

# Πώς να προστατεύουμε το κινητό μας από τους επίδοξους εισβολείς

/ [Επιστήμες, Τέχνες & Πολιτισμός](#)



**kinit** Αυτές είναι επιλογές που υπάρχουν σε συσκευές iPhone και Android.

Το χακάρισμα του iPhone του δολοφόνου του Σαν Μπερναρντίνο (San Bernardino) που έγινε από την αμερικανική κυβέρνηση μας υπενθυμίζει ότι τα τηλέφωνα και άλλες ηλεκτρονικές συσκευές δεν είναι αδιαπέραστα θησαυροφυλάκια.

## Νέα και μικρότερα iPhone και iPad

Ενώ οι περισσότεροι από εμάς δεν αποτελούμε στόχους των μυστικών υπηρεσιών και κάποιας κυβέρνησης, οι χάκερ ψάχνουν αφορμή συνεχώς για να υποκλέψουν τις οικονομικές και προσωπικές πληροφορίες εμάς των απλών ανθρώπων. Τα τηλεφωνα μας έχουν πολλά περισσότερα στην μνήμη τους από selfies. Για παράδειγμα η τοποθέτηση του λογαριασμού e-mail στο κινητό μας είναι μία δίοδος προς τους τραπεζικούς και άλλους σημαντικούς κωδικούς πρόσβασης.

## Κλειδώνετε το τηλέφωνο σας με κωδικό

Αν χρησιμοποιείται εξαψήφιος κωδικός αντί για τους κλασικούς 4ψήφιους το κινητό σας τηλέφωνο θα είναι 100 φορές πιο δύσκολο να βρεθεί ο κωδικός και αν θέλετε να τον κάνετε ακόμη πιο ευαίσθητο, μπορείτε να προσθέσετε γράμματα και άλλους χαρακτήρες για να αυξήσετε περαιτέρω τον αριθμό των πιθανών συνδυασμών.

Αυτές είναι επιλογές που υπάρχουν σε συσκευές iPhone και Android.

Ωστόσο βιομετρικά στοιχεία, όπως οι σαρωτές δακτυλικών αποτυπωμάτων, μας βοηθούν να έχουμε το κεφάλι μας ήσυχο και να μην χρειαστούμε όλα τα παραπάνω.

## Χρησιμοποιήστε κρυπτογράφηση

Τα iPhone με λογισμικό iOS 8 και μεταγενέστερο, παρέχουν πλήρη κρυπτογράφηση

του δίσκου τους χωρίς να το επιλέξει ο χρήστης. Αυτό σημαίνει ότι οι πληροφορίες που είναι αποθηκευμένες στο τηλέφωνο δεν μπορούν να εξαχθούν από τις αρχές, τους χάκερ ή να διαβαστούν από κάποιον υπολογιστή.

Αν η συσκευή είναι κλειδωμένη, οι πληροφορίες που μπορούν να ληφθούν είναι κωδικοποιημένες και δυσανάγνωστες.

Οι συσκευές Android όμως, πρέπει εσύ ο ίδιος να ενεργοποιήσεις το χαρακτηριστικό από τις ρυθμίσεις και σύμφωνα με την Google λόγω αυτού μόνο το 2,3% των χρηστών συσκευών Android είναι πλήρως προστατευόμενοι.

### **Κάντε backup**

Αν χρειαστεί να καθαρίσετε όλα τα δεδομένα του κινητού σας. Εφαρμογές όπως το Find My iPhone και Android Device Manager, μας επιτρέπουν να εξαιρέσουμε φωτογραφίες και άλλα σημαντικά στοιχεία από την ολική διαγραφή αυτών. Αρκεί μόνο να έχουμε επιλέξει την επιλογή προηγούμενης.

### **Ενεργοποιήστε την ανίχνευση του κινητού σας**

Η εφαρμογή Find My iPhone δεν είναι μόνο για την εύρεση του τηλεφώνου μας, αλλά αν η συσκευή μας έχει χαθεί, μπορούμε να ενεργοποιήσουμε το Lost Mode.

Έτσι η οθόνη κλειδώνει και μπαίνει αυτόματα κωδικός, αν δεν υπάρχει ήδη και μας επιτρέπει να εμφανίσουμε ένα προσαρμοσμένο μήνυμα με έναν αριθμό τηλεφώνου στην οθόνη του κινητού μας, έτσι ώστε να μπορέσουμε να το ανιχνεύσουμε πιο εύκολα. Η εφαρμογή θα πρέπει να έχει ενεργοποιηθεί πριν χάσουμε το τηλέφωνό μας.

Εντωμεταξύ το Activation Lock καθιστά σχεδόν ακατόρθωτο για τους κλέφτες να πουλήσουν την συσκευή. Το τηλέφωνο γίνεται άχρηστο γιατί δεν μπορεί να ενεργοποιηθεί χωρίς να γνωρίζει ο κάτοχος το Apple ID.

Αν όλα αυτά αποτύχουν ο χρήστης μπορεί εξ αποστάσεως να κάνει απαλοιφή των δεδομένων του τηλεφώνου.

Οι πληροφορίες θα χαθούν αλλά τουλάχιστον δεν θα καταλήξουν στα χέρια ενός αγνώστου.

Δεν υπάρχει τίποτα συγκρίσιμο στις συσκευές Android, αλλά η εφαρμογή της Google, Android Device Manager, κάνει όλα τα παραπάνω και μπορεί να την εγκαταστήσει κανείς πολύ απλά από το Google Play Store.

### **Διατηρείτε το λογισμικό σας ενημερωμένο**

Οι ενημερώσεις λογισμικού συχνά περιέχουν διορθώσεις για ελαττώματα που μπορεί να κρατούν ανοιχτό κάποιο παράθυρο της συσκευής μας στους χάκερ.

**Πηγή:** [onlycy.com](https://onlycy.com)