Προς Ακαδημαϊκό/Διοικητικό προσωπικό & φοιτητές ΤΕΙ Αθήνας

Με αφορμή παραπλανητικά μηνύματα αλληλογραφίας που στέλνονται κατά διαστήματα προς τους χρήστες του ιδρύματος και ζητούν να τους γνωρίσετε τους κωδικούς πρόσβασης των λογαριασμών σας, θα θέλαμε να σας ενημερώσουμε για τα ακόλουθα:

- Το Κέντρο Διαχείρισης Δικτύου του ΤΕΙ Αθήνας δεν θα στείλει πότε μήνυμα αλληλογραφίας με το οποίο θα ζητά από τους χρήστες του να κοινοποιήσουν τους κωδικούς πρόσβασης τους. Ποτέ μην απαντάτε σε e-mails ή ύποπτους δικτυακούς τόπους που σας ζητούν τον κωδικό πρόσβασης σας. Σε περίπτωση που έχετε ήδη απαντήσει και γνωστοποιήσει τον κωδικό πρόσβασης που σας παρέχει το ΚΔΔ του ΤΕΙΑ, θα πρέπει άμεσα να προχωρήσετε σε αλλαγή μέσω της ιστοσελίδας https://my.teiath.gr.
- Να είστε πολύ προσεκτικοί με τέτοια μηνύματα, τα οποία εντάσσονται στη λογική των παραπλανητικών μηνυμάτων τύπου phishing.
- Δεν θα πρέπει να αναγράφετε τον κωδικό πρόσβασης που σας δόθηκε από του ΚΔΔ του ΤΕΙ Αθήνας, σε "άγνωστους" δικτυακούς τόπους. Παρακάτω παραθέτουμε ενδεικτική λίστα με **ασφαλής** δικτυακούς τόπους του ΤΕΙ Αθήνας, του Υπουργείου Παιδείας και της ΕΔΕΤ :

- webmail.teiath.gr: (https://webmail.teiath.gr)
- my.teiath.gr: (https://my.teiath.gr)
- register.teiath.gr: (https://register.teiath.gr)
- eclass.teiath.gr (https://eclass.teiath.gr)
- webhosting.teiath.gr (https://webhosting.teiath.gr)
- www.eudoxus.gr (http://www.eudoxus.gr)**
- academicid.minedu.gov.gr: (http://academicid.minedu.gov.gr)**
- okeanos.grnet.gr (https://okeanos.grnet.gr)
- anafandon.grnet.gr (http://anafandon.grnet.gr ή www.anafandon.gr)
- mynetlab.grnet.gr: (https://mynetlab.grnet.gr/mynetlab)
- Κεντρικό σύστημα πιστοποίησης του ΚΔΔ του ΤΕΙΑ: https://idp.teiath.gr

****Σημείωση:** οι σελίδες του υπουργείου και την ΕΔΕΤ για την εισαγωγή password ανακατευθύνουν τον χρήστη στην σελίδα https://idp.teiath.gr

Γενικότερα είναι ιδιαίτερα σημαντικό να εισάγετε password μόνο σε ιστοσελίδες που έχουν εγκατεστημένο πιστοποιητικό ασφαλείας (στο url θα πρέπει να γράφει http**S** και όχι http), ώστε η επικοινωνία μεταξύ της ιστοσελίδας και το προγράμματος πλοήγησης(browser) σας να είναι κρυπτογραφημένη.

Αν και το Κέντρο Διαχείρισης Δικτύου του ΤΕΙ Αθήνας εφαρμόζει ένα σύνολο μηχανισμών προστασίας από την ενοχλητική αλληλογραφία (Spam) υπάρχουν περιπτώσεις μηνυμάτων που καταφέρνουν να παρακάμψουν τα φίλτρα προστασίας και να φτάσουν στην ηλεκτρονική σας θυρίδα.

Γενικότερα σας συνιστούμε να:

- Διαγράφετε τα άχρηστα μηνύματα e-mail χωρίς να τα ανοίγετε.
- Μην απαντάτε ποτέ σε παραπλανητικά μηνύματα και γενικά μηνύματα spam.
- Σκεφθείτε προσεκτικά πριν ανοίξετε συνημμένα αρχεία και πριν κάνετε κλικ σε συνδέσμους που περιέχονται σε μηνύματα e-mail ή άμεσα μηνύματα
- Μην προωθείτε αλυσιδωτά μηνύματα e-mail
- Μην αγοράζετε τίποτε και μην συνεισφέρετε σε εράνους που προωθούνται μέσω μηνυμάτων spam

Γενικά για την προστασία σας από πιθανή εξαπάτηση σας προτρέπουμε να εφαρμόζετε τα παρακάτω:

- Όταν λαμβάνετε μηνύματα αλληλογραφίας θα πρέπει να είστε πολύ προσεκτικοί:

- Να εξετάζετε προσεκτικά το περιεχόμενο τους ακόμη και αν φαίνεται να προέρχονται από γνωστούς αποστολείς.
- Να ελέγχετε αν στο κείμενο υπάρχουν ορθογραφικά ή συντακτικά σφάλματα. Κάτι τέτοιο θα πρέπει να σας βάζει σε υποψίες για την εγκυρότητα του μηνύματος.
- Να προσέχετε τους συνδέσμους που σας υποδεικνύει να ακολουθήσετε κάποιο μήνυμα. Κάποιοι σύνδεσμοι μπορεί να οδηγήσουν στην εγκατάσταση κακόβουλου λογισμικού, το οποίο μπορεί να δημιουργήσει θέματα ασφαλείας με τον υπολογιστή σας ή τις εφαρμογές που χρησιμοποιείτε.
- Θα ήταν καλό να ελέγχετε την γραμμή κατάστασης (status bar) του προγράμματος πλοήγησης για να βλέπετε την διεύθυνση που θα επισκεφθείτε αν ακολουθήσετε τον σύνδεσμο

- Διατηρείτε το πρόγραμμα πλοήγησης ιστοσελίδων (Internet Explorer, Mozilla, Chrome, Opera, MAC Safari κ.α.) που χρησιμοποιείτε ενημερωμένο (καλό είναι να έχετε πάντα την τελευταία σταθερή έκδοση) γιατί ενδεχομένως παλαιότερες εκδόσεις να είναι ευάλωτες σε προσπάθειες παραπλάνησης, πχ με ψεύτικες διευθύνσεις ιστοσελίδων (spoofed URLs).

Με την ευκαιρία επίσης, επισημαίνουμε την ιδιαίτερη προσοχή που πρέπει να δίνετε σε θέματα που αφορούν τον «Κωδικό Πρόσβασης (Password)».

- Ο προσωπικός σας «Κωδικός Πρόσβασης (Password)» διασφαλίζει την αποκλειστική και νόμιμη χρήση των υπηρεσιών που σας παρέχει το Κέντρο Διαχείρισης Δικτύου του ΤΕΙ Αθήνας αλλά και το Υπουργείο Παιδείας/ΕΔΕΤ. Για το λόγο αυτό δεν θα πρέπει να τον γνωστοποιείτε σε τρίτους. Επισημαίνεται ότι η χρήση του Λογαριασμού 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 σε τακτά χρονικά διαστήματα.
- Ο μόνος επίσημος τρόπος αλλαγής password είναι μέσω της ιστοσελίδας https://my.teiath.gr

- Κάθε άλλο URL αλλαγής password θα πρέπει να θεωρείται ύποπτο και να μην γίνεται αποδεκτό.

Εκ του Κέντρου Διαχείρισης Δικτύου του ΤΕΙ Αθήνας