



Χρήσιμες Συμβουλές Ασφάλειας

Αυθεντικότητα Ιστοσελίδων της ΑΑΔΕ

Για να είστε βέβαιοι ότι έχετε συνδεθεί στον επίσημο διαδικτυακό τόπο της ΑΑΔΕ, σας συνιστούμε να ακολουθείτε τους παρακάτω κανόνες:

- Να συνδέεστε στον επίσημο διαδικτυακό τόπο της ΑΑΔΕ πληκτρολογώντας απευθείας την ηλεκτρονική διεύθυνση www.aade.gr στον φυλλομετρητή σας (browser), και όχι μέσω συνδέσμων (links) που πιθανόν σας έχουν αποσταλεί ηλεκτρονικά ή έχουν δημοσιευτεί σε ιστοσελίδες τρίτων.
- Όταν κάνετε login στην ιστοσελίδα μιας ηλεκτρονικής υπηρεσίας της ΑΑΔΕ όπου σας ζητείται να συμπληρώσετε τον λογαριασμό χρήστη (username) καθώς και τον προσωπικό σας κωδικό πρόσβασης (password), να ελέγχετε αν η διεύθυνση αρχίζει με **https** (αντί του http) και υπάρχει εικονίδιο με λουκέτο. Με διπλό κλικ στο λουκέτο, θα εμφανιστούν πληροφορίες που θα σας βοηθήσουν να επιβεβαιώσετε ότι η ιστοσελίδα είναι γνήσια.
- Αφού ολοκληρώσετε τις ενέργειές σας, να αποσυνδέεστε από τη σελίδα (επιλέγοντας «Αποσύνδεση») πριν την εγκαταλείψετε.

Λήψη ηλεκτρονικών μηνυμάτων μέσω email

Σχετικά με τα ηλεκτρονικά μηνύματα που αποστέλλονται μέσω email, σας ενημερώνουμε ότι η Ανεξάρτητη Αρχή Δημοσίων Εσόδων:

- 1. Αναγράφει το όνομά σας και το όνομα χρήστη (Username) στο πάνω μέρος κάθε μηνύματος ηλεκτρονικού ταχυδρομείου που σας αποστέλλει**, εφόσον δεν αποτελεί απάντηση σε προηγούμενο δικό σας. Διαγράψτε αμέσως οποιοδήποτε μήνυμα αναφέρει ότι προέρχεται από την Ανεξάρτητη Αρχή Δημοσίων Εσόδων χωρίς να περιέχει τα στοιχεία αυτά, καθώς είναι πλαστό και πιθανώς να περιέχει κακόβουλο περιεχόμενο.
- 2. Δεν θα σας ζητήσει με κανέναν τρόπο και για κανένα λόγο να αποκαλύψετε προσωπικά σας στοιχεία** όπως όνομα, ΑΦΜ, ημερομηνία γέννησης, τραπεζικούς λογαριασμούς ή κωδικούς πρόσβασης (Username ή Password).
- 3. Δεν θα σας αποστείλει ποτέ μήνυμα που περιέχει προσωπικά φορολογικά στοιχεία** (π.χ. ποσά οφειλών ή επιστροφών). Τα δεδομένα αυτά αναρτώνται μόνο στη θυρίδα **e-Κοινοποιήσεις** της ψηφιακής πύλης myAADE, στην οποία μπορείτε να συνδεθείτε με τους προσωπικούς σας κωδικούς πρόσβασης ακολουθώντας τη διαδρομή myAADE > Μητρώο & Επικοινωνία > e-Κοινοποιήσεις.

Για την προστασία σας:

1. Να ελέγχετε με προσοχή τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα των μηνυμάτων. Απατηλά μηνύματα συχνά αποστέλλονται από άγνωστες ή παραφρασμένες



διευθύνσεις ηλεκτρονικού ταχυδρομείου που προσομοιάζουν με πραγματικές διευθύνσεις υπηρεσιών (ιδίως με αλλαγή ή προσθήκη χαρακτήρων). Επίσης συχνά το όνομα αποστολέα κρύβει άλλη διεύθυνση, άσχετη με την υπηρεσία από την οποία φαίνεται να αποστέλλεται το μήνυμα.

2. Εφόσον δεν είστε σίγουροι για τον αποστολέα του μηνύματος μην κάνετε ποτέ κλικ σε σύνδεσμο (link) που βρίσκεται σε μήνυμα που λαμβάνετε και μην ανοίγετε κανένα συνημμένο αρχείο.

3. Μην κάνετε ποτέ κλικ σε συνδέσμους (links) που σας καλούν να καταχωρίσετε τους κωδικούς σας ή άλλα προσωπικά σας στοιχεία.

4. Συνδεθείτε στην ψηφιακή πύλη myAADE μόνο από τη διεύθυνση myaade.gov.gr ή από την επίσημη ιστοσελίδα της Ανεξάρτητης Αρχής Δημοσίων Εσόδων www.aade.gr.

Διαχείριση Κωδικών Πρόσβασης

Ο κωδικός πρόσβασης (password) είναι πολύ σημαντικός για την ασφάλεια των συναλλαγών σας με την ΑΑΔΕ. Για αυτό το λόγο σας συνιστούμε να επιλέγετε ισχυρά passwords και να φροντίζετε να τα αλλάζετε ανά τακτά χρονικά διαστήματα. Για την ασφαλή χρήση του password, καλό είναι να έχετε υπόψη τα παρακάτω:

- Το password σας είναι προσωπικό και δε θα πρέπει να το μοιράζεστε με τρίτους, συμπεριλαμβανομένων και των υπαλλήλων της ΑΑΔΕ. Σε περίπτωση που υποψιάζεστε ότι το password σας έχει διαρρεύσει με οποιονδήποτε τρόπο, ενημερώστε αμέσως την ΑΑΔΕ ή, αν έχετε τη δυνατότητα, προβείτε άμεσα στην αλλαγή του.
- Σε καμία περίπτωση μην αποθηκεύετε ή κρατάτε σε σημειώσεις τα password σας.
- Επιλέξτε διαφορετικά passwords για τους σημαντικούς λογαριασμούς σας.
- Κατά την επιλογή password:
 - Επιλέξτε συνδυασμό γραμμάτων, αριθμών και συμβόλων στο password σας και αποφύγετε τη χρήση απλών λέξεων. Επιπλέον, αποφύγετε τη χρήση σειράς ίδιων χαρακτήρων (π.χ. g177777) ή χαρακτήρων με κάποια λογική συνέχεια (π.χ. 123456, abcde).
 - Επιλέξτε μια φράση που μόνο εσείς γνωρίζετε και αποφύγετε τη δημιουργία passwords που περιέχουν στοιχεία που σας ταυτοποιούν όπως το όνομά σας, η ημερομηνία γέννησης, ο αριθμός ταυτότητας ή το ΑΦΜ σας.
 - Χρησιμοποιήστε passwords με τουλάχιστον 8 χαρακτήρες.

Προστασία του υπολογιστή κατά τις συναλλαγές σας

Για την μέγιστη προστασία των συναλλαγών σας, πριν συνδεθείτε με τις ηλεκτρονικές υπηρεσίες της ΑΑΔΕ θα πρέπει να φροντίζετε για τα εξής:



- Να ενημερώνετε το λειτουργικό σύστημα των ηλεκτρονικών συσκευών σας και όλα τα προγράμματα που χρησιμοποιείτε για την πρόσβαση σας αυτή με τις τελευταίες ενημερώσεις ασφάλειας που δημοσιεύουν οι κατασκευάστριες εταιρίες τους.
- Να χρησιμοποιείτε ευρέως γνωστό φυλλομετρητή διαδικτύου (browser), ο οποίος είτε είναι προεγκατεστημένος στις προσωπικές ηλεκτρονικές συσκευές σας είτε προέρχεται από αξιόπιστο κατασκευαστή.
- Να προστατεύετε τις ηλεκτρονικές συσκευές σας με προγράμματα firewall, antivirus και antispyware και να φροντίζετε για τη συχνή ενημέρωσή τους με τις τελευταίες εκδόσεις.
- Να λαμβάνετε περιοδικά και τακτικά αντίγραφα ασφάλειας (backups). Με τον τρόπο αυτό, σε περίπτωση που το σύστημα σας προσβληθεί από ιό ή αντιμετωπίσει οποιεσδήποτε αποτυχίες λογισμικού ή υλικού, θα μπορέσετε να διασώσετε τα αρχεία σας και να το επαναφέρετε στην προηγούμενη του κατάσταση.

Χρήση κοινόχρηστων ηλεκτρονικών συσκευών

Κατά τη χρήση των ηλεκτρονικών υπηρεσιών της ΑΑΔΕ από ηλεκτρονικές συσκευές που δεν ανήκουν σε εσάς ή είναι κοινόχρηστοι, σας συνιστούμε:

- Να επιλέγετε τη χρήση ανώνυμης περιήγησης, αν αυτό είναι δυνατόν.
- Να μην επιλέγετε την αποθήκευση των προσωπικών σας κωδικών όταν σας ζητείται από τον browser.
- Να βεβαιώνετε ότι δεν σας παρακολουθούν όταν συμπληρώνετε το username και το password σας.
- Μετά το τέλος της χρήσης, να διαγράφετε όλα τα προσωρινά αποθηκευμένα αρχεία Internet όπως cookies, κωδικοί πρόσβασης, ιστορικό περιήγησης κλπ.

Σύνδεση μέσω δικτύου Wifi

Στην περίπτωση που το δίκτυο είναι οικιακό, φροντίστε για την ενεργοποίηση των παραμέτρων ασφάλειας του router σας. Παρόλα αυτά, ακόμη και στην περίπτωση που είναι ενεργοποιημένες οι παράμετροι ασφάλειας σε ένα δίκτυο, προτιμήστε την ενσύρματη πρόσβαση από την ασύρματη.

Στην περίπτωση που το ασύρματο δίκτυο δεν ελέγχεται από εσάς ή είναι δημόσιο, τότε μη το χρησιμοποιείτε για τη μετάδοση προσωπικών σας στοιχείων και εμπιστευτικών πληροφοριών και για την εισαγωγή των προσωπικών σας μυστικών κωδικών πρόσβασης (passwords), καθώς η ασφάλεια αυτών των δικτύων είναι χαμηλή και είναι πιθανό να υποκλαπούν τα δεδομένα που διακινούνται σε αυτά.



Γενικές Οδηγίες Ασφάλειας

- Μην ανοίγετε ηλεκτρονικά μηνύματα (e-mail, SMS) από άγνωστους σε εσάς αποστολείς.
- Σύνδεσμοι σε ψεύτικους ιστότοπους (web sites): Ελέγξτε πάντα που σας οδηγεί ο σύνδεσμος πριν τον πατήσετε. Τοποθετήστε τον κέρσορα πάνω στο URL και ελέγξτε εάν η διεύθυνση είναι η ίδια μ' αυτή που θα εμφανιστεί στο κάτω μέρος του φυλλομετρητή (browser).
- Μην εμπιστεύεστε ηλεκτρονικά μηνύματα που σας ζητούν προσωπικά σας στοιχεία ή σας παραπέμπουν σε ιστότοπους για να συμπληρώσετε το username, το password ή οποιαδήποτε άλλη προσωπική σας πληροφορία (όνομα, ΑΦΜ, ημερομηνία γέννησης κλπ). Η ΑΑΔΕ δεν πρόκειται ποτέ να σας στείλει τέτοιου είδους ηλεκτρονικά μηνύματα.
- Προσοχή στη διατύπωση. Συχνά τα ψεύτικα ηλεκτρονικά μηνύματα χρησιμοποιούν λανθασμένα Ελληνικά, τόσο ως προς την ορθογραφία όσο και ως προς το συντακτικό. Δίνουν την εντύπωση ότι έχουν γραφτεί από κάποιον που δεν γνωρίζει καλά Ελληνικά.
- Αποφεύγετε να κατεβάζετε αρχεία (παιχνίδια, μουσική, videos, δωρεάν προγράμματα κ.α.) από ιστότοπους που δεν εμπιστεύεστε.
- Εάν εντοπίσετε "περίεργες" συμπεριφορές του υπολογιστή σας, που πολύ πιθανόν να προκαλούνται από την εγκατάσταση κακόβουλων προγραμμάτων, χρησιμοποιήστε το πρόγραμμα προστασίας του υπολογιστή σας ή μιλήστε με κάποιον ειδικό.
- Περιορίστε τις πληροφορίες που κοινοποιείτε σε ιστοσελίδες κοινωνικής δικτύωσης (facebook, instagram, twitter κ.λπ.).
- Πρέπει να είστε πολύ προσεκτικοί με τηλεφωνικές κλήσεις από αγνώστους που προσποιούνται ότι είναι λογιστές ή εκπρόσωποι της ΑΑΔΕ και σας ζητούν προσωπικά στοιχεία (όνομα, ΑΦΜ, username, password) με πρόσχημα την επιστροφή φόρου ή την έγκριση κρατικής επιδότησης (Power Pass, Fuel Pass, Τουρισμός για όλους κ.λ.π.).