ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
ΔΙΕΥΘΥΝΣΗ ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΟΥ ΕΛΕΓΧΟΥ

Αριθμ. Πρωτ. ΑΝΑΦΟΡΩΝ: 1590
Ημερομ. Κατάθεσης: 4/4/2025

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

ΕΛΛΗΝΙΚΗ ΛΥΣΗ

# ΑΝΑΦΟΡΑ

Αθήνα, 1/4/2025

**Του:** Φωτόπουλου Στυλιανού, Βουλευτού Α' Ανατολικής Αττικής

**ΠΡΟΣ:** Την κ. Υπουργό Παιδείας, Θρησκευμάτων και Αθλητισμού
Τον κ. Υπουργό Ψηφιακής Διακυβέρνησης

**ΘΕΜΑ:** «Αίτημα του υπογράφοντος, αφενός, για επαλήθευση ή διάψευση της διαρροής προσωπικών δεδομένων των φοιτητών του Ελληνικού Ανοικτού Πανεπιστημίου (ΕΑΠ), και αφετέρου, για γνωστοποίηση των δράσεων στις οποίες προτίθεται να προβεί η αρμόδια πολιτική ηγεσία, τόσο για την αποφυγή της επανάληψης του ατυχούς και επιζήμιου για τους φοιτητές ως άνω γεγονότος, όσο και για τις κυρώσεις που θα επιβληθούν στα αρμόδια για την ασφαλή τήρηση των προσωπικών δεδομένων των φοιτητών στελέχη του ΕΑΠ, επειδή δεν έλαβαν τα απαραίτητα μέτρα για την αποφυγή μιας σχετικής διαρροής»

Κυρία και Κύριε Υπουργοί,

Δεκάδες φοιτητές του ΕΑΠ έθεσαν υπόψη μας δημοσίευση στο Διαδίκτυο, όπως επισυνάπτεται στην παρούσα, η οποία μας πληροφορεί για την διαρροή προσωπικών δεδομένων των φοιτητών του ΕΑΠ. Στο σχετικό κείμενο γίνεται κάποια αναφορά σε επιζήμιες συνέπειες του εν λόγω γεγονότος στους φοιτητές. Κατόπιν επικοινωνίας τους μαζί μας, οι ανωτέρω μας ζήτησαν να διαμεσολαβήσουμε ενώπιόν σας, ερωτώντας σας καταλλήλως, ώστε να τους διαβιβάσουμε απαντήσεις σας σχετικά, αφενός, με την επαλήθευση ή τη διάψευση της διαρροής προσωπικών δεδομένων των φοιτητών του Ελληνικού Ανοικτού Πανεπιστημίου (ΕΑΠ), και αφετέρου, για τη γνωστοποίηση των δράσεων στις οποίες προτίθεστε να προβείτε, τόσο για την αποφυγή της επανάληψης του ατυχούς και επιζήμιου για τους φοιτητές ως άνω γεγονότος, όσο και για τις κυρώσεις που θα επιβληθούν στα αρμόδια για την ασφαλή τήρηση των προσωπικών δεδομένων των φοιτητών στελέχη του ΕΑΠ, επειδή δεν έλαβαν τα απαραίτητα μέτρα για την αποφυγή μιας σχετικής διαρροής. Με δεδομένα όλα τα παραπάνω και αφού λάβετε υπόψη τα αναφερόμενα στο συνημμένο δημοσίευμα, σας παρακαλώ, να τα εξετάσετε και να αποφανθείτε σχετικά

**Ο Αναφέρων Βουλευτής**

**Φωτόπουλος Στυλιανός**

---

**Επισυνάπτεται:** Το ανωτέρω αναφερόμενο δημοσίευμα στο Διαδίκτυο

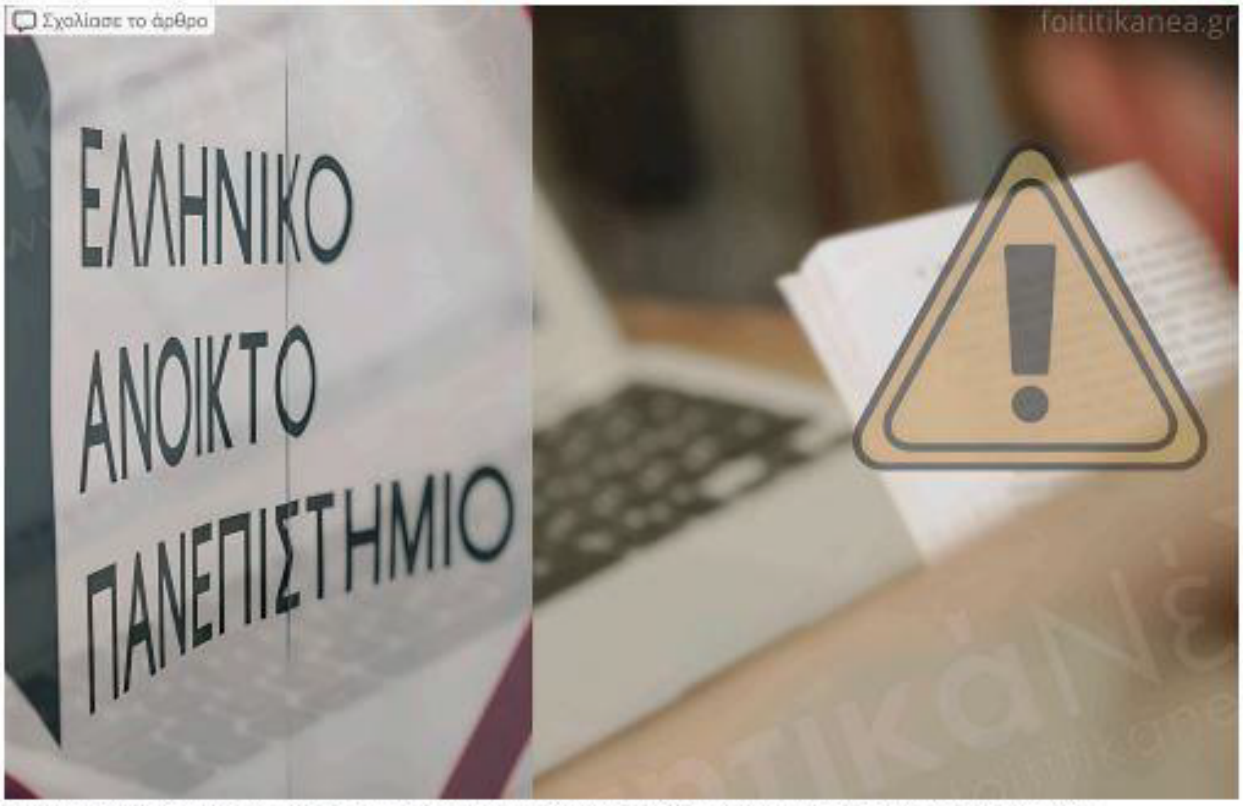
ΦοιτητικάΝέα
www.foititikanea.gr

Παρασκευή, 28 Μαρτίου 2025 18:45:05

# Ένας κυβερνοεφιάλτης για το ΕΑΠ / Επιβεβαιώνεται η διαρροή 813GB προσωπικών δεδομένων στο dark web!

FoititikaNea Newsroom | 17:09 - Παρασκευή, 28 Μαρτίου 2025

ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ




**Ένας κυβερνοεφιάλτης για το ΕΑΠ / Επιβεβαιώνεται η διαρροή 813GB προσωπικών δεδομένων στο dark web!**

Φοιτητικές Ειδήσεις: Το **Ελληνικό Ανοικτό Πανεπιστήμιο (ΕΑΠ)** επιβεβαιώνει σήμερα Παρασκευή, 28/03/2025, μετά την πάροδο πέντε μηνών, την **παραβίαση των πληροφοριακών του συστημάτων**, που είχε προκληθεί από μια κακόβουλη κυβερνοεπίθεση στις 25 Οκτωβρίου 2024.

Η επίθεση που είχε δεχτεί από τις 25/10/2024 το **ΕΑΠ** είχε θέσει εκτός λειτουργίας όλες τις βασικές **ηλεκτρονικές υπηρεσίες** (εκπαιδευτικές πλατφόρμες, μαθήματα, εφαρμογές κτλ), προκαλώντας πλήρη παράλυση της ομαλής λειτουργίας του Ιδρύματος για αρκετό χρονικό διάστημα. Τα **«Φοιτητικά Νέα»** είχαν αναδείξει από τις 03/11/2024, μέσω σχετικών ρεπορτάζ, πως η επίθεση είχε προκαλέσει σοβαρές ανησυχίες στους **φοιτητές** και τους **αποφοίτους** του Ιδρύματος καθώς κυκλοφορούσε στο διαδίκτυο η (ενδεχόμενη) πιθανότητα **διαρροής των προσωπικών τους δεδομένων**, σε περίπτωση που το ΕΑΠ **δεν κατέβαλε** τα απαιτούμενα λύτρα στους κυβερνοεγκληματίες εντός του συγκεκριμένου χρονικού διαστήματος που είχαν ορίσει. **Παράλληλα**, **φοιτητές** και **απόφοιτοι**, σε **επιστολές** τους προς τη **διοίκηση**, ζητούσαν **ξεκάθαρες** απαντήσεις, όπως **ποια δεδομένα** είχαν **διαρρεύσει**, **ποιοι είχαν πρόσβαση** και, κυρίως, **ποιες ενέργειες** έπρεπε να κάνουν για να **προστατευθούν**.

Όπως ανακοινώθηκε και επίσημα σήμερα από το Ελληνικό Ανοικτό Πανεπιστήμιο, η κυβερνοεπίθεση πραγματοποιήθηκε με **λογισμικό τύπου ransomware**, το οποίο κρυπτογράφησε το σύστημα διαχείρισης **εικονικών μηχανών** και προκάλεσε σοβαρές **δυσλειτουργίες** σε δευτερεύοντα συστήματα του ΕΑΠ.

## Διαρροή 813GB δεδομένων – Στο dark web προσωπικές πληροφορίες

Η επίθεση είχε ως αποτέλεσμα τη **διαρροή 813GB προσωπικών δεδομένων** στο **dark web** (όπως παρουσιάστηκε στο προ μηνών ρεπορτάζ του «Φοιτητικά Νέα»). Ειδικότερα, σύμφωνα με τον Υπεύθυνο Προστασίας Δεδομένων (DPO) του ΕΑΠ, τα υποκλαπέντα αρχεία περιέχουν προσωπικά στοιχεία σε μορφές **doc, pdf και excel**, ενώ η ανάκτησή τους από τρίτους δεν είναι εύκολη χωρίς

[redacted]

**εξειδικευμένες τεχνικές γνώσεις**. Ωστόσο, οι μέχρι τώρα αναλύσεις δείχνουν ότι **μόνο 65GB των δεδομένων έχουν ανακτηθεί** και είναι **διαθέσιμα προς λήψη**.

## Ποιες κατηγορίες προσωπικών δεδομένων ενδέχεται να διέρρευσαν

Το **ΕΑΠ** προχώρησε σε **αναλυτική ενημέρωση** για τα δεδομένα που ενδέχεται να έχουν διαρρεύσει, μεταξύ των οποίων περιλαμβάνονται:

- **Ονοματεπώνυμα, ΑΦΜ, ΑΜΚΑ, αριθμοί ταυτότητας, στοιχεία συγγενών**
- **Δεδομένα επικοινωνίας** όπως τηλέφωνα, emails, ταχυδρομικές διευθύνσεις
- **Ακαδημαϊκές επιδόσεις**, βαθμολογίες, τίτλοι σπουδών
- **Οικονομικά στοιχεία** όπως **IBAN, στοιχεία πληρωμών, τιμολόγια**
- **Δεδομένα υγείας, ερευνητική και επαγγελματική δραστηριότητα**

Παρότι οι πραγματικές διαρροές φαίνεται να είναι **μικρότερες**, το **ΕΑΠ** συνιστά **προσοχή και λήψη μέτρων προστασίας** από όσους ενδέχεται να επηρεάζονται.

## Οι ανησυχίες των φοιτητών και αποφοίτων επιβεβαιώθηκαν

Τα **«Φοιτητικά Νέα»** είχαν αναδείξει το ζήτημα από νωρίς, δημοσιεύοντας ρεπορτάζ με τις έντονες ανησυχίες των **φοιτητών** και **αποφοίτων** σχετικά με την ασφάλεια των προσωπικών τους δεδομένων και την ενδεχόμενη **διαρροή** τους. Οι πρώτες αντιδράσεις δεν άργησαν να έρθουν, καθώς πολλοί φοιτητές και απόφοιτοι εξέφρασαν πως τα **προσωπικά τους στοιχεία** έχουν ενδεχομένως εκτεθεί σε κακόβουλους τρίτους.

Η ανησυχία αυτή εντάθηκε και όταν το ζήτημα της κυβερνοεπίθεσης έφτασε στην Βουλή. Στις 06/11/2024 είχε κατατεθεί σχετική αναφορά προς τον τότε **Υπουργό Παιδείας, Θρησκευμάτων και Αθλητισμού, Κυριάκο Πιερρακάκη**, με βάση δημοσίευμα του «Φοιτητικά Νέα» για την ανησυχία των φοιτητών αναφορικά με την ασφάλεια των προσωπικών τους δεδομένων.

Ιδιαίτερη ανησυχία εκφράστηκε και από τους **στρατιωτικούς φοιτητές** και απόφοιτους του ΕΑΠ. Οι στρατιωτικοί είχαν προβεί σε δημόσιες ανακοινώσεις ότι η διαρροή προσωπικών δεδομένων μπορεί να αφορά ευαίσθητες **στρατιωτικές πληροφορίες**, οι οποίες μπορεί να σχετίζονται άμεσα με την **εθνική ασφάλεια**. Οι ανησυχίες τους επικεντρώνονταν κυρίως στις πληροφορίες που αφορούσαν το **ΑΦΜ**, **ΑΜΚΑ**, **στρατιωτικές ταυτότητες**, **οικονομικά και υγειονομικά στοιχεία** των στρατιωτικών. Η **Ένωση Στρατιωτικών Περιφερειακής Ενότητας Ξάνθης (Ε.Σ.Π.Ε.Ε.Ξ.)** είχε ζητήσει **άμεσες διευκρινίσεις** από το ΕΑΠ σχετικά με τη διαρροή των δεδομένων και τις ενέργειες που έχουν γίνει για την **προστασία των προσωπικών πληροφοριών** των στρατιωτικών φοιτητών.

Η **διοίκηση του ΕΑΠ**, την περίοδο που είχε πέσει θύμα της κακόβουλης επίθεσης, σε μια προσπάθεια να καθησυχάσει τους φοιτητές και αποφοίτους, απάντησε μέσω ανακοίνωσης στις 06 Νοεμβρίου 2024. Ο **Πρύτανης του ΕΑΠ**, **Μανώλης Κουτούζης**, υποστήριξε ότι μέχρι εκείνη τη στιγμή δεν υπήρχαν **τεκμηριωμένα στοιχεία** που να επιβεβαιώνουν τη διαρροή των προσωπικών δεδομένων, και ότι η **Εθνική Αρχή Κυβερνοασφάλειας** καθώς και η **Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος** είχαν ήδη ενημερωθεί.

## Οι ενέργειες του ΕΑΠ για την αντιμετώπιση της επίθεσης

Μετά την **κυβερνοεπίθεση**, το **ΕΑΠ** προχώρησε στις εξής ενέργειες:

- **Ενημέρωσε άμεσα** την **Εθνική Αρχή Κυβερνοασφάλειας** και τη **Δίωξη Ηλεκτρονικού Εγκλήματος**
- **Γνωστοποίησε το περιστατικό** στην **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**
- **Απέκλεισε την πρόσβαση των επιτιθέμενων** διακόπτοντας τα επηρεαζόμενα συστήματα
- **Συνεργάστηκε με εξειδικευμένες εταιρείες κυβερνοασφάλειας** για την **ανάκτηση και προστασία των δεδομένων**
- **Κατέθεσε μήνυση κατά αγνώστων**
- **Ενίσχυσε τα μέτρα ασφαλείας** και προχώρησε σε **αναβάθμιση των πληροφοριακών συστημάτων**

## Κίνδυνοι και οδηγίες προστασίας για τους χρήστες

Το **ΕΑΠ** προειδοποιεί ότι οι **χρήστες των υπηρεσιών του** ενδέχεται να είναι στόχοι **phishing επιθέσεων, απάτης ή παραβίασης της ιδιωτικής τους ζωής**. Συστήνει στους ενδιαφερόμενους να λάβουν **προληπτικά μέτρα προστασίας**, όπως:

- **Άμεση αλλαγή κωδικών πρόσβασης** με **ισχυρούς και μοναδικούς συνδυασμούς**
- **Αποφυγή ύποπτων emails και κλήσεων** που ζητούν προσωπικά δεδομένα
- **Ενημέρωση των τραπεζών** σε περίπτωση ύποπτων οικονομικών συναλλαγών

[redacted]

- **Ενεργοποίηση ειδοποιήσεων ασφαλείας** σε λογαριασμούς και ηλεκτρονικές υπηρεσίες

Για περισσότερες πληροφορίες, το **ΕΑΠ** έχει δημοσιεύσει έναν **αναλυτικό οδηγό προστασίας δεδομένων**, τον οποίο μπορείτε να τον δείτε παρακάτω.

Το **ΕΑΠ** διαβεβαιώνει ότι **συνεργάζεται πλήρως με τις αρμόδιες αρχές** και ότι η **αναβάθμιση των πληροφοριακών του συστημάτων βρίσκεται σε εξέλιξη**, με στόχο τη **διασφάλιση της ασφάλειας των δεδομένων των χρηστών**.

## Αναλυτικά η επίσημη ανακοίνωση του ΕΑΠ

Αξιότιμοι/ες κύριοι/ες,

Στο πλαίσιο της **υπεύθυνης και διαφανούς ενημέρωσής** σας, αναφορικά με την **κακόβουλη επίθεση** που είχε δεχτεί το Ίδρυμα, από ομάδα κυβερνοεγκληματιών, στις **25/10/2024**, θα θέλαμε, αρχικώς, να σας ενημερώσουμε ότι η διερεύνηση του συμβάντος βρίσκεται σε εξέλιξη αλλά με βάση τα έως τώρα ευρήματα είμαστε σε θέση να παρέχουμε **νέα ενημέρωση** πάνω σε αυτό το θέμα.

## Το περιστατικό

Στις **25/10/2024** εντοπίσαμε **ύποπτη δραστηριότητα** στα πληροφοριακά μας συστήματα, η οποία αφορούσε σε **μη εξουσιοδοτημένη πρόσβαση**. Η επίθεση πραγματοποιήθηκε με λογισμικό τύπου **ransomware (ransomware attack)**, κατά την οποία το κακόβουλο λογισμικό απέκτησε πρόσβαση, με **υποκλοπή συγκεκριμένων δικαιωμάτων**, στην **κύρια υποδομή πληροφορικής** και την **υποδομή αντιγράφων ασφαλείας** και προκάλεσε **κρυπτογράφηση** του συστήματος διαχείρισης εικονικών μηχανών και δυσλειτουργίες σε δευτερεύοντα συστήματα και στο δίκτυο δεδομένων. Η κρυπτογράφηση **δεν επηρέασε το σύνολο των εφεδρικών αντιγράφων**, το οποίο ανακτήθηκε από την υποδομή αντιγράφων ασφαλείας και χρησιμοποιήθηκε, μετά από **ενδελεχή έλεγχο ασφαλείας**, για την **ανάκαμψη των συστημάτων και υπηρεσιών** του Πανεπιστημίου.

## Η έκταση της διαρροής

Η επίθεση αυτή είχε ως αποτέλεσμα την **περιορισμένη διαρροή προσωπικών δεδομένων**. Το μέγεθος των δεδομένων που διέρρευσε ανέρχεται σε **813GB**, σύμφωνα με τα έως τώρα στοιχεία μας. Ωστόσο, είναι σημαντικό να διευκρινίσουμε ότι το συγκεκριμένο μέγεθος αντιπροσωπεύει ένα **εξαιρετικά μικρό ποσοστό**, σε σχέση με τον συνολικό όγκο δεδομένων που διατηρεί το Ίδρυμα (μεγέθους πολλών terabytes), γεγονός που υποδηλώνει ότι η διαρροή είναι **περιορισμένης κλίμακας**. Το μέγεθος αυτό μπορεί να συγκριθεί, ενδεικτικά, με τη χωρητικότητα τοπικού δίσκου ενός τυπικού υπολογιστή. Τα διαρρεύσαντα αρχεία περιείχαν, σύμφωνα με τις έως τώρα ενδείξεις, **προσωπικά δεδομένα** σε διάφορες μορφές αρχείων (κατά κύριο λόγο doc, pdf, excel). Επιπλέον, το αρχείο που έχει διαρρεύσει βρίσκεται στο **σκοτεινό διαδίκτυο (dark web)**, όπου η πρόσβαση απαιτεί **εξειδικευμένες, τεχνικές γνώσεις**.

Επιπρόσθετα, σύμφωνα με τις έως τώρα αναλύσεις, το συγκεκριμένο αρχείο που διέρρευσε **δεν είναι εφικτό**, στην παρούσα φάση, να ληφθεί ολόκληρο. Αυτό που μπορεί να καταστεί διαθέσιμο για λήψη, είναι αρκετά μικρότερο από το αρχικό σύνολο των δεδομένων που υποκλάπηκαν (περίπου **65 GB** έχουν ανακτηθεί).

## Κατηγορίες προσωπικών δεδομένων που ενδεχομένως να διέρρευσαν

Το Ίδρυμα προβαίνει σε ενημέρωση σχετικά με τις πιθανές κατηγορίες δεδομένων που ενδέχεται να έχουν επηρεαστεί. Η αναφορά μας περιλαμβάνει **δεδομένα/κατηγορίες δεδομένων** που θα μπορούσαν θεωρητικά να έχουν εκτεθεί.

- **Ονοματεπώνυμο, Πατρώνυμο / Μητρώνυμο, Ιδιότητα, Στοιχεία Συγγενών, Υπηκοότητα, Φύλο, Ημερομηνία Γέννησης, ΑΦΜ, ΑΜΚΑ, ΑΜ, ΑΔΤ, Υπογραφή (φυσική), Φωτογραφίες, όνομα χρήστη**
- **Δεδομένα Επικοινωνίας** (Ταχυδρομική Διεύθυνση, Αριθμός τηλεφώνου (σταθερό & κινητό), Διεύθυνση ηλεκτρονικού ταχυδρομείου (προσωπική & ιδρύματος), ηλεκτρονική αλληλογραφία)
- **Ακαδημαϊκά και Εκπαιδευτικά Δεδομένα & Τίτλοι Σπουδών** (Βαθμολογίες και επιδόσεις, Τίτλοι σπουδών, Βεβαιώσεις σπουδών)
- **Δεδομένα Υγείας**
- **Οικονομικά Δεδομένα** (IBAN, στοιχεία τιμολόγησης, στοιχεία πληρωμής δαπάνης)
- **Δεδομένα Επαγγελματικής & Ερευνητικής Δραστηριότητας** (Βιογραφικό σημείωμα, ερευνητικό / επαγγελματικό / διδακτικό / συγγραφικό έργο)
- **Δεδομένα Αποφάσεων Συλλογικών Οργάνων, αποφάσεις επιτροπών**
- **Δεδομένα Συμβάσεων, Αναδόχων & Προσφορών**

Ωστόσο, βάσει των μέχρι τώρα διαθέσιμων ενδείξεων και της συνεχιζόμενης έρευνας, η **πραγματική διαρροή** φαίνεται να περιορίζεται σε **σαφώς μικρότερο εύρος δεδομένων**.

[redacted]

## Ενέργειες που έγιναν προς αντιμετώπιση του περιστατικού

Το Ε.Α.Π. εφάρμοσε **όλα τα απαραίτητα μέτρα** για να διασφαλίσει την **ελάχιστη, δυνατή διαρροή** ενώ παράλληλα, συνεργάστηκε, **άμεσα**, με την **Εθνική Αρχή Κυβερνοασφάλειας**, τη **Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος** και την **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**.

Πιο συγκεκριμένα:

- Από την πρώτη στιγμή του συμβάντος (**25/10/2024**) ενημερώθηκε τόσο η **Εθνική Αρχή Κυβερνοασφάλειας** όσο και η **Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος**. Η ενημέρωση είναι **συνεχής**.
- Γνωστοποιήθηκε, **έγκαιρα**, το περιστατικό στην **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)**. Η αρχική δήλωση **επικαιροποιείται** ανάλογα με τα δεδομένα.
- Δημιουργήθηκε **Ομάδα Διαχείρισης Περιστατικού**.
- Οι **Τεχνικές Υπηρεσίες** του Ιδρύματος, σε συνεργασία με **εξειδικευμένη εταιρεία**, προέβησαν, **άμεσα**, σε όλες τις ενέργειες για την αντιμετώπιση του περιστατικού και τον **περιορισμό των επιπτώσεών** του. Πιο συγκεκριμένα, την ίδια ημέρα (**25/10/2024**), έγινε **απομόνωση του συμβάντος** (διακοπή λειτουργίας των συστημάτων που επηρεάζονται).
- **Ενημέρωση των υποκειμένων των δεδομένων** και παροχή ενδεικτικών οδηγιών για την προστασία των προσωπικών τους δεδομένων.
- **Ενίσχυση της ευαισθητοποίησης** του ακαδημαικού και διοικητικού προσωπικού σχετικά με την προστασία των προσωπικών δεδομένων και τους κινδύνους από κυβερνοεπιθέσεις.
- **Ετοιμασία προκήρυξης** για ενίσχυση της Τεχνικής Υπηρεσίας με επιπρόσθετο εξειδικευμένο προσωπικό.
- **Κατατέθηκε μηνυτήρια αναφορά** κατά αγνώστου και κατά παντός υπευθύνου για την κακόβουλη επίθεση.
- Έχουν, ήδη, τεθεί σε εφαρμογή **στοχευμένα μέτρα ενίσχυσης της ασφάλειας** των πληροφοριακών μας συστημάτων ενώ βρίσκεται σε εξέλιξη μία **συνολική αναβάθμιση της υποδομής μας**, η οποία περιλαμβάνει την ενίσχυση των υφιστάμενων μηχανισμών προστασίας και την προσθήκη επιπρόσθετων δικλίδων ασφαλείας.
- Για λόγους ασφαλείας, οι **ακριβείς, τεχνικές ενέργειες** που έχουν, ήδη, ληφθεί ή προγραμματιστεί να πραγματοποιηθούν **δε μπορούν να δημοσιοποιηθούν**.

## Ενδεχόμενες συνέπειες της διαρροής για τα υποκείμενα των δεδομένων

Μία διαρροή δεδομένων μπορεί να έχει **πιθανές συνέπειες** για τα υποκείμενα των δεδομένων, όπως:

- **Στοχευμένες επιθέσεις ηλεκτρονικού ψαρέματος (phishing)**.
- **Απόπειρες απάτης**, μέσω email ή τηλεφώνου.
- **Ενδεχόμενη, μη εξουσιοδοτημένη χρήση προσωπικών πληροφοριών** που μπορεί να οδηγήσουν σε απάτες και κακόβουλη χρήση αυτών των προσωπικών πληροφοριών από επιτήδειους ή εγκληματίες.
- **Κατάχρηση των δεδομένων** για δημιουργία ψεύτικων λογαριασμών ή πλαστογραφία στοιχείων.
- **Διαρροή πληροφοριών** που μπορεί να οδηγήσει σε κοινωνική μηχανική (social engineering).
- **Κακόβουλη χρήση των πληροφοριών**, με στόχο απάτη (κυρίως οικονομική).
- **Στόχευση για ανεπιθύμητη διαφήμιση ή ανεπιθύμητες κλήσεις (spam)**.
- **Παραβίαση της ιδιωτικής ζωής**, μέσω ενδεχόμενης διαρροής προσωπικών δεδομένων σε μη εξουσιοδοτημένα άτομα ή φορείς.
- **Υποκλοπή ταυτότητας (identity theft)** και χρήση των προσωπικών στοιχείων για δόλιες δραστηριότητες.

Σημειώνεται ότι ο **πιθανός αριθμός των εμπλεκόμενων υποκειμένων** φαίνεται να είναι, **αισθητά, περιορισμένος** ενώ και οι **κατηγορίες των δεδομένων** που ενδέχεται να έχουν διαρρεύσει είναι, **σημαντικά, λιγότερες** από όσες αναφέρονται. Παρ' όλα αυτά, **συνιστούμε σε όλους τους ενδιαφερόμενους να λαμβάνουν τα κατάλληλα μέτρα προστασίας**, διασφαλίζοντας τα δικαιώματά τους ως υποκείμενα δεδομένων. Με αυτόν τον τρόπο, όχι μόνο συμμορφώνονται με τις απαιτήσεις προστασίας αλλά και ενισχύουν, **ενεργά, την ιδιωτικότητά** τους.

## Μέτρα προστασίας για τα υποκείμενα των δεδομένων

Για την **προστασία σας**, σας συνιστούμε να ακολουθήσετε τις εξής οδηγίες:

- **Αλλάξτε, άμεσα, τους κωδικούς πρόσβασης** στους λογαριασμούς σας (ηλεκτρονικού ταχυδρομείου και υπηρεσιών μητρώου). Συνιστάται η χρήση ενός **μοναδικού και ισχυρού κωδικού**, με τουλάχιστον **10 χαρακτήρες** που να περιλαμβάνει

[redacted]

συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών και συμβόλων. Επιπλέον, προτείνεται η **τακτική αλλαγή του κωδικού**, ιδανικά κάθε έξι μήνες.

- **Αποφύγετε τη χρήση του ίδιου κωδικού πρόσβασης** σε πολλαπλές υπηρεσίες.
- **Να είστε προσεκτικοί** με emails ή τηλεφωνικές κλήσεις που ζητούν **προσωπικά στοιχεία ή οικονομικές πληροφορίες**.
- **Μην ανοίγετε συνδέσμους και μην κατεβάζετε συνημμένα** από άγνωστες ή ύποπτες πηγές.
- **Παρακολουθείτε τις συναλλαγές σας** για τυχόν μη εξουσιοδοτημένες κινήσεις και ενημερώστε, **άμεσα**, την τράπεζά σας, σε περίπτωση ύποπτης δραστηριότητας.
- **Χρησιμοποιήστε λογισμικό προστασίας από κακόβουλο λογισμικό** και διατηρήστε το **ενημερωμένο**.
- **Περιορίστε τη δημοσίευση προσωπικών πληροφοριών** σε δημόσιες πλατφόρμες και κοινωνικά δίκτυα.
- **Ρυθμίστε ειδοποιήσεις** για ύποπτες συνδέσεις ή δραστηριότητα στους λογαριασμούς σας.
- **Ενημερώστε, άμεσα, τον πάροχο υπηρεσιών σας** εάν παρατηρήσετε ύποπτη δραστηριότητα σε προσωπικούς ή επαγγελματικούς σας λογαριασμούς.
- Σε περίπτωση που αρχίσετε να λαμβάνετε **ανεπιθύμητες, εμπορικές κλήσεις**, εξετάστε την πιθανότητα εγγραφής σας, μέσω των σχετικών, νόμιμων διαδικασιών στο μητρώο της παρ. 2, άρθρου 11, Ν. 3471/2006.
- Σε περίπτωση που λαμβάνετε **ενοχλητικά, διαφημιστικά email, μηνύματα ή μηνύματα τα οποία δε σχετίζονται με την εκπαιδευτική διαδικασία** στις ηλεκτρονικές διευθύνσεις που σας έχουν δοθεί από το Ε.Α.Π., παρακαλούμε να τα γνωστοποιείτε στο **Γραφείο Δικτυακών και Πληροφοριακών Υπηρεσιών**, προωθώντας τα εν λόγω μηνύματα στην email διεύθυνση **abuse@eap.gr** , έτσι ώστε να λαμβάνονται όλα τα απαραίτητα μέτρα.

Επιπρόσθετα, μπορείτε να ενημερωθείτε για περισσότερες, ενδεικτικές, **καλές πρακτικές προστασίας προσωπικών δεδομένων**, στον κάτωθι οδηγό.

[..επισυνάπτεται ο οδηγός πιο κάτω..]

Η **ανάκτηση, η ταξινόμηση και η ανάλυση** των σχετικών αρχείων αποτελούν διαδικασίες που απαιτούν **εξειδικευμένες γνώσεις και τεχνικά προηγμένες μεθόδους**. Λόγω της **τεχνικής φύσης και την πολυπλοκότητας** αυτών των διαδικασιών και της ανάγκης συμμόρφωσης με το **νομικό πλαίσιο περί προστασίας προσωπικών δεδομένων**, η πλήρης διερεύνηση μπορεί να είναι **ιδιαίτερα χρονοβόρα**.

Θα θέλαμε να **τονίσουμε** ότι το Ε.Α.Π. **συνεργάζεται, πλήρως, με τις αρμόδιες, εποπτικές αρχές**, παρέχοντας **κάθε απαιτούμενη πληροφόρηση και διευκόλυνση**, στο πλαίσιο της διερεύνησης του περιστατικού, σε **πλήρη συμμόρφωση με το ισχύον, νομικό και κανονιστικό πλαίσιο**.

Δεδομένου ότι το **ψηφιακό περιβάλλον είναι δυναμικό και συνεχώς εξελισσόμενο**, με νέες προκλήσεις και τεχνολογικές μεταβολές που επηρεάζουν, **άμεσα, τις απαιτήσεις κυβερνοασφάλειας**, το Ε.Α.Π. **δεσμεύεται να διατηρεί ένα διαρκώς, επικαιροποιημένο και προσαρμοσμένο στις συνθήκες πλαίσιο προστασίας**, με στόχο τη **μέγιστη, δυνατή διασφάλιση της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των δεδομένων των χρηστών μας**.

Με εκτίμηση,

**Σεραφείμ Καραϊσκάκης**
**Υπεύθυνος Προστασίας Δεδομένων (DPO)**

## Ο οδηγός του ΕΑΠ

[redacted]