**From:** listserver@sch.gr

**To:** all@sch.gr

**Sent:** Tuesday, November 15, 2011 3:18 PM

**Subject:** Οδηγίες για Ασφαλή Πρόσβαση στο Διαδίκτυο

**Ενημερωτικό Σημείωμα: Οδηγίες για Ασφαλή Πρόσβαση στο Διαδίκτυο
Προστασία των δεδομένων σας από το φαινόμενο phishing**

**Πώς μπορώ να χρησιμοποιώ το Διαδίκτυο χωρίς να κινδυνεύω από παραβίαση των προσωπικών μου δεδομένων, απάτες, απειλές ή άλλες εγκληματικές ενέργειες**;

Παρακαλούμε διαβάστε τις παρακάτω οδηγίες για Ασφαλή Πρόσβαση στο Διαδίκτυο, με αφορμή παραπλανητικά μηνύματα αλληλογραφίας που μπορεί να έχετε λάβει από άγνωστους αποστολείς (προσποιούμενοι κάποιες φορές ότι είναι «διαχειριστές από το Πανελλήνιο Σχολικό Δίκτυο») και σας ζητούν να τους γνωρίσετε τους κωδικούς πρόσβασης των λογαριασμών σας:

* **Κανένας οργανισμός** (Πανελλήνιο Σχολικό Δίκτυο, τράπεζα ή οργανισμός) **δεν θα σας στείλει μήνυμα αλληλογραφίας** με το οποίο ζητά από τους χρήστες του να κοινοποιήσουν τους κωδικούς πρόσβασης.
* Όταν λαμβάνετε email από τράπεζες, να είστε πολύ καχύποπτοι. Καμία τράπεζα δεν θα έστελνε ποτέ ένα μήνυμα προσκαλώντας τους πελάτες της να συμπληρώσουν τα στοιχεία τους σε μια ιστοσελίδα.
* **Σε καμία περίπτωση δεν θα πρέπει να κάνετε τις ενέργειες που σας προτείνει το συγκεκριμένο παραπλανητικό μήνυμα αλληλογραφίας.** Το μήνυμα αυτό είναι πλαστό και επικίνδυνο και δεν προέρχεται από το Πανελλήνιο Σχολικό Δίκτυο).
* 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 σας στο ΠΣΔ **παρά μόνο σε δικτυακούς τόπους** του [**sch.gr**](http://sch.gr/),όπως η δικτυακή πύλη [ΠΣΔ](http://www.sch.gr/) , [webmail ΠΣΔ](http://webmail.sch.gr/), [πιστοποίηση Χρηστών](https://cas.sch.gr/login), [μαθητική πύλη](http://students.sch.gr/), [e-learning ΠΣΔ](http://e-learning.sch.gr/), [πλατφόρμα Ασύγχρονης τηλεκπαίδευση](http://istos.sch.gr/)ς, καθώς και την [Δικτυακή Εκπαιδευτική Πύλη του ΥΠΔΒΜΘ](http://www.e-yliko.gr/).
* Αν σας ζητείται password από άλλο δικτυακό τόπο, εκτός από τους προαναφερόμενους δεν θα πρέπει να τον παρέχετε.

*Αν και το Πανελλήνιο Σχολικό Δίκτυο εφαρμόζει πολιτική 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:
	+ Εξετάσετε προσεκτικά το περιεχόμενο τους ακόμη και αν φαίνεται να προέρχονται από γνωστούς αποστολείς.
	+ Ελέγχετε αν στο κείμενο υπάρχουν ορθογραφικά ή συντακτικά σφάλματα. Κάτι τέτοιο θα πρέπει να σας βάζει σε υποψίες για την εγκυρότητα του μηνύματος.
	+ **Προσοχή στους 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.
* *Μην* ακολουθείτε υπερσυνδέσμους (hyperlinks) από e-mail ή ιστοσελίδες, αλλά πάντα να πληκτρολογείτε τις διευθύνσεις που σας ζητούν να επισκεφθείτε. Επίσης προσθέστε τις ιστοσελίδες που χρησιμοποιείτε συχνά στα bookmarks / Favorites του προγράμματος πλοήγησης 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.
	+ Αν δεν είναι ορατή η γραμμής κατάστασης, στον internet explorer για την εμφάνιση της δείτε το άρθρο <http://support.microsoft.com/kb/330216>
* Διατηρείτε το πρόγραμμα πλοήγησης ιστοσελίδων (Internet Explorer, Mozilla, 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).
* Εγκαταστήστε ένα πρόγραμμα που σας ενημερώνει για ιστοσελίδες που περιέχουν περιεχόμενο που έχει ήδη αναφερθεί ως απειλή phishing, ή χρησιμοποιείτε πρόγραμμα πλοήγησης ιστοσελίδων που έχουν φίλτρα anti-phishing.

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 Π.Σ.Δ. 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 για την [Αλλαγή κωδικού πρόσβασης](http://www.sch.gr/password), ο οποίος ανακατευθύνεται [εδώ](https://register.sch.gr/password/change_password/).
* Κάθε άλλο URL αλλαγής password θα πρέπει να θεωρείται ύποπτο και να μην γίνεται αποδεκτό.

**Για περισσότερη ενημέρωση από το Πανελλήνιο Σχολικό Δίκτυο σε θέματα ασφάλειας σας προτείνουμε να επισκεφθείτε τους παρακάτω συνδέσμους:**

* [Βίντεο με οδηγίες χρήσης – Πρώτο μέρος](http://vod.sch.gr/video/view/850.html)
* [Βίντεο με οδηγίες χρήσης – Δεύτερο μέρος](http://vod.sch.gr/video/view/849.html)
* [Χρήσιμες οδηγίες από τον Ενημερωτικό Κόμβο Π.Σ.Δ
για την Ασφάλεια στο Διαδίκτυο](http://blogs.sch.gr/internet-safety/archives/tag/phishing)
* [Υπηρεσία Αντιμετώπισης Περιστατικών Ασφαλείας](http://cert.sch.gr/index.php?name=Reviews)
* [Προώθηση της ασφαλούς χρήσης του Διαδικτύου](http://www.sch.gr/safe)