

Lookout Mobile Security

ΒΑΣΙΚΕΣ ΟΔΗΓΙΕΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ



Together we can
vodafone
business

Ενεργοποίηση Λογαριασμού Διαχειριστή

01



Ενεργοποίηση Λογαριασμού Διαχειριστή

Με την επιτυχή ολοκλήρωση της παραγγελίας σας, λαμβάνετε ένα email από την **Lookout** για την πρώτη σας είσοδο στην πλατφόρμα.

Το email που έρχεται για την είσοδό σας στην πλατφόρμα και ενεργοποίηση της υπηρεσίας – θα το λάβετε από το **Lookout** (no-reply@lookout.com) με θέμα **«Lookout Mobile Security - Ενεργοποιήστε τις άδειές σας τώρα και προστατέψτε τις συσκευές σας»** – περιλαμβάνει:

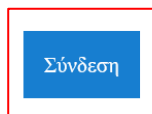
(α) το **Όνομα Χρήστη** (Username)

(β) τις **Βασικές Οδηγίες Ενεργοποίησης** του λογαριασμού διαχειριστή

(γ) την **κουμπί** με το **link** για τη πρώτη είσοδο στη πλατφόρμα και τον ορισμό κωδικού πρόσβασης

Για να ενεργοποιήσετε το Lookout από υπολογιστή ή laptop:

1. Συνδεθείτε στη Lookout Mobile Security Console παρακάτω.



2. Επιλέξτε «Εγγραφή Συσκευών» από τον κύριο πίνακα ελέγχου για να στείλετε προσκλήσεις ενεργοποίησης στους εργαζομένους σας.

3. Βεβαιωθείτε ότι οι εργαζόμενοί σας ακολουθούν τις οδηγίες για λήψη και ενεργοποίηση της εφαρμογής Lookout for Work στην κινητή συσκευή τους.

ΠΡΟΣΟΧΗ: το link ενεργοποίησης, σε κάθε email που λαμβάνετε, παραμένει ενεργό για 24 ώρες. Ωστόσο, μην ανησυχείτε, αν δεν προλάβετε να ακολουθήσετε τη διαδικασία ενεργοποίησης του λογαριασμού διαχειριστή, σε πρώτο χρόνο. Το email θα σας ξανασταλεί σε συχνότητα **3, 10, 21** ημερών από την ενεργοποίηση και μετά **κάθε 30 μέρες**, μέχρι να ολοκληρώσετε τη διαδικασία.

Αν χρειάζεστε υποστήριξη με το email ενεργοποίησης (π.χ. αλλαγή email διαχειριστή, είτε αποστολή σε συντομότερο διάστημα), παρακαλούμε καλέστε το **1399** ή τη **Τεχνική Υποστήριξη** για τη καλύτερη εξυπηρέτησή σας.

Πατώντας τη σχετική ένδειξη με το link, όπως φαίνεται παρακάτω, θα ανακατευθυνθείτε στη κονσόλα της Lookout, όπου και θα μπορείτε να ορίσετε τον **κωδικό πρόσβασης** σας καθώς και να ενεργοποιήσετε εύκολα το **Multi Factor Authenticator (MFA)**. Οι οδηγίες για τις παραπάνω διαδικασίες, θα εμφανιστούν βήμα-βήμα στην οθόνη σας.



Σημείωση: Σε περίπτωση που ξεχάσετε/χάσετε τον κωδικό πρόσβασης που ορίσατε, μπορείτε ανά πάσα στιγμή να πραγματοποιήσετε **«Επαναφορά κωδικού πρόσβασης»** μέσω της κεντρικής οθόνης ενεργοποίησης

Ενεργοποίηση Τελικών Χρηστών

Η διαδικασία ενεργοποίησης των τελικών χρηστών (συσκευών) είναι σχετικά απλή.

Εφόσον, ως Διαχειριστής της υπηρεσίας, έχετε ενεργοποιήσει τον λογαριασμό σας, θα πρέπει να εισέλθετε στη Κονσόλα Διαχείρισης της Lookout μέσω της σελίδας:

<https://app.lookout.com/>

Στη συνέχεια, θα πρέπει να πραγματοποιήσετε είσοδο στη κονσόλα με τα στοιχεία σας (email/όνομα χρήστη και κωδικό πρόσβασης).



Σύνδεση

[Επαναφορά κωδικού πρόσβασης](#)

Εφόσον, έχετε ορίσει MFA, στην επόμενη σελίδα θα χρειαστεί να εισάγετε το token/κωδικό που εμφανίζεται στο **Google Authenticator** App και να πατήσετε την ένδειξη «Επόμενο».





Έλεγχος ταυτότητας πολλών σημείων

Εισαγάγετε τον 6ψήφιο κωδικό από την εφαρμογή Google Authenticator. Αντιμετωπίζετε προβλήματα;
[Δοκιμάστε έναν κωδικό ανάκτησης](#)



Εισαγάγετε 6ψήφιο κωδικό

Εισαγάγετε κωδικό

[Πίσω](#) [Επόμενο](#)

Μόλις συνδεθείτε στη Κονσόλα Διαχείρισης, στην ενότητα «**Κεντρική Σελίδα**» θα ανακατευθυνθείτε στην ενότητα «**Εγγραφή**» (απευθείας από το αριστερό μενού είτε από την ένδειξη στο δεξί πάνω μέρος της οθόνης)



Lookout για μικρές επιχειρήσεις
Πίνακας εργαλείων ασφάλειας κινητού τελικού σημείου

[ΕΓΓΡΑΦΗ ΣΥΣΚΕΥΩΝ](#) [ΑΠΟΣΤΟΛΗ ΣΧΟΛΙΟΥ](#)

Κεντρική σελίδα

Συσκευές

Έρευνες

Πολιτικές και ρυθμίσεις προστασίας

Εγγραφή

Σύστημα →

Υποστήριξη

Vodafone Greece

LG Γρήγορη πρόσβαση

Powered by Lookout

ΑΡΧΙΣΤΕ ΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΕΛΙΚΟΥ ΣΗΜΕΙΟΥ ΚΙΝΗΤΟΥ

ΠΡΟΣΤΑΤΕΥΜΕΝΕΣ ΣΥΣΚΕΥΕΣ Συσκευές που προστατεύονται από το Lookout Security Cloud

231,049,765
ΠΡΟΣΤΑΤΕΥΕΤΑΙ ΠΑΓΚΟΣΜΙΩΣ

5
ΠΡΟΣΤΑΤΕΥΕΤΑΙ ΣΤΟΝ ΣΤΟΛΟ ΣΑΣ

ΑΝΑΛΥΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ Εφαρμογές που αναλύονται από το Lookout Security Cloud

375,751,649
ΑΝΑΛΥΕΤΑΙ ΠΑΓΚΟΣΜΙΩΣ

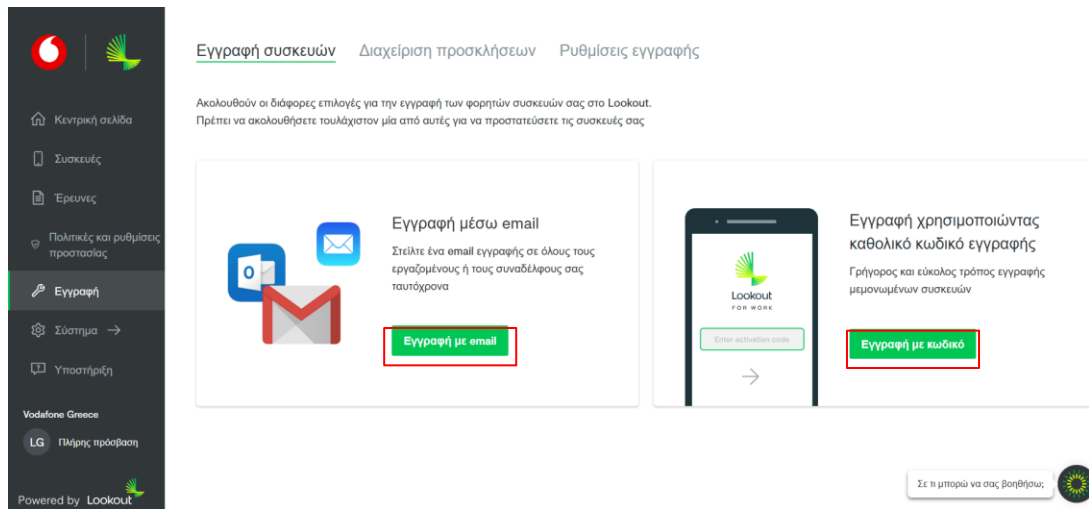
515
ΑΝΑΛΥΕΤΑΙ ΣΤΟΝ ΣΤΟΛΟ ΣΑΣ

ΚΑΤΑΣΤΑΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΤΑΣΤΑΣΗ ΑΝΑΠΤΥΞΗΣ

Σε η μπορού να σας βοηθήσουμε

Η εγγραφή τελικών χρηστών/συσκευών, μπορεί να γίνει με δύο (2) τρόπους:

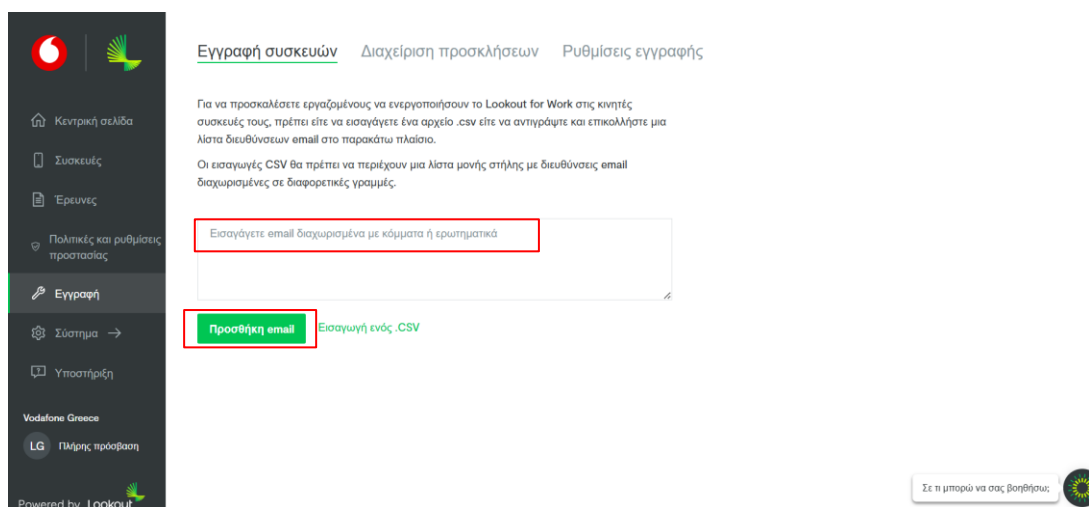




1. Εγγραφή μέσω email

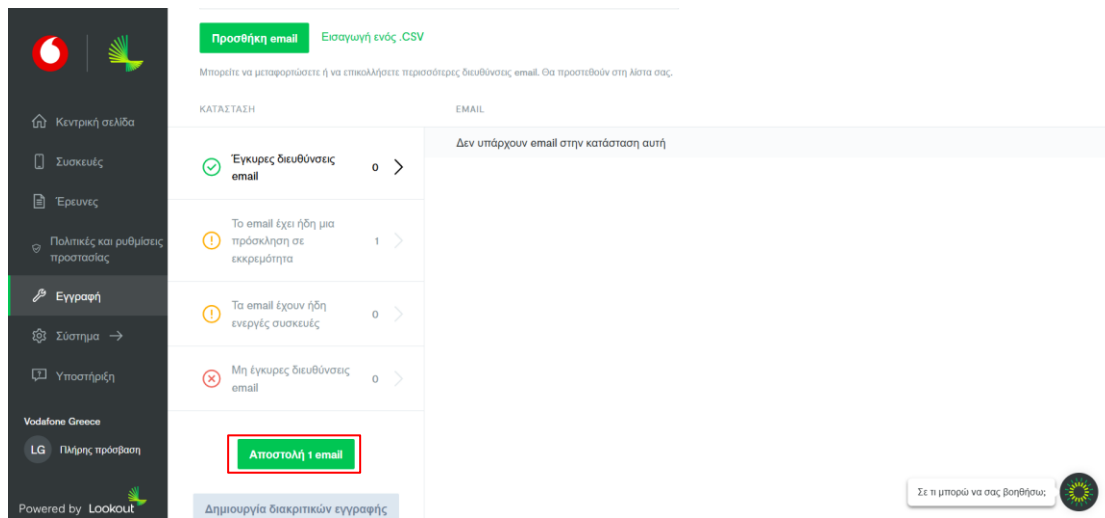
Με τη συγκεκριμένη επιλογή, ο διαχειριστής, έχει τη δυνατότητα να στείλει προσκλήσεις στους χρήστες που επιθυμεί, καταχωρώντας τα τις ηλεκτρονικές διευθύνσεις (emails) τους.

- Επιλογή ένδειξης «**Εγγραφή με email**»
- Στη σελίδα που θα ανοίξει, έχετε την επιλογή να εισάγετε τις διευθύνσεις email που επιθυμείτε είτε ένα csv αρχείο με περισσότερες διευθύνσεις email για μαζική εγγραφή (στη περίπτωση csv, οι διευθύνσεις θα πρέπει να είναι καταχωρημένες σε διαφορετικές γραμμές αλλά κάτω από την ίδια στήλη)

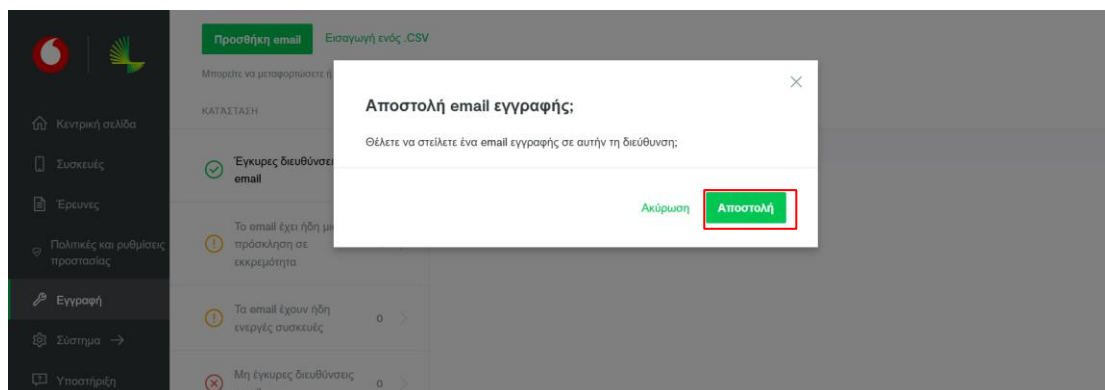


- Μόλις εισάγετε τη/τις διεύθυνση/διευθύνσεις που επιθυμείτε, επιλέξτε την ένδειξη «Προσθήκη email»

- d. Στην ενότητα που θα ανοίξει, θα μπορείτε να δείτε αν η/οι διεύθυνση/διευθύνσεις είναι έγκυρες ή όχι και αν υπάρχει κάποια πρόσκληση προς εκκρεμότητα



- e. Εφόσον, η διεύθυνση είναι έγκυρη, μπορείτε να επιλέξετε να γίνει «Αποστολή email» και στη συνέχεια να επιβεβαιώσετε την επιλογή σας, πατώντας «Αποστολή»



Κάθε χρήστης που προσκαλείται με αυτό τον τρόπο, λαμβάνει ένα email με τις οδηγίες που πρέπει να ακολουθήσει για να ενεργοποιηθεί γρήγορα και εύκολα

2. Εγγραφή χρησιμοποιώντας καθολικό κωδικό εγγραφής (token)

Αποτελεί τον πιο γενικό τρόπο εγγραφής, ενός τελικού χρήστη

- f. Επιλογή ένδειξης «**Εγγραφή με κωδικό**»
- g. Με την εγγραφή με κωδικό, ο τελικός χρήστης θα πρέπει να κατεβάσει την εφαρμογή **Lookout for Work** μέσω του App Store της συσκευής του
- h. Ο διαχειριστής, θα πρέπει να δώσει στον τελικό χρήστη τον κωδικό με τους 7 χαρακτήρες, που αναγράφεται στην οθόνη
- i. Ο τελικός χρήστης, θα πρέπει να καταχωρήσει τον κωδικό στην εφαρμογή **Lookout for Work**, μαζί με το email του (το οποίο θα είναι και το βασικό αναγνωριστικό για τον Διαχειριστή)

Εγγραφή συσκευών Διαχείριση προσκλήσεων Ρυθμίσεις εγγραφής

ΕΓΓΡΑΦΗ ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΚΩΔΙΚΟ ΨΙ ΕΓΓΡΑΦΗΣ

1. Αντιγράψτε και κοινοποιήστε τον παρακάτω σύνδεσμο στον επόλε σας με βάση το λειτουργικό σύστημα, ώστε να μπορούν να εγκαταστήσουν την εφαρμογή Lookout for Work στις κινητές συσκευές τους.

<https://apps.apple.com/us/app/lookout-for-work/id997193468>

<https://play.google.com/store/apps/details?id=com.lookout.enterprise&hl=el>

2. Ανοίξτε την εφαρμογή Lookout for Work.

3. Πληκτρολογήστε τον καθολικό κωδικό εγγραφής που φαίνεται παρακάτω. Ο τελικός χρήστης θα χρειαστεί να καταχωρήσει τη διεύθυνση email του μετά την εισαγωγή του κωδικού εγγραφής για να ολοκληρωθεί η ενεργοποίηση.

X F B D Q O G

Σε τι μπορεί να σας βοηθήσει.



Κεντρικό Μενού Διαχειριστή & Βασικές Ενότητες Διαχειριστή

02

Κεντρικό Μενού Διαχειριστή & Βασικές Ενότητες Διαχειριστή

Παρακάτω, παρουσιάζονται οι **βασικές ενότητες** της Διαχειριστικής Κονσόλας της Υπηρεσίας Lookout Mobile Security. Για λόγους demo, οι ενότητες και φωτογραφίες, είναι από το προϊόν Lookout for Small Business (Lookout για μικρές επιχειρήσεις).

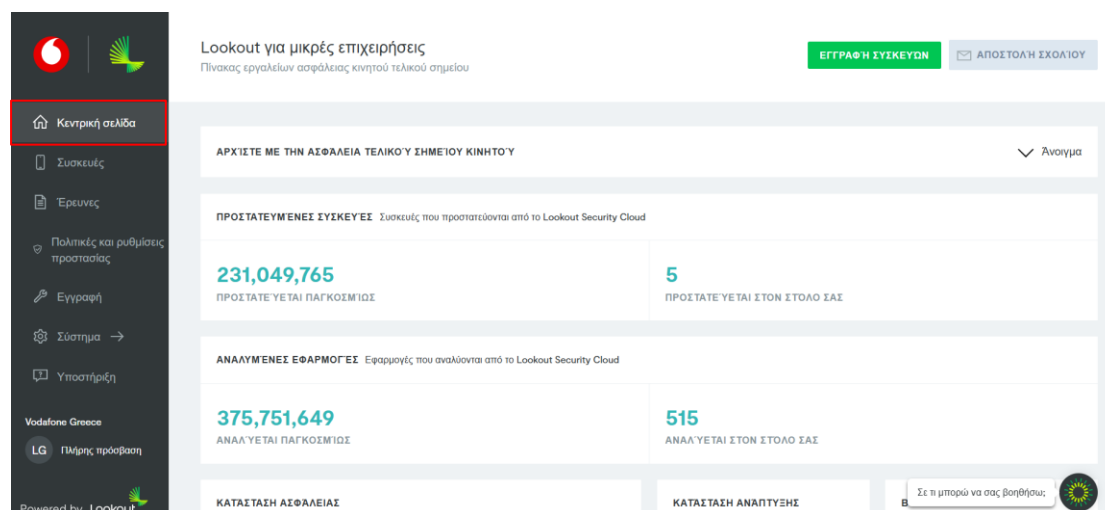
Όλες οι εκδόσεις, διαθέτουν αυτές τις βασικές ενότητες, ωστόσο διαφοροποιείται ελαφρώς το περιεχόμενο. Επιπροσθέτως, οι άλλες εκδόσεις διαθέτουν κάποιες επιπλέον ενότητες, οι οποίες ανταποκρίνονται στα επιπλέον τεχνικά χαρακτηριστικά των εν λόγω εκδόσεων.

1) Κεντρική Σελίδα

Η **κεντρική σελίδα**, είναι η πρώτη ενότητα στην οποία έχετε πρόσβαση ως Διαχειριστής, αφού συνδεθείτε στη Κονσόλα Διαχείρισης.

Σε αυτή την οθόνη, μπορείτε να δείτε πληροφορίες για τον στόλο σας (συσκευές σας) καθώς και να δείτε πόσες συσκευές προστατεύονται παγκοσμίως από τη Lookout.

Επιπλέον, μέσω της ένδειξης **«ΕΓΓΡΑΦΗ ΣΥΣΚΕΥΩΝ»**, μπορείτε να πραγματοποιήσετε ενεργοποίηση των συσκευών σας, σύμφωνα με τις οδηγίες που αναγράφονται στην ενότητα **Ενεργοποίηση Τελικών Χρηστών**.



2) Συσκευές

Μέσω της ενότητας **«Συσκευές»**, μπορείτε να παρακολουθείτε τη κατάσταση και τις βασικές πληροφορίες που αφορούν τις συσκευές του στόλου σας. Το βασικό αναγνωριστικό του χρήστη, είναι το email του, το οποίο και θα πρέπει να φαίνεται στη 3^η στήλη.

Στη 2^η στήλη, μπορείτε να δείτε τον τύπο συσκευής καθώς και το Λειτουργικό Σύστημα που είναι σε ισχύ, στην εν λόγω συσκευή. Στη 1^η και στη τελευταία στήλη,



μπορείτε να δείτε τη κατάσταση της συσκευής καθώς και το πότε συνδέθηκε τελευταία φορά (διαστήματα εντός του 24ώρου, θεωρούνται λογικά και αποδεκτά).

ΚΑΤΑΣΤΑΣΗ	ΤΥΠΟΣ ΣΥΣΚΕΥΗΣ	ΧΡΗΣΤΗΣ	ΣΥΝΔΕΣΗ
Ασφαλές	iPhone 13 Pro Max iOS 18.3.1	[Redacted]	Συνδέθηκε 16 ώρες πριν
Ασφαλές	iPhone 13 iOS 18.3.1	[Redacted]	Συνδέθηκε 6 ώρες πριν
Ασφαλές	SM-F946B Android 14	[Redacted]	Συνδέθηκε 2 ώρες πριν
Ασφαλές	iPhone 13 Pro iOS 18.3.1	[Redacted]	Συνδέθηκε μία ώρα πριν
Ασφαλές	iPhone 14 Pro iOS 18.1.1	[Redacted]	Συνδέθηκε 21 μέρες πριν

3) Έρευνες

Στην ενότητα «**Έρευνες**», μπορείτε να βρείτε άρθρα από την ερευνητική ομάδα της **Lookout**. Κάθε μήνα, υπάρχει αφιέρωμα σε ένα διαφορετικό θέμα, γύρω από το κόσμο της Κυβερνοασφάλειας και συνήθως η θεματολογία, βασίζεται στην επικαιρότητα.

REPORT NAME	DESCRIPTION	PUBLISHED
Mobile Threat Report - January 2025	A Chinese developer is distributing malware for lawful interce...	Feb 14, 2025
Mobile Threat Report - December 2024	An unknown developer seems to be creating a lawful intercep...	Jan 16, 2025
Mobile Threat Report - November 2024	Two Russian threat actor groups have been found to be target...	Dec 19, 2024
Mobile Threat Report - October 2024	A lawful intercept tool appears to have broader use across Ch...	Nov 15, 2024
Mobile Threat Report - September 2024	Russian and Chinese APT groups continue to develop their su...	Oct 11, 2024
Mobile Threat Report - August 2024	Further development of three known mobile surveillance fami...	Sep 13, 2024
Mobile Threat Report - July 2024	A known Chinese APT with a history of targeting international ...	Aug 16, 2024
Mobile Threat Report - June 2024	Russian and Chinese actors are continuing to iterate on existi...	

4) Πολιτικές και ρυθμίσεις προστασίας

Η ενότητα «**Πολιτικές και ρυθμίσεις προστασίας**», αποτελεί τη πιο σημαντική ενότητα στο περιβάλλον του Διαχειριστή.

Μέσω αυτής της ενότητας, ο Διαχειριστής, μπορεί να ορίσει διαφορετικές πολιτικές και ρυθμίσεις, στις διαφορετικές κατηγορίες απειλών καθώς και να ορίσει τον τρόπο με τον οποίο θέλει να αποκρίνεται στη κάθε απειλή.

Οι πολιτικές και το επίπεδο ρυθμίσεων, είναι προκαθορισμένα από τη Lookout. Ωστόσο, έχετε τη δυνατότητα επεξεργασίας τους, βάσει των αναγκών της



επιχείρησής σας. Αν σε οποιαδήποτε στιγμή, θέλετε να επαναφέρετε τις προεπιλεγμένες ρυθμίσεις, χρειάζεται απλά να επιλέξετε την ένδειξη «Επαναφορά προεπιλογών»

Οι Πολιτικές και ρυθμίσεις προστασίας που αναφέρονται εδώ έχουν ρυθμιστεί επί του παρόντος ως προεπιλογές Lookout. Δεν χρειάζεται να κάνετε καμία ενέργεια.

Πολιτικές και ρυθμίσεις προστασίας

Πολιτικές: Προστασία από ηλεκτρονικό ψάρεμα και προστασία περιεχομένου, Προστασία από απειλές στη συσκευή, Ηλεκτρονικό ψάρεμα μέσω SMS

Επαναφορά προεπιλογών Εξοικονόμηση 38 στοιχείων

Μοίρετε για τις Πολιτικές και ρυθμίσεις προστασίας

Φιλτράρισμα πολιτικών κατά...

ΕΝΕΡΓΟΠΟΙΗΣΗ	ΑΠΕΝΕΡΓΟΠΟΙΗΣΗ	ΤΥΠΟΣ ΠΟΛΙΤΙΚΗΣ	ΤΑΞΙΝΟΜΗΣΗ	ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ	ΠΕΡΙΓΡΑΦΗ	ΕΠΙΠΕΔΟ ΚΙΝΔΥΝΟΥ	ΑΠΟΚΡΙΣΗ
☐	☐	Εφαρμογή	Backdoor	iOS	Ανοίγει προεπιλεγμένα στοιχεία σε έναν ισχυρό	Υψηλή	Ειδοποίηση συσκευ...
☐	☐	Εφαρμογή	Bot	iOS	Επιτρέπει απομακρυσμένη πρόσβαση και έλεγχο της συσκευής	Υψηλή	Ειδοποίηση συσκευ...
☐	☐	Εφαρμογή	Exploit	iOS	Αξιοποιεί ελαττώματα του λειτουργικού συστήματος για να αποκτήσει κλεμμένα προνόμια συσκευής	Υψηλή	Ειδοποίηση συσκευ...
☐	☐	Εφαρμογή	Trojan	iOS	Εκτελεί κακόβουλες δραστηριότητες που δεν γνωστοποιούνται	Υψηλή	Ειδοποίηση συσκευ...
☐	☐	Δίκτυο	Επίθεση ενδόμενου στόχου	iOS	Επιτρέπει σε έναν κακόβουλο παράγοντα να υποκλέψει δεδομένα που αποστέλλονται μεταξύ δύο μερών	Υψηλή	Ειδοποίηση συσκευ...

Η άδεια αποθήκευσης που μας επιτρέπει να

Στις στήλες που παρουσιάζονται, μπορείτε να δείτε τη κατηγορία (τύπο) πολιτικής, τη ταξινόμηση της, τα λειτουργικά συστήματα που επηρεάζει καθώς και μια σύντομη περιγραφή. Αν πατήσετε στην ένδειξη «?» που βρίσκεται δίπλα από κάθε περιγραφή, μπορείτε να μάθετε περισσότερα για την εν λόγω πολιτική.

Στις στήλες «**ΕΠΙΠΕΔΟ ΚΙΝΔΥΝΟΥ**» και «**ΑΠΟΚΡΙΣΗ**», αναφέρονται το επίπεδο επικινδυνότητας καθώς και τον τρόπο που θα ανταποκριθεί το λογισμικό της Lookout, όταν εντοπίσει μια απειλή αυτής της κατηγορίας. Μπορείτε να επεξεργαστείτε τις προεπιλεγμένες ρυθμίσεις, βάσει των αναγκών της επιχείρησής σας.

Οι Πολιτικές και ρυθμίσεις προστασίας που αναφέρονται εδώ έχουν ρυθμιστεί επί του παρόντος ως προεπιλογές Lookout. Δεν χρειάζεται να κάνετε καμία ενέργεια.

Πολιτικές και ρυθμίσεις προστασίας

Πολιτικές: Προστασία από ηλεκτρονικό ψάρεμα και προστασία περιεχομένου, Προστασία από απειλές στη συσκευή, Ηλεκτρονικό ψάρεμα μέσω SMS

Επαναφορά προεπιλογών Εξοικονόμηση 38 στοιχείων

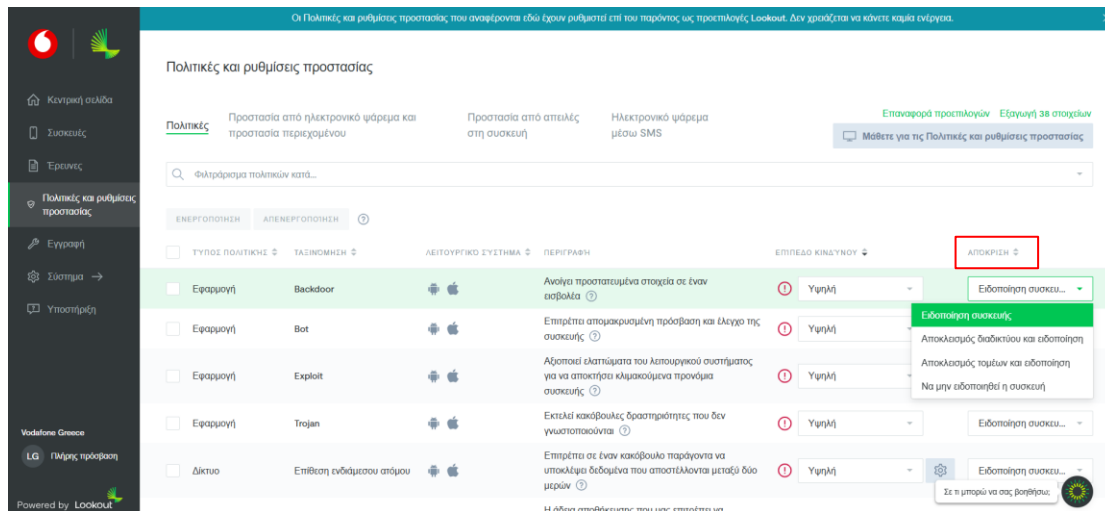
Μοίρετε για τις Πολιτικές και ρυθμίσεις προστασίας

Φιλτράρισμα πολιτικών κατά...

ΕΝΕΡΓΟΠΟΙΗΣΗ	ΑΠΕΝΕΡΓΟΠΟΙΗΣΗ	ΤΥΠΟΣ ΠΟΛΙΤΙΚΗΣ	ΤΑΞΙΝΟΜΗΣΗ	ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ	ΠΕΡΙΓΡΑΦΗ	ΕΠΙΠΕΔΟ ΚΙΝΔΥΝΟΥ	ΑΠΟΚΡΙΣΗ
☐	☐	Εφαρμογή	Backdoor	iOS	Ανοίγει προεπιλεγμένα στοιχεία σε έναν ισχυρό	Υψηλή	Ειδοποίηση συσκευ...
☐	☐	Εφαρμογή	Bot	iOS	Επιτρέπει απομακρυσμένη πρόσβαση και έλεγχο της συσκευής	Υψηλή	Ειδοποίηση συσκευ...
☐	☐	Εφαρμογή	Exploit	iOS	Αξιοποιεί ελαττώματα του λειτουργικού συστήματος για να αποκτήσει κλεμμένα προνόμια συσκευής	Υψηλή	Ειδοποίηση συσκευ...
☐	☐	Εφαρμογή	Trojan	iOS	Εκτελεί κακόβουλες δραστηριότητες που δεν γνωστοποιούνται	Υψηλή	Ειδοποίηση συσκευ...
☐	☐	Δίκτυο	Επίθεση ενδόμενου στόχου	iOS	Επιτρέπει σε έναν κακόβουλο παράγοντα να υποκλέψει δεδομένα που αποστέλλονται μεταξύ δύο μερών	Υψηλή	Ειδοποίηση συσκευ...

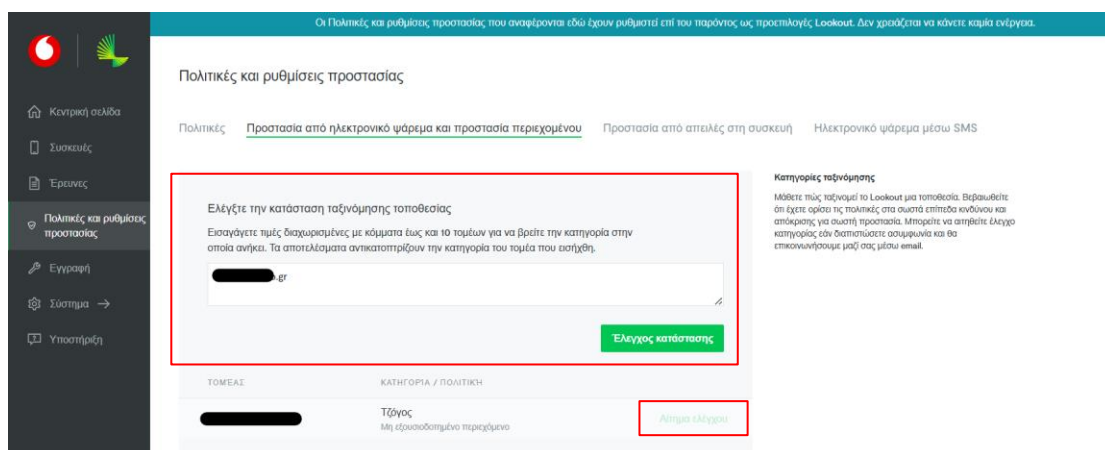
Η άδεια αποθήκευσης που μας επιτρέπει να





Αν επιλέξετε την υπο-ενότητα «**Προστασία από ηλεκτρονικό ψάρεμα και προστασία περιεχομένου**», μπορείτε να ρυθμίσετε τόσο το επιτρεπόμενο (whitelisted) και μη επιτρεπτό (denylisted) περιεχόμενο, στο οποίο θέλετε ή δεν θέλετε να έχουν πρόσβαση οι εργαζόμενοι σας.

Για να ελέγξετε τη κατηγορία ενός τομέα (domain), πριν προχωρήσετε σε whitelisting ή denylisting, μπορείτε να το καταχωρήσετε στο πλαίσιο που εμφανίζεται στην αρχή της σελίδας και στη συνέχεια να επιλέξετε την ένδειξη «**Ελεγχος κατάστασης**». Οι κατηγορίες, εμφανίζονται βάσει εκτεταμένης και διαρκώς ανανεώσιμης βάσης δεδομένων της Lookout. Ωστόσο, αν για κάποιο λόγο δεν συμφωνείτε με τα αποτελέσματα, μπορείτε να υποβάλλετε «**Αίτημα ελέγχου**» για τον συγκεκριμένο τομέα (domain).



Στη συνέχεια, μπορείτε να εισάγετε τον τομέα (domain) στο πλαίσιο που επιθυμείτε, επιλέγοντας την ένδειξη «**Προσθήκη μιας καταχώρησης**» κάτω από το εκάστοτε πλαίσιο.



Οι Πολιτικές και ρυθμίσεις προστασίας που αναφέρονται εδώ έχουν ρυθμιστεί επί του παρόντος ως προεπιλεγμένες Lookout. Δεν χρειάζεται να κάνετε καμία ενέργεια.

Επιτρεπόμενο περιεχόμενο

Προσθέτετε περιεχόμενο που θέλετε πάντα να εμπιστευόμαστε και μην αποκλείεται ποτέ. Η λίστα σας μπορεί να περιέχει έως και 100 καταχωρήσεις.

ΚΑΤΑΧΩΡΗΣΗ ⓘ ΠΕΡΙΓΡΑΦΗ

Δεν υπάρχουν τομείς.

Προσθήκη μιας καταχώρισης ή Μεταφόρτωση μιας λίστας μέσω .csv (100 διαθέσιμες καταχωρήσεις)

Απαγορευμένο περιεχόμενο

Προσθέτετε περιεχόμενο που δεν θέλετε να εμπιστευόμαστε ποτέ και ενεργοποιήστε πάντα τις ενέργειες πολιτικής. Η λίστα σας μπορεί να περιέχει έως και 100 καταχωρήσεις.

ΚΑΤΑΧΩΡΗΣΗ ⓘ ΠΕΡΙΓΡΑΦΗ

Προσθήκη μιας καταχώρισης ή Μεταφόρτωση μιας λίστας μέσω .csv (100 διαθέσιμες καταχωρήσεις)

Απαγορευμένο περιεχόμενο

Όταν απαγορεύετε περιεχόμενο, το Lookout ενδέχεται να αποκλείσει την πρόσβαση στο περιεχόμενο ανεξάρτητα από πιθανούς κινδύνους απάτης ή εξαπάτησης. Μπορείτε να ελέγξετε αυτήν τη συμπεριφορά χρησιμοποιώντας την πολιτική Απαγορευμένο περιεχόμενο. Αυτό σας επιτρέπει να παρακολουθείτε τη λίστα απαγορευμένων και να επιλέξετε πώς επηρεάζει τους χρήστες σας.

Στο πεδίο που θα ανοίξει, θα πρέπει να καταχωρήσετε τον τομέα (domain) που επιθυμείτε να επιτρέψετε ή αποκλείσετε, καθώς και τη κατηγορία του. Στη συνέχεια, θα πρέπει να επιλέξετε την ένδειξη «**ΠΡΟΣΘΗΚΗ**» για να ολοκληρωθεί η καταχώρηση.

ΚΑΤΑΧΩΡΗΣΗ ⓘ ΠΕΡΙΓΡΑΦΗ

Καταχώρηση Περιγραφή

Εισαγάγετε ένα TLD (.com) ή ένα πλήρως πιστοποιημένο όνομα τομέα (example.com). Όλοι οι τομείς ή/και οι υποτομείς κάτω από την καταχώρισή σας περιλαμβάνονται αυτόματα στη λίστα επιτρεπόμενων.

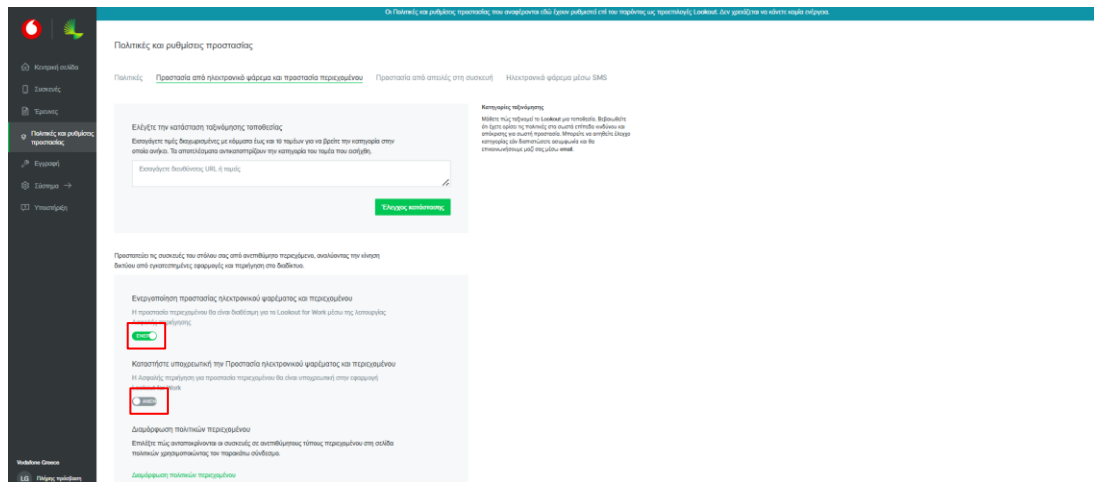
ΠΡΟΣΘΗΚΗ ΑΚΥΡΩΣΗ

Προσθήκη μιας καταχώρισης ή Μεταφόρτωση μιας λίστας μέσω .csv (100 διαθέσιμες καταχωρήσεις)

Μέσα από την ίδια υπό-ενότητα, μπορείτε να επιλέξετε αν η προστασία ηλεκτρονικού ψαρέματος (phishing) και περιεχομένου, θα είναι ενεργοποιημένη και στη συνέχεια, αν θα είναι και υποχρεωτική για τους τελικούς χρήστες που έχουν ενεργοποιήσει το λογισμικό.

Στις προεπιλογές της Lookout, η λειτουργία αυτή, είναι ενεργοποιημένη αλλά δεν είναι υποχρεωτική και άρα ο τελικός χρήστης, θα μπορεί να την απενεργοποιήσει από την εφαρμογή **Lookout for Work**, εφόσον το επιθυμεί.

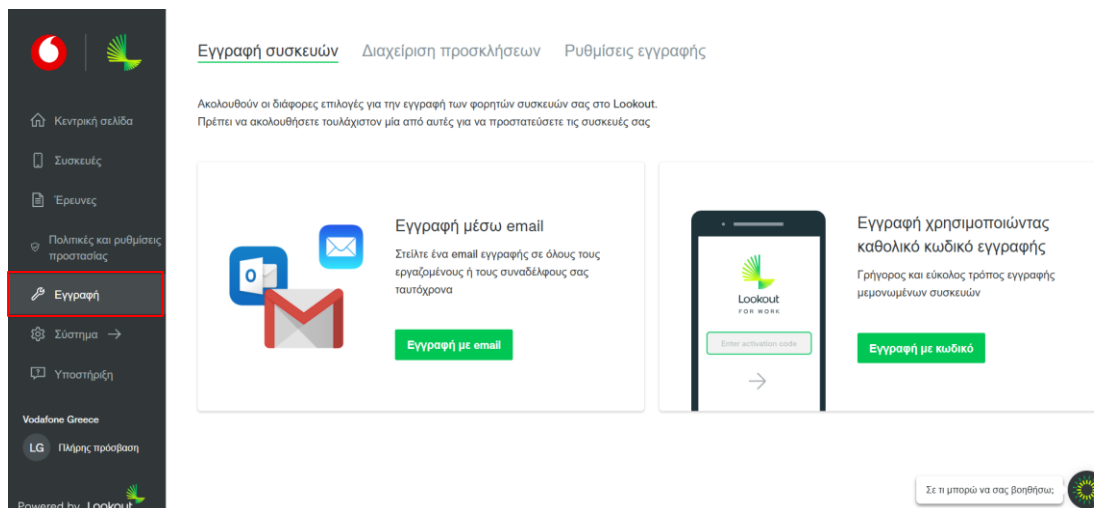




5) Εγγραφή (Συσκευών)

Στην ενότητα «Εγγραφή», έχετε τη δυνατότητα, να διαλέξετε τη μέθοδο με την οποία επιθυμείτε να προσκαλέσετε τους εργαζομένους σας στην υπηρεσία της Lookout και να εγγραφούν κάτω από τον λογαριασμό σας.

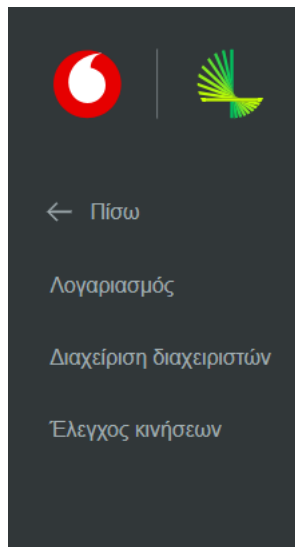
Περισσότερα για τον τρόπο ενεργοποίησης και εγγραφής των τελικών χρηστών, στην ενότητα **Ενεργοποίηση Τελικών Χρηστών**.



6) Σύστημα

Επιλέγοντας, την ενότητα «**Σύστημα**», θα εμφανιστεί ένα δεύτερο μενού με τις υπο-ενότητες «**Λογαριασμός**», «**Διαχείριση διαχειριστών**» και «**Έλεγχος κινήσεων**». Το συγκεκριμένο μενού, αφορά τον λογαριασμό σας καθώς και τους διαχειριστές που επιθυμείτε να ορίσετε.





Επιλέγοντας, την υπο-ενότητα «**Λογαριασμός**», μπορείτε να δείτε βασικά στοιχεία του λογαριασμού σας, το σύνολο των αδειών σας καθώς και των ενεργοποιημένων αδειών χρήσης. Επιπλέον, μπορείτε να εντοπίσετε τον καθολικό κωδικό εγγραφής που αντιστοιχεί στον λογαριασμό σας και με τον οποίο μπορεί να εγγραφεί ένας τελικός χρήστης (για περισσότερα, ανατρέξτε στην ενότητα **Ενεργοποίηση Τελικών Χρηστών**).

Στη συγκεκριμένη ενότητα, μπορείτε να επιλέξετε το διάστημα που επιθυμείτε να αποθηκεύει τα δεδομένα σας η Lookout (από 3 έως 36 μήνες), μέσω του dropdown που υπάρχει και να αποθηκεύσετε κάνοντας «Αποθήκευση αλλαγών».



Ο χρήστης-διαχειριστής, θα λάβει ένα email στη διεύθυνση που έχετε δηλώσει κατά τη προσθήκη και ακολουθώντας τα βήματα που αναγράφονται, θα μπορεί να ενεργοποιήσει τον λογαριασμό του.

×

Προσθήκη νέου διαχειριστή

Όνομα

Email

☒ Πλήρης πρόσβαση

☐ Περιορισμένη πρόσβαση

☐ Περιορισμένη πρόσβαση: Υπεύθυνος εγγραφών

☐ Πρόσβαση μόνο ανάγνωσης

Δεν είναι δυνατή η επεξεργασία της πολιτικής ασφάλειας, η εγγραφή συσκευών ή η επεξεργασία προτιμήσεων συστήματος. Μπορεί να διαχειριστεί μεμονωμένες συσκευές και προβλήματα, να εξάγει περιεχόμενο και να επεξεργαστεί τις δικές του προτιμήσεις.

Δεν είναι δυνατή η επεξεργασία της πολιτικής ασφάλειας, η εγγραφή συσκευών ή η επεξεργασία προτιμήσεων συστήματος. Μπορεί να προβάλει και να ανανεώσει διακριτικά προσκλήσεων που απαιτούνται για ενεργοποίηση του Lookout.

Δεν είναι δυνατή η επεξεργασία της πολιτικής ασφάλειας, η εγγραφή ή διαχείριση συσκευών, η διαχείριση προβλημάτων ή η επεξεργασία προτιμήσεων συστήματος. Δεν μπορούν να εξαχθούν περιεχόμενο και να επεξεργάζονται τις δικές τους προτιμήσεις.

Ακύρωση

Προσθήκη

Στην υπο-ενότητα «**Έλεγχος κινήσεων**», έχετε τη δυνατότητα να βλέπετε πότε συνδέθηκε ή αποσυνδέθηκε ένας χρήστης-διαχειριστής.



← Πίσω

Λογαριασμός

Διαχείριση διαδρομών

Έλεγχος κινήσεων

Έλεγχος κινήσεων

Εξαγωγή στοιχείων

1-30

DPA	ΠΑΡΑΓΟΝΤΑΣ	ΤΥΠΟΣ	ΛΕΠΤΟΜΕΡΕΙΕΣ ΣΥΜΒΑΝΤΟΣ	ΣΤΟΧΟΣ
10 Μαρ 2025 4:23 ΜΜ	[Redacted] (Πλήρης πρόσβαση)	Σύνδεση	Συνδέθηκε	Vodafone Greece
10 Μαρ 2025 2:28 ΜΜ	[Redacted] (Πλήρης πρόσβαση)	Σύνδεση	Συνδέθηκε	Vodafone Greece
10 Μαρ 2025 2:28 ΜΜ	[Redacted] (Πλήρης πρόσβαση)	Σύνδεση	Συνδέθηκε	Vodafone Greece

7) Λοιπές ενότητες

Όπως αναφέρθηκε και σε προηγούμενες ενότητες, είναι αναμενόμενο, οι διαφορετικές εκδόσεις του **Lookout Mobile Security** να περιέχουν και επιπλέον ενότητες, οι οποίες αντικατοπτρίζουν τα επιπλέον τεχνικά χαρακτηριστικά της εκάστοτε έκδοσης.

Για παράδειγμα, η έκδοση **Lookout Mobile Security Advanced**, περιέχει και τις ενότητες «**Ευπάθειες**» και «**Ενοποιήσεις**». Στην ενότητα «**Ευπάθειες**», ο



διαχειριστής μπορεί να εντοπίσει το επίπεδο ευπαθειών που έχει εντοπιστεί στο λειτουργικό σύστημα των συσκευών του στόλου του ενώ στην ενότητα «**Ενοποιήσεις**» σας δίνει τη δυνατότητα να ενοποιήσετε το λογισμικό της Lookout με λογισμικά/συστήματα διαχείρισης συσκευών και πρόσβασης (MDM/IEM/MAM/SIEM) που ενδεχομένως διαθέτετε.

Lookout

Κεντρική σελίδα

Προβλήματα

Συσκευές

Εφαρμογές

Ευπάθειες

Ερευνες

Πολιτικές και ρυθμίσεις προστασίας

Ενοποίησης

Σύστημα →

Υποστήριξη

LGΓρήγορη πρόσβαση

4 ευπάθειες

Εξοργιστή 4 στοιχείων

Φιλτράρισμα ενημερώσεων κώδικα κατά...

ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ	ΕΝΗΜΕΡΩΣΗ ΚΩΔΙΚΑ	ΗΜΕΡΟΜΗΝΙΑ ΚΥΚΛΟΦΟΡΙΑΣ	ΣΥΣΤΗΜΕΣ	ΑΡΙΘΜΟΣ ΕΥΠΑΘΕΙΩΝ	ΠΟΣΟΣΤΟ ΑΝΑΛΟΓΙΑΣ ΣΤΑΘΕΡΟΤΗΤΑΣ
Android	2025-02-01	3 Φεβ 2025	25%	66	
Android	2025-01-01	6 Ιαν 2025	25%	101	
iOS	18.2.1	6 Ιαν 2025	25%	29	
Android	2024-12-05	2 Δεκ 2024	25%	123	

Σε τι μπορώ να σας βοηθήσω?

Lookout

Κεντρική σελίδα

Προβλήματα

Συσκευές

Εφαρμογές

Ενοποίησης

Ερευνες

Πολιτικές και ρυθμίσεις προστασίας

Σύστημα →

Υποστήριξη

LGΓρήγορη πρόσβαση

Μπορείτε να συνδεθείτε σε υποστηρίξιμνα συστήματα διαχείρισης φορητών συσκευών (MDM), Διαχείρισης ταυτότητας και πρόσβασης (IAM), Διαχείρισης εφαρμογών για φορητές συσκευές (MAM) και Διαχείρισης πληροφοριών ασφάλειας και διαχείρισης συμβάντων (SIEM) για να συγχρονίσετε τις πληροφορίες απειλών Lookout και να αυτοματοποιήσετε την εγγραφή, την ενεργοποίηση και τη συμμόρφωση.

Συνδεδεμένα προϊόντα

Δεν υπάρχουν συνδεδεμένα προϊόντα.

Επιλέξτε ένα προϊόν για ρύθμιση

BlackBerry

Blackberry UEM

MDM Connector

ivantiEPMM

Ivanti EPMM (πρώην MobileIron Core)

MDM Connector

ivantiN-MDM

Ivanti Neurons MDM (πρώην MobileIron Cloud)

MDM Connector

IBM MaaS360

MaaS360

MDM Connector

Azure

Microsoft Azure

Πάροχος ταυτότητας

Microsoft Defender

Microsoft Defender ATP

Πληροφορίες ασφάλειας

Workspace ONE® UEM

Workspace ONE

MDM Connector

Σε τι μπορώ να σας βοηθήσω?



Εμπειρία Τελικού Χρήστη

03

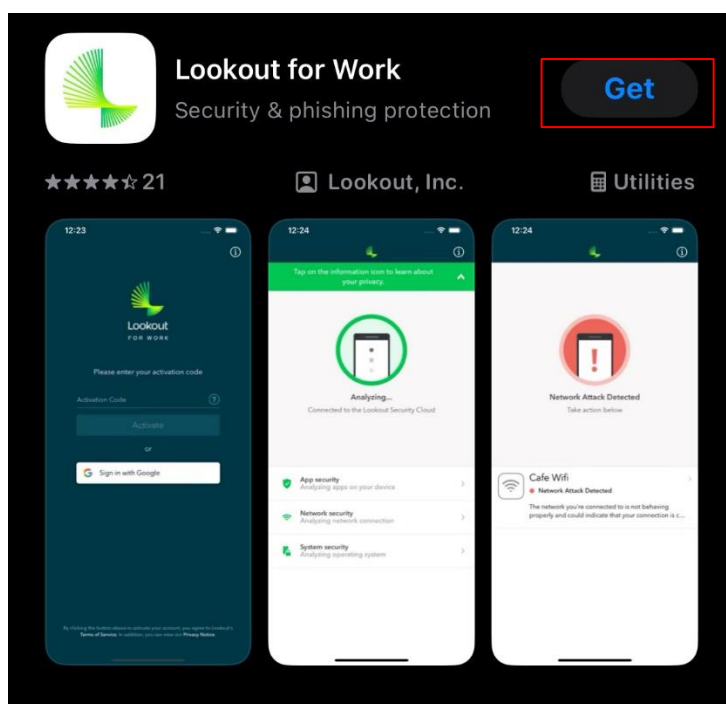
Εμπειρία Τελικού Χρήστη

Ο τελικός χρήστης (εργαζόμενος σας), χρειάζεται να ακολουθήσει κάποια βασικά και εύκολα βήματα για να ενεργοποιήσει τη Lookout άδεια στη κινητή συσκευή του. Από εκεί και πέρα, οι ειδοποιήσεις και η εικόνα που έχει ο τελικός χρήστης, μέσω της εφαρμογής «**Lookout for Work**», βοηθούν τον τελικό χρήστη, να έχει μια αρκετά απλοποιημένη αλλά ταυτόχρονα ασφαλή εμπειρία.

Σημαντική Σημείωση: Μια (1) άδεια χρήσης, αντιστοιχεί σε μια (1) κινητή συσκευή (smartphone ή tablet) του τελικού χρήστη. Αν έχετε τελικούς χρήστες με περισσότερες κινητές συσκευές και επιθυμείτε να ενσωματωθούν στο λογισμικό της Lookout, θα πρέπει να συμβουλευτείτε τον πωλητή σας και να προμηθευτείτε επιπλέον άδειες χρήσης.

1. Ενεργοποίηση Άδειας (Συσκευές Apple)

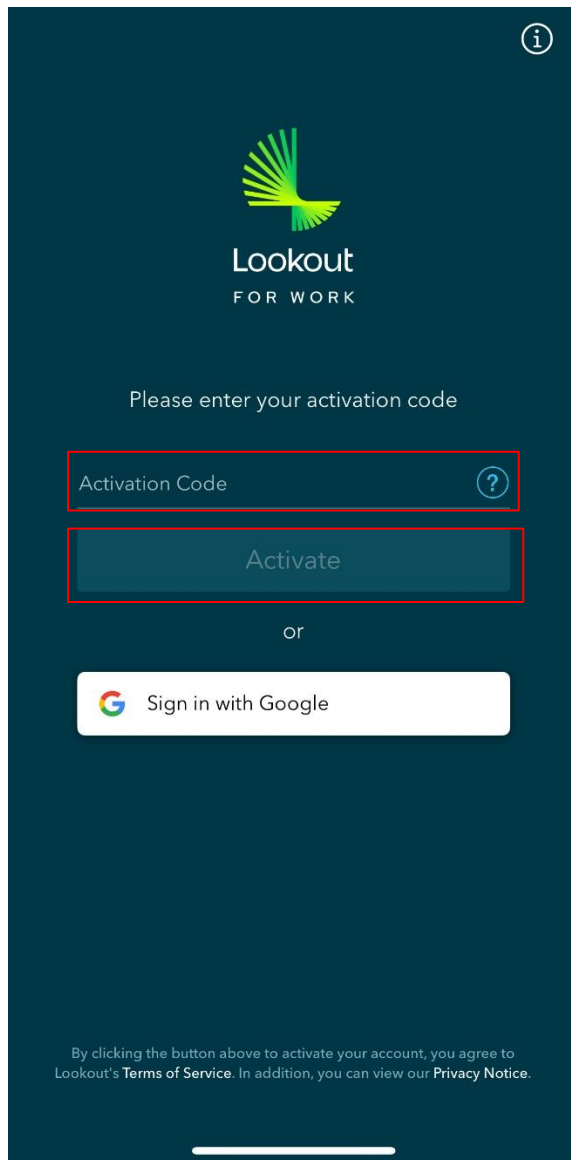
Το πρώτο βήμα που θα πρέπει να ακολουθήσει ο τελικός χρήστης, είναι να κατεβάσει την εφαρμογή **Lookout for Work**, μέσω του App Store.



Στη συνέχεια, ο χρήστης, θα πρέπει να ανοίξει την εφαρμογή **Lookout for Work** και να εισάγει τον **κωδικό/token ενεργοποίησης** που έχει λάβει, σύμφωνα με τη διαδικασία που έχει ακολουθηθεί (είτε με email πρόσκληση είτε με τον καθολικό κωδικό). Περισσότερα για τη διαδικασία ενεργοποίησης από πλευράς Διαχειριστή, μπορείτε να βρείτε στην ενότητα **Ενεργοποίηση Τελικών Χρηστών**.

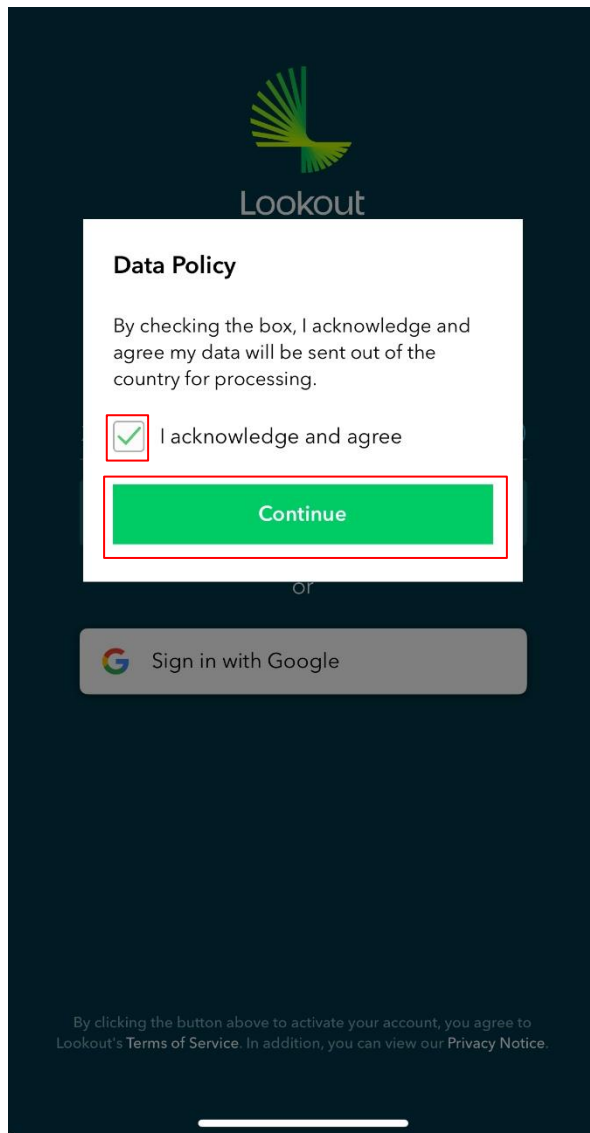
Για να προχωρήσει, ο τελικός χρήστης, θα πρέπει να επιλέξει την ένδειξη «**Ενεργοποίηση (Activate)**».





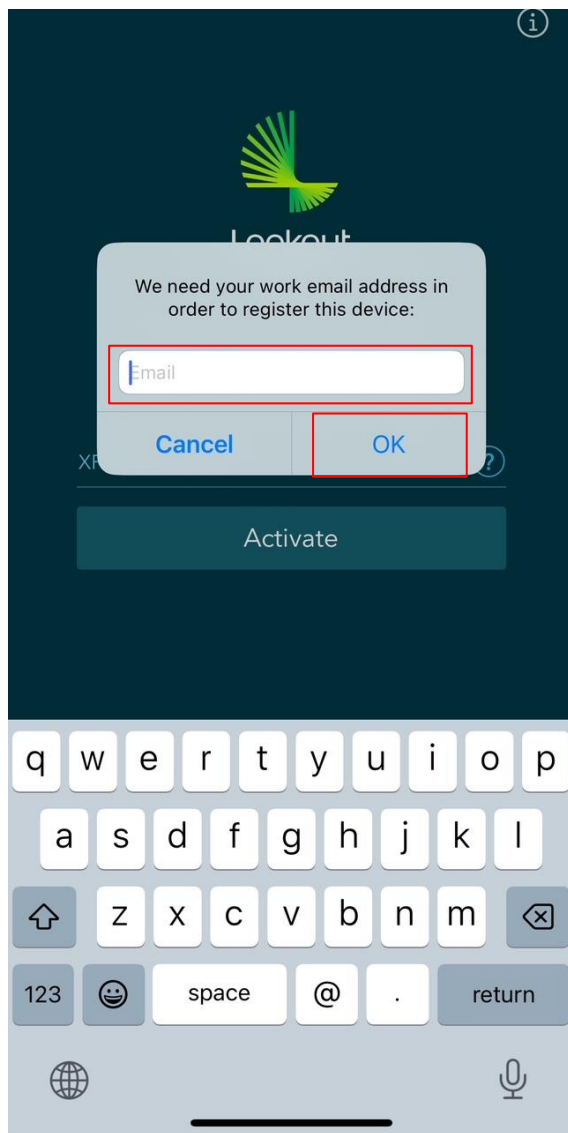
Στο παράθυρο που ανοίγει, ο τελικός χρήστης, καλείται να αποδεχθεί τη **Πολιτική Ιδιωτικότητας** της Lookout για να προχωρήσει. Εφόσον, ο χρήστης συμφωνεί με τους όρους, θα πρέπει να επιλέξει τη συγκεκριμένη επιλογή και να επιλέξει την ένδειξη «**Συνέχεια (Continue)**».





Στη συνέχεια, ο τελικός χρήστης, καλείται να εισάγει το email του, το οποίο και θα είναι το βασικό αναγνωριστικό της συσκευής του. Για να προχωρήσει στο επόμενο βήμα, ο τελικός χρήστης θα πρέπει να επιλέξει την ένδειξη **«OK»**





Στις συσκευές Apple, είναι απαραίτητο, να γίνει αποδοχή των ρυθμίσεων «**Ειδοποιήσεων (Notifications)**», «**VPN**» και «**Τοποθεσίας (Location)**». Αν ο χρήστης, έχει ήδη κάποιο λογισμικό που χρησιμοποιεί τις ρυθμίσεις VPN, θα πρέπει να τις απενεργοποιήσει για το εν λόγω λογισμικό και να τις ενεργοποιήσει για το λογισμικό της Lookout.

Let's get started! 🗝️

To setup the right protection and privacy we need your permission



Notifications

Notify you when a threat is detected.



VPN (Virtual Private Network)

Protect your identity & corporate data when you encounter threats.

- We don't collect or share your browsing history



Location

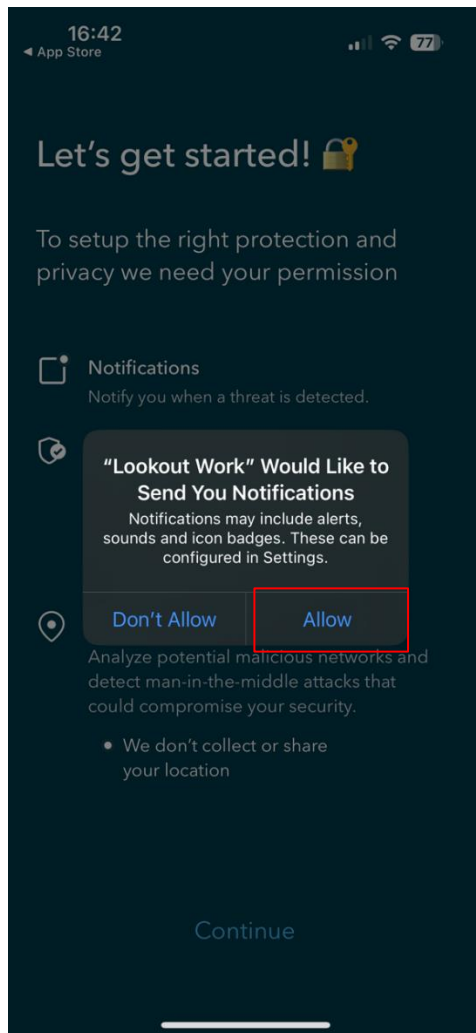
Analyze potential malicious networks and detect man-in-the-middle attacks that could compromise your security.

- We don't collect or share your location

Continue

Για να προχωρήσει στην αποδοχή και ενεργοποίηση αυτών των ρυθμίσεων, ο τελικός χρήστης, θα πρέπει να επιλέξει την ένδειξη «**Continue (Συνέχεια)**».



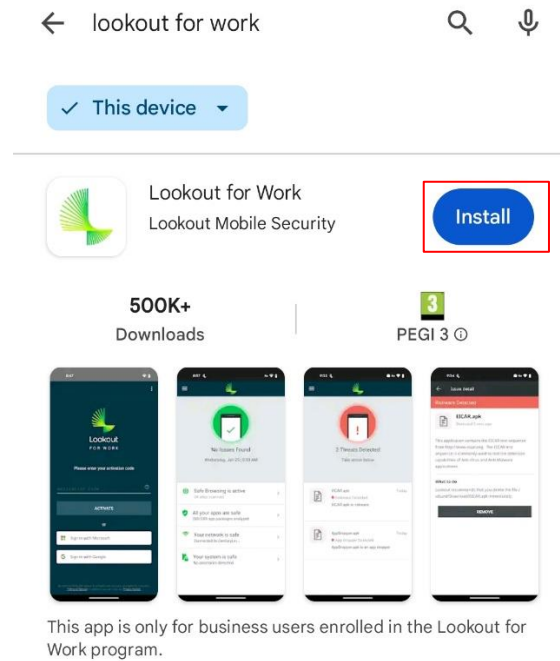


Και για τις τρείς (3) επιλογές, θα ανοίξουν αναδυόμενα (pop-up) παράθυρα, τα οποία θα πρέπει να αποδεχτεί ο τελικός χρήστης, επιλέγοντας την ένδειξη «**Allow (Αποδοχή)**». Ο χρήστης, δεν θα μπορέσει να ολοκληρώσει την εγκατάσταση της άδειας αν δεν αποδεχτεί όλα τα παράθυρα.

2. Ενεργοποίηση Άδειας (Συσκευές Android)

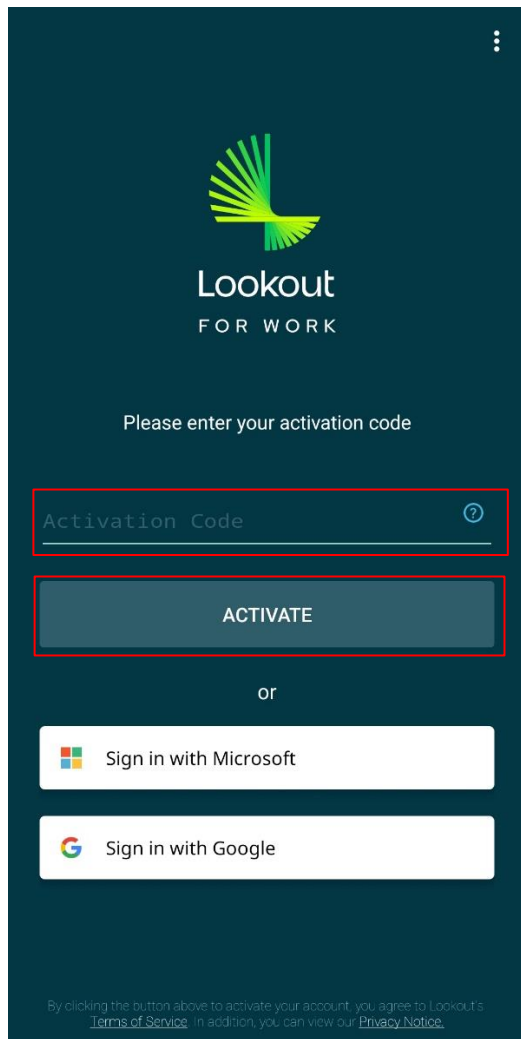
Το πρώτο βήμα που θα πρέπει να ακολουθήσει ο τελικός χρήστης, είναι να κατεβάσει την εφαρμογή **Lookout for Work**, μέσω του Play Store





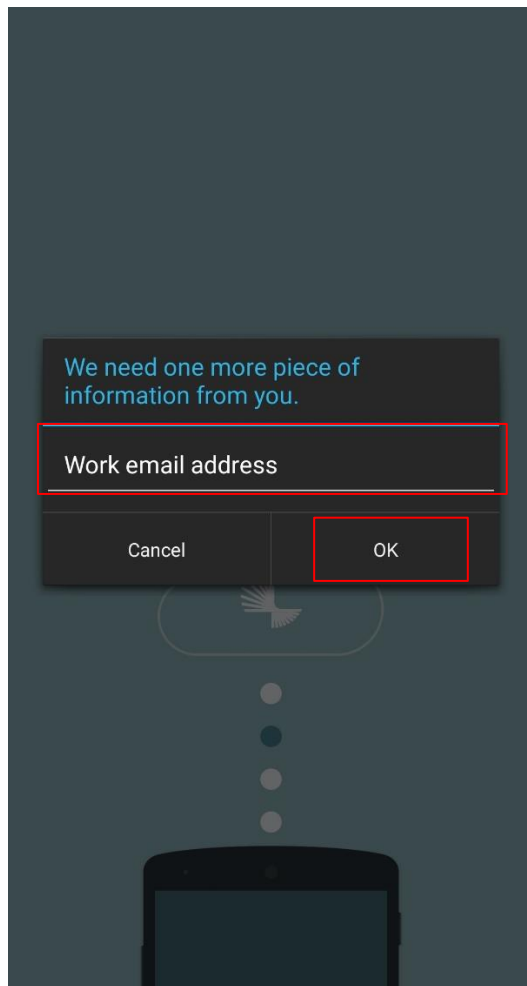
Στη συνέχεια, ο χρήστης, θα πρέπει να ανοίξει την εφαρμογή **Lookout for Work** και να εισάγει τον **κωδικό/token ενεργοποίησης** που έχει λάβει, σύμφωνα με τη διαδικασία που έχει ακολουθηθεί (είτε με email πρόσκληση είτε με τον καθολικό κωδικό). Περισσότερα για τη διαδικασία ενεργοποίησης από πλευράς Διαχειριστή, μπορείτε να βρείτε στην ενότητα **Ενεργοποίηση Τελικών Χρηστών**.

Για να προχωρήσει, ο τελικός χρήστης, θα πρέπει να επιλέξει την ένδειξη **«Ενεργοποίηση (Activate)»**.



The image shows a mobile app interface for 'Lookout FOR WORK'. At the top, there is a logo consisting of a green and yellow fan-like shape above the text 'Lookout FOR WORK'. Below the logo, the text 'Please enter your activation code' is displayed. Underneath this is a text input field labeled 'Activation Code' with a question mark icon to its right. Below the input field is a large, dark blue button labeled 'ACTIVATE'. Below the button is the word 'or'. Below 'or' are two white buttons: 'Sign in with Microsoft' (with the Microsoft logo) and 'Sign in with Google' (with the Google logo). At the bottom, there is a small line of text: 'By clicking the button above to activate your account, you agree to Lookout's [Terms of Service](#). In addition, you can view our [Privacy Notice](#).'

Στη συνέχεια, ο τελικός χρήστης, καλείται να εισάγει το email του, το οποίο και θα είναι το βασικό αναγνωριστικό της συσκευής του. Για να προχωρήσει στο επόμενο βήμα, ο τελικός χρήστης θα πρέπει να επιλέξει την ένδειξη «OK»



Στις συσκευές Android, είναι απαραίτητο, να γίνει αποδοχή των ρυθμίσεων «Αποθήκευσης (Storage)», «Ειδοποιήσεων (Notifications)», «Τοποθεσίας (Location)» και «Μηνυμάτων (SMS)» και «Επαφών (Contacts)».

Για να προχωρήσει στην αποδοχή και ενεργοποίηση αυτών των ρυθμίσεων, ο τελικός χρήστης, θα πρέπει να επιλέξει την ένδειξη «Continue (Συνέχεια)».



Please allow the following permissions to
enable full protection



Storage

Allow Lookout to analyze files on your device for threats.

*** We don't store any of your files or share them with your employer.**



Notification

Allow Lookout to send important and up to date information about the security of your device.



Location

For Lookout to provide full network security, allow background access to your location by tapping "While using the app" when prompted for the lo...

*** We don't collect your location or share it with your employer.**

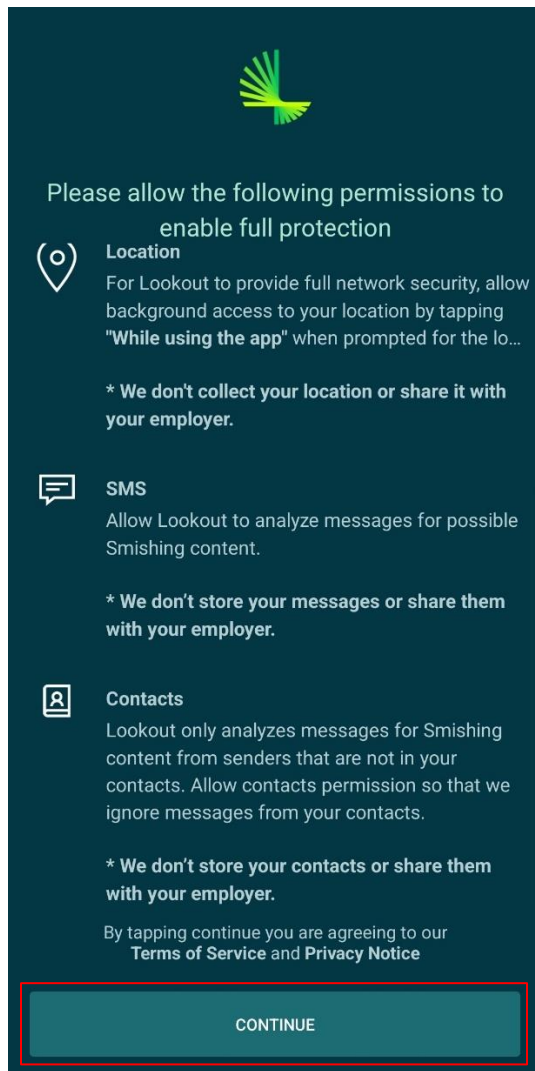


SMS

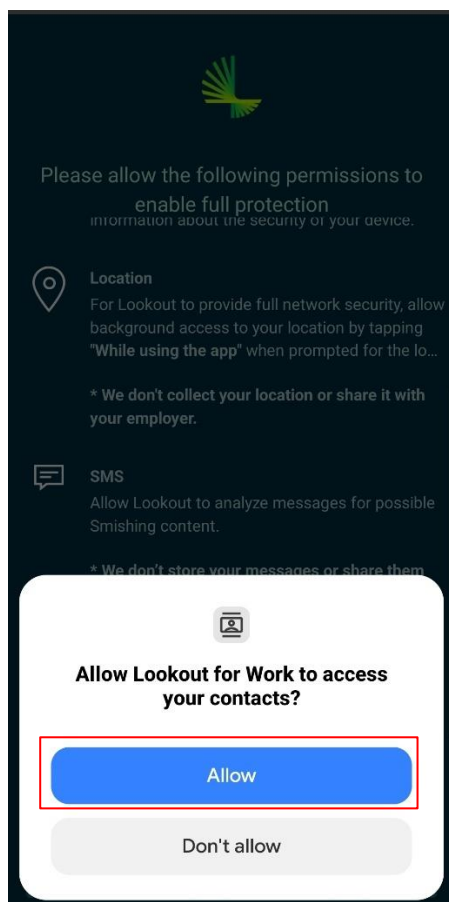
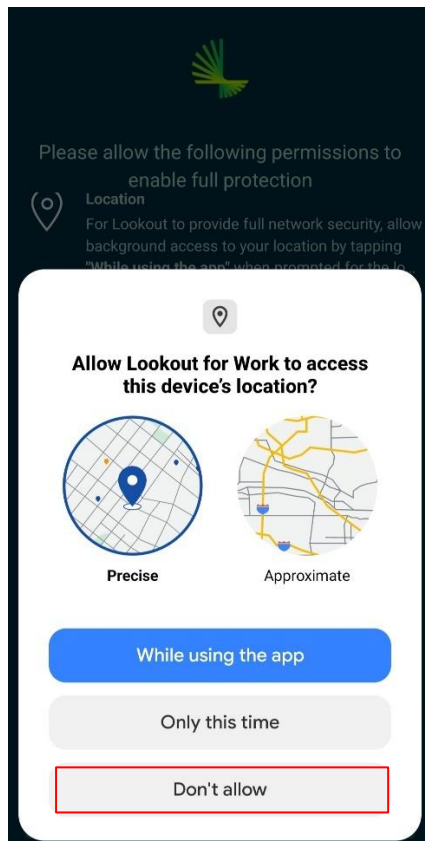
By tapping continue you are agreeing to our
Terms of Service and **Privacy Notice**

CONTINUE





Και για τις πέντε (5) επιλογές, θα ανοίξουν αναδυόμενα (pop-up) παράθυρα, τα οποία θα πρέπει να αποδεχτεί ο τελικός χρήστης, επιλέγοντας τις αντίστοιχες ενδείξεις που εμφανίζονται σε μπλε πλαίσιο και δίνουν άδεια στο λογισμικό να έχει πρόσβαση στις εν λόγω ρυθμίσεις. Ο χρήστης, δεν θα μπορέσει να ολοκληρώσει την εγκατάσταση της άδειας αν δεν αποδεχτεί όλα τα παράθυρα.





All files access

Allow access to manage all files



Allow this app to read, modify and delete all files on this device or any connected storage volumes. If granted, app may access files without your explicit knowledge.

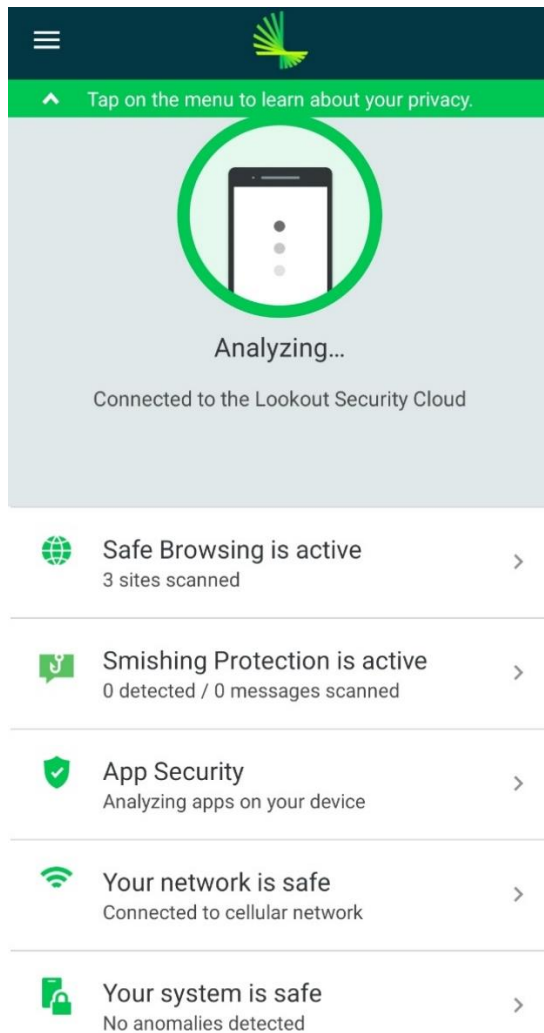
3. Χρήση Εφαρμογής Lookout for Work

Μέσω της εφαρμογής **Lookout for Work** και εφόσον ο τελικός χρήστης έχει ολοκληρώσει την ενεργοποίηση της άδειας του, θα μπορεί να βλέπει σε πραγματικό χρόνο κατά πόσο ασφαλής είναι η κινητή συσκευή του. Η εφαρμογή, **λειτουργεί 24/7 στο παρασκήνιο**, διατηρώντας τη συσκευή του τελικού χρήστη ασφαλή, ανά πάσα στιγμή.

Ο τελικός χρήστης, μπορεί να δει στοιχεία σχετικά με την ασφάλεια περιεχομένου και περιήγησης, την ασφάλεια των εφαρμογών του, την ασφάλεια του δικτύου στο οποίο έχει συνδεθεί καθώς και την ασφάλεια του λειτουργικού συστήματος της συσκευής.

Στα στιγμιότυπα που φαίνονται παρακάτω, μπορείτε να δείτε την κεντρική οθόνη της εφαρμογής Lookout for Work, όπως φαίνεται σε κινητές συσκευές Apple και Android, αντίστοιχα.





Support Links & Supporting Documentation

- [Lookout Mobile Security Συχνές Ερωτήσεις \(FAQs\) \(GR\)](#)
- [Lookout Videos για τις Πολιτικές & Ρυθμίσεις Προστασίας \(ENG\)](#)
- [Lookout Admin Account Demo Walkthrough \(ENG\)](#)
- [Υποστήριξη & Επικοινωνία Εταιρικών Πελατών Vodafone Business \(GR\)](#)



vodafone
business

Together we can