

ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ



Ασφάλεια συναλλαγών

Συμβουλές για την ασφάλεια των συναλλαγών



Phishing – Ηλεκτρονικό ψάρεμα

Phishing (ή ηλεκτρονικό ψάρεμα) είναι η κακόβουλη προσπάθεια επίδοξων απατεώνων να υποκλέψουν προσωπικά στοιχεία όπως, κωδικούς πρόσβασης web banking, αριθμούς ή PIN πιστωτικών / χρεωστικών καρτών, αριθμούς διαβατηρίων, αστυνομικών ταυτοτήτων, ΑΦΜ κλπ.

Phishing email



Πρόκειται για απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου (e-mails) που στέλνονται μαζικά σε τυχαίους λογαριασμούς ανυποψίαστων παραληπτών, όπου είτε δελεάζοντάς τους, είτε προσπαθώντας να τους πείσουν ότι είναι αναγκαίο, τους καλούν να πατήσουν σε έναν σύνδεσμο (link) που υπάρχει μέσα στο email. Ο σύνδεσμος αυτός οδηγεί σε ιστοσελίδες που έχουν φτιάξει επιτήδριοι, οι οποίες προσομοιάζουν με τις αυθεντικές ιστοσελίδες των Τραπεζών. Στόχος τους είναι να παραπλανήσουν τους χρήστες να πληκτρολογήσουν εκεί τα προσωπικά τους στοιχεία, τα οποία στη συνέχεια θα χρησιμοποιήσουν για να εισέλθουν στο περιβάλλον της ηλεκτρονικής τραπεζικής και να ενεργούν ως πραγματικοί πελάτες.

Phishing sms



Πρόκειται για απατηλά μηνύματα sms που μέσω ενός link που περιέχουν ζητούν να συνδεθείτε στη winbank επιλέγοντας αυτόν τον σύνδεσμο. Προσπαθούν να δελεάσουν τον πελάτη να επιλέξει τον σύνδεσμο χρησιμοποιώντας λεκτικό της μορφής π.χ. καλέστε έναν αριθμό για να ακυρώσετε/επαληθεύσετε μία συναλλαγή, να ξεκλειδώσετε/ενεργοποιήσετε το λογαριασμό σας, επικαιροποιήστε τα στοιχεία σας πατώντας εδώ, κλπ. Αν επιλέξετε τον κακόβουλο σύνδεσμο θα οδηγηθείτε σε περιβάλλον όμοιο με αυτό της Τράπεζας και θα σας ζητηθεί να καταχωρήσετε τους προσωπικούς σας κωδικούς και εν συνεχεία τους κωδικούς μιας χρήσης που λαμβάνετε.



Αν δηλώσετε τα στοιχεία σας όπως αναφέρεται παραπάνω οι επιτήδριοι θα εισέλθουν άμεσα στην εφαρμογή και θα έχουν τη δυνατότητα διαχείρισης των χρημάτων σας.



Phishing – Ηλεκτρονικό ψάρεμα

Τι μπορείτε να κάνετε αν δεχτείτε e-mail ή sms το οποίο περιέχει σύνδεσμο που σας προτρέπει να τον επιλέξετε για να καταχωρήσετε τα προσωπικά σας δεδομένα;

- ✓ Αποφύγετε να ανοίξετε e-mails/sms από αγνώστους σε εσάς αποστολείς.
- ✓ Σε καμία περίπτωση μη δηλώνετε τους κωδικούς σας και τα προσωπικά σας στοιχεία σε sites χωρίς πρώτα να επιβεβαιώσετε ότι ο οργανισμός που σας στέλνει το μήνυμα είναι όντως ο πραγματικός. Επίσης τα συγκεκριμένα μηνύματα συνήθως εμπεριέχουν λεκτικό με ορθογραφικά-γραμματικά ή και συντακτικά λάθη και ενδέχεται να απευθύνονται στον πελάτη με τρόπο που δεν είθισται στην επικοινωνία με την τράπεζα του (π.χ. προσφώνηση μικρού ή υποκοριστικού ονόματος κ.α.)
- ✓ Μπορείτε εύκολα επίσης να διαπιστώσετε ότι δεν προέρχονται από την Τράπεζα καθώς η διεύθυνση του αποστολέα αλλά και ο σύνδεσμος που σας ζητούν να επιλέξετε είναι διαφορετικά από αυτά της Τράπεζας μας.
- ✓ Αποφύγετε να κάνετε κλικ σε ηλεκτρονικούς συνδέσμους (links), συνημμένα αρχεία ή εικόνες που λαμβάνετε με μηνύματα κειμένου (sms) δίχως και πάλι να έχετε επαληθεύσει τον αποστολέα.
- ✓ Ποτέ μην απαντάτε σε μήνυμα κειμένου (sms) που σας ζητά τον κωδικό "PIN" ή τον κωδικό πρόσβασης ("password") στον τραπεζικό σας λογαριασμό ή οποιαδήποτε άλλα εξατομικευμένα διαπιστευτήρια ασφαλείας (π.χ. e-banking user name).



Phishing – Ηλεκτρονικό ψάρεμα



Συμβουλή

- Μην βιάζεστε. Πάρτε τον χρόνο σας και πραγματοποιήστε τους απαραίτητους ελέγχους προτού απαντήσετε.
- Εάν νομίζετε ότι ενδέχεται να έχετε απαντήσει σε ένα ύποπτο e-mail ή μήνυμα κειμένου (sms) και παρείχατε τα στοιχεία των τραπεζικών σας λογαριασμών, επικοινωνήστε αμέσως με την τράπεζα συνεργασίας σας.
- Μπορείτε να καλέσετε στο 2103288000 (24/7/365) για να μας αναφέρετε οποιοδήποτε «ύποπτο» e-mail ή sms που σας έχει σταλεί με υποτιθέμενο αποστολέα την Τράπεζα μας. Εξειδικευμένο προσωπικό θα είναι στη διάθεση σας για να σας καθοδηγήσει και να σας συμβουλευτεί.

Για την πιο άμεση εξυπηρέτηση σας μπορείτε να μας αναφέρετε περιεκτικά το λόγο κλήσης σας, ώστε να σας δοθεί προτεραιότητα μέσω της αυτοματοποιημένης πύλης φωνητικής αναγνώρισης και να επικοινωνήσετε άμεσα με εκπρόσωπο μας. (Π.χ. κακόβουλο e-mail/sms, απάτη e-banking, εξαπάτηση καρτών, phishing απάτη, κλοπή χρημάτων, αμφισβήτηση συναλλαγής κλπ.)



Μη ξεχνάτε!

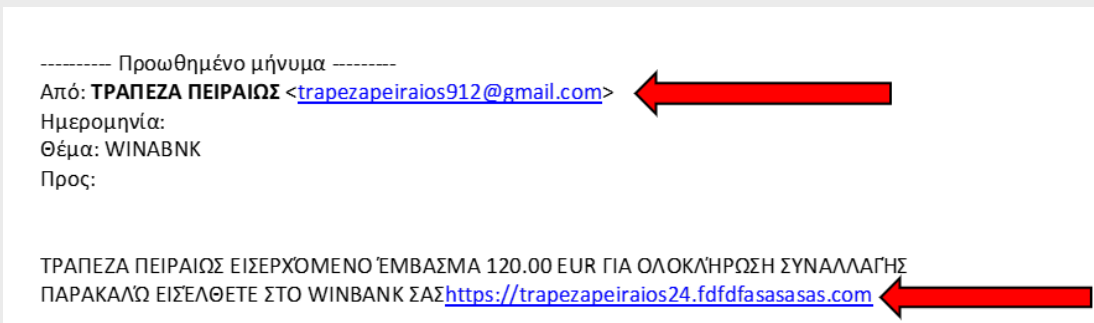
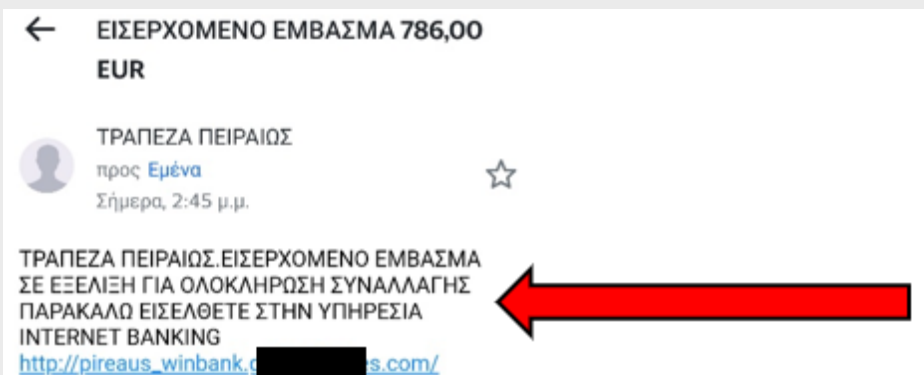
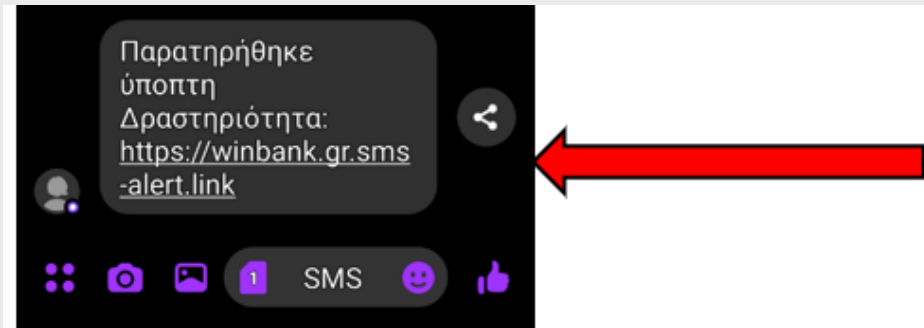
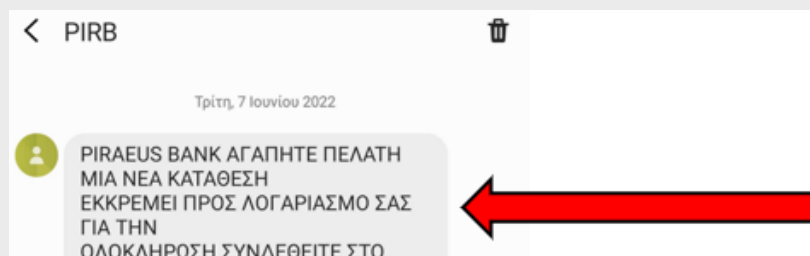
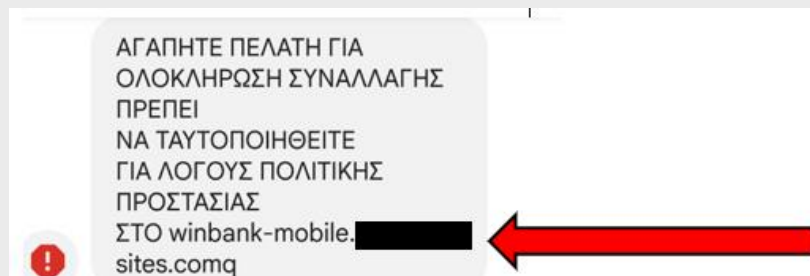
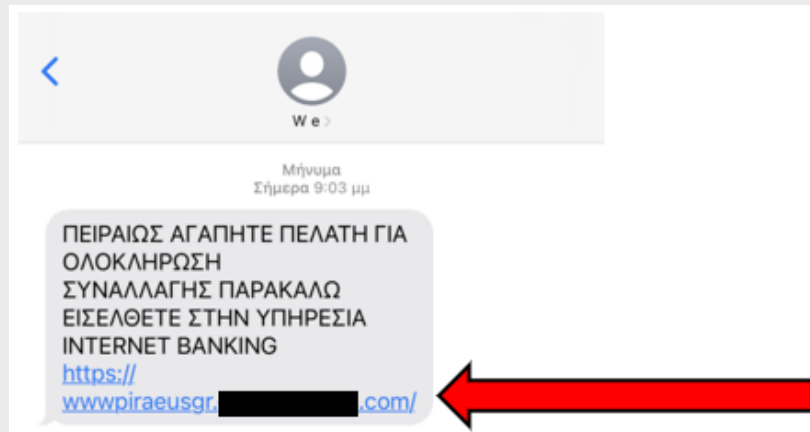
Η Τράπεζα Πειραιώς δεν θα σας ζητήσει ποτέ και με κανένα τρόπο (τηλεφωνικώς ή μέσω e-mail) στοιχεία λογαριασμών, στοιχεία καρτών, κωδικούς πρόσβασης.





Phishing – Ηλεκτρονικό ψάρεμα

Παραδείγματα





Phishing – Ηλεκτρονικό ψάρεμα

Παραδείγματα

----- Αρχικό μήνυμα -----

Θέμα: Νέα επιστολή από Winbank

Ημερομηνία:

Αποστολέας: Winbank <winbank@camepotsblstripmaster.org>

Παραλήπτης:

Αγαπητέ πελάτη,

Η εισερχόμενη διαδικτυακή μεταφορά

Winbank τέθηκε σε αναμονή εν αναμονή της διόρθωσης προφίλ λογαριασμού.

Κάντε κλικ εδώ [1] για να δείτε τις

λεπτομέρειες του εμβάσματος.

Σας ευχαριστούμε για την τραπεζική

συνεργασία μαζί μας.

Υποστήριξη εξυπηρέτησης πελατών.

Piraeus Winbank

Links:

[1] <http://3.137.201.73>

Από: WinBank Επαλήθευση <postmaster@vivirropartmasterdando.com>

Εστάλη:

Προς:

Θέμα: Απαιτείται επαλήθευση SMS



**PIRAEUS
BANK**

Χαίρετε,

Αυτή είναι η δεύτερη αδοποίηση.

Καθώς αλλάζει το πιο πρόσφατο σύστημά μας, ο αριθμός τηλεφώνου που είναι συνδεδεμένος στον λογαριασμό σας πρέπει να επιβεβαιωθεί μέσω επαλήθευσης μέσω SMS

Μεταβείτε στη διεύθυνση:

[web banking login](#)

και ακολουθήστε τις οδηγίες για να ολοκληρώσετε τη διαδικασία επαλήθευσης.

Έχετε υπόψη σας, εάν δεν ολοκληρώσετε αυτήν την επαλήθευση τις επόμενες 24 ώρες, ο λογαριασμός σας θα κλειδωθεί για λόγους ασφαλείας.

τις καλύτερες ευχές,

Εξυπηρέτηση πελατών

Σημαντική σημείωση:

Αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου στάλθηκε σε εσάς επειδή είστε πελάτης της Τράπεζα Πειραιώς. Για να βεβαιωθείτε ότι λαμβάνετε όλες τις επικοινωνίες μας, σας συνιστούμε να προσθέσετε τη διεύθυνση [customer-service](#) Αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου δημιουργήθηκε αυτόματα από μια διεύθυνση email μόνο αποστολή. Παρακαλώ μην απαντήσετε σε αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου

