Ηλεκτρονική τραπεζική

Στροφή από τις τράπεζες στα εναλλακτικά δίκτυα
Καλύτερη εξυπηρέτηση για τον καταναλωτή

Επιμέλεια: **ΕΦΗ ΚΑΡΑΓΕΩΡΓΟΥ**
Δημοσιογράφος

Καθώς τα περιθώρια διαφοροποίησης σε νέα προϊόντα και επιτόκια στενεύουν, οι τράπεζες στρέφονται σε νέες υπηρεσίες προκειμένου να προσελκύσουν πελάτες αλλά και να μειώσουν τα λειτουργικά τους έξοδα διατηρώντας ή/και αυξάνοντας με τον τρόπο αυτό εμμέσως την κερδοφορία τους. Νέο «πεδίο μάχης» στο χρηματοπιστωτικό τομέα θα αποτελέσουν τα εναλλακτικά δίκτυα.

Στόχος είναι:

- να περιοριστούν οι συναλλαγές στο κατάστημα στις πλέον εξειδικευμένες (π.χ. private banking, χορηγήσεις δανείων, επενδυτικές υπηρεσίες), μεταφέροντας αναλήψεις, καταθέσεις και πληρωμές στα εναλλακτικά δίκτυα,
- να δημιουργηθεί ένα σύστημα εύκολο στη χρήση, που να καλύπτει όλες τις ανάγκες των συναλλασσομένων και να είναι απόλυτα ασφαλές,
- να εξοικειωθούν οι πελάτες των τραπεζών με τη χρήση των εναλλακτικών δικτύων και να γνωρίσουν τα πλεονεκτήματα που αυτά τους προσφέρουν.

Μέσω των ηλεκτρονικών δικτύων, οι τράπεζες είναι πλέον σε θέση να καλύπτουν το σύνολο της χώρας, ακόμη και τις περιοχές εκείνες όπου, λόγω διαφόρων παραγόντων π.χ. γεωγραφική θέση, δεν είναι εφικτή η λειτουργία καταστήματος.

Η μείωση των λειτουργικών εξόδων που επιτυγχάνεται με τη χρήση των εναλλακτικών δικτύων δικαιολογεί την προσπάθεια εξάπλωσής τους: Ενώ μια συναλλαγή στο γκισέ κοστίζει στην τράπεζα περίπου 1,5 ευρώ (σε εργατοώρες, κόστος λειτουργίας καταστημάτων κ.λπ.) η ίδια συναλλαγή κοστίζει μόλις 0,25 ευρώ, αν πραγματοποιηθεί ηλεκτρονικά.

Οι οικονομίες κλίμακας που εξασφαλίζονται είναι ιδιαίτερα σημαντικές, ενώ οι επενδύσεις σε τεχνολογία που πραγματοποιούνται αφορούν ολόκληρο τον όμιλο της κάθε τράπεζας και –με μικρές διαφοροποιήσεις– χρησιμοποιούνται σε όλες τις χώρες όπου αυτή δραστηριοποιείται.

Επιλέγοντας να χρησιμοποιήσουν τα εναλλακτικά δίκτυα, οι πελάτες των τραπεζών ωφελούνται διπλά:

- δεν περιορίζονται από το τραπεζικό ωράριο, καθώς έχουν τη δυνατότητα να διενεργούν συναλλαγές όλο το 24ωρο, όλες τις ημέρες της εβδομάδας, από όπου και αν βρίσκονται,
- απολαμβάνουν ιδιαίτερα ευνοϊκής τιμολογιακής πολιτικής.

Για παράδειγμα, μεγάλος αριθμός συναλλαγών όπως π.χ. η μεταφορά χρημάτων από λογαριασμό σε λογαριασμό της ίδιας τράπεζας, η ενημέρωση υπολοίπου, η κατάθεση χρημάτων σε λογαριασμό τρίτου που τηρείται στην ίδια τράπεζα (π.χ. για πληρωμή ενοικίου) και η πληρωμή ΦΠΑ είναι δωρεάν, αν πραγματοποιηθούν μέσω internet ή τηλεφώνου, ενώ σε κάθε περίπτωση η χρέωση είναι ιδιαίτερα χαμηλή συγκρινόμενη με τις αντίστοιχες προμήθειες για τις συναλλαγές που πραγματοποιούνται στο γκισέ.

«Κλειδί» η ασφάλεια

Η ανασφάλεια των συναλλασσομένων και η έλλειψη εξοικείωσης με τις νέες τεχνολογίες είναι τα δύο μεγάλα εμπόδια που πρέπει να ξεπεράσουν οι υπέρμαχοι των εναλλακτικών δικτύων. Ενδεικτικό είναι ότι το ποσοστό διείσδυσης του internet στη χώρα μας είναι από τα χαμηλότερα στην ευρωζώνη, ενώ ακόμα λιγότεροι είναι εκείνοι που πραγματοποιούν ηλεκτρονικές συναλλαγές. Υπολογίζεται ότι μόνο 350.000 περίπου πελάτες των τραπεζών πραγματοποιούν ηλεκτρονικές συναλλαγές, το ύψος των οποίων ανήλθε πέρυσι σε 10 δισ. ευρώ περίπου.

Το αίσθημα της ασφάλειας των συναλλασσομένων αποτελεί αναγκαία προϋπόθεση για την αποτελεσματική διείσδυση των εναλλακτικών δικτύων σε μεγαλύτερες ομάδες πληθυσμού. Τα συστήματα αναγνώρισης εξελίσσονται διαρκώς, ενσωματώνοντας και βιομετρικά χαρακτηριστικά, όπως για παράδειγμα η χροιά της φωνής στις τηλεφωνικές συναλλαγές και τα δακτυλικά αποτυπώματα για τραπεζικές εργασίες μέσω internet. Στην κατεύθυνση αυτή οι τράπεζες εφοδιάζουν τους πελάτες τους με ξεχωριστούς κωδικούς μιας χρήσης για κάθε συναλλαγή που πραγματοποιούν, ενώ άλλες στέλνουν ειδικούς κωδικούς με μήνυμα sms στο κινητό του χρήστη για συγκεκριμένες συναλλαγές που απαιτούν αυξημένη ασφάλεια (π.χ. μεταφορές προς τρίτους, μαζικά εμβάσματα).

ATM

Σήμερα το 55% των τραπεζικών συναλλαγών πραγματοποιείται μέσω των ATM, τα οποία σε πολλές περιπτώσεις έχουν αντικαταστήσει το τραπεζικό γκισέ.

Αξίζει να σημειωθεί ότι, σε ετήσια βάση, μέσω των ATM πραγματοποιούνται περισσότερες από 100 εκ. συναλλαγές. Στη συντριπτική πλειοψηφία –ποσοστό 70%– οι συναλλαγές που πραγματοποιούν οι καταναλωτές στα ATM αφορούν ανάληψη μετρητών και ακολουθεί με 25% η ερώτηση υπολοίπου, ενώ 5% αφορά διάφορες άλλες συναλλαγές (πληρωμές, μεταφορές χρημάτων κ.λπ.).

Τα κρούσματα απάτης παραμένουν σε ιδιαίτερα χαμηλά επίπεδα, καθώς δεν ξεπερνούν τα 30 το μήνα, ενώ τα «χτυπήματα» που συνολικά δέχονται οι τράπεζες είναι πάνω από 200.

Internet

Μετά τη διαρκώς αυξανόμενη χρήση των ATM, το επόμενο βήμα είναι η επέκταση της ηλεκτρονικής και τηλεφωνικής τραπεζικής, στόχος για τον οποίο ήδη έχουν επενδυθεί δεκάδες εκατομμύρια ευρώ σε υποδομές. Η άνεση, η πληρότητα και η ασφάλεια είναι το τρίπτυχο στο οποίο θα στηριχθεί η επανάσταση των ηλεκτρονικών συναλλαγών, αναφέρουν τα αρμόδια τραπεζικά στελέχη. Ο τραπεζικός πελάτης έχει σήμερα στη διάθεσή του:

- Τραπεζικές συναλλαγές μέσω τηλεφώνου (κινητό-σταθερό) μόνο με φωνητικές εντολές
- Πλήρες «πακέτο» συναλλαγών και υπηρεσιών όλο το 24ωρο
- Μετατροπή της οθόνης του υπολογιστή σε ATM
- Βελτιωμένα συστήματα ασφαλείας με χρήση ειδικών, προσωπικών κωδικών
- Αυτοματοποιημένα συστήματα συναλλαγών χωρίς την παρουσία εκπροσώπου της τράπεζας

Σύμφωνα με αξιόπιστες έρευνες, οι υπηρεσίες internet banking που προσφέρουν οι ελληνικές τράπεζες είναι καλύτερες από τις αντίστοιχες ευρωπαϊκές, και καλύπτουν μεγάλη γκάμα προϊόντων και υπηρεσιών.

Η πλέον συνηθισμένη συναλλαγή μέσω internet banking είναι η αποστολή εμβάσματος (55% των συναλλαγών πραγματοποιείται μέσω internet) και ακολουθούν οι χρηματιστηριακές συναλλαγές (το 22% πραγματοποιείται μέσω διαδικτύου), οι πληρωμές ΦΠΑ, ΙΚΑ, ΤΕΒΕ (είναι χαρακτηριστικό ότι το 70% των συγκεκριμένων πληρωμών γίνονται μέσω του e-banking), καθώς και οι μεταφορές σε λογαριασμούς τρίτων.

Νέες υπηρεσίες

Ενδεικτικά της επανάστασης που πραγματοποιείται στο χώρο της ηλεκτρονικής και τηλεφωνικής τραπεζικής είναι τα νέα συστήματα συναλλαγών που επιχειρούν να εγκαταστήσουν οι τράπεζες.

Το τηλέφωνο, κινητό ή σταθερό, είναι το μέσο που έχουν επιλέξει οι τράπεζες για να «στήσουν» τις υπηρεσίες νέας γενιάς. Και αυτό –σε αντίθεση με το internet– λόγω της εξοικείωσης του συνόλου του πληθυσμού με την τηλεφωνική συσκευή. Ήδη αρκετές τράπεζες επιτρέπουν στους πελάτες τους να πραγματοποιήσουν μέσω του τηλεφώνου –σταθερού ή κινητού– σειρά από συναλλαγές, ενώ σύντομα αυτό θα μπορεί να γίνεται δίνοντας μόνο φωνητικές εντολές και χωρίς τη χρήση πλήκτρων. Η διαδικασία θα είναι πλήρως αυτοματοποιημένη, ενώ ο πελάτης θα μπορεί ανά πάσα στιγμή να μιλήσει με κάποιον εκπρόσωπο της τράπεζας, αν θέλει επιπλέον πληροφορίες ή έχει κάποιο ερώτημα.

Αντίστοιχα, οι χρήστες του internet θα έχουν τη δυνατότητα να μετατρέψουν την οθόνη του υπολογιστή τους σε ATM, ώστε να κάνουν τις συναλλαγές τους σε νέο περιβάλλον. Και έπεται συνέχεια, καθώς όσο βελτιώνεται η τεχνολογία, τόσο πολλαπλασιάζονται οι δυνατότητες. Η εποχή που ο υπολογιστής θα μετατρέπεται σε εικονικό κατάστημα, με τον πελάτη να περιφέρεται ψηφιακά σε αυτό πραγματοποιώντας τις συναλλαγές του, βρίσκεται προ των πυλών.

Τρόποι απάτης

Απάτη στο internet

Τεχνική phishing

Η πλέον διαδεδομένη μέθοδος κλοπής προσωπικών δεδομένων και εμπιστευτικών πληροφοριών μέσω διαδικτύου σήμερα είναι το phishing («ψάρεμα στο διαδίκτυο») .

Το phishing είναι η αποστολή e-mail από δήθεν νόμιμη επιχείρηση (συνήθως τράπεζα) με σκοπό να εξαπατήσει τον αποδέκτη του μηνύματος και να υποκλέψει ιδιωτικές πληροφορίες. Το e-mail με κάποια πρόφαση (π.χ. ενημέρωση αρχείου, επαλήθευση στοιχείων κ.λπ.) προτρέπει το χρήστη να επισκεφθεί μια ιστοσελίδα όπου του ζητείται να εισάγει τα προσωπικά του στοιχεία, όπως usernames, passwords, αριθμούς πιστωτικών καρτών, αριθμούς τραπεζικών λογαριασμών, που η εταιρεία υποτίθεται ότι ήδη έχει στην κατοχή της. Η ιστοσελίδα ωστόσο είναι πλαστή και έχει δημιουργηθεί με μοναδικό σκοπό να κλέψει τη ζητούμενη πληροφορία.

Θύματα των επιθέσεων phishing δεν είναι μόνο οι χρήστες, αλλά και οι ίδιες οι τραπεζικές επιχειρήσεις, οι οποίες αν και δεν εμπλέκονται στην απάτη, βλέπουν τη φήμη και την αξιοπιστία τους να κινδυνεύουν.

Οι επιθέσεις phishing αυξάνονται ραγδαία και με έξυπνο τρόπο. Σύμφωνα με έρευνες που διεξάγονται, ο ρυθμός εξάπλωσής τους διπλασιάζεται μέσα σε ένα εξάμηνο. Οι ίδιες έρευνες καταγράφουν ότι το phishing είναι εξαιρετικά αποτελεσματικό, γιατί:

- 90% των χρηστών μπορεί να παραπλανηθούν από μια καλή phishing ιστοσελίδα.
- 1 στους 4 χρήστες δεν κοιτάζει τις ενδείξεις ασφαλείας που υπάρχουν σε ένα web browser, όπως η διεύθυνση της ιστοσελίδας, η γραμμή κατάστασης του browser.
- Περίπου 1 στους 2 χρήστες e-banking χρησιμοποιούν τους ίδιους κωδικούς για όλες τις ηλεκτρονικές τραπεζικές υπηρεσίες που χρησιμοποιούν σε όλες τις τράπεζες.

Οι αρμόδιες υπηρεσίες ασφαλείας των τραπεζών, προκειμένου να αποφεύγονται απάτες τέτοιου τύπου, ενημερώνουν τακτικά τους χρήστες e-banking μέσω των δικτυακών τους τόπων ή ενημερωτικών φυλλαδίων. Σύμφωνα με αυτές, τα παρακάτω σημεία είναι βασικά για την αποφυγή των επιθέσεων phishing:

- Ποτέ καμία τράπεζα δεν ζητά προσωπικές πληροφορίες από τους πελάτες της μέσω e-mail ή τηλεφώνου.
- Οποιοδήποτε e-mail ζητά επειγόντως προσωπικά ή οικονομικά στοιχεία είναι ύποπτο.
- Να μη χρησιμοποιούνται ποτέ τα links που υπάρχουν σε e-mails, όταν δεν είναι βέβαιη η προέλευσή τους. Ο χρήστης πρέπει να πληκτρολογεί ο ίδιος τη διεύθυνση της ιστοσελίδας που επιθυμεί να επισκεφθεί.
- Να μη δίδονται προσωπικές πληροφορίες μέσω e-mails. Αυτές μπορούν να δίδονται μόνο μέσω ενός ασφαλούς site ή τηλεφώνου.
- Να ελέγχεται εάν η διεύθυνση της ιστοσελίδας είναι γραμμένη σωστά και επιπρόσθετα εάν ξεκινά από https:// και όχι από http://. Σημειώνεται ότι το s υποδηλώνει security δηλ. ασφάλεια, απαραίτητο όταν γίνονται τραπεζικές συναλλαγές. Η ασφάλεια της ιστοσελίδας διασφαλίζεται από την ύπαρξη εικονιδίου κλειδαριάς στη γραμμή κατάστασης του browser: ενεργοποιώντας το επιβεβαιώνεται η εγκυρότητα του ψηφιακού πιστοποιητικού, σύμφωνα με τις οδηγίες της τράπεζας.
- Να ενημερώνεται άμεσα η τράπεζα από την οποία υποτίθεται ότι προέρχεται το e-mail.

Οι τράπεζες, για την αντιμετώπιση της ηλεκτρονικής απάτης, έχουν εισαγάγει τεχνολογίες πιστοποίησης δύο παραγόντων με διάφορες μορφές (SMS, PINs, tokens, ψηφιακά πιστοποιητικά), γεγονός που σημαίνει ότι η πρόσβαση στις ασφαλείς ιστοσελίδες τους απαιτεί και ένα επιπλέον αναγνωριστικό που έχει συνήθως μικρή διάρκεια ζωής και δεν είναι τόσο εύκολο να υποκλαπεί.

Σε κάθε περίπτωση ο σωστά ενημερωμένος χρήστης έχει λιγότερες πιθανότητες να υποπέσει θύμα απάτης. Άλλωστε όπως έχει δηλώσει και ο Kevin Mitnick, ο πιο φημισμένος hacker, «ο αδύναμος κρίκος σε οποιαδήποτε απάτη είναι ο άνθρωπος».

Απάτη στα ATM

Τεχνική skimming

Η πιο διαδεδομένη μορφή απάτης που αντιμετωπίζουν οι περισσότερες χώρες είναι η μέθοδος αντιγραφής των στοιχείων της μαγνητικής ταινίας των καρτών με την τεχνική skimming. Τα στοιχεία της κάρτας διαβάζονται τη στιγμή που ο πελάτης πραγματοποιεί μια συναλλαγή στο ATM, μέσω μιας συσκευής υποκλοπής (skimmer) προσαρμοσμένης, συνήθως, με ταινία διπλής όψης, στον καρταναγνώστη του ATM. Οι κάρτες που έχουν «διαβαστεί» από το ειδικό εξάρτημα (skimmer) μπορούν αργότερα να αναπαραχθούν από τους δράστες στο «εργαστήριό τους».

Σε πολλές περιπτώσεις τα στοιχεία της κάρτας μεταδίδονται άμεσα σε κάποιο παραπλήσιο αυτοκίνητο ή μηχανή με κατάλληλο εξοπλισμό, ώστε η επεξεργασία τους να γίνεται αμέσως από τους δράστες.

Τεχνική Lebanese loop

Χρησιμοποιείται μια συσκευή παρακράτησης της κάρτας, η οποία προσαρμόζεται στον αναγνώστη καρτών του μηχανήματος (ATM).

Η συσκευή παγιδεύει την κάρτα ενώ ο πελάτης πιστεύει ότι η κάρτα του παρακρατήθηκε από δυσλειτουργία του ATM και απομακρύνεται χωρίς να ενημερώσει αμέσως την τράπεζα προκειμένου να του την απενεργοποιήσει.

Τρόποι υποκλοπής του PIN

Η απόσπαση του PIN γίνεται συνήθως με μικροκάμερες, μίνι βίντεο κάμερες ή ακόμη και χρησιμοποιώντας την κάμερα των κινητών τηλεφώνων, κατάλληλα προσαρμοσμένα στην πλαφονιέρα του ΑΤΜ, στα πλαϊνά του μέρη ή και στην τέντα ηλιοπροστασίας.

Ένας άλλος τρόπος που χρησιμοποιείται αρκετά το τελευταίο διάστημα είναι η τοποθέτηση ψεύτικου πληκτρολογίου (fake keypad) πάνω από το πραγματικό. Κατά την πληκτρολόγηση του PIN από τον κάτοχο τα στοιχεία καταγράφονται και στο ψεύτικο πληκτρολόγιο (το οποίο είναι πολύ λεπτό) με αποτέλεσμα οι δράστες να έχουν στη διάθεσή τους και το μυστικό αριθμό αναγνώρισης (PIN).

Στην περίπτωση της τεχνικής Lebanese loop, η απόσπαση του PIN γίνεται με τον τρόπο της προσφερόμενης βοήθειας από κάποιον δήθεν πελάτη που αντιμετώπισε το ίδιο πρόβλημα και παραμένει δίπλα στο ΑΤΜ, προτρέποντας το θύμα να πληκτρολογήσει το PIN του πάλι ώστε το ΑΤΜ να του βγάλει την κάρτα έξω.

Οι τράπεζες σε συνεργασία με τις προμηθεύτριες εταιρείες των ΑΤΜ, τοποθετούν ειδικούς μηχανισμούς εντοπισμού συσκευών υποκλοπής. Παράλληλα επενδύουν σημαντικά ποσά για τη θωράκισή τους απέναντι σε φαινόμενα απάτης, ενώ ιδιαίτερη έμφαση δίνουν και στη σωστή ενημέρωση της πελατείας τους. Ειδικότερα συμβουλεύουν τους πελάτες τους:

- Να χρησιμοποιούν, όσο είναι δυνατόν, τα ίδια ΑΤΜ ώστε να μπορούν να παρατηρούν τυχόν αλλαγές.
- Να ελέγχουν το χώρο του ΑΤΜ πριν από κάθε συναλλαγή (πληκτρολόγιο, φωτισμό, πλαϊνά μέρη) και να ενημερώνουν αμέσως την τράπεζα σε περίπτωση που παρατηρήσουν κάτι διαφορετικό.
- Να προφυλάσσουν το μυστικό αριθμό (PIN) κατά την πληκτρολόγησή του (π.χ. με την παλάμη του άλλου χεριού ή το πορτοφόλι).

Και φυσικά τους υπενθυμίζουν ότι δεν πρέπει να:

- σημειώνουν και φυλάσσουν PIN και κάρτα μαζί,
- γνωστοποιούν ποτέ το PIN σε συγγενικά τους πρόσωπα, σε τρίτους, σε υπαλλήλους της τράπεζας ή σε οποιαδήποτε Αρχή, ακόμη και αν αυτό τους ζητηθεί,
- εμπιστεύονται αγνώστους που θα προσφερθούν να βοηθήσουν κατά τη συναλλαγή τους στα ΑΤΜ.

Τέλος, θα πρέπει να επικοινωνούν ΜΟΝΟ στα τηλέφωνα που εμφανίζονται στην οθόνη του ΑΤΜ ή τους έχει χορηγήσει η τράπεζα με την οποία συνεργάζονται.

Οι ηλεκτρονικές διευθύνσεις των τραπεζών-τακτικών μελών της Ελληνικής Ένωσης Τραπεζών

Εθνική Τράπεζα	www.ethniki.gr
Alpha Bank	www.alpha.gr
EFG Eurobank	www.eurobank.gr
Τράπεζα Πειραιώς	www.piraeusbank.gr
ATEbank	www.ate.gr
Emporiki Bank	www.emporiki.gr
Ταχυδρομικό Ταμιευτήριο	www.ttbank.gr
Τράπεζα Κύπρου	www.bankofcyprus.gr
Citibank	www.citibank.gr
Geniki Bank	www.geniki.gr
Εγνατία Τράπεζα	www.egnatiabank.gr
Λαϊκή Τράπεζα	www.laiki.gr
HSBC	www.hsbc.gr
Millennium Bank	www.millenniumbank.gr
Attica Bank	www.atticabank.gr
Aspis Bank	www.aspisbank.gr
Probank	www.probank.gr
Bayerische Hypo Und Vereinsbank	www.hypovereinsbank.gr
Proton Bank	www.protonbank.gr
ABN-AMRO Bank	www.abnamro.com
FBB-Πρώτη Επιχειρηματική Τράπεζα	www.fbbank.gr
Ελληνική Τράπεζα	www.hellenicbank.gr
Πανελλήνια Τράπεζα	www.panelliniabank.gr
BNP Paribas	www.bnpparibas.gr