

## Τι πρέπει να γνωρίζετε για την εξαπάτηση μέσω πλαστών μηνυμάτων ηλεκτρονικής αλληλογραφίας (phishing e-mails)

### Τι είναι το phishing

Το **phishing** είναι ένας τύπος **εξαπάτησης** που έχει σχεδιαστεί για την **υποκλοπή στοιχείων της ταυτότητάς σας**. Σε μια περίπτωση απάτης phishing, κάποιο κακόβουλο άτομο σας παροτρύνει να δώσετε πληροφορίες, όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης, στοιχεία λογαριασμών ή άλλα προσωπικά στοιχεία, πείθοντάς σας με ψεύτικα προσχήματα. Οι επιθέσεις phishing (phishing attacks) φτάνουν σε εσάς συνήθως μέσω **ανεπιθύμητης ηλεκτρονικής αλληλογραφίας** (spam e-mails) ή μέσω **αναδυόμενων παραθύρων** (pop-ups).

### Πώς λειτουργεί το phishing:

Ο κακόβουλος χρήστης **στέλνει εκατομμύρια ηλεκτρονικά πλαστά μηνύματα** που εμφανίζονται σαν να προέρχονται από γνωστές διαδικτυακές τοποθεσίες ή από τοποθεσίες που εμπιστεύεστε, όπως η τράπεζά σας ή ο οργανισμός της πιστωτικής κάρτας. Τα μηνύματα ηλεκτρονικού ταχυδρομείου και οι διαδικτυακές τοποθεσίες στις οποίες σας παραπέμπουν, **μοιάζουν αρκετά επίσημα**, που εξαπατούν πολύ κόσμο στο να πιστέψει ότι είναι τα πραγματικά. Πιστεύοντας ότι τα μηνύματα αυτά είναι νόμιμα, οι ανυποψίαστοι χρήστες απαντούν συχνά στο αίτημα των ηλεκτρονικών μηνυμάτων για εισαγωγή των αριθμών των πιστωτικών καρτών, των κωδικών πρόσβασης, των πληροφοριών του λογαριασμού ή άλλων προσωπικών δεδομένων. Για να κάνει αυτά τα μηνύματα ακόμη πιο πιστευτά, ο αποστολέας ίσως τοποθετήσει μέσα στο πλαστό μήνυμα έναν σύνδεσμο προς κάποια νόμιμη διαδικτυακή τοποθεσία, αλλά **στην πραγματικότητα σας οδηγεί σε μια ψεύτικη τοποθεσία** ή σε κάποιο αναδυόμενο παράθυρο που είναι ακριβώς ίδιο με την επίσημη τοποθεσία. Αυτά τα αντίγραφα ονομάζονται «πλαστές διαδικτυακές τοποθεσίες». Μόλις βρεθείτε σε κάποια από αυτές τις πλαστές διαδικτυακές τοποθεσίες, ίσως ξεγελαστείτε και εισαγάγετε περισσότερα προσωπικά δεδομένα, τα οποία θα μεταδοθούν άμεσα στο άτομο που δημιούργησε την τοποθεσία και ο οποίος μπορεί έπειτα να χρησιμοποιήσει τα δεδομένα αυτά π.χ. για εγχρήματες συναλλαγές.

## Τι να κάνετε για να προστατευτείτε από το phishing

Όπως συμβαίνει και στον πραγματικό κόσμο, οι επαγγελματίες απατεώνες θα συνεχίσουν να αναπτύσσουν ακόμη πιο δόλιους τρόπους για να σας ξεγελάσουν στο Διαδίκτυο.

Ακολουθώντας όμως αυτά τα **πέντε βήματα** θα μπορέσετε να προστατέψετε τον εαυτό σας και τα προσωπικά σας δεδομένα.

1. **Ποτέ μην απαντάτε** σε αιτήσεις προσωπικών δεδομένων μέσω **ηλεκτρονικού ταχυδρομείου**. Εάν δεν είστε σίγουροι, καλέστε τον οργανισμό που υποτίθεται πως σας έστειλε το ηλεκτρονικό μήνυμα.
2. Επισκεφθείτε τη διαδικτυακή τοποθεσία της Τράπεζας **πληκτρολογώντας ο ίδιος τη διεύθυνση του web-banking** στη γραμμή διεύθυνσης και όχι μέσω εξωτερικών συνδέσμων (links).
3. Βεβαιωθείτε ότι η διαδικτυακή τοποθεσία της Τράπεζας χρησιμοποιεί **κρυπτογράφηση** και διαθέτει το **αυθεντικό πιστοποιητικό** από αναγνωρισμένο φορέα του Διαδικτύου (π.χ. VeriSign).
4. **Ελέγχετε τακτικά τα υπόλοιπα** των πιστωτικών σας καρτών και των τραπεζικών σας λογαριασμών.
5. **Καταγγείτε** άμεσα τις ύποπτες προσπάθειες **υποκλοπής των προσωπικών σας δεδομένων**.

**Βήμα 1°:** **Ποτέ μην απαντάτε** σε αιτήσεις προσωπικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου (e-mail). Η Πανελλήνια Τράπεζα **δεν θα σας ζητήσει ποτέ** με μήνυμα ηλεκτρονικού ταχυδρομείου (ή με οποιοδήποτε άλλο τρόπο) κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή άλλα προσωπικά δεδομένα. Εάν λάβετε κάποιο μήνυμα που σας ζητά τέτοιου είδους πληροφορίες, **μην απαντήσετε**. Εάν πιστεύετε πως το μήνυμα είναι νόμιμο, επικοινωνήστε τηλεφωνικά με την εταιρεία, για να επιβεβαιώσετε το αίτημα.

**Βήμα 2°:** Επισκεφθείτε τη διαδικτυακή τοποθεσία της Τράπεζας, **πληκτρολογώντας ο ίδιος τη διεύθυνση του web-banking** στη γραμμή διεύθυνσης και **όχι μέσω εξωτερικών συνδέσμων** (links). Εάν πιστεύετε πως κάποιο ηλεκτρονικό μήνυμα από την εταιρεία της πιστωτικής σας κάρτας, από την τράπεζα, από την ηλεκτρονική υπηρεσία πληρωμών, ή από κάποια άλλη διαδικτυακή τοποθεσία με την οποία συνεργάζεστε δεν είναι νόμιμο, μην χρησιμοποιήσετε

τους συνδέσμους προς τη διαδικτυακή τοποθεσία που υπάρχουν στο μήνυμα ηλεκτρονικού ταχυδρομείου. Ο σύνδεσμος αυτός ενδεχομένως να σας οδηγήσει σε κάποια πλαστή τοποθεσία που πιθανόν να στείλει όλες τις πληροφορίες που θα εισάγετε στον δημιουργό αυτής της τοποθεσίας. Ακόμη κι αν στη γραμμή διεύθυνσης εμφανίζεται η σωστή διεύθυνση, μην ξεγελαστείτε. Αυτοί που επιθυμούν να σας εξαπατήσουν, έχουν πολλούς τρόπους στη διάθεσή τους για να εμφανίσουν μια ψεύτικη διεύθυνση URL στη γραμμή διεύθυνσης του προγράμματος περιήγησης. Οι νεότερες εκδόσεις του Internet Explorer καθιστούν την πλαστογράφηση της γραμμής διεύθυνσης ακόμη πιο δύσκολη, έτσι καλό θα ήταν να επισκεπτεστε την τοποθεσία Windows Update τακτικά και να ενημερώνετε το λογισμικό σας.

**Βήμα 3<sup>ο</sup>:** Βεβαιωθείτε ότι η διαδικτυακή τοποθεσία χρησιμοποιεί **κρυπτογράφηση**. Εάν δεν μπορείτε να εμπιστευθείτε κάποια διαδικτυακή τοποθεσία από το περιεχόμενο της γραμμής διεύθυνσης, πώς μπορείτε να ξέρετε ότι είναι ασφαλής. Προτού εισαγάγετε τυχόν προσωπικά δεδομένα, βεβαιωθείτε ότι η διαδικτυακή τοποθεσία χρησιμοποιεί κρυπτογράφηση για την αποστολή των προσωπικών σας δεδομένων. Στον Internet Explorer υποδεικνύεται με την εμφάνιση ενός εικονιδίου κίτρινου λουκέτου στη γραμμή κατάστασης, **Εάν το λουκέτο είναι κλειστό, τότε η τοποθεσία χρησιμοποιεί κρυπτογράφηση**. Το σύμβολο αυτό υποδεικνύει ότι η τοποθεσία χρησιμοποιεί κρυπτογράφηση για την προστασία ευαίσθητων προσωπικών δεδομένων (π.χ. αριθμοί πιστωτικών καρτών, αριθμοί λογαριασμών, κωδικοί χρηστών) που εισαγάγετε. Κάντε διπλό κλικ στο εικονίδιο του λουκέτου για να προβάλλετε το πιστοποιητικό ασφαλείας για αυτήν την τοποθεσία. Το όνομα που βρίσκεται μετά την ένδειξη Κάτοχος πιστοποιητικού θα πρέπει να αντιστοιχεί στην τοποθεσία στην οποία βρίσκεστε. Εάν το όνομα διαφέρει, ίσως βρίσκεστε σε πλαστή τοποθεσία. Εάν δεν είστε σίγουροι εάν το πιστοποιητικό είναι νόμιμο, μην εισάγετε τα ευαίσθητα προσωπικά σας δεδομένα. Για τη δική σας ασφάλεια, θα πρέπει να εξέλθετε άμεσα από τη συγκεκριμένη διαδικτυακή τοποθεσία.

**Βήμα 4<sup>ο</sup>:** **Ελέγχετε τακτικά τα υπόλοιπα των λογαριασμών σας και τα υπόλοιπα των λογαριασμών της πιστωτικής σας κάρτας** (τουλάχιστον κάθε μήνα). Με αυτόν τον τρόπο μπορείτε να εντοπίσετε κάποια απάτη και να την αναφέρετε στην Τράπεζα.

**Βήμα 5<sup>ο</sup>:** **Καταγγείλετε άμεσα και με κάθε λεπτομέρεια τις ύποπτες προσπάθειες υποκλοπής των προσωπικών σας δεδομένων στην Τράπεζά σας.**

Παράδειγμα ενός phishing e-mail

Internet Banking" [onlin@internetbanking.gr](mailto:onlin@internetbanking.gr)

26/03/2009 01:05 πμ

**Subject:** The new service bank - with 0% fees for ATM transactions

Dear Customer,

Hellenic Bank Association (HBA), National Bank, Piraeus Bank, Emporiki Bank and other banks have a partnership for all owners of credit cards. If you activate, have 0% fees for all ATM transactions, or any online sites, please fill in the forms of promotion here.

Click here: [Parteners Banking Online](#)

Also, if you activate the new service within 48 hours you will receive 20 euros bonus.

The new partnership between banks association