

**Προσοχή!!! σε παραπλανητικά μηνύματα που ζητούν επιβεβαίωση του κωδικού σας ή παραπέμπουν σε επικίνδυνες και κακόβουλες ιστοσελίδες!**



Αξιότιμες κυρίες, αξιότιμοι κύριοι, φίλοι εκπαιδευτικοί

Με αφορμή μηνύματα που έχουν αποσταλεί σε χρήστες του Πανελληνίου Σχολικού Δικτύου τα οποία ζητούν επιβεβαίωση του κωδικού τους, **σας γνωρίζουμε ότι τα μηνύματα αυτά δεν προέρχονται από το Πανελλήνιο Σχολικό Δίκτυο**. Πρόκειται για κακόβουλα μηνύματα ηλεκτρονικού ψαρέματος, που σκοπό έχουν την υποκλοπή του κωδικού πρόσβασής σας.

Με αφορμή αυτό θα θέλαμε να υπενθυμίσουμε τα πιο κάτω σημεία τα οποία έχουμε επισημάνει πολλές φορές με σκοπό να αποτελέσουν πάγια αρχή για όλους τους χρήστες μας.

Η διακίνηση κακόβουλων μηνυμάτων με ηλεκτρονική αλληλογραφία είναι ένα συχνό φαινόμενο. Αυτό συμβαίνει και στα μέλη του ΠΣΔ, τα οποία κάποιες φορές λαμβάνουν μηνύματα που τους ζητούν να αποκαλύψουν τα μυστικά συνθηματικά πρόσβασης, προφασισζόμενα ότι προέρχονται από την τεχνική υποστήριξη του ΠΣΔ.

**Τονίζουμε κατηγορηματικά** ότι το Πανελλήνιο Σχολικό Δίκτυο **δεν θα ζητήσει ποτέ τους κωδικούς σας** μέσω e-mail.

Σας παρακαλούμε να ακολουθείτε τις ακόλουθες οδηγίες μας (αναγράφονται άλλωστε και στη σελίδα εισόδου του webmail <https://webmail.sch.gr/>) :

- **Μην συμπληρώνετε το όνομα χρήστη και τον κωδικό πρόσβασης σε ιστοσελίδες** που σας παροτρύνει ή σας ζητά κάποιο μήνυμα e-mail.
- **Μην απαντάτε σε e-mail** που σας ζητούν το όνομα χρήστη και τον κωδικό πρόσβασης σας.
- Μην συμπληρώνετε το όνομα χρήστη και κωδικό πρόσβασης που έχετε στο ΠΣΔ σε άλλες ιστοσελίδες εκτός των σελίδων εισόδου του ΠΣΔ [https://\[sso ή webmail ή register ή www ή lams\].sch.gr](https://[sso ή webmail ή register ή www ή lams].sch.gr).
- Πριν συμπληρώσετε τον κωδικό σας, ελέγξτε τη γραμμή διεύθυνσης του φυλλομετρητή σας, για να βεβαιωθείτε ότι η διεύθυνση της ιστοσελίδας είναι της μορφής: [https://\[sso ή webmail ή register ή www ή lams\].sch.gr](https://[sso ή webmail ή register ή www ή lams].sch.gr).

Αν έχετε ανταποκριθεί σε τέτοια μηνύματα και έχετε απαντήσει ή συμπληρώσει τα στοιχεία πρόσβασής σας, ή υπάρχει υπόνοια υποκλοπής του κωδικού πρόσβασής σας, θα πρέπει να προχωρήσετε άμεσα στην αλλαγή του κωδικού πρόσβασης από έναν καθαρό υπολογιστή από τη διεύθυνση [www.sch.gr/password](http://www.sch.gr/password).

Το πιο επικίνδυνο είναι ότι αρκετά από αυτά τα μηνύματα έχουν στο σώμα τους παλιά γνωστά μηνύματα που έχουν διακινηθεί στην αλληλογραφία χρηστών, σχολείων ή άλλων μονάδων του ΠΣΔ.

Επισημαίνουμε την προσοχή σας στο σημείο αυτό και συνιστούμε να εξετάζετε προσεκτικά την πραγματική e-mail διεύθυνση του αποστολέα και όχι μόνο το εμφανιζόμενο όνομα του. Θα πρέπει να ελέγχετε τι υπάρχει στο τελευταίο τμήμα που υπάρχει και οριοθετείται από τους χαρακτήρες <.....> στο e-mail του αποστολέα.

Συνιστούμε να διαβάσετε τις συμβουλές ασφαλείας του Πανελληνίου Σχολικού Δικτύου για:

- «Ασφάλεια και προστασία» - <https://www.sch.gr/security> και πιο ειδικά την ενότητα «προστασία από παραπλανητικά μηνύματα».
- Τη σχετική ενημέρωση που υπάρχει στη σελίδα εισόδου του webmail <https://webmail.sch.gr/>.
- Τη σελίδα <https://cert.sch.gr/el> για πληρέστερη ενημέρωση.

Παρακαλούμε να ενημερώσετε και τους μαθητές σας για την ανάγκη να εφαρμόζουν τις παραπάνω οδηγίες.

Σας ευχαριστούμε που χρησιμοποιείτε τις υπηρεσίες του Πανελληνίου Σχολικού Δικτύου.

Με εκτίμηση

ΠΑΝΕΛΛΗΝΙΟ ΣΧΟΛΙΚΟ ΔΙΚΤΥΟ

Υπηρεσία Υποστήριξης Χρηστών, <http://www.sch.gr/helpdesk>

e-mail: [info@sch.gr](mailto:info@sch.gr)