Συμβουλές για αναγνώριση κακόβουλων/παραπλανητικών μηνυμάτων(Phishing mails)

Ο όρος ηλεκτρονικό ψάρεμα(phishing) έχει να κάνει με τις κακόβουλες προσπάθειες τρίτων μέσω της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου με σκόπο την υποκλοπή προσωπικών δεδομένων. Για παράδειγμα κάποιος μας στέλνει ένα email, το οποίο μοιάζει με αυτά που συνήθως μας στέλνει η τράπεζα μας ώστε να μας ξεγελάσει και να υποκλέψει τα στοιχεία σύνδεσης του web-banking μας.

Συνήθως τέτοια κακόβουλα μηνύματα ενδέχεται να μας ζητήσουν τα εξής:

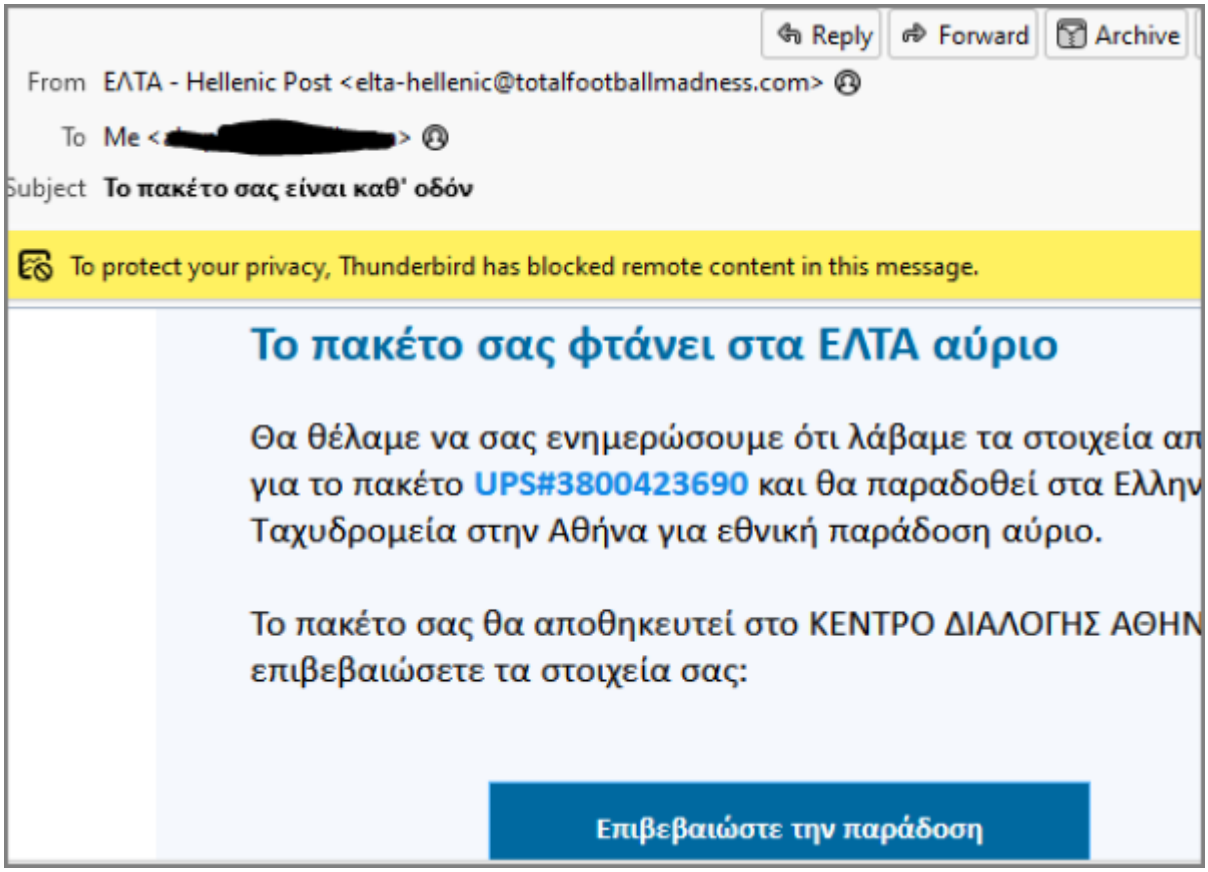
- Ονόματα χρήστη και κωδικούς πρόσβασης, περιλαμβανομένων αλλαγών στους κωδικούς πρόσβασης
- Αριθμούς κοινωνικής ασφάλισης
- Αριθμούς τραπεζικών λογαριασμών
- Κωδικούς PIN (Αριθμοί προσωπικής ταυτοποίησης)
- Αριθμούς πιστωτικών καρτών

Παρακάτω παραθέτουμε κάποιους απλούς ελέγχους που μπορείτε να κάνετε για να διαπιστώνετε την εγκυρότητα ενός μηνύματος

1) Μην εμπιστεύεστε το όνομα που εμφανίζεται στο πεδίο του αποστολέα

Πάντα εκτός από τό όνομα του του αποστολέα, να ελέγχετε και την ηλεκτρονική του διεύθυνση (e-mail). Αν για παράδειγμα λάβετε μήνυμα από κάποιον με όνομα John Papadoulos που δουλεύει στην Google και το e-mail του είναι george@yahoo.gr, τότε σίγουρα αυτό το μήνυμα δεν είναι γνήσιο. Ακόμη, ελέγξτε για τυχόν ορθογραφικά ή επιπλέον σύμβολα όπως τελείες και παύλες.

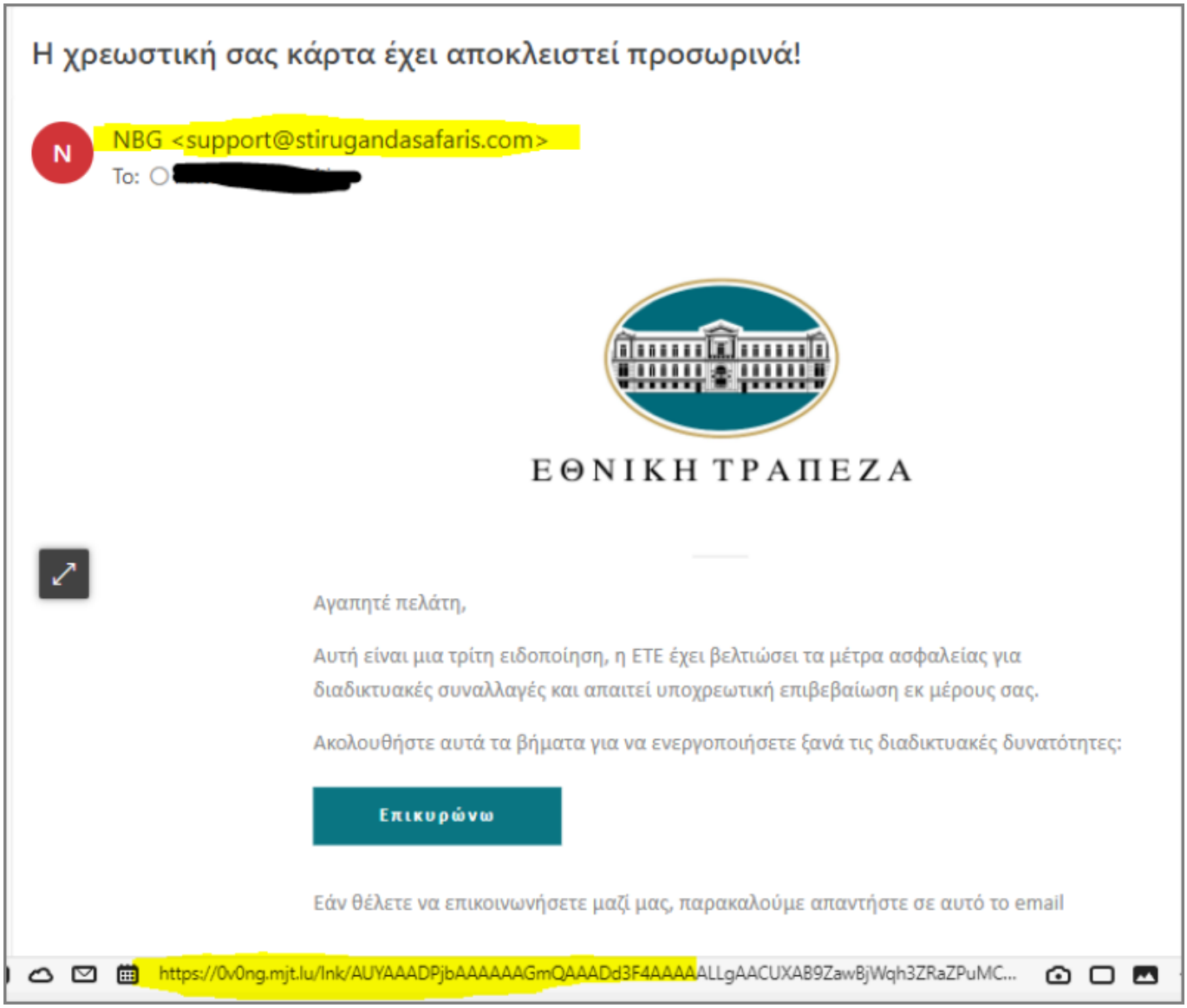
Στο παρακάτω παράδειγμα ο αποστολέας έχει δηλώσει ως όνομα “ΕΛΤΑ - Hellenic Post”, όμως η ηλεκτρονική διεύθυνση **“elta-hellenic@totalfootballmadness.com”** είναι φανερό ότι δεν έχει καμία σχέση με τα ΕΛΤΑ.



2) Ελέγξτε τους υπερσυνδέσμους (links) πριν τους επιλέξετε

Πριν επιλέξετε έναν υπερσύνδεσμο, βεβαιωθείτε πως αυτός οδηγεί στο site που περιμένετε να σας οδηγήσει π.χ. αν είναι του ΠΑΔΑ τότε θα πρέπει να τελειώνει σε **uniwa.gr**. Αν αφήσετε τον δείκτη του ποντικιού πάνω στο κείμενο ή το κουμπί που σας προτείνεται να επιλέξετε, στο κάτω μέρος του παραθύρου εμφανίζεται ο σύνδεσμος στον οποίο οδηγεί (δείτε την εικόνα παρακάτω). Αν πχ έχετε λάβει ένα μήνυμα από τη Microsoft, θα πρέπει να περιμένετε να δείτε έναν σύνδεσμο της μορφής **microsoft.com** ή **office.com** ενώ αν δείτε κάτι διαφορετικό, το πιο πιθανό είναι πως το μήνυμα δεν είναι γνήσιο.

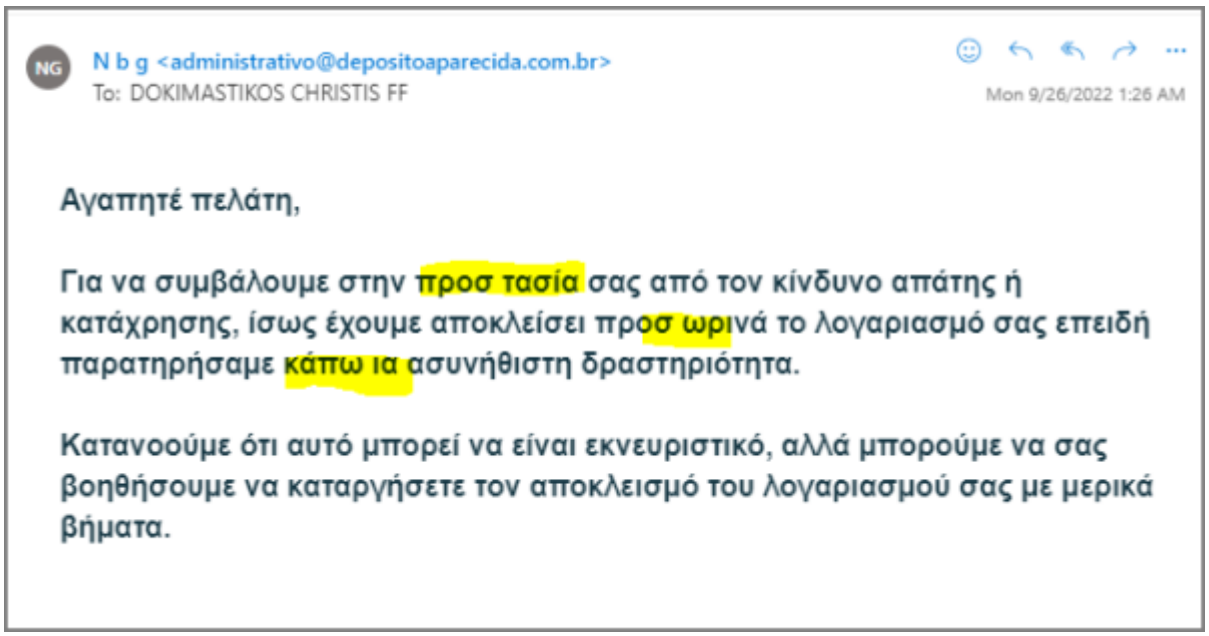
Στο παρακάτω παράδειγμα πηγαίνοντας τον κέρσορα πάνω από την επιλογή “Επικυρώνω”, κάτω αριστερά εμφανίζεται ο υπερσύνδεσμος(link). Όπως βλέπετε η διεύθυνση που εμφανίζεται δεν έχει καμία σχέση με την κανονική διεύθυνση της σχετικής τράπεζας.



3) Ελέγξτε για ορθογραφικά και συντακτικά λάθη

Αρκετά από τα κακόβουλα μηνύματα έχουν ορθογραφικά ή/και συντακτικά λάθη καθώς είτε δημιουργούνται αυτόματα από κάποιο πρόγραμμα είτε γίνεται μετάφραση μέσω κάποιας πλατφόρμας μετάφρασης.

Στο παρακάτω παράδειγμα το μήνυμα από την υποτιθέμενη τράπεζα έχει αρκετά ορθογραφικά λάθη, οπότε είναι πιθανόν να είναι παραπλανητικό.



4) Προσοχή στο άνοιγμα των επισυναπτόμενων αρχείων (attachments)

Θα πρέπει να προσέχετε ιδιαίτερα τον τύπο των επισυναπτόμενων αρχείων στα μηνύματα που λαμβάνετε. Δεν θα πρέπει να ανοίγετε μηνύματα με αρχεία τα οποία έχουν άγνωστο προς εσάς τύπο αρχείων, όπως .jar, .js, .html. Ακόμη μεγαλύτερη προσοχή θα πρέπει να δίνεται σε μηνύματα με επισυναπτόμενα που περιέχουν εκτελέσιμα (.exe, .msi) και συμπιεσμένα αρχεία (.zip, .rar, .gz, .7z) καθώς τέτοια αρχεία είναι συχνά κακόβουλα, ειδικότερα αν το μήνυμα προέρχεται από κάποιον που δεν γνωρίζετε.

Επίσης όταν ανοίγετε αρχεία του office(word, excel, κτλ) προτείνετε να μην ενεργοποιείτε τις μακροεντολές (macros) αν τα έχετε λάβει από το internet και ειδικότερα αν δεν περιμένετε το αρχείο να έχει κάποια επιπλέον λειτουργικότητα ή δεν γνωρίζετε τον αποστολέα.

5) Ενημερώσεις από το Τμήμα Υποστήριξης Δικτύων

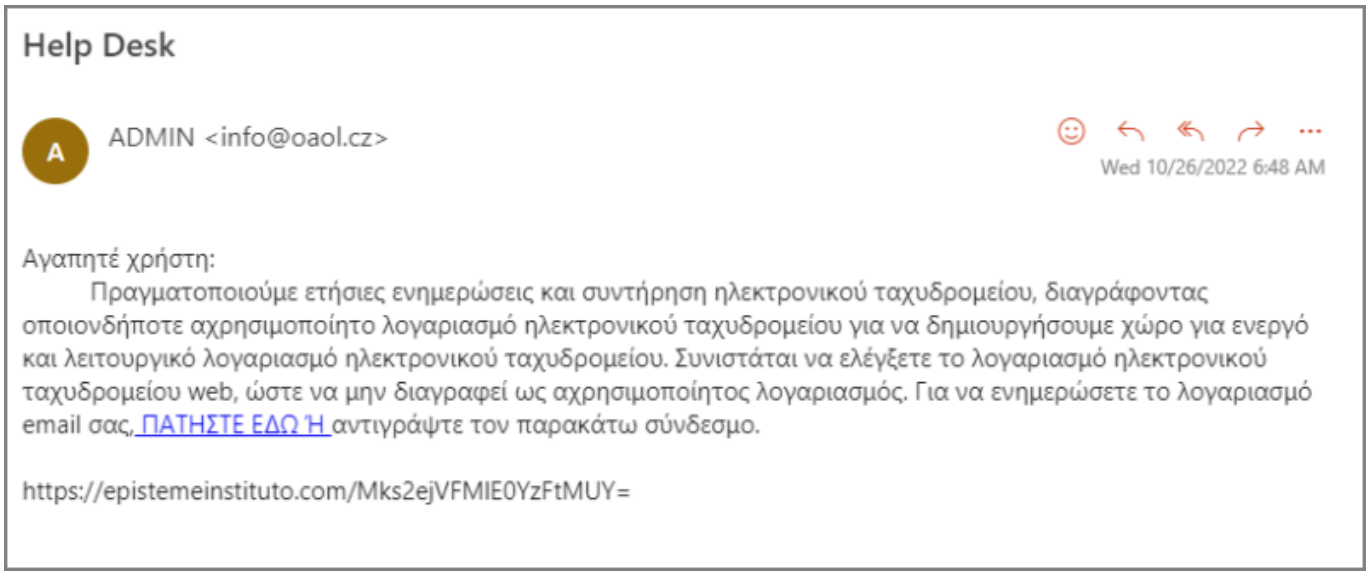
Υπενθυμίζεται ότι **ΠΟΤΕ** το Τμήμα Υποστήριξης Δικτύων δεν θα σας στείλει μήνυμα όπου θα ζητάει τους προσωπικούς σας κωδικούς. Αν λάβετε μήνυμα που πχ σας αναφέρει ότι το γραμματοκίβωτιο σας θα λήξει ή ότι γέμισε και σας ζητάει είτε να στείλετε τους κωδικούς σας , είτε να κάνετε κάπου login **είναι κακόβουλο και αγνοήστε το**.

Σε περίπτωση που έχετε ήδη απαντήσει και γνωστοποιήσει τον κωδικό πρόσβασης του ιδρυματικού σας λογαριασμού, θα πρέπει ΑΜΕΣΑ να προχωρήσετε σε αλλαγή του μέσω της εφαρμογής https://my.uniwa.gr

Στο παρακάτω παράδειγμα το μήνυμα φαίνεται να έχει σταλεί από κάποιον χρήστη με το όνομα ADMIN και ζητάει να κάνετε login σε ένα μη έγκυρο URL https://epistemeinstituto.com/Mks2ejVFMlE0YzFtMUY= ώστε να μην απενεργοποιηθεί ο λογαριασμός σας. Το συγκεκριμένο μήνυμα είναι κακόβουλο και παραπλανητικό με σκοπό να κλέψει τα ιδρυματικά σας στοιχεία αφού:

1. Έχει σταλεί από μη έγκυρο αποστολέα (info@oaol.cz)
2. Ο σύνδεσμος που παρατίθεται δεν είναι του ιδρύματος (πχ uniwa.gr)

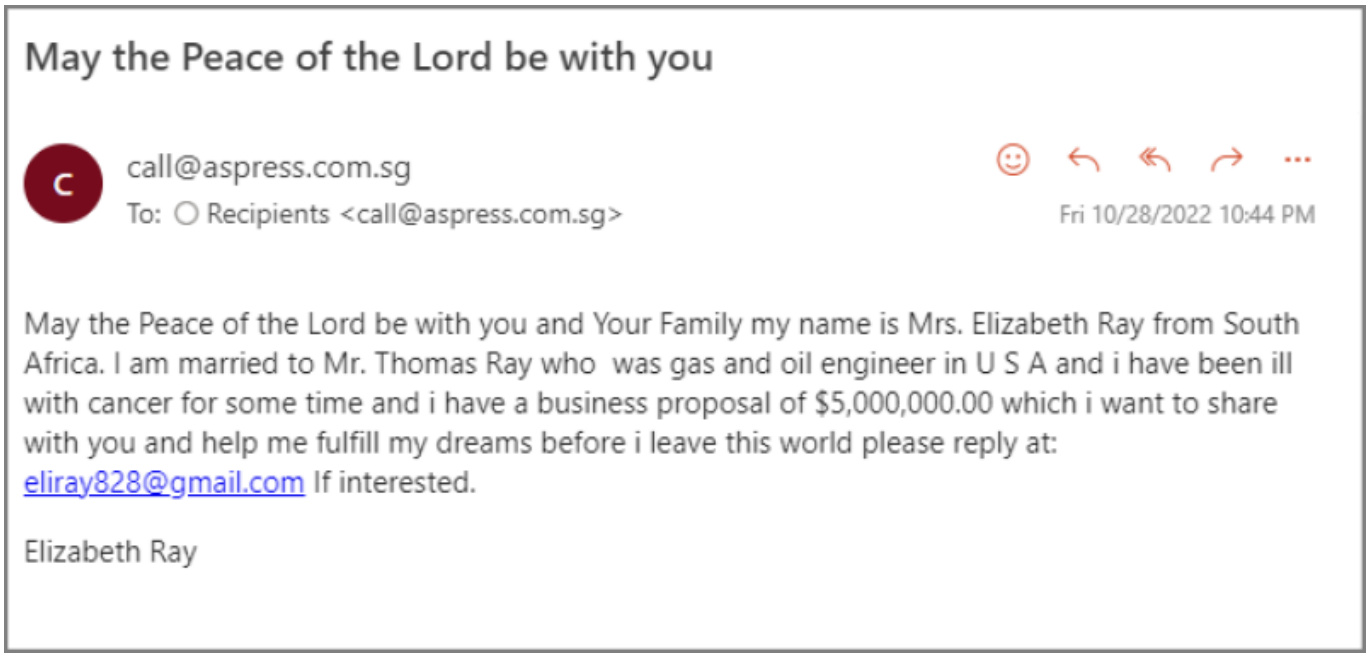
3. Γενικότερα δεν προβλέπεται από τις διαδικασίες του ιδρύματος ή απενεργοποίηση ανενεργών λογαριασμών.



6) Μην πιστεύετε μηνύματα από αγνώστους που σας χαρίζουν μεγάλο αριθμό χρημάτων

Αρκετά συχνά έρχονται μηνύματα που σας υπόσχονται ότι θα σας χαρίσουν ένα μεγάλο χρηματικό ποσο. Σκοπός των μηνυμάτων αυτών είναι να τους δώσετε πρόσβαση στον τραπεζικό σας λογαριασμό ώστε να σας υποκλέψουν χρήματα.

Στο παρακάτω παράδειγμα φαίνεται ένα τέτοιο μήνυμα. Αν απαντήσετε στο email αυτό, τότε είναι πολύ πιθανό σε επόμενο μήνυμα να σας ζητήσουν τα προσωπικά σας στοιχεία όπως πχ τον τραπεζικό σας λογαριασμό και ίσως τους κωδικούς σας για το web banking, με την πρόφαση ότι θα σας μεταφέρουν τα 5 εκατομμύρια δολάρια.



7) Διαχείριση κωδικού πρόσβασης

Θα θέλαμε να σας επισημάνουμε την ιδιαίτερη προσοχή που πρέπει να δίνετε σε θέματα που αφορούν τον «κωδικό πρόσβασης σας (Password)».

- Ο προσωπικός σας «κωδικός πρόσβασης (Password)» διασφαλίζει την αποκλειστική και νόμιμη χρήση των υπηρεσιών που σας παρέχει το Τμήμα Υποστήριξης Δικτύων του Πανεπιστημίου Δυτικής Αττικής αλλά και το Υπουργείο Παιδείας/ΕΔΕΤ. Για το λόγο αυτό δεν θα πρέπει να τον γνωστοποιείτε σε τρίτους. Η χρήση του Λογαριασμού σας από τρίτους εγκυμονεί κινδύνους, καθώς οι ηλεκτρονικές δραστηριότητες του Λογαριασμού σας συνδέονται πάντα με εσάς, τον επίσημο κάτοχο, ως φυσικό πρόσωπο.
- Για μεγαλύτερη ασφάλεια, θα πρέπει να αλλάζετε τον «Κωδικό Πρόσβασης (Password)» σας ανά τακτά χρονικά διαστήματα.
- **MHN** χρησιμοποιείτε τον ίδιο κωδικό σε άλλες εφαρμογές/υπηρεσίες.
- Ο μόνος επίσημος τρόπος αλλαγής password για τους λογαριασμούς του ΚΔΔ είναι μέσω της ιστοσελίδας https://my.uniwa.gr. Κάθε άλλο URL αλλαγής password θα πρέπει να θεωρείται ύποπτο και να μην γίνεται αποδεκτό.