Θέμα: Ενημέρωση για μέτρα προστασίας από παραπλανητικά και κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου

Πολλές φορές λαμβάνουμε κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου, που σκοπό έχουν την υποκλοπή του κωδικού πρόσβασης μας, προφασιζόμενα πολλές φορές ότι προέρχονται από γνώριμο σε εμάς οργανισμό π.χ. Τράπεζα (phishing emails). Η διακίνηση τέτοιων μηνυμάτων είναι συχνό φαινόμενο και για το λόγο αυτό θα πρέπει να είμαστε ιδιαίτερα προσεκτικοί.

Η κεντρική υπηρεσία ηλεκτρονικού ταχυδρομείου του Ιδρύματος, έχει υλοποιήσει κατάλληλα τεχνικά μέτρα για την προστασία μας από κακόβουλο λογισμικό και την μείωση, στο μέτρο του δυνατού, των παραπλανητικών και ανεπιθύμητων μηνυμάτων. Λόγω του τρόπου λειτουργίας των μηνυμάτων phishing που στηρίζονται στην εξαπάτηση των χρηστών, είναι κρίσιμο να λαμβάνουμε και εμείς οι χρήστες τα κατάλληλα μέτρα για την προστασία μας.

Σε περίπτωση που έχετε απαντήσει σε τέτοια μηνύματα και έχετε συμπληρώσει ή αποστείλει τα στοιχεία πρόσβασης σας ή ακόμα και αν υπάρχει υπόνοια υποκλοπής του κωδικού πρόσβασης σας, θα πρέπει **ΑΜΕΣΑ**, να αλλάξετε τον κωδικό πρόσβασης του ιδρυματικού σας λογαριασμού στη διεύθυνση https://myaccount.uoc.gr. Επιπλέον, συνιστάται ο έλεγχος των συσκευών σας με χρήση λογισμικού antivirus/antimalware.

Για αντιμετώπιση σχετικών θεμάτων και τεχνικές πληροφορίες μπορείτε να απευθυνθείτε στην Υπηρεσία Υποστήριξης Χρηστών (helpdesk@uoc.gr) του Πανεπιστημίου Κρήτης.

Μέτρα προστασίας κωδικού πρόσβασης:

Συχνή αλλαγή κωδικού πρόσβασης του ιδρυματικού μας λογαριασμού μέσω της ιστοσελίδας https://myaccount.uoc.gr.

Χρήση ισχυρού κωδικού. Συνιστάται να περιλαμβάνει συνδυασμό από γράμματα, κεφαλαία και μικρά, αριθμούς, σύμβολα και να έχει μήκος 12 χαρακτήρες και άνω. Καλό είναι να αποφεύγονται ημερομηνίες, ονόματα και τμήματα του ονόματος χρήστη ως μέρος του κωδικού. Επίσης καλό είναι να **αποφεύγονται** στους κωδικούς πρόσβασης κοινές λέξεις που συνήθως χρησιμοποιούνται, πχ “password”, “qwerty” , “123456” , “123456789” , “1q2w3e4r”

Αποφυγή χρήσης κοινόχρηστων συσκευών και συσκευών τρίτων για την πρόσβαση μας στο ηλεκτρονικό ταχυδρομείο και σε λοιπές υπηρεσίες με χρήση του ιδρυματικού μας λογαριασμού.

Αποφυγή επαναχρησιμοποίησης κωδικού. Αποφυγή χρήσης του κωδικού πρόσβασης του ιδρυματικού λογαριασμού σας και για άλλες ηλεκτρονικές υπηρεσίες ή χρήσεις.

Αποφυγή αποκάλυψης κωδικού πρόσβασης. Μην αποκαλύπτετε ποτέ τον κωδικό πρόσβασης του ιδρυματικού λογαριασμού σας σε τρίτους. Επίσης, μην αποστέλλετε τον κωδικό σας μέσω ηλεκτρονικού μηνύματος.

Προστασία από κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου:

Αιτήματα επικαιροποίησης λογαριασμού. Το Πανεπιστήμιο Κρήτης, οι Τράπεζες και άλλοι Οργανισμοί δεν θα σας ζητήσουν ποτέ μέσω email να στείλετε τα στοιχεία πρόσβασης των λογαριασμών σας, δηλαδή το όνομα χρήστη και τον κωδικό πρόσβασης. Μην απαντάτε ποτέ σε αυτά τα emails. Το Πανεπιστήμιο Κρήτης, οι Τράπεζες και άλλοι Οργανισμοί δεν θα σας ζητήσουν ποτέ μέσω email να επικαιροποιήσετε τους λογαριασμούς σας σε κάποια εξωτερική σελίδα. Όταν λαμβάνετε τέτοια email θα πρέπει άμεσα να τα διαγράφετε, χωρίς να πατάτε τους συνδέσμους που περιλαμβάνουν ή να ανοίγετε τα συνημμένα αρχεία.

Μηνύματα από άγνωστο αποστολέα. Όταν λαμβάνετε email από άγνωστο αποστολέα θα πρέπει να είστε ιδιαίτερα προσεκτικοί και να αποφεύγετε να πατάτε τους συνδέσμους και να ανοίγετε συνημμένα αρχεία που περιλαμβάνουν. Ειδικά στις περιπτώσεις που η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα αφορά σε άγνωστο σε εσάς οργανισμό ή παραπέμπει σε χώρα προέλευσης που δεν έχετε επαφές.

Έλεγχος διεύθυνσης αποστολέα. Η διεύθυνση του αποστολέα ενός μηνύματος ηλεκτρονικού ταχυδρομείου είναι ένα στοιχείο εύκολα παραποιήσιμο. Διενεργήστε έλεγχο στην διεύθυνση αποστολέα των μηνυμάτων κάνοντας χρήση των δυνατοτήτων που παρέχονται από το λογισμικό ηλεκτρονικής αλληλογραφίας που χρησιμοποιείτε. Στην περίπτωση της δικτυακής εφαρμογής ηλεκτρονικού ταχυδρομείου **mail.uoc.gr** αυτό είναι εφικτό αφήνοντας το ποντίκι σας πάνω από (mouse over) το πεδίο διεύθυνσης αποστολέα. Αντίστοιχα, η εφαρμογή **Mozilla Thunderbird**, από την έκδοση 102, υποστηρίζει την προβολή της πλήρης και πραγματικής διεύθυνσης του αποστολέα. Αρκεί να ενεργοποιήσετε την δυνατότητα αυτή, επιλέγοντας σε ένα εισερχόμενο μήνυμα 'More' -> 'Customize' ->'Always show sender's full address'.

Έλεγχος διεύθυνσης συνδέσμου. Προτού πατήσετε κάποιο σύνδεσμο προτείνεται η χρήση απλών τεχνικών αποτροπής εξαπάτησης. Για παράδειγμα μπορείτε να αφήσετε το ποντίκι σας πάνω από (mouse over) συνδέσμους ώστε να δείτε τις πραγματικές διευθύνσεις τους.

Έλεγχος για ορθογραφικά και συντακτικά λάθη. Ελέγχετε αν στο email υπάρχουν ορθογραφικά ή συντακτικά σφάλματα. Κάτι τέτοιο θα πρέπει να σας βάλει σε υποψία για την εγκυρότητα του μηνύματος.

Προστασία Συσκευών. Συνιστάται η χρήση ενημερωμένου λογισμικού Antivirus/Antimalware στις συσκευές (Η/Υ, smartphone, tablet) που χρησιμοποιούμε. Είναι σημαντικός ο τακτικός έλεγχος για ύπαρξη ιών και λοιπού κακόβουλου λογισμικού.

Χρήση γνήσιου και υποστηριζόμενου από τον κατασκευαστή λογισμικού (λειτουργικό σύστημα και λοιπό λογισμικό) στις συσκευές που χρησιμοποιούμε. Συχνή αναβάθμιση του φυλλομετρητή που χρησιμοποιείτε για πρόσβαση στο webmail, καθώς και της εφαρμογής email (thunderbird, outlook κ.α.).

Κέντρο Υποδομών και Υπηρεσιών Τεχνολογίας Πληροφορικής και Επικοινωνιών - ΚΥΥΤΠΕ

Πανεπιστήμιο Κρήτης