**Τ.Ε.Ι. ΠΑΤΡΩΝ**
**ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ**

ΘΕΜΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ:

# Η πληροφορική στο τραπεζικό σύστημα. Απλοποίηση,ταχύτητα,ασφάλεια συναλλαγών.

ΣΠΟΥΔΑΣΤΡΙΑ:
Θεοδωρακοπούλου Ουρανία

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:
**Αντωνόπουλος Γρηγόρης**

**Πάτρα, 15/10/09**

# ***Αφιέρωση***

*Στους γονείς μου*
*που στάθηκαν στο πλευρό*
*μου με υπομονή και με*
*βοήθησαν σε όλη τη*
*διάρκεια των σπουδών*
*μου....*

# ***Ευχαριστίες***

*Ευχαριστώ τον καθηγητή μου, κύριο Αντωνόπουλο Γρηγόρη, για τις πολύτιμες συμβουλές που μου προσέφερε.*

*Θέλω να ευχαριστήσω επίσης το διευθυντή κύριο Αθανάσιο Καραγιάννη, καθώς επίσης και όλο το προσωπικό της τράπεζας* Eurobank *για την κατανόηση και τη σημαντική βοήθειά τους στην έρευνα μου.*

# ΠΕΡΙΕΧΟΜΕΝΑ

## Α'Μέρος

## *ΚΕΦΑΛΑΙΟ 5: Πλεονεκτήματα και μειονεκτήματα και ανασταλτικοί παράγοντες ηλεκτρονικής τραπεζικής.*



## *ΚΕΦΑΛΑΙΟ 6: Η διεύρυνση της χρήσης της πληροφορικής στο τραπεζικό σύστημα – Επιχειρήσεις και ηλεκτρονική τραπεζική*



## *ΚΕΦΑΛΑΙΟ 7: Διατραπεζικά συστήματα ΔΙΑΣ.*

## *ΈΡΕΥΝΑ*



## *ΒΙΒΛΙΟΓΡΑΦΙΑ*

# ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία ασχολείται με το θέμα της πληροφορικής στο ευρύτερο τραπεζικό σύστημα όσον αφορά την απλοποίηση, την ταχύτητα καθώς και την ασφάλεια των συναλλαγών.Πιο συγκεκριμένα, αναλύεται η κατάσταση στην οποία βρίσκεται το ηλεκτρονικό τραπεζικό σύστημα και οι διάφορες έννοιες της βασικής ηλεκτρονικής τραπεζικής, οι οποίες χρησιμοποιούνται εκτενώς για τη διεκπεραίωση των ηλεκτρονικών συναλλαγών καθώς επίσης δίνεται σαφής και αναλυτική εμβάθυνση στους τρόπους με τους οποίους μπορούν να πραγματοποιηθούν αυτές οι ηλεκτρονικές τραπεζικές συναλλαγές.

Ιδιαίτερη σημασία δίνεται στα πλεονεκτήματα και τα μειονεκτήματα όσον αφορά τη ταχύτητα και την απλοποίηση που απορρέουν από τη σύγκριση του παραδοσιακού συστήματος συναλλαγών σε σχέση με το νέο αυτό τρόπο πραγματοποίησης ηλεκτρονικών συναλλαγών.Ακόμα, αναλύονται οι υπηρεσίες που προσφέρουν οι κυριότερες Ελληνικές τράπεζες,οι τρόποι και τα διάφορα μέσα προφύλαξης και ασφάλειας των προσωπικών δεδομένων των πελατών από τους διάφορους κινδύνους που περικλείει η χρήση των ηλεκτρονικών τραπεζικών συναλλαγών. Συγκεκριμένα οι τρόποι ταυτοποίησης πελατών καθώς και οι διάφορες μέθοδοι κρυπτογράφησης που εξελίσσονται ολοένα και περισσότερο με την πάροδο των ετών και έχουν σαν στόχο την να διασφαλίσουν την εμπιστοσύνη του πελατειακού τους κοινού καθως επίσης και να αυξήσουν οι ίδιες οι τράπεζες την μεταξύ τους ανταγωνιστικότητα.

Σκοπός της παρούσας εργασίας είναι να προσφέρει μια πλήρης ενημέρωση της κατάστασης και των νέων υπηρεσιών του τραπεζικού συστήματος, ώστε να δημιουργηθεί μια νέα μορφή εξοικείωσης και διευκόλυνσης των πελατών με ένα νέο τρόπο συναλλαγών, μέσα από τον οποίο παρέχεται όχι μόνο απλοποίηση και ταχύτητα αλλά προσφέρονται και ασφαλείς ηλεκτρονικές τραπεζικές συναλλαγές. 


# ΕΙΣΑΓΩΓΗ

Η παρούσα πτυχιακή εργασία επιχειρεί να καταγράψει τις ριζικές αλλαγές που «βιώνει» το τραπεζικό σύστημα σε σχέση με τα προηγούμενα χρόνια καθως επίσης, να αναλύσει αλλά και να δώσει απαντήσεις σε κρίσιμα ζητήματα που αφορούν στην απλοποίηση, την ταχύτητα, αλλά και την ασφάλεια των συναλλαγών μέσα από τη χρήση της πληροφορικής στο τραπεζικό σύστημα. Ο λόγοι που που παρουσιάζει ενδιαφέρον η συγκεκριμένη εργασία είναι ποικίλοι και αναφέρονται αναλυτικά παρακάτω.

Τα τελευταία χρόνια παρατηρούμε ότι έχουμε περάσει στην εποχή της πληροφορίας και καθοριστικό ρόλο πλέον διαδραματίζει η ταχύτητα διακίνησής της. Με αυτόν τον τρόπο, η χρήση του διαδικτύου εξαπλώνεται ολοένα και περισσότερο στη ζωή μας επηρεάζοντας τις καθημερινές μας συναλλαγές.

Η παγκοσμιοποίηση και η απελευθέρωση των αγορών δημιουργούν νέα δεδομένα στον οικονομικό χώρο.

Ειδικότερα, η μεγάλη ανάπτυξη του διαδικτύου (internet) έχει επιπτώσεις, όπως είναι φυσικό και στον τραπεζικό χώρο.

Το χαμηλό κόστος και η εύκολη πρόσβαση που προσφέρει το διαδίκτυο στον κάθε χρήστη, έχει ήδη προκαλέσει ένταση στον ανταγωνισμό του συγκεκριμένου κλάδου και καθιέρωση των εναλλακτικών δικτύων στην καθημερινή λειτουργία των τραπεζών αλλά και στη συνείδηση των πελατών.

Οι τράπεζες στην προσπάθεια τους να παρακολουθήσουν τις εξελίξεις και κάτω από την ένταση του ανταγωνισμού στον ευρύτερο χρηματοπιστωτικό χώρο καλούνται να βρούν απάντηση στα ερωτήματα για το πώς μπορούν να χαράξουν νέα στρατηγική και πως θα καταφέρουν να αξιοποιήσουν κατά τον βέλτιστο τρόπο τις δυνατότητες των νέων τεχνολογιών πληροφορίας και επικοινωνίας.το Internet καθιερώνει νέα κανάλια διανομής τραπεζικών προϊόντων και υπηρεσιών.

Στις μέρες μας πλησιάζει η τράπεζα τον πελάτη μέσα από τις ηλεκτρονικές σελίδες σε αντίθεση με παλαιότερα όπου πήγαινε ο πελάτης στην τράπεζα. Οι τράπεζες παγκοσμίως οδεύουν προς την πλήρη μεταμόρφωση τους με κύριο άξονα τους την ιδιαίτερη μεταχείριση κάθε πελάτη και βασικό όπλο τους την τεχνολογία μέσα από τη χρήση της πληροφορικής. Η βιωσιμότητα και η επιτυχία ενός χρηματοπιστωτικού ιδρύματος, θα εξαρτάται πλέον από την ικανότητα του στο πώς να προβλέπει, πως να ανταποκρίνεται, ακόμα και στο πως να ξεπερνά τις προσδοκίες των πελατών του.

Η παρούσα πτυχιακή εργασία έχει σαν στόχο να παρουσιάσει τη κατάσταση που επικρατεί στο τραπεζικό σύστημα αλλά κυρίως να εμβαθύνει στο τρόπο χρήσης της πληροφορικής,έτσι ώστε να συμβάλλει στην όσο το δυνατόν καλύτερη κατανόηση για το πώς οι τράπεζες μπορούν να προσφέρουν απλοποίηση, ταχύτητα και ασφάλεια στις καθημερινές συναλλαγές. Με αυτό το τρόπο οι τράπεζες θα καταφέρουν να επιτύχουν αύξηση του πελατειακού τους κοινού πράγμα που συνδέεται άμεσα με την προσπάθεια τους, για αύξηση της ανταγωνιστικότητας τους σε σχέση με τις υπόλοιπες τράπεζες του κλάδου.

Το όφελος από αυτή τη χρήση της πληροφορικής είναι αρκετα αξιόλογο γιατι με αυτό τον τρόπο οι τραπεζικές συναλλαγές περνούν σε ένα τελείως διαφορετικό επίπεδο απ' οτι ειχαμε συνηθισει μέχρι πριν από λίγα χρόνια, καθώς μπορούν να μας προσφέρουν απλοποίηση, ταχύτητα και ασφάλεια των συναλλαγών μας, και ελαχιστοποίηση του κόστους των συναλλαγών.

Αναλυτικότερα, στο πρώτο κεφάλαιο, γίνεται λόγος για τη σημασία της πληροφορικής στο τραπεζικό σύστημα, την ιστορία του τραπεζικού συστήματος και μια γενικότερη εικόνα για το πώς ειναι η ηλεκτρονική τραπεζική στην Ελλάδα σήμερα.

Το δεύτερο κεφάλαιο αναφέρεται στην έννοια της ηλεκτρονικής τραπεζικής, σε ποιους απευθύνεται και τι κυρίως εμπεριέχει.

Στο τρίτο κεφάλαιο, παρουσιάζονται τα διάφορα είδη της ηλεκτρονικής τραπεζικής όπως internet banking, phone banking, αυτόματες ταμειολογιστικές μηχανές ATMs και AEMs και οι μηχανές αυτόματης μεταφοράς κεφαλαίων E.F.T.P.O.S.

Στο τέταρτο κεφάλαιο, αναφέρονται οι κάρτες οι οποίες χρησιμοποιούνται για τη διενέργει των ηλεκτρονικών συναλλαγών.

Το πέμπτο κεφάλαιο, αναφέρεται στα πλεονεκτήματα της πληροφορικής στο τραπεζικό σύστημα γενικότερα και σε αυτά που αφορούν στο κόστος και το χρόνο. Στη συνέχεια, παραθέτονται τα πλεονεκτήματα, τα μειονεκτήματα, καθώς και οι ανασταλτικοί παράοντες.

Το έκτο κεφάλαιο δίνει μία σαφή εικόνα για τις τράπεζες στην Ελλάδα που χρησιμοποιούν την ηλεκτρονική τραπεζική και ποιές υπηρεσίες παρέχουν οι μεγαλύτερες ελληνικές τράπεζες.

Το έβδομο κεφάλαιο ασχολείται με την έννοια και τις υπηρεσίες που παρέχουν τα διατραπεζικά συστήματα ΔΙΑΣ τόσο στις τράπεζες, όσο και στους πελάτες.

Στο όγδοο κεφάλαιο, γίνεται λόγος για τις διάφορες χρεώσεις, ειδοποιήσεις, προμήθειες καθώς και για τα όρια συναλλαγών που εφαρμόζουν οι τράπεζες.

Στο ένατο κεφάλαιο αναλύεται η έννοια, οι στόχοι καθώς και οι διακρίσεις των στρατηγικών της ηλεκτρονικής τραπεζικής.

Το δέκατο κεφάλαιο παρουσιάζει τους κινδύνους της ηλεκτρονικής τραπεζικής που ελοχεύουν, όπως επίσης αναφέρεται σε συγκεκριμένες περιπτώσεις ηλεκτρονικών επιθέσεων.

Στο ενδέκατο κεφάλαιο γίνεται εισαγωγή και ανάλυση των βασικών συστημάτων ασφαλείας.

Στο δωδέκατο κεφάλαιο γίνεται λόγος για την έννοια και τα ταυτοποίηση χρήστη στι ηλεκτρονικές τραπεζικές συναλλαγές

Το δέκατο τρίτο κεφάλαιο,έχει σαν στόχο να παρουσιάσει τα βιομετρικά συστήματα αναγνώρισης των ανθρώπινων χαρακτηριστικών ώστε να διασφαλίζεται το απόρρητο των προσωπικών δεδομένων και να αποφεύγονται οι διάφοροι τυχόν κίνδυνοι.

Το δέκατο τέταρτο κεφάλαιο, αναφέρεται στη πιστοποίηση των ηλεκτρονικών καταστημάτων καθώς και στα μέτρα τα οποία λαμβάνονται για να είναι ασφαλείς οι ηλεκτρονικές αυτές συναλλαγές.

Στο δέκατο πέμπτο κεφάλαιο, αναλύονται τα κρυπτογραφικά συστήματα.


Α' Μέρος

# ΚΕΦΑΛΑΙΟ 1
# Εισαγωγή στη πληροφορική του τραπεζικού συστήματος - Ιστορική αναδρομή.

## 1.1 Η πληροφορική στον τραπεζικό σύστημα.

Το Διαδίκτυο εξελίσσεται μέρα με τη μέρα σε ένα ισχυρότατο νέο εμπορικό μέσο για όλους τους επαγγελματικούς κλάδους. Το επίτευγμα αυτό της νέας τεχνολογίας δεν θα μπορούσε να αφήσει ανεπηρέαστες και τις τραπεζικές συναλλαγές οι οποίες γίνονται ολοένα και με πιο αυτοματοποιημένο τρόπο σε συντομότερο χρονικό διάστημα και φυσικά με το χαμηλότερο δυνατό κόστος για τις τράπεζες. Η εποχή της ψηφιακής οικονομίας την οποία διανύουμε παρέχει αμέτρητες δυνατότητες σε κάθε κοινωνική και οικονομική δραστηριότητα.

Το πρώτο βήμα που έφερε την επανάσταση και το ηλεκτρονικό εμπόριο στο Internet ήταν οι πιστωτικές κάρτες. Τώρα είναι η σειρά του “E-Banking”,όρος που σημαίνει ολοκλήρωση των τραπεζικών συναλλαγών με την χρήση ηλεκτρονικών μέσων και που υπόσχεται να μεταφέρει την τράπεζα στην οθόνη του υπολογιστή μας.

Μέσα από το Internet μπορεί να συνδεθεί κανείς με όποια τράπεζα θέλει, να ρωτήσει για το υπόλοιπο του λογαριασμού του, να πληρώσει την πιστωτική του κάρτα, να υπολογίσει τους τόκους καταθέσεων, ακόμα και να εκτελέσει εντολές για το χρηματιστήριο.
Αυτό είναι μόνο η αρχή καθώς την πρόσβαση στο Internet διεκδικούν και άλλες συσκευές εκτός από το PC, όπως είναι τα μικρά ηλεκτρονικά organizer, ακόμα και τα κινητά τηλέφωνα.
Έτσι, έχουμε πρόσβαση στις τραπεζικές συναλλαγές μας εύκολα, γρήγορα και προπαντώς από οπουδήποτε και αν βρισκόμαστε.

Η εποχή όπου οι συναλλασσόμενοι με τις τράπεζες θα μπορούν να εξυπηρετούνται για το σύνολο των τραπεζικών υπηρεσιών ηλεκτρονικά και όλο το 24ωρο έχει γίνει πλέον εφικτή.
Αυτή η δυνατότητα παρέχεται μέσω της τεχνολογίας και της ηλεκτρονικής τραπεζικής που ήδη προσφέρουν οι υφιστάμενες τράπεζες, καθώς και από άλλες, αμιγώς ηλεκτρονικές τράπεζες, οι οποίες έρχονται να ανταγωνιστούν τις «παραδοσιακές» προσφέροντας ελκυστικότερα καταθετικά προϊόντα και πιθανόν φθηνότερα δάνεια.

Η ανάπτυξη των υπηρεσιών ηλεκτρονικής τραπεζικής (E-Banking) τα τελευταία χρόνια, υπήρξε μεγάλη και όλο και περισσότεροι πελάτες τραπεζών, εμπιστεύονται τις ηλεκτρονικές υπηρεσίες, απολαμβάνοντας πλήθος ευκολιών και εξοικονομώντας πολύτιμο χρόνο.

## 1.2 Η ιστορία της πληροφορικής στο τραπεζικό σύστημα.

Η τεχνολογία E-Banking ξεκίνησε τη δεκαετία του 1970 χρησιμοποιώντας ένα διεπαφές τερματικό -προς -κεντρικό υπολογιστή (terminal to host).

Το πρώτο σύστημα E-Banking χρησιμοποίησε δομή σημείο-προς-σημείο (point to point), με το οποίο μόνο ένας χρήστης μπορούσε να επικοινωνήσει με την τράπεζα και το αντίστροφο. Η χρήση User's ID και password εγγυώνται την ασφάλεια σε αυτό το σύστημα.

Το 1995 η SFNB (Security First Network Bank) ανοίγει τις εικονικές της πύλες και γίνετε ο πρώτος οικονομικός οργανισμός που χρησιμοποιεί το internet ως κύριο κανάλι διανομής των προϊόντων και υπηρεσιών του.

Ένα χρόνο μετά, το 1996, δημιουργήθηκε το «Ολοκληρωμένο Οικονομικό Δίκτυο» (ÌNF) (Integrated Network Financial) το οποίο αναπτύχθηκε από 14 τράπεζες και την IBM και παρείχε υπηρεσίες μέσω διεπαφών του Internet.

Τον ίδιο χρόνο η Microsoft ανακοινώνει το πακέτο «Ανοιχτής Οικονομικής Συνδεσιμότητας» που επιτρέπει την υλοποίηση συνδέσεων με ένα άλλο προσωπικό χρηματοοικονομικό πρόγραμμα της Microsoft, το Microsoft Money.

Αυτά τα καινοτόμα για την εποχή τους συστήματα μετασχηματίζονται σε ένα ολοκληρωμένο μέρος της επιχειρησιακής πορείας μιας εταιρείας.
Από το 1996 μέχρι σήμερα η επικοινωνιακή αναβάθμιση του Internet, η εξέλιξη των εργαλείων περιήγησης (Browsers), η ανάπτυξη των μηχανισμών Ηλεκτρονικής Ανταλλαγής Δεδομένων (EDI-Electronic Data Interchange) και οι αναμενόμενες εφαρμογές σύγκλισης με την τηλεόραση θα δώσουν νέα ώθηση στις τραπεζικές εφαρμογές μέσω του Διαδικτύου.

Σήμερα οι τράπεζες παγκοσμίως αντιμετωπίζουν την πρόκληση να δομήσουν υπηρεσίες E-Banking ώστε να παρέχουν υψηλό επίπεδο υπηρεσιών και ακεραιότητα πληροφοριών.

Ένας τρόπος μετάδοσης των πληροφοριών είναι για παράδειγμα μέσω του προγράμματος «Δία» και «Τειρεσία». Με τα προγράμματα αυτά επιτυγχάνεται μια συνεργασία όλων των τραπεζών on-line προκειμένου να γίνουν οι διατραπεζικές συναλλαγές.

## 1.3 Το Ελληνικό τραπεζικό σύστημα.

Στη σημερινή επιχειρηματική πραγματικότητα ο τραπεζικός κλάδος αναπτύσσεται διαρκώς και αποτελεί έναν από τους πιο κερδοφόρους κλάδους της Ελληνικής οικονομίας. Την τελευταία δεκαετία, οι αλλαγές που πραγματοποιούνται στο σύνολο των χρηματοπιστωτικών οργανισμών, είναι ριζικές και ειδικότερα το φαινόμενο των εξαγορών και των συγχωνεύσεων έχει πάρει τεράστιες διαστάσεις και στο Ελληνικό τραπεζικό σύστημα.

Ο ανταγωνισμός σε παγκόσμιο επίπεδο εντείνεται καθημερινά, με αποτέλεσμα οι τράπεζες να επιδιώκουν συνεχώς να προσαρμόζονται στα νέα δεδομένα, και να στοχεύουν με τις ακολουθούμενες πολιτικές τους στην βελτίωση της αποδοτικότητάς τους.Έτσι, πολλές φορές για να ισχυροποιήσουν την ηγετική τους θέση στην Ελληνική αγορά, αλλά και να αποκτήσουν μερίδιο αγοράς σε αγορές του εξωτερικού (π.χ. Βαλκάνια) προβαίνουν σε διαδικασίες ενοποίησης (εξαγορές, συγχωνεύσεις, στρατηγικές συμμαχίες) εντός του κλάδου που δραστηριοποιούνται.

Στην Ελλάδα το τραπεζικό σύστημα αποτελείται από την Κεντρική Τράπεζα (Τράπεζα της Ελλάδος), τις εμπορικές τράπεζες, τις συνεταιριστικές τράπεζες και από διάφορους ειδικούς πιστωτικούς οργανισμούς. Η Τράπεζα της Ελλάδος που λειτουργεί ως η κεντρική Τράπεζα της χώρας, είναι μέλος του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών (ΕΣΚΤ) και πρωταρχικός της σκοπός είναι η επιδίωξη της σταθερότητας των τιμών. Είναι υπεύθυνη για την ομαλή λειτουργία της τραπεζικής αγοράς και είναι αυτή που εφαρμόζει την εκάστοτε νομισματική πολιτική που πρέπει να ακολουθηθεί.

Οι τράπεζες στην προσπάθειά τους να ανταποκριθούν στις απαιτήσεις του διεθνούς επιχειρηματικού περιβάλλοντος, εκτός από τις ακολουθούμενες στρατηγικές ενοποίησης (εξαγορές, συγχωνεύσεις, στρατηγικές συμμαχίες) εντός του κλάδου, αναπτύσσουν το εύρος των προσφερόμενων υπηρεσιών τους και γίνονται περισσότερο πελατοκεντρικές. Επίσης, συνεχώς βελτιώνουν την ποιότητα των προσφερόμενων τραπεζικών προϊόντων και υπηρεσιών τους, και βελτιώνουν την παραγωγικότητά τους μέσω αφού ολοένα και περισσότερο επενδύουν στη νέα τεχνολογία και στο ανθρώπινο δυναμικό.

Με την αξιοποίηση των λύσεων που προσφέρει η σύγχρονη τεχνολογία, επιταχύνονται οι καθημερινές διαδικασίες, μειώνεται ο χρόνος διεκπεραίωσης των συναλλαγών και δημιουργούνται ευέλικτες βάσεις δεδομένων που βοηθούν πολύπλευρα στην αποδοτικότητα της τράπεζας (π.χ. βοηθούν τα τμήματα μάρκετινγκ στην επίτευξη πωλήσεων). Στην ουσία, με την επίδραση της τεχνολογίας ολόκληρος ο τραπεζικός κλάδος μετασχηματίζεται, εφόσον δημιουργούνται νέα προϊόντα, διευκολύνεται η πρόσβαση σε νέες αγορές (με την εξάλειψη των γεωγραφικών ορίων), διακινείται λιγότερο χαρτί, υπάρχει καλύτερη διαχείριση των πληροφοριών κ.ο.κ.

Με την δημιουργία νέων καναλιών διανομής και πώλησης των τραπεζικών προϊόντων και υπηρεσιών, των λεγόμενων εναλλακτικών δικτύων (ATM' s, internet banking, phone banking, mobile banking) έχει επέλθει μια ολοκληρωτική επανάσταση στον τραπεζικό χώρο, ο οποίος πλέον είναι σε θέση να εξυπηρετήσει τους πελάτες 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα και 365 ημέρες τον χρόνο. Αν και διείσδυση της ηλεκτρονικής τραπεζικής (e-banking) στον Ελλαδικό χώρο, δεν ήταν αντίστοιχη με ορισμένες αναπτυγμένες χώρες του εξωτερικού (π.χ. Η.Π.Α., Σκανδιναβικές χώρες), παρ' όλα αυτά κρίνεται ικανοποιητική και με τάση αυξητική για το μέλλον. Αυτόματα συστήματα συναλλαγών (ATM) και διασύνδεση υποκαταστημάτων on-line είναι ήδη καθεστώς στις περισσότερες ελληνικές τράπεζες.

Απώτερος στόχος θα πρέπει να είναι η εκμετάλλευση του Διαδικτύου με σκοπό την επίτευξη της μέγιστης ποιότητας αλλά και πληρότητας των παρεχομένων υπηρεσιών on-line, γεγονός που οδηγεί σε μεγάλη εξοικονόμηση χρόνου και χρήματος. Στον τραπεζικό τομέα οι χρήστες αναζητούν νέους τρόπους συνεργασίας με την τράπεζα τους για τις καθημερινές συναλλαγές τους.

Το E-Banking δημιουργήθηκε για να προσφέρεται ακριβώς αυτό το εναλλακτικό κανάλι επικοινωνίας στους πελάτες τους.
Αρκετές στατιστικές μελέτες έχουν διεξαχθεί σχετικά με θέματα που άπτονται του E-Banking και η ανάλυση αυτών πιστοποιεί την ανάπτυξη αυτού του τομέα Ηλεκτρονικού Εμπορίου και κυρίως του Ηλεκτρονικού «Επιχειρείν».
Έτσι αν και για άλλη μια φορά η ανάλυση των στοιχείων αυτών των ερευνών καθιστούν ναι μεν τις Η.Π.Α. ,στην πρώτη θέση σχετικά με την αξιοποίηση εναλλακτικών δικτύων παροχής τραπεζικών προϊόντων και υπηρεσιών, θέτουν και την Ευρώπη ικανή να ακολουθεί από κοντά τις κινήσεις που πραγματοποιούνται στο χώρο του παγκόσμιου E-Banking.

Οι αλλαγές στο τραπεζικό σκηνικό της Ευρώπης και της Ελλάδας επηρεάζονται και από την καθιέρωση του Ευρώ, του ενιαίου νομίσματος της Ευρωπαϊκής Ένωσης, στο οποίο συμμετέχει και η χώρας μας από 01.01.2001 καθώς και από τις εξαγορές και τις συμμαχίες των τραπεζικών ομίλων.

*Συμπέρασμα:*

Οι κρίσιμοι παράγοντες από τους οποίους θα κριθεί η επιτυχημένη προσαρμογή των τραπεζών στη νέα τάξη πραγμάτων είναι:

- Η χάραξη ολοκληρωμένης στρατηγικής μάρκετινγκ
- Η ανάπτυξη του ανθρώπινου και τεχνολογικού δυναμικούΗ παροχή υπηρεσιών υψηλής ποιότητας.
- Η αποτελεσματική διαχείριση των οικονομικών.
- Η ανάπτυξη μεθόδων για την αποτελεσματικότερη μέτρηση των μεγεθών που την ενδιαφέρουν.
- Η χρησιμοποίηση των κατάλληλων καναλιών διανομής για την εξυπηρέτηση πελατών-στόχων.

# ΚΕΦΑΛΑΙΟ 2
# Ορισμός ηλεκτρονικής τραπεζικής.
# Σε ποιους απευθύνεται-Τι εμπεριέχει.

## 2.1. Ορισμός της ηλεκτρονικής τραπεζικής.
## *(E-Banking/web-banking).*

Ως ηλεκτρονική τραπεζική ορίζεται ουσιαστικά η πραγματοποίηση τραπεζικών συναλλαγών μέσω του διαδικτύου. Θα μπορούσαμε να πούμε ότι "Μεταφέρει" την ίδια την τράπεζα στην οθόνη του υπολογιστή μέσω διαδικτύου, με άμεση πρόσβαση στους τραπεζικούς λογαριασμούς, παρέχοντας τη δυνατότητα διεκπεραίωσης συναλλαγών,παρακολούθησης της πορείας χαρτοφυλακίων,εξόφλησης λογαριασμών ΔΕΚΟ και πιστωτικών καρτών, καθώς και πλήθος άλλων υπηρεσιών."

Οι τράπεζες - ελληνικές και ξένες - δεν είναι υποχρεωμένες να παρέχουν στους πελάτες τους υπηρεσίες ηλεκτρονικής τραπεζικής. Κατά συνέπεια μόνο ορισμένες προσφέρουν τέτοιες υπηρεσίες (πάντα κατόπιν σχετικής αίτησης) - αν και ο αριθμός των τραπεζών που επεκτείνεται στο διαδίκτυο αυξάνεται συνεχώς.
Το διαδίκτυο, παρέχοντας τη δυνατότητα αμφίδρομης επαφής μεταξύ ανθρώπων, επιχειρήσεων και οργανισμών, έχει ήδη μέρος της ζωής εκατομμυρίων πολιτών του πλανήτη μας και επηρεάζει ποικιλόμορφα πολλές από τις ανθρώπινες δραστηριότητες.

Αν και ξεκίνησε ως καθαρά επιστημονικό εργαλείο, σήμερα έχει μεταβληθεί σε παγκόσμιο ανοιχτό δίαυλο επικοινωνίας που διαμορφώνει μία νέα οικονομία.

Τα χαρακτηριστικά αυτής της αλλαγής, που πηγάζει κυρίως από τις τεχνολογίες των τηλεπικοινωνιών και της πληροφορικής, είναι ότι εξαπλώνεται με πολύ μεγάλη ταχύτητα, δεν γνωρίζει σύνορα, θρησκείες ή έθνη και γίνεται εύκολα και ευχάριστα αποδεκτή από τις νέες ηλικίες.

Οι καταναλωτικές, επενδυτικές και αποταμιευτικές συνήθειες των ανθρώπων αλλάζουν. Το ταμειακό μέρος κάθε εμπορικής πράξης μέσω διαδικτύου είναι λογικό να διεκδικείται σε πρώτη φάση από τον τραπεζικό τομέα, είτε αυτό αφορά πληρωμή μέσω τραπεζικού λογαριασμού είτε πληρωμή μέσω πιστωτικής κάρτας. Η πρόκληση είναι μεγάλη και ο χώρος αυτός αποτελεί στρατηγική επιλογή για τις χρηματοπιστωτικές επιχειρήσεις.

Οι τράπεζες ήταν από τους πρώτους οργανισμούς που ενέταξαν (ήδη από τη δεκαετία του ΄60) τους ηλεκτρονικούς υπολογιστές στο ΄΄οπλοστάσιο΄΄ τους. Στη δεκαετία του ΄90 η εξέλιξη του τραπεζικού τομέα ταυτίστηκε άμεσα με την ανάπτυξη της ηλεκτρονικής τραπεζικής με αποτέλεσμα τα τελευταία χρόνια να επέλθει ριζική μεταβολή στη σχέση πελάτη- τράπεζας.

Μέσω του E-Banking, ο τραπεζικός πελάτης βρίσκει την υποδομή που τον εξυπηρετεί στην εκτέλεση των συναλλαγών του ενώ ταυτόχρονα απολαμβάνει μια σειρά από νέα προϊόντα και μία μορφή προσωπικής εξυπηρέτησης , η οποία μπορεί να είναι άυλη, αλλά τον φέρνει μόνο μία οθόνη ή ένα τηλεφώνημα μακριά από τη τράπεζά του. Η επαφή του πελάτη με το τραπεζικό υπάλληλο γίνεται πλέον πιο ποιοτική, με συμβουλευτικό χαρακτήρα και όχι απλά εκτελεστικό.

Η χρήση της ηλεκτρονικής τραπεζικής, μέσω των καναλιών του internet banking, του phone banking και του mobile banking παρέχει άνεση και ταχύτητα στον πελάτη καθώς αυτός μπορεί πλέον να εκτελεί τις τραπεζικές και χρηματιστηριακές συναλλαγές του, όλο το 24ωρο, όλο το χρόνο, απ' όποιο σημείο του κόσμου κι αν βρίσκεται χρειάζεται είναι να εγγραφεί στην αντίστοιχη υπηρεσία της τράπεζας που επιθυμεί να λάβει τους προσωπικούς του κωδικούς, προκειμένου να μπορεί να εκτελεί τις συναλλαγές του μέσω σταθερού ή κινητού τηλεφώνου και μέσω Ίντερνετ.

## 2.2. Σε ποιους απευθύνεται η πληροφορική του τραπεζικού συστήματος / ηλεκτρονική τραπεζική.

Η υπηρεσία της ηλεκτρονικής τραπεζικής απευθύνεται σε όλους τους πελάτες των τραπεζών, δηλαδή σε φυσικά και νομικά πρόσωπα μέσα από τη συμπλήρωση μιας ηλεκτρονικής αίτησης.
Σκοπός των τραπεζών είναι όλο και περισσότεροι πελάτες να χρησιμοποιούν αυτή την υπηρεσία για τις τραπεζικές συναλλαγές τους.

Με τον τρόπο αυτό δίνεται η δυνατότητα στο δίκτυο να απαλλαγεί από συναλλαγές ρουτίνας μετατρέποντας παράλληλα το κατάστημα σε ένα συμβουλευτικό χώρο τραπεζικών προϊόντων και υπηρεσιών.

## 2.3. Τι περιέχει η πληροφορική στο τραπεζικό σύστημα.

Το E-Banking καλύπτει ένα σύνολο υπηρεσιών και προϊόντων, που παρέχουν τα πιστωτικά ιδρύματα (τράπεζες) μέσω εναλλακτικών ηλεκτρονικών δικτύων διανομής. Έτσι, πέρα από τη χρήση των ταμειολογιστικών μηχανών (ATMs) τα οποία έχουν εγκαταστήσει οι τράπεζες στα υποκαταστήματα τους, για την εξυπηρέτηση των πελατών τους.

Ο όρος E-Banking ενσωματώνει και τους όρους του Mobile Banking δηλαδή η πραγματοποίηση των ηλεκτρονικών τραπεζικών εργασιών μέσου του κινητού τηλεφώνου, του Internet Banking στο οποίο οι συναλλαγές γίνονται από την οθόνη οποιουδήποτε υπολογιστή και του Phone banking από όπου οι συναλλαγές γίνονται μέσω ενός τηλεφωνικού κέντρου που έχει δημιουργήσει η τράπεζα για την εξυπηρέτηση των πελατών της.

Το E-Banking παρέχει στον πελάτη δυνατότητες μέσω spreadsheets (λογιστικών φύλλων) και χρηματοοικονομικών προσομοιώσεων, να αυξήσει το κέρδος του, να υπολογίσει τα έσοδα και έξοδά του και να σχεδιάσει τη βελτίωση της οικονομικής του θέσης. Πάντως, όπως επισημαίνουν παράγοντες της τραπεζικής αγοράς, στο μέλλον οι υπηρεσίες της ηλεκτρονικής τραπεζικής θα είναι περισσότερο προσωποποιημένες, για να προσαρμόζονται στις ιδιαίτερες ανάγκες των πελατών.

Οι νέες τεχνολογίες των υπολογιστών, και ειδικότερα το Ίντερνετ, έχουν φέρει την επανάσταση στον τρόπο των συναλλαγών και γενικότερα, του τραπεζικού συστήματος.

Οι περισσότερες εταιρίες πληρώνουν τους υπαλλήλους μέσω τραπεζικών λογαριασμών, στέλνοντας μηχανογραφικές καταστάσεις απευθείας στις τράπεζες. Έτσι, αποφεύγονται οι άσκοπες μετακινήσεις και μεταφορές χρημάτων. Οι περισσότεροι διαθέτουν έναν λογαριασμό απ' όπου μπορούν να σηκώσουν το ποσό που χρειάζονται όποτε το θελήσουν.

Τα Α.Τ.Μ. απλούστευσαν, βέβαια, αυτή τη διαδικασία, αλλά και πάλι θα πρέπει να εγκαταλείψει κάποιος το σπίτι ή το γραφείο του και να βρει το πιο κοντινό μηχάνημα.Το Ίντερνετ έρχεται να δώσει λύση και σε αυτή την περίπτωση. Οι τραπεζικές συναλλαγές μέσω Ίντερνετ δεν διαφέρουν πολύ από τη χρήση των Α.Τ.Μ. Απλώς, τη θέση του περιορισμένων δυνατοτήτων Α.Τ.Μ. παίρνει το έξυπνο PC,το οποίο διαθέτει μεγαλύτερες δυνατότητες.

Στην οθόνη του υπολογιστή είναι δυνατόν κάποιος, από την άνεση του σπιτιού του, να πληροφορηθεί για τα υπόλοιπα και τους τόκους των λογαριασμών του, για τις εντολές και τις πληρωμές λογαριασμών, για τις τιμές συναλλάγματος και ξένων χαρτονομισμάτων και πολλά άλλα. Η επιλογή γίνεται μέσα από τις ιστοσελίδες της συγκεκριμένης διεύθυνσης, αφού έχει προηγηθεί η απαραίτητη πιστοποίηση και αφού το πρόγραμμα αναζήτησης έχει μπει σε περιβάλλον ασφαλούς μεταφοράς και ο χρήστης έχει πληκτρολογήσει τον κωδικό πρόσβασης.

Σημαντικό ρόλο στην εξάπλωση του E-Banking παίζει η παγκόσμια εδραίωση αποδεκτών προτύπων ασφάλειας, που έχει επιτευχθεί τα τελευταία χρόνια. Κατ' αυτόν τον τρόπο τόσο η τράπεζα όσο και ο τελικός χρήστης-πελάτης δε χρειάζεται να ανησυχούν για ενδεχόμενη διαρροή ΄΄ευαίσθητων΄΄ στοιχείων, όπως αριθμοί πιστωτικών καρτών ή λογαριασμών.

Παράλληλα, σημαντικό είναι το ότι στη συντριπτική πλειοψηφία των περιπτώσεων δεν υπάρχει κόστος χρησιμοποίησης των υπηρεσιών. Ουσιαστικά, υποστηρίζεται κάθε χαρακτηριστικό που δεν περιλαμβάνει ανάληψη χρημάτων, ενώ στην συντριπτική πλειοψηφία των περιπτώσεων οι εν λόγω υπηρεσίες παρέχονται σε εικοσιτετράωρη και καθημερινή βάση.

Οι κύριες υποστηριζόμενες λειτουργίες είναι οι ακόλουθες:Διαχείριση λογαριασμών, έλεγχος και πληρωμή πιστωτικών καρτών, πληρωμή λογαριασμών και Φ.Π.Α., διαχείριση χαρτοφυλακίου και χρήση επιταγών.Όλες αυτές μπορούμε να τις συναντήσουμε στις ιστοσελίδες των τραπεζών που προσφέρουν E-Banking.

## 2.4. Τι χρειάζεται για να χρησιμοποιήσει κάποιος την υπηρεσία της ηλεκτρονικής τραπεζικής (E-Banking)

1. Ένας υπολογιστής ή ένα κινητό τηλέφωνο με πρόσβαση στο Internet.

2. Άνοιγμα λογαριασμού στη τράπεζα.

3. Συμπλήρωση αίτησης για Web Banking.

4. Υπογραφή αίτησης.

5. Παραλαβή κωδικών PIN και TAN.

Κάθε πελάτης της υπηρεσίας μπορεί οποιαδήποτε στιγμή και από οποιοδήποτε σημείο της γης να έχει τη τράπεζα μαζί του χωρίς κανένα κόστος εγγραφής. Αυτά είναι τα απαραίτητα-εργαλεία-για να χρησιμοποιήσει κάποιος την υπηρεσία E-Banking.

## 2.5. Το κόστος μεταξύ απλής και ηλεκτρονικής τραπεζικής εξυπηρέτησης

1. Μέσω γκισέ:0,95 ευρώ

2. Μέσω τηλεφώνου:0,5 ευρώ

3. Μέσω ATM:0,23 ευρώ

4. Μέσω Internet:0,03 ευρώ

Η διαφορά των 0,92€ ανάμεσα στη διαδικασία του γκισέ και σε αυτή του Internet Banking είναι σαφής ένδειξη για την μορφή που θα πάρουν οι τραπεζικές εργασίες στο μέλλον.Επίσης δικαιολογεί και τις μεγάλες επενδύσεις των τραπεζών παγκοσμίως στις νέες τεχνολογίες. Οι τραπεζικές υπηρεσίες και γενικότερα οι χρηματοοικονομικές υπηρεσίες αλλάζουν μορφή με ιλιγγιώδης ρυθμούς.

Τα ηλεκτρονιδίκτυα και ιδιαίτερα το Internet, η ταχύτατη εξάπλωση της κινητ τηλεφωνίας και κυρίως η σύγκλιση κινητής τηλεφωνίας και Internet διαμορφώνουν ένα νέο ,πολύ πιο σύνθετο περιβάλλον για τις τραπεζικές υπηρεσίες αλλά και γενικότερα για όλους τους κλάδους υπηρεσιών.

*Συμπέρασμα:*

Οι τράπεζες συνειδητοποιούν σταδιακά τις δυνατότητες της επιχειρηματικής εκμετάλλευσης του μέσου. Ήδη έχει εμφανιστεί και προσαρμόζεται η ηλεκτρονική τραπεζική (E-Banking), δηλαδή η υλοποίηση τραπεζικών συναλλαγών από απόσταση με χρήση εναλλακτικών καναλιών επικοινωνίας μεταξύ τράπεζας και πελάτη, που βασίζονται στη σύγχρονη τεχνολογές Έτσι σήμερα δημιουργείται διεθνώς μία κρίσιμη μάζα χρηστών χρηματοπιστωτικών υπηρεσιών μέσω διαδικτύου.Αντίστοιχα διαμορφώνονται συναλλακτικά ήθη και πρότυπα καταναλωτικής συμπεριφοράς. Με λίγα λόγια το E-banking (ή Internet banking) υπόσχεται την επανάσταση στις τραπεζικές συναλλαγές.

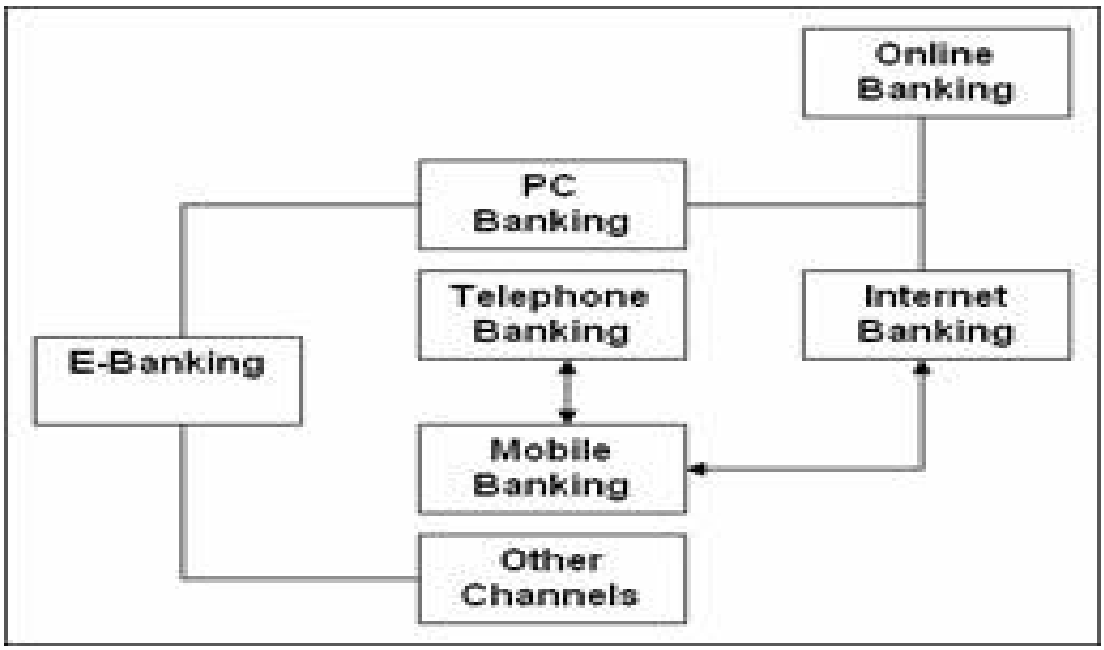
# ΚΕΦΑΛΑΙΟ 3

## Είδη ηλεκτρονικών τραπεζικών συναλλαγών και ηλεκτρονικά κανάλια διανομής.

## 3.1 Είδη διεκπεραίωσης συναλλαγών της ηλεκτρονικής τραπεζικής.

Είναι φανερό πως οι βάσεις για το remote banking (τραπεζική εξυπηρέτηση από απόσταση) έχουν ήδη μπει.

Τα δίκτυα που θα απαρτίσουν αυτή την εξυπηρέτηση «νέας γενιάς»είναι τα κέντρα τηλεφωνικής υποστήριξης (call centre),τα ATM, τα κέντρα εξυπηρέτησης μέσω Διαδικτύου (internet banking) η ηλεκτρονική διαβίβαση εντολών για αγοραπωλησίες μετόχων, η χρήση γραπτών μηνυμάτων μέσω κινητού τηλεφώνου, οι ηλεκτρονικές




πληρωμές με πιστωτική κάρτα μέσω Internet κ.τ.λ.

Η ηλεκτρονική τραπεζική (electronic banking ή E-Banking) χωρίζεται σε διάφορα είδη, σύμφωνα με το μέσο ή κανάλι, μέσω του οποίου πραγματοποιούνται οι τραπεζικές συναλλαγές. Η πραγματοποίηση αγορών αλλά και η διεκπεραίωση τραπεζικών συναλλαγών μέσω διαδικτύου μπορεί να γίνει με διάφορους τρόπους.

Οι τρόποι αυτοί είναι οι εξής:

### 3.1.1. Internet Banking
### (Τραπεζικές υπηρεσίες μέσω διαδικτύου).

Το“Internet Banking” που αποτελεί το σημαντικότερο κομμάτι του E-Banking, πραγματοποιείται κατά κύριο λόγο μέσω του διαδικτύου, αλλά και μέσω άλλων δικτύων όπως εσωτερικών ή εξωτερικών (Intranets ή Extranets).
Για να μπορέσει ένας χρήστης να χρησιμοποιήσει τις υπηρεσίες του, χρειάζεται απαραίτητα να διαθέτει έναν ηλεκτρονικό υπολογιστή και μια σύνδεση στο διαδίκτυο. Στην πλειονότητα των περιπτώσεων, τα παραπάνω αρκούν για την πρόσβαση στις ηλεκτρονικές υπηρεσίες, ωστόσο για λόγους μεγαλύτερης ασφάλειας, πολλές φορές απαιτούνται και ορισμένες συσκευές ασφάλειας, όπως έξυπνοι αναγνώστες ή ειδικό λογισμικό ασφάλειας (software) τα οποία τα παρέχουν οι τράπεζες στους πελάτες τους. Μέσω του “internet banking” ο πελάτης έχει τη δυνατότητα να επιλέξει ανάμεσα σε μια μεγάλη ποικιλία τραπεζικών υπηρεσιών.

Αξίζει να αναφέρουμε ότι τα χρηματοπιστωτικά ιδρύματα έχουν την τεχνογνωσία να προσωποποιούν τις προσφερόμενες ηλεκτρονικές υπηρεσίες τους, ανάλογα με την κατηγορία των πελατών που αυτές προορίζονται. Για παράδειγμα, σε εταιρικούς πελάτες, δηλαδή επιχειρήσεις, προσφέρονται περισσότερες δυνατότητες ηλεκτρονικών συναλλαγών, οι οποίες είναι ειδικά προσαρμοσμένες.

### 3.1.2. Phone Banking- Call Centre
### (Τραπεζικές υπηρεσίες μέσω τηλεφώνου).

Τα τελευταία χρόνια δίνεται μεγάλη έμφαση στη χρήση της τηλεφωνικής συσκευής για τη διανομή των τραπεζικών υπηρεσιών. Ανήκει στις υπηρεσίες του remote banking. Δηλαδή τις υπηρεσίες που προσφέρονται μέσω ηλεκτρονικών συσκευών οι οποίες συνδέονται με τα πληροφοριακά συστήματα των τραπεζών.

Η εισαγωγή στην αγορά των τηλεφωνικών συσκευών με οθόνη δίνει τη δυνατότητα στους συναλλασσόμενους της άμεσης πληροφόρησης σχετικά με μετοχές, ομόλογα, αμοιβαία κεφάλαια και ασφάλειες. Επειδή οι συγκεκριμένες συσκευές είναι ακριβές δεν έχουν καθιερωθεί ακόμη στην αγορά. Ελπίζεται ότι στο μέλλον οι εξελίξεις στην τεχνολογία σε αυτόν το χώρο θα επιτρέψουν τη μείωση του κόστους παραγωγής και την καθιέρωση τους στην αγορά.

Αν αυτά τα συστήματα συνδεθούν με το τμήμα μάρκετινγκ της τράπεζας θα αποτελέσουν τη βάση για ικανοποιητική αύξηση της πελατείας της.
Οι υπηρεσίες αυτές προσφέρονται είτε μέσα από ιδιωτικά δίκτυα που έχουν οι τράπεζες είτε μέσω κοινόχρηστων δικτύων που λειτουργούν σε όλες τις χώρες. Στην περίπτωση της τηλεφωνικής εξυπηρέτησης χρησιμοποιείται το τηλεφωνικό δίκτυο και μικρές συσκευές που κωδικοποιούν - αποκωδικοποιούν τα στοιχεία που ζητά ο χειριστής τους.

Οι υπηρεσίες που προσφέρει το “phone banking” χωρίζονται σε δύο κατηγορίες.

α) Αυτές που διεκπεραιώνονται από πράκτορες τηλεφωνικών κέντρων (call center agents) και

β) Αυτές που διεκπεραιώνονται αυτόματα μέσω ειδικών συστημάτων αναγνώρισης της φωνής (IVRs).

Και στις δύο περιπτώσεις το μόνο που απαιτείται από την πλευρά του πελάτη, είναι η ύπαρξη μιας τηλεφωνικής συσκευής και σύνδεσης.

Στις τραπεζικές συναλλαγές με πράκτορες τηλεφωνικών κέντρων, ο υπάλληλος της τράπεζας αρχικά ζητά από τον πελάτη κάποια στοιχεία ταυτοποίησης και επαλήθευσης, όπως ένας προσωπικός κωδικός αριθμός (Pin).

Αφού ο πελάτης δώσει σωστά αυτόν τον προσωπικό κωδικό, ο οποίος χρησιμοποιείται μόνο για τις συναλλαγές μέσω “phone banking” και όχι για άλλες συναλλαγές (π.χ. internet banking, ATMs), στη συνέχεια ο υπάλληλος του τηλεφωνικού κέντρου διεκπεραιώνει τις συναλλαγές που θα του υποδείξει ο πελάτης.
Αντίστοιχη είναι και η δεύτερη κατηγορία του phone banking, με τη μόνη διαφορά ότι στην άλλη άκρη της τηλεφωνικής γραμμής δεν είναι ένας υπάλληλος της τράπεζας, αλλά ένας υπολογιστής ή καλύτερα ένα αυτοματοποιημένο σύστημα αναγνώρισης της φωνής IVR (Interactive Voice Response).

Έτσι, η συγκεκριμένη διαδικασία είναι πλήρως αυτοματοποιημένη και ο πελάτης απαντά στα φωνητικά μηνύματα που ακούει.Όλες οι συνδιαλέξεις είτε μέσω μηχανήματος που ενεργοποιείται μέσω της φωνής, είτε μέσω υπαλλήλου της τράπεζας ανάλογα με το σύστημα που εφαρμόζει η κάθε τράπεζα, ηχογραφούνται για την ασφάλεια τόσο του πελάτη όσο και της τράπεζας.

Οι συναλλαγές μέσω τηλεφώνου μειώνουν τα τραπεζικά έξοδα και παράλληλα δίνουν τη δυνατότητα στον υπάλληλο που είναι αρμόδιος για αυτού του είδους τις συναλλαγές να εκμεταλλεύεται ευκαιρίες για διασταυρούμενες πωλήσεις τραπεζικών υπηρεσιών στην περίπτωση που πελάτες τηλεφωνούν για να ενημερωθούν για λοιπά τραπεζικά προϊόντα και υπηρεσίες. Σε περίπτωση που η τηλεφωνική εξυπηρέτηση γίνεται μέσω μηχανήματος υπάρχει η δυνατότητα ανταλλαγής στοιχείων που θα αποτελέσουν πολύτιμες πληροφορίες για πιθανή μελλοντική συνεργασία της τράπεζας με τον πελάτη.

Μέσω του “phone banking”, ο χρήστης του, δηλαδή ο πελάτης μιας τράπεζας έχει στη διάθεσή του πάρα πολλές τραπεζικές υπηρεσίες είτε σε επίπεδο πληροφόρησης, είτε σε επίπεδο οικονομικών συναλλαγών γενικότερα. Επιπλέον τους δίνεται η ευκαιρία να εντοπίσουν τους πελάτες που ενδιαφέρονται για νέες υπηρεσίες και προϊόντα. Πιό συνοπτικά, η τηλεφωνική εξυπηρέτηση δίνει τη δυνατότητα στις τράπεζες να μειώσουν το λειτουργικό τους κόστος μεταφέροντας τις απλές συναλλαγές από το γκισέ στο τηλέφωνο και παράλληλα να δημιουργήσουν ανταγωνιστικό πλεονέκτημα κτίζοντας την εικόνα της προοδευτικής πελατοκεντρικής τράπεζας.

### 3.1.3 Αυτόματες ταμειολογιστικές μηχανές AEMs. (Automatic Excange Machines)

Μέσω του δικτύου αυτού, μπορεί να γίνει αυτόματη συναλλαγματική συναλλαγή. Οι μηχανές αυτές ενεργοποιούνται με τη μαγνητική λωρίδα της κάρτας μετρητών (Cashcard) και τηνπληκτρολόγηση του προσωπικού κωδικού αριθμού του πελάτη.

### 3.1.4 Αυτόματες ταμειολογιστικές μηχανές ATMs. (Automatic Teller Machines )

Η Ηλεκτρομηχανική συσκευή που επιτρέπει στους εξουσιοδοτημένους χρήστες, με τη χρήση ειδικών πλαστικών καρτών, να αναλαμβάνουν μετρητά από τον λογαριασμό τους ή/και να έχουν πρόσβαση σε άλλες υπηρεσίες, όπως ερωτήσεις σχετικά με το υπόλοιπο λογαριασμού, μεταφορά κεφαλαίων.Οι αυτόματες ταμειολογιστικές μηχανές λειτουργούν είτε με άμεση σύνδεση (on-line) σε μία εξουσιοδοτημένη βάση δεδομένων, είτε με μεταγενέστερη σύνδεση (off-line).

Μέσω του δικτύου αυτού, μπορούν να γίνουν οι παρακάτω συναλλαγές:

- Ανάληψη και κατάθεση μετρητών.
- Μεταφορές ποσών από λογαριασμό σε λογαριασμό.
- Ενημέρωση για το υπόλοιπο λογαριασμών.
- Ανάληψη μετρητών με πιστωτική κάρτα.
- Πληρωμή λογαριασμών πιστωτικών καρτών.
- Πληρωμή καταναλωτικών δανείων.
- Πληρωμή λογαριασμών ΔΕΗ, ΟΤΕ και ύδρευσης.

Οι μηχανές αυτές προσφέρουν τη δυνατότητα στις τράπεζες να περιορίσουν τον αριθμό των συναλλαγών στα γκισέ όσο και το λειτουργικό τους κόστος, ενώ παράλληλα να διευρύνουν το δίκτυο διανομής των υπηρεσιών τους σε περιοχές που παρουσιάζουν συναλλακτικό ενδιαφέρον, όπως αεροδρόμια εμπορικά πολυκαταστήματα, πανεπιστήμια Super Markets, νοσοκομεία ξενοδοχεία, οργανισμούς κοινής ωφέλειας κ.α.

Από την πλευρά των τραπεζών η διεύρυνση του δικτύου διανομής τους με την εγκατάσταση ATMs σε χώρους εκτός τραπεζικών καταστημάτων επιτρέπει στις τράπεζες να μειώσουν το λειτουργικό τους κόστος και παράλληλα να αυξήσουν την πελατεία τους μέσω της ενίσχυσης του γοήτρου της.

### 3.1.5 Μηχανήματα Ηλεκτρονικής Μεταφοράς Κεφαλαίων (Electronic Funds Transfer at the Point of Sales-E.F.T.P.O.S.)

Τα μηχανήματα αυτά τοποθετούνται σε εμπορικά καταστήματα, πρατήρια, διόδια κτλ και με την χρήση μιας χρεωστικής; κάρτας διενεργούν αυτόματα, αντί την χρήση μετρητών ή επιταγών, την χρέωση του λογαριασμού του χρήστη με την αντίστοιχη πίστωση του λογαριασμού του τραπεζικού καταστήματος με το σύνολο της αξίας των αγορών.

Το E.FTP.O.S. είναι ένας από τους ταχύτερα αναπτυσσόμενους τομείς ηλεκτρονικών πληρωμών στην Ελλάδα. Τα πρώτα βήματα στην ελληνική αγορά έγιναν από την Εθνική Τράπεζα σε συνεργασία με την Εμπορική και το Diners Club με την σύσταση ενός κοινού δικτύου συσκευών EFTPOS με σκοπό την εξυπηρέτηση των πελατών που διαθέτουν πιστωτικές και χρεωστικές κάρτες.

Η τεχνολογία που καλύπτει τα EFTPOS δεν αφορά μόνο τις πιστωτικές κάρτες αλλά και κάθε τύπο κάρτας και ιδιαίτερα την αναπτυσσόμενη τεχνολογία των «έξυπνων καρτών». Ο ρυθμός εγκατάστασης τέτοιων συσκευών αυξάνεται με ταχύτατους ρυθμούς δημιουργώντας ένα ευρύτατο δίκτυο ηλεκτρονικών συναλλαγών. Σε αυτήν την περίπτωση τα πλεονεκτήματα για τον πελάτη είναι η ταχύτερη και ασφαλέστερη εξυπηρέτηση γιατί ελαχιστοποιείται το απαραίτητο ελάχιστο ποσό μετρητών που έχει μαζί του ο πελάτης.

Επιπλέον του παρέχεται ηλεκτρονική δυνατότητα να αντλεί κεφάλαια για τις συναλλαγές του χωρίς να είναι υποχρεωμένος να πηγαίνει συνέχεια στην τράπεζα και παράλληλα να εκμεταλλεύεται αποδοτικά τα χρήματα της κατάθεσης του μέχρι την στιγμή της αγοράς. Από την πλευρά των τραπεζών τα πλεονεκτήματα σχετίζονται με την μείωση του λειτουργικού κόστους και τη διατήρηση των καταθέσεων των πελατών στην τράπεζα μια και τα ποσά για τις πληρωμές μετατοπίζονται από το λογαριασμό ενός πελάτη της στο λογαριασμό άλλου πελάτη της. Το σύστημα έχει σχεδιαστεί και αναπτυχθεί από τη ΔΙΑΣ και τις τράπεζες σε συνεργασία με το Υπουργείο Οικονομικών με σκοπό να εκσυγχρονίσει τον υφιστάμενο τρόπο πληρωμής των πάσης φύσεως οικονομικών υποχρεώσεων των φορολογουμένων στις Δ.Ο.Υ., μέσω χρήσης πιστωτικών ή χρεωστικών καρτών.

*Συμπέρασμα:*Οι υπηρεσίες της ηλεκτρονικής τραπεζικής μπορούν να πραγματοποιηθούν μέσα από τα διάφορα είδη ηλεκτρονικής τραπεζικής που χάρις την εξέλιξη της τεχνολογίας χρόνο με το χρόνο βελτιώνονται και προσφέρουν εύκολη πρόσβαση στις συναλλαγές λόγω των προσιτό για το χρήστη προγραμμάτων. Επίσης μέσα από τη δημιουργία του διατραπεζικού συστήματος ΔΙΑΣ, με το οποίο οι τράπεζες συνεργάζονται μεταξύ τους μέσω ενός κοινού προγράμματος, ο χρήστης μπορεί να πραγματοποιεί τις συναλλαγές του από οποιαδήποτε τράπεζα με ευκολία και σε ελάχιστο χρονικό διάστημα τις συναλλαγές του.

# ΚΕΦΑΛΑΙΟ 4

# Κάρτες ηλεκτρονικών τραπεζικών συναλλαγών.

Οι τράπεζες προσφέρουν τρία βασικά είδη καρτών για συναλλαγές: τις πιστωτικές, τις χρεωστικές και τις προπληρωμένες κάρτες ηλεκτρονικών τραπεζικών συναλλαγών.


## 4.1. Πιστωτικές κάρτες (credit cards).

Είναι κάρτες οι οποίες παρέχουν στον κάτοχό τους επέκταση πίστωσης (πιστωτικό όριο). Επιτρέπει στον κάτοχο να προβεί σε αγορές και/ή να αναλαμβάνει μετρητά ύψους ενός προκαθορισμένου ποσού. Ο διακανονισμός της πίστωσης μπορεί να λάβει χώρα στο τέλος μίας συγκεκριμένης περιόδου ή τμηματικά, οπότε το εναπομείναν υπόλοιπο θεωρείται ως επέκταση πίστωσης. Το ποσό της επέκτασης πίστωσης επιβαρύνεται με τόκο. Ο κάτοχος της κάρτας επιβαρύνεται συνήθως με ετήσια συνδρομή. Το βασικό μειονέκτημα (ενίοτε θεωρείται και πλεονέκτημα) των πιστωτικών καρτών είναι ότι επιτρέπουν την υπερανάληψη χρημάτων. Δηλαδή, μπορεί να έχει κάποιος μηδενικό υπόλοιπο και να βρεθεί ξαφνικά χρεωμένος π.χ. με 1000 ευρώ. Η απόκτηση μιας πιστωτικής κάρτας προϋποθέτει το άνοιγμα ενός καταθετικού λογαριασμού (π.χ. ταμιευτηρίου).

Στη συνέχεια, ακολουθεί η συμπλήρωση μιας αίτησης από τον πελάτη, ο οποίος παραθέτει τα απαραίτητα έγγραφα. Ακολουθεί ένα μικρό χρονικό διάστημα, συνήθως 1-2 ημερών μέχρι να επεξεργαστούν τα στοιχεία ώστε να υπάρξει απάντηση από τα κεντρικά, για το αν η πιστωτική κάρτα εγκρίθηκε καθώς και για το διαθέσιμο υπόλοιπο που μπορεί να δωθεί στο συγκεκριμένο πελάτη αντίστοιχα. Μετά την έγκριση της πιστωτικής κάρτας, οι περισσότερες τράπεζες τις στέλνουν στο σπίτι του πελάτη 1-2 εβδομάδες μετά το άνοιγμα του λογαριασμού, ενώ άλλες τις παραδίδουν χέρι-χέρι στον πελάτη κατά την προσέλευση του σε τοπικό υποκατάστημα μετά από συμφωνία πελάτη-τράπεζας.

## 4.2 Χρεωστικές κάρτες (debit cards)

Σε αντίθεση με τις πιστωτικές, ο κάτοχος μιας χρεωστικής κάρτας για να χρησιμοποιηθεί για συναλλαγές θα πρέπει εκ των προτέρων να διαθέτει η κάρτα το χρηματικό υπόλοιπο που απαιτείται για μια αγορά.

Τα βασικά πλεονεκτήματα (ενίοτε και μειονεκτήματα) της χρεωστικής είναι δύο:

1. Δεν υπάρχει περίπτωση ο κάτοχος να βρεθεί υπερχρεωμένος καθότι δεν υπάρχει δικαίωμα υπερανάληψης για αυτές τις κάρτες.

2. Δεν υπάρχει περίπτωση ο κάτοχος να πληρώσει ποτέ τόκους καθώς πληρώνει πάντα κατά τη στιγμή της αγοράς.

Η απόκτηση μιας χρεωστικής κάρτας προϋποθέτει το άνοιγμα ενός καταθετικού λογαριασμού (π.χ. Ταμιευτηρίου). Μετά το άνοιγμα του λογαριασμού ακολουθεί η σύνδεση της κάρτας με αυτόν. Το διαθέσιμο υπόλοιπο της χρεωστικής κάρτας ισούται πρακτικά με το διαθέσιμο υπόλοιπο αυτού του λογαριασμού κάθε στιγμή. Για το άνοιγμα ενός καταθετικού λογαριασμού πολλές τράπεζες απαιτούν την κατάθεση ενός αρχικού ελάχιστου χρηματικού ποσού, άλλες πάλι όχι.

Διαφοροποίηση παρατηρείται και στο χρόνο παράδοσης των χρεωστικών καρτών από τις τράπεζες στον πελάτη τους. Οι περισσότερες τις στέλνουν στο σπίτι του πελάτη 1-2 εβδομάδες μετά το άνοιγμα του λογαριασμού, ενώ άλλες τις παραδίδουν χέρι-χέρι στον πελάτη κατά την προσέλευση του σε τοπικό υποκατάστημα για άνοιγμα λογαριασμού.

Σε κάθε περίπτωση η κάρτα που αποκτά ο χρήστης μπορεί να χρησιμοποιηθεί για αναλήψεις από ΑΤΜ είτε της συγκεκριμένης τράπεζας (δωρεάν) είτε άλλων τραπεζών μέσω του διατραπεζικού συστήματος ΔΙΑΣ (με χρέωση).

Όσον αφορά τις αγορές μέσω διαδικτύου, δεν είναι όλες οι χρεωστικές κάρτες εξίσου συμβατές με όλες τις online υπηρεσίες και επιχειρήσεις. Δυστυχώς, η ένδειξη Visa Electron σε μια κάρτα δεν αποτελεί αποδεικτικό πλήρους συνεργασίας της με όλα τα διαδικτυακά συστήματα πληρωμών.

Σημαντικό ρόλο σε αυτό το σημείο παίζουν οι εκάστοτε συμφωνίες που έχουν συνάψει οι τράπεζες με διάφορες επιχειρήσεις και οργανισμούς.
Πέρα από τις καθαρά καταναλωτικές αγορές, οι εν λόγω κάρτες μπορούν να χρησιμοποιηθούν και για την πληρωμή διαφόρων τακτικών λογαριασμών (ΦΠΑ, ΙΚΑ/ΟΑΕΕ, ΔΕΗ, ΟΤΕ, ΕΥΔΑΠ) και συνδρομών σε υπηρεσίες (σταθερής & κινητής τηλεφωνίας, Ίντερνετ, NOVA κ.α.) είτε ατελώς είτε με ελάχιστο κόστος (ανάλογα με τη συμφωνία που έχει προηγηθεί μεταξύ της τράπεζας και του οργανισμού / επιχείρησης).

### 4.1.3 Προπληρωμένες κάρτες (prepaid cards)

Ο κάτοχος μιας προπληρωμένης κάρτας, όπως και ο κάτοχος μιας χρεωστικής κάρτας. Για να χρησιμοποιηθεί για συναλλαγές θα πρέπει εκ των προτέρων να διαθέτει η κάρτα το χρηματικό υπόλοιπο που απαιτείται για μια αγορά.

- Δεν υπάρχει περίπτωση ο κάτοχος να πληρώσει ποτέ τόκους καθώς πληρώνει πάντα κατά τη στιγμή της αγοράς.

- Δεν υπάρχει περίπτωση ο κάτοχος να βρεθεί υπερχρεωμένος καθότι δεν υπάρχει δικαίωμα υπερανάληψης για αυτές τις κάρτες.

Τα βασικά μειονεκτήματα είναι ότι:

- Σε μερικές τράπεζες είναι ότι υπάρχει δυνατότητα επαναφόρτισης μόνο μέσω του ταμείου της τράπεζας.

- Κάθε φορά που κάνει κάποιος μια συναλλαγή η τράπεζα τον χρεώνει ένα ποσό (π.χ. 1-3 ευρώ) ως προμήθεια.

Σύμφωνα με πρόσφατη έρευνα της τράπεζας Κύπρου το σημερινό κόστος έναρξης λειτουργίας ενός μεγάλου τραπεζικού υποκαταστήματος είναι περίπου 880.410,86 € ενώ για ένα μικρό υποκατάστημα είναι περίπου 293.407,29 €.Επίσης τα ετήσια έξοδα ενός μεγάλου καταστήματος κυμαίνονται περίπου στα 693.000€ ενώ ενός μικρού 235.650 € ετησίως. Αυτά τα ποσά είναι σημαντικότατα ακόμα και για τους υψηλούς τραπεζικούς προϋπολογισμούς. Με την αύξηση των ηλεκτρονικών δικτύων, εκτός από το μέγεθος των καταστημάτων θα επηρεαστεί και η κερδοφορία των τραπεζών, τουλάχιστον μακροπρόθεσμα.

Βραχυπρόθεσμα θα υπάρξουν απώλειες εσόδων των τραπεζών καθώς με την καθιέρωση του Ευρώ ως κοινό νόμισμα οι συναλλαγές συναλλάγματος περιορίζονται στο ελάχιστο. Το ίδιο θα συμβεί σταδιακά και με το Διεθνές Εμπόριο (εισαγωγές-εξαγωγές) καθώς δεν θα χρειάζεται η διαμεσολάβηση των τραπεζών για τις εμπορικές συναλλαγές.

*Συμπέρασμα:*

Όπως διαπιστώνουμε, υπάρχουν πολλοί τρόποι με τους οποίους μπορεί κάποιος να πραγματοποιήσει ηλεκτρονικές τραπεζικές συναλλαγές.Αυτό γίνεται μέσα από τη χρήση πιστωτικών, χρεωστικών ή προπληρωμένων καρτών. Ο τρόπος απόκτησής τους είναι απλός, οικονομικός και σχεδόν καθόλου χρονοβόρος πάντα σε σχέση με τον παραδοσιακό τρόπο πραγματοποίησης των συναλλαγών.

# ΚΕΦΑΛΑΙΟ 5
# Πλεονεκτήματα - Μειονεκτήματα – Ανασταλτικοί παράγοντες E-Banking

## 5.1 Πλεονεκτήματα χρήσης E-Banking

Τα πλεονεκτήματα από τη χρήση του E-Banking, έχουν να κάνουν με το κόστος και το χρόνο. Οι ηλεκτρονικές συναλλαγές γίνονται απλά μέσω του ηλεκτρονικού υπολογιστή, χωρίς ανάγκη μετακίνησης και με αποφυγή της γραφειοκρατίας και της “ουράς”.

Οι πιο συχνές υπηρεσίες που προσφέρονται διαδικτυακά είναι η ενημέρωση για την κίνηση λογαριασμών, η μεταφορά χρημάτων μεταξύ λογαριασμών, η πληρωμή λογαριασμών και πιστωτικών καρτών.

Πρόσφατα δόθηκε η δυνατότητα καταβολής ΦΠΑ μόνο όμως σε όσους υποβάλλουν με τον ίδιο τρόπο φορολογική δήλωση. Πρέπει να σημειωθεί ότι σε πολλές τραπεζικές εργασίες απαιτείται η “φυσική” υπογραφή του πελάτη, όπως για παράδειγμα στα δάνεια, ώστε να μην είναι δυνατή η διάθεσή τους μέσω Internet.

### 5.1.1 Πλεονεκτήματα που αφορούν το κόστος και το χρόνο.

1. Οι ηλεκτρονικές συναλλαγές γίνονται απλά μέσω του ηλεκτρονικού υπολογιστή, χωρίς ανάγκη μετακίνησης και με αποφυγή της γραφειοκρατίας και της “ουράς”.

2. Οι πελάτες (ιδιώτες και επιχειρήσεις) ωφελούνται σημαντικά από τη χρήση των υπηρεσιών E-Banking, καθώς τους παρέχεται η δυνατότητα να διεκπεραιώνουν ένα μεγάλο μέρος των συναλλαγών τους με την τράπεζα εύκολα, γρήγορα και με ασφάλεια 24 ώρες το 24ωρο, 365 μέρες το χρόνο.

3. Για τις ΜΜΕ το όφελος είναι ακόμη μεγαλύτερο, καθώς περιορίζεται το κόστος λειτουργίας τους όσον αφορά σε λειτουργικά έξοδα, προμήθειες και κινδύνους απώλειας χρήματος, ενώ παράλληλα εξοικονομείται πολύτιμος χρόνος.

4. Με το E-Banking οι τραπεζικές υπηρεσίες προσφέρονται ανά πάσα στιγμή, ο δε καταναλωτής μπορεί να ενημερωθεί για κάθε προϊόν ή υπηρεσία ανέξοδα και χωρίς χρόνους αναμονής.

5. Συχνό είναι και το φαινόμενο των προσφορών ή της εφαρμογής ευνοϊκότερων όρων στην παροχή προϊόντων μέσω Internet, γεγονός που από μόνο του είναι ικανό να προσελκύσει σημαντική μερίδα καταναλωτών που αναζητούν προσφορές.

### 5.1.2 Πλεονεκτήματα για τους πελάτες

- Αποδέσμευση από το ωράριο. Ο πελάτης δεν είναι υποχρεωμένος να πραγματοποιήσει τις συναλλαγές του όταν τα καταστήματα των τραπεζών είναι ανοιχτά.

- Αποφυγή της προσέλευσης στο κατάστημα αφού οι συναλλαγές του γίνονται και από το σπίτι ή το γραφείο του.

- Περισσότερος ελεύθερος χρόνος αφού το μόνο που έχει να κάνει είναι να συνδεθεί με το Internet.

- Περισσότερη ευελιξία και άνεση.

- Αποφυγή της γραφειοκρατίας. Μπροστά στην οθόνη του υπολογιστή του βρίσκονται πολλές από τις εργασίες που μπορεί να πραγματοποιήσει.

- Ποιότητα και αξιοπιστία στις συναλλαγές.

- Γρήγορη εξυπηρέτηση.

### 5.1.3 Πλεονεκτήματα για τις επιχειρήσεις

• Αποδέσμευση από ωράριο

• Μείωση του κόστους εφόσον οι συναλλαγές μπορούν να γίνουν σε λιγότερο χρόνο. Έτσι δεν απασχολούνται υπάλληλοι για παραπάνω εργασία.

• Διευκόλυνση επαφών μεταξύ επιχειρήσεων. Μέσω της άμεσης εκτέλεσης των εργασιών που έχουν συμφωνηθεί μεταξύ των επιχειρήσεων δημιουργείται ένα κλίμα εμπιστοσύνης.

• Ποιότητα και αξιοπιστία στις συναλλαγές.

• Γρήγορη εξυπηρέτηση. Το on-line banking (οι ηλεκτρονικές συναλλαγές που γίνονται σε πραγματικό χρόνο) παρέχει στην τράπεζα που αποφασίζει να επενδύσει σε αυτό σημαντικά οφέλη:

- Αποκτά ένα συμπληρωματικό δίκτυο για την προσέγγιση πελατών, αφού δεν απαιτείται η φυσική παρουσία του πελάτη στο κατάστημα και άρα η ύπαρξη φυσικού δικτύου της τράπεζας.
- Στρέφει ένα μέρος του ανθρώπινου δυναμικού της σε εργασίες όπου η «προσωπική επαφή» είναι απαραίτητη, π.χ. σε συμβουλευτικές υπηρεσίες και πωλήσεις προς τους πελάτες.

- Μειώνει το λειτουργικό κόστος της, δεδομένου ότι οι συναλλαγές μέσω Internet έχουν πολύ χαμηλότερο κόστος και από τις συναλλαγές στο κατάστημα (υπολογίζεται ότι το κόστος μπορεί να μειωθεί από 1% έως 25%) αλλά και από τις συναλλαγές στο ATM ή στο τηλέφωνο μέσω phone banking.
  Επιπλέον, λόγω του μικρότερου κόστους, η τράπεζα έχει τη δυνατότητα να προσφέρει στους πελάτες της προϊόντα/υπηρεσίες με χαμηλότερα επιτόκια / υψηλότερους τόκους κλπ.
- Αποκτά πρόσβαση στο κοινό μιας ευρύτερης γεωγραφικά περιοχής, εκτός των στενών εθνικών συνόρων.

## 5.2 Μειονεκτήματα χρήσης E-Banking

Είναι γεγονός ότι το Internet banking παρόλο που αναμφισβήτητα παρουσιάζει πολλά πλεονεκτήματα τόσο για τους χρήστες όσο και για την τράπεζα, έχει και αρκετά μειονεκτήματα.

Ένα κρίσιμο και πολυσυζητημένο μειονέκτημα είναι η έλλειψη απόδειξης και υπογραφής στη πραγματοποίηση των τραπεζικών συναλλαγών καθώς έτσι δεν υπάρχει μεγάλη ασφάλεια.

Το θέμα της ασφάλειας είναι τεράστιο και αρκετοί πελάτες των τραπεζών εμφανίζονται ιδιαίτερα δύσπιστοι ως προς την εξασφάλιση της διαφάνειας και της ασφάλειας στη πραγματοποίηση των συναλλαγών τους μέσω διαδικτύου καθώς δεν αισθάνονται ιδιαίτερα προστατευμένοι.

Έχουν καταγραφεί κατά καιρούς σε διάφορες έρευνες που πραγματοποιήθηκαν παγκοσμίως για το θέμα της ασφάλειας διάφορα γεγονότα, όπως χρέωση λογαριασμού πελάτη από παραδρομή λόγω τεχνικού λάθους ή βλάβης, μη αποδοχή από πελάτη κακής πίστης μιας χρέωσης του λογαριασμού του που είναι ορθή και νόμιμη, ακάλυπτες πληρωμές, χρησιμοποίηση από μη-εξουσιοδοτημένο πρόσωπο κάρτας που έχει κλαπεί ή έχει απολεσθεί.

Βέβαια, συγκρίνοντας τους κινδύνους της ηλεκτρονικής πληρωμής με εκείνους της πληρωμής με επιταγή ή άλλο συμβατικό μέσο, οι έρευνες καταλήγουν στο συμπέρασμα ότι η ηλεκτρονική πληρωμή είναι ασφαλέστερη.

Όμως οι ΄΄ηλεκτρονικοί κακοποιοί΄΄ παρακολουθούν άμεσα την τεχνολογία και έτσι εμφανίστηκε ένα άλλο είδος κλοπής: η παρέμβαση στα τηλεπικοινωνιακά δίκτυα δεδομένων και η εκτροπή πιστώσεων από το λογαριασμό του νόμιμου δικαιούχου σε λογαριασμό της επιλογής του κακοποιού.

Το πρόβλημα αντιμετωπίζεται συνήθως με την αλλαγή κωδικών αλλά δεν έχει λυθεί. Ένα άλλο σοβαρό θέμα που εντάσσεται κι αυτό στα πλεονεκτήματα της ηλεκτρονικής τραπεζικής (E-Banking), είναι η συγκέντρωση πληροφοριών από ένα τρίτο μη εξουσιοδοτημένο πρόσωπο γύρω από την οικονομική ιδιωτική ζωή των πολιτών.

Τα προβλήματα ασφάλειας της πληρωμής και προστασία του πολίτη οφείλονται κατά μεγάλο μέρος στον εκσυγχρονισμό της νομοθεσίας σε βαθμό ανάλογο με ην ανάπτυξη της ηλεκτρονικής.

Ενώ οι νέες τεχνολογίες επιτρέπουν στους καταναλωτές-πελάτες μεγαλύτερες επιλογές, παράλληλα δημιουργούν και την ανάγκη να αναπτυχθεί ένα νέο πλέγμα θεσμών και κανόνων που θα προστατεύουν τον πελάτη-καταναλωτή στο νέο περιβάλλον συναλλαγών τουλάχιστον όσο και στο παρελθόν.

Συνεχίζοντας την καταγραφή και ανάλυση των μειονεκτημάτων της ηλεκτρονικής παροχής τραπεζικών υπηρεσιών θα πρέπει να αναφέρουμε και αυτό του κόστους. Παρόλο που όλες σχεδόν οι νέες τεχνικές υπόσχονται τον περιορισμό του κόστους, οι δαπάνες των τραπεζών διογκώνονται ανάλογα κάθε χρόνο. Αν και αντιφατικό σε πρώτη προσέγγιση , έχει σχεδόν αποδειχτεί ΄τι κάθε νέα εφαρμογή, στην εκκίνησή της κοστίζει περισσότερο από εκείνη που αντικαθιστά.

Η συναλλαγή με τις αυτόματες ταμειακές μηχανές (ATM's) κοστίζει λειτουργικά λιγότερο από ότι στον επανδρωμένο γκισέ, αλλά κάθε συσκευή ATM, ανάλογα με το βαθμό τελειότητας, κοστίζει πάρα πολύ για την τράπεζα.

Τα πληροφοριακά συστήματα διοίκησης (MIS) και οι εφαρμογές γραφείου με τη βοήθεια μικρών ηλεκτρονικών υπολογιστών (minicomputers), αυξάνουν βέβαια τη παραγωγικότητα του προσωπικού και ανοίγουν νέους ορίζοντες, αλλά τελικά ο αριθμός των απασχολούμενων δεν περιορίζεται σημαντικά.

Έτσι, παρόλο που οι επενδύσεις σε ηλεκτρονικό εξοπλισμό έφθασαν σε τεράστιο ύψος και οι τράπεζες παρουσιάζουν πολύ μεγάλο αυτοματισμό, καθώς με το ίδιο σχεδόν προσωπικό πολλαπλασίασαν την παραγωγή τους, δεν πολλαπλασίασαν τα κέρδη τους. Μία άλλη σοβαρή δαπάνη που θα πρέπει να αναφερθεί αφορά την επιμόρφωση προσωπικού, η ανάγκη της οποίας γίνεται κάθε χρόνο όλο και πιο έντονη όχι μόνο για την εξοικείωση στα τεχνολογικά μέσα, αλλά και για την επανατοποθέτηση του ρόλου του προσωπικού όπως αυτός μεταβάλλεται από τις νέες τεχνολογίες. Έτσι συμπεραίνουμε ότι η αξιοποίηση της νέας τεχνολογίας από τις τράπεζες είναι θέμα περισσότερο οικονομικό παρά τεχνικό.

Το πρόβλημα γίνεται ακόμη οξύτερο από τη στάση της πελατείας που έχει συνηθίσει να δέχεται τα νέες υπηρεσίες σαν αυτόνομη προσφορά των τραπεζών και να μη συμμετέχει στο κόστος.

## 5.3 Ανασταλτικοί παράγοντες χρήσης E-Banking

Οι σημαντικότεροι παράγοντες στους οποίους οφείλεται η σχετικά καθυστερημένη ανάπτυξη του E-Banking στη χώρα μας είναι:

1) Η μικρή διείσδυση του Internet.

2) Η έλλειψη ενός μοντέρνου και κατάλληλου νομοθετικού πλαισίου, το οποίο είναι απαραίτητο για τη σωστή ανάπτυξη και λειτουργία του e-banking.

3) Βασικό πρόβλημα που υπάρχει ακόμα και σήμερα είναι η ανάγκη φυσικής παρουσίας του πελάτη για το άνοιγμα ενός λογαριασμού, το οποίο είναι απαραίτητο για την πιστοποίηση του γνήσιου της υπογραφής του.

4) Επίσης, υπάρχει και η κατηγορία εκείνη των πελατών των τραπεζών που είναι γνώστες των νέων τεχνολογιών εξακολουθούν όμως να είναι διστακτικοί να τις εφαρμόσουν γιατί δεν εμπιστεύονται ακόμα τις δικτυακές συναλλαγές και φοβούνται σε θέματα ασφάλειας, κυρίως στο διαδίκτυο. Γι’ αυτό τον λόγο και πολλές τράπεζες δίσταζαν να επενδύσουν στο συγκεκριμένο χώρο.

*Συμπέρασμα:*

Σύμφωνα με τα παραπάνω, παρατηρούμε πως η χρήση της πληροφορικής στο τραπεζικό σύστημα έχει πολλά θετικά στοιχεία τα οποία αν και είναι ιδιαιτέρως αξιόλογα, παρουσιάζουν και ορισμένα σημαντικά μειονεκτήματα.
Βέβαια το αν θα υπερτερήσουν τα θετικά ή τα αρνητικά στοιχεία, αυτό εξαρτάται από τη κρίση του καθενός χρήστη.
Ίσως λόγω του ότι δεν υπάρχει αρκετή εξοικείωση ακόμα με το συγκεκριμένο τρόπο συναλλαγής, να υπάρχουν και αρκετοί επιφυλακτικοί πελάτες ,κάτι το οποίο διαφαίνεται μέσα από τους ανασταλτικούς παράγοντες.
Οι παράγοντες αυτοί αναφέρονται στους λόγους που ορισμένοι πελάτες είναι κάπως καχύποπτοι όσον αφορά τη χρησιμοποίηση αυτών των σχετικά νέων για το τραπεζικό σύστημα προσφερόμενων ηλεκτρονικών υπηρεσιών – συναλλαγών.

# ΚΕΦΑΛΑΙΟ 6

# Η διεύρυνση της χρήσης της πληροφορικής στο τραπεζικό σύστημα – Επιχειρήσεις και ηλεκτρονική τραπεζική.

## 6.1 Επιχειρήσεις που χρησιμοποιούν ηλεκτρονική στο τραπεζικό σύστημα.


## 6.2 Κατάταξη τραπεζών όσον αφορά την ποιότητα των υπηρεσιών που προσφέρουν.

| Γενική Κατάταξη | Τράπεζα |
|---|---|
| 1 | winbank |
| 2 | Eurobank |
| 3 | Alpha Bank |
| 4 | Marfin Egnatia Bank |
| 5 | Τράπεζα Κύπρου |
| 6 | ATEbank |
| 7 | Geniki Bank |
| 8 | Millennium Bank |
| 9 | Εθνική Τράπεζα |
| 10 | Citibank |
| 11 | Ελληνική Τράπεζα |
| 12 | Τράπεζα Αττικής |
| 13 | Emporiki Bank |
| 14 | Aspis Bank |


Κριτήρια Επιλογής Τράπεζας
Τιμολόγηση 73,0%
Online Βοήθεια 79,8%
Δυνατότητα Δοκιμής 78,5%
Ταχύτητα Πρόσβασης στο Site 86,2%
Καλαίσθητο Web Site 57,6%
Ευκολία Πλοήγησης 77,2%
Offline Διαφήμιση 22,5%
Online Διαφήμιση 23,9%
Συστάσεις/Γνώμη Πελατών 49,6%
Συστάσεις/Γνώμη Συνεργατών 56,4%
Συστάσεις/Γνώμη Ειδικών 53,8%
Εμπειρία στο eBanking 82,3%
Ασφάλεια Συναλλαγών 88,2%
Ποικιλία Υπηρεσιών 41,6%
Φήμη 68,2%
Μέγεθος 58,7%
Προηγούμενη Σχέση 62,6%
0% 20% 40% 60% 80% 100%


Υπηρεσίες eBanking που χρησιμοποιούνται
Παρακολούθηση Λογαριασμών
Μεταφορά Χρημάτων
Πληρωμή Λογαριασμών
Πληρωμή πιστωτικών καρτών
Πληρωμές σε τρίτους
ΦΠΑ
Μετοχές
Μισθοδοσία
Εμβάσματα
Online Εκκαθάριση
Δάνεια
Αμοιβαία Κεφάλαια
Επενδυτικοί Λογαριασμοί
Ασφαλιστικά Προϊόντα
0% 5% 10% 15% 20% 25% 30% 35% 40% 45%
Τώρα
Στο Μέλλον

## 6.3 Οι κυριότερες τράπεζες που χρησιμοποιούν τις υπηρεσίες ηλεκτρονικές συναλλαγές στην Ελλάδα.

### 6.3.1 Εθνική Τράπεζα της Ελλάδος

**Από τις πρώτες στο m-banking-Ολοκληρωμένες λύσεις μέσω Internet**

Ένα πλήρες πακέτο υπηρεσιών E-Banking τόσο για ιδιώτες όσο και για νομικά πρόσωπα, προσφέρει στους πελάτες της η Εθνική Τράπεζα της Ελλάδος (www.nbg.gr). Οι πιο πρόσφατες νέες online υπηρεσίες της Εθνικής Τράπεζας συμπεριλαμβάνουν την αποστολή εμβασμάτων σε τράπεζες του εσωτερικού και του εξωτερικού, την πληρωμή πιστωτικών καρτών άλλων τραπεζών, φόρου εισοδήματος και λογαριασμών της Vivodi Telecom και τη δυνατότητα μαζικών χρεώσεων (μόνο για φυσικά πρόσωπα).

Συγκεκριμένα, η Εθνική Τράπεζα προσφέρει ένα ευρύ φάσμα υπηρεσιών Internet Banking στην ηλεκτρονική διεύθυνση www.nbg .gr σα από το site της τράπεζας οι επισκέπτες έχουν τη δυνατότητα να ενημερωθούν για το υπόλοιπο και την κίνηση των λογαριασμών που έχουν συνδέσει με το σύστημα, να μεταφέρουν ποσά μεταξύ λογαριασμών τους, να μεταφέρουν ποσά σε λογαριασμούς τρίτων που τηρούνται στην τράπεζα και να ενημερωθούν σχετικά με το χαρτοφυλάκιο των μετοχών τους και των αμοιβαίων κεφαλαίων. Επιπλέον,μπορούν να διεκπεραιώσουν αγοραπωλησία μετοχών και να ενημερωθούν για την πρόοδο της εντολής τους.

Στις εργασίες μέσω Internet banking περιλαμβάνονται η πληρωμή των δόσεων των δανείων και οφειλών σε κάρτες, την πληρωμή λογαριασμών κοινής ωφελείας, την ενημέρωση για το χαρτοφυλάκιο άυλων τίτλων, τη διεκπεραίωση αγοραπωλησίας άυλων τίτλων και τη διαβίβαση αιτήσεων για στεγαστικά και καταναλωτικά δάνεια. Ήδη γίνεται η πληρωμή ΦΠΑ σε όσους φορολογούμενους υποβάλλουν δήλωση ηλεκτρονικά μέσω του TAXISnet.

Σε ότι αφορά το mobile banking, η Εθνική ήταν από τις πρώτες τράπεζες που το Δεκέμβριο του 1999 προσέφερε στην πελατεία της πρόσβαση στις τραπεζικές υπηρεσίες μέσω κινητού τηλεφώνου, υπηρεσίες τις οποίες αναβάθμισε σημαντικά τον Απρίλιο του 2000, με τη νέα γενιά του mobile banking.

Σήμερα στις υπηρεσίες mobile banking που παρέχονται στους κατόχους κινητών τηλεφώνων περιλαμβάνεται η πληροφόρηση για τους λογαριασμούς καταθέσεων και ανοικτού εθνοδανείου και τα υπόλοιπά τους, πληροφόρηση για τις πιστωτικές κάρτες και το διαθέσιμο πιστωτικό τους όριο, ειδοποίηση (alert) του κατόχου σε περίπτωση χρέωσης ή πίστωσης των συνδεδεμένων λογαριασμών του με ποσό πέραν του ορίου που ο ίδιος έχει θέσει και ειδοποίηση του κατόχου όταν το υπόλοιπο του λογαριασμού μειώνεται κάτω από το ποσό που ο ίδιος έχει θέσει ως όριο.

### 6.3.2 Marfin Εγνατία Τράπεζα

### Υπηρεσία Egnatia Teller με ειδοποίηση SMS και e-mail.

Η Εγνατία Τράπεζα (www.egnatiasite.egnatiabank.gr) παρέχει ένα πλήρες πακέτο online υπηρεσιών που καλύπτουν τους τομείς των τραπεζικών συναλλαγών, των επενδύσεων, του ηλεκτρονικού εμπορίου και της αναζήτησης ακινήτων. Η νέα υπηρεσία Egnatia Teller προσφέρει στους πελάτες της τράπεζας όλες τις «κλασικές» υπηρεσίες online τραπεζικής (μεταφορά κεφαλαίου, πληρωμή Φ.Π.Α., φόρου εισοδήματος, Ι.Κ.Α., Ο.Α.Ε.Ε., λογαριασμών, υπόλοιπο και κινήσεις λογαριασμού, κ.λπ.), ενώ περιλαμβάνει και μία σειρά από νέες δυνατότητες.

Μεταξύ αυτών περιλαμβάνονται η πληρωμή πιστωτικών καρτών άλλων τραπεζών, η πάγια εξόφληση πιστωτικών καρτών της Εγνατίας, η δυνατότητα τηλεειδοποίησης μέσω SMS ή e-mail για επιθυμητές συναλλαγές, η αίτηση παραγγελίας συναλλάγματος, κ.λπ.

Μέσα από το site της Εγνατίας Τράπεζας οι επισκέπτες μπορούν να υποβάλλουν αίτηση για να αποκτήσουν σε ελάχιστο χρόνο προϊόντα και υπηρεσίες όπως προσωπικά, καταναλωτικά και στεγαστικά δάνεια, πιστωτικές κάρτες και κάρτες ATM, προϊόντα bankassurance, ακόμη και να ανοίξουν τραπεζικό λογαριασμό. Το 1997 η Εγνατία επέλεξε το Internet ως το νέο κανάλι προώθησης των προϊόντων και των υπηρεσιών που παρέχει προς τους πελάτες της.

Την ίδια χρονιά η τράπεζα παρουσίασε το Web Teller, μέσω του οποίου οι πελάτες της, με απόλυτη ασφάλεια (η πρόσβαση γίνεται μόνο με τους απαραίτητους κωδικούς ασφαλείας που δίνονται στους πελάτες μετά από την αίτηση για σύνδεσή τους με το σύστημα), μπορούν να διενεργούν τις καθημερινές τραπεζικές τους συναλλαγές οποιαδήποτε στιγμή της ημέρας από έναν Η/Υ συνδεδεμένο με το Διαδίκτυο.

Αναλυτικότερα, μέσα από το Web Teller οι πελάτες της τράπεζας μπορούν να διαχειρίζονται τους λογαριασμούς τους μεταφέροντας κεφάλαια, αποστέλλοντας εμβάσματα στην Ελλάδα και στο εξωτερικό και έχοντας στη διάθεσή τους κάθε στιγμή αναλυτικά την κίνηση των λογαριασμών τους.

Οι χρήστες του Web Teller διαχειρίζονται τις παραμέτρους ασφάλειας που έχουν θέσει μέσω του personal identification number (PIN) και του transaction authentication number (TAN).

Για την πρόσβαση στο Web Teller το μόνο που απαιτείται είναι να συμπληρώσει ο πελάτης της σχετική αίτηση μέσω του site στην ηλεκτρονική διεύθυνση www.egnatiabank.gr. Το 1998 η Εγνατία παρουσίασε το Web Shop, μέσα από το οποίο οι επισκέπτες του site μπορούν να πραγματοποιούν ασφαλείς αγορές πολλών διαφορετικών προϊόντων και υπηρεσιών με την πιστωτική τους κάρτα Visa.

Η τράπεζα παρουσίασε άλλη μια νέα ηλεκτρονική υπηρεσία για online χρηματιστηριακές συναλλαγές με την ονομασία Web Trader. Προσφέρει real time παρακολούθηση της συνεδρίασης στο ΧΑΑ, online διεξαγωγή χρηματιστηριακών πράξεων και άμεση ενημέρωση του χαρτοφυλακίου του πελάτη μέσω Internet. Η καινοτομία της υπηρεσίας είναι ότι ο πελάτης θα μπορεί να χρησιμοποιεί αυτόματα μέσω του Web Teller τον καταθετικό λογαριασμό που έχει στην τράπεζα, για να καλύπτει τις χρηματιστηριακές του συναλλαγές. Επίσης, η νέα υπηρεσία θα προσφέρει ειδικές στήλες για την ενημέρωση των πελατών με άρθρα, αναλύσεις κλπ.

### 6.3.3. EFG Eurobank Ergasias.

**Δωρεάν πρόσβαση σε λογαριασμούς,Χαρτοφυλάκιο & ΧΑΑ. Υποστήριξη και από τα κινητά τηλέφωνα.**

Οι υπηρεσίες E-Banking της Eurobank (www.eurobank.gr) προσφέρουν μία ευρεία γκάμα δυνατοτήτων για ιδιώτες, επαγγελματίες και επιχειρήσεις.

Ο χρήσης των online υπηρεσιών της Eurobank μπορούν να πραγματοποιούν μία ευρεία σειρά τραπεζικών και χρηματιστηριακών συναλλαγών, όπως ενημέρωση για υπόλοιπα και κινήσεις λογαριασμών, μεταφορά κεφαλαίων, εξόφληση καρτών, Φ.Π.Α. και λογαριασμών, παρακολούθηση συνεδρίασης του Χ.Α., αγοροπωλησία μετοχών κ.λπ.

Η τράπεζα έχει, επίσης, δημιουργήσει και μία υπηρεσία ηλεκτρονικής τραπεζικής μέσω κινητού τηλεφώνου (m-banking), που παρέχει ένα πλήρες πακέτο υπηρεσιών ηλεκτρονικής τραπεζικής για τους χρήστες της κινητής τηλεφωνίας, ανεξαρτήτως δικτύου σύνδεσης ή συσκευής.

Η διαδικασία εγγραφής στην υπηρεσία είναι ίδια με αυτή του E-Banking και οι κωδικοί πρόσβασης κοινοί και στις δύο περιπτώσεις.

Η EFG Eurobank Ergasias (www.eurobank.gr) δίνει δωρεάν σε πελάτες της πρόσβαση σε τρεις σελίδες: Λογαριασμοί, Χαρτοφυλάκιο και ΧΑΑ. Μέσα από τη σελίδα “Λογαριασμοί”, ο πελάτης μπορεί να βλέπει το υπόλοιπο και τις κινήσεις λογαριασμών, να μεταφέρει χρήματα σε δικούς του λογαριασμούς ή τρίτων τόσο της ίδιας της τράπεζας όσο και άλλων, καθώς και να πληρώνει οφειλές από πιστωτικές κάρτες και ΦΠΑ.

Η σελίδα “Χαρτοφυλάκιο” αφορά τις χρηματιστηριακές συναλλαγές και ο πελάτης μπορεί να δίνει εντολές για όλες τις μετοχές, να αγοράζει και να πουλά μετοχές on-line, να συμμετέχει σε δημόσιες εγγραφές και να πραγματοποιεί Intraday.

Φυσικά, δίνεται η δυνατότητα πληροφόρησης για το χαρτοφυλάκιο και τα νέα της αγοράς, τα νέα των εισηγμένων εταιρειών, με τις αναλύσεις της EFG Eurobank Χρηματιστηριακής μέσα από τη σελίδα “ΧΑΑ”, όπου ο χρήστης μπορεί να δημιουργήσει εικονικά χαρτοφυλάκια, με εναλλακτικά σενάρια επενδύσεων και να παρακολουθεί τις τιμές των μετοχών του ΧΑΑ σε ζωντανή σύνδεση.

Η τράπεζα προσφέρει online υπηρεσίες για πελάτες με εταιρικούς λογαριασμούς. Αποκτώντας πρόσβαση στο E-Banking, έχουν τη δυνατότητα να βλέπουν τα υπόλοιπα των λογαριασμών, τις κινήσεις των λογαριασμών έως και 6 μήνες πίσω και να αποθηκεύουν τις κινήσεις στον υπολογιστή σε μορφή csv για επεξεργασία σε Microsoft Excel, Microsoft Money ή Quicken, καθώς και online πληρωμή του ΦΠΑ www.eurobank.gr/corporate.
Πρόκειται για υπηρεσίες που αναβαθμίζονται, ώστε οι εταιρικοί πελάτες να αποκτήσουν άλλο ένα κανάλι επικοινωνίας με την τράπεζα.

### 6.3.4 Aspis Bank

### Online μεταφορά χρημάτων και αποστολές εμβασμάτων.

Την πραγματοποίηση τραπεζικών και χρηματιστηριακών συναλλαγών παρέχει στους πελάτες της η Aspis Bank (www.aspisbank.gr), μέσω των υπηρεσιών Online Banking και Online Trading αντίστοιχα.Οι εγγεγραμμένοι χρήστες των υπηρεσιών μπορούν, μεταξύ άλλων, να ενημερώνονται για το υπόλοιπο και την κίνηση των λογαριασμών τους, να πραγματοποιούν online μεταφορές χρημάτων και αποστολές εμβασμάτων, να πληρώνουν λογαριασμούς και πιστωτικές κάρτες.

### 6.3.5. Emporiki Bank Ενημέρωση και διαχείριση ηλεκτρονικών λογαριασμών.

Η υπηρεσία Emporiki E.Banking εξελίσσεται συνεχώς και ανανεώνεται, προσφέροντας νέες υπηρεσίες στους πελάτες της Εμπορικής Τράπεζας (www.emporiki.gr)Οι νέες δυνατότητες της υπηρεσίας περιλαμβάνουν την αποστολή εμβασμάτων σε άλλες τράπεζες εντός Ελλάδας, την πληρωμή λογαριασμών ΟΤΕ, την πληρωμή φόρου εισοδήματος για φυσικά πρόσωπα, τη δυνατότητα παραλαβής κωδικού πρόσβασης στην υπηρεσία από ATM, κ.λπ.Οι χρήστες της υπηρεσίας μπορούν να ενημερώνονται και να διαχειρίζονται ηλεκτρονικά λογαριασμούς, άυλους τίτλους και μετοχές που έχουν στη διάθεσή τους, να καταβάλλουν πληρωμές δημοσίου και ταμείων (Φ.Π.Α., Ι.Κ.Α., Ο.Α.Ε.Ε.), λογαριασμών και πιστωτικών καρτών, να διαχειρίζονται πάγιες εντολές κ.λπ.

### 6.3.6. Citibank Online

**Εξόφληση προσωπικών λογαριασμών, δανείων και καρτών.**

Με νέες υπηρεσίες εμπλουτίστηκε το Citibank Online, το σύνολο των ηλεκτρονικών τραπεζικών υπηρεσιών της Citibank (www.citibank.com/greece). Οι χρήστες της υπηρεσίας, εκτός από τις δυνατότητες μεταφοράς χρημάτων, πληρωμής πιστωτικών καρτών και δανείων, μπορούν εφεξής να πληρώνουν τους προσωπικούς τους λογαριασμούς (π.χ. Ο.Τ.Ε., Ι.Κ.Α., Ο.Α.Ε.Ε., Φ.Π.Α.) αυθημερόν ή σε προκαθορισμένη μελλοντική ημερομηνία και να δίνουν πάγιες εντολές για αυτόματη μηνιαία ή τακτική πληρωμή άλλων λογαριασμών (όπως ενοίκιο, ασφάλιστρα, κ.λ.π.). Η τράπεζα παρέχει επίσης και την υπηρεσία Citiphone Banking για την πραγματοποίηση μιας σειράς τραπεζικών συναλλαγών ανά πάσα στιγμή μέσω τηλεφώνου.

### 6.3.7. Τράπεζα Κύπρου

**Επιπρόσθετες δυνατότητες για μεγαλύτερη ασφάλεια.**

Η υπηρεσία Internet banking της Τράπεζας Κύπρου (www.bankofcyprus.gr) έχει σχεδιαστεί ώστε να αποτελεί ένα εργαλείο πλήρους ενημέρωσης και πραγματοποίησης τραπεζικών συναλλαγών για τους πελάτες της τράπεζας. Εκτός των υπηρεσιών πληροφοριών, κινήσεων, μεταφορών, πληρωμών κ.λπ., διαθέτει και μία σειρά επιπρόσθετων σημαντικών δυνατοτήτων.

Σε αυτές περιλαμβάνονται οι δυνατότητες ορισμού supervisor, εξουσιοδότησης τρίτου προσώπου που λειτουργεί για λογαριασμό του πελάτη, η έκδοση επιπλέον κωδικού για μεγάλα ποσά, καθορισμού ενός συγκεκριμένου ποσού για κάθε κατηγορία συναλλαγών, κ.λπ.

Οι υπηρεσίες Internet banking της τράπεζας υποστηρίζονται και από την υπηρεσία Phone Banking.

### 6.3.8. Alpha Bank

**Δυνατότητα εξόφλησης ΦΠΑ και πολλών άλλων λογαριασμών.**

Το Alpha Web Banking, όπως ονομάζονται οι υπηρεσίες ηλεκτρονικής τραπεζικής της Alpha Bank (www.alpha.gr), προσφέρει στους πελάτες της τράπεζας ένα ευρύ φάσμα δυνατοτήτων. Μεταξύ αυτών συμπεριλαμβάνονται η μεταφορά κεφαλαίων σε λογαριασμούς της ίδιας τράπεζας ή άλλων τραπεζών του εσωτερικού και του εξωτερικού, καθώς και η ενημέρωση για κάθε κίνηση στους λογαριασμούς του χρήστη.Επίσης, παρέχεται η δυνατότητα πληρωμής Φ.Π.Α., η πραγματοποίηση παγίων εντολών (π.χ. πληρωμή ενοικίου), καθώς και πολλών ακόμη ειδών λογαριασμών (πιστωτικές κάρτες και δάνεια της τράπεζας, πιστωτικές κάρτες άλλων τραπεζών, λογαριασμοί σταθερής και κινητής τηλεφωνίας, καταβολή ασφάλιστρων, λογαριασμών δημοσίου, κ.λπ.)

Η Alpha Bank (www.alphabank.gr) προσφέρει τη δυνατότητα στους πελάτες της να εκτελούν τραπεζικές συναλλαγές μέσω του δικτύου Internet 24 ώρες το 24ωρο.

Εάν ο υποψήφιος συνδρομητής θέλει να εξοφλεί λογαριασμούς κοινής ωφελείας (ΟΤΕ, ΔΕΗ, ΕΥΔΑΠ), καρτών (Alpha Bank Visa, American Express, Alpha Bank Mastercard, κ.λπ.), καρτών επιχειρήσεων, προσωπικών δανείων (Alpha 700), ή να χρεώνει λογαριασμούς τρίτων, οφείλει να καταθέσει τα απαιτούμενα δικαιολογητικά (πληρωμών,καρτών και εξουσιοδοτήσεις).

Εάν η αίτηση εγκριθεί, τότε του αποστέλλονται ο κωδικός συνδρομητή και οι μυστικοί αριθμοί προσβάσεως (PIN). Και μπορεί να συνδεθεί στο Web Site της τράπεζας και να χρησιμοποιήσει το σύστημα.

Οι πελάτες-συνδρομητές του συστήματος έχουν τη δυνατότητα 24 ώρες το 24ωρο να δίνουν εντολές στην τράπεζα για εξόφληση λογαριασμών κοινής ωφελείας και δημοσίου, όπως ΦΠΑ, πιστωτικών καρτών ή δανείων, σε δραχμές ή σε ευρώ, να δίνουν εντολές στην τράπεζα να μεταφέρει χρήματα από ένα λογαριασμό σε άλλον, να πληροφορούνται για τα υπόλοιπα και τους τόκους των λογαριασμών τους, να πληροφορούνται για τις εντολές και πληρωμές λογαριασμών, τις τιμές συναλλάγματος.

Όσον αφορά το Χρηματιστήριο, μπορούν να πληροφορούνται για τις τιμές μετοχών επιλεγμένων εταιριών, καθώς και για τους δείκτες τιμών μετοχών και με 25 λεπτά περίπου καθυστέρηση να ενημερώνονται για τις τιμές κλεισίματος των μετοχών του ΧΑΑ.Ειδικά για τους πελάτες προσφέρει τη δυνατότητα να εκτελούν τραπεζικές συναλλαγές μέσω κινητού τηλεφώνου που διαθέτει υποστήριξη υπηρεσιών WAP.

Οι υπηρεσίες αφορούν ενημέρωση για υπόλοιπα λογαριασμών και οφειλές προς την τράπεζα και μεταφορά χρημάτων, όπως και πληρωμή οφειλών.

### 6.3.9. Τράπεζα Πειραιώς

**Εξυπηρέτηση μέσα από κάθε τεχνολογικό μέσο.**
**Η πρώτη ολοκληρωμένη υπηρεσία E-Banking.**

Η Τράπεζα Πειραιώς (www.winbank.gr) προσφέρει ένα ευρύ φάσμα τραπεζικών συναλλαγών στους πελάτες της, αξιοποιώντας όλα τα μέσα της νέας τεχνολογίας (Internet, σταθερή και κινητή τηλεφωνία, μηνύματα sms κ.λπ.).
Ο διαδικτυακές υπηρεσίες της Τράπεζας Πειραιώς διατίθενται στα ελληνικά και αγγλικά και περιλαμβάνουν δυνατότητες διαχείρισης λογαριασμών, καρτών, δανείων και επιταγών, πληρωμών και μεταφορών, χρηματιστηριακών συναλλαγών, τηλε-ειδοποιήσεων κ.λπ. Στις υπηρεσίες που απευθύνονται σε επιχειρήσεις προσφέρεται, επίσης, η δυνατότητα πολλαπλών χρηστών-υπαλλήλων που έχουν διαφορετικά δικαιώματα πρόσβασης σε αυτές. Επίσης, η τράπεζα προσφέρει την υπηρεσία winbank for cards, η οποία προσφέρει online και real time ενημέρωση στους κατόχους των καρτών της Τράπεζας Πειραιώς, χωρίς να απαιτείται προηγουμένως ειδική εγγραφή.

Τον Ιανουάριο του 2000 ο όμιλος Πειραιώς προχώρησε στη δημιουργία της πρώτης ολοκληρωμένης υπηρεσίας E-Banking, την Win Bank, με προοπτική την πιθανή μετεξέλιξή της σε αυτόνομη ηλεκτρονική τράπεζα του Ομίλου.
Η Win Bank προσφέρει μια σειρά ηλεκτρονικών υπηρεσιών μέσω Internet, σταθερού τηλεφώνου, κινητού τηλεφώνου και ATMs. Συγκεκριμένα με την υπηρεσία Win-Internet μέσα από το site www.winbank.gr ο πελάτης μπορεί να εκτελεί τραπεζικές και χρηματιστηριακές συναλλαγές μέσω Η/Υ, να παρακολουθεί το πλήρες χαρτοφυλάκιό του (προθεσμιακές καταθέσεις, αμοιβαία, δάνεια, ασφαλιστικά προϊόντα), να μεταφέρει χρήματα μεταξύ των λογαριασμών, να βλέπει συνοπτική παρουσίαση των λογαριασμών και των υπολοίπων τους σε δραχμές και σε ευρώ, να δίνει παραγγελίες για επιταγές, να πληρώνει πιστωτικές κάρτες και λογαριασμούς ΔΕΚ.

Το Win-Phone δίνει τη δυνατότητα στον πελάτη καλώντας ένα τηλεφωνικό αριθμό να εξυπηρετείται είτε από το κέντρο κλήσεων μέσω αντιπροσώπου είτε από το σύστημα προμαγνητοφωνημένων μηνυμάτων (IVR-Integrated Voice Response) για την εκτέλεση των τραπεζικών και χρηματιστηριακών συναλλαγών του.
Το Win-Mobile προσφέρει αμφίδρομη ανταλλαγή σύντομων γραπτών μηνυμάτων (SMS) μεταξύ της τράπεζας και του πελάτη.
Το Win-ATM, κάνοντας χρήση του πιο γνωστού μέσου της ηλεκτρονικής τραπεζικής, τα μηχανήματα αυτόματης ανάληψης, έρχεται να συμπληρώσει τη γκάμα των υπηρεσιών καλύπτοντας τις ανάγκες του πελάτη σε μετρητά, αλλά και δίνοντάς του μια σειρά άλλων τραπεζικών συναλλαγών.

*Συμπέρασμα:*

Στο συγκεκριμένο κεφάλαιο, αναλύθηκαν εκτενέστερα οι υπηρεσίες της ηλεκτρονικής τραπεζικής που παρέχει η κάθε τράπεζα ξεχωριστά και παρατηρείται πως αρχικά η τράπεζα Πειραιώς και στη συνέχεια και πολλές άλλες μεγάλες τράπεζες υιοθετούν αυτόν τον νέο τρόπο ηλεκτρονικής τραπεζικής για τη διευκόλυνση καθώς και για την ολοένα και συνεχόμενη βελτίωση των συναλλαγών.

# ΚΕΦΑΛΑΙΟ 7

# Διατραπεζικά συστήματα ΔΙΑΣ.

## 7.1. Τα διατραπεζικά συστήματα συναλλαγών ΔΙΑΣ

Τα Διατραπεζικά Συστήματα Δίας Α.Ε., είναι μια εταιρία η οποία ιδρύθηκε στις 28 Ιουνίου 1989 με πρωτοβουλία της Ένωσης Ελληνικών Τραπεζών. Οι τράπεζες - μέλη της Δίας Α.Ε. είναι γύρω στα σαράντα, ενώ ο μεγαλύτερος μέτοχος της εταιρίας είναι η Τράπεζα της Ελλάδος.

Σκοπός των Διατραπεζικών Συστημάτων είναι η παροχή προς τις τράπεζες-μέλη υπηρεσιών που συμβάλλουν στον εκσυγχρονισμό των τραπεζικών συναλλαγών και συντελούν στην καλύτερη εξυπηρέτηση του τραπεζικού κοινού, καθώς και στη μείωση του κόστους των συναλλαγών, με αποτέλεσμα να ωφελούνται οι τράπεζες και οι πελάτες τους, προς όφελος και της εθνικής οικονομίας.

Με τη λειτουργία της Δίας Α.Ε. στην Ελλάδα αναπτύχθηκε μια νέα αντίληψη στις σχέσεις μεταξύ πελάτη και τραπεζικού συστήματος, αφού παρέχεται η δυνατότητα να εξυπηρετούνται όλοι με τα σύγχρονα μέσα πληρωμών από όλες τις τράπεζες.

Τα Διατραπεζικά Συστήματα διαθέτουν ιδιόκτητες κτιριακές εγκαταστάσεις 5.200τ.μ. Το κτίριο έχει σχεδιαστεί με προδιαγραφές υψηλής ασφάλειας και η πρόσβαση σε αυτό είναι ελεγχόμενη μέσω ηλεκτρονικών συστημάτων.

Τα Διατραπεζικά Συστήματα διαθέτουν διπλά κεντρικά υπολογιστικά συστήματα και ιδιόκτητο τηλεπικοινωνιακό δίκτυο. Οι τράπεζες, για λόγους ασφάλειας και αδιάλειπτης λειτουργίας, είναι συνδεδεμένες με τη Δίας Α.Ε. με διπλές τηλεπικοινωνιακές γραμμές. Τα Συστήματα Πληρωμών της ΔΙΑΣ Α.Ε. χρησιμοποιούνται για πληρωμές, κυρίως μικρής αξίας (retail συναλλαγές), που καλύπτουν κατά βάση συναλλαγές με κάρτες, δοσοληψίες πληρωμής των υποχρεώσεων των επιχειρήσεων και του Δημοσίου (μισθοί, συντάξεις κ.λ.π.) καθώς και εισπράξεις των απαιτήσεών τους (από παροχή υπηρεσιών τηλεπικοινωνίας, ενέργειας, ύδρευσης, από απαιτήσεις φόρων) κ.λ.π.

### 7.1.1 Συμψηφισμός / Διακανονισμός.

Τα συστήματα της ΔΙΑΣ Α.Ε. ως net συστήματα πληρωμών, προβαίνουν σε εκκαθάριση των συναλλαγών και συμψηφισμό στο τέλος της εργάσιμης ημέρας. Τα αποτελέσματα του συμψηφισμού διαβιβάζονται μέσω του συστήματος TARGET στην Τράπεζα της Ελλάδος για αυθημερόν συνολικό διακανονισμό.

### 7.1.2 Διαχείριση κινδύνων.

Τα συστήματα της ΔΙΑΣ Α.Ε. έχουν χαρακτηρισθεί ως συστήματα χαμηλού συστημικού κινδύνου και ως εκ τούτου έχουν ληφθεί τα προβλεπόμενα μέτρα διαχείρισης ανάλογου κινδύνου, όπως καθορισμός ορίων αξίας για κάθε σύστημα σύμφωνα με τις ιδιαιτερότητές του. Πέραν όμως αυτών, πληρούνται επίσης ορισμένες από τις "Βασικές Αρχές για τα Συστημικώς Σημαντικά Συστήματα Πληρωμών" που έχει θεσπίσει η Τράπεζα Διεθνών Διακανονισμών.

Ο διακανονισμός γίνεται αυθημερόν στην Τράπεζα της Ελλάδος. Ο συμψηφισμός καθίσταται οριστικός μετά το διακανονισμό του. Η εντολή για εκτέλεση του συμψηφισμού καθίσταται ανέκκλητη από την εισαγωγή της στο σύστημα TARGET.

### 7.1.3 Μηνύματα on line.

Τα μηνύματα που χρησιμοποιούνται είναι είτε on line real time, είτε file transfer (batch), ανάλογα με την τεχνολογική υποδομή και τις απαιτήσεις κάθε συστήματος.

### 7.1.4 Χρησιμοποιούμενα πρότυπα.

Τα πρότυπα σύνταξης των μηνυμάτων είναι παραπλήσια των προτύπων SWIFT και ISO και έχουν συνταχθεί για να καλύπτουν τις ανάγκες της ΔΙΑΣ Α.Ε. και των τραπεζών.

### 7.1.5 Ασφάλεια συστημάτων (αρχείων και μηνυμάτων).

Τα αρχεία και τα μηνύματα που ανταλλάσσονται μέσω συστημάτων είναι κρυπτογραφημένα και πιστοποιημένα με βάση τα διεθνή πρότυπα ISO.

### 7.1.6 Εξασφάλιση αδιάλειπτης λειτουργίας.

Η ΔΙΑΣ Α.Ε. εξασφαλίζει την αδιάλειπτη λειτουργία της, σε περίπτωση καταστροφικού γεγονότος, μέσω Κέντρου Αποκατάστασης Εφαρμογών, που είναι

εγκατεστημένο σε άλλη Τράπεζα, επιλεγμένη για να καλύπτει τις ειδικές ανάγκες των συστημάτων. Χρησιμοποιείται η μέθοδος mirroring, σύμφωνα με την οποία σε πραγματικό χρόνο (real time) κάθε κίνηση των συστημάτων της ΔΙΑΣ Α.Ε. αποτυπώνεται και στο εφεδρικό κέντρο της.

### 7.1.7 Γραφείο εξυπηρέτησης πελατών.

Στη διάθεση των χρηστών της ΔΙΑΣ Α.Ε. βρίσκεται το Γραφείο Εξυπηρέτησης Πελατών, το οποίο λειτουργεί σύμφωνα με τις ανάγκες των Συστημάτων της.

### 7.1.8 Επίλυση διαφορών.

Για όλα τα συστήματα προβλέπεται διαδικασία διαχείρισης αμφισβητήσεων και επίλυσης διαφορών. Κάθε διαφορά, που δεν μπορεί να διευθετηθεί φιλικώς μεταξύ των συμβαλλομένων μερών, εισάγεται στη Διαιτητική Επιτροπή Επίλυσης Διαφορών.

### 7.1.9 Τηλεπικοινωνιακές διασυνδέσεις.

Η ΔΙΑΣ Α.Ε. συνδέεται ηλεκτρονικά με όλες τις τράπεζες, την Τράπεζα της Ελλάδος, καθώς επίσης και με ορισμένους φορείς και επιχειρήσεις, πελάτες των τραπεζών.

### 7.1.10 Πληροφόρηση και φύλαξη ιστορικών δεδομένων.

Τα συστήματα της εταιρείας παρέχουν την απαραίτητη πληροφόρηση στα συμμετέχοντα μέλη.
Η φύλαξη ιστορικών δεδομένων εξασφαλίζεται σύμφωνα με τις ανάγκες των συστημάτων και τις απαιτήσεις του νόμου.

*Συμπέρασμα:*

Στο κεφάλαιο αυτό διαφαίνεται ότι τα διατραπεζικά συστήματα ΔΙΑΣ παρέχουν υπηρεσίες όπως: πληροφόρηση και φύλαξη ιστορικών δεδομένων, επίλυση διαφορών γραφείο εξυπηρέτησης πελατών, τηλεπικοινωνιακές διασυνδέσεις, συμψηφισμό – διακανονισμό πληρωμών, εξασφάλιση αδιάλειπτης λειτουργίας, ασφάλεια συστημάτων( αρχείων και μηνυμάτων) καθώς και διαχείριση κινδύνων οι συμβάλλουν στην καλύτερη συνεργασία μεταξύ των τραπεζών ώστε να παρέχουν με το ταχύτερο και αξιόπιστο δυνατό τρόπο τις υπηρεσίες τους στο πελατειακό τους κοινό.

# ΚΕΦΑΛΑΙΟ 8
# Χρεώσεις, ειδοποιήσεις, προμήθειες και όρια συναλλαγών.

## 8.1.Όρια συναλλαγών.

Ένα ζήτημα το οποίο επιβάλλεται να αναφερθεί είναι για τη τα όρια που θέτει η τράπεζα στις συναλλαγές.
Βέβαια, ορισμένες τράπεζες - αν όχι όλες - δίνουν τη δυνατότητα στους πελάτες τους να προσαρμόζουν τα όρια αυτά στις προσωπικές τους ανάγκες, κατόπιν φυσικά ανάλογης εντολής τους προς την εκάστοτε τράπεζα. Τα συνηθέστερα όρια είναι:

- Όριο ημερήσιας ανάληψης χρημάτων από ΑΤΜ ίδιας τράπεζας.
- Όριο ημερήσιας ανάληψης χρημάτων από ΑΤΜ άλλης τράπεζας (σύστημα ΔΙΑΣ).
- Όριο ημερήσιων αγορών.

## 8.2. Χρέωση αδράνειας λογαριασμού.

Πολλές τράπεζες χρεώνουν κάποιο ποσό τους πελάτες τους είτε στην περίπτωση που ο λογαριασμός τους παραμένει αδρανής (καμία συναλλαγή) για μεγάλο χρονικό διάστημα είτε στην περίπτωση που ο λογαριασμός τους έχει μέσα κατά μέσο όρο πολύ λίγα χρήματα είτε σε περιπτώσεις συνδυασμού των δύο παραπάνω κριτηρία:

## 8.3. Ειδοποιήσεις κινήσεων λογαριασμού.

Ορισμένες τράπεζες παρέχουν δυνατότητες ενημέρωσης των πελατών τους για τις συναλλαγές που πραγματοποιούνται από ή προς τους λογαριασμούς τους με διάφορους τρόπους, όπως π.χ. με email, με sms κ.α. Κάποιες τράπεζες ενδέχεται να χρεώνουν όλους ή κάποιους από τους τρόπους ενημέρωσης των πελατών τους, ενώ άλλες όχι.

## 8.4. Προμήθειες επί των συναλλαγών.

Η μεταφορά κάποιου ποσού από και προς έναν τραπεζικό λογαριασμό υπάρχει περίπτωση να υπόκειται σε προμήθεια επί της συναλλαγής. Η ύπαρξη ή όχι προμήθειας καθώς και το ποσό αυτής ποικίλει από τράπεζα σε τράπεζα και εξαρτάται από πολλούς παράγοντες, κυριότεροι των οποίων είναι:

1. Αν πρόκειται για μεταφορά χρημάτων σε λογαριασμό άλλης ή ίδιας τράπεζας.
2. Αν πρόκειται για μεταφορά χρημάτων σε λογαριασμό (υποκαταστήματος) άλλης τράπεζας που βρίσκεται εντός ή εκτός ΕΕ.
3. Αν πρόκειται για μεταφορά χρημάτων στο ίδιο ή σε διαφορετικό νόμισμα αποστολέα και παραλήπτη. Στις δύο τελευταίες περιπτώσεις συνηθίζεται οι τράπεζες να χρεώνουν προμήθειες.

*Συμπέρασμα:*

Παρατηρούμε ότι οι τράπεζες μέσω της ηλεκτρονικής τραπεζικής προσφέρουν υπηρεσίες για το όριο συναλλαγών και την ειδοποίηση κινήσεων λογαριασμού. λόγω του ότι υπερτερεί έναντι της μεταφοράς χρημάτων μέσω ΑΤΜ ή μέσω γκισέ υποκαταστημάτων καθώς επιφέρει - όχι μηδενικές, αλλά τουλάχιστον – χαμηλότερες προμήθειες.

# ΚΕΦΑΛΑΙΟ 9
# Οι στρατηγικές της ηλεκτρονικής τραπεζικής.

## 9.1. Η έννοια της στρατηγικής της ηλεκτρονικής τραπεζικής όσον αφορά την παροχή υπηρεσιών.

Όλες οι επιχειρήσεις που λειτουργούν σε περιβάλλον οξυμένου ανταγωνισμού, όπως και οι τράπεζες, συνεχώς επιδιώκουν την μείωση του κόστους τους, ώστε να παραμείνουν βιώσιμες και ανταγωνιστικές στο σημερινό διεθνοποιημένο οικονομικό περιβάλλον. Όπως στις περισσότερες επιχειρήσεις, έτσι και στα χρηματοπιστωτικά ιδρύματα, οι ανθρώπινοι πόροι αποτελούν το βασικό οδηγό κόστους σε κάθε συναλλαγή, είτε είναι οικονομικής φύσεως είτε πληροφοριακής.
Θέλοντας λοιπόν, μία τράπεζα να μειώσει τα λειτουργικά της έξοδα και να αυξήσει την κερδοφορία της, παράλληλα με την ικανοποίηση της πελατειακής της βάσης, μία στρατηγική που μπορεί να ακολουθήσει είναι αυτή της δημιουργίας εναλλακτικών δικτύων.

Θα πρέπει να τονίσουμε ότι στο παρελθόν και ειδικότερα σε χώρες της Δύσης έγιναν προσπάθειες να δημιουργηθούν εξ'ολοκλήρου διαδικτυακές τράπεζες, δηλαδή τράπεζες που να παρέχον αποκλειστικά υπηρεσίες ηλεκτρονικής τραπεζικής. Οι περισσότερες από αυτές είτε "εξαφανίστηκαν" είτε εξαγοράστηκαν από άλλα τραπεζικά ιδρύματα που διέθεταν φυσικά δίκτυα.

Ίσως λοιπόν μια παράλληλη χρησιμοποίηση φυσικών και εναλλακτικών δικτύων από έναν χρηματοπιστωτικό οργανισμό να είναι η σοφότερη επιλογή, τουλάχιστον για τα σημερινά χρόνια.
Κανείς δεν είναι σε θέση να προβλέψει το μέλλον, αλλά αναμένεται να αυξηθεί με την πάροδο των χρόνων η κρίσιμη μάζα ηλεκτρονικών χρηστών που απαιτείται για την βιωσιμότητα μιας πλήρως διαδικτυακής τράπεζας.

Αυτό είναι απολύτως φυσικό, καθώς οι νεότερες γενιές θα είναι περισσότερο εξοικειωμένες με τις νέες τεχνολογίες και το διαδίκτυο και οι τεχνολογικές υποδομές γενικότερα θα έχουν αναπτυχθεί σε μεγαλύτερο βαθμό.

Στη συνέχεια, θα αναφερθούμε σε στρατηγικές που θα μπορούσε να ακολουθήσει μια τράπεζα για να αναπτύξει και να είναι σε θέση να προσφέρει υπηρεσίες ηλεκτρονικής τραπεζικής στους πελάτες της.

## 9.2. Όραμα και στρατηγικοί στόχοι ηλεκτρονική τραπεζικής.

Η ανώτερη διοίκηση (top management) του χρηματοπιστωτικού οργανισμού θα πρέπει να αναπτύξει ένα σαφώς προσδιορισμένο όραμα για την ηλεκτρονική τραπεζική, για να μπορέσει να ανταποκριθεί στις προκλήσεις της νέας οικονομίας και να πρωταγωνιστήσει στον διαφαινόμενο ανταγωνισμό.

Μέσω αυτού του οράματος ο χρηματοπιστωτικός οργανισμός επιδιώκει να διευρύνει το μερίδιο της αγοράς του μέσω της χρήσης των εναλλακτικών δικτύων (υπηρεσίες ηλεκτρονικής τραπεζικής) και της ανάπτυξης νέων χρηματοοικονομικών προϊόντων και υπηρεσιών. Επίσης, μέσα από τα ηλεκτρονικά κανάλια προώθησης των προϊόντων του οργανισμού επιδιώκεται η μείωση του κόστους και η παροχή καλύτερης ποιότητας εξυπηρέτησης τόσο στον εξωτερικό πελάτη (χρήστη), όσο και στον εσωτερικό (εργαζόμενο).
Με αυτόν τον τρόπο, το όραμα για μια τράπεζα που επιθυμεί να ακολουθήσει μια στρατηγική ηλεκτρονικού επιχειρείν, θα πρέπει να είναι πελατοκεντρικό, προσπαθώντας να παρέχει προϊόντα και υπηρεσίες προσανατολισμένα σε αυτόν, με μικρότερο κόστος και καλύτερη ποιότητα.

Γενικότερα, οι στόχοι που πρέπει να επιτευχθούν μέσω της εφαρμογής μιας στρατηγικής ηλεκτρονικής τραπεζικής είναι οι εξής :

1. Ικανοποίηση της πελατειακής βάσης: Μέσω διευκόλυνσης των συναλλαγών με παροχή καλύτερης ποιότητας εξυπηρέτησης και χωρίς την παρουσία των πελατών στα φυσικά δίκτυα (υποκαταστήματα).

2. Χρηματοοικονομική αποτελεσματικότητα: Μέσω της αύξησης των πωλήσεων και της κερδοφορίας ανά πελάτη αλλά και της διεύρυνσης της πελατειακής βάσης.

3. Εσωτερική αποτελεσματικότητα: Μέσω της αποτελεσματικής διαχείρισης των ανθρώπινων πόρων, την ανάπτυξη συνεργειών εντός της επιχείρησης αλλά και της πλήρης αξιοποίησης των νέων τεχνολογιών.

## 9.3 Εναλλακτικά σενάρια στρατηγικής προσφοράς υπηρεσιών ηλεκτρονικής τραπεζικής.

Οι στρατηγικές που αφορούν την ανάπτυξη και την προσφορά υπηρεσιών ηλεκτρονικής τραπεζικής και γενικότερα της ηλεκτρονικής επιχειρηματικής, από τα χρηματοπιστωτικά ιδρύματα είναι κυρίως δύο.

Η πρώτη περίπτωση αφορά τις τράπεζες που ακολουθούν αμυντική στρατηγική (Defenders) και κατά συνέπεια ακολουθούν το μοντέλο της διεύρυνσης των υπαρχόντων καναλιών διανομής της τράπεζας.

Η δεύτερη στρατηγική αφορά τα χρηματοπιστωτικά ιδρύματα που ακολουθούν επιθετική στρατηγική (Attackers) και στην ουσία αναπτύσσουν ένα νέο μοντέλο λειτουργίας.Και οι δύο στρατηγικές τοποθετήσεις διαφέρουν στην ανάπτυξη της πελατειακή βάσης του οργανισμού, στον αριθμό των παρεχόμενων προϊόντων και υπηρεσιών αλλά και στα κανάλια διανομής των τελευταίων.

Παρακάτω, αναλύονται πιο διεξοδικά οι παραπάνω στρατηγικές.

### 9.3.1. Αμυντική στρατηγική (Defenders)

Τα χρηματοπιστωτικά ιδρύματα τα οποία ακολουθούν τη λεγόμενη αμυντική στρατηγική (Defenders) στις υπηρεσίες ηλεκτρονικής τραπεζικής, προσπαθούν να διευρύνουν τα κανάλια διανομής που ήδη διαθέτουν, χρησιμοποιώντας το διαδίκτυο κυρίως για την παροχή των προϊόντων και των υπηρεσιών τους προς τους πελάτες. Τα υπόλοιπο εναλλακτικά κανάλια (τηλέφωνο, κινητό τηλέφωνο, ATM's ) υποστηρίζουν στην ουσία το κύριο κανάλι (διαδίκτυο) και συμπληρώνουν τα παραδοσιακά κανάλια του οργανισμού (υποκαταστήματα). Συνήθως, οι τράπεζες που ακολουθούν τη συγκεκριμένη στρατηγική, διατηρούν την ίδια εμπορική επωνυμία (brand name),που ήδη γνωρίζουν οι πελάτες της και έχουν ασφάλεια και εμπιστοσύνη σε αυτή.

Επίσης, στην αρχή της εφαρμογής αυτής της στρατηγικής, οι τράπεζες προσφέρουν έναν περιορισμένο εύρος προϊόντων και υπηρεσιών μέσω διαδικτύου στους πελάτες τους, διευρύνοντας και εμπλουτίζοντας τη γκάμα αυτών μετέπειτα.

Συνοπτικά μέσω αυτής της τακτικής επιδιώκεται η διατήρηση της υπάρχουσας πελατειακής βάσης και όχι η προσέλκυση νέας.

### 9.3.2 Επιθετική στρατηγική (Attackers)

Τα χρηματοπιστωτικά ιδρύματα τα οποία ακολουθούν τη λεγόμενη επιθετική στρατηγική (Attackers) στις υπηρεσίες ηλεκτρονικής τραπεζικής, προσπαθούν να χρησιμοποιήσουν το διαδίκτυο ως το κύριο κανάλι προώθησης των προϊόντων τους, το οποίο υποστηρίζεται από τα δευτερεύοντα εναλλακτικά κανάλια (σταθερό τηλέφωνο, κινητό τηλέφωνο, ATM' s). Στην ουσία, οι τράπεζες αυτές, τείνουν να υιοθετήσουν ή και να δημιουργήσουν από την αρχή, ένα καινούργιο μοντέλο λειτουργίας, αρκετά διαφορετικό από αυτό που στηριζόταν στα παραδοσιακά κανάλια (υποκαταστήματα).

Επειδή, στόχος αυτής της πολιτικής είναι η προσέλκυση νέων πελατών (οι οποίοι είναι τακτικοί χρήστες του διαδικτύου), οι τράπεζες συνήθως δημιουργούν μια καινούργια εμπορική επωνυμία (brand name).
Χαρακτηριστικό παράδειγμα στον Ελληνικό τραπεζικό χώρο, είναι η εμπορική επωνυμία "Winbank " που αφορά τις ηλεκτρονικές υπηρεσίες της τράπεζας Πειραιώς.
Οι τράπεζες που ακολουθούν επιθετική πολιτική, προσφέρουν ένα ολοκληρωμένο εύρος προϊόντων είτε αρχικά, είτε στη συνέχεια της πορείας τους.

Στην επόμενη ενότητα ακολουθεί ένα παράδειγμα μιας συγκεκριμένης στρατηγικής, η στρατηγική άμεσης επέκτασης σε νέες αγορές.

### 9.3.3. Στρατηγική άμεσης επέκτασης σε νέες αγορές.

Η συγκεκριμένη στρατηγική αφορά τράπεζες που επιθυμούν να αξιοποιήσουν και να υιοθετήσουν συστήματα ηλεκτρονικής τραπεζικής και να επεκταθούν σε νέες αγορές, παίζοντας πρωταγωνιστικό ρόλο σε αυτές. Φυσικά, σε κάθε περίπτωση τα φυσικά κανάλια προώθησης των τραπεζικών προϊόντων και υπηρεσιών (υποκαταστήματα) θα διατηρηθούν, ενώ θα δημιουργηθούν νέα κανάλια που θα λειτουργούν συμπληρωματικά, τα λεγόμενα εναλλακτικά κανάλια (διαδίκτυο, σταθερό τηλέφωνο, κινητό τηλέφωνο).

Από τη χρησιμοποίηση των ηλεκτρονικών δικτύων, η τράπεζα στοχεύει, με τη συγκεκριμένη στρατηγική, στη διεύρυνση του μεριδίου αγοράς της αλλά και στο σχηματισμό μιας νέας εικόνας προς τους πελάτες της. Συγκεκριμένα, αποσκοπεί στην οριζόντια διείσδυση σε νέα τμήματα της αγοράς όπως η λιανική τραπεζική, οι μεγάλες επιχειρήσεις, οι νέοι επιχειρηματίες κ.ο.κ. Στην ουσία επιθυμεί να γίνει η ίδια πρωταγωνιστής στο ανταγωνιστικό τοπίο της νέας ψηφιακής εποχής μέσα από μια ενιαία παροχή τραπεζικών προϊόντων και υπηρεσιών (φυσικά δίκτυα + εναλλακτικά δίκτυα) αλλά και μια μεγάλη ποικιλία προσφερόμενων υπηρεσιών προς τους πελάτες. Το πλαίσιο της παραπάνω στρατηγικής εστιάζεται κυρίως στα εξής σημεία:

1. Προώθηση τόσο των παραδοσιακών τραπεζικών προϊόντων και υπηρεσιών, όσο και νέων πιο εξειδικευμένων, που πιθανόν να απευθύνονται σε άλλες κατηγορίες πελατών.

2. Προσέλκυση νέων πελατών, διατήρηση των υπαρχόντων και γενικά αύξηση της κερδοφορίας ανά πελάτη, δημιουργώντας μια κρίσιμη μάζα "πιστών" πελατών.

3. Ολοκληρωμένη εκπαίδευση του τμήματος ανθρωπίνου δυναμικού στη χρήση των νέων τεχνολογιών.

4. Μείωση του λειτουργικού κόστους της τράπεζας και ιδιαίτερα στα εναλλακτικά δίκτυα.

5. Προσπάθεια ανάπτυξης στρατηγικών συμμαχιών με άλλες επιχειρήσεις για την παροχή των προϊόντων και των υπηρεσιών των τελευταίων, μέσα από τα εναλλακτικά δίκτυα της τράπεζας.

*Συμπέρασμα:*

Από όλες τις παραπάνω πληροφορίες αυτού του κεφαλαίου,συμπεραίνουμε πόσο σημαντική είναι η υιοθέτηση ορισμένων κρίσιμων στρατηγικών ώστε να επιτευχθεί η εξέλιξη καθώς και η διάρκειά στο τη χρησιμοποίησης της πληροφορικής στο τραπεζικό σύστημα. Ανάλογα δηλαδή τι στόχο επιδιώκει να πετύχει η κάθε τράπεζα, υιοθετεί και την κατάλληλη στρατηγική, ή ακόμα συνδυάζει σε ένα βαθμό περισσότερες από μία διαφορετικές στρατηγικές.

# ΚΕΦΑΛΑΙΟ 10
# Κίνδυνοι ηλεκτρονικών τραπεζικών συναλλαγών και περιπτώσεις ηλεκτρονικών επιθέσεων.

## 10.1 Κίνδυνοι στα συστήματα συναλλαγών ηλεκτρονική τραπεζικής.

Αν και οι ηλεκτρονικές επιθέσεις δεν αποτελούν νέο φαινόμενο, η συχνότητά τους τα τελευταία χρόνια αυξάνεται μια και όλο και περισσότερες τράπεζες παρέχουν στους πελάτες τους on-line υπηρεσίες. Η αύξηση αυτή δεν είναι τεράστια, εντούτοις όμως αποτελεί ένα ανησυχητικό φαινόμενο μια και πολλοί θεωρούν τις οικονομικές πληροφορίες που τους αφορούν άκρως απόρρητες και διατηρούν μια επιφυλακτική στάση απέναντι σε διαδικασίες που τις καθιστούν ευάλωτες στο ευρύ κοινό, όπως είναι το E-Banking.

Στοιχεία για το ηλεκτρονικό έγκλημα δεν κοινοποιούνται δημοσίως, αλλά υπολογίζεται ότι στις Η.Π.Α. χάνονται ετησίως περίπου 11 δισεκατομμύρια δολάρια από εταιρείες και καταναλωτές λόγω αυτής της μορφής εγκλήματος. Το μεγαλύτερο μέρος προέρχεται από οικονομικά ιδρύματα. Μάλιστα το μεγαλύτερο μέρος των ζημιών δεν προκύπτει από τις κλοπές χρημάτων, αλλά από έξοδα που κάνουν οι εταιρείες μετά από τέτοιου είδους επιθέσεις, προκειμένου να διασφαλίσουν τα συστήματά τους ώστε να μην ξανασυμβούν.

Ειδικοί σε θέματα ασφάλειας έχουν υπολογίσει ότι μια τράπεζα μπορεί να ξοδέψει μέχρι και ένα εκατομμύριο δολάρια σε εξοπλισμό και συμβούλους ασφάλειας προκειμένου να διορθώσει τις ατέλειες και να κλείσει τις «τρύπες» στο σύστημά της.

Το πρόβλημα πάντως δεν προβάλλεται στις πλήρεις του διαστάσεις για ευνόητους λόγους. Οι μεγαλύτερες και εντυπωσιακότερες επιθέσεις είναι αυτές που θα δοθούν στη δημοσιότητα, οι υπόλοιπες και περισσότερες, κρατούνται κρυφές. Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους πάντως να επιτύχουν τους σκοπούς τους.

Παρά τις οποιεσδήποτε τεχνικές αδυναμίες των συστημάτων για online banking, οι μεγαλύτεροι κίνδυνοι προέρχονται από τον ανθρώπινο παράγοντα. Έρευνες που έχουν γίνει από ειδικούς σε θέματα ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είχαν την εκούσια ή ακούσια βοήθεια και κάποιου που εργαζόταν στην τράπεζα.

Και χωρίς τη βοήθεια εκ των έσω, πάντως, οι εισβολείς μπορούν να εκμεταλλευτούν την πρόσβαση που έχουν οι πελάτες της τράπεζας από το σπίτι τους, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια.Οι άνθρωποι αυτοί αποτελούν τους πιο προκλητικούς στόχους, μια και δεν έχουν συνείδηση του μεγέθους της ζημιάς που μπορούν να κάνουν ανοίγοντας απλά μια επισύναψη στο ηλεκτρονικό τους ταχυδρομείο ή ακολουθώντας ένα link.Οι απλοί χρήστες πέφτουν πολύ εύκολα θύματα προγραμμάτων που υποτίθεται ότι κάνουν κάτι χρήσιμο για αυτούς, αλλά στην πραγματικότητα ανοίγουν «τρύπες» ασφάλειας στο σύστημα επιτρέποντας σε χάκερ, να έχουν πρόσβαση σε αυτό.

Οι κλεμμένες πληροφορίες αποτελούν την πρώτη φάση μιας αρκετά επίπονης διαδικασίας η οποία μπορεί να διαρκέσει μέχρι και εβδομάδες, έτσι ώστε ο χάκερ να υποδυθεί κάποιον άλλο στο διαδίκτυο. Η οποία όμως διευκολύνεται συνεχώς με καινούρια προγράμματα που κυκλοφορούν στην αγορά. Η εποχή που πολλές επιθέσεις θα γίνονται με αυτοματοποιημένο τρόπο δεν απέχει πολύ, σύμφωνα με αρκετούς ειδικούς.

Μια άλλη μέθοδος που τις περισσότερες φορές έχει αποτελέσματα δεν επικεντρώνεται στην τράπεζα ευθέως, αλλά σε μια από τις εταιρείες που συνεργάζονται με αυτήν προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με τους πελάτες της.

Σε πολλές περιπτώσεις οι τράπεζες επιτρέπουν στις εταιρείες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, ο εισβολέας θα πρέπει να μελετήσει τον τρόπο με τον οποίο οι εταιρείες επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα. Μόλις βρεθεί μια αδυναμία κάνουν την κίνησή τους.

Ένας άλλος τρόπος είναι να χτυπήσουν τις μικρές, τοπικές τράπεζες οι οποίες μπήκαν στον τομέα του E-Banking εσπευσμένα προκειμένου να διατηρήσουν τον ανταγωνισμό με τις μεγαλύτερες τράπεζες.

Δυστυχώς όμως λόγω αυτής της βιασύνης, οι τράπεζες αφήνουν πολλές «τρύπες» στα συστήματά τους, κάτι που οι επίδοξοι εισβολείς εκμεταλλεύονται πολύ εύκολα. Οι ειδικοί μας πληροφορούν ότι κλοπές ποσών από 5 μέχρι 10 χιλιάδες δολαρίων μπορούν να πραγματοποιηθούν σε χρονικό διάστημα μερικών εβδομάδων. Για ποσά μέχρι και 1 εκατομμυρίου δολαρίων χρειάζονται 4 μέχρι και 6 μήνες.

Αυτές οι απειλές και οι επιθέσεις μπορεί να είναι:

- Υποκλοπή απορρήτων πληροφοριών

- Κατάρρευση του συστήματος από επιθέσεις Denial-of- service, (οι εισβολείς μπορούν να γεμίσουν το σύστημα με εκατομμύρια αιτήσεων και να το οδηγήσουν σε κατάρρευση).

- Ιοί που μπορούν να καταστρέψουν κάποια αρχεία ή ολόκληρο το σύστημα.

Τα απόρρητα δεδομένα μπορεί να καταλήξουν σε λάθος χέρια. Αυτού του είδους οι υποκλοπές θεωρούνται παράνομες. Έτσι, οι υποκλοπές υπάρχει πιθανότητα να έχουν ως φυσικό επακόλουθο τις εξής απώλειες:

- Μείωση φήμης πελατείας.

- Συρρίκνωση μεριδίου αγοράς.

- Μείωση τιμής μετοχής.

## 10.2 Περιπτώσεις ηλεκτρονικών επιθέσεων.

Ποιος:Citibank

Πότε:1994

Περιστατικό:Ο Ρώσος χάκερ Βλαντιμίρ Λέβιν απέσπασε πόσο από λογαριασμούς της Citibank που υπολογίστηκε ότι ανερχόταν στα 10 εκατομμύρια δολάρια. Απέκτησε πρόσβαση στα δίκτυα της τράπεζας από την Αγία Πετρούπολη στη Ρωσία. Όταν συνελήφθη από την Σκότλαντ Γιαρντ και το FBI, παραδέχτηκε ότι χρησιμοποίησε κλεμμένους κωδικούς και passwords από πελάτες της τράπεζας και μετέφερε ποσά στο λογαριασμό του. Το 1998, ένα δικαστήριο στις Η.Π.Α. τον καταδίκασε σε 3χρόνια κάθειρξη. Η τράπεζα ανέκτησε όλο το ποσό εκτός από 400.000 δολάρια.

Ποιος: Barclays Bank

Μια αγγλική τράπεζα που ισχυρίζεται ότι διαχειρίζεται τους περισσότερους online λογαριασμούς σε όλο το Ηνωμένο Βασίλειο.

Πότε: Ιούλιος 2000

Περιστατικό: Ένα ελάττωμα στο λογισμικό του συστήματος της τράπεζας επέτρεπε στους πελάτες της να βλέπουν τις λεπτομέρειες των λογαριασμών των υπόλοιπων πελατών. Η τράπεζα έκλεισε το σύστημα μόλις ανακάλυψε το πρόβλημα.

Ποιος: ABN AMRO

Μια ολλανδική πολυεθνική τράπεζα.

Πότε: Σεπτέμβριος 2000

Περιστατικό: Ένα ολλανδικό τηλεοπτικό πρόγραμμα αποκάλυψε πως χάκερs, έκλεβαν σημαντικές πληροφορίες των πελατών της τράπεζας. Οι χάκερs έστελναν στους πελάτες της τράπεζας μηνύματα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι προέρχονταν από την τράπεζα. Τα mails αυτά εγκαθιστούσαν στους υπολογιστές των πελατών προγράμματα τα οποία επέτρεπαν στους χάκερ να έχουν πρόσβαση σε κρίσιμες πληροφορίες των λογαριασμών τους και με αυτόν τον τρόπο να μεταφέρουν χρήματα από αυτούς.

Ποιος: E*Trade

Πότε: Σεπτέμβριος 2000

Περιστατικό: Η εταιρεία παραδέχτηκε πως ο δικτυακός της τόπος είχε ένα τρωτό σημείο από όπου κάποιος χάκερ θα μπορούσε να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα. Ο προγραμματιστής που το ανακάλυψε δήλωσε πως ένας χάκερ εκμεταλλευόμενος το πρόβλημα αυτό, θα μπορούσε να αποκτήσει τον κωδικό και το username κάθε χρήστη.

Ποιος: Contour Software

Μια εταιρεία με βάση στην Καλιφόρνια που αναπτύσσει λογισμικό επεξεργασίας υποθηκών που χρησιμοποιείται από πολλές επιχειρήσεις.

Πότε: Νοέμβριος 2000

Περιστατικό: Ένα πρόβλημα στο λογισμικό αποκάλυψε πληροφορίες για τη δανειοληπτική κατάσταση 700 περίπου αμερικανών στο διαδίκτυο. Αντιπρόσωπος της εταιρείας χαρακτήρισε το συμβάν σπάνιο και κατηγόρησε ένα πρώην εργαζόμενο της εταιρείας, ότι απενεργοποίησε τις ρυθμίσεις ασφαλείας.

Ποιος: Nara Bank, Western Union, Central National Bank – Waco (Texas) κ.α
Πότε: Απρίλιος 2001
Περιστατικό: Αμερικανοί εισαγγελείς κατηγόρησαν δύο Ρώσους για ηλεκτρονικά εγκλήματα που σχετίζονταν με μια σειρά επιθέσεων σε δίκτυα τραπεζών και άλλων εταιρειών. Οι δύο χάκερς, εισέβαλαν στα συστήματα των εταιρειών, έκλεψαν πολύτιμες πληροφορίες και κατόπιν εμφανίζονταν στις εταιρείες ως σύμβουλοι ασφάλειας και προσέφεραν τις υπηρεσίες τους για διορθωθούν τα σφάλματα.

*Συμπέρασμα:*

Από όλα τα παραπάνω συνπεραίνουμε πως πραγματικά είναι δικαιολογημένο που υπάρχουν ακόμα πολλοί ανασταλτικοί παράγοντες που επηρεάζουν τους πελάτες αρνητικά στο να χρησιμοποιήσουν το νέο αυτό τροπο συναλλαγών της ηλεκτρονικής τραπεζικής. Ωστόσο όμως, παρά τα διάφορά περιστατικά και τους διάφορους άλλους κινδύνους που υπάρχουν όσον αφορά την ασφάλεια των συναλλαγών αυτών, οι τράπεζες λαμβάνουν όλα αυτά τα δεδομένα υπ' ό ψιν τους και προσπαθούν με κάθε τρόπο ώστε να καλυτερεύουν τα διάφορα συστήματα το συντομότερο δυνατό ώστε να αποκτήσουν ή ακόμα και να εμπνεύσουν την εμπιστοσύνη του πελάτη με κυρίαρχο στόχο να χρησιμοποιήσει αυτές τις παρεχόμενες ηλεκτρονικές τραπεζικές συναλλαγές.


# ΚΕΦΑΛΑΙΟ 11

# Βασικά θέματα ασφαλείας των ηλεκτρονικών τραπεζικών συναλλαγών.

## 11.1 Τι περιλαμβάνουν τα βασικά θέματα ασφαλείας:

### 11.1.1 Η προστασία του υπολογιστή

Ενδεικτικά αναφέρονται τα κατωτέρω μέτρα προστασίας:

1. Ενημέρωση και αναβάθμιση των παραμέτρων ασφάλειας του υπολογιστή μας. συμπεριλαμβανομένου και του λειτουργικού μας συστήματος.

2. Εγκατάσταση προγραμμάτων στον υπολογιστή για την προστασία του από ιούς. Η εμφάνιση νέων και εξελιγμένων ιών καθιστά τη συχνή ανανέωση των προγραμμάτων που τους καταπολεμούν απαραίτητη.

3. Προσοχή κατά τη χρήση της υπηρεσίας E-Banking από υπολογιστές οι οποίοι δεν μας ανήκουν, όπως ενδεικτικά σε αεροδρόμια, internet cafe, κ.λπ.

4. Συχνή αλλαγή κωδικών πρόσβασης.

5. Προστασία ηλεκτρονικού ταχυδρομείου.

Ωστόσο θα πρέπει:

- Να ενημερώνουμε το λειτουργικό σύστημα του υπολογιστή μας με τις τελευταίες εκδόσεις που υπάρχουν σε θέματα ασφάλειας.

- Να ενεργοποιούμε πρόγραμμα που δεν επιτρέπει να ανοίγουν αυτόματα παράθυρα (pop up blocker). Σε περίπτωση που επισκεφτούμε website όπου η πληροφορία που χρειάζεστε είναι διαθέσιμη μέσω pop up window, θα πρέπει να απενεργοποιήσουμε το εν λόγω πρόγραμμα. Συνιστάται η εγκατάσταση προγραμμάτων προστασίας (antispyware, antivirus, firewall) του υπολογιστή μας.

### 11.1.2 Προγράμματα Antivirus – Antispyware.

1. Τα προγράμματα Antispyware μας προφυλάσσουν από την εγκατάσταση προγραμμάτων που καταγράφουν τις κινήσεις σας στο Internet, ενώ παράλληλα απομακρύνουν ήδη τέτοια εγκατεστημένα προγράμματα.

2. Τα προγράμματα αντιμετώπισης ιών (AntisVirus) μας προστατεύουν από ιούς που μπορούν να προκαλέσουν ποικίλα προβλήματα στον υπολογιστή μας. Το λογισμικό αυτό θα πρέπει:

- Να ενεργοποιείται αυτόματα κατά τη φόρτωση του λειτουργικού συστήματος.

- Να παραμένει συνεχώς ενεργό.

- Να ενημερώνεται αυτόματα σε τακτικά χρονικά διαστήματα.

Όλα τα σύγχρονα antivirus χρησιμοποιούν βάσεις υπογραφών ιών (virus signature databases) για την ανίχνευση υπαρχόντων, γνωστών ιών.Βέβαια, όλα τα antivirus δεν είναι εξίσου αποτελεσματικά.

Τα πλέον προηγμένα διακρίνονται για τις εξελιγμένες μηχανές ανίχνευσης που ενσωματώνουν,οι οποίες είναι σε θέση να εντοπίζουν:
Πολυμορφικούς/μεταμορφικούς ιούς καθώς και νέους ιούς για τους οποίους δεν είναι ήδη ενήμερες οι βάσεις τους.

### 11.1.3 Ασφάλεια κωδικών πρόσβασης.

Ως προς τους κωδικούς πρόσβασης που χρησιμοποιούνται για τις διαδικτυακές συναλλαγές:

- Θα πρέπει να αλλάζουμε συχνά τους κωδικούς πρόσβασης και πάντα στην περίπτωση που υποψιαζόμαστε ότι έχουν εκτεθεί.

- Καλό θα ήταν να μην χρησιμοποιούμε ως κωδικό πρόσβασης την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να βρεθούν και από άλλα έγγραφα

- Θα πρέπει να αποφεύγουμε να έχουμε τον προσωπικό μας κωδικό πρόσβασης μέσα σε πορτοφόλια, τσάντες ή ατζέντες. Σε περίπτωση απώλειας ή κλοπής τους θα διευκολύνουμε πολύ τους δράστες.

- Αποφεύγουμε να χρησιμοποιούμε τους ίδιους κωδικούς πρόσβασης σε περισσότερες από μια κάρτες σας.

- Δε πρέπει να δίνουμε τον κωδικό πρόσβασης μας σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεστεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό πρόσβασης για επαλήθευση, δε πρέπει να το δώσουμε.

Οι Τράπεζες δεν ακολουθούν αυτή την πρακτική. Εάν έχουμε αναγνώριση κλήσης, θα πρέπει να καταγράψουμε τον αριθμό που αναγράφηκε στην τηλεφωνική μας συσκευή και να ενημερώσουμε αμέσως την Αστυνομία.

- Επικοινωνούμε με την τράπεζά αν νομίζουμε ότι κάποιος γνωρίζει τον κωδικό μας πρόσβασης στην υπηρεσία Internet banking.

- Απενεργοποιούμε τη λειτουργία «Αυτόματης Καταχώρησης» του προγράμματος περιήγησης. Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή, γεγονός που τους καθιστά έκθετους.

- Κάνουμε αγορές μόνο από γνωστές εταιρείες που μας παρέχουν εγγυήσεις ασφάλειας. Αν κάνουμε συχνά αγορές από το διαδίκτυο, χρησιμοποιούμε μια κάρτα, αποκλειστικά για αυτή τη χρήση. Έτσι, αν πέσετε θύμα απάτης δεν θα χρειαστεί να ακυρώσουμε όλες τις κάρτες μας.

- Προστατεύουμε τον υπολογιστή μας με κωδικό πρόσβασης προκειμένου να αποτρέψουμε την πρόσβαση σε αυτόν μη εξουσιοδοτημένων χρηστών.

### 11.1.4 Προστασία ηλεκτρονικού ταχυδρομείου.

Προκειμένου να αποκτήσουν οι κακόβουλοι χρήστες απομακρυσμένη πρόσβαση σε συστήματα τρίτων συνηθίζουν να στέλνουν μηνύματα με συνημμένα αρχεία είτε μέσω ηλεκτρονικού ταχυδρομείου (email) είτε μέσω λογισμικών αποστολής στιγμιαίων μηνυμάτων (chat, irc, msn). Συνεπώς, ένας καλός κανόνας προφύλαξης είναι να μην ανοίγουμε τέτοια αρχεία όταν δε γνωρίζουμε τον αποστολέα του μηνύματος.
Ωστόσο, υπάρχουν περιπτώσεις κατά τις οποίες είτε δεν τηρούμε τον παραπάνω κανόνα είτε κάποιος γνωστός μας στέλνει ένα συνημμένο αρχείο που περιέχει ιό - χωρίς να το ξέρει ο ίδιος φυσικά. Σε αυτά τα ενδεχόμενα το antivirus αναλαμβάνει να μας προστατέψει εξετάζοντας το περιεχόμενο των αρχείων πριν το άνοιγμα τους. Αν παρόλα αυτά ένα συνημμένο αρχείο περιέχει trojan και το antivirus δεν καταφέρει να το εντοπίσει τότε αυτό θα ενεργοποιηθεί με το άνοιγμα του. Το trojan αφού ενεργοποιηθεί θα προσπαθήσει να καταγράψει τους κωδικούς και να τους στείλει σε κάποιον κακόβουλο χρήστη μέσω διαδικτύου.

- Τα προγράμματα τείχους προστασία (Firewall) εμποδίζουν την εισχώρηση προγραμμάτων ή ιών στον υπολογιστή μας χωρίς τη δική μας άδεια.
  Καταρχήν, η χρήση ενός τείχους προστασίας (firewall) κρίνεται απαραίτητη. Το firewall σε γενικές γραμμές αποτρέπει τις ανεπιθύμητες εισερχόμενες και εξερχόμενες συνδέσεις προς και από τον υπολογιστή μας.

- Δε θα πρέπει να αποστέλλουμε απόρρητα προσωπικά δεδομένα μέσω ηλεκτρονικού ταχυδρομείου.

- Δε θα πρέπει να απαντάμε σε μηνύματα που ζητούν να επιβεβαιώσουμε προσωπικές πληροφορίες (π.χ. αριθμούς πιστωτικών καρτών, passwords κ.λ.π.) ακόμα και εάν φαινομενικά ο αποστολέας είναι γνωστός. Καμία τράπεζα δεν ζητά τέτοιες πληροφορίες και μάλιστα με ένα απλό e-mail.

- Πρέπει να διαγράφουμε ηλεκτρονικά μηνύματα που λαμβάνουμε από άγνωστες πηγές.

- Καλό είναι να αποφεύγουμε να συμπληρώνουμε ηλεκτρονικές φόρμες που παραλαμβάνουμε με email.

- Θα πρέπει να μην ανοίγουμε αρχεία τύπου .exe, .pif, .vbs, .bat που παραλαμβάνουμε με ηλεκτρονικό ταχυδρομείο, διότι είναι πολύ πιθανόν να μεταφέρουν ιούς και θα πρέπει να διαγράφονται άμεσα.

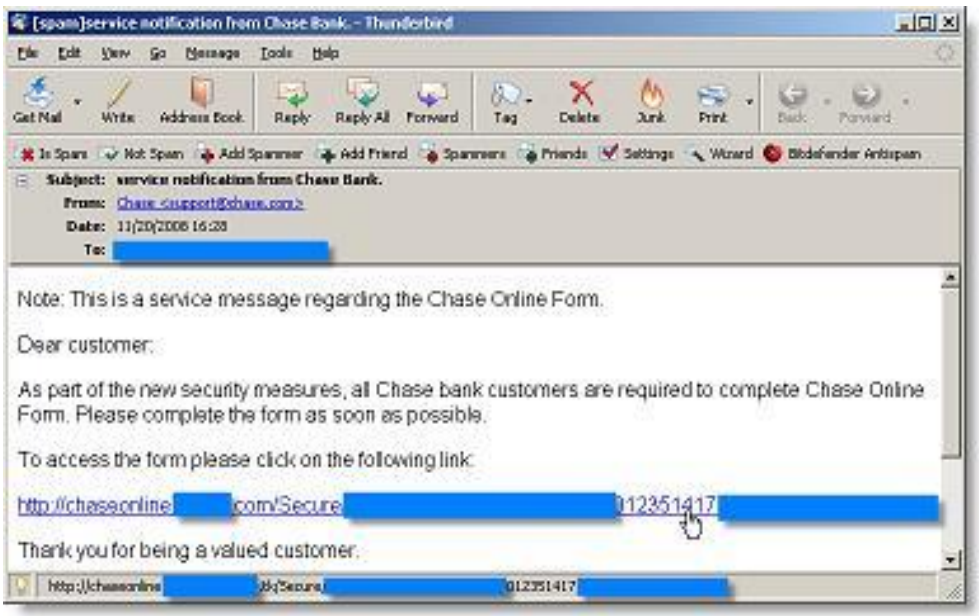
- Πρέπει να προσέχουμε σε ποια sites κάνουμε εγγραφή. Ορισμένοι αποστολείς spam προμηθεύονται καταλόγους ηλεκτρονικών διευθύνσεων από αυτά τα sites. Επίσης, μπορούν να προμηθευτούν την ηλεκτρονική μας διεύθυνση από ομάδες συζητήσεων (chat rooms), κανάλια συνομιλίας κ.λ.π.

Για το λόγο αυτό, όταν κάνουμε εγγραφή σε άλλα sites είναι καλύτερα να χρησιμοποιούμε διαφορετικό email address από το προσωπικό μας.

- Να μην επισκεπτόμαστε websites χρησιμοποιώντας links που παραλάβαμε με e-mail. Καλύτερα να πληκτρολογούμε τη διεύθυνση που επιθυμούμε να επισκεφθούμε απευθείας στον browser.

- Θα πρέπει να βεβαιωθούμε ότι ο Internet Provider που χρησιμοποιούμε μας παρέχει προστασία από ιούς σε εισερχόμενα ηλεκτρονικά μηνύματα.

- Θα πρέπει να εγκαταστήσουμε ψηφιακό φίλτρο που μπλοκάρει τα spam emails. Να μην επιλέγουμε την αυτόματη διαγραφή τους, αλλά την προσωρινή τοποθέτησή τους σε κάποιο φάκελο ξεχωριστό από τον φάκελο των εισερχομένων.



## 11.1.5 Ασφάλεια ATM.


1. Ο προσωπικός κωδικός ασφαλείας PIN απενεργοποιείται αυτόματα, αν εισαχθεί λανθασμένα στο ATM τέσσερις φορές.

2. Ηχητικά / οπτικά σήματα και οθόνες μας καθοδηγούν στα βήματα κάθε συναλλαγής προειδοποιώντας μας σε περίπτωση που ξεχνάμε την κάρτα ή τα χρήματά μας στο ATM.

Αν παρ' όλα αυτά ξεχάσουμε την κάρτα ή τα χρήματά μας στο ATM, σε εύλογο χρονικό διάστημα, το μηχάνημα δεσμεύει στο εσωτερικό του την κάρτα ή τα χρήματα. Επίσης:

-Ο κωδικός ασφαλείας PIN είναι αυστηρά προσωπικός και απόρρητος.Τον απομνημονεύουμε και δεν τον γνωστοποιούμε σε κανέναν.

-Μόλις παραλάβουμε την κάρτα μας, υπογράφουμε με στυλό στην ταινία που βρίσκεται στο πίσω μέρος της.

-Δε θα πρέπει να διστάζουμε να αλλάξουμε τον κωδικό PIN μας απο το μενού συναλλαγών των ATM.Όταν πληκτρολογούμε τον κωδικό PIN στο ATM, βεβαιωνόμαστε ότι δεν γίνεται ορατός σε τρίτους.

*Συμπέρασμα:*
Παρατηρούμε πως η πρόοδος τη τεχνολογίας έχει συμβάλλει στο να μπορούν να αντιμετωπιστούν σε αρκετά ικανοποιητικό βαθμό οι διάφοροι παράγοντες κινδύνου οι οποίοι απειλούν τη χρήση των ηλεκτρονικών τραπεζικών συναλλαγών. Το βέβαιο όμως είναι,ότι δε θα πρέπει να επαναπαυόμαστε αλλά να βρισκόμαστε συνέχεια σε επαγρύπνηση για τους νέους και δίαφορους κινδύνους που μπορεί να υπάρξουν,καθώς και να είμαστε όσο το δυνατόν περισσότερο φειδωλοί στη χρήση των υπηρεσιών αυτών.

# ΚΕΦΑΛΑΙΟ 12
# Ταυτοποίηση χρήστη στις ηλεκτρονικές τραπεζικές συναλλαγές.

## 12.1 Είδη ταυτοποίησης χρήστη.

Οι τράπεζες επικεντρώνουν τις προσπάθειές τους στη διασφάλιση της συναλλαγής με τον τελικό χρήστη, σε όλα τα στάδια που περιλαμβάνονται μέχρι την επιτυχή ολοκλήρωσή τους. Μία από τις δικλείδες ασφαλείας των συναλλαγών του πελάτη είναι το πρώτο στάδιο όπου πραγματοποιείται η ταυτοποίηση του χρήστη. Όταν ο πελάτης εγγραφεί στις υπηρεσίες της ηλεκτρονικής τραπεζικής, μετά την πάροδο λίγων ημερών θα του αποσταλούν σε ειδικό φάκελο ασφαλείας οι κωδικοί πρόσβασης του.

Το επόμενο βήμα λοιπόν είναι η σύνδεση και ταυτοποίηση του χρήστη στην αντίστοιχη ιστοσελίδα της τράπεζας, για να ξεκινήσει τις συναλλαγές του.

Η κάθε τράπεζα όμως χρησιμοποιεί διαφορετικούς τρόπους πρόσβασης στις υπηρεσίες της ηλεκτρονικής τραπεζικής και κατά συνέπεια επηρεάζεται και ο βαθμός ασφάλειας που απολαμβάνουν οι χρήστες.
Έτσι, ανάλογα με την πολιτική ασφαλείας που ακολουθεί ο κάθε χρηματοπιστωτικός οργανισμός, υπάρχουν διάφορα είδη ταυτοποίησης του χρήστη και πρόσβασής του στις υπηρεσίες ηλεκτρονικής τραπεζικής μέσω του διαδικτύου (internet banking). Ειδικότερα, τα είδη ταυτοποίησης είναι τα εξής:

### 12.1.1 Ταυτοποίηση με όνομα – κωδικός χρήστη. (User name – Password)

Αποτελεί την πιο συνηθισμένη μέθοδο πρόσβασης (ειδικά στις Ελληνικές τράπεζες) αλλά και την πλέον αδύναμη σε σύγκριση με τις άλλες προηγμένες που υπάρχουν. Η ευκολία αυτού του τρόπου πρόσβασης είναι προφανής, καθώς ο χρήστης θα πρέπει να θυμάται μόνο 2 κωδικούς, που κατά κανόνα τον έναν (username) τον επιλέγει ο ίδιος κατά την εγγραφή του.

Για λόγους ασφαλείας, κοινή πρακτική των τραπεζών είναι να μπλοκάρουν τους κωδικούς των πελατών τους, σε συνεχείς λανθασμένες καταχωρήσεις από την πλευρά τους. Βέβαια, ο αναφαινόμενος κίνδυνος εδώ, είναι να υποκλέψει κάποιος αυτούς τους προσωπικούς κωδικούς του πελάτη και να πραγματοποιήσει συναλλαγές στο όνομά του.

Υπάρχουν πολλοί τρόποι υποκλοπής των κωδικών που "κυκλοφορούν" στο διαδίκτυο από επίδοξους χάκερs, γι' αυτό το λόγο πρέπει να είναι κρυπτογραφημένοι με κάποιον κώδικα (π.χ. 128 bit). Η κρυπτογράφηση των προσωπικών κωδικών των χρηστών, από τη στιγμή που πληκτρολογούνται από τους ίδιους στην ιστοσελίδα της τράπεζας (και "κυκλοφορούν" στο διαδίκτυο), είναι ζήτημα που άπτεται της ακολουθούμενης πολιτικής των τραπεζών.

Επίσης, τα χρηματοπιστωτικά ιδρύματα είναι υπεύθυνα για θέματα καθορισμού του κατάλληλου μήκους κωδικού (αριθμός ψηφίων), απενεργοποίησης των κωδικών (μετά από ορισμένο χρονικό διάστημα) και τερματισμού (log-out) της σύνδεσης χρηστών μετά από ένα χρονικό διάστημα μη χρήσης των υπηρεσιών.

Σε κάθε περίπτωση οι τράπεζες πρέπει να ενημερώνουν τους χρήστες της ηλεκτρονικής τραπεζικής για το ευαίσθητο θέμα της ασφάλειας τους, προτρέποντας τους για παράδειγμα, την αλλαγή των προσωπικών τους κωδικών ανά τακτά χρονικά διαστήματα.


Τα τελευταία χρόνια μερικές τράπεζες έχουν υιοθετήσει για λόγους επιπρόσθετης ασφάλειας, τα λεγόμενα "εικονικά πληκτρολόγια". Αυτά δημιουργήθηκαν για να αποτρέψουν ορισμένους επιτήδειους από την κλοπή κωδικών (και αριθμών πιστωτικών καρτών) μέσω της πληκτρολόγησης του χρήστη. Αυτό λοιπόν το πρόβλημα της "καταγραφής πληκτρολογήσεων" (key logging) αποφεύγεται μέσω της εγκατάστασης κατάλληλου υλικού ή λογισμικού στον υπολογιστή του χρήστη της ηλεκτρονικής τραπεζικής.

### 12.1.2 Ταυτοποίηση μέσω των κωδικών TAN :

Οι αριθμοί ή λίστες TAN (Transaction Authorization Numbers) είναι μια επιπλέον μέθοδος ταυτοποίησης και άρα και ασφάλειας των συναλλαγών. Στην ουσία είναι κάποιοι επιπλέον μοναδικοί κωδικοί αριθμοί σε λίστα, οι οποίοι παρέχονται στον πελάτη (μετά από αίτησή του) και τους χρησιμοποιεί κατά την είσοδό του στις υπηρεσίες ηλεκτρονικής τραπεζικής.

Οι κωδικοί TAN είναι πλέον απαραίτητοι σε κάθε συναλλαγή E-Banking. Αντίθετα με τις πιστωτικές κάρτες, στο E-Banking η κάθε τράπεζα έχει τον απόλυτο έλεγχο της πολιτικής και των μηχανισμών ασφάλειας που επιθυμεί να εφαρμόσει.

Έτσι, μπορεί να επιβάλλει την εξουσιοδότηση κάθε εγχρήματης συναλλαγής ξεχωριστά με ειδικό κωδικό μιας χρήσης. Αυτό στην πράξη γίνεται με την χορήγηση λίστας πρόσθετων κωδικών εξουσιοδότησης στους πελάτες του E-Banking, κάτι σαν password μιας χρήσης προσωπικά σε κάθε πιστοποιημένο πελάτη της

Στην περίπτωση του E-Banking τα πράγματα είναι κάπως πιο περίπλοκα στο θέμα της εταιρικής/τραπεζικής ευθύνης, αλλά εδώ υπάρχει σαφώς αυστηρότερος έλεγχος από την ίδια την τράπεζα σε ότι αφορά το επίπεδο ασφάλειας των συναλλαγών, σε σχέση με την αντίστοιχη ηλεκτρονική χρήση των πιστωτικών καρτών.

Πρακτικά, η τράπεζα επιβάλλει μια σειρά πρόσθετων μηχανισμών ασφαλείας που δεν υπάρχουν στην περίπτωση των πιστωτικών καρτών, πράγμα που κάνει το σύστημα ουσιαστικά απαραβίαστο αν η χρήση των μηχανισμών αυτών είναι σωστή από την πλευρά του πελάτη (π.χ. χρήση λίστας κωδικών TAN, Transaction Authorization Numbers – Αριθμοί Εξουσιοδότησης Συναλλαγής).

Παρόλα αυτά, αν ο πελάτης κατά λάθος καταστεί θύμα απάτης από websites παραποίησης ταυτότητας, δηλαδή δώσει τα στοιχεία του σε κόμβο που προσποιείται ότι είναι αυτός της τράπεζας, η ίδια η τράπεζα λέει ότι εφόσον έχει ενημερώσει σχετικά τον πελάτη της και αυτός έκανε κάτι εκτός του δικού της δικτύου, δεν φέρει καμία απολύτως ευθύνη (εδώ δεν ισχύει η αρχή της απόδειξης της μη-εντιμότητας όπως για τις πιστωτικές κάρτες). Μάλιστα, στους όρους χρήσης της λίστας κωδικών TAN γνωστής τράπεζας αναφέρεται ρητά ότι:

*"...Κανένας άλλος δεν πρέπει να γνωρίζει τους αριθμούς TAN. Η τράπεζα δεν φέρει καμία ευθύνη, για συναλλαγές που έγιναν από άλλο πρόσωπο, παρά τη θέλησή μας, σε περίπτωση απώλειας ή διαρροής αριθμών TAN..."*

Με άλλα λόγια, η τράπεζα καλύπτει το δικό της μερίδιο της ευθύνης με την προσφορά αυτού του πρόσθετου (υποχρεωτικού) μέτρου ασφάλειας, αλλά έγκειται στον ίδιο τον χρήστη να διαφυλάξει την σωστή εφαρμογή του.

Θα πρέπει πάντως να σημειωθεί πως σήμερα το επίπεδο κατάρτισης του προσωπικού των τραπεζών και, αντίστοιχα, της ενημέρωσης των πελατών τους σχετικά με την διάθεση και χρήση των νέων συσκευών παραγωγής κωδικών TAN μιας χρήσης, είναι τουλάχιστον τραγική. Για παράδειγμα, η προμήθεια των αντίστοιχων συσκευών TAN χρεώνεται στον πελάτη ως πρόσθετη προαιρετική υπηρεσία (όπως δηλαδή οι πιστωτικές κάρτες), χωρίς όμως να παρέχεται μαζί αναλυτικό ούτε εγχειρίδιο 94 οδηγιών, ούτε οι αναλυτικές τεχνικές προδιαγραφές, ούτε καν οι αναλυτικοί όροι χρήσης όπου καθορίζονται τα όρια ευθύνης του κάθε μέρους (της τράπεζας και του πελάτη). Αυτό ίσως να οφείλεται στο γεγονός ότι η διάδοση και η χρήση παρόμοιων διαδικασιών στις ηλεκτρονικές συναλλαγές είναι ακόμη πολύ πρώιμη στην Ελλάδα, με αποτέλεσμα το αντίστοιχο ενδιαφέρον να είναι περιορισμένο, τόσο από την μεριά των πελατών, που συνήθως δεν επιδιώκουν περαιτέρω ενημέρωση, όσο και από την ίδια την τράπεζα, που δεν θέλει να επωμιστεί το βάρος και το κόστος της "εκπαίδευσης" των πελατών σε αυτά τα νέα συστήματα.

**Πλεονεκτήματα κωδικών TAN:**

Το πλεονέκτημα των κωδικών TAN είναι ότι, εν γένει, πρόκειται για κωδικούς οι οποίοι δεν αποθηκεύονται πουθενά στο σύστημα του χρήστη-πελάτη αλλά αντίθετα βρίσκονται σε τυπωμένη μορφή, άρα είναι αδύνατο να υποκλαπούν ηλεκτρονικά από το σύστημά του.Αντίστοιχα, στο σύστημα E-Banking της τράπεζας όπου τηρούνται αντίγραφα των κωδικών αυτών για αντιπαραβολή, υπάρχουν τα κατάλληλα μέτρα εξασφάλισης της εμπιστευτικότητας σε πολύ υψηλό επίπεδο, ώστε αντίστοιχα η κλοπή τους, φυσική ή ηλεκτρονική, να είναι ουσιαστικά ανέφικτη. Κατά συνέπεια, ακόμα και αν ο κύριος κωδικός (username/password) του χρήστη-πελάτη παραβιαστεί και κάποιος τρίτος αποκτήσει πρόσβαση στον λογαριασμό E-Banking, δεν μπορεί να κάνει καμία εγχρήματη συναλλαγή αφού δεν διαθέτει αντίστοιχους έγκυρους κωδικούς TAN.

## Τρόπος λειτουργίας των κωδικών TAN και MAC.

Η λογική της λειτουργίας των κωδικών TAN βασίζονται στην ιδέα της κρυπτογράφησης μέσω κωδικό βιβλίων (codebooks) μιας χρήσης ή αλλιώς συστημάτων one-time-pads, τα οποία είναι τα μόνα μοντέλα κρυπτογράφησης των οποίων το απαραβίαστο εξασφαλίζεται 100% και αποδεικνύεται θεωρητικά.
Γι' αυτό άλλωστε χρησιμοποιούνται ακόμη και σήμερα σε μερικούς τύπους στρατιωτικών επικοινωνιών (συστήματα χαμηλού ρυθμού μετάδοσης).

Στην περίπτωση των κωδικών TAN, τα κωδικοβιβλία δεν χρησιμοποιούνται για κρυπτογράφηση αλλά απλώς για την χορήγηση κωδικών "γνησιότητας". Αυτή η μορφή αναφέρεται συχνά ως Κωδικός Αυθεντικοποίησης Μηνύματος (MAC – Message Authentication Code), ο οποίος συνοδεύει κάθε μήνυμα και χρησιμοποιείται για την διάκριση των γνήσιων από τα πλαστά μηνύματα. Για να εξασφαλιστεί η κρυπτασφάλεια των "γνήσιων" κωδικών, υπάρχει μια κοινή λίστα μυστικών κωδικών στα δύο άκρα της επικοινωνίας, δηλαδή ένα κωδικοβιβλίο με κωδικούς μιας χρήσης, τους οποίους χρησιμοποιούν και διασταυρώνουν για τον έλεγχο κάθε μηνύματος.

Εντούτοις, το βασικό πρόβλημα είναι η μεταφορά και αποθήκευση των αντίστοιχων κωδικοβιβλίων με ασφαλή τρόπο και στα δύο μέρη που επικοινωνούν.

Στους κωδικούς TAN αυτό εξασφαλίζεται από την ίδια την τράπεζα, απαιτώντας την προσωπική ταυτοποίηση και παράδοση της λίστας TAN στον ίδιο τον πελάτη αυτοπροσώπως, και μάλιστα σε μορφή εν γένει μη-αποθηκεύσιμη στον Η/Υ του.

Όμως η διαδικασία έκδοσης και προσωπικής παραλαβής της λίστας TAN είναι συχνά χρονοβόρα και δυσχερής, μια και ακυρώνει μέρος της ίδιας της έννοιας του E-Banking.

Για την εξασφάλιση της κρυπτασφάλειας του συστήματος των MAC και ταυτόχρονα την άμεση συσχέτισή τους με το ίδιο το περιεχόμενο του μηνύματος, συχνά εφαρμόζονται δύο πρόσθετα στάδια επεξεργασίας και ένα μοναδικό μυστικό κλειδί, έτσι ώστε να μην χρειάζεται η χρήση ειδικού κωδικοβιβλίου όπως προβλέπει το αρχικό μοντέλο των one-time-pads. Συγκεκριμένα, το περιεχόμενο του μηνύματος περνά μέσα από μια διαδικασία επεξεργασίας που ονομάζεται Συνάρτηση Κατακερματισμού "Μη Αντιστρέψιμη" ή "Μιας Κατεύθυνσης" (One-Way Hashing Function).

Η διαδικασία αυτή αντιστοιχεί το σύνολο των δεδομένων του μηνύματος σε έναν μοναδικό κωδικό αναγνώρισης συγκεκριμένου μεγέθους (π.χ. 128 ή 256 bits), από τον οποίο δεν μπορεί να εξαχθεί το περιεχόμενο του αρχικού μηνύματος με κανέναν τρόπο λόγω των μαθηματικών ιδιοτήτων της συγκεκριμένης συνάρτησης. Επιπλέον, είναι σχεδόν αδύνατο η συνάρτηση αυτή να δημιουργήσει τον ίδιο κωδικό αναγνώρισης για δύο διαφορετικά μηνύματα.

Στη συνέχεια, ο κωδικός αυτός κρυπτογραφείται με το μοναδικό μυστικό κλειδί κρυπτογράφησης πριν μεταδοθεί στο κανάλι μετάδοσης. Η διαδικασία ονομάζεται Keyed-HMAC (Hashed Message Authentication Code with Key) και ουσιαστικά κάνει περιττή την χρήση ειδικών κωδικοβιβλίων τύπου one-time-pad για αυτό το σκοπό, διατηρώντας εξαιρετικά μικρή θεωρητικά (αλλά όχι αδύνατη πλέον, όπως στο one-time-pad) την πιθανότητα παραβίασης της κρυπτασφάλειας του συστήματος.

Με το σύστημα των keyed-HMAC εξασφαλίζεται ότι (α) κανένας δεν μπορεί να "πειράξει" το αρχικό μήνυμα χωρίς να "ακυρώσει" το συγκεκριμένο κωδικό αυθεντικοποίησης του μηνύματος και (β) ότι κανένας άλλος δεν μπορεί να παράγει γνήσιους κωδικούς αυθεντικοποίησης εφόσον δεν διαθέτει το αντίστοιχο μυστικό κλειδί.

Στην πράξη, το μοντέλο αυτό εφαρμόζεται στις επικοινωνίες σαν ένας εύκολη και γρήγορη εναλλακτική λύση έναντι της εφαρμογής των πιο πολύπλοκων και εξειδικευμένων μοντέλων ψηφιακών υπογραφών (digital signatures).

### 12.1.3 Συσκευές δημιουργίας κωδικών TAN


Σε αναλογία με την εφαρμογή των keyed-HMAC για την αντικατάσταση των κωδικοβιβλίων, υπάρχουν τρόποι να αντικατασταθεί η εκτυπωμένη λίστα TAN με αντίστοιχη συσκευή παραγωγής μεμονωμένων κωδικών από τον ίδιο τον πελάτη, πάντα απομονωμένη από τον Η/Υ τον οποίο χρησιμοποιεί για την πρόσβαση στο σύστημα E-Banking, και φυσικά σε συσχέτιση με αντίστοιχο μηχανισμό διασταύρωσής τους από το σύστημα της τράπεζας.

Πρακτικά αυτό υλοποιείται με ένα συνδυασμό τριών πραγμάτων:

1. Μια γεννήτρια ψευδοτυχαίων αριθμών (PRNG)

2. Ένα κύκλωμα χρονισμού υψηλής ακρίβειας (CLOCK)

3. Ένα μυστικό ηλεκτρονικό κλειδί της τράπεζας (KEY)

Ο ακριβής τρόπος λειτουργίας είναι αρκετά πολύπλοκος για να εξηγηθεί πλήρως σε κάποιον μη-ειδικό, αλλά η βασική διαδικασία είναι η εξής:

Η γεννήτρια PRNG χρειάζεται έναν αρχικό κωδικό για να ξεκινήσει και στην συνέχεια μπορεί να παράγει αριθμούς οι οποίοι είναι "επαρκώς τυχαίοι" ώστε να μην είναι προβλέψιμοι με κανέναν τρόπο αν κάποιος δεν γνωρίζει τον κωδικό αρχικοποίησης. Αυτό είναι αρμοδιότητα της τράπεζας, δηλαδή να αρχικοποιεί τις συσκευές αυτές έτσι ώστε να μπορεί να "αναπαράγει" μόνο η ίδια την ακολουθία των αριθμών αυτών.

Επιπλέον, το κύκλωμα CLOCK μπορεί να χρησιμοποιηθεί για να αρχικοποιεί και πάλι την συσκευή σε τακτά χρονικά διαστήματα, τα οποία επίσης γνωρίζει η τράπεζα χωρίς να χρειάζεται περαιτέρω επικοινωνία ή σύνδεση με την συσκευή του πελάτη. Αυτό γιατί αρκεί απλά το CLOCK ή "ρολόι" της συσκευής TAN να είναι συγχρονισμένο με αυτό του συστήματος της τράπεζας.

Για το λόγο αυτό το κύκλωμα CLOCK της κάθε συσκευής TAN πρέπει να είναι υψηλής πιστότητας, με ελάχιστη απόκλιση (π.χ. 60 δευτερόλεπτα max) στη διάρκεια ζωής της συσκευής (π.χ. 3 χρόνια)
Με τους δύο παραπάνω μηχανισμούς, δηλαδή τον κωδικό αρχικοποίησης του κυκλώματος PRNG και το κύκλωμα CLOCK για την περιοδική επανα-αρχικοποίηση, η συσκευή TAN μπορεί να παράγει πλέον "τυχαίους" κωδικούς TAN, προβλέψιμους μόνο από το αντίστοιχο σύστημα της ίδιας της τράπεζας.

Όμως, η τράπεζα πρέπει σαν πρόσθετο μέτρο ασφάλειας να μπορεί να ελέγχει την γνησιότητα των κωδικών TAN που εισάγει ο χρήστης-πελάτης της, για να αποκλειστεί η περίπτωση κάποιος να "ανακαλύψει" τις λεπτομέρειες σχεδίασης και αρχικοποίησης των κυκλωμάτων PRNG και CLOCK της συσκευής TAN και να κατασκευάσει μια δική του, μη-πιστοποιημένη συσκευή για την παραγωγή ψευδών αλλά επαληθεύσιμων κωδικών.

Σε μερικές περιπτώσεις στην παραπάνω διαδικασία υπάρχει και μια δεύτερη φάση, η οποία περιλαμβάνει την παραγωγή ενός πρόσθετου μικρότερου κωδικού ελέγχου (CHECK) μετά από κάθε κωδικό TAN. Αυτό γίνεται για να ενημερώσει τον χρήστη-πελάτη για την επιτυχημένη και έγκυρη ολοκλήρωση της συναλλαγής στο σύστημα E-Banking της τράπεζας. Με άλλα λόγια, ο πελάτης είναι αυτός που τώρα συγκρίνει τον κωδικό ελέγχου CHECK που επιστρέφει το σύστημα E-Banking της τράπεζας για να διαπιστώσει ότι όλα πήγαν καλά.

Τέλος, για την εξασφάλιση της ίδιας της συσκευής υπάρχει εσωτερικά φυσικός μηχανισμός "αυτοκαταστροφής" της συσκευής TAN σε περίπτωση που παραβιαστεί με φυσικό τρόπο. Αν δηλαδή κάποιος επιχειρήσει να την ανοίξει για να "διαβάσει" τα αντίστοιχα ηλεκτρονικά κυκλώματα, οι σημαντικές πληροφορίες (π.χ. KEY) διαγράφονται αυτόματα και μόνιμα από την συσκευή TAN, ώστε η ανάκτησή τους να είναι αδύνατη. Επιπλέον, ως μέρος των παραπάνω μηχανισμών, η τράπεζα αναγνωρίζει κάθε μεμονωμένη συσκευή TAN με έναν μοναδικό σειριακό αριθμό, που βρίσκεται στο πίσω μέρος της, και που "δεσμεύει" τη συγκεκριμένη συσκευή με τον λογαριασμό του αντίστοιχου πελάτη-χρήστη.

### 12.1.4 Πρακτική χρήση και περιορισμοί κωδικών TAN

Σήμερα, οι συσκευές TAN που διατίθενται από τις ελληνικές τράπεζες ενσωματώνουν τους παραπάνω βασικούς μηχανισμούς με κατάλληλο τρόπο, όχι πάντα ταυτόσημο.

Για παράδειγμα, σε κάποιες περιπτώσεις οι συσκευές TAN παράγουν κωδικούς μιας χρήσης μόνο μετά από αίτημα του χρήστη (πάτημα ενός ενσωματωμένου πλήκτρου), ενώ άλλες παράγουν συνεχώς κωδικούς οι οποίοι ανανεώνονται αυτόματα κάθε 60 δευτερόλεπτα, είτε χρησιμοποιούνται είτε όχι.

Γενικά δεν υπάρχει διαφορά στο επίπεδο ασφάλειας που προσφέρουν, όμως οι ίδιες οι συσκευές TAN έχουν ένα συγκεκριμένο χρονικό διάστημα (ή αντίστοιχα πλήθος παραγόμενων κωδικών) "ασφαλούς χρήσης", πέρα από το οποίο η "τυχαιότητά" τους δεν θεωρείται πλέον εξασφαλισμένη.
Συνήθως το διάστημα αυτό είναι 3 χρόνια ή 2 εκατομμύρια κωδικοί TAN.

Σε αυτή την περίπτωση, η συσκευή είτε αντικαθίσταται με νέα είτε αρχικοποιείται και πάλι από την τράπεζα με νέους κωδικούς και είναι έτοιμη για χρήση για άλλο τόσο διάστημα, δηλαδή σαν να ήταν καινούργια.

*Συμπέρασμα:*

Αναφορικά με τα παραπάνω,θα μπορούσαμε να συμπεράνουμε πως οι τράπεζες παρόλες τις κακόβουλες πράξεις ορισμένων επιτήδειων έχουν καταφέρει να προσπεράσουν πολλά από τα εμπόδια που προκύπτουν στην πορεία της δράσης της μέσα από τη συνεχή ενημέρωση και χρησιμοποίηση της τελευταίας λέξης της τεχνολογίας ώστε να αποφευχθούν τα χειρότερα και να καταφέρουν να προσφέρουν αξιόπιστα και με ταχύτητα της προσφερόμενες ηλεκτρονικές τραπεζικές συναλλαγές τους.

# ΚΕΦΑΛΑΙΟ 13

## Βιομετρικά συστήματα αναγνώρισης χαρακτηριστικών .

Τα υπολογιστικά συστήματα διαθέτουν μια πλειάδα μεθόδων αναγνώρισης του χρήστη - κωδικοί ασφαλείας (password), PINs, «έξυπνες κάρτες», tokens. Αλλά όλα αυτά μπορούν να χαθούν, ναξεχαστούν, να κλαπούν, να πλαστογραφηθούν. Άρα, δεν αποτελούν ισχυρή απόδειξη της ταυτότητας ενός ατόμου.

Η βασική εφαρμογή των βιομετρικών μεθόδων είναι ο έλεγχος της φυσικής ασφάλειας. Σε χώρους περιορισμένης ή ελεγχόμενης πρόσβασης, τα βιομετρικά συστήματα προσφέρουν δυνατότητα ελέγχου χωρίς την παρουσία φύλακα. Στους Ολυμπιακούς Αγώνες του 1996, 65.000 άνθρωποι ελέγχθηκαν μέσω βιομετρικών συστημάτων. Επίσης, η Disney World χρησιμοποιεί «σαρωτή» δακτυλικών αποτυπωμάτων για να επιβεβαιώσει την ταυτότητα των πελατών της που διαθέτουν εισιτήρια διαρκείας.

Στον τομέα της λογικής ασφάλειας των υπολογιστικών συστημάτων, βιομετρικές μέθοδοι έχουν βρει ένα πολύ καλό πεδίο εφαρμογής. Για να μπορέσει ο χρήστης να μπει στον υπολογιστή του γραφείου του, πρέπει πρώτα να περάσει από έλεγχο της ταυτότητας του. Ο έλεγχος αυτός μπορεί να γίνει με βιομετρικές μεθόδους, όπως είναι η αναγνώριση του δακτυλικού του αποτυπώματος ή της φωνής του.

Μία άλλη εφαρμογή των βιομετρικών μεθόδων αφορά το ηλεκτρονικό εμπόριο. Για παράδειγμα, πολλές τράπεζες σκέπτονται να υιοθετήσουν ένα σύστημα «έξυπνης κάρτας», η οποία περιέχει το δακτυλικό αποτύπωμα του ιδιοκτήτη της για την πραγματοποίηση συναλλαγών μέσω Internet.

Τα βιομετρικά συστήματα έχουν γίνει κατά τα τελευταία χρόνια πιο προσιτά, λόγω της πτώσης του κόστους τους. Έτσι προβλέπεται ότι θα επεκταθεί κατά πολύ η χρήση τους. Δεν πρόκειται, όμως, να αντικαταστήσουν τις υπάρχουσες μεθόδους, αλλά να τις ισχυροποιήσουν.

Ας μην ξεχνάμε ότι η εξακρίβωση της ταυτότητας ενός ατόμου βασίζεται είτε σε κάτι που το άτομο γνωρίζει (password, PIN), είτε σε κάτι που έχει (smart card, token), είτε σε κάτι που είναι (biometrics). Ο συνδυασμός, δύο τουλάχιστον εκ των τριών μεθόδων είναι η βάση μιας ασφαλούς αναγνώρισης.

Κάθε άνθρωπος έχει ορισμένα μετρήσιμα χαρακτηριστικά, τα οποία είναι μοναδικά και τον κάνουν να διαφέρει από κάθε άλλον.

Τα βιομετρικά συστήματα χωρίζονται σε δυο κατηγορίες, ανάλογα με το εάν μετρούν φυσιολογικά χαρακτηριστικά ή στοιχεία της συμπεριφοράς ενός ατόμου.

Στην πρώτη κατηγορία ανήκουν τα συστήματα που αναγνωρίζουν τα δακτυλικά αποτυπώματα, για τη γεωμετρία του ανθρώπινου χεριού), τα χαρακτηριστικά του ανθρώπινου προσώπου και χαρακτηριστικά του ματιού (για την ακρίβεια, του αμφιβληστροειδούς χιτώνα, ή της ίριδας).

## 13.1 Δακτυλικά αποτυπώματα και γεωμετρία χεριού.

Τα πλέον διαδεδομένα βιομετρικά συστήματα είναι εκείνα που αναγνωρίζουν δακτυλικά αποτυπώματα. Η ακρίβεια τέτοιων συστημάτων εξαρτάται από την ποιότητα των αποτυπωμάτων.

Βέβαια,οι υπολογιστές παρουσιάζουν δυσκολίες στην αναγνώριση δακτυλικών αποτυπωμάτων από πολύ μικρά χέρια και δάκτυλα. Οι άνθρωποι που κάνουν χειρωνακτικές εργασίες, είτε για κάποιον λόγο έχουν χτυπήματα και αμυχές στα δάκτυλα τους, αφήνουν δυσδιάκριτα δακτυλικά αποτυπώματα.

Τα βιομετρικά συστήματα δακτυλικών αποτυπωμάτων ενσωματώνονται σε πληκτρολόγια και ποντίκια υπολογιστών και γι' αυτό τον λόγο είναι τα πλέον δημοφιλή στις περιπτώσεις ασφάλειας των υπολογιστών γραφείου (workstations). Συστήνονται για εφαρμογές όπου δεν είναι μεγάλος ο αριθμός των χρηστών.

Στα βιομετρικά συστήματα γεωμετρίας χεριού αναλύεται η γεωμετρία της παλάμης ή του χεριού. Έχουν μεγάλη ακρίβεια και γι' αυτό ενδείκνυνται για εφαρμογές με μεγάλο αριθμό χρηστών.

## 13.2 Σύστημα αναγνώρισης χαρακτηριστικών ανθρώπινου ματιού.

Τα βιομετρικά συστήματα αναγνώρισης του αμφιβληστροειδούς χιτώνα του ματιού διαθέτουν ιδιαίτερα μεγάλη ακρίβεια.

Σαρώνοντας το πίσω μέρος του οφθαλμού με υπέρυθρη ακτίνα, αναλύουν και μετρούν τις μικρές φλέβες οι οποίες βρίσκονται εκεί. Η διαδικασία αναγνώρισης δεν είναι και τόσο φιλική προς τον χρήστη. Πρέπει το μάτι να τοποθετηθεί σε συγκεκριμένη υποδοχή - χωρίς γυαλιά, βέβαια - και να εστιάσει κοιτώντας ακριβώς προς την πηγή του υπέρυθρου φωτός.

Γι' αυτό τον λόγο, η μέθοδος αυτή δεν υιοθετείται εύκολα, παρά μόνο σε ορισμένες περιπτώσεις που απαιτείται μεγάλος βαθμός ασφάλειας. Τα βιομετρικά συστήματα, που αναγνωρίζουν την ίριδα του ματιού, είναι πιο- φιλικά προς του χρήστη. Η κάμερα κάνει ζουμ στο μπροστινό μέρος του ανθρώπινου ματιού και για να γίνει η αναγνώριση δεν απαιτείται ο χρήστης να είναι πολύ κοντά σε αυτήν, ούτε να βγάλει, εάν έχει, τα γυαλιά του. Είναι, όμως, απαραίτητο να υπάρχει καλός φωτισμός.

Οι μέθοδοι αναγνώρισης του ανθρώπινου ματιού είναι οι πλέον ακριβείς. Τα χαρακτηριστικά του αμφιβληστροειδούς χιτώνα θεωρούνται μοναδικά, ακόμα και σε δίδυμους που προέρχονται από το ίδιο ωάριο. Η ίριδα θεωρείται η πιο πλούσια σε χαρακτηριστικά περιοχή του ανθρώπου που βρίσκεται σε συνεχή έκθεση. Η ίριδα έχει 250 διαφορετικά χαρακτηριστικά, σε σύγκριση με τα 40 ή 50 που έχει το δακτυλικό αποτύπωμα.

## 13.3 Σύστημα αναγνώρισης φωνής.

Η μέθοδος της αναγνώρισης της φωνής (voice recognition) έχει το πλεονέκτημα ότι δεν χρειάζεται ιδιαίτερο εξοπλισμό για να λειτουργήσει σε ένα PC. Στην πράξη, όμως, εμφανίζονται διάφορα προβλήματα, λόγω του εξωτερικού θορύβου που συνήθως υπάρχει και της διακύμανσης της ανθρώπινης ομιλίας, ανάλογα με την περίσταση (συναισθηματική φόρτιση, κρυολόγημα κλπ).

## 13.4 Σύστημα αναγνώρισης χαρακτήρα πληκτρολόγησης.

Κάθε άνθρωπος έχει έναν διαφορετικό χαρακτήρα πληκτρολόγησης. Η τεχνική keystroke dynamics παρακολουθεί την ταχύτητα και τον τρόπο πληκτρολόγησης, με αποτέλεσμα να μπορεί να αναγνωρίσει την ταυτότητα του χρήστη από αυτό το χαρακτηριστικό. Έτσι, ακόμη και εάν κάποιος γνωρίζει τον κωδικό ασφάλειας ενός χρήστη, δεν μπορεί να μιμηθεί τον τρόπο με τον οποίο το πληκτρολογεί και έτσι δεν μπορεί να «κλέψει» την ταυτότητα του.

*Συμπέρασμα:*

Ένας βιομετρικός αναγνώστης μετράει ένα μοναδικό φυσικό χαρακτηριστικό ή συμπεριφορά ενός ανθρώπου και το συγκρίνει με ένα αποθηκευμένο ψηφιακό πρότυπο για να τον πιστοποιήσει. Ένα από τα πιο συνηθισμένα βιομετρικά συστήματα είναι αυτά των δακτυλικών αποτυπωμάτων, που μπορούν να χρησιμοποιηθούν αντί των προσωπικών κωδικών αναγνώρισης (PIN's) των χρηστών.Άλλα συστήματα βιομετρικών αναγνωστών μπορούν να αφορούν χαρακτηριστικά, όπως η ίριδα του ματιού, η φωνή του πελάτη κ.τ.λ. Σε αντίθεση με τις μεθόδους που προαναφέραμε,τα βιομετρικά συστήματα θεωρούνται ασφαλέστερα και ισχυρότερα.

# ΚΕΦΑΛΑΙΟ 14
# Πιστοποίηση ηλεκτρονικών καταστημάτων και μέτρα για ασφαλείς ηλεκτρονικές τραπεζικές συναλλαγές.

## 14.1. Πιστοποίηση ηλεκτρονικών καταστημάτων.

Το πρόβλημα εδώ έγκειται στο διαχωρισμό των αξιόπιστων ηλεκτρονικών καταστημάτων από τα πιθανώς εικονικά και επικίνδυνα. Αξίζει σε αυτό το σημείο να σημειωθεί ότι και τα μεν και τα δε είναι πιθανό να υποστηρίζουν κρυπτογραφημένη επικοινωνία για την αποφυγή παρεμβολών.

Ωστόσο ελλοχεύει ακόμη ο κίνδυνος υποκλοπής των στοιχείων της κάρτας από έναν εικονικό πωλητή καθώς αυτός - σε αντίθεση με κάποιον που παρεμβάλλεται στην επικοινωνία - είναι σε θέση να αποκρυπτογραφήσει τα στοιχεία της κάρτας.

Η λύση σε αυτό το πρόβλημα δίνεται με την πιστοποίηση των ηλεκτρονικών καταστημάτων από διεθνείς εταιρίες/οργανισμούς πιστοποίησης (π.χ. VeriSign,thawte). Ένα ηλεκτρονικό κατάστημα προκειμένου να θεωρηθεί αξιόπιστο καταθέτει αίτηση έκδοσης πιστοποιητικού σε μία τέτοια εταιρία.

Εφόσον η αίτηση του εγκριθεί από την εταιρία το κατάστημα πληρώνει ένα χρηματικό ποσό ως αντίτιμο για την έκδοση του πιστοποιητικού (το οποίο έχει συγκεκριμένη χρονική διάρκεια) και έπειτα χρησιμοποιεί αυτό το πιστοποιητικό στον ιστότοπο του για να ενημερώσει τους υποψήφιους αγοραστές ότι αποτελεί πιστοποιημένο κατάστημα (π.χ. μέσω του ειδικού σήματος της VeriSign) και ως εκ τούτου θα πρέπει να θεωρείται αξιόπιστο.

## 14.2 Ψηφιακά πιστοποιητικά PKI.
## (Personal Key Identification)

Ορισμένες τράπεζες χρησιμοποιούν τα λεγόμενα ψηφιακά πιστοποιητικά (digital certificates), ως τρόπο πρόσβασης και ως ένα μέσο πρόσθετης ασφάλειας. Ένα ψηφιακό πιστοποιητικό αποτελεί το μέσο που παρέχει τη δυνατότητα στον κάτοχό του, να υπογράφει ψηφιακά τις συναλλαγές που πραγματοποιεί μέσω της ηλεκτρονικής τραπεζικής. Από τη στιγμή που το τελευταίο εγκατασταθεί στον υπολογιστή του χρήστη, προσφέρει τη δυνατότητα ταυτοποίησής του ίδιου και επιτρέπει τη διεξαγωγή οικονομικών συναλλαγών μόνο από αυτόν. Τα συστήματα αυτά είναι γνωστά και ως PKI (Personal Key Identification) και παρέχουν πιστοποίηση, ακεραιότητα δεδομένων και ασφάλεια συναλλαγών.Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για να πιστοποιήσουν ότι το άτομο που στέλνει πληροφορίες ή έναν αριθμό πιστωτικής κάρτας ή ένα μήνυμα ή οτιδήποτε άλλο στο internet είναι πραγματικά αυτό που δηλώνει ότι είναι. Τα πιστοποιητικά τοποθετούν τις πληροφορίες στον σκληρό δίσκο του χρήστη και χρησιμοποιούν τεχνολογία απόκρυψης για να δημιουργήσουν ένα μοναδικό ψηφιακό πιστοποιητικό για κάθε χρήστη. Όταν κάποιος που διαθέτει ένα ψηφιακό πιστοποιητικό επισκεφτεί κάποιο site ή στείλει e-mail το πιστοποιητικό αυτό παρουσιάζεται στο site ή επισυνάπτεται στο e-mail και πιστοποιεί ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι. Τα ψηφιακά πιστοποιητικά είναι αρκετά ασφαλή επειδή χρησιμοποιούν πανίσχυρη τεχνολογία απόκρυψης. Στην πραγματικότητα είναι πιο ασφαλή και από τις υπογραφές. Στην πραγματική ζωή μια υπογραφή μπορεί να πλαστογραφηθεί. Αντιθέτως στο internet δεν μπορεί να πλαστογραφηθεί το ψηφιακό πιστοποιητικό. Τα ψηφιακά πιστοποιητικά εκδίδονται έναντι χρέωσης από ιδιωτικές εταιρείες που ονομάζονται Digital Authorities.

## 14.3 Η ηλεκτρονική-ψηφιακή υπογραφή (e-signature)

Η "νομιμοποίηση" ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που έφερε. Καθώς τα ηλεκτρονικά έγγραφα κάθε είδους τείνουν να αντικαταστήσουν τα "παραδοσιακά" χειρόγραφα, αντίστοιχα και η υπογραφή του συντάκτη γίνεται "εικονική", "ηλεκτρονική."

Η ανάπτυξη του διαδικτύου, το εμ΄ποριο και οι ηλεκτρονικές συναλαγές μέσω ανοιχτών δικτύων καθιστούν επιτακτική την ανάγκη ασφάλειας, η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, την ταυτότητα δηλαδή των συναλλασσομένων.

Το πρόβλημα της πιστοποίησης της γνησιότητας μιας πληροφορίας που λαμβάνεται σε ηλεκτρονική μορφή είναι ένα από τα σημαντικότερα σήμερα, καθώς η τάση για όλο και περισσότερο απρόσωπες και απομακρυσμένες συναλλαγές επιτάσσει την αντικατάσταση των παραδοσιακών τρόπων πιστοποίησης με βάση την υπογραφή με το χέρι, τις σφραγίδες των οργανισμών και την ανάλυση γραφικού χαρακτήρα με τρόπους που μπορούν να χειριστούν τα παραπάνω στοιχεία σε ηλεκτρονική μορφή.Στις καθημερινές συναλλαγές των ανθρώπων, είναι αναγκαίο να πιστοποιούνται ημερομηνίες αποστολής εγγράφων (π.χ. εμπρόθεσμες φορολογικές δηλώσεις), η ταυτότητα του αποστολέα μιας πληροφορίας (χωρίς τη χρήση της αστυνομικής του ταυτότητας), η ταυτότητα του υπολογιστή από τον οποίο στάλθηκε μια πληροφορία καθώς και πλήθος στοιχείων που μέχρι τώρα βασιζόταν σε παραδοσιακά μέσα επεξεργασίας πληροφοριών.

Η ψηφιακή υπογραφή, είναι ένα μέσο με το οποίο πολλά από αυτά τα στοιχεία μπορούν να πιστοποιηθούν. Δοσμένου ενός ηλεκτρονικού εγγράφου, η ψηφιακή του υπογραφή είναι μία πληροφορία που σχηματίζεται με βάση το έγγραφο και ενός προσωπικού αριθμού (κλειδί) του αποστολέα. Ενώ η κλασσική υπογραφή βασίζεται στο ότι ο γραφικός χαρακτήρας ενός ανθρώπου είναι απίθανο να μοιάζει με το γραφικό χαρακτήρα κάποιου άλλου, οι ψηφιακή υπογραφή βασίζεται στο ότι ο προσωπικός αριθμός ενός ανθρώπου είναι μοναδικός και δεν μπορεί να μαθευτεί από άλλους.Είναι ο συνδυασμός ενός μηνύματος που προκύπτει από την επεξεργασία του πιστοποιητικού με κάποιον αλγόριθμο και με το private key και ενός public key για κάθε μέρος.Με απλά λόγια, είναι σαν ο Α να έχει δύο κλειδιά, να δίνει στον Β το public key του για να κλειδώσει το κουτί μέσα στο οποίο θα του στείλει τα δεδομένα και να το επιστρέψει στον Α, που θα το ξεκλειδώσει με το private key του, και αντίστροφα.

Η εγγενής αδυναμία του πρωτοκόλλου TCP/IP, που χρησιμοποιείται για τη μεταφορά των δεδομένων, αντιμετωπίζεται με την κρυπτογράφηση της διακινούμενης πληροφορίας, έτσι ώστε, ακόμη και αν κάποιος την καταγράψει, να μην έχει τη δυνατότητα να την αποκρυπτογραφήσει ή να τη μεταβάλει. Το πρωτόκολλο που φροντίζει για τη μετάδοση κρυπτογραφημένης πληροφορίας λέγεται SSL (Secure Socket Layer).

Το κλειδί της κρυπτογράφησης μπορεί να έχει μήκος 40 χαρακτήρων (SSL 40 bit) ή 128 χαρακτήρων (SSL 128bit, που αποτελεί αυτή τη στιγμή τη μεγαλύτερη ασφάλεια). Για το χρήστη, αυτό σημαίνει ότι οι πιθανοί συνδυασμοί είναι 2128 για το SSL 128bit και 240 για το SSL 40bit, αλλά σε κάθε επίσκεψη στις ασφαλείς σελίδες του site, μόνο ένας ενεργοποιείται.

Εμπιστευτικότητα: Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (μήνυμα ή κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα άτομα.

Αυθεντικότητα: Σε μια τέτοια συναλλαγή, ο παραλήπτης πρέπει να είναι βέβαιος για την ταυτότητα του αποστολέα.

Μη αποποίηση ευθύνης: Η συμμετοχή σε μία ηλεκτρονική συναλλαγή προϋποθέτει ότι τα εμπλεκόμενα μέρη δεν έχουν νόμιμο δικαίωμα να αρνηθούν εκ των υστέρων τη συμμετοχή τους στη συναλλαγή αυτή.

*Συμπέρασμα:*

Η πιστοποίηση ηλεκτρονικών καταστημάτων είναι ένας από τους σημαντικότερους τρόπους προστασίας που προσφέρουν ασφάλεια στις ηλεκτρονικες τραπεζικές συναλλαγές. Όλα τα παραπάνω μέτρα ασφάλειας κυρίως όμως εξαρτώνται και από την ευχέρεια χρήσης και συνεχής ενημέρωσης του πελάτη για τους νέους κάθε φορά τρόπους που μπορεί να προφυλαχτεί από τις διάφορες κακόβουλες επιθέσεις των γνωστών σε όλους μας. Στο κεφάλαιο αυτό, διαπιστώνουμε τη σοβαρότητα και την σημαντική επανάσταση που φέρνει η χρήση της ηλεκτρονικής υπογραφής στις τραπεζικές μας συναλλαγές λόγω του ότι προσφέρει ασφάλεια στο κάθε πελάτη με αποτέλεσμα να τον παροτρύνει στο να χρησιμοποιήσει τις ηλεκτρονικές τραπεζικές συναλλαγές.
Όσον αφορά τα πρωτόκολλα κρυπτογράφησης δεδομένων επικοινωνίας θα αναφερθούμε αναλυτικότερα στο επόμενο κεφάλαιο.

# ΚΕΦΑΛΑΙΟ 15
# Κρυπτογραφικά συστήματα

## 15.1. Κρυπτογράφηση: Το Α και το Ω της δικτυακής ασφάλειας.

Ο τρόπος που δουλεύουν οι υπολογιστές είναι πάνω κάτω γνωστός. Τα δεδομένα μετατρέπονται σε ψηφιακή μορφή (δηλαδή σε λέξεις – bytes, ακολουθίες που περιέχουν τα bits 0 και 1) με κατάλληλη χρήση συγκεκριμένων πρωτοκόλλων.

Το πιο διαδεδομένο αυτή τη στιγμή πρωτόκολλο είναι το ASCII ,όπου κάθε χαρακτήρας αντιπροσωπεύεται από μία επταψήφια ή οκταψήφια λέξη (π.χ. το Α είναι το 1000001, το 3 είναι 00110011 κτλ). Από τη στιγμή που έχουμε αυτή τη μορφή για το δεδομένο μας χρησιμοποιούμε τις δυνατότητες που μας παρέχουν οι κώδικες. Όταν λέμε κώδικες εννοούμε ένα σύστημα που περιέχει ένα αλφάβητο (π.χ. το {0,1} ή το {0,1,2,3}κτλ.), τις λέξεις που σχηματίζονται από αυτό και τους κανόνες που διέπουν το σύστημα.

Με διάφορους αλγόριθμους μπορούμε να μετατρέψουμε την « φράση » μας σε άλλο κώδικα και άρα να αλλάξουμε το μέγεθος, να την καμουφλάρουμε ή γενικά να κάνουμε τα πάντα χωρίς βέβαια να χαθεί το πραγματικό της νόημα, κοινώς να την κρυπτογραφήσουμε.Οι σύγχρονες επιχειρηματικές ανάγκες απαιτούν συχνά τη μετάδοση εμπιστευτικών δεδομένων μέσω του Διαδικτύου. Η νέα ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου του επαγγελματικού απορρήτου. Βασική τεχνολογία στον τομέα της ασφάλειας στο Internet είναι η κρυπτογράφηση.

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα προσωπικών δεδομένων του κάθε χρήστη του Internet.

Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα(ciphertext).
Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος. Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς τη χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος.
Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

## 15.2. Μέθοδοι κρυπτογράφησης.

Οι περισσότερες τράπεζες ακολουθούν το πρωτόκολλο SET (Secure Electronic Transaction),που υποστηρίζεται από τους δύο σημαντικότερους χρηματοπιστωτικούς οργανισμούς, τη MasterCard και τη Visa, καθώς και από εταιρίες όπως η IBM, η Microsoft και η Netscape. Το πρωτόκολλο SET βασίζεται στην κρυπτογραφία.

Δύο είναι οι κύριες μέθοδοι κρυπτογράφησης: η συμμετρική και η ασύμμετρη. Στη συμμετρική, η κρυπτογράφηση υλοποιείται με τη χρήση του ίδιου "κλειδιού", τόσο στην κωδικοποίηση όσο και στην αποκωδικοποίηση. Πράγμα το οποίο σημαίνει ότι ο αποστολέας και ο παραλήπτης του μηνύματος μοιράζονται το ίδιο κλειδί.Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται.

Ένας από τους πιο γνωστούς αλγόριθμους που χρησιμοποιούν αυτή τη μέθοδο είναι το DES (Data Description Standard), που χρησιμοποιείται από τραπεζικούς οργανισμούς για τη δημιουργία των αριθμών PIN.
Η ασύμμετρη κρυπτογράφηση χρησιμοποιεί δύο κλειδιά: το ένα (κοινό κλειδί) για να κωδικοποιήσει το μήνυμα και ένα άλλο (ιδιωτικό κλειδί) για να το αποκωδικοποιήσει. Ένα μήνυμα που θα κωδικοποιηθεί με το ένα κλειδί θα μπορέσει να αποκωδικοποιηθεί μόνο με το άλλο. Η τράπεζα μπορεί να διανείμει το κοινό κλειδί, κρατώντας το ιδιωτικό κλειδί για την αποκωδικοποίηση.
Όσον αφορά στις τραπεζικές συναλλαγές, κάθε τράπεζα ακολουθεί τη δική της λύση, όπως είναι οι αριθμοί PIN, τα ψηφιακά πιστοποιητικά και οι αριθμοί TAN, που ακολουθούν κάθε συναλλαγή.

Υπάρχουν αρκετές εταιρίες που μπορεί να χρησιμοποιήσει ένας οργανισμός για να πετύχει ασφαλή πρόσβαση. Μία από αυτές είναι η VeriSign, το λογισμικό της οποίας χρησιμοποιείται στις τραπεζικές όσο και σε άλλου τύπου διαδικτυακές συναλλαγές.

Η πιστοποίηση της ταυτότητας του χρήστη και κάθε συναλλαγή του εξασφαλίζονται με τη βοήθεια ενός μοναδικού ψηφιακού πιστοποιητικού (digital certificate). Αυτό το πιστοποιητικό αναγνωρίζει τον υπολογιστή του χρήστη και επιτρέπει τις συναλλαγές και τις μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από το συγκεκριμένο υπολογιστή.

Τα πιστοποιητικά αυτά εξασφαλίζονται εγκαθιστώντας ένα πρόγραμμα από την αντίστοιχη εταιρία πιστοποίησης.

## 15.3. Οπτική επιβεβαίωση κρυπτογραφημένης επικοινωνίας.

Για να διαπιστώσουμε αν η επικοινωνία μας ως αγοραστές με κάποιο ηλεκτρονικό κατάστημα είναι κρυπτογραφημένη πριν την αποστολή των στοιχείων της κάρτας μας ή/και άλλων προσωπικών δεδομένων αρκεί να δούμε στον περιηγητή μας είτε το σύμβολο της κλειστής κλειδαριάς (λουκέτου) σε προκαθορισμένο σημείο του γραφικού περιβάλλοντος του (συνήθως κάτω δεξιά) είτε το πρόθεμα https στην ηλεκτρονική διεύθυνση στην οποία βρισκόμαστε.

Συνήθως κάνοντας κλικ πάνω στο σύμβολο της κλειδαριάς εμφανίζονται επιπλέον πληροφορίες αναφορικά με τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται και τον ιδιοκτήτη του καταστήματος. Όλοι οι αλγόριθμοι κρυπτογράφησης που υπάρχουν σήμερα δεν είναι εξίσου ασφαλείς, παρόλα αυτά σχεδόν όλα τα ηλεκτρονικά καταστήματα τείνουν να χρησιμοποιούν τους πλέον ασφαλείς.

## 15.4. Διακρίσεις κρυπτογράφησης.

Ο κλάδος της Κωδικοποίησης, δηλαδή της διαχείρισης, μετατροπής και μεταφοράς δεδομένων, μπορεί να χωρισθεί σε δύο κατηγορίες ανάλογα με τον σκοπό που εξυπηρετείται και κάθε κατηγορία εντάσσεται σε ξεχωριστό επιστημονικό ( κυρίως μαθηματικό ) πεδίο . Αναλυτικότερα :

Α) Η «Θεωρία της Πληροφορίας» είναι το επιστημονικό κομμάτι που ασχολείται με την αποτελεσματικότητα στη διαχείριση της πληροφορίας. Ασχολείται με το πως θα συμπιέσουμε τα δεδομένα ώστε να πετύχουμε την γρηγορότερη μετάδοση, τον μικρότερο χώρο αποθήκευσης αλλά και την εύκολη αποσυμπίεση.

Β) Η «Θεωρία Κωδίκων» μελετά την προστασία της πληροφορίας κατά την μετάδοση από τους διάφορους «θορύβους». Εδώ επιδιώκεται τα δεδομένα που θα σταλούν να παραληφθούν με όσο το δυνατόν λιγότερες αλλοιώσεις και τυχόντα λάθη να διορθωθούν.

Σε τεχνικό επίπεδο οι δύο αυτοί κλάδοι, συνδυάζοντας τις κατακτήσεις των μοντέρνων Μαθηματικών (Άλγεβρα, Γραμμική Άλγεβρα, Αριθμητική Ανάλυση, Άλγεβρα Boole, Θεωρία Πολυπλοκότητας κτλ.), συγκροτούν ένα οικοδόμημα εξαιρετικά υψηλού επιστημονικά υπόβαθρου, τα αποτελέσματα του οποίου τα βιώνουμε καθημερινά χρησιμοποιώντας τους Η/Υ (π.χ. όταν στέλνουμε mail, όταν ανοίγουμε σελίδες στο διαδίκτυο, όταν κατεβάζουμε ή ανεβάζουμε torrents και γενικά σε οποιαδήποτε μεταφορά δεδομένων) χωρίς όμως να το συνειδητοποιούμε. Παράλληλα όμως η ψηφιακή αυτή μορφή καθιστά την πληροφορία ευάλωτη και εύκολα μπορεί να υποκλαπεί από τον όποιο ενδιαφερόμενο.

## 15.5 Πρωτόκολλα Κρυπτογράφησης δεδομένων SSL και SET.

### 15.5.1 Πρωτόκκολο κρυπτογράφσης δεδομένων SSL.

Το SSL, (Secure Sockets Layer) εξασφαλίζει τη δημιουργία ενός ασφαλούς διαύλου επικοινωνίας. Το κανάλι εγγυάται ότι τα δεδομένα θα μεταφερθούν ακέραια και ότι το περιεχόμενο τους δεν πρόκειται να αλλάξει κατά τη διάρκεια της μεταφοράς, ενώ πιστοποιεί τον Web server, δηλαδή ο Web browser επιβεβαιώνει ότι ο server είναι αυτός που δηλώνει ότι είναι.

Η πληροφορία πρώτα κρυπτογραφείται και έπειτα μεταδίδεται (ταυτόχρονα συμπιέζεται) για να αποκρυπτογραφηθεί από τον Web browser. Αποτελεί αδιαφανή για το χρήστη διαδικασία, ο οποίος δεν αντιλαμβάνεται τίποτα από όλα αυτά, παρά μόνο τα σημάδια στον browser του: Το "http" έχει μετατραπεί σε https:// και υπάρχει ένα σύμβολο κλειστής κλειδαριάς (λουκέτου) στο ,κάτω μέρος της οθόνης.

Όταν σε μια σύνδεση χρησιμοποιείται το SSL, οτιδήποτε μεταφέρεται ανάμεσα στο χρήστη και τον Web server είναι κρυπτογραφημένο, όπως το URL του κειμένου, τα περιεχόμενα του κειμένου που μεταδίδεται, τα περιεχόμενα που αποστέλλονται από το χρήστη μέσω φόρμας (άρα και τα στοιχεία του πελάτη και ο αριθμός της πιστωτικής κάρτας του).
Το SSL εγγυάται ότι οι πληροφορίες που εισάγουμε σε μια φόρμα φτάνουν στον προορισμό τους αναλλοίωτες. Για να το πετύχει αυτό, χρησιμοποιείται συμμετρική κρυπτογράφηση.

Οι πληροφορίες που μεταδίδονται κρυπτογραφούνται με βάση ένα μυστικό κλειδί που έχει δημιουργηθεί για την περίσταση, το οποίο γνωρίζουν ο broWser του χρήστη και ο server.
Επίσης εγγυάται ότι οι πληροφορίες στέλνονται στο σωστό άνθρωπο και όχι σε τρίτους.

Για την πραγματοποίηση μη εγχρήματων συναλλαγών ασφαλείας μέσω Internet Banking (IB) όπως ενημέρωση χαρτοφυλακίου μετοχών, κίνηση λογαριασμών για τις περισσότερες τράπεζες αρκούν ο κωδικός ταυτότητας (user/D) που αποτελεί την ταυτότητα του χρήστη για την είσοδο στο IB και ο Μυστικός Κωδικός Αναγνώρισης (password) ο οποίος και αναγνωρίζει ως συγκεκριμένο χρήστη/πελάτη κι επιτρέπει την πρόσβαση στο Σύστημα.

### 15.5.2 Πρωτόκκολο κρυπτογράφησης δεδομένων SET.

Το SET (Secure Electronic Transactions) αποτελεί εξειδικευμένο πρωτόκολλο για τη διασφάλιση των ηλεκτρονικών συναλλαγών μέσω πιστωτικών καρτών, ενώ πρόσφατα αρχίζει να χρησιμοποιείται και στις ηλεκτρονικές τραπεζικές συναλλαγές. Κατασκευάστηκε από τις Visa, MasterCard, IBM, Netscape, Microsoft, GTE, Verisign. ITO SET αυτοί που συμμετέχουν σε μια συναλλαγή είναι ο πελάτης, ο έμπορος, η τράπεζα του πελάτη και η τράπεζα του εμπόρου, καθένας από τους οποίους πρέπει να έχει ψηφιακά πιστοποιητικά (digital certificates).

Με τη χρήση των ψηφιακών αυτών πιστοποιητικών επιβεβαιώνεται από τα συναλλασσόμενα μέρη (πωλητής και έμπορος) η ταυτότητα τους. Αυτό αποτελεί την πρώτη φάση της συναλλαγής (αυθεντικοποίηση των δύο μερών). Οι πελάτες επιβεβαιώνουν ότι οι έμποροι από τους οποίους επιθυμούν να αγοράσουν είναι νόμιμοι μέσα από την ψηφιακή ταυτότητα τους, όπως και οι έμποροι για τους πελάτες. Η εμπιστοσύνη αυτή εδραιώνεται μέσω των πιστοποιητικών. Ένα πιστοποιητικό περιέχει το όνομα του προσώπου για το οποίο εκδίδεται (έμπορος ή πελάτης), την ψηφιακή υπογραφή του, το δημόσιο (και το αντίστοιχο ιδιωτικό κλειδί του) και την υπογραφή της αρχής που εξέδωσε το πιστοποιητικό.

Το πρωτόκολλο SET στηρίζεται στην κρυπτογραφία, μια μέθοδο που χρησιμοποιείται εδώ και πολλά χρόνια για να προστατέψει τη μετάδοση ευαίσθητων πληροφοριών από μια τοποθεσία σε κάποια άλλη.

Σε ένα κρυπτογραφικό σύστημα οι πληροφορίες μεταδίδονται με μορφή μηνυμάτων, τα οποία κωδικοποιούνται με την βοήθεια ενός κλειδιού.

Το κωδικοποιημένο μήνυμα μεταφέρεται στον παραλήπτη όπου αποκρυπτογραφείται, με ένα αντίστοιχο κλειδί, για να εμφανιστεί η αρχική του μορφή. Η κρυπτογράφηση είναι ουσιαστικά ένας τρόπος κωδικοποίησης της πληροφορίας μέχρι αυτή να φτάσει στον αποδέκτη της, ο οποίος θα την αποκωδικοποιήσει με το κατάλληλο κλειδί.Κάθε φορά που συνδέεται κάποιος με μια υπηρεσία Web Banking, η επικοινωνία ανάμεσα στον υπολογιστή του και τα συστήματα της τράπεζας κρυπτογραφείται με χρήση κλειδιού 128bit. Όταν δηλαδή σταλούν πληροφορίες προς το σύστημα, το πρόγραμμα αναζήτησης κατ' αρχήν της τις αποκρυπτογραφεί με την χρήση ενός αλγορίθμου που στηρίζεται σε αριθμούς με 128bit και στην συνέχεια της τις στέλνει στο σύστημα.

Το σύστημα της τράπεζας αποκρυπτογραφεί πρώτα της πληροφορίες που λαμβάνει χρησιμοποιώντας το ίδιο κλειδί (που προκαθορίζεται με την έναρξη της σύνδεσης με την υπηρεσία)και κατόπιν τις επεξεργάζεται.

Η ίδια διαδικασία κρυπτογράφησης εφαρμόζεται και στην αποστολή των πληροφοριών από την τράπεζα προς τον χρήστη. Η απόρρητη γραμμή (55ί.)φαίνεται με το μικρό εικονίδιο του λουκέτου που εμφανίζεται στο κάτω μέρος της οθόνης του προγράμματος πλοήγησης. Οι περισσότερες τράπεζες χρησιμοποιούν την υλοποίηση της Verisign.

Όταν ο πελάτης δώσει μια παραγγελία, ο browser του λαμβάνει το πιστοποιητικό του εμπόρου, προκειμένου να ελεγχθεί αν είναι όντως νόμιμος - αν σχετίζεται με κάποιον χρηματοπιστωτικό οργανισμό.
Στην τράπεζα στέλνεται πληροφορία σχετικά με την πληρωμή, κρυπτογραφημένη με το δημόσιο κλειδί της τράπεζας.

Το μεγάλο πλεονέκτημα του είναι ότι με αυτόν τον τρόπο δεν στέλνεται πληροφορία με τον αριθμό της πιστωτικής κάρτας στον έμπορο. Το SET δεν έχει ακόμα χρησιμοποιηθεί ευρέως, παρόλο που αποτελεί ένα από τα πιο ασφαλή πρωτόκολλα. Σιγά-σιγά εμφανίζονται προϊόντα από μεγάλες εταιρίες του χώρου που χρησιμοποιούν το πρωτόκολλο. Για τις συναλλαγές που επιτρέπουν μόνο πληροφορίες, όπως είναι το υπόλοιπο ενός λογαριασμού, αρκεί η αρχική ταυτοποίηση με το όνομα του χρήστη και τον κωδικό πρόσβασης. Υπάρχουν επίσης οι συναλλαγές που εκτελούνται την ίδια στιγμή, σε πραγματικό χρόνο, και αυτές που παραμένουν για να εκτελεστούν σε μία άλλη χρονική στιγμή, όπως είναι τα εμβάσματα και οι πάγιες εντολές πληρωμής.

*Συμπέρασμα:*

Η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι.

# Συμπέρασμα ασφάλειας E-Banking

Είναι φανερό ότι η τεχνολογία για την πλήρη εξασφάλιση των συναλλαγών μέσω E-Banking υπάρχει. Τα σημερινά συστήματα κρυπτασφάλισης είναι αρκετά ασφαλή και ταυτόχρονα τόσο προσιτά στην καθημερινή χρήση τους, ώστε λίγοι συνειδητοποιούν τι ακριβώς συμβαίνει όταν κάποιος χρησιμοποιεί μια τραπεζική κάρτα σε ένα μηχάνημα αυτόματης ανάληψης χρημάτων (ATM).

Εντούτοις, υπάρχει σοβαρή έλλειψη τεχνογνωσίας και (κυρίως) εκπαίδευσης του αρμόδιου προσωπικού των τραπεζικών οργανισμών στα αντίστοιχα θέματα, με αποτέλεσμα η όλη διαδικασία να γίνεται εξαιρετικά δύσκολη και δυσνόητη για τους ενδιαφερόμενους πελάτες, οι οποία κατά κανόνα είναι λιγότερο ειδικοί επί των θεμάτων ασφαλούς χρήσης των υπηρεσιών E-Banking.

Προτού λοιπόν οι αρμόδιοι φορείς ασχολούνται με την εξαγγελία Νέων Τεχνολογιών, για την Κοινωνία της Πληροφορίας και για εντυπωσιακούς όρους όπως e-Government, καλό είναι να εστιάσουν την προσοχή τους στα πραγματικά προβλήματα και την καθημερινότητα των τεχνολογιών αυτών, το πως δηλαδή θα γίνουν κτήμα όλων, από τον πρώτο μέχρι τον τελευταίο πολίτη.

## Διακρίσεις τραπεζών όσον αφορά την ασφάλεια και την ταχύτητα των προσφερόμενων υπηρεσιών.

PCWorld (Απρίλιος 2008)

«Άριστη Υπηρεσία» για τρίτη χρονιά ανακήρυξε την υπηρεσία E-Banking της Eurobank το περιοδικό τεχνολογίας PCWorld, στο συγκριτικό τεστ που διεξήγαγε για τις υπηρεσίες E-Banking Ελληνικών τραπεζών.

" Η πληθώρα επιπλέον χαρακτηριστικών η ισχυρή ασφάλεια και η άψογη λειτουργικότητα της προσφέρουν αριστείο "

RAM (Φεβρουάριος 2008)

Για 6η συνεχή φορά οι συντάκτες του περιοδικού τεχνολογίας RAM (τεύχος Φεβρουάριου 2008) ανακήρυξε την υπηρεσία E-Banking της Eurobank «Κορυφαία Επίδοση» για το 2007. Μεταξύ άλλων αναφέρουν ότι: «Η Eurobank παρέχει πληθώρα υπηρεσιών, πλήρη υποστήριξη των πιστωτικών καρτών, αλλά και εξασφαλίζει άμεση εκτέλεση στις περισσότερες συναλλαγές. Όλες οι συναλλαγές που γίνονται σε λογαριασμούς και πιστωτικές κάρτες της Eurobank εκτελούνται σε πραγματικό χρόνο ολόκληρο το 24ωρο»

Technology Excellence Awards 2007 (Φεβρουάριος 2008 - PC Magazine Special Edition).Τον τίτλο "E-Bank of the Year" κατέκτησε η Eurobank στα Technology Excellence Awards 2007 που διοργάνωσαν για πρώτη φορά τα περιοδικά τεχνολογίας PC Magazine & T3. Οι συντάκτες του περιοδικού έγραψαν: «Η Eurobank κατάφερε να κερδίσει τις προτιμήσεις, ως η ηλεκτρονική τράπεζα της χρονιάς, επικρατώντας του e-ανταγωνισμού.»

# ΣΥΜΠΕΡΑΣΜΑ

Η πρόοδος της τεχνολογίας και η έλευση της πληροφορικής και του διαδικτύου έχει επιδράσει σημαντικά και στο τρόπο που διεξάγονται οι χρηματοοικονομικές συναλλαγές. Οι συναλλαγές γίνονται πιο εύκολα και με μικρότερο κόστος και πελάτες και πωλητές χρηματοοικονομικών προϊόντων έχουν άμεση πρόσβαση σε πληροφορίες. Έχουν απαλειφθεί οι μεσάζοντες και ο πωλητής έρχεται άμεσα σε επαφή με τον αγοραστή, μια διαδικασία που ονομάζεται «αποδιαμεσολάβηση».Ο όρος «αποδιαμεσολάβηση» αφορά την διεθνή τάση κατάργησης του μονοπωλίου παροχής χρηματοπιστωτικών υπηρεσιών από τις τράπεζες και την είσοδο νέου τύπου χρηματοοικονομικών υπηρεσιών από τις τράπεζες και την είσοδο νέου τύπου χρηματοοικονομικών μηχανισμών παροχής και άντλησης κεφαλαίων. Κυρίως αφορά τη δημιουργία απευθείας σχέσεων μεταξύ δανειστών/ δανειζομένων, αγοραστών/ πωλητών, προσφοράς και ζήτησης χρηματοοικονομικών υπηρεσιών,με τη παράκαμψη του άλλοτε κυρίαρχου ρόλου του τραπεζικού συστήματος.

Στο παρελθόν, ένας συνδυασμός παραγόντων οδήγησε τις τράπεζες να επανεξετάσουν τη στρατηγική τους και να παρέχουν υπηρεσίες στους πελάτες τους οπουδήποτε, οποτεδήποτε και οπωσδήποτε. Καθώς οι καταναλωτές αισθάνονται ολοένα και πιο άνετα με τη χρήση της νέας τεχνολογίας, υπάρχει μία μετατόπιση από τις δαπανηρές πρόσωπο με πρόσωπο συναλλαγές σε ένα σχήμα οικονομικότερο και ευκολότερο. Το πέρασμα από τις παραδοσιακές τραπεζικές συναλλαγές στην ηλεκτρονική τραπεζική δε θα γίνει από τη μία στιγμή στην άλλη, αλλά με αργούς ρυθμούς.

Η περίοδος που διανύουμε είναι μεταβατική στην εξοικείωση με το E-Banking που δε θα αντικαταστήσει τις παραδοσιακές τράπεζες, αλλά θα τις συμπληρώσει. Το Internet και οι τράπεζες έχουν κάποια ξεχωριστά χαρακτηριστικά που κάνουν την συνεργασία τους ιδανική.

Η πληροφορική έρχεται να φέρει την επανάσταση στις ηλεκτρονικές τραπεζικές συναλλαγές μέσα από τη χρήση του διαδικτύου, οι οποίες χρόνο με το χρόνο βελτιώνονται και προσφέρουν εμπιστοσύνη στο ευρύ κοινο λόγω της απλοποίησης της ταχύτητας και της ασφάλειας αυτών των υπηρεσιών τους.

# ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ

## *1) Χρήση E-Banking ανα ηλικία.*

Παρατηρούμε ότι το 36,6% και άρα το μεγαλύτερο ποσοστό του δείγματος συγκριτικά βρίσκεται στις ηλικίες μεταξύ 20-29 ετών.

Αυτές οι ηλικίες είναι πιό εξοικιωμένες με τη χρήση των κινητών τηλεφώνων, του ηλεκτρονικού υπολογιστή και κατ'επέκταση είναι πιό ανοιχτές στη χρήση των ηλεκτρονικών τραπεζικών συναλλαγών λόγω του οι νέες τεχνολογίες έχουν διεισδύσει κατά κάποιο τρόπο στη ζωή τους από τη σχολική ηλικία. Οι ηλικίες που βρίσκονται μεταξύ 30-39 ετών κάνουν χρήση των υπηρεσιών αυτών σε συγκριτικά ικανοποιητικό βαθμό, στο ποσοστό του 28%.

Η γενιά αυτή θα μπορούσαμε να πούμε πώς είναι ίσως λιγότερο εξοικειωμένη σε σχέση με την προηγούμενη. Παρ'όλα αυτά, συμμετέχουν με ένα αρκετά ικανοποιητικό ποσοστό.

Οι ηλικίες μεταξύ 40-49 ετών σύμφωνα με την έρευνα, κάνουν χρήση των υπηρεσιών E-Banking κατά 22%.

Αν και η χρήση χρήση των νέων τεχνολογιών δεν είναι απαραίτητο πάντα να συμβαδίζει με την ηλικία αλλα έχει να κάνει και με το κάτα πόσο το κάθε άτομο είναι ανοιχτό στι νέες τεχνολογίες και στο κατά πόσο δύναται να προσαρμόζεται κάθε φορά στα δεδομένα της εποχής.

Οι ηλικίες μεταξύ 50-59 ετών, χρησιμοποιούν τον σχετικά νέο αυτό τρόπο ηλεκτρονικών συναλλαγών, κατα 7,3%.

Παρατηρούμε όμως, πως σε αυτές τις ηλικίες αρχίζει μια σημαντική πτώση στη χρήση των υπηρεσιών αυτών.

Ένας από τους προφανείς λόγους είναι η δυσκολία εξοικείωσης τους με τα νέα δεδομένα που προσφέρει η εξέλιξη της τεχνολογίας, καθώς είναι δύσκολο να αποχωριστούν κατά κάποιο τρόπο την σιγουρία και την ασφάλεια που τους δημιουργούσε όλα αυτά τα χρόνια ο παραδοσιακός τρόπος συναλλαγών.

Επίσης παρατηρούμε πως οι ηλικίες μεταξύ 60-69 χρονών χρησιμοποιούν το E-Banking κατα 3,3%. Αυτό λογικά θα μπορούσε να συμβαίνει για το λόγω του ότι η γενια αυτή καθε αυτή αρχίζει να απομακρύνεται από την παραγωγική ηλικία γι' αυτό η ανάγκης τους για τη χρήση των υπηρεσιών αυτών παύει να είναι μείζονος σημασίας.

Ωστόσο, συγκριτικά με τις προηγούμενες γενιές, αυτή η γενιά είναι λιγότερο εξοικειωμένη με τις νέες τεχνολογίες και έτσι δεν είναι τόσο εφικτή η προσαρμογή τους στη νέα τάξη πράγματων και γι' αυτό το λόγω προτιμούν να παραμείνουν στη σιγουριά που είχαν συνηθίσει, του παραδοσιακού τρόπου συναλλαγής.

Επίσης παρατηρουμε πώς οι γυναίκες, αλλά και σε λίγο μεγαλύτερο βαθμό οι άντρες, ηλικίας μεταξύ 20-29 ετών εεμπιστεύονται ευκολότερα και είναι πιο πολύ εξοικειωμένοι με τη χρήση των προσφερόμενων υπηρεσιών ηλεκτρονικής τραπεζικής.

## *2) Πόσο συχνά χρησιμοποιείτε το διαδίκτυο;*

Παρατηρούμε πώς το μέγαλύτερο ποσοστό του δείγματος της έρευνας, χρησιμοποιεί πολύ συχνά κατά 31% το διαδίκτυο στη καθημερινή του ζωή.

Αρκετά αξιοσημείωτο είναι και το ποσοστό που συνδέεται καθημερινά στο διαδίκτυο έστω και για το χρονικό διάστημα των τριάντα λεπτών.

Αυτό το ποσοστό αγγίζει το 26%.Ακολουθεί το 21% των ερωτηθέντων το οποίο δηλώνει ότι χρησιμοποιεί το διαδίκτυο συχνά. Το 14% συνδέεται σπάνια γιατί δε διαθέτει κάποιο υπολογιστή στο σπίτι και συνήθως χρησιμοποιεί το διαδίκτυο όταν βρίσκεται στον εργασιακό χώρο.

Ωστόσο το 8% δηλώνει ότι δε συνδέεται ποτέ με το διαδίκτυο λόγω του ότι δεν επιθυμεί να χρησιμοποιεί τη νέα τεχνολογία.

### *3)Πόσα χρόνια χρησιμοποιείτε το διαδίκτυο;*

Σύμφωνα με τα δεδομένα της έρευνας, το μεγαλύτερο ποσοστό των ερωτηθέντων χρησιμοποιεί το διαδίκτυο συχνότερα τα τελευταία 2 έως 3 χρόνια, σε ποσοστό 28%. Έπειτα βλέπουμε πως το 24% απαντάει πως συνδέεται στο διαδίκτυο συχνότερα τα τελευταία 1 έως 2 χρόνια.

Στη συνέχεια παρατηρούμε ότι το 21% των ερωτηθέντων κάνει χρήση του ίντερνετ τα τελευταία 3 έως 5 χρόνια ενώ το 15% απαντάει πως έχει λιγότερο από ένα χρόνο που έχει αρχίσει να το χρησιμοποιεί.

Ακόμα υπάρχει και ένας μικρός αριθμός ατόμων, σχεδόν το 5% ο οποίος υποστηρίζει πως κάνει χρήση του διαδικτύου πάνω από πέντε χρόνια.

Από τα παραπάνω στοιχεία παρατηρούμε οι ερωτηθέντες χρησιμοποιούν σε συχνή βάση το διαδίκτυο τα τελευταία έτη. Σε αυτό είναι προφανές ότι έχουν συμβάλλει και τα διάφορά οικονομικά πακέτα σύνδεσης ίντερνετ που κυκλοφορούν στην αγορά και τα οποία προσφέρουν πολλές εναλλακτικές και συμφέρουσες λύσεις στον υποψήφιο αγοραστή με αποτέλεσμα να πείθεται να τα χρησιμοποιήσει.

Τέλος οφείλουμε και εδώ να επισημάνουμε πως οι ηλικίες που χρησιμοποιούν τα τελευταία χρόνια το διαδικτυο είναι μεταξύ 20 και 39 ετών.

## *4) Πόσο ενημερωμένοι είστε για το Internet Banking;*

Παρατηρούμε πώς το μεγαλύτερο ποσοστό το οποίο αγγίζει το 31% είναι λίγο ενημερωμένο όσον αφορά την ηλεκτρονική τραπεζική, ενώ ακολουθεί με ποσοστό 27% το ποσοστό των ατόμων που απάντησε πώς είναι μέτρια ενημερωμένο για τις υπηρεσίες αυτές. Τα ατομά που ανήκουν σε αυτές τις δύο κατηγορίες αξίζει να σημειωθεί πως απάντησαν κατ' αυτόν τον τρόπο βασιζόμενοι στην άποψη ότι αν και θα ήθελαν να έχουν λάβει περισσότερη ενημέρωση από τις τράπεζες για τη λειτουργία των σχετικά νέων αυτών τρόπων παροχής υπηρεσιών, επισημαίνουν πώς υπάρχει μια γενικότερα ελλειπής ενημέρωση από τις ίδιες τις τράπεζες,στο πελατειακό τους κοινό.

Ακολουθεί το 19% των ερωτηθέντων οι οποίοι δηλώνουν πώς έχουν πολύ λίγη γνώση γιατί οι τράπεζες δεν παρέχουν αναλυτικότερη ενημέρωση αλλά και γιατί δεν έχουν και τα ίδια τα άτομα το ανάλογο ενδιαφέρον για να ενημερωθούν σχετικά. Αξίζει να σημειωθεί πώς το μεγαλύτερο ποσοστό των ερωτηθέντων που απάντησαν πως είναι λίγο ή πολύ λίγο ενημερωμένοι σχετικά με τις υπηρεσίες αυτές, ανήκει στις ηλικίες από σαράντα ετών και άνω.

Στη συνέχεια, παρατηρούμε το 14% στην ερώτηση αυτή απαντάει πως είναι πολύ ενημερωμένο, ενώ το μόλις 9% απαντάει πως έχει λάβει πλήρη ενημέρωση των υπηρεσιών αυτών.

Σε αυτό το σημείο θα πρέπει να επισημανθεί πως τα ποσοστά των ατόμων που έχουν απαντήσει πως έχουν ενημερωθεί πολυ και πάρα πολύ ανήκουν στην κατηγορία ηλικιών από 20 έως και 29 ετών.

***5)Σε ποιές η που συνεργάζεστε κάνετε χρήση των υπηρεσιών E-Banking***;

Με βάση τα δεδομένα μας παρατηρούμε πώς τη πρώτη θέση στις προτιμήσεις του ερωτηθέντους κοινού κατέχει η τράπεζα Πειραιώς με 19%.
Στη συνέχεια ακολουθεί η τράπεζα EFG Eurobank με μόνο μία ποσοστιαία μονάδα διαφορά του 18%. Τρίτη στη σειρά βρίσκεται η Εμπορική τράπεζα με 16% και λίγο πιό κάτω η Alphabank με 13%. Στην πέμπτη θέση συγκριτικά με ποσοστό 10%είναι η Εθνική τράπεζα.
Λίγο πιο κάτω με ποσοστό 8% επιλέγεται η ATEbank, την οποία εν συνεχεία ακολουθεί η Marfin Egnatia τράπεζα.

Τέλος παρατηρούμε πως στην προτελευταία θέση με το ποσοστό του 5% επιλέγεται η Attica bank, ενώ στην την τελευταία θέση βλέπουμε ότι κατέχει με ποσοστό 4% η τράπεζα Κύπρου. Από τα παραπάνω δεδομένα της έρευνας παρατηρούμε πώς οι τράπεζες τις οποίες έχουν επιλέξει οι συμμετέχοντες για τη χρήση των υπηρεσιών ηλεκτρονικής τραπεζικής συμπίπτουν με τις τράπεζες που χρησιμοποιούν συνηθέστερα και σε μεγαλύτερο βαθμό και για τι απλές καθημερινές τους συναλλαγές. Αυτό συμβαίνει για το λόγο του ότι σε αυτές αισθάνονταιμεγαλύτερη εμπιστοσύνη.

Επίσης είναι εύλογο να σημειώσουμε πώς τα αποτελέσματα της έρευνας αυτής συμπίπτουν σε ένα μεγάλο βαθμό με τη πρόσφατη έρευνα της τράπεζας Ελλάδος,η οποία εμφανίζει σχεδόν με την ίδια σειρά τη προτίμησης την επιλογή τραπεζών των πελάτων όσον αφορά την επιλογή των τραπεζών για τη χρήση των ηλεκτρονικών τραπεζικών συναλλαγών.

***6) Γενικά μιλώντας, πόσο ευχαριστημένος/η είστε από τις υπηρεσίες E-Banking;***

Στο ερώτημα αυτό, το μεγαλύτερο μέρος των ερωτηθέντων απαντάει πως είναι μέτρια ικανοποιημένο από τις παρεχόμενες αυτές υπηρεσίες σε ποσοστό 34%. Στη συνέχεια ακολουθεί ένα ποσοστό ατόμων 27% το οποίο δηλώνει πως είναι ευχαριστημένο πολύ από τις παρεχόμενες αυτές υπηρεσίες. Επίσης το 16% του δείγματος απαντάει πως είναι πολυ ευχαριστημένο από αυτόν τον νέο τρόπο συναλλαγής. Ωστόσο, υπάρχει και ένα σημαντικό ποσοστό το οποίο αγγίζει το 23% και το οποίο δηλώνει πως είναι δυσαρεστημένο από το E-Banking. Σχετικά με τα παραπάνω αποτελέσματα της έρευνας, θα πρέπει να σημειωθεί πως αρκετοί είναι εκείνοι που δε γνωρίζουν όλες τις υπηρεσίες της ηλεκτρονικής τραπεζικής στον ίδιο βαθμό ίσως να απάντησε ο κάποιος για μία, κάποιος άλλος για δύο και κάποιος άλλος για τρείς ή περισσότερε υπηρεσίες που του ήταν γνώριμες.

***7) Πόσο συχνά χρησιμοποιείτε τις παρακάτω υπηρεσίες E-Banking;***

Παρατηρούμε σύμφωνα με τα δεδομένα τη έρευνας πώς το μεγαλύτερο ποσοστό των ερωτηθέντων, δηλαδή το 27% διαχειρίζεται τους λογαριασμούς του μέσω του του E-Banking.Το 25% σημειώνεται ότι πραγματοποιεί πάγιες εντολές-πληρωμές, ένω το 18% χρησιμοποιεί τις υπηρεσίες ηλεκτρονικές τραπεζικές υπηρεσίες για να κάνει συναλλαγές μέσω των καρτών. Εδώ θα πρέπει να σημειώσουμε πως μέσα στον όρο κάρτες, συμπεριλαμβάνονται εκτός από τις πιστωτικές, οι οποίες είναι περισσότερο διαδεδομένες, οι χρεωστικές αλλα και οι προπληρωμένες κάρτες. Όσον αφορά τα δάνεια, η χρήση τους γίνεται με διαφορά τριών μονάδων από των καρτών, σε ποσοστό 15%. Στη συνέχεια η χρηματιστηριακές συναλλαγές διενέργούνται από το 11% του δείγματος.

Τέλος οι επιταγές από την έρευνα φαίνεται πώς είναι στο τέλος των προτιμήσεών τους σε ποσοστό 4%. Αυτό είναι λογικό να συμβαίνει, λόγω του ότι οι επιταγες χρησιμοποιούνται από ένα ορισμένο αριθμό πελατών και για συγκεκριμένου είδους συναλλαγές.

### *8) Θεωρώ απλό το να αποκτήσω πρόσβαση και να πραγματοποιήσω την συναλλαγή που επιθυμώ μέσω της E-Banking.*

Το 31% το οποίο είναι και το υψηλότερο ποσοστό του δείγματος, δηλώνει πως συμφωνεί με αυτή την πρόταση. Ένα μεγάλο μέρος του δείγματος το οποίο εκπροσωπεί το 26% θα λέγαμε πως ούτε συμφωνεί αλλά ούτε και διαφωνεί με την πρόταση αυτή.
Επίσης το 20% του δείγματος συμφωνεί απόλυτα με αυτή την άποψη.
Ωστόσο, υπάρχει και ένα 14% που διαφωνεί με αυτή την γνώμη. Ακόμα, ένα μικρό αλλα άξιο και αυτό προσοχής ποσοστό διαφωνεί απόλυτα και αντιμετωπίζει τη πρόσβαση στις υπηρεσίες αυτές με δυσανασχέτιση. Θα πρέπει να τονίσουμε πως αυτή η διάσταση απόψεων είναι φυσιολογική, αν αναλογιστούμε την διαφορετική οπτική γωνία με την οποία το κάθε άτομο βλέπει τα πράγματα.
Αυτό συμβαίνει πρώτον επειδή κάποια άτομα είναι πιο εξοικειωμένα με τις νέες τεχνολογίες και γι αυτό το λόγο για κάποιον που δε γνωρίζει τα βασικά πράγματα να του φαντάζει αρκέτα έως πολύ δύσκολο.
Δεύτερον, μερικά άτομα είναι προκατειλημμένα απέναντι στη νέα τεχνολογία και όντας κατα κάποιο τρόπο καχύποπτα,αρνούνται να την ακολουθήσουν.

Τρίτον μπορούμε να δικαιολογήσουμε- κατανοήσουμε τις απόψεις των ερωτηθέντων και να κατανοήσουμε τις αρνητικές τους απαντήσεις επειδή ακόμα οι ηλεκτρονικές τραπεζικές συναλλαγές βρίσκονται ακόμα στο στάδιο της εξέλιξης και έτσι όρισμένες τράπεζες,μπορεί να υπερτερούν σε σχέση με άλλες όσον αφορά την παροχή των υπηρεσιών αυτών. Το ίδιο ακριβώς συμβαίνει και στην περίπτωση που ο χρήστης θέλει να πραγματοποιήσει τη συναλλαγή που επιθυμεί μέσω του E-Banking.

## 9) Η χρήση του Internet Banking με βοηθάει στο να χρησιμοποιώ τις τραπεζικες υπηρεσίες φθηνότερα.

Διαπιστώνουμε πως με την άποψη αυτή το 33% συμφωνεί απολύτως και το 27% απαντάει θετικά ότι συμφωνεί. Ωστόσο, υπάρχει ένα ποσοστό 21% το οποίο ουτε συμφωνεί ούτε διαφώνει,πράγμα που σημαινει πώς είτε στερείται γνώσης, είτε είναι και φιδωλό ώς προς το να δείξει εμπιστοσυνη σε αυτό το νέο είδος συναλλαγής. Ακόμα, το 11% διαφωνεί με την άποψη αυτή, ενώ συναντάμε και ένα ποσοστό 8% το οποίο διαφωνεί απόλυτα με την άποψη αυτή καθεαυτή.

Σε αυτή την περίπτωση, επειδη γνωρίζουμε πως ισχύει πράγματι πως οι συναλλαγές μέσω της ηλεκτρονικής τραπεζικής είναι φθηνότερες σε σχέση με το παραδοσιακό τρόπο συναλλαγής, θα μπορούσαμε να υποθέσουμε πως το ποσοστό το οποίο διαφωνεί προέρχεται από άτομα κυρίως μεγαλύτερης ηλικίας τα οποια φοβούνται να εμπιστευτούν το σχετικά νέο αυτό τρόπο συναλλαγών επειδή έχουν ακούσει πως τίθεται σοβαρά προβλήματα σχετικά με την αξιοπιστία αυτών,είτε από άτομα τα οποία είχαν πέσει θύμα κάποιας υπερχέωσης από δικό τους λάθος ή ακομα,αν και πιο σπάνιο,από λάθος της ίδιας της τράπεζας μέσα από το site του E-Banking της.

**10) Οι συναλλαγές μέσω του Internet Banking είναι περισσότερο ασφαλείς σε σχέση με αυτές που κάνω μέσω του τραπεζικού καταστήματος.**

Παρατηρούμε πως το 31% συμφωνεί με την άποψη αυτή. Υπάρχει όμως και ένα σημαντικό ποσοστό το οποίο αγγίζει το 24 % και σημειώνει ότι ούτε συμφωνεί ούτε διαφωνεί.
Συγκεκριμένα διαπιστώνουμε μία κατά κάποιο τρόπο σύγχυση γνώμεων ως προς το θέμα της ασφάλειας με το 18% να απαντάει ότι διαφωνεί, το 16% να συμφωνεί απόλυτα ενώ το 11% να διαφωνεί απόλυτα.

**11) Τα θέματα ασφάλειας, δεν επηρεάζουν τη χρήση εκ μέρους μου, του Internet Banking.**

Σε αυτή την ερώτηση, διαπιστώνουμε πως όντως υπάρχει μια αρκετά μεγάλη επιφύλαξη όσον αφορά την ασφάλεια των προσφερόμενων ηλεκτρονικών τραπεζικών συναλλαγών, λόγω του ότι το 32% διαφωνεί με την παραπάνω άποψη, το 22% παρατηρούμε ότι διαφωνεί απόλυτα και το 19% ούτε συμφωνεί αλλα ούτε και διαφωνει με τη πρόταση αυτή. Επίσης το 16% παραδέχεται ότι συμφωνεί και μόνο ένα 11% δείχνει να συμφωνεί απόλυτα με τη γνώμη αυτή. Από αυτέ τις απαντήσεις μπορούμε να κατανοήσουμε ότι υπάρχει ένα σημαντικό θέμα ασφάλειας το οποίο απασχολεί σε αρκετά μεγαλό βαθμό τους ερωτηθέντες.

# ΣΥΜΠΕΡΑΣΜΑ ΕΡΕΥΝΑΣ

Συνοψίζοντας όλα τα παραπάνω στοιχεία της έρευνας, μπορούμε να συμπεράνουμε αρχικά πως η ηλικία παίζει καθοριστικό ρόλο στη στάση του όσον αφορά την προσαρμοστικότητα του αλλα και την εξοικείωση του στις νέες τεχνολογικές υπηρεσίες.

Ιδιαίτερο ρόλο δεν έδειξε να διαδραματίζει το φύλο του χρήστη,καθώς όπως διαφάνηκε στην έρευνα η γυναίκες δεν έχουν ίδιαίτερη διαφορά στη προτίμηση χρήσης των υπηρεσιών ηλεκτρονικής τραπεζικής αν και οι άντρες σύμφωνα με την έρευνα, φαίνεται οι άντρες να χρησιμοποιούν λίγο παραπάνω τις ηλεκτρονικές τραπεζικές αυτές υπηρεσίες έναντι των γυναικών.

Ένας άλλος καθοριστικός παράγοντας είναι η μόρφωση. Παρατηρήθηκε πως τα άτομα που κατείχαν μόρφωση πρωτοβάθμιας και δευτεροβάθμιας εκπαιδευσης, πως παρουσίαζαν μεγαλύτερη δυσκολία στο να χειριστούν τις υπηρεσίες της ηλεκτρονικής τραπεζικής σε σχέση με αυτούς που ανήκαν στην ανώτερη και ανώτατη εκπαίδευση. Επίσης παρατηρήθηκε πως οι ερωτηθέντες οι οποίοι είχαν πρωτοβάθμια και δευτεροβάθμια μόρφω μόρφωση, πως λειτουργούν πιο καχύποπτα απέναντι στο σχετικά νέο αυτό τρόπο συναλλαγών.

Ωστόσο σημαντικό είναι να αναφέρουμε πως σε αυτό το οποίο σχεδόν όλοι οι συμμετέχοντες ανεξαρτήτως της ομάδας στην οποία ανήκαν, συμφωνούσαν κατα κάποιο τρόπο στο ότι υπάρχει ακόμα ένα πολύ σημαντικό θέμα όσον αφορά την ασφάλεια την ταχύτητα και την απλοποίηση των συναλλαγών.

Αυτό σημαίνει ότι εδώ θα πρέπει οι τράπεζες να εφιστήσουν τη προσοχή τους, λόγω του ότι ο κόσμος διακατέχεται από μία αρκετά μεγάλη επιφύλαξη για το κατά πόσο ασφαλείς είναι οι συναλλαγές αυτές οι οποίες οι οποίες παρέχουν οι τράπεζες. Σίγουρα η τεχνολογία έχει κατορθώσει να κάνει σημαντικά βήματα σε πολλούς τομείς και αναμφισβήτητα και στον τραπεζικό τομέα τα τελευταία χρόνια αλλα το μόνο σίγουρο είναι ότι χρειάζεται ακόμα χρόνος για την εξοικείωση των πελατών για αυτό τον νέο και πολύ χρήσιμο τρόπο τραπεζικών συναλλαγών , αλλα και αρκετή προσπάθεια από μέρους των τραπεζών ώστε να επιτευχθεί το προσδοκώμενο αποτέλεσμα: Η απλοποίηση, η ταχύτητα και η ασφάλεια των συναλλαγών.

# ***ΒΙΒΛΙΟΓΡΑΦΙΑ***

## ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ


*Michael Kunz, 18 January 2001, Regulation of electronic banking.*

*Claudio Deplazes, 26 January 2002, Internet banking and the law.*

*Krishna Kishore, 28 March 2008, Internet Banking Multi- Dimensional Perspectices.*

*Mary Cronin, 29 August 1997, Banking and Finance on the internet (Internet managment series).*

*Solomon Okhiria, 23 June 2009, Personal finance and online banking.*

*G. Chapman, 15 April 2004, Internet Banking and shopping for the older generation(BP).*

Attila Hucker, 1 January 2000, Internet-banking.

R. Uppal, 19 January 2008, Banking with Technology.

Apostolos Ath Gkoutzinis, November 2006, Internet Banking and the law in Europe: Regulation. Financeintergration and electronic commerce.

David Morris, 22 January 2005, The U.S. Market for online banking.

Michael Kunz, 27 January 2001, Electronic Banking.

# ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ


*Σινανιώτη – Μαρούδη, 2005, Ηλεκτρονική τραπεζική, Εκδόσεις: Σακούλας Αντ.Ν.*

*Γιαννακόπουλος Διονύσιος, Πολλάλης Γιάννης,2007, Ηλεκτρονικό επιχειρείν, Εκδόσεις: Σταμούλης.*

*Ψυχομάνης Σπύρος, 2002, Τραπεζικές δραστηριοτητες αμφισβητήσιμης νομιμότητας, Εκδόσεις: Σάκκουλας.*

*Γεωργακόπουλος Λεωνίδας, 2003, Χρηματιστηριακό και τραπεζικό δίκαιο, Εκδόσεις: Σάκκουλας.*

*Καρακώστας Γιάννης, 2001, Γενικοί όροι των τραπεζικών συναλλαγών, Εκδόσεις: Σάκκουλας.*

*Κιάντος Βασίλειος, 1993, Το τραπεζικό απόρρητο και οι εργασιες συναλλάγματος, Εκδόσεις: Σάκουλας.*

*Τραγακης Γεώργιος, 1996, Συνεταιριστικές τράπεζες στην Ελλάδα, Εκδόσεις: Σάκκουλας.*

*Ντόκας Μιχαήλ, 2003, Γενικό τραπεζικό απόρρητο των καταθέσεων, Εκδόσεις: Σάκκουλας.*

*Ντόκας Μιχαήλ, 2004, Η προστασία του καταναλωτή στις τραπεζικές συναλλαγές, Εκδόσεις: Σάκκουλας Αντώνης.*

*Βασίλης Αγγελής, 2005, Η βίβλος του E-Banking, Γ. Εκδόσεις: Νέων τεχνολογιών.*

*Ρεπούσης Σπύρος, 2005, Τραπεζικές υπηρεσίες, Εκδόσεις: Σάκκουλας.*

*Χρυσάνθης Χρήστος Σ., 1997, Η ηλεκτρονική τραπεζική των σύγχρονων τραπεζικών συναλλαγών, Εκδόσεις: Σάκκουλας.*

*Ρόκας Νικόλαος, 2002, Στοιχεία τραπεζικού δικαίου, Εκδόσεις: Σάκκουλας.*

*Ρεπούσης Σπύρος, 2008, Σύγχρονα τραπεζικά θέματα, Εκδόσεις: Σάκκουλας.*

*Κουτσούκης Δημήτρης, 1998, Τραπεζικό απόρρητο, Εκδόσεις: Σάκκουλας.*

*Μηλιαράκης Πέτρος, 1994, Τραπεζικό Δίκαιο, Εκδόσεις: Σμπίλιας.*

## ΙΣΤΟΣΕΛΙΔΕΣ

www.academon.com/essay-e-banking/62265

www.en.wikipedia.org/wiki/online_bankingurity.info/

*http://internet-banking-security.info/*

http://www.go-online.gr/ebusiness/ebanking.html

www.go-online.gr/preview.html

www.eede.gr/pdf/13_banking_forum.pdf

www.go-onine.gr/ebanking.html

www.realize.gr/launch.html

www.marfinegnatiabank.gr*marfinegnatia.gr*

*www.ebanking.geniki.gr/index.aspx*

www.dart.gov.gr/newslinner.aspx

www.hypovereinsbank.grpebanking.*gr*.*htm*

www.ameinfo.com/news/e-banking/

www.combank.gr/

www.e-pcmag.gr/e-banking

www.ebank.emporiki.gr

www.ubs.com/1/e/banking.html

https://www.alpha.gr/ib/secureehtm/gr/signon_1.asp

www.ebanking.bankofcyprus.gr/

www.dir.vres.gr/category.php

www.ebanking.hsbc.com.hk/

www.elock.com/e-banking.htm

www.imerisia.gr/article.asp

www.ebanking.eurobank.gr

www.tieto.com/default.asp

www.financea.com/article.aspx

www.bis.org/pupl/bcbs82.htm.