Καλές πρακτικές
στον τομέα της Κυβερνοασφάλειας

Ομάδα Υποστήριξης Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών του Πανεπιστημίου Πατρών

cybersectf@upatras.gr

https://cybersecurity.upatras.gr

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Τι είναι η κυβερνοασφάλεια & γιατί μας αφορά

Κυβερνοασφάλεια είναι το σύνολο των τεχνολογιών, διαδικασιών και πρακτικών που προστατεύουν συστήματα, δίκτυα και δεδομένα από ψηφιακές επιθέσεις, μη εξουσιοδοτημένη πρόσβαση ή καταστροφή.

Τι είναι η κυβερνοασφάλεια & γιατί μας αφορά

Στην πράξη, σημαίνει ότι θα πρέπει να κρατάμε ασφαλή:

- τα δεδομένα που διαχειριζόμαστε
- τους υπολογιστές και τα πληροφοριακά μας συστήματα
- τα δίκτυα και τις εφαρμογές που χρησιμοποιούμε στον χώρο εργασίας

...ώστε να αποφεύγουμε:

- την πρόσβαση από άτομα που δεν έχουν δικαίωμα
- τη διαρροή ή την αλλοίωση δεδομένων
- κακόβουλες επιθέσεις, με ιούς, ransomware ή προσπάθειες εξαπάτησης
- προβλήματα που μπορεί να προκύψουν από λάθη ή απρόσεκτη χρήση των συστημάτων

Τι είναι η κυβερνοασφάλεια & γιατί μας αφορά

Σε προσωπικό επίπεδο, πρέπει να προστατεύουμε τον Ιδρυματικό μας λογαριασμό, τα δεδομένα που διαχειριζόμαστε και τον υπολογιστή μας.

Σε επίπεδο Οργανισμού, είναι ευθύνη όλων μας να προστατεύουμε τα δίκτυα και τις υπηρεσίες του Πανεπιστημίου εφαρμόζοντας καλές πρακτικές.

Χρησιμοποιώντας τον υπολογιστή μας με ασφάλεια

Στη διεύθυνση https://cybersecurity.upatras.gr/ μπορείτε να βρείτε οδηγίες για την ψηφιακή ασφάλεια και φόρμα για αναφορά περιστατικού ασφαλείας

https://cybersecurity.upatras.gr/report-form/

Η σωστή και ασφαλής χρήση των υπολογιστών και των πληροφοριακών συστημάτων του Πανεπιστημίου Πατρών, αποτελεί βασικό παράγοντα για την εύρυθμη λειτουργία των διοικητικών και ακαδημαϊκών διαδικασιών.

Καθημερινά διαχειριζόμαστε έγγραφα, προσωπικά δεδομένα, αλληλογραφία και πληροφοριακά συστήματα που είναι κρίσιμα για την εξυπηρέτηση φοιτητών, προσωπικού, μελών Δ.Ε.Π. και συνεργατών.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Θα δούμε μαζί απλές και πρακτικές κατευθύνσεις,

συνοψίζοντας τι χρειάζεται να αποφεύγουμε

και ποιες πρακτικές είναι καλό να εφαρμόζουμε, σε σχέση με:

- Κωδικούς πρόσβασης
- Email & συνημμένα αρχεία
- Αποθήκευση και φύλαξη φυσικών και ηλεκτρονικών αρχείων
- Cloud sharing-τον Διαμοιρασμό αρχείων
- Χρήση Παραγωγικής Τεχνητής Νοημοσύνης-GenAI
- Πρόσβαση από εξωτερικά δίκτυα
- Χρήση προσωπικών και υπηρεσιακών ηλεκτρονικών υπολογιστών
- Ransomware, ιούς, spam/phishing
- Τι πρέπει να κάνουμε σε περίπτωση εντοπισμού περιστατικού ασφαλείας

Κωδικοί πρόσβασης

- Έχουμε την ευθύνη των κωδικών μας και δεν τους μοιραζόμαστε με άλλους.

Ο ιδρυματικός λογαριασμός UpnetID σας είναι προσωπικός και με αυτόν έχετε πρόσβαση σε όλες τις υπηρεσίες ΤΠΕ που παρέχει το Πανεπιστήμιο Πατρών, καθώς και τις υπηρεσίες συνεργαζόμενων φορέων.

Η χρήση του από τρίτους εγκυμονεί κινδύνους, καθώς οι ηλεκτρονικές δραστηριότητες του λογαριασμού σας συνδέονται πάντα με εσάς, τον επίσημο κάτοχο, ως φυσικό πρόσωπο!

Η προστασία των κωδικών πρόσβασης στον ιδρυματικό λογαριασμό και τα πληροφοριακά συστήματα του Πανεπιστημίου είναι ένα πολύ σημαντικό κομμάτι της ασφάλειας.

- Τυχόν emails τα οποία ζητάνε καταχώρηση κωδικού για την διατήρηση/ανανέωση λογαριασμών, πρέπει να αντιμετωπίζονται ως spam/phishing.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Κωδικοί πρόσβασης

Κανένας Οργανισμός (Π.Π., τράπεζα κ.α.)
δεν θα ζητήσει ποτέ, με οποιονδήποτε τρόπο,
να κοινοποιήσετε τον κωδικό πρόσβασής σας.

Τυχόν email τα οποία ζητάνε αποκάλυψη κωδικών,
πρέπει να αντιμετωπίζονται ως spam/phishing.

Κωδικοί πρόσβασης

- Δεν χρησιμοποιούμε τον ίδιο κωδικό σε όλα τα συστήματα
- Δεν γράφουμε κωδικούς σε χαρτιά τα οποία είναι εκτεθειμένα (για παράδειγμα επάνω στο γραφείο μας)
- Φυλάσσουμε τους κωδικούς μας με ασφάλεια (π.χ. password managers, κλειδωμένο ερμάριο, κρυπτογραφημένο usb)

Προτείνεται να ακολουθείτε για τους υπηρεσιακούς σας κωδικούς την ίδια διαδικασία φύλαξης που ακολουθείτε στους προσωπικούς σας (π.χ. κωδικούς εφορίας, κωδικούς e-banking)

Κωδικοί πρόσβασης

- Δεν αποθηκεύουμε τους κωδικούς μας στους υπολογιστές που χρησιμοποιούμε, είτε στον χώρο εργασίας, είτε στο σπίτι.

Σε περίπτωση που υπάρχουν αποθηκευμένοι κωδικοί για παράδειγμα σε browsers (Chrome, Firefox, Edge), θα πρέπει να σβηστούν. Δεν πρέπει στις οθόνες σύνδεσης (για παράδειγμα στο υπηρεσιακό email, στο DocuTracks, στην ψηφιακή υπογραφή κ.λπ.) να εμφανίζονται προσυμπληρωμένα τα πεδία των κωδικών.

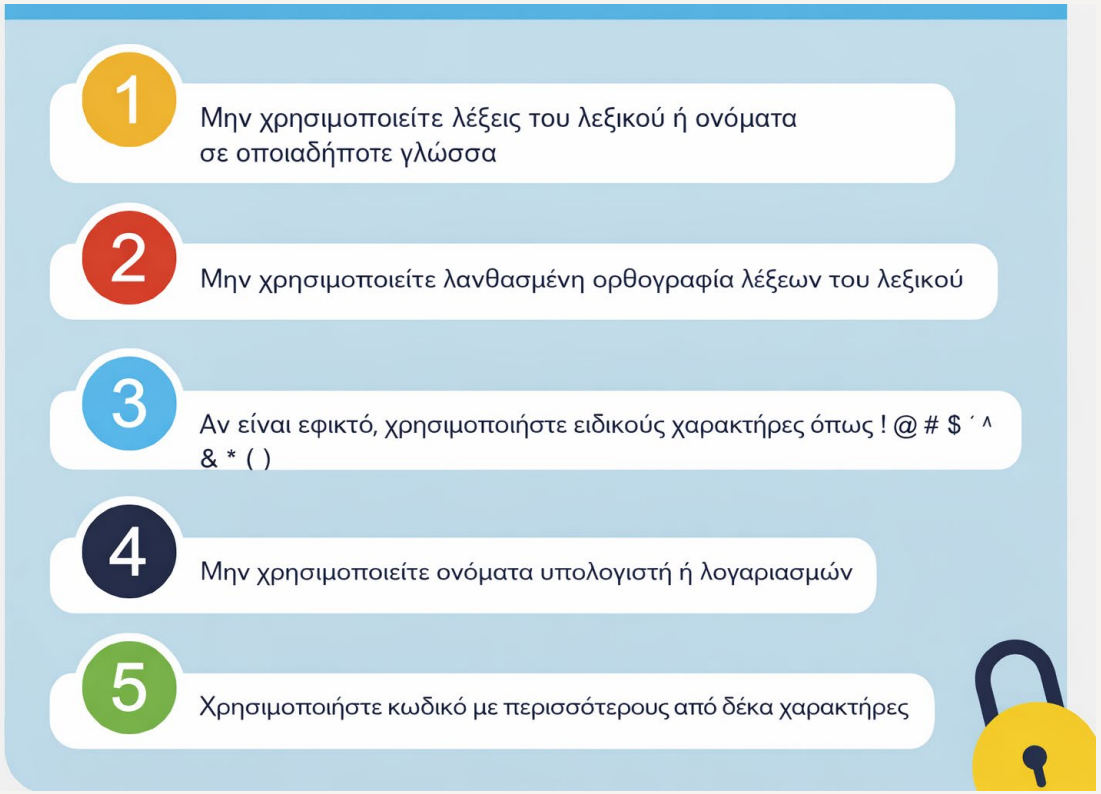
- Αλλάζουμε τους κωδικούς μας συχνά.

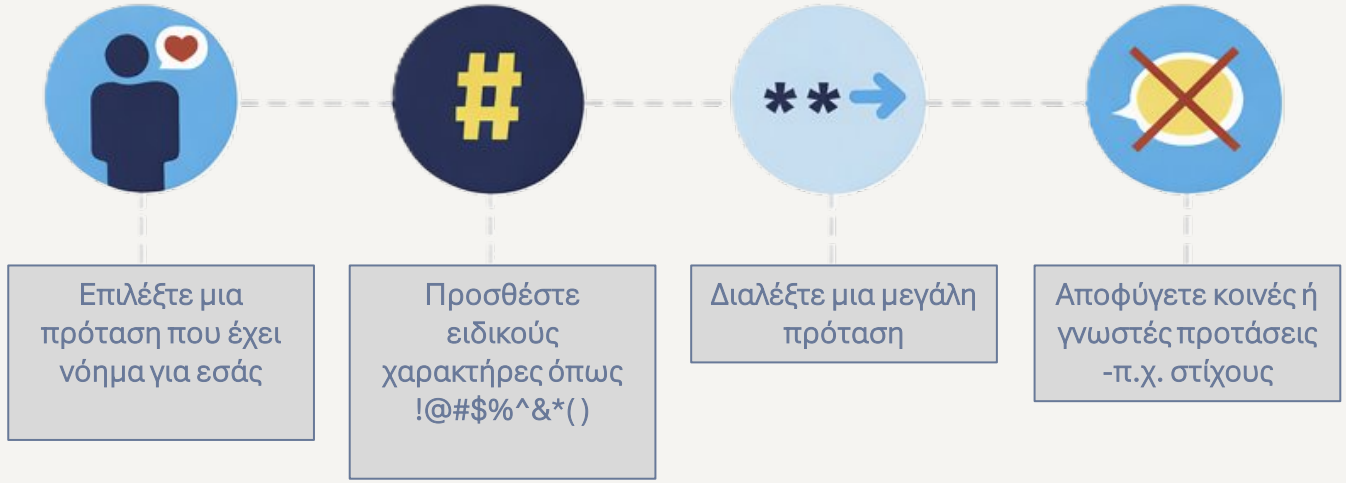
Καλό είναι οι κωδικοί να περιέχουν πεζά και κεφαλαία γράμματα, ειδικά σύμβολα και αριθμούς και να μην περιέχουν το όνομα χρήστη του λογαριασμού.

Για την αλλαγή του κωδικού του ιδρυματικού μας λογαριασμού, συνδεόμαστε στη διεύθυνση https://mussa.upnet.gr/

Κωδικοί πρόσβασης: τι κωδικό να διαλέξω;

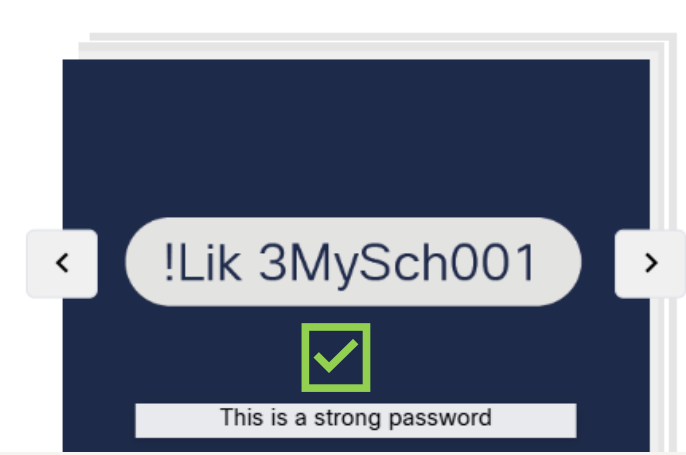
Δημιουργήσετε έναν **ισχυρό κωδικό** ή χρησιμοποιήστε **φράση πρόσβασης (Passphrase)**

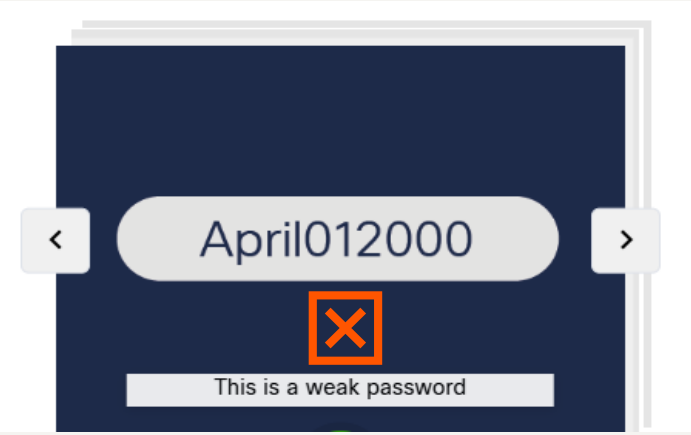


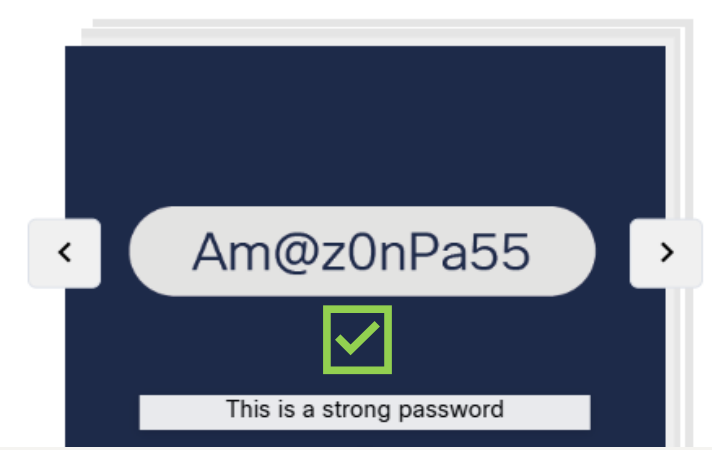


Κωδικοί πρόσβασης

Καλοί και κακοί κωδικοί πρόσβασης





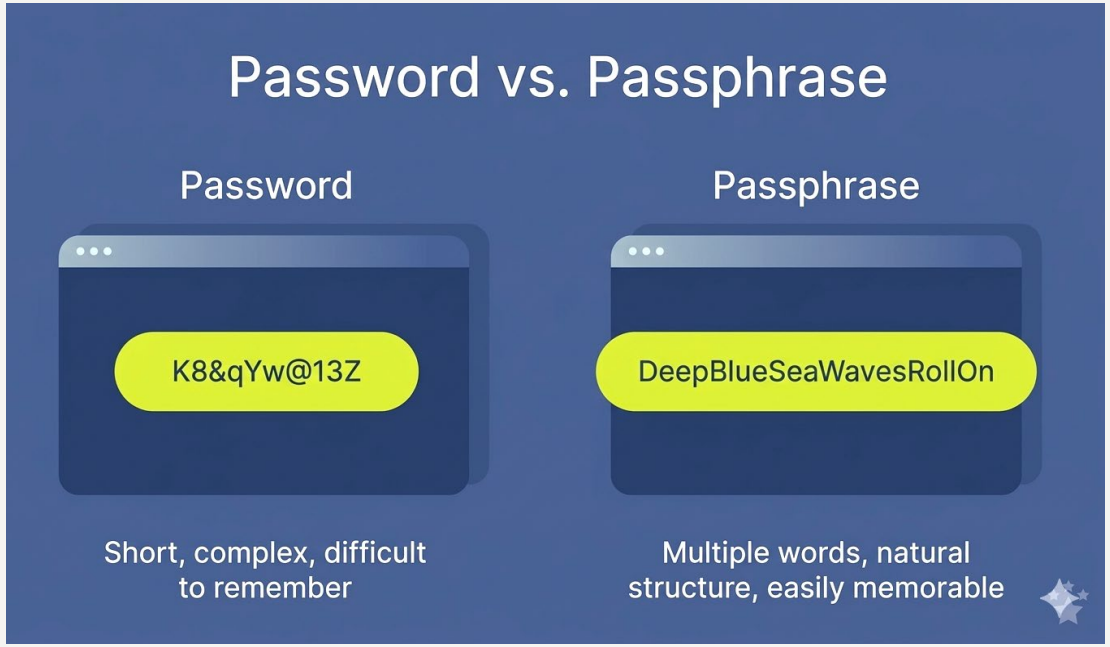


Φράσεις πρόσβασης (passphrases)

Γιατί να χρησιμοποιούμε μια **φράση πρόσβασης (passphrase)**;

- Μεγαλύτερη ασφάλεια: μεγαλύτερες, τυχαίες ακολουθίες χαρακτήρων είναι πιο ασφαλείς.
- Ευκολία απομνημόνευσης: είναι πιο εύκολο να θυμάται κανείς μια φράση πρόσβασης σε σύγκριση με σύνθετους, σύντομους κωδικούς όπως «P@ssw0rd1!».
- Ιδανικές για κλειδιά: Χρησιμοποιούνται συνήθως για την προστασία κλειδιών κρυπτογράφησης, λογαριασμών χρηστών και ως κύριοι κωδικοί (master passwords) σε διαχειριστές κωδικών πρόσβασης.

Οι φράσεις πρόσβασης προσφέρουν τον καλύτερο συνδυασμό υψηλής ασφάλειας και ευχρηστίας.



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Ύποπτα email

Ελέγχουμε την εγκυρότητα των μηνυμάτων που έρχονται στον λογαριασμό μας.

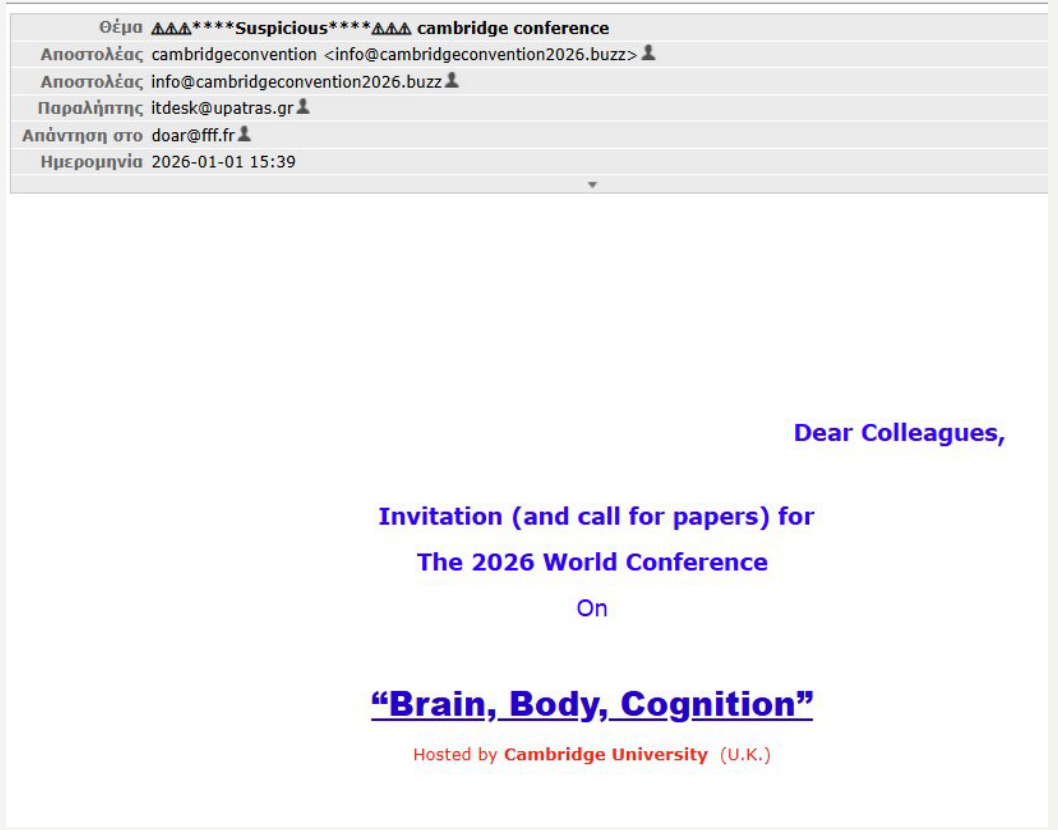
Στα διάφορα προγράμματα περιήγησης email, οι ηλεκτρονικές διευθύνσεις εμφανίζονται με την μορφή:

Επωνυμία <onoma@domain.com_gr_ktl>

Ελέγχουμε πάντα ΚΑΙ τα πεδία “onoma” και “domain”, εκτός από το “Επωνυμία”, γιατί το “Επωνυμία” είναι εύκολα παραποιήσιμο, ενώ τα “onoma” και “domain” όχι.

Παραδείγματα κακόβουλων αποστολέων:

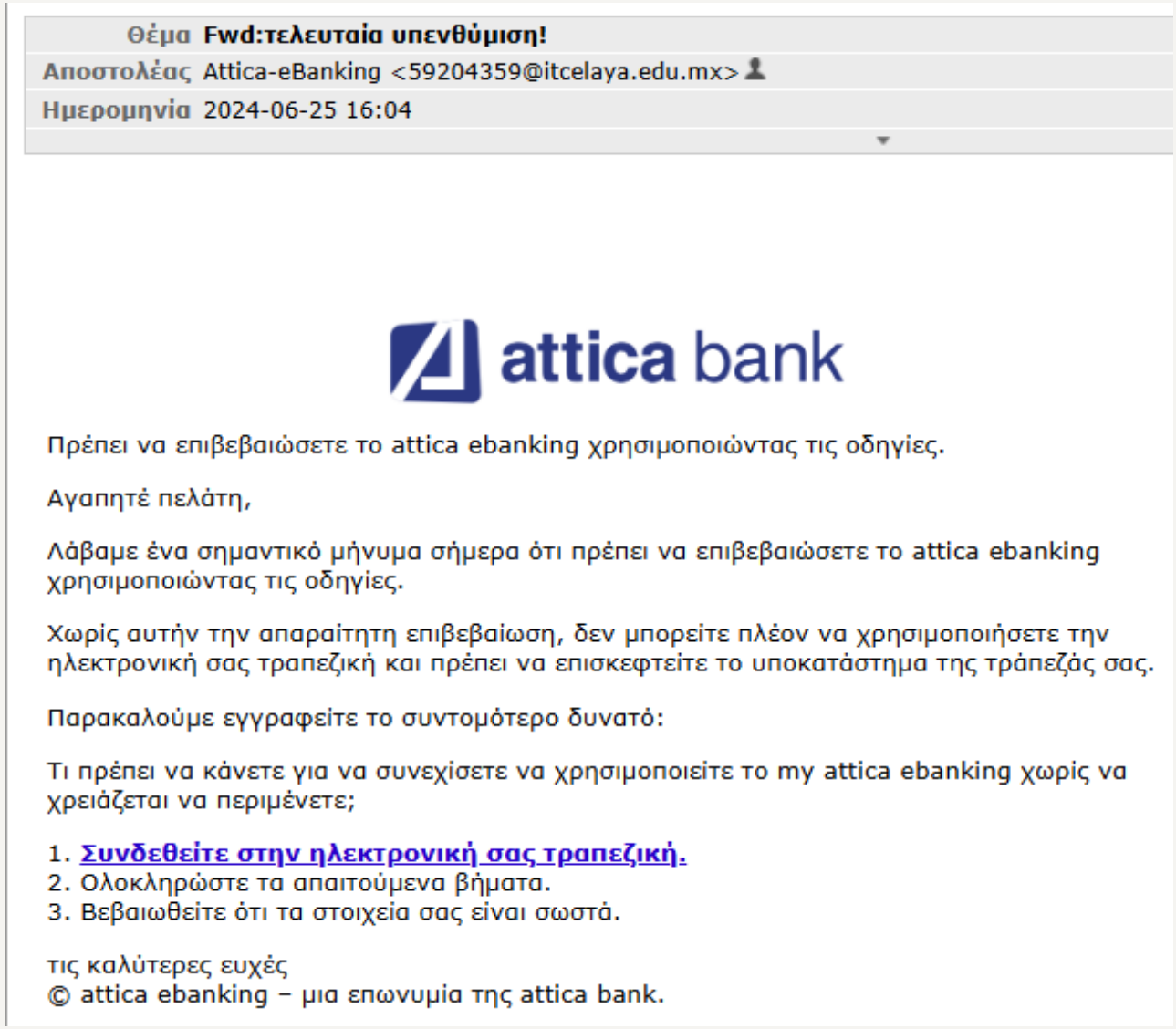
- Nikos Papadopoulos <Nikos.Papadopoulos@gr.ey.com>
- Upatras <sales@a1-model.asia>
- IT HELP DESK <ouvidoria@guaranidasmissoes.rs.gov.br>
- Piraeus Bank <a.hammerlik@fs-jessen.bildung-lsa.de>



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Ύποπτα email

Μπορείτε να εντοπίσετε "ύποπτα" στοιχεία στο παρακάτω e-mail;



Θέμα Fwd:τελευταία υπενθύμιση!
Αποστολέας Attica-eBanking <59204359@itcelaya.edu.mx>
Ημερομηνία 2024-06-25 16:04

attica bank

Πρέπει να επιβεβαιώσετε το attica ebanking χρησιμοποιώντας τις οδηγίες.

Αγαπητέ πελάτη,

Λάβαμε ένα σημαντικό μήνυμα σήμερα ότι πρέπει να επιβεβαιώσετε το attica ebanking χρησιμοποιώντας τις οδηγίες.

Χωρίς αυτήν την απαραίτητη επιβεβαίωση, δεν μπορείτε πλέον να χρησιμοποιήσετε την ηλεκτρονική σας τραπεζική και πρέπει να επισκεφτείτε το υποκατάστημα της τράπεζάς σας.

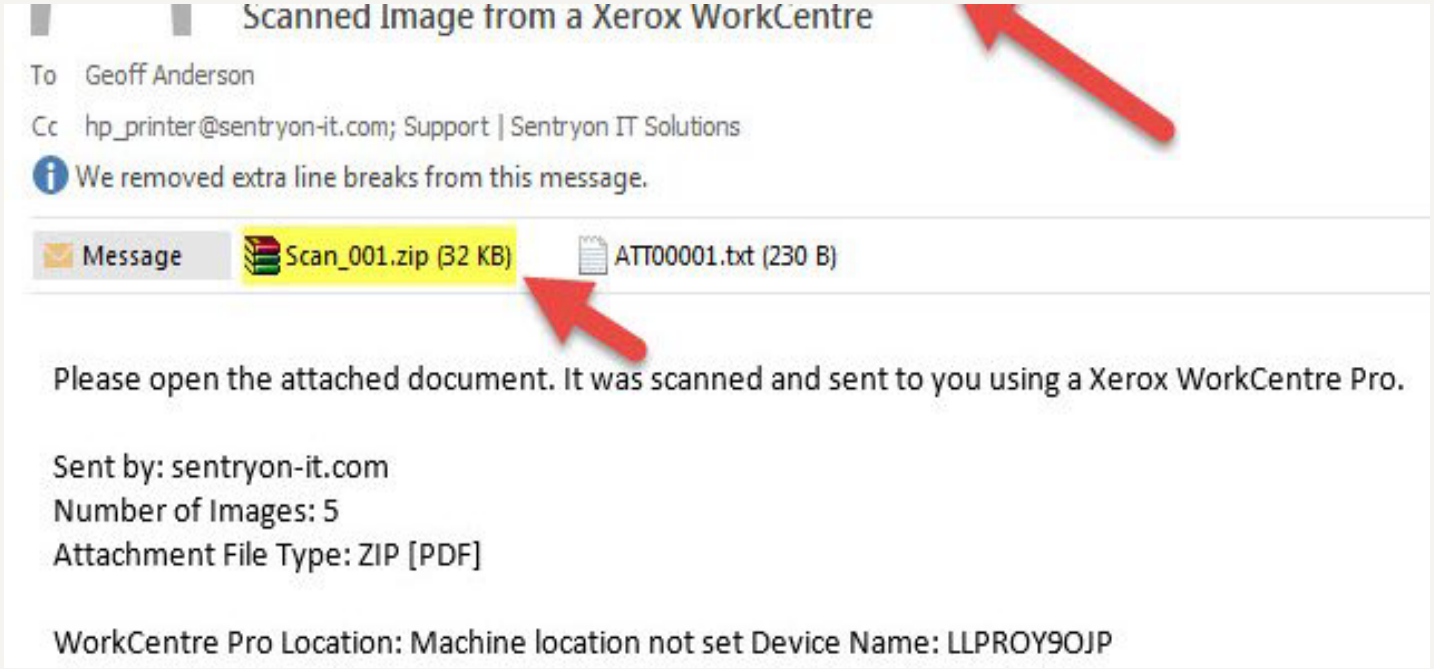
Παρακαλούμε εγγραφείτε το συντομότερο δυνατό:

Τι πρέπει να κάνετε για να συνεχίσετε να χρησιμοποιείτε το my attica ebanking χωρίς να χρειάζεται να περιμένετε;

1. Συνδεθείτε στην ηλεκτρονική σας τραπεζική.
2. Ολοκληρώστε τα απαιτούμενα βήματα.
3. Βεβαιωθείτε ότι τα στοιχεία σας είναι σωστά.

τις καλύτερες ευχές
© attica ebanking – μια επωνυμία της attica bank.

Ύποπτα email & συνημμένα αρχεία

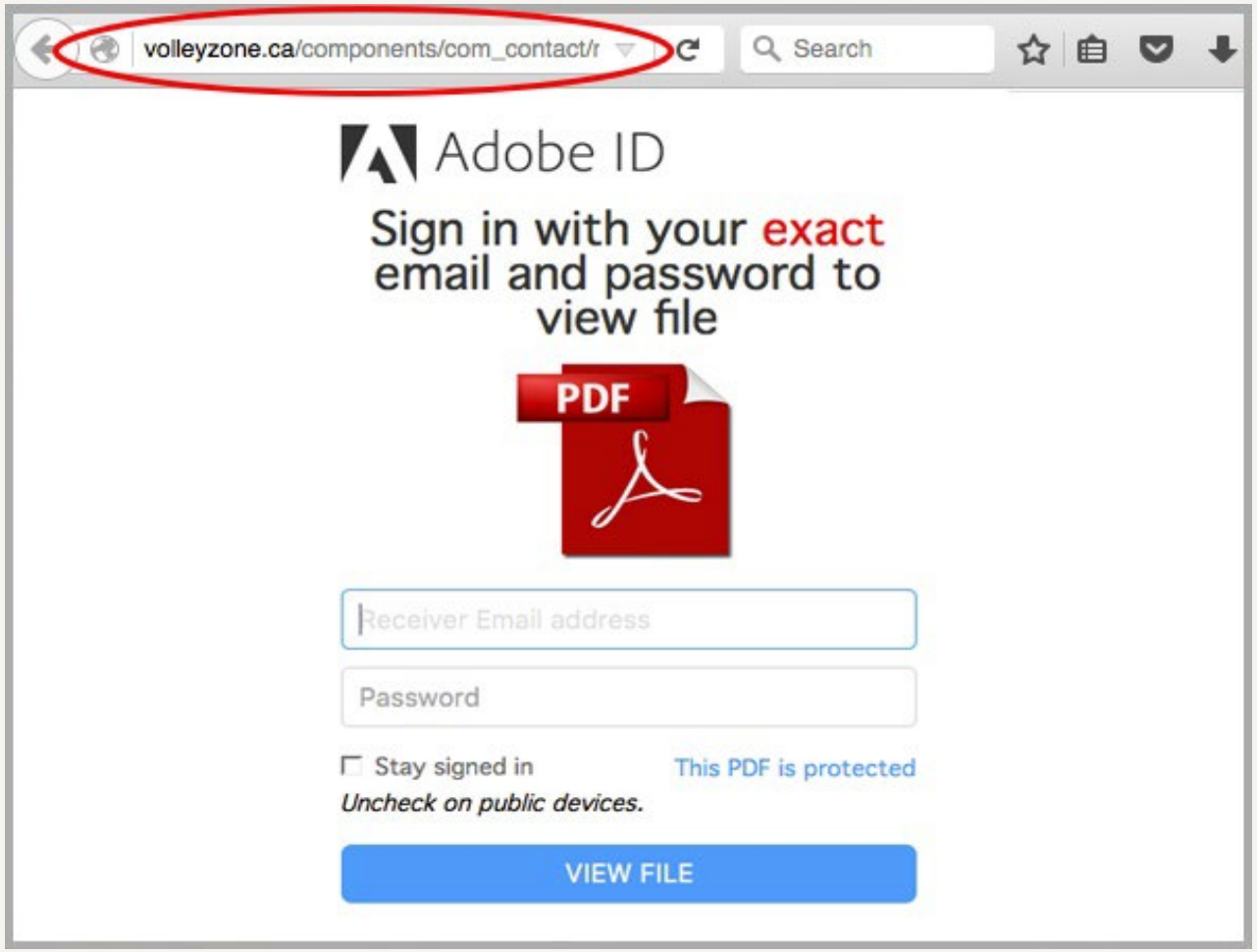


Σε πολλές περιπτώσεις ένα τέτοιο e-mail μπορεί να έχει μαζί και συνημμένα αρχεία.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Ύποπτα email & συνημμένα αρχεία

- Σε καμία περίπτωση δεν ανοίγουμε link ή αρχεία από ύποπτα μηνύματα.
- Αν ένα email μας προβληματίζει, ζητάμε βοήθεια για έλεγχο πριν το ανοίξουμε είτε από τον τεχνικό υπεύθυνο είτε από το helpdesk του Πανεπιστημίου.
- Διαγράφουμε spam ή ύποπτα μηνύματα.
- Αν ανοίξουμε κατά λάθος ύποπτο αρχείο ή ανοίξουμε link και συμπληρώσουμε κωδικούς θα πρέπει να γίνει έλεγχος στον υπολογιστή από τον τεχνικό υπεύθυνο και να γίνει άμεσα αλλαγή του κωδικού.
- Αν υποψιαζόμαστε ότι ο κωδικός μας έχει διαρρεύσει, θα πρέπει τον αλλάξουμε άμεσα στο https://mussa.upnet.gr/



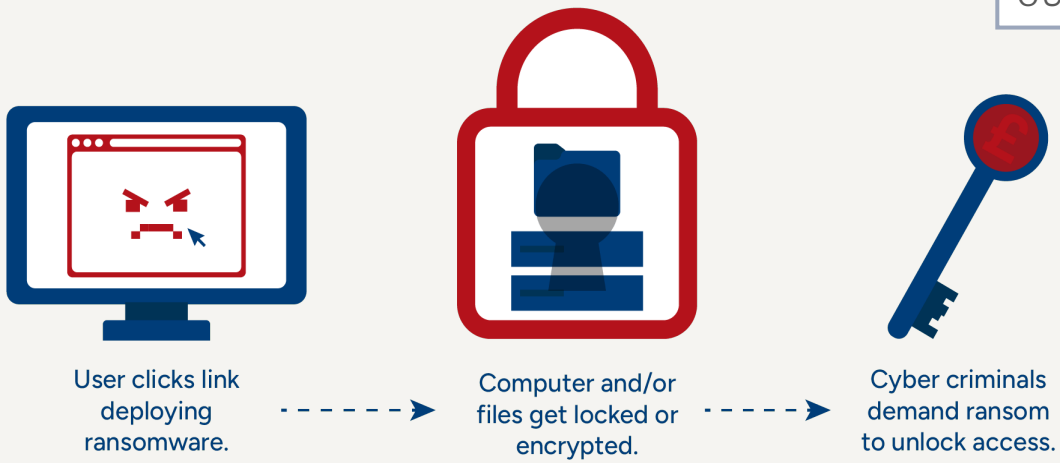
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Ransomware & ιοί

- Δεν αγνοούμε τις προειδοποιήσεις ασφαλείας.
- Δεν ανοίγουμε αρχεία που ζητούν “Ενεργοποίηση περιεχομένου” ή macros.
- Δεν κατεβάζουμε συνημμένα αρχεία από το email τα οποία φαίνονται ύποπτα, ούτε τα ανοίγουμε, ούτε πατάμε σε ύποπτα links.
- Πρέπει να επιτρέπουμε στα Windows να ολοκληρώνουν τις ενημερώσεις τους και να κάνουμε επανεκκίνηση όταν μας το ζητάει το σύστημα.

Τα **Ransomware** είναι προγράμματα τα οποία αφού μπουν σε έναν υπολογιστή μπορεί να κλειδώσουν ή να κρυπτογραφήσουν τα αρχεία και στη συνέχεια να ζητηθούν λύτρα για την αποκρυπτογράφηση.
Τα ransomware τρέχουν κρυφά και μπορεί να μην αντιληφθούμε ότι βρίσκονται στον υπολογιστή μας.

Ένας **Ιός** είναι πρόγραμμα που μπαίνει στον υπολογιστή, αντιγράφει τον εαυτό του, μολύνει αρχεία ή προγράμματα και εξαπλώνεται από σύστημα σε σύστημα μέσα από το δίκτυο.



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Αποθήκευση και φύλαξη ηλεκτρονικών αρχείων

- Δεν συνδέουμε στον υπολογιστή μας **φλασάκια USB** “τυχαίας προέλευσης”, ή προσωπικά μας και γενικά φλασάκια που δεν χρησιμοποιούνται αποκλειστικά για υπηρεσιακούς λόγους.
- Για αρχεία που είναι σημαντικά, είναι καλή πρακτική να κρατάμε **αντίγραφα ασφαλείας** ανά τακτά χρονικά διαστήματα σε υπολογιστική υποδομή ή εξωτερικό μέσο αποθήκευσης, σύμφωνα με τις υποδείξεις της υπηρεσίας.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Cloud sharing-Διαμοιρασμός αρχείων

Δεν πρέπει

- να αποθηκεύουμε
- να επεξεργαζόμαστε
- να διακινούμε υπηρεσιακά έγγραφα

με μη ιδρυματικές cloud υπηρεσίες (πχ Google Drive, Dropbox, We Transfer, iLovePDF) με μη ιδρυματικούς λογαριασμούς.

Cloud sharing-Διαμοιρασμός αρχείων

Το Πανεπιστήμιο διαθέτει τις υπηρεσίες

- Cloud Hub (https://cloudhub.upatras.gr)
- Microsoft One Drive (https://upatrasgr-my.sharepoint.com) μέσω του ιδρυματικού λογαριασμού.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Χρήση Παραγωγικής Τεχνητής Νοημοσύνης-GenAI

Θα πρέπει να είμαστε ιδιαίτερα προσεκτικοί όταν χρησιμοποιούμε εργαλεία τεχνητής νοημοσύνης, όπως το ChatGPT, το Gemini, το Grok, κτλ.

- Δεν θα πρέπει να τους δίνουμε πρόσβαση σε ευαίσθητα δεδομένα, όπως προσωπικά δεδομένα, κωδικούς πρόσβασης ή σε όλα τα αρχεία της συσκευής μας.
- Δεν θα πρέπει επίσης να ανεβάζουμε σε εργαλεία AI αρχεία της Υπηρεσίας με ευαίσθητα δεδομένα (για παράδειγμα στοιχεία υπαλλήλων, Φοιτητών, μελών ΔΕΠ, οικονομικά στοιχεία, οικογενειακά κ.λπ.)

Πρόσβαση από εξωτερικά δίκτυα - Η υπηρεσία VPN του Πανεπιστημίου Πατρών

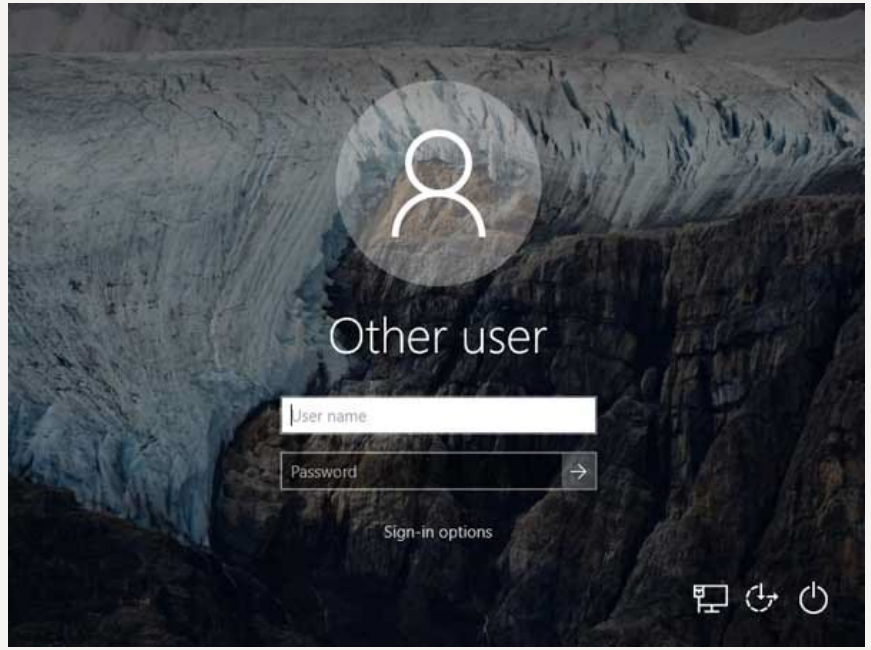
Όταν συνδεόμαστε από εξωτερικά δίκτυα, π.χ. από wifi άλλων οργανισμών ή χώρων εστίασης, θα πρέπει να συνδεόμαστε μέσω του VPN του Πανεπιστημίου, έτσι ώστε τα δεδομένα που δέχεται και στέλνει η συσκευή μας να είναι κρυπτογραφημένα και προστατευμένα.

Στη διεύθυνση https://www.upnet.gr/services/vpn/ του UPnet μπορείτε να βρείτε οδηγίες για τη σύνδεση στην υπηρεσία VPN του Πανεπιστημίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Χρήση προσωπικών και υπηρεσιακών ηλεκτρονικών υπολογιστών

- Χρησιμοποιούμε διαφορετικές ηλεκτρονικές συσκευές (σταθερούς ή φορητούς υπολογιστές, κινητά τηλέφωνα κτλ.) για **προσωπική** και για **υπηρεσιακή** χρήση.
- Δεν αποθηκεύουμε υπηρεσιακά αρχεία τοπικά στις προσωπικές συσκευές και δεν χρησιμοποιούμε το υπηρεσιακό ή άλλο email σαν αποθηκευτικό χώρο.
- Ο υπηρεσιακός υπολογιστής πρέπει να είναι πάντοτε προστατευμένος, με ισχυρό **κωδικό** (password) χρήστη τον οποίο πρέπει να αλλάζουμε κατά διαστήματα.



Περίπτωση εντοπισμού περιστατικού ασφαλείας

Ποια είναι τα πρώτα βήματα που πρέπει να κάνουμε;

Σε περίπτωση που εμφανιστεί στην οθόνη του υπολογιστή μας κάποιο μήνυμα που να δηλώνει παραβίαση, ή διαπιστώσουμε ότι έχουν "κλειδώσει" αρχεία, ακολουθούμε τα παρακάτω βήματα:

- Ενημερώνουμε αμέσως την Ομάδα Ασφάλειας Πληροφοριακών Συστημάτων στη φόρμα https://cybersecurity.upatras.gr/report-form/ ή στο e-mail: **cybersectf@upatras.gr**

Ενημερώνεται άμεσα επίσης ως εξής:

- αν η παραβίαση αφορά Διοικητικές Υπηρεσίες, ο Προϊστάμενος του Τμήματος.
- αν η παραβίαση αφορά Εργαστήριο, ο Διευθυντής του Εργαστηρίου, ο οποίος ενημερώνει τον Πρόεδρο και τον Τεχνικό Υπεύθυνο του Τμήματος.
- αν η παραβίαση αφορά Ακαδημαϊκό Τμήμα, ο Πρόεδρος και ο Τεχνικός Υπεύθυνος του Τμήματος.

Ο καθένας από τους προηγούμενους θα πρέπει να διατηρήσει επικοινωνία με την Ομάδα Ασφαλείας Πληροφοριακών Συστημάτων για την παρακολούθηση της εξέλιξης του περιστατικού στο email: cybersectf@upatras.gr

Περίπτωση εντοπισμού περιστατικού ασφαλείας

Παράλληλα:

- **Αποσυνδέουμε τον υπολογιστή από το δίκτυο** βγάζοντας το καλώδιο δικτύου από το πίσω μέρος της κεντρικής μονάδας του υπολογιστή ή από τον τοίχο. Αν χρησιμοποιούμε laptop που συνδέεται ασύρματα, κλείνουμε το ασύρματο δίκτυο. Αποσυνδέουμε εξωτερικές συσκευές που τυχόν είναι συνδεδεμένες (π.χ. USB και εξωτερικούς δίσκους)
- **Δεν κάνουμε επανεκκίνηση ή τερματισμό** στον υπολογιστή μας, ούτε διαγράφουμε αρχεία.
- Μόνο σε περίπτωση που δεν μπορούμε να βρούμε ποιο είναι το καλώδιο δικτύου για να αποσυνδέσουμε τον υπολογιστή, τον σβήνουμε.
- **Δεν επιχειρούμε μόνοι μας να "διορθώσουμε" μολύνσεις, ούτε διαγράφουμε αρχεία,** ακόμα και αν φαίνονται κλειδωμένα.

Ομάδα Υποστήριξης Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών του Πανεπιστημίου Πατρών

cybersectf@upatras.gr

https://cybersecurity.upatras.gr/

ΠΑΝΕΠΙΣΤΉΜΙΟ ΠΑΤΡΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS