

## Προσωπικά Δεδομένα

### Περιγραφή

Τα προσωπικά σου δεδομένα είναι όλες οι πληροφορίες που αναφέρονται σε σένα. Είναι το όνομά σου, η διεύθυνσή σου, ο αριθμός του κινητού σου, το σχολείο στο οποίο πηγαίνεις, τα μέρη όπου συχνάζεις. Μερικές φορές τα προσωπικά σου δεδομένα αφορούν ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής σου ζωής, όπως στο θρήσκευμά σου, στις πολιτικές σου πεποιθήσεις ή στην κατάσταση της υγείας σου και άλλα. Πολλές φορές, ιδιαίτερα στα κοινωνικά δίκτυα, δημοσιεύεις δεδομένα σου που μπορούν να χρησιμοποιηθούν από άτομα που δε γνωρίζεις με κακόβουλο σκοπό. Προσεκτικός πρέπει να είσαι όχι μόνο όταν δημοσιεύεις πληροφορίες για σένα τον ίδιο αλλά και πληροφορίες που αφορούν άλλα άτομα. Για να το κάνεις αυτό θα πρέπει να έχεις πάντα τη συγκατάθεσή τους. Διατηρώντας τον έλεγχο των προσωπικών μας δεδομένων ουσιαστικά διατηρούμε τον έλεγχο της ιδιωτικής μας ζωής.

### Καλές πρακτικές για να παραμείνουμε ασφαλείς στο Διαδίκτυο

Η καλύτερη μέθοδος είναι η **πρόληψη**

**("Κάλλιον τό προλαμβάνειν, παρά τό θεραπεύειν", Ιπποκράτης 460 – 337 πΧ.)**

- Προστατεύουμε τα προσωπικά μας δεδομένα στο Διαδίκτυο, ιδιαίτερα τα ευαίσθητα δεδομένα, τις φωτογραφίες μας και τα βίντεο. Δε δημοσιοποιούμε ανεξέλεγκτα, περιοριζόμαστε στα απολύτως απαραίτητα.
- Δε δημοσιεύουμε προσωπικά δεδομένα στο Διαδίκτυο, όπως: όνομα, τηλέφωνο, διεύθυνση, σε ποιο σχολείο πηγαίνουμε, σε ποια μέρη συχνάζουμε ή στοιχεία για την οικογένειά μας, με τα οποία κάποιος θα μπορούσε να μας εντοπίσει στον πραγματικό κόσμο.
- Όταν μπαίνουμε σε ιστοχώρους που ζητούν προσωπικά μας δεδομένα, συμβουλευόμαστε κάποιον ενήλικα και διαβάζουμε πάντα τους «όρους χρήσης» και την «πολιτική απορρήτου» του κάθε ιστοχώρου.
- Δε δίνουμε ποτέ τους κωδικούς μας σε κανέναν. Επιλέγουμε «ισχυρούς» κωδικούς, αποτελούμενους από 8 τουλάχιστον χαρακτήρες και τους αλλάζουμε συχνά. Όπου συνδεόμαστε με κωδικό, στο τέλος κάνουμε πάντα αποσύνδεση.
- Διαχειριζόμαστε τα cookies που αποθηκεύονται στον υπολογιστή μας όταν χρησιμοποιούμε φυλλομετρητές (browsers).
- Χρησιμοποιούμε ψευδώνυμα σε ιστολόγια (blogs) και όταν κάνουμε chat για να προστατέψουμε την ταυτότητά μας.
- Προσέχουμε ποιες εφαρμογές «κατεβάζουμε» και από ποιον ιστότοπο. Απεγκαθιστούμε εφαρμογές και διαγράφουμε παλιά προφίλ που δε χρησιμοποιούμε πια για να μην έχουν πρόσβαση στα προσωπικά μας δεδομένα.
- Κρατάμε τον υπολογιστή μας ασφαλή. Χρησιμοποιούμε προγράμματα τείχους ασφαλείας (firewall) και προστασίας από ιούς (antivirus).
- Θυμόμαστε ότι δεν είμαστε ποτέ αόρατοι στο Διαδίκτυο. Όλοι μας αφήνουμε «ψηφιακά αποτυπώματα» κατά την πλοήγησή μας. Γι' αυτό, πρέπει να ελέγχουμε τακτικά τη διαδικτυακή μας φήμη. (Google το όνομά μας)
- Δημιουργούμε ασφαλή προφίλ στις ιστοσελίδες κοινωνικής δικτύωσης. Ρυθμίζουμε το προφίλ μας, ώστε να μην είναι ορατό σε αγνώστους (ιδιωτικό) και δε δεχόμαστε για διαδικτυακούς φίλους άτομα που δε γνωρίζουμε στον πραγματικό κόσμο.

- Προσέχουμε στα κοινωνικά δίκτυα που κάνουμε Like ή καρδούλα, τις κοινοποιήσεις και τα σχόλιά μας.
- Σεβόμαστε και δε δημοσιεύουμε προσωπικά δεδομένα άλλων ατόμων χωρίς τη συγκατάθεσή τους.
- Θυμόμαστε ότι οτιδήποτε ανεβάζουμε στο Διαδίκτυο μπορεί να μείνει εκεί για πάντα. Αισθανόμαστε άνετα αν τις πληροφορίες ή φωτογραφίες που δημοσιεύουμε στο Διαδίκτυο τις δει ο καθηγητής μας, ο μελλοντικός μας φίλος, ο μελλοντικός μας εργοδότης; Εάν η απάντηση είναι «όχι», τότε δε θα πρέπει να τις δημοσιεύουμε.
- Ενημερωνόμαστε τακτικά από έγκυρους φορείς, όπως: το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου με τις 3 δράσεις του, (<https://saferinternet4kids.gr>, <http://help-line.gr>, <http://www.safeline.gr/>), τον κόμβο του Πανελληνίου Σχολικού Δικτύου για την Ασφάλεια στο Διαδίκτυο, (<https://internet-safety.sch.gr/>), το eSafety - Ψηφιακή Ασφάλεια, (<https://www.scoop.it/t/isafe/>), τον ιστότοπο της Δίωξης Ηλεκτρονικού Εγκλήματος (<https://cyberalert.gr/>).

## Μη ασφαλείς κωδικοί πρόσβασης στο Διαδίκτυο

Το SplashData αποκάλυψε τους κορυφαίους 25 χειρότερους κωδικούς πρόσβασης του 2018 και οι "123456" και "Password" συνέχισαν να κρατούν τις # 1 & # 2 θέσεις για πέμπτη συνεχόμενη χρονιά.

Το SplashData συγκεντρώνει αυτούς τους καταλόγους από το 2012 και έχει χρησιμοποιήσει περισσότερους από 5 εκατομμύρια κωδικούς πρόσβασης που έχουν διαρρεύσει μέσω διαφόρων παραβιάσεων δεδομένων.

Η Splash Data ελπίζει ότι με τη δημοσίευση αυτών των λιστών, ενθαρρύνει όλους τους χρήστες ανά τον κόσμο να συνειδητοποιήσουν τη σημασία της επιλογής ενός ισχυρού κωδικού πρόσβασης.

Οι κορυφαίοι **25 χειρότεροι κωδικοί πρόσβασης** του 2018 παρατίθενται παρακάτω:

- |              |               |
|--------------|---------------|
| 1. 123456    | 14. 666666    |
| 2. password  | 15. abc123    |
| 3. 123456789 | 16. football  |
| 4. 12345678  | 17. 123123    |
| 5. 12345     | 18. monkey    |
| 6. 111111    | 19. 654321    |
| 7. 1234567   | 20. !@#\$%^&* |
| 8. sunshine  | 21. charlie   |
| 9. qwerty    | 22. aa123456  |
| 10. iloveyou | 23. donald    |
| 11. princess | 24. password1 |
| 12. admin    | 25. qwerty123 |
| 13. welcome  |               |

## Πηγές:

<https://saferinternet4kids.gr/nea/25passwords/>

<https://saferinternet4kids.gr/hot-topics-ef/proswpika-dedomena-ef/>

<https://saferinternet4kids.gr/wp-content/uploads/2018/05/cookies-per-page.pdf>

<https://saferinternet4kids.gr/gdpr/>

<https://www.scoop.it/t/isafe/>

[http://gym-gaziou.ira.sch.gr/images/pdf\\_files/privacy.pdf](http://gym-gaziou.ira.sch.gr/images/pdf_files/privacy.pdf)

[https://www.forth.gr/index\\_main.php?l=q&c=28&i=1439](https://www.forth.gr/index_main.php?l=q&c=28&i=1439)

Διαδραστικό εργαστήριο «Ο GDPR και οι 40 κλέφτες», Δημήτρης Γραμμένος & Ανθή Στρατάκη, ITE