**Α**ΝΩΤΑΤΟ **Τ**ΕΧΝΟΛΟΓΙΚΟ **Ε**ΚΠΑΙΔΕΥΤΙΚΟ **Ι**ΔΡΥΜΑ **Π**ΑΤΡΩΝ

**ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ**

**ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ**

# ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

## Υπηρεσίες - χρήση του e-banking στην Ελλάδα

Σπουδάστριες: Δήμου Τερέζα Μαρία (8392)
Τυροπάνη Αντωνία (8334)

Επιβλέπων Καθηγητής: κ. Χριστολουκάς Λουκάς

ΠΑΤΡΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2010

# Περίληψη

Σε αυτήν την πτυχιακή εργασία, σκοπός μας είναι να εξετάσουμε το επίπεδο στο οποίο βρίσκεται η ηλεκτρονική τραπεζική στη χώρα μας.

Για το λόγο αυτό, αρχικά γίνεται μία εισαγωγή στο e-banking, όπου αναφέρονται συνοπτικά τα είδη του, καταγράφονται οι υπηρεσίες που μπορούν να χρησιμοποιηθούν μέσω της ηλεκτρονικής τραπεζικής καθώς επίσης και οι υπηρεσίες προστιθέμενης αξίας που προσφέρονται στους χρήστες της συγκεκριμένης υπηρεσίας.

Επίσης, γίνεται συνοπτική αναφορά στα πλεονεκτήματα αλλά και στα μειονεκτήματα που έχει η χρήση της online τραπεζικής στους πελάτες που την χρησιμοποιούν, είτε αυτοί είναι ιδιώτες είτε είναι επιχειρήσεις καθώς και στα πλεονεκτήματα - μειονεκτήματα που έχουν οι τράπεζες από το e- banking.

Ένα πολύ σημαντικό ζήτημα, το οποίο δεν θα μπορούσε να παραληφθεί, είναι αυτό της ασφάλειας των ηλεκτρονικών συναλλαγών. Για το λόγο αυτό γίνεται αναλυτικά καταγραφή των κινδύνων και των απειλών που καραδοκούν στις ηλεκτρονικές συναλλαγές, και αναλύονται τα μέτρα που λαμβάνουν οι τράπεζες προκειμένου να προστατεύσουν τους πελάτες – χρήστες.

Στη συνέχεια, γίνεται μία συνοπτική παρουσίαση της χρήσης του Internet και του e-Banking βασισμένη σε έρευνες που έλαβαν χώρα στην Ελλάδα, και παρουσιάζεται ένας πίνακας με τις προσφερόμενες υπηρεσίες των τραπεζών που δραστηριοποιούνται στην χώρα μας.

Τέλος, αναλύονται τα αποτελέσματα τα οποία προέκυψαν από την έρευνα που πραγματοποιήθηκε στα πλαίσια της συγκεκριμένης εργασίας τα οποία και μας βοηθούν να δούμε το επίπεδο στο οποίο βρίσκεται η ηλεκτρονική τραπεζική στη χώρα μας σήμερα, τόσο από την πλευρά των τραπεζών που παρέχουν την συγκεκριμένη υπηρεσία όσο και από την πλευρά των χρηστών.

Συνοπτικά θα μπορούσαμε να πούμε ότι το επίπεδο της ηλεκτρονικής τραπεζικής στην Ελλάδα βρίσκεται σε ικανοποιητικό επίπεδο αν και ο αριθμός των χρηστών στη χώρα μας είναι ακόμα αρκετά μικρός.

# Ευχαριστίες

Η παρούσα Πτυχιακή Εργασία είναι αποτέλεσμα μεγάλης προσπάθειας από μέρους μας. Όμως δεν θα ήταν δυνατή η ολοκλήρωσή της χωρίς τη βοήθεια ορισμένων ανθρώπων. Για αυτό ευχαριστούμε τους γονείς μας για την αμέριστη βοήθεια και στήριξή τους, τον επιβλέποντα καθηγητή μας για την καθοδήγηση του καθώς και τις τράπεζες και τους χρήστες που βοήθησαν στην έρευνά μας.

**Δήμου Τερέζα Μαρία**

**Τυροπάνη Αντωνία**

# Περιεχόμενα

**Περίληψη** .....2

**Ευχαριστίες** .....3

**Λίστα Γραφημάτων**.....7

**Πίνακες** .....9

**Εισαγωγή** .....10

**Κεφάλαιο 1. Εισαγωγικές έννοιες του e-Banking**

1.1 Το Internet στην Ελλάδα .....11

1.2 E- Banking…….....14

1.3 Τα είδη του e- banking.....15

**Κεφάλαιο 2. Υπηρεσίες– Δυνατότητες του e- Banking**

2.1 Internet Banking .....18

2.2 Phone Banking.....26

2.3 Mobile Banking .....28

**Κεφάλαιο 3. Πρόσθετες υπηρεσίες**

3.1 E- Investment.....32

3.2 E- Commerce (e- Payments) .....33

3.3 Alerts.....36

3.4 P2P Πληρωμές .....37

3.5 Πώληση ασφαλιστικών προϊόντων.....37

3.6 Trade Finance (online εισαγωγές – εξαγωγές) .....38

3.7 Συναλλαγές πραγματικού χρόνου.....38

3.8 Electronic Bill & Presentment (EBPP).....38

3.9 Σύνδεση internet banking με συστήματα logistics .....40

3.10 Αυτόματο άνοιγμα καταθετικού λογαριασμού χωρίς φυσική παρουσία του πελάτη. .....40
3.11 Ολοκληρωμένα Portals .....41

**Κεφάλαιο 4. Πλεονεκτήματα και μειονεκτήματα χρήσης e-Banking για Τράπεζες και Χρήστες**
4.1 Για τον πελάτη .....42
4.2 Για την τράπεζα .....44

**Κεφάλαιο 5. Απειλές και Κίνδυνοι από τη χρήση του e-banking**
5.1 Sniffers.....47
5.2 Key Loggers.....48
5.3 Κοινωνική μηχανική .....49
5.4 Δούρειοι Ίπποι .....50
5.5 Phishing .....50
5.6 Pharming.....53

**Κεφάλαιο 6 Ασφάλεια - Τρόποι προστασίας από on line απάτες**
6.1 Κρυπτογράφηση .....57
6.2 PKI…….....60
6.3 Πιστοποίηση δύο παραγόντων.....65
6.4 Έξυπνες κάρτες (Smart Cards) .....66
6.5 Πιστοποίηση δύο παραγόντων και PKI.....68
6.6 Single Sign On (SSO) .....70
6.7 Firewalls.....72

**Κεφάλαιο 7. Έρευνες για το e-Banking στην Ελλάδα**
7.1 Το e- Banking στην Ελλάδα .....74
7.2 Ελληνικές τράπεζες και e-Banking.....79

**Κεφάλαιο 8.Πρωτογενής Έρευνα για την Ηλεκτρονική τραπεζική στην Ελλάδα**

**Μέρος Α - Τράπεζες**.....85
8.1 e-Banking & προσφερόμενες υπηρεσίες .....85
8.2 Στρατηγική – Στόχοι .....90
8.3 Τράπεζες & νέες τεχνολογίες.....90
8.4 Απειλές και κίνδυνοι – Μέθοδοι προστασίας.....92
8.5 Εμπόδια υιοθέτησης e-Banking από τις τράπεζες .....93
8.6 Οφέλη χρήσης e-Banking για τις τράπεζες.....94

**Μέρος Β - Χρήστες** .....95
8.7 Φύλο – Ηλικία- Μόρφωση .....96
8.8 Τόπος πρόσβασης και σύνδεση στο διαδίκτυο.....97
8.9 Υπηρεσίες ηλεκτρονικής τραπεζικής & φόβοι μη χρηστών.....99
8.10 Ασφάλεια .....102
8.11 Βαθμός ικανοποίησης χρηστών.....103

**Συμπεράσματα έρευνας** .....108

**Βιβλιογραφία** .....112

**Παραρτήματα**.....119

# Λίστα Γραφημάτων

**Γράφημα 1.** Χρήση Διαδικτύου.....12

**Γράφημα 2.** Πρόσβαση στο διαδίκτυο.....13

**Γράφημα 3.** Οφέλη χρήσης Ηλεκτρονικής Τραπεζικής – Μείωση κόστους.....43

**Γράφημα 4.** Κόστος Συναλλαγών.....45

**Γράφημα 5.** Χώρες που φιλοξενούν phishing sites .....53

**Γράφημα 6.** Χρήση e-Banking στην Ελλάδα την τελευταία τριετία. .....75

**Γράφημα 7.** Δημοφιλέστερες υπηρεσίες του e- Banking. .....77

**Γράφημα 8.** Λόγοι Αποφυγής e-Banking από Έλληνες χρήστες. .....78

**Γράφημα 9.** Είδη του Banking.....86

**Γράφημα 10**. Υπηρεσίες e-Banking .....87

**Γράφημα 11.** Υπηρεσίες m-Banking . .....88

**Γράφημα 12.** Υπηρεσίες προστιθέμενης αξίας .....89

**Γράφημα 13.** Νέες τεχνολογίες και ελληνικές τράπεζες. .....91

**Γράφημα 14.** Αποτελεσματικότητα νέων τεχνολογιών. .....91

**Γράφημα 15.** Μέθοδοι προστασίας e-Banking.....93

**Γράφημα 16.** Οφέλη χρήσης e-Banking . .....95

**Γράφημα 17.** Φύλο – Ηλικία – Μόρφωση.....96

**Γράφημα 18.** Ετήσιο Εισόδημα . .....97

**Γράφημα 19.** Τόπος πρόσβασης στο Internet – Είδος σύνδεσης .....98

**Γράφημα 20.** Το Internet στην Ελλάδα . .....99

**Γράφημα 21.** Δημοφιλέστερες υπηρεσίες του e-Banking . .....100

**Γράφημα 22.** Λόγοι αποφυγής e-Banking . .....101

**Γράφημα 23.** Είδη ηλεκτρονικής τραπεζικής . .....101

**Γράφημα 24.** Κίνδυνοι του e-Banking.....102

**Γράφημα 25.** Τρόποι προστασίας στο e-Banking .....103

**Γράφημα 26.** Βαθμός ικανοποίησης από το e-Banking & τις προσφερόμενες υπηρεσίες . .....104

**Γράφημα 27.** Βαθμός ικανοποίησης από την ασφάλεια που προσφέρουν οι τράπεζες . .....105

**Γράφημα 28.** Οφέλη χρήσης e-Banking . .....106

**Γράφημα 29.** Πρόσθετες Υπηρεσίες .....107

# Πίνακες

**Πίνακας 1.** Ενέργειες που πρέπει να κάνουν οι τράπεζας για να αυξήσουν την εμπιστοσύνη του καταναλωτή στο e-banking. .....56

**Πίνακας 2.** Χρήστες και συναλλαγές μέσω Διαδικτύου .....75

**Πίνακας 3.** Προσφερόμενες υπηρεσίες των τραπεζών που δραστηριοποιούνται στην Ελλάδα. .....82

# Εισαγωγή

Η ανάπτυξη του e-Banking στη χώρα μας υπήρξε αλματώδης, παρά το γεγονός ότι η χρονική παρουσία του στην Ελλάδα είναι αρκετά μικρότερη σε σχέση με άλλες χώρες του εξωτερικού. Οι υπηρεσίες του είναι παρόμοιες με αυτές του εξωτερικού ,ασφαλείς και αξιόπιστες. Ήδη όλο και περισσότεροι πελάτες τραπεζών εμπιστεύονται τις ηλεκτρονικές υπηρεσίες, απολαμβάνοντας πλήθος ευκολιών και εξοικονομώντας πολύτιμο χρόνο.

Το e-banking αποτελεί ηλεκτρονικό εναλλακτικό δίκτυο πληρωμών και παροχής πληροφοριών. Οι τραπεζικοί οργανισμοί του εξωτερικού, διέκριναν νωρίς την ανάγκη δημιουργίας εναλλακτικών μέσων. Προσπάθησαν λοιπόν να εκμεταλλευτούν τη διαδεδομένη χρήση του internet ώστε να προσφέρουν αρκετές τραπεζικές συναλλαγές μέσω αυτού, δίνοντας μεγάλο βάρος στα θέματα ασφάλειας των συναλλαγών.

Τις τράπεζες του εξωτερικού, ακολούθησαν και οι εγχώριοι τραπεζικοί οργανισμοί, οι οποίοι επένδυσαν αρκετά σε τεχνογνωσία και τεχνολογία προκειμένου οι ηλεκτρονικές τους υπηρεσίες να είναι ασφαλείς και ανταγωνιστικές. Έτσι, φτάσαμε σήμερα, οι περισσότερες τράπεζες που δραστηριοποιούνται στον ελλαδικό χώρο να δίνουν στους πελάτες τους τη δυνατότητα να διαχειρίζονται τις όποιες συναλλαγές τους μέσω διαδικτύου, χωρίς να χρειάζεται να σπαταλούν χρόνο και χρήμα στα καταστήματα τους.

# Κεφάλαιο 1.

## Εισαγωγικές έννοιες του e-Banking

### 1.1 Το Internet στην Ελλάδα

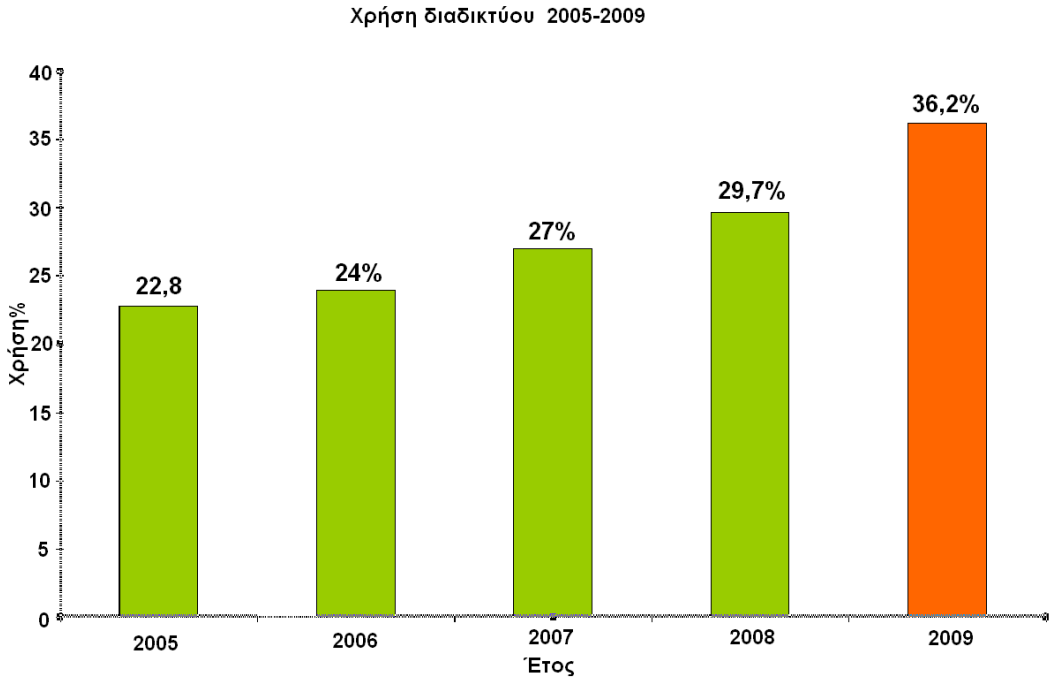
Πριν από μερικές δεκαετίες, οι υπολογιστές χρησιμοποιούνταν μόνο από ειδικούς ή από επαγγελματίες που δραστηριοποιούνταν σε πολύ συγκεκριμένους κλάδους. Η δυσκολία χρήσης τους και το υψηλό κόστος απόκτησής τους ήταν απαγορευτικό για το ευρύ κοινό. Οι ραγδαίες εξελίξεις όμως στις Τεχνολογίες της Πληροφορικής και των Επικοινωνιών, και ειδικότερα η εξάπλωση του Internet, έχουν κάνει τους υπολογιστές προσιτούς, και, στις περισσότερες περιπτώσεις, απαραίτητους σε όλους.

Έτσι, οι υπολογιστές και το Internet χρησιμοποιούνται σήμερα από ανθρώπους διαφορετικών ηλικιών και επαγγελμάτων, τόσο για επαγγελματικούς, όσο και γα προσωπικούς λόγους.

Σύμφωνα με έρευνα της εταιρίας Metron analysis για το internet στην Ελλάδα (*γράφημα 1.*), το 2009 η διείσδυση του Internet στην Ελλάδα κυμαίνεται ακόμα σε σχετικά χαμηλά επίπεδα (36,2%) στις ηλικίες 18 και άνω, σε σύγκριση με τα αντίστοιχα ποσοστά των χωρών της Β. Ευρώπης και των Ηνωμένων Πολιτειών της Αμερικής, τα οποία σε αρκετές περιπτώσεις ξεπερνούν ακόμα και το 50%.

Το στοιχείο αυτό, αποτελεί ένδειξη του μεγάλου περιθωρίου αύξησης της διείσδυσης του διαδικτύου αλλά και γενικότερα των ηλεκτρονικών αγαθών στη χώρα μας.

**Γράφημα 1. Χρήση Διαδικτύου**




**Πηγή: Metron analysis *(2009)***

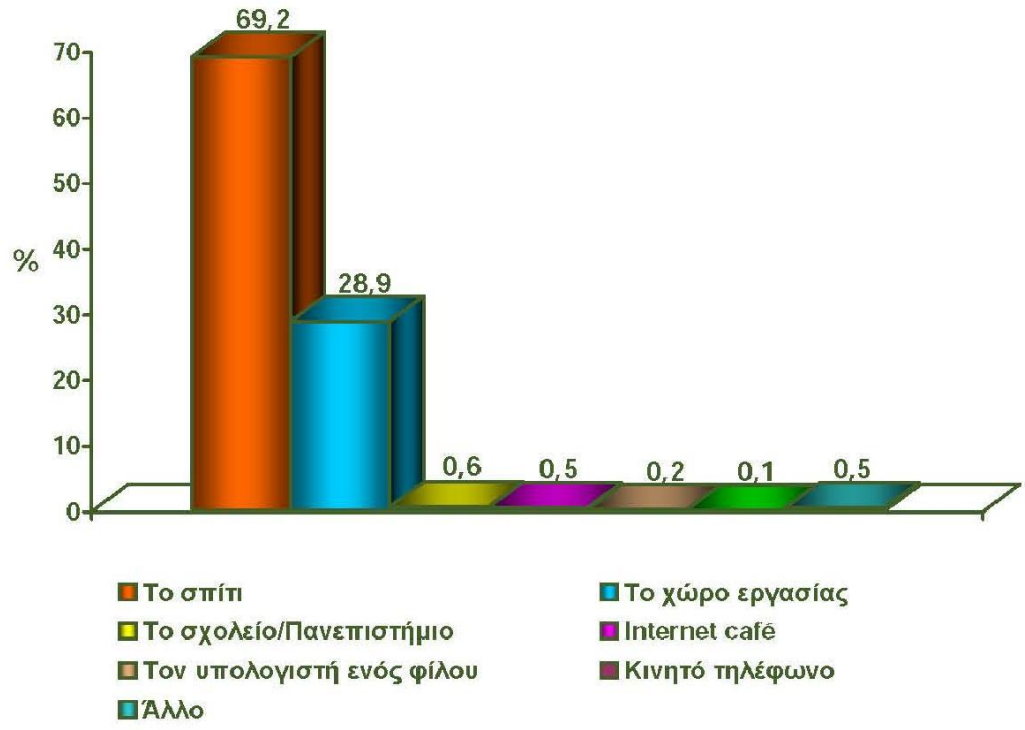
Τα πιο υψηλά ποσοστά χρήσης Η/Υ και πρόσβασης στο Διαδίκτυο σημειώνονται αντίστοιχα για το 2009 σύμφωνα με έρευνα που διεξήγαγε το παρατηρητήριο για την κοινωνία της πληροφορίας (2009) και αφορούσε στην ταυτότητα των χρηστών του Internet στην Ελλάδα, για τα άτομα ηλικίας 25-34 ετών . Η χρήση του Η/Υ και του Διαδικτύου φαίνεται να είναι αντιστρόφως ανάλογη ως προς την ηλικία των χρηστών καθώς τα ποσοστά χρήσης μειώνονται όσο αυξάνεται η ηλικία των χρηστών και ειδικά για τα άτομα ηλικίας 65-74 καταγράφονται πολύ χαμηλά ποσοστά (4,7% χρήση Η/Υ και 2,5% πρόσβαση στο Διαδίκτυο).

Επίσης, σύμφωνα με την ίδια έρευνα, πολύ υψηλά ποσοστά χρήσης Η/Υ σημειώνονται σε άτομα ανώτερης και ανώτατης εκπαίδευσης, χαμηλά ποσοστά σε απόφοιτους δημοτικού και γυμνασίου ενώ περίπου 1 στους 2 αποφοίτους λυκείου χρησιμοποιεί τον Η/Υ. Ακόμα σημαντική αύξηση παρατηρείται για τους αποφοίτους λυκείου (κατά περίπου 4,5%), ενώ σημαντική πτώση σημειώνεται για τους αποφοίτους Γυμνασίου (4% περίπου). Ενδιαφέρον παρουσιάζει το γεγονός ότι ως προς τη χρήση του Διαδικτύου σημαντική αύξηση σημειώνεται και για τους

αποφοίτους Ανωτέρων και Ανωτάτων σχολών της τάξεως των 7 με 8 περίπου ποσοστιαίων μονάδων.

Από τους Έλληνες χρήστες του Internet, το μεγαλύτερο ποσοστό ανήκει στους άνδρες. Περίπου δύο στους τρεις συνδέονται καθημερινά στο διαδίκτυο, κυρίως από το σπίτι ή από την εργασία του (*γράφημα 2*).

**Γράφημα 2. Πρόσβαση στο διαδίκτυο**




**Πηγή:** ***έρευνα e-metrics, AGB Nielsen Media Research (2008)***

Γενικά θα μπορούσαμε να πούμε ότι το Internet στην Ελλάδα αποτελεί ένα χώρο υπό διαμόρφωση και ανάπτυξη. Αν κρίνει κανείς από τα γενικά χαρακτηριστικά του προφίλ των χρηστών, θα μπορούσαμε ακόμα να πούμε ότι το Internet στην Ελλάδα είναι υπόθεση των λίγων και δεν έχει αρχίσει να διαδίδεται στα ευρύτερα στρώματα του πληθυσμού ( *Παράρτημα 1*).

## 1.2 E- Banking

Η ηλεκτρονική τραπεζική είναι ένα σχετικά νέο εναλλακτικό τραπεζικό μέσο. Στην Ελλάδα πρωτοεμφανίστηκε το 1997 από την ΕΓΝΑΤΙΑ τράπεζα και στη συνέχεια το παράδειγμά της ακολούθησαν και οι υπόλοιπες εγχώριες τράπεζες.

Με τον όρο e-banking ή ηλεκτρονική τραπεζική εννοούμε όλες εκείνες τις υπηρεσίες που παρέχουν οι τράπεζες μέσω του Διαδικτύου, χωρίς δηλαδή τη φυσική παρουσία του πελάτη στο υποκατάστημα μιας τράπεζας. Εναλλακτικά θα μπορούσαμε να ορίσουμε την ηλεκτρονική τραπεζική ως την παροχή νέων και παραδοσιακών προϊόντων και υπηρεσιών χρηματοοικονομικής φύσης, απευθείας στους πελάτες μέσω ηλεκτρονικών, αλληλεπιδραστικών καναλιών επικοινωνίας.

Σήμερα υπηρεσίες ηλεκτρονικής τραπεζικής διαθέτει η πλειοψηφία των εγχώριων τραπεζικών οργανισμών. Παρά το γεγονός ότι η ηλεκτρονική τραπεζική χρησιμοποιείται λίγα χρόνια στη χώρα μας, έχει πραγματοποιήσει μεγάλη πρόοδο.

Τα περισσότερα sites ηλεκτρονικών συναλλαγών στην Ελλάδα, μπορούν επάξια να ανταγωνιστούν sites του εξωτερικού, τόσο ως προς το πλήθος και την ποιότητα των προσφερόμενων υπηρεσιών, όσο και ως προς το φιλικό τους περιβάλλον και την ευκολία χρήσης τους.

Η ηλεκτρονική τραπεζική δεν περιορίζεται μόνο σε εφαρμογές τραπεζικής μέσω διαδικτύου (internet banking). Εφαρμογές της συναντάμε ακόμα και στους χώρους του ηλεκτρονικού εμπορίου ( e- Commerce ) και των ηλεκτρονικών επενδύσεων (e-investment). Επίσης υπηρεσίες ηλεκτρονικής τραπεζικής διεκπεραιώνονται και από άλλα κανάλια, όπως το σταθερό (Phone Banking) και το κινητό τηλέφωνο (Mobile banking).

## 1.3 Τα είδη του e- banking

Το e-banking, κατά βάση χωρίζεται σε τρία είδη, ανάλογα με τον εξοπλισμό και τα προγράμματα λογισμικού που χρησιμοποιούνται. Τα είδη αυτά είναι:

1. Internet banking (Τραπεζική μέσω διαδικτύου)
2. Phone banking (Τραπεζική μέσω τηλεφώνου)
3. Mobile banking (Τραπεζική μέσω κινητού)

Ανάλογα με το μέσο που χρησιμοποιείται για τη διενέργεια συναλλαγών, εντοπίζοντας ιδιαίτερα χαρακτηριστικά για το κάθε ένα από αυτά.

### ➢ Internet Banking

Το Internet banking, το οποίο μερικές φορές ονομάζεται και online banking, χρησιμοποιεί το Internet ως μέσο διεξαγωγής τραπεζικών δραστηριοτήτων. Για να μπορέσει ένας χρήστης να χρησιμοποιήσει τις υπηρεσίες του e- banking πρέπει να διαθέτει ηλεκτρονικό υπολογιστή και να έχει σύνδεση στο διαδίκτυο. Ωστόσο σε ορισμένες περιπτώσεις απαιτούνται περισσότερες συσκευές ασφαλείας όπως εγκατάσταση ειδικού λογισμικού ασφαλείας ή ψηφιακό πιστοποιητικό.

Ο πελάτης μίας τράπεζας, μέσω του Internet banking, έχει τη δυνατότητα να εκτελεί, σχεδόν όλες τις τραπεζικές συναλλαγές και να λαμβάνει την πληροφόρηση που επιθυμεί.

*"Οι τράπεζες έχουν πλέον την τεχνογνωσία και τις δυνατότητες να προσωποποιούν τις ηλεκτρονικές τους υπηρεσίες, ανάλογα με την κατηγορία πελατών που αντιπροσωπεύει ο χρήστης και με τον τρόπο αυτό υπάρχουν για παράδειγμα επιπρόσθετες δυνατότητες για εταιρικούς χρήστες σε σχέση με ιδιώτες "*(*Αγγέλης, 2005*). Μεγάλη βαρύτητα δίνεται και στο θέμα της ασφάλειας που είναι ιδιαίτερα κρίσιμο για την αξιοπιστία των ηλεκτρονικών τραπεζικών συστημάτων.

## ➢ Phone Banking

Μέσω του Phone Banking, η Τράπεζα, γίνεται πλέον προσιτή από το σπίτι, το γραφείο, το αυτοκίνητο, ενώ ταυτόχρονα διατηρείται ως ένα βαθμό και η παραδοσιακή τραπεζική σχέση μεταξύ υπαλλήλου και πελάτη.

Οι υπηρεσίες που προσφέρονται μέσω phone banking χωρίζονται σε δύο κατηγορίες:

• Αυτές που διεκπεραιώνονται από πράκτορες (agents) τηλεφωνικού κέντρού, και
• Αυτές που διεκπεραιώνονται αυτόματα μέσω συστημάτων αναγνώρισης φωνής (IVRs).

Στην πρώτη περίπτωση, ο πελάτης επικοινωνεί φωνητικά με τον πράκτορα της τράπεζας και μεταβιβάζει τα αιτήματά του. Οι πράκτορες, πρέπει να ταυτοποιήσουν τα στοιχεία του πελάτη, ώστε να εξασφαλίσουν την ακεραιότητα, αλλά και την εμπιστευτικότητα των συναλλαγών και αιτημάτων του.

Στη δεύτερη περίπτωση, η διαδικασία είναι αυτοματοποιημένη και ο πελάτης απαντά στα φωνητικά μηνύματα που ακούει στο τηλέφωνο του. Όπως και προηγουμένως, έτσι και τώρα, ακολουθούνται διαδικασίες πιστοποίησης και ταυτοποίησης του πελάτη που εξασφαλίζουν την ασφάλεια των συναλλαγών του.

Το phone banking, δίνει τη δυνατότητα στον πελάτης μίας τράπεζας, να έχει στη διάθεση του, σχεδόν όλες τις συναλλαγές είτε οικονομικές είτε πληροφοριακές που έχει και μέσω Internet banking.

- **Mobile Banking**

Το Mobile banking παρά τα πλεονεκτήματα, τις ευκολίες και την ευχρηστία του, δεν έχει καταφέρει ακόμη να πείσει το ελληνικό καταναλωτικό κοινό και συνεπώς δεν έχει εδραιωθεί ακόμα σε σχέση με το internet και το phone banking. Αν λάβουμε υπόψη όμως την ανάπτυξη της κινητής τηλεφωνίας στην εγχώρια αγορά, τότε το Mobile banking έχει όλες τις προοπτικές να αποτελέσει στο άμεσο μέλλον ένα ευρέως χρησιμοποιούμενο κανάλι πραγματοποίησης ηλεκτρονικών συναλλαγών.

Συσκευές που είναι εφοδιασμένες με την τεχνολογία WAP και μπορούν να συνδεθούν στο Internet μπορούν να παρέχουν στους χρήστες τους τη δυνατότητα διεξαγωγής τραπεζικών συναλλαγών.

Μεγάλη σημασία δίνεται επίσης σε ότι αφορά το Mobile banking, στην ασφάλεια των συναλλαγών και στην πιστοποίηση του χρήστη.

Ο χρήστης, με το Mobile banking έχει τη δυνατότητα να παρακολουθεί το χαρτοφυλάκιο του και τα υπόλοιπά των λογαριασμών του, να μεταφέρει χρήματα, να πληρώνει λογαριασμούς και κάρτες, να αιτείται τραπεζικά προϊόντα και υπηρεσίες (*Παρατηρητήριο για την κοινωνία της πληροφορίας, 2009*).

# Κεφάλαιο 2.

## Υπηρεσίες – Δυνατότητες του e- Banking

### 2.1 Internet Banking

Το Internet banking αποτελεί τη βάση του e- banking, όσον αφορά την ποικιλία των υπηρεσιών που προσφέρει. Οι υπηρεσίες αυτές χωρίζονται σε τέσσερις μεγάλες διακριτές κατηγορίες.

- Οικονομικές συναλλαγές
- Πληροφοριακές συναλλαγές
- Αιτήσεις
- Άλλες υπηρεσίες

Αναλυτικά παρουσιάζονται οι υπηρεσίες αυτές στις ακόλουθες παραγράφους, σύμφωνα με τα όσα αναφέρει ο Βασίλης Αγγέλης στο βιβλίο του "*Η βίβλος του e- Banking*", *(2005).*

- **Οικονομικές συναλλαγές**

Οι οικονομικές συναλλαγές καλύπτουν όλες τις συναλλαγές που μπορεί να κάνει ο συναλλασσόμενος και στο κατάστημα της τράπεζας. Οι συναλλαγές αυτές αφορούν ενδοτραπεζικές συναλλαγές, όπως μεταφορές κεφαλαίων, πληρωμή καρτών και δανείων, συναλλαγές που υλοποιούνται ύστερα από διμερείς συμφωνίες της τράπεζας με τρίτο οργανισμό, όπως πληρωμές λογαριασμών εταιριών σταθερής και κινητής τηλεφωνίας και συναλλαγές που υλοποιούνται στα πλαίσια διατραπεζικών συστημάτων, κυρίως της ΔΙΑΣ Α.Ε, αλλά και άλλων όπως το σύστημα «ΕΡΜΗΣ».

- **Μεταφορές εντός τράπεζας**

Οι μεταφορές κεφαλαίων εντός τράπεζας, διακρίνονται σε :

• **Μεταφορές σε λογαριασμό ιδίου**, όπου ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και τον τραπεζικό λογαριασμό πίστωσης, πληκτρολογεί το ποσό που θέλει να μεταφέρει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή και έχει τη δυνατότητα να εκτυπώσει την εντολή μεταφοράς, η οποία είναι αντίστοιχη με το παραστατικό της συναλλαγής.

• **Μεταφορές σε λογαριασμό τρίτου**, όπου και σε αυτή την περίπτωση ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και στη συνέχεια πληκτρολογεί τον αριθμό του λογαριασμού πίστωσης του δικαιούχου. Ο χρήστης πρέπει να είναι ιδιαίτερα προσεκτικός στο σημείο αυτό, ώστε τα λεφτά να πιστωθούν στο σωστό λογαριασμό. Έπειτα πληκτρολογεί το ποσό που θέλει να μεταφέρει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή.

- **Εμβάσματα Εσωτερικού – Εξωτερικού**

Για την αποστολή εμβάσματος, ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης, στη συνέχεια επιλέγει την τράπεζα του δικαιούχου , από ένα σύνθετο πεδίο που περιέχει όλες τις τράπεζες του εσωτερικού ή του εξωτερικού. Έπειτα πληκτρολογεί τον αριθμό του λογαριασμού δικαιούχου και καταχωρεί την επωνυμία του δικαιούχου.

- **Πληρωμές δανείων**

Η πληρωμή δανείου είναι συναλλαγή μεταφοράς εντός τράπεζας και όπως στις παραπάνω περιπτώσεις μεταφοράς εντός τράπεζας εκτελείται άμεσα.

Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και το λογαριασμό δανείου και στη συνέχεια πληκτρολογεί το ποσό που θέλει να μεταφέρει για την

πληρωμή της δόσης του δανείου και την ημερομηνία που επιθυμεί να γίνει η πληρωμή.

- **Πληρωμές πιστωτικών καρτών**

  Οι πληρωμές πιστωτικών καρτών διακρίνονται σε τρεις κατηγορίες:

- **Πληρωμή πιστωτικών καρτών ιδίου:** Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και τον αριθμό της πιστωτικής κάρτας που επιθυμεί να πληρώσει. Ακολούθως πληκτρολογεί το ποσό που θέλει να μεταφέρει για την πληρωμή της πιστωτικής κάρτας και την ημερομηνία που επιθυμεί να γίνει η πληρωμή. Ο χρήστης έχει την δυνατότητα πραγματοποίησης μεταχρονολογημένων πληρωμών, γεγονός που τον διευκολύνει να προγραμματίζει τις πληρωμές του.

- **Πληρωμή πιστωτικών καρτών τρίτου:** Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης**,** στη συνέχεια πληκτρολογεί τον αριθμό της πιστωτικής κάρτας. Ο χρήστης πρέπει να είναι ιδιαίτερα προσεκτικός στο σημείο αυτό, ώστε τα λεφτά να πιστωθούν στη σωστή πιστωτική κάρτα. Ακολούθως πληκτρολογεί το ποσό που θέλει να μεταφέρει για την πληρωμή της πιστωτικής κάρτας και την ημερομηνία που επιθυμεί να γίνει η πληρωμή.

- **Πληρωμή πιστωτικών καρτών άλλης τράπεζας:** Οι πληρωμές πιστωτικών καρτών άλλης τράπεζας πραγματοποιούνται μέσω του διατραπεζικού συστήματος Dias transfer. Για την πληρωμή πιστωτικών καρτών άλλης τράπεζας, ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης στη συνέχεια επιλέγει την τράπεζα δικαιούχου, από ένα σύνθετο πεδίο που περιέχει όλες τις τράπεζες εσωτερικού. Έπειτα ο πελάτης καλείται να πληκτρολογήσει τον αριθμό της πιστωτικής κάρτας. Ακολούθως πληκτρολογεί το ποσό που θέλει να μεταφέρει για την πληρωμή της πιστωτικής κάρτας και την ημερομηνία που επιθυμεί να γίνει η πληρωμή.

- **Πληρωμές Δημοσίου**

Πολλές πληρωμές ενός πελάτη έναντι του Δημοσίου, μπορούν να ολοκληρώνονται μέσω e-banking. Οι περισσότερες από αυτές διεκπεραιώνονται μέσω του διατραπεζικού συστήματος DIAS DEBIT. Οι πληρωμές Δημοσίου παρέχουν όλο το πακέτο των ηλεκτρονικών πληρωμών, καθιστώντας το πολύ ελκυστικό για πολλούς επαγγελματίες της χώρας μας.

Οι πληρωμές Δημοσίου, αναφέρονται σε πληρωμές :

• Φ.Π.Α.
• Εργοδοτικές εισφορές Ι.Κ.Α
• Ασφαλιστικές εισφορές Τ.Ε.Β.Ε
• Είσπραξη Φόρου Εισοδήματος Φυσικών Προσώπων
• Τέλη κυκλοφορίας

- **Πληρωμές Λογαριασμών ΔΕΚΟ**

Σχεδόν όλες οι μονάδες ηλεκτρονικής τραπεζικής της χώρας, παρέχουν στους πελάτες τους, ολοκληρωμένο πακέτο πληρωμών λογαριασμών ΔΕΚΟ. Ονομαστικά οι πληρωμές αυτές είναι:

• ΟΤΕ
• ΔΕΗ
• ΕΥΔΑΠ

- **Πληρωμές σταθερής και κινητής τηλεφωνίας**

Η πληρωμή λογαριασμών σταθερής και κινητής τηλεφωνίας παρέχεται πλέον στις περισσότερες τράπεζες. Κάποιες από αυτές τις πληρωμές πραγματοποιούνται μέσω του διατραπεζικού συστήματος DIAS DEBIT, ενώ άλλες αποτελούν προϊόν διμερούς συμφωνίας μεταξύ τραπεζών και εταιριών.

- **Πληρωμές Ασφαλιστικών**

Αρκετές ασφαλιστικές εταιρίες συνάπτουν συμφωνίες με τράπεζες, δίνοντας τη δυνατότητα στους πελάτες τους να πληρώνουν τα ασφάλιστρα τους μέσω αυτών.

- **Πληρωμές τρίτων**

Αρκετές εταιρίες δημιουργούν συμφωνίες με τράπεζες, δίνοντας τη δυνατότητα στους πελάτες τους να πληρώνουν τις υποχρεώσεις τους σε αυτές μέσω υπηρεσιών που προσφέρουν οι τράπεζες.

- **Μαζικές πληρωμές- Μισθοδοσίες**

Μία ακόμα υπηρεσία που προσφέρουν πολλές τράπεζες, είναι η εκτέλεση μισθοδοσιών ή μαζικών πληρωμών μέσω αρχείου.

Τα αρχεία αυτά μπορούν να παράγονται είτε από τις ίδιες τις εταιρίες με χρήση των μηχανογραφικών τους συστημάτων, είτε μέσω ειδικής εφαρμογής που διαθέτουν οι τράπεζες στους πελάτες τους.

- **Κατάσταση Εντολών**

Το Internet banking, πρέπει να δίνει στον πελάτη του, εύκολη ενημέρωση για την κατάσταση των εντολών οικονομικής φύσης.

Μία εντολή που καταχωρείται μέσω του Internet μπορεί να περάσει από διάφορες καταστάσεις, μέχρι να καταλήξει στην οριστική. Για το λόγο αυτό ο χρήστης του e-banking καλό είναι να ενημερώνεται και να παρακολουθεί συχνά την κατάσταση των συναλλαγών του, ώστε να γνωρίζει ανά πάσα στιγμή ποιες εντολές του δεν εκτελέσθηκαν.

Οι καταστάσεις εντολών είναι οι ακόλουθες :

- Προς επεξεργασία
- Ακυρωμένη από χρήστη
- Ακυρωμένη από Τράπεζα
- Ακυρωμένη από Οργανισμό
- Επιβεβαιωμένη από Τράπεζα
- Εκτελεσμένη
- Μερικώς εκτελεσμένη

### o Προμήθειες Συναλλαγών

Ένας χρήστης, πριν ξεκινήσει να κάνει οικονομική συναλλαγή μέσω Internet banking, πρέπει να ενημερώνεται για τις προμήθειες των συναλλαγών. Οι τράπεζες οφείλουν να έχουν σε δημόσια θέα το τιμολόγιο τους.

Λόγω μεγάλου ανταγωνισμού, είναι πιθανό, οι τράπεζες να προβαίνουν συχνά σε αναπροσαρμογές των τιμολογίων τους. Ένα βασικό πλεονέκτημα των ηλεκτρονικών συναλλαγών, είναι οι μειωμένες προμήθειες.

Σήμερα καμία τράπεζα δεν χρεώνει προμήθεια στις μεμονωμένες μεταφορές κεφαλαίων εντός τράπεζας και οι περισσότερες από αυτές, δεν χρεώνουν προμήθεια στις πληρωμές δημοσίου.

## ➢ Πληροφοριακές συναλλαγές

Πολύ σημαντικό είναι το κομμάτι των πληροφοριακών συναλλαγών που καλύπτει το Internet banking. Ο χρήστης μπορεί να πάρει πληροφορίες για όλες τις υπηρεσίες που διαθέτει η τράπεζα. Οι συναλλαγές αυτές διακρίνονται σε τέσσερις μεγάλες κατηγορίες οι οποίες αναλύονται παρακάτω.

**• Πληροφορίες λογαριασμών**

Ο χρήστης μπορεί να δει όλες τις πληροφορίες που σχετίζονται με τον τραπεζικό του λογαριασμό μέσω του διαδικτύου (Παράρτημα 2).

Ο αριθμός λογαριασμού εμφανίζεται με την διεθνή IBAN μορφή του. Ο χρήστης βλέπει την επωνυμία του δικαιούχου, το είδος του τραπεζικού λογαριασμού, το κατάστημα διαχείρισης, το επιτόκιο του και το νόμισμά του.

Ακόμα, γνωρίζει το διαθέσιμο υπόλοιπό, το λογιστικό υπόλοιπο, το τοκιζόμενο υπόλοιπο και τυχών δεσμεύσεις που υπάρχουν στο λογαριασμό του.

Επίσης, μερικές τράπεζες εμφανίζουν την τελευταία πίστωση και τελευταία χρέωση του λογαριασμού του, καθώς και τα στοιχεία των συνδικαιούχων, αν υπάρχουν τέτοιοι λογαριασμοί.

**• Πληροφορίες καρτών**

Στην περίπτωση αυτή, ο χρήστης βλέπει τον αριθμό πιστωτικής κάρτας, την επωνυμία του δικαιούχου, τον τύπο της κάρτας, το επιτόκιο της, το πιστωτικό όριο και το νόμισμά της.

Εμφανίζονται πληροφορίες για το επιτόκιο υπερημερίας, το ποσό συνδρομής, το διαθέσιμο υπόλοιπο, το οφειλόμενο υπόλοιπο, το ποσό μη εκκαθαρισμένων συναλλαγών, την ημερομηνία έκδοσης του τελευταίου παραστατικού, το ελάχιστο ποσό καταβολής, και την ημερομηνία προθεσμίας καταβολής.

Επίσης μερικές τράπεζες εμφανίζουν την τελευταία πληρωμή, μαζί με την ημερομηνία που έγινε.

**• Πληροφορίες Επιταγών**

Ο χρήστης έχει την δυνατότητα, επιλέγοντας αρχικά τραπεζικό λογαριασμό, στον οποίο συνδέεται το μπλοκ επιταγών του, να δει αναλυτικά όλες τις επιταγές του και την κατάσταση αυτών.

Οι τράπεζες δίνουν τη δυνατότητα στους χρήστες να κάνουν και ανάκληση επιταγής.

Παράλληλα, αρκετές τράπεζες επιτρέπουν και επεξεργασία επιταγών, ώστε να διευκολύνουν τους πελάτες τους στην παρακολούθηση αυτών.

• **Πληροφορίες δανείων**

Ένας χρήστης που έχει πάρει δάνειο, οποιασδήποτε μορφής από την τράπεζα, έχει τη δυνατότητα να ενημερώνεται για αυτό μέσω του internet.

Μπορεί ανά πάσα στιγμή να βλέπει το ποσό που του έχει απομείνει για την αποπληρωμή του, την κατάσταση των δόσεων του και τις καταναλωτικές ημερομηνίες πληρωμής τους, το επιτόκιο και άλλες χρήσιμες πληροφορίες που το αφορούν.

## ➢ Αιτήσεις

Οι τράπεζες προκειμένου να διευκολύνουν τους πελάτες τους, ενσωμάτωσαν στο internet banking, ηλεκτρονικές αιτήσεις για τα περισσότερα από τα προϊόντα τους.

Μερικές από τις ηλεκτρονικές αιτήσεις είναι :

- Αίτηση ανοίγματος λογαριασμού
- Αίτηση για δάνειο
- Αίτηση για παραγγελία συναλλάγματος
- Αίτηση παραγγελίας μπλοκ επιταγών
- Αίτηση πιστωτικής κάρτας
- Αίτηση μεταφοράς υπολοίπου (Παράρτημα 3)

## ➢ Βοηθητικές Υπηρεσίες

Πολλές τράπεζες πέραν των υπηρεσιών που προσφέρουν στους χρήστες τους, παρέχουν και βοηθητικά εργαλεία που διευκολύνουν τη ζωή των πελατών τους. Συνήθως τα εργαλεία αυτά είναι διαθέσιμα και στους απλούς επισκέπτες του site της τράπεζας.

Τέτοιες βοηθητικές υπηρεσίες είναι :

• Υπολογισμός IBAN
• Μετατροπή νομισμάτων
• Υπολογισμός δόσεων δανείων

## 2.2 Phone Banking

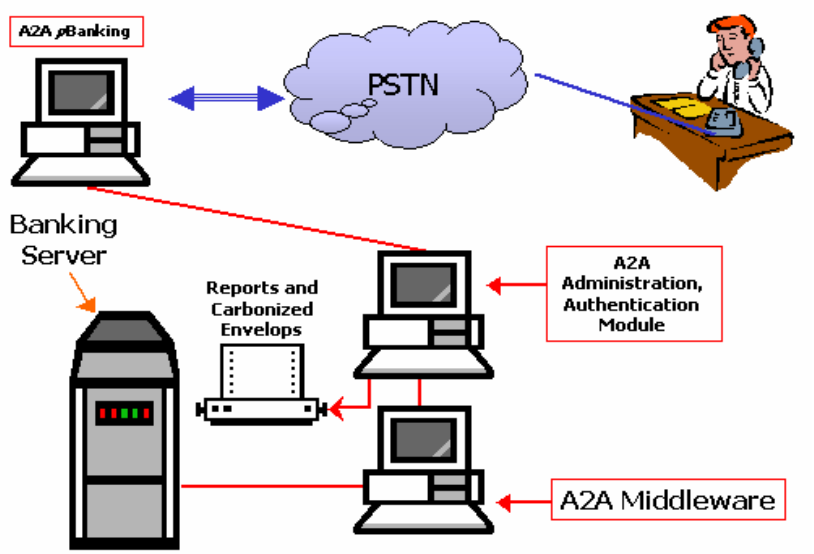
Τα τελευταία χρόνια ήταν φανερή η πρόθεση των μεγάλων ελληνικών τραπεζών να καλλιεργήσουν τις σχέσεις τους με τη νέα τεχνολογία και να προχωρήσουν σε στρατηγικές συμμαχίες με εταιρείες των κλάδων πληροφορικής και των τηλεπικοινωνιών, καθώς και με εταιρείες παροχής πρόσβασης στο διαδίκτυο.

Το πρώτο βήμα έγινε στον τομέα της τηλεφωνικής τραπεζικής εξυπηρέτησης, (*Κάπα research, Ιούνιος 2006*), «*Η σχέση των ΜΜΕ με το τραπεζικό σύστημα»*.

Το Phone Banking αποτελεί ένα εναλλακτικό κανάλι του e- banking, που επιτρέπει στους πελάτες της τράπεζας να πραγματοποιούν τραπεζικές συναλλαγές χρησιμοποιώντας οποιοδήποτε τηλέφωνο 24 ώρες το 24ωρο (*φωτογραφία σελ.27*).
Οι χρήστες διαθέτουν τη δυνατότητα εξυπηρέτησης μέσω :

• Του συστήματος προ- μαγνητοφωνημένων μηνυμάτων (IVR), όπου πιστοποιείται ο χρήστης χωρίς την παρέμβαση ανθρώπινου παράγοντα, πληκτρολογώντας τους κωδικούς του στη συσκευή του τηλεφώνου.

• Τους εξειδικευμένους αντιπροσώπους του τηλεφωνικού κέντρου. Οι υπάλληλοι της Τράπεζας (αντιπρόσωποι) που βρίσκονται στην άλλη άκρη της τηλεφωνικής γραμμής, με την βοήθεια σύγχρονων συστημάτων (CTI, CRM ) μπορούν να παρέχουν συνεχή τηλεφωνική υποστήριξη και ενημέρωση των πελατών για ένα συνεχώς διευρυνόμενο πλήθος τραπεζικών προϊόντων και υπηρεσιών.

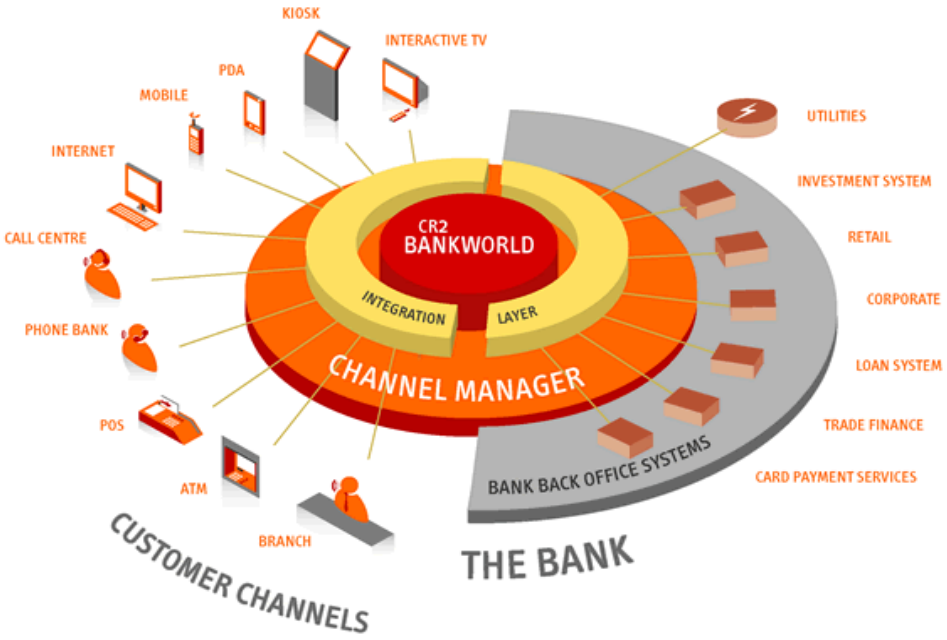



**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.access2arabia.com***

Πολλές είναι οι τράπεζες που είτε με δικούς τους πόρους είτε μέσω εξωτερικών πόρων, παρέχουν στους πελάτες τους τη δυνατότητα συναλλαγών , μέσω μιας οποιασδήποτε τηλεφωνικής συσκευής.

Οι διαθέσιμες συναλλαγές του phone banking είναι οι παρακάτω :

- Ενεργοποίησης και ακύρωσης κάρτας ανάληψης χρημάτων
- Ακυρώσεις πιστωτικών καρτών
- Αλλαγή στοιχείων αλληλογραφίας καρτούχων
- Εξυπηρέτηση καρτούχων για αμφισβητήσεις χρεώσεων
- Ενημέρωση για απόδοση και αποτίμηση αμοιβαίων κεφαλαίων
- Ενημέρωση για όλα τα προϊόντα που έχει ο πελάτης στην τράπεζα
- Ανάλυση υπολοίπου των λογαριασμών
- Ανάλυση υπολοίπου πιστωτικής κάρτας και ενημέρωση κινήσεων
- Κίνηση λογαριασμού
- Έκδοση και ανάκληση μπλοκ επιταγών
- Μεταφορές – Πληρωμές
- Υπηρεσίες πελάτη ( π.χ. Αλλαγή κωδικού ασφαλείας )
- Αιτήσεις




**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.cr2.com***

## 2.3 Mobile Banking

Οι υπηρεσίες Mobile Banking δεν είναι τόσο διαδεδομένες στην Ελλάδα, με συνέπεια προς το παρόν να το διαθέτουν λίγες τράπεζες. Το Mobile Banking υποστηρίζουν συσκευές νέας τεχνολογίας με ενσωματωμένο περιηγητή στο διαδίκτυο (web browser), όπως:

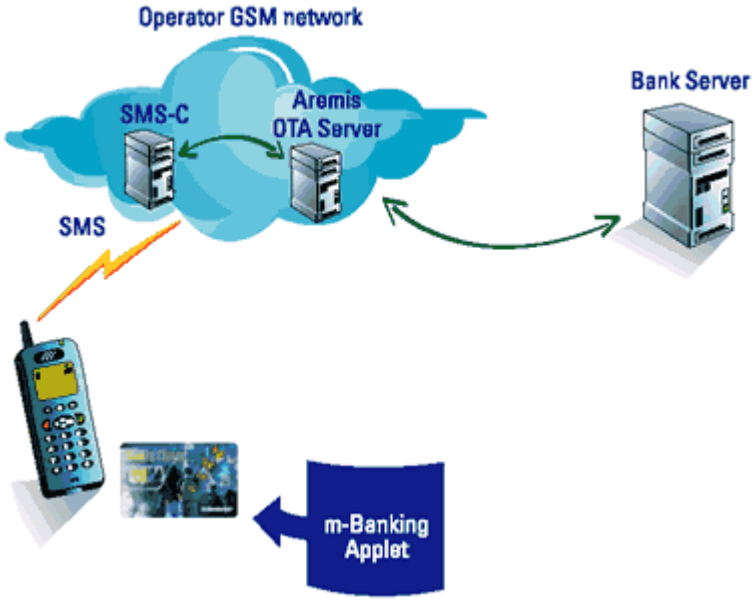
- Κινητά τηλέφωνα προηγμένης τεχνολογίας (smart phones)
- Υπολογιστές χειρός ( PDAs)

Η πρόσβαση στις υπηρεσίες είναι διαθέσιμη στους πελάτες όλων των εταιριών κινητής τηλεφωνίας και γίνεται άμεσα και γρήγορα, χωρίς επιπλέον ρυθμίσεις (*φωτογραφία σελ. 28*). Ο πελάτης μπορεί να έχει πρόσβαση στην ιστοσελίδα των ηλεκτρονικών υπηρεσιών της τράπεζας:

• Απευθείας στην ηλεκτρονική διεύθυνση της

• Μέσω του i-mode

Μοναδική προϋπόθεση για την πρόσβαση στην ιστοσελίδα των ηλεκτρονικών υπηρεσιών της τράπεζας, είναι ο χρήστης να έχει κωδικούς πρόσβασης στην υπηρεσία mobile banking και να έχει ενεργοποιήσει τη σύνδεση του στο internet.




**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.axalto.com***

Το mobile banking διαθέτει τις εξής συναλλαγές :

• Διαχείριση λογαριασμών

• Διαχείριση καρτών

• Διαχείριση δανείων

• Πληρωμές – Μεταφορές

• Προσωπικές υπηρεσίες πελάτη

• Παραγγελία για πλήρη statements

• Αγορά και πώληση μετοχών

• Ενημέρωση εντός ολίγων λεπτών για εκτέλεση εντολής

• Ενημέρωση σε πραγματικό χρόνο (real time) για την τιμή της μετοχής προς αγορά ή πώληση

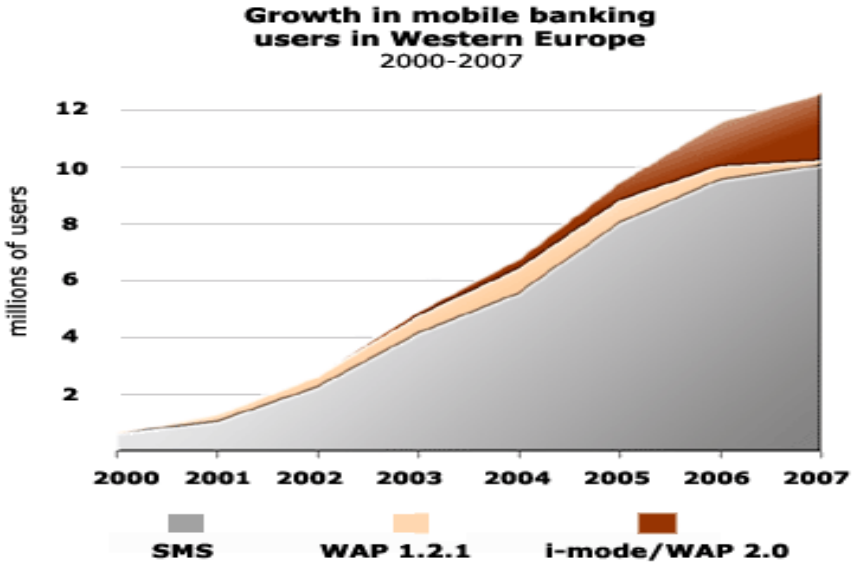
• Παρακολούθηση και αποτίμηση χαρτοφυλακίου

• Αναλυτική πληροφόρηση για παρελθούσες κινήσεις στο χαρτοφυλάκιο

• Πληροφορίες και διαφημιστικά μηνύματα για υπηρεσίες, προϊόντα και προσφορές της τράπεζας

• Αλλαγή του απόρρητου κωδικού PIN

• Προσωπικά μηνύματα




**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.usolab.com***

*" Παρά τα πλεονεκτήματα, τις ευκολίες και την ευχρηστία του, το mobile banking δεν έχει καταφέρει ακόμη να πείσει το ελληνικό καταναλωτικό κοινό. Αυτό οφείλεται ενδεχομένως στη χρήση του κινητού ως κατεξοχήν μέσου επικοινωνίας, συνεπώς η αποδοχή της αξιοπιστίας του ως μέσου διεξαγωγής χρηματοοικονομικών συναλλαγών δεν είναι εύκολη".*

Οι Έλληνες χρήστες και οι επιχειρήσεις δείχνουν να εμπιστεύονται περισσότερο το Internet, γεγονός που εξηγεί τα μεγαλύτερα ποσοστά διείσδυσης του e-banking έναντι του mobile banking.

Ωστόσο, με αργούς αλλά σταθερούς ρυθμούς τα πράγματα αλλάζουν. Οι επιχειρήσεις, και ειδικότερα οι μικρομεσαίες, αλλά και οι ιδιώτες έχουν αρχίσει να αντιλαμβάνονται ότι οι υπηρεσίες mobile banking αποφέρουν κέρδος σε πολύτιμο χρόνο και, κατά συνέπεια, χρήμα *(Ίδρυμα Οικονομικών και Βιομηχανικών Ερευνών, Σεπτέμβριος 2007).*

# Κεφάλαιο 3.

## Πρόσθετες υπηρεσίες

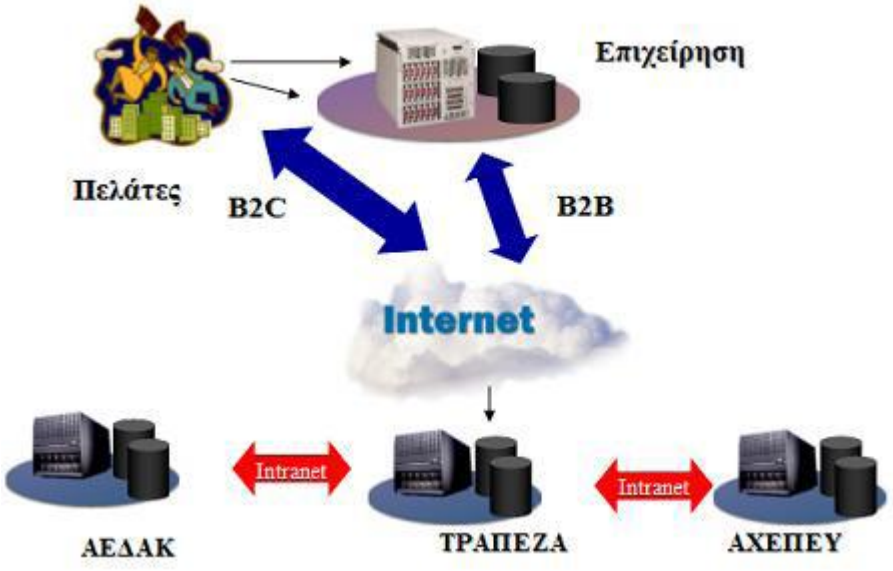
Πέραν των υπηρεσιών που αναφέρθηκαν στο προηγούμενο κεφάλαιο, το e-banking δεν περιορίζεται μόνο σε αυτές. Υπάρχει πλήθος προϊόντων που συμπληρώνουν το internet banking και καλύπτουν τις ανάγκες ακόμα και του πιο απαιτητικού χρήστη.

### 3.1 E- Investment

Το e- Investment (e- επενδύσεις) περιλαμβάνει κυρίως χρηματιστηριακές συναλλαγές, καθώς και συναλλαγές αμοιβαίων κεφαλαίων και αμοιβαίων λογαριασμών *(φωτογραφία σελ. 32)*.

Βασική προϋπόθεση για την εκτέλεση χρηματιστηριακών συναλλαγών μέσω e-banking είναι ο πελάτης της τράπεζας να είναι και πελάτης της χρηματιστηριακής εταιρίας (ΑΧΕΠΕΥ) με την οποία συνεργάζεται η τράπεζα, ενώ για την εξαγορά και διάθεση Α/Κ και Α/Λ να είναι πελάτης της ΑΕΔΑΚ με την οποία συνεργάζεται η τράπεζα *(Αγγέλης, 2005)*.

**Σχηματική Αναπαράσταση e-Investment**




**Πηγή φωτογραφίας: *E-banking – Ηλεκτρονική τραπεζική, Β. Αγγελή, (2005).***

## 3.2 E- Commerce (e- Payments)

Οι ηλεκτρονικές εισπράξεις αποτελούν σημαντικό μέρος της δραστηριότητας των μονάδων e- banking. Αρκετές τράπεζες ασχολούνται με το κομμάτι των e- payments. Οι τράπεζες αυτές συνεργάζονται με κάθε μορφής επιχείρηση και παρέχουν λύση για την ασφαλή και αξιόπιστη διεκπεραίωση των ηλεκτρονικών πληρωμών από τους πελάτες της επιχείρησης, σε συνδυασμό και με συμβουλευτικές υπηρεσίες. Οι λύσεις αυτές περιλαμβάνουν :

- Εισπράξεις από Internet sites
- Εισπράξεις από τηλεφωνικές πληρωμές πελατών
- Εισπράξεις από αρχεία με μαζικές εντολές πελατών

Μέσω των ασφαλών πλατφόρμων διεκπεραίωσης ηλεκτρονικών πληρωμών των τραπεζών, ολοκληρώνονται ηλεκτρονικές συναλλαγές για αγορές προϊόντων και υπηρεσιών με χρέωση οποιασδήποτε πιστωτικής κάρτας, καθώς και με χρέωση τραπεζικού λογαριασμού της εκάστοτε τράπεζας που προσφέρει την λύση *(Μπάσιος, 2007)*.

Οι πλατφόρμες ηλεκτρονικών εισπράξεων αποτελούν σήμερα μια από τις καλύτερες λύσεις για τις ανάγκες των επιχειρήσεων για την ηλεκτρονική εκκαθάριση των εισπράξεών τους. Τα κύρια χαρακτηριστικά των πλατφόρμων είναι :

- Υψηλή διαθεσιμότητα και αξιοπιστία
- Backup και recovery διαδικασίες
- Κρυπτογραφημένη επικοινωνία
- Trusted Third Party πιστοποίηση
- Συμβατότητα με κάθε τεχνολογική και λειτουργική πλατφόρμα υλοποίησης του ηλεκτρονικού καταστήματος
- Αυξημένη ασφάλεια με τη χρήση του κωδικού πιστοποίησης κάρτας (CVV2)
- Εγγύηση ασφάλειας των συναλλαγών σε συνεργασία με τους διεθνείς οργανισμούς VISA INTERNATIONAL και MASTERCARD EUROPAY.

Οι πλατφόρμες ηλεκτρονικών πληρωμών και οι υπηρεσίες που προσφέρουν παρέχουν μια σειρά από πρωτοποριακές δυνατότητες, όπως :

• Συναλλαγές με όλες τις πιστωτικές κάρτες Visa και MasterCard
• Ευχάριστο και φιλικό περιβάλλον για τον χρήστη
• Δυνατότητα χρέωσης με άτοκες δόσεις
• On-line, real-time απάντηση για την έγκριση ή απόρριψη της συναλλαγής
• On-line, real-time ενημέρωση της επιχείρησης για κάθε συναλλαγή στο ηλεκτρονικό του κατάστημα
• Πλήρη & ευέλικτη διαχείριση όλων των συναλλαγών μέσω διαχειριστικού εργαλείου που δίδεται στους συνεργάτες της τράπεζας
• Δυνατότητα αυτόματης αποστολής συναλλαγών για εκκαθάριση στο τέλος της ημέρας, χωρίς τη χειροκίνητη παρέμβαση της επιχείρησης
• Αυτόματη πίστωση του τραπεζικού λογαριασμού της επιχείρησης

Η συνεργασία της τράπεζας με το ηλεκτρονικό εμπόριο μπορεί να έχει μία από τις ακόλουθες μορφές:

### ➢ Πληρωμές σε ηλεκτρονικό κατάστημα (e-shop)

Η λύση αυτή απευθύνεται σε όλους τους εμπόρους που διαθέτουν ηλεκτρονικά καταστήματα και πουλούν προϊόντα / υπηρεσίες μέσω internet, ή ενδιαφέρονται να δραστηριοποιηθούν στο χώρο του ηλεκτρονικού εμπορίου. Η πληρωμή εκ μέρους του πελάτη του ηλεκτρονικού εμπόρου διεκπεραιώνεται αυτόματα και το ποσό κατατίθεται στο λογαριασμό του εμπόρου στην τράπεζα. Ο έμπορος – συνεργάτης της τράπεζας έχει επιλογές ανάλογα με την ετοιμότητα του e-shop του να δεχθεί ηλεκτρονικές πληρωμές.

Ανάλογα της μορφής του e-shop του ηλεκτρονικού συνεργάτη εμπόρου, οι τράπεζες διαθέτουν τις ακόλουθες λύσεις :

• Μετάβαση σε ασφαλή σελίδα της τράπεζας
• Επικοινωνία μέσω web service
• Πληρωμή μέσω τραπεζικού λογαριασμού

- **Πληρωμές μέσω εξ' αποστάσεως παραγγελίας (virtual POS)**

Η λύση αυτή απευθύνεται σε επιχειρήσεις για τα προϊόντα και τις υπηρεσίες τους εξ' αποστάσεως μέσω τηλεφώνου, fax κτλ. (φωτογραφία σελ. 35). Η πληρωμή διεκπεραιώνεται αυτόματα και το ποσό κατατίθεται στο λογαριασμό του εμπόρου της τράπεζας *(Αγγέλης, 2005)*.

**Σχηματική Αναπαράσταση e-Commerce**


**Πηγή φωτογραφίας:** ***E-banking – Ηλεκτρονική τραπεζική, Β. Αγγελή, (2005).***

- **Αρχείο μαζικών πληρωμών (Batch file)**

Η υπηρεσία αυτή σχεδιάστηκε από τις τράπεζες για να εξυπηρετήσει εμπόρους που πιθανών να εκτελούν τακτικά χρεώσεις των πελατών τους μέσω πιστωτικών καρτών. Ο έμπορος αποστέλλει στο σύστημα ηλεκτρονικών πληρωμών της τράπεζας το αρχείο μαζικών πληρωμών, το οποίο πρέπει να πληρεί τις προδιαγραφές που θέτει η τράπεζα. Οι συναλλαγές εκτελούνται άμεσα πιστώνοντας το λογαριασμό του εμπόρου της τράπεζας.

- **Άλλες υπηρεσίες του e- Commerce**

Πέραν των ηλεκτρονικών πληρωμών, αρκετές τράπεζες προσφέρουν και άλλες πιο εξειδικευμένες υπηρεσίες στον χώρο του ηλεκτρονικού εμπορίου. Στα πλαίσια αυτά, οι τράπεζες εισάγουν νέες υπηρεσίες για την διευκόλυνση τόσο του εμπόρου, όσο και του τελικού καταναλωτή στην διεξαγωγή αγορών μέσω web. Παράλληλα δίνεται έμφαση σε συγκεκριμένους τομείς του ηλεκτρονικού εμπορίου.

Παρακάτω αναφέρονται ονομαστικά οι εξειδικευμένες αυτές υπηρεσίες.

• Πληρωμή υπηρεσιών
• Προπληρωμένες κάρτες (Prepaid cards) αγορών στο Internet
• Ticketing

## 3.3 Alerts

Τα τελευταία χρόνια, εξαιτίας της ανάπτυξης των τεχνολογικών μέσων, συμπεριλαμβανομένων και των μέσων επικοινωνίας, προέκυψε η ανάγκη τόσο από την πλευρά των πελατών, όσο και από την πλευρά των τραπεζών για άμεση και έγκυρη ενημέρωση.

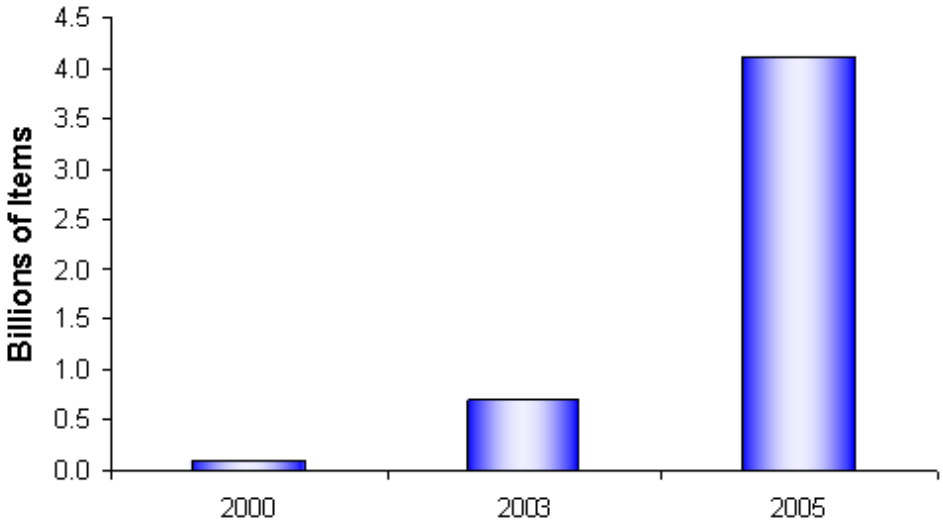
Οι μεν πελάτες, επιθυμούν να ενημερώνονται σε πραγματικό χρόνο για τις μεταβολές στο τραπεζικό τους χαρτοφυλάκιο, για την τύχη των συναλλαγών τους, για την επάρκεια του υπολοίπου των λογαριασμών τους για πληρωμή υποχρεώσεων τους και για πολλούς άλλους λόγους.

Οι δε τράπεζες θέλουν να προσφέρουν υπηρεσίες υψηλής ποιότητας στους πελάτες τους, και να προσθέσουν αξία σε όλη τη γκάμα των προϊόντων τους. Άρα η παροχή έγκυρης και έγκαιρης ενημέρωσης με χρήση των τελευταίων μέσων της τεχνολογίας όπως το e-mail και το sms αποτελεί προτεραιότητα.

*" Η ενημέρωση μέσω τηλεειδήσεων, λόγω της φύσης τους και των μέσων που χρησιμοποιούνται, υλοποιείται κυρίως από τις μονάδες ηλεκτρονικής τραπεζικής. Ωστόσο η συγκεκριμένη υπηρεσία, απευθύνεται σε όλο το πελατολόγιο μιας τράπεζας και όχι αποκλειστικά στους χρήστες του e-banking", (Ορφανίδου, 2006).*

## 3.4 P2P Πληρωμές

Οι P2P πληρωμές είναι ηλεκτρονικές μεταφορές κεφαλαίων μεταξύ ιδιωτών. Με χρήση ηλεκτρονικών υπολογιστών και κινητών τηλεφώνων, οι ιδιώτες μπορούν να χρησιμοποιούν P2P υπηρεσίες, οποιαδήποτε στιγμή, στέλνοντας χρήματα σε άλλα μέλη της οικογένειάς τους, τακτοποιώντας οφειλές σε φίλους τους, αγοράζοντας προϊόντα από on-line δημοπρασίες.




**Πηγή φωτογραφίας:** ***Έλενα Ορφανίδου, Νοέμβριος 2006***

## 3.5 Πώληση ασφαλιστικών προϊόντων

Ένας τομέας που πρόκειται να εμφανιστεί σύντομα στη χώρα μας, είναι η πώληση ασφαλιστικών προϊόντων μέσω e-banking. Οι τράπεζες σε συνεργασία με ασφαλιστικές εταιρίες, δίνουν τη δυνατότητα στον πελάτη τους να αγοράσει ασφαλιστικά προϊόντα.

### 3.6 Trade Finance (online εισαγωγές – εξαγωγές)

Μία πολύ ιδιαίτερη υπηρεσία είναι οι online συναλλαγές εισαγωγών – εξαγωγών. Οι τράπεζες αναγνωρίζοντας την ανάγκη που αντιμετωπίζουν οι επιχειρήσεις για μείωση του λειτουργικού κόστους και για συνεχή αύξηση της αποτελεσματικότητάς τους, προσφέρουν πλέον τη δυνατότητα σε αυτές να ολοκληρώνουν συναλλαγές εισαγωγών – εξαγωγών (π.χ. εμβάσματα) μέσω e banking υπηρεσιών.

### 3.7 Συναλλαγές πραγματικού χρόνου

Μεγάλη πρόκληση είναι η αύξηση του πλήθους των οικονομικών συναλλαγών που διενεργούνται σε πραγματικό χρόνο. Η εκτέλεση των συναλλαγών άμεσα θα προσφέρει σημαντικά πλεονεκτήματα στους πελάτες των τραπεζών και θα αποτελέσει ισχυρό κίνητρο για την υιοθέτηση της ηλεκτρονικής φύσης των συναλλαγών.

### 3.8 Electronic Bill Presentment & Payment (EBPP)

"*Ο όρος Electronic Bill Presentment and Payment (EBPP) αναφέρεται στη χρήση του Διαδικτύου προκειμένου να παρουσιαστεί ο λογαριασμός στον πελάτη και, εν συνεχεία, όπου είναι απαραίτητο, να εξοφληθεί online", (Αριστέα, e-Banking 2007).*

Δηλαδή, η ηλεκτρονική παρουσίαση και πληρωμή λογαριασμών αναφέρεται σε on line υπηρεσίες που εξυπηρετούν τον καταναλωτή να λάβει, δει και εκτελέσει την πληρωμή των λογαριασμών του. Με λίγα λόγια, ο πελάτης θα βλέπει το λογαριασμό του με τη μορφή που τον λαμβάνει σήμερα ταχυδρομικώς, θα μπορεί να τον εκτυπώσει και να προβεί άμεσα στην πληρωμή του.

Θα πρέπει να γίνει σαφές ότι, ενώ το EBPP ανήκει σε αυτό που γενικά χαρακτηρίζουμε "ηλεκτρονικό εμπόριο", εντούτοις δεν περιορίζεται μόνο στα προϊόντα και τις υπηρεσίες που παρέχονται μέσω Internet.

Χαρακτηριστικό παράδειγμα, για να κατανοήσουμε αυτή την παρατήρηση, είναι οι τηλεπικοινωνιακές υπηρεσίες που παρέχονται από τα δίκτυα σταθερής ή κινητής τηλεφωνίας. Μπορεί, λοιπόν, οι υπηρεσίες να παρέχονται από ένα μέσο και με μία συγκεκριμένη διαδικασία, ωστόσο η παρουσίαση και πληρωμή του λογαριασμού μπορεί να γίνουν διαδικτυακά. Φυσικά, το EBPP μπορεί κάλλιστα να εφαρμοστεί και στις περιπτώσεις κατά τις οποίες ολόκληρη η συναλλαγή γίνεται μέσω Internet, για παράδειγμα όταν αγοράζουμε ένα ηλεκτρονικό βιβλίο (e-book).

Το EBPP έχει υιοθετηθεί μερικώς στο εξωτερικό, ενώ σε επίπεδο σχεδιασμού και μελετών έχει απασχολήσει και τις εγχώριες τράπεζες. Ωστόσο δεν έχει προχωρήσει ακόμα σε υλοποίηση του *(φωτογραφία σελ. 39)*.


**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.celent.com .***

Υπάρχουν πλεονεκτήματα σε σχέση με την εισαγωγή του EBPP σε περιβάλλον on line τραπεζικών υπηρεσιών :

• **Προσελκύει πελάτες με υψηλή κερδοφορία (profitability)**: Οι πελάτες που ενδιαφέρονται για την ηλεκτρονική παρουσίαση και πληρωμή λογαριασμών είναι πελάτες με υψηλά εισοδήματα και εξοικειωμένοι με την τεχνολογία. Αυτοί συνήθως είναι οι πελάτες με την υψηλή κερδοφορία.

• **Συμβάλλει στην αφοσίωση του πελάτη (loyalty)**: Από τη στιγμή που ο πελάτης θα λαμβάνει τους λογαριασμούς του σε μία τράπεζα και θα τους πληρώνει μέσω αυτής, δύσκολα θα τη αποχωριστεί.

### 3.9 Σύνδεση internet banking με συστήματα logistics

Η μονάδα ηλεκτρονικής τραπεζικής αναζητά συνεργάτες εταιρίες πληροφορικής που υλοποιούν και προμηθεύουν logistics, ώστε να ενσωματώσουν σε αυτά τη λειτουργικότητα του e- banking ω επιπλέον module αυτών.

Το βασικό πλεονέκτημα για τις επιχειρήσεις που χρησιμοποιούν logistics με απευθείας σύνδεση με internet banking τράπεζες, είναι ότι δεν χρειάζεται να επισκέπτονται το site της τράπεζας για την εκτέλεση των συναλλαγών τους.

Ο χειριστής της εταιρίας έχει τη δυνατότητα μέσα από το μηχανογραφικό σύστημα της επιχείρησης να πληρώσει το ΦΠΑ της, τις εργοδοτικές εισφορές της στο ΙΚΑ, να εκτελέσει τη μισθοδοσία της και να αποστείλει μαζικές πληρωμές, να πληρώσει υποχρεώσεις προς τρίτους κ.α. , αλλά και να ενημερώνει online το μηχανογραφικό σύστημα με τις κινήσεις των λογαριασμών της εταιρίας και των πιστωτικών της καρτών.

### 3.10 Αυτόματο άνοιγμα καταθετικού λογαριασμού χωρίς φυσική παρουσία του πελάτη.

Η δυνατότητα ανοίγματος καταθετικού λογαριασμού χωρίς να απαιτείται η φυσική παρουσία του πελάτη σε κατάστημα της τράπεζας είναι πολύ σημαντική και μετριάζει την ανάγκη επίσκεψης καταστημάτων της τράπεζας στο ελάχιστο. Το έργο αυτό όμως απαιτεί εμπεριστατωμένη εξέταση των νομικών του διαστάσεων.

Το αυτόματο άνοιγμα καταθετικού λογαριασμού χωρίζεται σε τρεις διακριτές κατηγορίες, ανάλογα με τον τύπο του πελάτη :

• Υφιστάμενος πελάτης τράπεζας και χρήστης του internet banking.
• Υφιστάμενος πελάτης τράπεζας, μη χρήστης του internet banking.
• Νέος πελάτης

Οι δύο πρώτες περιπτώσεις είναι αυτές που μπορούν να υλοποιηθούν ευκολότερα, έχουν όμως το μειονέκτημα ότι απευθύνονται σε υφιστάμενους

πελάτες και δεν συμβάλλουν στη διεύρυνση της πελατειακής βάσης. Ωστόσο και η παροχή αυτής της δυνατότητας σε χρήστες του e-banking είναι σημαντική.

Η τρίτη περίπτωση αποτελεί τη μεγαλύτερη πρόκληση, αλλά εμπεριέχει το μεγαλύτερο ρίσκο και την προσεκτική μελέτη και σχεδιασμό της. Όλες οι περιπτώσεις είναι πιο σύνθετες όταν αφορούν Νομικά Πρόσωπα.

## 3.11 Ολοκληρωμένα Portals

Οι τράπεζες πρέπει να ξεκινήσουν να προσανατολίζονται στη δημιουργία ολοκληρωμένων internet banking portals. Τα portals αυτά πρέπει να προσφέρουν στο χρήστη και επιπλέον πληροφορίες και λειτουργίες, πέραν του περιβάλλοντος συναλλαγών που προσφέρουν σήμερα.

Τα portals θα περιλαμβάνουν :

- Περιβάλλον ηλεκτρονικών συναλλαγών
- Εκπαιδευτικό υλικό για το e-banking
- Εκπαιδευτικό υλικό για τραπεζικά θέματα
- Νέα – ειδήσεις από το χώρο του e-banking
- Νέα – ειδήσεις από τον τραπεζικό χώρο
- Forums χρηστών
- On line χρηστών
- Ψυχαγωγία
- Διαγωνισμούς
- Χρήσιμα εργαλεία
- Επενδυτικούς οδηγούς
- Ημερολόγιο κ.α.

Το internet banking πρέπει να γίνει ο συχνότερος τόπος επίσκεψης του πελάτη στον παγκόσμιο ιστό. Ο πελάτης πρέπει να νιώθει ικανοποιημένος και να μη θεωρεί την επίσκεψή του σε αυτό ως υποχρέωση απλά για τη διενέργεια πληρωμών και άποψη λογαριασμών και καρτών *(Σηφακάκη, Πάστρα, Σκαρμούτσος, Σδόγκου, 2005).*

# Κεφάλαιο 4.

## Πλεονεκτήματα και μειονεκτήματα χρήσης e-Banking για Τράπεζες και Χρήστες

Είναι πολύ σημαντικό, ο πελάτης αλλά και η τράπεζα, να γνωρίζουν τα πλεονεκτήματα και τα μειονεκτήματα που αποφέρει σε αυτούς η χρήση του e-banking. Παρακάτω, αναφέρονται συνοπτικά τα πλεονεκτήματα και τα μειονεκτήματα αυτά, σύμφωνα με όσα αναφέρει ο Βασίλης Γ. Αγγέλης, στο βιβλίο του "Η βίβλος του e-banking".

### 4.1 Για τον πελάτη

**Πλεονεκτήματα**

• **Εξυπηρέτηση 24/7 :** Οι υπηρεσίες του e-banking είναι διαθέσιμες και προσφέρονται 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα. Συνεπώς ο πελάτης μπορεί να εξυπηρετηθεί οποιαδήποτε στιγμή αυτός επιθυμεί.

• **Εξοικονόμηση χρόνου :** Ο χρήστης του e-banking κερδίζει χρόνο, αφού δεν είναι απαραίτητο να μεταβεί σε κάποιο από τα καταστήματα της τράπεζας προκειμένου να εκτελέσει τη συναλλαγή που θέλει.

• **On line παρακολούθηση τραπεζικών προϊόντων:** Ο χρήστης ενημερώνεται εύκολα και γρήγορα για τα υπόλοιπά του, τις κινήσεις του, τις εντολές του, κ.α., on line.

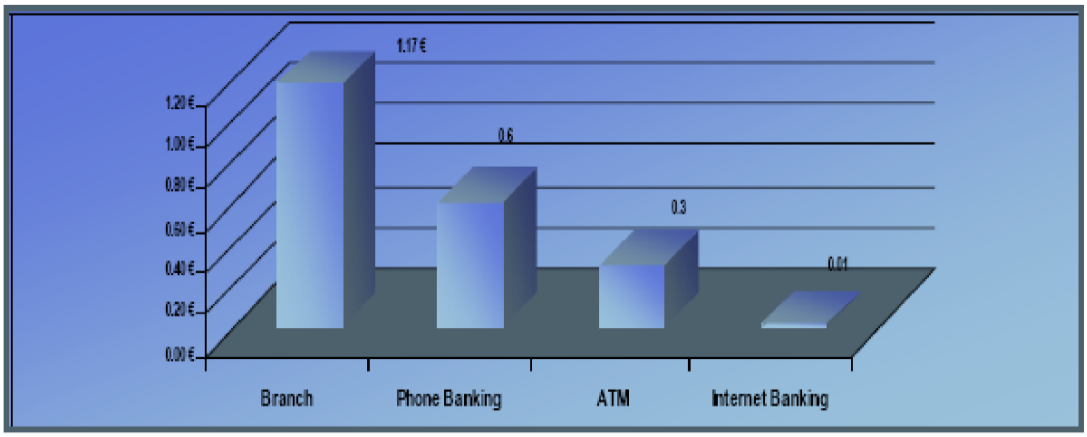
• **On line μεταφορές κεφαλαίων:** Με συνοπτικές διαδικασίες ο χρήστης μπορεί να μεταφέρει κεφάλαια εντός της τράπεζάς του, όσο και σε άλλες τράπεζες, ελέγχοντας πλήρως τις οφειλές και τις υποχρεώσεις του.

• **Μείωση χρήσης χαρτιού :** Τα statement των λογαριασμών, οι κινήσεις τους, οι κινήσεις καρτών, οι δόσεις δανείων, η κατάσταση των επιταγών

είναι διαθέσιμα μέσω internet banking. Όποτε επιθυμεί ο χρήστης μπορεί να εκτυπώσει μόνο την πληροφορία που θέλει.

• **Εύκολη πρόσβαση από οποιοδήποτε σημείο του κόσμου :** Από τη στιγμή που ο πελάτης μιας τράπεζας διαθέτει πρόσβαση στο internet, μπορεί ανά πάσα στιγμή και από οποιοδήποτε σημείο του κόσμου να έχει άμεση πρόσβαση στο τραπεζικό του χαρτοφυλάκιο και να εκτελεί τις συναλλαγές.

**Γράφημα 3. Οφέλη χρήσης Ηλεκτρονικής Τραπεζικής – Μείωση κόστους**




**Πηγή φωτογραφίας:** ***E-banking – Ηλεκτρονική τραπεζική, Β. Αγγέλη (2005).***

**Μειονεκτήματα**

• **Χρονοβόρα εγγραφή πελατών:** Για να γραφτεί κάποιος στο online πρόγραμμα της τράπεζάς του, θα πρέπει να δώσει στοιχεία ταυτότητας και να υπογράψει ένα έντυπο στο τραπεζικό κατάστημα ή αν πρόκειται για μια αποκλειστικά ηλεκτρονική τράπεζα, τα έντυπα θα του αποσταλούν ταχυδρομικώς έτσι ώστε να συμπληρωθούν και να σταλούν ξανά στην τράπεζα.

• **Δυσκολία στο χειρισμό:** Οι τραπεζικοί δικτυακοί τόποι ίσως φανούν δύσχρηστοι σε κάποιον που δεν ξέρει να χειρίζεται καλά το Internet. Το

άνοιγμα ενός online λογαριασμού ή η online λήψη ενός δανείου μπορεί να τρομάζει κάποιους λόγω ελλιπών γνώσεων πάνω στις νέες τεχνολογίες.

• **Δυσπιστία του χρήστη:** Πολλοί άνθρωποι δεν εμπιστεύονται την ηλεκτρονική τραπεζική. Θέλουν να βλέπουν αυτόν που θα επεξεργαστεί το λογαριασμό τους, ενώ η ηλεκτρονική μεταφορά χρημάτων τους προκαλεί αμφιβολίες.

## 4.2 Για την τράπεζα

**Πλεονεκτήματα**

• **Εναλλακτικά δίκτυα :** Το e-banking δίνει τη δυνατότητα στις τράπεζες να εξυπηρετούν τους πελάτες τους και να διεκπεραιώνουν τις συναλλαγές τους μέσω νέων καναλιών που δεν προϋπήρχαν πριν μερικά χρόνια, όπως το internet, το τηλέφωνο και το κινητό.

• **Καινοτομικές υπηρεσίες :** Δίνετε η δυνατότητα στις τράπεζες να εκμεταλλευτούν τα προνόμια που προσφέρει η τεχνολογία και να δημιουργήσουν καινοτομικές και πρωτοποριακές υπηρεσίες, οι οποίες σε διαφορετική περίπτωση δεν θα μπορούσαν να πραγματοποιηθούν.
• **Μείωση λειτουργικού κόστους :** Η εξοικονόμηση που κάνει η τράπεζα μέσω των καναλιών του e-banking είναι πολύ σημαντική αν συγκρίνουμε τα κόστη που έχει για τη διεκπεραίωση συναλλαγών μέσω ταμείου σε σχέση με τα αντίστοιχα κόστη των εναλλακτικών δικτύων *(γράφημα 4)*.

• **Αύξηση ποιότητας εξυπηρέτησης :** Η ποιότητα εξυπηρέτησης μπορεί όχι μόνο να αυξηθεί, αλλά πλέον να πιστοποιείται από εξουσιοδοτημένους φορείς, προσφέροντας κύρος στις μονάδες ηλεκτρονικής τραπεζικής.

• **Αύξηση πελατειακής βάσης :** Η δημιουργία προς το χρήστη φιλικών πλατφόρμων, που παρέχουν ολοκληρωμένα πακέτα συναλλαγών και υπηρεσιών, συμβάλλουν στην προσέλκυση νέων πελατών και στην αύξηση της πελατειακής βάσης.

• **Ενίσχυση της αφοσίωσης των πελατών:** Πολλοί τραπεζικοί αναλυτές υποστηρίζουν ότι μέσω των υπηρεσιών της ηλεκτρονικής τραπεζικής ενισχύεται η αφοσίωση των πελατών καθώς η σχέση μεταξύ πελάτη και τράπεζας τίθεται σε νέα βάση. Επομένως, οι πελάτες που έχουν εξοικειωθεί με τις ηλεκτρονικές υπηρεσίες που προσφέρει μια τράπεζα είναι πολύ πιο διστακτικοί να αλλάξουν τράπεζα.

• **Καλή φήμη :** Το e-banking αποτέλεσε και αποτελεί ένα είδος βιτρίνας για τους τραπεζικούς οργανισμούς. Υπάρχουν παραδείγματα μικρών τραπεζών, που στηρίζουν μέρος της καλής τους εικόνας στο e-banking τους.

**Γράφημα 4. Κόστος Συναλλαγών**


**Πηγή φωτογραφίας:** ***Τραπεζικές Συναλλαγές μέσω Internet, , www.google.gr***

**Μειονεκτήματα**

• **Υψηλό αρχικό κόστος εγκατάστασης:** Η επένδυση που πρέπει να κάνει η τράπεζα για να αγοράσει τον απαιτούμενο εξοπλισμό αλλά και για να εκπαιδεύσει το προσωπικό της πάνω στις νέες τεχνολογίες είναι μεγάλη και πρέπει να γίνει με προσοχή και να είναι συμβατή με τη γενικότερη επιχειρηματική στρατηγική της τράπεζας.

• **Ασφάλεια:** Οι ηλεκτρονικές επιθέσεις και η μη εξουσιοδοτημένη πρόσβαση στα τραπεζικά ηλεκτρονικά συστήματα είναι συχνή. Η ασφάλεια λοιπόν των συναλλαγών και η προστασία των συναλλασσομένων είναι θέματα ύψιστης σημασίας για τις τράπεζες. Καθώς κανένα υπολογιστικό σύστημα δεν είναι 100% ασφαλές.

# Κεφάλαιο 5.

## Απειλές και Κίνδυνοι από τη χρήση του e-banking

Αν και οι ηλεκτρονικές επιθέσεις δεν αποτελούν νέο φαινόμενο, η συχνότητά τους τα τελευταία χρόνια αυξάνεται, αφού 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 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 1 εκατομμύριο δολάρια σε εξοπλισμό και συμβούλους ασφάλειας προκειμένου να διορθώσει τις ατέλειες και να κλείσει τις «τρύπες» που υπάρχουν στο σύστημά της *(Γεωργιάδου, Ζιαζιάς, 2007)*.

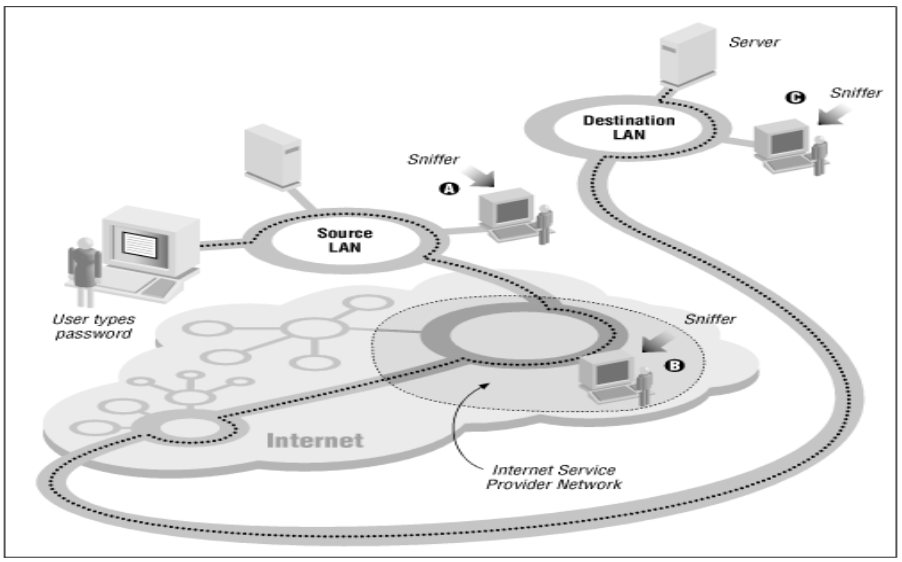
Το πρόβλημα πάντως δεν προβάλλεται στις πλήρεις του διαστάσεις για ευνόητους λόγους. Οι μεγαλύτερες και εντυπωσιακότερες επιθέσεις είναι αυτές που θα δοθούν στη δημοσιότητα, οι υπόλοιπες και περισσότερες, κρατούνται κρυφές. Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους πάντως να επιτύχουν τους σκοπούς 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 χάκερς, να έχουν πρόσβαση σε αυτό" (Γεωργιάδου, Ζιαζιάς, 2007).*
Οι κίνδυνοι, τους οποίους ενδεχομένως αντιμετωπίσουμε είναι :

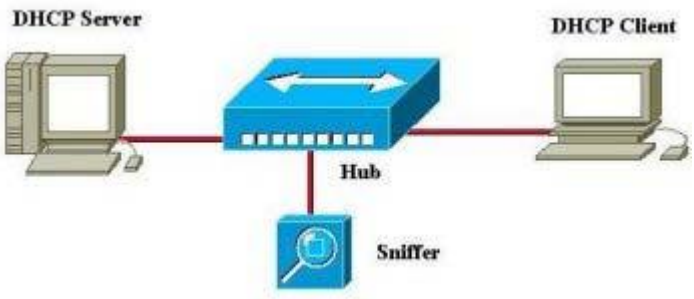
## 5.1 Sniffers

Ένα sniffer είναι ένα πρόγραμμα ή μία συσκευή που παρακολουθεί κρυφά την κίνηση ενός δικτύου με σκοπό να αρπάξει πληροφορία που ταξιδεύει σε αυτό. Ουσιαστικά οι sniffers είναι τεχνολογία υποκλοπής δεδομένων *(βλ. φωτογραφία παρακάτω)*.




**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.unix.org.***

Η πλειοψηφία των δικτύων χρησιμοποιεί τεχνολογία εκπομπής, όπου τα μηνύματα από ένα υπολογιστή μπορούν να διαβαστούν από άλλο υπολογιστή σε αυτό το δίκτυο. Πρακτικά, όλοι οι υπόλοιποι υπολογιστές του δικτύου αγνοούν το μήνυμα, πλην αυτού που είναι ο παραλήπτης του. Ωστόσο, οι υπολογιστές μπορούν να διαμορφωθούν, ώστε να δέχονται μηνύματα ακόμα και αν δεν είναι για αυτούς. Αυτό γίνεται με τη χρήση ενός sniffer *(βλ. φωτογραφία παρακάτω)*.

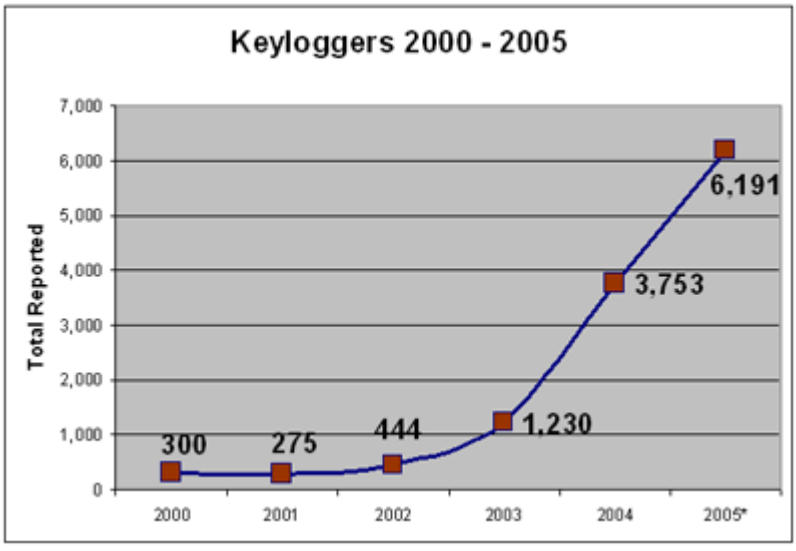



**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.foromsn.com.***

## 5.2 Key Loggers

Το key loggers (καταγραφή πληκτρολογήσεων) συμβαίνει όταν καταγράφονται οι πληκτρολογήσεις του χρήστη, χωρίς ο ίδιος να το ξέρει ή να το επιτρέπει.

Χρησιμοποιείται από επιτήδειους για την κλοπή στοιχείων πιστωτικής κάρτας, τραπεζικών συναλλαγών και προσωπικών κωδικών και αποτελεί σοβαρή απειλή για τη διαρροή προσωπικών αλλά και εταιρικών στοιχείων *(βλ. φωτογραφία παρακάτω)*.




**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.verising.com.***

Η καταγραφή και αποθήκευση των πληκτρολογήσεων γίνεται από ειδικό λογισμικό (hardware), το οποίο είναι εύκολο να εγκατασταθεί και ταυτόχρονα δύσκολο να εντοπισθεί. Ωστόσο, υπάρχει και ανάλογο λογισμικό (software),το οποίο μπορεί να ληφθεί από το internet. Τα key loggers καταγράφουν και αποθηκεύουν τις πληκτρολογήσεις και τα mouse clicks σε ειδικό αρχείο, το οποίο και αποστέλλουν μέσω internet σε αυτόν που κατασκοπεύει το χρήστη.

## 5.3 Κοινωνική μηχανική

Η κοινωνική μηχανική ορίζεται ως ένα μη τεχνικό είδος παράνομης εισβολής που βασίζεται κυρίως στην ανθρώπινη επικοινωνία και συχνά περιλαμβάνει κόλπα τα οποία ωθούν τους ανθρώπους να καταργήσουν τις οριζόμενες διαδικασίες ασφάλειας.
Σενάρια κοινωνικής μηχανικής μπορούν να περιλαμβάνουν:

• Τηλεφωνική επικοινωνία του κοινωνικού μηχανικού με το χρήστη, όπου ο κοινωνικός μηχανικός προσποιείται ότι είναι μέλος της ομάδας IT, που χρειάζεται τους κωδικούς πρόσβασης του χρήστη και άλλες πληροφορίες με σκοπό να διορθώσει προβλήματα που εμφανίστηκαν στο λογαριασμό του χρήστη στο δίκτυο.

• Τηλεφωνική επικοινωνία με το τμήμα IT μιας εταιρίας, προσποιούμενος υψηλό διευθυντικό στέλεχος της εταιρίας που έχει ξεχάσει το password του και απαιτεί άμεσα την πληροφορία για λόγους εξαιρετικής επαγγελματικής ανάγκης.

• Δημιουργία μιας προσωπικής σχέσης με ένα χρήστη ή ένα μέλος ομάδας IT με σκοπό την κουβέντα και το κοινωνικό σχόλιο, ώστε αποκτώντας την εμπιστοσύνη του συνομιλητή να εκμαιεύονται εμπιστευτικές πληροφορίες.

Ένας καλός κοινωνικός μηχανικός δεν είναι μόνο καλός ηθοποιός, είναι επίσης καλός στο να «διαβάζει» τους ανθρώπους και να αποφασίζει ποιου είδους τέχνασμα θα λειτουργήσει καλύτερα με το συγκεκριμένο άνθρωπο. Όταν ένας hacker συνδυάζει ικανότητες κοινωνικής μηχανικής με μεγάλη τεχνική εμπειρία, μπορεί εύκολα να διεισδύσει σε οποιοδήποτε δίκτυο.

## 5.4 Δούρειοι Ίπποι

Ένας δούρειος ίππος είναι ένα φαινομενικά χρήσιμο πρόγραμμα για τον υπολογιστή που περιέχει καμουφλαρισμένες εντολές, οι οποίες όταν εκτελεσθούν δημιουργούν αθέμιτες ή βλαπτικές δράσεις (π.χ καταστροφή αρχείων). Διαδίδονται όταν οι χρήστες ανοίξουν ένα πρόγραμμα διότι θεωρούν ότι έρχεται από νόμιμη πηγή.

Οι δούρειοι ίπποι δεν μπορούν να δημιουργήσουν πανομοιότυπα αντίγραφα, αυτόματα. Η εγκατάσταση τους εξαρτάται από τους χρήστες, ή από εισβολείς που έχουν αποκτήσει μη εγκεκριμένη πρόσβαση στον υπολογιστή με κάποιο τρόπο. Οι δούρειοι ίπποι μπορούν να κάνουν οτιδήποτε που μπορεί να κάνει ο χρήστης που τους εγκατέστησε, όπως :

• Διαγραφή αρχείων, που μπορεί και ο χρήστης να διαγράψει.

• Μετάδοση οποιουδήποτε αρχείου στον εισβολέα, που μπορεί να διαβάσει ο χρήστης.

• Αλλαγή αρχείων που μπορεί ο χρήστης να μεταβάλει.

• Εγκατάσταση προγραμμάτων με τα δικαιώματα του χρήστη του υπολογιστή που παρέχουν μη εγκεκριμένη πρόσβαση στο δίκτυο.

• Εγκατάσταση ιών.

• Εγκατάσταση άλλων δούρειων ίππων.

## 5.5 Phishing

Το Phishing είναι η αποστολή e-mail σε χρήστη, προσποιούμενο ότι προέρχεται από μια νόμιμη επιχείρηση, κυρίως τράπεζα ή τηλεπικοινωνιακό πάροχο, με σκοπό να εξαπατήσει τον χρήστη και να πάρει ιδιωτικές πληροφορίες που θα χρησιμοποιηθούν για κλοπή της ταυτότητάς τους.

Το e-mail προτρέπει το χρήστη να επισκεφθεί ένα web site όπου του ζητούνται να ενημερώσει τις προσωπικές του πληροφορίες, όπως password και αριθμούς πιστωτικών καρτών, αριθμούς τραπεζικών λογαριασμών, οπού η εταιρία υποτίθεται έχει ήδη στην κατοχή της. Το web site ωστόσο είναι πλαστό και έχει δημιουργηθεί με μοναδικό σκοπό να κλέψει τη ζητούμενη πληροφορία.

Την ίδια ώρα αυτοί που κρύβονται πίσω από το ψεύτικο μήνυμα αποκτούν πρόσβαση στα στοιχεία αυτά και στη συνέχεια μπορούν να κάνουν ηλεκτρονικές απάτες εις βάρος των θυμάτων τους *(Παπαδόπουλος, 2005)*.

Οι επιθέσεις phishing αυξάνονται ραγδαία και με έξυπνο τρόπο. Σύμφωνα με έρευνες, ο ρυθμός εξάπλωσής τους διπλασιάζεται μέσα σε ένα εξάμηνο.

Εναλλακτικές μορφές:

**Vishing:** Σε αυτή την εκδοχή του phishing, για να πειστεί ευκολότερα το θύμα, του δίνεται τηλεφωνικός αριθμός εξυπηρέτησης ή του ζητείται το δικό του τηλέφωνο ώστε να μπορούν να επικοινωνήσουν μαζί του οι υποτιθέμενοι εκπρόσωποι της εταιρίας. Η πρακτική αυτή στηρίζεται στις τεχνολογίες Voip που προσφέρει το Διαδίκτυο.

**Social Networking Phishing:** Αντλώντας πληροφορίες και πολλά προσωπικά δεδομένα από τα προφίλ των χρηστών των ιστοσελίδων κοινωνικής δικτύωσης, οι απατεώνες στέλνουν εξατομικευμένα μηνύματα. Σε πρόσφατο πείραμα που πραγματοποιήθηκε στις Ηνωμένες Πολιτείες το 70% όσων έλαβαν το εξατομικευμένο παραπλανητικό μήνυμα πάτησε το σύνδεσμο που περιέχετο σε αυτό και συμπλήρωσε τα στοιχεία του στο εικονικό site.

Οι συνηθέστερες μέθοδοι που χρησιμοποιούνται για επιθέσεις Phishing με ηλεκτρονικό ταχυδρομείο περιλαμβάνουν:

1. Χρήση ηλεκτρονικής αλληλογραφίας που μοιάζει να έχει σταλεί από έμπιστη πηγή.
2. Χρήση αντιγράφων ηλεκτρονικής αλληλογραφίας στα οποία έχουν γίνει αλλαγές σε περιεχόμενα URLs και hyperlinks.
3. Χρήση HTML ηλεκτρονικής αλληλογραφίας στην οποία έχουν γίνει αλλαγές σε περιεχόμενα URLs και hyperlinks.

4. Χρήση ιών (viruses) και σκουληκιών (worms) συνημμένων σε ηλεκτρονική αλληλογραφία
5. Χρήση αντί-spam εργαλείων
6. Χρήση εξατομικευμένης ηλεκτρονικής αλληλογραφίας
7. Χρήση ηλεκτρονικής αλληλογραφίας με τροποποιημένη ένδειξη αποστολέα σε συνδυασμό με χρήση Open Mail Relays διακομιστών για την απόκρυψη της προέλευσης της ηλεκτρονικής αλληλογραφίας.

Το phishing είναι εξαιρετικά αποτελεσματικό, γιατί σύμφωνα με τα αποτελέσματα της εταιρίας Infosury :

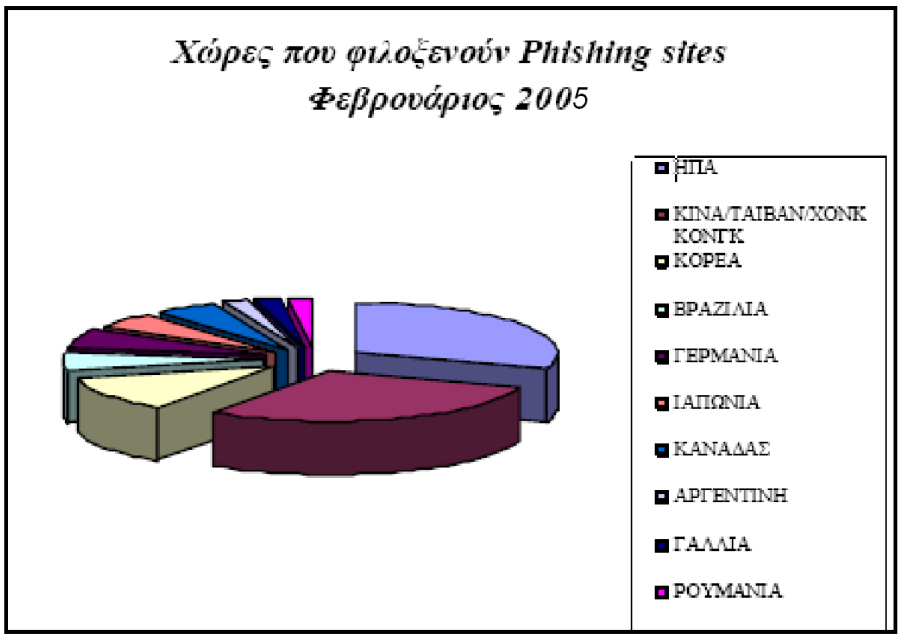
• Το 44% των χρηστών του e-banking χρησιμοποιούν τους ίδιους κωδικούς για όλες τις ηλεκτρονικές τραπεζικές υπηρεσίες που έχουν σε όλες τις τράπεζες.

• Το 37% των χρηστών του e-banking χρησιμοποιούν τους ίδιους κωδικούς και σε λιγότερο ασφαλή site π.χ ηλεκτρονικές βιβλιοθήκες.

• Το 79% των χρηστών ελέγχουν αν υπάρχει η κλειδαριά ασφαλείας στο κάτω μέρος μιας ασφαλούς σελίδας, αλλά μόνο το 40% πατάει πάνω της για να δει τις λεπτομέρειες του πιστοποιητικού. Το εικονίδιο της κλειδαριάς μπορεί εύκολα να αντιγραφεί.

• Το 70% των χρηστών έχουν μικρές πιθανότητες να απαντήσουν σε ένα e mail από την τράπεζά τους και περισσότεροι από τους μισούς έχουν να εγγραφούν ή να συνεχίσουν να χρησιμοποιούν τις on line υπηρεσίες εξαιτίας του phishing.

**Γράφημα 5. Χώρες που φιλοξενούν phishing sites**



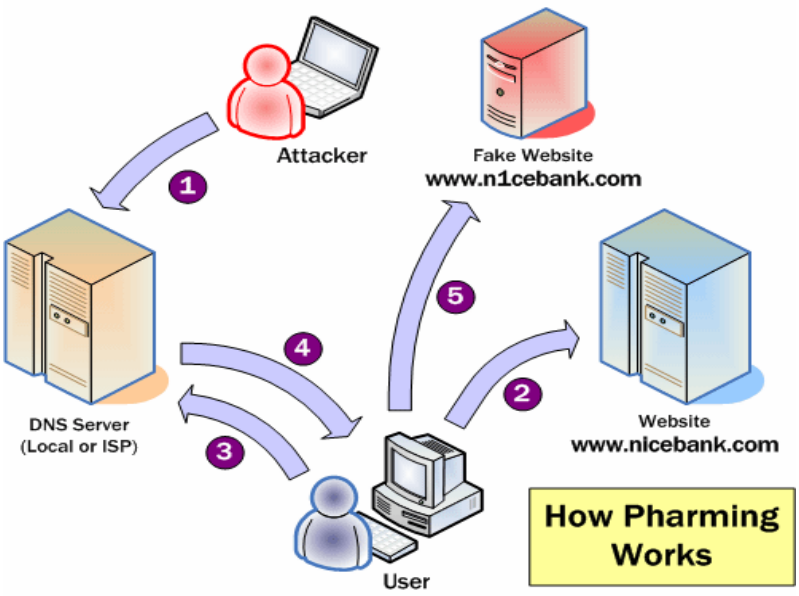

**Πηγή φωτογραφίας:** ***Αγγέλης Βασίλης. (2005)***

## 5.6 Pharming

Καθώς οι χρήστες και οι οργανισμοί είναι πλέον περισσότερο προσεκτικοί στις επιθέσεις phishing, οι απατεώνες προχώρησαν ένα βήμα παραπάνω. Η νέα τάση στην ηλεκτρονική υποκλοπή κωδικών ονομάζεται pharming.

Το Pharming είναι μια μορφή απάτης της ηλεκτρονικής διεύθυνσης (domain name) που έχει ως αποτέλεσμα να πιστεύουν οι χρήστες, ότι βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL. Ωστόσο, στην πραγματικότητα έχουν παραπεμφθεί σε μια ψεύτικη *( www.saferinternet.gr ).*

Οι χάκερς εκμεταλλευόμενοι κάποια κενά στην ασφάλεια μιας ιστοσελίδας στην οποία οι χρήστες μπαίνουν για να πραγματοποιήσουν διάφορες συναλλαγές, καταφέρνουν να εκτρέψουν την ροή των επισκεπτών σε άλλο ιστοχώρο όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών (*βλ. φωτογραφία παρακάτω)*. Τέτοιου είδους εκτροπή δεν μπορεί να γίνει σε ιστοσελίδες που χρησιμοποιούν το πρωτόκολλο SSL *(ΚΥΔ Πανεπιστημίου Μακεδονίας).*




**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.plynt.com.***

Οι βασικές διαφορές του pharming από το phishing είναι δύο, σύμφωνα με όσα αναφέρει ο Αγγέλης (2005):

1. Η επίθεση μπορεί να γίνει μαζικά σε πολλούς χρήστες και όχι μεμονωμένα σε κάθε χρήστη (μέσω e-mail).

2. Η μετακίνηση σε pharming site γίνεται χωρίς την παρέμβαση του χρήστη (π.χ επιλογή link από e-mail).

Οι τρόποι δράσης των απατεώνων είναι οι ακόλουθοι :

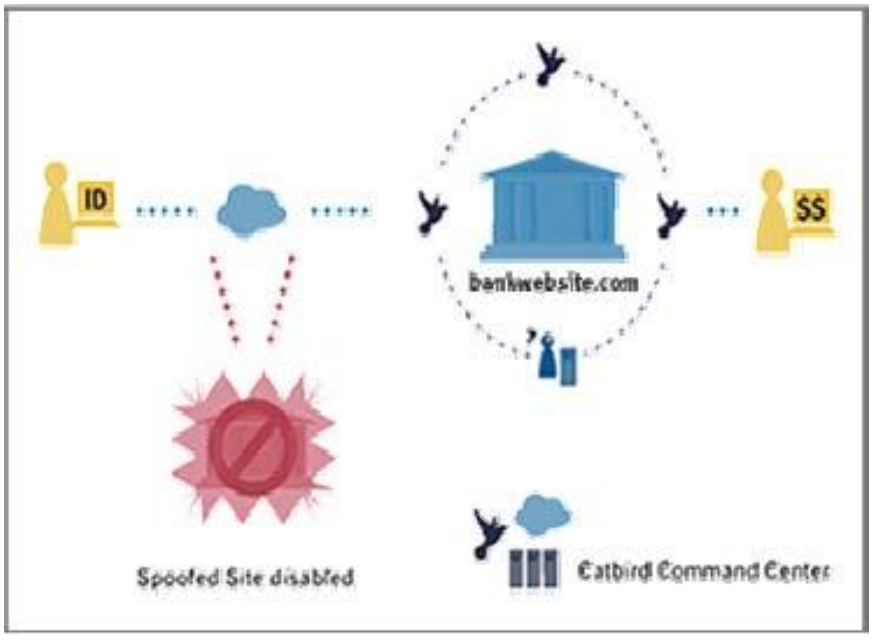
• **Αποστολή ιών μέσω e-mail :** Οι ιοί αυτοί (π.χ Banker Trojan) αντικαθιστούν τα τοπικά host αρχεία του υπολογιστή του χρήστη με άλλα. Τα host αρχεία μετατρέπουν τα URLs σε αριθμητικές συμβολοσειρές που είναι κατανοητές από τον υπολογιστή. Ένας υπολογιστής με αλλαγμένα host αρχεία θα μεταβεί σε λαθεμένο site ακόμα και αν ο χρήστης πληκτρολογήσει το σωστό URLs.

• **Παραποίηση DNS :** Η κυριότερη απειλή του pharming είναι η παραποίηση DNS ( Domain Name System ) ενός εταιρικού site. Αυτό έχει ως αποτέλεσμα τη μετάβαση μεγάλου αριθμού σε site χωρίς καν να ο αντιλαμβάνονται.

Ιδιαίτερα διαδεδομένη είναι η χρήση **ψευδών τραπεζικών sites (Fake Banks).**

Στην περίπτωση αυτή οι εισβολείς δημιουργούν sites πανομοιότυπα με αυτά των νόμιμων τραπεζών, με μικρές διαφοροποιήσεις, ή ακόμα και sites που υποτίθεται ότι είναι νέες τράπεζες (Παράρτημα 4). Σε αρκετές περιπτώσεις υπάρχουν και φωτογραφίες ανυποψίαστων θυμάτων, τα οποία εμφανίζονται ως η διοίκηση της on line τράπεζας.

Αρκετοί είναι οι χρήστες που εξαπατώνται και διενεργούν εικονικές συναλλαγές χωρίς καμία υπόσταση σε τέτοια sites, δίνοντας έτσι κωδικούς, αριθμούς λογαριασμών και καρτών εν αγνοία τους, *(Παπαδόπουλος, 2005)*.




**Πηγή φωτογραφίας:** ***Από το διαδίκτυο, www.catbird.com.***

# Κεφάλαιο 6.

## Ασφάλεια - Τρόποι προστασίας από on line απάτες

Η ευκολία της χρήσης και τα πλεονεκτήματα των εναλλακτικών δικτύων τα έχουν κάνει ευρέως αποδεκτά από τους πελάτες των τραπεζών. Ωστόσο, όπως συμβαίνει σε κάθε παρόμοια περίπτωση, η ευρεία αποδοχή των εναλλακτικών δικτύων έχει τραβήξει την προσοχή επίδοξων απατεώνων, οι οποίοι χρησιμοποιούν μια σειρά μεθόδων με σκοπό να αποσπάσουν προσωπικά στοιχεία των χρηστών και να πραγματοποιήσουν παράνομα κέρδη εις βάρος των τραπεζών, αλλά και εις βάρος των ανυποψίαστων πελατών.

Για να ελαχιστοποιηθούν τα κρούσματα αυτά, οι τράπεζες από την πλευρά τους υιοθετούν όλα τα απαραίτητα μέτρα για τη διατήρηση του υψηλότερου δυνατού επιπέδου ασφαλείας κατά τη διάρκεια των συναλλαγών *(βλ. Παράρτημα5)*.

Σύμφωνα με πρόσφατη έρευνα που έγινε σε καταναλωτές αμερικανικών e-banking, διαπιστώθηκε ότι σχεδόν το 71% σκέφτονται σοβαρά την on line απάτη *(Αγγέλης, 2005)*. Από την έρευνα προέκυψε ο παρακάτω πίνακας 1.

**Πίνακας 1. Ενέργειες που πρέπει να κάνουν οι τράπεζες για να αυξήσουν την εμπιστοσύνη του καταναλωτή στο e-banking.**

| | |
|---|---|
| Παροχή καλύτερων back-end συστημάτων ανίχνευσης απάτης | 43% |
| Δημιουργία μοντέλων ανίχνευσης απάτης | 41% |
| Παροχή εκπαιδευτικών πληροφοριών σχετικά με την on line τραπεζική απάτη | 35% |
| Τακτική επικοινωνία με πελάτη για τις ενέργειές αποφυγής on line απάτης | 34% |
| Διενέργεια διαφημιστικών καμπανιών με οδηγίες αποφυγής της on line απάτης | 22% |

## 6.1 Κρυπτογράφηση

Οι επιχειρήσεις, συμπεριλαμβανομένων και των τραπεζών, αντικαθιστούν πλέον τις βασισμένες σε χαρτί, φυσικές τους διαδικασίες με ηλεκτρονικές και ψηφιακές διαδικασίες. Σε αυτό το κλίμα περιλαμβάνεται η αποστολή προϊόντων και υπηρεσιών, η ηλεκτρονική ανταλλαγή δεδομένων, η μεταφορά κεφαλαίων, οι εκκαθαρίσεις και το internet banking.

Οι τράπεζες απαιτείται να σχεδιάζουν σφιχτούς ελέγχους σε αυτά τα νέα μοντέλα εργασίας, ώστε να διαχειρίζονται το ρίσκο. Οι βασικές ανάγκες για διασφάλιση των ιδιωτικών δεδομένων, εμπιστοσύνη και πιστοποίηση θα συνεχίσουν να υφίστανται και στον ψηφιακό, όπως και στο φυσικό κόσμο. Η κρυπτογράφηση προσφέρει αξιόλογες λύσεις.

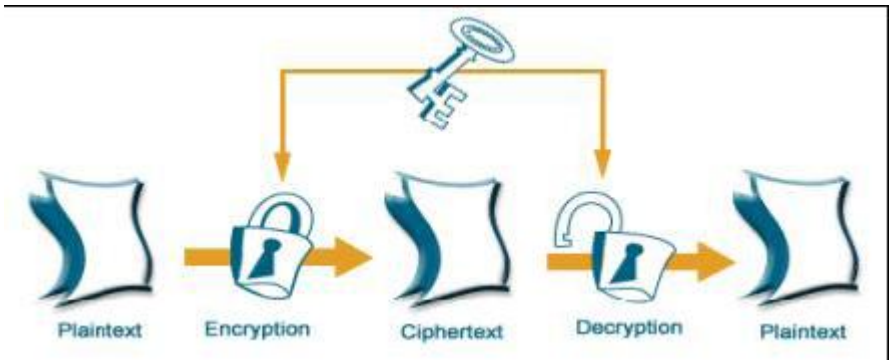
### ➢ Διαφορετικά Είδη Κρυπτογράφησης

Υπάρχουν δύο διαφορετικά είδη κρυπτογράφησης με δύο ξεχωριστούς στόχους. Ένας στόχος είναι η διατήρηση του ιδιωτικού χαρακτήρα και το απαραβίαστο της πληροφορίας. Ο άλλος στόχος είναι η πιστοποίηση της ταυτότητας των εμπλεκόμενων μερών μιας συναλλαγής. Και τα δύο είδη κρυπτογράφησης συνήθως χρησιμοποιούνται μαζί για την προστασία των μηνυμάτων και την πιστοποίηση των εμπλεκόμενων μερών. Κάθε ένα από τα δύο είδη έχει συγκεκριμένα βιομηχανικά πρότυπα.

Οι προμηθευτές της τεχνολογίας κρυπτογράφησης, την παρέχουν είτε ως προϊόν λογισμικού, είτε ως συγκεκριμένο εξάρτημα συσκευής.

Οι δύο αυτοί θεμελιώδεις τύποι κρυπτογράφησης είναι η **συμμετρική** και η **ασύμμετρη**. Η συμμετρική είναι επίσης γνωστή και ως κρυπτογράφηση με μυστικό κλειδί (secret key cryptography). Η συμμετρική κρυπτογράφηση *(βλ. Σχήμα Α)*, χρησιμοποιεί το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση. Αρχικά, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

**Σχήμα (Α) : Συμμετρική Κρυπτογραφία**




**Πηγή φωτογραφίας:** ***Γεωργιάδου ,Ζιαζιάς, Ιούλιος 2007***

Τα πλεονεκτήματα της κρυπτογράφησης με μυστικό κλειδί συνοψίζονται στα ακόλουθα:

• Είναι ασφαλές
• Έχει ευρύτητα χρήση και διάδοση, και
• Είναι γρήγορο

Τα μειονεκτήματα είναι τα παρακάτω :

• Η διαχείριση του μυστικού κλειδιού είναι περίπλοκη, απαιτώντας και από τα δύο μέρη να διατηρούν τον απόλυτο έλεγχο στην ανταλλαγή κλειδιών,
• Δεν περιλαμβάνει ξεχωριστό μηχανισμό αυθεντικότητας και,
• Δεν έχει non repudiation (αδιάσειστη απόδειξη συμμετοχής και του αποστολέα και του παραλήπτη).

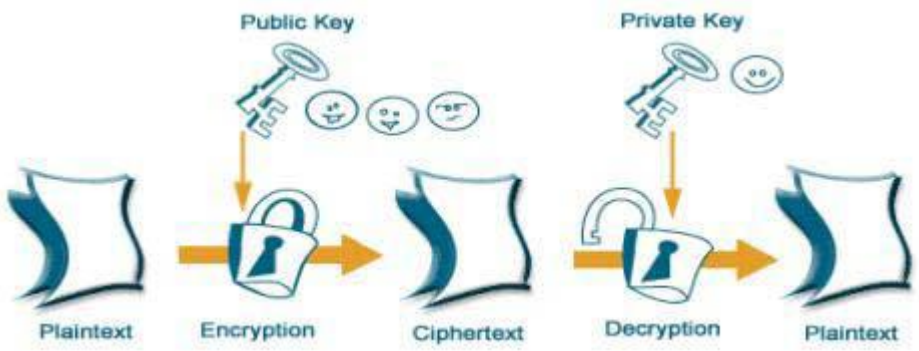
Η ασύμμετρη *(βλ. Σχήμα Β),* είναι επίσης γνωστή και ως κρυπτογράφηση με δημόσιο/ ιδιωτικό κλειδί (public/private key cryptography), περιλαμβάνει δύο κλειδιά.

Τα κλειδιά αυτά παράγονται έτσι ώστε να έχουν τις εξής ιδιότητες:

• Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.

• Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.

**Σχήμα Β: Ασύμμετρη κρυπτογραφία**




**Πηγή φωτογραφίας:** ***Γεωργιάδου, Ζιαζιάς, Ιούλιος 2007***

"*Το 1976 οι Diffie και Hellman διατύπωσαν την βασική αρχή της κρυπτογραφίας δημόσιου κλειδιού, ενώ το 1977 οι Rivest, Shamir και Adleman δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων" (Γεωργιάδου, Ζιαζιάς, 2007).*

Για να αποκατασταθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δε μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογραφία προσφέρει μεγαλύτερη ασφάλεια από τη συμμετρική.

Ένα από τα πλεονεκτήματα της κρυπτογράφησης με δημόσιο /ιδιωτικό κλειδί είναι ότι απλοποιεί τη διαχείριση των κλειδιών. Ενώ το κυριότερο μειονέκτημα είναι ότι η κρυπτογράφηση με δημόσιο κλειδί είναι πολύ πιο αργή από την κρυπτογράφηση με ιδιωτικό κλειδί. Για το λόγο αυτό χρησιμοποιείται κυρίως για την πιστοποίηση τμημάτων μηνυμάτων, παρά για την κρυπτογράφηση ενός ολόκληρου μηνύματος.

## 6.2 PKI

Η τεχνολογία PKI (Public Key Infrastructure) είναι μία πολύ γνωστή τεχνολογία που μπορεί να χρησιμοποιηθεί για να αναγνωρίσει οντότητες, να κρυπτογραφήσει πληροφορία και να υπογράψει ηλεκτρονικά έγγραφα.

Η PKI αναγνωρίζει και διαχειρίζεται σχέσεις μεταξύ των μελών μιας ηλεκτρονικής ανταλλαγής δεδομένων, εξυπηρετεί ένα μεγάλο εύρος αναγκών ασφαλείας, συμπεριλαμβανομένων ελέγχου πρόσβασης, εμπιστευτικότητα, ακεραιότητα, πιστοποίηση και μη αποποίηση ευθύνης.

Η PKI χρησιμοποιεί επίσης μοναδικά ψηφιακά πιστοποιητικά για να ασφαλίσει το e-banking και το e-commerce, το e-mail,την ανταλλαγή δεδομένων καθώς και τα VIPs και τα intranets.

Τέλος η PKI τεχνολογία χρησιμοποιείται για να πιστοποιήσει την ταυτότητα και τα δεδομένα του κάθε χρήστη. Επιπρόσθετα η Αρχή Πιστοποίησης, που είναι αυτή που εγγυάται την PKI τεχνολογία, παρέχει ένα ολοκληρωμένο πακέτο διαχείρισης των δημοσίων κλειδιών και πιστοποιητικών, που περιλαμβάνει την έκδοση, την πιστοποίηση, την αποθήκευση, την πρόσβαση, το backup, την ανάνηψη, την ενημέρωση και την ανανέωση.

Όλοι οι χρήστες της PKI πρέπει να έχουν μία εγκεκριμένη ταυτότητα, η οποία είναι αποθηκευμένη σε ένα ψηφιακό πιστοποιητικό που εκδίδει η Αρχή Πιστοποίησης. Αυτό λειτουργεί ως ο σύνδεσμος της εμπιστοσύνης στο PKI.

Απομακρυσμένοι χρήστες και δικτυακοί τόποι που χρησιμοποιούν δημόσια και ιδιωτικά κλειδιά και πιστοποιητικά δημοσίων κλειδιών μπορούν να πιστοποιηθούν με υψηλό βαθμό εμπιστοσύνης. Η πιστοποίηση αυτή εξαρτάται από τρεις συνθήκες :

• Πρέπει να κατοχυρώνεται ότι το δημόσιο κλειδί που κατέχει το κάθε μέρος, δεν έχει κλαπεί ή αντιγραφεί από τον ιδιοκτήτη του.

• Το πιστοποιητικό πρέπει να εκδίδεται στον ιδιοκτήτη σε αρμονία με την καταγεγραμμένη πολιτική του εκδότη πιστοποιητικών.

• Οι πολιτικές του εκδότη πιστοποιητικών πρέπει να ικανοποιούν τα εμπλεκόμενα μέρη, όσον αφορά την πιστοποίηση της ταυτότητας. Από τη στιγμή που ικανοποιούνται οι τρεις αυτές συνθήκες, τότε υπάρχει η σωστή βάση για την εξασφάλιση της ασφάλειας.

### ➢ Δημόσια και ιδιωτικά κλειδιά

Η PKI χρησιμοποιεί ένα σύστημα ζευγαριών κλειδιών, που είναι ασύμμετρα, συνδέονται μαθηματικά μεταξύ τους και εκτελούν αντίθετες ενέργειες, δηλαδή ότι κλειδώνει το ένα κλειδί, μόνο το άλλο μπορεί να ξεκλειδώσει.

Τα δημόσια και ιδιωτικά κλειδιά είναι μοναδικά για κάθε χρήστη σε ένα PKI σύστημα. Το ιδιωτικό κλειδί δημιουργείται πρώτα. Τα ιδιωτικά κλειδιά πρέπει να προστατεύονται από υποκλοπές και συνήθως αποθηκεύονται σε φυσικές

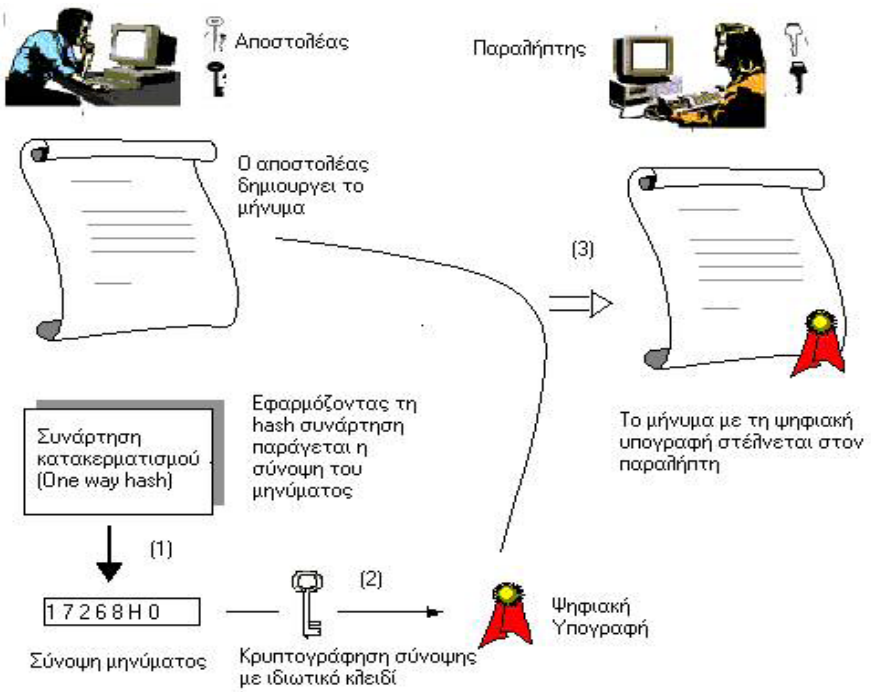
συσκευές όπως είναι οι έξυπνες κάρτες ή τα tokens. Τα δημόσια κλειδιά από την άλλη μεριά είναι διαθέσιμα σε όλους.

Οποιοσδήποτε επιθυμεί να κάνει ασφαλείς συναλλαγές χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη ως μέρος της διαδικασίας κρυπτογράφησης.

Κρυπτογραφώντας κάτι με το δημόσιο κλειδί κάποιου άλλου, εξασφαλίζεται ότι μόνο αυτός μπορεί να το αποκωδικοποιήσει. Αν για οποιοδήποτε λόγο το μήνυμα αποστολής μιας κρυπτογραφημένης συναλλαγής παραβιαστεί, είναι απίθανο αυτό το μήνυμα να αποκωδικοποιηθεί και εκτελεστεί.

## ➢ Ψηφιακές υπογραφές

Όταν παραλαμβάνεται ένα κρυπτογραφημένο μήνυμα ή συναλλαγή, είναι σημαντικό να υπάρχει η δυνατότητα πιστοποίησης ότι ο αποστολέας του, είναι όντως αυτός που ισχυρίζεται. Αυτό επιτυγχάνεται μέσω της ψηφιακής υπογραφής. Μιας μοναδικής διαδικασίας υπογραφής μηνύματος που αποκαλύπτει την ταυτότητα του αποστολέα και πιστοποιεί την ακεραιότητα του μηνύματος *(βλ. φωτογραφία παρακάτω)*.




**Πηγή φωτογραφίας*: Χαλαστής Κ. , Σεπτέμβριος 2007***

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της.

Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Οι ψηφιακές υπογραφές είναι αδιάψευστες, μοναδικές για κάθε συναλλαγή και είναι σχεδόν απίθανο να αντιγραφούν ή μεταφερθούν.

- **Ψηφιακά Πιστοποιητικά**

Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο.

Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι, και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί, ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε, *μη αποποίηση (e Business Forum, 2004)*.

Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που

εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί. Η οντότητα αυτή είναι ο Πάροχος Υπηρεσιών Πιστοποίησης.

Τα πιστοποιητικά μπορούν να περιέχουν μια ποικιλία πληροφοριών, συμπεριλαμβανομένων της επωνυμίας του κατόχου, του δημοσίου κλειδιού, της ημερομηνίας λήξης του πιστοποιητικού, των λειτουργιών που πρέπει να εκτελέσει το δημόσιο κλειδί (κρυπτογράφηση, αποκρυπτογράφηση ή επαλήθευση ψηφιακής υπογραφής), της ψηφιακής υπογραφής του εκδότη, του σειριακού του αριθμού και της μεθόδου κρυπτογράφησης.

## ➢ Αρχές Πιστοποίησης

Ο κύριος σκοπός μιας αρχής πιστοποίησης είναι η έκδοση ψηφιακών πιστοποιητικών και η επιβεβαίωση του ατόμου που συνδέεται με το πιστοποιητικό.

Η αρχή πιστοποίησης προσθέτει ένα επιπλέον επίπεδο εμπιστοσύνης στις συναλλαγές που βασίζονται στην PKI.

1. Ο συνδρομητής (αποστολέας) αιτείται στην αρχή πιστοποίησης ένα ψηφιακό πιστοποιητικό.

2. Η αρχή πιστοποίησης επαληθεύει τον συνδρομητή και εκδίδει το ψηφιακό πιστοποιητικό.

3. Η αρχή πιστοποίησης δημοσιεύει το πιστοποιητικό, σε ένα on line repository.

4. Ο συνδρομητής υπογράφει το μήνυμα του με ένα ιδιωτικό κλειδί και τα στέλνει στους παραλήπτες.

5. Ο παραλήπτης επαληθεύει την ψηφιακή υπογραφή με χρήση του δημοσίου κλειδιού του αποστολέα και αιτείται επαλήθευση του ψηφιακού πιστοποιητικού του αποστολέα από το δημόσιο repository.

6. Το repository αναφέρει το status του ψηφιακού πιστοποιητικού του αποστολές.

Αφού το υπογεγραμμένο και κρυπτογραφημένο μήνυμα παραληφθεί, το μήνυμα αποκρυπτογραφείται και επαληθεύεται η ακεραιότητα του περιεχομένου του.

## 6.3 Πιστοποίηση δύο παραγόντων

Οι περισσότεροι ειδικοί του IT συμφωνούν ότι η πιστοποίηση δύο παραγόντων είναι ζωτική για την αποτελεσματική ασφάλεια δικτύων. Ωστόσο κάθε οργανισμός πρέπει να επιλέξει ποια από όλες τις παρεχόμενες λύσης πιστοποίησης δύο παραγόντων είναι κατάλληλη για τις ανάγκες του *(Αγγέλης, 2005)*. Υπάρχουν τρεις διαφορετικές λύσεις :

1. Challenge – Response
2. Event – Synchronous
3. Time – Synchronous

Παρακάτω παρατίθεται οι διαφορές μεταξύ των τριών λύσεων.

**Challenge – Response**

1. Ο χρήστης εισάγει username και password
2. Ο server στέλνει ένα Challenge
3. Ο χρήστης εισάγει το Challenge
4. Ένα response εμφανίζεται στην οθόνη του token
5. Ο χρήστης εισάγει το response και γίνεται το validation

**Event – Synchronous**

1. Ο χρήστης ενεργοποιεί τον επόμενο κωδικό του token πατώντας ένα κουμπί σε αυτό.
2. Ο χρήστης εισάγει username και pass code.
3. Ο server πιστοποιεί τον χρήση ταιριάζοντας το pass code του χρήστη μα το pass code του server.

**Time – Synchronous**

1. Ο χρήστης εισάγει username και pass code.
2. Ο server και το token υπολογίζουν τον κωδικό του token συνδυάζοντας το seed και την τρέχουσα ώρα Greenwich. Ο server πιστοποιεί τον χρήστη ταιριάζοντας το pass code με το pass code του server.

Η πιστοποίηση με Time – Synchronous ταυτοποίηση θεωρείται πιο αποτελεσματική από τις άλλες δύο για τους παρακάτω λόγους:

• **Ενίσχυση ασφάλειας :** Η Time – Synchronous προσέγγιση της ταυτοποίησης δύο παραγόντων είναι πολύ πιο ασφαλείς από τις λοιπές. Η τεχνολογία αυτή βασίζεται στο μυστικό seed του token, που ουσιαστικά δεν μπορεί να σπάσει. Οι άλλες προσεγγίσεις είναι λιγότερο τεχνικά εξελιγμένες και ευάλωτες.

• **Ευκολία χρήσης:** είναι διαδικασία δύο βημάτων μόνο, σε αντίθεση με τις άλλες δύο που είναι πέντε και τριών αντίστοιχα, άρα και πιο ευάλωτες σε λάθη χρηστών.

• **Μικρότερο διαχειριστικό κόστος:** Επειδή απαιτούνται λίγα μόνο πατήματα πλήκτρων, υπάρχουν μικρότερες πιθανότητες να κλειδωθεί ο χρήστης και άρα να πρέπει ο διαχειριστής να τον ξεκλειδώνει.

• **Φορητότητα:** Τα Time – Synchronous tokens είναι εντελώς φορητά, επειδή σε καμία περίπτωση δεν εγκαθίσταται μόνιμα στον υπολογιστή του χρήστη.

## 6.4 Έξυπνες κάρτες (Smart Cards)

Αρκετοί από εμάς χρησιμοποιούμε ήδη μία ή περισσότερες έξυπνες κάρτες στην καθημερινή μας ζωή. Για παράδειγμα, έξυπνη κάρτα είναι η κάρτα SIM που χρησιμοποιείται στο σύστημα κινητής τηλεφωνίας GSM. Οι έξυπνες κάρτες είναι ουσιαστικά μικροσκοπικοί υπολογιστές, που έχουν το μέγεθος και τη φόρμα μίας

πιστωτικής κάρτας, πάνω στην οποία είναι ενσωματωμένο ένα ολοκληρωμένο κύκλωμα (chip).

Το κύριο γνώρισμα των έξυπνων καρτών είναι η ικανότητα να αποθηκεύουν και να επεξεργάζονται πληροφορίες με ένα ασφαλή τρόπο, ενώ τα πλεονεκτήματα των έξυπνων καρτών είναι η προστασία των δεδομένων που περιέχουν, η φορητότητα και η ευκολία χρήσης.

Η τεχνολογία των έξυπνων καρτών μπορεί να χρησιμοποιηθεί για να δημιουργήσει κάρτες που παρέχουν ισχυρή ταυτοποίηση και αυτό γίνεται με την ενσωμάτωση ηλεκτρονικών κλειδιών στην κάρτα. Ένα μεγάλο ζήτημα σχετικά με τις έξυνες κάρτες είναι η χρήση τους για πιστοποίηση.

Στην πραγματικότητα, οι έξυπνες κάρτες μπορούν να παρέχουν προσωπικές πληροφορίες του κατόχου, κλειδιά για ψηφιακή υπογραφή κ.α. Φυσικά για να αποφευχθεί το γεγονός οι πληροφορίες που προσφέρει μία κάρτα να καταντήσουν περιορισμός και όχι πλεονέκτημα για τις ηλεκτρονικές υπηρεσίες, οι τελευταίες πρέπει να σχεδιάζονται χωρίς να λαμβάνουν υπόψη τις έξυπνες κάρτες που υπάρχουν. Αυτό συμβαίνει γιατί αρκετοί πελάτες δεν θα έχουν στην κατοχή τους για μεγάλο χρονικό διάστημα τέτοιου είδους κάρτες *(e- Business Forum, 2003).*

### ➢ Βασικά Χαρακτηριστικά Έξυπνων Καρτών

- Κόστος
- Αξιοπιστία
- Ικανότητα αποθήκευσης
- Ευκολία χρήσης
- Ασφάλεια
- Ταχύτητα ανάγνωσης
- Υπολογιστική ισχύς

### ➢ Εμπόδια κατά την αποδοχή των Έξυπνων Καρτών

- Σχετικά υψηλότερο κόστος
- Έλλειψη παρούσας υποδομής
- Έλλειψη προτύπων για την εξασφάλιση διαλειτουργικότητας
- Ο καταναλωτής πρέπει να είναι τεχνικά πεπειραμένος

- **Τύποι έξυπνων καρτών**

• Κάρτα μνήμης
• Κάρτες με μικρο-επεξεργαστή
•Contact κάρτα
•Contactless κάρτα
•Υβριδικές και Combi κάρτες
• Κάρτες που επιδέχονται φόρτωση προγραμμάτων

## 6.5 Πιστοποίηση δύο παραγόντων και PKI

Για περισσότερη ασφάλεια, ένας τραπεζικός οργανισμός μπορεί να απαιτεί το ψηφιακό πιστοποιητικό του πελάτη να αποθηκεύεται στο token ή σε μία έξυπνη κάρτα.

Οι έξυπνες κάρτες και άλλες συσκευές για τον καταναλωτή που περιέχουν ηλεκτρονικά τσιπς είναι πιο ακριβές λύσεις από λύσεις λογισμικού. Έχουν όμως το πλεονέκτημα, αποθηκεύοντας ιδιωτικά κλειδιά σε tokens αντί στον σκληρό δίσκο του υπολογιστή να αποτρέπουν την πρόσβαση μη εγκεκριμένων χρηστών στον υπολογιστή του πελάτη με σκοπό την αντιγραφή των κρυπτογραφημένων κλειδιών χωρίς να έχει γνώση ο χρήστης.

- **USB Tokens**

Το eToken είναι μια ειδική συσκευή στο μέγεθος ενός κλειδιού, η οποία περιέχει έναν κρυπτογραφικό μηχανισμό που δίνει τη δυνατότητα στον κάτοχό του να δημιουργήσει και να αποθηκεύσει το απαραίτητο λογισμικό ώστε να λειτουργεί σαν την ηλεκτρονική του υπογραφή.

Όταν συνδεθεί με οποιονδήποτε υπολογιστή μέσω της USB θύρας, το eToken δίνει στον χρήστη τη δυνατότητα να υπογράφει ψηφιακά όλες τις προσωπικές του συναλλαγές. Έτσι, μέσω της προσωπικής ταυτοποίησης επιτυγχάνεται η μέγιστη δυνατή παροχή ασφάλειας.

Ο χρήστης της υπηρεσίας έχει δυνατότητα να εγκαταστήσει το πιστοποιητικό είτε στον υπολογιστή του είτε στην ειδική συσκευή eToken. Τα USB Tokens όταν συνδυάζονται με την PKI τεχνολογία παρέχουν ισχυρή πιστοποίηση δύο παραγόντων.

Τα πλεονεκτήματα που απορρέουν είναι τα ακόλουθα :

• **Υψηλή Ασφάλεια :** Οι συσκευές δεν μπορούν να αντιγραφούν, ενώ το PIN του αποθηκεύεται κρυπτογραφημένο, έτσι προστατεύεται το PKI ψηφιακό ID του χρήστη από κλοπή.

• **Πολλές δυνατότητες :** Το PKI ψηφιακό ID του χρήστη μπορεί να χρησιμοποιηθεί για πολλές λειτουργίες, όπως πιστοποίηση, ψηφιακή υπογραφή, κρυπτογράφηση κ.α. Επίσης το ψηφιακό ID μπορεί να χρησιμοποιηθεί για ασφάλεια του χρήστη σε περισσότερες από μία εφαρμογές.

• **Ευκολία χρήσης :** Τα USB Tokens μπορούν εύκολα να μεταφέρονται. Συνδέονται εύκολα με το υπολογιστή μέσω USB θύρας και δεν απαιτούν επιπρόσθετο εξοπλισμό. Βοηθούν το χρήστη να μη χρειάζεται να απομνημονεύει πολλούς κωδικούς, αφού τα αναγνωριστικά του αποθηκεύονται με ασφάλεια στο token.

### ➢ Έξυπνες κάρτες και ψηφιακά πιστοποιητικά

Και στην περίπτωση των έξυπνων καρτών ισχύουν τα πλεονεκτήματα που αναφέρθηκαν στην προηγούμενη παράγραφο. Ωστόσο καλό είναι να εξετασθούν

και τα αβαντάζ από τον συνδυασμό τα πιστοποίησης δύο παραγόντων και της PKI τεχνολογίας, σε σχέση μόνο με την χρήση PKI.

• **Τρωτότητα :** Η αποθήκευση των κλειδιών και των ψηφιακών πιστοποιητικών στους σκληρούς δίσκους των υπολογιστών έχει αρκετά μειονεκτήματα, όπως καταστροφή του υλικού, δυσκολία στις αναβαθμίσεις λογισμικού, μεγαλύτερες πιθανότητες υποκλοπής.

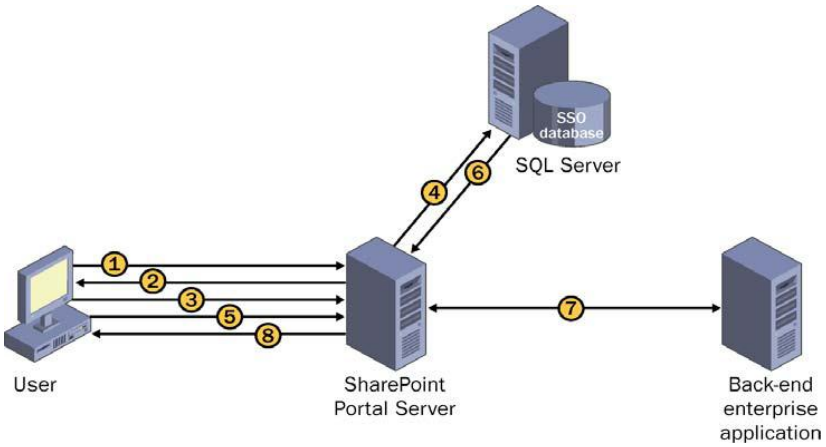
• **Ευελιξία- Φορητότητα :** Τόσο τα Tokens όσο και οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν και σε άλλες εφαρμογές που δεν γίνονται launch αποκλειστικά μέσω του υπολογιστή του χρήστη, όπως για παράδειγμα ATMs, αλλά μπορούν να χρησιμοποιηθούν και από οποιοδήποτε άλλο υπολογιστή πλην αυτού που έχει ο χρήστης.

## 6.6 Single Sign On (SSO)

Καθώς τα IT συστήματα πολλαπλασιάζονται για να υποστηρίξουν τις επιχειρηματικές διαδικασίες, οι χρήστες και οι διαχειριστές τους αντιμετωπίζουν ένα αυξανόμενο πολύπλοκο περιβάλλον για να ολοκληρώσουν τις εργασίες τους.

Προβλήματα αντιμετωπίζουν και οι διαχειριστές (administrators) των συστημάτων που πρέπει να διαχειρίζονται λογαριασμούς χρηστών μέσα σε κάθε σύστημα και να εξασφαλίζουν την ακεραιότητα επιβολής της πολιτικής ασφάλειας *(Αγγέλης, 2005)*.

Η παραδοσιακή λύση για την πρόσβαση σε πολλαπλά συστήματα είναι η παροχή διαφορετικών κωδικών για είσοδο σε όλα τα domains, primary και secondary. Συνεπώς, ο χρήστης που έχει καταχωρήσει τα αναγνωριστικά του στο primary domain, δεν μπορεί να αιτηθεί υπηρεσίες από τα secondary παρά μόνο εισάγοντας κωδικούς χρήσης για την πρόσβαση σε αυτά.




**Πηγή φωτογραφίας:** ***Από το διαδίκτυο,*** **www.blogs.developpeur.com**

Η συγκεκριμένη προσέγγιση, τόσο από άποψη χρηστικότητας, όσο και από άποψη ασφάλειας, δίνει αφορμή για την ανάγκη συντονισμού και ενοποίησης όπου αυτό είναι δυνατό, των λειτουργιών εισόδου των χρηστών και των λειτουργιών διαχείρισης των λογαριασμών των χρηστών, ώστε αυτές να βρίσκονται σε ένα ενιαίο περιβάλλον μέσα στον οργανισμό.

Μία υπηρεσία που παρέχει τέτοιο συντονισμό και ενοποίηση, δίνει πολλά πλεονεκτήματα όπως :

• Μείωση του χρόνου που καταναλώνουν οι χρήστες για είσοδο σε διαφορετικές υπηρεσίες.

• Μείωση της πιθανότητας λαθών στις διαδικασίες sign on.

• Βελτίωση της ασφάλειας εξαιτίας του γεγονότος ότι ο χρήστης δεν χρειάζεται να διατηρεί και να θυμάται πολλά sets κωδικών.

• Μείωση του χρόνου διαχείρισης λογαριασμών χρηστών, για τους administrators.

• Βελτίωση της ασφάλειας μέσω της ενσωματωμένης δυνατότητας για τους administrators να συντηρούν την ακεραιότητα της δομής διαχείρισης χρηστών.

Τέτοιου είδους υπηρεσία καλείτε single Sign On. Το σύστημα συλλέγει όλη την πληροφορία του sign on στο primary domain, που περιλαμβάνει όλα τα αναγνωριστικά που απαιτούνται για secondary domains. Η πληροφορία αυτή που δίνει ο χρήστης, χρησιμοποιείται από την SSO υπηρεσία ώστε να πιστοποιεί τον χρήστη κάθε φορά που αυτός αλληλεπιδρά με άλλα domains.

Από άποψη διαχείρισης το μοντέλο SSO, προσφέρει ένα περιβάλλον διαχείρισης μοναδικών λογαριασμών χρηστών, μέσω του οποίου όλα τα domains διαχειρίζονται και συντονίζονται με ένα συγκεκριμένο τρόπο.

Σημαντικά θέματα ασφάλειας σχετικά με το SSO είναι :

• Το secondary domain πρέπει να εμπιστεύεται το primary domain ώστε :

- Να διαβεβαιώνουν ορθά την ταυτότητα και τα αναγνωριστικά πιστοποίησης του χρήστη
- Να προστατεύουν τα αναγνωριστικά πιστοποίησης που χρησιμοποιούνται για την επαλήθευση της ταυτότητας του χρήστη στο secondary domain από μη εγκεκριμένη χρήση

• Τα αναγνωριστικά πιστοποίησης πρέπει να προστατεύονται όταν μεταδίδονται μεταξύ primary και secondary domain απέναντι σε απειλές υποκλοπής που μπορούν να οδηγήσουν σε καλά καλυμμένες επιθέσεις.

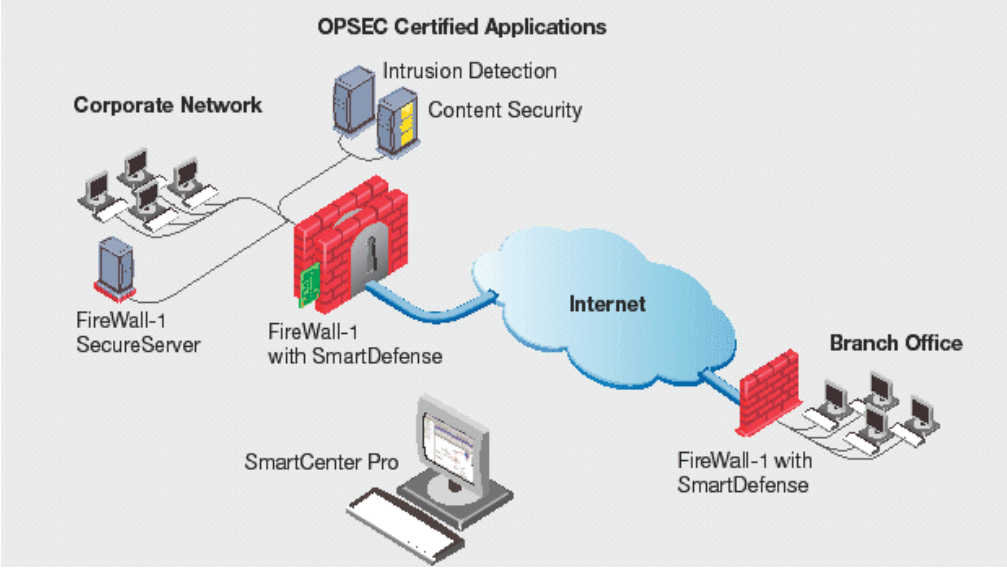
## 6.7 Firewalls

Ο όρος firewall έχει επικρατήσει τα τελευταία χρόνια σαν ένας από τους πιο καλούς τρόπους για να διατηρήσει κάποιος ασφαλή τα δεδομένα του στον υπολογιστή του, όταν αυτός είναι συνδεδεμένος στο διαδίκτυο. Το firewall, ή αλλιώς ο τοίχος της φωτιάς, είναι ένα λογισμικό το οποίο αναλαμβάνει να ελέγχει όλες τις πληροφορίες που φθάνουν στον υπολογιστή μας από τον "έξω" κόσμο. Το firewall μπορεί να είναι εκτός από software και hardware, μια συσκευή δηλαδή που τοποθετείται στην σύνδεση του ηλεκτρονικού υπολογιστή με το διαδίκτυο *(Βενέτης, 2007)*.

Στην περίπτωση που έχουμε εγκαταστήσει ένα λογισμικό firewall στον προσωπικό μας υπολογιστή τότε με αυτό μπορούμε να καθορίσουμε από ποιους υπολογιστές και με ποιους τρόπους θα δεχόμαστε πληροφορίες. Αυτό επιτυγχάνεται με την χρήση διάφορων φίλτρων τα οποία αναλύουν τα εισερχόμενα πακέτα και ανάλογα με τις οδηγίες που υπάρχουν τα αφήνουν να περάσουν ή όχι.

Η μεγάλη σημασία του firewall έγκειται στο ότι δεν μπορούμε να γνωρίζουμε απόλυτα τι λογισμικά υπάρχουν εγκατεστημένα στον υπολογιστή μας και ποιες "πόρτες" είναι ανοιχτές. Για παράδειγμα ο υπολογιστής μας μπορεί να είναι μολυσμένος από ένα worm το οποίο δίνει τη δυνατότητα σε κάποιον άλλο υπολογιστή να χρησιμοποιεί το CPU μας!

Το firewall δηλαδή είναι αυτό που συγκεντρώνει τον πλήρη έλεγχο των πακέτων που εισέρχονται στον υπολογιστή αποτελώντας ουσιαστικά έναν πύργο ελέγχου της πληροφορίας. Βέβαια η σημασία του firewall είναι πολύ πιο μεγάλη όταν πίσω από αυτό δεν υπάρχει μόνο ένας υπολογιστής αλλά μια μεγάλη ομάδα υπολογιστών π.χ. μια εταιρία, η οποία εμπιστεύεται το firewall για όλα τα πακέτα που καταφθάνουν σε αυτήν.




**Πηγή φωτογραφίας:** ***Βενέτης Χ., Μάιος 2007, Personal Firewalls***

# Κεφάλαιο 7.

## Έρευνες για το e-Banking στην Ελλάδα

Πολλές είναι οι έρευνες οι οποίες έχουν λάβει χώρα εντός αλλά και εκτός των ελληνικών συνόρων, για το e-Banking, με σκοπό, να ενημερώσουν τους καταναλωτές για τα πλεονεκτήματα που προσφέρει η χρήση του, αλλά και για να παρουσιάσουν τις υπηρεσίες τις οποίες προσφέρει, το ποσοστό του κοινού που το χρησιμοποιεί, και τους λόγους για τους οποίους μία μεγάλη μερίδα ακόμα δεν το χρησιμοποιεί κ.α.

Παρακάτω ακολουθεί μία συνοπτική παρουσίαση κάποιων ερευνών που έλαβαν χώρα στην Ελλάδα.

### 7.1 Το e- Banking στην Ελλάδα

Το e-banking εμφανίζει σημαντική αύξηση των ποσοστών συμμετοχής στη χώρα μας. Η χρήση των υπηρεσιών της ηλεκτρονικής τραπεζικής στην Ελλάδα κάθε χρόνο αυξάνεται κατά 100%. Αυτό δεν σημαίνει ότι δεν αντιμετωπίζει ακόμη προβλήματα που αναμένεται να λυθούν προοδευτικά παράλληλα με την ανάπτυξη του internet στην Ελλάδα.

Η διείσδυση της ηλεκτρονικής τραπεζικής παραμένει χαμηλή, καθώς ακόμη πολλοί πελάτες τραπεζών είτε δεν είναι εξοικειωμένοι με την τεχνολογία, είτε προτιμούν ακόμη την παραδοσιακή μέθοδο συναλλαγών του «γκισέ».

Ωστόσο, τα εμπόδια που ανακύπτουν στην διαδικασία ανάπτυξης του e-banking δεν φαίνονται ικανά να περιορίσουν τη δυναμική του φαινομένου, καθώς τόσο τα χρηματοπιστωτικά ιδρύματα, όσο και οι καταναλωτές αντιλαμβάνονται ότι το μέλλον των τραπεζικών συναλλαγών περνά από το διαδίκτυο.

Εκτιμήσεις που έγιναν πριν τέσσερα χρόνια, ανέφεραν ότι τα τραπεζικά ιδρύματα που δεν θα εκμεταλλευτούν τις νέες τεχνολογίες για την επέκταση των εργασιών τους, θα χάσουν μέχρι και το 50% της χρηματιστηριακής αξίας τους.

Σύμφωνα με τα στοιχεία της Τράπεζας της Ελλάδος και της Ένωσης Ελληνικών τραπεζών, το 2005 περίπου 300.000 Έλληνες (3% του συνολικού πληθυσμού), χρησιμοποιούσαν το e-banking, ενώ την επόμενη χρονιά αυξήθηκαν στους 421.000 και το 2007 οι συνδρομητές του e-banking ξεπέρασαν τους 500.000

(βλ. πίνακα 2). Σύμφωνα με εκτιμήσεις των τραπεζών, το 2005 ο τσίρος έφτασε τα 20 δις Euro. Το 2006 τα ποσό αυτό αυξήθηκε σε 28 δις , ενώ το 2007 έφτασε τα 36 δις Euro.

**Πίνακας 2. Χρήστες και συναλλαγές μέσω Διαδικτύου.**

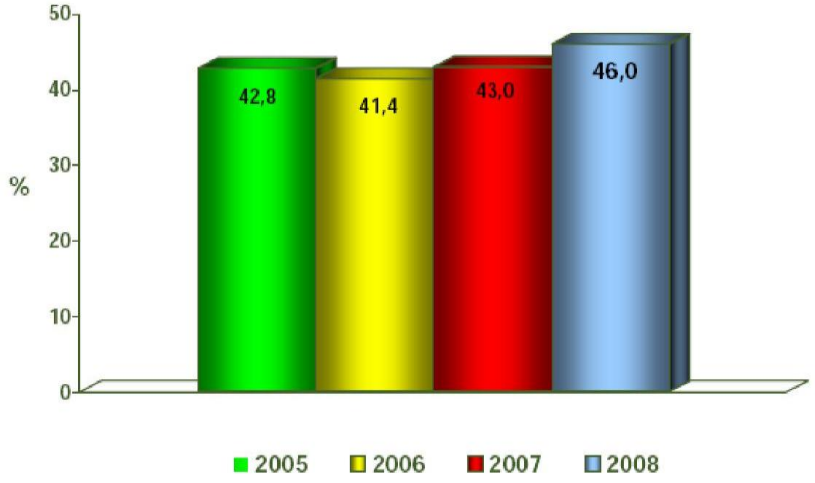
| ΤΡΑΠΕΖΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ ΜΕΣΩ INTERNET | | | |
|---|---|---|---|
| **ΕΤΟΣ** | **ΧΡΗΣΤΕΣ** | **ΑΡΙΘΜΟΣ ΣΥΝΑΛΛΑΓΩΝ** | **ΤΖΙΡΟΣ (δις €)** |
| 2005 | 300.000 | 4.000.000 | 20 |
| 2006 | 421.000 | 5.149.689 | 28 |
| 2007 | 500.000 | 7.000.000 | 36 |

**Πηγή:** ***Περιοδικό Ram Οκτωβρίου 2007, τεύχος 184, σελ 122.***

Σύμφωνα όμως, με τα στοιχεία που προέκυψαν από έρευνα που διεξήχθη από το Money Show για το έτος 2007, υπάρχουν περίπου 80 εκατομμύρια e-Bankers στην Ευρωπαϊκή Ένωση *(πηγή Forrester)*.

Παρατηρώντας το παρακάτω γράφημα (6) βλέπουμε ότι υπάρχει σταθερότητα στη χρήση του e-banking την τελευταία τετραετία.

**Γράφημα 6. Χρήση e-Banking στην Ελλάδα την τελευταία τετραετία.**




**Βάση: Όσοι συμμετείχαν στην e-metrics**
**Πηγή:** ***έρευνα e-metrics, AGB Nielsen Media Research (2008)***

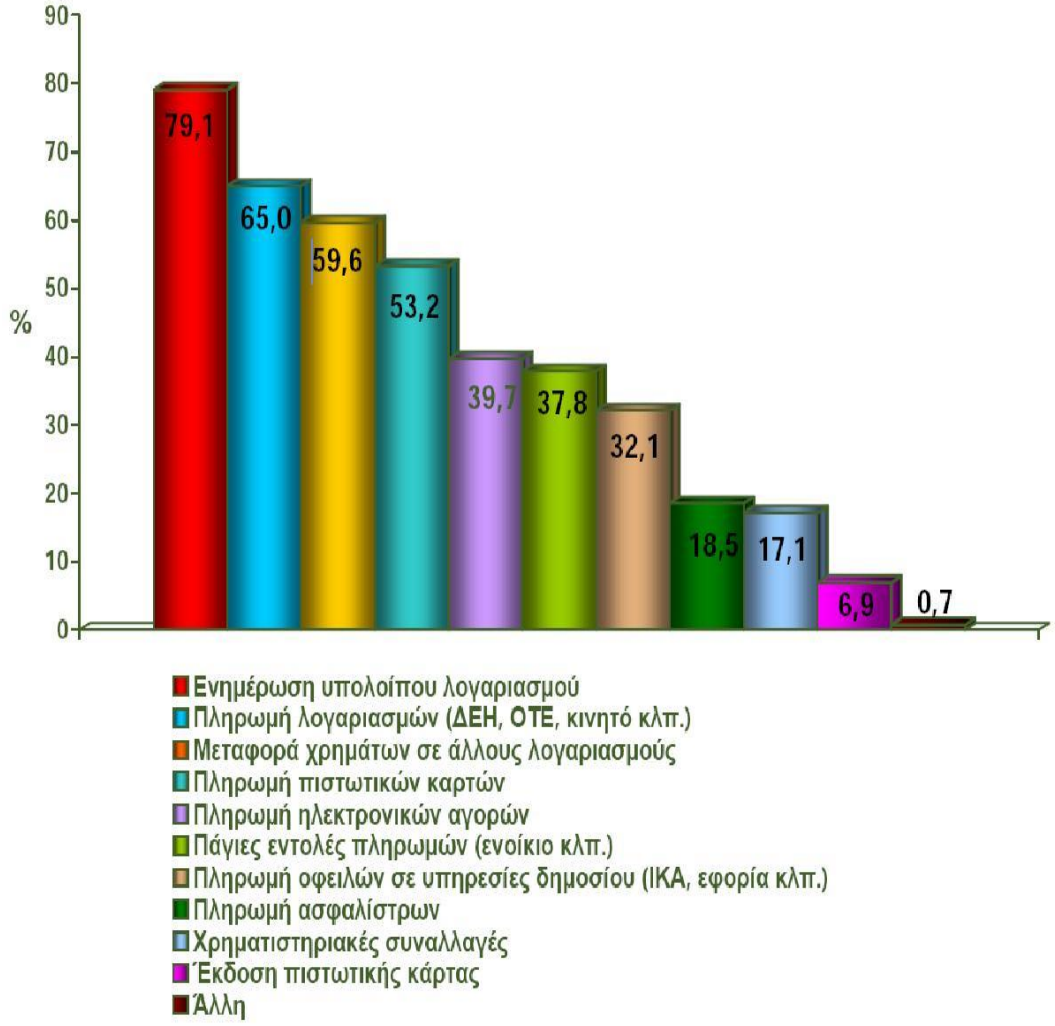
Σύμφωνα με την ίδια έρευνα, οι δημοφιλέστερες υπηρεσίες του e-Banking είναι :

- Ενημέρωση υπολοίπου λογαριασμού
- Μεταφορά χρημάτων σε άλλους λογαριασμούς
- Πληρωμή πιστωτικών καρτών
- Πληρωμή ηλεκτρονικών αγορών
- Πληρωμή οφειλών σε υπηρεσίες δημοσίου (ΙΚΑ, εφορία κλπ.)
- Πάγιες εντολές πληρωμών (ενοίκιο κλπ.)
- Χρηματιστηριακές συναλλαγές
- Πληρωμή ασφαλίστρων
- Έκδοση πιστωτικής κάρτας

Από τις παραπάνω υπηρεσίες, το μεγαλύτερο ποσοστό στην προτίμηση των χρηστών, καταλαμβάνουν κυρίως οι υπηρεσίες οι οποίες αφορούν πληροφοριακούς σκοπούς και όχι αυτές που αφορούν στη διενέργεια συναλλαγών.

Συνοπτικά θα μπορούσαμε να αναφέρουμε ότι το 79,1% των χρηστών, χρησιμοποιεί το e- banking για ενημέρωση του υπολοίπου του λογαριασμού του, το 59,6% για μεταφορά χρημάτων σε άλλους λογαριασμούς, ενώ μόλις το 17,1% για χρηματιστηριακές συναλλαγές και το 6,9% για έκδοση πιστωτικών καρτών.

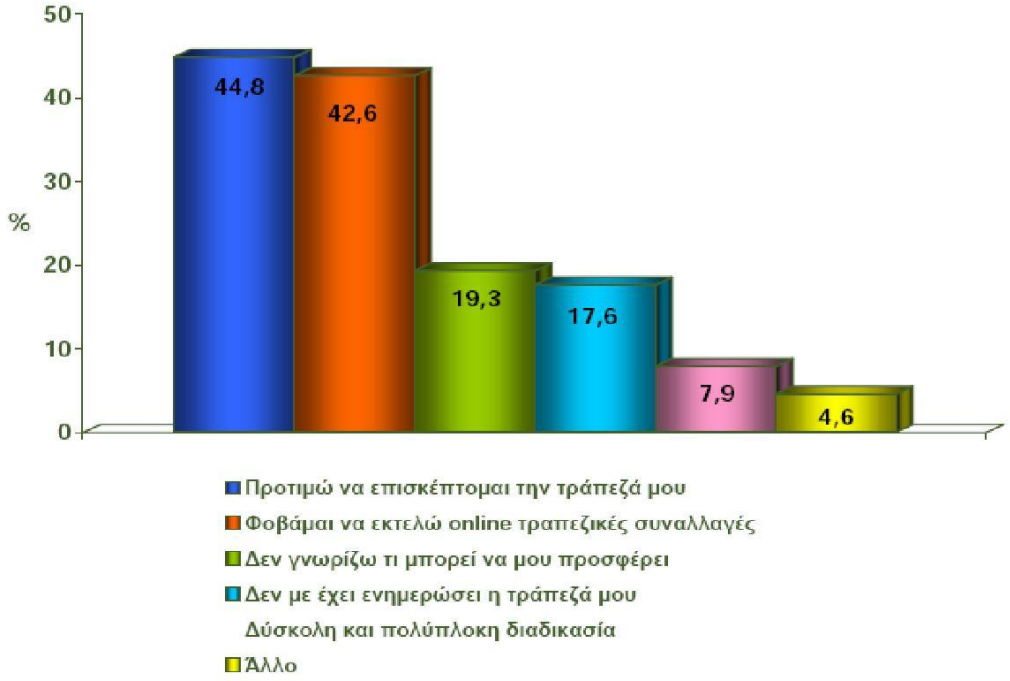
**Γράφημα 7. Δημοφιλέστερες υπηρεσίες του e- Banking.**




**Βάση: Όσοι συμμετείχαν στην e-metrics**
**Πηγή:** ***έρευνα e-metrics, AGB Nielsen Media Research (2008)***

Αρκετοί όμως είναι και οι λόγοι οι οποίοι συντελούν στην αποφυγή της χρήσης του e-banking. Το μεγαλύτερο ποσοστό, 44,8%, καταλαμβάνει, ο φόβος εκτέλεσης online τραπεζικών συναλλαγών. Παρακάτω ακολουθεί αναλυτικό γράφημα (8) στο οποίο παρατίθενται αναλυτικά οι κυριότεροι φόβοι των χρηστών.

**Γράφημα 8. Λόγοι Αποφυγής e-Banking από Έλληνες χρήστες.**




**Βάση: Όσοι συμμετείχαν στην e-metrics**
**Πηγή:** ***έρευνα e-metrics, AGB Nielsen Media Research (2008)***

Ευρύτεροι λόγοι μη χρήσης του e- banking είναι :

- Ευρύτερη δυσχέρεια με την τεχνολογία Η/Υ & internet
- Ελλιπής πληροφόρηση / προώθηση από τις Τράπεζες
- Φόβοι υποκλοπής δεδομένων / απώλειας χρημάτων
- Έλλειψη ικανού κινήτρου
  - Μείωση Κόστους Συναλλαγών
  - Αποκλειστική Προσφορά Περισσότερων Συναλλαγών
- Ευχαριστημένοι με το κατάστημα ή το ΑΤΜ
  - Π.χ. Προσωπική Επαφή με το προσωπικό του καταστήματος
- Φόβος αλλαγής συνήθειας

## 7.2 Ελληνικές τράπεζες και e-Banking

Το e-banking είναι μια σχετικά νέα υπηρεσία των τραπεζών και ο χρήστης δεν είναι απόλυτα εξοικειωμένος με την εφαρμογή του. Σπουδαίο ρόλο λοιπόν παίζει, το πόσο εύκολο γι' αυτόν είναι να πραγματοποιεί μεταφορές κεφαλαίων μεταξύ λογαριασμών, να πληρώνει την πιστωτική του κάρτα ή το δάνειο, να στέλνει εμβάσματα και γενικά να εκτελεί όλες τις εργασίες .

Οι τράπεζες για να βοηθήσουν το χρήστη έχουν καταχωρίσει στις σελίδες τους demo εκμάθησης των υπηρεσιών.

Από τα demo που ξεχώρισαν είναι αυτό της Εθνικής. Εδώ ο χρήστης πραγματοποιεί όλες τις προσφερόμενες υπηρεσίες του e-banking με εικονικούς λογαριασμούς και στοιχεία, προκειμένου να εξοικειωθεί με το περιβάλλον εργασίας. Επίσης καλό demo διαθέτει η Εμπορική. Η Aspis bank, η Citibank και η Marfin Egnatia Bank δίνουν μέσα από τα demo τους πληροφορίες σχετικά με τις διαδικασίες ολοκλήρωσης της κάθε συναλλαγής, έτσι ο χρήστης καλείται να μελετήσει και να συγκρατήσει τον τρόπο εκτέλεσης τους *(Χανιωτάκη, 2007)*.

Θα πρέπει να επισημάνουμε ότι όλες οι τράπεζες έχουν δημιουργήσει στις ιστοσελίδες τους τέτοιο περιβάλλον εργασίας ώστε η εκτέλεση των συναλλαγών να είναι εύκολη για κάθε τύπο χρήστη.

Η πλοήγηση είναι γρήγορη και εύκολη σε όλες τις τράπεζες. Κάθε link ανοίγει καινούργιο παράθυρο με νέες επιλογές και έτσι γίνεται μια αλυσίδα μέχρι ο χρήστης να φτάσει στο επιθυμητό αποτέλεσμα.

Με βάση το κριτήριο των προσφερόμενων υπηρεσιών, αξιολογήθηκαν για το πλήθος των υπηρεσιών που θα πρέπει να έχει μια ιδανική εφαρμογή. Η κίνηση και το υπόλοιπο των λογαριασμών υποστηρίζονται από όλες τις τράπεζες. Άλλες πάλι όπως η υποστήριξη δανείων, παρέχονται από κάποιες μόνο.

Θα πρέπει να επισημάνουμε επίσης, ότι ολοένα και περισσότερες υπηρεσίες προστίθενται από τις τράπεζες για την εξυπηρέτηση των πελατών τους. Η τράπεζα η οποία ξεχωρίζει για το πλήθος των υπηρεσιών που προσφέρει είναι η Win bank του ομίλου Πειραιώς και την ακολουθούν η Alpha bank και Eurobank. Η Win bank είναι και η μόνη τράπεζα που δίνει την δυνατότητα ανοίγματος λογαριασμού ηλεκτρονικά.

Η Citibank με τη Marfin Egnatia Bank καταλαμβάνουν τις τελευταίες θέσεις καθώς παρέχουν περιορισμένες υπηρεσίες, ιδιαίτερα αυτές που αφορούν τις

επενδύσεις αλλά και τις διάφορες ηλεκτρονικές αιτήσεις (αλλαγής password, παραγγελία δανείου, πιστωτικής κάρτας).

Άξιο αναφοράς είναι ότι όλες οι τράπεζες υστερούν στην αποστολή εμβασμάτων ιδιαίτερα του εξωτερικού.

Η υλοποίηση της ασφάλειας των συναλλαγών είναι διαφορετική ανάλογα την τράπεζα. Η Εθνική και η Marfin Egnatia Bank διαθέτουν το σύστημα, με τους αριθμούς επικύρωσης των συναλλαγών TAN. Η Eurobank χρησιμοποιεί ένα διαφορετικό σύστημα δίνοντας στον πελάτη τη δυνατότητα να εκτελεί τραπεζικές συναλλαγές ταυτόχρονα μόνο από δύο υπολογιστές.

Μαζί με τους κωδικούς πρόσβασης ο πελάτης θα παραλάβει ένα κωδικό με τον αριθμό του πιστοποιητικού. Μόλις ξεκινήσει τις συναλλαγές για πρώτη φορά η εφαρμογή θα εγκαταστήσει το πιστοποιητικό στον σκληρό δίσκο του υπολογιστή. Με αυτόν τον τρόπο είναι ακόμα πιο δύσκολο να περιέλθουν οι κωδικοί σε λάθος χέρια.

Από την άλλη ο πελάτης περιορίζεται ως προς τη χρήση πρόσθετων υπολογιστών, όπως στην περίπτωση ενός φορητού υπολογιστή. Για να γίνει θα πρέπει να απενεργοποιηθεί το πιστοποιητικό και να εγκατασταθεί εκ νέου στο φορητό.

Τα τελευταία χρόνια οι τράπεζες άρχισαν να χρεώνουν τις πιο χρήσιμες συναλλαγές, όπως είναι τα εμβάσματα και οι πληρωμές πιστωτικών καρτών άλλων τραπεζών. Πάντως η προμήθεια μέσω του e-banking είναι μικρότερη – φτάνει συνήθως το 50%- από ότι στο γκισέ. Ο υπολογισμός στις προμήθειες που χρεώνουν οι τράπεζες για εμβάσματα και άλλες εγχρήματες συναλλαγές είναι ένα σύνθετο έργο, ειδικότερα όσον αφορά το e-banking.

Το e-banking άρχισε να εφαρμόζεται από τις τράπεζες με σκοπό της εξυπηρέτηση των πελατών τους από το σπίτι, απαλλάσσοντας τους από την ταλαιπωρία και την καθυστέρηση που δημιουργείται στα ταμεία τους.

Βέβαια σημαντικό είναι, πέρα από αυτό, η εφαρμογή να είναι διαθέσιμη 24 ώρες το 24ωρο, 365 μέρες το χρόνο. Αρχικά η δυνατότητα αυτή δεν ήταν διαθέσιμη από όλες τις τράπεζες, τώρα πια το e-banking λειτουργεί 24 ώρες, κάθε μέρα. Υπάρχουν βέβαια υπηρεσίες, που εκτελούνται συγκεκριμένες ώρες, όπως π.χ. η πληρωμή των τελών κυκλοφορίας από την Alpha bank, γίνεται τις εργάσιμες ημέρες κατά τις ώρες 7:30 με 11:00.

Εδώ θα πρέπει να τονίσουμε ότι ξεχωριστό χαρακτηριστικό των τραπεζών, είναι η δυνατότητα να παρέχουν τεχνική υποστήριξη και help desk 24 ώρες το 24ωρο, καθώς δεν είναι λίγες οι φορές που αντιμετωπίζει κανείς ένα πρόβλημα που μπορεί να οφείλεται είτε στη γραμμή του internet, είτε στην ίδια την τράπεζα ή ακόμα και στον απλό χρήστη. Όλες πάντως οι τράπεζες διαθέτουν τηλέφωνο ανάγκης, φυσικά χωρίς χρέωση. Για κάποιον πάντως που θέλει να πάρει πληροφορίες για οτιδήποτε και όχι άμεσα μπορεί να στείλει e-mail στην τράπεζα και να έχει απάντηση μέσα σε σύντομο χρονικό διάστημα.

Παρακάτω παρατίθεται ένας πίνακας με τις υπηρεσίες του e-banking και ποιες από αυτές υποστηρίζονται από την κάθε τράπεζα *(Χανιωτάκη, 2007)*.

**Πίνακας 3. Προσφερόμενες υπηρεσίες των τραπεζών που δραστηριοποιούνται στην Ελλάδα.**

| ΤΡΑΠΕΖΕΣ | EURO BANK | WIN BANK | MARFIN EGNATIA BANK | ALPHA BANK | ΕΜΠΟΡΙΚΗ | ASPIS | ΕΘΝΙΚΗ | CITI BANK |
|---|---|---|---|---|---|---|---|---|
| ΠΡΟΣΦΕΡΟΜΕΝΕΣ ΥΠΗΡΕΣΙΕΣ | | | | | | | | |
| **ΛΟΓΑΡΙΑΣΜΟΙ** | | | | | | | | |
| Κινήσεις | √ | √ | √ | √ | √ | √ | √ | √ |
| Υπόλοιπο | √ | √ | √ | √ | √ | √ | √ | √ |
| Πληροφορίες | √ | √ | √ | √ | √ | √ | √ | √ |
| Ενημέρωση για IBAN | | √ | | | √ | √ | | |
| **ΠΛΗΡΩΜΕΣ** | | | | | | | | |
| ΔΕΗ | √ | √ | √ | √ | √ | | √ | |
| ΟΤΕ | √ | √ | √ | √ | √ | √ | | |
| ΕΥΔΑΠ | | | √ | √ | √ | | | |
| ΦΠΑ | √ | √ | √ | √ | √ | | √ | |
| ΤΕΒΕ/ ΙΚΑ | √ | √ | √ | √ | √ | | √ | |
| Κινητή τηλεφωνία | | √ | √ | √ | | | | |
| Σταθερή τηλεφωνία | √ | √ | √ | √ | √ | | | |
| **ΠΑΓΙΕΣ ΕΝΤΟΛΕΣ** | | | | | | | | |
| ΔΕΗ/ΟΤΕ | √ | √ | √ | √ | √ | | | |
| ΕΥΔΑΠ | √ | √ | √ | √ | √ | | | |
| ΤΕΒΕ | √ | √ | √ | √ | √ | | | |
| Κινητή τηλεφωνία | √ | √ | √ | √ | √ | | | |
| Σταθερή τηλεφωνία | √ | | | | √ | | | |
| **ΕΜΒΑΣΜΑΤΑ** | | | | | | | | |
| Σε λογ/μό ιδίου στην ίδια τράπεζα | √ | √ | √ | √ | √ | √ | √ | √ |
| Σ λογ/μό άλλου στην ίδια τράπεζα | √ | √ | √ | √ | | √ | √ | √ |
| Σε άλλη τράπεζα | √ | √ | √ | √ | √ | √ | √ | √ |
| Στο εξωτερικό | √ | √ | √ | √ | √ | √ | √ | |
| Πληρωμή πιστωτικών καρτών άλλης τράπεζας | √ | √ | | √ | | | | |
| **ΔΑΝΕΙΑ** | | | | | | | | |
| Υπόλοιπο | √ | √ | | √ | | √ | | |
| Πληρωμή | √ | √ | | √ | | | | |
| Κινήσεις | √ | √ | | | | | | |
| **ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ** | | | | | | | | |
| Υπόλοιπο | √ | √ | √ | √ | √ | √ | √ | √ |
| Πληρωμή | √ | √ | √ | √ | √ | √ | √ | √ |
| Αμεσότητα συναλλαγών | √ | | | | | | | √ |

| ΤΡΑΠΕΖΕΣ | EURO BANK | WIN BANK | MARFIN EGNATIA BANK | ALPHA BANK | ΕΜΠΟΡΙΚΗ | ASPIS | ΕΘΝΙΚΗ | CITI BANK |
|---|---|---|---|---|---|---|---|---|
| ΠΡΟΣΦΕΡΟΜΕΝΕΣ ΥΠΗΡΕΣΙΕΣ | | | | | | | | |
| ΕΠΙΤΑΓΕΣ | | | | | | | | |
| Βιβλιάριο επιταγών | √ | √ | √ | √ | √ | √ | √ | √ |
| Παρακολούθηση επιταγής | | | | | | √ | | |
| Ακύρωση επιταγής | √ | √ | √ | | | | | |
| ΕΚΤΥΠΩΣΕΙΣ | | | | | | | | |
| Σε απλό κείμενο | | √ | | | √ | | √ | √ |
| Σε μορφή ιστοσελίδας | √ | √ | √ | √ | √ | √ | | √ |
| Σε acrobat reader | | | | | | | √ | |
| Εκτύπωση με χρονοσφραγίδα | | √ | | | | | √ | |
| ΧΡΗΜΑΤΙΣΤΗΡΙΟ | | | | | | | | |
| Τιμές μετοχών | √ | √ | √ | √ | √ | √ | √ | |
| Αγορά-Πώληση Μετοχής | √ | √ | | | √ | √ | √ | |
| Ανάκληση αγοράς-πώλησης μετοχής | √ | | | | | | √ | |
| Κίνηση χαρτοφυλακίου | √ | √ | √ | √ | √ | √ | √ | |
| Συναλλαγές | √ | √ | √ | √ | √ | √ | √ | |
| ΑΣΦΑΛΕΙΑ | | | | | | | | |
| Αλλαγή κωδικού | | √ | | √ | | | | √ |
| Αλλαγή PIN | √ | √ | √ | √ | √ | √ | √ | √ |
| Παραγγελία TAN | | | √ | | | | √ | |
| ΔΙΑΘΕΣΙΜΟΤΗΤΑ | | | | | | | | |
| Ημέρες ONLINE | Κάθε μέρα | Κάθε μέρα | Κάθε μέρα | Κάθε μέρα | Κάθε μέρα | Κάθε μέρα | Κάθε μέρα | Κάθε μέρα |
| Ώρες λειτουργίας | 24 ώρες | 24 ώρες | 24 ώρες | 24 ώρες | 24 ώρες | 24 ώρες | 24 ώρες | 24 ώρες |
| ΑΛΛΕΣ ΥΠΗΡΕΣΙΕΣ | | | | | | | | |
| Εγγραφή στο e-banking | | √ | √ | √ | √ | | | |
| Δήλωση –απώλεια κλοπής πιστωτικής κάρτας | | | | | √ | | | |
| Αλλαγή προσωπικών στοιχείων | √ | √ | | √ | √ | √ | | |
| Πληρωμή τελών κυκλοφορίας | | | √ | √ | | √ | | |
| Άνοιγμα λογ/μου καταθέσεων | | √ | | | | | | |

# Κεφάλαιο 8.

## Πρωτογενής Έρευνα για την Ηλεκτρονική Τραπεζική στην Ελλάδα

Στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας, πραγματοποιήθηκε έρευνα για το e- Banking στην Ελλάδα με την μέθοδο των ερωτηματολογίων, τα οποία στάλθηκαν μέσω ηλεκτρονικού ταχυδρομείου ή δόθηκαν χειρόγραφα σε τράπεζες και χρήστες. Η έρευνα διήρκησε περίπου δύο μήνες και χωρίστηκε σε δύο μέρη.

Το πρώτο μέρος, αφορά στη συλλογή στοιχείων σχετικά με την παροχή υπηρεσιών Internet Banking από τις τράπεζες στην Ελλάδα μέσω ερωτηματολογίων (Παράρτημα 6) . Συγκεκριμένα εξετάστηκε η στάση των ελληνικών τραπεζών απέναντι σε αυτό το νέο μέσο παροχής υπηρεσιών, οι προσφερόμενες υπηρεσίες από κάθε οργανισμό καθώς και η ικανοποίηση από την ανταπόκριση των πελατών τους. Επίσης, εξετάστηκε η άποψη και η γνώση που έχουν πάνω στις απειλές ασφαλείας και τους κινδύνους που μπορεί να εγκυμονεί η χρήση του e-banking, τις μεθόδους προστασίας που υιοθετούν για την ασφάλεια των πελατών τους καθώς επίσης και η γνώση τους πάνω στις νέες τεχνολογίες για την προσφορά τραπεζικών υπηρεσιών . Σε αυτό το κομμάτι της έρευνας, ερωτήθηκαν οκτώ Τράπεζες οι οποίες είναι οι εξής : Eurobank, Win Bank, Marfin Egnatia Bank, Alpha Bank, Εμπορική Τράπεζα, ASPIS, Εθνική Τράπεζα και Citi Bank.

Το δεύτερο μέρος της έρευνας έχει σκοπό τη συλλογή στοιχείων μέσω ερωτηματολογίων (Παράρτημα 7), σχετικά με την αποδοχή και το βαθμό ικανοποίησης των Ελλήνων χρηστών. Συγκεκριμένα διερευνήθηκε το προφίλ των Ελλήνων χρηστών του διαδικτύου που χρησιμοποιούν τις ηλεκτρονικές υπηρεσίες των τραπεζών, οι προσφερόμενες υπηρεσίες από τους οργανισμούς καθώς και ο βαθμός ικανοποίησης τους από το νέο αυτό μέσο συναλλαγών. Ακόμα, εξετάστηκαν οι λόγοι αμφισβήτησης που επικαλούνται οι μη χρήστες της ηλεκτρονικής τραπεζικής καθώς και οι γνώσεις των χρηστών πάνω στις νέες τεχνολογίες, τους κινδύνους και την ασφάλεια που προσφέρει το e-banking.

Οι απαντήσεις που λάβαμε στο κομμάτι της έρευνας που απευθύνεται στους χρήστες της ηλεκτρονικής τραπεζικής, ανήλθαν στις εκατόν είκοσι δύο. Απαντήσεις λάβαμε επίσης και από εκατόν σαράντα μη χρήστες.

Παρακάτω, καταγράφονται τα αποτελέσματα που προέκυψαν από τη συγκεκριμένη έρευνα.

## Μέρος Α - Τράπεζες

Αυτό το κομμάτι της έρευνας, όπως αναφέρθηκε και παραπάνω, απευθύνεται στις ελληνικές τράπεζες που παρέχουν στους πελάτες τους τη δυνατότητα να διαχειρίζονται τους λογαριασμούς τους μέσω e-banking.

Στο ερωτηματολόγιο που δημιουργήσαμε για την συγκεκριμένη έρευνα, προσπαθήσαμε να συμπεριλάβουμε ερωτήσεις που να καλύπτουν όλο το φάσμα των δυνατοτήτων που μπορεί να παρέχει μια τράπεζα στους πελάτες της, με σκοπό να δούμε ποιο είναι το επίπεδο της ηλεκτρονικής τραπεζικής στη Ελλάδα, τόσο από την πλευρά των παρεχόμενων υπηρεσιών, όσο και από την πλευρά της ασφάλειας των συναλλαγών και κατά συνέπεια των συναλλασσόμενων.

Σύμφωνα με τις απαντήσεις που έδωσαν οι υπεύθυνοι του e-banking κάθε τράπεζας, προέκυψαν τα παρακάτω αποτελέσματα.

### 8.1 e-Banking & προσφερόμενες υπηρεσίες

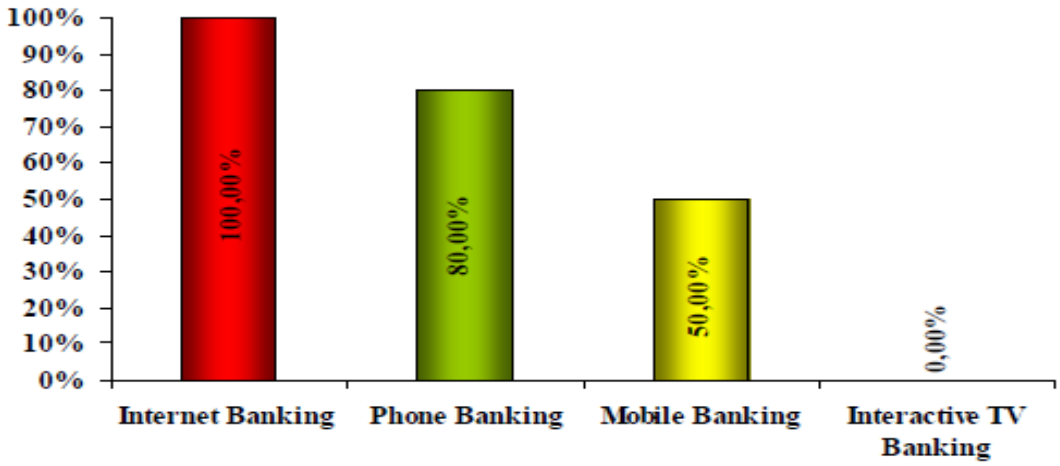
Αρχικά, θελήσαμε να μάθουμε ποια από τα είδη του e-banking (Internet Banking, Phone Banking, Mobile Banking και Interactive TV Banking), προσφέρουν οι περισσότερες ελληνικές τράπεζες, με σκοπό να διαπιστώσουμε, το επίπεδο της ηλεκτρονικής τραπεζικής στη χώρα μας, από πλευράς προσφερόμενων υπηρεσιών.

Σύμφωνα με τα αποτελέσματα που προέκυψαν από τις απαντήσεις που λάβαμε, παρατηρούμε ότι όλες οι τράπεζες που έλαβαν μέρος στην παρούσα έρευνα, προσφέρουν Internet Banking, οκτώ στις δέκα Phone Banking και μόλις πέντε στις δέκα Mobile Banking, ενώ καμία ελληνική τράπεζα, δεν παρέχει ακόμα Interactive TV Banking.

Με βάση τα παραπάνω αποτελέσματα, μπορούμε να πούμε, ότι οι περισσότερες εγχώριες τράπεζες, δίνουν τη δυνατότητα στους πελάτες τους, να χειρίζονται τους τραπεζικούς τους λογαριασμούς ηλεκτρονικά, είτε μέσω του διαδικτύου, είτε μέσω κάποιου σταθερού τηλεφώνου.

Ενώ, όπως μπορούμε να δούμε και στο γράφημα (9), οι υπηρεσίες Mobile Banking δεν είναι τόσο διαδεδομένες στην Ελλάδα, με συνέπεια προς το παρόν να το διαθέτουν λίγες τράπεζες.

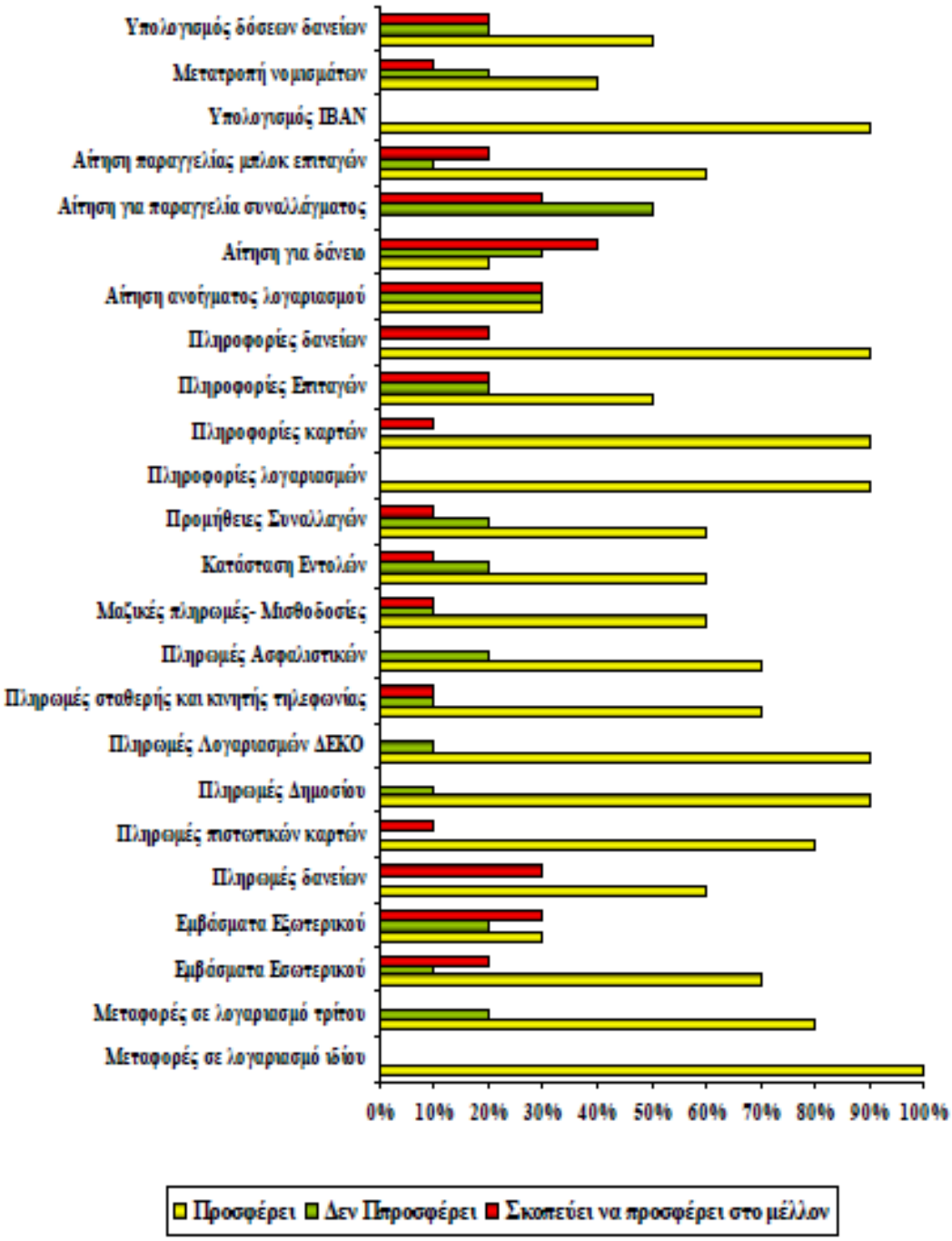
**Γράφημα 9. Είδη του Banking**



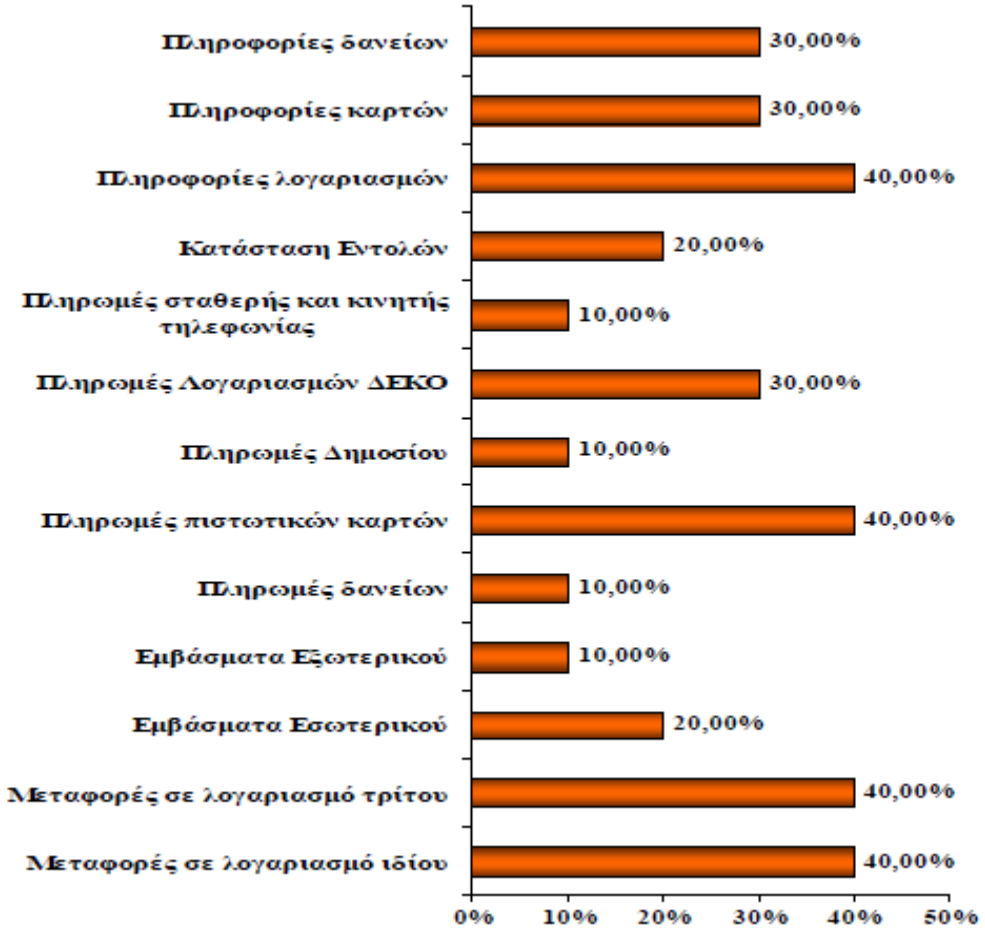

Οι υπηρεσίες που προσφέρονται από τις περισσότερες τράπεζες στο online Banking, καλύπτουν σχεδόν ολόκληρη των γκάμα των συναλλαγών που ο πελάτης θα πραγματοποιούσε και στο γκισέ της τράπεζας, όπως για παράδειγμα μεταφορές σε λογαριασμό ιδίου ή τρίτου, πληρωμές δημοσίου, επιταγών , δανείων, πληροφορίες λογαριασμών κ.α.

Παρακάτω ακολουθεί γράφημα (10), στο οποίο καταγράφονται οι υπηρεσίες που προσφέρονται από τις ελληνικές τράπεζες , καθώς επίσης και γράφημα (11) με τις υπηρεσίες που προσφέρονται από όσες τράπεζες παρέχουν Mobile Banking.

**Γράφημα 10. Υπηρεσίες e-Banking**



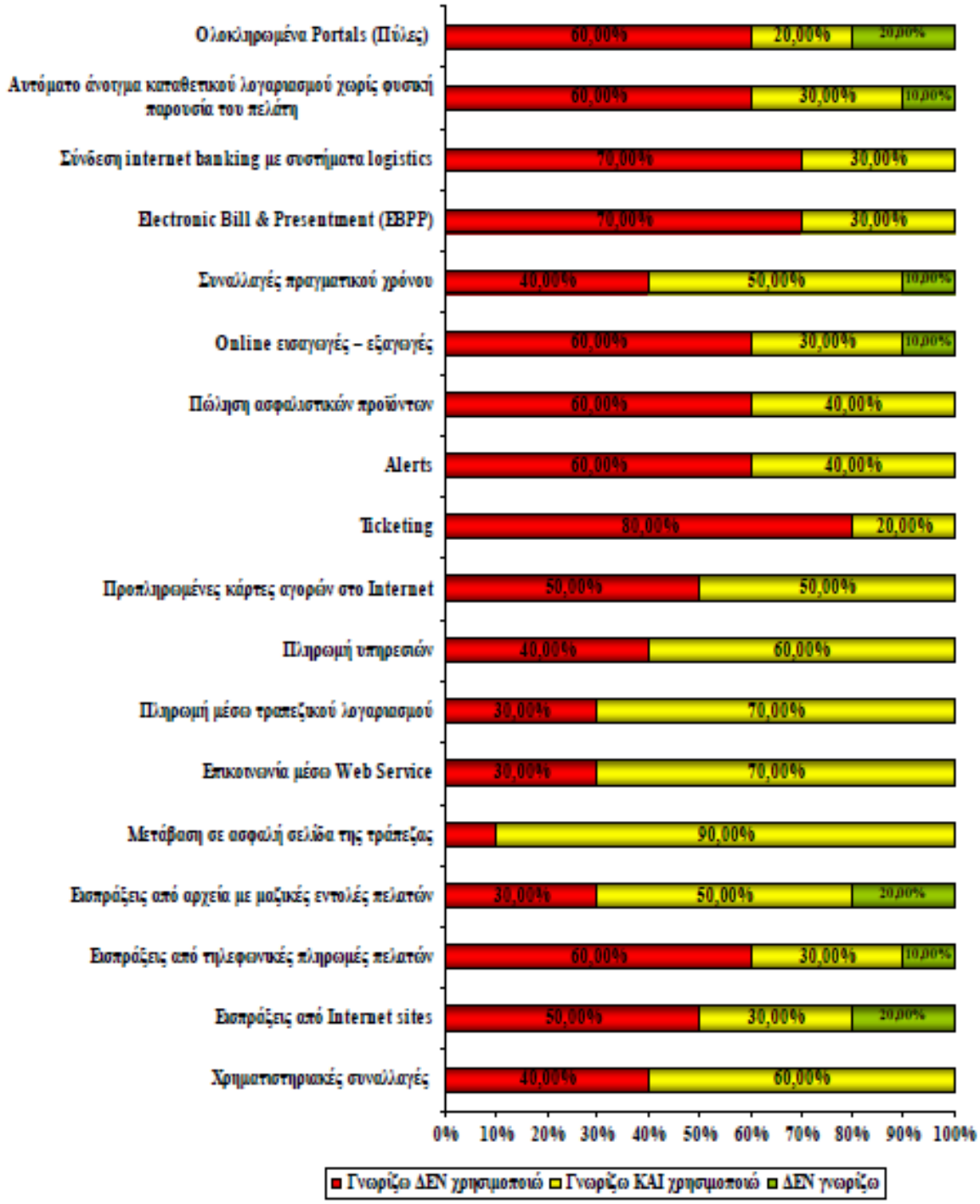
**Γράφημα 11. Υπηρεσίες m-Banking**




Η ηλεκτρονική τραπεζική, εκτός από τις υπηρεσίες που προαναφέρθηκαν, δίνει τη δυνατότητα στους πελάτες της να μπορούν να χρησιμοποιήσουν και κάποιες πρόσθετες υπηρεσίες όπως να πραγματοποιούν χρηματιστηριακές συναλλαγές, Ticketing, Alerts, Πώληση ασφαλιστικών προϊόντων, Electronic Bill & Presentment (EBPP), κ.α. Κατά πόσο όμως οι εγχώριες τράπεζες γνωρίζουν όλες αυτές τις υπηρεσίες και κατά πόσο τις χρησιμοποιούν;

Οι περισσότερες από τις πρόσθετες υπηρεσίες που αναφέρθηκαν παραπάνω, είναι γνωστές στις τράπεζες, όμως το ποσοστό των τραπεζών που δίνουν τη δυνατότητα στους χρήστες του e- banking τους να τις εκμεταλλευτούν κυμαίνεται ακόμα σε χαμηλά επίπεδα.

**Γράφημα 12. Υπηρεσίες προστιθέμενης αξίας**



## 8.2 Στρατηγική – Στόχοι

Κάθε επιχείρηση για να καταφέρει να επιτύχει τους στόχους που θέλει, διαμορφώνει μία στρατηγική, βάση της οποίας και λειτουργεί αφού όμως πρώτα έχει αποφασίσει για το ποιοι είναι οι στόχοι αυτοί και ποιο είναι το κοινό στο οποίο θέλει να απευθυνθεί. Το ίδιο συμβαίνει και στο e-banking.

Σύμφωνα με τις απαντήσεις που λάβαμε, κάθε τράπεζα, σχεδιάζει μια συγκεκριμένη στρατηγική βάση των στόχων που έχει θέσει και αποφασίζει για το ποιο θα είναι το target group στο οποίο θα απευθυνθεί. Επίσης, δημιουργεί ξεχωριστό επιχειρηματικό πλάνο για το e-banking της. Μερικές από τις απαντήσεις που λάβαμε στην ερώτηση ποιο είναι το κοινό - στόχος στο οποίο απευθύνεστε είναι οι εξής:

- Άτομα ηλικίας 22-45 ετών, μέσου και ανώτερου μορφωτικού επιπέδου, άνδρες και γυναίκες,
- Ιδιώτες, Επιχειρήσεις, κ Μεγάλες Επιχειρήσεις ,
- Ιδιώτες 25-40 ετών Πανεπιστημιακή εκπαίδευσης, ελεύθεροι επαγγελματίες, επιχειρήσεις όλων των μεγεθών.

## 8.3 Τράπεζες & νέες τεχνολογίες

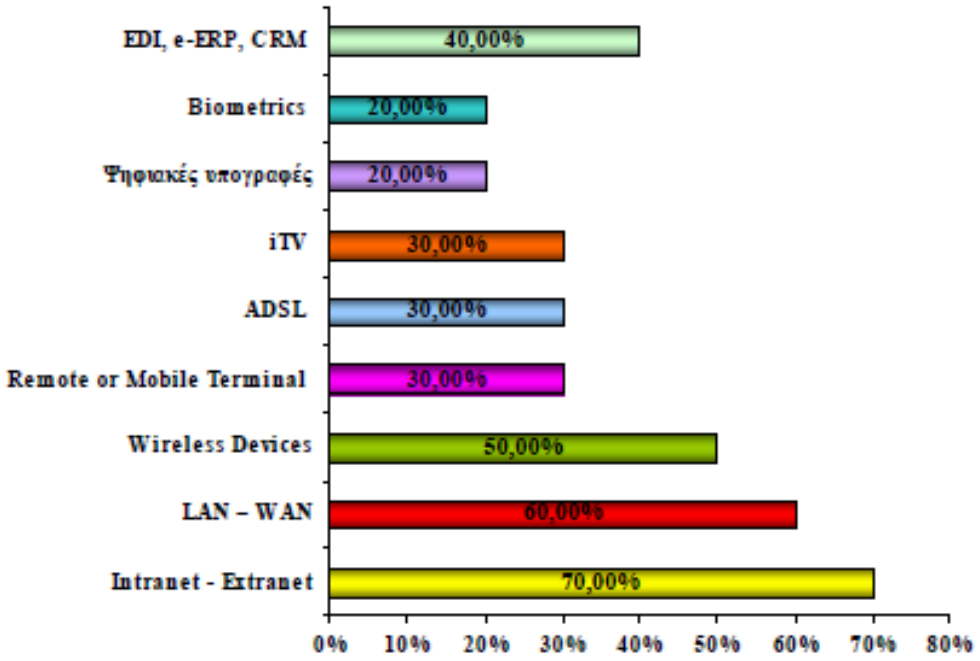
Κατά πόσο οι τράπεζες στη χώρα μας είναι εξοικειωμένες με την υιοθέτηση νέων τεχνολογιών για τη λειτουργία τους; Ποιες από αυτές τις τεχνολογίες χρησιμοποιούν και πόσο αποτελεσματικές θεωρούν πως είναι;

Οι περισσότερο διαδεδομένες και κατά συνέπεια χρησιμοποιούμενες τεχνολογίες από τις εγχώριες τράπεζες σύμφωνα με τα αποτελέσματα που προέκυψαν στην παρούσα έρευνα είναι οι εξής:

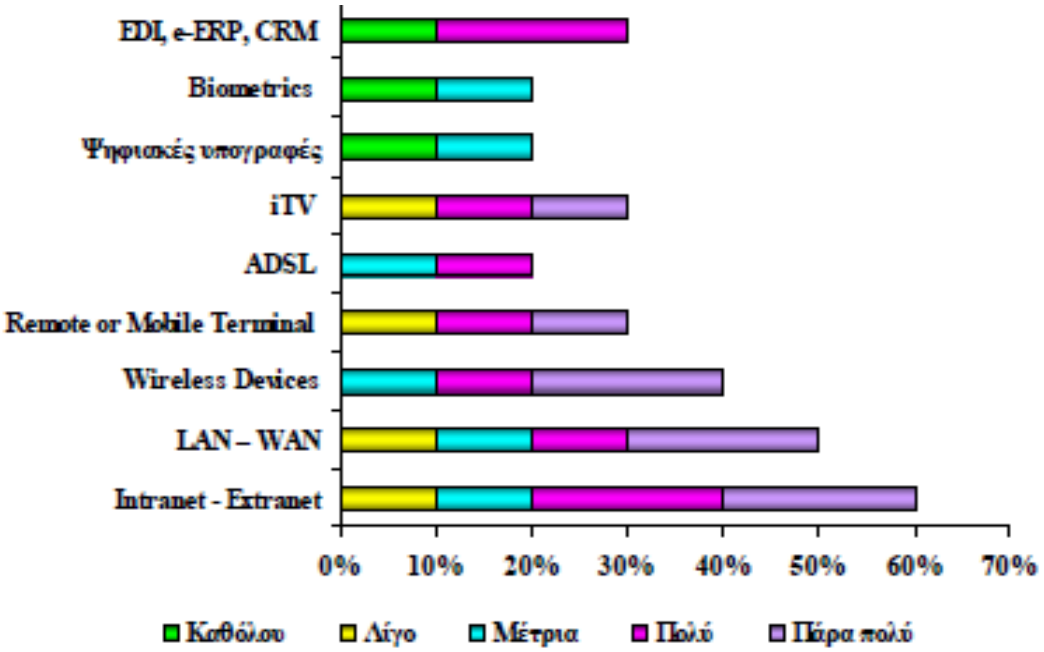
- Intranets
- Extranets
- LAN
- WAN
- e-ERP
- CRM
- EDI

Ακολουθεί γράφημα (13), στο οποίο καταγράφονται τα ποσοστά χρήσης νέων τεχνολογιών από τις ελληνικές τράπεζες, καθώς και γράφημα (14), με τα ποσοστά ικανοποίησης των τραπεζών από τη χρήση των τεχνολογιών αυτών.

**Γράφημα 13. Νέες τεχνολογίες και ελληνικές τράπεζες**




**Γράφημα 14. Αποτελεσματικότητα νέων τεχνολογιών**



Στην υιοθέτηση όμως των τεχνολογιών αυτών υπάρχουν και κάποια εμπόδια. Τα κυριότερα από αυτά είναι το υψηλό κόστος απόκτησης των τεχνολογιών, η έλλειψη γνώσεων από τους πελάτες, η έλλειψη εξειδικευμένου προσωπικού, η αβεβαιότητα των πελατών για την ασφάλεια των συναλλαγών και η έλλειψη υποστήριξης από τη διοίκηση.

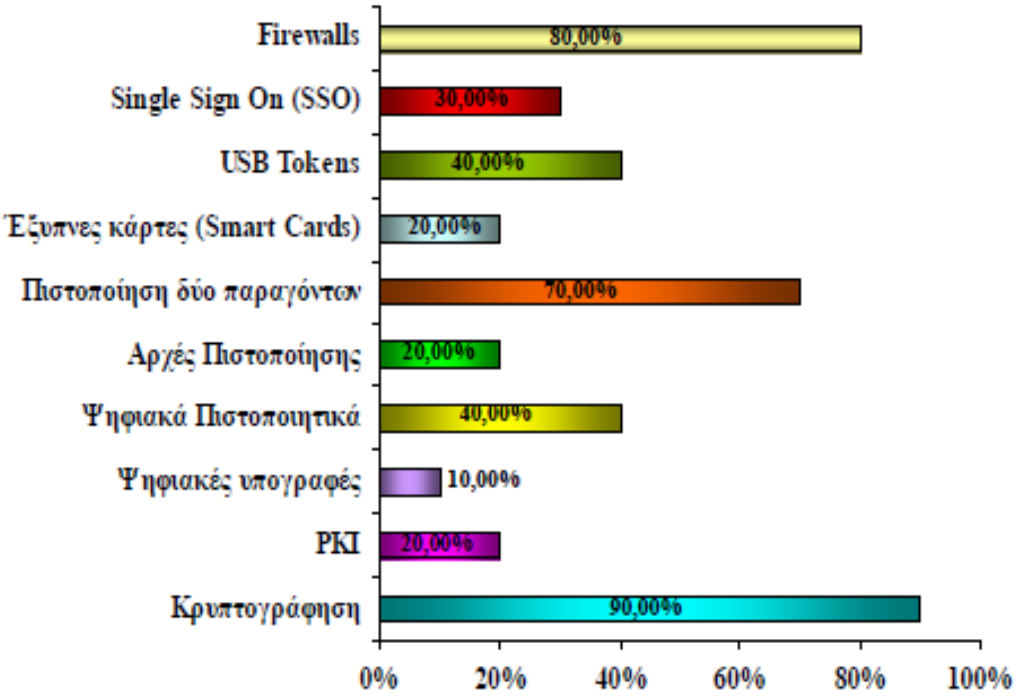
## 8.4 Απειλές και κίνδυνοι – Μέθοδοι προστασίας

Θα ήταν παράληψή μας, να μην αναφερθούμε και στο θέμα της ασφάλειας από την πλευρά των τραπεζών. Δηλαδή, κατά πόσο οι τράπεζες γνωρίζουν τους κινδύνους που εγκυμονεί η χρήση της ηλεκτρονικής τραπεζικής για τους πελάτες αλλά και για την ίδια την τράπεζα και ποιες μεθόδους προστασίας χρησιμοποιούν για να αντιμετωπίσουν τυχόν προβλήματα.

Σύμφωνα με τις απαντήσεις που λάβαμε , το επίπεδο γνώσης των τραπεζών σχετικά με τους κινδύνους της ηλεκτρονικής τραπεζικής είναι αρκετά υψηλό. Ένα μειονέκτημα όμως των ελληνικών τραπεζών, σε σχέση με τις τράπεζες του εξωτερικού είναι ότι οι εγχώριες τράπεζες, δεν έχουν καταφέρει ακόμα να χρησιμοποιήσουν όλες τις μεθόδους προστασίας που υπάρχουν, ώστε να αποφύγουν τους κινδύνους αυτούς.

Οι ευρέως χρησιμοποιούμενες μέθοδοι προστασίας στη χώρα μας είναι η κρυπτογράφηση, τα Firewalls και η πιστοποίηση δύο παραγόντων. Λίγες είναι οι εγχώριες τράπεζες που χρησιμοποιούν και άλλες μεθόδους όπως ψηφιακές υπογραφές, ψηφιακά πιστοποιητικά, και έξυπνες κάρτες. Παρακάτω ακολουθεί γράφημα (15) στο οποίο καταγράφεται το ποσοστό χρήσης των κυριότερων μεθόδων προστασίας από τις ελληνικές τράπεζες.

**Γράφημα 15. Μέθοδοι προστασίας e-Banking**




## 8.5 Εμπόδια υιοθέτησης e-Banking από τις τράπεζες

Το να αποφασίσει μία τράπεζα να εντάξει την ηλεκτρονική τραπεζική στις υπηρεσίες τις οποίες προσφέρει, δεν είναι εύκολή διαδικασία. Θα χρειαστεί να αντιμετωπίσει αρκετά εμπόδια και να πάρει μεγάλο ρίσκο αφού ο αριθμός των online πελατών στη χώρα μας είναι ακόμα μικρός. Μερικά από τα εμπόδια που ίσως αντιμετωπίσει, είναι η αβεβαιότητα των πελατών για το επίπεδο ασφάλειας των online συναλλαγών, το υψηλό κόστος απόκτησης της συγκεκριμένης υπηρεσίας, η έλλειψη γνώσεων σχετικά με το e-Banking καθώς και ο φόβος να δημιουργηθεί αρνητική επίπτωση στα συμβατικά κανάλια πωλήσεων.

Μερικά από τα παραπάνω εμπόδια ίσως να μην υπήρχαν, εάν το επίπεδο εμπιστοσύνης των χρηστών στην πραγματοποίηση ηλεκτρονικών συναλλαγών ήταν υψηλότερο. Για το λόγο αυτό θεωρήσαμε σημαντικό να αναφέρουμε κάποιες ενέργειες που πρέπει να γίνουν από τις τράπεζες, οι οποίες θα ήταν ικανές να αυξήσουν την εμπιστοσύνη των καταναλωτών στο e-banking.

Οι ενέργειες αυτές είναι οι εξής:

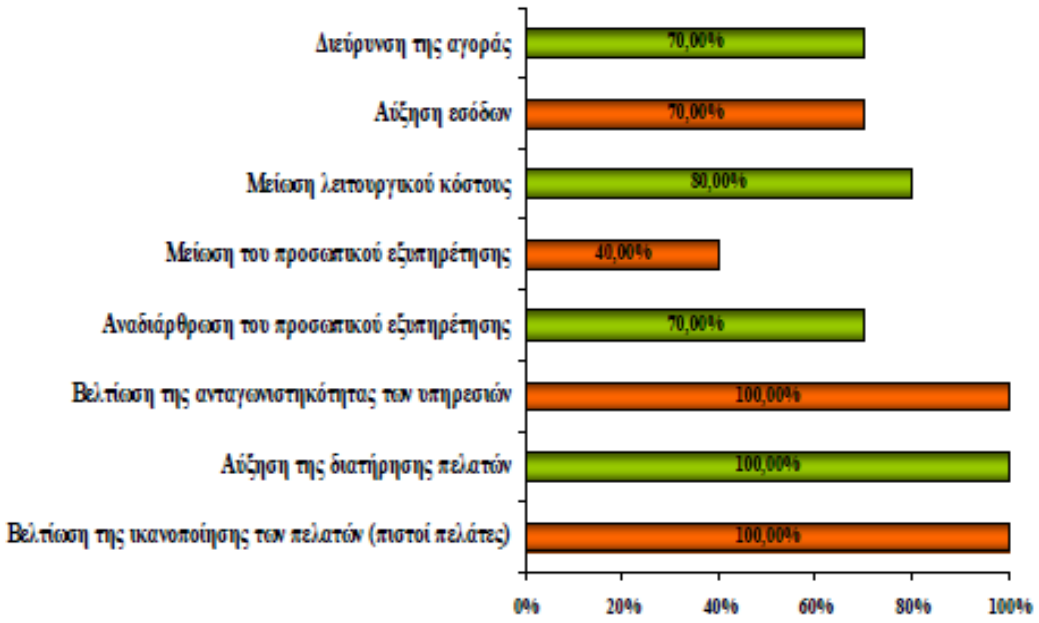
- Παροχή εκπαιδευτικών πληροφοριών σχετικά με την on line τραπεζική απάτη,
- Τακτική επικοινωνία με τον πελάτη για τις ενέργειές αποφυγής online απάτης,
- Διενέργεια διαφημιστικών καμπανιών με οδηγίες αποφυγής της online απάτης,
- Δημιουργία μοντέλων ανίχνευσης απάτης,
- Παροχή καλύτερων ‘back-end’ συστημάτων ανίχνευσης απάτης.

## 8.6 Οφέλη χρήσης e-Banking για τις τράπεζες

Εκτός από τα πλεονεκτήματα τα οποία αποκτούν οι χρήστες της ηλεκτρονικής τραπεζικής , πολλά είναι και τα οφέλη που απολαμβάνουν οι τράπεζες. Σύμφωνα με το γράφημα (16), οι τράπεζες που παρέχουν e- banking, έχουν παρατηρήσει :

- βελτίωση της ικανοποίησης των πελατών τους,
- αύξηση της διατήρησης των πελατών και των εσόδων τους,
- μείωση του λειτουργικού τους κόστους και
- βελτίωση της ανταγωνιστικότητας των υπηρεσιών.

**Γράφημα 16. Οφέλη χρήσης e-Banking**




Όμως, στη χώρα μας το ποσοστό των χρηστών της online τραπεζικής κυμαίνεται ακόμα σε χαμηλά επίπεδα, και κατά συνέπεια ο βαθμός ικανοποίησης των τραπεζών από την ανταπόκριση των πελατών τους στη νέα αυτή υπηρεσία είναι ακόμα μικρός.

## Μέρος Β – Χρήστες

Το κομμάτι αυτό της έρευνας, αφορά στη συλλογή στοιχείων σχετικά με την αποδοχή και το βαθμό ικανοποίησης των Ελλήνων χρηστών. Αφιερώσαμε όμως και ένα μέρος της έρευνας μας στους μη χρήστες, με σκοπό να διαπιστώσουμε τους λόγους για τους οποίους είναι διστακτικοί στο να χρησιμοποιήσουν την ηλεκτρονική τραπεζική.

Στην παρούσα έρευνα, τα αποτελέσματα τα οποία αφορούν τους χρήστες του e-Banking, δεν διαφοροποιούνται πολύ σε σχέση με αυτά των ερευνών που παρουσιάστηκαν στο έβδομο κεφάλαιο.

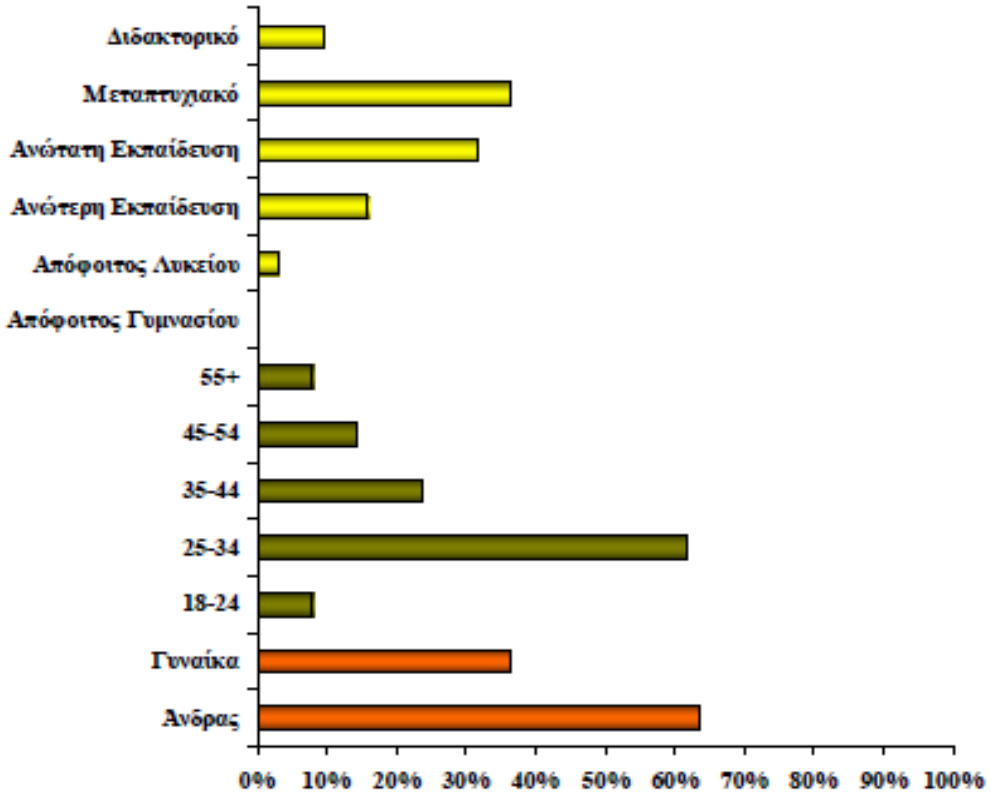
Και εδώ, το ποσοστό των χρηστών της ηλεκτρονικής τραπεζικής, εξακολουθεί να βρίσκεται σε χαμηλό επίπεδο, σε σχέση με αυτό των μη χρηστών. Όμως η διαφορά αυτή, με την πάροδο των ετών συνεχώς μειώνεται.

## 8.7 Φύλο – Ηλικία- Μόρφωση

Για ακόμα μία φορά, οι άνδρες είναι αυτοί οι οποίοι δείχνουν να εξοικειώνονται ευκολότερα με τις τεχνολογικές εξελίξεις και δεν διστάζουν να χρησιμοποιήσουν τις νέες ηλεκτρονικές υπηρεσίες που προσφέρονται.

Με διαφορά περίπου είκοσι ποσοστιαίων μονάδων, οι άνδρες παρουσιάζουν υψηλότερα ποσοστά από τα αντίστοιχα των γυναικών ως προς τη χρήση του Internet Banking στη χώρα μας (63,49% και 36,51% αντίστοιχα).

**Γράφημα 17. Φύλο – Ηλικία – Μόρφωση**

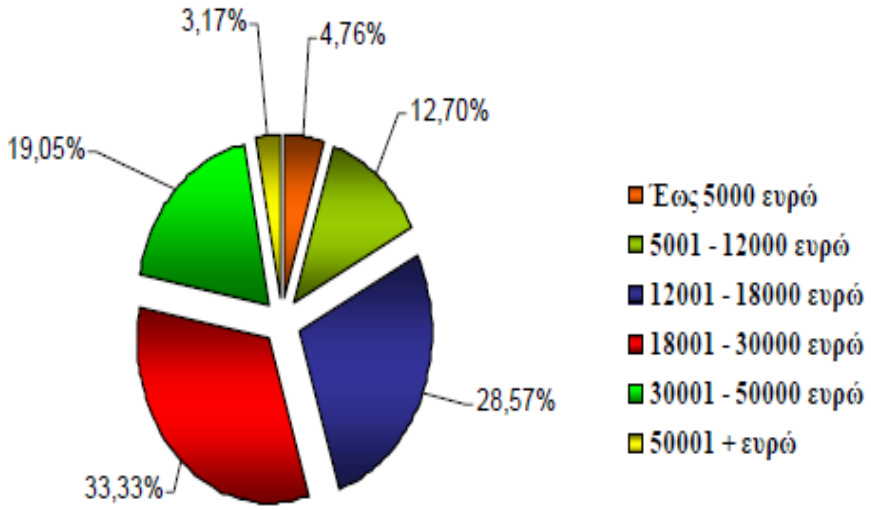



Τα πιο υψηλά ποσοστά χρήσης του e-Banking ως προς την ηλικία, σημειώνονται στα άτομα 25 – 34 ετών με ποσοστό 61,90%, και ακολουθούν τα άτομα ηλικίας 35 – 45 ετών με ποσοστό 23,81%.

Ως προς το μορφωτικό επίπεδο των χρηστών του Internet Banking, πολύ υψηλά ποσοστά, σημειώνονται σε άτομα με μεταπτυχιακό τίτλο σπουδών 36,51% , άτομα ανώτατης και ανώτερης εκπαίδευσης, ενώ ακολουθούν όσοι διαθέτουν διδακτορικό και οι απόφοιτοι λυκείου.

Όπως μπορούμε να δούμε, στο γράφημα (18) τα άτομα τα οποία χρησιμοποιούν την ηλεκτρονική τραπεζική, είναι κυρίως άτομα με υψηλό ετήσιο εισόδημα.

**Γράφημα 18. Ετήσιο Εισόδημα**



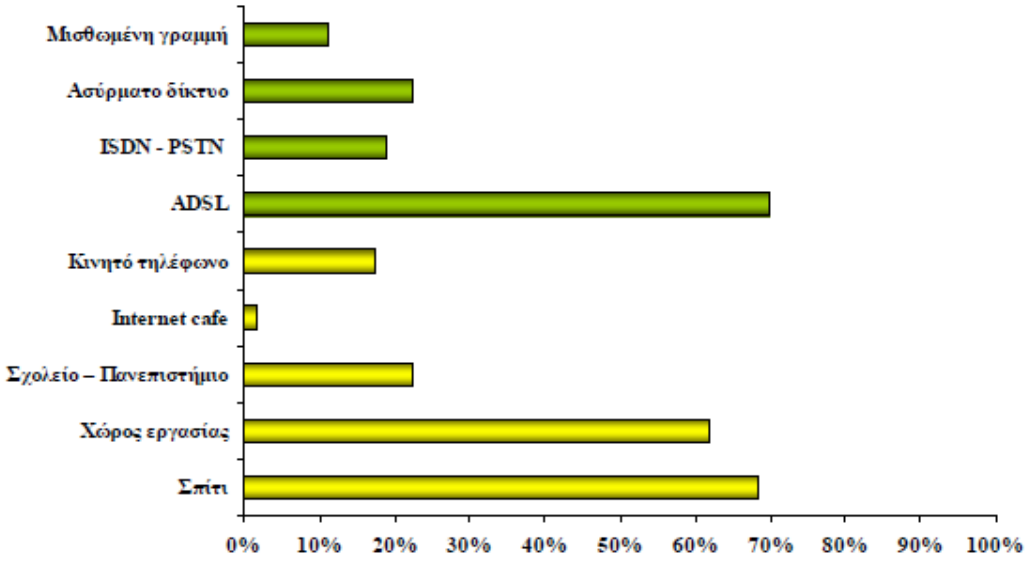

## 8.8 Τόπος πρόσβασης και σύνδεση στο διαδίκτυο

Ένα πολύ σημαντικό στοιχείο που καλό είναι να λαμβάνεται υπόψη σε όλες τις αναφορές στο e-banking, είναι η χρήση των τηλεπικοινωνιακών μέσων και ιδιαίτερα του internet. Για το λόγο αυτό, δεν θα μπορούσαμε να μη συμπεριλάβουμε στο ερωτηματολόγιο μας ερωτήσεις οι οποίες θα αφορούν στη χρήση του διαδικτύου.

Ο κύριος τόπος πρόσβασης, σύμφωνα με τις απαντήσεις που έδωσαν στην παρούσα έρευνα οι χρήστες του e- Banking, στο διαδίκτυο και κατά συνέπεια στους ηλεκτρονικούς τραπεζικούς τους λογαριασμούς, είναι το σπίτι με ποσοστό 68,25% και ακολουθεί ο χώρος εργασίας 61,90%, ενώ μικρό είναι ακόμα το ποσοστό όσον χρησιμοποιούν το κινητό τους τηλέφωνο 17,46%.

Ενώ όπως μπορούμε να δούμε και στο γράφημα 19, η πλειοψηφία των χρηστών του Internet Banking που έλαβαν μέρος στην παρούσα έρευνα, χρησιμοποιούν σύνδεση ADSL σε ποσοστό 69.84% για να συνδεθούν στο Internet.

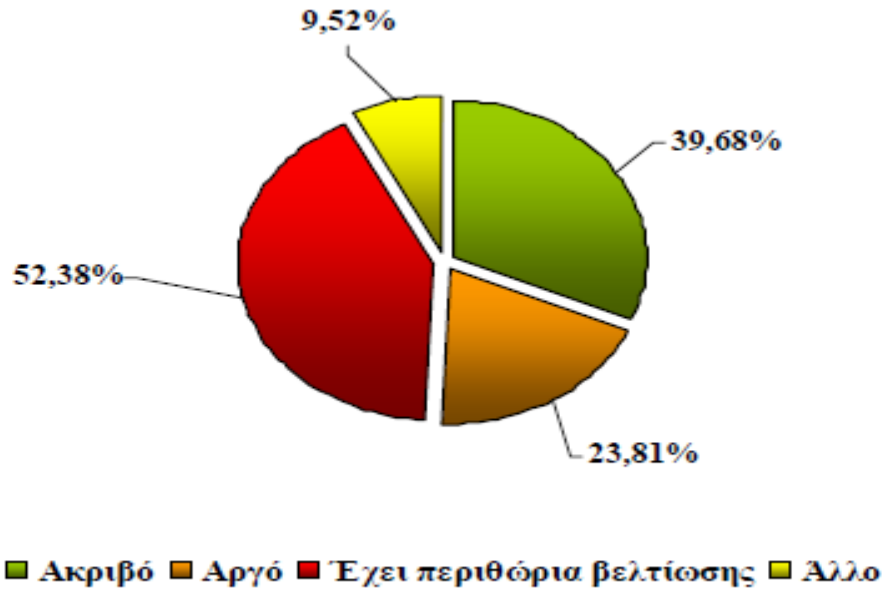
**Γράφημα 19. Τόπος πρόσβασης στο Internet – Είδος σύνδεσης**




Είναι σημαντικό να σημειωθεί ότι το μεγαλύτερο ποσοστό των χρηστών της ηλεκτρονικής τραπεζικής, έχει πραγματοποιήσει έστω και μία φορά αγορά μέσω του διαδικτύου.

Γενικά, σύμφωνα με τις απαντήσεις των χρηστών του e-banking άρα και του διαδικτύου, το internet στην Ελλάδα έχει βελτιωθεί κατά πολύ σε σχέση με τα προηγούμενα χρόνια. Πιστεύουν όμως, ότι υπάρχει περιθώριο για περαιτέρω βελτίωση, ειδικά σε ότι αφορά την ταχύτητα αλλά και το κόστος χρήσης του.

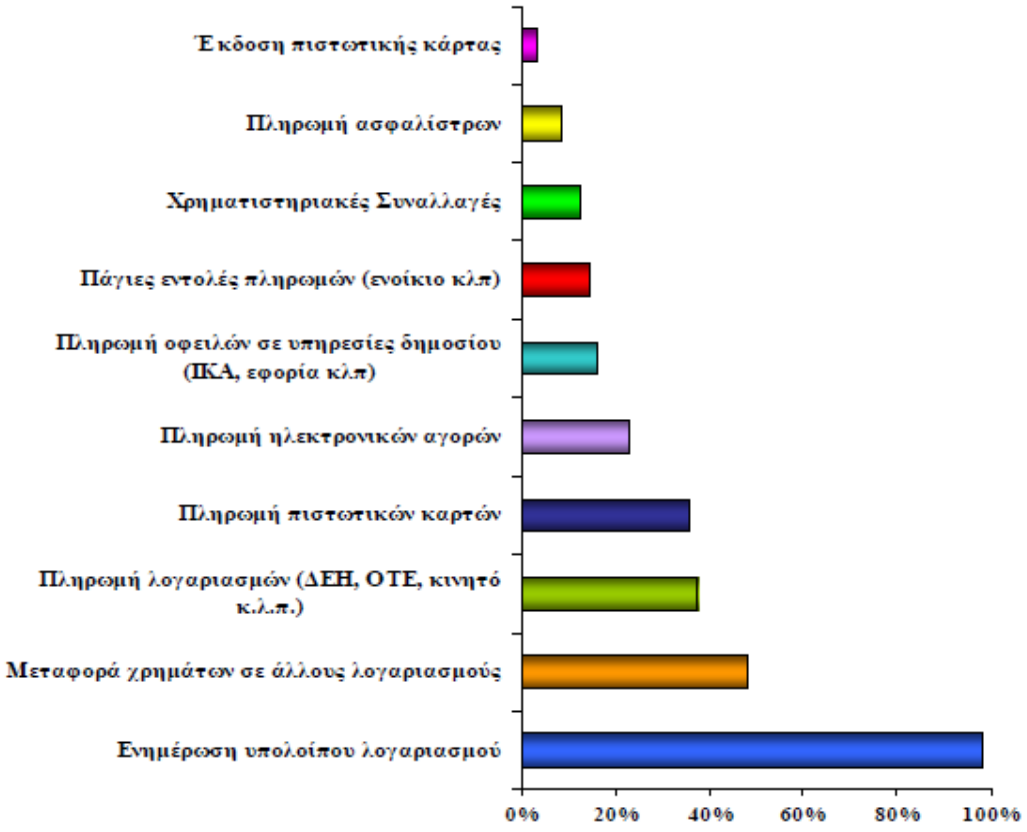
**Γράφημα 20. Το Internet στην Ελλάδα**




## 8.9 Υπηρεσίες ηλεκτρονικής τραπεζικής & φόβοι μη χρηστών

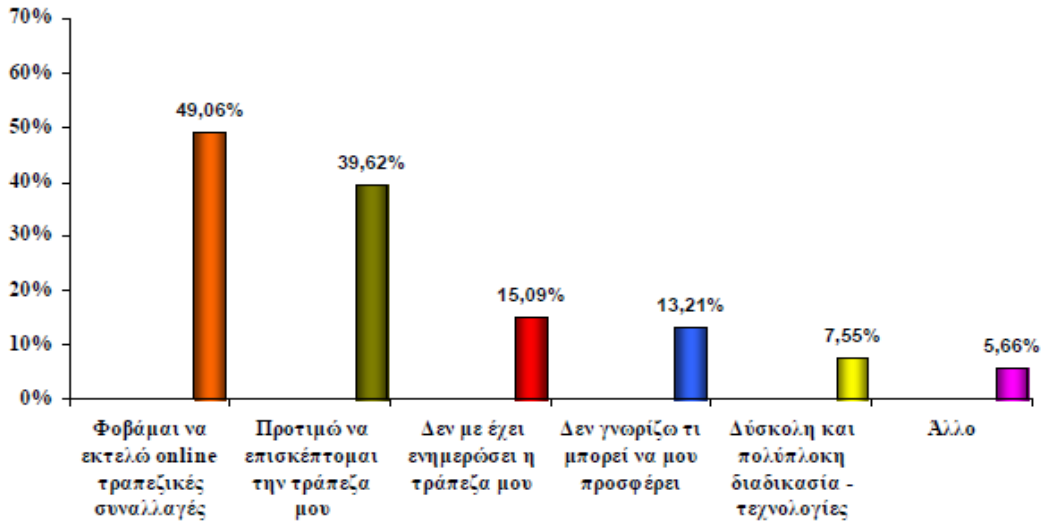
Σύμφωνα με τους χρήστες της ηλεκτρονικής τραπεζικής που έλαβαν μέρος στην έρευνα, οι υπηρεσίες που χρησιμοποιούν περισσότερο, είναι η ενημέρωση υπολοίπου λογαριασμού σε ποσοστό 98,41% , ακολουθεί η μεταφορά χρημάτων σε άλλους λογαριασμούς, η πληρωμή λογαριασμών (ΔΕΗ, ΟΤΕ, κινητό, κ.α), και η πληρωμή πιστωτικών καρτών. Παρακάτω, ακολουθεί γράφημα (21), στο οποίο παρουσιάζονται αναλυτικά, οι υπηρεσίες που χρησιμοποιούνται πιο πολύ από τους χρήστες του internet banking.

**Γράφημα 21. Δημοφιλέστερες υπηρεσίες του e-Banking**



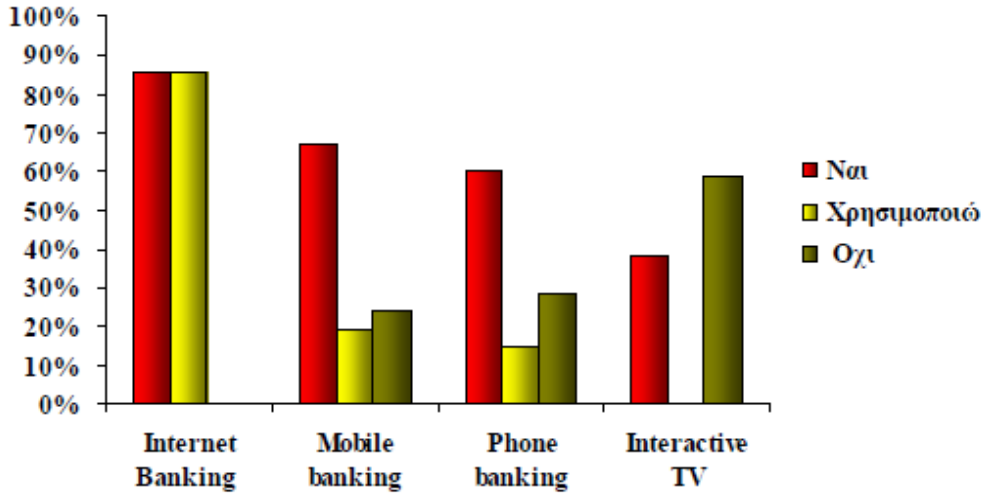

Ενώ οι κυριότεροι φόβοι, που εμποδίζουν όσους δεν χρησιμοποιούν ακόμα την συγκεκριμένη υπηρεσία, να τη χρησιμοποιήσουν, είναι ο φόβος online τραπεζικών συναλλαγών, η προτίμηση να επισκέπτονται το κατάστημα τράπεζας, η έλλειψη ενημέρωσης από την τράπεζα και γνώσης των δυνατοτήτων της ηλεκτρονικής τραπεζικής. Παρακάτω παρουσιάζεται γράφημα (22), με τους βασικότερους λόγους αποφυγής του e- Banking σύμφωνα με τις απαντήσεις των μη χρηστών.

**Γράφημα 22. Λόγοι αποφυγής e-Banking**




Σύμφωνα με το γράφημα 23, στην ερώτηση αν οι χρήστες της ηλεκτρονικής τραπεζικής γνωρίζουν και χρησιμοποιούν, τις τεχνολογίες Internet Banking, Mobile Banking, Phone Banking και Interactive TV, οι χρήστες του e-banking απάντησαν ως εξής:

**Γράφημα 23. Είδη ηλεκτρονικής τραπεζικής**



Παρατηρούμε λοιπόν, ότι το μεγαλύτερο ποσοστό των Ελλήνων χρηστών, γνωρίζουν τους τρόπους με τους οποίους μπορούν να διαχειριστούν ηλεκτρονικά τους λογαριασμούς τους, όμως οι περισσότεροι από αυτούς, προτιμούν να χρησιμοποιούν το internet banking. Ενώ λίγοι είναι ακόμα όσοι χρησιμοποιούν κάποια άλλη συσκευή όπως για παράδειγμα το σταθερό ή το κινητό τους τηλέφωνο.

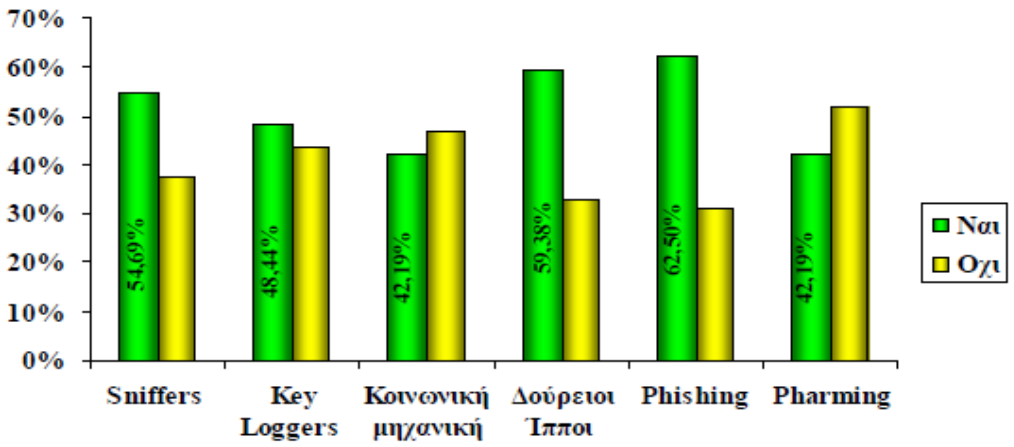
## 8.10 Ασφάλεια

Ένα από τα σημαντικότερα ζητήματα, που απασχολούν τους χρήστες του ebanking, σύμφωνα με τις απαντήσεις που λάβαμε, είναι αυτό της ασφάλειας.

Γνωρίζουν όμως οι χρήστες, τους κινδύνους που εγκυμονεί η ηλεκτρονική τραπεζική και τους τρόπους με τους οποίους μπορούν να προστατευθούν από τους κινδύνους αυτούς;

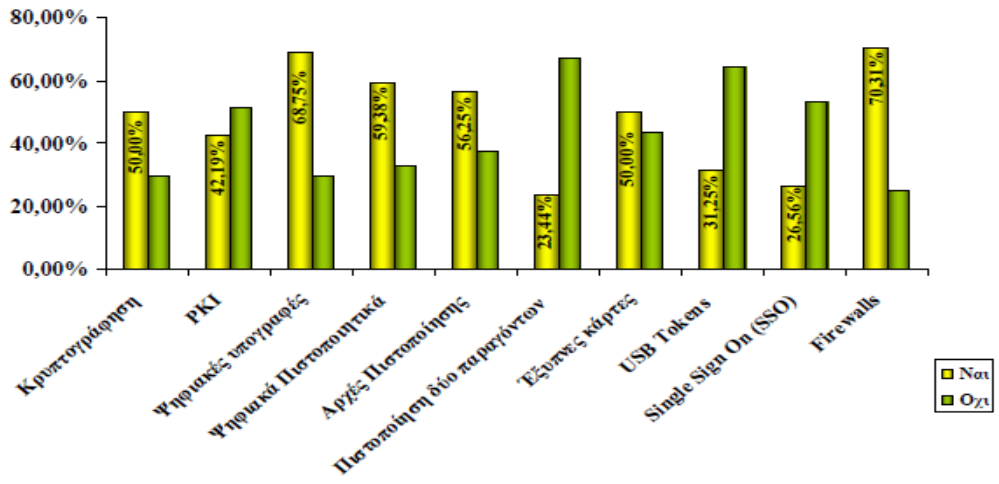
Σύμφωνα με το παρακάτω γράφημα (24), περίπου το 1/2 των χρήστες της ηλεκτρονικής τραπεζικής, γνωρίζουν τους κινδύνους που πιθανών να αντιμετωπίσουν κατά τη χρήση του e-banking. Το ποσοστό αυτό, δεν είναι καθόλου ικανοποιητικό, αφού οι ηλεκτρονικές επιθέσεις καθημερινά αυξάνονται.

**Γράφημα 24. Κίνδυνοι του e-Banking**



Το ίδιο περίπου ισχύει και για τις μεθόδους προστασίας του online banking. Οι περισσότερες από αυτές είναι γνωστές σε μεγάλη μερίδα των χρηστών. Υπάρχουν όμως και κάποιες μέθοδοι, όπως η πιστοποίηση δύο παραγόντων, τα usb tokens και η Single sign on που δεν είναι ακόμα ευρέως διαδεδομένες.

**Γράφημα 25. Τρόποι προστασίας στο e-Banking**

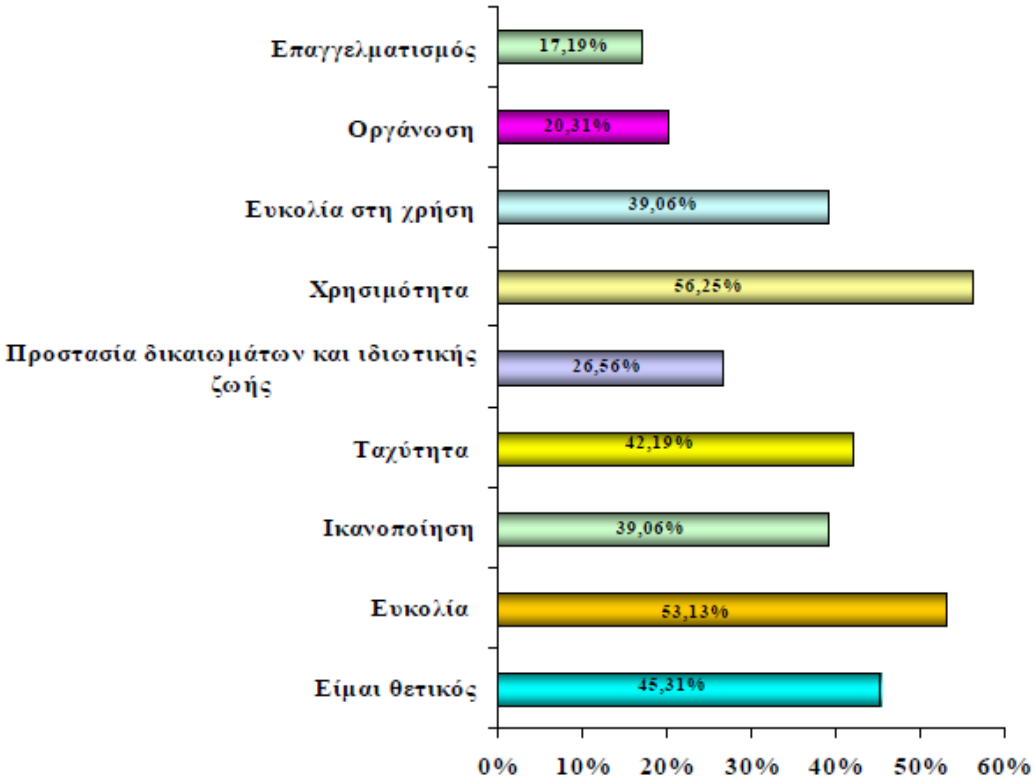



## 8.11 Βαθμός ικανοποίησης χρηστών

Ένας από τους βασικούς στόχους αυτής της έρευνας, είναι να δούμε, κατά πόσο είναι ικανοποιημένοι οι χρήστες της ηλεκτρονικής τραπεζικής από τη χρήση της, αλλά και από τις υπηρεσίες που προσφέρει, τι τους αρέσει και τι τους δυσαρεστεί, ποιες είναι οι προσδοκίες που έχουν από αυτήν, καθώς επίσης πόσο ευχαριστημένοι είναι από την ασφάλεια που τους προσφέρει η εκάστοτε τράπεζα.

Στο γράφημα (26) παρατηρούμε ότι στο μεγαλύτερο ποσοστό τους, οι χρήστες, έχουν θετική άποψη για το internet banking, θεωρούν ότι είναι εύκολο στη χρήση του, γρήγορο στην εκτέλεση συναλλαγών, και ότι υπάρχει οργάνωση από τις τράπεζες σε ότι αφορά τη διεξαγωγή ηλεκτρονικών συναλλαγών. Ενώ, το μικρότερο ποσοστό ικανοποίησης, αφορά στην προστασία δικαιωμάτων και ιδιωτικής ζωής των χρηστών.

**Γράφημα 26. Βαθμός ικανοποίησης από το e-Banking & τις προσφερόμενες υπηρεσίες**




Πολλά όμως, είναι και τα στοιχεία, τα οποία δυσαρεστούν τους χρήστες, στη χρήση του e-banking. Ενδεικτικά αναφέρουμε παρακάτω μερικές από τις απαντήσεις που λάβαμε.

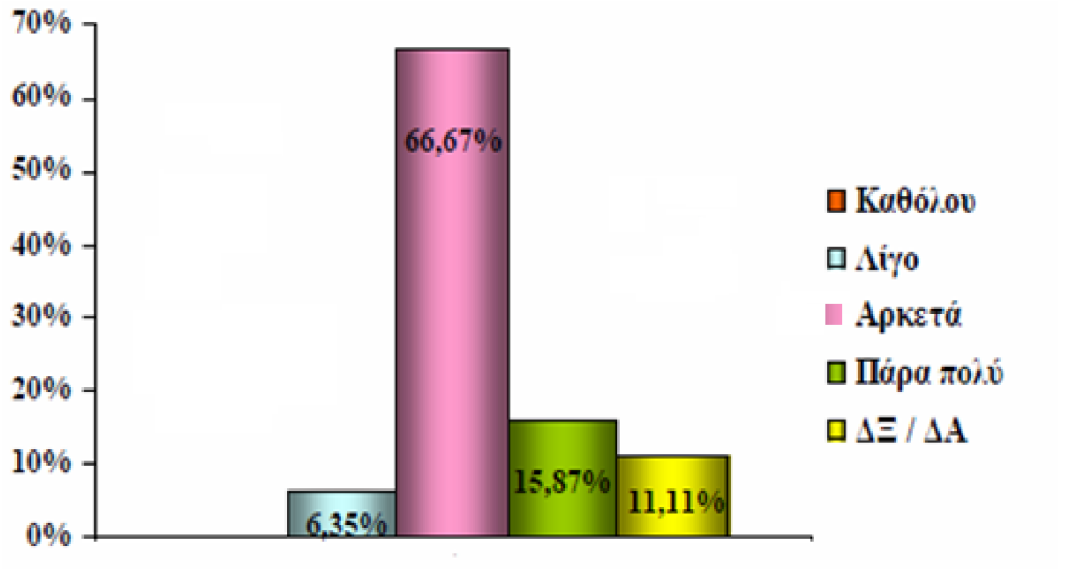
« Πρέπει το σύστημα ασφάλειας να γίνει πιο εύχρηστο»,
« Η εμφάνιση των συναλλαγών με πιστωτικές δεν είναι άμεση»,
«Ευκολία στην υποκλοπή στοιχείων (pin, username κ.α), των άπειρων χρηστών»,
«Με ενοχλεί το ότι δεν είναι σε εμφανές σημείο η λέξη έξοδος από το σύστημα και δεν είμαι σίγουρος αν με την απλή επιλογή του σχετικού εικονιδίου έχω πράγματι εξέλθει από την ιστοσελίδα με τα προσωπικά μου δεδομένα»,
«Σε κάποιες τράπεζες συχνά μπλοκάρουν οι κωδικοί, χωρίς να έχει γίνει λάθος στην καταχώρησή τους.»,
«Θα επιθυμούσα να έχω την δυνατότητα να ανακαλέσω αναλυτικά ιστορικά στοιχεία του λογαριασμού μου για περιόδους που να υπερβαίνουν τον 1 μήνα από

την ημερομηνία πρόσβασης. Μέχρι στιγμής είμαι σε θέση να έχω πρόσβαση σε στοιχεία έως ένα μήνα πριν και δεν υπάρχει δυνατότητα να δω τα σχετικά στοιχεία πέραν αυτής της περιόδου.»

Υπάρχουν όμως και στοιχεία ή υπηρεσίες, τα οποία " αρέσουν" στους χρήστες, όπως : άμεση ενημέρωση, ευκολία χρήσης, γρήγορη εξυπηρέτηση χωρίς αναμονή, Online βοήθεια, μηδενικές προμήθειες, υποστήριξη σχεδόν του συνόλου των τραπεζικών συναλλαγών, ταχύτητα και ασφάλεια στις συναλλαγές, 24 ώρες 365 μέρες το χρόνο, έλεγχος λογαριασμών εξωτερικού.

Όσων αφορά την ασφάλεια, το 66,67% των χρηστών, δείχνουν να είναι αρκετά ικανοποιημένοι από τις μεθόδους προστασίας που χρησιμοποιεί η τράπεζα τους, το 15,87% πάρα πολύ ικανοποιημένοι, ενώ μόλις το 6,35% λίγο ικανοποιημένοι *(βλ. γράφημα 27)*.

**Γράφημα 27. Βαθμός ικανοποίησης από την ασφάλεια που προσφέρουν οι Τράπεζες**




Ποιες όμως είναι οι προσδοκίες των χρηστών της ηλεκτρονικής τραπεζικής, από αυτήν και πως θεωρούν ότι θα είναι το online banking στο μέλλον;

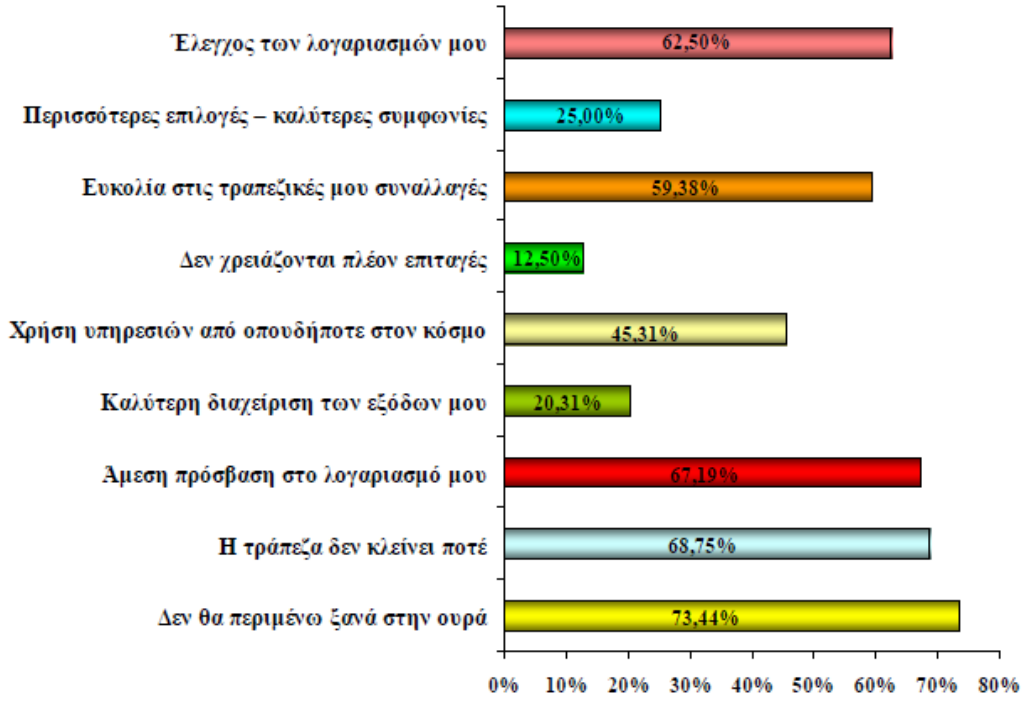
Σύμφωνα με τις απαντήσεις που λάβαμε, οι περισσότεροι χρήστες, προσδοκούν: καλύτερη πληροφόρηση , μεγαλύτερο φάσμα εργασιών, εξοικονόμηση χρόνου, καλύτερη οργάνωση και διαχείριση των χρημάτων, μεγαλύτερη ασφάλεια, εξάπλωση της χρήσης, ευκολία στην πρόσβαση και στις

συναλλαγές, μεγαλύτερη ευελιξία στις αγορές μέσω ηλεκτρονικού εμπορίου, εύκολη ενημέρωση κινήσεων. Ενώ θεωρούν ότι το e- banking στο μέλλον, θα είναι ευρέως διαδεδομένο, πιο ευέλικτο στις συναλλαγές, θα περιλαμβάνει το σύνολο των τραπεζικών συναλλαγών και θα είναι πια στην συνείδηση του κόσμου σαν ασφαλές και χρήσιμο μέσο.

Τέλος, θεωρήσαμε σημαντικό να ρωτήσουμε τους χρήστες, τι οι ίδιοι θεωρούν ότι έχουν "κερδίσει" από τη χρήση του e-banking, ποιες πρόσθετες υπηρεσίες επιθυμούν να προσφέρει η τράπεζα τους στο μέλλον και κατά πόσο θα ενθάρρυναν και άλλους να χρησιμοποιήσουν τη συγκεκριμένη υπηρεσία.

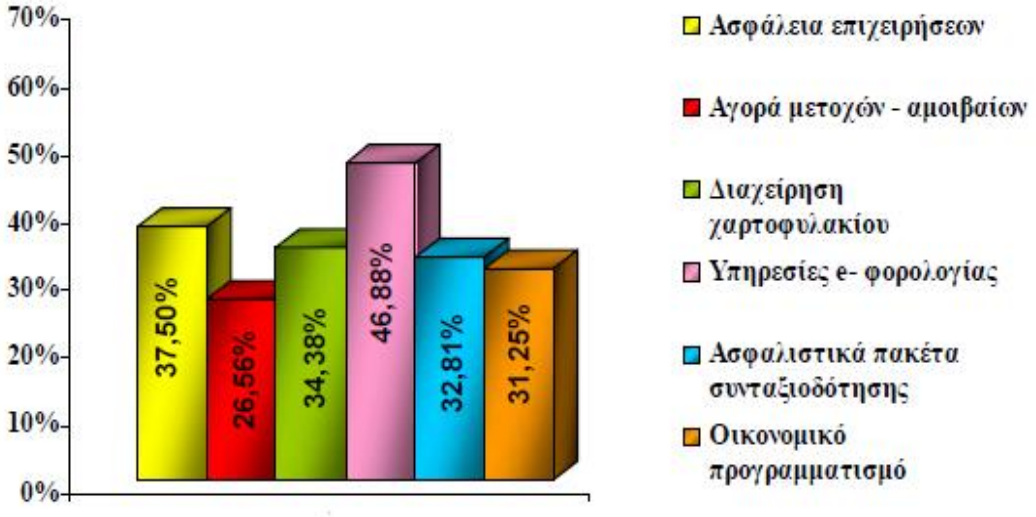
Σύμφωνα με το γράφημα (28), το 73,44% των χρηστών, απάντησε, ότι ένας από τους σημαντικότερους λόγους που χρησιμοποιεί το internet banking, είναι ότι δεν θα χρειαστεί να περιμένει ξανά στις ουρές των τραπεζών, σπαταλώντας πολύ από το χρόνο του για να πραγματοποιήσει τις συναλλαγές του, το 68,75% ότι μπορεί να εκτελεί τις συναλλαγές που επιθυμεί εφτά ημέρες την εβδομάδα, εικοσιτέσσερις ώρες το εικοσιτετράωρο, το 67,19% ότι έχει άμεση πρόσβαση στους λογαριασμούς του και το 62,50% ότι με τη χρήση της συγκεκριμένης υπηρεσίες, ελέγχει καλύτερα τους λογαριασμούς του.

**Γράφημα 28. Οφέλη χρήσης e- Banking**



Στο ερώτημα ποιες πρόσθετες υπηρεσίες θα θέλατε να προσφέρει η τράπεζα σας, το 46,88% απάντησε υπηρεσίες e-φορολογίας, το 37,50% ασφάλεια για επιχειρήσεις και το 32,81% ασφαλιστικά πακέτα συνταξιοδότησης (βλ. γράφημα 29).

**Γράφημα 29. Πρόσθετες Υπηρεσίες**



# Συμπεράσματα έρευνας

Ολοκληρώνοντας αυτήν την εργασία και με βάση τα αποτελέσματα τα οποία προέκυψαν από την παρούσα έρευνα και καταγράφηκαν παραπάνω, είμαστε σε θέση να αξιολογήσουμε το επίπεδο στο οποίο βρίσκεται η ηλεκτρονική τραπεζική στη χώρα μας, τόσο από την πλευρά των τραπεζών που παρέχουν τη συγκεκριμένη υπηρεσία, όσο και από την πλευρά των χρηστών.

Σήμερα, σχεδόν όλες οι τράπεζες στη χώρα μας, προσφέρουν στους πελάτες τους τη δυνατότητα να μπορούν να πραγματοποιούν τις συναλλαγές τους μέσω της ηλεκτρονικής τραπεζικής, χωρίς να χρειάζεται η φυσική τους παρουσία στο κατάστημα της τράπεζας.

Οι ελληνικές τράπεζες, παρά το ρίσκο που αντιμετωπίζουν υιοθετώντας μία υπηρεσία που δεν είναι ακόμα ευρέως διαδεδομένη, δεν έχουν να ζηλέψουν σε τίποτα τις τράπεζες του εξωτερικού, σε ότι έχει να κάνει με το e-banking.

Η υιοθέτηση της συγκεκριμένης υπηρεσίας σε μία χώρα όπως η Ελλάδα, η οποία δεν είναι ακόμα πλήρως εξοικειωμένη με την ταχύτατη ανάπτυξη της τεχνολογίας μπορεί να χαρακτηριστεί ως ριψοκίνδυνη.

Οι περισσότερες ελληνικές τράπεζες που προσφέρουν υπηρεσίες e-banking, χρησιμοποιούν internet banking, ενώ με την πάροδο των ετών όλο και περισσότερες είναι οι τράπεζες που δίνουν τη δυνατότητα στους πελάτες τους να διαχειρίζονται τους λογαριασμούς του μέσω σταθερού ή κινητού τηλεφώνου.

Οι υπηρεσίες που προσφέρουν καλύπτουν σχεδόν όλες τις ανάγκες των καταναλωτών χωρίς ο πελάτη να χρειάζεται να σπαταλά το χρόνο του περιμένοντας στο γκισέ κάποιας τράπεζας.

Οι κυριότερες υπηρεσίες που προσφέρονται από τις ελληνικές τράπεζες είναι:

- μεταφορές σε λογαριασμό ιδίου ή τρίτου,
- εμβάσματα εσωτερικού και εξωτερικού,
- πληροφορίες λογαριασμών, καρτών και δανείων
- πληρωμές καρτών – λογαριασμών – δανείων

Επιπλέον, οι ελληνικές τράπεζες, μέσω της ηλεκτρονικής τραπεζικής προσφέρουν στους πελάτες τους και υπηρεσίες προστιθέμενης αξίας όπως: Ticketing, Electronic Bill & Presentment, Σύνδεση internet banking με συστήματα

logistics, αυτόματο άνοιγμα καταθετικού λογαριασμού και πληρωμές μέσω τραπεζικού λογαριασμού οι οποίες διαφοροποιούν κάθε οργανισμό.

Τα οφέλη τα οποία έχουν αποκομίσει οι τράπεζες, είναι πολλά και αρκετά προσοδοφόρα, αφού με τη χρήση της ηλεκτρονικής τραπεζικής, καταφέρνουν να μειώσουν τα λειτουργικά έξοδα την τράπεζας, αυξάνοντας ταυτόχρονα των αριθμό των πελατών της.

Παρά τα οφέλη τα οποία έχουν οι τράπεζες από την παροχή της συγκεκριμένης υπηρεσίας, πολλά συνεχίζουν να είναι και τα εμπόδια τα οποία αντιμετωπίζουν σχετικά με την υιοθέτηση της, όπως το υψηλό κόστος και ο μικρός αριθμός των χρηστών στη χώρα μας.

Το κοινό στόχος (target group) στο οποίο απευθύνονται οι περισσότερες τράπεζες στη χώρα μας αφορά άτομα νεαρής ηλικίας με υψηλό μορφωτικό και οικονομικό επίπεδο, καθώς επίσης και ελεύθερους επαγγελματίες και επιχειρήσεις όλων των μεγεθών.

Το επίπεδο ασφάλειας που προσφέρουν οι ελληνικές τράπεζες στους χρήστες της ηλεκτρονικής τραπεζικής , μπορούμε να πούμε ότι βρίσκεται σε ικανοποιητικό επίπεδο όμως τα περιθώρια βελτίωσης του είναι ακόμα μεγάλα αν κρίνουμε και από την συνεχή εμφάνιση νέων κινδύνων – απειλών στις ηλεκτρονικές συναλλαγές.

Πιο συγκεκριμένα, στο σύνολό τους οι ελληνικές τράπεζες, γνωρίζουν όλους τους κινδύνους και τις απειλές που μπορούν να προκύψουν κατά τη χρήση καθώς επίσης, είναι ενημερωμένες και παρέχουν τους περισσότερους τρόπους με τους οποίους μπορούν να αντιμετωπιστούν οι κίνδυνοι αυτοί.

Σαν τελικό συμπέρασμα θα μπορούσαμε να πούμε ότι για να είναι επιτυχημένες οι τράπεζες στο μέλλον, θα πρέπει να έχουν διαμορφώσει στρατηγικές προσαρμοσμένες στις εξελίξεις της αγοράς και του σύγχρονου οικονομικού περιβάλλοντος καθώς και οργανωτικές δομές, που θα αποσκοπούν στην καλύτερη δυνατή διαχείριση πελατών και όχι προϊόντων.

Όσον αφορά τους χρήστες τις ηλεκτρονικής τραπεζικής, μπορούμε να πούμε ότι στην πλειοψηφία τους, είναι νεαρά άτομα, ηλικίας από 25-35 ετών, με υψηλό μορφωτικό επίπεδο και υψηλό εισόδημα. Άτομα δηλαδή εξοικειωμένα με την τεχνολογική ανάπτυξη, τα οποία δεν διστάζουν να ρισκάρουν χρησιμοποιώντας μία νέα υπηρεσία, η οποία όμως είναι ικανή να απλουστεύσει πολλά προβλήματα της καθημερινής τους ζωής.

Οι έλληνες καταναλωτές, έχουν δείξει ότι δύσκολα εμπιστεύονται κάτι άγνωστο σε αυτούς, πόσο μάλλον όταν αυτό έχει να κάνει με τη διαχείριση των χρημάτων τους. Έτσι το ποσοστό χρήσης του e-banking στη χώρα μας βρίσκεται ακόμα σε χαμηλά επίπεδα.

Ο κύριος τόπος πρόσβασης, των χρηστών της ηλεκτρονικής τραπεζικής , στο διαδίκτυο και κατά συνέπεια στους ηλεκτρονικούς τραπεζικούς τους λογαριασμούς, είναι το σπίτι και ο χώρος εργασίας ενώ μόνο ένα μικρό ποσοστό των χρηστών μέχρι σήμερα, διαχειρίζεται τους λογαριασμούς του μέσω κινητού τηλεφώνου. Η πλειοψηφία των χρηστών του Internet Banking που έλαβαν μέρος στην έρευνα μας, χρησιμοποιούν σύνδεση ADSL για να συνδεθούν στο Internet.

Το μεγαλύτερο ποσοστό των χρηστών της online τραπεζικής, αρχικά προτιμούν μόνο να ενημερώνονται για τα υπόλοιπα των λογαριασμών τους αλλά με την πάροδο του χρόνου και αφού έχουν εξοικειωθούν με την συγκεκριμένη υπηρεσία αρχίζουν να πραγματοποιούν και άλλες συναλλαγές.

Τα οφέλη που αποκομίζουν οι χρήστες τις ηλεκτρονικής τραπεζικής από τη χρήση της, είναι πολλά. Τα σημαντικότερα από αυτά σύμφωνα με την έρευνα είναι ότι δεν χρειάζεται πια να περιμένουν με τις ώρες στις ουρές των τραπεζών για να πραγματοποιήσουν τις συναλλαγές τους, αφού μπορούν να το κάνουν καθισμένοι στον καναπέ του σπιτιού τους ή στην καρέκλα του γραφείου τους. Επίσης γνωρίζουν ότι η τράπεζά τους δεν κλείνει ποτέ αφού το e-banking τους δίνει τη δυνατότητα να πραγματοποιούν όποια συναλλαγή επιθυμούν οποιαδήποτε ημέρα της εβδομάδας καθώς και να ενημερώνονται για τα υπόλοιπα τους όποτε αυτοί το επιθυμούν.

Το επίπεδο γνώσης των χρηστών της ηλεκτρονικής τραπεζικής σε θέματα σχετικά με την ασφάλεια των ηλεκτρονικών τους συναλλαγών, τους κινδύνους και τις απειλές που πιθανόν να αντιμετωπίσουν καθώς και τους τρόπους με τους οποίους μπορούν να προστατευθούν, δεν είναι ακόμα αρκετά υψηλό στη χώρα μας.

Σύμφωνα με τα αποτελέσματα της έρευνας, ένας στους δύο χρήστες της ηλεκτρονικής τραπεζικής είναι ενημερωμένος για τους περισσότερους κινδύνους που μπορούν να προκύψουν κατά τη στιγμή που είναι συνδεδεμένος με τον τραπεζικό του λογαριασμό. Το ίδιο ισχύει και για τους τρόπους προστασίας που μπορούν να χρησιμοποιήσουν οι χρήστες για να αποφύγουν τους κινδύνους αυτούς. Για το λόγο αυτό, οι περισσότερες τράπεζες θα πρέπει να ενημερώνουν τους πελάτες τους έγκαιρα για τις απειλές που μπορεί να συναντήσουν κατά την

πλοήγηση τους στις υπηρεσίες της online τραπεζικής καθώς και για τις μεθόδους προστασίας που διαθέτουν.

Γενικά θα μπορούσαμε να πούμε, ότι στο μεγαλύτερο ποσοστό τους, οι χρήστες έχουν θετική άποψη για το internet banking, θεωρούν ότι είναι εύκολο στη χρήση του και γρήγορο στην εκτέλεση συναλλαγών. Θεωρούν ότι υπάρχει οργάνωση από τις τράπεζες σε ότι αφορά τη διεξαγωγή ηλεκτρονικών συναλλαγών και θα προέτρεπαν και άλλους να χρησιμοποιήσουν τις online υπηρεσίες. Τέλος, είναι αρκετά ευχαριστημένοι και από το επίπεδο ασφάλειας το οποίο προσφέρουν οι ελληνικές τράπεζες στις ηλεκτρονικές συναλλαγές.

Χρόνο με το χρόνο το ποσοστό των χρηστών της ηλεκτρονικής τραπεζικής στη χώρα μας αυξάνεται σημαντικά και προβλέπεται ότι σε μερικά χρόνια η ηλεκτρονική τραπεζική θα έχει γίνει αναπόσπαστο κομμάτι της καθημερινότητας μας.

# Βιβλιογραφία

## Άρθρα περιοδικού τύπου


1. Γκαργκάνας, Ν., «Η εξέλιξη του ελληνικού τραπεζικού συστήματος την τελευταία δεκαετία», εφημερίδα Εξπρές, τεύχος Νοεμβρίου 2003.

2. Εναλλακτικά Δίκτυα: « Η τραπεζική δεν είναι πια όπως τη γνωρίζαμε», Netweek περιοδικό, 13 Οκτωβρίου 2003

3. Ηλεκτρονικές απάτες - PHARMING / Παραπλάνηση, «Απάτη με pharming (παραπλάνηση): ανακατεύθυνση του browser σε ψεύτικες ιστοσελίδες.», www.nuked.gr

4. «Η τράπεζα στο σπίτι σας», Το ΒΗΜΑ, 29/04/2001, Σελ.: Ε18, Κωδικός άρθρου: Β13250Ε181, ID: 234903, www.tovima.gr

5. Καρακατσάνης Κ., «Αφιέρωμα e-banking», Περιοδικό Ram, Τεύχος 184,Σελ.115- 140.

6. Μαλλιαρά Ν., «Νέο πεδίο «αναμέτρησης» των τραπεζών, Το Διαδίκτυο μειώνει δραστικά το λειτουργικό κόστος των τραπεζικών ιδρυμάτων και προσελκύει πελατεία», Το ΒΗΜΑ, 17/06/2001, Σελ.: D10,Κωδικός άρθρου: Β13289D101, ID : 236315, www.tovima.gr

7. «Ουραγός η Ελλάδα στη χρήση του διαδικτύου», 04/12/07 Ναυτεμπορική Σελίδα 6, www.naftemporiki.gr

8. Παναγόπουλος Θ., «Κωδικοί μιας χρήσης για ασφαλείς συναλλαγές μέσω Internet», 19/9/2007, www. Silicon.com

9. Συρμακέζης Σ., «24ωρες τραπεζικές συναλλαγές», Απαντά ο διευθυντής Ηλεκτρονικής Τραπεζικής και Καρτών της Τράπεζας Πειραιώς, Το ΒΗΜΑ, 17/08/2003 , Σελ.: D24 Κωδικός άρθρου: B13940D241,www.tovima.gr

10. Συρμακέζης Σ., «Περισσότερες συναλλαγές από τον ηλεκτρονικό υπολογιστή, Οι τράπεζες πρέπει να παρουσιάσουν τώρα τη νέα γενιά του Internet banking», Το ΒΗΜΑ, 31/12/2000 , Σελ.: Ε05, Κωδικός άρθρου: B13156E051, ID:231429, www.tovima.gr

11. «Τι πρέπει να προσέχετε στις συναλλαγές μέσω Internet banking», Το ΒΗΜΑ,23/09/2007 , Σελ.: D29, Κωδικός άρθρου: B15172D292, ID: 289509,www.tovima.gr

12. Φετοκάκης Γ., «E-banking στις υπηρεσίες σας», Περιοδικό PC Magazine, τεύχος 37, Σελ. 98-110.

## Βιβλία

1. 5ο Retailing Bank Forum (2005), «Οι προκλήσεις και απαιτήσεις της πελατοκεντρικής στρατηγικής των τραπεζικών οργανισμών».

2. Αγγέλης Β. (2005), «Η βίβλος του e- banking», εκδόσεις Νέων Τεχνολογιών

3. Βενέτης Χ., (2007), «Personal Firewalls».

4. Γεωργιάδου Μ., Ζιαζιάς Α., (2007), «Ασφάλεια στο διαδίκτυο», Διπλωματική εργασία, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

5. Γκριτζαλης Δ., Γκριτζαλης Σ., Κατσικα Σ. (2003), «Ασφάλεια Δικτύων υπολογιστών», Εκδόσεις Παπασωτηρίου

6. Γλύκας Μ., Ξηρογιάννης Γ. (2004), «Στρατηγική ηλεκτρονικού επιχειρήν χρηματοπιστωτικών ιδρυμάτων», εκδόσεις Ελληνικά γράμματα.

7. Calisti M., Rollon K., Lang W., Nolle D. (2000), «Internet Banking: Market Developments and regulatory issues, Society of government economists Conference».

8. Centeno C. (2002), «Building Security and Customer trust in internet payments – The potential of soft measures».

9. Comparison of smart cards technologies, (Μάιος 2002)

10. Daniel E. (1999), «Provision of electronic banking in the UK and the republic of Ireland», MCB University Press, pp. 72-82

11. Εγνατία Τράπεζα, (2004), «E-Banking – Ηλεκτρονική τραπεζική»

12. Ένωση Ελληνικών Τραπεζών (2000), «e-Banking: Νέοι ορίζοντες στο τραπεζικό επιχειρείν»

13. Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (2005), «Συστήματα ηλεκτρονικών πληρωμών»

14. eBusinessForum (2001), «Συνοπτική Παρουσίαση Πανελλαδικής Έρευνας για τη Χρήση των Υπολογιστών, Internet και Κινητής Τηλεφωνίας»

15. eBusinessForum (Οκτώβριος 2002), «Έξυπνες Κάρτες», Ομάδα εργασίας Γ3

16. eBusinessForum (2004), «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης», Ομάδα εργασίας Ε2

17. Θωμάς Κ. Πλάτων (2000), «Ερευνα αγοράς Πρακτικός Οδηγός», εκδόσεις Interbooks.

18. Ινστιτούτο Εργασίας ΟΤΟΕ (1996), «Τεχνικός – Οργανωτικός Εκσυγχρονισμός του Τραπεζικού Συστήματος», ΙΝΕ/ ΟΤΟΕ.

19. Κάπα Research (2007), «Η σχέση των ΜΜΕ με το τραπεζικό σύστημα»

20. Kantor capital A.E., (2006), «Επισκόπηση τραπεζικού τομέα 2005».

21. Κασκαβέλης Χ. (2002), e-Banking: «Τι επιφυλάσσει το Μέλλον», e-Banking Forum

22. Κουτούπης Θ., (1992), «Νέος Πρακτικός οδηγός Δημοσίων Σχέσεων», εκδόσεις Ν.Σ Γαλιλαίος και ΣΙΑ Ο.Ε.

23. Λιάκος Η., Τρίγκας Ε. (2001), «e-Banking - Αξιολόγηση σχετικών προγραμμάτων»

24. Λουκά Σ. (2005), «Διαδίκτυο για την επαρχία».

25. Λυμπερόπουλος Κων/νος (1994), «Στρατηγικό Τραπεζικό Μάρκετινγκ», εκδόσεις Interbooks.

26. Μαλλιάρης Π., (2001), «Εισαγωγή στο Marketing», εκδόσεις Σταμούλης Α.Ε.

27. Metron Analysis (Ιούλιος 2001), «Προσεγγιστική παρουσίαση της εξέλιξης του Internet παγκοσμίως», Αναδημοσίευση στο Παραδοτέο "Ηλεκτρονικό Επιχειρείν και Πολίτης-Καταναλωτής", Ομάδα Εργασίας Α1, eBusinessForum, http://www.ebusinessforum.gr/old_omades/docs/final_1.doc

28. Metron Analysis (2009), «Έρευνα για το internet στην Ελλάδα».

29. Mitnick K., (2003), «Η Τέχνη της απάτης – Ο ανθρώπινος παράγοντας στην ασφάλεια», εκδόσεις Ωκεανίδα.

30. Μπάσιος Χ., (2007), «Mobile Payment».

31. Money Show (2007), «Ηλεκτρονική τραπεζική».

32. Οικονομίδης Α., Κακγάνη Α. (2002), «Smart Cards», Πανεπιστήμιο Μακεδονίας.

33. Ορφανίδου Ε., (2006), «Αντιμετώπιση θεμάτων ευχρηστίας κατά το σχεδιασμό ηλεκτρονικής τραπεζική», Τράπεζα Πειραιώς.

34. Παπαδόπουλος Μ., (2005), «Phishing - Η νέα μέθοδος εξαπάτησης στο internet, ηλεκτρονικό Έγκλημα».

35. Παρατηρητήριο για την Κοινωνία της Πληροφορίας (2008), «Ταυτότητα Χρηστών Internet στην Ελλάδα».

36. Πατρινός Δ., (1999), «Χρήμα – Τράπεζες και Χρηματοπιστωτική Πολιτική»,εκδόσεις Παπαζήση

37. Πομπόρτσης Α., Παπαδημητρίου Γ. (2003), «Ασφάλεια Δικτύων Υπολογιστών».

38. Πουλάκης Δ.,( 2005), «Κρυπτογραφία, η επιστήμη της ασφαλούς επικοινωνίας», εκδόσεις Ζήτη.

39. Σηφακάκη Μ., Πάστρα Ε., Σκαρμούτσος Ν., Σδόγκου Α., (2005),«Αξιολόγηση Portals», hci.gr

40. Σύνδεσμος Επιχειρήσεων Πληροφορικής και επικοινωνιών Ελλάδος (2005), «Πλάνο δράσης και ανάπτυξης του internet στην Ελλάδα».

41. Συρμακέζης Σ., (2005), «Building an electronic Bank».

42. Τσουρβάκας Γ., (2006), «Internet και Ελληνική Οικογένεια», Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

43. United States Internet Council (2000), «State of the Internet», Διαθέσιμο ηλεκτρονικά στη δικτυακή διεύθυνση http://www.usic.org

44. Χαλάστης Κ., (2007), «Ηλεκτρονική υπογραφή – Παρούσα κατάσταση», Προοπτικές, 12ο Συνέδριο εφαρμογών πληροφορικής.

45. Χανιωτάκη Μαρία, (2007), «Η ηλεκτρονική προώθηση των τραπεζικών προϊόντων», Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Μακεδονίας.

46. Χολέβας Ι., (1995), «Τραπεζικές Εργασίες», εκδόσεις Interbooks.

## Διαδικτυακοί τόποι

1. Alpha bank, (07/02/2010 ), http://www.alpha.gr
2. Computer για όλους ( 02/02/2010 ), http://www.cgomag.gr
3. Εθνική Τράπεζα ( 07/02/2010), http://www.nbg.gr
4. Εμπορική Τράπεζα ( 07/02/2010 ), http://www.combank.gr
5. Eurobank, ( 07/02/2010 ), http://www.eurobank.gr
6. Euro 2 Day, ( 12/02/2010 ), www.euro2day.gr
7. Ινστιτούτο Εργασίας (ΙΝΕ) ΟΤΟΕ, http://www.otoe.gr
8. Ναυτεμπορική, ( 16/ 02/2010), www.naftemporiki.gr
9. Οικονομικός ταχυδρό/ος ( 16/02/2010 ) ,http://oikonomikos.dolnet.gr
10. Περιοδικό Chip ( 18/02/2010 ) , http://www.chip.gr

11. Περιοδικό Χρήμα ( 19/02/2010 ), http://www.xrima.gr
12. Τράπεζα Marfin ( 07/02/2010 ), http://www.marfinbank.gr
13. Win bank, ( 07/02/2010 ), http://www.winbank.gr
14. www.ecommerce.internet.com ( 22/02/2010 )
15. www.hellasnet.gr (22/02/2010 )
16. www.government.gr ( 22/02/2010 )
17. www.infosociety.gr ( 22/02/2010 )
18. www.capitallink.com ( 01/03/2010 )
19. www.thea.gr ( 02/03/2010 )
20. www.intersoft.gr ( 02/03/010 )
21. www.compulink.gr ( 05/03/2010 )
22. www.imerisia-ver.gr ( 09/03/2010 )
23. www.esee.gr ( 11/03/2010 )
24. www.edweek.gr ( 12/03/2010 )
25. www.ekt.gr ( 14/03/2010 )
26. www.economics.gr ( 14/03/2010 )
27. www.unic.gr ( 14/03/2010 )
28. www.saferinterrnet.gr ( 14/03/2010 )

## Μηχανές αναζήτησης

1. www.google.com
2. www.in.gr
3. www.forthnet.gr

# Παραρτήματα

## Παράρτημα 1: Ουραγός η Ελλάδα στη χρήση του διαδικτύου

*Αποκαλυπτικά συμπεράσματα της Eurostat*

# Ουραγός η Ελλάδα στη χρήση του Διαδικτύου

Το πρώτο τρίμηνο του 2007, μόνο ένα στα 14 ελληνικά νοικοκυριά είχε πρόσβαση στο ευρυζωνικό (γρήγορο) Ιντερνετ και η χώρα μας ήταν τελευταία στην Ευρωπαϊκή Ενωση, στην οποία ο μέσος όρος διείσδυσης ήταν 42%. [ΒΡΥΞΕΛΛΕΣ, ΤΟΥ ΑΝΤΑΠΟΚΡΙΤΗ ΜΑΣ ΝΙΚΟΥ ΜΠΕΛΛΟΥ]

**ΣΥΜΦΩΝΑ** με τα στοιχεία που έδωσε χθες στη δημοσιότητα η Eurostat, το πρώτο τρίμηνο του 2007 το 7% των ελληνικών νοικοκυριών είχε πρόσβαση στο γρήγορο Ιντερνετ, έναντι 4% το 2006. Προτελευταίοι ήταν οι Ρουμάνοι με 8% και ακολουθούν οι Βούλγαροι με 15%.

Στην πρώτη θέση στην Ευρωπαϊκή Ενωση σε πρόσβαση στο γρήγορο Ιντερνετ ήταν οι Ολλανδοί, με ποσοστό διείσδυσης 74% των νοικοκυριών, στη δεύτερη θέση οι Δανοί με 70% και στην τρίτη οι Σουηδοί με 67%.

Στο απλό Ιντερνετ, η διείσδυση των ελληνικών νοικοκυριών έφτασε 25% το πρώτο τρίμηνο του 2007, από 23% το 2006. Χειρότερη επίδοση από την Ελλάδα στο απλό Ιντερνετ είχαν μόνο η Ρουμανία (14% το ποσοστό διείσδυσης) και η Βουλγαρία (17%). Ο μέσος όρος στην Κοινότητα ήταν υπερδιπλάσιος της Ελλάδας (54%), ενώ η Ολλανδία βρίσκεται στην πρώτη θέση με 83%, ακολουθούμενη από τη Σουηδία (79%) και τη Δανία (78%). Αλλο εντυπωσιακό στοιχείο της έρευνας στην Ελλάδα είναι ότι μόνο το 26% από τα νοικοκυριά που έχουν πρόσβαση στο Διαδίκτυο κάνει χρήση του ηλεκτρονικού ταχυδρομείου (e-mail), όταν ο μέσος όρος στην Κοινότητα είναι 50%.

Στις άλλες επιμέρους εργασίες, το 36% απάντησε ότι χρησιμοποιεί τη μηχανή αναζήτησης, το 13% το σύστημα για την αντιμετώπιση των ιών, το 6% χρησιμοποιεί το Ιντερνετ για τηλεφωνικές επικοινωνίες, το 6% για ανταλλαγές βίντεο και μουσικής, ενώ το 5% έχει δημιουργήσει δική του ιστοσελίδα. Σε όλες τις επιμέρους χρήσεις, η Ελλάδα βρίσκεται στις τελευταίες θέσεις.

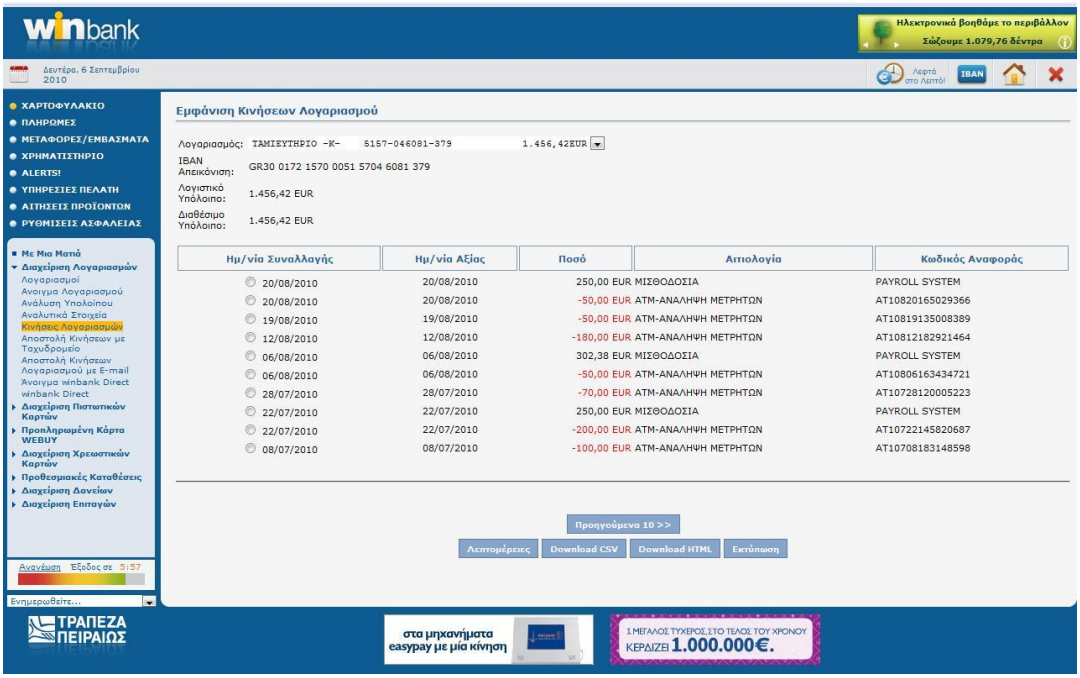
[SID:26020021]

**ΧΡΗΣΗ ΤΟΥ ΙΝΤΕΡΝΕΤ ΣΤΗΝ Ε.Ε.**

| | Πρόσβαση σε Ιντερνετ | | Πρόσβαση σε γρήγορο Ιντερνετ | |
|---|---|---|---|---|
| | 2006 | 2007* | 2006 | 2007* |
| Ε.Ε. | 49% | 54% | 30% | 42% |
| Ελλάδα | 23% | 25% | 4% | 7% |
| Κύπρος | 37% | 39% | 12% | 20% |
| Βέλγιο | 54% | 60% | 48% | 56% |
| Βουλγαρία | 17% | 19% | 10% | 15% |
| Τσεχία | 29% | 35% | 17% | 28% |
| Δανία | 79% | 78% | 63% | 70% |
| Γερμανία | 67% | 71% | 34% | 50% |
| Εσθονία | 46% | 53% | 37% | 48% |
| Ιρλανδία | 50% | 57% | 13% | 31% |
| Ισπανία | 39% | 45% | 29% | 39% |
| Γαλλία | 41% | 49% | 30% | 43% |
| Ιταλία | 40% | 43% | 16% | 35% |
| Λετονία | 42% | 51% | 23% | 32% |
| Λιθουανία | 35% | 44% | 19% | 34% |
| Λουξεμβούργο | 70% | 75% | 44% | 58% |
| Ουγγαρία | 32% | 38% | 22% | 33% |
| Ολλανδία | 80% | 83% | 66% | 74% |
| Αυστρία | 52% | 60% | 33% | 46% |
| Πολωνία | 36% | 41% | 22% | 30% |
| Πορτογαλία | 35% | 40% | 24% | 30% |
| Ρουμανία | 14% | 22% | 5% | 8% |
| Σλοβενία | 54% | 58% | 34% | 44% |
| Φινλανδία | 65% | 69% | 53% | 60% |
| Σουηδία | 77% | 79% | 51% | 67% |
| Ην. Βασίλειο | 63% | 67% | 44% | 57% |

*Α΄ τρίμηνο 2007

## Παράρτημα 2: Εμφάνιση Κινήσεων λογαριασμού




## Παράρτημα 3: Αίτηση μεταφοράς υπολοίπου

## Παράρτημα 4: Ηλεκτρονικές απάτες - PHARMING / Παραπλάνηση

### Απάτη με pharming (παραπλάνηση): ανακατεύθυνση του browser σε ψεύτικες ιστοσελίδες.

Έχετε ακούσει για το pharming, όπου η κίνηση του Διαδικτύου ανακατευθύνεται από μία τοποθεσία σε μία άλλη, πανομοιότυπη που είναι όμως απάτη; "Pharming" σημαίνει όταν εγκληματίες χάκερ ανακατευθύνουν την κίνηση του Διαδικτύου από μία ιστοσελίδα σε μια άλλη, πανομοιότυπη έτσι ώστε να σας ξεγελάσουν και να καταχωρίσετε το όνομα χρήστη και τον κωδικό χρήστη στη βάση δεδομένων της πλαστής ιστοσελίδας. Ιστοσελίδες τραπεζών ή αντίστοιχων οικονομικών οργανισμών είναι συχνά στόχοι τέτοιων επιθέσεων, κατά τις οποίες εγκληματίες προσπαθούν να αποσπάσουν προσωπικά δεδομένα, με σκοπό να βρουν πρόσβαση στον τραπεζικό σας λογαριασμό, να κλέψουν την ταυτότητά σας ή να διαπράξουν άλλου είδους απάτη στο όνομά σας.

Το Pharming (παραπλάνηση), η χρήση δηλαδή ψεύτικων ιστοσελίδων πιθανόν να θυμίζει τις απάτες ψαρέματος από ηλεκτρονικά μηνύματα, όμως η παραπλάνηση είναι πιο ύπουλη, αφού μπορεί να κατευθυνθείτε σε μία ψεύτικη ιστοσελίδα χωρίς να το γνωρίζετε.

Εώς σήμερα έχουν γίνει αρκετές επιθέσεις, γεγονός που έχει αρχίσει να ανησυχεί αρκετά κυβερνήσεις και επιχειρήσεις. Είναι επίσης σημαντικό να θυμάστε πως το Διαδίκτυο είναι μια δωρεάν και ανεξάρτητη πηγή, όπως μία βιβλιοθήκη ή άλλες δημόσιες υπηρεσίες, στον τόπο όπου ζείτε. Εάν παρατηρήσετε κάτι ύποπτο σχετικά με μία ιστοσελίδα που εμπιστεύεστε, αναφέρετέ το — τηλεφωνικά εάν είναι δυνατόν—στην επιχείρηση ή στον ιδιοκτήτη της ιστοσελίδας.

Πώς μπορεί κάποιος απατεώνας που θέλει να με παραπλανήσει, να κατευθύνει το browser μου σε κάποια άλλη ιστοσελίδα; Με τη χρήση μιας διαδικασίας που ονομάζεται "δηλητηρίαση DNS" κατά την οποία κάποιος εισβολέας αποκτά πρόσβαση στις τεράστιες βάσεις δεδομένων που χρησιμοποιούν οι πάροχοι υπηρεσιών Διαδικτύου για να δρομολογήσουν τη διαδικτυακή κίνηση και μπορεί να κάνει τροποποιήσεις σε κάποιο σημείο έτσι ώστε να εκτρέπεστε στην ψεύτικη ιστοσελίδα πριν αποκτήσετε πρόσβαση σε αυτή που τελικά επιθυμούσατε. Κάποιες εταιρίες υποστηρίζουν πως το λογισμικό firewall (τείχος

προστασίας) που χρησιμοποιούν προστατεύει και από την παραπλάνηση (pharming).

Κάποιοι πάροχοι υπηρεσιών διαδικτυακής ασφάλειας πιστεύουν πως οι πελάτες τους που καθοδηγούν όλη τους την διαδικτυακή κίνηση μέσω των δικών τους, ασφαλών, διακομιστών είναι και προστατευμένοι από επιθέσεις παραπλανήσεις. Η φύση της παραπλάνησης υποδεικνύει το αντίθετο αλλά, ανεξάρτητα από το τι υποστηρίζει η κάθε εταιρεία, είναι καλή ιδέα να αναζητάτε προσεκτικά τα προϊόντα ασφαλείας πριν επενδύσετε και εμπιστευτείτε κάποιες λύσεις λογισμικού.

Δεν μπορώ να αναγνωρίσω εάν μία ιστοσελίδα είναι ψεύτικη απλά μετακινώντας το δείκτη πάνω από τα link και παρατηρώντας εάν ο κώδικας με οδηγεί σε κάποιο εμφανώς άσχετο σημείο εκτός ιστοσελίδας; Όχι απαραίτητα. Οι ψεύτικες ιστοσελίδες που χρησιμοποιούνται στις απάτες παραπλάνησης συνήθως "πλαστογραφούν" τα link τους έτσι ώστε να μοιάζουν ακριβώς με αυτά που αναμένετε να δείτε, ακόμη και στον κώδικα που εμφανίζεται όταν το ποντίκι περάσει πάνω από αυτά. Επίσης, οι ιστοσελίδες πιθανόν να αλλάζουν τον κώδικα των δικών τους links αρκετά συχνά και για διάφορους λόγους, όπως όταν αναβαθμίζουν το λογισμικό τους, την πλατφόρμα του διακομιστή τους ή τις μεθόδους ανάλυσης των στατιστικών κίνησης της ιστοσελίδας τους.

## Παράρτημα 5:Τι πρέπει να προσέχετε στις συναλλαγές μέσω Internet banking

### * Για να ελαχιστοποιήσουν κρούσματα χάκινγκ, οι τράπεζες έχουν υιοθετήσει τα απαραίτητα μέτρα για τη διατήρηση του υψηλότερου δυνατού επιπέδου ασφαλείας κατά τη διάρκεια των συναλλαγών

Πληθώρα συναλλαγών από τον προσωπικό τους χώρο μπορούν να πραγματοποιήσουν πλέον οι πελάτες των τραπεζών, οι οποίες αναβαθμίζουν συνεχώς τα εναλλακτικά δίκτυα με νέες υπηρεσίες, εκμεταλλευόμενες τα άλματα που σημειώνονται στην τεχνολογία τα τελευταία χρόνια. Ο αριθμός των ελληνικών νοικοκυριών που κάνουν χρήση του Internet banking αυξάνεται χρόνο με τον χρόνο. Πλέον κάποιος από το σπίτι του μπορεί ηλεκτρονικά να πληρώσει τον ΦΠΑ ή τον φόρο εισοδήματος, τους λογαριασμούς του (ΟΤΕ, ΔΕΗ, κινητή τηλεφωνία), τις οφειλές από τις πιστωτικές κάρτες, το ενοίκιο ή να αποστείλει εμβάσματα στο εξωτερικό. Τα εναλλακτικά δίκτυα των τραπεζών (Internet banking, phone και mobile banking) προσφέρουν ευκολία και άνεση, καθώς ο πελάτης μπορεί να πραγματοποιήσει τις συναλλαγές του απ' οπουδήποτε, την ημέρα και την ώρα που επιθυμεί, χωρίς να δεσμεύεται από τα ωράρια λειτουργίας των καταστημάτων και αποφεύγοντας τον συνωστισμό και το χάσιμο χρόνου των παραδοσιακών δικτύων. Καθώς όμως βελτιώνονται και εμπλουτίζονται οι υπηρεσίες των τραπεζών, αυξάνονται και οι ηλεκτρονικοί ληστές, οι οποίοι επίσης εκσυγχρονίζονται.

Η ευκολία της χρήσης και τα πλεονεκτήματα των εναλλακτικών δικτύων τα έχουν κάνει ευρέως αποδεκτά από τους πελάτες των τραπεζών. Ωστόσο, όπως συμβαίνει σε κάθε παρόμοια περίπτωση, η ευρεία αποδοχή των εναλλακτικών δικτύων έχει τραβήξει την προσοχή επίδοξων απατεώνων, οι οποίοι χρησιμοποιούν μια σειρά μεθόδων με σκοπό να αποσπάσουν προσωπικά στοιχεία των χρηστών και να πραγματοποιήσουν παράνομα κέρδη εις βάρος των τραπεζών, αλλά και εις βάρος των ανυποψίαστων πελατών. Για να ελαχιστοποιηθούν τα κρούσματα αυτά, οι τράπεζες από την πλευρά τους υιοθετούν όλα τα απαραίτητα μέτρα για τη διατήρηση του υψηλότερου δυνατού επιπέδου ασφαλείας κατά τη διάρκεια των συναλλαγών. Συγκεκριμένα, όλα τα ευαίσθητα προσωπικά δεδομένα των πελατών διαφυλάσσονται σε ειδικούς χώρους, κάθε επικοινωνία μεταξύ της τράπεζας και των υπολογιστών των χρηστών είναι κρυπτογραφημένη με τις πλέον σύγχρονες

μεθόδους κρυπτογράφησης, ενώ ακολουθούνται μέθοδοι διπλής ταυτοποίησης των χρηστών, ώστε να μην είναι δυνατή η πραγματοποίηση συναλλαγών από τρίτους.

Όπως σημειώνουν τραπεζικά στελέχη, *«αυτό που πρέπει να γίνει κατανοητό είναι ότι οι τράπεζες ουδέποτε έχουν πέσει θύματα των απατεώνων».* Η αλήθεια είναι ότι, αντιμέτωποι με τα υψηλά επίπεδα ασφαλείας των τραπεζικών συστημάτων, οι απατεώνες έχουν στραφεί προς τους πελάτες των εναλλακτικών δικτύων με αντικειμενικό σκοπό να αποκτήσουν τους προσωπικούς αριθμούς πρόσβασης στα δίκτυα. Για να το επιτύχουν αυτό χρησιμοποιούν ένα σύνολο μεθόδων (phishing) οι οποίες περιλαμβάνουν παραπλανητικές τηλεφωνικές κλήσεις και αποστολή παραπλανητικών e-mails, δημιουργία πλαστών ιστοσελίδων (spoofing), καθώς και εγκατάσταση ιών και άλλου κακόβουλου λογισμικού στους υπολογιστές των χρηστών (viruses, Trojans, keyloggers). Με τις παραπάνω μεθόδους προσπαθούν είτε να εκμαιεύσουν τις απαραίτητες πληροφορίες απευθείας από τους χρήστες των εναλλακτικών δικτύων ή να τις υφαρπάξουν με τεχνικές παρακολούθησης κατά την εισαγωγή τους.

Το βέβαιο είναι ότι όλοι οι χρήστες πρέπει να βρίσκονται σε εγρήγορση ώστε να μην πέσουν θύματα των παραπάνω κυκλωμάτων. Αναλυτικότερα, υπάρχουν κάποια απλά βήματα που πρέπει να ακολουθούν οι πελάτες των τραπεζών, ώστε να είναι βέβαιοι ότι θα έχουν το κεφάλι τους ήσυχο όταν πραγματοποιούν συναλλαγές online.
Συγκεκριμένα:

* **e-mails που σας ζητούν προσωπικά σας στοιχεία**. Η τράπεζα δεν πρόκειται να σας ζητήσει προσωπικά στοιχεία μέσω e-mail ή με οποιονδήποτε άλλον τρόπο.

* **Links που εμφανίζονται σε e-mails που φαίνεται να προέρχονται από την τράπεζα**. Οι επίδοξοι απατεώνες συχνά καθοδηγούν τα υποψήφια θύματα σε ιστοσελίδες που μοιάζουν με τις επίσημες ιστοσελίδες των τραπεζών. Εκεί ζητούν προσωπικά στοιχεία ή κατεβάζουν στον υπολογιστή των επισκεπτών κακόβουλο λογισμικό.

* **Web site της τράπεζας**. Για να μεταβείτε στο site της τράπεζας πληκτρολογείτε την πλήρη διεύθυνση στη γραμμή διευθύνσεων του προγράμματος πλοήγησης που

χρησιμοποιείτε. Αν δεν θέλετε να πληκτρολογείτε τη διεύθυνση, αποθηκεύστε τη στα Αγαπημένα (Favorites, Bookmarks, ανάλογα με το πρόγραμμα πλοήγησης).

* **Viruses και κακόβουλο λογισμικό (spyware, Trojans, keyloggers)**. Ενημερώνετε συχνά τα προγράμματα με τις τελευταίες εκδόσεις και κάνετε περιοδικούς ελέγχους του υπολογιστή σας για τυχόν κακόβουλο λογισμικό που έχει εγκατασταθεί εν αγνοία σας.

**Το ΒΗΜΑ, 23/09/2007 , Σελ.: D29**
**Κωδικός άρθρου: B15172D292**
**ID: 289509**

**Παράρτημα 6**

# ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ 1: ΤΡΑΠΕΖΕΣ

Επωνυμία :…….
Υποκατάστημα:…….

1) Ποια είδη του e-banking προσφέρετε;
   - □ Internet Banking □ Phone Banking
   - □ Mobile Banking □ Interactive TV Banking

2) Ποιες υπηρεσίες e-banking προσφέρετε;

   ➢ Υπολογισμός δόσεων δανείων
   □ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

   ➢ Μετατροπή νομισμάτων
   □ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

   ➢ Υπολογισμός IBAN
   □ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

   ➢ Αίτηση παραγγελίας μπλοκ επιταγών
   □ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

   ➢ Αίτηση για παραγγελία συναλλάγματος
   □ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

   ➢ Αίτηση για δάνειο
   □ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

   ➢ Αίτηση ανοίγματος λογαριασμού
   □ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Πληροφορίες δανείων

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Πληροφορίες Επιταγών

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Πληροφορίες καρτών

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Πληροφορίες λογαριασμών

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Προμήθειες συναλλαγών

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Κατάσταση εντολών

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Μαζικές πληρωμές-Μισθοδοσίες

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Πληρωμές Ασφαλιστικών

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Πληρωμές σταθερής και κινητής τηλεφωνίας

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Πληρωμές Λογαριασμών ΔΕΚΟ

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Πληρωμές Δημοσίου

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Πληρωμές πιστωτικών καρτών

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να Προσφέρει

➢ Πληρωμές δανείων

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να Προσφέρει

➢ Εμβάσματα Εξωτερικού

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Εμβάσματα Εσωτερικού

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Μεταφορές σε λογαριασμό τρίτου

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

➢ Μεταφορές σε λογαριασμό ιδίου

□ Προσφέρει □ Δεν προσφέρει □ Σκοπεύει να προσφέρει

3) Ποιες υπηρεσίες Mobile Banking προσφέρετε;
   - □ Πληροφορίες δανείων
   - □ Πληροφορίες καρτών
   - □ Πληροφορίες λογαριασμών
   - □ Κατάσταση εντολών
   - □ Πληρωμές σταθερής και κινητής τηλεφωνίας
   - □ Πληρωμές λογαριασμών ΔΕΚΟ
   - □ Πληρωμές δημοσίου
   - □ Πληρωμές πιστωτικών καρτών
   - □ Πληρωμές δανείων
   - □ Εμβάσματα εξωτερικού
   - □ Εμβάσματα εσωτερικού
   - □ Μεταφορές σε λογαριασμό τρίτου
   - □ Μεταφορές σε λογαριασμό ιδίου

4) Κατά πόσο γνωρίζετε και χρησιμοποιείτε τις παρακάτω πρόσθετες υπηρεσίες e-Banking;

➢ Ολοκληρωμένα portals

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Αυτόματο άνοιγμα καταθετικού λογαριασμού

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Σύνδεση internet banking με συστήματα logistics

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Electronic Bill & Presentment (EBPP)

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Συναλλαγές πραγματικού χρόνου

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ On-line εισαγωγές-εξαγωγές

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Πώληση ασφαλιστικών προϊόντων

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Alerts

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Ticketing

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Προπληρωμένες κάρτες αγορών στο Internet

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Πληρωμή υπηρεσιών

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Πληρωμή μέσω τραπεζικού λογαριασμού

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Επικοινωνία μέσω Web Service

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Μετάβαση σε ασφαλή σελίδα της τράπεζας

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Εισπράξεις από αρχεία με μαζικές εντολές πελατών

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Εισπράξεις από τηλεφωνικές πληρωμές πελατών

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

➢ Εισπράξεις από Internet sites

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

- Χρηματιστηριακές συναλλαγές

□ Γνωρίζω ΔΕΝ χρησιμοποιώ □ Γνωρίζω ΚΑΙ χρησιμοποιώ □ ΔΕΝ γνωρίζω

5) Χρησιμοποιείτε νέες τεχνολογίες και αν ναι πόσο αποτελεσματικές είναι;

- EDI, e-ERP, CRM
  - □ Δεν χρησιμοποιώ
  - □ Καθόλου □ Λίγο □Μέτρια □Πολύ □Πάρα πολύ

- Biometrics
  - □ Δεν χρησιμοποιώ
  - □Καθόλου □ Λίγο □Μέτρια □Πολύ □Πάρα πολύ

- Ψηφιακές υπογραφές
  - □ Δεν χρησιμοποιώ
  - □Καθόλου □ Λίγο □Μέτρια □Πολύ □Πάρα πολύ

- iTV
  - □ Δεν χρησιμοποιώ
  - □Καθόλου □ Λίγο □Μέτρια □Πολύ □Πάρα πολύ

- ADSL
  - □ Δεν χρησιμοποιώ
  - □Καθόλου □ Λίγο □Μέτρια □Πολύ □Πάρα πολύ

- Remote or Mobile Terminal
  - □ Δεν χρησιμοποιώ
  - □Καθόλου □ Λίγο □Μέτρια □Πολύ □Πάρα πολύ

- Wireless Devices
  - □ Δεν χρησιμοποιώ
  - □Καθόλου □ Λίγο □Μέτρια □Πολύ □Πάρα πολύ

- LAN-WAN
  - □ Δεν χρησιμοποιώ
  - □Καθόλου □ Λίγο □Μέτρια □Πολύ □Πάρα πολύ

- Intranet-Extranet
  - □ Δεν χρησιμοποιώ
  - □Καθόλου □ Λίγο □Μέτρια □Πολύ □Πάρα πολύ

6) Ποιες μεθόδους προστασίας e-banking χρησιμοποιείτε;
   - □ Firewalls
   - □ Single Sign On (SSO)
   - □ USB Tokens
   - □ Έξυπνες κάρτες (Smart Cards)
   - □ Πιστοποίηση δυο παραγόντων
   - □ Αρχές πιστοποίησης
   - □ Ψηφιακά Πιστοποιητικά
   - □ Ψηφιακές υπογραφές
   - □ PKI
   - □ Κρυπτογράφηση

7) Ποια από τα παρακάτω οφέλη πιστεύετε ότι έχει το e-banking για εσάς?
   - □ Διεύρυνση της αγοράς
   - □ Αύξηση εσόδων
   - □ Μείωση λειτουργικού κόστους
   - □ Μείωση του προσωπικού εξυπηρέτησης
   - □ Αναδιάρθρωση του προσωπικού εξυπηρέτησης
   - □ Βελτίωση της ανταγωνιστικότητας των υπηρεσιών
   - □ Αύξηση της διατήρησης πελατών
   - □ Βελτίωση της ικανοποίησης των πελατών (πιστοί πελάτες)

**Σας ευχαριστούμε πολύ.**

**Παράρτημα 7:**

# ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ 2:ΧΡΗΣΤΕΣ

Όνομα:……. Φύλο:…….. Ηλικία:……
Εκπαίδευση:…….....

1) Ετήσιο εισόδημα.
   - □ Έως 5000 ευρώ □ 5001-12000 ευρώ □ 12001-18000 ευρώ
   - □ 18001-30000 ευρώ □ 30001-50000 ευρώ □ 50001+ ευρώ

2) Τόπος πρόσβασης στο e-banking.
   - □ Σπίτι □ Χώρος εργασίας □ Κινητό τηλέφωνο
   - □ Internet cafe □ Σχολείο – Πανεπιστήμιο

3) Ποιο είναι το είδος της σύνδεσης σας;
   - □ Μισθωμένη γραμμή □ Ασύρματο δίκτυο
   - □ ISDN – PSTN □ ADSL

4) Πως βρίσκετε το internet στην Ελλάδα;
   - □ Ακριβό □ Αργό □ Έχει περιθώρια βελτίωσης
   - □ Άλλο ……..

5) Ποιες από τις παρακάτω υπηρεσίες e-banking χρησιμοποιείτε περισσότερο;
   - □ ενημέρωση υπολοίπου λογαριασμού
   - □ μεταφορά χρημάτων σε άλλους λογαριασμούς
   - □ πληρωμή λογαριασμών (ΔΕΗ, ΟΤΕ, κινητό, κ.α.)
   - □ πληρωμή ηλεκτρονικών αγορών
   - □ πληρωμή οφειλών σε υπηρεσίες δημοσίου (ΙΚΑ, εφορία κ.α.)
   - □ πάγιες εντολές πληρωμών(ενοίκιο κ.α.)
   - □ πληρωμή πιστωτικών καρτών
   - □ πληρωμή ασφαλίστρων
   - □ έκδοση πιστωτικής κάρτας
   - □ χρηματιστηριακές συναλλαγές

6) Ποιοι είναι οι λόγοι που δεν χρησιμοποιείτε το e-banking;
   - □ Προτιμώ να επισκέπτομαι την τράπεζα μου
   - □ Φοβάμαι να εκτελώ online τραπεζικές συναλλαγές
   - □ Δεν με έχει ενημερώσει η τράπεζα μου
   - □ Δύσκολη και πολύπλοκη διαδικασία-τεχνολογίες
   - □ Δεν γνωρίζω τι μπορεί να μου προσφέρει
   - □ Άλλο……

7) Γνωρίζετε τα είδη του e-banking και ποια χρησιμοποιείτε;
   - Internet Banking
     □ Ναι □ Όχι □ Χρησιμοποιώ
   - Mobile Banking
     □ Ναι □ Όχι □ Χρησιμοποιώ
   - Phone Banking και
     □ Ναι □ Όχι □ Χρησιμοποιώ
   - Interactive TV
     □ Ναι □ Όχι □ Χρησιμοποιώ

8) Γνωρίζετε τους κινδύνους που εγκυμονεί η ηλεκτρονική τραπεζική;
   - Sniffers
     □ Ναι □ Όχι
   - Key Loggers
     □ Ναι □ Όχι
   - Κοινωνική μηχανική
     □ Ναι □ Όχι
   - Δούρειοι Ίπποι
     □ Ναι □ Όχι
   - Phishing
     □ Ναι □ Όχι
   - Pharming
     □ Ναι □ Όχι

9) Γνωρίζετε τους τρόπους με τους οποίους μπορείτε να προστατευτείτε από τους κινδύνους αυτούς;

℘ Κρυπτογράφηση

□ Ναι □ Όχι

℘ Πιστοποίηση δυο παραγόντων

□ Ναι □ Όχι

℘ PKI

□ Ναι □ Όχι

℘ Έξυπνες κάρτες

□ Ναι □ Όχι

℘ Ψηφιακές υπογραφές

□ Ναι □ Όχι

℘ USB Tokens

□ Ναι □ Όχι

℘ Ψηφιακά πιστοποιητικά

□ Ναι □ Όχι

℘ Single sing on(SSO)

□ Ναι □ Όχι

℘ Αρχές πιστοποίησης

□ Ναι □ Όχι

℘ Firewalls

□ Ναι □ Όχι

10) Ποια στοιχεία των προσφερόμενων υπηρεσιών e-Banking σας ικανοποιούν:

□ Επαγγελματισμός □ Οργάνωση □ Ευκολία στην χρήση
□ Χρησιμότητα □ Ταχύτητα
□ Προστασία δικαιωμάτων και ιδιωτικής ζωής
□ Ικανοποίηση □ Ευκολία □ Είμαι θετικός

Τι σας έχει δυσαρεστήσει:
……
……..…….
…..……..

11) Είστε ικανοποιημένοι από τις μεθόδους προστασίας που χρησιμοποιεί η τράπεζα σας;

□ Καθόλου □ Λίγο □ Αρκετά
□ Πάρα πολύ □ ΔΞ/ΔΑ

12) Ποια οφέλη πιστεύετε ότι έχετε από τη χρήση του e-banking;

- Έλεγχο των λογαριασμών μου
- Περισσότερες επιλογές-καλύτερες συμφωνίες
- Ευκολία στης τραπεζικές μου συναλλαγές
- Δεν χρειάζονται πλέον επιταγές
- Χρήση υπηρεσιών από οπουδήποτε στον κόσμο
- Καλύτερη διαχείριση των εξόδων μου
- Άμεση πρόσβαση στον λογαριασμό μου
- Η τράπεζα δεν κλείνει ποτέ
- Δεν θα περιμένω ξανά στην ουρά

13) Ποιες πρόσθετες υπηρεσίες επιθυμείτε να προσφέρει η τράπεζα σας στο μέλλον;

- Ασφάλεια επιχειρήσεων
- Αγορά μετοχών-αμοιβαίων
- Διαχείριση χαρτοφυλακίου
- Υπηρεσίες e-φορολογίας
- Ασφαλιστικά πακέτα συνταξιοδότησης
- Οικονομικό προγραμματισμό

**Σας ευχαριστούμε πολύ.**