει κατασκευάσει ένα έξυπνο σύστημα σύγχρονων εργαλείων και εφαρμογών παρέχοντας ολοκληρωμένες ιδέες σε πελάτες αλλά και σε μικρομεσαίες επιχειρήσεις, το ίδιο συμβαίνει και με την Τράπεζα Πειραιώς (https://pireausbank.gr/).

1.8.1 Για τον καταναλωτή

Σ’ αυτή την ενότητα αναλύονται τα σύγχρονα προϊόντα και οι υπηρεσίες ψηφιακής μορφής που δημιούργησε η Τράπεζα Πειραιώς κατά την διαδικασία της ψηφιακής της μετατροπής. Στο επίκεντρο βρίσκονται οι καταναλωτές και οι μικρομεσαίες επιχειρήσεις, καθώς οι διαδικασίες αυτές έχουν ως κύριο μέλημα την εξοικείωσή τους με τις νέες τεχνολογίες του τραπεζικού κλάδου.

1.8.1.1 Contactless Payment

Η Τράπεζα Πειραιώς παρέχει τη δυνατότητα των ανέπαφων συναλλαγών, οι οποίες βασίζονται στην ασύρματη τεχνολογία μικρής εμβέλειας NFC (Near Field Communication) και δίνουν τη δυνατότητα στον πελάτη να πραγματοποιήσει τις αγορές του πλησιάζοντας απλά την κάρτα του στο κατάλληλο μηχάνημα. Ο πελάτης επωφελείται από την ταχύτητα και την ασφάλεια, διότι αφενός όλες οι συναλλαγές ολοκληρώνονται μέσα σε ελάχιστα λεπτά και αφετέρου, ο συγκεκριμένος τρόπος πραγματοποίησης αγορών είναι ασφαλέστερος σε σχέση με τα μετρητά, αφού η κάρτα μένει πάντοτε στα χέρια του πελάτη κατά τη διαδικασία της πληρωμής. Τέλος, σημαντικό είναι το γεγονός ότι παρέχεται μεγάλη ευκολία, διότι δεν χρειάζεται να αναζητεί ο πελάτης κέρματα ή να πληκτρολογεί τον Προσωπικό Μυστικό Αριθμό (PIN) για μικρές αγορές.

1.8.1.2 e-branch

Το e-branch είναι το νέο και καινοτόμο κατάστημα της Τράπεζας Πειραιώς που προσφέρει τραπεζικές συναλλαγές μέσα από έξυπνες υπηρεσίες. Οι νέοι τρόποι εξυπηρέτησης είναι οι εξής:

- Ταμίας από Απόσταση, όπου μπορεί ο πελάτης να συνδεθεί μέσω βίντεο κλήσης με τον ταμία και να πραγματοποιήσει οποιαδήποτε συναλλαγή επιθυμεί, όπως κατάθεση μετρητών, μεταφορά χρημάτων, πληρωμή λογαριασμών αλλά και πληρωμή ηλεκτρονικού παραβόλου.
- Πρωτοποριακές υπηρεσίες για Άτομα με Αναπηρία. Τα άτομα με προβλήματα όρασης πραγματοποιούν συναλλαγές ταμείου μέσω της παραπάνω υπηρεσίας

με τη βοηθητική χρήση ειδικής σήμανσης στο μηχάνημα σε γραφή Braille. Ακόμη, προσφέρεται η δυνατότητα πλοήγησης στις υπηρεσίες με την φωνητική υποστήριξη. Στα άτομα με προβλήματα ακοής παρέχονται οθόνες αφής και οι συναλλαγές γίνονται με εκπαιδευμένους στη νοηματική γλώσσα. Τέλος, στα άτομα με κινητικά προβλήματα η εξυπηρέτηση γίνεται με την υπηρεσία του Ταμία από Απόσταση.

1.8.1.3 e-Statements

Με την εν λόγω υπηρεσία ο πελάτης μπορεί να ελέγξει όλους τους ηλεκτρονικούς λογαριασμούς του όπου και αν βρίσκεται, να τους εκτυπώσει και να τους αποθηκεύσει με ασφάλεια, με αποτέλεσμα να δημιουργείται μια επιπρόσθετη ευκολία στην οργάνωση του πελάτη. Τα ηλεκτρονικά αρχεία που διαθέτει η εφαρμογή δεν μπορούν να παραπέσουν ή να χαθούν, διότι μόνο ο πελάτης έχει πρόσβαση σε αυτά. Ακόμη και αν χαθεί κάποιο αρχείο, μπορεί εύκολα να ανακτηθεί, εφόσον η εφαρμογή κρατάει τα αρχεία των πελατών για ένα χρονικό διάστημα δύο ετών. Επιπλέον, εξίσου σημαντικό πλεονέκτημα είναι ότι με την αντικατάσταση των φυσικών με ηλεκτρονικών αντιγράφων προστατεύει σε μεγάλο βαθμό το περιβάλλον. Ασφαλώς, επιτυγχάνεται μεγάλη εξοικονόμηση χαρτιού, εφόσον η διαδικασία γίνεται ηλεκτρονικά και περιορίζονται οι περιβαλλοντολογικές επιπτώσεις.

1.8.1.4 Garmin Pay

Το Garmin Pay είναι ένας καινούριος τρόπος υλοποίησης ανέπαφων συναλλαγών με την χρήση της κάρτας σε τερματικά POS και με την χρήση των smartwatches. Όλες οι συναλλαγές πραγματοποιούνται με μεγάλη ασφάλεια, διότι ο πελάτης λαμβάνει έναν μοναδικό ψηφιακό αριθμό, ο οποίος δεν αποθηκεύεται στην συσκευή και δεν κοινοποιείται. Ιδιαίτερης σημασίας αποτελεί το γεγονός ότι ο πελάτης μπορεί να πραγματοποιήσει πληρωμές και αγορές με Garmin Pay ακόμη κι αν εκείνη την στιγμή δεν είναι συνδεδεμένος στο διαδίκτυο ή ακόμη κι αν δεν έχει κοντά το κινητό. Η έκβαση της πληρωμής θα εμφανισθεί στο τερματικό POS καθώς και στην απόδειξη που θα εκδοθεί. Τέλος, σε περίπτωση

που το ρολόι χαθεί ή κλαπεί, ο πελάτης μπορεί να διαγράψει την κάρτα από την εφαρμογή Garmin Connect, διότι αυτές οι επιλογές είναι διαθέσιμες στο μενού το Garmin Pay και μπορούν να επιλεγούν χωρίς να είναι συνδεδεμένο το ρολόι.

1.8.1.5 e-loan on-line δάνειο

Η Τράπεζα Πειραιώς παραμένει σταθερά προσανατολισμένη στην στρατηγική κατεύθυνση του ψηφιακού μετασχηματισμού, με γνώμονα τη συνεχή βελτίωση των προϊόντων και υπηρεσιών που παρέχει στο κοινό. Πρωτοπόρος σε θέματα τεχνολογίας και ψηφιακών υπηρεσιών, η Τράπεζα Πειραιώς προσέφερε πρώτη στην ελληνική αγορά το 2018, το e-loan on-line, ένα μοναδικό, καινοτόμο και σύγχρονο προϊόν, με σκοπό την ηλεκτρονική χορήγηση καταναλωτικών δανείων στους πελάτες. Ο πελάτης με εύκολες και συνοπτικές διαδικασίες μπορεί να αιτηθεί ηλεκτρονικά για να λάβει ένα καταναλωτικό δάνειο, υπογράφοντας ψηφιακά τη σύμβαση και εκταμιεύοντας το δάνειο που επιθυμεί από τον χώρο του χωρίς την φυσική παρουσία σε κάποιο κατάστημα της τράπεζας. (https://www.pireausbank.gr/).

1.9. Για τις επιχειρήσεις: easypay POINT

Αναντίρρητα, η Τράπεζα Πειραιώς έχει δημιουργήσει καινοτόμες και πρωτοποριακές λύσεις στην ελληνική αγορά με απώτερο στόχο να αυξήσει την επισκεψιμότητα των πελατών, τον ανταγωνισμό συγκριτικά με τις υπόλοιπες τράπεζες αλλά και να ενισχύσει την κερδοφορία της. Έτσι, μέσω της υπηρεσίας easypay POINT οι επιχειρήσεις και οι επαγγελματίες μπορούν να εξοφλούν λογαριασμούς διαφόρων οργανισμών και εταιριών, όπως ρεύμα, συνδρομητική τηλεόραση, φυσικό αέριο. με τη χρήση χρεωστικής, πιστωτικής ή prepaid κάρτας. Η δρομολόγηση και η ολοκλήρωση των συναλλαγών πραγματοποιείται μέσω του τεχνολογικού εξοπλισμού epay POS της Τράπεζας Πειραιώς, εξοπλισμένης με αναγνώστη γραμμάτων κωδικών (barcode reader) για να επιτυγχάνεται η απευθείας επικοινωνία με τα κεντρικά συστήματα της Τράπεζας. Με αυτό τον τρόπο η πληρωμή

γίνεται σε πραγματικό χρόνο εύκολα και γρήγορα και το αποδεικτικό της εξόφλησης παραδίνεται την ίδια στιγμή στον πληρωτή.

1.9.1 Εξ αποστάσεως εξυπηρέτηση με βιντεοκλήση

Η Τράπεζα Πειραιώς έχοντας ως προτεραιότητα την καλύτερη δυνατή εξυπηρέτηση των πελατών δημιούργησε έναν νέο τρόπο επικοινωνίας για την απόκτηση τραπεζικών προϊόντων. Η εξ' αποστάσεως εξυπηρέτηση εξοικονομεί πολύτιμο χρόνο από τους επαγγελματίες, οι οποίοι μπορούν να κάνουν τις τραπεζικές εργασίες με μία μόνο κλήση, σαν να βρίσκονται στο φυσικό κατάστημα. Το μόνο που απαιτείται είναι να έχουν ενεργούς κωδικούς στην υπηρεσία ηλεκτρονικής τραπεζικής winbank, καθώς και να υπάρχει εγκατεστημένη η εφαρμογή Microsoft Teams στο κινητό ή στον υπολογιστή. Έτσι, με ένα κλικ ο επιχειρηματικός συνεργάτης θα εμφανιστεί στην οθόνη του κινητού ή του υπολογιστή και θα ολοκληρώσει εύκολα, γρήγορα και με μεγάλη ασφάλεια τις απαραίτητες διαδικασίες για την απόκτηση κάποιου προϊόντος που επιθυμεί ο επαγγελματίας ή για την εκπλήρωση κάποιας συναλλαγής.

1.9.2 Διαχείριση χαρτοφυλακίου μέσω winbank

Μέσω της εφαρμογής winbank web banking μπορεί ο κάτοχος μιας επιχείρησης να διαχειρίζεται όλο το χαρτοφυλάκιο αποτελεσματικά είτε από τον υπολογιστή είτε από το κινητό. Ενδεικτικά, θα παραταθούν ορισμένα πλεονεκτήματα από την χρήση της συγκεκριμένης εφαρμογής:

- Ρευστά διαθέσιμα: ο επιχειρηματίας μπορεί να κάνει μεταφορά εμβασμάτων στο εσωτερικό, να δει αναλυτικά τα στοιχεία για κάθε λογαριασμό αλλά και να πραγματοποιήσει μαζικές πληρωμές υπαλλήλων.
- Επενδυτικό χαρτοφυλάκιο: μπορεί να ενημερωθεί για τις τιμές που επικρατούν στις διεθνείς αγορές σε πραγματικό χρόνο αλλά και να αποτιμήσει το χαρτοφυλάκιό του online

- Δάνεια: μπορεί να παρακολουθήσει αναλυτικά τα στοιχεία για το τρέχον δάνειο που ενδεχομένως έχει λάβει, να πληρώσει τις δόσεις αλλά και να δει το ιστορικό πληρωμών.

Επιλέγοντας να διαχειρίζεται κανείς το χαρτοφυλάκιο και τα διαθέσιμα της επιχείρησης μέσω της συγκεκριμένης εφαρμογής βοηθάει στην προστασία του περιβάλλοντος, διότι εξοικονομείται χαρτί και μειώνεται η κατανάλωση του ηλεκτρικού ρεύματος. Ακόμη, εντάσσοντας την ηλεκτρονική τραπεζική στην καθημερινότητα της επιχείρησης, εξοικονομείται χρόνος από την άσκοπη παραμονή στο φυσικό κατάστημα και αυξάνεται η προστασία του περιβάλλοντος. Καταλήγοντας, είναι αντιληπτό ότι οι τράπεζες προσπαθούν να προοδεύουν σταδιακά και να γίνονται ολοένα και περισσότερο φιλικές προς το περιβάλλον, αξιοποιώντας τις νέες τεχνολογίες που απλοποιούν και βελτιώνουν συνεχώς την ταχύτητα στις καθημερινές συναλλαγές, παρέχοντας, παράλληλα, μεγάλη ασφάλεια για τον χρήστη.

1.9.3 epay One-Click-Pay

Η υπηρεσία epay One-Click-Pay έχει αναπτυχθεί εξ’ ολοκλήρου από την Τράπεζα Πειραιώς κατόπιν μελέτης της παγκόσμιας αγοράς και των αναγκών των πελατών. Η συγκεκριμένη πλατφόρμα επιτρέπει σε μια επιχείρηση που δραστηριοποιείται στον χώρο του ηλεκτρονικού εμπορίου να προσφέρει στους πελάτες την δυνατότητα ολοκλήρωσης μιας αγοράς με ένα μόνο κλικ. Επιπλέον, είναι ιδανική για επιχειρήσεις που δέχονται επαναλαμβανόμενες πληρωμές από του πελάτες. Με την πρώτη συναλλαγή του πελάτη δημιουργείται στο ηλεκτρονικό κατάστημα της επιχείρησης ένας μοναδικός αριθμός που ονομάζεται token και η επιχείρηση αποθηκεύει αυτό τον αριθμό αντί των ευαίσθητων στοιχείων που εμπεριέχει η κάρτα πληρωμής. Ο αριθμός token είναι μοναδικός και δεν μπορεί να χρησιμοποιηθεί για συναλλαγές σε άλλο ηλεκτρονικό κατάστημα ακόμη και αν κλαπεί. Έτσι, όταν ο πελάτης κάνει μια νέα συναλλαγή δεν θα χρειαστεί να καταχωρήσει εκ νέου την κάρτα του.

ΚΕΦΑΛΑΙΟ 2: ΣΥΓΧΡΟΝΟΙ ΜΕΘΟΔΟΙ ΣΥΝΑΛΛΑΓΩΝ

Στην παρούσα ενότητα του κεφαλαίου, θα αναλυθούν διεξοδικά οι σύγχρονοι μέθοδοι συναλλαγών, όπως η τεχνολογία soundwave, η τεχνολογία NFC και ορισμένα βιομετρικά δεδομένα, δηλαδή η σάρωση αμφιβληστροειδούς, η σάρωση ίριδας, το δακτυλικό αποτύπωμα καθώς και τα συστήματα αναγνώρισης προσώπου και αυτιών. Η τεχνολογία NFC και το δακτυλικό αποτύπωμα είναι αρκετά γνώριμα και χρησιμοποιούνται σχεδόν καθημερινά από τους χρήστες. Οι υπόλοιπες μορφές αν και δεν είναι τόσο γνώριμες και συνηθισμένες, παρουσιάζουν ένα ιδιαίτερο ενδιαφέρον μιας και είναι πολύ σύγχρονες και πρωτοποριακές.

2.1. Τεχνολογία Soundwave

Η τεχνολογία Soundwave είναι μια μορφή ψηφιακής πληρωμής που αξιοποιεί το μέσο του ήχου για τη διενέργεια συναλλαγών (Kumar, 2019). Τα μηχανήματα ηλεκτρονικής καταγραφής δεδομένων που πωλούνται, έχουν την ιδιότητα να συλλέγουν και να μεταδίδουν ηχητικά κύματα. Ουσιαστικά, η τεχνολογία ηχητικών κυμάτων είναι ο δίαυλος επικοινωνίας μεταξύ του πελάτη και του εμπόρου. Στην συγκεκριμένη τεχνολογία, η συσκευή πληρωμών του προμηθευτή μεταφέρει ασφαλή και κρυπτογραφημένα δεδομένα μέσω ενός μοναδικού ηχητικού κύματος, όπου το τηλέφωνο του πελάτη τα λαμβάνει και τα μετατρέπει σε ανάλογα σήματα ώστε να εκπληρωθεί η διαδικασία της συναλλαγής (Kumar, 2019). Μια τέτοια πρωτοποριακή τεχνολογία ενδεχομένως να καταφέρει να επωφελήσει τόσο τους πελάτες όσο και τους προμηθευτές, εφόσον δεν είναι απαραίτητη η κατασκευή μιας φυσικής υποδομής για να πραγματοποιηθούν οι συναλλαγές, με αποτέλεσμα το κόστος να είναι μηδενικό.

Το μεγαλύτερο και ίσως σημαντικότερο πλεονέκτημα της τεχνολογίας ηχητικών κυμάτων είναι το γεγονός ότι μπορεί να συμβάλει στην οικονομική ανάπτυξη μιας χώρας. Αυτό οφείλεται στο ότι η ευκολία πρόσβασης στις ψηφιακές συναλλαγές που προσφέρει αυτή η τεχνολογία μπορεί να εξυπηρετήσει ακόμη και τις πιο απομονωμένες και απομακρυσμένες περιοχές μιας κοινωνίας, διότι το ανύπαρκτο κόστος της για το κοινό και για τις εταιρίες θα δημιουργήσει ένα μοντέλο ζήτησης

και προσφοράς στην αγορά, προκαλώντας νέες ευκαιρίες ανάπτυξης (Kumar, 2019). Ακόμη, δεδομένου ότι προσφέρει καλύτερη διαθεσιμότητα και οικονομική αποδοτικότητα, πολλοί πιστεύουν ότι θα επιφέρει ανατρεπτικές αλλαγές στην μείωση της απάτης στον χώρο των ψηφιακών συναλλαγών (Sinha,2022).

2.2. Τεχνολογία NFC

Η επικοινωνία κοντινού πεδίου Near Field Communication (NFC) είναι μια τεχνολογία επικοινωνίας χωρίς επαφή και έχει αναπτυχθεί ραγδαία τα τελευταία χρόνια. Χρησιμοποιείται σε διάφορες εφαρμογές, όπως στις ηλεκτρονικές πληρωμές, στην έκδοση εισιτηρίων, στις ηλεκτρονικές επαγγελματικές κάρτες και η επικοινωνία δεδομένων μεταξύ δύο συσκευών NFC πρέπει να γίνεται σε μικρή απόσταση, τουλάχιστον δέκα εκατοστών (Chabbi et al., 2022). Αυτή η μικρή απόσταση μετάδοσης έχει επιλεγεί για να επιτρέπει στον χρήστη να ανταλλάσσει δεδομένα με μια απλή χειρονομία, προκειμένου να εκτελέσει μια ανέπαφη υπηρεσία με ευκολία και με χαμηλό κόστος (Malik & Annuar, 2021). Πράγματι, οι εφαρμογές NFC έχουν γίνει πολύ δημοφιλείς και περιζήτητες τα τελευταία χρόνια, ιδίως με την εμφάνιση συσκευών κινητής τηλεφωνίας. Η τεχνολογία NFC λειτουργεί σε συχνότητα 13,56 MHz με ρυθμούς μεταφοράς 106, 212 και 424 kbits ανά δευτερόλεπτο και η συσκευή που ξεκινάει την επικοινωνία ονομάζεται εκκινητής, ενώ η συσκευή που ανταποκρίνεται ονομάζεται στόχος (Chabbi et al., 2022). Για να προκληθεί επικοινωνία ραδιοσυχνοτήτων μεταξύ των συσκευών εκπομπής και λήψης χρησιμοποιούνται κεραίες και κυκλώματα επαγωγικής και μαγνητικής σύζευξης αλλά και τεχνικές κωδικοποίησης. Σε αυτό το σημείο είναι σημαντικό να αναφερθεί ότι υπάρχουν τρεις τρόποι λειτουργίας της τεχνολογίας NFC και είναι οι εξής;

- Λειτουργία ανάγνωσης και εγγραφής, όπου στην λειτουργία ανάγνωσης η συσκευή NFC λειτουργεί ως εκκινητής και διαβάζει πληροφορίες από την ετικέτα που περιέχει τις πληροφορίες. Στην λειτουργία εγγραφής, η συσκευή εγγράφει νέες πληροφορίες στην ετικέτα NFC, με αποτέλεσμα τα παλαιότερα δεδομένα που υπάρχουν να διαγράφονται (Tafti et al., 2021).
- Λειτουργία εξομείωσης κάρτα, όπου η κινητή συσκευή NFC λειτουργεί ως έξυπνη κάρτα. Όταν η συγκεκριμένη συσκευή βρίσκεται κοντά στον αναγνώστη, ο αναγνώστης ξεκινάει την μεταφορά δεδομένων. Χαρακτηριστικά παραδείγματα είναι οι κινητές πληρωμές, τα εισιτήρια και οι υπηρεσίες ταυτότητας (Tafti et al., 2021).
- Λειτουργία ομότιμου δικτύου, όπου οι συσκευές NFC επικοινωνούν για να ανταλλάξουν δεδομένα. Η σύνδεση μεταξύ των δύο συσκευών θεωρείται αμφίδρομη και μόνο ένα άτομο μπορεί να στέλνει δεδομένα κάθε φορά (Tafti et al., 2021).

Πολλές φορές, η χρήση και η εφαρμογή της εν λόγω τεχνολογίας απαιτεί την επεξεργασία σημαντικών προσωπικών δεδομένων του χρήστη.. Γι' αυτό τον λόγο, είναι πολύ σημαντικό να υπάρχει ο κατάλληλος εξοπλισμός των συστημάτων με τεχνικές και πρωτόκολλα, τα οποία αυξάνουν το επίπεδο ασφάλειας των προσωπικών στοιχείων των ατόμων. Επίσης, οι πολιτικές ασφαλείας οφείλουν να προστατεύουν όχι μόνο τα δεδομένα που είναι αποθηκευμένα σε μια συσκευή, αλλά ακόμη και όταν πρόκειται να μεταφερθούν σε μια άλλη συσκευή NFC. Ένα πολύ σύνηθες φαινόμενο είναι οι εισβολείς να υποκλέπτουν εξ' αποστάσεως τα τραπεζικά δεδομένα του πελάτη, που μπορεί να είναι αποθηκευμένα σε μια τραπεζική κάρτα NFC ή σε ένα κινητό τηλέφωνο NFC και φυσικά, χωρίς τη γνώση του, βλάπτοντας έτσι τον πελάτη. Ως επακόλουθο, η χρήση της τεχνολογίας NFC είναι πιθανόν να θέσει σε κίνδυνο την ασφάλεια των συναλλαγών από κακόβουλα λογισμικά που χρησιμοποιούν οι εισβολείς, προκειμένου να αποσπάσουν τα δεδομένα που επιθυμούν.

2.3. Βιομετρικά χαρακτηριστικά

Τα τελευταία χρόνια, έχει παρατηρηθεί ότι η εξέλιξη της τεχνολογίας φέρνει νέα δεδομένα στις τραπεζικές συναλλαγές με αποτέλεσμα να αυξηθεί η ασφάλεια των συναλλαγών. Οι τεχνολογίες αυτές επεξεργάζονται βιομετρικά δεδομένα, όπως είναι η αναγνώριση προσώπου, η αναγνώριση αυτιών, η γεωμετρία της παλάμης, η αναγνώριση φωνής, η εξακρίβωση δακτυλικού αποτυπώματος, η σάρωση της ίριδας του ματιού και η σάρωση αμφιβληστροειδούς. Οι συγκεκριμένες τεχνολογίες είναι αρκετά γνώριμες και οι άνθρωποι είναι εξοικειωμένοι, διότι αρκετές από αυτές χρησιμοποιούνται ήδη (Burt, 2021). Παρακάτω, θα αναλυθούν ορισμένες περιπτώσεις βιομετρικής τεχνολογίας.

2.3.1 Σάρωση αμφιβληστροειδούς

Ο αμφιβληστροειδής είναι ένα λεπτό στρώμα κυττάρων στο πίσω μέρος του ματιού που αποτελείται από ένα περίπλοκο δίκτυο αιμοφόρων αγγείων που είναι μοναδικό για κάθε άτομο. Ανακαλύφθηκε και μελετήθηκε για πρώτη φορά το 1981 η σάρωση του αμφιβληστροειδούς και μέχρι σήμερα, θεωρείται από τις πιο διάσημες βιομετρικές τεχνολογίες αλλά από τις λιγότερο χρησιμοποιούμενες (Boldea et al.,

2022). Όταν σαρώνεται ο αμφιβληστροειδής, χαρτογραφείται το μοτίβο των αιμοφόρων αγγείων στο εσωτερικό του ματιού. Τα αιμοφόρα αγγεία αναγνωρίζονται εύκολα συγκριτικά με άλλους ιστούς, επειδή προσελκύουν περισσότερο φως. Η σάρωση πραγματοποιείται με τη ρίψη μιας αόρατης δέσμης υπέρυθρων λέιζερ στο μάτι ενός ατόμου και η δέσμη φωτός στη συνέχεια, ανιχνεύει μια τυποποιημένη διαδρομή στον αμφιβληστροειδή (Boldea et al., 2022). Μετά τη λήψη της εικόνας από τον σαρωτή, το λογισμικό εκτελεί όλες τις διαδικασίες που απαιτούνται για την ανάλυση του μοτίβου των αιμοφόρων αγγείων και τη μετατροπή σε ένα μοναδικό πρότυπο. Ο σαρωτής αμφιβληστροειδούς απαιτεί εικόνες υψηλής ανάλυσης, ώστε να μπορέσει να επεξεργαστεί το δίκτυο των αιμοφόρων κυττάρων από το μάτι ενός ατόμου. Επειδή το δίκτυο των αιμοφόρων αγγείων του αμφιβληστροειδούς είναι πιο απορροφητικό στο υπέρυθρο φως από το υπόλοιπο μάτι, η ποσότητα αντανάκλασης μεταβάλλεται κατά τη διαδικασία της σάρωσης, μετατρέπεται σε κώδικα υπολογιστή και μεταφέρεται σε μια βάση δεδομένων (Boldea et al., 2022).

Δυστυχώς, ο αμφιβληστροειδής δεν παραμένει αμετάβλητος. Οι περισσότερες αλλαγές κατά τη διάρκεια της ζωής ενός ατόμου προκαλούνται από ασθένειες, όπως ο διαβήτης και το γλαύκωμα (Boldea et al., 2022). Έτσι, αν κάποιο άτομο βασίζεται αυστηρά σε αυτή την μέθοδο πληρωμής και ο αμφιβληστροειδής έχει μολυνθεί ή έχει μεταβληθεί λόγω κάποιας ασθένειας, δεν θα μπορέσει να πραγματοποιήσει την πληρωμή. Επιπρόσθετα, η δυσκολία λήψης και απόκτησης εικόνας θεωρείται ένα από τα πιο σημαντικά μειονεκτήματα λόγω του ότι η διαδικασία εγγραφής με σάρωση αμφιβληστροειδούς διαρκεί πολύ και απαιτείται η λήψη πολλαπλών εικόνων, κάτι που ενδεχομένως να ταλαιπωρήσει αρκετά τον χρήστη. Εξίσου σημαντικό μειονέκτημα είναι το γεγονός ότι ο σαρωτής απαιτεί από το άτομο να εισέλθει πολύ κοντά στην συσκευή και αυτό μπορεί να προκαλέσει ένα επιπρόσθετο άγχος στον χρήστη. Όπως προαναφέρθηκε παραπάνω, επειδή η απαιτούμενη ποιότητα της εικόνας είναι δύσκολο να ληφθεί, μπορεί να ζητηθεί από το άτομο να περάσει την συγκεκριμένη διαδικασία πολλές φορές μέχρι να βγει το σωστό αποτέλεσμα.

Οι τράπεζες προκειμένου να υιοθετήσουν αυτή τη μορφή πληρωμής πρέπει να δαπανήσουν ένα υψηλό χρηματικό ποσό, που ενδεχομένως να μην διαθέτουν. Ακόμη και αν προβούν σε αυτή την ενέργεια, με βάση τα παραπάνω γίνεται αντιληπτό ότι η πληρωμή δεν μπορεί να πραγματοποιηθεί εύκολα, διότι ο αμφιβληστροειδής ενός

ατόμου μεταβάλλεται με την πάροδο του χρόνου και έτσι δεν μπορεί να υπάρξει σε μεγάλο βαθμό αξιοπιστία στις συναλλαγές.

Από την άλλη πλευρά, το βασικό πλεονέκτημα αυτής της εφαρμογής είναι ότι οι προγραμματιστές έχουν καταφέρει να προγραμματίσουν το λογισμικό με τέτοιο τρόπο ώστε να είναι σε θέση να ανιχνεύει σοβαρές ασθένειες για τον οργανισμό ενός ανθρώπου, όπως το AIDS ή η ελονοσία (Boldea et al., 2022).

2.3.2 Σάρωση ίριδας

Η τεχνολογία σάρωσης της ίριδας είναι μια μέθοδος ταυτοποίησης με βάση τα μάτια, που σημαίνει ότι εξαρτάται από μοναδικά φυσιολογικά χαρακτηριστικά του άτομο (Omolara et al., 2019). Για να μπορέσει ο σαρωτής ίριδας να εκτελέσει τις διαδικασίες που απαιτούνται στον υπολογιστή, εκτοξεύει μια δέσμη υπέρυθρου λέιζερ στο εσωτερικό του οφθαλμού και η δέσμη λέιζερ αντανακλάται στον σαρωτή της ίριδας. Οι εικόνες μετατρέπονται σε δυαδικούς κώδικες και αντιπροσωπεύουν την ταυτότητα του κάθε ατόμου (Omorala et al., 2019).

Οι τράπεζες προκειμένου να χρησιμοποιήσουν την τεχνολογία της ίριδας και να μην επιβαρυνθούν με το κόστος υποδομής, μπορούν να κατασκευάσουν μια απλή εφαρμογή που ονομάζεται FingerEye και να λειτουργεί στους υπάρχοντες υπολογιστές που διαθέτουν (Omorala et al., 2019). Έπειτα, η συγκεκριμένη εφαρμογή θα ενσωματωθεί με την ψηφιακή κάμερα της τράπεζας για να είναι σε αυτόματη λειτουργία με σκοπό να συλλέγονται τα στοιχεία των πελατών τους και στη συνέχεια, να γίνεται ο έλεγχος της ταυτότητάς τους. Έτσι, όταν ο πελάτης επιθυμεί να πραγματοποιήσει μια συναλλαγή, πηγαίνει σε κάποιο μηχάνημα ATM και πιστοποιεί την ταυτότητά του κοιτάζοντας απευθείας το μηχάνημα.

Επειδή ο σαρωτής ίριδας λειτουργεί ως φωτογραφική μηχανή υπάρχει η πιθανότητα πολλές διαφορετικές συσκευές σαρωτή ίριδας να ξεγελαστούν από μια ποιοτική φωτογραφία ίριδας ενός ατόμου. Προκειμένου να αποφευχθεί αυτό το σενάριο, τα τελευταία δύο χρόνια οι περισσότεροι σαρωτές ίριδας εφαρμόζουν μια διαφορετική τεχνολογία, όπου μπορεί να ελέγξει αν το μάτι που παρουσιάζεται μπροστά στον σαρωτή είναι πράγματι αληθινό ή αν είναι μια φωτογραφία καλής

ανάλυσης (Boldea et al., 2022). Επιπλέον, αφού ληφθεί η φωτογραφία του οφθαλμού, καταγράφεται για λίγα δευτερόλεπτα και η κίνηση του ματιού.

Αναμφίβολα, λόγω του ότι οι επιθέσεις στον κυβερνοχώρο και η παραβίαση προσωπικών δεδομένων βρίσκονται σε υψηλά επίπεδα, οι βάσεις δεδομένων με ευαίσθητες πληροφορίες συχνά στοχοποιούνται από τους εγκληματίες. Η επίθεση υποκλοπής είναι δυνατή σε ένα σύστημα ελέγχου ταυτότητας που χρησιμοποιεί κωδικούς επαλήθευσης, Στην συγκεκριμένη περίπτωση, επειδή η επαλήθευση γίνεται με την σάρωση της ίριδας η υποκλοπή είναι ανέφικτη. Ακόμη, ο μέσος χρόνος πιστοποίησης της ταυτότητας ενός ατόμου με την χρήση της ίριδας είναι 1,4 δευτερόλεπτα σε σχέση με ένα σύστημα που απαιτεί κωδικούς πρόσβασης και διαρκεί 6,5 δευτερόλεπτα, με αποτέλεσμα λόγω της αυξημένης ταχύτητας, οι συναλλαγές πραγματοποιούνται γρηγορότερα και με μεγάλη ασφάλεια (Omorala et al., 2019).

2.3.3 Δακτυλικό αποτύπωμα

Η αξιόπιστη προσωπική ταυτοποίηση έχει μετατραπεί σε ένα δύσκολο ζήτημα τα τελευταία χρόνια λόγω της αύξησης του εγκλήματος στον κυβερνοχώρο. Η τεράστια χρήση εφαρμογών ηλεκτρονικών τραπεζικών συναλλαγών και ηλεκτρονικού εμπορίου έχει οδηγήσει στην χρήση βιομετρικών συστημάτων για την ασφάλισή τους έναντι επιθέσεων. Ένα βιομετρικό σύστημα, το οποίο χρησιμοποιεί τα φυσιολογικά χαρακτηριστικά ενός ατόμου για την αξιόπιστη ταυτοποίηση είναι το δακτυλικό αποτύπωμα (Maltoni et al., 2009). Τα συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων είναι περιζήτητα τα τελευταία χρόνια λόγω της αξιοπιστίας τους και προτιμώνται παγκοσμίως για την διασφάλιση δεδομένων από χάκερ (Maltoni et al., 2009 & Peralta et al., 2015). Αποτελείται από μοτίβα κορυφογραμμών και κοιλάδων, τα οποία σχηματίζονται από γενετικούς και περιβαλλοντολογικούς παράγοντες (Patil & Ingle., 2021). Οι κορυφογραμμές κάθε δακτύλου είναι μοναδικές και αμετάβλητες για κάθε άτομο κατά τη διάρκεια της ζωής του και επομένως, αυτό το χαρακτηριστικό διευκολύνει την χρήση του για την αναγνώριση. Οι τραυματισμοί και τα εγκαύματα μπορεί να βλάψουν προσωρινά το δακτυλικό αποτύπωμα, αλλά επανέρχεται μόλις επουλωθεί η πληγή.

Τα συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων αποτελούνται από δύο παράγοντες, την επαλήθευση και την ταυτοποίηση. Η επαλήθευση περιλαμβάνει την αντιστοίχιση δύο δακτυλικών αποτυπωμάτων για να διαπιστωθεί αν αντιστοιχούν στο ίδιο δάχτυλο. Στην ταυτοποίηση, ένα δακτυλικό αποτύπωμα εισόδου συγκρίνεται με όλα τα υπόλοιπα δακτυλικά αποτυπώματα σε μια βάση δεδομένων (Peralta et al., 2017). Δύο δακτυλικά αποτυπώματα ονομάζονται γνήσια, όταν αντιπροσωπεύουν το ίδιο δάχτυλο και ψεύτικα, όταν αντιπροσωπεύουν διαφορετικό δάχτυλο.

Ορισμένες πλατφόρμες όπως η Alipay, η WeChat Pay και η Apple Pay έχουν υιοθετήσει τεχνολογίες βιομετρικού ελέγχου ταυτότητας στις υπηρεσίες πληρωμών μέσω κινητών τηλεφώνων (Liu, 2020). Έτσι, ο παραδοσιακός κωδικός πρόσβασης αντικαθίστανται από έναν βιομετρικό κωδικό πρόσβασης, για την επαλήθευση ταυτότητας των πελατών, προσφέροντας μεγαλύτερη ευκολία και ασφάλεια στην συναλλαγή. Ωστόσο, το δακτυλικό αποτύπωμα πρέπει να ληφθεί από μια συσκευή σε κοντινή απόσταση, με αποτέλεσμα να είναι πιο χρονοβόρο σε σχέση με άλλα βιομετρικά χαρακτηριστικά. Καταλήγοντας, παρότι αυτές οι εφαρμογές επιτρέπουν στους χρήστες να στέλνουν και να λαμβάνουν χρήματα εύκολα χωρίς να χρησιμοποιούν μετρητά, ο ρυθμός υιοθέτησης των βιομετρικών χαρακτηριστικών εξακολουθεί να είναι χαμηλός (Paysafe, 2019).

2.3.4 Σύστημα αναγνώρισης προσώπου

Το πρόσωπο είναι ίσως ένα από τα πιο δημοφιλή βιομετρικά χαρακτηριστικά. Έχει ένα ευρύ φάσμα εφαρμογών, από κάμερες ασφαλείας σε αεροδρόμια μέχρι καθημερινές χρήσεις για τον έλεγχο ταυτότητας κινητών τηλεφώνων. Το σύστημα αναγνώρισης προσώπου χρησιμοποιεί αλγορίθμους για την σύλληψη, τη σύγκριση και την εξαγωγή των βιομετρικών χαρακτηριστικών των ατόμων για να επαληθευτεί η προσωπική τους ταυτότητα κατά τη διενέργεια μιας συναλλαγής (Zhang & Hang, 2019). Κατά την πραγματοποίηση μιας αγοράς, ο χρήστης πρέπει να στέκεται ακίνητος και να κοιτάζει την κάμερα μιας συσκευής που εμπεριέχει το σύστημα αναγνώρισης ή ενός smartphone και στη συνέχεια, οι συλλεχθείσες πληροφορίες προσώπου συγκρίνονται με τις πληροφορίες που είναι αποθηκευμένες σε μια βάση

δεδομένων για την επικύρωση της συναλλαγής. Όταν τα δύο σύνολα πληροφοριών ταυτιστούν, η συναλλαγή έχει ολοκληρωθεί.

Πρώτον, το βασικό πλεονέκτημα αυτής της ψηφιακής μεθόδου είναι ότι η διαδικασία επικύρωσης διαρκεί μερικά δευτερόλεπτα (Moriuchi, 2021). Δεύτερον, η διαδικασία είναι εντελώς ανέπαφη. Οι χρήστες δεν χρειάζεται να αγγίξουν τίποτα, παρά μόνο να σταθούν μπροστά στην κάμερα της συσκευής που διαθέτει αυτό το σύστημα, ώστε να σαρώσει τα στοιχεία του προσώπου τους. Τρίτον, είναι μια αρκετά βολική μέθοδος, κυρίως όταν οι χρήστες ξεχνούν τις πιστωτικές τους κάρτες ή όταν τα χέρια τους είναι γεμάτα με άλλα αγορασμένα αγαθά και δεν μπορούν να εισάγουν έναν κωδικό PIN ή να σαρώσουν το δακτυλικό τους αποτύπωμα κατά την πραγματοποίηση άλλης αγοράς (Liu, 2020). Τέλος, με την ραγδαία ανάπτυξη των τρισδιάστατων καμερών και της τεχνητής νοημοσύνης, το σύστημα αναγνώρισης προσώπου θεωρείται ότι είναι αρκετά ασφαλές (Vazquez-Fernandez & Gonzalez-Jimenez, 2016).

Από την άλλη πλευρά, το σύστημα αναγνώρισης προσώπου εξακολουθεί να εγείρει ανησυχίες σχετικά με την αβεβαιότητα και τους κινδύνους ως προς τους χρήστες, ιδίως όσον αφορά την προστασία της ιδιωτικής ζωής και την ασφάλεια, διότι μπορεί να παραβιαστεί. Η παραποίηση φωτογραφιών και βίντεο και η μορφοποίηση είναι οι βασικές τεχνικές που χρησιμοποιούν οι χάκερς πλαστοπροσωπίας (Cho & Jeong, 2017, Li et al., 2018, Ryu et al., 2021, Yeung et al., 2020), προκειμένου να παραβιάσουν το συγκεκριμένο σύστημα και να προκαλέσουν προβλήματα στους χρήστες. Οι χάκερς μπορούν εύκολα να αποκτήσουν φωτογραφίες ή βίντεο από τα μέσα κοινωνικής δικτύωσης και να τα παρουσιάσουν σε ένα σύστημα αναγνώρισης προσώπου (Cho & Jeong, 2017).

Παρόλο που τα τρέχοντα συστήματα έχουν υιοθετήσει αλγορίθμους ενίσχυσης της ιδιωτικότητας για την αντιμετώπιση των παραβιάσεων, η μορφοποίηση εξακολουθεί να είναι μια σημαντική πρόκληση παραποίησης (Li et al., 2018, Yeung et al., 2020). Ακόμη, οι πληροφορίες προσώπου που συλλέγονται από τα συστήματα αναγνώρισης προσώπου είναι υψηλής ποιότητας για την διασφάλιση της ακρίβειας. Όμως, τα συλλεχθέντα δεδομένα μπορούν να χρησιμοποιηθούν για τον εντοπισμό και την παρακολούθηση ατόμων σε δημόσιους χώρους εκτός του συστήματος ανίχνευσης προσώπου (Yeung et al., 2020). Εξαιτίας αυτών των προβλημάτων αυξάνεται η

αίσθηση της ευπάθειας των χρηστών, γεγονός που μπορεί να μειώσει την εμπιστοσύνη σε αυτή την τεχνολογία πληρωμών.

2.3.5 Σύστημα αναγνώρισης αυτιών

Τα τελευταία χρόνια το αυτί έχει προκαλέσει σημαντικό ενδιαφέρον στην βιομετρική ταυτότητα λόγω των εγγενών χαρακτηριστικών του. Σε αντίθεση με άλλα σημεία του προσώπου, το αυτί δεν επηρεάζεται από τις εκφράσεις, τα συναισθήματα και παραμένει αμετάβλητο (Kamboj et al., 2021). Με βάση αυτό και εξαιτίας της μοναδικής δομής του σχήματος που διαθέτουν, μπορούν να κατασκευαστούν αξιόπιστα συστήματα αναγνώρισης σε διάφορες συσκευές. Επίσης, το σύστημα αναγνώρισης αυτιών μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, όπως στην εγκληματολογία, στον έλεγχο ταυτότητας, στο ξεκλείδωμα συσκευών του χρήση και σε άλλα (Alshazly et al., 2020). Ακόμη, έχουν γίνει πολλές προσπάθειες για την ανάπτυξη ενός αξιόπιστου συστήματος αναγνώρισης αυτιών. Οι κλασικές μέθοδοι που χρησιμοποιούνται για την αναγνώριση αυτιών είναι οι εξής:

- Γεωμετρικές, οι οποίες προσπαθούν να εξάγουν το σχήμα του αυτιού (Hansley et al. 2018, Khaldi & Benzaoui, 2020)
- Ολιστικές, οι οποίες εξάγουν τα χαρακτηριστικά από την εικόνα του αυτιού (Hansley et al. 2018, Khaldi & Benzaoui, 2020)
- Τοπικές, οι οποίες χρησιμοποιούν συγκεκριμένα ένα τμήμα της εικόνας
- Υβριδικές, στις οποίες γίνεται ένας συνδυασμός των παραπάνω μεθόδων (Dodge et al. 2018, Alshazly et al. 2019, Omara et al 2021).

Η αναγνώριση αυτιών είναι ένα πιο πρόσφατο βιομετρικό χαρακτηριστικό που διερευνούν οι επιστήμονες συγκριτικά με τα υπόλοιπα που αναφέρθηκαν παραπάνω και το έργο του παρόντος συστήματος αναγνώρισης αναμένεται να αυξηθεί μελλοντικά. Ωστόσο, για να καταφέρουν να εντάξουν οι τράπεζες το συγκεκριμένο σύστημα πληρωμής αφενός θα χρειαστούν μεγάλα χρηματικά ποσά και αφετέρου, υπάρχει τεράστια πιθανότητα να δυσκολέψει αρκετά τους χρήστες και ιδίως τους ηλικιωμένους μιας και δεν είναι αρκετά έως καθόλου εξοικειωμένοι με τα συστήματα.

Παρ’ όλα αυτά, δεν μπορεί να παραλειφθεί το γεγονός ότι προσφέρει αρκετά μεγάλη αξιοπιστία. Οι πελάτες μπορούν αντί να χρησιμοποιούν έναν προσωπικό κωδικό για να εκπληρώσουν μια συναλλαγή, να πλησιάσουν το ATM και με την υβριδική ή ολιστική μέθοδο που αναφέρθηκε παραπάνω να εκτελεσθεί η πληρωμή. Πιο συγκεκριμένα, μέσω ξεχωριστών συστημάτων που θα τοποθετήσουν οι τράπεζες στα καταστήματα, θα εξάγεται το σχήμα του αυτιού από ειδικές κάμερες κι έτσι θα καταφέρνουν οι χρήστες να διεκπεραιώνουν τις συναλλαγές τους. Επίσης, η διαδικασία είναι ανέπαφη και ολοκληρώνεται σε λίγα μόνο δευτερόλεπτα, γλιτώνοντας τους πολύτιμο χρόνο. Με τις συχνές επιθέσεις που γίνονται στα συστήματα τραπεζών, αυτή η μορφή συναλλαγής θα βοηθούσε σημαντικά στην μείωση της υποκλοπής χρηματικών ποσών από τους χάκερ.

ΚΕΦΑΛΑΙΟ 3: ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Συχνά γίνεται λόγος για τα προσωπικά δεδομένα και για το γεγονός ότι τα υποκείμενα πρέπει να πολύ προσεκτικά όταν τους ζητείται να συναινέσουν στην παραχώρηση των προσωπικών δεδομένων για την διενέργεια μις πράξης. Στην παρούσα ενότητα, θα διευκρινιστούν οι αρχές νομιμότητας της επεξεργασίας, οι προϋποθέσεις νόμιμης επεξεργασίας, θα δοθούν παραδείγματα επεξεργασίας προσωπικών δεδομένων και τέλος, θα παραταθούν διάφορα μέτρα που οφείλουν να λάβουν τα υποκείμενα για να μην είναι εκτεθειμένα σε πιθανούς κινδύνους και να προστατευθούν σε μεγάλο βαθμό από τους επιτήδειους.

3.1. Αρχές νομιμότητας επεξεργασίας

Σύμφωνα με το άρθρο 5 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), για να είναι επιτρεπτή και δίκαιη η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να καθορίζεται από ορισμένες αρχές και αξίες που είναι οι εξής (www.dpa.gr) :

- Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας, όπου τα δεδομένα πρέπει να υποβάλλονται σε νομότυπη επεξεργασία, με διαφανή τρόπο συγκριτικά με το υποκείμενο των δεδομένων. Η ενημέρωση του υποκειμένου πρέπει να είναι συνοπτική και κατανοητή. Για παράδειγμα, οι τράπεζες οφείλουν να ενημερώσουν τον πελάτη όταν προχωρούν στην επεξεργασία προσωπικών δεδομένων από τις πιστωτικές και χρεωστικές τους κάρτες.
- Η αρχή του περιορισμού του σκοπού, όπου τα δεδομένα πρέπει να συλλέγονται για νόμιμους σκοπούς και να μην υποβάλλονται σε επιπρόσθετη επεξεργασία. Για παράδειγμα, λήψη στοιχείων ταυτότητας ή διαβατηρίου για το άνοιγμα ενός τραπεζικού λογαριασμού.
- Η αρχή της αναλογικότητας, σύμφωνα με την οποία τα δεδομένα πρέπει να έχουν συνοχή για τους επιδιωκόμενους λόγους επεξεργασίας, όπως δεδομένα που κρατούν νοσοκομεία ή γιατροί για λόγους υγείας.

- Η αρχή της ακρίβειας των δεδομένων, με βάση την οποία πρέπει να υπάρχει ακρίβεια των δεδομένων και σε περίπτωση ανακρίβειας να εκλαμβάνονται άμεσα τα ορθά μέτρα και οι κανόνες για την διόρθωσή τους. Για παράδειγμα, η ακριβής διεύθυνση του υποκειμένου για την αποστολή τραπεζικών εγγράφων.
- Η αρχή του καθορισμού της χρονικής διάρκειας της επεξεργασίας, όπου τα δεδομένα πρέπει να τηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων. Οι τράπεζες, κατά τη διάρκεια χορήγησης ενός επενδυτικού προϊόντος κρατούν προσωπικά στοιχεία του πελάτη, όπως ταυτότητα, ΑΦΜ, κινητό τηλέφωνο και διεύθυνση. Όταν πωληθεί το επενδυτικό προϊόν, οι τράπεζες διαγράφουν τα στοιχεία του πελάτη που είχαν διατηρήσει.
- Η αρχή της ακεραιότητας και εμπιστευτικότητας, με την οποία τα δεδομένα χρειάζεται να επεξεργάζονται με ασφαλές τρόπο και να προστατεύονται από παράνομες επεξεργασίες. Για παράδειγμα λήψη στοιχείων σχετικά με το εισόδημα για την χορήγηση ενός δανείου.
- Η αρχή της λογοδοσίας του υπευθύνου της επεξεργασίας, όπου ο υπεύθυνος επεξεργασίας πρέπει να αποδεικνύει την συμμόρφωσή του με τον ΓΚΠΔ ενώπιων των δικαστηρίων και των αρχών σε περίπτωση που προβεί σε επεξεργασία φυλετικής καταγωγής του υποκείμενου.

3.2. Προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων

Σύμφωνα με το άρθρο 6 του ΓΚΠΔ η επεξεργασία είναι σύννομη μόνο αν ακολουθούνται οι εξής προϋποθέσεις (www.dpa.gr) :

- Το υποκείμενο να έχει δώσει την συγκατάθεσή του για την επεξεργασίας των δεδομένων του. Στην περίπτωση εξόφλησης ενός χρηματικού ποσού στην τράπεζα.
- Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης, όταν συνάπτεται μια εργασιακή σχέση με οποιαδήποτε τράπεζα για ένα εύλογο χρονικό διάστημα.

- Η επεξεργασία είναι απαραίτητη για την εκπλήρωση εκ του νόμου υποχρέωσης του υπευθύνου επεξεργασίας. Οι τράπεζες ορίζουν έναν υπάλληλο ως υπεύθυνο για την επεξεργασία προσωπικών δεδομένων των πελατών όταν είναι απαραίτητο.
- Η επεξεργασία είναι αναγκαία για την άσκηση δημοσίου συμφέροντος. Χαρακτηριστικό παράδειγμα αποτελούν τα βιομετρικά και γενετικά δεδομένα.
- Η επεξεργασία είναι αναγκαία για την άσκηση εννόμου συμφέροντος, όταν κάποιος έχει διαπράξει μια απάτη σε βάρος της τράπεζας.

3.3. Επεξεργασία βιομετρικών δεδομένων

Η συλλογή των βιομετρικών δεδομένων γίνεται κατά την διαδικασία εγγραφής του ατόμου σε διάφορα βιομετρικά συστήματα. Σύμφωνα με τον ΓΚΠΔ, τα βιομετρικά δεδομένα ανήκουν στην ειδική κατηγορία δεδομένων προσωπικού χαρακτήρα και απαγορεύεται αυστηρά η επεξεργασία τους σύμφωνα με το άρθρο 9 παρ. 1. Κατ' εξαίρεση, η επεξεργασία αυτών επιτρέπεται μόνο σε ειδικές περιπτώσεις που καθορίζονται στην παράγραφο 2 του άρθρου 9 (www.dpa.gr). Οι φορείς που δημιουργούν καινοτόμες μεθόδους επεξεργασίας βιομετρικών δεδομένων οφείλουν να είναι ιδιαίτερα προσεκτικοί, διότι η επεξεργασία τους ενδέχεται να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων σύμφωνα με τα άρθρα 35-36 του ΓΚΠΔ (www.dpa.gr). Όσον αφορά την χρήση βιομετρικών συστημάτων για την ταυτοποίηση των εργαζομένων σε μια επιχείρηση, είναι επιτρεπτή μόνο όταν επιβάλλεται από ιδιαίτερες απαιτήσεις ασφαλείας των χωρών εργασίας και εφόσον δεν διατίθεται εναλλακτικό μέσο για την επίτευξη του συγκεκριμένου σκοπού και συγχρόνως, να υπάρχει ειδική διάταξη που να επιτρέπει τη λειτουργία τέτοιων συστημάτων.

Χαρακτηριστικό παράδειγμα αποτελεί η Αρχή με βάση την Απόφαση 57/2022 όπου έκανε παρατήρηση και ζήτησε τον άμεσο παραδειγματισμό της γνωστής εταιρίας κινητής τηλεφωνίας Cosmote, για παραβάσεις της αρχής λογοδοσίας και της αρχής διαφάνειας κατά τη διάρκεια επεξεργασίας βιομετρικών στοιχείων (Απόφαση57/2022). Πιο αναλυτικά, η Αρχή μελέτησε μια διαμαρτυρία ενός

συνδρομητή της κινητής τηλεφωνίας αναφορικά με τον τρόπο της απομακρυσμένης δημιουργίας συμβολαίων με την χρήση της υπηρεσίας digital onboarding, όπου ζητήθηκε ηλεκτρονική ταυτοποίηση με την επεξεργασία βιομετρικών στοιχείων, δηλαδή την αποστολή φωτογραφίας σε εύλογο χρονικό διάστημα. Από την εξέταση της υπόθεσης παρατηρήθηκε ότι υπήρχαν ασάφειες ενημέρωσης προς τον συνδρομητή, οι οποίες αφορούσαν τα βιομετρικά δεδομένα (www.dpa.gr). Έτσι, η Αρχή απηύθυνε επίπληξη στην εταιρία κινητής τηλεφωνίας για τις διαπιστωθείσες ελλείψεις στην ενημέρωση των υποκειμένων (άρθρο 5 παρ. 1 α' και 13 ΓΚΠΔ). Ακόμη, η Αρχή ζήτησε την τροποποίηση του κειμένου με σκοπό την πλήρη συμμόρφωση στην αρχή της διαφάνειας της επεξεργασίας (άρθρο 5 παρ. 1' ΓΚΠΔ).

3.4. Επεξεργασία δεδομένων μέσω χρεωστικών και πιστωτικών καρτών

Η Αρχή εξέτασε, κατόπιν καταγγελιών κατά της Εθνικής Τράπεζας της Ελλάδος το πρόβλημα της επεξεργασίας προσωπικών δεδομένων μέσω ανέπαφων συναλλαγών με χρεωστικές και πιστωτικές κάρτες. Η Αρχή διαπίστωσε ότι σε κάποιες περιπτώσεις πιστωτικών ή χρεωστικών καρτών τύπου Mastercard υπάρχει στο chip της κάρτας αποθηκευμένο το ιστορικό πρόσφατων συναλλαγών που πραγματοποιήθηκαν, οι οποίες μπορούν να αναγνωριστούν ανέπαφα χωρίς να λάβει την σχετική ενημέρωση ο πελάτης. Ο πελάτης δήλωσε ότι δεν επιθυμούσε να έχει κάρτα με δυνατότητα πραγματοποίησης ανέπαφων πληρωμών και ζήτησε είτε να απενεργοποιήσει η τράπεζα την ανέπαφη λειτουργία ή να του χορηγηθεί νέα κάρτα χωρίς το δικαίωμα ανέπαφης συναλλαγής. Δεδομένου ότι η τράπεζα δεν ενημέρωσε τον πελάτη και προχώρησε στην αντικατάσταση πιστωτικών και χρεωστικών καρτών με την δυνατότητα πραγματοποίησης ανέπαφης συναλλαγής, η Αρχή με την Απόφαση 53/2022 επέβαλε πρόστιμο 20.000 ευρώ στην Εθνική Τράπεζα προς συμμόρφωση για την παραβίαση του άρθρου 13 του Κανονισμού (ΕΕ) 2016/679, σύμφωνα με το άρθρο 58 παρ. 2 θ' του ΓΚΠΔ μαζί με το άρθρο 83 παρ. 5 του ΓΚΠΔ (www.dpa.gr).

3.5. Επιβολή προστίμου σε Τράπεζα για παράνομη διαβίβαση και παραβίαση δεδομένων

Η Αρχή μελέτησε την καταγγελία ενός πελάτη της Τράπεζας Πειραιώς, όπου ο καταγγέλλων στράφηκε κατά της τράπεζας εξαιτίας της παράνομης χορήγησης οικονομικών στοιχείων στον αντίδικό του εν αγνοία του. Η τράπεζα κατόπιν εξακρίβωσης της υπόθεσης εντόπισε ότι, λόγω ενός σφάλματος του υπαλλήλου της πράγματι χορήγησε στον αντίδικο του καταγγέλλοντος τα οικονομικά στοιχεία, παρά τις σαφείς οδηγίες που είχαν δοθεί στον υπάλληλο, ότι δεν επιτρέπεται η έκθεση προσωπικών στοιχείων σε τρίτους χωρίς την ύπαρξη σοβαρής αιτίας (www.dpa.gr). ΓΙ' αυτό το λόγο, η Αρχή, σύμφωνα με το άρθρο 5 παρ. 1^{α} παρατήρησε ότι έγινε παραβίαση της αρχής νομιμότητας επεξεργασίας και εμπιστευτικότητας των δεδομένων και με βάση την Απόφαση 4/2023 επιβλήθηκε πρόστιμο 30.000 ευρώ στην τράπεζα προς παραδειγματισμό και αποφυγή τέτοιων σοβαρών και ανεπίτρεπτων λαθών.

3.6. Προσδιορισμός μέτρων ασφάλειας προσωπικών δεδομένων

Για τον προσδιορισμό των κατάλληλων μέτρων ασφάλειας και την αποφυγή κινδύνων για τα υποκείμενα των δεδομένων, οι φορείς οφείλουν να λάβουν υπόψη τις εξελίξεις της τεχνολογίας, το κόστος υλοποίησης των μέτρων ασφάλειας, τους κινδύνους, τα προνόμια και τις ευελιξίες επεξεργασίας των φυσικών προσώπων (www.dpa.gr). Σύμφωνα με το άρθρο 32 του ΓΚΠΔ τα μέτρα που προτείνονται είναι τα εξής:

- Χρήση ψευδωνύμων και Κρυπτογράφηση
- Διασφάλιση Απορρήτου, Ακεραιότητας και Αξιοπιστίας
- Αποκατάσταση Διαθεσιμότητας σε περίπτωση συμβάντος
- Διαρκή αξιολόγηση της αποτελεσματικότητας των μέτρων.

Οι υπεύθυνοι επεξεργασίας οφείλουν να λάβουν υπόψη τα παραπάνω μέτρα και να τα εφαρμόζουν όταν είναι απαραίτητο. Από τα παραπάνω γίνεται σαφές ότι η ασφάλεια στον ΓΚΠΔ εφαρμόζει και τεχνικές προστασίας της ιδιωτικότητας με τη χρήση ψευδωνύμων και κρυπτογράφησης. Ακόμη, αξίζει να αναφερθεί ότι με τον ΓΚΠΔ διατηρείται η υποχρέωση λήψης μέτρων για να εξασφαλίζεται το γεγονός ότι το κάθε φυσικό πρόσωπο που έχει πρόσβαση σε προσωπικά δεδομένα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας (www.dpa.gr). Τέλος, είναι ιδιαίτερα σημαντικό τα υλοποιημένα μέτρα να υποβάλλονται σε περιοδική αναθεώρηση.

3.5.1 Τεχνικά μέτρα ασφάλειας

i. **Έλεγχος πρόσβασης**

- Μηχανισμοί ελέγχου πρόσβασης των χρηστών, ώστε να υπάρχουν ορθά μέτρα που να εξασφαλίζουν την ταυτοποίηση των χρηστών για να μην εισέρχονται μη εξουσιοδοτημένοι χρήστες σε πόρους, αρχεία και ευαίσθητα προσωπικά δεδομένα.
- Διαχείριση συνθηματικών. Για την μέγιστη ασφάλεια τα συνθηματικά δεν θα πρέπει να είναι καταγεγραμμένα σε ηλεκτρονική μορφή, αλλά ακόμη και αν συμβαίνει αυτό πρέπει να είναι σε μη αναγνωρίσιμη μορφή και να μην υπάρχει η δυνατότητα ανάκτησης. Επιπλέον, οι χρήστες οφείλουν να αλλάζουν το συνθηματικό της σε σύντομα χρονικά διαστήματα και να χρησιμοποιούν πολύπλοκους χαρακτήρες.
- Αποτυχημένες προσπάθειες πρόσβασης, όπου θα πρέπει να υπάρχουν κατάλληλα μέτρα τα οποία θα αποτρέπουν την είσοδο σε έναν εξουσιοδοτημένο χρήστη μετά από πολλαπλές προσπάθειες πρόσβασης.
- Αδρανοποίηση υπολογιστή. Για να αποφευχθούν περιπτώσεις πρόσβασης οποιουδήποτε επιτήδειου στα προσωπικά δεδομένα ενός χρήστη, πρέπει να αναπτυχθούν μορφές αυτόματης αποσύνδεσης ή ενεργοποίηση προφύλαξης οθόνης με την χρήση κωδικού (www.dpa.gr).

ii. **Αντίγραφα ασφαλείας**

- Δημιουργία αντιγράφων ασφαλείας, όπου θα υπάρχουν κανόνες που θα αφορούν την επιλογή αρχείων που χρήζουν δημιουργία αντιγράφων ασφαλείας, τη συχνότητα λήψης αντιγράφων, την αποθήκευσή τους και την ορθή ανάκτησή τους όταν απαιτείται(www.dpa.gr).

iii. Σωστή διαμόρφωση ηλεκτρονικών υπολογιστών

- Προστασία από κακόβουλα λογισμικά, με την χρήση προγραμμάτων antivirus και firewall, τα οποία θα διαθέτουν τις πιο πρόσφατες ενημερώσεις.
- Σύνδεση αποσπώμενων μέσων, όπου θα πρέπει να απαγορεύεται ρητά στους χρήστες να εξάγουν δεδομένα με την χρήση αποσπώμενων μέσων εκτός αν κάτι τέτοιο επιτρέπεται από τον Υπεύθυνο Ασφαλείας.
- Υπολογιστές με δυνατότητα πρόσβασης στο διαδίκτυο. Στην συγκεκριμένη περίπτωση δεν πρέπει να αποθηκεύονται ευαίσθητα δεδομένα σε υπολογιστές οι οποίοι έχουν πρόσβαση στο διαδίκτυο εκτός αν κάτι τέτοιο είναι απολύτως αναγκαίο.

iv. Αρχεία καταγραφής (log files)

- Τήρηση και σωστός έλεγχος αρχείων καταγραφής. Για να διασφαλιστεί η ακεραιότητα και η προστασία των αρχείων είναι πολύ σημαντικό να ελέγχονται οι ενέργειες όλων των χρηστών συμπεριλαμβανομένων και των χρηστών των συστημάτων.
- Ειδικές ενέργειες καταγραφής που αφορούν την εκτύπωση αρχείων με προσωπικά δεδομένα, τις προσπάθειες μη εξουσιοδοτημένης πρόσβασης και γενικότερα κάθε ενέργεια η οποία μπορεί να υποδηλώνει κάποια κορφή επίθεσης.
- Διαγραφή αρχείων καταγραφής, όπου δεν θα επιτρέπεται η δυνατότητα διαγραφής αρχείων καταγραφής από ένα άτομο, αλλά κάτι τέτοιο να υφίσταται με την παρουσία δύο ατόμων.

v. Ασφάλεια επικοινωνίας

- Έλεγχος δικτυακών συσκευών, όπου η σύνδεση και η χρήση συσκευών των χρηστών θα πρέπει να ελέγχεται και αν χρειαστεί, να περιορίζεται.
- Απομακρυσμένη πρόσβαση, η οποία πρέπει να καταγράφεται και να πραγματοποιείται υπό τον έλεγχο του υπευθύνου επεξεργασίας. Επίσης, εξίσου σημαντικό είναι το γεγονός ότι οι τεχνολογίες απομακρυσμένης

πρόσβασης πρέπει να χρησιμοποιούνται μόνο από εξουσιοδοτημένα πρόσωπα ιδίως για πολύ ειδικούς σκοπούς.

- Κανάλι επικοινωνίας , ώστε η επικοινωνία μεταξύ υπολογιστών να είναι απολύτως ασφαλής, για παράδειγμα με την χρήση κρυπτογράφησης. Επίσης, κάθε υπηρεσία που θα προσφέρεται στο κοινό είναι αναγκαίο να ακολουθεί ένα κατάλληλο πρωτόκολλο ασφάλειας.
- Περιμετρική ασφάλεια, για τον επαρκή έλεγχο των εσωτερικών δικτύων του υπευθύνου επεξεργασίας από και προς το διαδίκτυο.

vi. Ασφάλεια αποσπώμενων μέσων αποθήκευσης

- Δεδομένης της αυξημένης διαρροής προσωπικών δεδομένων, είναι απαραίτητοι οι ισχυροί και σύγχρονοι αλγόριθμοι κρυπτογράφησης για την καλύτερη αντιμετώπιση του προβλήματος.

vii. Ασφάλεια λογισμικού

- Σχεδιασμός εφαρμογών, ο οποίος πρέπει να εφαρμόζεται σύμφωνα με τη λογική και τις βασικές αρχές προστασίας των δεδομένων (άρθρο 25 ΓΚΠΔ). Ακόμη, οι εφαρμογές πρέπει να τηρούν την αρχή της ελαχιστοποίησης και της ακρίβειας των δεδομένων, ενώ παράλληλα πρέπει να δημιουργηθούν τα απαιτούμενα τεχνικά μέσα ασφάλειας για την προστασία των προσωπικών δεδομένων από οποιαδήποτε μορφή αθέμιτης επεξεργασίας.
- Ασφαλής ανάπτυξη εφαρμογών ώστε να εντοπιστούν εγκαίρως τυχόν ευπάθειες του λογισμικού και να διορθωθούν άμεσα προτού ξεκινήσει η λειτουργική φάση.
- Προστασία λειτουργικών αρχείων και προγραμμάτων λογισμικού από μη εξουσιοδοτημένους χρήστες (www.dpa.gr).

viii. Ορθή διαχείριση αλλαγών

- Κατά την δημιουργία λογισμικού θα πρέπει να χρησιμοποιούνται δοκιμαστικά και όχι πραγματικά δεδομένα προς αποφυγή κινδύνων διαρροής πολλών πληροφοριών. Ωστόσο, ακόμη και αν είναι απολύτως απαραίτητο να χρησιμοποιηθούν τα πραγματικά δεδομένα αυτό μπορεί να γίνει σε ανώνυμη μορφή (www.dpa.gr).

ΚΕΦΑΛΑΙΟ 4: ΕΠΙΘΕΣΕΙΣ ΣΥΝΑΛΛΑΓΩΝ

Έχει διαπιστωθεί ότι τα τελευταία χρόνια οι επιθέσεις στα συστήματα πληρωμών αυξάνονται ολοένα και περισσότερο, με αποτέλεσμα οι επιτήδειοι να καταφέρουν με δόλιους τρόπους να υποκλέπτουν προσωπικά στοιχεία των χρηστών και μεγάλα χρηματικά ποσά. Δεδομένου ότι η ψηφιακή τεχνολογία χρησιμοποιείται από πολλούς ανθρώπους, πολλές φορές λόγω άγνοιας δεν χρησιμοποιούνται σωστά οι μέθοδοι ασφάλειας και προκύπτουν σοβαρά προβλήματα στις συναλλαγές. Γι' αυτό τον λόγο, στην συγκεκριμένη ενότητα του κεφαλαίου θα αναφερθούν αρκετοί τρόποι επιθέσεων στα συστήματα πληρωμών.

4.1. Επιθέσεις σε τραπεζικές κάρτες και σε smartphones NFC

Η τεχνολογία NFC αν και είναι εύκολη στην χρήση της και αρκετά διαδεδομένη τα τελευταία χρόνια, πολλές φορές εγκυμονεί κινδύνους στις συναλλαγές των χρηστών, εξαιτίας των εισβολέων που προσπαθούν να υποκλέψουν τα δεδομένα τους. Οι βασικές επιθέσεις στις τραπεζικές κάρτες και στα smartphones NFC είναι οι εξής:

- Επιθέσεις σχετικές με απώλεια, δανεισμό ή κλοπή, στις οποίες αν ο επιτιθέμενος καταφέρει να ανακτήσει μια τραπεζική κάρτα μέσω της απώλειας, του δανεισμού ή της κλοπής, μπορεί να κάνει μια συναλλαγή NFC, διότι δεν απαιτείται να εισαγάγει προσωπικό αριθμό αναγνώρισης (PIN). Όμως, για ένα smartphone NFC η διαδικασία είναι περίπλοκη, γιατί ο επιτιθέμενος χρειάζεται έναν κωδικό πρόσβασης για να αποκτήσει τα δεδομένα και να πραγματοποιήσει την συναλλαγή που επιθυμεί (Affia et al., 2022).
- Επιθέσεις Brute Force, όπου ένας εισβολέας μπορεί να ανακαλύψει τον κωδικό πρόσβασης του χρήστη, δοκιμάζοντας όλους τους πιθανούς συνδυασμούς γραμμάτων ή αριθμών που μπορεί να σκεφτεί. Προκειμένου ένας εισβολέας να καταφέρει να βρει τον κωδικό πρόσβασης ενός smartphone NFC, αρχικά συλλέγει βασικές προσωπικές πληροφορίες του χρήστη, όπως ονοματεπώνυμο, κινητό τηλέφωνο και έπειτα δοκιμάζει τυχαίους κωδικούς βάσει των πληροφοριών που έχει συλλέξει. Παρομοίως, ο επιτιθέμενος για να

μπορέσει να βρει τον κωδικό μιας κάρτας NFC ακολουθεί την ίδια διαδικασία του smartphone (Chabbi et al., 2022). Το βασικό κίνητρο αυτής της επίθεσης είναι η καταστροφή ευαίσθητων πληροφοριών των χρηστών και έχουν κατασκευαστεί διάφορα εργαλεία για την εκτέλεση της επίθεσης. Ορισμένα από αυτά είναι το Hashcat, το Hashtopolis και το Footnote (Chimuco et al., 2023)

- Επιθέσεις skimming, όπου ο επιτιθέμενος μπορεί να υποκλέψει δεδομένα πληρωμής με μια φυσική συσκευή. Ωστόσο, υπάρχουν τα πρότυπα ασφάλειας των ανέπαφων συναλλαγών προκειμένου να αποφευχθούν οι κακόβουλες επιθέσεις (Singth et al., 2018).
- Επιθέσεις κλωνοποίησης, όπου οι επιτιθέμενοι προσπαθούν κακόβουλα να κλέψουν ή να αντιγράψουν τα δεδομένα που είναι αποθηκευμένα στις κάρτες (Leclerc et al., 2022). Στη συνέχεια, οι πληροφορίες που έχουν αντιγράφει, μπορούν να εγγραφούν είτε σε άλλη κάρτα είτε να προσομοιωθούν, με αποτέλεσμα το αντίγραφο της κάρτας ή οι προσομοιωμένες πληροφορίες να χρησιμοποιηθούν από τους επιτιθέμενους μελλοντικά και να εμφανίζονται παρόμοια ή ακριβή χαρακτηριστικά με αυτά της αρχικής κάρτας. Μια κλωνοποιημένη κάρτα μπορεί να επιτρέψει σε ένα άτομο να αποκτήσει πρόσβαση σε μια υπηρεσία, εάν δεν απαιτείται άλλο αποδεικτικό εκτός από την κάρτα (Leclerc et al., 2022). Αυτό σημαίνει ότι οι συγκεκριμένες επιθέσεις μπορούν να προκαλέσουν σοβαρά προβλήματα, όπως διαρροή προσωπικών δεδομένων και οικονομικών απωλειών. Ακόμη, κατά την διαδικασία της επίθεσης εφαρμόζονται μέθοδοι υποκλοπών για να ληφθούν τα δεδομένα από την αρχική κάρτα και να δημιουργηθεί ένα αντίγραφο.
- Επιθέσεις καταγραφής οθόνης, όπου ο επιτιθέμενος εγκαθιστά μια κάμερα κοντά σε κάποιο ATM ή POS, η οποία δεν είναι εμφανής στους χρήστες. Αυτή η διαδικασία γίνεται για να βιντεοσκοπηθεί και να κλαπεί το PIN του χρήστη και να γίνουν βλαβερές επιθέσεις.

4.2. Επιθέσεις στην τραπεζική επικοινωνία NFC

Εκτός από τις επιθέσεις NFC στις τραπεζικές κάρτες και στα smartphones, υπάρχουν και επιθέσεις τραπεζικής επικοινωνίας NFC και είναι οι εξής:

- Επίθεση eavesdropping: Η υποκλοπή είναι ένα είδος επίθεσης που ο επιτιθέμενος προσπαθεί να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες νόμιμων χρηστών από τα ηχητικά μηνύματα και τα βίντεο που ανταλλάσσουν οι χρήστες μεταξύ τους (Chimuco et al., 2023). Ο βασικός στόχος της επίθεσης είναι η δόλια απόκτηση κρίσιμων στοιχείων για οικονομικούς, πολιτικούς και για άλλους λόγους. Μερικές φορές η συγκεκριμένη επίθεση μπορεί να είναι νόμιμη όταν παρέχεται εξουσιοδότηση από την δικαιοσύνη για την διερεύνηση τρομοκρατικών ενεργειών και άλλων αντίστοιχων σοβαρών περιπτώσεων (Chimuco et al., 2023).
- Επιθέσεις επανάληψης πληρωμών NFC (NFC payment replay attack): Στη συγκεκριμένη μορφή επίθεσης τα τραπεζικά δεδομένα που ανταλλάσσονται μεταξύ της έξυπνης κάρτας και του τερματικού σημείου πώλησης δεν είναι κρυπτογραφημένα. Αυτή η επίθεση συμβαίνει όταν ο επιτιθέμενος μεταδίδει εκ νέου την επικοινωνία που σχετίζεται με τον έλεγχο ταυτότητας μεταξύ μιας έξυπνης κάρτας VISA ή Mastercard και ενός τερματικού αυτόματης πληρωμής. Δεδομένου ότι η επίθεση είναι κρυφή τόσο η έξυπνη κάρτα όσο και το τερματικό πληρωμής δεν την αντιλαμβάνονται. Σε αυτή την περίπτωση, εφόσον ο επιτιθέμενος έχει γνώσεις στην ραδιοηλεκτρονική, μπορεί να τις χρησιμοποιήσει για να κλέψει τα προσωπικά δεδομένα της έξυπνης κάρτας του θύματος (Chimuco et al., 2023).
- Επιθέσεις αναμετάδοσης (Relay attacks): Σε αυτό το είδος επίθεσης γίνεται μεταφορά ασύρματης επικοινωνίας. Ο επιτιθέμενος μπορεί να περάσει την επικοινωνία μέσω μιας εικονικής κάρτας που ονομάζεται proxy, η οποία χρησιμοποιείται για την εκτέλεση συναλλαγών με έναν αναγνώστη NFC. Έπειτα, ο επιτιθέμενος λαμβάνει σήματα από μια συσκευή που ονομάζεται mole και έτσι, έχει αποκτήσει φυσική πρόσβαση στην πραγματική τραπεζική κάρτα, διενεργώντας κακόβουλα προβλήματα.

4.3. Επιθέσεις στο σύστημα αναγνώρισης προσώπου

Η ραγδαία εξέλιξη των συστημάτων αναγνώρισης προσώπου έχει δημιουργήσει νέες ανησυχίες σχετικά με την ικανότητά τους να αντιστέκονται στις απειλές.

Δεδομένου ότι το πρόσωπο είναι ένα ορατό μέρος του ανθρώπινου σώματος, μπορεί κανείς να αποκτήσει εύκολα φωτογραφίες και βίντεο από τις ποικίλες πλατφόρμες κοινωνικής δικτύωσης. Ως εκ τούτου, μπορεί κανείς να υποκλέψει, να καταχραστεί και να τροποποιήσει τις υπάρχουσες ταυτότητες για οποιαδήποτε παράνομη δραστηριότητα, με στόχο την εξαπάτηση των συστημάτων αναγνώρισης προσώπου. Υπάρχουν δύο βασικές κατηγορίες πλαστοπροσωπίας που είναι η άμεση και η έμμεση (Rusia et al., 2023). Στην πρώτη κατηγορία είναι το μακιγιάζ και θεωρείται άμεση μορφή πλαστοπροσωπίας, όπου με την χρήση διαφόρων μοτίβων και φίλτρων μπορεί να αλλάξει η εμφάνιση του προσώπου, οδηγώντας σε αποτυχία του συστήματος αναγνώρισης, ιδίως στην περίπτωση των ηλικιωμένων. Στην δεύτερη κατηγορία, οι κακόβουλοι χρήστες χρησιμοποιούν διάφορα τεχνουργήματα όπως τρισδιάστατες φωτογραφίες και βίντεο προσώπου, προκειμένου να ξεγελάσουν την συσκευή αναγνώρισης και να παραβιάσουν σε μεγάλο βαθμό την αυθεντικότητα της (Rusia et al., 2023).

4.4. Επιθέσεις Vishing

Η επίθεση vishing είναι μια μέθοδος υποκλοπής προσωπικών δεδομένων που περιλαμβάνει τη χρήση της φωνής (Alabdan, 2020). Οι απατεώνες χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης για να χειραγωγήσουν τα θύματά τους. Συνήθως, παρουσιάζονται ως ένας σημαντικός φορέας, δηλαδή ως τράπεζα και προσπαθούν να δημιουργήσουν την αίσθηση ότι πρόκειται για ένα επείγον συμβάν. Οι απατεώνες που χρησιμοποιούν τεχνικές φωνητικού ψαρέματος, ακολουθούν πολλές τακτικές για να κάνουν τις απάτες τους ακόμη πιο επιτυχημένες. Οι βασικές τακτικές είναι οι εξής:

- Εργαλεία πλαστογράφησης αναγνώρισης κλήσης, τα οποία μπορούν να χρησιμοποιηθούν για την απόκρυψη τοποθεσίας του απατεώνα και την αλλαγή των αριθμών τηλεφώνου ώστε να φαίνεται ότι η κλήση πραγματοποιήθηκε από κάποιο αξιόπιστο οργανισμό (Alabdan, 2020).
- Απάτη με συνδυαστική χρήση διαφορετικών τακτικών, που μπορεί να ξεκινούν με ένα ψεύτικο ηλεκτρονικό ή φωνητικό μήνυμα, με σκοπό να ενθαρρύνουν τον χρήστη να απαντήσει .
- Απάτη κοινωνικών μέσων, όπου οι απατεώνες κάνοντας μια έρευνα στα κοινωνικά μέσα μπορούν να βρουν πληθώρα πληροφοριών για τα θύματά

τους. Έτσι, μπορούν να χρησιμοποιήσουν τις πληροφορίες που έχουν συλλέξει και να στοχεύσουν σε συγκεκριμένα άτομα, όπως σε υπαλλήλους εταιριών με προνομιακούς λογαριασμούς. Τέλος, για να γίνει πιο νομιμοφανής η επικοινωνία, οι απατεώνες μπορεί να παραθέσουν ορισμένα προσωπικά στοιχεία στο θύμα, με σκοπό να καταφέρουν να αποσπάσουν τις απαραίτητες πληροφορίες για να υλοποιήσουν την κακόβουλη ενέργειά τους (Alabdan, 2020).

4.5. Επιθέσεις Smishing

Το smishing αποτελεί μια μορφή ηλεκτρονικής απάτης η οποία πραγματοποιείται μέσω συνοπτικών μηνυμάτων με τη χρήση κινητών τηλεφώνων. Στη συγκεκριμένη επίθεση, συνήθως, το θύμα λαμβάνει ένα μήνυμα το οποίο εμπεριέχει έναν σύνδεσμο (link). Πατώντας τον σύνδεσμο, ο ανυποψίαστος χρήστης κατεβάζει αυτόματα στην συσκευή του το κακόβουλο λογισμικό ή ανακατευθύνεται σε παραπλανητική ιστοσελίδα, όπου του ζητείται να παραχωρήσει δεδομένα, όπως ευαίσθητα προσωπικά στοιχεία, τραπεζικό λογαριασμό ή κάρτα, κωδικούς και άλλα (Alabdan, 2020).

4.6. Επιθέσεις QRishing

Το QRishing αποτελεί τη νέα δράση των χάκερς αξιοποίησης πληροφοριών του υποκειμένου δεδομένων που συλλέγονται από ένα σημείο και απόκτησης πρόσβασης σε άλλα πολύτιμα δεδομένα του (Alabdan, 2020). Οι κωδικοί QR υπάρχουν εδώ και πολλά χρόνια αλλά η τεχνολογία με τη δυνατότητα σάρωσης έχει αναζωπυρωθεί το τελευταίο χρονικό διάστημα. Οι μοναδικοί τετράγωνοι κωδικοί έχουν χρησιμοποιηθεί για την αντικατάσταση διαφόρων χάρτινων εντύπων σε μια προσπάθεια παροχής ανέπαφων υπηρεσιών. Με αυτό τον τρόπο, οι χρήστες χρησιμοποιούν κινητά τηλέφωνα για να σαρώσουν εύκολα και γρήγορα έναν κωδικό QR, που τους κατευθύνει σε διάφορες μορφές ψηφιακών περιεχομένων. Πολλές επιχειρήσεις και οργανισμοί εξακολουθούν να χρησιμοποιούν κωδικούς QR λόγων των πολλαπλών πλεονεκτημάτων που προσφέρουν. Μερικά από αυτά περιλαμβάνουν το μειωμένο κόστος, την ευκολία ηλεκτρονικής επεξεργασίας και την καλύτερη προσαρμογή των υπηρεσιών.

Ωστόσο, οι επιχειρήσεις και οι οργανισμοί θα πρέπει να είναι ιδιαίτερα προσεκτικοί όταν χρησιμοποιούν κωδικούς QR προς αποφυγή παραβιάσεων απορρήτου. Πιο αναλυτικά, ένας χρήστης μπορεί να ανακατευθυνθεί σε έναν ιστότοπο και να παρακολουθείται η συμπεριφορά του, διότι συνήθως αποθηκεύονται οι προτιμήσεις του. Συγκεκριμένα, κάθε φορά που ένας χρήστης σαρώνει έναν κωδικό QR μπορούν να συλλεχθούν ορισμένα δεδομένα, όπως ο τύπος συσκευής που χρησιμοποιεί, η τοποθεσία, διεύθυνση IP, ημερομηνία καθώς και άλλες προσωποποιημένες πληροφορίες. Η συγκεκριμένη τεχνολογία θα μπορούσε να θεωρηθεί ευάλωτη σε εγκληματίες του κυβερνοχώρου που προσπαθούν να συλλέξουν δεδομένα από την συσκευή που χρησιμοποιεί τον κωδικό QR ή να ανακατευθύνουν τον σαρωτή σε διαφορετική διεύθυνση URL (Alabdan, 2020). Η διαδικασία γίνεται ακόμη πιο επικίνδυνη αν εμπλέκονται τα στοιχεία πληρωμής των χρηστών. Τέλος, για να αποφευχθούν τα παραπάνω προβλήματα στον κυβερνοχώρο, οι κωδικοί QR πρέπει να χρησιμοποιούνται σωστά και με τις κατάλληλες διασφαλίσεις.

4.7. Επιθέσεις Spear Phishing

Οι εγκληματίες του κυβερνοχώρου προσπαθούν κάθε φορά να χρησιμοποιούν νέα μεθόδους απόσπασης ευαίσθητων προσωπικών δεδομένων από τους χρήστες. Στόχος, λοιπόν, της επίθεσης Spear Phishing είναι να αποστέλλει ηλεκτρονικά μηνύματα, τα οποία μοιάζουν να προέρχονται από κάποιο άτομο ή επιχείρηση που ο χρήστης γνωρίζει, με σκοπό να αποκτήσουν τους αριθμούς της πιστωτικής κάρτας και τις οικονομικές πληροφορίες που ενδεχομένως να έχει αποθηκευμένες ο χρήστης στον υπολογιστή ή στο κινητό τηλέφωνο (Ali et al., 2019). Ο spear phisher μπορεί να παρουσιαστεί ως φίλος στον χρήστη και να ζητήσει τον κωδικό πρόσβασης. Αν ο χρήστης απαντήσει στο μήνυμα δίνοντας τους κωδικούς, εκείνοι θα τους χρησιμοποιήσουν για να χρεώσουν τον χρήστη. Διαφορετικά, ο spear phisher μπορεί να χρησιμοποιήσει τις ίδιες πληροφορίες για να παριστάνει κάποιον εκπρόσωπο ηλεκτρονικού καταστήματος και να ζητήσει από τον χρήστη να κάνει επαναφορά του κωδικού ή επαλήθευση του αριθμού της πιστωτικής κάρτας (Ali et al., 2019). Αν ο χρήστης προβεί σε αυτή την ενέργεια οι εγκληματίες θα τον βλάψουν οικονομικά, με αποτέλεσμα να χάσει όλα τα χρήματα.

4.8. Επιθέσεις Ransomware

Το ransomware είναι μια μορφή κακόβουλου λογισμικού που προσπαθεί να δημοσιεύσει τα προσωπικά δεδομένα του θύματος μέχρι να δοθούν λύτρα από το θύμα. Η συγκεκριμένη μορφή επίθεσης έχει επηρεάσει ένα ευρύ φάσμα υπηρεσιών, όπως μεταφορές, τηλεπικοινωνίες, χρηματοπιστωτικές εταιρίες και υπηρεσίες υγείας. Είναι η πιο κυρίαρχη απειλή στον κυβερνοχώρο μιας και οι εισβολείς που εξαπολύουν επιθέσεις ransomware χρησιμοποιούν τεχνικές για να κρυπτογραφήσουν τα αρχεία και τους πόρους του θύματος καθιστώντας τα μη προσβάσιμα και ζητώντας χρήματα για την αποκρυπτογράφησή τους (Anon, 2021 & Kumar, 2020). Οι συγκεκριμένες επιθέσεις πραγματοποιούνται συνήθως με την χρήση ενός ιού Trojan, ο οποίος φαίνεται σαν ένα κακόβουλο αρχείο που αποστέλλεται με κάποιο ηλεκτρονικό μήνυμα και ο χρήστης παραπλανάται και το κατεβάζει στον υπολογιστή του. Έχει παρατηρηθεί ότι οι περισσότεροι παραβιασμένοι υπολογιστές και οι κινητές συσκευές χρησιμοποιούσαν λειτουργικά συστήματα Windows και Android, αντίστοιχα (Nadir & Bakhshi, 2018). Δεν είναι λίγες οι φορές που οι εισβολείς στοχεύουν σε μεγάλους οργανισμούς και επιχειρήσεις, διότι γνωρίζουν πως μπορούν να πληρώσουν υψηλότερα χρηματικά ποσά. Πολλές εταιρίες προκειμένου να αποφύγουν την διαρροή των ευαίσθητων προσωπικών και οικονομικών στοιχείων, επιλέγουν να πληρώσουν τα λύτρα, ώστε να μην διακινδυνεύσουν περαιτέρω και προκληθούν νέες επιθέσεις από τους εγκληματίες του κυβερνοχώρου.

4.9. Επιθέσεις Man-in-the-Middle (MIMT)

Η επίθεση man-in-the-middle στα δίκτυα επικοινωνίας αποτελεί έναν τρόπο παραβίασης της ασφάλειας. Ο επιτιθέμενος καταφέρνει να παρεμποδίσει μια νόμιμη επικοινωνία μεταξύ δύο ατόμων, με απώτερο στόχο την απόσπαση και παραποίηση πληροφοριών και συναλλαγών που αποστέλλονται μέσω του συστήματος επικοινωνίας από τους συμμετέχοντες (Ferrag et al., 2020). Συνήθως ο επιτήδειος βρίσκεται στο ίδιο δίκτυο με τα θύματα που θέλει να εξαπατήσει, παρακολουθώντας τη ροή της επικοινωνίας. Ακόμη, μπορεί να προκληθεί και αλλοίωση των μηνυμάτων, αφού ο επιτιθέμενος έχει την δυνατότητα να κρυφακούει τις συνομιλίες, χωρίς να το

γνωρίζουν οι συμμετέχοντες. Για να συμβούν τα παραπάνω, οι επιτήδειοι πρέπει πρώτα να αποκτήσουν πρόσβαση σε ένα ασύρματο, μη ασφαλές δίκτυο. Αυτό το υποκλέπτουν όταν βρίσκουν δημόσια Wi-Fi από χρήστες που δεν έχουν φροντίσει για την ασφάλεια και την προστασία των δικτύων τους (Ferrag et al., 2020). Έτσι, μόλις εντοπιστεί ένα ευάλωτο δίκτυο, οι χάκερς χρησιμοποιούν τα κατάλληλα εργαλεία προκειμένου να υποκλέψουν προσωπικές και τραπεζικές πληροφορίες.

Χαρακτηριστικό παράδειγμα αποτελούν οι τράπεζες, όπου ο man-in-the-middle αποστέλλει ένα ηλεκτρονικό μήνυμα σε έναν χρήστη που εξ' αρχής φαίνεται νόμιμο και δημιουργεί μια σελίδα όμοια με αυτή της τράπεζας που χρησιμοποιεί ο εκάστοτε χρήστης για να τον πείσει να δώσει όλες τις προσωπικές πληροφορίες. Στην πραγματικότητα, ο χρήστης δεν συνδέεται στην τράπεζα, αλλά σε μια ψεύτικη σελίδα που ομοιάζει με τράπεζα, μέσω της οποίας ο χάκερ καταφέρνει να αποσπάσει τα στοιχεία που επιθυμεί για να υλοποιήσει την κακόβουλη ενέργειά του.

4.10. Επιθέσεις SIM Swapping

Μεγάλες διαστάσεις έχει πάρει η νέα μορφή απάτης που ονομάζεται SIM Swapping, με την οποία οι επιτήδειοι αποκτούν πρόσβαση στις κάρτες SIM των συνδρομητών κινητής τηλεφωνίας. Προκειμένου λοιπόν οι δράστες να αποκτήσουν πρόσβαση στο κινητό τηλέφωνο του θύματος και κατά συνέπεια να διενεργήσουν συναλλαγές από το e-banking του, εμπνεύστηκαν τη μέθοδο SIM Swapping, σύμφωνα με την οποία απευθύνονται στον πάροχο κινητής τηλεφωνίας του χρήστη και προσποιούμενοι τον ίδιο ή κάποιον εξουσιοδοτημένο από αυτόν, ζητούν αντικατάσταση της κάρτας SIM του κινητού του τηλεφώνου. Με την ενεργοποίηση της νέας κάρτας η παλιά αυτομάτως ακυρώνεται κι έτσι οι δράστες μπορούν να λαμβάνουν όλες τις ειδοποιήσεις της τράπεζας που απευθύνονται στο θύμα (Awale, 2019). Η δυνατότητα αυτή σε συνδυασμό με την πρόσβαση στους κωδικούς e-banking την οποία έχουν φροντίσει να αποκτήσουν εκ των προτέρων μέσω άλλων μεθόδων, τους παρέχει πλήρη πρόσβαση στο τραπεζικό προφίλ του θύματος και ευχέρεια διενέργειας πλήθους συναλλαγών έως ότου ο νόμιμος χρήστης αντιληφθεί ότι έχει απενεργοποιηθεί η κάρτα SIM.

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ

Συμπερασματικά, τα θέματα εμπιστοσύνης και ασφάλειας στις ανέπαφες συναλλαγές έχουν σημαντικό αντίκτυπο στη συμπεριφορά των χρηστών. Οι χρήστες βασίζονται ολοένα και περισσότερο στις ανέπαφες πληρωμές, λόγω της ευκολίας, της προσβασιμότητας και της αποτελεσματικότητας. Ωστόσο, η αυξανόμενη χρήση έχει οδηγήσει σε ανησυχίες σχετικά με την ασφάλεια και το απόρρητο των προσωπικών και οικονομικών πληροφοριών. Για να αντιμετωπιστούν αυτές οι ανησυχίες, οι τραπεζικές υπηρεσίες οφείλουν να δώσουν προτεραιότητα στην ανάπτυξη και εφαρμογή ισχυρών μέτρων ασφάλειας. Επιπλέον, είναι ζωτικής σημασίας οι πάροχοι να είναι διαφανείς με τους πελάτες τους σχετικά με τα μέτρα που εφαρμόζουν για την προστασία των δεδομένων τους. Οι πελάτες πρέπει επίσης να λαμβάνουν μέτρα για να προφυλάξουν τη δική τους ασφάλεια, όπως η χρήση ισχυρών κωδικών πρόσβασης, η αποφυγή δημοσίων Wi-Fi και η τακτική παρακολούθηση των λογαριασμών για οποιαδήποτε ύποπτη δραστηριότητα. Με προτεραιότητα στην ασφάλεια και τη διαφάνεια μπορεί να δημιουργηθεί μια σχέση εμπιστοσύνης μεταξύ των υπηρεσιών και των χρηστών και να συνεχίσουν να αναπτύσσονται σύγχρονοι και καινοτόμοι μέθοδοι πληρωμών.

Εν κατακλείδι, στα πλαίσια της συγκεκριμένης μελέτης έγινε αναφορά στις καινοτόμες μορφές ανέπαφων συναλλαγών και παράλληλα αναλύθηκαν οι πιθανές επιθέσεις και οι κίνδυνοι που εγκυμονούν πίσω από τα συστήματα πληρωμών. Επίσης, αναλύθηκε διεξοδικά η ψηφιακή τραπεζική και οι σύγχρονες μορφές εφαρμογών που χρησιμοποιούν οι τράπεζες για τις κινητές συσκευές. Γίνεται κατανοητό ότι τα οφέλη της τεχνολογίας είναι πολλά και οι συναλλαγές πλέον μπορούν να πραγματοποιηθούν κυριολεκτικά με το πάτημα ενός κουμπιού σε ένα ευκολονόητο περιβάλλον. Το κύριο πρόβλημα δυσπιστίας που χρειάστηκε να αντιμετωπίσουν τόσο οι τράπεζες όσο και οι ίδιοι οι χρήστες ήταν η ασφάλεια των συναλλαγών, αλλά με τα συστήματα ασφαλείας που αναπτύχθηκαν περιορίστηκε σημαντικά. Σε κάθε περίπτωση, στη συγκεκριμένη εργασία δόθηκε έμφαση στα βιομετρικά χαρακτηριστικά των ανέπαφων συναλλαγών, στους πιθανούς κινδύνους καθώς και στην ασφάλεια αυτών. Οι πιθανές αδυναμίες βιομετρικών δεδομένων και η εφαρμογή τους σε άλλους κλάδους θα αποτελούσαν ενδιαφέρουσα θεματολογία για μελλοντική έρευνα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ξενόγλωσση

Aiadi, O., Khaldi, B., & Saadeddine, C. (2022). MDFNet: an unsupervised lightweight network for ear print recognition. *Journal of Ambient Intelligence and Humanized Computing*, 1-14.

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, *12*(10), 168.

Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, *100*, 408-427.

Alshazly, H., Linse, C., Barth, E., & Martinetz, T. (2020). Deep convolutional neural networks for unconstrained ear recognition. *IEEE Access*, *8*, 170295-170310.

Aris, F., Ismail, K., & Mohezar, S. (2022). Fostering Mobile Payment Adoption: A Case of Near Field Communication (NFC). *International Journal of Business and Society*, *23*(3), 1535-1553.

Awale, S. M., & Gupta, D. P. (2019). Awareness of sim swap attack. *International Journal of Trend in Scientific Research and Development*, *3*(4), 995-997.

Boldea, B. I., & Boldea, C. R. (2022). Facial recognition technology used in the payment system.

Chabbi, S., El Madhoun, N., & Khamer, L. (2022, October). Security of NFC Banking Transactions: Overview on Attacks and Solutions. In *2022 6th Cyber Security in Networking Conference (CSNet)* (pp. 1-5). IEEE.

Chanti, S., & Chithralekha, T. (2022). A literature review on classification of phishing attacks. *International Journal of Advanced Technology and Engineering Exploration*, *9*(89), 446-476.

Chimuco, F. T., Sequeiros, J. B., Lopes, C. G., Simões, T. M., Freire, M. M., & Inácio, P. R. (2023). Secure cloud-based mobile apps: attack taxonomy, requirements, mechanisms, tests and automation. *International Journal of Information Security*, 1-35.

Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2020). Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommunication Systems*, *73*, 317-348.

Kumar A. (2019). The significance of soundwave technology-based payments. https://www.entrepreneur.com/article/342435. Accessed 5 Aug 2022

Leclerc, S., & Kärrström, P. (2022). CLONING ATTACKS AGAINST NFC-BASED ACCESS CONTROL SYSTEMS.

Lee, C. T., & Pan, L. Y. (2023). Resistance of facial recognition payment service: a mixed method approach. *Journal of Services Marketing*, *37*(3), 392-407.

Li, C., & Li, H. (2023). Disentangling Facial Recognition Payment Service Usage Behavior: A Trust Perspective. *Telematics and Informatics*, 101939.

Limna, P., Kraiwanit, T., & Siripipatthanakul, S. (2022). The growing trend of digital economy: A review article. *International Journal of Computing Sciences Research*, *6*, 1-11.

Litvishko, O., Beketova, K., Akimova, B., Azhmukhamedova, A., & Islyam, G. (2020). Impact of the digital economy on the banking sector. In *E3S Web of Conferences* (Vol. 159, p. 04033). EDP Sciences.

Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: A survey. *Artificial Intelligence Review*, 1-49.

Norov, A. R., Elbusinova, U. X., Norov, A. R., & Mirpulatova, L. M. (2022). The role of digital technologies in the development of commercial banks. Academicia Globe: Inderscience Research, 3(4), 1-9.

Omolara, A. E., Jantan, A., Abiodun, O. I., Arshad, H., & Mohamed, N. A. (2019). Fingereye: improvising security and optimizing ATM transaction time based on iris-scan authentication. *International Journal of Electrical & Computer Engineering (2088-8708)*, *9*(3).

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013.

Rusia, M. K., & Singh, D. K. (2023). A comprehensive survey on techniques to handle face identity threats: challenges and opportunities. *Multimedia Tools and Applications*, *82*(2), 1669-1748.

Sinha, M., Chacko, E., & Makhija, P. (2022). AI Based Technologies for Digital and Banking Fraud During Covid-19. *Integrating Meta-Heuristics and Machine Learning for Real-World Optimization Problems*, *1038*, 443.

Sreeja, N. K., & Sankar, A. (2016). A hierarchical heterogeneous ant colony optimization based approach for efficient action rule mining. *Swarm and Evolutionary Computation*, *29*, 1-12.

Tafti, F. S. M., Mohammadi, S., & Babagoli, M. (2021). A new NFC mobile payment protocol using improved GSM based authentication. *Journal of Information Security and Applications*, *62*, 102997.

Lee, J., Wewege, L., & Thomsett, M. C. (2020). Disruptions and digital banking trends. *Journal of Applied Finance & Banking*, *10*(6), 1792-6599.

Ελληνική

Smith, J. (2019). OuterBox, *Στατιστικά για ηλεκτρονικό εμπόριο για κινητά το 2018 και τις μελλοντικές διαδικτυακές αγορές Τάσεις του mCommerce.* Ανακτήθηκε στις 6 Μαΐου 2019 από https://www.outerboxdesign.com/web-design-articles/mobile-ecommerce-statistics

Διαδικτυακοί Σύνδεσμοι

https://ibankpay.nbg.gr/iBankPay/el/

https://www.nbg.gr/el/epaggelmaties/proionta-upiresies/eisprakseis-plirwmes/upiresies-e-commerce

https://www.nbg.gr/el/idiwtes/kathimerines-sunallages/digital-banking/dunatotites-internet-mobile-banking/i-bank-statements

https://www.piraeusbank.gr/el/idiwtes/trapezikes-ypiresies/e-banking/dimofileis-ilektronikes-trapezikes-synallages/e-statements

https://www.piraeusbank.gr/el/idiwtes/kanalia-eksypiretisis/e-branch

https://www.piraeusbank.gr/el/idiwtes/trapezikes-ypiresies/kathimerines-synallages/anepafes-pliromes-me-to-garmin-smartwatch-meso-garmin-pay

https://www.piraeusbank.gr/el/idiwtes/trapezikes-ypiresies/eidikes-trapezikes-ypiresies/easypay-point

https://www.piraeusbank.gr/el/epiheiriseis-epaggelmaties/ypiresies-epixeiriseon/e-banking/diaheirisi-hartofylakiou-diathesimon-epiheiriseon-winbank

https://www.piraeusbank.gr/el/epiheiriseis-epaggelmaties/ypiresies-epixeiriseon/exeidikeumenes-ypiresies/remote-banking-service

https://www.piraeusbank.gr/el/epiheiriseis-epaggelmaties/anakalypse-ta-xrimatodotika-ergaleia-sou/lyseis-emporon/sxetikes-ipiresies/one-click-pay

https://www.euro2day.gr/specials/opinions/article/2170563/krisimes-symvoyles-gia-asfalh-hrhsh-ton-qr-codes.html

https://www.nbg.gr/el/epaggelmaties/proionta-upiresies/eisprakseis-plirwmes/upiresies-e-commerce/i-bank-e-enterpise

Νομολογία της ΑΠΔΠΧ

Απόφαση 57/2022

Απόφαση 53/2022

Απόφαση 4/2023