



**ΕΘΝΙΚΗ ΥΠΗΡΕΣΙΑ  
ΠΛΗΡΟΦΟΡΙΩΝ**

# **ΟΔΗΓΙΕΣ ΓΙΑ ΑΣΦΑΛΗ ΧΡΗΣΗ ΥΠΟΛΟΓΙΣΤΩΝ**

## **WINDOWS 11**



# ΠΡΟΛΟΓΟΣ | Μήνυμα του Διοικητή

Είναι προφανές ότι η αλματώδης ανάπτυξη της τεχνολογίας τα τελευταία χρόνια δημιουργεί νέες, εντυπωσιακές δυνατότητες που, με την κατάλληλη χρήση, ανοίγουν νέους ορίζοντες για άτομα, κράτη, οργανισμούς, επιχειρήσεις και κοινωνίες, αλλά και για την ανάπτυξη, την ασφάλεια, την υγεία, την εκπαίδευση και τον πολιτισμό. Όμως, οι δυνατότητες αυτές είναι πια στη διάθεση και κακόβουλων δρώντων που, με την κατάλληλη χρήση διάφορων μέσων, εύκολα και, ακριβώς λόγω των νέων τεχνολογικών δυνατοτήτων, με ελάχιστο κόστος και χωρίς ιδιαίτερους κινδύνους γι' αυτούς, μπορούν να δημιουργήσουν τεράστια προβλήματα σε ενεργειακά ή επικοινωνιακά δίκτυα και γενικότερα σε κρίσιμες υποδομές, απειλώντας άμεσα ακόμα και την εθνική μας ασφάλεια. Η θωράκιση λοιπόν της χώρας μας έναντι των δράσεων που μπορούν να θέσουν σε κίνδυνο τα εθνικά μας συμφέροντα αποτελεί ύψιστη προτεραιότητα.

Στις σχετικές, απαραίτητες για κάθε σύγχρονο κράτος, προσπάθειες ο νομοθέτης έχει αναθέσει, για τη χώρα μας, κομβικό ρόλο στην ΕΥΠ, η οποία έχει οριστεί ως Εθνική Αρχή Ασφάλειας Πληροφοριών (INFOSEC). Για την εκπλήρωση της αποστολής της αυτής, η ΕΥΠ ασκεί συντονιστικό ρόλο στην προστασία των κρατικών φορέων έναντι κάθε είδους περιστατικών ασφαλείας.

Στα καθήκοντά της περιλαμβάνεται και η σύνταξη πολιτικών ασφαλείας και οδηγιών διαχείρισης των διαβαθμισμένων πληροφοριών και δικτύων. Γιατί τα μηχανήματα τα χειρίζονται άνθρωποι. Ο δε τρόπος με τον οποίο οι άνθρωποι αυτοί τα χειρίζονται αποτελεί συνήθως τον «αδύναμο κρίκο», το πιο ευάλωτο σημείο στο πλέγμα και στη διάδραση μεταξύ συσκευών και ανθρώπων, που θα τύχει εκμετάλλευσης από κακόβουλους δρώντες για να εισβάλλουν σε ένα δίκτυο.

Γι' αυτό είναι απαραίτητο κάθε χρήστης Η/Υ, που χειρίζεται διαβαθμισμένες πληροφορίες, να είσαι σε διαρκή επαγρύπνηση, να ενημερώνεται συνεχώς και να έχει υψηλό βαθμό ευθύνης, έχοντας διαμορφώσει μια κουλτούρα ασφαλείας ικανή να εξασφαλίσει ένα αποτελεσματικό πλαίσιο άμυνας κατά κάθε ενέργειας παραβίασης της ασφαλείας της συσκευής του και της ιδιωτικότητας των δεδομένων του.

Αυτούς ακριβώς τους στόχους εξυπηρετεί η έκδοση του οδηγού αυτού, που φιλοδοξούμε να λειτουργήσει ως ένα απλό, ενημερωμένο και εικονογραφημένο με παραδείγματα εγχειρίδιο, χρήσιμο σε όσους χειρίζονται υπολογιστές και δεδομένα, κρίσιμα για τη λειτουργία του φορέα τους αλλά, τελικά και για την εθνική μας ασφάλεια.

Γιατί η ασφάλεια στη χρήση διαβαθμισμένου υλικού είναι εθνική υπόθεση και επιταγή. Είναι όμως και προσωπική ευθύνη όλων μας.

**Ο Διοικητής**  
Θεμιστοκλής Δεμίρης

# 1 Εισαγωγή

Ο οδηγός, που κρατάτε στα χέρια σας, απευθύνεται σε φορείς του Δημοσίου και πιο συγκεκριμένα σε εργαζομένους, που χρησιμοποιούν υπολογιστές, οι οποίοι χειρίζονται ευαίσθητα ή διαβαθμισμένα δεδομένα και έχει σκοπό να παρέχει χρήσιμες συμβουλές, αλλά και βασικές οδηγίες για:

- ▶ Την προστασία και την ενίσχυση της ασφάλειας του υπολογιστή
- ▶ Την προστασία των προσωπικών δεδομένων (ιδιωτικότητα) του χρήστη
- ▶ Τη διασφάλιση του απορρήτου των διαβαθμισμένων πληροφοριών

Απευθύνεται κυρίως σε προσωπικό που έχει ρόλο «απλού» χρήστη (simple/standard user) στον εκάστοτε υπολογιστή. Περιέχει όμως και αναφορές σε βασικές διαδικασίες και ρυθμίσεις που ενδέχεται να είναι διαθέσιμες μόνο στον/στους Διαχειριστή/ές του συστήματος (Administrator user).

Οι συγκεκριμένες οδηγίες αναφέρονται στην πιο πρόσφατη έκδοση των Windows, τα Windows 11. Επισημαίνεται ότι συνίσταται η χρήση γνήσιας έκδοσης του λειτουργικού συστήματος.

Οι οδηγίες επικεντρώνονται στα εξής θέματα:

## 1. Προστασία και ασφάλεια προσωπικού υπολογιστή

- ▶ Εγκατάσταση και λήψη ενημερωμένων εκδόσεων λειτουργικού συστήματος, ενημερώσεων ασφαλείας και εφαρμογών
- ▶ Χρήση λογισμικού κατά των ιών (anti-virus)
- ▶ Χρήση τείχους προστασίας (firewall)
- ▶ Δημιουργία τακτικών αντιγράφων ασφαλείας (backups)
- ▶ Χρήση λογαριασμού Διαχειριστή μόνο από εξουσιοδοτημένο χρήστη
- ▶ Προσοχή κατά τη σύνδεση εξωτερικών συσκευών, όπως οδηγό USB, για μεταφορά αρχείων

## 2. Προστασία προσωπικών δεδομένων (ιδιωτικότητα) του χρήστη

- ▶ Χρήση ισχυρών κωδικών πρόσβασης
- ▶ Ρύθμιση παραμέτρων προστασίας της ιδιωτικότητας του χρήστη τόσο στον υπολογιστή του, όσο και στους περιηγητές Ιστού (Web browsers) που χρησιμοποιεί
- ▶ Προσοχή κατά την κοινοποίηση προσωπικών δεδομένων σε ιστότοπους
- ▶ Προσοχή κατά την πλοήγηση στο διαδίκτυο για την αποφυγή αποπειρών απάτης και ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου

Συμπεριλαμβάνονται όμως και οδηγίες σε σχέση με την προστασία τυχόν ευαίσθητων ή διαβαθμισμένων πληροφοριών, με έμφαση στην προστασία συσκευών/εξοπλισμού εκτός οργανισμού. Τέλος, ιδιαίτερη προσοχή αποδίδεται στην ασφαλή χρήση του ηλεκτρονικού ταχυδρομείου.

Επισημαίνεται ότι ο οδηγός αφορά κυρίως τη χρήση προσωπικών υπολογιστών στο χώρο εργασίας.

Όσον αφορά τη χρήση φορητών συσκευών (όπως laptop) που ενδεχομένως χρησιμοποιούνται για την εξ αποστάσεως εργασία ή σε επαγγελματικά ταξίδια, **απαιτείται η λήψη επιπλέον μέτρων προστασίας, όπως:**

- ▶ Απενεργοποίηση ασύρματων συνδέσεων, όταν δεν είναι απαραίτητες
- ▶ Προσοχή στα σημεία αναμετάδοσης ασύρματου σήματος (Wi-Fi hotspots), καθώς η ασφάλεια αυτών των δικτύων είναι χαμηλή και είναι πιθανόν να υποκλαπούν προσωπικά δεδομένα.
- ▶ Περιορισμός του τύπου των δραστηριοτήτων που εκτελούνται (να μην χρησιμοποιείται για τη μετάδοση προσωπικών στοιχείων και την εισαγωγή προσωπικών κωδικών πρόσβασης)
- ▶ Προσαρμογή των ρυθμίσεων ασφαλείας της συσκευής σας, ώστε να μην επιτρέπεται σε άλλα άτομα να έχουν πρόσβαση σε αυτήν.
- ▶ Προσοχή στη χρήση κοινόχρηστων υπολογιστών.

**Επιπλέον, συστήνεται:**

- ▶ Να επιλεγεί η χρήση ανώνυμης/ιδιωτικής περιήγησης, αν αυτό είναι δυνατόν
- ▶ Να μην επιλέγεται η αποθήκευση των προσωπικών κωδικών, όταν ζητείται από τον browser
- ▶ Μετά το τέλος της χρήσης, να διαγράφονται όλα τα προσωρινά αποθηκευμένα αρχεία Internet, όπως cookies, ιστορικό περιήγησης, κωδικούς πρόσβασης κ.λπ.

Για τη λήψη του οδηγού, μπορείτε να αποστείλετε το αίτημά σας  
στο: [infosec@nis.gr](mailto:infosec@nis.gr)