Τ.Ε.Ι. ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

e-Banking

ΜΙΧΑΗΛ ΜΙΧΑΛΗΣ
ΓΕΩΡΓΙΟΥ ΓΙΑΝΝΗΣ
ΜΙΧΑΗΛ ΛΑΖΑΡΟΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: Δρ. ΑΡΗΣ Ν. ΜΠΑΚΑΛΗΣ

ΠΑΤΡΑ - 2010

Περίληψη

Είναι πλέον φανερό ότι η τεχνολογία μετασχηματίζει τον τραπεζικό κλάδο. Σήμερα η ηλεκτρονική τραπεζική υπόσχεται την επανάσταση στις συναλλαγές μας με τις τράπεζες καθώς μεταφέρει την τράπεζα στην οθόνη του υπολογιστή μειώνοντας έτσι δραστικά το κόστος τόσο για τους πελάτες όσο και για την ίδια την τράπεζα.

Το νέο κανάλι διανομής των τραπεζικών προϊόντων και υπηρεσιών έχει πολλά πλεονεκτήματα. Παρά την πληθώρα των πλεονεκτημάτων που συνεπάγεται η νέα μορφή τραπεζικής εξυπηρέτησης, μερίδα πελατών εξακολουθεί ακόμα και σήμερα να την αντιμετωπίζει με σκεπτικισμό εξαιτίας κυρίως των φαινόμενων «ηλεκτρονικής απάτης». Ο βαθμός υιοθέτησης του Internet Banking διεθνώς ποικίλλει και αποτελεί συνάρτηση πολλών παραγόντων. Η υιοθέτησή του όμως κρύβει και κινδύνους για τους οποίους πρέπει να βρεθούν αποτελεσματικοί τρόποι διαχείρισης. Για να μπορέσει η τράπεζα να παραμείνει ανταγωνιστική στο νέο περιβάλλον, πρέπει να εντάξει την ηλεκτρονική τραπεζική στους στρατηγικούς της στόχους.

Οι τράπεζες συνεχώς εκσυγχρονίζουν τα συστήματά τους που αφορούν στην ασφάλεια των συναλλαγών αλλά και προσπαθούν να παρέχουν νέες καινοτομίες υπηρεσίες μέσω του Internet Banking με σκοπό να διευρύνουν την πελατειακή τους βάση. Η παρούσα εργασία με τίτλο «e- Banking» προσπαθεί να προσεγγίσει την έννοια του Internet Banking σε θεωρητικό πλαίσιο. Κυρίαρχος στόχος της θεωρητικής προσέγγισης είναι να διασαφηνιστεί η έννοια, οι δυνατότητες, τα πλεονεκτήματα και τα μειονεκτήματα του νέου τραπεζικού καναλιού διανομής.

Τέλος η καινοτομία και η εφαρμογή βέλτιστων πρακτικών προσφέρουν ανταγωνιστικά πλεονεκτήματα στις επιχειρήσεις που τα εφαρμόζουν δημιουργώντας με αυτό τον τρόπο ηγέτες στο χώρο της ηλεκτρονικής τραπεζικής

Περιεχόμενα

Κεφαλαίο 5 : Διαδικτυακό έγκλημα και κίνδυνοι του e-banking

Κεφαλαίο 6 : Στρατηγικές επιλογές των τραπεζών σε θέματα E-banking

Κεφάλαιο 7 : Έργα ηλεκτρονικής τραπεζικής

Κεφαλαίο 8 : Νομικά Θέματα Ηλεκτρονικής τραπεζικής

Εισαγωγή

Η μεγάλη ανάπτυξη του Διαδικτύου που πραγματοποιείται και παρατηρείται παγκοσμίως την τελευταία δεκαετία έχει επιπτώσεις, όπως είναι φυσικό, και στον τραπεζικό χώρο. Παραδοσιακά οι τραπεζικοί οργανισμοί ανταγωνίζονταν μεταξύ τους χρησιμοποιώντας ως κανάλια διανομής για τα προϊόντα και τις υπηρεσίες τους τα δίκτυα των υποκαταστημάτων τους. Οι τεχνολογικές όμως εξελίξεις άλλαξαν τα δεδομένα του παιχνιδιού. Στα πλαίσια της συνεχούς βελτίωσης των παρεχόμενων υπηρεσιών των τραπεζών και της πληρέστερης κάλυψης των αναγκών και απαιτήσεων των πελατών τους, οι τράπεζες προχώρησαν στην εισαγωγή νέων ηλεκτρονικών υπηρεσιών εκμεταλλευόμενοι τα οφέλη που απορρέουν από την χρήση του Internet.

Ο όρος ηλεκτρονική τραπεζική που εμπεριέχει όρους όπως web banking, Internet banking, online banking και mobile banking μέχρι πριν μερικά χρόνια ήταν άγνωστος. Όσο επεκτείνεται η χρήση του Internet είναι λογικό αυτό να προτιμάται για τις συναλλαγές από το σπίτι ή το γραφείο. Για αυτό το λόγο όσες τράπεζες παρέχουν τέτοιες δυνατότητες πλεονεκτούν έναντι των υπόλοιπων. Στις μέρες μας οι περισσότερες τράπεζες έχουν υιοθετήσει την ηλεκτρονική τραπεζική παράλληλα με την παραδοσιακή εκτέλεση τραπεζικών εργασιών στα υποκαταστήματα, ενώ μη τραπεζικοί οργανισμοί όπως αλυσίδες λιανικής πώλησης, ασφαλιστικές εταιρίες και εταιρίες πληροφορικής έχουν μπει στην αγορά του e-banking καθιστώντας τον ανταγωνισμό ακόμα πιο έντονο. Το χαμηλό κόστος σε συνδυασμό με την εύκολη πρόσβαση που προσφέρει το Διαδίκτυο σε κάθε χρήστη έχουν σαν αποτέλεσμα η ηλεκτρονική τραπεζική να κερδίζει διαρκώς έδαφος καθώς παρέχει σημαντική εξοικονόμηση χρόνου, χρήματος αλλά και ταλαιπωρίας για τη διεκπεραίωση των τραπεζικών συναλλαγών.

Η έννοια του Internet Banking ή Διαδικτυακής Τραπεζικής (όπως είναι η ελληνική απόδοση του όρου), δηλαδή της διεξαγωγής τραπεζικών συναλλαγών μέσω του Διαδικτύου, αποτελεί τον κεντρικό άξονα γύρω από τον οποίο περιστρέφεται η παρούσα εργασία.

Στο πρόσφατο παρελθόν η έννοια του Internet Banking αποτελούσε μια καινοτομία που μόνον ελάχιστοι καινοτόμοι πελάτες αλλά και τράπεζες επιχείρησαν να υιοθετήσουν. Η καινοτομία που άλλοτε αντιμετωπιζόταν καχύποπτα σήμερα κατακτά ολοένα και περισσότερους υποστηρικτές. Η πλειοψηφία των τραπεζών προσφέρει σήμερα σύγχρονες υπηρεσίες Internet Banking με πολλαπλά οφέλη τόσο για τους πελάτες όσο και για τις τράπεζες. Εντούτοις παρά την επιτυχημένη πορεία που διέγραψε τα τελευταία χρόνια και συνεχίζει να διαγράφη η Διαδικτυακή Τραπεζική , υπάρχουν ακόμα επικριτές της οι οποίοι εγείρουν κυρίως θέματα ασφάλειας των συναλλαγών και διαδικτυακών απατών πάνω στα οποία στηρίζουν την απόφασή τους να μην υιοθετήσουν τη νέα αυτή μορφή τραπεζικής εξυπηρέτησης.

Στην παρούσα εργασία επιχειρείται κατά κύριο λόγο να μελετηθεί και να αναλυθεί η Διαδικτυακή Τραπεζική (e-banking). Παράλληλα ενσωματώνονται και διάφορες πρακτικές γύρω από το Internet Banking που συναντώνται διεθνώς. Η μελέτη που πραγματοποιήθηκε κατά την συγγραφή της συγκεκριμένης εργασίας προσεγγίζεται η έννοια του Internet Banking θεωρητικά μέσα από την ελληνική και διεθνή βιβλιογραφία καθώς και μέσα από τις ίδιες τις τραπεζικές ιστοσελίδες. Η παρούσα εργασία χωρίστηκε σε 6 κεφάλαια το περιεχόμενο των οποίων παρουσιάζεται συνοπτικά παρακάτω.

Στο πρώτο κεφάλαιο της θεωρητικής προσέγγισης επιχειρείται να προσδιοριστεί η έννοια του Internet Banking μέσα από τη διεθνή βιβλιογραφία.

Επιπλέον γίνεται μια ιστορική αναδρομή με αναφορές σε πρόδρομες μορφές της σύγχρονης Διαδικτυακής Τραπεζικής και παρουσιάζονται τα κυρίαρχα επιχειρηματικά μοντέλα που συναντώνται στο χώρο, οι ομαδοποιημένες κατηγορίες των προσφερόμενων από τις τράπεζες υπηρεσιών καθώς και τα ουσιαστικότερα πλεονεκτήματα και μειονεκτήματα του Internet Banking τόσο από την πλευρά των πελατών όσο και από την πλευρά των τραπεζικών ιδρυμάτων. Επίσης αναφερόμαστε τι είναι οι ηλεκτρονικές πληρωμές, ηλεκτρονικό χρήμα και τι μπορούμε να κάνουμε με το e-banking. Έγινε προσπάθεια να παρουσιαστεί μια εικόνα γύρω από τη διάδοση του Internet Banking σε εθνικό αλλά και σε διεθνές επίπεδο.

Προχωρώντας στο δεύτερο κεφάλαιο αναφερόμαστε στο νομικό υπόβαθρο της ηλεκτρονικής τραπεζικής. Ποιοι μπορούν να εκδώσουν ηλεκτρονικό χρήμα, τι γίνεται στην περίπτωση που αμφισβητηθεί η ηλεκτρονική πληρωμή , οι πληροφορίες που πρέπει να παρέχονται στον καταναλωτή μετά την συναλλαγή αλλά και οι υποχρεώσεις του κατόχου του ηλεκτρονικού χρήματος.

Όσον αφορά το τρίτο κεφάλαιο, στο οποίο περιγράφεται διεξοδικά ένα πολύ σημαντικό ζήτημα η ασφάλεια των ηλεκτρονικών συναλλαγών και η βασική τεχνολογία στον τομέα της ασφάλειας που είναι η κρυπτογράφηση.

Στο κεφάλαιο 4 καταγράφονται οι κίνδυνοι και οι απειλές του e-banking. Οι μεγαλύτεροι κίνδυνοι δεν προέρχονται από ατέλειες των συστημάτων ασφαλείας και κρυπτογράφησης αλλά από τον ανθρώπινο παράγοντα. Επίσης αναφέρουμε επιγραμματικά πραγματικές περιπτώσεις ηλεκτρονικών επιθέσεων. Επιπροσθέτως αναλύουμε προληπτικές ενέργειες του χρήστη , του ηλεκτρονικού υπολογιστή , διαδικτύου και για το internet banking οι οποίες αποτρέπουν τις ηλεκτρονικές επιθέσεις.

Στο 5 κεφάλαιο αναλύονται οι στρατηγικές επιλογές των τραπεζών σε θέματα e-banking. Για να διαμόρφωση την στρατηγική της η τράπεζα πρέπει προηγουμένως να λάβει υπόψη της, τις ευκαιρίες και τις απειλές από το συνεχώς μεταβαλλόμενο περιβάλλον. Οι βασικές στρατηγικές που εφαρμόζουν οι τράπεζες είναι η ενσωμάτωση του e-banking στο υπάρχον σύστημα διανομής προϊόντων και υπηρεσιών, δημιουργία ξεχωριστών ανεξάρτητων ηλεκτρονικών τραπεζών, δημιουργία ηλεκτρονικών τραπεζών από εταιρείες εκτός του κλάδου των χρηματοοικονομικών υπηρεσιών και προσφορά προϊόντων και υπηρεσιών on line που εμπλουτίζονται από προϊόντα τρίτων.

Προκειμένου να κατανοήσουμε τα έργα ηλεκτρονικής τραπεζικής και την πορεία αυτών (στο κεφάλαιο 6) , παρατίθενται αρχικά αρχιτέκτονες e-banking, δηλαδή πως είναι στημένες η ηλεκτρονικές υπηρεσίες , αλλά και σύγχρονες τεχνολογίες που εφαρμόζονται στην υλοποίηση των προϊόν ηλεκτρονικής τραπεζικής.

Στο τέλος της συγκεκριμένης εργασίας και έχοντας ο αναγνώστης προσεγγίσει το Internet Banking , παρατίθενται μια σειρά προτάσεων που θα μπορούσαν να αποτελέσουν έναυσμα για ενδεχόμενη περαιτέρω μελλοντική έρευνα πάνω στο θέμα της διαδικτυακής Τραπεζικής. Το όλο εγχείρημα της παρούσας εργασίας κλείνει με τον επίλογο, ο οποίος ακολουθείται από το Παράρτημα και τις βιβλιογραφικές αναφορές.

Κεφάλαιο 1: Έννοια του e-banking

1.1 Ορισμός E-banking

Ο διεθνής όρος e-banking αποδίδεται στην ελληνική ως «Ηλεκτρονική Τραπεζική». 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 αυτοματοποιημένη παροχή νέων και παραδοσιακών προϊόντων και υπηρεσιών χρηματοοικονομικής φύσης, απευθείας στους πελάτες μέσω ηλεκτρονικών, αλληλεπιδραστικών καναλιών επικοινωνίας.

Ανάλογα με το κανάλι που χρησιμοποιείται για να διανεμηθούν οι υπηρεσίες, διακρίνουμε το e-banking σε Internet Banking όπου το Internet χρησιμοποιείται ως μέσο διεξαγωγής τραπεζικών δραστηριοτήτων, σε Mobile Banking όπου οι συναλλαγές πραγματοποιούνται μέσω κινητού τηλεφώνου ή PDA και σε Phone Banking όπου χρησιμοποιείται το τηλέφωνο. Οι πιο συνηθισμένες υπηρεσίες που παρέχονται online στα πλαίσια της ηλεκτρονικής τραπεζικής αφορούν πληροφορίες σχετικά με λογαριασμούς, κινήσεις λογαριασμών, υπόλοιπα και κινήσεις πιστωτικών καρτών, πληρωμές δόσεων δανείων, εξοφλήσεις κάθε είδους λογαριασμών και πάγιων εντολών πληρωμής προς ΔΕΚΟ. Επιπλέον, διατίθενται και πιο εξειδικευμένες υπηρεσίες όπως real-time χρηματιστηριακές συναλλαγές και παρακολούθηση του χαρτοφυλακίου των μετοχών του πελάτη καθώς επίσης και προσωπικές υπηρεσίες πελάτη όπως για παράδειγμα προσωπικά μηνύματα από την τράπεζα, εκτύπωση αποδείξεων συναλλαγών και προσωπικές προσφορές. Πιο συγκεκριμένα το e-banking αναφέρεται στην ικανότητα ενός συνδρομητή του διαδικτύου να έχει πλήρη πρόσβαση στο τραπεζικό σύστημα και ως αποτέλεσμα αυτού να διαλέγει και να χρησιμοποιεί προϊόντα και υπηρεσίες διαμέσου του Internet όπως θα έκανε αν βρισκόταν σε κάποιο «φυσικό» υποκατάστημα της τράπεζας.

1.1.1 PC banking

Είναι ο όρος που περιγράφει τις συναλλαγές που γίνονται μέσω του PC του πελάτη. Η μεταφορά των δεδομένων σε μια τέτοια συναλλαγή γίνεται μέσω των τηλεφωνικών γραμμών (αναλογικές ή ψηφιακές). Μπορούμε να διακρίνουμε δύο είδη PC banking:

- Το Online banking στο οποίο οι συναλλαγές γίνονται μέσω ¨κλειστών δικτύων¨. Για να γίνει μια συναλλαγή ο πελάτης πρέπει να προμηθευτεί ειδικό software από την τράπεζα. Ο τρόπος αυτός συναλλαγών εμφανίζεται στη Γερμανία στις αρχές της δεκαετίας του .80 με ένα σύστημα που λεγόταν BTX (German Federal Post Office).

- Το Internet banking είναι ο γνωστός τρόπος συναλλαγής του χρήστη με την τράπεζα από όποιο τερματικό και αν βρίσκεται ανά πάσα στιγμή, με τη χρήση ενδεχομένως συγκεκριμένων κωδικών.

1.1.2 Mobile banking

Πολλές φορητές συσκευές όπως τα κινητά τηλέφωνα, οι φορητές ατζέντες (PDA) και οι υπολογιστές παλάμης (Hand-held PCs) μπορούν να έχουν πρόσβαση στο internet μέσω της τεχνολογίας WAP. Έτσι οι χρήστες μπορούν να εκτελέσουν internet banking από άλλες συσκευές, εκτός του PC. Αυτού του είδους οι συναλλαγές περιγράφονται με τον όρο mobile banking.

1.2 Ιστορική Αναδρομή

Για να υπάρξει το e-banking απαραίτητο συστατικό στοιχείο είναι η δυνατότητα πρόσβασης στο λεγόμενο διαδίκτυο ή Internet όπως αποκαλείται διεθνώς, εργαλείο το οποίο τα τελευταία χρόνια έχει εισβάλει στη ζωή μας και τείνει να αποκτήσει δεσπόζουσα θέση στην καθημερινότητά μας.

Όλα ξεκίνησαν στα τέλη της δεκαετίας του ‘60, όταν ο οργανισμός ARPA (Advanced Research Projects Agency) στις ΗΠΑ, προσανατολισμένος σε ερευνητικά προγράμματα υψηλής τεχνολογίας, ξεκίνησε μια ερευνητική δραστηριότητα σχετικά με τα δίκτυα, δημιουργώντας το ARPAnet το οποίο αποτέλεσε πρόδρομο του Internet. Το 1971, μόνον τέσσερις υπερυπολογιστές ήταν συνδεδεμένοι στο δίκτυο. Το 1995, οι συνολικοί κόμβοι ήταν δεκάδες χιλιάδες, ενώ περισσότεροι από πέντε εκατομμύρια περίπου χρήστες ανά τον κόσμο συνδέονται καθημερινά στο δίκτυο για τις συναλλαγές τους, για να συνομιλήσουν, ν’ ανταλλάξουν απόψεις, γνώσεις και προγράμματα.

Σταθμός στην ιστορία του διαδικτύου αποτελεί το έτος 1993 οπότε και κατασκευάστηκε ο παγκόσμιος ιστός (World Wide Web) στο CERN της Ελβετίας. Ο παγκόσμιος ιστός συνέβαλε στη δημιουργία μιας ευρύτερης και πιο εύκολα προσβάσιμης δικτυακής υποδομής. Το 1994 ανακαλύφθηκε ο Netscape Navigator, ο πρώτος περιηγητής του διαδικτύου (browser), που καθιστούσε πλέον δυνατή την περιήγηση στο Internet οποιουδήποτε διέθετε έναν ηλεκτρονικό υπολογιστή και ένα modem.

Η ιστορία του e-banking ξεκινά στα τέλη της δεκαετίας του 80 όταν οι μεγαλύτερες τράπεζες των Ηνωμένων Πολιτειών εισήγαγαν την έννοια του Home Banking (ή PC Banking). Με το Home Banking οι τράπεζες έδιναν τη δυνατότητα στους πελάτες τους να πραγματοποιούν τις βασικές τραπεζικές τους συναλλαγές από το σπίτι μέσω ηλεκτρονικού υπολογιστή. Οι τράπεζες, έχοντας αναπτύξει τα κατάλληλα δίκτυα και παρέχοντας στους πελάτες τους δωρεάν λογισμικό, στόχευαν να εξαπλωθεί η καινούρια αυτή υπηρεσία στους πλέον απαιτητικούς και εύπορους πελάτες. Ο κύκλος ζωής του Home Banking ήταν σύντομος καθώς στα μέσα της δεκαετίας του 90 επικράτησε το e-banking. Το σημαντικότερο πλεονέκτημα που προσέφερε το e-banking σε σχέση με τον προκάτοχό του ήταν το γεγονός ότι οι τράπεζες δεν απαιτούνταν πλέον να συντηρούν ιδιωτικά δίκτυα τα οποία συνεπάγονταν υψηλό κόστος. Επιπλέον ούτε οι πελάτες χρειαζόταν να εφοδιάζονται με κάποιο ιδιαίτερο λογισμικό ώστε να έχουν πρόσβαση στο σύστημα της τράπεζας. Το Internet ως ανοιχτό σύστημα αποτέλεσε πρόκληση για τις τράπεζες οι οποίες διέκριναν την ευκαιρία να διευρύνουν μέσω αυτού την πελατειακή τους βάση.
Το 1995 η αμερικανική Wells Fargo ήταν η πρώτη τράπεζα η οποία έδωσε στους πελάτες της την δυνατότητα online πρόσβασης στους τραπεζικούς τους λογαριασμούς. Τον Οκτώβριο του 1995 ιδρύθηκε στο Κεντάκι των Ηνωμένων Πολιτειών η πρώτη αμιγώς διαδικτυακή τράπεζα η

“Security First Network Bank”. Στην Ελλάδα η πρώτη εφαρμογή e-banking παρουσιάστηκε τον Φεβρουάριο του 1998. Την καινοτομία αυτή εισήγαγε στην Ελλάδα, που αριθμούσε τότε λίγο περισσότερους από 100000 συνδρομητές Internet, η Εγνατία Τράπεζα παρουσιάζοντας την ολοκληρωμένη υπηρεσία WebTeller μέσω τις οποίας οι καταναλωτές είχαν τη δυνατότητα να διεκπεραιώνουν τις τραπεζικές τους συναλλαγές μέσω του Internet.

1.3 Τι είναι οι ηλεκτρονικές πληρωμές

Η ηλεκτρονική πληρωμή είναι η χρηματική εκκαθάριση των συναλλαγών με ηλεκτρονικά μέσα. Τα είδη της ηλεκτρονικής πληρωμής είναι η ηλεκτρονική καταβολή μέσω ηλεκτρονικής μεταφοράς κεφαλαίων (EFT), η χρήση πιστωτικών καρτών για συναλλαγές που γίνονται στο διαδίκτυο και το ηλεκτρονικό χρήμα.

1.4 Τι είναι το ηλεκτρονικό χρήμα (e-money)

Ηλεκτρονικό χρήμα ένα σύγχρονό μέσο πληρωμής στο διαδίκτυο. Βασίζεται στην ανταλλαγή πραγματικού χρήματος σε μια τράπεζα με ηλεκτρονικό τρόπο. Ένα συγκεκριμένο , δηλαδή, ποσό αληθινών χρημάτων ανταλλάσσεται με «κυβερνονομίσματα». Για την ύπαρξη δηλαδή ηλεκτρονικού χρήματος είναι απαραίτητα τρία στοιχεία:

1) η νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη να είναι αποθηκεμένη σε ηλεκτρονικό υπόθεμα,

2) να έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού τουλάχιστον ίσου με την εκδοθείς νομισματική αξία,

3) γίνεται δεκτή ως μέσο πληρωμής από άλλες επιχειρήσεις πέραν της εκδότριας.

1.5 Τι μπορώ να κάνω με το e-banking

Στις περισσότερες περιπτώσεις με το e-banking μπορείτε να έχετε πρόσβαση στις ίδιες υπηρεσίες που θα είχατε και στη τράπεζα , εκτός βεβαία από αυτές που απαιτούν τη φυσική σας παρουσία όπως ανάληψη ή κατάθεση μετρητών. Έτσι μπορείτε για παράδειγμα να πληρώσετε το λογαριασμό της πιστωτικής σας κάρτας , να κάνετε μια μεταφορά χρημάτων . να πληρώσετε λογαριασμούς κοινωφελών οργανισμών κ.α. . Και όλα αυτά χωρίς να περιμένετε στην ουρά , χωρίς να χρειάζεται να πάτε ο ίδιος στην τράπεζα , χωρίς τέλος πάντων να είστε υποχρεωμένοι να χάσετε σημαντικό μέρος από το πολύτιμο χρόνο σας. Και βεβαία οι online τράπεζες είναι ανοικτές 24 ώρες το 24ωρο είτε είστε στο σπίτι είτε στη δουλεία , σε διακοπές στο εξωτερικό , οπουδήποτε.

1.6 Διείσδυση του e - banking στην Ελλάδα

Στον χώρο της ηλεκτρονικής τραπεζικής δραστηριοποιούνται με επιτυχία εδώ και

αρκετά χρόνια οι περισσότερες ελληνικές και πολυεθνικές τράπεζες που λειτουργούν στην ελληνική επικράτεια. Παρ' όλα, αυτά παρατηρείται σχετικά χαμηλή διείσδυση του e-banking στην Ελλάδα σε σχέση με τις υπόλοιπες ευρωπαϊκές χώρες. Το γεγονός αυτό οφείλεται στα γενικότερα χαμηλά ποσοστά εξοικείωσης του ελληνικού κοινού με τις νέες τεχνολογίες, το οποίο έχει ως αποτέλεσμα ο κόσμος να αντιμετωπίζει την ηλεκτρονική τραπεζική με σχετική δυσπιστία ακόμη και σήμερα. Εντούτοις, σύμφωνα με τραπεζικούς κύκλους, την τελευταία πενταετία ο αριθμός των χρηστών τέτοιου είδους υπηρεσιών αυξάνεται με γρήγορους ρυθμούς. Πιο συγκεκριμένα, στα τέλη του 2006 οι χρήστες υπηρεσιών ηλεκτρονικής τραπεζικής ξεπέρασαν τους 500.000, γεγονός ιδιαίτερα αισιόδοξο για το μέλλον αν αναλογιστεί κανείς ότι το αντίστοιχο νούμερο το 2001 δεν ξεπερνούσε τους 150.000 χρήστες. Το Παρατηρητήριο για την Κοινωνία της Πληροφορίας εκτιμά από την πλευρά του ότι οι χρήστες των online τραπεζικών υπηρεσιών στην Ελλάδα ανέρχονται σήμερα στο 15% του συνόλου των χρηστών του Internet στη χώρα, ενώ ένα ποσοστό 7% χρησιμοποιεί το Διαδίκτυο και για χρηματιστηριακές συναλλαγές. Εκτιμάται επιπλέον ότι οι online υπηρεσίες των 17 ελληνικών τραπεζών δεν υστερούν σε τίποτα από τις αντίστοιχες των τραπεζών του εξωτερικού, εξασφαλίζοντας αμεσότητα, ικανοποιητική εξυπηρέτηση και ασφάλεια στους χρήστες. Τα ποσοστά που προαναφέρθηκαν αναμένεται στο άμεσο μέλλον να αυξηθούν καθώς ο ανταγωνισμός μεταξύ των παροχών ευρυζωνικού Internet έχει ενταθεί, πράγμα που οδηγεί στην πτώση των τιμών και στη συνεχώς αυξανόμενη διείσδυση του Internet στα ελληνικά νοικοκυριά.

1.7 Διείσδυση του e - banking στον κόσμο

Σύμφωνα με έρευνα που διεξήγαγε η εταιρία "Celent Communications" παρατηρούνται μεγάλες διαφορές όσον αφορά τη διείσδυση των online τραπεζικών συναλλαγών από χώρα σε χώρα σε παγκόσμια κλίμακα. Ηγετική θέση στον κόσμο στην υιοθέτηση του e-banking το 2002 κατείχε η Νορβηγία με ποσοστό διείσδυσης 43% επί των χρηστών του Internet στη χώρα. Αντίστοιχη εικόνα παρουσίαζαν και οι άλλες Σκανδιναβικές χώρες όπου το Internet banking βρίσκει εξίσου μεγάλη αποδοχή. Πιο συγκεκριμένα τα ποσοστά ήταν 40% για την Φινλανδία και 36% για τη Σουηδία. Τη μεγαλύτερη αποδοχή στην Ασία βρίσκει η ηλεκτρονική τραπεζική στη Νότια Κορέα όπου το ποσοστό επί των συνολικών χρηστών του Διαδικτύου έφτασε το 40%. Ο Καναδάς και οι ΗΠΑ ακολουθούσαν με ποσοστά 23% και 22% αντίστοιχα. Η έρευνα έδειξε ότι στην Ευρώπη (με εξαίρεση τη Σκανδιναβία) η διείσδυση του e-banking το 2002 ήταν σχετικά χαμηλή. Από τις εκτός Σκανδιναβίας χώρες προηγείται η Αγγλία με ποσοστό 20%, ενώ ακολουθεί η Γερμανία με ποσοστό 13%.

Μια άλλη έρευνα που διεξήχθη στα τέλη του 2004 για λογαριασμό της αμερικάνικης "Pew Internet & American Life" έδειξε ότι ένα ποσοστό της τάξης του 44% όσων είχαν σύνδεση Internet στις ΗΠΑ χρησιμοποιούσαν τις υπηρεσίες του online banking, δηλαδή περίπου 53.000.000 χρήστες. Αν αναλογιστούμε το ποσοστό της προηγούμενης έρευνας που για τις ΗΠΑ το 2002 έφτανε το 22%, μέσα σε διάστημα 2 ετών η διείσδυση διπλασιάστηκε. Από αυτή την έρευνα προκύπτουν και άλλα ενδιαφέροντα συμπεράσματα για το προφίλ των χρηστών του e-banking. Πιο συγκεκριμένα, η διείσδυση αγγίζει το 60% στις ηλικίες 28-39 ετών. Αναφορικά με το εισόδημα των χρηστών το 55% των Αμερικανών χρηστών Internet με ετήσιο εισόδημα μεγαλύτερο των $75.000 χρησιμοποιεί υπηρεσίες e-banking, ποσοστό που μειώνεται στο 32% για εισοδήματα μικρότερα των $30.000. Τέλος παρατηρείται μεγαλύτερη διείσδυση σε άτομα με ανώτατη μόρφωση, στους άνδρες και σε όσους έχουν ευζωνική σύνδεση Internet. Η εξάπλωση

του e-banking είναι ραγδαία σε όλο τον κόσμο. Ειδικοί εκτιμούν ότι στο μέλλον οι σύγχρονες τράπεζες θα δραστηριοποιούνται αποκλειστικά μέσω των νέων τεχνολογιών.

1.8 Πως θα κάνω λογαριασμό e-banking

Σκέφτεστε ότι έχετε έναν προσωπικό υπολογιστή και μια σύνδεση στο διαδίκτυο. Τι άλλο χρειάζεστε; Εκπληκτικά, όχι αλλά πολλά . Αλλά υπάρχουν διάφορα πράγματα που πρέπει να εξετάσετε για να αρχίστε την απευθείας σύνδεση με τραπεζική εμπειρία σας, που περιλαμβάνει όλους τους προσωπικούς πόρους χρηματοδότησής σας κάτω από μια στέγη.

Τι χρειάζεται για να συνδεθείς με την τράπεζα σου

Χρειάζεστε ένα υπολογιστή, φυσικά, που να εξοπλίζεται με λογισμικό web browser όπως το internet explorer ή το Netscape Navigator . Πρόκειται επίσης να χρειαστείτε έναν φορέα παροχής υπηρεσιών Διαδικτύου ISP χρησιμεύει ως η πύλη του υπολογιστή σας στο World Wide Web. Ένα άλλο σημαντικό συστατικό είναι πώς να συνδεθείτε με το ISP σας, όπως μέσω ενός τηλεφωνικού modem (συστήνουμε ως γρήγορη σύνδεση δεδομένων ότι πρέπει να πάρετε τουλάχιστο 56K) ή ενός καλωδίου Modem.

Τι πρέπει να ξέρετε τώρα

Με το internet banking που καλούμε on line banking ο υπολογιστής συνδέετε με την τράπεζά σας μέσω του λογισμικού web browser, όπως ο internet explorer. θελήστε να σιγουρευτείτε ότι χρησιμοποιείτε τις πιο πρόσφατες εκδόσεις των προϊόντων (internet explorer , nescape navigator) για να εξασφαλίσετε ότι παίρνετε πλήρη οφέλη από όλη την ασφάλεια που παρέχουν .

Διαλέγετε την τράπεζα σας

Οι αγορές σε απευθείας σύνδεση με τη τράπεζα μπορούν να φανούν απλές, αλλά μπορεί να υπάρχει λίγη αποθάρρυνση και σύγχυση. Για ένα πράγμα, δεν θα υπάρχει έλλειψη στης πληροφορίες για το θέμα e-banking όταν είστε στο διαδίκτυο. Εν τω μεταξύ, πίσω στον κόσμο χωρίς απευθείας σύνδεση με το internet ακούτε πιθανώς για τις απευθείας σύνδεσης με τραπεζικές εργασίες στην τηλεόραση και στις διαφημίσεις ραδιοφώνων. Ο ανταγωνισμός είναι άγριος για την επιχείρηση σας, και οι τράπεζες ξοδεύουν τα μεγάλα ποσά για να σας πάρουν στον κόσμο του internet και του online banking.
Η πρώτη τράπεζα Διαδικτύου στην Ινδιάνα, ξόδεψε $800.000 σε μόνο μια τετράμηνη περίοδο για να πάρουν τα χρήματά των πελατών τους και όχι μονό στους ηλεκτρονικούς λογαριασμούς τους (e-account) . Αυτή η τράπεζα διαφημίζετε ακόμη και στο εξωτερικό, είναι μέσα στην κάρδια της Αμερικής αλλά έχει πελάτες από τη Φλώριδα Καλιφόρνια και σε άλλες πολλές πολιτείες της Αμερικής που η τράπεζα δεν υπάρχει εκεί . Ο David Becker, Πρόεδρος της τράπεζα, αποκάλυψε ότι πέντε τοις εκατό των πελατών του ζουν έξω από τη χώρα ή είναι ταξιδιώτες.
Μπορεί να είχατε λάβει ένα γράμμα η ένα φυλλάδιο από την τράπεζα σας που να σας ενθαρρύνει να θεωρήσετε ότι ότι είναι η καλύτερη τράπεζα για Online συναλλαγές και εσείς να

σκεφτείτε γιατί οι τράπεζες μας θέλουν να πάμε με το on-line banking; Τι θα κερδίσουν ; και φυσικά εδώ η απάντηση είναι ότι παρέχουν στους καταναλωτές γρηγορότερη εξυπηρετήσει και περισσότερες υπηρεσίες. Όταν σας κρατούν από τις γραμμές των ταμείων έχουν λιγότερα ταμεία για να σας πληρώσουν.
Η επιλογή μιας τράπεζας σε απευθείας σύνδεση με το λογαριασμό σας θα βάλει να σκεφτείτε για το πώς εσείς αυτήν την περίοδο χρησιμοποιήστε το χρηματοδοτικό οργανισμό σας. Πόσο συχνά στους προηγούμενους μήνες σας έχει τύχει για κάποιο
λόγο να επισκεφτεί ένα από τα γραφεία της τράπεζάς σας προσωπικά; Εάν εσείς
να είστε κύριοι μιας μικρής επιχείρησης, θα πρέπει να εξετάσετε τα τραπεζικά προϊόντα
και υπηρεσίες που χρησιμοποιείτε συχνά, καθώς επίσης και πόσο συχνά πρέπει να επισκεφτείτε προσωπικά την τράπεζά σας για να καταθέσετε της επιταγές σας η κάτι που να έχει σχέση με εσάς ή την επιχείρηση σας.

Αρχίστε με την τράπεζα σας

Εάν συμπαθείτε τα προϊόντα και τις υπηρεσίες που παίρνετε από την
τρέχων τράπεζα σας καλώ θα ήταν να κοιτάζετε τι προσφέρει το on-line banking της τράπεζας. Αυτό θα μπορεί να σας σώσει χρόνο και μερικές δαπάνες όπως ξανά τυπώσει των επιταγών σας καθιερώνοντας τις νέες υπηρεσίες άμεσος.
Θα θελήσετε να υποβάλετε κάποιες ερωτήσεις προφανώς για το πώς λειτουργεί. Πρώτα θα ελέγξτε τον ισόχωρο της τράπεζάς σας Συγκρίνετε τον ιστοχώρο της τρέχουσας τράπεζάς σας με άλλες τράπεζες και συγκρίνετε για την καλύτερη , και καλύτερα θα ήταν για σας να επιλέξετε τράπεζα που θα μπορέσετε να παραστείτε φυσικά εάν προκύψει κάποιο πρόβλημα.

Συγκεντρωτικός Πίνακας Τραπεζών που προσφέρουν υπηρεσίες e-banking στην Ελλάδα

Στον πιο κάτω Πίνακα παρατίθενται οι σημαντικότερες τράπεζες που παρέχουν
υπηρεσίες Internet Banking στην Ελλάδα καθώς και οι δικτυακοί τόποι για να
εισέλθει κάποιος στα συστήματα των τραπεζών όπου θα του ζητηθεί να εισάγει τους
προσωπικούς του κωδικούς. Το HTTPS (Secure HTTP) χρησιμοποιείται για να
δηλώσει μία ασφαλή σύνδεση. Το πρόθεμα https που παρατηρούμε ότι
χρησιμοποιούν οι τράπεζες υποδηλώνει ότι θα χρησιμοποιηθεί κανονικά το
πρωτόκολλο HTTP, αλλά η σύνδεση θα γίνει σε διαφορετική θύρα και τα δεδομένα
θα ανταλλάσσονται κρυπτογραφημένα. Έκτος από τις τράπεζες χρησιμοποιείται
ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια και διακινούνται ευαίσθητες πληροφορίες.

	Επωνυμία Τράπεζας	URL
	Alpha Bank	https://www.alpha.gr

	Aspis Bank	https://ebanking.aspisbank.gr/eBanking
	Bayerisch Hypovereinsbank	https://www.hvbrsce.com/eBanking/Athens/Pages/ElectronicBanking.htm
	Citibank	https://cgrehb1.cd.citibank.gr/CappWebAppGreece/productone/capp/usersignon.do
	EFG – Eurobank	www.eurobank.gr/online/home
	First Business Bank	https://ebank.fbb.gr
	Geniki Bank	https://ebanking.geniki.gr/Geniki/pages/login/index.aspx
	Marfin – Egnatia	https://ebanking.marfinegnatiabank.gr
	Millennium	https://ebanking.millenniumbank.gr
	Αγροτική	https://webbanking.atebank.gr
	Αττικής	https://ebanking.atticabank.gr
	Εθνική	http://homebank.nbg.gr
	Ελληνική	https://www.securecy.hellenicnetbanking.com/personalgr_gr
	Εμπορική	https://ebank.emporiki.gr/EMPB_EBANKWeb/transactions/login
	Κύπρου	https://ebanking.bankofcyprus.gr
	Παγκρήτια Συνεταιριστική	https://www.e-coopbank.gr
	Πανελλήνια	https://www.e-coopbank.gr
	Πειραιώς	https://www.winbank.gr
	Συνεταιριστική Δωδεκανήσου	https://www.e-coopbank.gr

1.9 Επιχειρηματικά Μοντέλα[1] e-banking

Τα πιστωτικά ιδρύματα που δραστηριοποιούνται στο χώρο της παροχής τραπεζικών υπηρεσιών μέσω διαδικτύου ακολουθούν κατά βάση ένα από τα ακόλουθα 2 γενικά επιχειρηματικά μοντέλα :

1.9.1.Μοντέλο Brick & Click ή Click & Mortar

Το μοντέλο αυτό ακολουθείται από τράπεζες που διαθέτουν φυσική υπόσταση, δηλαδή έχουν ένα εδραιωμένο δίκτυο «φυσικών» καταστημάτων και επιπλέον έχουν[2] εισάγει το e-banking ως ένα εναλλακτικό δίκτυο διανομής των προϊόντων και υπηρεσιών τους, το οποίο δρα συμπληρωματικά στο ήδη υπάρχον δίκτυο διανομής που έχουν και δεν το υποκαθιστά. Οι τράπεζες θεωρούν ότι εφαρμόζοντας αυτό το μοντέλο αυξάνουν την αποτελεσματικότητά τους και την επιχειρηματική τους αξία καθώς παρέχουν τη δυνατότητα στους πελάτες τους να συνδυάσουν το δίκτυο καταστημάτων με το Internet ώστε να εξυπηρετούνται με τον καλύτερο δυνατό τρόπο. Σε μερικές περιπτώσεις οι τράπεζες που ακολουθούν το συγκεκριμένο μοντέλο δημιουργούν για τα κανάλια τους μέσω διαδικτύου μια ξεχωριστή επωνυμία. Η διάκριση αυτή γίνεται για λόγους marketing καθώς οι διαδικτυακές τράπεζες που δημιουργούνται δεν έχουν ξεχωριστή οντότητα αλλά ανήκουν στην τράπεζα που τις ίδρυσε.

1.9.2.Μοντέλο Virtual ή Internet only Bank[2]

Το μοντέλο αυτό αφορά πιστωτικά ιδρύματα που δεν έχουν «φυσικό» δίκτυο διανομής, δηλαδή καταστήματα αλλά έχουν παρουσία αποκλειστικά στο Internet, το οποίο και χρησιμοποιούν ως κύριο κανάλι διανομής των προϊόντων και υπηρεσιών τους. Οι τράπεζες που ακολουθούν αυτό το μοντέλο επιχειρηματικής δράσης έχουν πολύ λιγότερα λειτουργικά έξοδα από τις τράπεζες που διαθέτουν καταστήματα και επομένως μπορούν να μετακυλίσουν το ανταγωνιστικό αυτό πλεονέκτημα στους πελάτες τους προσφέροντας χαμηλότερες χρεώσεις και ελκυστικά επιτόκια.

1.10. Προσφερόμενες Υπηρεσίες

Τα είδη των παρεχόμενων τραπεζικών υπηρεσιών μέσω του Internet μπορούν να διαχωριστούν στις τρεις επόμενες ευρείες κατηγορίες :

[1] Σύμφωνα με ορισμό του καθηγητή Michael Rappa (2001) ένα επιχειρηματικό μοντέλο είναι μια μέθοδος να ασκεί κανείς επιχειρηματική δραστηριότητα, από την οποία μπορεί η επιχείρηση να στηριχθεί από μόνη της, δηλαδή να παράγει εισόδημα.

[2] Η στρατηγική των τραπεζών που ακολουθούν αυτό το επιχειρηματικό μοντέλο συναντάται στη διεθνή βιβλιογραφία ως “Pure Play Internet Business Strategy”.

1.10.1. Υπηρεσίες παροχής πληροφοριών μόνο

Στην περίπτωση αυτή χρησιμοποιούνται συστήματα που επιτρέπουν την πρόσβαση σε πληροφορίες που διατίθενται δημοσίως ή σχετίζονται με το μάρκετινγκ μίας τράπεζας. Κατά συνέπεια, η τράπεζα διαθέτει ηλεκτρονικά τις πληροφορίες που οι πελάτες εύρισκαν παραδοσιακά σε έντυπα ή σε άλλα μέσα ενημέρωσης. Ωστόσο, ακόμη και σε αυτή την περίπτωση, με τη χρήση της σημερινής τεχνολογίας οι συλλεγόμενες πληροφορίες για τους επισκέπτες πελάτες μπορούν να δημιουργήσουν στόχους για συγκεκριμένα προϊόντα, υπηρεσίες ή πληροφορίες που έχουν ήδη ζητηθεί. Οι μάνατζερ μπορούν επίσης να χρησιμοποιήσουν αυτές τις πληροφορίες για τη δημιουργία και προώθηση νέων προϊόντων.

1.10.2. Υπηρεσίες ανταλλαγής πληροφοριών

Εδώ τα χρησιμοποιούμενα ηλεκτρονικά συστήματα είναι αλληλοδραστικά (Interactive), δίνοντας τη δυνατότητα μεταφοράς ευαίσθητων μηνυμάτων, εγγράφων ή αρχείων μεταξύ των χρηματοπιστωτικών οργανισμών και των πελατών τους. Ουσιαστικά , στην περίπτωση αυτή χρησιμοποιείται το ηλεκτρονικό ταχυδρομείο που επιτρέπει τη μεταφορά εμπιστευτικών πληροφοριών, καθώς και συστήματα που επιτρέπουν την αμφίπλευρη μεταφορά στοιχείων μεταξύ βάσεων δεδομένων και δικτύων των τραπεζών και των πελατών. Μία θέση (Web Site) στο Internet που επιτρέπει την on-line κατάθεση αίτησης για ένα δάνειο ή για ένα λογαριασμό καταθέσεων αποτελεί παράδειγμα υπηρεσίας αυτής της κατηγορίας. Βασικό ζητούμενο αυτών των υπηρεσιών είναι η ασφάλεια των δεδομένων, που περικλείει την εμπιστευτικότητα των προσωπικών πληροφοριών, την ακεραιότητα των πληροφοριών, την πιστοποίηση της αυθεντικότητας των χρηστών κ.λπ.

1.10.3. Υπηρεσίες ολοκληρωμένων συναλλαγών

Εδώ τα χρησιμοποιούμενα συστήματα παρέχουν όλες τις προηγούμενες δυνατότητες, αλλά και τη δυνατότητα on-line συναλλαγών, διαχείρισης λογαριασμών, μεταφοράς χρημάτων μεταξύ λογαριασμών, την πληρωμή υποχρεώσεων κ.λπ. Εδώ συμπεριλαμβάνονται ουσιαστικά τα ηλεκτρονικά συστήματα πληρωμών (Electronic Payment Systems). Τα συστήματα αυτά προσομοιάζουν τα αντίστοιχα παραδοσιακά συστήματα αφού προέρχονται από το ίδιο μοντέλο νομισματικής χρήσης. Υπό αυτή την έννοια, ακολουθούν τα ίδια γενικά βήματα μέσα στον κύκλο πληρωμών (εισαγωγή εντολής, διευθέτηση, αποστολή πληρωμής).

Σε όλες τις περιπτώσεις η εμπιστοσύνη προς τους συμμετέχοντες (π.χ.τράπεζες και οργανισμούς που εκδίδουν τις εντολές, διαχειρίζονται και διευθετούν τις πληρωμές) αλλά και τη διαδικασία αποτελούν κρίσιμους παράγοντες για την αποδοχή και την επιβίωση αυτού του συστήματος πληρωμών. Άλλα κριτήρια είναι η ασφάλεια, η νομιμότητα των συναλλαγών, η αποτελεσματικότητα, το κόστος και η αξιοπιστία, καθώς και η αποδοχή εκ μέρους του εμπορικού κόσμου. Η εκμετάλλευση των παραπάνω δυνατοτήτων στηρίζεται και στην ύπαρξη της αναγκαίας ηλεκτρονικής υποδομής και εντός των τραπεζών, για την παροχή τόσο των κλασσικών υπηρεσιών, όσο και των υπηρεσιών που αναδύονται μέσα από τις νέες συνθήκες λειτουργίας της οικονομίας. Συνοπτικά θα αναφερθούν τα απαιτούμενα στοιχεία υποδομής και

για την παροχή on-line χρηματιστηριακών υπηρεσιών, που αποτελούν βασικό πρόσθετο πεδίο δραστηριοποίησης των τραπεζών.
Αυτά είναι τα εξής :

1) Στοιχεία και πληροφορίες για τους πελάτες (client management).
2) Κεντρική διαχείριση χαρτοφυλακίου (portfolio management).
3) Πωλήσεις χρηματιστηριακών πληροφοριών (interface - vendor of financial data).
4) Διεκπεραίωση συναλλαγών (trading and order management).

1.11 Πλεονεκτήματα-Μειονεκτήματα

Η χρήση του διαδικτύου και των νέων τεχνολογιών από τα χρηματοπιστωτικά ιδρύματα έχει αλλάξει τον τρόπο διεξαγωγής των συναλλαγών, οι οποίες πλέον δεν απαιτούν τη φυσική παρουσία των συναλλασσομένων. Τα πλεονεκτήματα όσο και τα μειονεκτήματα που συνεπάγεται η νέα αυτή κατάσταση αγγίζουν τόσο τις τράπεζες όσο και τους πελάτες αυτών. Πιο συγκεκριμένα:

1.11.1 Πλεονεκτήματα για τους πελάτες

1. Διαθεσιμότητα
Οι δικτυακοί τόποι των τραπεζών που προσφέρουν υπηρεσίες e-banking δεν κλείνουν ποτέ (μόνο για λόγους συντήρησης). Επομένως ο πελάτης δεν περιορίζεται από το ωράριο λειτουργίας των «φυσικών» τραπεζικών καταστημάτων και μπορεί επί 24ώρου βάσεως 365 μέρες το χρόνο να πραγματοποιήσει μέσω του Internet τις συναλλαγές που επιθυμεί. Το γεγονός αυτό είναι ιδιαίτερης σημασίας για τους πολυάσχολους πελάτες οι οποίοι δεν είναι διατεθειμένοι να περιμένουν στην ουρά σε κάποια τράπεζα για να εξυπηρετηθούν.

2. Φορητότητα
Δεν υπάρχει γεωγραφικός περιορισμός στις υπηρεσίες που προσφέρονται μέσω του e-banking. Αυτό σημαίνει ότι ο πελάτης μπορεί από οποιοδήποτε σημείο της γης και αν βρίσκεται να συνδεθεί με την τράπεζά του και να πραγματοποιήσει συναλλαγές με μοναδική προϋπόθεση να έχει πρόσβαση στον Παγκόσμιο Ιστό. Επομένως το νέο εναλλακτικό κανάλι διανομής καταργεί τα σύνορα και εκμηδενίζει τις αποστάσεις. Πλέον το τραπεζικό κατάστημα απέχει όσο και το πάτημα ενός κουμπιού στον υπολογιστή. Επιπλέον δεν απαιτείται από τον πελάτη η προμήθεια εξειδικευμένου λογισμικού, όπως συνέβαινε παλαιότερα με τον πρόδρομο του Internet Banking το Home Banking.

3. Ευκολία-Ταχύτητα συναλλαγών
Όλες οι υπηρεσίες που προσφέρονται μέσω της διαδικτυακής Τραπεζικής είναι συγκεντρωμένες σ΄ έναν και μόνο δικτυακό τόπο της τράπεζας με αποτέλεσμα ο πελάτης να μπορεί εύκολα και γρήγορα να επιλέξει τη συναλλαγή που επιθυμεί να πραγματοποιήσει. Με ένα click και μέσα σε λίγα δευτερόλεπτα ολοκληρώνονται συναλλαγές όπως πληρωμή ενός λογαριασμού ή εξόφληση μιας πιστωτικής κάρτας, οι οποίες με την «παραδοσιακή» τραπεζική ή ακόμα και μέσω των ATMs απαιτούσαν πολύ περισσότερο κόπο και χρόνο.

4. Αποτελεσματικότητα
Οι περισσότερες τράπεζες που δραστηριοποιούνται στο Online Banking προσφέρουν στις ιστοσελίδες τους εύχρηστα εργαλεία όπως υπηρεσίες τύπου Alert[3], υπολογισμός δόσεων δανείων, προγράμματα διαχείρισης χαρτοφυλακίου κ.α. Η χρήση των εργαλείων αυτών καθιστά αποτελεσματικότερο το χειρισμό των περιουσιακών στοιχείων εκ μέρους των πελατών.

1.11.2 Μειονεκτήματα για τους πελάτες

1. Χρονοβόρα εγγραφή πελατών
Η εγγραφή ενός νέου πελάτη στις υπηρεσίες του e-banking μπορεί να γίνει με τη συμπλήρωση μιας αίτησης η οποία μπορεί να υποβληθεί από τον ίδιο τον πελάτη σε κάποιο κατάστημα της τράπεζας ή μπορεί να αποσταλεί ηλεκτρονικά. Σε μερικές περιπτώσεις ο νέος πελάτης μπορεί να χρειαστεί να περιμένει αρκετά (1 ημέρα έως 2 εβδομάδες) μέχρις ότου να του δοθούν οι κωδικοί πρόσβασης και να μπορεί να ενεργοποιήσει τις υπηρεσίες του e-banking.

2. Δυσκολία στο χειρισμό
Οι τραπεζικοί δικτυακοί τόποι που παρέχουν υπηρεσίες e-banking μπορεί να φανούν δύσχρηστοι σε πελάτες με μικρή εξοικείωση με το Internet. Το άνοιγμα ενός online λογαριασμού ή η online αίτηση για λήψη δανείου μπορεί για κάποιους που είναι εξοικειωμένοι να είναι κάτι το απλό. Κάποιους άλλους μπορεί να τους τρομάζει και να τους καθιστά διστακτικούς λόγω των ελλιπών γνώσεων τους στις νέες τεχνολογίες.

3. Δυσπιστία χρηστών
Αρκετοί χρήστες του διαδικτύου αντιμετωπίζουν ακόμα και σήμερα την ηλεκτρονική τραπεζική με δυσπιστία. Τα φαινόμενα ηλεκτρονικής απάτης, σε συνδυασμό με την ελλιπή ενημέρωση των πελατών για τα συστήματα ασφαλείας των τραπεζών, τους αποθαρρύνουν από το να χρησιμοποιούν τις υπηρεσίες μέσω διαδικτύου. Πιο συγκεκριμένα οι «ηλεκτρονικοί» απατεώνες αδυνατώντας να αντιμετωπίσουν τα υψηλά επίπεδα ασφαλείας των τραπεζών, 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-mail, δημιουργία πλαστών ιστοσελίδων (Spoofing), 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 είτε να τις υφαρπάξουν με τεχνικές παρακολούθησης κατά την εισαγωγή τους. Οι τράπεζες από την πλευρά τους συμβουλεύουν τους χρήστες του e-banking να βρίσκονται σε εγρήγορση και να τηρούν μια σειρά συμβουλών ώστε να μην πέσουν θύματα απάτης.

[3] Ο όρος αυτός αναφέρεται σε συνεχείς ενημερώσεις των πελατών μέσω email ή γραπτών μηνυμάτων όσον αφορά μεταβολές των λογαριασμών, χρηματιστηριακές συναλλαγές κ.α.

1.11.3 Πλεονεκτήματα για τις τράπεζες

1. Μείωση λειτουργικού κόστους
Η απόφαση μιας τράπεζας να ξεκινήσει να παρέχει υπηρεσίες ηλεκτρονικής τραπεζικής θα έχει ως αποτέλεσμα το κόστος λειτουργίας της να μειωθεί σημαντικά καθώς οι συναλλαγές που πραγματοποιούν οι πελάτες σ' ένα τραπεζικό υποκατάστημα στοιχίζουν στην τράπεζα πολύ περισσότερο από τις αυτοματοποιημένες online συναλλαγές της ηλεκτρονικής τραπεζικής. Σύμφωνα με στοιχεία της McKinsey & Consultants για την αμερικανική αγορά, το κόστος μιας τυπικής τραπεζικής συναλλαγής μέσω υποκαταστήματος είναι κατά μέσο όρο $2,5, μέσω τηλεφώνου πέφτει στο $1, μέσω ATM στα $0,24, ενώ μέσω Internet είναι μόλις $0,1. Εξαιρετικής σημασίας προς αυτή την κατεύθυνση είναι και το γεγονός ότι όσο αυξάνονται οι πελάτες που χρησιμοποιούν το e-banking σε μια τράπεζα τόσο μειώνεται το μέσο κόστος ανά συναλλαγή καθώς η ίδια υποδομή χρησιμοποιείται από ολοένα και περισσότερα άτομα. Αυτό δε θα συμβεί αν αυξηθούν οι πελάτες στο «φυσικό» κατάστημα μιας τράπεζας καθώς μια τέτοια αύξηση θα οδηγούσε ενδεχομένως στην πρόσληψη επιπλέον προσωπικού, πράγμα που θα αύξανε το μέσο κόστος συναλλαγής.

2. Διεύρυνση πελατειακής βάσης
Η υιοθέτηση της ηλεκτρονικής τραπεζικής από μια τράπεζα δίνει στην τράπεζα τη δυνατότητα να αποκτήσει περισσότερα κανάλια διανομής για τα προϊόντα και τις υπηρεσίες της. Επιπλέον, η παροχή online υπηρεσιών δεν περιορίζει γεωγραφικά την τράπεζα. Με τον τρόπο αυτό υπάρχει η δυνατότητα να προσελκύσει απομακρυσμένους πελάτες και να διευρύνει την πελατειακή της βάση. Υποψήφιοι πελάτες πλέον των τραπεζών δεν είναι όσοι μένουν κοντά σε κάποιο νέο υποκατάστημα αλλά ολόκληρος ο κόσμος. Αυτό έχει σαν αποτέλεσμα να δημιουργούνται οικονομίες κλίμακας καθώς όσο αυξάνονται οι χρήστες του e-banking, τόσο μειώνεται το κόστος ανά συναλλαγή καθώς η υποδομή όπως προαναφέρθηκε είναι η ίδια για όλους τους χρήστες.

3. Ενίσχυση αφοσίωσης 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. Επιπλέον έρευνες αναφορικά με τα δημογραφικά χαρακτηριστικά των πελατών του e-banking καταδεικνύουν ότι αποτελούν άτομα ανώτατης μόρφωσης με αυξημένο ετήσιο εισόδημα. Το γεγονός αυτό αποτελεί ισχυρή ένδειξη ότι οι πελάτες αυτοί είναι πιο κερδοφόροι για τις τράπεζες σε σύγκριση με τον μέσο πελάτη των τραπεζικών καταστημάτων. Χαρακτηριστικά είναι τα αποτελέσματα που προέκυψαν από έρευνα που διεξήχθη για λογαριασμό της εταιρίας Forrester το 2004. Σε ερώτημα που τέθηκε σε νοικοκυριά του Καναδά για το αν σκοπεύουν αλλάξουν τράπεζα στα επόμενα χρόνια, θετικά ή μάλλον θετικά απάντησε μόλις το 4% των πελατών που έκαναν χρήση e-banking ενώ το αντίστοιχο ποσοστό για τους πελάτες που δεν έκαναν χρήση του έφτασε το 8%.

4. Κερδοφόρες νέες υπηρεσίες – Financial portals
Πολλές τράπεζες στρέφονται σήμερα στη δημιουργία ενός financial portal, δηλαδή μιας χρηματοοικονομικής δικτυακής πύλης όπου ο πελάτης εκτός των συνηθισμένων τραπεζικών προϊόντων και υπηρεσιών έχει πρόσβαση σε υπηρεσίες όπως ασφάλειες, leasing, αγοραπωλησία μετοχών κ.λ.π. Η ενσωμάτωση τέτοιων υπηρεσιών στις ήδη υπάρχουσες τραπεζικές συμβάλλει στην αύξηση της κερδοφορίας των τραπεζών.

1.11.4 Μειονεκτήματα για τις τράπεζες

1. Υψηλό αρχικό κόστος εγκατάστασης
Όπως συμβαίνει με όλες τις νέες τεχνολογίες, το αρχικό κόστος εγκατάστασης είναι υψηλό. Η επένδυση που πρέπει να κάνει η τράπεζα για να αγοράσει τον απαιτούμενο εξοπλισμό (υλικό και λογισμικό) 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. Επιπλέον πρέπει να σημειωθεί ότι η απόσβεση της επένδυσης αναμένεται να απέλθει μέσο-μακροπρόθεσμα, όταν δηλαδή δημιουργηθεί η απαραίτητη πελατειακή βάση ώστε να προκύψουν οι προσδοκόμενες οικονομίες κλίμακας. Η ύπαρξη αυτών των οικονομιών θα έχει ως αποτέλεσμα την επιθυμητή για την τράπεζα κερδοφορία.

2. Ασφάλεια συναλλαγών – Προστασία προσωπικών δεδομένων
Οι ηλεκτρονικές επιθέσεις και η μη εξουσιοδοτημένη πρόσβαση στα τραπεζικά ηλεκτρονικά συστήματα είναι συχνή. Η ασφάλεια λοιπόν των συναλλαγών και η προστασία των συναλλασσόμενων είναι θέματα ύψιστης σημασίας για τις τράπεζες. Καθώς κανένα υπολογιστικό σύστημα δεν είναι 100% ασφαλές, οι τράπεζες πρέπει με κάποιο τρόπο να διασφαλίσουν τα περιουσιακά στοιχεία των πελατών τους από επιθέσεις hacker και ηλεκτρονικές απάτες. Από έρευνες που πραγματοποιήθηκαν στις ΗΠΑ, έχει υπολογιστεί ότι κάθε χρόνο χάνονται περίπου 11δις. δολάρια λόγω της ελλιπούς ασφάλειας. Για να καταστήσουν οι τράπεζες την ηλεκτρονική τραπεζική ασφαλή για τους πελάτες τους σε μια εποχή που το Phising και το “Identity Theft” καλπάζει, έχουν κάνει μεγάλες επενδύσεις για την υλοποίηση στρατηγικών για την ταυτοποίηση του πελάτη και της συναλλαγής του. Οι επικρατέστερες στρατηγικές σήμερα είναι: α) η απλή ταυτοποίηση του πελάτη κατά την είσοδό του σε μία ηλεκτρονική υπηρεσία με τη χρήση κωδικών διαπίστευσης (Username και Password), β) η «υπογραφή» των συναλλαγών του πελάτη από κωδικούς μίας χρήσης TANs (Transaction Authorization Numbers), τους οποίους εκδίδει η τράπεζα και αποστέλλει περιοδικά στον πελάτη πάνω από μη ασφαλή κανάλια (fax, email, ταχυδρομείο), γ) η χρήση ψηφιακών πιστοποιητικών με τη μεθοδολογία PKI (Public Key Infrastructure), μία υψηλής τεχνολογίας και ασφαλείας λύση, που δυστυχώς εμπλέκει σημαντικό κόστος αρχικής επένδυσης και διαχείρισης και, τέλος, δ) η ταυτοποίηση δύο παραγόντων (Dual Factor Authentication) μέσω Security Tokens. Η τελευταία στρατηγική αφορά τη διανομή μικρών συσκευών στους χρήστες (Tokens) οι οποίες έχουν τη δυνατότητα, με ισχυρούς αλγόριθμους κρυπτογράφησης (π.χ. 3DES), να παράγουν από microchip που έχουν ενσωματωμένο δυναμικά: 1) OTPs (One Time Passwords) δηλαδή κωδικούς πρόσβασης μίας χρήσης και 2) E-Signatures δηλαδή ψηφιακές υπογραφές οικονομικών συναλλαγών μίας χρήσης. Επιπρόσθετα οι τράπεζες επενδύουν σε εξοπλισμό που περιλαμβάνει firewalls (φίλτρα πρόσβασης)[4] και συστήματα ενεργούς παρακολούθησης, καθώς και σε ανθρώπινο δυναμικό προσλαμβάνοντας ειδικούς συμβούλους σε θέματα ασφαλείας δικτύων.

[4] Είναι εξοπλισμός hardware & software που παρεμβάλλονται μεταξύ του Internet και των συστημάτων της τράπεζας και φιλτράρουν τα δεδομένα που κυκλοφορούν σύμφωνα με τις πολιτικές ασφαλείας που καθορίζει η τράπεζα και τα διεθνή πρότυπα. Με αυτό το φιλτράρισμα προστατεύονται όλα τα σημεία του δικτύου της τράπεζας στα οποία ο εξωτερικός και εσωτερικός μη εξουσιοδοτημένος χρήστης δεν πρέπει να έχει πρόσβαση.

1.12 Μελλοντικές τάσεις-Συμπεράσματα

Σύμφωνα με μελέτη της Datamonitor με τίτλο “European E-banking Technology Strategies”, οι ευρωπαϊκές τράπεζες αναμένεται να δαπανήσουν 3δις. δολάρια σε τεχνολογίες που σχετίζονται άμεσα ή έμμεσα με το Internet ως το 2009. Στην ίδια μελέτη επισημαίνεται ότι οι τράπεζες του Ηνωμένου Βασιλείου αποτελούν τη μεγαλύτερη ebanking αγορά της Ευρώπης, η ανάπτυξή τους όμως τα επόμενα χρόνια θα είναι πολύ μικρότερη σε σχέση με τις τράπεζες των περισσότερων ευρωπαϊκών κρατών, μιας και οι βρετανικές τράπεζες έχουν ήδη αναβαθμίσει τον τεχνολογικό τους εξοπλισμό. Στην περαιτέρω ανάπτυξη του e-banking αναμένεται να συμβάλλει αποφασιστικά και η συνεχώς αυξανόμενη ευρυζωνικότητα του Internet. Επιπλέον, λόγω αυξανόμενου ανταγωνισμού από την είσοδο μη τραπεζικών φορέων στην ηλεκτρονική τραπεζική αγορά, αναμένεται να ενισχυθεί η καμπάνια μάρκετινγκ και διαφήμισης εκ μέρους των παροχών τέτοιου είδους υπηρεσιών. Τέλος όπως επισημαίνουν παράγοντες της τραπεζικής αγοράς, στο μέλλον οι υπηρεσίες του e-banking θα είναι περισσότερο προσωποποιημένες για να προσαρμόζονται στις ιδιαίτερες ανάγκες των πελατών.

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

2.1.1 Οικονομικές συναλλαγές

Οι οικονομικές συναλλαγές καλύπτουν όλες τις συναλλαγών 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».

2.1.1.1 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 υπέχει θέση παραστατικού της συναλλαγής.

• Μεταφορές σε λογαριασμό τρίτου, όπου και σε αυτή την περίπτωση ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και στη συνέχεια καλείται να πληκτρολογήσει 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. Ακολούθως πληκτρολογεί το ποσό που θέλει να μεταφέρει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή.

2.1.1.2 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.

2.1.1.3 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.

2.1.1.4 Πληρωμές πιστωτικών καρτών

Οι πληρωμές πιστωτικών καρτών διακρίνονται σε τρεις κατηγορίες:

1) 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 πολυτέλεια και μεταχρονολογημένων πληρωμών, γεγονός που τον διευκολύνει να προγραμματίζει τις πληρωμές του.

2) Πληρωμή πιστωτικών καρτών τρίτου: Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης, στη συνέχεια καλείται να πληκτρολογήσει 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.

3) Πληρωμή πιστωτικών καρτών άλλης τράπεζας: Οι πληρωμές πιστωτικών καρτών άλλης τράπεζας διεκπεραιώνεται 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.

2.1.1.5 Πληρωμές Δημοσίου

Πολλές πληρωμές ενός πελάτη έναντι του Δημοσίου, μπορούν να ολοκληρώνονται μέσω e-banking. Οι περισσότερες εξ αυτών 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

2.1.1.6 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

2.1.1.7 Πληρωμές σταθερής και κινητής τηλεφωνίας

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

2.1.1.8 Πληρωμές Ασφαλιστικών

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

2.1.1.9 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.

2.1.1.10 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.

2.1.1.11 Κατάσταση Εντολών

Το Internet banking, πρέπει να δίνει στον πελάτη του, εύκολη ενημέρωση για το status 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 ebanking καλό είναι να ενημερώνεται και να παρακολουθεί συχνά το status των συναλλαγών του, ώστε να γνωρίζει ανά πάσα στιγμή ποιες εντολές του δεν εκτελεστήκαν.

Οι καταστάσεις εντολών είναι οι ακόλουθες :
• Προς επεξεργασία
• Ακυρωμένη από χρήστη
• Ακυρωμένη από Τράπεζα
• Ακυρωμένη από Οργανισμό
• Επιβεβαιωμένη από Τράπεζα
• Εκτελεσμένη
• Μερικώς εκτελεσμένη

2.1.1.12 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.

2.1.2 Πληροφοριακές συναλλαγές

Πολύ σημαντικό είναι το κομμάτι των πληροφοριακών συναλλαγών που καλύπτει το Internet banking. Ο χρήστης μπορεί να πάρει πληροφορίες για όλα τα προϊόντα 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 on line. 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 statement, 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.

2.1.3 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

2.1.4 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 τηςτράπεζας. Τέτοιες βοηθητικές υπηρεσίες είναι :

- Υπολογισμός IBAN
- Μετατροπή νομισμάτων
- Υπολογισμός δόσεων δανείων

2.2 Phone Banking

Τα τελευταία χρόνια ήταν έκδηλη 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 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 το τηλεφώνου.

• Τους εξειδικευμένους αντιπροσώπους του call center. 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.

Πολλές είναι οι τράπεζες που είτε με δικούς τους πόρους είτε μέσω Outsourcing, 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

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 web browser, όπως:

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

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

• Απευθείας στην ηλεκτρονική διεύθυνση της
• Μέσω του i-mode

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

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

Κεφάλαιο 3:Πρόσθετες υπηρεσίες – Υπηρεσίες προστιθέμενης αξίας

Πέραν των υπηρεσιών που αναφέρθηκαν στο προηγούμενο κεφάλαιο, το ebanking 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 περιλαμβάνει κυρίως χρηματιστηριακές συναλλαγές, καθώς και συναλλαγές αμοιβαίων κεφαλαίων και αμοιβαίων λογαριασμών Βασική προϋπόθεση για την εκτέλεση χρηματιστηριακών συναλλαγών μέσω ebanking 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.

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. 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:

3.2.1 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 τις 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

3.2.2 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. Η πληρωμή διεκπεραιώνεται αυτόματα και το ποσό κατατίθεται στο λογαριασμό του εμπόρου της τράπεζας

3.2.3 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.

3.2.4 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.

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.

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 πλέων 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 (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. πλεονεκτήματα σε σχέση με την εισαγωγή του EBPP σε περιβάλλον on line τραπεζικών υπηρεσιών :

• Προσελκύει πελάτες με υψηλό 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 στο loyalty του πελάτη : 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, 2001).

Κεφάλαιο 4: ΑΣΦΑΛΕΙΑ

4.1 Η ασφάλεια των συναλλαγών

Οι σύγχρονες επιχειρηματικές ανάγκες απαιτούν συχνά τη μετάδοση εμπιστευτικών δεδομένων μέσω του Διαδικτύου. Η νέα ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου του επαγγελματικού απορρήτου , κάθε οργανισμός τράπεζα πρέπει να παρέχει ασφάλεια Οι περισσότερες τράπεζες ακολουθούν το πρωτόκολλο SET (Secure Electronic Transaction), που υποστηρίζεται από τους δύο σημαντικότερους χρηματοπιστωτικούς οργανισμούς, τη MasterCard και τη Visa, καθώς και από εταιρίες όπως η IBM, η Microsoft και η Netscape. Το πρωτόκολλο SET βασίζεται στην κρυπτογραφία.

4.2 Κρυπτογράφηση

Οι σύγχρονες επιχειρηματικές ανάγκες απαιτούν συχνά τη μετάδοση εμπιστευτικών δεδομένων μέσω του Διαδικτύου. Η νέα ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου του επαγγελματικού απορρήτου. Βασική τεχνολογία στον τομέα της ασφάλειας στο Internet είναι η κρυπτογράφηση. Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων του κάθε χρήστη του Internet. Η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα(ciphertext).Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος. Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς τη χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.
Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

Το παρελθόν: Ο αλγόριθμος του Καίσαρα. Η κρυπτογράφηση δεν είναι νέα υπόθεση. Ακόμη και στην αρχαιότητα χρησιμοποιούνταν διάφορες μέθοδοι κρυπτογράφησης, με χαρακτηριστικότερη αυτή του Ιουλίου Καίσαρα, ο οποίος επινόησε έναν απλό αλγόριθμο για να

επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί, π.χ. το 3. Η κρυπτογράφηση δηλαδή του μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται τρεις θέσεις δεξιότερά του στο αλφάβητο. Διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί, παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.

Το μέλλον: Κβαντική κρυπτογράφηση. Οι σημερινές τεχνολογίες κρυπτογράφησης, παρότι παρέχουν μεγάλο ποσοστό ασφάλειας, έχει αποδειχθεί ότι δεν είναι άτρωτες. Η απάντηση στο πρόβλημα είναι η χρήση της κβαντικής Φυσικής, όπως υποστηρίζει ο Νικολά Ζισίν, πρωτοπόρος της συγκεκριμένης τεχνολογίας στο Πανεπιστήμιο της Γενεύης. Εν συντομία, το σκεπτικό έχει ως εξής: οποιαδήποτε προσπάθεια παρατήρησης ενός κβαντικού συστήματος αυτόματα προκαλεί την "αλλοίωσή" του. Κατ' αυτό τον τρόπο, ακόμη και η παραμικρή προσπάθεια υποκλοπής γίνεται αμέσως αντιληπτή. Η κβαντική κρυπτογράφηση βρίσκεται εδώ και μια δεκαετία στο στάδιο των εργαστηριακών δοκιμών, αλλά σύντομα αναμένεται να εφαρμοστεί και εμπορικά.

4.2.1 Γιατί πρέπει να χρησιμοποιείται

Δεν είναι λίγοι αυτοί που πιστεύουν ότι η χρήση κρυπτογραφικών εργαλείων αφορά μόνο κατασκόπους ή μανιώδεις χρήστες υπολογιστών. Στην πραγματικότητα, όταν κάποιος αποστέλλει ένα προσωπικό e-mail ή ανταλλάσσει εμπιστευτικές εμπορικές πληροφορίες για ένα έργο μέσω του ηλεκτρονικού ταχυδρομείου, οφείλει να γνωρίζει ότι, εάν δεν έχει κρυπτογραφηθεί, είναι σαν να το στέλνει με καρτ-ποστάλ: μπορεί να το διαβάσει σχεδόν οποιοσδήποτε.
Ένα e-mail, εκτός από τον αποστολέα και τον παραλήπτη, μπορεί να διαβαστεί εύκολα και από τους εργαζόμενους στον ISP (εταιρία παροχής Internet) του αποστολέα, τους εργαζόμενους στον ISP του παραλήπτη, από οποιονδήποτε ελέγχει τους routers από τους οποίους θα περάσουν τα "πακέτα" του μηνύματος και από οποιονδήποτε έχει πρόσβαση στον εξοπλισμό τηλεφωνίας στην τηλεφωνική εταιρία. Αν το μήνυμα αποστέλλεται ή παραλαμβάνεται από κινητό τηλέφωνο με σύνδεση στο Διαδίκτυο, τότε μπορεί να υποκλαπεί από άτομα με ειδικές συσκευές υποκλοπής συνομιλιών και μηνυμάτων κινητής τηλεφωνίας. Επιπλέον, είναι πολύ απλό να πλαστογραφηθεί η διεύθυνση αποστολής, ακόμα και με ένα τυπικό πρόγραμμα e-mail. Με λίγο περισσότερη δουλειά, κάποιος επιτήδειος μπορεί να αποκρύψει και άλλα σημάδια που δείχνουν από πού πραγματικά προέρχεται ένα μήνυμα. Λύση στα παραπάνω προβλήματα δίνουν οι τεχνολογίες κρυπτογράφησης. Οι τεχνολογίες αυτές εξασφαλίζουν ότι το μήνυμα θα μπορεί να το διαβάσει μόνο ο παραλήπτης του, καθώς στα ενδιάμεσα στάδια το μήνυμα εμφανίζεται με ακατάληπτους χαρακτήρες, είναι δηλαδή μη αναγνώσιμο. Εκτός από την κρυπτογράφηση, μια άλλη τεχνολογία που παρέχει τέτοιου είδους ασφάλεια είναι η ηλεκτρονική υπογραφή. Αξίζει, πάντως, να σημειώσουμε ότι είναι δυνατόν ένα μήνυμα να κρυπτογραφηθεί και ταυτόχρονα να υπογραφεί ηλεκτρονικά. Έτσι εξασφαλίζονται εξίσου η ασφάλεια στην επικοινωνία και η πιστοποίηση περιεχομένου και ταυτότητας αποστολέα.

4.2.2 Συμμετρική κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική. Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με πιο γνωστό τον Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης πόρρητων πληροφοριών.

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα έχουν αναπτυχθεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos, του MIT (Massachusetts Institute of Technology).

4.2.3 Ασύμμετρη κρυπτογράφηση

Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο 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

Προκειμένου να επιτευχθεί 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, συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν 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 αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.
Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από ό,τι η συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής.

4.3 Η υποδομή δημόσιου κλειδιού

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure - PKI) αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο, και παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

Το PKI ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση του PKI περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα προσφέρει σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών. Οι βασικές λειτουργίες/υπηρεσίες των Υποδομών Δημόσιου Κλειδιού είναι οι εξής:

Εμπιστευτικότητα (Confidentiality): Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. Η Υποδομή Δημόσιου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Ακεραιότητα (Integrity): Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους. Παρέχεται από μηχανισμούς κρυπτογραφίας όπως οι ηλεκτρονικές υπογραφές.

Μη Άρνηση Αποδοχής (Non-Repudiation): Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας. Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. Η ασύμμετρη κρυπτογραφία παρέχει ηλεκτρονικές υπογραφές, κατά συνέπεια μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει τη συγκεκριμένη υπογραφή. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά ο παραλήπτης του μηνύματος, μπορεί να επιβεβαιώσει την ηλεκτρονική υπογραφή του αποστολέα.

Πιστοποίηση (Authentication): Πρόκειται για την επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Κάθε χρήστης που επιθυμεί να επιβεβαιώσει την ταυτότητα ενός άλλου προσώπου ή εξυπηρετητή με τον οποίο επικοινωνεί, βασίζεται στην πιστοποίηση. Οι παραδοσιακές μέθοδοι πιστοποίησης είναι οι εξής:

- Με κάποιον κωδικό που γνωρίζουμε, όπως το PIN μιας τραπεζικής κάρτας ή το password ενός λογαριασμού
- Με κάποιο αντικείμενο που έχουμε στην ιδιοκτησία μας, λόγου χάρη το κλειδί μιας πόρτας ή μια τραπεζική κάρτα
- Με δακτυλικά αποτυπώματα, φωνή κ.λπ.

Το πιστοποιητικό (certificate) είναι ο τρόπος με τον οποίο η Υποδομή Δημόσιου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών ή πληροφορίες που σχετίζονται με αυτά, ή και τα δύο.

Η εκδότρια αρχή των πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (Certificate Authority - CA). Οι Αρχές Πιστοποίησης διασφαλίζουν τη δημοσίευση και τη διανομή των δημόσιων κλειδιών και λαμβάνουν το δημόσιο κλειδί του ενδιαφερόμενου χρήστη. Εάν ο χρήστης ενεργεί στη συγκεκριμένη περίπτωση ως ιδιώτης, θα πρέπει να παραχωρήσει όλα τα απαραίτητα στοιχεία που αποδεικνύουν την ταυτότητά του. Σε αντίθετη περίπτωση, ο χρήστης θεωρείται ότι ενεργεί εκ μέρους κάποιας επιχείρησης, οπότε οφείλει να παραχωρήσει όλες τις νομικές πληροφορίες που απαιτούνται για την αξιοπιστία και τη νόμιμη λειτουργία της.

Ουσιαστικά ένα ψηφιακό πιστοποιητικό αποτελεί μια ψηφιακά υπογεγραμμένη δήλωση από μια αρχή πιστοποίησης, η οποία:

1. Προσδιορίζει την αρχή πιστοποίησης που το εξέδωσε

2. Περιέχει το όνομα και κάποιες άλλες πληροφορίες του εγγεγραμμένου

3. Περιέχει το δημόσιο κλειδί του εγγεγραμμένου, το οποίο είναι ψηφιακά υπογεγραμμένο από την αρχή πιστοποίησης που το εξέδωσε

Για την πιστοποίηση της ταυτότητας των συναλλασσόμενων χρησιμοποιούνται τα πιστοποιητικά ασφαλείας, που επιπλέον εγγυώνται και την ασφάλεια ενός δικτυακού τόπου. Υπάρχουν δύο είδη πιστοποιητικών:

- Τα προσωπικά πιστοποιητικά, τα οποία αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη και κωδικός πρόσβασης. Στη συνέχεια, οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας που απαιτεί πιστοποιητικό. Επίσης, ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.

- Τα πιστοποιητικά δικτυακών τόπων, τα οποία περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας, ασφαλούς τοποθεσίας. Επίσης, τα πιστοποιητικά δικτυακών τόπων χρονολογούνται κατά την έκδοσή τους. Όταν προσπαθείτε να συνδεθείτε με το website ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκεμένοι στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν οι πληροφορίες αυτές δεν είναι έγκυρες ή εάν έχει παρέλθει η ημερομηνία λήξης, εμφανίζεται προειδοποιητικό μήνυμα (Warning).

Έχουν αναπτυχθεί ή βρίσκονται υπό κατασκευή διάφορα πρωτόκολλα ασφαλείας που κάνουν χρήση των παραπάνω τεχνικών, όπως το SSL (Secure Sockets Layer), της Netscape, και το SET (Secure Electronic Transactions), που αναπτύχθηκε από τη Visa και τη MasterCard. Από αυτά σήμερα χρησιμοποιείται το SSL. Αρκετές ιστοσελίδες είναι εξοπλισμένες με προγράμματα που χρησιμοποιούν το πρωτόκολλο αυτό, αποτρέποντας έτσι τα μη εξουσιοδοτημένα πρόσωπα από

την πρόσβασή τους σε δεδομένα που αποστέλλονται από και προς αυτές τις ιστοσελίδες. Τέτοια sites ονομάζονται "ασφαλή".

Οι πιο γνωστοί φυλλομετρητές ιστοσελίδων (browsers) υποστηρίζουν το πρωτόκολλο SSL και την κρυπτογράφηση που προσφέρει, ενώ ενημερώνουν το χρήστη ότι βρίσκεται σε ασφαλή τοποθεσία και μπορεί να στέλνει πληροφορίες ακίνδυνα. Με το πρωτόκολλο αυτό οι επικοινωνίες πραγματοποιούνται σε κωδικοποιημένη μορφή και επιπλέον γίνεται έλεγχος της αυθεντικότητας της ιστοσελίδας.

4.4 Η διαδικασία μιας ασφαλούς επικοινωνίας

Η διαδικασία μιας ασφαλούς επικοινωνίας έχει ως εξής:

- Ο φυλλομετρητής συνδέεται με τον ασφαλή δικτυακό τόπο.
- Ο δικτυακός τόπος δηλώνει την ταυτότητά του, η οποία ελέγχεται με τα πιστοποιητικά που εκδίδονται από υπηρεσίες πιστοποίησης.
- Η ασφαλής ιστοσελίδα και ο browser συμφωνούν στη χρήση συγκεκριμένου κλειδιού/αλγορίθμου που χρησιμοποιείται για την κρυπτογράφηση της υπόλοιπης επικοινωνίας.
- Τα δεδομένα που διακινούνται είναι κρυπτογραφημένα με το κλειδί/αλγόριθμο που συμφωνήθηκε στο προηγούμενο βήμα.

Η κρυπτογράφηση γίνεται με χρήση αλγορίθμου 40bit ή 128bit. Εάν έχει χρησιμοποιηθεί κρυπτογράφηση 40bit, τότε για να αποκρυπτογραφήσει κανείς τα δεδομένα που ανταλλάχθηκαν, θα πρέπει να δοκιμάσει περίπου 240 διαφορετικά κλειδιά, ενώ, εάν έχει χρησιμοποιηθεί κρυπτογράφηση 128bit, τότε θα πρέπει να δοκιμάσει περίπου 2.128 διαφορετικά κλειδιά. Με τη χρήση μεγάλης υπολογιστικής ισχύος, η αποκρυπτογράφηση του κλειδιού των 40bit μπορεί να επιτευχθεί σε μερικές ημέρες, ενώ η αποκρυπτογράφηση του κλειδιού των 128bit, με τα σημερινά δεδομένα, είναι πρακτικά αδύνατη. Θα πρέπει να σημειωθεί ότι απαγορεύεται από τη νομοθεσία των ΗΠΑ η εξαγωγή και χρήση προγραμμάτων που υποστηρίζουν κωδικοποίηση 128bit εκτός των Ηνωμένον Πολιτειών και του Καναδά.
Στο πλαίσιο των προσπαθειών που καταβάλλονται για την ανάπτυξη των ηλεκτρονικών συναλλαγών, έχει επιτραπεί η χρήση της τεχνολογίας SGC (Server Gated Cryptography) ή International Step-Up Encryption, που αποτελεί επέκταση του πρωτοκόλλου SSL, από πιστωτικά ιδρύματα και άλλων χωρών. Η επέκταση αυτή επιτρέπει στα πιστωτικά ιδρύματα, εφόσον διαθέτουν το κατάλληλο πιστοποιητικό, να επικοινωνούν με τους πελάτες τους με κωδικοποίηση 128bit.

4.5 Ταυτοποίηση Χρήστη (user authentication) και συναλλαγών

Τι σημαίνει ταυτοποίηση Χρήστη

Η ταυτοποίηση του χρήστη ενός συστήματος είναι η αναγνώριση της ταυτότητάς του από το σύστημα, ώστε να διασφαλίζεται ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε αυτό.

Πως διασφαλίζεται η ταυτοποίηση χρήστη στην υπηρεσία e-banking;

(α) Ταυτοποίηση χρήστη κατά την είσοδο στην υπηρεσία

Η είσοδος στην υπηρεσία ebanking επιτυγχάνεται με τη συνδυασμένη χρήση των προσωπικών κωδικών : Όνομα Χρήστη (user name) και Κωδικός Πρόσβασης (PIN). Οι κωδικοί αυτοί αποστέλλονται μετά την εγγραφή στην υπηρεσία ebanking και είναι απενεργοποιημένοι για λόγους ασφαλείας. Μόλις οι κωδικοί αυτοί φθάσουν στα χέρια του χρήστη θα πρέπει να επικοινωνήσει με την Διεύθυνση της τράπεζας του , και αφού επιβεβαιωθούν τα στοιχεία του, μπορεί να ζητήσει την ενεργοποίησή τους.

Για ακόμα μεγαλύτερη ασφάλεια κατά την διαδικασία εισόδου στην υπηρεσία ebanking, οι περισσότερες τράπεζες απαιτούν και τη καταχώρηση της Ηλεκτρονικής Υπογραφής Συναλλαγής. Η Ηλεκτρονική Υπογραφή Συναλλαγής είναι μία νέα πρωτοποριακή μέθοδος ταυτοποίησης χρηστών και στηρίζεται στην δημιουργία κωδικών μιας χρήσης (one time passwords) οι οποίοι παράγονται από την ειδική συσκευή Security Token που σας παρέχει η Τράπεζα.

(β) Ταυτοποίηση κατά την πραγματοποίηση συναλλαγών

Η διαδικασία ταυτοποίησης του χρήστη δεν σταματάει εδώ. Για την πραγματοποίηση οποιασδήποτε οικονομικής συναλλαγής ή και συναλλαγής που μεταβάλλει σημαντικά για σας στοιχεία (π.χ. αλλαγή PIN), απαιτείται η καταχώρηση της Ηλεκτρονικής Υπογραφής Συναλλαγής. Η Ηλεκτρονική Υπογραφή Συναλλαγής είναι ο κωδικός μιας χρήσης που προμηθεύεστε από την ειδική συσκευή Security Token, η οποία παράγει αυτόματα τον απαιτούμενο κωδικό. Η παραγωγή του κωδικού μίας χρήσης, πραγματοποιείται από τη συσκευή με τη βοήθεια ισχυρών μαθηματικών αλγορίθμων και άλλων τυχαία μεταβαλλόμενων παραμέτρων, όπως για παράδειγμα η χρονική στιγμή χρήσης της συσκευής.

4.6 Κρυπτογράφηση δεδομένων

Τι σημαίνει κρυπτογράφηση δεδομένων;

Προκειμένου όλες οι πληροφορίες που διακινούνται από τον υπολογιστή σας προς την Τράπεζα και αντιστρόφως να είναι απόρρητες, πρέπει να ταξιδεύουν σε κρυπτογραφημένη μορφή.

Πώς διασφαλίζεται η κρυπτογράφηση δεδομένων στην υπηρεσία ebanking;

Η υπηρεσία e-banking υποστηρίζεται από το πρωτόκολλο επικοινωνίας SSL με κρυπτογράφηση 128bit. Η κρυπτογράφηση στα 128 bit θεωρείται πρακτικά αδύνατο να παραβιαστεί, δεδομένου ότι ένα σύγχρονο υπολογιστικό σύστημα θα χρειαζόταν αρκετά δισεκατομμύρια έτη για να διαβάσει τέτοια κρυπτογραφημένα δεδομένα.

Μπορείτε να επιβεβαιώνετε ότι βρίσκεστε σε σελίδα με ενεργοποιημένη κρυπτογράφηση, εφόσον στην ηλεκτρονική διεύθυνση της σελίδας το «http» έχει μετατραπεί σε «https» (όπου s σημαίνει secure) και ταυτόχρονα υπάρχει το εικονίδιο με το λουκέτο στο κάτω μέρος της σελίδας αυτής.

Μεγέθη κωδικών και χρόνος δόκιμης όλων των πιθανών κωδικών

Key size	Number of Possible keys	Time to check all keys at 1.6 million keys per second	Time to check all keys at 10 million keys per second
40	1.099.511.627.776	8 Days	109 second
56	72.057.594.037.927	1,427 years	83 days
64	18.446,744,073,709	365,338 years	58.5 years
128	3,40282E+38	6,73931E+24 Years	1,07829E+ 21 years

4.7 Πιστοποίηση Τράπεζας και φίλτρα πρόσβασης στα συστήματα

Η πιστοποίηση παρέχεται στην Τράπεζα μέσω Πιστοποιητικού Αυθεντικότητας που εκδίδουν εξουσιοδοτημένες για το σκοπό αυτό ανεξάρτητες εταιρείες και διασφαλίζουν ότι κανείς άλλος δεν μπορεί να προσποιηθεί στον χρήστη ότι είναι η Τράπεζα και να υποκλέψει με τον τρόπο αυτό τις πληροφορίες του. Φίλτρα πρόσβασης στα συστήματα της Τράπεζας –

Firewalls. Είναι εξοπλισμός hardware & software που παρεμβάλλεται μεταξύ του Internet και των συστημάτων της Τράπεζας και φιλτράρουν τα δεδομένα που κυκλοφορούν σύμφωνα με τις πολιτικές ασφαλείας που καθορίζει η Τράπεζα και τα διεθνή πρότυπα. Με αυτό το φιλτράρισμα προστατεύονται όλα τα σημεία του δικτύου της Τράπεζας στα οποία ο εξωτερικός και εσωτερικός μη εξουσιοδοτημένος χρήστης δεν πρέπει να έχει πρόσβαση.

4.8 Εικονικό πληκτρολόγιο

Για περισσότερη ασφάλεια , οι περισσότερες τράπεζες χρησιμοποιούν ένα εικονικό πληκτρολόγιο. Το εικονικό πληκτρολόγιο είναι ένα κανονικό πληκτρολόγιο που εμφανίζεται στην οθόνη του υπολογιστή . και δίνει τη δυνατότητα να το χρησιμοποιήσετε για να συμπληρώσετε συγκεκριμένα στοιχεία στην οθόνη εισόδου στην υπηρεσία e-banking, αντικαθιστώντας το πραγματικό πληκτρολόγιο που είναι συνδεδεμένο με τον υπολογιστή.

Γιατί χρησιμοποιείται το εικονικό πληκτρολόγιο στην υπηρεσία e-banking;

Το εικονικό πληκτρολόγιο εμφανίζεται στην οθόνη εισόδου της υπηρεσίας e-banking για να συμπληρώσετε μέσω αυτού τους κωδικούς πρόσβασής σας στην υπηρεσία. Με τον τρόπο αυτό αποτρέπεται κάθε δυνατότητα υποκλοπής των κωδικών σας, μέσω ιών που μπορούν να καταγράψουν τις πληκτρολογήσεις από το πραγματικό πληκτρολόγιο.

4.9 Αυτόματος Τερματισμός Επικοινωνίας με την υπηρεσία ebanking

Όταν δεν χρησιμοποιείτε ένα σύστημα με το οποίο είστε συνδεδεμένος για συγκεκριμένο χρονικό διάστημα, διακόπτεται αυτόματα η σύνδεσή σας για λόγους ασφαλείας.

Πώς εφαρμόζεται ο αυτόματος τερματισμός επικοινωνίας στην υπηρεσία e-banking

Η επικοινωνία σας με την υπηρεσία e-banking τερματίζεται αυτόματα εφόσον δεν πραγματοποιήσετε κάποια ενέργεια μέσω αυτής για διάστημα μεγαλύτερο των 5 λεπτών. Με τον τρόπο αυτό αν είστε συνδεδεμένος με την υπηρεσία e-banking στον υπολογιστή σας και λείπετε από τη θέση σας, μειώνεται στο ελάχιστο ο χρόνος που θα είχε στη διάθεσή του κάποιος τρίτος για να κάνει χρήση της υπηρεσίας με τους κωδικούς σας.

Κλείδωμα κωδικών πρόσβασης

Όταν καταχωρούνται λανθασμένα συνεχόμενες φορές οι κωδικοί πρόσβασης σε ένα σύστημα κλειδώνονται, ώστε αν κάποιος προσπαθεί να μαντέψει τους κωδικούς αυτούς να μην έχει απεριόριστες προσπάθειες.

Πώς εφαρμόζεται το κλείδωμα κωδικών πρόσβασης στην υπηρεσία e-banking;

Οι κωδικοί πρόσβασης στην υπηρεσία e-banking (user name και PIN) κλειδώνονται αυτόματα στις 3 συνεχόμενες λανθασμένες καταχωρήσεις τους στην οθόνη εισόδου της υπηρεσίας. Γιατί έχει χαμηλά ποσοστά διείσδυσης το e-banking στην Ελλάδα και τι ρόλο παίζει ο φόβος για αδυναμίες στην ασφάλεια συναλλαγών

4.10 Έλλειψη προβολής ebanking η δυσφήμιση από τις τράπεζες;

Δεν υπάρχει θέμα δυσφήμισης. Στο παρελθόν είχαν παρερμηνευθεί κάποια μεμονωμένα περιστατικά προσπαθειών υποκλοπής στοιχείων από χρήστες internet banking, τα οποία ίσως να δημιούργησαν δυσπιστία σε μερίδα του κοινού ως προς την ασφάλεια των ηλεκτρονικών συναλλαγών. Θεωρούμε όμως πως η παρερμηνεία αυτή έγινε από άγνοια.

Οι τράπεζες δεν προέβαλαν σημαντικά στο παρελθόν τις ηλεκτρονικές τους υπηρεσίες. Τον τελευταίο καιρό βλέπουμε αυτή την πολιτική να αλλάζει και τον διαφημιστικό προϋπολογισμό που προσφέρουν για την προώθηση των σχετικών αυτών υπηρεσιών να αυξάνεται σημαντικά.

Φαίνεται ότι ένας από τους λόγους για τα χαμηλά ποσοστά διείσδυσης του internet banking στην Ελλάδα, είναι ο φόβος για αδυναμίες στην ασφάλεια συναλλαγών. Αν το δούμε από τη πλευρά “καλός” “χρήστης” της τεχνολογίας , ξέρουμε ότι αν ο παροχέας της υπηρεσίας χρησιμοποιεί κρυπτογράφηση στη μετάδοση των δεδομένων (π.χ. όταν κάποιος δίνει τα στοιχεία της κάρτας του και.. πατάει enter για να κάνει μια συναλλαγή ..) τότε δεν υπάρχει περίπτωση να υποκλέψει κάποιος τρίτος αυτά τα δεδομένα. Από τις καλές πρακτικές στην επικοινωνία αυτών των θεμάτων είναι να δηλώνεται με σαφή τρόπο , το χαρακτηριστικό της κρυπτογράφησης .

Κάθε είδος ηλεκτρονικής συναλλαγής εμπεριέχει πιθανότητα για φθορές , αλλά και πάλι αυτό εξαρτάται από το μέσο : συναλλαγή μέσω internet ή ATM . Δεν πρέπει να ξεχνάμε όμως και τη σωστή ενημέρωση του χρήστη των υπηρεσιών π.χ. δεν πρέπει να αφήνετε κωδικούς πάνω στο πορτοφόλι σε δημόσια σημεία .. – το ζήτημα της ασφάλειας πηγαίνει και στη σωστή χρήση.Οι νέες τεχνολογίες στο χώρο του ebanking από τα ATM , το phone banking , οι συναλλαγές μέσω κινητού κτλ είναι για το καταναλωτή το ίδιο πράγμα , αφού προσπαθεί να βρει τις ίδιες υπηρεσίες που θα έβρισκε και στο ταμείο . με τη διαφορά όμως ότι με αυτά τα κανάλια συναλλαγών κάνεις όποτε θέλεις τη δουλειά σου και γλιτώνεις χρόνο.

4.11 Συμπεράσματα

Η ανάπτυξη ασφαλών συστημάτων που θα είναι φιλικά προς το χρήστη και στα οποία θα πραγματοποιείται η διακίνηση ευαίσθητων πληροφοριών χωρίς κίνδυνο υποκλοπής ή αλλοίωσης αναμένεται ότι θα συντελέσει στην αύξηση της χρήσης του Internet τόσο στον τομέα των εμπορικών συναλλαγών όσο και γενικότερα στις επικοινωνίες. Ειδικότερα, η προστασία των προσωπικών δεδομένων στο πλαίσιο λειτουργίας του ηλεκτρονικού εμπορίου αποτελεί κρίσιμο παράγοντα για την επιτυχημένη εκπλήρωση των στόχων του στην Κοινωνία της Πληροφορίας. Οι κίνδυνοι προσβολής της προσωπικότητας μπορούν να προστατευθούν με την εφαρμογή των κατάλληλων μέτρων προστασίας κάθε εμπλεκόμενου φορέα σε μια ηλεκτρονική συναλλαγή. Τεχνικές που στοχεύουν στην ανωνυμοποίηση των καναλιών επικοινωνίας, τεχνολογίες ασφάλειας των πληροφοριών και προστασίας της ιδιωτικότητας (όπως η κρυπτογράφηση) είναι άμεσα συνδεδεμένες με ένα επιτυχημένο περιβάλλον ηλεκτρονικού επιχειρεί.
Μικρομεσαίες επιχειρήσεις που χρησιμοποιούν το Διαδίκτυο ή δραστηριοποιούνται σ' αυτό, δεν έχουν ουσιαστικά άλλη επιλογή από το να υιοθετούν σε μικρό ή μεγάλο βαθμό τεχνικές κρυπτογράφησης.

Κεφαλαίο 5:Διαδικτυακό έγκλημα και κίνδυνοι του e-banking

5.1 e-banking και διαδικτυακό έγκλημα

Παρά τις εξελιγμένες μεθόδους για τη διασφάλιση των τραπεζικών συναλλαγών, η συχνότητα των ηλεκτρονικών επιθέσεων αυξάνεται τα τελευταία χρόνια. Η αύξηση αυτή προκαλεί ανησυχία στους ειδικούς, καθώς διακυβεύονται τεράστια ποσά, ειδικά στις περιπτώσεις κατά τις οποίες θύματα απάτης γίνονται επιχειρήσεις. Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους για να επιτύχουν τους σκοπούς τους. Οι μεγαλύτεροι κίνδυνοι δεν προέρχονται από ατέλειες των συστημάτων ασφαλείας και κρυπτογράφησης αλλά από τον ανθρώπινο παράγοντα. Έρευνες ειδικών σε θέματα ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είτε είχαν την ακούσια -συνήθως- βοήθεια και κάποιου που εργαζόταν στην τράπεζα, είτε υπέκλεψαν κωδικούς χρηστών. Οι επιχειρήσεις-πελάτες είναι συνήθως προσεκτικές και χρησιμοποιούν συστήματα ασφαλείας στα δίκτυά τους. Την ίδια "σοφία" ή προσοχή δεν δείχνουν και οι ιδιώτες πελάτες, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια. Οι απλοί χρήστες γίνονται εύκολα θύματα προγραμμάτων που στην πραγματικότητα ανοίγουν "τρύπες" ασφάλειας στο σύστημα επιτρέποντας σε επιτήδειους να έχουν πρόσβαση σε αυτό. Ωστόσο και οι επιχειρήσεις δεν είναι πάντοτε ασφαλείς. Σε ορισμένες περιπτώσεις, εταιρίες συνεργάζονται με τράπεζες προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με εταιρικούς πελάτες. Οι τράπεζες ενίοτε επιτρέπουν στις εταιρίες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, οι επιτήδειοι μελετούν τον τρόπο με τον οποίο οι επιχειρήσεις επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα. Μόλις βρεθεί μια αδυναμία, μεταφέρουν με λίγες απλές κινήσεις ολόκληρους εταιρικούς λογαριασμούς στις προσωπικές τους θυρίδες. Να σημειωθεί, πάντως, πως η πρακτική αυτή, η διαχείριση δηλαδή τραπεζικού δικτύου από εταιρικό πελάτη, δεν συνηθίζεται στην Ελλάδα. Εξάλλου μέχρι σήμερα δεν έχουν δει το φως της δημοσιότητας περιπτώσεις απάτης στον τομέα του ελληνικού e-banking.

5.2 Κίνδυνοι του e-banking

Αν και οι ηλεκτρονικές επιθέσεις δεν αποτελούν νέο φαινόμενο, η συχνότητά τους τα τελευταία χρόνια αυξάνεται μια και όλο και περισσότερες τράπεζες παρέχουν στους πελάτες τους on-line υπηρεσίες. Η αύξηση αυτή δεν είναι τεράστια, εντούτοις όμως αποτελεί ένα ανησυχητικό φαινόμενο μια και πολλοί θεωρούν τις οικονομικές πληροφορίες που τους αφορούν άκρως απόρρητες και διατηρούν μια επιφυλακτική στάση απέναντι σε διαδικασίες που τις καθιστούν ευάλωτες στο ευρύ κοινό, όπως είναι το e-banking.
Στοιχεία για το ηλεκτρονικό έγκλημα δεν κοινοποιούνται δημοσίως, αλλά υπολογίζεται ότι στις Η.Π.Α. χάνονται ετησίως περίπου 11 δισεκατομμύρια δολάρια από εταιρείες και καταναλωτές λόγω αυτής της μορφής εγκλήματος. Το μεγαλύτερο μέρος προέρχεται από οικονομικά ιδρύματα. Μάλιστα το μεγαλύτερο μέρος των ζημιών δεν προκύπτει από τις κλοπές χρημάτων, αλλά από έξοδα που κάνουν οι εταιρείες μετά από τέτοιου είδους επιθέσεις, προκειμένου να διασφαλίσουν τα συστήματά τους ώστε να μην ξανασυμβούν. Ειδικοί σε θέματα ασφάλειας έχουν υπολογίσει ότι μια τράπεζα μπορεί να ξοδέψει μέχρι και 1 εκατομμύριο δολάρια σε

εξοπλισμό και συμβούλους ασφάλειας προκειμένου να διορθώσει τις ατέλειες και να κλείσει τις «τρύπες» στο σύστημά της.
Το πρόβλημα πάντως δεν προβάλλεται στις πλήρεις του διαστάσεις για ευνόητους λόγους. Οι μεγαλύτερες και εντυπωσιακότερες επιθέσεις είναι αυτές που θα δοθούν στη δημοσιότητα, οι υπόλοιπες και περισσότερες, κρατούνται κρυφές. Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους πάντως να επιτύχουν τους σκοπούς τους. Παρά τις οποιεσδήποτε τεχνικές αδυναμίες των συστημάτων για on-line 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. αι 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.
Οι κλεμμένες πληροφορίες αποτελούν την πρώτη φάση μιας αρκετά επίπονης διαδικασίας η οποία μπορεί να διαρκέσει μέχρι και εβδομάδες, έτσι ώστε ο χάκερ να υποδυθεί κάποιον άλλο στο διαδίκτυο. Η οποία όμως διευκολύνεται συνεχώς με καινούρια προγράμματα που κυκλοφορούν στην αγορά. Η εποχή που πολλές επιθέσεις θα γίνονται με αυτοματοποιημένο τρόπο δεν απέχει πολύ, σύμφωνα με αρκετούς ειδικούς.
Μια άλλη μέθοδος που τις περισσότερες φορές έχει αποτελέσματα δεν επικεντρώνεται στην τράπεζα ευθέως, αλλά σε μια από τις εταιρείες που συνεργάζονται με αυτήν προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με τους πελάτες της. Σε πολλές περιπτώσεις οι τράπεζες επιτρέπουν στις εταιρείες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, ο εισβολέας θα πρέπει να μελετήσει τον τρόπο με τον οποίο οι εταιρείες επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα. Μόλις βρεθεί μια αδυναμία κάνουν την κίνησή τους.
Ένας άλλος τρόπος είναι να χτυπήσουν τις μικρές, τοπικές τράπεζες οι οποίες μπήκαν στον τομέα του e-banking εσπευσμένα προκειμένου να διατηρήσουν τον ανταγωνισμό με τις μεγαλύτερες τράπεζες. Δυστυχώς όμως λόγω αυτής της βιασύνης, οι τράπεζες αφήνουν πολλές «τρύπες» στα συστήματά τους, κάτι που οι επίδοξοι εισβολείς εκμεταλλεύονται πολύ εύκολα. Οι ειδικοί μας πληροφορούν ότι κλοπές ποσών από 5 μέχρι 10 χιλιάδες δολαρίων μπορούν να πραγματοποιηθούν σε χρονικό διάστημα μερικών εβδομάδων. Για ποσά μέχρι και 1 εκατομμυρίου δολαρίων χρειάζονται 4 μέχρι και 6 μήνες.

5.3 Διαχείριση Κινδύνων για το e-banking

Ο κάθε τραπεζικός οργανισμός είτε δραστηριοποιείτε ηλεκτρονικά εδώ και κάποια χρόνια είτε τώρα διαμορφώνει τη στρατηγική του στο e-επιχειρεί, θα πρέπει να έχει υπόψη ότι κάθε επιχείρηση οφείλει να είναι εξοικειωμένη με την Διαχείριση Κρίσεων και Επιχειρηματικού Κινδύνου. Πρόκειται για μια διαδικασία που έχει εφαρμογή στη διασύνδεση των διαφόρων

λειτουργιών εντός της επιχείρησης αλλά και στις σχέσεις της με τους πελάτες και τους εξωτερικούς συνεργάτες.
Οι τράπεζες που πιστεύουν ότι μπορούν να προστατευτούν, εγκαθιστώντας κάποιο αντι-ιικόν (anti-virus), ένα firewall και κάποια εφαρμογή κρυπτογράφησης δύστυχος απατώνται.
Ένα πραγματικά αποτελεσματικό πρόγραμμα διαχείρισης κινδύνων και κρίσεων ηλεκτρονικής τραπεζικής ενσωματώνει ασφαλιστικά προϊόντα μετριασμού του επιχειρηματικού κινδύνου και του κόστους που προκύπτει έπειτα από μια ηλεκτρονική καταστροφή.

5.4 Αποτίμηση επιχειρηματικού κινδύνου

Προκειμένου η τράπεζα να αποτιμήσει τους κινδύνους που έχουν σχέση με την ηλεκτρονική τραπεζική, πρέπει να προβεί σε μια ανάλυση.

Ανάλυση Επιχειρηματικού Μοντέλου

- Διαθέτει η τράπεζα λογιστική οργάνωση βασισμένη σε ηλεκτρονικές διαδικασίες;
- Ποιοι είναι οι στόχοι ως προς την τεχνολογική ολοκλήρωση των ενδοεπιχειρησιακων διαδικασιών; Ελέγχονται από την ίδια τράπεζα ή γίνεται ανάθεση σε εξωτερικούς συνεργάτες;
- Παρέχει υπηρεσίες προς τρίτους με ηλεκτρονικά μέσα;

Ανάλυση Πνευματικού Κεφαλαίου

- Ποια είναι η άξια του πνευματικού κεφαλαίου της τράπεζας, όπως βάσεις δεδομένων, πνευματικά δικαιώματα, εμπορικά σήματα, κ.λπ. ;

Συνεργασίες

- Με ποιους συνεργάζεται ηλεκτρονικά στις βασικές της δραστηριότητες, οι οποίοι θα μπορούσαν να επηρεάσουν από μια πιθανή κρίση

Τεχνολογική Ανάλυση

- Η τεχνολογική υποδομή καλύπτει τις ανάγκες της στρατηγικής στο e-baking;

Λειτουργικοί Περιορισμοί

- Είναι σε θέση το e-banking να ανταποκριθεί σε παροχή υπηρεσιών 24 ώρες το 24ωρο;

Ασφάλεια Δεδομένων

- Πόσο καλό είναι το επίπεδο προστασίας των προσωπικών δεδομένων πελατών, υπαλλήλων, επιχειρηματικών συνεργατών, καθώς και των οικονομικών και νομικών πληροφοριών της τράπεζας;

Εξωτερικοί Παράγοντες

- Είναι η τράπεζα εναρμονισμένη με τη σχετική νομοθεσία, όπως οι κανονισμοί EU Data Directive, Digital Millennium Copyright Act, κ.α;
- Πόσο ασφαλείς είναι οι ηλεκτρονικές συναλλαγές;

Συμβατικές Υποχωρήσεις

- Παρέχει η τράπεζα δηλώσεις προστασίας προσωπικών δεδομένων, παραίτησης από ευθύνη, κ.α;
- Γνωρίζει τις κυρώσεις σε περίπτωσης που αποδειχθεί ότι παρέβη κάποια από τις παραπάνω δηλώσεις;

5.5 Διαχείριση ηλεκτρονικών κρίσεων

Άμεσοι κίνδυνοι

- Προβλήματα τεχνολογικής υποδομής, τα οποία περιορίζουν την ικανότητα της τράπεζας να διεξαγάγει με ασφάλεια τις κύριες εμπορικές διαδικασίες, συμπεριλαμβανομένης της επικοινωνίας με τους προμηθευτές, τους διανομής και τους πελάτες.
- Αποτυχία των εσωτερικών διαδικασιών να ελέγξουν την ασφάλεια δικτύωσης, με αποτέλεσμα τη μη διαθεσιμότητα εταιριών δικτύων ή εφαρμογών, και την πιθανή εισβολή και ζημιά στο πνευματικό κεφάλαιο και τις ευαίσθητες πληροφορίες της επιχείρησης από χάκερ, ιούς, κ.α.
- Δημοσιοποίηση απορρήτων εταιρικών πληροφοριών, σχεδίων ή άλλων εμπιστευτικών εμπορικών στοιχείων.
- Μη εξουσιοδοτημένη εσωτερική ή εξωτερική πρόσβαση σε εφαρμογές ή δεδομένα της τράπεζας.
- Αποτυχία διεξαγωγής online συναλλαγών.

Έμμεσοι κίνδυνοι

- Δυσφήμηση του ονόματος της τράπεζας
- Απώλεια κεφαλαίων
- Ακούσια παραβίαση των προσωπικών δεδομένων των πελατών μέσο της κοινοποίησης των προσωπικών τους στοιχείων
- Απώλειες από ηλεκτρονικές απάτες ή κλοπές
- Δικαστική δίωξη από τρίτα μέρη

5.6 Πλαίσιο διαχείρισης ηλεκτρονικών κρίσεων

Το πλαίσιο διαχείρισης ηλεκτρονικών κινδύνων περιλαμβάνει μια σειρά από συνιστώσες που βοηθούν στην αποτελεσματικότητα του.

Υποδομή

- Ανάπτυξη, συντήρηση και προστασία βάσεων δεδομένων.
- Επεκτασιμότητα δικτύων και server.
- Προστασία υποδομής από φυσικές καταστροφές
- Δομικές καλής λειτουργίας μεμονωμένων στοιχείων.
- 24ωρη παρακολούθηση δικτύων και συστημάτων
- Δομικές υπερφορτώσεις δικτύων
- Ανάπτυξη συστήματος έγκαιρης ειδοποίησης σε περίπτωσης εκτάκτων αναγκών
- Επαναφορά / ανάληψη έπειτα από καταστροφή και καθορισμό διαδικασιών και ευθυνών για την αδιάκοπη λειτουργία της επιχείρησης
- Έλεγχος πληροφορικών συστημάτων και ασφάλεια διαδικασιών αναβάθμισης εφαρμογών ή εξοπλισμού
- Έλεγχος ποιότητας των υπηρεσιών που παρέχονται από τρίτα μέρη και αφορούν σε κρίσιμες λειτουργίες της επιχείρησης.

5.7 Απειλές - Κίνδυνοι

Sniffers

Ένας sniffer είναι ένα πρόγραμμα ή μια συσκευή που παρακολουθεί κρυφά την κίνηση ενός δικτύου με σκοπό να αρπάξει πληροφορία που ταξιδεύει σε αυτό. Ουσιαστικά οι sniffer είναι τεχνολογία υποκλοπής δεδομένων. Λειτουργούν επειδή το Ethernet κατασκευάστηκε γύρω από την αρχή του sharing. 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, υπολογιστές μπορούν να διαμορφωθούν, ώστε να δέχονται μηνύματα ακόμα και αν δεν είναι για αυτούς. Αυτό γίνεται με την χρήση ενός sniffer.

Key Loggers

Το key logging (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 / εταιρικών στοιχείων. Η καταγραφή και αποθήκευση των πληκτρολογήσεων γίνεται από ειδικό υλικό (hardware), το οποίο είναι εύκολο να εγκατασταθεί και ταυτόχρονα δύσκολο να εντοπιστεί. 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 μέσο internet σε αυτόν που κατασκοπεύει το χρήστη.

Δούρειοι Ίπποι

Ένας Δούρειος Ίππος (Trojan Horse) είναι ένα φαινομενικά χρήσιμο πρόγραμμα για τον υπολογιστή που περιέχει καμουφλαρισμένες εντολές, οι οποίες όταν εκτελεστούν δημιουργούν αθέμιτες ή βλαπτικές δράσεις. Οι δούρειοι ίπποι δεν μπορούν να δημιουργούν πανομοιότυπα αντίγραφα, αυτόματα. Η εγκατάσταση τους εξαρτάτε από τους χρηστές, ή από εισβολείς που έχουν αποκτήσει μη εγκεκριμένη πρόσβαση σε 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 οποιοδήποτε αρχείου στον εισβολέα, που μπορεί να διαβάσει ο χρηστής
- Αλλαγή αρχείων που μπορεί ο χρηστής να μεταβάλει
- Εγκατάσταση προγραμμάτων με τα δικαιώματα του χρήστη του υπολογιστή που παρέχουν μη εγκεκριμένη πρόσβαση σε δίκτυο.
- Εγκατάσταση ιών
- Εγκατάσταση άλλων δούρειων ίππων

Phishing

Το Phishing είναι η αποστολή e-mail σε χρήστη, προσποιούμενος ότι προέχετε από μια νόμιμη επιχείρηση, κυρίως Τράπεζα, με σκοπό να εξαπατήσει τον χρήστη και να πάρει ιδιωτικές πληροφορίες που θα χρησιμοποιηθούν για κλοπή της ταυτότητος τους. Το e-mail προτρέπει τον χρήστη να επισκεφθεί ένα web site όπου του ζητούνται να ενημερώσει τις προσωπικές του πληροφορίες, όπως passwords και αριθμούς πιστωτικών καρτών, αριθμούς τραπεζικών λογαριασμών, που η εταιρεία υποτίθεται έχει ήδη στην κατοχή της. Το web site ωστόσο είναι πλαστό και έχει δημιουργηθεί με μοναδικό σκοπό να κλέψει ζητούμενη πληροφορία.

Pharming

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

Οι βασικές διαφορές του pharming είναι δύο:

1. Η επίθεση μπορεί να γίνει μαζικά σε πολλούς χρήστες και όχι μεμονωμένα σε κάθε χρήση (μέσω e-mail).
2. Η μετακίνηση σε pharming site γίνεται χωρίς την παρεμβολή 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 πληκτρολόγηση το σωστό URL.

-Παραποίηση DNS: Η κυριότερη απειλή του pharming είναι η παραποίηση του DNS (Domain Name System) ενός εταιρικού site. Αυτό έχει ως αποτέλεσμα την μετάβαση μεγάλου αριθμού χρηστών σε sites απατεώνων χωρίς καν να το αντιλαμβάνονται.

Ιδιαίτερα διαδεδομένη είναι η χρήση ψευδών τραπεζικών sites (Fake Banks). Στην περίπτωση αυτή, οι εισβολείς δημιουργούν sites πανομοιότυπα με αυτά των νομικών τραπεζικών, με μικρές διαφοροποιήσεις, ή ακόμα τα νέα sites που υποτίθεται ότι είναι ηλεκτρονικές τράπεζες. 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 καμιά υπόσταση σε τέτοια sites, δίνοντας έτσι κωδικούς, αριθμούς λογαριασμών και καρτών εν αγνοία τους.

5.8 Επιθέσεις δηλητηρίασης SQL κώδικα

Σε αυτή τη νέα εποχή, οι επιχειρήσεις, οι οργανισμοί, οι κυβερνήσεις, αλλά και μεμονωμένα άτομα χρησιμοποιούν όλο και περισσότερο εφαρμογές ιστού, γιατί είναι σε θέση να προσφέρουν αποδοτικότερες, αποτελεσματικότερες και φθηνότερες λύσεις στις προκλήσεις της επικοινωνίας και της διεξαγωγής εμπορικών συναλλαγών.
Η χρήση εφαρμογών ιστού προσφέρει σημαντικά πλεονεκτήματα τόσο για τον πάροχο όσο και για τον χρήστη. Τα κυριότερα από αυτά είναι η εξάλειψη περιορισμών χρόνου και χώρου, δεδομένου ότι μια ηλεκτρονική συναλλαγή μπορεί να πραγματοποιηθεί οποιαδήποτε στιγμή (διαθεσιμότητα 24 ώρες επί 7 ημέρες), χωρίς να απαιτείται η φυσική παρουσία του χρήστη. Καθώς όμως η ζήτηση για δεδομένα και πληροφορίες αυξάνεται, παράλληλα προκύπτουν κρίσιμα ζητήματα που αφορούν την ασφάλεια των εφαρμογών, των βάσεων δεδομένων και των πληροφοριών.
Μια από τις σημαντικότερες απειλές για την ασφάλεια των εφαρμογών ιστού είναι οι επιθέσεις δηλητηρίασης SQL κώδικα. Μια ευπάθεια δηλητηρίασης SQL κώδικα υπάρχει όταν ένας επιτιθέμενος είναι σε θέση να εισάγει μια σειρά δηλώσεων σε ένα SQL ερώτημα, παραποιώντας τα δεδομένα που εισάγει σε μια εφαρμογή ιστού.
Σήμερα παρατηρείται μια πληθώρα εφαρμογών ιστού που καλύπτουν ένα ευρύ φάσμα δραστηριοτήτων. Ενδεικτικά μπορούν να αναφερθούν συναλλαγές ηλεκτρονικού εμπορίου (e-commerce), ηλεκτρονικές τραπεζικές συναλλαγές (e-banking), υπηρεσίες ηλεκτρονικής διακυβέρνησης (e-government), ηλεκτρονικές ψηφοφορίες (e-voting), ή ηλεκτρονικές υπηρεσίες υγείας (e-health).
Στην ουσία οι εφαρμογές ιστού στηρίζονται σε μια αρχιτεκτονική πελάτη (client) - διακομιστή (server) που αλληλεπιδρούν μέσω του πρωτοκόλλου HTTP (Hypertext Transfer Protocol) . Από την πλευρά του πελάτη υπάρχει τυπικά ένας φυλλομετρητής ιστού (web browser), ενώ από την πλευρά του διακομιστή υπάρχουν κατανεμημένοι διακομιστές εφαρμογών (application servers), που συνδέονται με πολλαπλές πηγές δεδομένων. Ο χρήστης αλληλεπιδρά με την εφαρμογή ιστού, στέλνοντας τις επιλογές ή τα δεδομένα του. Η αλληλεπίδραση αυτή μπορεί να κυμανθεί από μια απλή αναζήτηση δεδομένων, έως μεγάλες ενδοεπιχειρησιακές εφαρμογές που εκτελούν σε πραγματικό χρόνο πωλήσεις και διαχείριση απογραφής επικίνδυνους τύπους επιθέσεων που

προσβάλουν εφαρμογές ιστού. Μέχρι σήμερα έχουν αναφερθεί πολλά περιστατικά επιτυχών επιθέσεων. Διαδεδομένα εργαλεία λογισμικού έχουν βρεθεί ευπαθή, όπως τα PHPNuke, vBulletin, WordPress, WBBlog, μεταξύ πολλών άλλων. Ίσως το πιο γνωστό περιστατικό SQL έγχυσης συνέβηκε το 2005 με την έκθεση της βάσης δεδομένων της CardSystems Solutions , που είχε ως αποτέλεσμα την κλοπή εκατομμυρίων αριθμών πιστωτικών καρτών.
Ο οργανισμός OWASP (Open Web Application Security Project) σε ένα ενημερωτικό δελτίο για το έτος 2007 κατατάσσει τις επιθέσεις έγχυσης στη δεύτερη θέση ανάμεσα στις δέκα πιο σημαντικές ευπάθειες που συναντιούνται σε εφαρμογές ιστού.
Εισαγωγή 4 Ανάλογα συμπεράσματα προκύπτουν και από τις αναλύσεις του οργανισμού WASC (Web Application Security Consortium), από τις οποίες προκύπτει ότι το 26,38% των εφαρμογών ιστού είναι ευπαθείς σε επιθέσεις SQL έγχυσης.
Η ασφάλεια της εφαρμογής δεν μπορεί να καλυφθεί μέσω των παραδοσιακών συστημάτων ανίχνευσης παρεισφρήσεων (Intrusion Detection Systems) και των αναχωμάτων ασφαλείας (firewalls), γιατί απλά δεν έχουν σχεδιαστεί για να χειριστούν τη δυσκολία που συνεπάγεται αυτός ο τύπος ασφάλειας.
Για να θωρακιστεί η ασφάλεια μιας εφαρμογής ιστού από διάφορες μεθόδους επιθέσεων, οι υπεύθυνοι για την ανάπτυξη της μπορούν να ακολουθούν πρακτικές ασφαλούς κώδικα , με σκοπό να περιοριστούν οι ευπάθειες που μπορεί να παρουσιαστούν σε μια εφαρμογή. Σε αυτό ακριβώς το σημείο εντοπίζεται η αχίλλειος πτέρνα της ασφάλειας όλου του συστήματος. Σε αντίθεση με τους διαχειριστές των δικτύων και των βάσεων δεδομένων, οι υπεύθυνοι για την ανάπτυξη εφαρμογών ιστού συνήθως έχουν έλλειψη γνώσεων πάνω σε θέματα ασφάλειας και επιπλέον δίνουν προτεραιότητα σε άλλους τομείς, όπως η ευχρηστία, η απόδοση και η καλαισθησία των εφαρμογών, και όχι στην ασφάλεια. Το αποτέλεσμα είναι η εφαρμογή να παρουσιάζει αρκετά κενά ασφάλειας, που είναι πολύ δύσκολο να καλυφτούν εκ των υστέρων με βελτιώσεις και προσθήκες στον κώδικα της εφαρμογής.
Πρέπει να σημειωθεί ότι γενικά οι διάφοροι τύποι επίθεσης δεν χρησιμοποιούνται μεμονωμένα. Η συνήθης πρακτική ορίζει δύο ή περισσότεροι τύποι επίθεσης δηλητηρίασης SQL κώδικα να συνδυάζονται ώστε να πετύχουν το επιθυμητό από τον επιτιθέμενο αποτέλεσμα. Ένα ακόμα πιθανό σενάριο είναι να προηγηθεί μια επίθεση δηλητηρίασης SQL κώδικα με στόχο την αναγνώριση του συστήματος (λειτουργικό σύστημα, σύστημα διαχείρισης βάσεων δεδομένων, τύπος διακομιστή) και στη συνέχεια, να ακολουθήσει μια τυπική δικτυακή επίθεση. Η διαδικασία αναγνώρισης του συστήματος είναι γνωστή ως ιχνηλάτηση (foot printing). Η ιχνηλάτηση αποτελεί ένα προκαταρτικό βήμα, κατά το οποίο κατασκευάζεται μια ολοκληρωμένη εικόνα του συστήματος και των ευπαθειών που αυτό ενδεχομένως να παρουσιάζει, ώστε να καθοριστεί ο τρόπος επίθεσης που θα ακολουθηθεί από τον επιτιθέμενο.

Ταυτολογίες

Ο γενικός στόχος μιας επίθεσης βασισμένης σε ταυτολογία (tautology) είναι να εισαχθεί κώδικας σε μια ή περισσότερες δηλώσεις συνθήκης έτσι ώστε αυτές να αποτιμώνται πάντα σε αληθείς. Οι συνέπειες αυτής της επίθεσης εξαρτώνται από τον τρόπο με τον οποίο τα αποτελέσματα του ερωτήματος χρησιμοποιούνται μέσα στην εφαρμογή. Οι πιο κοινές χρήσεις είναι η παράκαμψη της διαδικασίας πιστοποίησης και η εξαγωγή δεδομένων.
Σε αυτόν τον τύπο επίθεσης, ένας κακόβουλος χρήστης εκμεταλλεύεται ένα πεδίο εισόδου, η τιμή του οποίου χρησιμοποιείται σε μία συνθήκη WHERE ενός SQL ερωτήματος. Ο μετασχηματισμός της συνθήκης σε μια ταυτολογία προκαλεί την επιστροφή όλων των γραμμών του πίνακα της βάσης δεδομένων που συνδέεται με το ερώτημα. Γενικά, για να δουλέψει μια

επίθεση βασισμένη σε ταυτολογία, ο επιτιθέμενος πρέπει να εξετάσει όχι μόνο τις τρωτές παραμέτρους, αλλά και τη σχεδίαση του κώδικα που αποτιμά τα αποτελέσματα του ερωτήματος. Η επίθεση είναι επιτυχής όταν η εφαρμογή, είτε εμφανίζει όλες τις επιστρεφόμενες εγγραφές, είτε εκτελεί κάποια ενέργεια εάν τουλάχιστον μια εγγραφή επιστρέφεται.

Ερωτήματα ένωσης

Στις επιθέσεις με ερωτήματα ένωσης (UNION), ένας επιτιθέμενος εκμεταλλεύεται μια τρωτή παράμετρο για να αλλάξει το σύνολο των δεδομένων που επιστρέφονται από ένα συγκεκριμένο SQL ερώτημα. Με αυτήν την τεχνική, ένας επιτιθέμενος μπορεί να εξαπατήσει την εφαρμογή αναγκάζοντας την να επιστρέψει δεδομένα από έναν πίνακα διαφορετικό από αυτόν που αρχικά σχεδίασε ο υπεύθυνος για την ανάπτυξη της εφαρμογής. Οι επιτιθέμενοι μπορούν να το πετύχουν αυτό με την έγχυση μιας δήλωσης της μορφής UNION SELECT < υπόλοιπο της εγχεόμενης ερώτησης > αποτέλεσμα αυτής της επίθεσης οδηγεί τη βάση δεδομένων να επιστρέψει ένα σύνολο δεδομένων που αποτελεί ένωση των αποτελεσμάτων του πρωτότυπου ερωτήματος με τα αποτελέσματα του εγχεόμενου δεύτερου ερωτήματος.

Πρόσθετες SQL δηλώσεις

Ο σκοπός αυτού του είδους επίθεσης μπορεί να είναι η εξαγωγή, η προσθήκη, ή η τροποποίηση δεδομένων, η πρόκληση άρνησης εξυπηρέτησης της εφαρμογής, ή η εκτέλεση απομακρυσμένων εντολών.
Σε αυτόν τον τύπο επίθεσης, ένας επιτιθέμενος προσπαθεί να εγχύσει πρόσθετες SQL δηλώσεις στο αρχικό ερώτημα. Διακρίνουμε αυτόν τον τύπο από άλλους, επειδή σε αυτήν την περίπτωση ο επιτιθέμενος δεν προσπαθεί να τροποποιήσει το αρχικό ερώτημα, αλλά αντίθετα, προσπαθεί να συμπεριλάβει νέα ξεχωριστά ερωτήματα που έπονται του αρχικού. Κατά συνέπεια, η βάση δεδομένων λαμβάνει και εκτελεί Ταξινόμηση επιθέσεων δηλητηρίασης πολλαπλά SQL ερωτήματα. Το πρώτο από αυτά είναι το κανονικό ερώτημα, ενώ τα επόμενα είναι τα εγχεόμενα ερωτήματα, τα οποία εκτελούνται διαδοχικά μετά από το πρώτο. Αυτός ο τύπος επίθεσης μπορεί να είναι εξαιρετικά επιβλαβής. Εάν επιτύχει η επίθεση, ένας κακόβουλος χρήστης μπορεί ουσιαστικά να παρεμβάλει οποιαδήποτε SQL εντολή στα πρόσθετα ερωτήματα και να την εκτελεστεί μαζί με το αρχικό ερώτημα. Η ευπάθεια σε αυτόν τον τύπο επίθεσης εξαρτάται συχνά από το εάν η ρυθμίσεις του συστήματος βάσεων δεδομένων επιτρέπουν πολλαπλές δηλώσεις να συμπεριλαμβάνονται σε μια ενιαία σειρά.
Έχοντας συλλέξει τις απαραίτητες πληροφορίες με μια διαδικασία ιχνηλάτησης της βάσης δεδομένων, ο επιτιθέμενος είναι σε θέση να εισάγει δεδομένα, χωρίς να είναι εξουσιοδοτημένος για αυτή την ενέργεια.

Αποθηκευμένες διαδικασίες

Στις επιθέσεις αυτής της κατηγορίας, ο επιτιθέμενος προσπαθεί να εκτελέσει αποθηκεμένες διαδικασίες που βρίσκονται εγκατεστημένες στη βάση δεδομένων. Σήμερα, τα περισσότερα συστήματα διαχείρισης βάσεων δεδομένων περιέχουν ένα τυποποιημένο σύνολο αποθηκεμένων διαδικασιών που επεκτείνουν τη λειτουργία της βάσης δεδομένων και επιτρέπουν την αλληλεπίδραση με το λειτουργικό σύστημα. Επομένως, μόλις ο επιτιθέμενος προσδιορίσει ποιο DBMS χρησιμοποιείται, μια επίθεση δηλητηρίασης SQL κώδικα μπορεί να κατασκευαστεί με

σκοπό την εκτέλεση κάποιων αποθηκευμένων διαδικασιών που παρέχονται από το συγκεκριμένο σύστημα.
Η εκμετάλλευση αποθηκευμένων διαδικασιών επιτρέπει στους επιτιθεμένους να εκτελέσουν αυθαίρετο κώδικα στον διακομιστή ή να αυξήσουν τα προνόμιά τους . Επιπλέον, λόγω του ότι οι αποθηκευμένες διαδικασίες γράφονται συχνά σε ειδικές γλώσσες σεναρίων (scripting languages), μπορούν να περιέχουν άλλους τύπους ευπαθειών, όπως υπερχείλιση μνήμης (buffer overflow).
Για να πετύχουν πολλά από τα ακόλουθα παραδείγματα, θα πρέπει ο διακομιστής ιστού να συνδέεται με τη βάση δεδομένων με το λογαριασμό ενός διαχειριστή συστήματος. Παρόλο που κάτι τέτοιο μπορεί να προκαλέσει μεγάλο ρήγμα στην ασφάλεια του συστήματος, πολλοί προγραμματιστές εφαρμογών ιστού συνηθίζουν να χρησιμοποιούν Ταξινόμηση επιθέσεων δηλητηρίασης SQL κώδικα 37 αυτό τον τρόπο. Στην τρέχουσα ενότητα γίνεται αυτή η υπόθεση, για να διευκολυνθεί η παρουσίαση του συγκεκριμένου τύπου επίθεσης.
Ένα πιθανό σενάριο θα ήταν να δημιουργηθεί ένας νέος λογαριασμός χρήστη για τη βάση δεδομένων. Αυτό θα επέτρεπε στον επιτιθέμενο να συνδεθεί απευθείας στη βάση δεδομένων και θα ήταν χρήσιμο για την εκτέλεση κάποιων τύπων εντολών.
Με κατάλληλα προνόμια, ο επιτιθέμενος μπορεί να δημιουργήσει το δικό του λογαριασμό στη βάση δεδομένων.

Εξαγωγή συμπεράσματος

Οι επιτιθέμενοι τυπικά ελέγχουν για ευπάθειες στέλνοντας στην εφαρμογή εισόδους που δημιουργούν ένα εσφαλμένο ερώτημα, με αποτέλεσμα ο διακομιστής να επιστρέψει μηνύματα λάθους. Τα μηνύματα αυτά, όπως έχει ειπωθεί, βοηθούνε τον επιτιθέμενο να συλλέξει αρκετές πληροφορίες. Ένας τρόπος προστασίας είναι να παρεμποδιστεί η εμφάνιση μηνυμάτων σφάλματος του διακομιστή βάσεων δεδομένων. Δυστυχώς, αυτός ο τρόπος εκτιμάται ότι δεν είναι αρκετός, καθώς ο επιτιθέμενος μπορεί να εξάγει συμπεράσματα χωρίς την εμφάνιση μηνυμάτων σφάλματος.
Σε αυτόν τον τύπο έγχυσης, οι επιτιθέμενοι προσπαθούν γενικά να επιτεθούν σε μια σελίδα που έχει υψηλή ασφάλεια, η οποία δεν παρέχει καμία ανατροφοδότηση μέσω μηνυμάτων λάθους. Εφόσον από τη βάση δεδομένων δεν επιστρέφονται μηνύματα λάθους για να αποκαλύψουν πληροφορίες στον επιτιθέμενο, ο τελευταίος πρέπει να χρησιμοποιήσει μια διαφορετική μέθοδο για να αποκομίσει απαντήσεις από τη βάση δεδομένων. Ο επιτιθέμενος εγχέει εντολές στη σελίδα και έπειτα παρατηρεί τον τρόπο που αλλάζει η λειτουργία/απόκριση της εφαρμογής. Με προσεκτική παρατήρηση όταν η σελίδα συμπεριφέρεται το ίδιο και όταν η συμπεριφορά της αλλάζει, ο επιτιθέμενος μπορεί να συναγάγει όχι μόνο εάν ορισμένες παράμετροι είναι τρωτές, αλλά και πρόσθετες πληροφορίες για τις τιμές στη βάση δεδομένων. Υπάρχουν δύο γνωστές τεχνικές επίθεσης που βασίζονται στην εξαγωγή συμπεράσματος, η τυφλή έγχυση (Blind Injection) και οι επιθέσεις χρονισμού (Timing Attacks).

Τυφλή έγχυση

Στη μέθοδο της τυφλής έγχυσης, οι πληροφορίες πρέπει να προκύψουν από τη συμπεριφορά της σελίδας, θέτοντας αληθή ή ψευδή ερωτήματα προς την εφαρμογή . Εάν η εγχεόμενη δήλωση αποτιμηθεί ως αληθής, η σελίδα συνεχίζει να λειτουργεί κανονικά. Εάν η δήλωση αποτιμηθεί ψευδής, αν και δεν υπάρχει κανένα μήνυμα σφάλματος, η σελίδα διαφέρει σημαντικά από την κανονική λειτουργία της, αποδεικνύοντας ότι η επίθεση πέτυχε.

Επιθέσεις χρονισμού

Μια επίθεση χρονισμού επιτρέπει σε έναν επιτιθέμενο να λάβει πληροφορίες από μια βάση δεδομένων παρατηρώντας χρονικές καθυστερήσεις στην απόκριση της βάσης δεδομένων . Αυτή η επίθεση είναι παρόμοια με την τυφλή έγχυση, αλλά χρησιμοποιεί μια διαφορετική μέθοδο εξαγωγής συμπεράσματος. Για να εκτελέσει μια επίθεση χρονισμού, ο επιτιθέμενος χρησιμοποιεί ένα κατασκεύασμα SQL που απαιτεί ένα γνωστό χρονικό διάστημα για να εκτελεστεί, (π.χ. ο όρος WAITFOR προκαλεί τη βάση δεδομένων να καθυστερήσει την απάντησή της για έναν καθορισμένο χρόνο). Μετρώντας την αύξηση ή τη μείωση στο χρόνο απόκρισης της βάσης δεδομένων, ο επιτιθέμενος μπορεί να συμπεράνει ποια είναι η απάντηση στο εγχεόμενο ερώτημα.

5.9 Περιπτώσεις ηλεκτρονικών επιθέσεων

Ποιος: Citibank
Πότε: 1994
Περιστατικό: Ο Ρώσος χάκερ Βλαντιμίρ Λέβιν απέσπασε πόσο από λογαριασμούς της Citibank που υπολογίστηκε ότι ανερχόταν στα 10 εκατομμύρια δολάρια. Απέκτησε πρόσβαση στα δίκτυα της τράπεζας από την Αγία Πετρούπολη στη Ρωσία. Όταν συνελήφθη από την Σκότλαντ Γιαρντ και το FBI, παραδέχτηκε ότι χρησιμοποίησε κλεμμένους κωδικούς και passwords από πελάτες της τράπεζας και μετέφερε ποσά στο λογαριασμό του. Το 1998, ένα δικαστήριο στις Η.Π.Α. τον καταδίκασε σε 3 χρόνια κάθειρξη. Η τράπεζα ανέκτησε όλο το ποσό εκτός από 400.000 δολάρια.

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

Πότε: Ιούλιος 2000
Περιστατικό: Ένα ελάττωμα στο λογισμικό του συστήματος της τράπεζας επέτρεπε στους πελάτες της να βλέπουν τις λεπτομέρειες των λογαριασμών των υπόλοιπων πελατών. Η τράπεζα έκλεισε το σύστημα μόλις ανακάλυψε το πρόβλημα.

Ποιος: ABN AMRO
Μια ολλανδική πολυεθνική τράπεζα.
Πότε: Σεπτέμβριος 2000
Περιστατικό: Ένα ολλανδικό τηλεοπτικό πρόγραμμα αποκάλυψε πως χάκερς, έκλεβαν σημαντικές πληροφορίες των πελατών της τράπεζας. Οι χάκερς έστελναν στους πελάτες της τράπεζας μηνύματα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι προέρχονταν από την τράπεζα. Τα mails αυτά εγκαθιστούσαν στους υπολογιστές των πελατών προγράμματα τα οποία επέτρεπαν στους χάκερς να έχουν πρόσβαση σε κρίσιμες πληροφορίες των λογαριασμών τους και με αυτόν τον τρόπο να μεταφέρουν χρήματα από αυτούς. Η τράπεζα διένειμε καινούριες εκδόσεις του λογισμικού της.

Ποιος: E*Trade
Πότε: Σεπτέμβριος 2000
Περιστατικό: Η εταιρεία παραδέχτηκε πως ο δικτυακός της τόπος είχε ένα τρωτό σημείο από όπου κάποιος χάκερ θα μπορούσε να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα. Ο προγραμματιστής που το ανακάλυψε δήλωσε πως ένας χάκερ εκμεταλλευόμενος το πρόβλημα αυτό, θα μπορούσε να αποκτήσει τον κωδικό και το username κάθε χρήστη.

Ποιος: Contour Software
Μια εταιρεία με βάση στην Καλιφόρνια που αναπτύσσει λογισμικό επεξεργασίας υποθηκών που χρησιμοποιείται από πολλές επιχειρήσεις.
Πότε: Νοέμβριος 2000
Περιστατικό: Ένα πρόβλημα στο λογισμικό αποκάλυψε πληροφορίες για τη δανειοληπτική κατάσταση 700 περίπου αμερικανών στο διαδίκτυο. Αντιπρόσωπος της εταιρείας χαρακτήρισε το συμβάν σπάνιο και κατηγόρησε ένα πρώην εργαζόμενο της εταιρείας, ότι απενεργοποίησε τις ρυθμίσεις ασφαλείας.

Ποιος: Charles Schwab
Η μεγαλύτερη online χρηματιστηριακή εταιρεία στις Η.Π.Α.
Πότε: Δεκέμβριος 2000
Περιστατικό: Ο δικτυακός τόπος της εταιρείας έδινε τη δυνατότητα σε χάκερς να έχουν πρόσβαση σε όλους τους λογαριασμούς των πελατών της. Μάλιστα, όσο ο πελάτης ήταν συνδεδεμένος στο σύστημα, ο χάκερ μπορούσε να αγοράσει και να πουλήσει μετοχές από το λογαριασμό του.

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

5.10 ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ

Εκατομμύρια χρήστες έχουν αποκτήσει πλέον τα πλεονεκτήματα χρήσης του e-banking και ευκολίας διαχείρισης των οικονομικών τους οποιαδήποτε στιγμή, από οποιοδήποτε χώρο. Ο χρήστης χρειάζεται να λαμβάνει ορισμένες προφυλάξεις πριν εισέλθει σε on line τραπεζικές υπηρεσίες. Οι βασικοί κανόνες για την ασφάλεια και την πρόληψη δυσάρεστων ακολουθούν παρακάτω:

Προληπτικές Ενέργειες Χρήστη

-Δεν ανοίγουμε ποτέ e-mails με συνημμένα που δεν αναμέναμε.

-Δεν κάνουμε κλικ σε links που υπάρχουν μέσα σε e-mails, εκτός και είναι από πηγή που εμπιστευόμαστε.
-Κάνουμε downloading λογισμικού μόνο από αναγνωρισμένα sites.
-Δεν δίνουμε ποτέ προσωπικές πληροφορίες (username, password, αριθμό πιστωτικής κάρτας, αριθμό τραπεζικού λογαριασμού, κ.α) on line, εκτός αν το site είναι ασφαλές και πιστοποιημένο.
-Ελέγχουμε την πιστοποίηση του κάθε ασφαλούς site κάνοντας κλικ στο εικονίδιο της κλείδας που εμφανίζεται στην γραμμή κατάστασης του browser.
-Αλλάζουμε συχνά τους κωδικούς πρόσβασης σε on line υπηρεσίες.
-Προληπτικές Ενέργειες για τον υπολογιστή
-Περιορίζουμε τον αριθμό των ατόμων που μπορούν να χρησιμοποιήσουν τον υπολογιστή μας και εγκαθιστούμε κωδικό πρόσβασης σε αυτόν εφόσον υπάρχει αυτή η δυνατότητα.
-Εγκαθιστούμε λογισμικό προσωπικού firewall και λογισμικό αντιβιοτικού.
-Κατεβάζουμε συχνά αναβαθμίσεις του αντιβιοτικού λογισμικού του λειτουργικού συστήματος και του προγράμματος πλοήγησης (browser).
-Προληπτικές Ενέργειες για το internet
-Πάντα αποσυνδεόμαστε από τον internet, όταν δεν το χρησιμοποιούμε.
-Δεν διενεργούμε on line συναλλαγές σε sites, αν αυτά σεν είναι ασφαλή και πιστοποιημένα.
-Προληπτικές Ενέργειες για το internet Banking
-Διαλέγουμε κωδικούς πρόσβασης που είναι εύκολο να τους θυμόμαστε, αλλά δύσκολο να τους μαντέψει κάποιος. Δεν χρησιμοποιούμε την ημερομηνία γέννησης, ονόματα της οικογένειας μας, τηλεφωνικούς αριθμούς και κοινά ονόματα.
-Δεν γνωστοποιούμε τους κωδικούς internet banking σε κανέναν (περιλαμβανομένων και του προσωπικού της Τράπεζας και της αστυνομίας).
-Δεν καταγράφουμε πουθενά τους κωδικούς e-banking (χαρτί, αποθηκευτικό μέσο).
-Δεν χρησιμοποιούμε τους ίδιους κωδικούς με αυτούς του e-banking, σε άλλες on line υπηρεσίες (π.χ email, κ.α)
-Δεν χρησιμοποιούμε ποτέ links από e-mail ή μηχανές αναζήτησης για να αποκτήσουμε πρόσβαση σε e-banking υπηρεσίες. Πάντα πληκτρολογούμε τη διεύθυνση στον browser μας.
-Κλείνουμε όλα τα υπόλοιπα παράθυρα του browser, προτού μπούμε σε e-banking, ώστε να προστατεύσουμε τις οικονομικές μας πληροφορίες από μη εγκεκριμένη πρόσβαση από άλλο site.
-Απενεργοποιούμε τη λειτουργία αυτόματης συμπλήρωσης (Auto Complete) του browser μας.
-Πάντα αποσυνδεόμαστε μόλις τερματίσουμε τις εργασίες μας στο e-banking.
-Ποτέ δεν μπαίνουμε στο internet banking από δημόσιους υπολογιστές (π.χ Internet cafes)
-Ελέγχουμε τακτικά τακτικά το υπόλοιπο των λογαριασμών μας και τις κινήσεις μας. Μπορούμε να το κάνουμε 24ωρες το 24ωρο μέσω e-banking. Αν αντιληφθούμε λάθη ή κινήσεις που δεν έχουμε κάνει, ειδοποιούμε αμέσως την Τράπεζα.
-Παρακολουθούμε τακτικά και ακολουθούμε τις συμβουλές ασφαλείας που εκδίδει η Τράπεζα.
-Προληπτικές Ενέργειες για το Phishing

Ο αριθμός των απατών μέσω phising συνεχίζει να αυξάνεται δραστικά. Προκειμένου να αποφεύγονται επιθέσεις τέτοιου τύπου, παρατίθεται μία λίστα με συστάσεις που πρέπει να λαμβάνονται υπόψη:
-Είμαστε υποψιασμένοι με οποιοδήποτε e-mail έχει επείγουσες αιτήσεις για προσωπικές οικονομικές πληροφορίες
-Αν το μήνυμα δεν έχει υπογραφή, δεν μπορούμε να είμαστε σίγουροι ότι δεν έχει παραβιαστεί.
-Οι επιτιθέμενοι συνήθως περιλαμβάνουν ωραίες (αλλά εσφαλμένες) προτάσεις στα e-mail τους, ώστε να αναγκάζουν το λήπτη να αντιδράσει άμεσα

-Ζητούν συνήθως πληροφορίες όπως usernames, passwords, αριθμούς πιστωτικών καρτών, κ.α.
-Τα e-mail των επιτιθέμενων δεν είναι συνήθως προσωποποιημένα, ενώ μηνύματα από Τράπεζες συνήθως είναι.
-Δεν χρησιμοποιούμε links που υπάρχουν σε e-mails, αν υποπτευόμαστε ότι το e-mail δεν είναι αυθεντικό.
-Σε μία τέτοια περίπτωση καλούμε την εταιρία, ή πληκτρολογούμε με τη διεύθυνση του link στο browser μας.
-Αποφεύγουμε να συμπληρώνουμε φόρμες σε e-mail που ζητάνε προσωπικές πληροφορίες
-Επικοινωνούμε τέτοιες πληροφορίες, όπως αριθμούς πιστωτικών καρτών, ή αριθμούς τραπεζικών λογαριασμών μόνο μέσω ενός ασφαλούς site ή τηλεφώνου.
-Πάντα διασφαλίζουμε ότι είμαστε σε ασφαλές site όταν δίνουμε προσωπική πληροφορία μέσω του browser
-Ελέγχουμε τη διεύθυνση του site αν ξεκινά από https:// και όχι από http://
-Ελέγχουμε αν υπάρχει εικονίδιο κλειδαριάς στη γραμμή κατάστασης του browser.
-Αναφέρουμε την επίθεση phishing με e-mails
-Στέλνουμε το e-mail στην εταιρία, από την οποία υποτίθεται ότι έχει έρθει.
-Στο e-mail που στέλνουμε συμπεριλαμβάνουμε όλο το πρωτότυπο e-mail με την πρωτότυπη πληροφορία του header του.
-Προληπτικές Ενέργειες για το Key Logging

Δυστυχώς οι key loggers είναι δύσκολο να ανιχνευθούν από τα windows. Σε περιπτώσεις που πιστεύετε ότι υπάρχει κίνδυνος να παρακολουθούνται οι πληκτρολογήσεις σας, υπάρχει ειδικό λογισμικό (anti-key loggers), που χρησιμοποιείται για τον εντοπισμό τους. Ωστόσο, η καλύτερη αντιμετώπιση του key logging είναι η λήψη προληπτικών μέτρων, όπως τα εξής:
-Έλεγχος όταν το θεωρείτε αναγκαίο του βύσματος (port) του υπολογιστή, ώστε να διαπιστώσετε αν έχει προσαρτηθεί key logger υλικό. Το υλικό αυτό συνήθως είναι καλώδιο που παρεμβάλλεται ανάμεσα στο βύσμα του πληκτρολογίου και του υπολογιστή.
-Σε περιπτώσεις πολλών χρηστών (groups), θα πρέπει να εφαρμόζεται αυστηρή πολιτική σχετικά με την προστασία των κωδικών.
-Στις ομάδες χρηστών δικαίωμα εγκατάστασης λογισμικού θα πρέπει να έχει μόνο μια μικρή ομάδα εξειδικευμένων διαχειριστών. Οι διαχειριστές (administrators) δεν θα πρέπει να εισέρχονται σε υπολογιστή με κωδικούς διαχειριστή και να συνδέονται με τον υπολογιστή αυτό στο internet , διότι είναι πιθανό να εγκατασταθεί key logging λογισμικό στον υπολογιστή από τρίτους.
Μπορείτε να προμηθευτείτε anti-key logger εφαρμογές από εταιρείες που ασχολούνται με την προστασία δεδομένων κατά την πλοήγηση στο internet.

Κεφάλαιο 6 : Στρατηγικές επιλογές των τραπεζών σε θέματα e-banking

6.1 Έννοια της στρατηγικής

Με τον όρο στρατηγική εννοούμε την κύρια κατεύθυνση την οποία πρέπει να ακολουθήσει μια επιχείρηση, βάσει ενός προκαθορισμένου σχεδίου, που ενοποιεί τους στρατηγικούς της στόχους, τους προϋπολογισμούς και τις πολιτικές της σε μια συνεκτική ολότητα. Με άλλα λόγια, περιλαμβάνει τους πόρους που πρέπει να δεσμευτούν και τα μέσα που πρέπει να χρησιμοποιηθούν ώστε να επιτευχθούν οι στρατηγικοί σκοποί που θέτει η επιχείρηση.

6.2 Διαμόρφωση τραπεζικής στρατηγικής

Για να διαμορφώσει τη στρατηγική της η τράπεζα πρέπει προηγουμένως να λάβει υπόψη τις ευκαιρίες και τις απειλές από το συνεχώς μεταβαλλόμενο περιβάλλον, τη θέση των ανταγωνιστών της και τα ισχυρά και αδύνατα σημεία που διαθέτει. Η τράπεζα που αποφασίζει να επενδύσει στην ηλεκτρονική τραπεζική οφείλει να εντάξει αυτή της την απόφαση στους στρατηγικούς της στόχους, οι οποίοι πρέπει να είναι συγκεκριμένοι, μετρήσιμοι και κυρίως επιτεύξιμοι. Αδιαμφισβήτητα το e-banking, όπως άλλωστε και κάθε εξέλιξη της τεχνολογίας που μπορεί να βρει εφαρμογή στον τραπεζικό τομέα, αποτελεί επιχειρηματική ευκαιρία. Για να αποβεί όμως θετική για την επίτευξη του στόχου και της αποστολής της τράπεζας πρέπει να απαντηθούν ερωτήματα όπως:

α) Μπορεί να εξασφαλιστεί ο απαραίτητος μηχανικός εξοπλισμός έγκαιρα και με λογικό κόστος;

β) Μπορούν να εκπαιδευτούν οι υπάλληλοι ή να προσληφθούν νέοι με λογικό κόστος;

γ) Υπάρχουν τα αναγκαία κεφάλαια που θα χρηματοδοτήσουν την επένδυση;

Εφόσον απαντηθούν τα ερωτήματα αυτά και ολοκληρωθεί η μελέτη σκοπιμότητας, η τράπεζα είναι έτοιμη να αναπτύξει τη στρατηγική εκμετάλλευση της ευκαιρίας αυτής.

6.3 Τύποι επιχειρηματικών στρατηγικών αναφορικά με το e-banking

Τα νέα δεδομένα που δημιούργησε το Διαδίκτυο επηρεάζουν τα χρηματοπιστωτικά ιδρύματα κατά τρόπο διαφορετικό. Έτσι ανάλογα με το μέγεθος και τη θέση της κάθε τράπεζας στην αγορά, υιοθετούνται διαφορετικές προσεγγίσεις και στρατηγικές όσον αφορά το e-banking. Πιο συγκεκριμένα, η πλειοψηφία των επιχειρήσεων που προσφέρουν υπηρεσίες ηλεκτρονικής τραπεζικής εφαρμόζουν μια από τις ακόλουθες στρατηγικές:

Α) Ενσωμάτωση του e-banking στο υπάρχον σύστημα διανομής προϊόντων και υπηρεσιών (Integrated Approach). Αυτός ο τύπος στρατηγικής χαρακτηρίζεται ως αμυντική στρατηγική αφού δε στοχεύει στην ανάπτυξη αλλά στη διατήρηση του μεριδίου αγοράς. Ακολουθείται κυρίως από μεγάλες τράπεζες με εδραιωμένη πελατειακή βάση. Μειονέκτημά της όμως αποτελεί το αυξημένο κόστος τουλάχιστον βραχυχρόνια από τη διατήρηση ενός συστήματος πολλαπλών καναλιών διανομής, ενώ ως πλεονέκτημα θεωρείται η ευκολία υλοποίησής της. Χαρακτηριστικά παραδείγματα τραπεζών στην ελληνική επικράτεια που ακολούθησαν τη στρατηγική αυτή είναι η Winbank του ομίλου Πειραιώς και η Άλφα τράπεζα.

Β) Δημιουργία ξεχωριστών ανεξάρτητων ηλεκτρονικών τραπεζών (Standalone Internet Bank). Αυτός ο τύπος στρατηγικής χαρακτηρίζεται ως επιθετική στρατηγική αφού στοχεύει στο μερίδιο αγοράς και στην πελατεία των ανταγωνιστών του κλάδου. Προτιμάται κυρίως από παραδοσιακές τράπεζες μικρού και μεσαίου μεγέθους. Αυτές οι ηλεκτρονικές τράπεζες έχουν μικρό λειτουργικό κόστος, αλλά υψηλό κόστος διαφήμισης και μάρκετινγκ, και στόχος τους είναι μέσω της προσφοράς ιδιαίτερα ελκυστικών τιμών σε μια γκάμα προϊόντων να προσελκύσουν πελάτες από τον ανταγωνισμό. Πολλές τράπεζες επιλέγουν αυτή τη στρατηγική με σκοπό να επεκτείνουν τη δράση τους πέρα των εθνικών τους συνόρων λόγω της χαμηλής αρχικής επένδυσης και του μικρούλειτουργικού κόστους. Η πιο γνωστή ηλεκτρονική τράπεζα αυτής της κατηγορίας είναι η Uno-e που είναι joint venture της ισπανικής τράπεζας BBVA (51%) και του τηλεπικοινωνιακού οργανισμού Telefonica (49%).

Γ) Δημιουργία ηλεκτρονικών τραπεζών από εταιρίες εκτός του κλάδου των χρηματοοικονομικών υπηρεσιών (Virtual Bank). Αυτόν τον τύπο στρατηγικής ακολουθούν κυρίως εταιρίες πληροφορικής και ασφαλιστικές που εισέρχονται με τον τρόπο αυτό σε έναν κλάδο ξένο προς τη συνηθισμένη επιχειρηματική τους δραστηριότητα. Η στρατηγική των Virtual Banks είναι η πλέον επιθετική αφού στοχεύει μέσω χαμηλότερων τιμών να προσελκύσει την πελατεία των άλλων τραπεζών. Μειονέκτημα της στρατηγικής αυτής είναι ότι οι Virtual Banks δεν είναι κερδοφόρες τα πρώτα χρόνια της λειτουργίας τους. Οι πιο γνωστές τράπεζες αυτής της κατηγορίας είναι η Egg και η First-e. Η τελευταία συγχωνεύτηκε με την Uno-e.

Δ) Προσφορά προϊόντων και υπηρεσιών online που εμπλουτίζονται από προϊόντα τρίτων (Virtual Financial Supermarket). Η στρατηγική αυτή ακολουθείται συνήθως από μεγάλους χρηματοοικονομικούς ομίλους που παρέχουν online εκτός από τα προϊόντα και τις υπηρεσίες τους και υπηρεσίες τρίτων όπως για παράδειγμα ασφάλειες, leasing, factoring και συμβουλές αγοραπωλησίας ακινήτων. Η Deutsche Bank έχει δημιουργήσει τέτοιο χρηματοοικονομικό πολυκατάστημα σε συνεργασία με τη Lycos, τη MediaRtl και την ισπανική τράπεζα La Caixa. Το χρηματοοικονομικό αυτό πολυκατάστημα ονομάζεται Moneyshelf.com

6.4 Στρατηγική απόφαση κατά την υιοθέτηση του e - banking

Μια απόφαση στρατηγικής σημασίας που καλείται να λάβει η διοίκηση της τράπεζας που σκοπεύει να υιοθετήσει την ηλεκτρονική τραπεζική είναι αν θα παρέχει η ίδια τις υπηρεσίες e-banking (με το να δημιουργήσει, να αγοράσει ή να νοικιάσει το σύστημα) ή αν θα κάνει outsourcing των υπηρεσιών σε έναν Technology Service Provider (TSP). Η επιλογή του να γίνει outsourcing σε έναν παροχέα τεχνολογικών υπηρεσιών (TSP) μπορεί να βοηθήσει την τράπεζα αφού αυξάνεται η ταχύτητα υλοποίησης του συστήματος, μειώνεται το αρχικό κόστος και δεν απαιτείται τεχνική κατάρτιση εκ μέρους του προσωπικού της. Από την άλλη, η συνεργασία με έναν TSP μπορεί να κρύβει κινδύνους και να δημιουργήσει ανεπιθύμητες αλληλεξαρτήσεις μεταξύ της τράπεζας και του outsourcer. Οποιαδήποτε κι αν είναι τελικά η απόφαση της διοίκησης, αυτή θα πρέπει να στηρίζεται σε μια προσεκτική μελέτη σκοπιμότητας και ανάλυση κόστους-οφέλους της προς ανάληψη επένδυσης.

6.5 Επιχειρηματική θεώρηση του e-banking

Το αν μια τράπεζα θα υιοθετήσει ή όχι το e-banking δεν είναι μια απόφαση που μπορεί να βασίζεται σε επιπόλαιες θεωρήσεις ή στην ακολουθία των τεχνολογικών trend της εποχής. Είναι μια απόφαση που καλείται να λάβει κάθε επιχείρηση ξεχωριστά, σύμφωνα με τις δικές τις ανάγκες και δυνατότητες. Η υιοθέτηση των ηλεκτρονικών συναλλαγών μπορεί να υπόσχεται μεγάλα οφέλη, όπως και κάθε νέα τεχνολογία άλλωστε, αλλά και τα επιχειρηματικά ρίσκα είναι μεγάλα. Η επένδυση που απαιτείται είναι τεράστια και τα αποτελέσματα, τουλάχιστον σε βραχυπρόθεσμο ορίζοντα, είναι αναμφίβολα.

6.5.1 Προσδοκώμενα οφέλη για τις επιχειρήσεις που εφαρμόζουν το e-banking

Αποδοτικότητα: Οι τράπεζες οι οποίες αντιμετωπίζουν με επιτυχία τις τεχνολογικές προκλήσεις που παρουσιάζονται, θα έχουν νέες ευκαιρίες να επεκτείνουν τη θέση τους στη αγορά. Η ψηφιοποίηση των συναλλαγών μειώνει το κόστος και αυξάνει την αποτελεσματικότητα, αν και αρχικά χρειάζονται εκτεταμένες επενδύσεις σε πληροφορική τεχνολογία.
Συνέπεια της έντονης χρησιμοποίησης της νέας τεχνολογίας στις τραπεζικές συναλλαγές είναι και η τάση για ¨προτυποποίηση¨ των τραπεζικών προϊόντων, η οποία είναι γνωστή με τον όρο ¨commodisation¨. Αυτό για τις τράπεζες είναι από τη μια θετικό διότι προσθέτει αποτελεσματικότητα και ευκολία στις επιχειρηματικές διαδικασίες αλλά από την άλλη μειώνει την ¨πίστη¨ των πελατών σ'αυτές αφού μειώνεται το switching cost μιας ενδεχόμενης αλλαγής τράπεζας. Είσοδος σε νέα επιχειρηματικά πεδία. Το internet banking συγκεκριμένα θα επιτρέψει τα χρηματοπιστωτικά ιδρύματα να δράσουν και ως ¨αρχές έκδοσης ψηφιακών πιστοποιητικών¨ στις νέας μορφής ηλεκτρονικές αγορές που δημιουργούνται. Πολλές και ευκίνητες τράπεζες σε συνεργασία για παράδειγμα με ISPs, εταιρείες τηλεπικοινωνιών, εταιρείες παραγωγής software αλλά και άλλους φορείς μπορούν να εκμεταλλευτούν την ευκαιρία αυτή. Χαρακτηριστικό παράδειγμα αποτελούν οι 4 μεγαλύτερες τράπεζες της Γερμανίας που αγόρασαν από κοινού το 1999 εταιρεία παροχής υπηρεσιών ασφάλειας στις ηλεκτρονικές συναλλαγές.
Νέοι αλλά και ¨ελκυστικοί¨ πελάτες. Οι τράπεζες μπορούν να αποκτήσουν νέους πελάτες μέσω της παρουσίας τους στο internet. Πολλοί είναι εκείνοι που θα μπουν στον πειρασμό να δοκιμάσουν ένα προϊόν μιας τράπεζας όταν το μόνο που χρειάζεται για κάτι τέτοιο είναι μερικά clicks. Οι περισσότεροι χρήστες του internet είναι άτομα δυναμικά, με υψηλό μορφωτικό και βιοτικό επίπεδο, άτομα δηλαδή που οι τράπεζες θέλουν για πελάτες τους καθώς κατανοούν καλύτερα τις νέες μορφές συναλλαγών αλλά και τα νέα προϊόντα. Από την άλλη έχουν όμως και μεγαλύτερες απαιτήσεις.

6.5.2 Επιχειρηματικά ρίσκα των επιχειρήσεων που εφαρμόζουν το e-banking

Εκτός από τις παραπάνω ευκαιρίες και πλεονεκτήματα που προσφέρει το e-banking στα χρηματοπιστωτικά ιδρύματα, υπάρχουν και ρίσκα που σχετίζονται με αυτό, και ιδιαίτερα με την αυξημένη χρήση της πληροφορικής τεχνολογίας.

Στρατηγικά ρίσκα: Το κυριότερο στρατηγικό ρίσκο στη διαδικασία του e-banking είναι να μην είναι ικανή η επιχείρηση να ακολουθήσει πιστά τις νέες τεχνολογίες

που απαιτείται να υιοθετηθούν. Από τη στιγμή που μια τράπεζα αποφασίσει να υιοθετήσει πρακτικές e-banking, τότε πρέπει συνεχώς να επενδύει σε νέες τεχνολογίες, διότι όπως είναι κατανοητό το e-banking στηρίζεται κυρίως σε αυτές. Όπως είναι φυσικό οι καινοτόμες επιχειρήσεις αναλαμβάνουν μεγαλύτερο ρίσκο από τις υπόλοιπες. Είναι όμως συχνά αδύνατο να προβλεφθεί αν ένα προϊόν θα επιβιώσει στην αγορά ή ένα project θα ολοκληρωθεί με επιτυχία. Τα αποτυχημένα project, ειδικά στον τομέα της τεχνολογίας, είναι αποτυχημένες επενδύσεις και συχνά αντί να μειώσουν το κόστος κάποιον διαδικασιών, έχουν το αντίθετο αποτέλεσμα. Για το λόγο αυτό πολλές τράπεζες ακολουθούν τη λογική της ¨μίμησης¨. Στην περίπτωση αυτή εξοικονομούνται χρήματα αλλά μειώνεται και ο κίνδυνος της αποτυχίας αφού υπάρχουν ήδη σημάδια για το αν η αγορά αποδέχθηκε τους νέους τρόπους συναλλαγής και επικοινωνίας (τους οποίους άλλες τράπεζες, καινοτόμες, πρώτες εφήρμοσαν). Το μειονέκτημα της μεθόδου αυτής είναι ότι μεγάλο ενδεχομένως τμήμα της αγοράς να έχει ήδη καταληφθεί από τους ¨πρωτοπόρους¨. Τέτοιου είδους αποφάσεις, για την υιοθέτηση δηλαδή ή όχι του e-banking από μια τράπεζα, πρέπει να λαμβάνονται όσο το δυνατόν πιο γρήγορα αλλά και έξυπνα διότι τόσο οι τεχνολογίες αλλά και οι προτιμήσεις των καταναλωτών αλλάζουν πολύ γρήγορα, με αποτέλεσμα να υπάρχει συχνά αβεβαιότητα και δισταγμός από τη μεριά των τραπεζών.

Λειτουργικά ρίσκα: Πρόκειται για τα ρίσκα που στοχεύουν στις επιχειρηματικές διαδικασίες. Πηγές τέτοιων ρίσκων είναι τεχνικές δυσλειτουργίες, ανθρώπινα λάθη, λανθασμένες ή ανεπαρκείς επιχειρηματικές δομές. Αν αυτά τα ρίσκα δεν διαχειριστούν αποτελεσματικά τότε θα υπάρχουν οικονομικές συνέπειες αλλά και καθαρά λειτουργικές όπως κατειλημμένο τηλεφωνικό κέντρο, ¨κατάρρευση¨ του server. Τέτοιου είδους κίνδυνοι δεν είναι νέοι, αλλά με την εκτεταμένη χρήση της τεχνολογίας, έγιναν περισσότερο καταφανείς. Στον τομέα αυτό ανήκει και η ασφάλεια των συστημάτων, ίσως το πιο σημαντικό λειτουργικό θέμα όσον αφορά το e-banking. Χωρίς να θέλουμε να αναλύσουμε διεξοδικά το θέμα της ασφάλειας των συναλλαγών μπορούμε να αναφέρουμε μερικές από τις πιο συχνές δυσλειτουργίες ενός συστήματος e-banking, οι οποίες μπορεί να συμβούν είτε τυχαία είτε μετά από οργανωμένη επίθεση στο σύστημα:

>Υπερφόρτωση συστήματος, με συνέπεια την αδυναμία λειτουργίας του.
>Μεταβολή στατικού ή άλλου περιεχομένου.
>Κατάρρευση των e-mail servers μετά από υπερφόρτωση.
>Παρεμβολές στην επικοινωνία.

Κατά τον στρατηγικό σχεδιασμό πρέπει να γίνεται από την τράπεζα ανάλυση των κινδύνων που πιθανόν θα αντιμετωπίσει το σύστημα. Τα σημαντικότερα ερωτήματα που πρέπει να απαντηθούν κατά την ανάλυση του κινδύνου είναι τα εξής:

- Ποιοι πόροι πρέπει να προστατευθούν και από ποιόν.
- Ποιο είναι το κόστος μιας πιθανής παραβίασης.
- Ποιο είναι το κόστος ασφάλειας.
- Ποια είναι η πιθανότητα παραβίασης.

Γνωρίζοντας κατά το δυνατό τις απαντήσεις στα παραπάνω ερωτήματα μπορούμε να υπολογίσουμε τον λόγο επιχειρηματικού κόστους παραβίασης προς το κόστος ασφάλειας, ώστε να ληφθούν οι σωστές και πιο επικερδής αποφάσεις όσον αφορά την ασφάλεια. Μια άλλη σημαντική απόφαση η οποία πρέπει να ληφθεί αφορά το λεγόμενο outsourcing της

πληροφορικής τεχνολογίας, την ανάθεση δηλαδή της παροχής και υποστήριξης της απαραίτητης τεχνολογίας σε εξειδικευμένο προσωπικό εκτός τράπεζας. Κάτι τέτοιο ωφελεί κυρίως μικρές κατά κανόνα επιχειρήσεις οι οποίες μπορούν με αυτόν τον τρόπο να προσφέρουν υπηρεσίες e-banking χωρίς να χρειαστούν μεγάλες επενδύσεις σε πληροφορική τεχνολογία. Από την άλλη πλευρά είναι κατανοητό πως η άμεση εξάρτηση της τράπεζας από πρόσωπα εκτός αυτής (όπως οι software providers) αυξάνει κατακόρυφα τα λειτουργικά ρίσκα. Οι εξωτερικού συνεργάτες, εκτός από άριστα καταρτισμένοι πάνω σε τεχνικά θέματα, πρέπει να είναι πλήρως ενημερωμένοι για τις πολύπλοκες διαδικασίες που ακολουθεί μια τράπεζα αλλά και το τεράστιο κόστος που μπορεί να έχει μια ενδεχόμενη αστοχία του συστήματος.

Νομικά ρίσκα : Τα ρίσκα αυτά προέρχονται από το γεγονός ότι το νομικό πλαίσιο το οποίο διέπει τις ηλεκτρονικές συναλλαγές είναι ακόμη ρευστό στις περισσότερες χώρες. Ακόμη, συχνά διαφέρει σημαντικά από χώρα σε χώρα γεγονός που δυσκολεύει τις συναλλαγές ενός καταναλωτή με μια τράπεζα του εξωτερικού. Αβεβαιότητα επίσης υπάρχει ως προς το ποιος φορέας έχει τη δικαιοδοσία στις διακρατικές συναλλαγές. Η τράπεζα συχνά διατρέχει τον κίνδυνο να παραβιάσει εν αγνοία της νόμους μιας ξένης χώρας. Τέλος, η πιθανότητα να χρησιμοποιηθεί το e-banking ως μέσο νομιμοποίησης παράνομων κεφαλαίων, καθιστά τις τράπεζες υπεύθυνες ώστε να γνωρίζουν με ακρίβεια αυτόν που συναλλάσσεται μαζί τους, γεγονός που επίσης κρύβει πολλά ρίσκα.

Ρίσκα που αφορούν τη φήμη της τράπεζας . Ο τραπεζικός τομέας είναι ιδιαίτερα ευαίσθητος και στηρίζεται στο καλό όνομα που αποκτά η τράπεζα στην αγορά αλλά και στη σχέση εμπιστοσύνης που αποκτά με τους πελάτες της. Πρέπει λοιπόν από τη στιγμή που υιοθετήσει το e-banking να είναι έτοιμη να ανταποκριθεί απόλυτα στις απαιτήσεις των πελατών της με ταχύτητα και συνέπεια. Οι πελάτες που ούτος ή άλλως είναι επιφυλακτικοί στα νέα κανάλια επικοινωνίας μπορεί να επηρεαστούν πολύ αρνητικά στη πρώτη δυσλειτουργία του συστήματος με αποτέλεσμα να κλονιστεί η εμπιστοσύνη τους στην τράπεζα. Η τράπεζα το σημαντικότερο ίσως ρίσκο που αναλαμβάνει είναι να διατηρήσει το ίδιο επίπεδο εξυπηρέτησης των πελατών και μέσα από τα νέα κανάλια προσφέροντας υψηλής ποιότητας υπηρεσίες και ασφαλής συναλλαγές αλλιώς ο κίνδυνος δυσφήμησης της είναι μεγάλος

6.6 Στρατηγικές που ακολουθούν οι τράπεζες στην Κύπρο για προστασία των πελατών τους

Τέσσερις κυπριακές τράπεζες προσφέρουν e-banking στους πελάτες τους σήμερα, με μια τεράστια γκάμα υπηρεσιών, φθηνότερες τιμολογήσεις και ταχύτητα εξυπηρέτησης. Οι εκστρατείες προώθησης της ηλεκτρονικής τραπεζικής μέσω διαφημίσεων και διαφόρων εκστρατειών και τα μεγάλα κονδύλια που επενδύονται σε αυτήν κάθε χρόνο, δείχνουν την έμφαση που δίνουν οι οργανισμοί αυτοί στην προώθησή της. Οι συνεχείς αναβαθμίσεις των ηλεκτρονικών υπηρεσιών τους, της ασφάλειας των συναλλαγών και των προσωπικών δεδομένων, γίνονται με σκοπό την αύξηση της εμπιστοσύνης των χρηστών και την αύξηση της χρήσης των υπηρεσιών αυτών. Είναι όμως ασφαλή τα προσωπικά δεδομένα και τα χρήματα των

πελατών-χρηστών; Παραθέτουμε ενδεικτικά τις κοινές στρατηγικές που εφαρμόζουν οι τράπεζες στην Κύπρο για ασφάλεια των συναλλαγών των πελατών τους στην ηλεκτρονική τραπεζική.

Για την είσοδο στις ιστοσελίδες που παρέχουν τραπεζικές υπηρεσίες, οι τράπεζες εκδίδουν δύο κωδικούς για τον κάθε χρήστη. Ο πελάτης-χρήστης έχει τον δικό του, μοναδικό κωδικό συνδρομητή που κυμαίνεται από 6 μέχρι και 15 ψηφία, ανάλογα με το σύστημα της κάθε τράπεζας, ως επίσης και τον δικό του μυστικό κωδικό (Pin) που κυμαίνεται από 4 έως 6 ψηφία. Οι δύο αυτοί κωδικοί παρέχουν πρόσβαση στους λογαριασμούς του πελάτη-χρήστη.

Οι τράπεζες, για μεγαλύτερη ασφάλεια των πελατών τους, εκτός από τους κωδικούς πρόσβασης, παρέχουν και μια καινούρια υπηρεσία, τον εφοδιασμό των πελατών-χρηστών τους με συσκευές παροχής πρόσθετου κωδικού ασφαλείας μιας χρήσης για πρόσβαση στην ηλεκτρονική τραπεζική, αλλά και για την εκτέλεση συγκεκριμένων συναλλαγών όπως μεταφορές σε τρίτους, πληρωμές λογαριασμών, εμβάσματα σε άλλες τράπεζες κ.α. Η συσκευή πρόσθετου κωδικού ασφαλείας χρησιμοποιεί ένα κρυπτογραφημένο αλγόριθμο και παράγει ένα αριθμό μιας χρήσης με τον οποίο πιστοποιείται ότι η συναλλαγή προέρχεται από τον κάτοχο της συσκευής. Η συσκευή αυτή στοιχίζει για τον χρήστη από 7 μέχρι και 10 ευρώ.

Οι τράπεζες παρέχουν πλούσιο ενημερωτικό υλικό στα καταστήματα και τις ιστοσελίδες τους, ως επίσης και μέσω ηλεκτρονικών μηνυμάτων στους λογαριασμούς των πελατών τους, ώστε η χρήση της ηλεκτρονικής τραπεζικής να είναι ασφαλής.

Κάποιες από τις συχνότερες επισημάνσεις τους είναι η αλλαγή του μυστικού κωδικού ανά τακτά χρονικά διαστήματα, η χρήση μη προβλέψιμων κωδικών, η ασφαλής φύλαξή τους ή απενεργοποίηση της λειτουργίας απομνημόνευσης κωδικών από το πρόγραμμα πλοήγησης του υπολογιστή που θα χρησιμοποιήσουν και η μη αποκάλυψη του μυστικού κωδικού σε κανένα. Δίνουν επίσης έμφαση στις πρόσφατες μεθόδους υποκλοπής κωδικών πρόσβασης μέσω μηνυμάτων ή μέσω τηλεφωνικής επικοινωνίας, από επιτήδειους που παριστάνουν υπαλλήλους της τράπεζας. Επισημαίνουν τις σύγχρονες μεθόδους προστασίας των υπολογιστών των χρηστών με προστατευτικά από ιούς προγράμματα (antivirus) και χρήση τοίχου προστασίας (firewall), την αποφυγή χρήσης υπολογιστών δημόσιας χρήσης ή του ανοίγματος μηνυμάτων τύπου SPAM ή επισυνημμένα αρχεία από άγνωστες πηγές. Κυριότερη προτροπή των τραπεζών είναι η ηλεκτρονική πρόσβαση στις τράπεζες να λαμβάνει χώρα μόνο μέσω της επίσημης ιστοσελίδας τους. Κυρίως προτρέπουν τους πελάτες να προβαίνουν σε συνετή χρήση των υπηρεσιών αυτών και γενικότερα του διαδικτύου για την δική τους ασφάλεια.

Οι τράπεζες, γνωρίζοντας τις διάφορες μεθόδους που μηχανεύονται οι επιτήδειοι για υποκλοπή κωδικών πρόσβασης των πελατών τους, παρέχουν εύκολη και γρήγορη απενεργοποίηση των κωδικών. Πρόκειται για μια υπηρεσία που προσφέρουν επί εικοσιτετραώρου βάσεως μέσω της

τηλεφωνικής εξυπηρέτησης πελατών και μπορεί ο πελάτης να την χρησιμοποιήσει μόλις αντιληφθεί μη εξουσιοδοτημένη συναλλαγή.

Οι περισσότερες τράπεζες προσφέρουν και υπηρεσία μηνυμάτων στους πελάτες τους. Η υπηρεσία αυτή προσφέρει την δυνατότητα στον πελάτη, με κάθε συναλλαγή που πραγματοποιείται στους λογαριασμούς ή στις κάρτες του, να λαμβάνει ενημερωτικό μήνυμα στο κινητό του. Με τον τρόπο αυτό, με την εκτέλεση οποιασδήποτε συναλλαγής από μη εξουσιοδοτημένο από τον κάτοχο του λογαριασμού άτομο, ο πελάτης ενημερώνεται άμεσα και μπορεί έτσι να δράσει σε σύντομο χρόνο, ενημερώνοντας την τράπεζά του για προστασία των λογαριασμών του και για εντοπισμό της μη εξουσιοδοτημένης συναλλαγής .

Ο πελάτης μπορεί να θέσει ανώτατο όριο συναλλαγών στους λογαριασμούς του, σαν επιπρόσθετο μέτρο προστασίας των χρημάτων του. Η υπηρεσία αυτή δίνει την δυνατότητα στους χρήστες της ηλεκτρονικής τραπεζικής να θέσουν ανώτατο όριο συναλλαγών για κάθε μέρα, ανάλογα με τις δικές τους ανάγκες, ώστε και σε περίπτωση υποκλοπής των κωδικών πρόσβασης να μην είναι δυνατό να αποσυρθούν όλα τα χρήματα.

Οι Τράπεζες προνοούν για τα τελευταίας τεχνολογίας λογισμικά που χρησιμοποιούν με ψηλά επίπεδα κρυπτογράφησης, ως επίσης και την συνεχή παρακολούθησή τους, για την διαφύλαξη των προσωπικών δεδομένων των πελατών τους και για την επίτευξη μέγιστης ασφάλειας για τις τραπεζικές συναλλαγές.

Η χρήση της ηλεκτρονικής τραπεζικής γίνεται επί εικοσιτετραώρου βάσεως , και για αυτό οι τράπεζες προσφέρουν ολοήμερη τηλεφωνική εξυπηρέτηση στους χρήστες για βοήθεια, απορίες, αλλά και καταγγελίες ύποπτων μηνυμάτων. Οι τράπεζες διατηρούν ειδικά τμήματα όπου εξειδικευμένο προσωπικό χειρίζεται τις πληροφορίες που δίνουν οι πελάτες-χρήστες για προσπάθειες υποκλοπής κωδικών μέσω μηνυμάτων στο ηλεκτρονικό ταχυδρομείο και μέσω παράνομων ιστοσελίδων, που εμφανίζονται πανομοιότυπες με αυτές των τραπεζών.

Κάποιες επιπρόσθετες στρατηγικές προστασίας της ηλεκτρονικής τραπεζικής που χρησιμοποιούν μεγάλοι τραπεζικοί οργανισμοί της Ευρώπης και μπορούν να υιοθετηθούν και από τις κυπριακές τράπεζες είναι: Η δωρεάν παροχή προγραμμάτων προστασίας από ιούς μέσω των ιστοσελίδων τους, η δωρεάν παροχή σε όλους τους χρήστες της ηλεκτρονικής τραπεζικής των συσκευών πρόσθετου κωδικού πρόσβασης μιας χρήσης, η τηλεφωνική επικοινωνία με τους πελάτες για επιβεβαίωση συναλλαγών έξω από τις συνηθισμένες κινήσεις του συγκεκριμένου χρήστη και γενικότερα σε περίπτωση που η τράπεζα υποψιαστεί απάτη.

6.7 Συμπεράσματα

Αναμφισβήτητα το e-banking αποτελεί μια δελεαστική επιχειρηματική ευκαιρία
για κάθε τράπεζα. Κύριο μέλημά της διοίκησης πρέπει να είναι η υιοθέτηση της σωστής στρατηγικής για την εκμετάλλευση της εταιρίας αυτής. Ανάλογα με το μέγεθος και τη θέση που έχει στην αγορά κάθε τράπεζα υιοθετεί διαφορετική στρατηγική όσον αφορά το e-banking. Υπάρχουν 4 κυρίαρχες στρατηγικές. Η στρατηγική ενσωμάτωσης του e-banking στο υπάρχον σύστημα διανομής προϊόντων και υπηρεσιών, η στρατηγική της δημιουργίας ανεξάρτητων ηλεκτρονικών τραπεζών από τράπεζες, η στρατηγική της δημιουργίας ανεξάρτητων ηλεκτρονικών τραπεζών από άλλες εταιρίες και η στρατηγική προσφοράς προϊόντων και υπηρεσιών online που εμπλουτίζονται από προϊόντα τρίτων. Τέλος η τράπεζα καλείται να αποφασίσει αν θα δημιουργήσει η ίδια το σύστημα του e-banking ή θα αναθέσει τις υπηρεσίες e-banking σε κάποιον παροχέα τεχνολογικών υπηρεσιών.

ΚΕΦΑΛΑΙΟ 7 : ΕΡΓΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΙΚΗΣ

Τα έργα της ηλεκτρονικής τραπεζικής, είναι πολυσύνθετα. Αυτό οφείλεται στο γεγονός ότι περιλαμβάνουν πολλούς διαφορετικούς τομείς, που πρέπει να συμπλέκονται αρμονικά. Τα έργα υλοποιούνται με σύγχρονα εργαλεία και τεχνολογίες, εξυπηρετούν τις τραπεζικές εργασίες για τις οποίες προορίζονται, είναι σύμφωνα με την κείμενη νομοθεσία και λαμβάνεται υπόψη το βάθος χρόνου ζωής των παραδοτέων.

7.1 Σύγχρονες στρατηγικές τεχνολογίας

Η τεχνολογία αποτελεί το θεμέλιο λίθο των στρατηγικών ηλεκτρονικών οικονομικών υπηρεσιών. Η τεχνολογία των πολυκαναλικών λύσεων πρέπει να είναι σύμφωνη με τα βιομηχανικά standards και να στηρίζεται σε ανοιχτή αρχιτεκτονική.

Οι επενδύσεις που γίνονται στον τεχνολογικό τομέα είναι μικρές. Το γεγονός αυτό δικαιολογείται εν μέρει:

-αρκετές εταιρείες δεν επενδύουν λόγω της σφιχτής οικονομικής πολιτικής που εφαρμόζουν.

-παράλληλα λαμβάνεται σταθερά υπόψη η φοβία του χρήστη απέναντι στο internet και την τεχνολογία γενικότερα.

-παρά τη μεγάλη διεισδύσει της κινητής τηλεφωνίας, τεχνολογίες όπως WAP, GPRS, και i-mode δεν γνωρίζουν την αναμενόμενη επιτυχία.

-οι Διοικήσεις των τραπεζών και τα IT τμήματα αυτών είναι σκεπτικές σε μεγάλες επενδύσεις στον τομέα της τεχνολογίας, ειδικότερα είναι ίσως οι εταιρείες που υιοθετούν νέες τεχνολογίες, αφού θέλουν χειροπιαστά αποτελέσματα επιτυχούς εφαρμογής αυτών σε άλλους τομείς.

Ωστόσο το γεγονός είναι ότι οι αποφάσεις για επένδυση σε νέες τεχνολογίες πρέπει παίρνονται με τη ταχύτητα που κινείται και το internet. Η αρχιτεκτονική αυτή παρά το γεγονός ότι είναι απαράδεκτη, υιοθετείται από αρκετές τράπεζες είτε λόγω του επείγοντος της υλοποίησης των εφαρμογών της, είτε λόγο έλλειψης της απαραίτητης τεχνογνωσίας. Γίνεται εύκολα αντιληπτό ότι προκειμένου να εξυπηρετηθεί μια ίδια συναλλαγή από τρία διαφορετικά κανάλια, αναπτύσσεται κώδικας για τη ξεχωριστή εφαρμογή καναλιού. Παρόλο αυτά το κεντρικό σύστημα εκτελεί με ένα και μοναδικό τρόπο την συναλλαγή.

Η σωστή προσέγγιση έχει τα ακόλουθα χαρακτηριστικά:

- Κεντρική επεξεργασία και συντήρηση των συναλλαγών
- Διαχωρισμός της επιχειρηματικής λογικής με τη λογική της παρουσίασης της
- Υψηλής τεχνολογίας διεπαφές
- «Ελαφρά» μετάδοση συναλλαγής

Ο στόχος είναι μια μοναδική πλατφόρμα να εξυπηρετεί όλα τα κανάλια. Οι αποδεκτές τεχνολογίες για να επιτευχθεί ο στόχος είναι η XML και τα web services. Αμφότερες έχουν καθολική διασυνδεσιμότητα με οποιοδήποτε προγραμματιστικό εργαλείο χρησιμοποιηθεί.

Η XML:
-αποτελεί βιομηχανικό standard για την ενσωμάτωση επιχειρησιακών εφαρμογών
- αποτελεί τεχνολογικό standard για τον μετασχηματισμό σε λογική παρουσίασης.
Τα web services δεν έχουν να κάνουν ούτε με web servers, ούτε με web sites.

Η υλοποίηση τους είναι σημαντική για τους εξής λόγους:

-Αποτελούν τον standard τρόπο για την ανταλλαγή XML μηνυμάτων μέσω δικτύου
-Προσθέτουν αξία στην XML υλοποίηση
-Είναι βασικά συστατικά της επιχειρησιακής λογικής και είναι ανεξάρτητα πρωτοκόλλων και καναλιών
- Εστιάζουν αποκλειστικά στην επίλυση επιχειρηματικών προβλημάτων
- Εξυπηρετούν την πρόσβαση τους με πολλαπλούς τρόπους.

Τα πλεονεκτήματα που αποκομίζει ο τραπεζικός οργανισμός που υιοθετεί XML και web services είναι πολύ σημαντικά και παρατίθενται παρακάτω:

-Το επίπεδο παρουσίασης και περιεχομένου του καναλιού δεν επηρεάζεται από την υλοποίηση των συναλλαγών. Αυτό σημαίνει μικρότερο κόστος υλοποίησης νέων καναλιών και ταχύτερη προώθηση αυτών.
-Επαναχρησιμοποίηση των διεπαφών
-Επεκτασιμότητα και κεντρική συντήρηση της λογικής της συναλλαγής
-Μείωση κόστους ανάπτυξης εφαρμογών γρήγορα
-Μεγιστοποίηση του ROI
-Ελαχιστοποίηση του TOC

7.2 Προδιαγραφές Έργων

Τα έργα της ηλεκτρονικής τραπεζικής χωρίζονται σε τρεις διακριτές κατηγορίες με τους φορείς υλοποίησης:

1.Εσωτερικά έργα μονάδας
2. In house έργα τράπεζας
3. Out- sourced έργα

Η πρώτη κατηγορία αφορά έργα μικρά, τόσο σε χρονικό ορίζοντα όσο και ανθρώπινους πόρους. Στελέχη της μονάδας αναλαμβάνουν την διαχείριση των έργων εξ ολοκλήρου.
Οι άλλες κατηγορίες περιλαμβάνουν πιο «βαριά» έργα. Στα έργα αυτά εμπλέκονται και άλλες μονάδες της Τράπεζας ή εξωτερικοί συνεργάτες. Η χρονική διάρκεια των έργων αυτών είναι σημαντικά μεγαλύτερη σε σχέση με αυτά της πρώτης κατηγορίας και η διαχείριση τους, είναι δυσκολότερη καθώς απαιτεί το συντονισμό και το συγχρονισμό ανθρώπινων πόρων διαφορετικών μονάδων και φορέων.
Προκειμένου να ξεκινήσει ένα έργο, προηγείται μελέτη σκοπιμότητας, στην οποία περιγράφονται ο σκοπός του έργου, ο χρονικός ορίζοντας ολοκλήρωσης του έργου, οι εμπλεκόμενοι φορείς και μονάδες, τα οφέλη από την υλοποίηση του, οι ενδεχόμενες αλλαγές

στην πολιτική της τράπεζας. Η μελέτη σκοπιμότητας παραδίδεται στον επικεφαλή της μονάδας εφόσον το έργο είναι in-house και out-sourced.
Ακολουθεί η σύνταξη λειτουργικών και τεχνικών προδιαγραφών του έργου. Στην περίπτωση in-house έργων, το σύνολο των προδιαγραφών συντάσσεται από την μονάδα Ηλεκτρονικής Τραπεζικής, ενώ σε out-sourced έργα για τη σύνταξη των προδιαγραφών υπάρχει συνεργεία των στελεχών της μονάδας με στελέχη του εξωτερικού συνεργάτη. Πάντα βέβαια τον τελευταίο λόγο σε θέματα business loc in τον έχει η διεύθυνση ηλεκτρονικής τραπεζικής. Οι τεχνικές προδιαγραφές περιέχουν την αναλυτική προδιαγραφή των διεπαφών που θα χρησιμοποιηθούν π.χ το σχηματισμό βάσεων δεδομένων, τις ελάχιστες τεχνικές απαιτήσεις για την λειτουργία του έργου καθώς και τις προβλέψεις σε εξοπλισμό για τον έλεγχο του έργου.
Στα in house έργα το σύνολο των προδιαγραφών αποστέλλεται σε όλες τις εμπλεκόμενες μονάδες, προκειμένου να ενημερωθούν και να γίνουν τυχών διορθώσεις και προσθήκες. Με την εργασία των εμπλεκόμενων σχεδιάζεται το χρονοδιάγραμμα υλοποίησης στο οποίο αναφέρονται οι φάσεις όπως και τα συγκεκριμένα άτομα που αναλαμβάνουν την διεκπεραίωση τους.
Στα out sourced έργα οι προδιαγραφές αποτελούν αναπόσπαστο μέρος του ιδιωτικού συμφωνητικό υπογράφει η τράπεζα με τον εξωτερικό συνεργάτη.

7.3 Υλοποίηση έργων

Οι παράμετροι οποιουδήποτε έργου είναι τρεις: Κόστος, Χρόνος, Ποιότητα.
Οι τρεις παραπάνω παράμετροι πρέπει να είναι ισομερώς καταμερισμένες. Αν κάποια από αυτές τις παραμέτρους ξεφύγει από τον αρχικό προγραμματισμό, αυτό γίνεται εις βάρος κάποιας άλλης. Η υλοποίηση των διάφορων φάσεων του έργου γίνεται με βάση τις προδιαγραφές του έργου και τον χρονοπρογραμματισμό του. Η παρακολούθηση της πορείας των έργων γίνεται με συνδρομή εργαλείων λογισμικού για το σκοπό αυτό, όπως το Microsoft Project, που είναι ένα ευρύτατα διαδεδομένο εργαλείο παρακολούθησης και διαχείρισης έργων.
Το περιβάλλον στο οποίο υλοποιείται μια ηλεκτρονική υπηρεσία είναι συνήθως περιβάλλον development. Στη φάση αυτή ο κατασκευαστής δουλεύει απερίσπαστος, ενημερώνοντας την μονάδα ηλεκτρονικής τραπεζικής.

7.4 Έλεγχος Αποδοχής

Ο έλεγχος αποδοχής είναι σημαντικό κομμάτι στην πορεία του έργου. Όσοι εμπλέκονται στον έλεγχο δεν πρέπει να είχαν εμπλακεί στην υλοποίηση του. Ο κανόνας αυτός είναι βασικός για την επιτυχία των δοκιμών. Ο έλεγχος γίνεται από στελέχη που γνωρίζουν τον σκοπό και τις απαιτήσεις του έργου και ουσιαστικά λειτουργούν ως τελικοί χρήστες της υπηρεσίας.

Κατά την διάρκεια των δοκιμών πρέπει να ελέγχονται όλες οι παράμετροι της εφαρμογής:

-Αισθητικό αποτέλεσμα
-Περιεχόμενο
-Λειτουργικό αποτέλεσμα
-Ορθή λειτουργία δικτύων
-Ορθή λειτουργία τραπεζικών συναλλαγών
-Ορθή ενημέρωση της βάσης δεδομένων

-Ασφάλεια έργου

Για την διευκόλυνση των ελέγχων, απαραίτητο είναι να καταγραφούν σενάρια ελέγχου. Τα σενάρια ελέγχου περιλαμβάνουν ομαλές ροές εργασιών, αλλά και απρόβλεπτες και μη συχνές καταστάσεις.

Τα αποτελέσματα του ελέγχου αποδοχής καταγράφονται σε αναφορά και παραδίδονται στον κατασκευαστή, ώστε να κάνει τις απαραίτητες διορθώσεις. Η τακτική αυτή συνεχίζεται μέχρι να εξαλειφθούν οι παρατηρήσεις, οπότε και ακολουθεί η επίσημη αποδοχή και παραλαβή του έργου από τη μονάδα ηλεκτρονικής τραπεζικής.

7.5 Μετάβαση σε περιβάλλον παραγωγής

Η μετάβαση του παραδοτέου σε περιβάλλον παραγωγής γίνεται αφού προηγηθούν συγκεκριμένες ενέργειες από την πλευρά της Διεύθυνσης Ηλεκτρονικής Τραπεζικής:

-Ενημέρωση όλης της τράπεζας για το νέο προϊόν ή υπηρεσία.
-Εκπαίδευση όλων των εμπλεκόμενων στελεχών
-Καταγραφή εσωτερικών διαδικασιών
-Εξασφάλιση budget για το promotion του νέου προϊόντος
-Σχεδιασμός διαφημιστικής καμπάνιας

Κατόπιν των παραπάνω ενεργειών, η μονάδα Ηλεκτρονικής Τραπεζικής αποφασίζει και ενημερώνει τους λοιπούς εμπλεκόμενους για την ημερομηνία έναρξης παραγωγής. Η μετάβαση γίνεται είτε με ευθύνη της τράπεζας, είτε με την βοήθεια του εξωτερικού συνεργάτη (αν το έργο έγινε από αυτόν). Συνήθως για λόγους ασφαλείας, ακόμα και στα out-sourced έργα η μετάβαση πραγματοποιείται με εμπλοκή μόνο της Τράπεζας.

7.6 Συντήρηση ηλεκτρονικών υπηρεσιών

Κάθε έργο απαιτεί και την διαρκή συντήρηση των παραδοτέων του. Αν το έργο είναι in-house την ευθύνη συντήρησης έχει η ίδια η τράπεζα. Σε περίπτωση που το έργο είναι out-sourced υπάρχουν δύο εναλλακτικές λύσεις:

-Υπογραφή συμβολαίου τεχνικής υποστήριξης: η τράπεζα υπογράφει σύμβαση τεχνικής υποστήριξης με τον εξωτερικό συνεργάτη, ο οποίος έχει την ευθύνη συντήρησης, καθώς και άμεσης παροχής υπηρεσιών σε περίπτωση εμφάνισης προβλημάτων ή διόρθωσης δυσλειτουργιών.

-Αγορά του source code: η τράπεζα αγοράζει τον πηγαίο κώδικα των παραδοτέων και αναλαμβάνει η ίδια εξ ολοκλήρου την συντήρηση και υποστήριξη του.

Η απόφαση της μιας από τις δύο λύσεις είναι δύσκολη και πρέπει να λαμβάνονται υπόψη όλα τα κριτήρια που την επηρεάζουν, όπως κόστος, απόσβεση του έργου , διαθεσιμότητα εσωτερικών στελεχών, ύπαρξη απαραίτητης τεχνογνωσίας, ασφάλεια, μελλοντικές ανάγκες κ.α.

7.7 Συνεργάτες σε Έργα In-house Συνεργάτες

Κυριότερος συνεργάτης της Διεύθυνσης Ηλεκτρονικής Τραπεζικής είναι η Διεύθυνση Πληροφορικής. Το ανθρώπινο δυναμικό της πληροφορικής είναι αυτό που είναι υπεύθυνο για το κεντρικό σύστημα της τράπεζας. Συνεπώς οποιοδήποτε έργο του e-banking απαιτείται απαραίτητα και την συνδρομή αυτής.
Άλλες οργανωτικές μονάδες που συμμετέχουν στην πλειοψηφία των έργων ηλεκτρονικής τραπεζικής είναι:

- Η νομική υπηρεσία της τράπεζας η οποία έχει λόγο σε όλες τις συμβάσεις που υπογράφονται εκ μέρους του οργανισμού, καθώς και γνωμοδοτεί για νέες υπηρεσίες ή συνεργασίες για την εγκυρότητα αυτών βάση της κείμενης νομοθεσίας.

- Η διεύθυνση εσωτερικού ελέγχου που διενεργεί συχνά ελέγχους στις ηλεκτρονικές υπηρεσίες και εισηγείται για ζητήματα που πρέπει να δοθεί ιδιαίτερη προσοχή κατά την διάρκεια εκτέλεσης των έργων.

- Η διεύθυνση marketing που αναλαμβάνει την επικοινωνία νέων προϊόντων στο ευρύ κοινό.

- Ο τομέας εκπαίδευσης ο οποίος σε συνεργασία με την μονάδα ηλεκτρονικής τραπέζης οργανώνει την εκπαίδευση των εσωτερικών συνεργατών στα νέα προϊόντα.

- Η διεύθυνση δικτύου που είναι υπεύθυνη για την ενημέρωση των καταστημάτων της τράπεζας για νέες ηλεκτρονικές υπηρεσίες.

-Η διεύθυνση οικονομικών υπηρεσιών που είναι υπεύθυνη για τη σωστή λογιστική απεικόνιση και τις οικονομικές υποχρεώσεις που απορρέουν από τα έργα του e banking.

Κεφαλαίο 8 : Νομικά Θέματα Ηλεκτρονικής τραπεζικής

8.1 Ποιοι μπορούν να εκδίδουν ηλεκτρονικό χρήμα;

Ηλεκτρονικό χρήμα μπορούν να εκδίδουν μόνο πρόσωπα ή επιχειρήσεις που αποτελούν πιστωτικά ιδρύματα κατά την έννοια της οδηγίας 2000/12/ΕΚ, άρθρο 1, σημείο 1 πρώτο εδάφιο - "πιστωτικό ίδρυμα": επιχείρηση, της οποίας η δραστηριότητα συνίσταται στην αποδοχή καταθέσεων ή άλλων επιστρεπτέων κεφαλαίων από το κοινό και στη χορήγηση πιστώσεων για ίδιο λογαριασμό.

8.2 Τι γίνεται στην περίπτωση που αμφισβητηθεί η ηλεκτρονική πληρωμή με ηλεκτρονικό χρήμα;

Αυτή η πληρωμή είναι μία τριπλή λειτουργία. Η τράπεζα πιστώνει τον πωλητή ,αφού εξακριβώσει τους κρυφούς κώδικες του ηλεκτρονικού χρήματος, με το ποσό που πληρώθηκε από τον καταναλωτή, του οποίου χρεώθηκε ο τρέχον λογαριασμός. Η τράπεζα επιβεβαιώνει την επιτυχή σύναψη της συναλλαγής και η πληρωμή δεν μπορεί να αμφισβητηθεί από τον πελάτη λόγω δέσμευσής της τράπεζας του να διαφυλάττει τους μυστικούς του κώδικες.

8.3 Τι θα συμβεί αν η ηλεκτρονική πληρωμή με πιστωτική κάρτα δεν γίνει αποδεκτή από τον κάτοχο της κάρτας;

Οι συμβατικοί κανόνες και οι διαδικασίες που υιοθετούν οι τράπεζες καθιερώνουν για όσους αποδέχονται πληρωμές μέσω πιστωτικής κάρτας την υποχρέωση να λαμβάνουν μία υπογεγραμμένη εντολή πληρωμής και να εξακριβώνουν ότι η υπογραφή ανταποκρίνεται σ'αυτήν της κάρτας. Είναι όμως φανερό ότι αυτό δεν μπορεί να εφαρμοστεί στην περίπτωση πληρωμής με πιστωτική κάρτα μέσω διαδικτύου. Επομένως η θέση του πωλητή στη συγκεκριμένη περίπτωση δεν είναι ισχυρή από νομικής πλευράς, αφού ο αγοραστής μπορεί να αρνηθεί την εντολή αγοράς. Χρησιμοποιώντας την διαδικασία Ασφαλούς Ηλεκτρονικής Συναλλαγής (SET- Secure Electronic Transaction), δίνεται η δυνατότητα βελτίωσης της αποδεικτικής ικανότητας. Αν ο πελάτης αμφισβητεί τη συναλλαγή, η Τράπεζα πρέπει να αποδείξει ότι η εν λόγω συναλλαγή έχει πραγματοποιηθεί και ότι ο πελάτης έχει δώσει την έγκρισή του.

8.4 Ποιες πληροφορίες πρέπει να έχει στη διάθεσή του ο καταναλωτής από τον εκδότη ηλεκτρονικού χρήματος

Κατά την υπογραφή της σύμβασης του ηλεκτρονικού μέσου πληρωμής ο εκδότης ανακοινώνει στον κάτοχο τους συμβατικούς όρους που διέπουν την έκδοση και χρησιμοποίηση του ηλεκτρονικού μέσου πληρωμής. Οι όροι γνωστοποιούνται εγγράφως.
Οι όροι πρέπει να περιλαμβάνουν απαραίτητα τα πιο κάτω:
α) περιγραφή του ηλεκτρονικού μέσου πληρωμής

β) περιγραφή των αντίστοιχων υποχρεώσεων και ευθυνών του κατόχου και του εκδότη αναφέρονται ιδίως οι βασικές προφυλάξεις που πρέπει να λαμβάνει κάτοχος για να εξασφαλίσει την ασφάλεια του μέσου ηλεκτρονικής πληρωμής καθώς και τα μέσα που του επιτρέπουν να το χρησιμοποιεί (προσωπικός αριθμός αναγνώρισης ταυτότητας ή άλλος κωδικός αριθμός)
γ) κατά περίπτωση την κανονική περίοδο εντός της οποίας χρεώνεται ή πιστώνεται ο λογαριασμός του κατόχου
δ) τα είδη των τυχόν εξόδων που βαρύνουν τον κάτοχο.
ε) τη χρονική περίοδο εντός της οποίας μια συγκεκριμένη συναλλαγή μπορεί να αμφισβητηθεί από τον κάτοχο και αναφορά των διαδικασιών καταγγελίας

8.5 Ποιες πληροφορίες πρέπει να παρέχονται στον καταναλωτή μετά τη συναλλαγή

Ο εκδότης ηλεκτρονικού χρήματος πρέπει να παρέχει στον κάτοχο πληροφορίες σχετικά με τις συναλλαγές που έχουν γίνει με ηλεκτρονικό μέσο πληρωμής.
Οι πληροφορίες αυτές που πρέπει να παρέχονται εγγράφως και περιλαμβάνουν τουλάχιστον τα ακόλουθα:
α) ένδειξη που επιτρέπει στον κάτοχο να εντοπίσει τη συναλλαγή
β) το ποσό της συναλλαγής που χρεώνεται στον κάτοχο στο νόμισμα τιμολόγησης και κατά περίπτωση το ποσό σε ξένο νόμισμα
γ) το ποσό τυχόν προμηθειών και εξόδων που εφαρμόζονται σε ορισμένα είδη συναλλαγών.
Ο εκδότης γνωστοποιεί επίσης στον κάτοχο τη συναλλαγματική ισοτιμία βάσει της οποίας γίνονται οι μετατροπές συναλλαγών σε ξένο νόμισμα.
Ο εκδότης ενός μέσου ηλεκτρονικού χρήματος παρέχει στον κάτοχο τη δυνατότητα να ελέγχει τις τελευταίες πέντε συναλλαγές που εκτελέστηκαν με το μέσο αυτό και την απομένουσα αποθηκευμένη αξία σ' αυτό.

8.6 Ποιες είναι οι υποχρεώσεις του κατόχου ηλεκτρονικού χρήματος ;

Ο κάτοχος ηλεκτρονικού χρήματος πρέπει να:

α) χρησιμοποιεί το μέσο ηλεκτρονικής πληρωμής σύμφωνα με τους όρους που διέπουν την έκδοση και χρήση του μέσου πληρωμής και ειδικότερα να λαμβάνει όλα τα απαραίτητα μέτρα για την ασφαλή φύλαξη του μέσου ηλεκτρονικής πληρωμής και των μέσων (προσωπικός αριθμός αναγνώρισης ταυτότητας ή άλλος κωδικός αριθμός) που επιτρέπουν τη χρησιμοποίησή του.

β) ειδοποιεί χωρίς καθυστέρηση τον εκδότη μόλις αντιληφθεί:
- την απώλεια ή κλοπή του μέσου ηλεκτρονικής πληρωμής ή των μέσων που επιτρέπουν τη χρησιμοποίησή του
- τον καταλογισμό στο λογαριασμό του οποιασδήποτε συναλλαγής που έγινε παρά τη βούλησή του
- τυχόν σφάλμα ή άλλη ανωμαλία στην τήρηση του λογαριασμού του από τον εκδότη.

γ) να μην καταγράφει τον προσωπικό του αριθμό αναγνώρισης ταυτότητας ή άλλο κωδικό αριθμό επί του μέσου ηλεκτρονικής πληρωμής ή άλλου αντικειμένου που φυλάσσει ή μεταφέρει μαζί με το μέσο ηλεκτρονικής πληρωμής
δ) να μην ανακαλεί εντολή που έχει δώσει με το μέσο ηλεκτρονικής πληρωμής εκτός εάν το ποσό της δεν είχε προσδιοριστεί όταν δόθηκε η εντολή πληρωμής.

8.7 Πως και πότε μπορεί ο καταναλωτής να ζητήσει την εξαργύρωση του ηλεκτρονικού χρήματος που κατέχει

Ο κάτοχος ηλεκτρονικού χρήματος δικαιούται, κατά την περίοδο ισχύος τον χρήματος αυτού, να ζητήσει την εξαργύρωση του στην ονομαστική αξία σε κέρματα και χαρτονομίσματα ή με μεταφορά σε τραπεζικό λογαριασμό χωρίς άλλα τέλη από τα απολύτως αναγκαία για την εκτέλεση της συγκεκριμένης πράξης.
Η σύμβαση μεταξύ του εκδότη και τον κομιστή πρέπει να ορίζει σαφώς τους όρους εξαργύρωσης και να προβλέπει ένα ελάχιστο όριο εξαργύρωσης, το οποίο δεν μπορεί να υπερβαίνει τα 10 ευρώ.

8.8 Τι προβλέπεται για την προστασία των προσωπικών δεδομένων και την ασφάλεια των συναλλαγών στη χρήση του ηλεκτρονικού χρήματος

Η ηλεκτρονική πληρωμή έχει οριστικό χαρακτήρα. Η εντολή που δίνεται μέσω μιας κάρτας πληρωμής είναι ανέκκλητη και δεν επιτρέπει επομένως καμία αντίθετη εντολή.
Τα δεδομένα που διαβιβάζονται, τη στιγμή της πληρωμής, στην τράπεζα του παρέχοντος υπηρεσίες και στη συνέχεια στον εκδότη δεν πρέπει σε καμία περίπτωση να θέσουν σε κίνδυνο την προστασία της ιδιωτικής ζωής και περιορίζονται αυστηρά στα στοιχεία που προβλέπονται συνήθως για τις επιταγές και τις μεταφορές ποσών από λογαριασμό σε λογαριασμό.
Όλα τα προβλήματα που συνδέονται με την προστασία των δεδομένων και την ασφάλεια πρέπει να αναφέρονται ρητά και να επιλύονται σε όλα τα στάδια της σύναψης των συμβάσεων μεταξύ των συμβαλλόμενων μερών. Οι συμβάσεις δεν πρέπει να θέτουν σε κίνδυνο την ελευθερία διαχείρισης των παρεχόντων υπηρεσιών και τον ανταγωνισμό μεταξύ τους.

Κεφαλαίο 9 : Αναλυτικά η υπηρεσίες e-banking των τραπεζών

9.1 Υπηρεσίες e-banking εθνικής τράπεζας

9.1.1 Internet Banking:

Οι υπηρεσίες μας

Το Internet Banking της Εθνικής Τράπεζας σας παρέχει πλήθος συναλλαγών και υπηρεσιών, εξασφαλίζοντας την άνετη και γρήγορη εξυπηρέτησή σας. Με το Internet Banking της Εθνικής Τράπεζας έχετε τη δυνατότητα να πραγματοποιείτε τις συναλλαγές σας 24 ώρες το 24ωρο, εύκολα, γρήγορα και με ασφάλεια, από οποιοδήποτε σημείο υπάρχει σύνδεση στο Internet: PC, laptop ή ακόμα και κινητό τηλέφωνο τεχνολογίας i-mode® (για συνδρομητές Cosmote).
Επιπλέον, με την εγγραφή σας στο Internet Banking αποκτάτε αμέσως πρόσβαση και στην υπηρεσία του Phone Banking, για διενέργεια συναλλαγών μέσω τηλεφώνου, από την Ελλάδα και το εξωτερικό. Με το Phone Banking εξυπηρετείστε από οποιοδήποτε τηλέφωνο (σταθερό ή κινητό), με απλές φωνητικές εντολές ή με τη βοήθεια εκπροσώπου μας. Το Internet Banking σας παρέχει μεγάλο εύρος συναλλαγών που σας εξασφαλίζουν την παρακολούθηση και διαχείριση των καταθετικών, δανειακών και επενδυτικών λογαριασμών σας σε πραγματικό χρόνο, όπως:

- **Πληροφόρηση λογαριασμών** (υπόλοιπα & κινήσεις)
- **Πληροφόρηση και πληρωμή πιστωτικών καρτών**
- **Μεταφορά ποσών** σε λογαριασμούς ιδίου ή τρίτων στην Εθνική και σε άλλες τράπεζες, στην Ελλάδα και στην Ε.Ε.
- **Πληρωμή λογαριασμών:** ΔΕΗ, ΟΤΕ, κινητή /σταθερή τηλεφωνία, ασφαλιστήρια συμβόλαια κ.ά.
- **Χρηματιστηριακές συναλλαγές** και ενημέρωση συναλλαγών Χ.Α.Α. (10λεπτη καθυστέρηση)
- **Πάγιες εντολές**

Επιπλέον το Internet Banking παρέχει λύσεις, ειδικά σχεδιασμένες για επιχειρήσεις.

Οι συναλλαγές που παρέχονται μέσω του Internet Banking συνεχώς εμπλουτίζονται. Στην Εθνική Τράπεζα φροντίζουμε κάθε συναλλαγή που προστίθεται στο Internet Banking να διατίθεται παράλληλα από όλα τα Εναλλακτικά Δίκτυα. Έτσι, είναι στη δική σας ευχέρεια να επιλέξετε το μέσον που σας εξυπηρετεί κάθε φορά: Τα ATMs, το Internet, το κινητό ή σταθερό σας τηλέφωνο, απολαμβάνοντας 24ωρη εξυπηρέτηση, όποτε εσείς θέλετε.

Είσοδος και διενέργεια συναλλαγών στο Internet Banking

Η Εθνική Τράπεζα έχει αναβαθμίσει το περιβάλλον του Internet Banking, το οποίο διαθέτει, πλέον, αυξημένες λειτουργικές δυνατότητες.
Η είσοδος στο Internet Banking γίνεται από το Web Site της Τράπεζας στη διεύθυνση http://www.nbg.gr. Η διεύθυνση https://homebank.nbg.gr παραπέμπει στο προηγούμενο περιβάλλον του Internet Banking και θα εξακολουθήσει να ισχύει για μικρό χρονικό διάστημα.

Για την είσοδό σας στο Internet Banking απαιτείται:

- Ο **Κωδικός Εισόδου (UserID)**, ο οποίος αποτελεί την ταυτότητά σας ως χρήστη Internet Banking.
- Ο **Μυστικός Κωδικός (Password):** Ο Κωδικός αυτός επιτρέπει την πρόσβασή σας στο Internet Banking.

Για τη διενέργεια εγχρήματων συναλλαγών και συναλλαγών ασφαλείας απαιτείται η επιπλέον εισαγωγή ενός κωδικού μιας χρήσης που παράγεται από τη συσκευή i-code.

Για το Μυστικό Κωδικό (Password) θα πρέπει να γνωρίζετε ότι:

- **Κατά την εγγραφή σας στο Internet Banking** παραλαμβάνετε τον Κωδικό Εισόδου (UserID) και τη συσκευή i-code, ενώ **το Password αποστέλλεται ταχυδρομικά**, στη διεύθυνση επικοινωνίας, με συστημένη αλληλογραφία.

- **Κατά την πρώτη είσοδό σας στο Internet Banking**, σας ζητείται να αντικαταστήσετε το Μυστικό Κωδικό (Password) με πενταψήφιο αριθμό της επιλογής σας (πέντε χαρακτήρες, με αριθμούς, γράμματα του λατινικού αλφαβήτου ή συνδυασμός των δύο), τον οποίο πρέπει να απομνημονεύσετε.

- **Μπορείτε να αλλάζετε** τον Μυστικό Κωδικό, μέσω του μενού «Ασφάλεια» του Internet Banking όσο συχνά θέλετε. Από το μενού αυτό μπορείτε να πραγματοποιήσετε δέσμευση του Κωδικού σας. Με τον τρόπο αυτό δεν θα έχετε πλέον πρόσβαση στο σύστημα και δεν θα μπορείτε να διενεργήσετε καμία συναλλαγή. Για να χρησιμοποιήσετε πάλι το σύστημα θα πρέπει να επικοινωνήσετε με το Help Desk.

- **Εάν ο Μυστικός Κωδικός παραμένει αμετάβλητος για χρονικό διάστημα 2 μηνών,** το σύστημα θα σας ζητήσει να τον αλλάξετε υποχρεωτικά.

- **Κανένας άλλος δεν πρέπει να γνωρίζει το Μυστικό Κωδικό σας:** Για τη δική σας ασφάλεια πρέπει να τον απομνημονεύετε ή να τον φυλάτε σε ασφαλές μέρος. Σε περίπτωση διαρροής του, θα πρέπει να προχωράτε στην **αλλαγή του.** Η Τράπεζα δεν φέρει καμία ευθύνη, σε περίπτωση απώλειας του Κωδικού σας, για συναλλαγές που έγιναν από άλλο πρόσωπο, παρά τη θέλησή σας.

Μετά απο τέσσερις συνεχείς προσπάθειες εισαγωγής λανθασμένου Κωδικού Εισόδου (UserID) ή /και Μυστικού Κωδικού (Password), **το σύστημα δεν σας επιτρέπει πλέον την πρόσβαση.** Στην περίπτωση αυτή θα πρέπει να επικοινωνήσετε με το Help Desk.

<u>Το Internet Banking για επιχειρήσεις</u>

Το Internet Banking παρέχει λύσεις, ειδικά σχεδιασμένες για επιχειρήσεις, που συντελούν στην αυτοματοποίηση των διαδικασιών, μειώνοντας παράλληλα το λειτουργικό κόστος και την απασχόληση προσωπικού, όπως:

- **Εξυπηρέτηση μισθοδοσίας**
- **Εξόφληση οφειλών σε συνεργάτες και προμηθευτές,** με αποστολή εμβασμάτων (απλών και μαζικών) σε λογαριασμούς Εθνικής Τράπεζας και άλλων τραπεζών (στην Ελλάδα και στην ΕΕ)
- **Μαζικές εισπράξεις από οφειλέτες,** με αυτόματη χρέωση των λογαριασμών τους στην Εθνική Τράπεζα
- **Εξόφληση οφειλών προς το Δημόσιο:** ΔΕΗ, ΙΚΑ, ΦΠΑ, φόρος Εισοδήματος κ.λπ.
- **Πληρωμές** σε εταιρείες τηλεφωνίας και Internet, ασφαλιστικές εταιρείες, συνταξιοδοτικά ταμεία κ.ά.
- **Πληροφόρηση και ανάλυση κινήσεων πιστωτικών καρτών πελατών** της επιχείρησης μέσω P.O.S.

Με το Internet Banking εξυπηρετείστε εύκολα, γρήγορα και με ασφάλεια, 24 ώρες το 24ωρο, με μηδενικά ή ελάχιστα έξοδα, από οποιοδήποτε σημείο υπάρχει σύνδεση στο internet.

Για να εγγραφείτε ως επιχείρηση στο Internet Banking θα πρέπει:

- Να έχετε υποβάλλει στο Κατάστημα συνεργασίας τα Νομιμοποιητικά σας έγγραφα και να είναι σε ισχύ.
- Να έχετε ένα τουλάχιστον εταιρικό λογαριασμό σε ΕΥΡΩ σε οποιοδήποτε Κατάστημα της Τράπεζας.

Στο Internet Banking επιχειρήσεων ορίζετε εξουσιοδοτημένους χρήστες (Θέσεις Εργασίας):

- Μπορείτε να καθορίσετε **όσες Θέσεις Εργασίας επιθυμείτε.**
- Μπορείτε να αποδώσετε **συγκεκριμένα δικαιώματα και ευχέρειες** σε κάθε Θέση Εργασίας. Ειδικότερα:
    - **Σε ποιους λογαριασμούς της επιχείρησης θα έχει πρόσβαση** (χορηγητικούς, καταθετικούς, επενδυτικούς).
    - Αν θα μπορεί να διενεργεί **εγχρήματες συναλλαγές** ή μόνο **πληροφοριακές** (υπόλοιπα /κινήσεις).
    - Σε περίπτωση που μία Θέση Εργασίας έχει **δικαίωμα διενέργειας εγχρήματων συναλλαγών:**

- **Ποιες από τις διαθέσιμες συναλλαγές** στο Internet Banking θα μπορεί να διενεργεί.
- **Ανώτατο όριο ποσού**
- Αν θα διεκπεραιώνει τις εγχρήματες συναλλαγές μόνη της ή με έγκριση και από άλλη Θέση Εργασίας (μέχρι δύο Θέσεις Εργασίας επιπλέον).

o Αν μία Θέση Εργασίας θα έχει το **δικαίωμα έγκρισης εγχρήματων συναλλαγών** σε άλλες Θέσεις Εργασίας.

Για παράδειγμα:

- Ο λογιστής της εταιρείας μπορεί να εξοφλεί μόνο λογαριασμούς (ΔΕΗ, ΟΤΕ κ.λπ.) και ΦΠΑ /ΙΚΑ /ΟΑΕΕ μόνος του ή με σύμπραξη άλλου στελέχους.
- Ο υπεύθυνος επενδύσεων μπορεί να δίνει εντολές για αγοραπωλησία μετοχών μόνος του ή με σύμπραξη άλλου στελέχους, π.χ. του Οικονομικού Διευθυντή, μέχρι ένα συγκεκριμένο όριο ποσού.
- Οποιοδήποτε ανώτερο στέλεχος (π.χ. ο Οικονομικός Διευθυντής ή ο Γενικός Διευθυντής) μπορεί να παρακολουθεί την κίνηση όλων ή μερικών από τους λογαριασμούς της επιχείρησης.

Κάθε θέση εργασίας καθορίζεται:

- Από τον **Κωδικό Εισόδου (UserID)**
- Από τον **Μυστικό Κωδικό (Password)**
- Από τη συσκευή **Ηλεκτρονικού Κλειδαρίθμου (i-code).**

Τα τρία αυτά στοιχεία μαζί αποτελούν μία και μοναδική «Θέση Εργασίας». Ο Κωδικός Εισόδου (UserID) και η συσκευή i-Code παραλαμβάνονται από το νόμιμο εκπρόσωπο της επιχείρησης στο Κατάστημα. Ο Μυστικός Κωδικός (Password) αποστέλλεται ταχυδρομικώς, με συστημένη αλληλογραφία.
Ο νόμιμος εκπρόσωπος της επιχείρησης παραδίδει τα στοιχεία αυτά σε όποιο στέλεχος ή υπάλληλο επιθυμεί, χωρίς να γνωστοποιεί στην Τράπεζα ποιος κάνει χρήση αυτής της Θέσης Εργασίας.

Ο καθορισμός των Θέσεων Εργασίας γίνεται:

- **Από το Κατάστημα:** Οι νόμιμοι εκπρόσωποι της επιχείρησης, με την εγγραφή στο Internet Banking δηλώνουν πόσες Θέσεις Εργασίας επιθυμούν, καθώς και τις ευχέρειές τους, υπογράφοντας αντίστοιχο αριθμό αιτήσεων. Στην περίπτωση αυτή, τυχόν μεταβολές ευχερειών για κάθε Θέση Εργασίας αλλά και εισαγωγή νέων Θέσεων, διαγραφή υφισταμένων κ.λπ. γίνονται από το Κατάστημα.

- **Από το Διαχειριστή Θέσεων Εργασίας,** από τα γραφεία της επιχείρησης ή οπουδήποτε υπάρχει σύνδεση στο internet: Οι νόμιμοι εκπρόσωποι της επιχείρησης ορίζουν έναν ή περισσότερους Διαχειριστές Θέσεων Εργασίας, συμπληρώνοντας αντίστοιχο αριθμό αιτήσεων στο Κατάστημα.

Με τον καθορισμό Διαχειριστή Θέσεων Εργασίας η επιχείρηση αποκτά ευελιξία, εξοικονόμηση χρόνου και πλήρη εποπτεία της χρήσης του Internet Banking, χωρίς τη διαμεσολάβηση της Τράπεζας. Ειδικότερα, ο Διαχειριστής Θέσεων Εργασίας:

- **Δημιουργεί νέες Θέσεις Εργασίας** στο Internet Banking, με το επιθυμητό προφίλ: πρόσβαση σε λογαριασμούς /συναλλαγές, διενέργεια εγχρήματων συναλλαγών ή όχι, όριο ποσού, απαιτούμενες «υπογραφές» (αριθμός στελεχών που απαιτούνται να συμπράξουν για την ολοκλήρωση της συναλλαγής), έγκριση συναλλαγών σε άλλες Θέσεις Εργασίας ή όχι κ.λπ.
- **Μεταβάλλει το προφίλ** μιας Θέσης Εργασίας
- **Εποπτεύει τις κινήσεις** όλων των Θέσεων Εργασίας στο Internet Banking
- **Δεν έχει δυνατότητα διεξαγωγής συναλλαγών.**
-

Οι Θέσεις Εργασίας και οι ευχέρειές τους μπορούν να καθορίζονται με τη σύμπραξη περισσοτέρων του ενός Διαχειριστών.

<u>Προδιαγραφές τεχνικού εξοπλισμού</u>

Οι **ελάχιστες προδιαγραφές** που θα πρέπει να έχετε σε software / hardware για να έχετε πρόσβαση στο Internet Banking είναι οι εξής:

Για υπολογιστές με λειτουργικό σύστημα Windows:

- Επεξεργαστής Intel Pentium 4 / 1.20 GHz (ή συμβατός με: Intel Celeron ή AMD family)
- Microsoft Windows 2000 ενημερωμένο με το τελευταίο service pack
- 512 MB RAM
- Internet Explorer 6.0, Firefox 2.x
- Adobe® Acrobat Reader® 6.0
- 1 GB (gigabyte) ελεύθερο χώρο στο σκληρό δίσκο
- Ανάλυση οθόνης 1024x768 pixels
- Modem 56Kbps ή ADSL 1Mbps Line

Για υπολογιστές με λειτουργικό σύστημα Mac:

- Επεξεργαστής PowerPC G4 533MHz
- MAC OS X 10.3
- 512 MB RAM
- Firefox 2.x
- 1 GB (gigabyte) ελεύθερο χώρο στον σκληρό δίσκο
- Ανάλυση οθόνης 1024x768 pixels
- Modem 56Kbps ή ADSL 386Kbps Line

Οι **προτεινόμενες προδιαγραφές**, από μέρους της Τράπεζάς μας, για την ταχύτερη πρόσβαση στο Διαδίκτυο και κατά συνέπεια στις υπηρεσίες Internet Banking, είναι:

Για υπολογιστές με λειτουργικό σύστημα Windows:

- Επεξεργαστής Intel Pentium 4 / 3.2 GHz (ή συμβατός με: Intel Celeron ή AMD family)

- Microsoft Windows 2000/XP ενημερωμένο με το τελευταίο service pack
- 1 GB (gigabyte) RAM
- Internet Explorer 6.0 /7.0, Firefox 2.x
- Adobe® Acrobat Reader® 6.0
- 10 GB (gigabytes) ελεύθερο χώρο στο σκληρό δίσκο
- Ανάλυση οθόνης 1024x768 pixels
- Modem 56Kbps ή ADSL 1Mbps Line

Για υπολογιστές με λειτουργικό σύστημα Mac:

- Επεξεργαστής PowerPC G4 (1.8GHz+)/G5(2GHz+) ή Core Solo/Duo Intel
- MAC OS X 10.4+\
- 1 GB (gigabyte) RAM
- Firefox 2.x10
- GB (gigabytes) ελεύθερο χώρο στο σκληρό δίσκο
- Ανάλυση οθόνης 1024x768 pixels
- Modem 56Kbps ή ADSL 1Mbps Line

Προκειμένου να χρησιμοποιήσετε την υπηρεσία «**Ενημέρωση για Επενδυτές**» θα πρέπει ο Ηλεκτρονικός Υπολογιστής σας να πληροί τις παρακάτω προδιαγραφές:

Internet Explorer 6.0 και άνω.
Java RunTime Enviroment 1.4.2 (Παρέχεται δωρεάν από τον δικτυακό τόπο της υπηρεσίας "Ενημέρωση για Επενδυτές").

9.1.2 Phone Banking:

Τι υπηρεσίες παρέχονται μέσω του Phone Banking

Στην Εθνική Τράπεζα, γνωρίζοντας τις σύγχρονες ανάγκες των πελατών μας, αξιοποιήσαμε την πιο προηγμένη τεχνολογία αναγνώρισης φωνητικών εντολών (IVR) και είμαστε κοντά σας, οποτεδήποτε και οπουδήποτε μας χρειαστείτε:

Καλώντας το **181818** από σταθερό ή κινητό τηλέφωνο, από την Ελλάδα ή το **+30 210 4848484** από το εξωτερικό, συνδέεστε με το Phone Banking της Εθνικής.

Μπορείτε να εξυπηρετηθείτε **24 ώρες την ημέρα, 365 μέρες τον χρόνο, με απλές φωνητικές εντολές ή με τη βοήθεια εκπροσώπου μας** για:

- **Δήλωση απώλειας της κάρτας σας** (χρεωστικής ή πιστωτικής)
- **Πληροφορίες για τις πιστωτικές σας κάρτες:** υπόλοιπο, κίνηση, τρόποι εξόφλησης κ.λπ.
- **Ενημέρωση για προϊόντα / υπηρεσίες, σημεία εξυπηρέτησης (Καταστήματα /ATMs), τιμές συναλλάγματος κ.ά.** Η ενημέρωση αυτή παρέχεται ακόμα και αν δεν είστε πελάτης της Τράπεζας και μπορεί να ληφθεί είτε με φωνητικές εντολές και απαντήσεις από το αυτόματο σύστημα είτε από εκπρόσωπο.

- **Συναλλαγές:** Όλες οι διαθέσιμες συναλλαγές στο Internet Banking μπορούν να πραγματοποιηθούν και μέσω τηλεφώνου. Η υπηρεσία αυτή διατίθεται για συνδρομητές Internet /Phone /Mobile Banking.
- **Σύνδεση** με εκπρόσωπό μας.

Τι χρειάζεσθε για να πραγματοποιήσετε συναλλαγές μέσω της υπηρεσίας Phone Banking

Εάν είστε συνδρομητής του Internet Banking, έχετε παράλληλα τη δυνατότητα χρήσης της υπηρεσίας Phone Banking της Τράπεζάς μας:

- **Για την είσοδό σας στην υπηρεσία Phone Banking** απαιτείται ο 6ψήφιος αριθμητικός Κωδικός Εισόδου (User ID), που είναι ο ίδιος με τον Κωδικό Εισόδου του Internet Banking και ένας κωδικός μιας χρήσης που παράγεται από τη συσκευή i-code. Εάν έχετε αλφαριθμητικό Κωδικό Εισόδου (User ID), παρέχεται η δυνατότητα άμεσης παραλαβής του νέου, αριθμητικού κωδικού, που θα σας επιτρέπει την παράλληλη πρόσβαση στο Phone Banking, μέσω του menu «Αιτήσεις» του Internet Banking.
- **Για τη διενέργεια εγχρήματων συναλλαγών και συναλλαγών ασφαλείας** απαιτείται η εισαγωγή ενός ακόμη κωδικού i-code.

Πώς θα πραγματοποιήσετε τις συναλλαγές σας μέσω του Phone Banking (επιλογή: «ΣΥΝΑΛΛΑΓΕΣ»)

- Μέσω του Phone Banking εξυπηρετούνται όλες οι συναλλαγές που είναι διαθέσιμες στο Internet Banking, από οποιοδήποτε τηλέφωνο (σταθερό ή κινητό), 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα, από την Ελλάδα και το εξωτερικό.
- Οι συναλλαγές πραγματοποιούνται είτε μέσω του αυτόματου συστήματος αναγνώρισης φωνητικών εντολών είτε με τη βοήθεια εκπροσώπου.
- Για να συνδεθείτε με την υπηρεσία Phone Banking και να πραγματοποιήσετε συναλλαγές ακολουθείτε τα παρακάτω βήματα:
    1. Καλείτε το **181818** από σταθερό (αστική χρέωση) ή κινητό τηλέφωνο, από την Ελλάδα ή το **+30 210 4848484** από το εξωτερικό.
    2. Μια φιλική φωνή σας καθοδηγεί στο μενού υπηρεσιών και περιμένει τις οδηγίες σας, προτείνοντάς σας κάθε φορά την κατάλληλη λέξη – κλειδί για να συνεχίσετε. Περιηγείστε στο μενού υπηρεσιών με απλές, φωνητικές εντολές λέγοντας κάθε φορά τη λέξη που σας έχει προτείνει το αυτόματο σύστημα.
    3. Για να πραγματοποιήσετε οποιαδήποτε από τις συναλλαγές που είναι διαθέσιμες και στο Internet Banking (πληροφοριακές ή εγχρήματες), θα πρέπει να πείτε «Συναλλαγές»:
    - Το αυτόματο σύστημα αναγνώρισης φωνητικών εντολών σας ζητά να πείτε ή να πληκτρολογήσετε το **UserID** σας και έναν αριθμό ηλεκτρονικού κλειδαρίθμου **(i-code).**
    - Εφόσον τα στοιχεία αυτά είναι σωστά, ακούτε τις διαθέσιμες επιλογές: Πληροφορίες Λογαριασμών, Πιστωτικές Κάρτες, Μεταφορά Χρηματικών Ποσών, Πληρωμή Λογαριασμών, Χρηματιστηριακές Συναλλαγές, Αίτηση έκδοσης βιβλιαρίων επιταγών ή καρτών, Πάγιες Εντολές.

- Σε κάθε μία από τις επιλογές αυτές περιλαμβάνονται οι συναλλαγές της αντίστοιχης ομάδας. Οδηγείστε στη συναλλαγή που επιθυμείτε λέγοντας τη λέξη που σας προτείνει το σύστημα π.χ. υπόλοιπα λογαριασμών.
- Για να πραγματοποιήσετε τη συναλλαγή που έχετε επιλέξει, το αυτόματο σύστημα σας καθοδηγεί προτείνοντάς σας τις κατάλληλες λέξεις –κλειδιά ή ζητώντας σας να πείτε ή να πληκτρολογήσετε τα απαιτούμενα στοιχεία (π.χ. αριθμός λογαριασμού, αριθμός ηλεκτρονικού κλειδαρίθμου κ.λπ.).
- Σε ορισμένες συναλλαγές το σύστημα σας παραπέμπει απευθείας σε εκπρόσωπο. Οι συναλλαγές αυτές δεν πραγματοποιούνται μέσω του αυτόματου συστήματος.
- Οποιαδήποτε στιγμή, ακόμη και κατά τη διάρκεια μιας συναλλαγής, μπορείτε να διακόψετε για να συνδεθείτε με κάποιο εκπρόσωπο, λέγοντας τη λέξη «Εκπρόσωπος».

Πώς θα πληροφορηθείτε για τους Τραπεζικούς σας Λογαριασμούς, τις Πιστωτικές σας Κάρτες ή το Δάνειό σας (επιλογή: «ΠΛΗΡΟΦΟΡΙΕΣ»)

- Εάν είστε κάτοχος πιστωτικής κάρτας Εθνικής Τράπεζας, έχετε τη δυνατότητα να πληροφορηθείτε, μέσω της υπηρεσίας Phone Banking, ακόμη και αν δεν είστε συνδρομητής Internet /Phone Banking:
  - το όριο της πιστωτικής σας κάρτας,
  - το ποσό των μελλοντικών δόσεων (το συνολικό ποσό που εκκρεμεί από συναλλαγές άτοκων δόσεων),
  - την τρέχουσα οφειλή (συνολικό ποσό οφειλής),
  - το διαθέσιμο υπόλοιπο για αγορές,
  - τις τελευταίες κινήσεις της κάρτας σας (αγορές, αναλήψεις ή πληρωμές),
  - τους τρόπους εξόφλησης του λογαριασμού της πιστωτικής σας κάρτας (π.χ. μέσω ATM, μέσω Internet ή Phone Banking, με χρέωση λογαριασμού, στα καταστήματα της ΕΤΕ κ.λπ.) και
  - τους τρόπους με τους οποίους μπορείτε να υποβάλλετε αίτημα για αλλαγή διεύθυνσης κατοικίας, επικοινωνίας κ.λπ.

Τα υπόλοιπα /κινήσεις πιστωτικών καρτών μπορούν να αποστέλλονται και με fax, SMS ή e-mail.

- Για να συνδεθείτε με την υπηρεσία Phone Banking προκειμένου να έχετε την παραπάνω πληροφόρηση:
  - Καλείτε το **181818** από σταθερό (αστική χρέωση) ή κινητό τηλέφωνο, από την Ελλάδα ή το **+30 210 4848484** από το εξωτερικό.
  - Ακούτε το μενού υπηρεσιών. Για να επιλέξετε τη συγκεκριμένη υπηρεσία θα πρέπει να πείτε **«Πληροφορίες».**
  - Η επιλογή αυτή σας παραπέμπει σε εκπρόσωπό μας, ο οποίος αφού σας ζητήσει τα απαιτούμενα στοιχεία, προκειμένου να σας ταυτοποιήσει, σας παρέχει την πληροφόρηση που επιθυμείτε.
  - Μέσω της επιλογής αυτής **εξυπηρετούνται και συνδρομητές Internet / Phone Banking** για ενημέρωση σχετικά με τους λογαριασμούς ή τα δάνειά τους, οι οποίοι ταυτοποιούνται με το UserID και έναν κωδικό i-code.
  - Οι συνδρομητές Internet / Phone Banking μπορούν να εξυπηρετηθούν και μέσω του αυτόματου συστήματος αναγνώρισης φωνητικών εντολών (για υπόλοιπα

/κινήσεις πιστωτικών καρτών, λογαριασμών και δανείων) επιλέγοντας **«Συναλλαγές».**

9.1.3 Mobile Banking:

Οι ηλεκτρονικές υπηρεσίες i-bank της Εθνικής Τράπεζας σας παρέχουν την επιλογή του **i-bank Mobile Banking**, με τη χρήση έξυπνων συσκευών κινητών (Smartphones):

- Αν η συσκευή σας είναι **iPhone™**, **iPod touch®**, **BlackBerry™** ή **Windows Mobile®** και είστε **χρήστης των υπηρεσιών i-bank Internet /Phone Banking**, αξιοποιήστε σήμερα κιόλας τις νέες υπηρεσίες που σας προσφέρει η Εθνική Τράπεζα, για πρόσβαση σε πληροφορίες και συναλλαγές, 24ώρες το 24ωρο, οπουδήποτε και αν βρεθείτε.

<u>i-bank Mobile Banking για «έξυπνες» πληροφοριακές & εγχρήματες συναλλαγές:</u>

Για εσάς που είστε χρήστες Internet /Mobile Banking, σχεδιάσαμε μια σειρά από 'έξυπνες' δυνατότητες. Πλοηγηθείτε στο Μενού της Smartphone συσκευής σας, 24 ώρες το 24ωρο, με την ευκολία και ασφάλεια που σας παρέχουν οι υπηρεσίες i-–bank. Επιλέξτε "**Mobile Banking**" και στη συνέχεια:

- **«Λογαριασμοί»**: Για να ενημερωθείτε για το υπόλοιπο και τις 10 τελευταίες κινήσεις των συνδεδεμένων καταθετικών σας λογαριασμών. Η δυνατότητα αυτή παρέχεται και για τις επιχειρήσεις που χρησιμοποιούν το Internet Banking της Τράπεζας (και ειδικότερα για τις «Θέσεις Εργασίας» που έχουν πρόσβαση σε υπόλοιπα –κινήσεις λογαριασμών).
- **«Κάρτες»**: Για να ενημερωθείτε για την τρέχουσα οφειλή και τις 10 τελευταίες κινήσεις των πιστωτικών σας καρτών Εθνικής Τράπεζας.
- **«Μεταφορές Ποσών»**: Για να μεταφέρετε χρήματα σε λογαριασμούς δικούς σας ή τρίτων στην Εθνική Τράπεζα.
- **«Πληρωμές»**: Για να πληρώσετε οφειλές στις εταιρείες Cosmote και Vodafone καθώς και στις πιστωτικές σας κάρτες Εθνικής Τράπεζας.
- **«Επικοινωνήστε μαζί μας»**, για να επικοινωνήσετε με το Κέντρο Τηλεφωνικής Εξυπηρέτησης (Contact Center) της Τράπεζάς μας.
- **«ΑΤΜ /Κατάστημα»**, για να:
    - Εντοπίσετε τα 10 πλησιέστερα σε σας Καταστήματα ή ΑΤΜ της Εθνικής Τράπεζας,
    - Πληροφορηθείτε τη διεύθυνση των Καταστημάτων ή ΑΤΜ της Εθνικής Τράπεζας που επιθυμείτε.

(Η υπηρεσία εντοπισμού ΑΤΜ/Καταστήματος δεν είναι διαθέσιμη σε κινητά με λειτουργικό σύστημα Windows Mobile®)

<u>i-bank Mobile Banking για ασφάλεια:</u>

Οι συναλλαγές μέσω i-bank Mobile Banking διασφαλίζονται με το ίδιο επίπεδο και τα μέτρα ασφάλειας που παρέχονται και στο Internet Banking, δεδομένου ότι:

- Η τεχνολογία αυτή επιτρέπει τη μεταφορά δεδομένων μέσω του πρωτοκόλλου ασφαλούς επικοινωνίας SSL (Secure Sockets Layer).

- **Η ταυτοποίηση του χρήστη** και η πρόσβασή του στην εφαρμογή i-bank Mobile Banking πραγματοποιείται με τον Κωδικό Εισόδου (UserID) και το Μυστικό Κωδικό (Password). **Η επιπλέον διασφάλιση των εγχρήματων συναλλαγών** στο Internet, Mobile & Phone Banking πραγματοποιείται με κωδικούς μιας χρήσης που παράγονται ηλεκτρονικά από τη συσκευή i-code.
- Επιπλέον, δεν αποθηκεύεται καμία πληροφορία στο κινητό τηλέφωνο.

i-bank Mobile Banking για οικονομία:

Επιλέγοντας να πραγματοποιείτε τις συναλλαγές σας μέσω της Smart Phone συσκευής σας, εξοικονομείτε όχι μόνο χρόνο, αλλά και έξοδα:

- Η πληροφόρηση και οι διαθέσιμες σήμερα συναλλαγές παρέχονται δωρεάν. Ισχύουν μόνο οι χρεώσεις χρήσης του δικτύου του παρόχου.
- Δεν υπάρχουν χρεώσεις από την Τράπεζα για τη εγκατάσταση της εφαρμογής i-bank Mobile Banking.
- Όσον αφορά στη χρήση του Internet / Phone / Mobile Banking (παράδοση ή αντικατάσταση της συσκευής i-code) υπάρχει προνομιακή τιμολόγηση για ορισμένες κατηγορίες πελατών μας:
    - Εάν είστε φοιτητής (προπτυχιακός ή μεταπτυχιακός, ανεξαρτήτως ηλικίας) είναι δωρεάν.
    - Εάν είστε δικαιούχος λογαριασμού Μισθοδοτικού Plus, Επαγγελματικού Plus ή Αγροτικού Plus η χρήση του Internet / Phone / Mobile Banking έχει μειωμένη προμήθεια.

9.1.4 Ασφάλεια

Ακολουθείστε τις παρακάτω συμβουλές ασφαλείας για να προστατευτείτε απο κακόβουλες ενέργειες:

 Βεβαιωθείτε ότι παραλαμβάνετε e-mail από το contact.center@nbg.gr αναζητώντας σε αυτό την ψηφιακή σήμανση (υπογραφή) που σας εγγυάται τον αποστολέα και το περιεχόμενο.

 Η Εθνική Τράπεζα δεν θα σας ζητήσει ποτέ και με κανένα τρόπο (τηλεφωνικώς, μέσω e-mail ή οποιοδήποτε άλλο μέσο επικοινωνίας) τους κωδικούς σας User ID & Password.

 Μην απαντάτε σε e-mail που σας ζητούν προσωπικά σας στοιχεία. Διαγράψτε τα αμέσως. Σε περίπτωση που έχετε ήδη απαντήσει σε τέτοιου είδους μήνυμα και έχετε συμπληρώσει στοιχεία σας, επικοινωνήστε άμεσα με την 24ωρη τηλεφωνική υπηρεσία της Τράπεζας (Help Desk) στα τηλέφωνα: 18 18 18 ή +30 210 48 48 48 4 και μη χρησιμοποιήσετε το Internet Banking της Τράπεζας πριν έλθετε σε επικοινωνία με τα παραπάνω τηλέφωνα.


Μην παρασύρεστε από συνδέσμους (links) που πιστεύετε ότι θα σας οδηγήσουν σε site της Εθνικής Τράπεζας. Πάντα πληκτρολογείτε τη διεύθυνση της ιστοσελίδας μόνοι σας (www.nbg.gr) και όχι μέσω σύνδεσης (link) που πιθανόν σας σταλεί μέσω e-mail ή δημοσιεύεται σε ιστοσελίδες άλλων εταιρειών, μηχανών αναζήτησης κλπ.


Προστατεύστε τον υπολογιστή σας με προγράμματα antivirus και antispyware και φροντίστε για την συχνή ενημέρωσή τους με τις τελευταίες εκδόσεις.
Η πολιτική ασφάλειας που εφαρμόζει η Εθνική Τράπεζα για τη διενέργεια συναλλαγών μέσω i-bank, διασφαλίζει το απόρρητο και απαραβίαστο των συναλλαγών και των προσωπικών σας στοιχείων με τις πιο προηγμένες και πρωτοποριακές μεθόδους:

- Η μυστικότητα και το αναλλοίωτο των δεδομένων στο Internet Banking διασφαλίζονται μέσω του πρωτοκόλλου ασφαλούς επικοινωνίας SSL (Secure Sockets Layer) με ισχυρή κρυπτογράφηση στα 128 bit. Το ίδιο επίπεδο ασφάλειας παρέχεται και στις συναλλαγές μέσω Mobile Banking (για συνδρομητές Cosmote με κινητό τηλέφωνο i -mode®), δεδομένου ότι η τεχνολογία i -mode® επιτρέπει την μεταφορά δεδομένων μέσω του πρωτοκόλλου ασφαλούς επικοινωνίας SSL.
- Η ελεγχόμενη πρόσβαση στα συστήματα της Τράπεζας προστατεύεται από την τελευταία τεχνολογία Firewall.
- Η αυθεντικότητα της Τράπεζας εξασφαλίζεται με το πιστοποιητικό της Verisign, έναν από τους μεγαλύτερους, διεθνούς κύρους, οργανισμούς έκδοσης πιστοποιητικών παρουσίας στο internet.
- Η ταυτοποίηση του χρήστη και η πρόσβασή του στο Internet Banking πραγματοποιείται με τον Κωδικό Χρήστη (UserID) και το Μυστικό Κωδικό (Password). Ειδικά για τη διενέργεια συναλλαγών μέσω τηλεφώνου (Phone Banking) η ταυτοποίηση του χρήστη γίνεται με τον εξαψήφιο, αριθμητικό Κωδικό Εισόδου (UserID) και ένα Κωδικό μιας χρήσης που παράγεται από τη συσκευή i-code. Για περισσότερες πληροφορίες σχετικά με την αποτροπή εισαγωγής μη εξουσιοδοτημένου χρήστη στο σύστημα πιέστε εδώ.
- Η επιπλέον διασφάλιση των εγχρήματων συναλλαγών και συναλλαγών ασφαλείας πραγματοποιείται με κωδικούς μιας χρήσης που παράγει η συσκευή ηλεκτρονικού κλειδαρίθμου (i-code).
- Η διαχείριση παραμέτρων ασφαλείας, μέσω του Internet Banking, επιτρέπει στον χρήστη:
    - Να αλλάζει το Password, όποτε εκείνος επιθυμεί.
    - Να δεσμεύει το Password.
    - Να κλειδώνει τη συσκευή i-code, εάν την έχει χάσει. Επιπλέον, για λόγους μεγαλύτερης ασφάλειας, το σύστημα ζητά αλλαγή Password κάθε δύο μήνες.
- Ειδικά για τις επιχειρήσεις:
    - Η συσκευή i-code για Επιχειρήσεις παρέχει πρόσθετη διασφάλιση με χρήση PIN που ορίζει ο κάτοχος.

Ο καθορισμός εξουσιοδοτημένων χρηστών (Θέσεων Εργασίας) στο Internet Banking, με διαφορετικές ευχέρειες και δικαιώματα

- πρόσβασης, «μεταφέρει» στο Internet Banking την εκπροσώπηση και τους περιορισμούς που υπάρχουν π.χ. στο Καταστατικό ή τον εσωτερικό Κανονισμό της επιχείρησης.

- Ο Διαχειριστής Θέσεων Εργασίας, καθορίζει και διαχειρίζεται τις ευχέρειες όλων των Θέσεων Εργασίας από οποιοδήποτε σημείο υπάρχει πρόσβαση στο internet, χωρίς τη διαμεσολάβηση της Τράπεζας. Επιπλέον, έχει πλήρη εποπτεία της χρήσης του Internet Banking, δηλ. των κινήσεων που γίνονται από τις Θέσεις Εργασίας.

Η Αυθεντικότητα της Τράπεζας

Η Εθνική Τράπεζα έχει προμηθευτεί πιστοποιητικό αυθεντικότητας παρουσίας της στο Διαδίκτυο από τη Verisign, έναν από τους μεγαλύτερους, διεθνούς κύρους, Οργανισμούς έκδοσης πιστοποιητικών παρουσίας στο Διαδίκτυο. Το πιστοποιητικό εμφανίζεται στο χρήστη κάθε φορά που επισκέπτεται τη Login σελίδα του Internet Banking και είναι διαθέσιμο όσο ο χρήστης χρησιμοποιεί την εφαρμογή, με τις παρακάτω μορφές:

Για χρήστες Internet Explorer 6 και παλαιότερες εκδόσεις του, σαν κλειδαριά  στο κάτω τμήμα της οθόνης.
Για χρήστες Internet Explorer 7 ή Firefox 2 και νεότερες εκδόσεις τους στη μπάρα ηλεκτρονικής διεύθυνσης με τη μορφή: 

αν εισέρχεστε στο νέο Internet Banking μέσω της ιστοσελίδας www.nbg.gr , ή με τη μορφή 

αν εισέρχεστε στο Internet Banking μέσω της διεύθυνσης http://homebank.nbg.gr/. Για τους κανόνες ελέγχου της αυθεντικής ιστοσελίδας της Τράπεζας, στην περίπτωση αυτή, πιέστε εδώ.

Σε κάθε εισαγωγή σας στο Internet Banking (πριν δηλ. από την εισαγωγή των προσωπικών σας κωδικών στη Login σελίδα) είτε μέσω της ιστοσελίδας http://www.nbg.gr (νέο Internet Banking) είτε μέσω της παλαιάς ιστοσελίδας http://homebank.nbg.gr (προσωρινά ακόμη διαθέσιμη), θα πρέπει να βεβαιώνεστε ότι έχετε συνδεθεί με τον πραγματικό δικτυακό τόπο (Web Site) της Τράπεζας, γεγονός που επιβεβαιώνεται με την ύπαρξη των αντίστοιχων ψηφιακών πιστοποιητικών:
Χρησιμοποιείστε τα προγράμματα περιήγησης στο Διαδίκτυο (Internet browsers) που αναγνωρίζουν τις αυξημένες δυνατότητες των νέων ψηφιακών πιστοποιητικών (π.χ. Internet Explorer 7), τα οποία παρέχονται δωρεάν.
Ακολουθείτε πάντα τους κανόνες αυθεντικότητας της ιστοσελίδας.

Ασφάλεια στον υπολογιστή σας

Οι προσπάθειες υποκλοπής προσωπικών κωδικών και προσωπικών δεδομένων στρέφονται κυρίως σε χρήστες που δεν λαμβάνουν τα κατάλληλα μέτρα προστασίας του υπολογιστή τους. Η ύπαρξη & διάδοση ιών είναι μια πραγματικότητα στο Διαδίκτυο. Είναι απαραίτητο λοιπόν, το PC

με το οποίο ο χρήστης συνδέεται στο Internet να διαθέτει πρόγραμμα ελέγχου ιών (antivirus). Επίσης, ο χρήστης θα πρέπει να ελέγχει ότι το antivirus του υπολογιστή είναι ενεργοποιημένο και ενημερωμένο. Καλό θα ήταν η ενημέρωση του antivirus να γίνεται αυτόματα κάθε φορά που επιτυγχάνεται σύνδεση με το Internet.
Τα λειτουργικά συστήματα και τα προγράμματα πλοήγησης στο Διαδίκτυο έχουν αδυναμίες ασφάλειας και δίνουν τη δυνατότητα σε άλλους «κακούς» χρήστες του Διαδικτύου να υποκλέπτουν πληροφορίες από τον υπολογιστή σας. Ενημερωθείτε από τις σελίδες των αντίστοιχων εταιρειών για τους τρόπους προστασίας που προτείνουν για τα προϊόντα τους. Είναι απαραίτητο να ενημερώνετε το λειτουργικό σας και όλα τα προγράμματα με τις τελευταίες ενημερώσεις ασφάλειας που δημοσιεύουν οι κατασκευάστριες εταιρείες.

Η επιπλέον διασφάλιση των εγχρήματων συναλλαγών και συναλλαγών ασφαλείας

Κάθε χρήστης Internet /Phone /Mobile Banking παραλαμβάνει τη συσκευή Ηλεκτρονικού Κλειδαρίθμου (i-code), που παράγει κωδικούς μιας χρήσης. Με την εισαγωγή ενός κωδικού i-code πιστοποιείται ότι κάθε συναλλαγή προέρχεται πράγματι από τον κάτοχο συγκεκριμένης συσκευής, ενώ η ισχύς κάθε κωδικού είναι μόλις 32’’, με την παρέλευση των οποίων ακυρώνεται και δεν μπορεί να χρησιμοποιηθεί. Το γεγονός αυτό καθιστά αδύνατη την υποκλοπή κωδικών από τρίτους, για μεταγενέστερη χρήση (π.χ. περιπτώσεις phising).
Μετά τη διεκπεραίωση της συναλλαγής εμφανίζεται στην οθόνη του Internet Banking ένας τριψήφιος Κωδικός Επιβεβαίωσης, ο οποίος πρέπει να είναι ίδιος με τον τριψήφιο Κωδικό που παράγεται, στη συνέχεια, από τη συσκευή i-code.
Η παραγωγή των κωδικών i-code βασίζεται στον ισχυρό αλγόριθμο κρυπτογράφησης 3DES. Ο αλγόριθμος αυτός είναι πρακτικά απαραβίαστος, το δε επίπεδο ασφαλείας που παρέχει πιστοποιείται από διεθνείς οργανισμούς.

9.2 Υπηρεσίες e-banking Ελληνικής Τράπεζα

9.2.1 Περιγραφή

Η Υπηρεσία Ηλεκτρονικής τράπεζας έχει σχεδιαστεί με στόχο την όσο το δυνατόν μεγαλύτερη ευκολία στην πρόσβαση και παρουσίαση των δεδομένων που ενδιαφέρουν γι' αυτό και η πλοήγηση είναι απλή και κατανοητή για τους πελάτες της Ελληνικής Τράπεζας που επιθυμούν να πληροφορούνται για την κίνηση των λογαριασμών τους σε πραγματικό χρόνο και να εκτελούν τις τραπεζικές τους συναλλαγές άμεσα, ολόκληρο το εικοσιτετράωρο, οπουδήποτε και αν βρίσκονται, Κύπρο ή στο εξωτερικό.
Οι διαθέσιμες δραστηριότητες είναι διαχωρισμένες σε πέντε κατηγορίες για μεγαλύτερη ταχύτητα στην επιλογή του χρήστη καθ΄ όλη την διάρκεια της σύνδεσης με την Ηλεκτρονική Τράπεζα.
Οι κατηγορίες αυτές είναι:

- Τραπεζικά : Παρουσίαση και εκτέλεση οικονομικών συναλλαγών από τον υπολογιστή ή το κινητό τηλέφωνο του χρήστη. Τέτοιες συναλλαγές είναι η μεταφορά χρημάτων εντός και εκτός Κύπρου, πληρωμές σε Υπηρεσίες της Ελληνικής Τράπεζας και άλλους Οργανισμούς στην Κύπρο, δημιουργία Πάγιων εντολών, παρουσίαση υπολοίπων και

αναλυτική κατάσταση λογαριασμών και η δημιουργία / διατήρηση πρωτοποριακών προϊόντων που έχουν σχεδιαστεί αποκλειστικά για τους χρήστες της Ηλεκτρονικής τράπεζας.

- Ταχυδρομείο
- Ασφαλής ανταλλαγή ηλεκτρονικών μηνυμάτων με την Ελληνική Τράπεζα για ταχύτερη εξυπηρέτηση.
- Ειδοποίηση
- Προετοιμασία και ρύθμιση συγκεκριμένων μηνυμάτων για αποστολή τους απο την
- Ηλεκτρονική τράπεζα στο κινητό του χρήστη για άμεση πληροφόρηση στην διαφοροποίηση των υπολοίπων των λογαριασμών του.
- Ρυθμίσεις :Παρακολούθηση προσωπικών δεδομένων του χρήστη με την Ηλεκτρονική τράπεζα και αντικατάσταση / ρύθμιση προσωπικών κωδικών έγκρισης / Συσκευής Digipass για σκοπούς εκτέλεσης οικονομικών συναλλαγών.
- Βοήθεια : Καθ' όλη την διάρκεια της σύνδεσης με την Ηλεκτρονική Τράπεζα, ο χρήστης έχει την δυνατότητα πρόσβασης σε κείμενα με περισσότερες λεπτομέρειες και πληροφορίες που αφορούν τις διαθέσιμες δραστηριότητες της Υπηρεσίας αυτής.

9.2.2 Χαρακτηριστικά

Χαρακτηριστικά e-banhing:

- Υπόλοιπα λογαριασμών, τόκοι, επιτόκια, λεπτομέρειες λογαριασμών.
- Αναλυτική κατάσταση Λογαριασμών με λεπτομέρειες συναλλαγών πέραν των πέντε χρόνων
- Εκτύπωση και φύλαξη των υπολοίπων και κατάστασης των λογαριασμών σε αρχείο.
- Μεταφορές χρημάτων εντός και εκτός Κύπρου
- Δημιουργία και παρακολούθηση Πάγιων Εντολών
- Δημιουργία και παρακολούθηση εικονικών καρτών για χρήση από το διαδύκτιο (Net Secure)
- Δημιουργία Ηλεκτρονικού λογαριασμού (Net Account) με ή χωρίς όριο με ευνοϊκότερο επιτόκιο
- Δημιουργία Ηλεκτρονικού λογαριασμού προθεσμίας (Net Fixed) με ευνοϊκότερο επιτόκιο
- Παρακολούθηση των υφιστάμενων λογαριασμών προθεσμίας
- Αίτηση για Ηλεκτρονικό Δάνειο (Net Loan) με ευνοϊκότερο επιτόκιο
- Υπόλοιπα λογαριασμών, Κατάσταση Λογαριασμών, μεταφορές χρημάτων, Τιμές συναλλάγματος κλπ μέσω κινητού τηλεφώνου (NetSMS)
- Τιμές Συναλλάγματος για περίοδο πέραν των πέντε χρόνων
- Ασφαλής επικοινωνία με την Ελληνική Τράπεζα (Bank Mail)
- Δημιουργία και παρακολούθηση Ειδοποίησης (Alerts)
- Παραγγελίας Βιβλιαρίου Επιταγών)
- Παρακολούθηση επιταγών που έχουν παρουσιαστεί στην τράπεζα για πληρωμή
- Ανάκληση Επιταγών

- Βοήθεια Χρήστη

9.2.3 Εγγραφή

Για εγγραφή στην Υπηρεσία Ηλεκτρονικής Τράπεζας χρειάζεται να συμπληρωθεί η αίτηση εγγραφής η οποία είναι διαθέσιμη στην ιστοσελίδα της υπηρεσίας ή σε οποιοδήποτε κατάστημα. Με την υπογραφή της συμφωνίας για εγγραφή στην Ηλεκτρονική Τράπεζα, ο χρήστης προμηθεύεται με προσωπικούς κωδικούς πρόσβασης για πρόσβαση στους λογαριασμούς που έχει ζητήσει να παρακολουθεί μέσω διαδυκτίου.
Εάν ο χρήστης επιθυμεί να εκτελεί μεταφορές χρημάτων από την Ηλεκτρονική τράπεζα με μεγάλα ποσά, τότε για σκοπούς επιπρόσθετης ασφάλειας στις συναλλαγές του θα πρέπει να προμηθευτεί από την τράπεζα του και να χρησιμοποιεί την συσκευή Digipass.
Σύμφωνα με τους γενικούς κανονισμούς της τράπεζας και τις νομοθεσίες της Κυπριακής Δημοκρατίας, η διαδικασία εγγραφής στην Ηλεκτρονική τράπεζα ολοκληρώνεται εφόσον όλα τα απαραίτητα έντυπα φέρουν την πρωτότυπη υπογραφή του / των προσώπων που αναφέρονται στην συγκεκριμένη εγγραφή.

9.2.4 Προϋποθέσεις πρόσβασης

Η σύνδεση με την Ηλεκτρονική Τράπεζα επιτυγχάνεται εφόσον υπάρχει σύνδεση του υπολογιστή με το διαδύκτιο. Για την μεγαλύτερη δυνατή ασφάλεια, η πρόσβαση στην Υπηρεσία επιτυγχάνεται με τις ακόλουθες προϋποθέσεις:

- Ταχύτητα διασύνδεσης με το διαδύκτιο τουλάχιστον 28.8kps.

- Ανάλυση χρωμάτων οθόνης (Resolution) 1024x768 για μεγαλύτερη ταχύτητα και ευκρίνεια στην παρακολούθηση των δεδομένων.

Υπολογιστές με λειτουργικό λογισμικό (Operating System) Microsoft :

- Λογισμικό πλοήγησης στο διαδύκτιο (Internet Browser) - Microsoft Internet Explorer 5.5+ ή Netscape 6+, με κρυπτογράφηση 128 Bit.
- Επεξεργαστής (processor) Πέντιουμ III (Pentium III) με μνήμη τουλάχιστον 128MB (Ram).\

Υπολογιστές Macintosh:
- Λειτουργικό Λογισμικό - Mac OS 8.6+ Επεξεργαστής (Processor) - G3+ με μνήμη τουλάχιστον 128MB (Ram).
- Λογισμικό πλοήγησης στο διαδύκτιο (Internet Browser) –Netscape communicator 4.72+ and Netscape Navigator 6+, με κρυπτογράφηση 128 Bit.

9.2.5 Ασφάλεια

Η Υπηρεσία Ηλεκτρονικής Τράπεζας διατηρεί ψηλό επίπεδο ασφαλείας με λογισμικά που υποστηρίζουν ψηλά επίπεδα κρυπτογράφησης (Data Encryption) και λογισμικά Firewalls τελευταίας τεχνολογίας για την διαφύλαξη της εμπιστευτικότητας των προσωπικών δεδομένων των πελατών της τράπεζας και έχει εφαρμόσει την τεχνολογία Digipass για ακόμη μεγαλύτερη ασφάλεια στις συναλλαγές μέσω διαδυκτίου.
Η συσκευή 'Digipass' είναι μικρή σε μέγεθος και μπορεί να μεταφερθεί και πάνω στο μπρελόκ των κλειδιών σας. Δεν χρειάζεται καμία εγκατάσταση λογισμικού ή οποιασδήποτε συσκευής στον υπολογιστή σας. Λειτουργεί με μπαταρία και έχει ζωή 3-5 χρόνια, ανάλογα με την χρήση του. Όταν αυτό τεθεί εκτός λειτουργίας, η μπαταρία δεν μπορεί να αντικατασταθεί και θα πρέπει να προμηθευτεί ο χρήστης άλλη συσκευή από οποιοδήποτε κατάστημα της τράπεζας.
Η λειτουργία της συσκευής είναι απλή. Με το πάτημα ενός κουμπιού και για διάρκεια 20 δευτερολέπτων, εμφανίζεται στην οθόνη της ένας μοναδικός εξαψήφιος κωδικός. Θα πρέπει να εισαχτεί ο αριθμός αυτός στο ανάλογο πεδίο που παρέχεται, για έγκριση της συναλλαγής που επιθυμεί ο πελάτης σε συνδυασμό πάντοτε με τον μοναδικό κωδικό έγκρισης (Authorisation PIN) που έχει ήδη δοθεί από την τράπεζα.
Είναι ευθύνη των χρηστών της Ηλεκτρονικής Τράπεζας για την ασφαλή φύλαξη των προσωπικών κωδικών πρόσβασης τους, οι οποίοι είναι το εισιτήριο εισόδου τους στην Υπηρεσία. Η τράπεζα δεν θα σας ζητήσει ποτέ τον Κωδικό Πρόσβασης ή τον Κωδικό Έγκρισης μέσω τηλεφώνου, ηλεκτρονικού μηνύματος, ή μέσω οποιασδήποτε γραπτής επικοινωνίας.

9.3 E-banking τράπεζας Κύπρου (1bank)

9.3.11bank

Η Υπηρεσία **1bank** προσφέρεται δωρεάν, τόσο σε Ιδιώτες όσο και Επιχειρήσεις, 24*7 στο Τηλέφωνο και στο διαδίκτυο.
1bank προσφέρει :

1. Μεταφορές Χρημάτων
2. Υπόλοιπα Λογαριασμών
3. Συναλλαγές Λογαριασμών
4. Παραγγελία Βιβλιαρίου Επιταγών
5 .Παραγγελία Κατάστασης Λογαριασμών
6. Εντολή για Μη Πληρωμή Επιταγών
7 .Πληρωμή λογαριασμών οργανισμών κοινής ωφελείας

9.3.2 Χρεώσεις ebanking Τράπεζας Κύπρου

Υπηρεσία	Χρέωση Μέσω Καταστημάτων	**Χρέωση Μέσω 1bank**
Μεταφορές από λογαριασμούς με προειδοποίηση (κατ.05&06)	Μέχρι € 2.000 ανάληψη μια φορά το μήνα χωρίς χρέωση. 2% χρέωση στο	**Μέχρι € 1.000 ΗΜΕΡΗΣΙΩΣ χωρί**

	ποσό ανάληψης χωρίς προειδοποίηση.	**χρέωση και χωρίς προειδοποίηση ΔΩΡΕΑΝ**
Εξόφληση λογαριασμών κοινής ωφελείας	€ 0,85	**ΔΩΡΕΑΝ**
Μεταφορές μεταξύ δύο λογαριασμών στο ίδιο ξένο νόμισμα εντός Κύπρου (μεταξύ λ/σμών Τρ. Κύπρου ίδιου πελάτη)	€ 1,70	**ΔΩΡΕΑΝ**
Μεταφορές μεταξύ δύο λογαριασμών στο ίδιο ξένο νόμισμα εντός Κύπρου (σε λογ/σμό Τρ. Κύπρου άλλου πελάτη)	€ 5	**ΔΩΡΕΑΝ**
Επανέκδοση κατάστασης λογαριασμού	€ 2,50 - 5,00	**ΔΩΡΕΑΝ**
Παραγγελία κατάστασης λογαριασμού για Κάρτες	€ 3,40	**ΔΩΡΕΑΝ**
Οδηγία ακύρωσης πληρωμής επιταγής	€ 6,80 - 17,00	**ΔΩΡΕΑΝ**
Έκδοση πιστοποιητικού τόκων	€ 3,40	**ΔΩΡΕΑΝ**
Έκδοση πιστοποιητικού τόκων ΟΧΤΚ	€ 1,70	**ΔΩΡΕΑΝ**
Άνοιγμα τραπεζικών εντολών για πίστωση άλλου λογαριασμού	€ 6,80	**ΔΩΡΕΑΝ**
Αρχείο Ψηφιακής Εικόνας Επιταγών	€ 3,40 - € 17 Για αντίγραφο επιταγής.	**ΔΩΡΕΑΝ από το Int Banking μέχρι και 6 πίσω (ισχύει μόνο γι ιδιώτες)**
Παραγγελία βιβλιαρίου επιταγών	€ 10,00	**€ 6,80**
Μεταφορά χρημάτων σε άλλες τράπεζες JCC/SEPA/SWIFT (*) ***Regulated payments**	Ποσά μέχρι €1,000 : €5 Ποσά από €1001 - €50,000 : €12	**Ποσά μέχρι €1,000 :** **Ποσά από €1001 - €5** **: €6**
Επανέκδοση Κάρτας λόγω φθοράς	€ 8,50 (πλην Platinum)	**€ 5**
Επανέκδοση Κάρτας λόγω απώλειας / κλοπής	€ 8,50 (πλην Platinum) Μη παραλαβή ανανέωσης και υπόθεση FRAUD δεν χρεώνεται	**€ 5**
Έκδοση Μυστικού Κωδικού για Κάρτες	€ 8,50 (Πλην Platinum) Μη παραλαβή κωδικού δεν χρεώνεται	**€ 5**
Αγορά τηλεκαρτών So-easy (χωρίς επιπρόσθετη επιβάρυνση)	N/A	**€5, €10, €20, €35**

(*) ***Regulated Payment*** είναι όταν:

1. Η αποστέλλουσα και παραλαμβάνουσα Τράπεζα βρίσκονται σε χώρα μέλος της Ευρωπαϊκής Ένωσης ή στις χώρες Ισλανδία, Λίχτενσταϊν, Μονακό, Νορβηγία, Ελβετία, Βατικανό και Σαν Μαρίνο. Επιπρόσθετα καλύπτονται και οι περιοχές Martinique, Guadeloupe, French Guiana, Reunion, Gibraltar, Azores, Madeira, Canary Islands, Ceuta and Melilla and Aland Islands.

2. Το νόμισμα του εμβάσματος είναι Ευρώ.
3. Το ποσό του εμβάσματος είναι μέχρι €50.000.
4. Υπάρχει ορθό IBAN δικαιούχου και ορθό BIC για την Τράπεζα του δικαιούχου.
5. Η ένδειξη για χρέωση των εξόδων είναι για εντολέα και δικαιούχο "SHA".
6. Η ημερομηνία αξίας είναι μεταγενέστερη της ημερομηνίας εκτέλεσης

9.3.3 Τηλεφωνική τράπεζα

Η Τηλεφωνική Τράπεζα σας παρέχει την ευκαιρία να πραγματοποιείτε όλες σας τις τραπεζικές συναλλαγές μέσω τηλεφώνου. Μπορείτε να το κάνετε αυτό είτε με την βοήθεια ενός Λειτουργού εξυπηρέτησης είτε μέσω του Αυτοματοποιημένου Συστήματος εξυπηρέτησης χρησιμοποιώντας το πληκτρολόγιο του τηλεφώνου σας.

Οι λειτουργίες που προσφέρονται μέσω του τηλεφώνου είναι:

1. Λειτουργίες με τη βοήθεια Λειτουργού Εξυπηρέτησης (Υπόλοιπα Λογαριασμών, Κινήσεις λογαριασμών, Μεταφορές Χρημάτων)
2. Παραγγελία Κατάστασης Λογαριασμού
3. Πληροφορίες πληρωμής επιταγών
4. Παραγγελία Βιβλιαρίου επιταγών
5. Εντολή για να σταματήσει η πληρωμή μιας επιταγής
6. Πληρωμή Λογαριασμών
7. Εντολή για άνοιγμα αυτόματης τραπεζικής εντολής
8. Στατιστικά στοιχεία

9.3.4 Συναλλαγές μέσω κινητού τηλέφωνου

Με το mobile banking της τράπεζας Κύπρου, μπορείτε να διεκπεραιώσετε τραπεζικές συναλλαγές και να πάρετε πληροφορίες για τους λογαριασμούς σας χρησιμοποιώντας την τεχνολογία WAP.

Οι λειτουργίες που προσφέρονται μέσω του κινητού τηλεφώνου είναι:

1. Πληρωμή λογαριασμών
2. Υπόλοιπα Λογαριασμών
3. Μεταφορές χρημάτων μεταξύ των λογαριασμών σας
4. Μεταφορές σε λογαριασμούς τρίτων ατόμων
5. Οδηγίες για μη πληρωμή επιταγής
6. Τιμές Μετοχών
7. Πληροφορίες Ξένου Συναλλάγματος

Όλες οι πιο πάνω λειτουργίες προσφέρονται σε Συνδρομητές. Πελάτες μη Συνδρομητές μπορούν να έχουν πρόσβαση όσον αφορά μόνο Τιμές Μετοχών και Πληροφορίες Συναλλάγματος.

Τι είναι το WAP;

WAP (Wireless Application Protocol) είναι η υπηρεσία η οποία επιτρέπει την πρόσβαση στο Διαδίκτυο, μέσω κινητού τηλεφώνου. Μέχρι τώρα η σύνδεση στο Διαδίκτυο ήταν εφικτή μόνο μέσω Ηλεκτρονικών Υπολογιστών.Η Υπηρεσία αυτή επιτρέπει την εμφάνιση πληροφοριών σε οθόνες κινητών τηλεφώνων.

Πως να θέσετε σε λειτουργία το WAP;

1. Βεβαιωθείτε ότι το κινητό σας τηλέφωνο υποστηρίζει τη λειτουργία αυτή
2. Βάλτε τις ρυθμίσεις στο κινητό σας ανάλογα με τον παροχέα της υπηρεσίας WAP που θέλετε.
3. Επιλέξτε από την λίστα τον παροχέα σας για να βρείτε τις πληροφορίες που χρειάζονται με σκοπό την ενεργοποίηση του WAP στο κινητό σας.

Για την εταιρία LOGOSNET: **http://wireless.logosnet.cy.net/mobile/mobile.html**

Για την εταιρία SPIDERNET: **http://www.spidernet.net**

Για την εταιρία CYTANET: **http://www.cytanet.com.cy/wap/english.html**

Για την εταιρία AVACOMNET: www.avacom.net/wap/index.html

Πως να χρησιμοποιείτε την Υπηρεσία WAP
Αφού συνδεθείτε με τον παροχέα σας θα δείτε τις πιο κάτω λειτουργίες. Τις οποίες και μπορείτε να χρησιμοποιήσετε:

1. Banking Services (Τραπεζικές Υπηρεσίες) - Διαθέσιμες μόνο σε Συνδρομητές
2. Shares (Μετοχές)
3. Exchange Rates (Τιμές Συναλλάγματος)
4. Branch and ATM Locations

[Banking Services - Τραπεζικές Υπηρεσίες]
Διαλέγοντας Τραπεζικές Υπηρεσίες, αυτόματα σας ζητά του πιο κάτω κωδικούς αριθμούς:

1. Balances
2. Account Information
3. Funds Transfer
4. Payments
5. Insurance Info
6. Account Services
7. Other Services

2. Μετοχές

Υπάρχουν δύο επιλογές:

- Όλες - Μπορείτε να δείτε όλες τις μετοχές
- Συγκεκριμένη Μετοχή - Μπορείτε να επιλέξετε συγκεκριμένη μετοχή για να δείτε την τιμή της

3. Τιμές Συναλλάγματος

Μπορείτε να δείτε τις τιμές αγοράς και πώλησης των μεγαλύτερων νομισμάτων σε σχέση με το euro.

4. [Branches and ATM Locations]

Θα βρείτε πληροφορίες αναφορικά με τις τοποθεσίες που βρίσκονται τα καταστήματα και ATMs του Συγκροτήματος της Τράπεζας Κύπρου.

9.3.5 Συσκευή Digipass

Η Τράπεζα Κύπρου στα πλαίσια της συνεχούς αναβάθμισης της ασφάλειας στη χρήση των καναλιών του 1bank, έχει εισάξει ένα ακόμα επίπεδο ασφάλειας στις συναλλαγές χρηστών του 1bank προς τρίτους.
Το νέο επίπεδο ασφάλειας αποτελεί η χρήση της συσκευής Digipass για τη διενέργεια μεταφορών σε τρίτους μέσω των καναλιών του 1bank (διαδικτύου και τηλεφώνου).
Η συσκευή Digipass παράγει δυναμικούς Μυστικούς Κωδικούς Αριθμούς μιας χρήσης, που χρησιμοποιούνται πέραν του User ID και του σταθερού Κωδικού Ασφαλείας.
Η εφαρμογή της τεχνολογίας Digipass δίνει νέα υπόσταση στην ασφάλεια της Ηλεκτρονικής Τράπεζας, χωρίς την ανάγκη εγκατάστασης νέων προγραμμάτων ή συστημάτων στους Ηλεκτρονικούς Υπολογιστές των χρηστών.
Υπάρχουν 2 είδη ηλεκτρονικών συσκευών δημιουργίας δυναμικών μυστικών κωδικών Digipass οι οποίες είναι φιλικές στη χρήση και λειτουργούν με μπαταρία διάρκειας 3-5 ετών (σε περίπτωση που η μπαταρία τελειώσει θα πρέπει να προμηθευτείτε με νέα συσκευή):

1. Η συσκευή **Digipass 0550** που προσφέρεται ήδη από την Τράπεζα Κύπρου για πρόσβαση στα κανάλια του 1bank, για διενέργεια μεταφορών σε τρίτους ή για οδηγίες μέσω φάξ στο κατάστημα

2. Η συσκευή **Digipass Go 3** χρησιμοποιείται για διενέργεια μεταφορών σε τρίτους μόνο.

Επισημαίνεται ότι η χρήση της συσκευής Digipass (οποιασδήποτε εκ των δύο) είναι απαραίτητη για τη διενέργεια μεταφορών σε τρίτους (εξαιρούνται οι πληρωμές λογαριασμών κοινής ωφελείας)

1. Digipass Go 3

Η συσκευή είναι μικρή και ελαφριά και μπορείτε να την έχετε πάντα μαζί σας χρησιμοποιώντας την και σαν μπρελόκ. Δημιουργεί δυναμικούς κωδικούς πρόσβασης μιας χρήσης με το πάτημα ενός κουμπιού.
Χρησιμοποιείται μόνο για συναλλαγές (πληρωμές, μεταφορές, κλπ) σε τρίτους, σε συνδυασμό με το User ID σας και τον Κωδικό Ασφαλείας.
Με τη χρήση της συσκευής διασφαλίζετε ότι, ακόμα και αν οι κωδικοί πρόσβασης σας (User ID και Κωδικός Ασφαλείας) περιέλθουν εις γνώση κάποιου τρίτου, είναι αδύνατον να διενεργηθεί

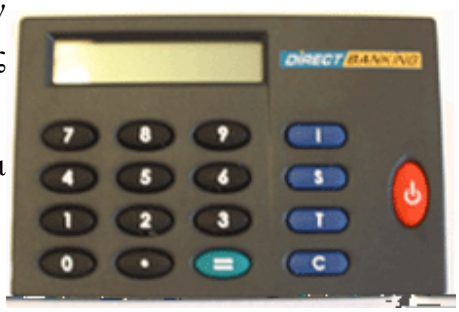
οποιαδήποτε συναλλαγή σε όφελος τρίτου από τους λογαριασμούς σας χωρίς την καταχώριση του δυναμικού κωδικού μιας χρήσης, που παράγεται από τη συσκευή Digipass.
Σημειώνεται ότι αν χάσετε τη συσκευή σας, δεν μπορεί κάποιος τρίτος να τη χρησιμοποιήσει αν δεν γνωρίζει το User ID και τον Κωδικό Ασφαλείας σας. Η συσκευή είναι προσωπική και δεν μπορεί να χρησιμοποιηθεί από άλλο χρήστη.
Το κόστος της συσκευής είναι € 10. Μπορείτε να την προμηθευτείτε συμπληρώνοντας την αίτηση Digipass.

Οδηγίες χρήσης Digipass Go 3

1. Ενωθείτε με το 1bank (Διαδίκτυο ή Τηλέφωνο), ετοιμάστε την συναλλαγή σας (μεταφορά χρημάτων προς τρίτους) και πατήστε "Submit".
2. Το σύστημα θα σας ζητήσει κωδικό.
3. Πατήστε το κουμπί στο Digipass Go 3 και χρησιμοποιήστε τον εξαψήφιο κωδικό που θα εμφανιστεί στην οθόνη σας.
4. Επαναλάβετε κάθε φορά που θα διενεργήσετε καινούρια συναλλαγή.

2. Digipass 0550

Η συσκευή είναι σαν μια μικρή υπολογιστική μηχανή 2" x 3". Για να ενεργοποιηθεί, χρειάζεται ένας 5ψήφιος κωδικός ο οποίος δίδεται αρχικά από την Τράπεζα αλλά στη συνέχεια εσείς καθορίζετε το δικό σας κωδικό πρόσβασης στη συσκευή.



Η συσκευή παράγει δυναμικούς κωδικούς μιας χρήσης και δεν μπορεί να χρησιμοποιηθεί από άλλο χρήστη.

Μπορεί να χρησιμοποιηθεί από τον χρήστη:

- για πρόσβαση(sign-on) στα κανάλια του 1bank (Internet Banking & Τηλεφωνική Τράπεζα).
- για διενέργεια μεταφορών σε τρίτους μέσω 1bank.
- Επίσης μπορεί να χρησιμοποιηθεί για οδηγίες μέσω φαξ (σε συνεννόηση πάντα με το κατάστημα σας).

Το κόστος της συσκευής είναι €40. Μπορείτε να την προμηθευτείτε συμπληρώνοντας την αίτηση Digipass.

ΑΡΧΙΚΟΣ ΜΥΣΤΙΚΟΣ ΚΩΔΙΚΟΣ (PIN) ΓΙΑ ΤΗΝ ΣΥΣΚΕΥΗ

Πριν να χρησιμοποιήσετε τη συσκευή σας θα πρέπει να αλλάξετε το PIN σας ως εξής:

1. Πατήστε το START. Στην οθόνη της συσκευής θα εμφανιστεί το μήνυμα "INITIAL PIN" (Αρχικός Προσωπικός Κωδικός Αριθμός)
2. Πληκτρολογήστε τον Αρχικό Προσωπικό Κωδικό Αριθμό που σας στάληκε με τη συσκευή και πατήστε "=" . Στην οθόνη θα αναγράφεται το μήνυμα "NEW PIN" (Νέος Προσωπικός Κωδικός Αριθμός)
3. Καταχωρήστε ένα νέο 5ψήφιο αριθμό και πατήστε το "=". Στην οθόνη θα αναγράφεται το μήνυμα "REPEAT PIN" (Επαναλάβετε τον 5ψήφιο αριθμό). (Σημ. Η συσκευή δεν

επιτρέπει την καταχώρηση αριθμών σε συνδυασμούς οι οποίοι εμπερικλείουν κινδύνους πχ 12345, 11111 κτλ)

4. Καταχωρήστε ξανά τον 5ψήφιο κωδικό αριθμό που έχετε επιλέξει και πατήστε "=". Στην οθόνη θα σας δοθεί το μήνυμα "OK" (η αλλαγή του Προσωπικού Κωδικού σας αριθμού έγινε με επιτυχία).

ΠΑΡΑΓΩΓΗ ΚΩΔΙΚΟΥ ΑΡΙΘΜΟΥ (PIN) ΓΙΑ ΧΡΗΣΗ ΣΤΗΝ ΥΠΗΡΕΣΙΑ 1bank (ΠΡΟΣΒΑΣΗ Ή ΜΕΤΑΦΟΡΕΣ)

1. Από τώρα και στο εξής κάθε φορά που πατάτε το START θα εμφανίζονται στην οθόνη τα ψηφία "I, S, T".
2. Πατήστε το "I". Στην οθόνη θα εμφανιστεί το μήνυμα "YOUR PIN".
3. Καταχωρήστε τον 5ψήφιο κωδικό αριθμό σας και πατήστε "=".
4. Η συσκευή θα σας δώσει ένα 6ψήφιο κωδικό αριθμό τον οποίο θα πρέπει να καταχωρήσετε είτε στο πεδίο "Passcode" στην αρχική σελίδα της Υπηρεσίας μας στο internet είτε στο πεδίο "Digipass Code" κατά τη διάρκεια κάποιας συναλλαγής σας. Ο κάθε 6ψήφιος αριθμός μπορεί να χρησιμοποιηθεί μόνο 1 φορά για αυτό θα πρέπει να επαναλάβετε αυτή τη διαδικασία κάθε φορά που θέλετε να χρησιμοποιήσετε αυτές τις υπηρεσίες.

ΠΑΡΑΓΗ ΚΩΔΙΚΟΥ ΑΡΙΘΜΟΥ (PIN) ΓΙΑ ΑΠΟΣΤΟΛΗ ΟΔΗΓΙΩΝ ΓΙΑ ΕΜΒΑΣΜΑΤΑ (PAYMENT ORDERS) ΜΕΣΩ ΦΑΞ

Παρακαλώ βεβαιωθείτε ότι έχετε υπογράψει τα σχετικά έντυπο (Fax Indemnity) πριν να χρησιμοποιήσετε αυτή την υπηρεσία.

1. Πατήστε το START. Στην οθόνη θα εμφανιστούν τα ψηφία "I, S, T".
2. Πατήστε το "S". Στην οθόνη θα δείτε το μήνυμα "Your PIN". Καταχωρήστε τον 5ψήφιο κωδικό σας αριθμό και πατήστε "=".
3. Η οθόνη θα εμφανίσει το σύμβολο "_". Πληκτρολογήστε το ποσό που θέλετε να μεταφέρετε, χωρίς δεκαδικούς αριθμούς (πχ 200 όχι 200.00) και μετά πατήστε 2 φορές το "=" .
4. Η συσκευή θα σας δώσει τον 6ψήφιο κωδικό αριθμό τον οποίο θα πρέπει να καταχωρήσετε μαζί με το User ID σας, το ποσό και την ημερομηνία όταν θα στείλετε τις οδηγίες στο κατάστημα σας μέσω φαξ. Επαναλάβετε τη διαδικασία κάθε φορά που θα στείλετε καινούργιες οδηγίες.

ΑΛΛΑΓΗ 5ΨΗΦΙΟΥ ΠΡΟΣΩΠΙΚΟΥ ΚΩΔΙΚΟΥ ΑΡΙΘΜΟΥ (PIN)

1. Πατήστε το START. Στην οθόνη θα εμφανιστούν τα ψηφία "I, S, T". Πατήστε το "T". Η οθόνη θα εμφανίσει "CHANGE PIN?".
2. Πατήστε το "=". Στην οθόνη θα αναγράφετε το μήνυμα "YOUR PIN".
3. Καταχωρήστε τον 5ψήφιο Προσωπικό Κωδικό Αριθμό που είχατε μέχρι σήμερα και πατήστε το "=".
4. Στην οθόνη θα εμφανιστεί το μήνυμα "NEW PIN". Καταχωρήστε τον νέο 5ψήφιο Προσωπικό Κωδικό Αριθμό σας.
5. Η συσκευή θα σας ζητήσει να καταχωρήσετε ξανά τον Προσωπικό σας Κωδικό Αριθμό ("REPEAT PIN"). Καταχωρήστε ξανά τον νέο 5ψήφιο Προσωπικό Κωδικό Αριθμό σας και πατήστε το "=".
6. Εάν όλα τα βήματα γίνουν σωστά, στην οθόνη θα εμφανιστεί το μήνυμα "OK".

9.3.6 Ασφάλεια

Η Ηλεκτρονική Τράπεζα της Τράπεζας Κύπρου σας προσφέρει ασφάλεια τελευταίας τεχνολογίας. Λεπτομερείς στοιχεία αναφέρονται πιο κάτω:

1. SSL-3 128-bit encryption technology

Με άδεια από την κυβέρνηση των Ηνωμένων Πολιτειών για χρήση από χρηματοοικονομικούς οργανισμούς

2. User ID και Κωδικός Ασφαλείας

Με σκοπό να αποτρέψει οποιαδήποτε μη εγκεκριμένη πρόσβαση στους λογαριασμούς σας, η Τράπεζα Κύπρου, σας δίνει User ID και Κωδικό Ασφαλείας. Ο Κωδικός Ασφαλείας είναι γνωστός μόνο σ' εσάς και μπορείτε να τον αλλάξετε ανά πάσα στιγμή.

3. Παρακολούθηση Συστημάτων

Υπάρχει συνεχής παρακολούθηση των συστημάτων ούτως ώστε να διασφαλίζουμε στο μέγιστο βαθμό την ασφάλεια και την εμπιστευτικότητα.

4. Αυτόματη Αποσύνδεση

Σε περίπτωση που για 10 συνεχή λεπτά δεν υπάρξει καμία κίνηση ενώ είστε συνδεδεμένοι στην Ηλεκτρονική Τράπεζα, το σύστημα αυτόματα θα σας αποσυνδέσει. Για να μπορέσετε να συνεχίσετε θα πρέπει να καταχωρήσετε εκ νέου τους κωδικούς σας. Με αυτό τον τρόπο το σύστημα εμποδίζει την αποκάλυψη των στοιχείων σας σε τρίτα άτομα σε περίπτωση που θα απομακρυνθείτε για λίγο από τον υπολογιστή σας.

5. Μέγιστη Ασφάλεια με την χρήση Firewalls

Η πρόσβαση στην Ηλεκτρονική Τράπεζα καθώς και τα δεδομένα που προσφέρονται μέσω αυτής ελέγχονται από Firewalls. Δεν επιτρέπει καμία μη εξουσιοδοτημένη πρόσβαση στα συστήματα. Επιπρόσθετα, τα συστήματα μας είναι μέρος του εσωτερικού δικτύου του Συγκροτήματος της Τράπεζας Κύπρου και ως εκ τούτου δεν υπάρχει απευθείας σύνδεση με το Διαδίκτυο.

9.4 Marfin Λαικη ebanking

Η υπηρεσία καλύπτει ένα ολοκληρωμένο φάσμα τραπεζικών υπηρεσιών και περιλαμβάνει:

- Πληροφορίες (για λογαριασμούς, επιταγές, τραπεζικές εντολές. κάρτες, επιτόκια)

- Υπόλοιπα και καταστάσεις λογαριασμών (από την 1η Ιανουαρίου του προηγούμενου χρόνου)
- Εντολές για έκδοση βιβλιαρίου επιταγών και κατάσταση λογαριασμού
- Μεταφορές ποσών σε δικούς σας λογαριασμούς σε οποιοδήποτε νόμισμα (με άμεση ή μελλοντική ημερομηνία εκτέλεσης)
- Μεταφορές ποσών σε λογαριασμούς τρίτων στη Λαϊκή Τράπεζα σε οποιοδήποτε νόμισμα (με άμεση ή μελλοντική ημερομηνία εκτέλεσης)
- Μεταφορές ποσών σε λογαριασμούς τρίτων σε οποιαδήποτε τράπεζα στην Κύπρο σε οποιοδήποτε νόμισμα (με άμεση ή μελλοντική ημερομηνία εκτέλεσης)
- Μεταφορές ποσών σε λογαριασμούς τρίτων στο εξωτερικό σε οποιοδήποτε νόμισμα (με άμεση ή μελλοντική ημερομηνία εκτέλεσης)
- Εντολές για άνοιγμα τραπεζικής εντολής
- Εντολές για άνοιγμα αυτόματης εντολής πληρωμής λογαριασμών κοινής ωφελείας (ΑΤΗΚ, Areeba, ΑΗΚ, Υδατοπρομήθεια Λευκωσίας και Λεμεσού, Συμβούλιο Αποχετεύσεων Λευκωσίας και Λεμεσού - Αμαθούντας)
- Πληρωμές καρτών, δανείων και εισφορών
- Πληρωμές λογαριασμών κοινής ωφελείας (ΑΤΗΚ, Areeba, ΑΗΚ, Υδατοπρομήθεια Λευκωσίας και Λεμεσού, Συμβούλιο Αποχετεύσεων Λευκωσίας και Λεμεσού - Αμαθούντας)
- Ακύρωση και επανέκδοση καρτών
- Ανάκληση πληρωμής επιταγής ή βιβλιαρίου επιταγών
- Αλλαγή ή ακύρωση οδηγιών σας που δεν έχουν ακόμη εκτελεστεί
- Πληροφορίες για τα συμβόλαιά σας με τη Λαϊκή Χρηματοδοτήσεις και τη Laiki Cyprialife

Μπορείτε ακόμη να διαχειρίζεστε την υπηρεσία:

- Να αλλάζετε το PIN σας
- Να καταχωρείτε ή αλλάζετε την ηλεκτρονική σας διεύθυνση
- Να δημιουργήσετε λίστα δικαιούχων για μεταφορές σε τρίτα πρόσωπα σε λογαριασμούς Λαϊκής
- Να απενεργοποιήσετε μεταφορές χρημάτων σε τρίτους

9.4.1 Laiki eBank Alerts

Η υπηρεσία ***Laiki eBank Alerts*** είναι μια πρωτοποριακή υπηρεσία η οποία προσφέρεται δωρεάν σε όλους τους συνδρομητές της Laiki eBank, ιδιώτες και επιχειρήσεις. Αποστέλλει γραπτά μηνύματα (SMS) στο κινητό τηλέφωνο ή μηνύματα στο ηλεκτρονικό ταχυδρομείο (e-mail) των συνδρομητών και τους ενημερώνει σχετικά με τις τραπεζικές και χρηματιστηριακές τους δραστηριότητες, για τιμές μετοχών και ισοτιμίες ξένου συναλλάγματος. Ο καθορισμός μηνυμάτων γίνεται μέσω του Διαδικτύου.

Η υπηρεσία Laiki eBank Alerts προσφέρει τα πιο κάτω είδη μηνυμάτων:

- **Τραπεζικά Alerts** για μηνύματα σχετικά με τα υπόλοιπα λογαριασμών, τις συναλλαγές σε λογαριασμούς, τις αγορές μέσω καρτών, τις αναλήψεις μετρητών και την λήξη του προσωρινού ορίου λογαριασμών.
- **Χρηματιστηριακά Alerts**, για μηνύματα σχετικά με την εκτέλεση των εντολών σας και την αξία του χαρτοφυλακίου σας.
- **Alerts για Τιμές Μετοχών** για μηνύματα σχετικά με διαφοροποιήσεις στις τιμές μετοχών ή για τις τιμές κλεισίματος μετοχών ή κλαδικών δεικτών.
- **Alerts για Ξένο Συνάλλαγμα**, για μηνύματα που αφορούν τις τρέχουσες τιμές συναλλάγματος των νομισμάτων που σας ενδιαφέρουν σε σχέση με το τοπικό νόμισμα.

Τραπεζικά Alerts:

- **Υπόλοιπο**

  Το υπόλοιπο του λογαριασμού ή της κάρτας σας καθημερινά, εβδομαδιαία ή μηνιαία σε ώρα που έχετε καθορίσει. Όταν τα υπόλοιπο του λογαριασμού ή της κάρτας σας υπερβεί ή πέσει κάτω από το ποσό που έχετε καθορίσει.

- **Διαθέσιμο Υπόλοιπο**

Όταν το διαθέσιμο υπόλοιπο του λογαριασμού ή της κάρτας σας υπερβεί ή πέσει κάτω από το ποσό που έχετε καθορίσει.

- **Ανάληψη Μετρητών**

Όταν το ποσό ανάληψης από το λογαριασμό ή την κάρτα σας υπερβαίνει το ποσό που έχετε καθορίσει.

- **Αγορά με Κάρτα**

Όταν το ποσό αγοράς με την κάρτα σας υπερβαίνει το ποσό που έχετε καθορίσει.

- **Συναλλαγές**

Όταν γίνεται χρεωστική ή πιστωτική συναλλαγή στο λογαριασμό ή την κάρτα σας και το ποσό της συναλλαγής ξεπερνά το ποσό που έχετε καθορίσει.

- **Προσωρινό Όριο**

Ειδοποίηση για την λήξη του προσωρινού ορίου στο λογαριασμό σας, σε χρόνο που έχετε καθορίσει.

Χρηματιστηριακά Alerts:

- **Επιβεβαίωση Εντολής**\

Όταν οι εντολές σας για αγορά ή πώληση μετοχών εκτελεστούν

- **Αξία Χαρτοφυλακίου**

Η αξία του χαρτοφυλακίου σας κατά το κλείσιμο της χρηματιστηριακής συνάντησης.

Alerts για Τιμές Μετοχών:

- **Τιμές Μετοχών**

Όταν οι τιμές των μετοχών που σας ενδιαφέρουν διαφοροποιηθούν πιο ψηλά ή πιο χαμηλά από μια συγκεκριμένη τιμή που έχετε καθορίσει κατά την διάρκεια της χρηματιστηριακής συνάντησης ή όταν διαφοροποιηθούν σε ποσοστό που έχετε καθορίσει σε σχέση με τις τιμές κλεισίματος της προηγούμενης χρηματιστηριακής συνάντησης.

- **Αξίες Κλάδων**

Όταν οι αξίες των κλάδων που σας ενδιαφέρουν διαφοροποιηθούν πιο ψηλά η πιο χαμηλά από μια συγκεκριμένη τιμή που έχετε καθορίσει κατά την διάρκεια της χρηματιστηριακής συνάντησης ή διαφοροποιηθούν σε ποσοστό που έχετε καθορίσει σε σχέση με τις τιμές κλεισίματος της προηγούμενης χρηματιστηριακής συνάντησης.

- **Τιμές Κλεισίματος Μετοχών**

Τις τιμές κλεισίματος των μετοχών που σας ενδιαφέρουν κατά το κλείσιμο της χρηματιστηριακής συνάντησης.

- **Αξίες Κλεισίματος Κλάδων**

Τις τιμές κλεισίματος των κλάδων που σας ενδιαφέρουν κατά το κλείσιμο της χρηματιστηριακής συνάντησης.

Μηνύματα για τιμές ξένου συναλλάγματος:

- Τις τρέχουσες τιμές συναλλάγματος των νομισμάτων που σας ενδιαφέρουν έναντι του τοπικού νομίσματος σε καθημερινή, εβδομαδιαία ή μηνιαία βάση, σε ώρα που έχετε καθορίσει

Ενεργοποιήσει

Για να ενεργοποιήσετε την υπηρεσία ***Laiki eBank Alerts*** θα πρέπει πρώτα να συνδεθείτε με την υπηρεσία **SMS/ALERTS**, με τον υφιστάμενο Αριθμό Συνδρομητή σας και τον Προσωπικό Μυστικό Αριθμό σας (PIN).
Αν είστε ήδη συνδεδεμένοι σε κάποια άλλη υπηρεσία της Laiki eBank, απλά κάντε κλικ στο κουμπί SMS/Alerts και η οθόνη Προφίλ θα εμφανιστεί αυτόματα.
Στην οθόνη Προφίλ, μπορείτε να επιλέξετε να ενεργοποιήσετε την υπηρεσία και να δώσετε τον αριθμό του κινητού σας τηλεφώνου και/ή την ταχυδρομική σας διεύθυνση, τα οποία θέλετε να χρησιμοποιήσετε για να λαμβάνετε Alerts.
Εάν καταχωρήσετε τον αριθμό του κινητού σας τηλεφώνου, τότε θα πρέπει αυτό να επιβεβαιωθεί και γι' αυτό θα εμφανιστεί η οθόνη Επιβεβαίωσης. Θα λάβετε στον αριθμό του κινητού που έχετε καταχωρήσει ένα τετραψήφιο αριθμό, τον οποίο θα πρέπει να πληκτρολογήσετε στην οθόνη Επιβεβαίωσης. Εάν ο αριθμός που καταχωρήσατε είναι ορθός, τότε η υπηρεσία Laiki eBank Alerts θα ενεργοποιηθεί!

9.4.2 Laiki eTrading

Με την υπηρεσία Laiki eTrading έχετε τη δυνατότητα άμεσης πρόσβασης στο Χρηματιστήριο Αθηνών και στο Χρηματιστήριο Αξιών Κύπρου μέσω του Διαδικτύου για να αγοράζετε και να πουλάτε αξίες, να διαχειρίζεστε το προσωπικό σας χαρτοφυλάκιο και να έχετε ζωντανή ενημέρωση για τιμές, ειδήσεις και άλλες οικονομικού περιεχομένου πληροφορίες.

Απευθείας Επενδύσεις στο ΧΑΚ και στο ΧΑ
Με τη Laiki eTrading, μπορείτε:

- Να μεταβιβάζετε άμεσα εντολές για αγορά ή πώληση αξιών στο ΧΑΚ και /ή στο ΧΑ. Διαλέξετε μεταξύ εντολών «στο όριο», «στο άνοιγμα», «στο κλείσιμο» και «μέχρι ημερομηνίας».
- Να Τροποποιήσετε ή ακυρώσετε τις εντολές σας πριν να εκτελεστούν.
- Να παίρνετε άμεση επιβεβαίωση για την εκτέλεση των εντολών σας.
- Να ενημερώνεστε συνεχώς για την κατάσταση του χαρτοφυλακίου σας, το οποίο ενημερώνεται με τις τρέχουσες τιμές.
- Να χρησιμοποιείτε αμέσως το προϊόν πώλησης αξιών για αγορά νέων αξιών.
- Να λαμβάνετε Ζωντανές τιμές στα ΧΑΚ και ΧΑ (υπάρχει χρέωση για την υπηρεσία αυτή).
- Να λαμβάνετε χρηματοοικονομική πληροφόρηση όπως τιμές, ειδήσεις, ανακοινώσεις, γραφήματα και μελέτες, σε σχέση με την εταιρεία που θέλετε να επενδύσετε, και να σας δίνεται η ικανότητα να υποβάλετε την εντολή σας χωρίς να χάνετε από τα μάτια σας αυτή την πληροφόρηση.
- Να ενημερώνεστε άμεσα και να παρακολουθείτε τους συνδεδεμένους επενδυτικούς λογαριασμούς σας χωρίς να χρειάζεται να επισκεφτείτε άλλη υπηρεσία.
- Να μεταφέρετε ποσά αμέσως, μέσω του συστήματος, από το λογαριασμό συναλλαγών σας σε δικούς σας λογαριασμούς της Λαϊκής Τράπεζας και αντίστροφα.

- Να καθορίσετε αυτόματα προειδοποιητικά μηνύματα (τα οποία θα παίρνετε στο κινητό ή στην ηλεκτρονική σας διεύθυνση) για τιμές μετοχών, κλαδικών δεικτών, επιβεβαίωση εντολών και αξία χαρτοφυλακίου, μέσω της υπηρεσίας Laiki eBank Alerts.
- Να έχετε εύκολη πρόσβαση σε όλες τις υπηρεσίες της Laiki eBank.

Laiki eTrading για το ΧΑΚ

Εκτός από τις χρηματιστηριακές συναλλαγές που αναφέρονται πιο πάνω, η Laiki eTrading, σε συνεργασία με την εταιρεία Stockwatch Ltd, σας προσφέρει ολοκληρωμένη ενημέρωση για το ΧΑΚ η οποία περιλαμβάνει:

- Ζωντανή πληροφόρηση για τις τιμές των μετοχών στη διάρκεια της χρηματιστηριακής συνάντησης.
- Επίσημες ανακοινώσεις εταιρειών, που περιλαμβάνουν πληροφορίες για εταιρικές δραστηριότητες και προκαταρκτικά αποτελέσματα, εξαγορές και συγχωνεύσεις και για αλλαγές μετοχικού κεφαλαίου.
- Οικονομικές καταστάσεις για όλες τις εισηγμένες εταιρείες στο ΧΑΚ που περιλαμβάνουν το λογαριασμό αποτελεσμάτων, τον ισολογισμό και την κατάσταση ταμειακής ροής.
- Θεμελιώδη ανάλυση που περιλαμβάνει πάνω από 40 χρηματοοικονομικούς και λογιστικούς δείκτες για όλες τις εισηγμένες εταιρείες.
- Εξαμηνιαίες καταστάσεις (interim results) που περιλαμβάνουν το λογαριασμό αποτελεσμάτων, τον ισολογισμό και την κατάσταση ταμειακής ροής.
- Σύγκριση τιμών και γραφικών παραστάσεων, σύγκριση τιμών και Κλάδων.
- Αναβαθμισμένα εργαλεία αναζήτησης που καλύπτουν ειδήσεις, ανακοινώσεις, ανασκοπήσεις Τύπου, ιστορικό εταιρειών και δραστηριότητες, συνδεδεμένα πρόσωπα, κτλ.
- Αναβαθμισμένα εργαλεία σύγκρισης στοιχείων που περιλαμβάνουν τιμές, θεμελιώδη στοιχεία εταιρειών, κτλ.
- Τιμές κλεισίματος και ιστορικά στοιχεία για τις τιμές των μετοχών, καθώς και ημερήσιες, εβδομαδιαίες, μηνιαίες, εξαμηνιαίες και ετήσιες γραφικές παραστάσεις.
- Συναλλαγές συνδεδεμένων προσώπων (insider trading).
- Ανασκόπηση του οικονομικού Τύπου που περιλαμβάνει επιλεγμένα άρθρα από τις τέσσερις κυπριακές εφημερίδες με τη μεγαλύτερη κυκλοφορία.

Laiki eTrading για το ΧΑ

Η Laiki eTrading παρέχει τη δυνατότητα απευθείας επένδυσης στο ΧΑ, διευρύνοντας σημαντικά τις επενδυτικές επιλογές σας. Σε συνεργασία με τις εταιρεία Stockwatch, σας παρέχει, παράλληλα, συνεχή οικονομική ενημέρωση για όλα τα γεγονότα που διαμορφώνουν τα δεδομένα στο ΧΑ, δίδοντάς σας έτσι ένα σημαντικό εργαλείο για την επιλογή των επενδύσεών σας.

Η δωρεάν αυτή ολοκληρωμένη ηλεκτρονική πληροφόρηση περιλαμβάνει, μεταξύ άλλων:

- Ζωντανή ενημέρωση σχετικά με τις τιμές διαπραγμάτευσης των μετοχών στο ΧΑ.
- Όλες τις επίσημες ανακοινώσεις των εταιρειών των οποίων οι αξίες είναι εισηγμένες στο ΧΑ.

- Τις τιμές κλεισίματος και ιστορικά στοιχεία για τις τιμές των μετοχών καθώς και αντίστοιχες γραφικές παραστάσεις.
- Γενική ανασκόπηση του ελληνικού οικονομικού Τύπου.

9.5 Υπηρεσίες e-banking τράπεζας Πειραιώς

9.5.1 Ιδιώτες

9.5.1.1 Διαχείριση Λογαριασμών

- Ενημερωθείτε για συνολική εικόνα του χαρτοφυλακίου σας στην Τράπεζα Πειραιώς με την τρέχουσα αξία του και δείτε αναλυτικές πληροφορίες όλων των λογαριασμών σας, το υπόλοιπο τους και τις συναλλαγές σας.
- Υπόλοιπα και Κινήσεις Λογαριασμών.
- Αποστολή Κινήσεων μέσω Ταχυδρομείου και e-mail (csv, txt, html).
- Ανάλυση Υπολοίπου.
- Αναλυτικά Στοιχεία Λογαριασμού.
- Επιτόκια Χορηγήσεων / Καταθέσεων.
- Ενημέρωση για το Διεθνή Αριθμό Λογαριασμού (IBAN).
- Καθορισμός Ευκολομνημόνευτων Ονομάτων για τους Λογαριασμούς σας, το ΑΦΜ σας, τον Αριθμό της Πιστωτικής σας Κάρτας, κλπ.
- Άμεση Αλλαγή Προσωπικών Στοιχείων.
- Επιπλέον έχετε τη δυνατότητα να παράσχετε πλήρη ή μερική πρόσβαση για τη διαχείριση των λογαριασμών σας σε τρίτους -φυσικά πρόσωπα- που δεν είναι συνδικαιούχοι.

9.5.1.2 Διαχείριση Επιταγών

Διαχειριστείτε τις επιταγές που εκδίδετε και παρακολουθείστε την πορεία τους από την έκδοση μέχρι και την εξόφλησή τους.
Συγκεκριμένα, μέσω της υπηρεσίας winbank internet σας παρέχονται οι ακόλουθες δυνατότητες:

- Παραγγελία Βιβλιαρίου Επιταγών με παράδοση από Courier.
- Αναλυτικά Στοιχεία και Παρακολούθηση Επιταγών, ώστε να προγραμματίζετε τις πληρωμές σας.
- Αναζήτηση ανά Αριθμό/Σελίδα επιταγής, Χρονική Περίοδο και Κατάσταση.
- Καταχώρηση Στοιχείων και Επεξεργασία Διαθέσιμων και Ανεξόφλητων Επιταγών.
- Ενημέρωση της Κατάστασης (π.χ. εξοφλημένες, ακυρωμένες, ανακλημένες, κτλ).

- Ανάκληση Βιβλιαρίου Επιταγών ή Επιταγής.

9.5.1.3 Διαχείριση Πιστωτικών Καρτών

Διαχειριστείτε τις Πιστωτικές Κάρτες σας και παρακολουθείστε τις κινήσεις και τα στοιχεία τους.
Συγκεκριμένα, μέσω της υπηρεσίας winbank internet σας παρέχονται οι ακόλουθες πληροφορίες:

- Υπόλοιπα και Κινήσεις Πιστωτικών Καρτών.
- On-line Εμφάνιση & Εκτύπωση Μηνιαίων Λογαριασμών.
- Αποστολή Μηνιαίων Λογαριασμών μέσω Ταχυδρομείου & e-mail.
- Αναλυτικά Στοιχεία Πιστωτικών Καρτών.
- Πληρωμή Άμεσα ή σε Μελλοντική Ημερομηνία.
- Καθορισμός Ευκολομνημόνευτων Ονομάτων για τον Αριθμό της Πιστωτικής σας Κάρτας, τους Λογαριασμούς σας, το ΑΦΜ σας, κλπ.

9.5.1.4 Προπληρωμένη Κάρτα - WEBUY

Η WEBUY, είναι η πρώτη "άυλη" (virtual) προπληρωμένη κάρτα που σχεδιάστηκε για να χρησιμοποιείται **αποκλειστικά για τις εξ αποστάσεως συναλλαγές σας**, όπως αγορές στο **Internet** (αγορές παιχνιδιών, προγραμμάτων ή αντικειμένων σε ηλεκτρονικά καταστήματα - e-shops), **τηλεφωνικές παραγγελίες** από όλο τον κόσμο, παραγγελίες από **καταλόγους κ.ά.**
Μέσω της υπηρεσίας winbank internet και του Πειραιώς phone banking μπορείτε, 24 ώρες το 24ωρο, να:

- **Εκδώσετε** real - time τη νέα σας κάρτα, όποια στιγμή θελήσετε
- **Δείτε** συνοπτικά όλα τα στοιχεία της κάρτας σας
- **Φορτίζετε** (γεμίζετε) άμεσα, σε πραγματικό χρόνο, τη δική σας κάρτα ή την κάρτα τρίτου μεταφέροντας χρήματα από τον τραπεζικό σας λογαριασμό ή χρεώνοντας την πιστωτική σας κάρτα της Τράπεζας Πειραιώς
- **Εκφορτίζετε** (αδειάζετε) άμεσα, σε πραγματικό χρόνο, την κάρτα σας μεταφέροντας το ποσό που επιθυμείτε σε λογαριασμό σας
- **Παρακολουθείτε** αναλυτικά, σε πραγματικό χρόνο, τις κινήσεις που έχετε πραγματοποιήσει με την κάρτα σας (Αγορές, Φορτίσεις και Εκφορτίσεις).
- **Αλλάζετε**, άμεσα, το Ημερήσιο Όριο Συναλλαγών[1] της κάρτας σας σύμφωνα με τις ανάγκες σας
- **Ακυρώσετε** πλήρως την κάρτας σας ή / και να ζητήσετε ταυτόχρονη έκδοση καινούριας κάρτας με νέα στοιχεία (αριθμό, ημερομηνία λήξης και κωδικό επαλήθευσης CVC).

… κι όλα αυτά, όπου κι αν βρίσκεστε!

9.5.1.5 Διαχείριση Δανείων

Διαχειριστείτε on-line και με ευκολία όλα τα δανειακά προϊόντα που έχετε στην Τράπεζα Πειραιώς.
Μέσω της υπηρεσίας winbank internet, έχετε άμεσα διαθέσιμες όλες τις πληροφορίες σχετικά με τα δάνειά σας:

- Συνολική Απεικόνιση των Δανείων σας.
- Αναλυτικά Στοιχεία για κάθε Δάνειο, όπως η Κατάστασή του, το Διαθέσιμο, Ληξιπρόθεσμο και Ανεξόφλητο Ποσό, την Ημέρα Πληρωμής κ.ά.
- Πληρωμή Δόσεων και Ιστορικό.

9.5.1.6 Πληρωμές - Μεταφορές

Μέσω της winbank, μπορείτε εύκολα και γρήγορα να καταχωρήσετε εντολές πληρωμών, εμβάσματα και μεταφορές ή ακόμα και να ζητήσετε την πάγια εξόφληση των οφειλών σας. Συγκεκριμένα, μπορείτε να εκτελέσετε:

Μεταφορές
- Σε Λογαριασμό του Ιδίου.
- Σε Λογαριασμούς Τρίτων.
- Μαζικές Πληρωμές (Μισθοδοσία, Εμβάσματα).
- Από Κάρτα Visa σε Άλλη Κάρτα ή e-mail - Visa Direct
- Για Πληρωμή CLA.

Μεμονωμένες Εντολές Πληρωμών
- Πιστωτικής Κάρτας της Τράπεζας Πειραιώς.
- Πιστωτικής Κάρτας Άλλης Τράπεζας.
- ΔΕΚΟ (ΟΤΕ, ΔΕΗ).
- Ασφαλιστικά Ταμεία (ΙΚΑ, ΦΠΑ, ΤΕΒΕ).
- Ασφαλιστικοί Φορείς (ALLIANZ ΑΕΓΑ, ΑΕΑΖ, ING).
- Εταιρίες Σταθερής Τηλεφωνίας (Tellas, Q-Telecom, ΟΤΕ).
- Εταιρίες Κινητής Τηλεφωνίας (COSMOTE, VODAFONE).
- Ανανέωση Προπληρωμένου Χρόνου Ομιλίας (**VODAFONE Refill**).
- Φόρου Εισοδήματος Φυσικών Προσώπων.

Για όλες τις προαναφερθέντες εντολές και μεταφορές μπορείτε να:
- Ζητήσετε την περιοδική εκτέλεση τους με συχνότητα που εσείς καθορίζετε.
- Αποθηκεύσετε τακτικές πληρωμές για άμεση επανάληψη.
- Καταχωρήσετε αιτιολογία πληρωμών προς ενημέρωση του αποδέκτη.

Παράλληλα, από την επιλογή "**Ιστορικό Πληρωμών**" μπορείτε ανά πάσα στιγμή να διαχειριστείτε τις εντολές σας αυτές. Μεταξύ άλλων έχετε τη δυνατότητα να:

- Τροποποιήσετε τις λεπτομέρειες των αποθηκευμένων εντολών πληρωμών.
- Αναβάλετε ή να ακυρώσετε αποθηκευμένες εντολές πληρωμών.
- Δείτε το ιστορικό όλων των πληρωμών που έχετε εκτελέσει.

Πάγιες Εντολές Πληρωμής
- ΔΕΚΟ (ΔΕΗ, ΟΤΕ, ΕΥΔΑΠ).

- Κινητής Τηλεφωνίας (COSMOTE, VODAFONE, TIM).
- Συνδρομητικής Τηλεόρασης (NOVA/FILMNET).
- ΤΕΒΕ.

Επιπλέον από το μενού διαχείρισης των Παγίων μπορείτε να ζητήσετε την:

- Προσωρινή απενεργοποίηση & μεταβολή πάγιων εντολών.
- Διακοπή πάγιων εντολών.
- Εμφάνιση του ιστορικού πληρωμών μέσω οποιασδήποτε πάγιας εντολής σας.

Εντολές Εμβασμάτων

- Αποστολή **μεμονωμένων εμβασμάτων** στην Ελλάδα και στο Εξωτερικό.
- Αποστολή μαζικών εμβασμάτων μέσω αρχείων στην **Ελλάδα** και στο **Εξωτερικό**

Για όλα τα εμβάσματα σας μπορείτε να δείτε:

- Ανάλυση εξόδων και προμηθειών (advice).
- Αντίγραφο μηνύματος πληρωμής (swift confirmation).
- Ιστορικό όλων των πληρωμών και εμβασμάτων.

9.5.1.7 Τηλε-ειδοποιήσεις / alert

Τώρα έχετε τη δυνατότητα να ενημερώνεστε, εύκολα και γρήγορα, χωρίς να χρειαστεί να επικοινωνήσετε εσείς με την Τράπεζα!
Μέσω της υπηρεσίας τηλε-ειδοποιήσεων winbank alert σας παρέχονται πληροφορίες για τα τραπεζικά και χρηματιστηριακά σας θέματα **real-time, 24X7**, **οπουδήποτε και αν βρίσκεστε.**
Η Τράπεζα Πειραιώς παρέχει πλέον τη δυνατότητα ενεργοποίησης της πρωτοποριακής υπηρεσίας winbank alert σε **όλους τους πελάτες** της, ανεξαρτήτως αν είναι εγγεγραμμένοι χρήστες άλλων υπηρεσιών ηλεκτρονικής τραπεζικής, winbank.
Κάθε πελάτης που έχει ένα κινητό ή/και σταθερό τηλέφωνο, καθώς και όσοι έχουν πρόσβαση σε e-mail μπορούν να την αξιοποιήσουν άμεσα και εύκολα.
Απαραίτητη και μοναδική προϋπόθεση για την ενεργοποίηση της υπηρεσίας, είναι η ύπαρξη τουλάχιστον ενός καταθετικού λογαριασμού στη Τράπεζα Πειραιώς.
Κάντε την **αίτησή** σας άμεσα και καθορίσετε τις τηλε-ειδοποιήσεις σας, on-line ή μέσω του Κέντρου Εξυπηρέτησης Πελατών μας στα τηλέφωνα 801 802 803 804 (χρέωση αστικής κλήσης) ή 210 32 88 000 210 32 88 000 (από κινητό ή από το εξωτερικό).

9.5.1.8 Χρηματιστήριο

Παρακολούθηση on-line και real-time τα ενδοσυνεδριακά δεδομένα του Χ.Α.,
εισάγετε νέες εντολές αγοράς ή πώλησης μετοχών και ενημερωθείτε για την
τρέχουσα αξία του επενδυτικού χαρτοφυλακίου σας.

- Real-time Παρακολούθηση των Τιμών των Μετοχών του Χ.Α.Α.

- On-line, Real-time Αποτίμηση Χαρτοφυλακίου.
- Ημερήσιο και Ιστορικό Γράφημα Τιμών Μετοχών.
- Real-time Ενημέρωση για τις Τιμές των Δεικτών των Ξένων αγορών.
- Άμεση Ενημέρωση για τα Οικονομικά, Επιχειρηματικά και Χρηματιστηριακά Νέα της Ελληνικής και Ξένης αγοράς.
- Ισοτιμίες των Ξένων Νομισμάτων.
- Τιμές Αμοιβαίων Κεφαλαίων της Τράπεζας.
- Εντολές Αγοράς Μετοχών με Χρέωση Λογαριασμού.
- Εντολές Πώλησης Μετοχών με Πίστωση Λογαριασμού.
- Άμεση Ενημέρωση για την Κατάσταση (status) των Χρηματιστηριακών Εντολών σας.
- Εντολές Επαναπώλησης Μετοχών που Αγοράστηκαν μέσα στην Ίδια Μέρα.
- Ενημέρωση για την Εκτέλεση των Εντολών (πινακίδια).
- Συμμετοχή σε Δημόσιες Εγγραφές (underwritting).

9.5.1.9 Ασφάλεια

Αναγνώριση Πελάτη

Μετά την υπογραφή της σύμβασής σας, παραλαμβάνετε το κουτί σας (winbox), το οποίο εκτός από την επιστολή καλωσορίσματος και τους οδηγούς των υπηρεσιών περιέχει και τους κωδικούς σας. Οι κωδικοί που χρησιμοποιούνται για την αναγνώρισή σας είναι δύο: ο Κωδικός Εισόδου (UserID) και ο Προσωπικός Κωδικός Ασφαλείας (PIN), τους οποίους καταχωρείτε κάθε φορά που χρησιμοποιείτε την υπηρεσία. Την πρώτη φορά που θα χρησιμοποιήσετε την υπηρεσία, για τη δική σας ασφάλεια, το σύστημα σας υποχρεώνει να μεταβάλετε τον Κωδικό Εισόδου (UserID) και τον Προσωπικό Κωδικό Ασφαλείας (PIN).
Επίσης το σύστημα σας παραπέμπει σε υποχρεωτική αλλαγή του Προσωπικού Κωδικού Ασφαλείας (PIN) κάθε δύο μήνες ή κάθε φορά που ζητάτε επανέκδοση. Ωστόσο η winbank σας δίνει τη δυνατότητα να μεταβάλλετε τους κωδικούς σας όσο συχνά επιθυμείτε από την επιλογή στο μενού "Ρυθμίσεις Ασφαλείας>Κωδικοί
Εισόδου - Ασφαλείας> Αλλαγή Κωδικού".

Εξασφάλιση του Απορρήτου της Μεταφοράς των Δεδομένων

Για την εξασφάλιση του απορρήτου της μεταφοράς των δεδομένων, χρησιμοποιούμε το πρωτόκολλο κρυπτογράφησης SSL 128bit. Το σύστημα έχει υλοποιηθεί σε συνεργασία με την εταιρία **Verisign,** η οποία ειδικεύεται σε θέματα ασφαλείας συναλλαγών.

Αυτόματη Αποσύνδεση

Εάν δεν υπάρξει καμία δραστηριότητα για επτά λεπτά γίνεται αυτόματη αποσύνδεση από την υπηρεσία winbank internet.

Ελεγχόμενη Πρόσβαση (firewall)

Η πρόσβαση στα συστήματα της Τράπεζας (servers) ελέγχεται από firewall το οποίο επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών από τους πελάτες/επισκέπτες απαγορεύοντας, παράλληλα, την

πρόσβαση σε συστήματα και βάσεις δεδομένων με απόρρητα στοιχεία και πληροφορίες της Τράπεζας.

Κλείδωμα Κωδικών

Σε περίπτωση που εισάγετε τρεις φορές λάθος τον Προσωπικό σας Κωδικό Ασφαλείας (PIN), τότε το σύστημα για τη δική σας ασφάλεια κλειδώνει τους κωδικούς σας και απαγορεύει την πρόσβασή σας στην υπηρεσία winbank internet. Για να ξεκλειδώσετε τους κωδικούς σας πρέπει να καλέσετε το κέντρο εξυπηρέτησης πελατών της Τράπεζας Πειραιώς στο 18 28 38 (από σταθερό ή κινητό εντός Ελλάδος) ή στο 0030 210 32 88000 0030 210 32 88000 (από το εξωτερικό) και να γίνει πιστοποίηση των στοιχείων σας από κάποιον winbank agent.

Κωδικός extraPIN

Ο κωδικός extraPIN ζητείται μετά την είσοδό σας στην υπηρεσία winbank internet και μόνο για την εκτέλεση των ακόλουθων συναλλαγών:

- Μεταφορές προς Τρίτους
- Πληρωμή Πιστωτικής Κάρτας άλλης Τράπεζας Εμβάσματα
- Φόρτιση Webuv
- Μαζικές Πληρωμές
- Μαζικά Εμβάσματα
- Μισθοδοσίες
- Visa Direct
- Εξαίρεση Λογαριασμών
- Αίτηση Ανοίγματος Καταθετικού Λογαριασμού και
- Διαχείριση των Αιτήσεών σας
- Λεφτά στο Λεπτό
- Αλλαγή των προσωπικών σας στοιχείων

Οι κωδικοί extraPIN είτε θα αποστέλλονται με sms στο κινητό σας είτε θα παράγονται από τη συσκευή extraPIN generator

Συσκευή παραγωγής κωδικών μίας χρήσης extraPIN generator

Η συσκευή extraPIN generator παράγει 6ψήφιους κωδικούς μίας χρήσης που μπορείτε να καταχωρείτε κατά την είσοδό σας στην υπηρεσία και κατά τη διάρκεια εκτέλεση συγκεκριμένων συναλλαγών μέσω της υπηρεσίας. Ο κωδικός εμφανίζεται στην οθόνη LCD της συσκευής. Η οθόνη της συσκευής μένει πάντα ενεργή και εμφανίζεται σε αυτή ο 6ψήφιος τυχαίος κωδικός μίας χρήσης ο οποίος ανανεώνεται κάθε 60 δευτερόλεπτα. Ο κωδικός αυτός όταν καταχωρηθεί παύει να ισχύει.

Εξαίρεση Λογαριασμών

Επιπλέον μέσω των υπηρεσιών winbank internet και phone σας δίνεται η δυνατότητα να επιλέξτε τους λογαριασμούς που ΔΕΝ επιθυμείτε να έχετε πρόσβαση μέσω των καναλιών winbank internet, mobile, sms και phone.

Οι λογαριασμοί που εξαιρείτε ΔΕΝ ακυρώνονται, απλά δε θα εμφανίζονται μέσω των παραπάνω καναλιών. Συγκεκριμένα δε θα μπορείτε να εκτελείτε συναλλαγές, δε θα μπορείτε να ενημερωθείτε για τις κινήσεις τους και το υπόλοιπό τους και δε θα μπορείτε να πραγματοποιήσετε οποιαδήποτε άλλη εγχρήματη ή μη συναλλαγή η οποία θα σχετίζεται με τους λογαριασμούς που εξαιρέσατε

9.5.2 Επιχειρήσεις & Επαγγελματίες

Ειδικότερα, η υπηρεσία winbank internet business σας παρέχει τη **δυνατότητα πολλαπλών χρηστών-υπαλλήλων** της εταιρίας, οι οποίοι έχουν **διαφορετικά δικαιώματα πρόσβασης** στην υπηρεσία (π.χ. μόνο παρακολούθηση υπολοίπων, διενέργεια συναλλαγών μόνο μεταξύ προϊόντων της εταιρίας, προετοιμασία συναλλαγών προς ολοκλήρωση / έγκριση από άλλο χρήστη, κλπ). Η δυνατότητα αυτή καλύπτει θέματα:

- «Διπλής» υπογραφής ανά συναλλαγή.
- Διαφορετικά χρηματικά όρια ανά είδος συναλλαγής.
- Διαφορετικά εγκριτικά επίπεδα ή επίπεδα πρόσβασης.
- Ύπαρξη ενός administrative master κωδικού (UserID) ανά εταιρεία, ο οποίος θα έχει τη δυνατότητα παρακολούθησης όλων των κινήσεων που διενεργούνται από όλους τους άλλους χρήστες της ίδιας εταιρείας.

Για όλες τις υπηρεσίες είναι δυνατή η επιλογή γλώσσας: **ελληνικά και αγγλικά**.

9.5.2.1 Διαχείριση Λογαριασμών

Ενημερωθείτε για συνολική εικόνα του χαρτοφυλακίου σας στην Τράπεζα Πειραιώς με την τρέχουσα αξία του και δείτε αναλυτικές πληροφορίες όλων των λογαριασμών σας, το υπόλοιπο τους και τις συναλλαγές σας.

- Υπόλοιπα και Κινήσεις Λογαριασμών.
- Αποστολή Κινήσεων μέσω Ταχυδρομείου και e-mail (csv, txt, html).
- Ανάλυση Υπολοίπου.
- Αναλυτικά Στοιχεία Λογαριασμού.
- Επιτόκια Χορηγήσεων / Καταθέσεων.
- Ενημέρωση για το Διεθνή Αριθμό Λογαριασμού (IBAN).
- Καθορισμός Ευκολομνημόνευτων Ονομάτων για τους Λογαριασμούς σας, το ΑΦΜ σας, τον Αριθμό της Πιστωτικής σας Κάρτας, κλπ.

9.5.2.2 Διαχείριση Επιταγών

Διαχειριστείτε τις επιταγές που εκδίδετε και παρακολουθείστε την πορεία τους από την έκδοση μέχρι και την εξόφλησή τους.
Συγκεκριμένα, μέσω της υπηρεσίας winbank internet σας παρέχονται οι ακόλουθες δυνατότητες:

- Παραγγελία Βιβλιαρίου Επιταγών με παράδοση από Courier.
- Αναλυτικά Στοιχεία και Παρακολούθηση Επιταγών, ώστε να προγραμματίζετε τις πληρωμές σας.
- Αναζήτηση ανά Αριθμό/Σελίδα επιταγής, Χρονική Περίοδο και Κατάσταση.
- Καταχώρηση Στοιχείων και Επεξεργασία Διαθέσιμων και Ανεξόφλητων Επιταγών.
- Ενημέρωση της Κατάστασης (π.χ. εξοφλημένες, ακυρωμένες, ανακλημένες, κτλ).
- Ανάκληση Βιβλιαρίου Επιταγών ή Επιταγής.

9.5.2.3 Διαχείριση Καρτών

Διαχειριστείτε τις πιστωτικές σας κάρτες και παρακολουθείστε τις κινήσεις και τα στοιχεία τους.
Συγκεκριμένα, μέσω της υπηρεσίας winbank internet σας παρέχονται οι ακόλουθες πληροφορίες:

- Υπόλοιπα και Κινήσεις Πιστωτικών Καρτών.
- On-line Εμφάνιση & Εκτύπωση Μηνιαίων Λογαριασμών.
- Αποστολή Μηνιαίων Λογαριασμών μέσω Ταχυδρομείου & e-mail.
- Αναλυτικά Στοιχεία Πιστωτικών Καρτών.
- Πληρωμή Δόσης Άμεσα ή σε Μελλοντική Ημερομηνία.

9.5.2.4 Διαχείριση Δανείων

Διαχειριστείτε on-line και με ευκολία όλα τα δανειακά προϊόντα που έχετε στην Τράπεζα Πειραιώς.

- Μέσω της υπηρεσίας winbank internet, έχετε άμεσα διαθέσιμες όλες τις πληροφορίες σχετικά με τα δάνειά σας:
- Συνολική Απεικόνιση των Δανείων σας.
- Αναλυτικά Στοιχεία για κάθε Δάνειο, όπως η Κατάστασή του, το Διαθέσιμο, Ληξιπρόθεσμο και Ανεξόφλητο Ποσό, την Ημέρα Πληρωμής κ.ά.
- Πληρωμή Δόσεων και Ιστορικό.

9.5.2.5 Διαχείριση Χορηγήσεων

Διαχειριστείτε on-line και με ευκολία τις χορηγήσεις σας και συγκεκριμένα τους Ανοιχτούς Αλληλόχρεους Λογαριασμούς που έχετε στην Τράπεζα Πειραιώς.
Μέσω της winbank, έχετε άμεσα διαθέσιμες όλες τις πληροφορίες σχετικά με τις συγκεκριμένες χορηγήσεις σας.
Συγκεκριμένα:

- Συνολική Απεικόνιση των Ανοιχτών Αλληλόχρεων Λογαριασμών (ΑΑΛ) σας Αναλυτικά Στοιχεία για κάθε ΑΑΛ, όπως η Κατάστασή του, το Ληξιπρόθεσμο Κεφάλαιο

και Τόκοι καθώς και την Συνολική Οφειλή, το Ενήμερο και το Ακαθάριστο Ποσό κ.ά.
- Ιστορικό Κινήσεων του κάθε ΑΑΛ όπως εμφανίζονται στην καρτέλα πελάτη.

9.5.2.6 Πληρωμές-Μεταφορές

Μέσω της winbank, μπορείτε εύκολα και γρήγορα να καταχωρήσετε εντολές πληρωμών, εμβάσματα και μεταφορές ή ακόμα και να ζητήσετε την πάγια εξόφληση των οφειλών σας. Συγκεκριμένα, μπορείτε να εκτελέσετε:

Μεταφορές
- Σε Λογαριασμό του Ιδίου.
- Σε Λογαριασμούς Τρίτων.
- Μαζικές Πληρωμές (Μισθοδοσία, Εμβάσματα).
- Από Κάρτα Visa σε Άλλη Κάρτα ή e-mail -**Visa Direct**.
- Για Πληρωμή CLA.

Μεμονωμένες Εντολές Πληρωμών
- Πιστωτικής Κάρτας της Τράπεζας Πειραιώς.
- Πιστωτικής Κάρτας Άλλης Τράπεζας.
- ΔΕΚΟ (ΟΤΕ, ΔΕΗ).
- Προς Ασφαλιστικά Ταμεία (ΙΚΑ, ΦΠΑ, ΤΕΒΕ).
- Προς Ασφαλιστικούς Φορείς (ALLIANZ ΑΕΓΑ, ΑΕΑΖ, ING).
- Προς Εταιρίες Σταθερής Τηλεφωνίας (Tellas, Q-Telecom, ΟΤΕ).
- Προς Εταιρίες Κινητής Τηλεφωνίας (COSMOTE, VODAFONE).
- Ανανέωση Προπληρωμένου Χρόνου Ομιλίας (VODAFONE Refill).
- Φόρου Εισοδήματος Φυσικών Προσώπων.

Για όλες τις προαναφερθείσες εντολές και μεταφορές μπορείτε να:
- Ζητήσετε την Περιοδική Εκτέλεση τους με Συχνότητα που εσείς καθορίζετε.
- Αποθηκεύσετε Τακτικές Πληρωμές για Άμεση Επανάληψη.
- Καταχωρήσετε αιτιολογία Πληρωμών προς Ενημέρωση του Αποδέκτη.

Παράλληλα, από την επιλογή "Ιστορικό Πληρωμών" μπορείτε ανά πάσα στιγμή να διαχειριστείτε τις εντολές σας αυτές. Μεταξύ άλλων έχετε τη δυνατότητα να:
- Τροποποιήσετε τις Λεπτομέρειες των Αποθηκευμένων Εντολών Πληρωμών.
- Αναβάλετε ή να Ακυρώσετε Αποθηκευμένες Εντολές Πληρωμών.
- Δείτε το Ιστορικό όλων των Πληρωμών που έχετε εκτελέσει.

Πάγιες Εντολές Πληρωμής
- ΔΕΚΟ (ΔΕΗ, ΟΤΕ, ΕΥΔΑΠ).
- Κινητής Τηλεφωνίας (COSMOTE, VODAFONE, TIM).
- Συνδρομητικής Τηλεόρασης (NOVA/FILMNET).
- ΤΕΒΕ.

- Επιπλέον από το μενού διαχείρισης των Παγίων μπορείτε να ζητήσετε την:
- Προσωρινή Απενεργοποίηση & Μεταβολή Πάγιων Εντολών.
- Διακοπή Πάγιων Εντολών.
- Εμφάνιση του Ιστορικού Πληρωμών μέσω οποιασδήποτε Πάγιας Εντολής σας.
- Εντολές Εμβασμάτων
- Αποστολή Εμβασμάτων.
- Αποστολή Μαζικών Εμβασμάτων μέσω Αρχείου.
- Για όλα τα εμβάσματα σας μπορείτε να δείτε:
- Ανάλυση Εξόδων & Προμηθειών (advice).
- Αντίγραφο Μηνύματος Πληρωμής (swift confirmation).
- Ιστορικό όλων των Πληρωμών & Εμβασμάτων.

9.5.2.7 Χρηματιστήριο

Παρακολούθηση on-line και real-time τα ενδοσυνεδριακά δεδομένα του Χ.Α.,
εισάγετε νέες εντολές αγοράς ή πώλησης μετοχών και ενημερωθείτε για την
τρέχουσα αξία του επενδυτικού χαρτοφυλακίου σας.
Real-time Παρακολούθηση των Τιμών των Μετοχών του Χ.Α.Α.
On-line, Real-time Αποτίμηση Χαρτοφυλακίου.
Ημερήσιο και Ιστορικό Γράφημα Τιμών Μετοχών.
Real-time Ενημέρωση για τις Τιμές των Δεικτών των Ξένων αγορών.
Άμεση Ενημέρωση για τα Οικονομικά, Επιχειρηματικά και Χρηματιστηριακά Νέα της Ελληνικής και Ξένης αγοράς.
Ισοτιμίες των Ξένων Νομισμάτων.
Τιμές Αμοιβαίων Κεφαλαίων της Τράπεζας.
Εντολές Αγοράς Μετοχών με Χρέωση Λογαριασμού.
Εντολές Πώλησης Μετοχών με Πίστωση Λογαριασμού.
Άμεση Ενημέρωση για την Κατάσταση (status) των Χρηματιστηριακών Εντολών σας.
Εντολές Επαναπώλησης Μετοχών που Αγοράστηκαν μέσα στην Ίδια Μέρα.
Ενημέρωση για την Εκτέλεση των Εντολών (πινακίδια).
Συμμετοχή σε Δημόσιες Εγγραφές (underwritting).

9.5.2.8 Ασφάλεια

Αναγνώριση Πελάτη

Μετά την υπογραφή της σύμβασής σας, παραλαμβάνετε το κουτί σας (winbox), το οποίο εκτός από την επιστολή καλωσορίσματος και τους οδηγούς των υπηρεσιών περιέχει και τους κωδικούς σας. Οι κωδικοί που χρησιμοποιούνται για την αναγνώρισή σας είναι δύο: ο Κωδικός Εισόδου (UserID) και ο Προσωπικός Κωδικός Ασφαλείας (PIN), τους οποίους καταχωρείτε κάθε φορά που χρησιμοποιείτε την υπηρεσία. Την πρώτη φορά που θα χρησιμοποιήσετε την υπηρεσία, για τη δική σας ασφάλεια, το σύστημα σας υποχρεώνει να μεταβάλετε τον Κωδικό Εισόδου (UserID) και τον Προσωπικό Κωδικό Ασφαλείας (PIN).

Επίσης το σύστημα σας παραπέμπει σε υποχρεωτική αλλαγή του Προσωπικού Κωδικού Ασφαλείας (PIN) κάθε δύο μήνες ή κάθε φορά που ζητάτε επανέκδοση. Ωστόσο η winbank σας δίνει τη δυνατότητα να μεταβάλλετε τους κωδικούς σας όσο συχνά επιθυμείτε από την επιλογή στο μενού "Ρυθμίσεις Ασφαλείας>Κωδικοί
Εισόδου - Ασφαλείας> Αλλαγή Κωδικού".

Εξασφάλιση του Απορρήτου της Μεταφοράς των Δεδομένων

Για την εξασφάλιση του απορρήτου της μεταφοράς των δεδομένων, χρησιμοποιούμε το πρωτόκολλο κρυπτογράφησης SSL 128bit. Το σύστημα έχει υλοποιηθεί σε συνεργασία με την εταιρία **Verisign,** η οποία ειδικεύεται σε θέματα ασφαλείας συναλλαγών.

Αυτόματη Αποσύνδεση

Εάν δεν υπάρξει καμία δραστηριότητα για επτά λεπτά γίνεται αυτόματη αποσύνδεση από την υπηρεσία winbank internet.

Ελεγχόμενη Πρόσβαση (firewall)

Η πρόσβαση στα συστήματα της Τράπεζας (servers) ελέγχεται από firewall το οποίο επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών από τους πελάτες/επισκέπτες απαγορεύοντας, παράλληλα, την πρόσβαση σε συστήματα και βάσεις δεδομένων με απόρρητα στοιχεία και πληροφορίες της Τράπεζας.

Κλείδωμα Κωδικών

Σε περίπτωση που εισάγετε τρεις φορές λάθος τον Προσωπικό σας Κωδικό Ασφαλείας (PIN), τότε το σύστημα για τη δική σας ασφάλεια κλειδώνει τους κωδικούς σας και απαγορεύει την πρόσβασή σας στην υπηρεσία winbank internet. Για να ξεκλειδώσετε τους κωδικούς σας πρέπει να καλέσετε το κέντρο εξυπηρέτησης πελατών της Τράπεζας Πειραιώς στο 18 28 38 (από σταθερό ή κινητό εντός Ελλάδος) ή στο 0030 210 32 88000 0030 210 32 88000 (από το εξωτερικό) και να γίνει πιστοποίηση των στοιχείων σας από κάποιον winbank agent.

Κωδικός extraPIN

Ο κωδικός extraPIN ζητείται μετά την είσοδό σας στην υπηρεσία winbank internet και μόνο για την εκτέλεση των ακόλουθων συναλλαγών:

- Μεταφορές προς Τρίτους
- Πληρωμή Πιστωτικής Κάρτας άλλης Τράπεζας Εμβάσματα
- Φόρτιση Webuv
- Μαζικές Πληρωμές
- Μαζικά Εμβάσματα
- Μισθοδοσίες

- Visa Direct
- Εξαίρεση Λογαριασμών
- Αίτηση Ανοίγματος Καταθετικού Λογαριασμού και
- Διαχείριση των Αιτήσεών σας
- Λεφτά στο Λεπτό
- Αλλαγή των προσωπικών σας στοιχείων

Οι κωδικοί extraPIN είτε θα αποστέλλονται με sms στο κινητό σας είτε θα παράγονται από τη συσκευή extraPIN generator

Συσκευή παραγωγής κωδικών μίας χρήσης extraPIN generator

Η συσκευή extraPIN generator παράγει 6ψήφιους κωδικούς μίας χρήσης που μπορείτε να καταχωρείτε κατά την είσοδό σας στην υπηρεσία και κατά τη διάρκεια εκτέλεση συγκεκριμένων συναλλαγών μέσω της υπηρεσίας. Ο κωδικός εμφανίζεται στην οθόνη LCD της συσκευής. Η οθόνη της συσκευής μένει πάντα ενεργή και εμφανίζεται σε αυτή ο 6ψήφιος τυχαίος κωδικός μίας χρήσης ο οποίος ανανεώνεται κάθε 60 δευτερόλεπτα. Ο κωδικός αυτός όταν καταχωρηθεί παύει να ισχύει.

Εξαίρεση Λογαριασμών

Επιπλέον μέσω των υπηρεσιών winbank internet και phone σας δίνεται η δυνατότητα να επιλέξτε τους λογαριασμούς που ΔΕΝ επιθυμείτε να έχετε πρόσβαση μέσω των καναλιών winbank internet, mobile, sms και phone.

Οι λογαριασμοί που εξαιρείτε ΔΕΝ ακυρώνονται, απλά δε θα εμφανίζονται μέσω των παραπάνω καναλιών. Συγκεκριμένα δε θα μπορείτε να εκτελείτε συναλλαγές, δε θα μπορείτε να ενημερωθείτε για τις κινήσεις τους και το υπόλοιπό τους και δε θα μπορείτε να πραγματοποιήσετε οποιαδήποτε άλλη εγχρήματη ή μη συναλλαγή η οποία θα σχετίζεται με τους λογαριασμούς που εξαιρέσατε

9.6 Υπηρεσίες e-banking Alpha Bank

9.6.1 Περιγραφή

Το e-banking είναι ηλεκτρονική υπηρεσία που προσφέρει άμεση πρόσβαση στις τραπεζικές εργασίες και συναλλαγές μέσω διαδικτύου, οπουδήποτε και οποτεδήποτε.

Δίνει τη δυνατότητα:

- Ενημέρωσης για τα υπόλοιπα και την κίνηση των λογαριασμών και των καρτών.
- Μεταφοράς χρημάτων μεταξύ των λογαριασμών του χρήστη και σε λογαριασμούς τρίτων στην Alpha Bank ή άλλες τράπεζες στην Κύπρο και στο εξωτερικό.
- Εξόφλησης λογαριασμών ηλεκτρικού ρεύματος και τηλεφώνου.

- Πληρωμής δόσεων των δανείων και των καρτών.
- Πληρωμής ασφάλιστρων στην Alpha Ασφαλιστική.
- Παραγγελίας βιβλιάριων επιταγών.
- Καταχώρισης αιτήσεων πάγιων εντολών και αυτόματης πληρωμής λογαριασμών.
- Καταχώρισης αιτήσεων ακύρωσης επιταγών.
- Καταχώρισης αιτήσεων επανεκτύπωσης επίσημων καταστάσεων λογαριασμών.
- Ενημέρωσης για τις ισοτιμίες ξένων νομισμάτων.
- Καταβολής δωρεών σε φιλανθρωπικά ιδρύματα.
- Καταχώρησης αιτήσεων εξαργύρωσης βαθμών για το πρόγραμμα "Alpha Βαθμοί & Δώρα".

Επιπρόσθετα, ο χρήστης έχει τη δυνατότητα να διαχειρίζεται την υπηρεσία για να:

- Προσθέτει νέους ή να αφαιρεί υφιστάμενους λογαριασμούς.
- Επηρεάζει τη δυνατότητα διενέργειας χρεώσεων ή πιστώσεων στους λογαριασμούς του.
- Αποδίδει διαφορετικά επίπεδα πρόσβασης για κάθε συνδεδεμένο λογαριασμό.
- Καθορίζει και να επηρεάζει τα επίπεδα πρόσβασης άλλων χρηστών στους λογαριασμούς του.

9.6.2 Επίπεδα Πρόσβασης Χρηστών

Το e-banking δίνει τη δυνατότητα στους χρήστες του να φέρουν κοινά ή διαφορετικά επίπεδα πρόσβασης για κάθε ένα από τους συνδεδεμένους με την υπηρεσία λογαριασμούς. Ενισχύεται έτσι η προοπτική αξιοποίησης της υπηρεσίας σε εργασιακούς χώρους που απαιτούν σταδιακή διεκπεραίωση συναλλαγών, καθώς και η παρεχόμενη ασφάλεια στη διαδικασία ηλεκτρονικών συναλλαγών. Το βασικό πλεονέκτημα εστιάζεται στη δυνατότητα ελέγχου και διεκπεραίωσης συναλλαγών ενός λογαριασμού από ένα ή και περισσότερους χρήστες ανεξάρτητα από τη γεωγραφική τους θέση ή το ωράριο εργασίας τους.

Μέσα από την υπηρεσία παρέχονται τα ακόλουθα επίπεδα πρόσβασης στους χρήστες:

- **Περιορισμένη Πρόσβαση:** Δυνατότητα ενημέρωσης για υπόλοιπα και κινήσεις λογαριασμών.
- **Ελεγχόμενη Πρόσβαση:** Δυνατότητα ενημέρωσης για υπόλοιπα και κινήσεις λογαριασμών, και δυνατότητα καταχώρησης συναλλαγών που απαιτούν έγκριση από χρήστη με Πρόσβαση Εγκρίσεων ή Σύνθετη Πρόσβαση.
- **Πρόσβαση Εγκρίσεων:** Δυνατότητα ενημέρωσης για υπόλοιπα και κινήσεις λογαριασμών, και δυνατότητα έγκρισης συναλλαγών που καταχωρούνται από χρήστες με Ελεγχόμενη Πρόσβαση.

- **Πλήρης Πρόσβαση:** Δυνατότητα ενημέρωσης για υπόλοιπα και κινήσεις λογαριασμών, και δυνατότητα άμεσης εκτέλεσης συναλλαγών.
- **Σύνθετη Πρόσβαση:** Δυνατότητα ενημέρωσης για υπόλοιπα και κινήσεις λογαριασμών, δυνατότητα άμεσης εκτέλεσης συναλλαγών, και δυνατότητα έγκρισης συναλλαγών που καταχωρούνται από χρήστες με Ελεγχόμενη Πρόσβαση.

Στην περίπτωση φυσικών προσώπων, ο νόμιμος κάτοχος των λογαριασμών/ καρτών μπορεί να φέρει τα ακόλουθα επίπεδα πρόσβασης για κάθε λογαριασμό του: Περιορισμένη Πρόσβαση, Πλήρη Πρόσβαση, ή Σύνθετη Πρόσβαση. Επιπρόσθετα, έχει τη δυνατότητα να αποδώσει σε τρίτα πρόσωπα παράλληλη πρόσβαση στους λογαριασμούς του.

Στην περίπτωση νομικών προσώπων, το Διοικητικό Συμβούλιο έχει τη δυνατότητα να διορίσει φυσικά πρόσωπα ως χρήστες, προσδίδοντας τους διαφορετικά δικαιώματα πρόσβασης στους λογαριασμούς που ελέγχει. Ένας εκ των χρηστών, ο οποίος πρέπει να φέρει δικαίωμα υπογραφής (authorized signatory), καθορίζεται ως ο Διαχειριστής Λογαριασμών. Οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν ένα από τα επίπεδα πρόσβασης που παρέχει η υπηρεσία στους συνδεδεμένους τους λογαριασμούς. Πέραν από τα δικαιώματα που απορρέουν από τα Επίπεδα Πρόσβασης, ο Διαχειριστής Λογαριασμών μπορεί επιπρόσθετα να διαχειρίζεται την υπηρεσία για να:

- Προσθέτει νέους και να αφαιρεί υφιστάμενους λογαριασμούς από την υπηρεσία.
- Επηρεάζει τη δυνατότητα άλλων χρηστών για μεταφορά χρημάτων από και προς τους λογαριασμούς που διαχειρίζεται.
- Αφαιρεί και να τροποποιεί τα δικαιώματα χρηστών με Περιορισμένη ή Ελεγχόμενη Πρόσβαση στους λογαριασμούς που διαχειρίζεται.

9.6.3 Τεχνικές Προδιαγραφές

Οι ελάχιστες προδιαγραφές που θα πρέπει να έχει ο ηλεκτρονικός υπολογιστής του χρήστη και τα λογισμικά προγράμματα είναι:

- Ηλεκτρονικός υπολογιστής με λειτουργικό σύστημα Windows 98 ή νεότερο, Linux, Macintosh, Apple.
- Μνήμη 64MB RAM ή μεγαλύτερη.
- Ανάλυση οθόνης 1024x768 pixels.
- Πλοηγό διαδικτύου Microsoft Internet Explorer 5.5 ή Netscape Communicator 6.x ή νεότερο.
- Τηλεπικοινωνιακή σύνδεση με ταχύτητα σύνδεσης 56Kbps ή ταχύτερη.

9.6.4 Ασφάλεια

Το Alpha Web Banking προσφέρει τα ακόλουθα μέτρα για την ασφαλή διεκπεραίωση των συναλλαγών του κάθε χρήστη.

- **Τη μυστικότητα και το αναλλοίωτο των δεδομένων:** Εξασφαλίζονται μέσω του πρωτοκόλλου επικοινωνίας SSL 128 bit encryption.

- **Την αυθεντικότητα του χρήστη:** Το Alpha Express Banking "αναγνωρίζει" τους χρήστες και επιτρέπει την πρόσβαση τους στο σύστημα, με τους κωδικούς User ID και PIN. Σε περίπτωση εισαγωγής διαδοχικά λανθασμένων κωδικών, η σύνδεση απενεργοποιείται, ο μυστικός κωδικός αχρηστεύεται και εκδίδεται νέος μυστικός κωδικός μετά από σχετική αίτηση του χρήστη προς την Τράπεζα.
- **Την αυθεντικότητα της Τράπεζας:** Η Alpha Bank έχει προμηθευτεί πιστοποιητικό αυθεντικότητας της παρουσίας της στο Διαδίκτυο από τη διεθνώς αναγνωρισμένη εταιρία VeriSign. Το πιστοποιητικό εμφανίζεται στον χρήστη κάθε φορά που χρησιμοποιεί την υπηρεσία, με τη μορφή κλειδαριάς στο κάτω τμήμα της οθόνης. Επιπλέον, εμφανίζεται πιστοποιητικό υπογραφής προγραμμάτων της VeriSign, το οποίο πιστοποιεί τη γνησιότητα των προγραμμάτων του συστήματος.
- **Την αυθεντικότητα των συναλλαγών:** Στις περιπτώσεις έγκρισης συναλλαγών από χρήστες με Ελεγχόμενη Πρόσβαση καθώς και στις περιπτώσεις αποστολής συναλλαγών από χρήστες με Πληρη Πρόσβαση, απαιτείται η χρήση Πρόσθετων Κωδικών Ασφαλείας. Οι κωδικοί αυτοί αποτελούν την ηλεκτρονική επιβεβαίωση του χρήστη που εγκρίνει τις συναλλαγές για την ορθότητα και αυθεντικότητα των στοιχείων των συναλλαγών που θα εκτελεσθούν από την Alpha Bank.

Επίλογος

Ολοκληρώνοντας αυτήν την εργασία και με βάση τα αποτελέσματα τα οποία προέκυψαν από ερευνες , 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 που δεν είναι ακόμα ευρέων 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, 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 είναι ότι δεν χρειάζεται πια να περιμένουν με τις ώρες στις ουρές των τραπεζών για να πραγατοποιήσουν 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 αποτελέσματα 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

C. Anley, “Advanced SQL Injection in SQL Server Applications”, White paper, Next Generation Security Software Ltd, 2002, Retrieved from http://www.ngssoftware.com/papers/advanced_sql_injection.pdf

C. Anley, “(more) Advanced SQL Injection”, White paper, Next Generation Security Software Ltd, 2002, Retrieved from http://www.ngssoftware.com/papers/more_advanced_sql_injection.pdf

S. Boyd and A. Keromytis, “SQLrand: Preventing SQL Injection Attacks”, In Proceedings of the 2nd Applied Cryptography and Network Security Conference (ACNS), pp 292–302, June 2004

1.Carl Shapiro, Hal R. Varian «Οδηγός στρατηγικής στη δικτυακή οικονομία»
Εκδόσεις Καστανιώτη 2002

Dixon, Mary, Dixon, Brian <<SAMS TEACH YOURSELF E-BANKING>>
e-Book edition 2000

Αγγέλης, Βασίλειος Γ. <<Η βίβλος του e-banking >> Εκδόσεις Νέων Τεχνολογιών

Δικτυακοί Τόποι

http://www.wikipedia.org
http://www.go-online.gr
http://www.networkworld .com
http://www.bworldonline .com
http://www.nbg.gr
http://www.bankofcyprus.com
http://www.marfinegnatiabank.gr
http://www.hellenicbank.com
http://www.piraeusbank.gr/
http://www.alpha.gr/

Παραρτήματα

Παράρτημα 1

24ωρες τραπεζικές συναλλαγές Απαντά ο διευθυντής Ηλεκτρονικής Τραπεζικής και Καρτών της Τράπεζας Πειραιώς κ. Σ. Συρμακέζης

Γ. ΠΑΠΑΪΩΑΝΝΟΥ

Η υποδομή ασφαλείας των τραπεζικών συναλλαγών μέσω του Internet, δηλαδή του e-banking, τόσο στην Ελλάδα όσο και παγκοσμίως, ακολουθεί συγκεκριμένα πρότυπα ασφαλείας. Αυτό επισημαίνει ο κ. Σ. Συρμακέζης, διευθυντής Ηλεκτρονικής Τραπεζικής και Καρτών της Τράπεζας Πειραιώς. Προσθέτει δε ότι θεωρητικά η ασφάλεια μέσω Internet είναι πολύ μεγαλύτερη από αυτήν μέσω των παραδοσιακών μέσων εκτέλεσης συναλλαγών (κατάστημα, τηλέφωνο, ΑΤΜ κτλ.) καθώς όλη η επικοινωνία είναι κρυπτογραφημένη με μεθόδους που κάνουν αδύνατη την αποκρυπτογράφηση.
- Κύριε Συρμακέζη, μετά τις ΑΤΜ οι πελάτες των τραπεζών εξοικειώνονται τώρα και με το e-banking. Ποιες είναι οι υπηρεσίες που προσφέρονται σήμερα μέσω του Διαδικτύου και τι κερδίζουν όσοι τις χρησιμοποιούν;
«Με το e-banking ο πελάτης μπορεί πράγματι να γίνει "τραπεζίτης του εαυτού του". Έχει άμεση και πλήρη εικόνα όλων των τραπεζικών προϊόντων του με μια ματιά. Για τους τραπεζικούς λογαριασμούς του μπορεί να βλέπει τα διαθέσιμα και λογιστικά υπόλοιπά τους καθώς και όλες τις κινήσεις τους σε αρκετό βάθος χρόνου, ενώ έχει πλήρη διαχείριση των επιταγών του. Αντίστοιχα έχει αναλυτική πληροφόρηση για τις πιστωτικές κάρτες του καθώς μπορεί να δει τα όριά τους, τα τρέχοντα υπόλοιπά τους και όλες τις συναλλαγές τους. Το πιο σημαντικό όμως είναι η δυνατότητα πληρωμών. Π.χ., εν όψει των διακοπών του μπορεί να στείλει την προκαταβολή για το ξενοδοχείο χωρίς να μετακινηθεί αλλά και να ζητήσει να γίνει η πληρωμή διδάκτρων κατά τη διάρκεια της απουσίας του. Επιπλέον μπορεί να ορίσει την πληρωμή του ενοικίου του την πρώτη ημέρα κάθε μήνα καθώς και τη μεταφορά ενός σταθερού ποσού τη 15η ημέρα κάθε μήνα στον λογαριασμό του παιδιού του που σπουδάζει. Ακόμη ο πελάτης μπορεί να πληρώσει τον ΦΠΑ, το ΙΚΑ και το ΤΕΒΕ και την πιστωτική του κάρτα καθώς και να εξοφλήσει τους λογαριασμούς του (ΟΤΕ, ΔΕΗ, κινητή τηλεφωνία κτλ.). Οι πελάτες-κάτοχοι μετοχών έχουν άμεση πρόσβαση στο χαρτοφυλάκιο των μετοχών τους, με άμεση ενημέρωση για την τιμή κάθε μετοχής τους, ενώ βέβαια μπορούν να πουλήσουν μετοχές τους και να αγοράσουν νέες μετοχές κατά τη διάρκεια της συνεδρίασης του Χρηματιστηρίου. Ορισμένες τράπεζες μάλιστα, όπως η Τράπεζα Πειραιώς, δίνουν στον πελάτη τους τη δυνατότητα να ορίζει τηλε-ειδοποιήσεις (alerts) ώστε, όπου και αν βρίσκεται, να ενημερώνεται άμεσα με SMS ή/και e-mail κάθε φορά που οι λογαριασμοί του χρεώνονται ή πιστώνονται. Οι πελάτες που ξεκινούν να αξιοποιούν τις υπηρεσίες ebanking - εφόσον μείνουν ικανοποιημένοι - σπανίως επιστρέφουν στα ταμεία των καταστημάτων. Εχουν στα χέρια τους ό,τι χρειάζονται για να εκτελέσουν το 80% των συναλλαγών τους (όσων δεν εμπεριέχουν μετρητά), 24 ώρες την ημέρα, επτά ημέρες την εβδομάδα, χωρίς να χρειάζεται να μετακινηθούν και να χάσουν χρόνο».

- Υπάρχει διαφοροποίηση στα τιμολόγια που χρεώνουν οι τράπεζες για συναλλαγές μέσω του γκισέ και μέσω του Δικτύου;

«Στην Τράπεζα Πειραιώς παρέχουμε γενική έκπτωση 30% στις προμήθειες εκτέλεσης εμβασμάτων μέσω Internet, ενώ σύντομα η έκπτωση θα είναι ακόμη μεγαλύτερη. Επίσης όλες οι πληρωμές για τις οποίες υπάρχει χρέωση προμήθειας στο ταμείο (λ.χ., ΦΠΑ, ΙΚΑ, ΤΕΒΕ) παρέχονται χωρίς αντίστοιχη χρέωση μέσω Internet. Για την πρόσβαση στην υπηρεσία υπάρχει εφάπαξ χρέωση τριών ευρώ, ενώ δεν υπάρχει οποιαδήποτε άλλη χρέωση συνδρομητικής φύσης».

- Πόσο ασφαλείς είναι οι συναλλαγές μέσω του Διαδικτύου και τι θα λέγατε σε κάποιον για να τον πείσετε να χρησιμοποιήσει το e-banking;

«Η υποδομή ασφαλείας του e-banking, τόσο στην Ελλάδα όσο και παγκοσμίως, ακολουθεί συγκεκριμένα πρότυπα ασφαλείας. Από θεωρητική άποψη η ασφάλεια μέσω Internet είναι πολύ μεγαλύτερη από αυτήν μέσω των παραδοσιακών μέσων εκτέλεσης συναλλαγών (κατάστημα, τηλέφωνο, ΑΤΜ κτλ.) καθώς όλη η επικοινωνία είναι κρυπτογραφημένη με μεθόδους που κάνουν αδύνατη την αποκρυπτογράφηση. Από πρακτική άποψη οι "απάτες" στο Internet banking είναι απειροελάχιστες συγκρινόμενες με αυτές των παραδοσιακών μέσων. Αυτονόητο είναι βέβαια ότι οι πελάτες πρέπει να δείχνουν ιδιαίτερη προσοχή στο να μη διαρρεύσουν οι κωδικοί πρόσβασης που τους δίνουμε. Ειδικά για τις επιχειρήσεις το e-banking παρέχει τη δυνατότητα επιλεκτικής πρόσβασης στους εξουσιοδοτημένους υπαλλήλους. Η ίδια η επιχείρηση καθορίζει ποιοι θα έχουν πρόσβαση, ποιες συναλλαγές μπορεί να εκτελεί κάθε υπάλληλος, ποιο είναι το μέγιστο ποσό, καθώς και αν απαιτούνται δύο υπογραφές».

- Ποιες είναι οι εκτιμήσεις σας για την πορεία του e-banking και ποια νέα προϊόντα και υπηρεσίες ετοιμάζουν οι τράπεζες;

«Κοιτάξτε, δεν είναι τυχαίο ότι το e-banking είναι μία από τις ελάχιστες διαδικτυακές υπηρεσίες που κερδίζουν σταθερά έδαφος. Στην Τράπεζα Πειραιώς οι συναλλαγές μέσω Winbank Internet παρουσιάζουν ραγδαία ανάπτυξη: το 2003 οι εγχρήματες συναλλαγές αυξάνονται με ρυθμό της τάξεως του 150% έναντι του 2002. Επίσης συμμετέχουν σημαντικά στο σύνολο των τραπεζικών συναλλαγών: το 50% όλων των πληρωμών ΙΚΑ γίνεται μέσω Internet ενώ οι χρηματιστηριακές συναλλαγές μέσω Internet αποτελούν πάνω από 15% του συνόλου. Οι πελάτες των ελληνικών τραπεζών θα πρέπει πρώτα να αφομοιώσουν αυτά που ήδη τους προσφέρονται ώστε να είναι σε θέση να αξιοποιήσουν και τις μελλοντικές υπηρεσίες. Γι' αυτό καλό θα είναι οι τράπεζες, αντί να τους "βομβαρδίζουμε" με νέες δυνατότητες, να ρίξουμε το βάρος των προσπαθειών μας στη βελτίωση της ευχρηστίας, στην αύξηση της ταχύτητας και στη μεγιστοποίηση της διαθεσιμότητας των συστημάτων μας, καθώς και στην ελαχιστοποίηση των προβλημάτων τηλεφωνικής εξυπηρέτησης των πελατών μας, προσκαλώντας όλο και περισσότερους νέους πελάτες στην ηλεκτρονική πολιτεία των e-bankers».

Το ΒΗΜΑ, 17/08/2003 , Σελ.: D24
Κωδικός άρθρου: B13940D241

Παράρτημα 2
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 κών, 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:2602002]

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

4/12/07 Ναυτεμπορική Σελίδα 6

Παράρτημα 3

Νέο πεδίο «αναμέτρησης» των τραπεζών
* Το Διαδίκτυο μειώνει δραστικά το λειτουργικό κόστος των τραπεζικών ιδρυμάτων και προσελκύει πελατεία

Μεγαλύτερη στροφή προς τη σύγχρονη τεχνολογία για την παροχή προϊόντων και υπηρεσιών προκειμένου να επιτύχουν διεύρυνση των μεριδίων αγοράς με χαμηλότερο κόστος πραγματοποιούν οι ελληνικές τράπεζες. Το χαμηλότερο κόστος αποτελεί σημείο-κλειδί για την ανάπτυξη των εναλλακτικών δικτύων παροχής τραπεζικών υπηρεσιών (προσωπικός υπολογιστής, σταθερό ή κινητό τηλέφωνο, αυτόματες\ ταμειολογιστικές μηχανές) καθώς, αν μια απλή συναλλαγή μέσω του τραπεζικού γκισέ κοστολογείται 320 δρχ., τότε το κόστος της μειώνεται στις 170 δρχ. αν πραγματοποιηθεί μέσω τηλεφώνου, στις 80 δρχ. αν πραγματοποιηθεί μέσω ATM και μόλις στις 10 δρχ. αν πραγματοποιηθεί μέσω Internet!
Η τραπεζική από απόσταση, χωρίς τη μεσολάβηση του παραδοσιακού τραπεζικού καταστήματος, λαμβάνει ολοένα και μεγαλύτερες διαστάσεις στο εξωτερικό, όπου οι «εικονικές» τράπεζες αυξάνονται με καταιγιστικούς ρυθμούς προσελκύοντας στα ηλεκτρονικά γκισέ ολοένα περισσότερους καταναλωτές. Σύμφωνα με στοιχεία της Ενωσης Γερμανικών Τραπεζών, πάνω από το 40% των Γερμανών που κάνουν χρήση του Διαδικτύου πραγματοποιούν «ιντερνετικές» τραπεζικές συναλλαγές, ενώ στις ΗΠΑ 22.800.000 οικογένειες έχουν πρόσβαση σε κάποια υπηρεσία Internet banking.
* Εναλλακτικά δίκτυα διανομής
Η αγορά των Ηνωμένων Πολιτειών κατέχει βεβαίως τα πρωτεία στη χρήση του Διαδικτύου στις χρηματοοικονομικές συναλλαγές, με αποτέλεσμα οι εικονικές τράπεζες στις ΗΠΑ να έχουν αυξηθεί από 24 το 1999 σε 44 το 2000 ενώ εφέτος εκτιμάται ότι θα φθάσουν τις 64. Μερικές από τις γνωστότερες αμερικανικές εικονικές τράπεζες είναι η Virtual, η WingSpan, η SFNB, η Wells Fargo και η Capital One, ενώ, όπως διαπιστώνει μελέτη του GartnerGroup (Σεπτέμβριος 2000), ως το τέλος του 2001 το 70% των αμερικανικών τραπεζών θα έχουν συγκεντρώσει όλα τα εναλλακτικά τους δίκτυα διανομής προϊόντων και υπηρεσιών (Internet, Call Center, ATM) υπό ενιαίο και ξεχωριστό για την καθεμιά φορέα. Σημειώνεται ότι στις ΗΠΑ οι οικογένειες που πληρώνουν τους λογαριασμούς τους on line αναμένεται να αυξηθούν κατά 40 φορές ως το 2005. Στην Ευρώπη ο αριθμός των... εραστών της σύγχρονης τραπεζικής αυξάνεται με εντυπωσιακούς ρυθμούς καθώς το φλερτ αυτό ενισχύεται τόσο από τους χρηματοοικονομικούς οργανισμούς που επιδιώκουν να φθάσουν σε μεγαλύτερες μάζες καταναλωτών με το μικρότερο δυνατόν κόστος όσο και από την προοπτική εφαρμογής του ενιαίου νομίσματος που βρίσκεται προ των πυλών. Σύμφωνα με έρευνα της JP Morgan που πραγματοποιήθηκε τον Ιούνιο του 2000, στη Γερμανία 1.500.000 καταναλωτές, οι οποίοι αντιπροσωπεύουν το 54% των χρηστών του Διαδικτύου στην Ευρώπη, πραγματοποιούν τραπεζικές συναλλαγές μέσω Internet, ενώ 546.500 (το 18% των χρηστών Internet στην Ευρώπη) είναι οι πελάτες της αμιγώς ηλεκτρονικής χρηματιστηριακής εταιρείας ComDirect. Στη Γαλλία και στη Σουηδία οι χρήστες του Internet για τραπεζικές συναλλαγές ανέρχονται σε 310.000 στην κάθε χώρα, στη Βρετανία φθάνουν τους 200.000, έχοντας αυξηθεί κατά 800% μέσα στο τελευταίο δωδεκάμηνο, και στην Ιταλία αριθμούν τους 150.000, με ποσοστό αύξησης κατά 275% μέσα στο τελευταίο εξάμηνο. Στην Ελλάδα ο κλάδος παροχής υπηρεσιών ηλεκτρονικής τραπεζικής (e-banking), ο οποίος αφορά παροχή προϊόντων και υπηρεσιών καθώς και διεκπεραίωση συναλλαγών μέσω ATM, Internet και σταθερού ή κινητού τηλεφώνου, αναπτύσσεται ταχύτατα, αν και υπάρχει ακόμη διστακτικότητα από τους

καταναλωτές, κυρίως λόγω της ανεπαρκούς κατανόησης των συστημάτων ασφαλείας που διέπουν συγκεκριμένες συναλλαγές εξ αποστάσεως. Παράλληλα όλες οι τράπεζες προχωρούν σε αναβάθμιση των ιστοσελίδων τους (σχεδόν το 100% των τραπεζών που δραστηριοποιούνται στην Ελλάδα έχουν μπει στο electronic banking), ενώ αυξάνονται τα sites που προσφέρουν τη δυνατότητα ηλεκτρονικών αγορών. Η μάχη των ηλεκτρονικών γκισέ δίνεται για την απόκτηση μεγαλύτερων μεριδίων του 6% των ελλήνων χρηστών, οι οποίοι, όπως προκύπτει από έρευνα του Οικονομικού Πανεπιστημίου Αθηνών, πραγματοποιούν συχνά τραπεζικές συναλλαγές μέσω Internet. Αξίζει να σημειωθεί ότι εκτιμήσεις των τραπεζιτών κάνουν λόγο για εκτίναξη του ανωτέρω ποσοστού στο 40%-50% μέσα στην προσεχή πενταετία καθώς ενεργά μέλη της αγοράς γίνονται νεαρά άτομα που είναι πιο εξοικειωμένα με τη σύγχρονη τεχνολογία.

* Καινούργιες ευκαιρίες

Όπως εκτιμούν τραπεζίτες, η ανάπτυξη των ηλεκτρονικών συναλλαγών θα δημιουργήσει νέες ευκαιρίες για την αξιοποίηση των οικονομιών κλίμακας στους χρηματοπιστωτικούς οργανισμούς παρέχοντάς τους παράλληλα τη δυνατότητα πρόσβασης ακόμη και στις πιο απομακρυσμένες αγορές. Επιπλέον τόσο η τεχνολογία της πληροφορικής όσο και οι εφαρμογές της στις τηλεπικοινωνίες θα αλλάξουν τη μορφή των παραδοσιακών τραπεζικών εργασιών αφενός στον τομέα της διαχείρισης της πληροφόρησης και αφετέρου στον ευρύτερο τομέα της τηλε τραπεζικής.

Σύμφωνα με μελέτη του αναπληρωτή καθηγητή στο Τμήμα Οικονομικών Επιστημών του Πανεπιστημίου Αθηνών και οικονομικού συμβούλου της Alpha Bank κ. Γεωργίου Προβόπουλου και του οικονομολόγου της Διεύθυνσης Οικονομικών Μελετών της Alpha Bank κ. Παναγιώτη Καπόπουλου, το μεγαλύτερο μέρος των επιπτώσεων της τεχνολογικής επανάστασης στον τομέα της διαχείρισης των πληροφοριών φαίνεται ότι έχει ήδη απορροφηθεί από τα τραπεζικά συστήματα των σύγχρονων βιομηχανικών χωρών, με p_p_p_p_p_αποτέλεσμα η καθημερινή τραπεζική εργασία σήμερα να μην έχει καμία σχέση με εκείνη προ δεκαπενταετίας.

Όπως εκτιμούν οι κκ. Προβόπουλος και Καπόπουλος, η τραπεζική Διαδικτύου θα επιφέρει τρεις σημαντικές μεταβολές στη δομή του χρηματοοικονομικού συστήματος. Πρώτον, θα επιφέρει συνθήκες πλήρους ανταγωνισμού στην τραπεζική αγορά, με αποτέλεσμα να μειωθεί το πάγιο κόστος για τη δημιουργία μιας τράπεζας, μιας χρηματιστηριακής ή μιας ασφαλιστικής εταιρείας κ.ο.κ., ενώ παράλληλα θα αυξηθεί σημαντικά η σημασία του μεταβλητού κόστους για την παροχή on line διευκολύνσεων.

Δεύτερον, το Διαδίκτυο θα δημιουργήσει στους χρηματοοικονομικούς οργανισμούς νέες ευκαιρίες κερδοφορίας καθώς θα ευνοήσει την ανάπτυξη νέων προϊόντων και την υλοποίηση καινοτομιών στην παροχή υπηρεσιών υψηλότερης ποιότητας. Νέες σχέσεις με την πελατεία θα οικοδομηθούν και ρηξικέλευθες ιδέες μάρκετινγκ θα εφαρμοστούν με στόχο την εμπέδωση μιας μοντέρνας και δυναμικής εταιρικής ταυτότητας, καθώς και την αύξηση της αξίας του οργανισμού για τον μέτοχο.

ΟΙ ΤΡΑΠΕΖΕΣ ΤΟΥ INTERNET

Αλλαγή οργανωτικής δομής
Η τραπεζική Διαδικτύου θα αλλάξει δραστικά την υφιστάμενη οργανωτική δομή των τραπεζικών σχημάτων οδηγώντας σε πιο ευέλικτες εργασιακές σχέσεις και σε εκτεταμένη αναδιάρθρωση (ή ακόμη και σχετική απαξίωση) της υπάρχουσας υποδομής και των δικτύων. Οι τεχνολογικές εξελίξεις θα αναμορφώσουν σημαντικά το τοπίο του τραπεζικού ανταγωνισμού τόσο από την πλευρά της ζήτησης, καθώς οι πελάτες θα μπορούν ευκολότερα να προβαίνουν σε συγκρίσεις προϊόντων και να επιλέγουν αναλόγως, όσο και από την πλευρά της προσφοράς, καθώς τα εμπόδια εισόδου στην αγορά, κυρίως της λιανικής τραπεζικής, θα υποχωρήσουν αισθητά αφού οι τράπεζες Διαδικτύου έχουν πολύ μικρότερο πάγιο κόστος εγκατάστασης. Παράλληλα με την αλλαγή του τοπίου σε επίπεδο ανταγωνισμού οι τράπεζες θα έχουν να αντιμετωπίσουν και διαφορετικής φύσεως κινδύνους. Όπως επισημαίνουν τραπεζίτες, η ανάπτυξη της ηλεκτρονικής τραπεζικής αφενός εγείρει κινδύνους που συνδέονται με την τεχνολογία (π.χ., οι τράπεζες αντιμετωπίζουν τον κίνδυνο της επένδυσης σε τεχνολογίες που ενδέχεται να απαξιωθούν σύντομα ή να αφιερώσουν σημαντικούς πόρους στην εισαγωγή νέων προϊόντων χωρίς να έχει προηγηθεί ενδελεχής ανάλυση της ζήτησης και του βαθμού αποδοχής από την πελατεία), αφετέρου εντείνει υφισταμένους κινδύνους των τραπεζών, όπως ο λειτουργικός, ο οποίος μπορεί να αυξηθεί αν οι τράπεζες δεν αναβαθμίσουν τα συστήματα εσωτερικού ελέγχου. Επιπλέον δεν θα πρέπει να παραβλέπεται ο νομικός κίνδυνος που πηγάζει από τις δυσχέρειες στον έλεγχο της ασφάλειας των συναλλαγών στον κυβερνοχώρο. Εκείνο που επισημαίνουν όλοι οι τραπεζίτες είναι η αναγκαιότητα της εμπλοκής των τραπεζών στην ηλεκτρονική τραπεζική προκειμένου να διασφαλιστεί η ίδια η επιβίωσή τους. Οπως προαναφέρθηκε, σχεδόν όλες οι ελληνικές τράπεζες προσφέρουν ευρεία γκάμα υπηρεσιών μέσω ηλεκτρονικών γκισέ. Ωστόσο πρωτοποριακή για την ελληνική αγορά, καθώς απεικονίζει την τάση που επικρατεί στην πλέον ανεπτυγμένη τεχνολογικά οικονομία των ΗΠΑ, θεωρείται η κίνηση του ομίλου της Τράπεζας Πειραιώς να εντάξει όλες τις υπηρεσίες τηλε-τραπεζικής σε μια εξειδικευμένη ηλεκτρονική τράπεζα, τη Winbank. Οι πελάτες της Winbank έχουν ήδη ξεπεράσει τους 12.500 πελάτες, ενώ η τράπεζα προχώρησε πρόσφατα σε επένδυση άνω του 1,5 δις. δρχ. για τον εμπλουτισμό του Winbank Internet και συγκεκριμένα για την εξειδίκευσή του σε Winbank Internet personal για τους ιδιώτες πελάτες και Winbank Internet business για τις επιχειρήσεις.

ΝΕΝΑ ΜΑΛΛΙΑΡΑ
Το ΒΗΜΑ, 17/06/2001 , Σελ.: D10
Κωδικός άρθρου: B13289D101
ID: 236315

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.

WWW.NUKED.GR

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. Οπως 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