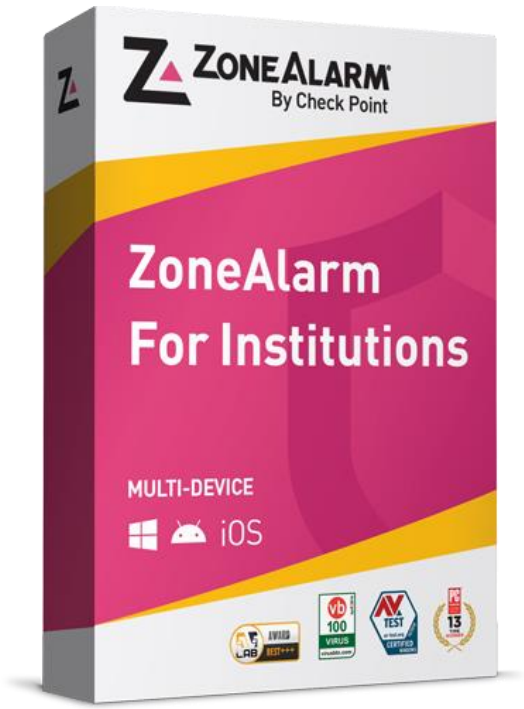
ZoneAlarm
For Institutions

Οδηγίες χρήσης για PC, Android και iOS Συσκευές



Περιεχόμενα

Οδηγός χρήσης υπολογιστή

Οφέλη Προϊόντος

Μεταφρασμένο στα Ελληνικά
Όλα τα μενού και τα περιεχόμενα της εφαρμογής είναι πλήρως μεταφρασμένα στα Ελληνικά.

Προηγμένο τείχος προστασίας (Advanced Firewall)
Το ZoneAlarm for Institutions παρακολουθεί συμπεριφορές στον υπολογιστή σας για εντοπισμό και διακοπή ακόμη και των πιο εξελιγμένων νέων επιθέσεων που παρακάμπτουν τις παραδοσιακές σουίτες προστασίας από ιούς και ασφαλείας

AV επόμενης γενιάς
Το επόμενης γενιάς Antivirus του ZoneAlarm for Institutions χρησιμοποιεί αναστολείς συμπεριφοράς και ευρετική ανάλυση για τον εντοπισμό και την άρση των κακόβουλων λογισμικών, Spyware, Keystrokes loggers, Trojans, Rootkits, κλπ.

Anti-Phishing
Προστατεύει τις συσκευές σας σε πραγματικό χρόνο από νέες και άγνωστες επιθέσεις ηλεκτρονικού "ψαρέματος", με χρήση στατικών και δυναμικών τεχνικών μηχανικής μάθησης(machine learning).

Ασφαλής περιήγηση
Η Ελληνική έκδοση του Zone Alarm for Institutions προστατεύει από κακόβουλους ιστότοπους και διατίθεται με αυτόματα προεγκατεστημένη την ρύθμιση πρόσβασης (URL filtering) σε όλες τις υποστηριζόμενες εφαρμογές περιήγησης (Edge, Chrome, Firefox) αποκλείοντας ακατάλληλο περιεχόμενο.

Ανάλυση απειλών σε πραγματικό χρόνο
Η ZoneAlarm αξιοποιεί τη μεγαλύτερη βάση δεδομένων πληροφοριών για απειλές στον κόσμο, με το Check Point Threat Cloud.

Ασφάλεια κατά τη χρήση
Εντοπίζει κακόβουλα λογισμικά, κακόβουλες εφαρμογές και μη ασφαλή δίκτυα. Σταματά το ηλεκτρονικό ‘’ψάρεμα’’, τα λογισμικά υποκλοπής spyware και αλλά και τα bots από την “κατάληψη” της κάμερας και του μικροφώνου της συσκευής σας.

Προστασία προσωπικών δεδομένων
Η ZoneAlarm Extreme Security εγγυάται ότι τα δεδομένα σας παραμένουν εντελώς απόρρητα. Όλες οι αναλύσεις ασφαλείας πραγματοποιούνται στη συσκευή με ανώνυμα metadata που συλλέγονται από το λειτουργικό σύστημα, τις εφαρμογές και τα δίκτυα.

Αντι-Λυτρισμική Προσταστία
Εντοπίζει, αποκλείει και καταργεί επιθέσεις ransomware και επαναφέρει κρυπτογραφημένα αρχεία, χρησιμοποιώντας τεχνολογίες που βασίζονται σε συμπεριφορά και δεν βασίζονται σε ενημερώσεις υπογραφής (signature updates).

Ασφαλής περιήγηση για παιδιά
Η ZoneAlarm συνοδεύεται από ένα ενσωματωμένο φίλτρο περιεχομένου που τα παιδιά σας δεν μπορούν να απενεργοποιήσουν ή να αλλάξουν. Επιτρέπει στα παιδιά σας να έχουν πρόσβαση στο διαδίκτυο με ασφάλεια σε όλα τα προγράμματα περιήγησης και τις πλατφόρμες.

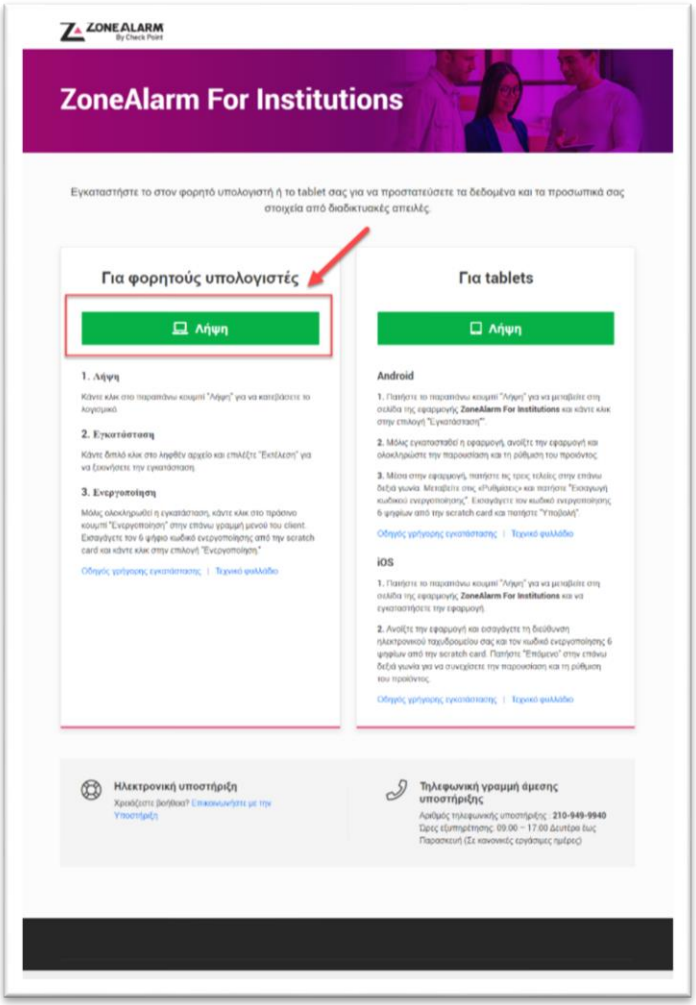
Απαιτήσεις συστήματος

Microsoft Windows 10 Όλες οι εκδόσεις 32-bit / 64-bit, 2 GB RAM 2 GHz ή ταχύτερος επεξεργαστής 1,5 GB διαθέσιμου χώρου στον σκληρό δίσκο **Microsoft .NET framework** Έκδοση 3.5 ή νεότερη
Επεκτάσεις προγράμματος περιήγησης
Google Chrome, Microsoft Edge, Mozilla Firefox

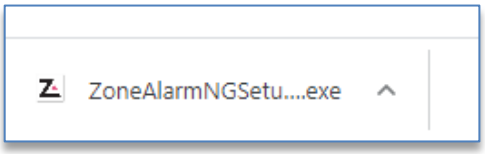
1. Εγκατάσταση και Ενεργοποίηση PC

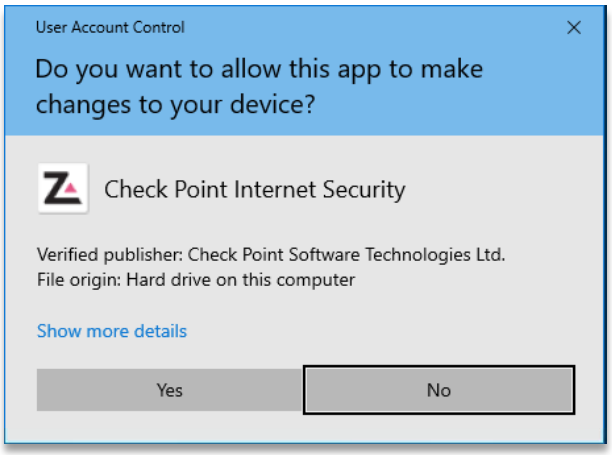
1. Μεταβείτε στη σελίδα λήψης «ZoneAlarm For Institutions» Σελίδα λήψης: https://www.zonealarm.com/gr-card

2. Κάντε κλικ στο πράσινο κουμπί λήψης και κάντε διπλό κλικ στο ληφθέν αρχείο για να ξεκινήσετε την εγκατάσταση.

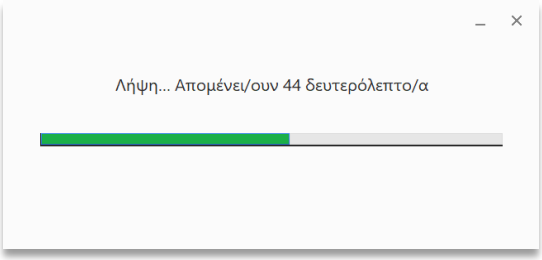


Κάντε διπλό κλικ στο αρχείο .exe που έχετε κατεβάσει και κάντε κλικ στο κουμπί “Yes" στο παράθυρο διαλόγων των Windows για να ξεκινήσετε την εγκατάσταση.

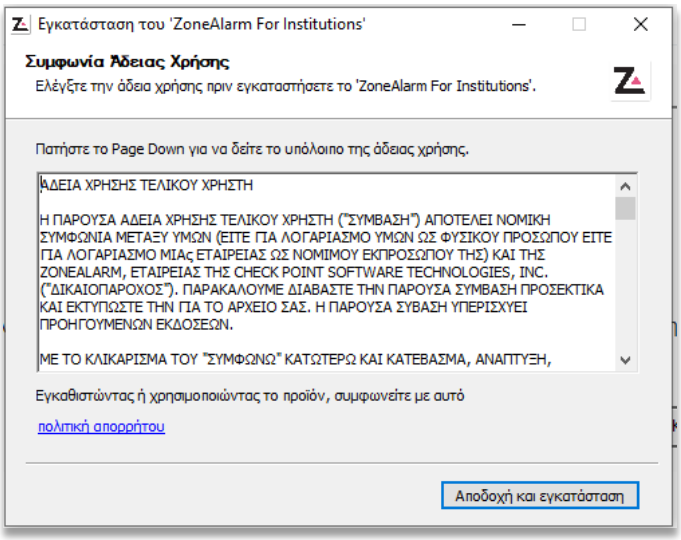




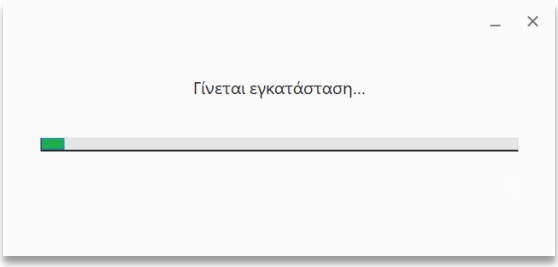
Περιμένετε λίγα λεπτά όσο η εφαρμογή εγκαθίσταται.



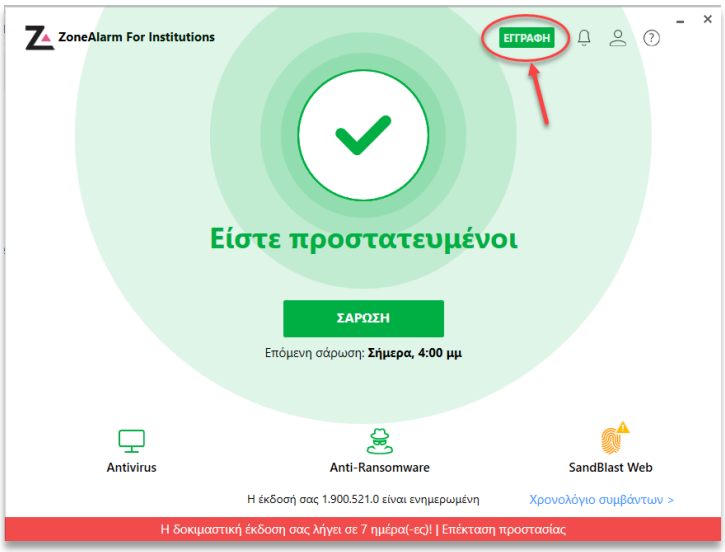
Αποδεχτείτε το ”Άδεια χρήσης τελικού χρήστη”



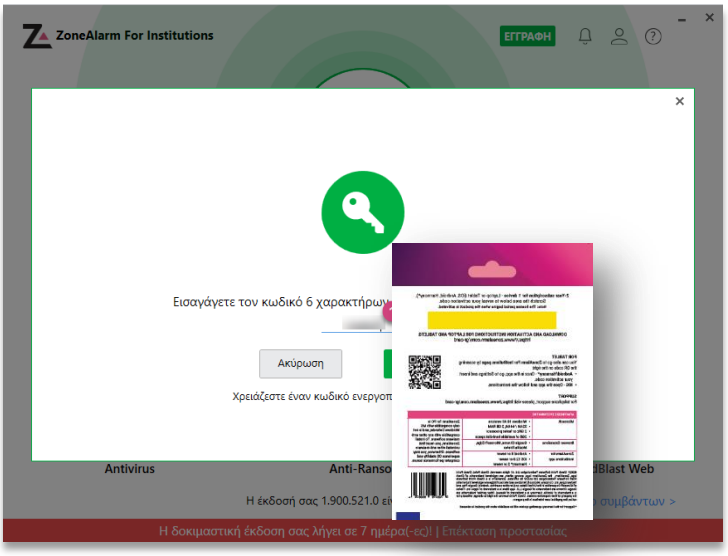
Περιμένετε όσο η εγκατάσταση ολοκληρώνεται...



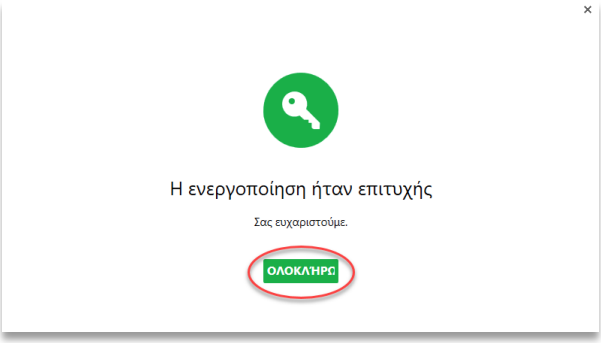
Κάντε κλικ στην επιλογή "ΕΓΓΡΑΦΗ" στην γραμμή μενού.



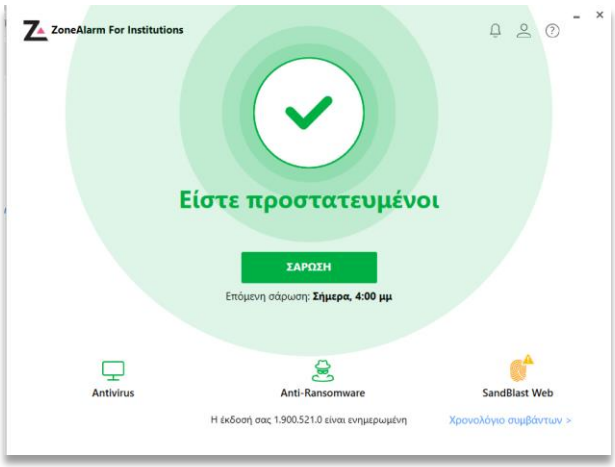
Εισάγετε το κλειδί της άδειας χρήσης από την κάρτα και κάντε κλικ στην επιλογή “ΕΓΓΡΑΦΗ”



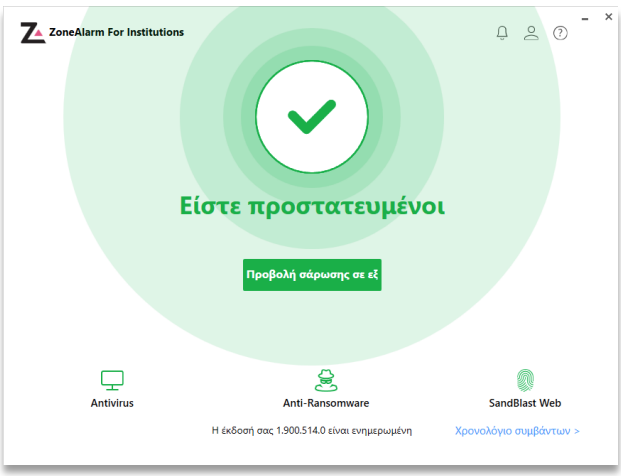
Επιλέξτε “Ολοκλήρωση”



”Sandblast Web” – Οι επεκτάσεις του προγράμματος περιήγησης του ZoneAlarm, θα εγκατασταθούν αυτόματα όταν ανοίξετε ή επανεκκινήσετε το πρόγραμμα περιήγησης(Chrome, Edge and Firefox).



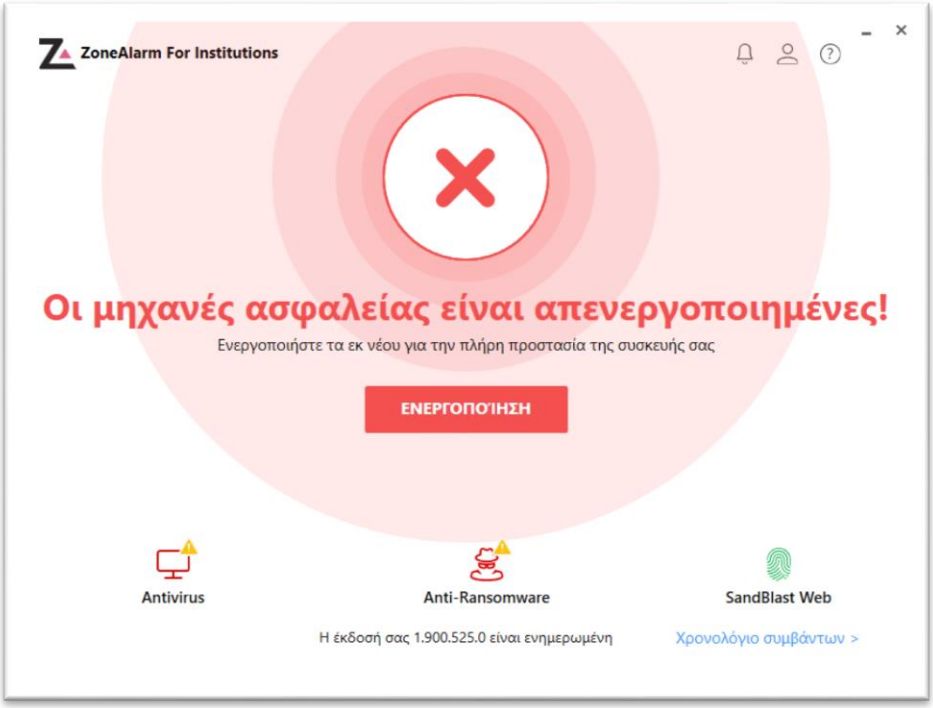
Η συνδρομή σας είναι πλέον ενεργοποιημένη και είστε προστατευμένοι!



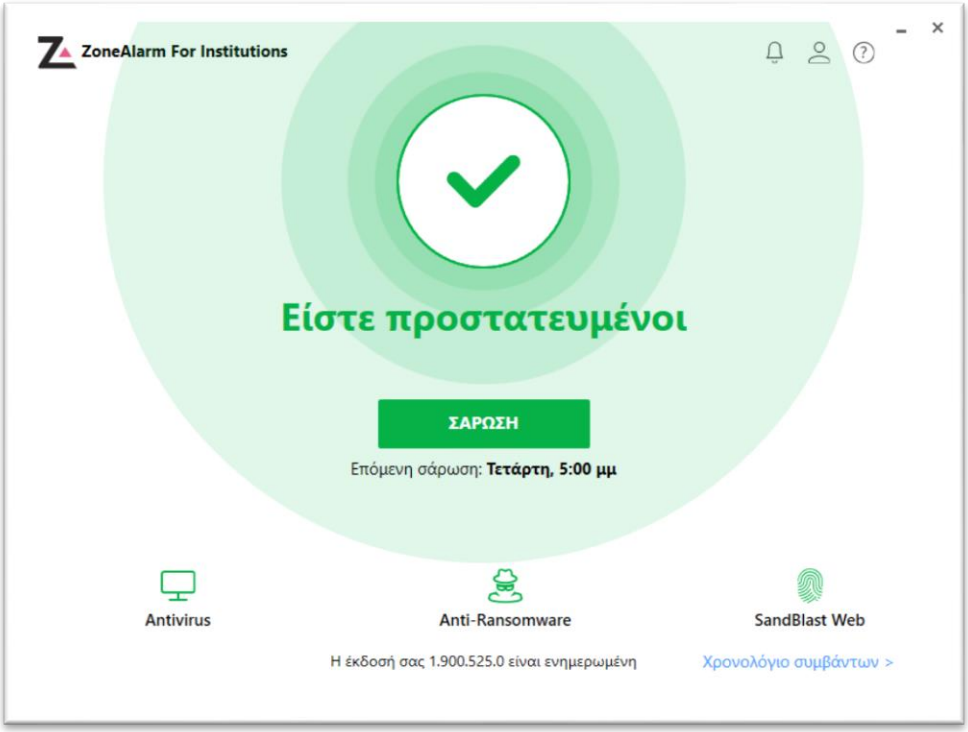
2. Κεντρική Σελίδα Εφαρμογής

Κατά την εκκίνηση του *ZoneAlarm For Institutions*, θα εμφανιστεί η Αρχική σελίδα. Στην Αρχική σελίδα εμφανίζεται η κατάσταση του συστήματός σας και το επίπεδο ασφαλείας στο οποίο βρίσκεται αυτήν τη στιγμή. Τα βήματα για να ασφαλίσετε το σύστημά σας είναι τα εξής:

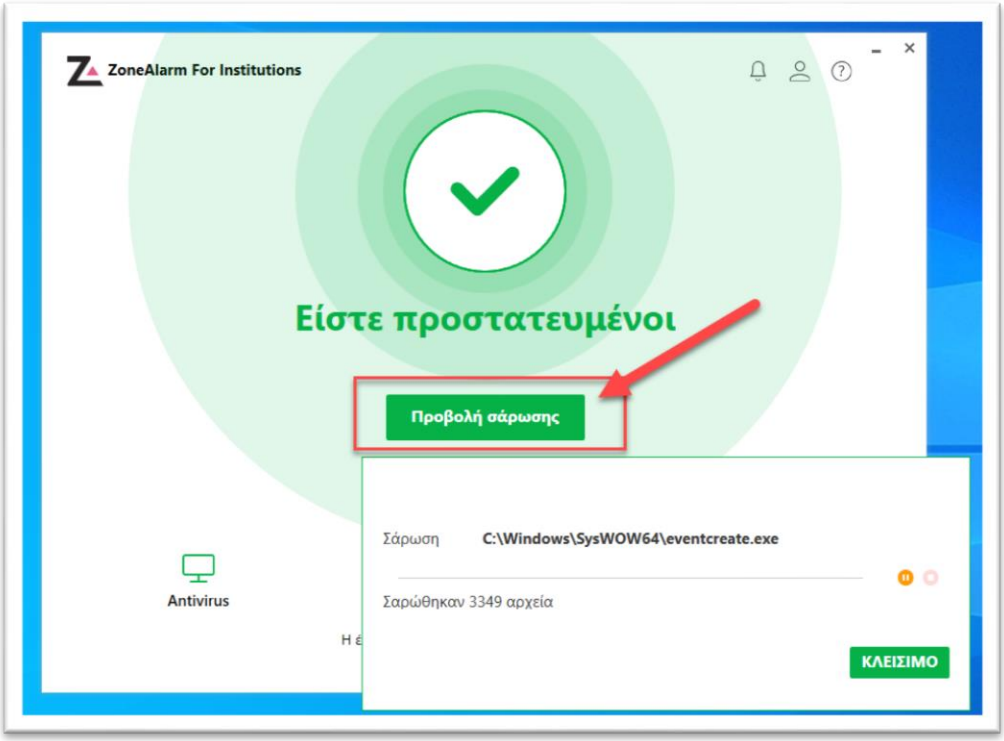
1. Πάντα επιλέγετε το κουμπί **ΕΝΕΡΓΟΠΟΙΗΣΗ** όταν λαμβάνετε την παρακάτω ενημέρωση από το ZoneAlarm For Institutions..



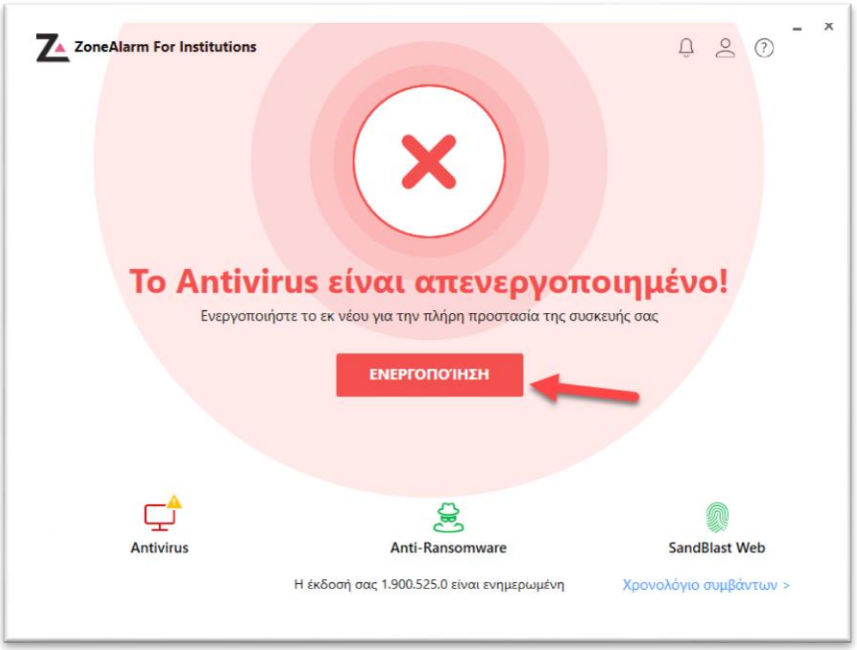
2. Το παρακάτω μήνυμα θα εμφανίζεται όταν δεν υπάρχει κανένα συμβάν και είστε προστατευμένοι. Μπορείτε επίσης να σαρώσετε τη συσκευή σας από την αρχική σελίδα. Επιλέξτε **Σάρωση**.

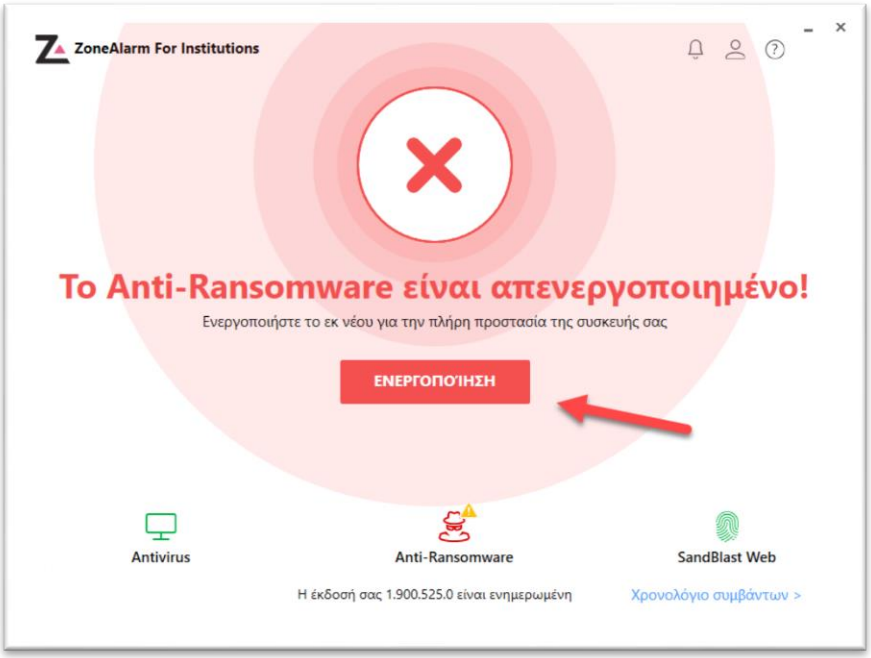


3. Η σάρωση του συστήματος ξεκινάει στο παρασκήνιο. Για να δείτε την πρόοδο της σάρωσης, επιλέξτε την επιλογή **Προβολή σάρωσης.**



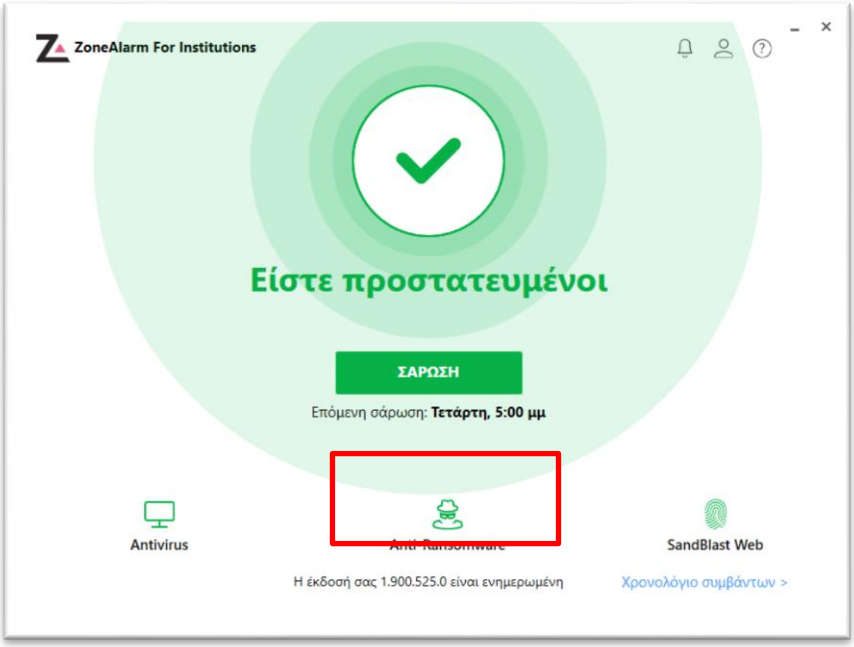
4. Πατήστε το κουμπί ΕΝΕΡΓΟΠΟΙΗΣΗ αν το ZoneAlarm For Institutions σας υποδεικνύει κάποια από τις ακόλουθες εικόνες.



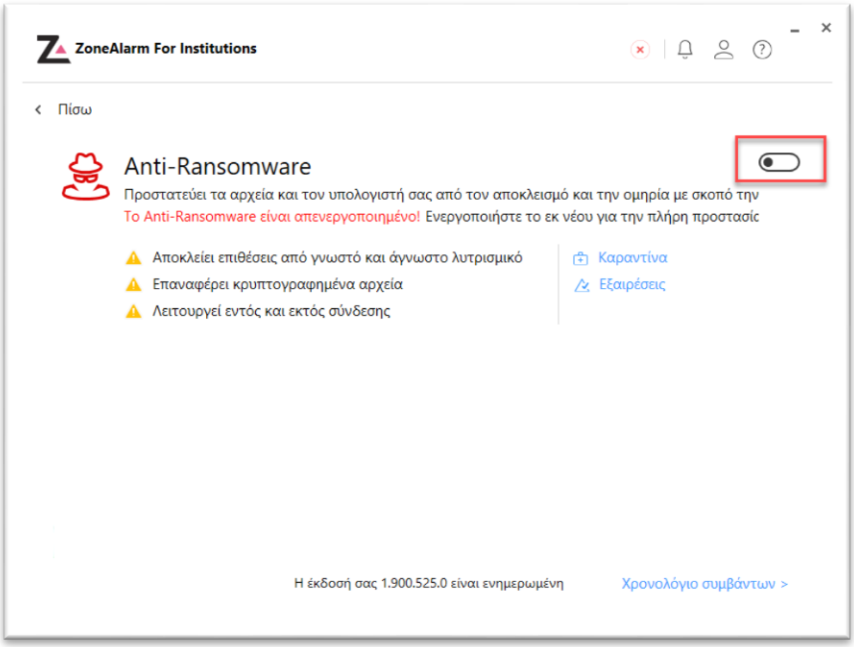


3. Προστασία Anti-Ransomware

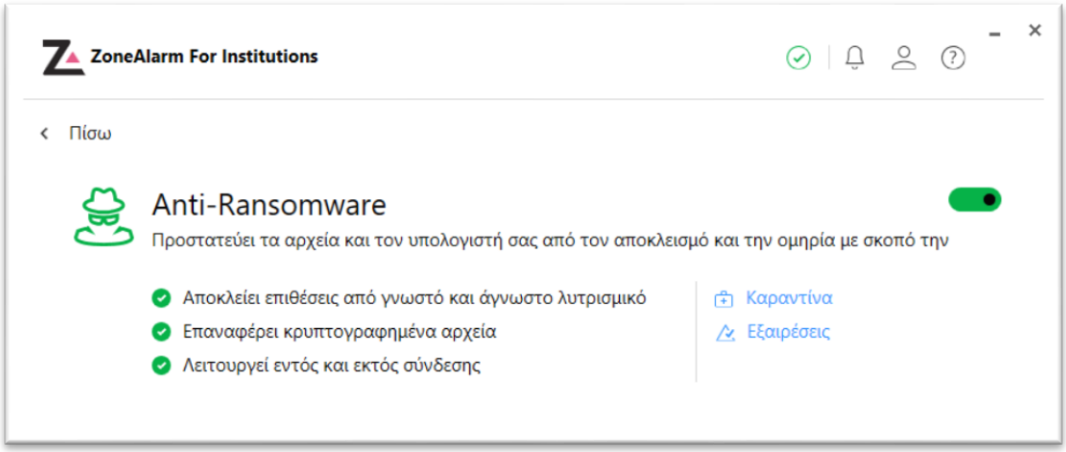
Επιλέξτε το εικονίδιο **Anti-Ransomware**.



Κάντε κλικ στο κουμπί **Εναλλαγής** για να ενεργοποιήσετε ή να απενεργοποιήσετε την προστασία Anti-Ransomware στη συσκευή σας

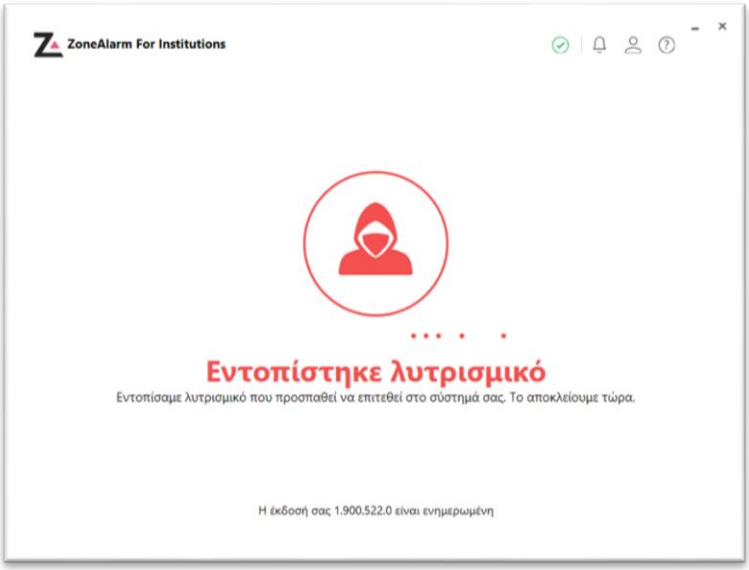


Το Anti-Ransomware είναι τώρα ενεργό.



a. Anti-Ransomware Διαδικασία Ανίχνευσης Συμβάντων

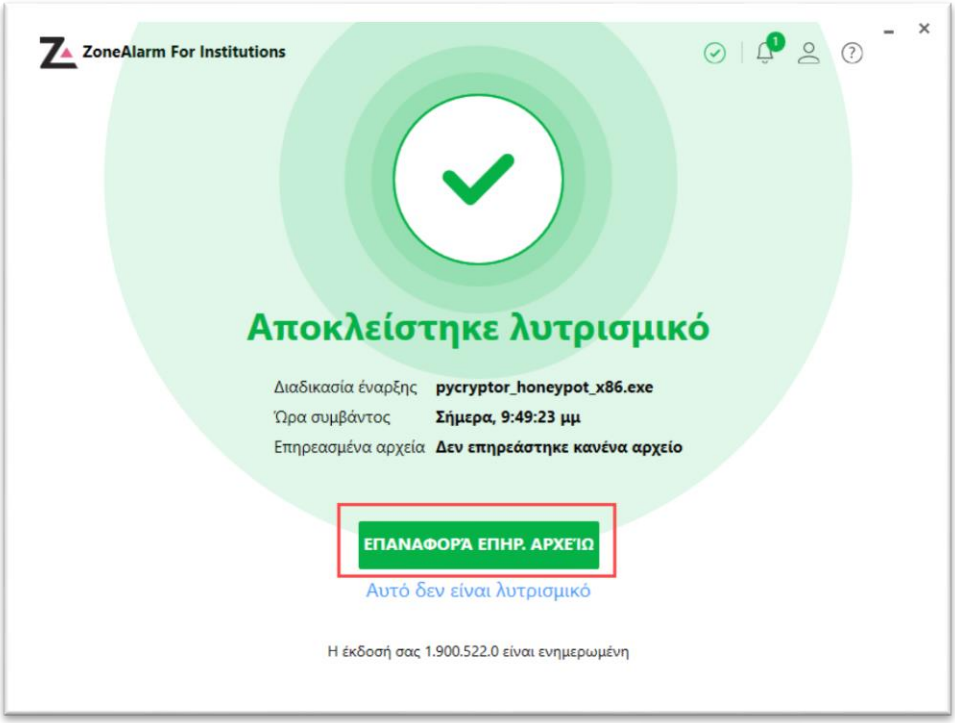
Όταν το Anti-Ransomware είναι ενεργό, το ZoneAlarm For Institutions εντοπίζει και σας ειδοποιεί κάθε φορά που ένα malware ransomware προσπαθεί να επιτεθεί στη συσκευή σας.

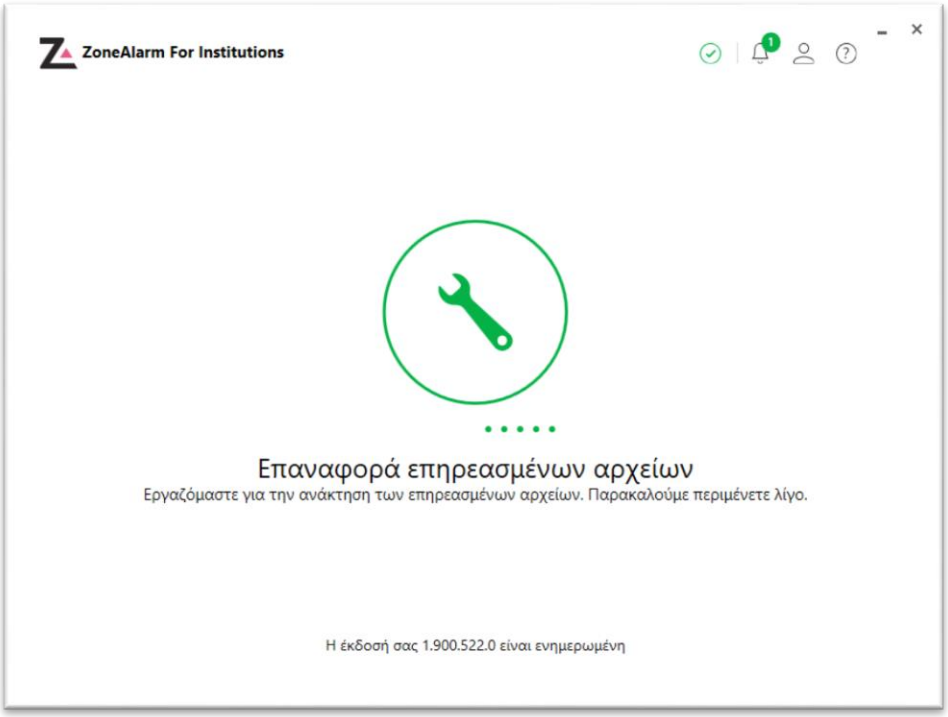


Το ZoneAlarm For Institutions θα αποκλείει αυτόματα τη συγκεκριμένη επίθεση. Βοηθά επίσης στην ανάκτηση των αρχείων σας εάν κάποια έχουν ήδη προλάβει να κρυπτογραφηθούν, και επαναφέρει το σύνστημα στην ασφαλή κατάσταση στην οποία βρισκόταν πριν δεχθείτε την επίθεση ransomware.

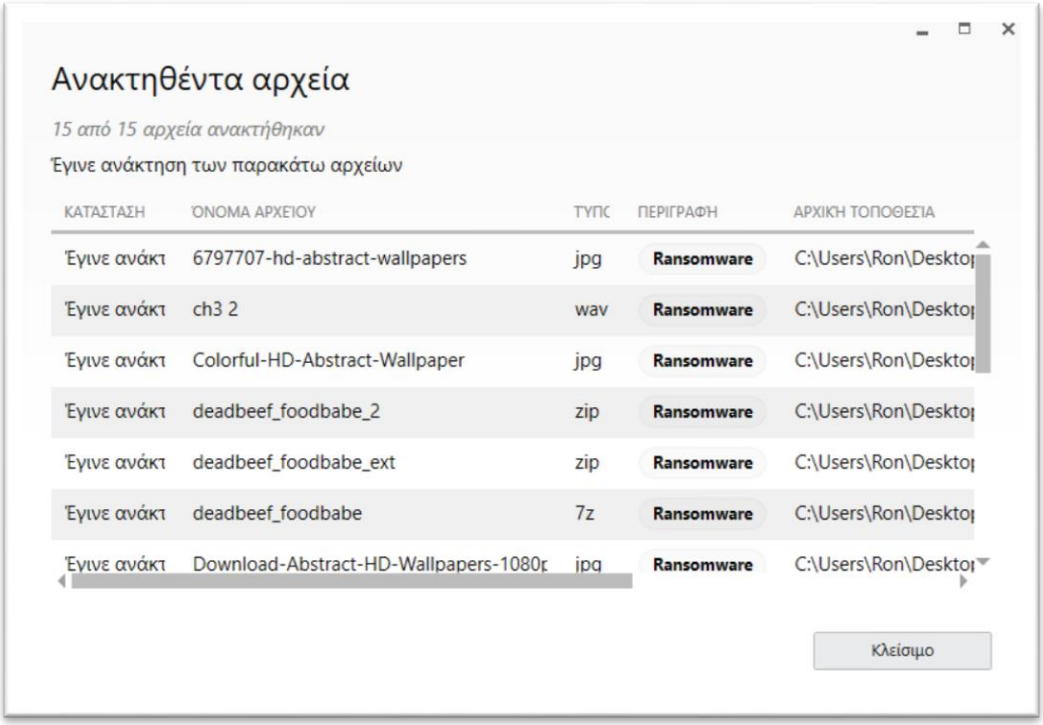
Επιλέξτε Ε**παναφορά Επηρεασμένων Αρχείων**.

Η διαδικασία ανάκτησης των αρχείων ξεκινά στο παρασκήνιο και θα δείτε το ακόλουθο μήνυμα.



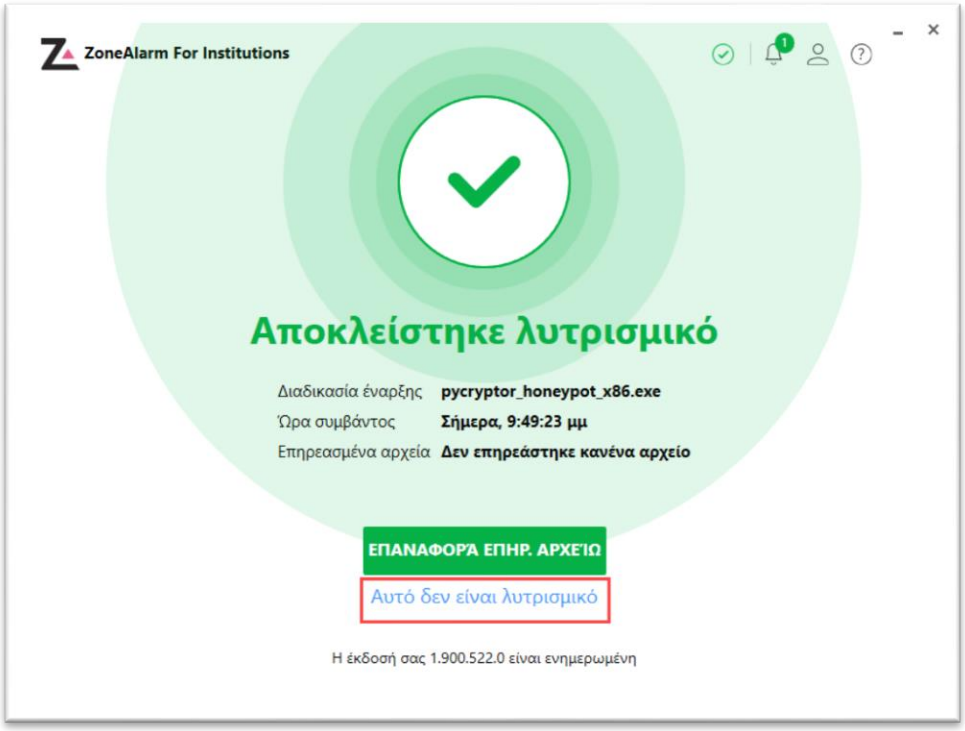


Η λίστα των **Ανακτηθέντων Αρχείων** εμφανίζεται σε πίνακα.



b. Ψευδώς θετικός εντοπισμός Ransomware / λυτρισμικό

Επιλέξτε *"Αυτό δεν είναι λυτρισμικό"* αν είστε σίγουροι ότι εμπιστεύεστε το συγκεκριμένο αρχείο και την πηγή που το λάβατε προκειμένου να το εξαιρέσετε από την Anti-Ransomware προστασία.



Το αρχείο θα αποκατασταθεί και θα επισημανθεί ως εξαίρεση, ώστε να μην εντοπιστεί ξανά.

Να είστε πολύ προσεκτικοί όταν χρησιμοποιείτε αυτήν την επιλογή, επειδή θα μπορούσατε να επαναφέρετε το λυτρισμικό που έχει μεταμφιεστεί αλλάζοντας το όνομα αρχείου του!

c. Περίπτωση Ransomware Επίθεσης / Λυτρισμικό

Ας δούμε τώρα μία περίπτωση επίθεσης Λυτρισμικού και πώς το ZoneAlarm For Institutions βοηθά στον αποκλεισμό του Λυτρισμικού και στην ανάκτηση των αρχείων.

Δείτε τον παρακάτω σύνδεσμο στο Youtube:
https://www.youtube.com/watch?v=oaG_6fOR44w

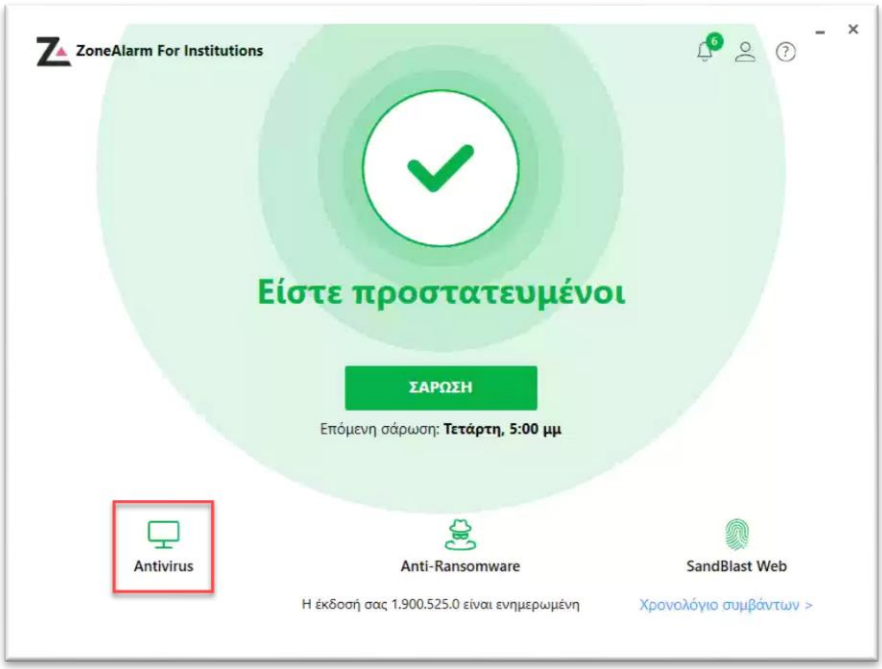
4. AntiVirus

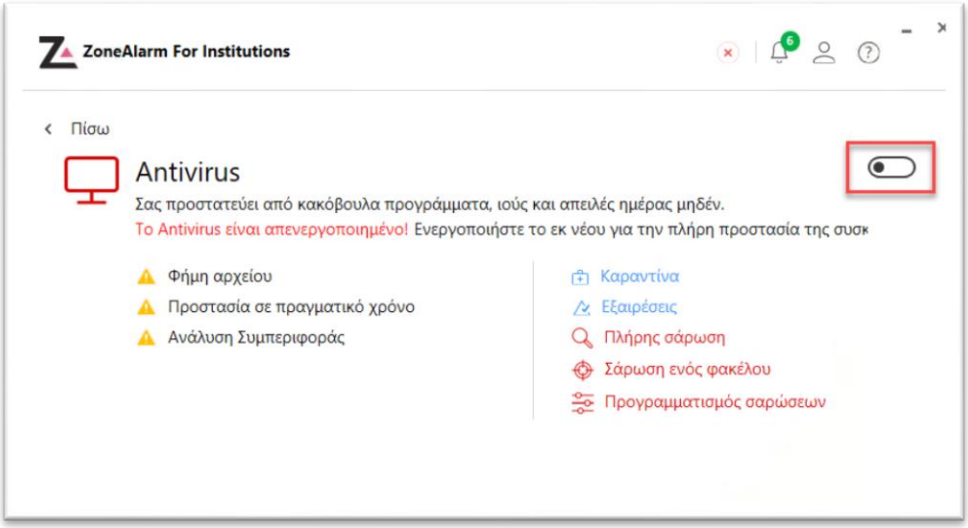
Το ZoneAlarm For Institutions είναι ένα ολοκληρωμένο πολυεπίπεδο λογισμικό ασφαλείας που σταματά τους πιο εξελιγμένους ιούς και χάκερ. Είναι η απόλυτη λύση για την ψηφιακή σας ασφάλεια για να διασφαλίσετε ότι είστε 100% προστατευμένοι.

Πως λειτουργεί το ZoneAlarm Antivirus

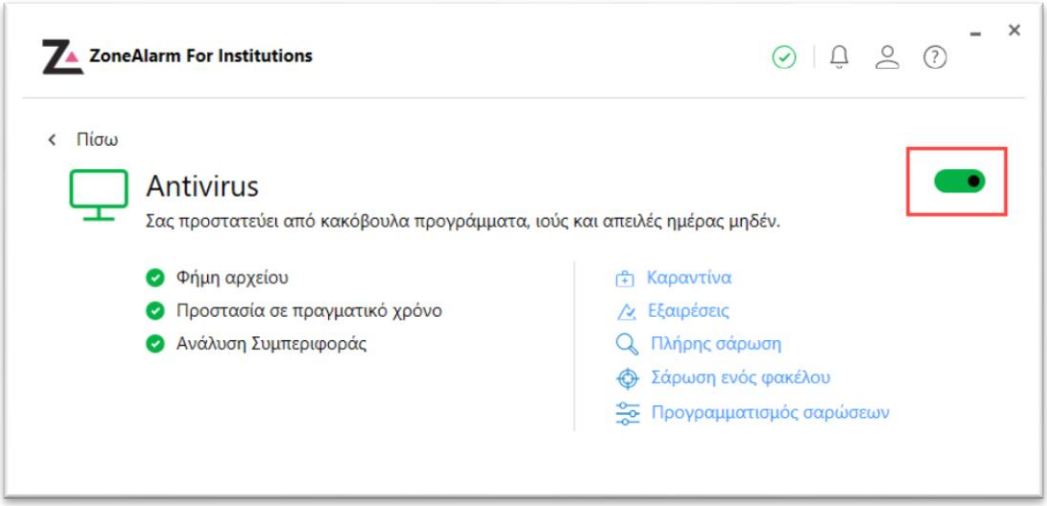
Εντοπίζει και αφαιρεί ιούς, λογισμικά υποκλοπής spyware, Trojans , worms υπολογιστή, bots και πολλά άλλα είδη ιών. Δοκιμασμένο από ανεξάρτητους φορείς για την παροχή ανώτατης προστασίας.
Οι λειτουργίες σάρωσης σάς επιτρέπουν να προσαρμόσετε την προστασία σας.
Ελέγχει τα αρχεία μέσω μιας Cloud-based βάσης δεδομένων σε πραγματικό χρόνο για να διασφαλίσει ότι δεν θα αποσιωπηθούν ακόμη και οι νεότερες απειλές.

Πατήστε το εικονίδιο **Antivirus**.





Για να το ενεργοποιήσετε τη συγκεκριμένη προστασία, στη σελίδα Antivirus πατήστε το κουμπί **Εναλλαγής.**

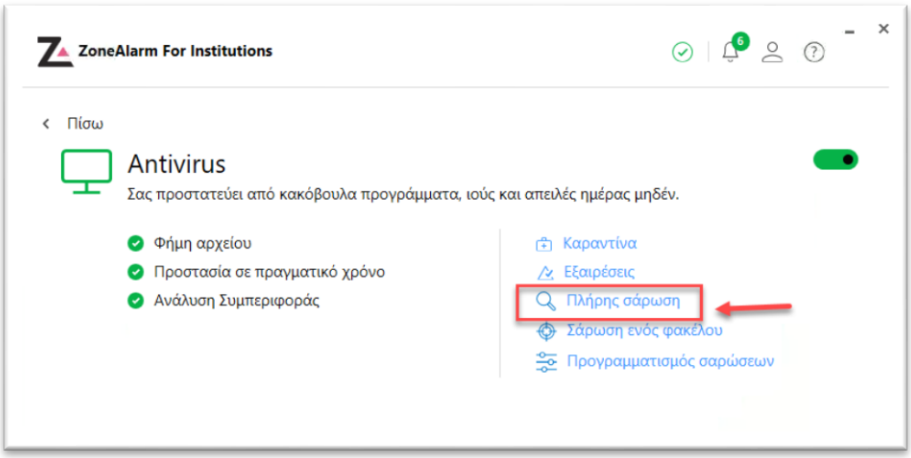


Το ZoneAlarm For Institutions είναι ενεργοποιημένο.

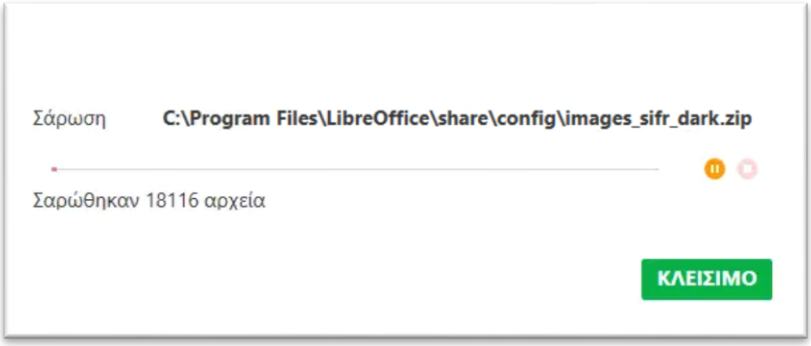
a. Πλήρης Σάρωση

Η επιλογή "Πλήρης σάρωση" σαρώνει όλα τα αρχεία και τους φακέλους του συστήματος. Τα βήματα για την εκτέλεση μιας πλήρους σάρωσης είναι τα εξής:

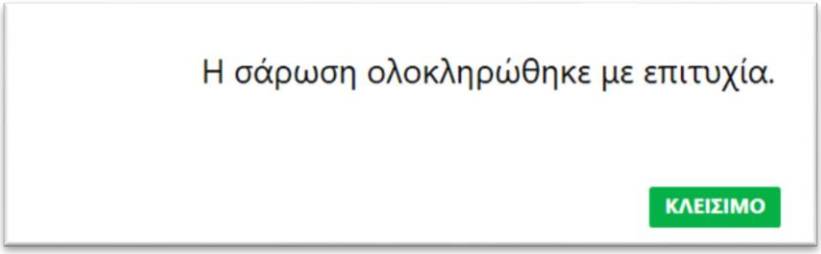
1. Στην καρτέλα **Antivirus**, πατήστε **Πλήρης Σάρωση**.



2. Θα εμφανιστεί μια πρόοδος σάρωσης στην οθόνη που θα εμφανίζει τα αρχεία και τους φακέλους που σαρώνονται. Συνιστάται να μην κλείσετε και να ακυρώσετε τη σάρωση όταν αυτή βρίσκεται σε εξέλιξη και ειδικότερα κατά την πρώτη φορά που διενεργήται η σάρωση μετά την εγκατάσταση.

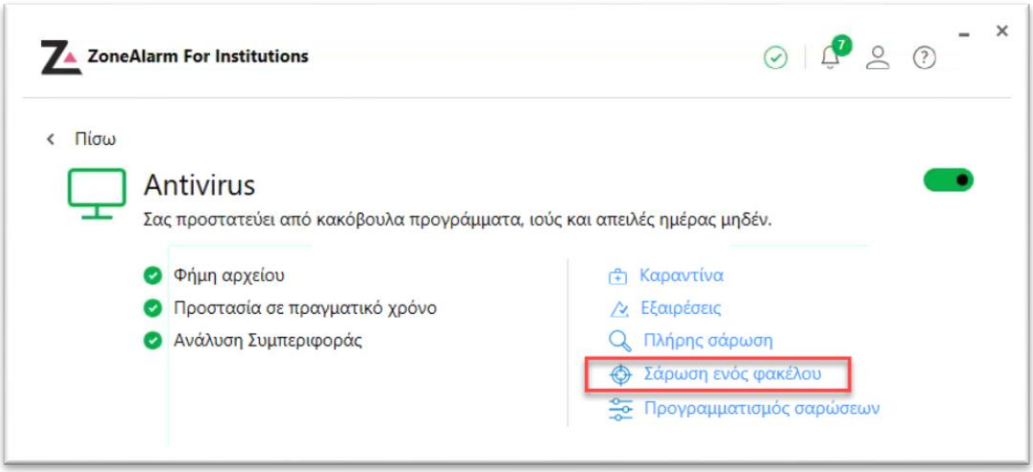


3. Με την ολοκλήρωση της σάρωσης, θα εμφανιστεί μια ειδοποίηση που θα δηλώνει ότι **η σάρωση ολοκληρώθηκε με επιτυχία**.

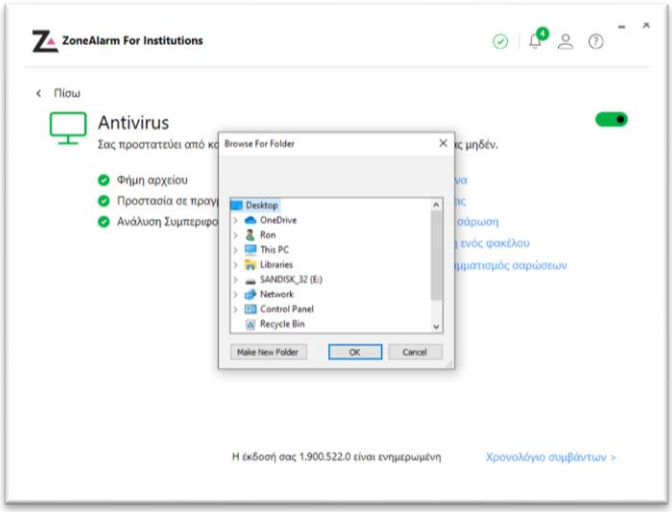


b. Σάρωση ενός φακέλου

Το ZoneAlarm For Institutions επιτρέπει την εκτέλεση της σάρωσης για συγκεκριμένους φακέλους, σύμφωνα με τις απαιτήσεις σας. Επιλέξτε την επιλογή **Σάρωση φακέλου** στην καρτέλα "Antivirus".

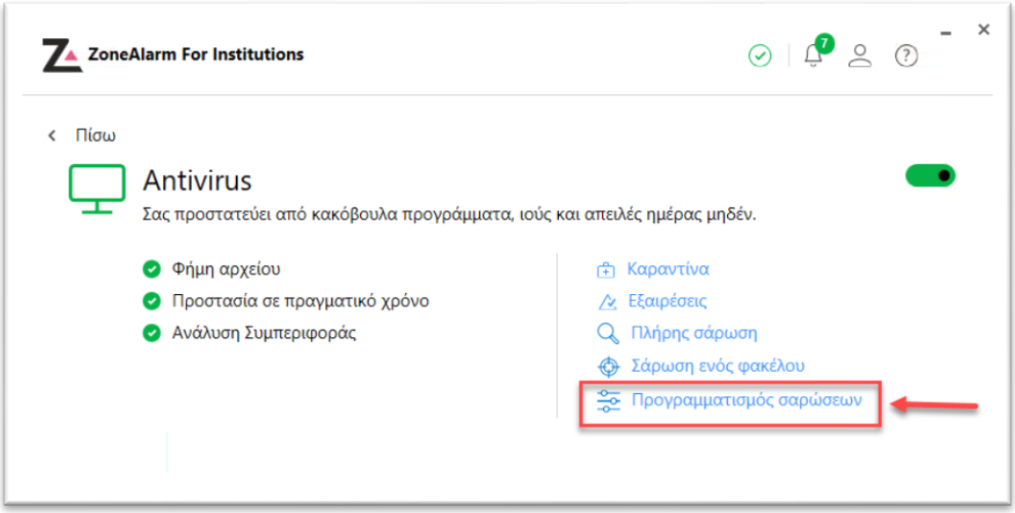


Οι φάκελοι που πρέπει να σαρωθούν μπορούν να επιλεγούν από την αναδυόμενη οθόνη και μπορεί να γίνει μια σάρωση γι' αυτούς.

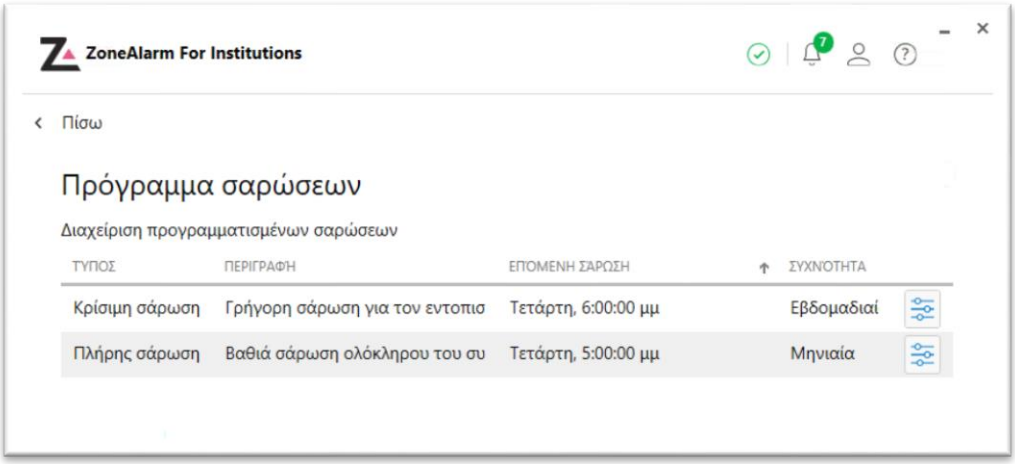


c. Προγραμματισμός σαρώσεων

Οι σαρώσεις μπορούν να προγραμματιστούν σε μια επιθυμητή χρονική συχνότητα για επαναλαμβανόμενες σαρώσεις. Για να δείτε τις προγραμματισμένες σαρώσεις, επιλέξτε **Προγραμματισμός σαρώσεων**.

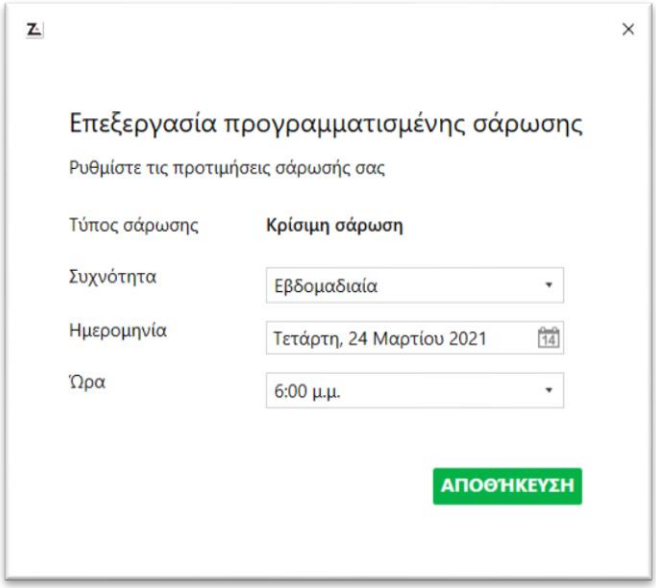


Θα εμφανιστεί μια λίστα σαρώσεων. Η σελίδα "**Προγραμματισμός σαρώσεων**" εμφανίζει τον τύπο σάρωσης, την περιγραφή της και τον επόμενο προγραμματισμό σάρωσης μαζί με τη συχνότητα.



Για να επεξεργαστείτε ένα χρονοδιάγραμμα, επιλέξτε το εικονίδιο **Edit**

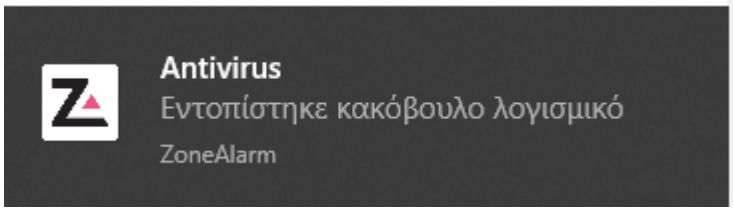
Θα εμφανιστεί ένα αναδυόμενο παράθυρο "**Προγραμματισμός σάρωσης**" στην οθόνη. Αλλαγές όπως ο ορισμός συχνότητας (ημερήσια, εβδομαδιαία, μηνιαία κ.λπ.) μπορούν να επιλεγούν από την αναπτυσσόμενη λίστα. Η ημερομηνία μπορεί να οριστεί επιλέγοντας μια ημερομηνία από το αναδυόμενο παράθυρο του ημερολογίου. Με παρόμοιο τρόπο, ο χρόνος για τη σάρωση μπορεί επίσης να οριστεί επιλέγοντας τον επιθυμητό χρόνο από την αναπτυσσόμενη λίστα. Επιλέξτε **Αποθήκευση** για να αποθηκεύσετε τις αλλαγές.



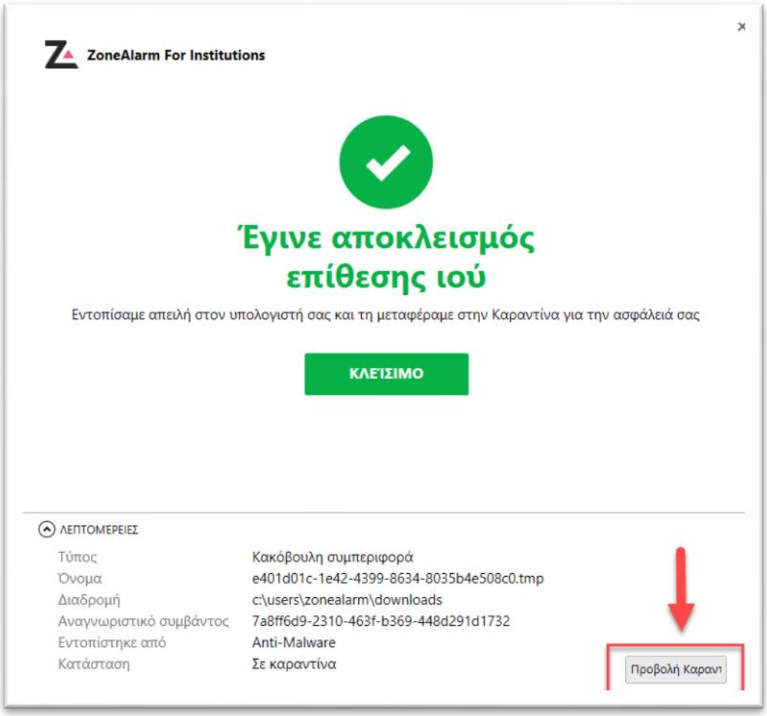
d. Antivirus (Anti-Malware) Διαδικασία ανίχνευσης συμβάντων

Η διαδικασία που θα ακολουθηθεί κατά τον εντοπισμό ενός κακόβουλου λογισμικού φαίνεται σε αυτή την ενότητα.

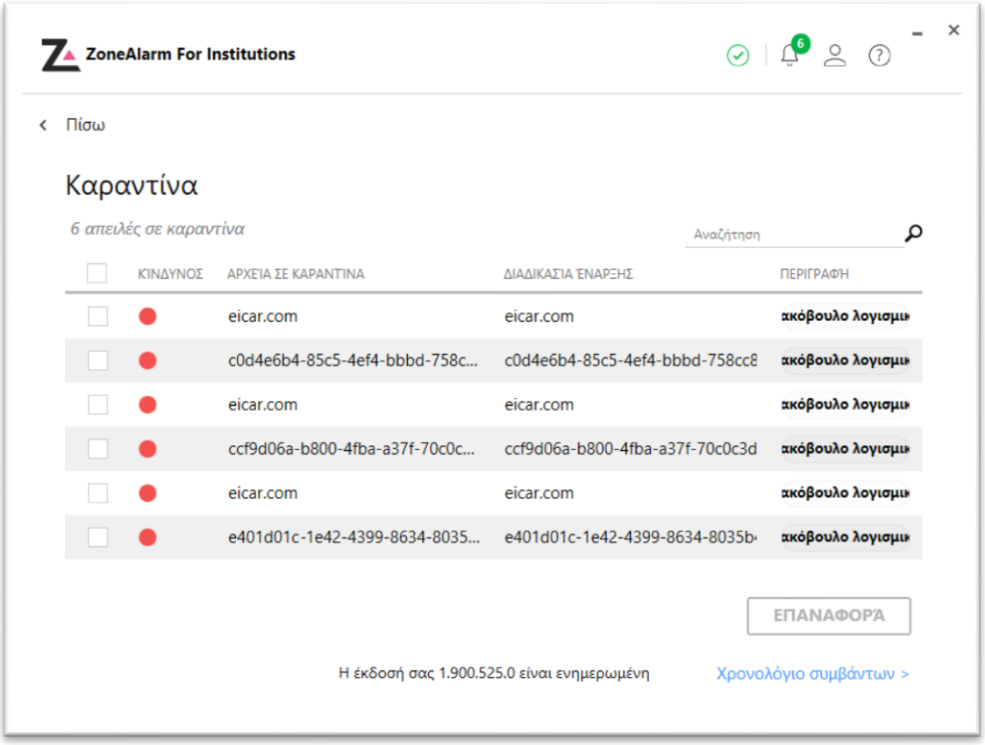
1. **Εντοπισμός κακόβουλου λογισμικού:** Κατά τον εντοπισμό κακόβουλου λογισμικού, εμφανίζεται μια ειδοποίηση από το ZoneAlarm For Institutions.



2. **Έγινε αποκλεισμός επίθεσης ιού**: Στη συνέχεια, τα αρχεία που σχετίζονται με την απειλή μετακινούντε σε καραντίνα και οι λεπτομέρειες που περιγράφουν τον **Τύπο, το Όνομα, τη Διαδρομή,το Αναγνωριστικό συμβάντος** και την **Κατάσταση του συστήματος** μπορούν να προβληθούν με την επέκταση της καρτέλας **Λεπτομέρειες**.

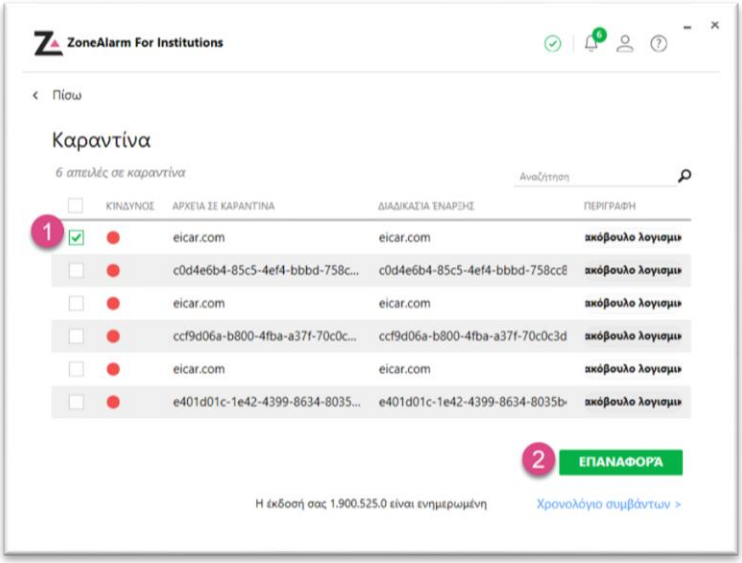


3. **Προβολή καραντίνας**: Για γρήγορη πρόσβαση στο φάκελο Καραντίνα, πατήστε το κουμπί **Προβολή Καραντίνας**. Αυτός ο φάκελος εμφανίζει όλα τα εντοπισμένα κακόβουλα λογισμικά. Η γραμμή αναζήτησης μπορεί να χρησιμοποιηθεί για την επιλογή ενός συγκεκριμένου αρχείου σε καραντίνα ή μπορούν να επιλεγούν πολλά αρχεία για την εκτέλεση περαιτέρω ενεργειών.

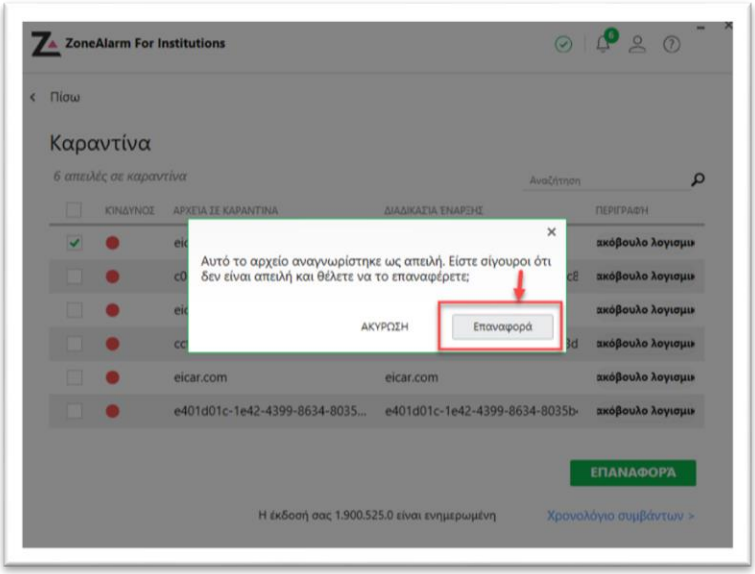


e. Αναφορά ψευδών θετικών μολύνσεων και επαναφορά αρχείων

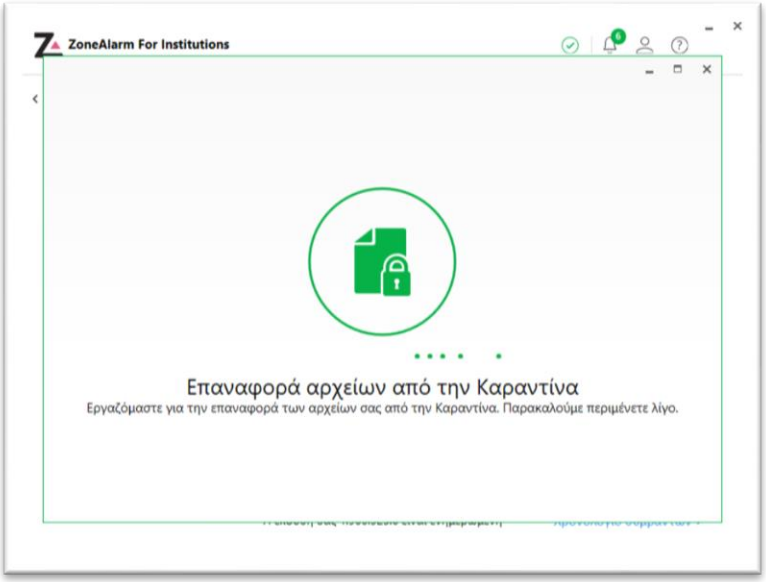
Όταν το ZoneAlarm For Institutions υποπτεύεται ένα μολυσμένο αρχείο στον Υπολογιστή σας, βάζει το αρχείο σε καραντίνα. Η επαναφορά των αρχείων σε καραντίνα μπορεί να συμβεί εάν τα αρχεία έχουν ληφθεί από αξιόπιστη πηγή και αναφέρονται ψευδώς ως Θετικά.
Για να κάνετε επαναφορά ενός αρχείου από την Καραντίνα που πιστεύετε ότι προέρχεται από αξιόπιστη πηγή, επιλέξτε το αρχείο και, στη συνέχεια, πατήστε το κουμπί **Επαναφορά**.



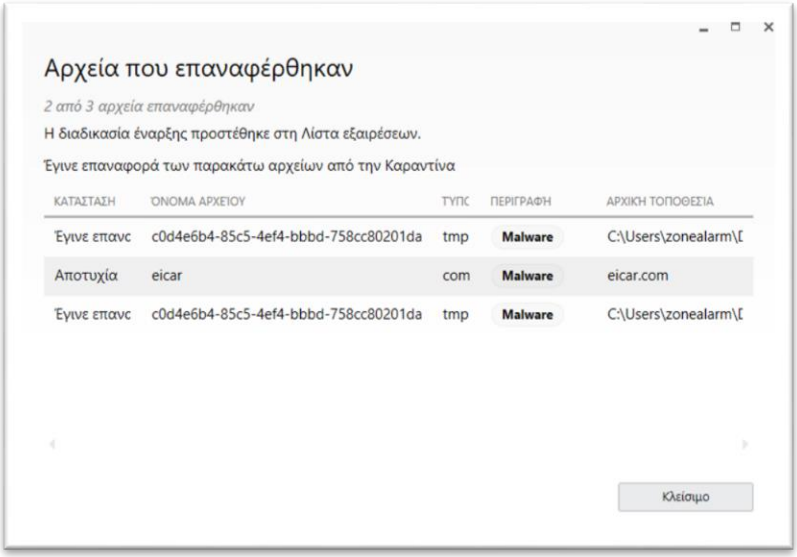
Στο αναδυόμενο παράθυρο, πατήστε **Επαναφορά** για επιβεβαίωση.



Ξεκινά η διαδικασία επαναφοράς για το επιλεγμένο αρχείο.



Μετά την ολοκλήρωση, θα εμφανιστεί ένα μήνυμα επιβεβαίωσης στην οθόνη που θα αναφέρει την Κατάσταση, το Όνομα Αρχείου, τον Τύπο, την Περιγραφή και την Αρχική Θέση του αρχείου.



Οι δύο ενέργειες που διενεργούνται από το ZoneAlarm For Institutions είναι οι εξής:

1. Η διαδικασία ενεργοποίησης προστίθεται στη λίστα εξαιρέσεων. Αυτό σημαίνει ότι η υπογραφή του αρχείου κρίνεται κατάλληλη για μελλοντικές λήψεις αυτών των ετικετών για παρόμοια αρχεία.
2. Το εν λόγω αρχείο μετακινείται από την καραντίνα στον αρχικό του φάκελο του υπολογιστή.

Αυτή η διαδικασία ακολουθείται και για το Anti-virus και για το Anti-Ransomware.

5. Επεκτάσεις για Chrome/Edge και Firefox Browsers

Το Sandblast Web του ZoneAlarm for Institutions περιλαμβάνει την πιο πρόσφατη πρόληψη νέων απειλών για το πρόγραμμα περιήγησης και τις διαδικτυακές σας δραστηριότητές. Συνοδεύεται από ένα ενσωματωμένο φίλτρο περιεχομένου, το οποίο τα παιδιά σας δεν μπορούν να το απενεργοποιήσουν ή να το αλλάξουν. Οι επεκτάσεις επιτρέπουν στα παιδιά σας να έχουν ασφαλή πρόσβαση στο διαδίκτυο με όλα τα προγράμματα περιήγησης και τις πλατφόρμες.

Πως λειτουργεί το ZoneAlarm Sandblast Web

Anti-Phishing

Το σύστημα θα καθορίσει αν ο ιστότοπος είναι αξιόπιστος ή όχι χρησιμοποιώντας το ThreatCloud™ της CheckPoint, τη μεγαλύτερη βάση δεδομένων απειλών στον κόσμο. Εάν ο ιστότοπος διαπιστωθεί ότι είναι ύποπτος, θα ειδοποιηθείτε αμέσως και θα αποκλειστεί η πρόσβασή σας σε αυτόν.

Κατάργηση απειλών

Η κατάργηση απειλών του ZoneAlarm καταργεί εκμεταλλεύσιμο περιεχόμενο από κοινά αρχεία, όπως Microsoft Word, Excel, PowerPoint, και Adobe PDF. Καταργεί μακροεντολές υψηλού κινδύνου, ενεργά και ενσωματωμένα αντικείμενα και εξωτερικές συνδέσεις που μπορούν να αξιοποιηθούν κακόβουλα για να μολύνουν τους υπολογιστές και τα δίκτυά σας.

Ανακατασκευάζει τα αρχεία σας με γνωστά ασφαλή στοιχεία και σας παρέχει αμέσως ασφαλές περιεχόμενο ή καθαρές εκδόσεις δυνητικά κακόβουλων αρχείων σε μορφή PDF. Εφαρμόζει έναν τύπο ανάπτυξης λειτουργίας «πρόληψης» σε αντίθεση με τη λειτουργία «ανίχνευσης» που χρησιμοποιούν συχνά οι παραδοσιακές τεχνολογίες ανίχνευσης.

Φιλτράρισμα Περιεχομένου

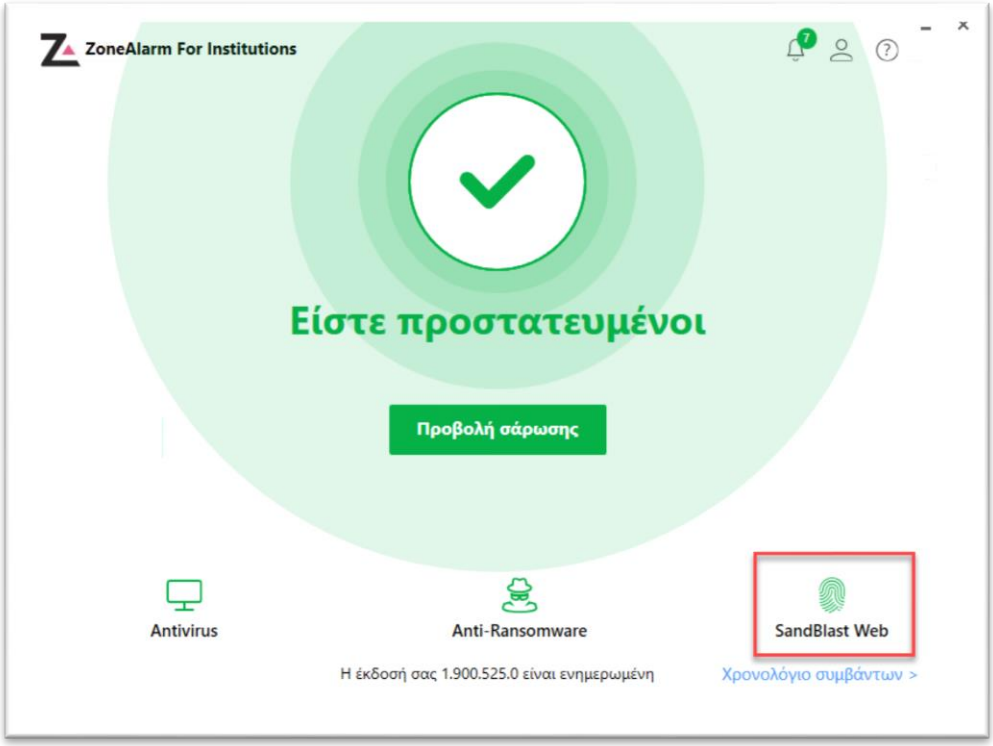
Αποκλείει ένα σύνολο προκαθορισμένων διευθύνσεων URL που **δεν είναι δυνατό να ξεμπλοκαριστούν**.

Ακολουθούν οι προκαθορισμένες κατηγορίες στις οποίες αποτρέπεται η πρόσβαση :
Αλκοόλ & Καπνός, Anonymizer, Κακοποίηση, Τυχερά παιχνίδια, Μίσος/Ρατσισμός, Παράνομος/αμφισβητήσιμος, Παράνομα ναρκωτικά, Ανενεργές τοποθεσίες, Μαριχουάνα, Πορνογραφία, Σεξ

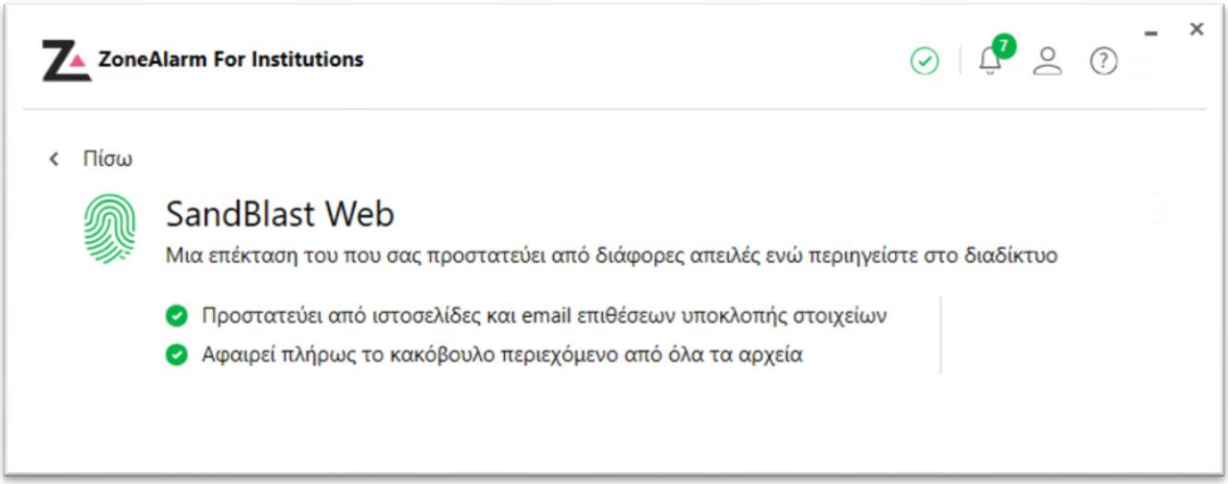
Sandblast Web Panel

Το SandBlast Web ενεργοποιείται αυτόματα στο πρόγραμμα περιήγησης μετά το άνοιγμα ή την επανεκκίνηση του προγράμματος περιήγησης μετά την εγκατάσταση του ZoneAlarm For Institution (βλ. σελίδα 5). Οι επεκτάσεις του προγράμματος περιήγησης στο Web sandblast είναι για τα προγράμματα περιήγησης **Chrome, Edge και Firefox**.

Επιλέξτε **Sandblast Web**



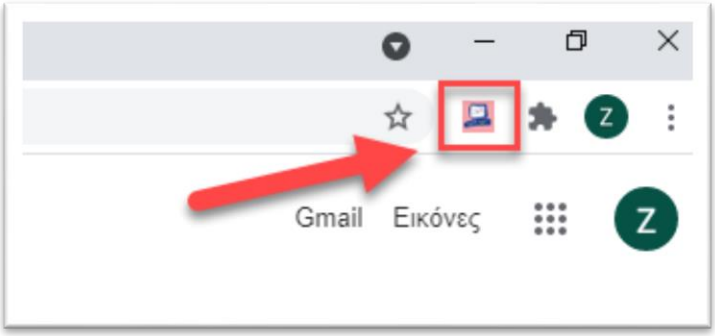
Οι επεκτάσεις Sandblast Web για chrome **δεν** μπορούν να ενεργοποιηθούν ή να απενεργοποιηθούν για λόγους ασφαλείας των παιδιών.



Sandblast Web Επέκταση Περιηγητή

Η επέκταση του προγράμματος περιήγησης στο Web Sandblast βρίσκεται στην επάνω δεξιά γωνία του προγράμματος περιήγησης.

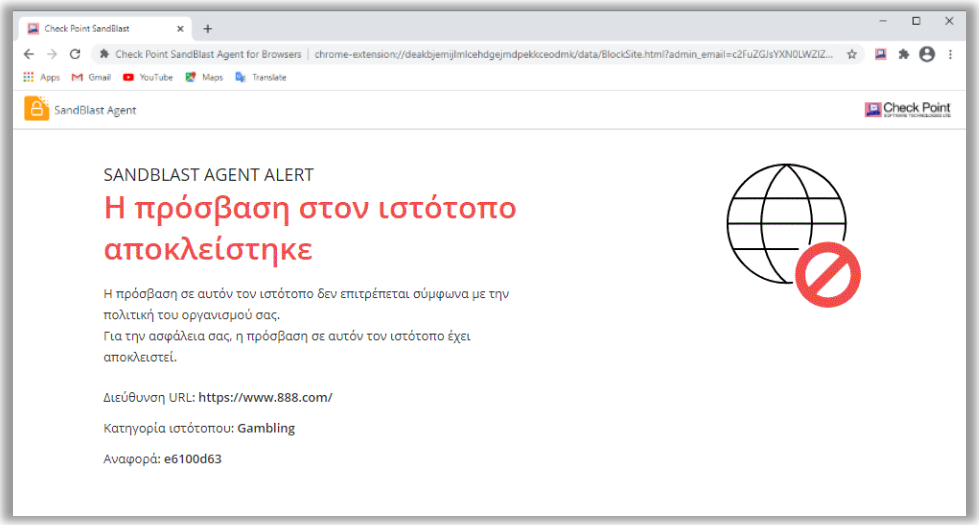
Οι εικόνες και η διαδικασία σε αυτόν τον οδηγό λαμβάνονται από το πρόγραμμα περιήγησης Chrome, αλλά μπορούν να εφαρμοστούν σε όλα τα προγράμματα περιήγησης Edge και Firefox.



Φιλτράρισμα Περιεχομένου για την ασφάλεια των παιδιών

Οι προκαθορισμένες κατηγορίες είναι οι εξής: Αλκοόλ & Καπνός, Anonymizer, Κακοποίηση, Τυχερά παιχνίδια, Μίσος/Ρατσισμός, Παράνομος/αμφισβητήσιμος, Παράνομα ναρκωτικά, Ανενεργές τοποθεσίες, Μαριχουάνα, Πορνογραφία, Σεξ

Κάθε φορά που ένας ιστότοπος εμπίπτει σε μία από τις παραπάνω κατηγορίες, ο ιστότοπος θα αποκλείεται αμέσως.

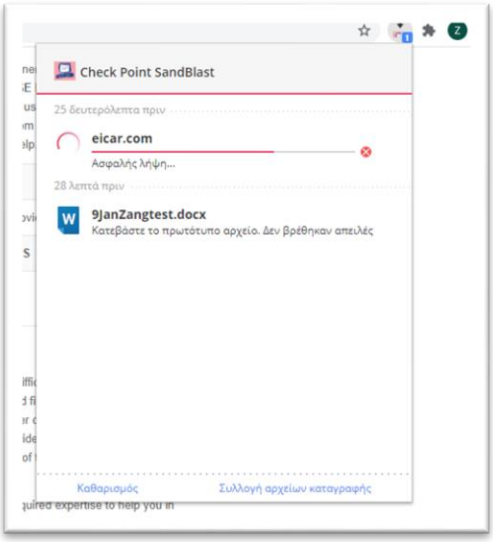


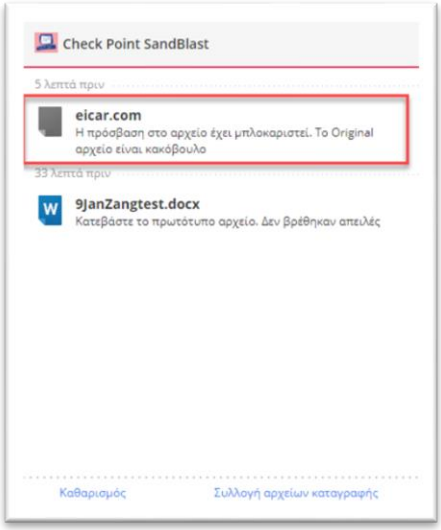
Λήψη Αρχείων

Επιλέξτε το εικονίδιο για να επεξεργαστείτε τις ρυθμίσεις και να δείτε τις ασφαλείς λήψεις σας.

Η δυνατότητα κατάργησης απειλών για λήψεις αρχείων, «καθαρίζει» αρχεία διαφόρων μορφών, όπως .pdf, .doc, .xls, .ppt, κ.ο.κ. από πιθανόν κακόβουλο περιεχόμενο.

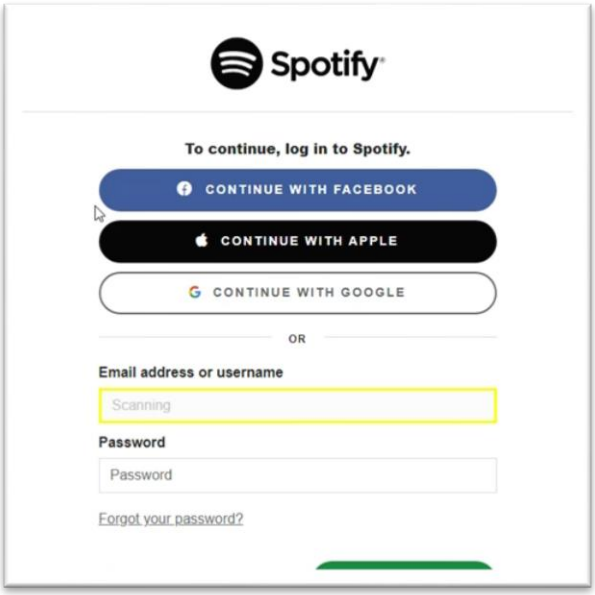
Όλα τα ληφθέντα αρχεία θα σαρωθούν και τα κακόβουλα στοιχεία θα καταργηθούν ή θα αποκλειστούν.



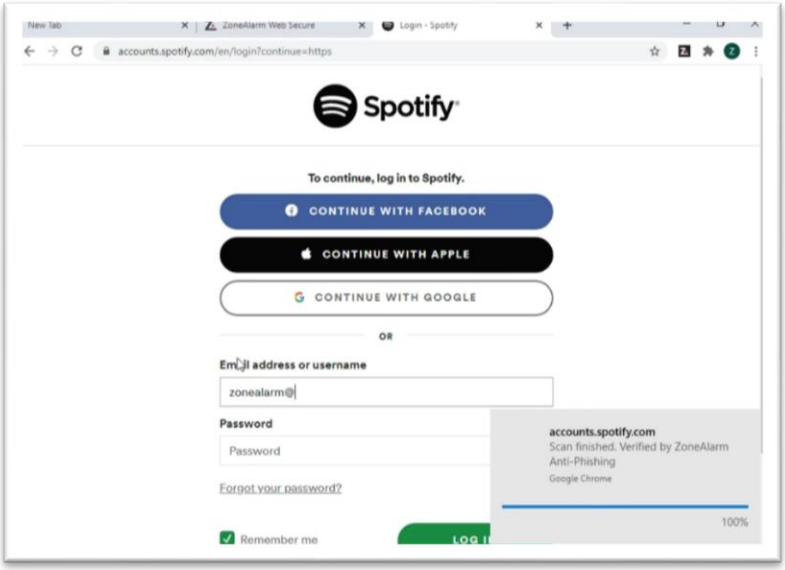


Anti-Phising

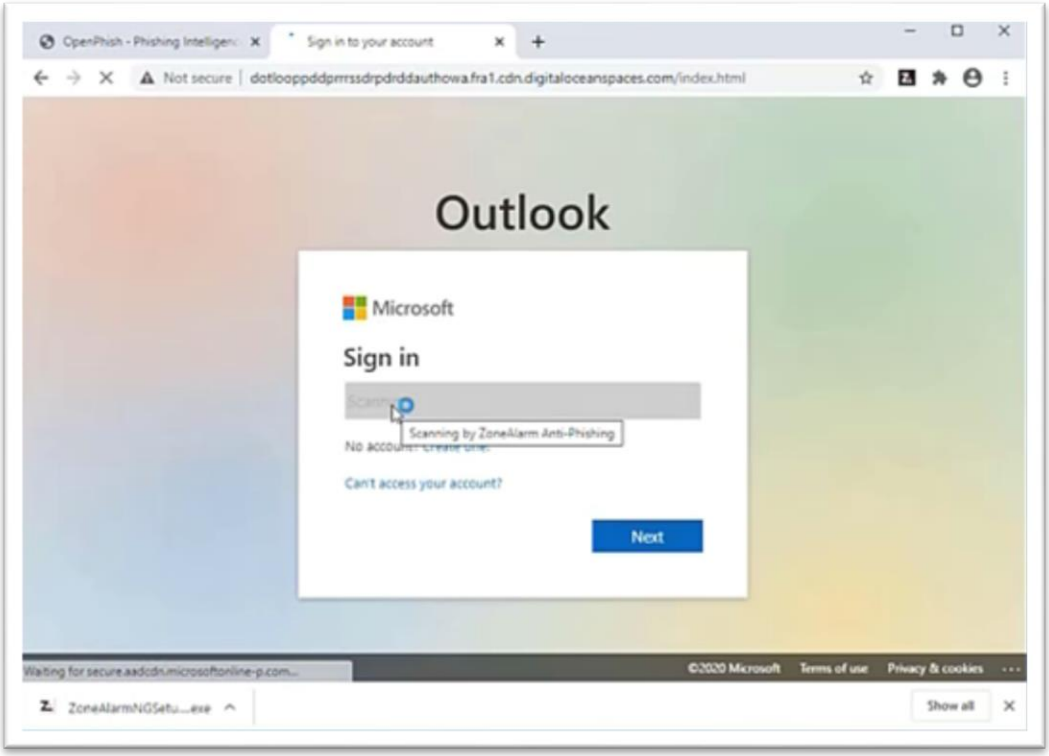
Το ZoneAlarm For Institutions μπορεί να σαρώσει τοποθεσίες Web για να ανιχνεύσει οποιαδήποτε anti-phishing ιστοσελίδα που μπορεί να προκαλέσει ζημιά σε εσάς ή το σύστημά σας αποκλέπτοντας τα στοιχεία αυθεντικοποίησής σας. Στο παρακάτω παράδειγμα, μπορείτε να δείτε ότι η σελίδα σύνδεσης ενός ιστότοπου σαρώνεται.



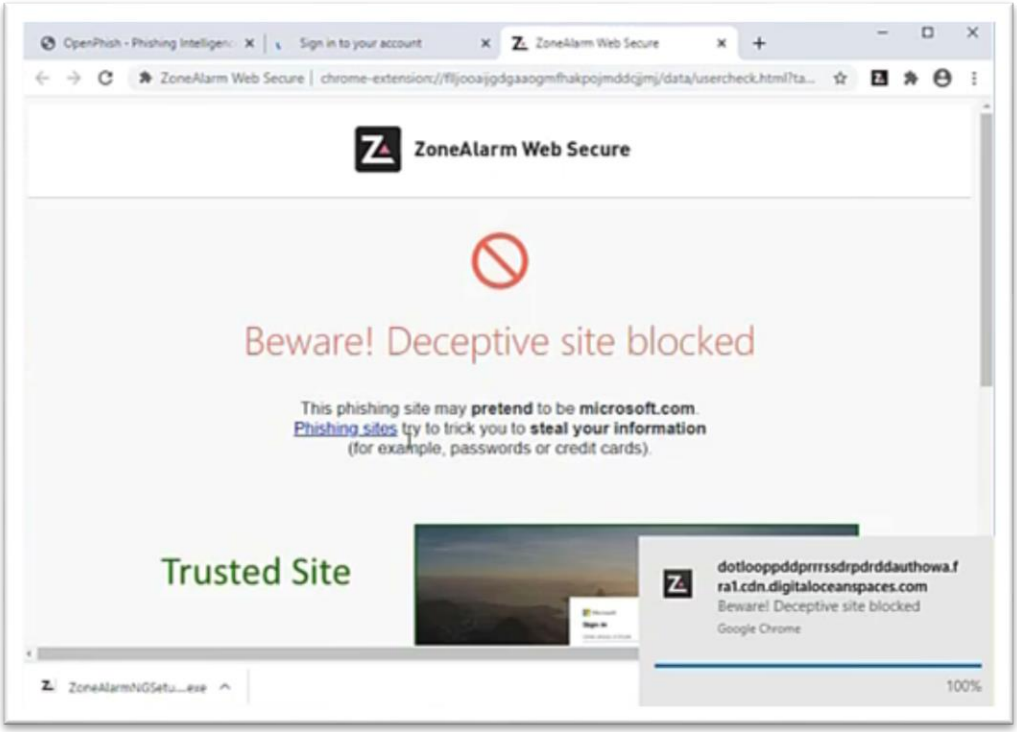
Μετά την ολοκλήρωση της σάρωσης, μια ειδοποίηση δείχνει ότι η σάρωση έχει ολοκληρωθεί και δεν εντοπίστηκε κάποια δραστηριότητα phishing.



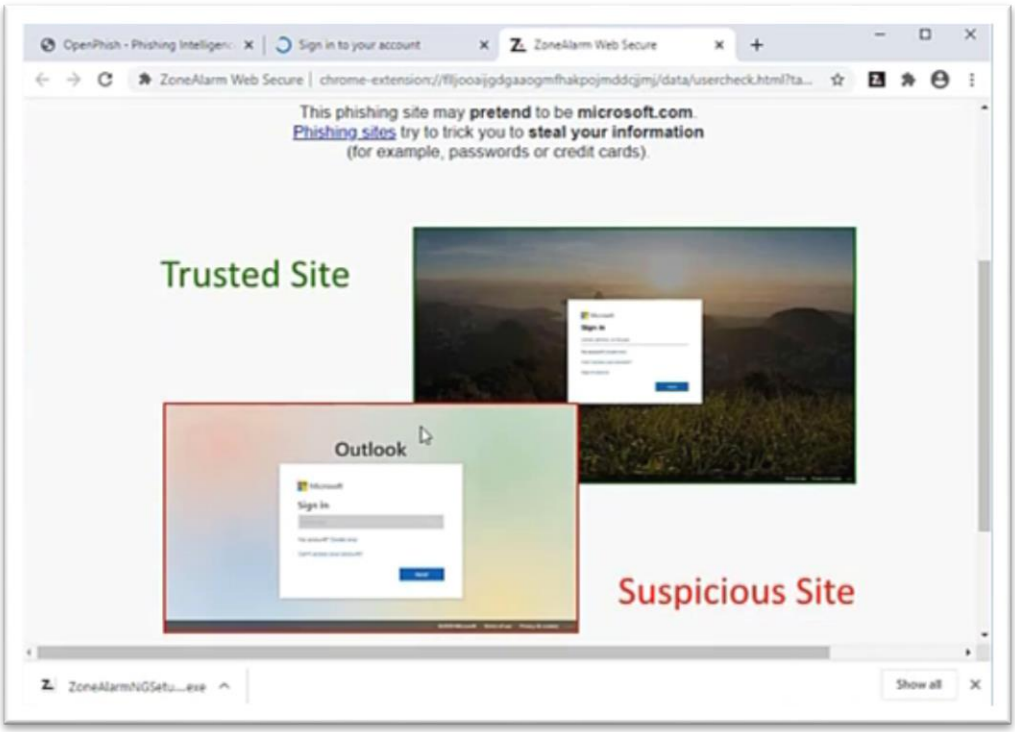
Τώρα ας δούμε ένα παράδειγμα phishing επίθεσης την οποία ο χρήστης αντιμετωπίζει κάνοντας πλοήγηση σε μια παραπλανητική τοποθεσία.
Το ZoneAlarm For Institutions σαρώνει όλες τις τοποθεσίες Web , όπως το Microsoft Outlook στο παρακάτω παράδειγμα.



Αυτός ο ιστότοπος έπειτα από τον έλεγχο διαπιστώνεται ότι δεν είναι ασφαλής, και «μιμείται» οπτικά τον αυθεντικό προορισμό. Το ZoneAlarm For Institutions ειδοποιεί τον χρήστη με μια ειδοποίηση και επίσης αποκλείει τον παραπλανητικό ιστότοπο.



Το ZoneAlarm θα εμφανίσει επίσης μια σύγκριση μεταξύ του αξιόπιστου και του ύποπτου ιστότοπου.



a. Περίπτωση – Κατάργηση Απειλών

Ας δούμε τώρα δύο σενάρια για το πώς το ZoneAlarm For Institutions βοηθά με τις τεχνικές κατάργησης απειλών.

Δείτε τον παρακάτω σύνδεσμο στο Youtube:

Περίπτωση 1 – Σε μακροεντολή
https://www.youtube.com/watch?v=BvpL0PPVKKY&t=25s

Περίπτωση 2 – Σε PDF
https://www.youtube.com/watch?v=iHMCorVt-PA&t=3s

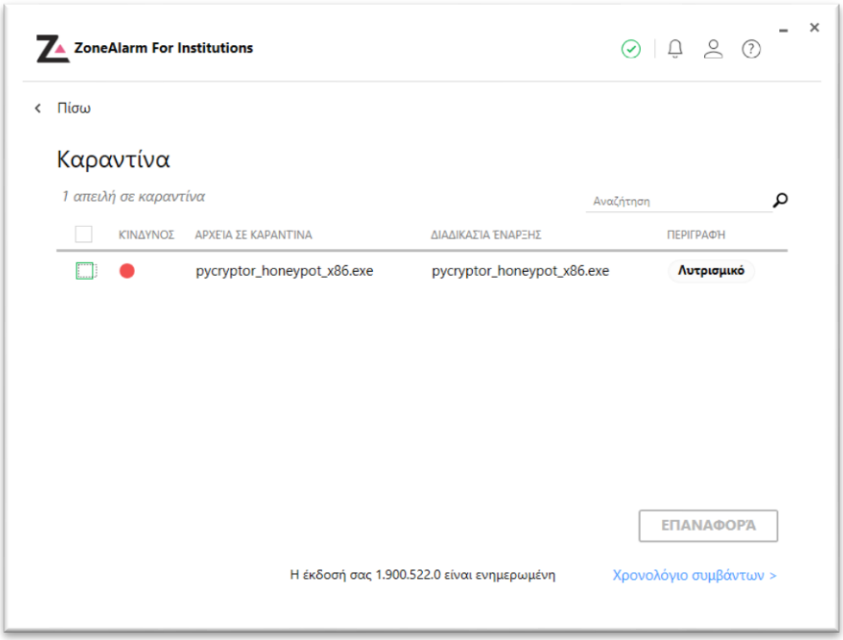
b. Περίπτωση – Anti-Phishing

Ας δούμε τώρα ένα σενάριο επίθεσης phishing και πώς το ZoneAlarm For Institutions βοηθά με τις anti-phising τεχνικές του.

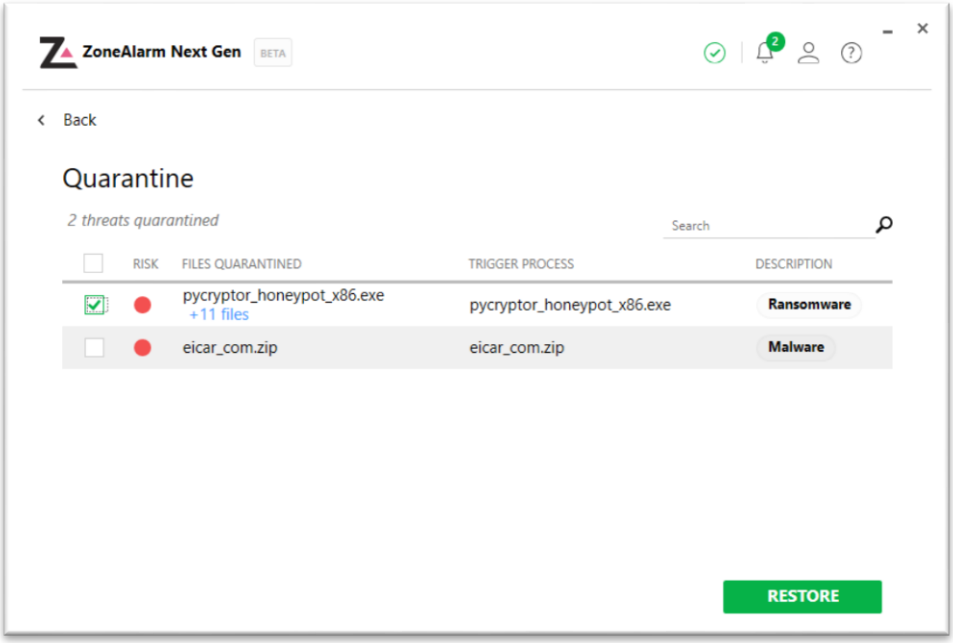
Δείτε τον παρακάτω σύνδεσμο στο Youtube:
https://www.youtube.com/watch?v=oaG_6fOR44w

6. Πίνακας Καραντίνας

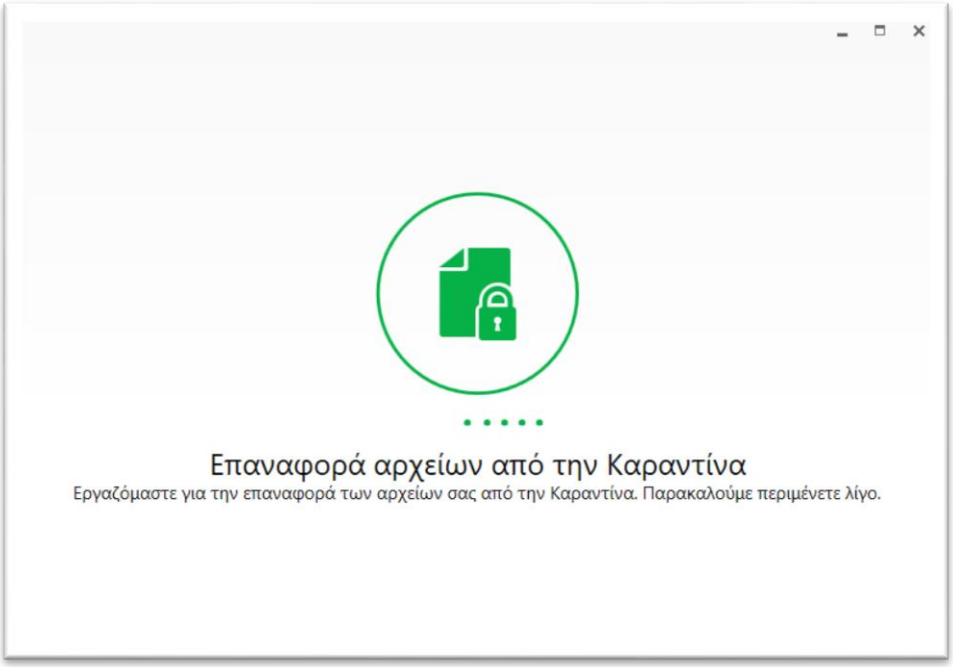
Όταν το ZoneAlarm For Institutions δεν μπορεί να καθαρίσει τα μολυσμένα αρχεία, τα βάζει σε καραντίνα. Τα αρχεία σε καραντίνα δεν διαγράφονται ή χρησιμοποιούνται, αλλά καθίστανται αβλαβή. Ο πίνακας καραντίνας εμφανίζει τα κακόβουλα αρχεία που εντοπίστηκαν και μπήκαν σε καραντίνα από το ZoneAlarm For Institutions.



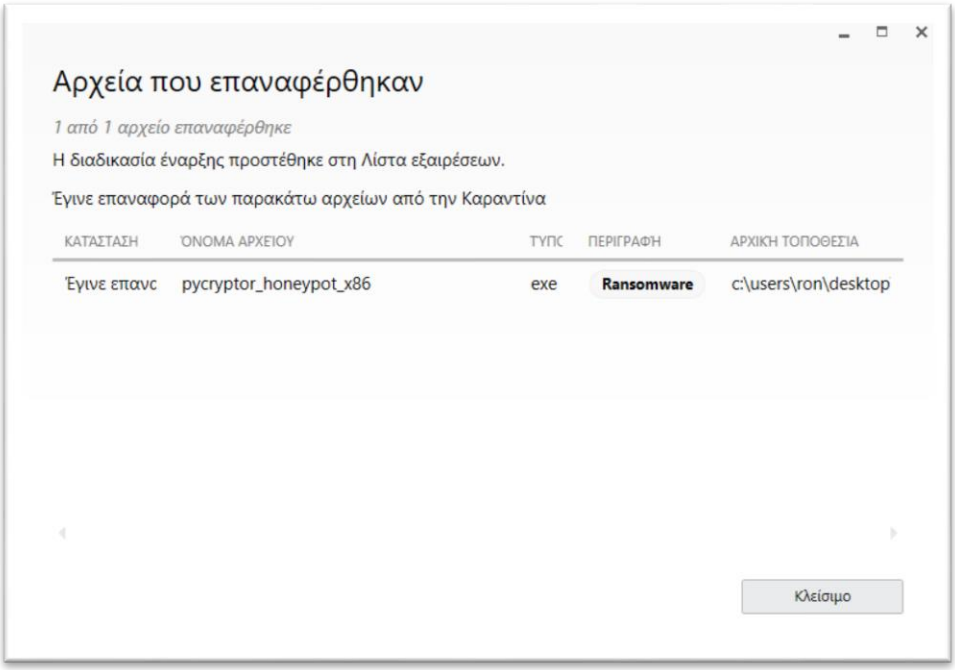
Για να καταργήσετε οποιοδήποτε αρχείο έχει αποκλειστεί στην Καραντίνα, το οποίο πιστεύετε ότι προέρχεται από αξιόπιστη πηγή, επιλέξτε το αρχείο και, στη συνέχεια, επιλέξτε την επιλογή **Επαναφορά**.



Ειδοποίηση για την επαναφορά αρχείων



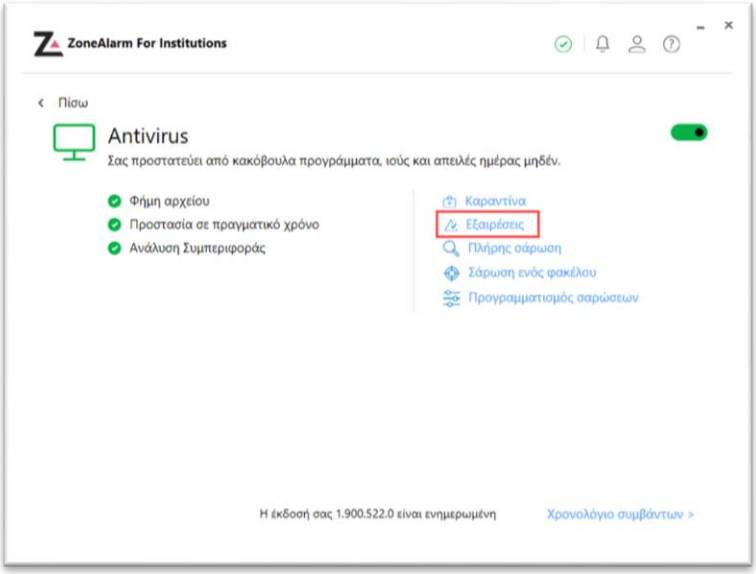
Επιβεβαίωση επαναφοράς αρχείων



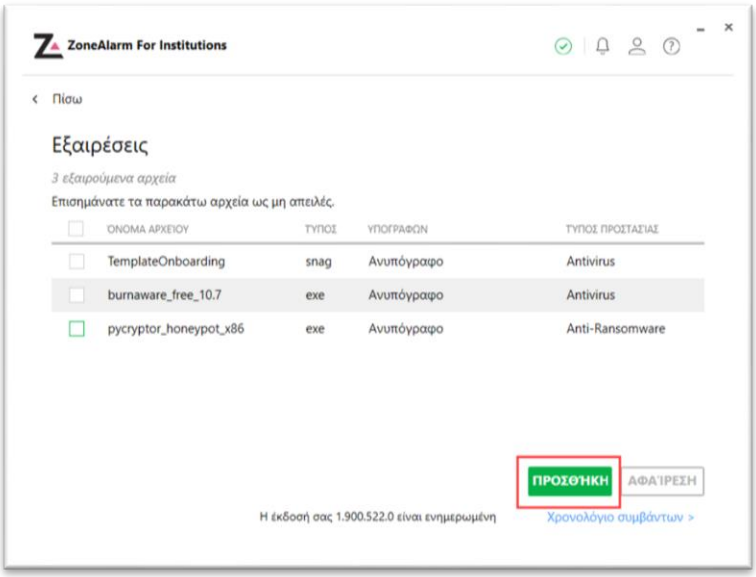
7. Πίνακας Εξαιρέσεων

Ο πίνακας Εξαιρέσεων, σαςεπιτρέπει να καθορίσετε καταλόγους, αρχεία ή προγράμματα που δεν θέλετε να σαρώσετε για ιούς και κακόβουλο λογισμικό. Αυτό μπορεί να είναι χρήσιμο σε περιπτώσεις όπου γνωρίζετε ότι κάποια αρχεία και προγράμματα που χρησιμοποιείτε είναι ασφαλή, αλλά η εξαίρεση θα μειώσει πιθανόν το συνολικό επίπεδο προστασίας σας. Μπορείτε να προσθέσετε με χειροκίνητο τρόπο εξαιρέσεις ή να τις προσθέσετε μόλις εντοπιστεί το αρχείο από το ZoneAlarm For Institutions. Τα βήματα για την προσθήκη και κατάργηση εξαιρέσεων χειροκίνητα είναι τα εξής:

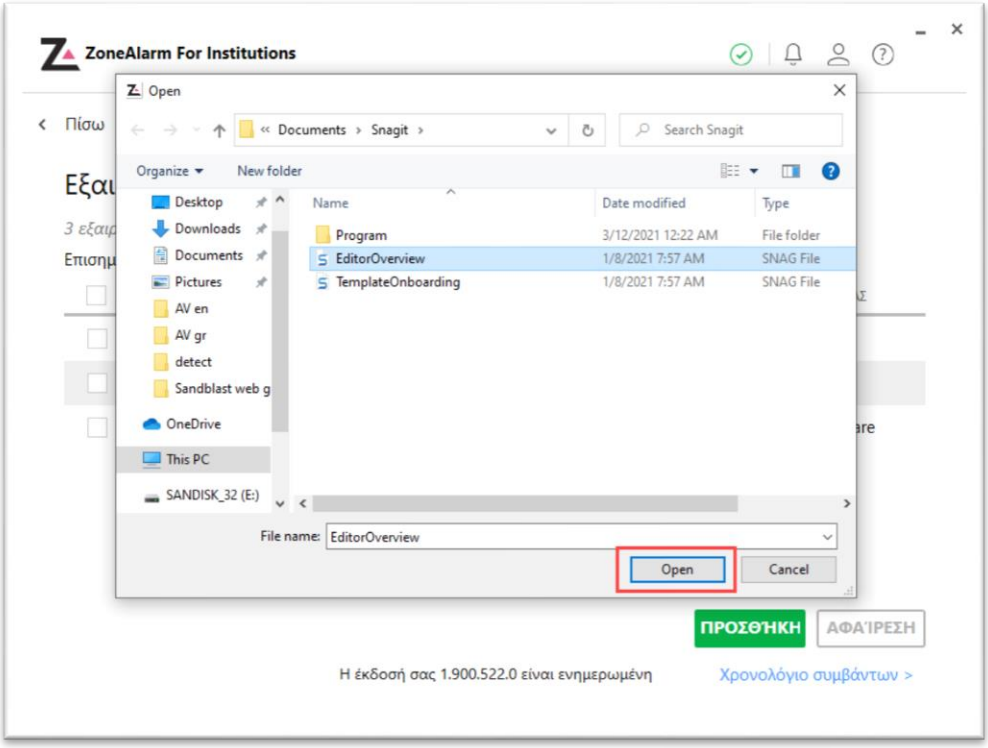
1. Κάντε κλικ στην επιλογή "Εξαιρέσεις" στην καρτέλα Antivirus



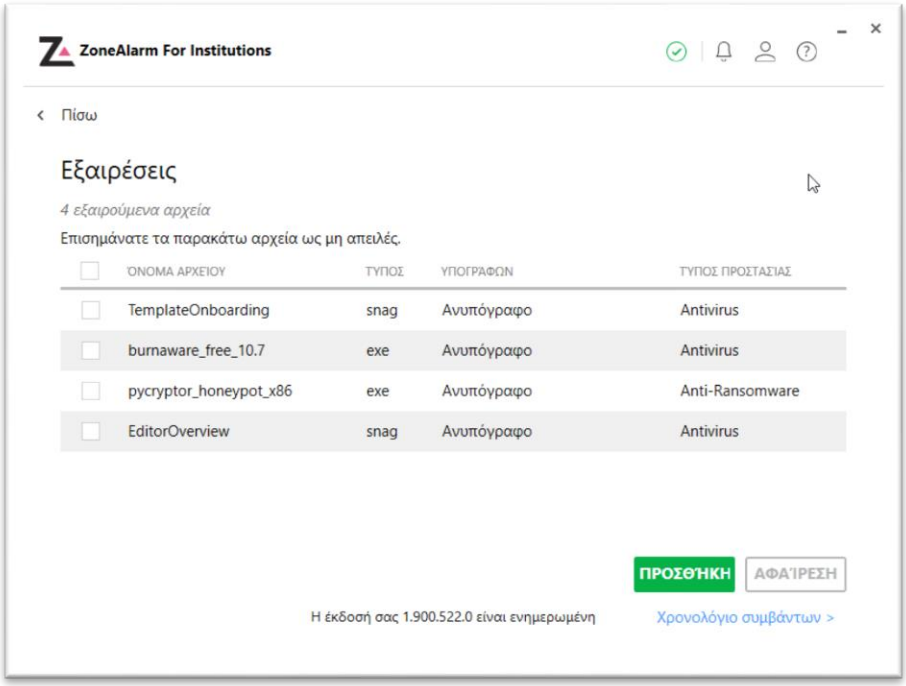
2. Πατήστε το κουμπί **Προσθήκη**.



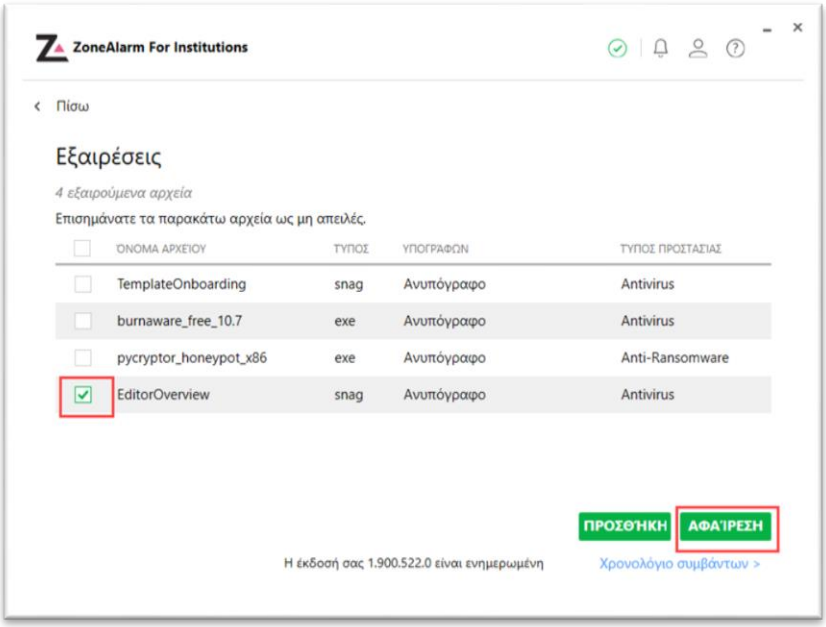
3. Επιλέξτε το αρχείο που θα προστεθεί στις εξαιρέσεις.



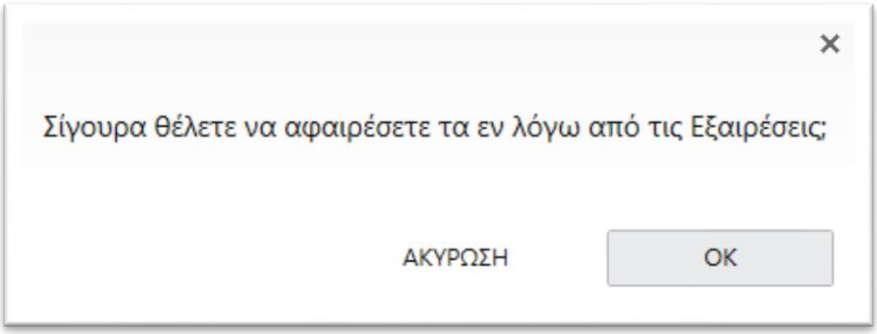
4. Το αρχείο θα προστεθεί στη λίστα των εξαιρούμενων αρχείων.



5. Για να καταργήσετε ένα αρχείο από τις εξαιρέσεις, επιλέξτε το αρχείο και, στη συνέχεια, επιλέξτε την επιλογή **Αφαίρεση**.



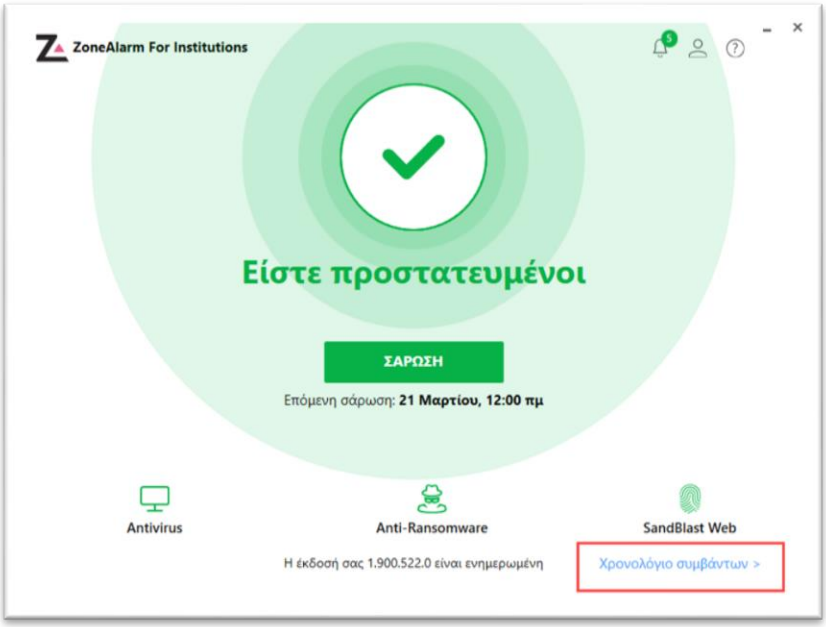
6. Θα σας ζητηθεί να επιβεβαιώσετε την επιλογή σας. Επιλέξτε **OK**.



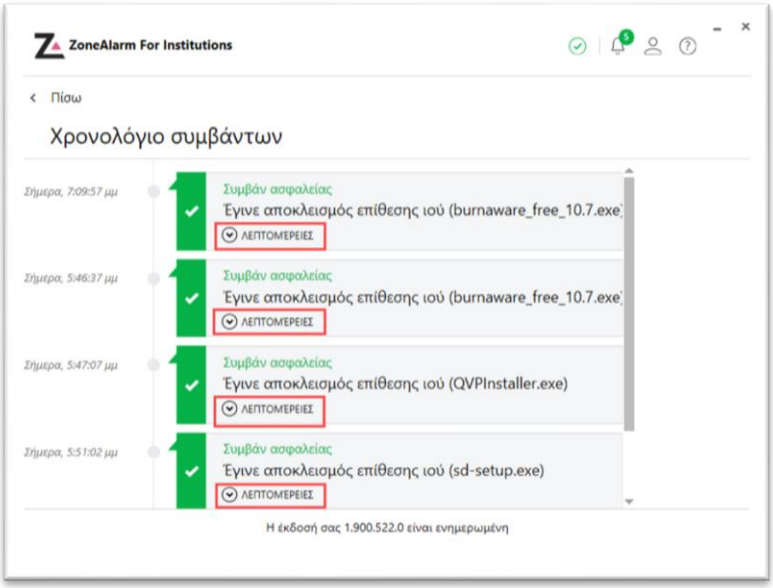
8. Χρονολόγιο Συμβάντων

Το ZoneAlarm For Institutions καταγράφει όλα τα συμβάντα ασφάλειας σε ένα αρχείο καταγραφής συμβάντων. Από προεπιλογή, το ZoneAlarm καταγράφει όλες τις σαρώσεις, τις ενημερώσεις και τις ανιχνεύσεις απειλών σε ένα αρχείο καταγραφής. Τα βήματα για την προβολή του Χρονολογίου Συμβάντων είναι τα εξής:

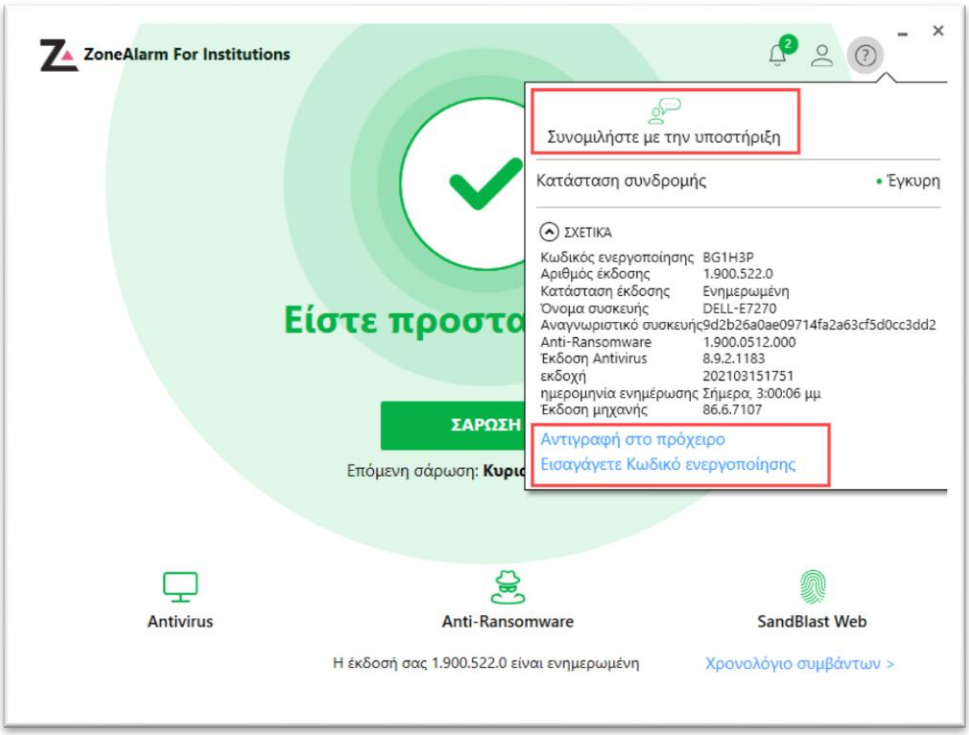
1. Επιλέξτε το σύνδεσμο Χ**ρονολίο Συμβάντων** στην κάτω δεξιά γωνία της σελίδας.



2. Εμφανίζονται όλα τα συμβάντα. Επιλέξτε **Λεπτομέρειες** για να δείτε επιπλέον πληροφορίες.



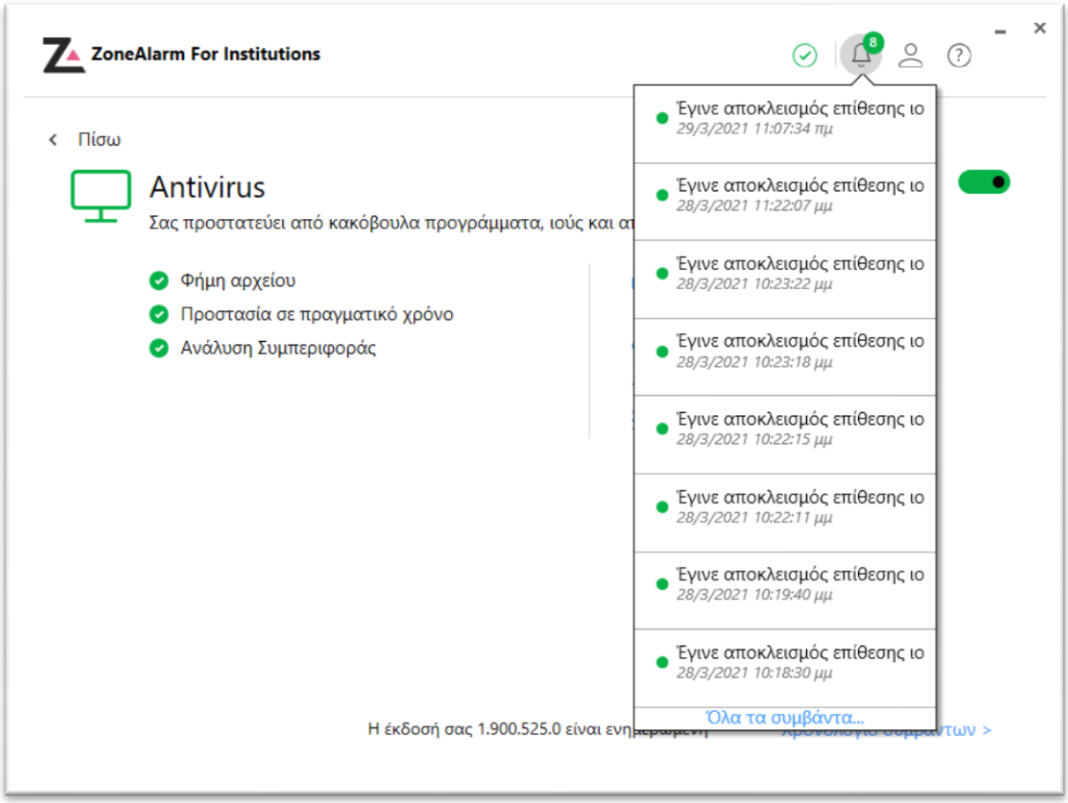
3. Οι λεπτομέρειες του συμβάντος εμφανίζονται μαζί με την κατάσταση. Κάντε κύλιση προς τα κάτω για να δείτε περισσότερα συμβάντα.



Μπορείτε επίσης να εκτελέσετε διάφορες ενέργειες από το **Χρονολόγιο Συμβάντων**, όπως η προβολή του πίνακα καραντίνας και η επισήμανση της απειλής ως λυτρισμικό ή κακόβουλο λογισμικό.

9. Ειδοποιήσεις

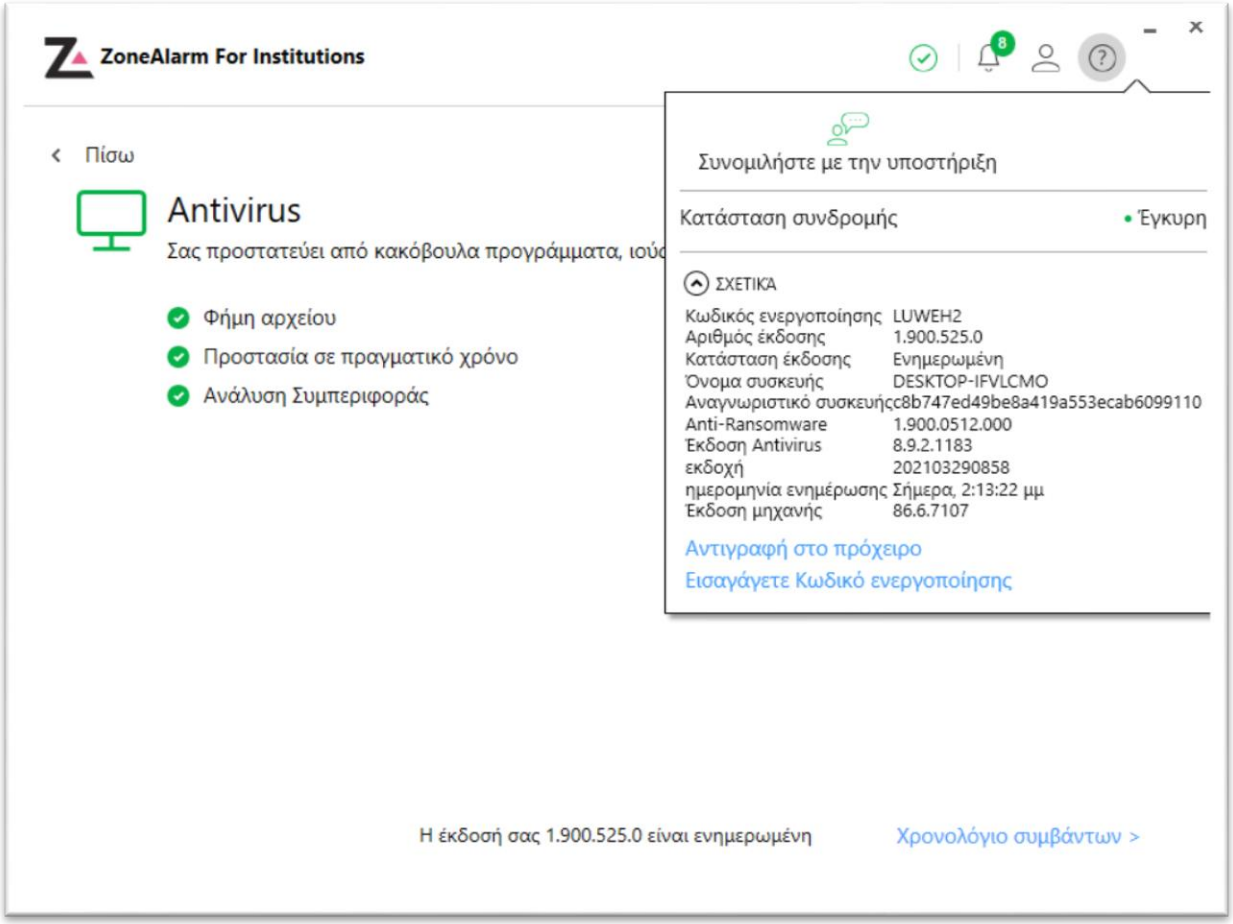
Το εικονίδιο ειδοποιήσεις σας επιτρέπει να προβάλετε τα πρόσφατα συμβάντα που έχουν συμβεί στο ZoneAlarm For Institutions. Επιλέξτε **Όλα τα συμβάντα** για να δείτε όλα τα συμβάντα στη καρτέλα **Χρονολόγιο Συμβάντων**.



10. Σχετικά

Επιλέξτε το εικονίδιο ⓘ **Σχετικά** για να προβάλετε όλες τις λεπτομέρειες σχετικά με το ZoneAlarm For Institutions που είναι εγκατεστημένο στο σύστημά σας. Μπορείτε να προβάλλετε τις λεπτομέρειες, όπως κατάσταση συνδρομής, αριθμός έκδοσης, κατάσταση έκδοσης κ.λπ.. Υπάρχουν επίσης οι ακόλουθες ενέργειες χρήστη που μπορείτε να εκτελέσετε μέσω του μενού "Σχετικά":

1. Συνομιλία με την υποστήριξη για τυχόν ερωτήματα
2. Αντιγραφή των δεδομένων "Σχετικά" στο Πρόχειρο
3. Συλλογή αρχείων καταγραφής και άλλων σχετικών αναφορών
4. Εισαγωγή Κωδικού Ενεργοποίησης



Οδηγός χρήσης γιαAndroid /Harmony* Συσκεύες

Οφέλη Προϊόντος

Μεταφρασμένο στα Ελληνικά
Όλα τα μενού και τα περιεχόμενα της εφαρμογής είναι πλήρως μεταφρασμένα στα Ελληνικά.

Προστασία προσωπικών δεδομένων από το σχεδιασμό
Η ZoneAlarm εγγυάται ότι τα δεδομένα σας παραμένουν εντελώς απόρρητα. Όλες οι αναλύσεις ασφαλείας πραγματοποιούνται στη συσκευή με ανώνυμα μεταδεδομένα που συλλέγονται από το λειτουργικό σύστημα, τις εφαρμογές, το διαδίκτυο και τα δίκτυα.

Προστασία από υποκλοπές
Η ZoneAlarm διασφαλίζει ότι το δίκτυό σας είναι ασφαλές και δεν σας υποκλέπτει κάποιος τρίτος.

Προστασία από ηλεκτρονικές απάτες
Η ZoneAlarm Anti-Phishing τεχνολογία σας προστατεύει από τη διαρροή των διαπιστευτηρίων σας σε γνωστές και άγνωστες ψεύτικες ιστοσελίδες που προσπαθούν να διαπράξουν ηλεκτρονικό "ψάρεμα" (phishing).

Ασφαλείς λήψεις και περιήγηση
Κατεβάστε εφαρμογές και περιηγηθείτε στο διαδίκτυο χωρίς καμία ανησυχία – Η ZoneAlarm Mobile Security ελέγχει για λήψεις κακόβουλων εφαρμογών και URL σε πραγματικό χρόνο.

Χωρίς διαφημίσεις
Δεν θα βλέπετε διαφημίσεις, ακόμα και κατά τη διάρκεια της δοκιμαστικής έκδοσης.

Εξατομικευμένες εβδομαδιαίες αναφορές
Η εβδομαδιαία αναφορά συμβάντων ασφαλείας στη συσκευή, σας ενημερώνει σχετικά με τις πιο πρόσφατες απειλές από τις οποίες η ZoneAlarm προφύλαξε τη συσκευή σας.

Ασφαλής περιήγηση για παιδιά
Η ZoneAlarm συνοδεύεται από ένα ενσωματωμένο φίλτρο περιεχομένου που τα παιδιά σας δεν μπορούν να απενεργοποιήσουν ή να αλλάξουν. Επιτρέπει στα παιδιά σας να έχουν πρόσβαση στο διαδίκτυο με ασφάλεια σε όλα τα προγράμματα περιήγησης και τις πλατφόρμες.

Αλληλεπιδραστικό περιβάλλον εργασίας χρήστη
Η εφαρμογή ZoneAlarm είναι απλή, γρήγορη και εύκολη στη χρήση.

Απόλυτη εμπειρία συσκευής
Ελάχιστη επίδραση στη διάρκεια ζωής της μπαταρίας και την απόδοση της συσκευής.

Ανάλυση απειλών σε πραγματικό χρόνο
Η ZoneAlarm αξιοποιεί τη μεγαλύτερη βάση δεδομένων πληροφοριών για απειλές στον κόσμο, με το Check Point Threat Cloud.

Δυνατότητες προϊόντος

Ασφάλεια δικτύου Wi-Fi
Προστατεύει τους χρήστες από το να παγιδευτούν σε επιθέσεις Man-in-the-Middle όταν συνδέονται με Wi-Fi

Κατάταξη ασφάλειας Wi-Fi
Κατατάσσει τα διαθέσιμα ενεργά σημεία γύρω σας με βάση το επίπεδο ασφάλειάς τους, διασφαλίζοντας ότι συνδέεστε με την πιο ασφαλή διαθέσιμη επιλογή.

Προστασία από κακόβουλες εφαρμογές
Προστατεύει από γνωστές και άγνωστες κακόβουλες εφαρμογές και ενημερώσεις.

Zero-Day Anti-Phishing
Αποκλείει επιθέσεις ηλεκτρονικού "ψαρέματος" τόσο από γνωστούς όσο και από άγνωστους ιστότοπους ηλεκτρονικού "ψαρέματος" και εφαρμογές.

Ασφαλής περιήγηση
Η Ελληνική έκδοση του Zone Alarm for Institutions προστατεύει από κακόβουλους ιστότοπους και διατίθεται με αυτόματα προεγκατεστημένη την ρύθμιση πρόσβασης (URL filtering) σε όλες τις εφαρμογές περιήγησης αποκλείοντας ακατάλληλο περιεχόμενο .

Αντι-λυτρισμική προστασία
Εντοπίζει και αποκλείει ύποπτες δραστηριότητες λυτρισμικών λογισμικών πριν κρυπτογραφηθούν οποιαδήποτε αρχεία σας.

USB και Bluetooth
Προστατεύει από κακόβουλες εφαρμογές που προέρχονται από συνδέσεις USB και Bluetooth.

Anti-Bot
Εμποδίζει τους χάκερ να πάρουν τον έλεγχο της συσκευής σας αποκλείοντας επιθέσεις bot.

Ασπίδα συσκευής
Ειδοποιεί το χρήστη για τυχόν επικίνδυνες ρυθμίσεις στη συσκευή.

Εντοπισμός Rooting
Εντοπίζει ύποπτες συμπεριφορές συσκευής και ειδοποιεί αν κάποιος έχει αποκτήσει τον έλεγχο του λειτουργικού σας συστήματος.

Ασφάλεια Δικτύου

Η ZoneAlarm Mobile Security χρησιμοποιεί μια μοναδική υποδομή ασφάλειας δικτύου – την **Προστασία δικτύου συσκευών (ONP)** – για να επικυρώσει όλη την επισκεψιμότητα του χρήστη στη συσκευή χωρίς να μεταφέρει τα δεδομένα του χρήστη στο cloud. Αυτό εξασφαλίζει την προστασία των προσωπικών δεδομένων των χρηστών και επιτρέπει την απρόσκοπτη εμπειρία περιήγησης και τον ελάχιστο αντίκτυπο στην απόδοση και την μπαταρία.

Κάθε σύνδεσμος στον οποίο κάνετε «κλικ», ανεξάρτητα από το αν είναι σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ένα μήνυμα σε μια εφαρμογή μέσων κοινωνικής δικτύωσης κ.λπ., επικυρώνεται σε πραγματικό χρόνο με δυναμικές πληροφορίες ασφαλείας που παρέχονται από το **Check Point ThreatCloud**, το μεγαλύτερο δίκτυο πληροφοριών στον κυβερνοχώρο στον κόσμο. Εάν η διεύθυνση URL εντοπιστεί ως κακόβουλη, για παράδειγμα βρεθεί ότι είναι μια ιστοσελίδα ηλεκτρονικού "ψαρέματος", αποκλείεται αμέσως και ο χρήστης ειδοποιείται να μην εισέλθει στην ιστοσελίδα.

Προστασία Wi-Fi συνδέσεων

Μία από τις πιο κοινές επιθέσεις που βασίζονται στο δίκτυο σε κινητές συσκευές είναι η **Man-in-the-Middle (MitM)**, όπου ο εισβολέας ξεγελάει ανυποψίαστους χρήστες να συνδεθούν σε ένα ύποπτο δίκτυο Wi-Fi.

Οι χάκερ χρησιμοποιούν δύο είδη μεθόδων MitM:

- **SSL striping:** αφαίρεση του πιστοποιητικού SSL χωρίς τη γνώση του χρήστη και αποκρυπτογράφηση της επισκεψιμότητας.
- **SSL bumping:** χρήση πλαστών πιστοποιητικών SSL για να ξεγελάσουν εφαρμογές και προγράμματα περιήγησης ώστε να πιστέψουν ότι χρησιμοποιούν ασφαλείς συνδέσεις.

Με αυτόν τον τρόπο, οι εγκληματίες του κυβερνοχώρου μπορούν να υποκλέψουν επικοινωνίες, επιτρέποντάς τους να παρακολουθούν και να κλέβουν δεδομένα κατά τη μεταφορά τους. Η ZoneAlarm Mobile Security επικυρώνει την ακεραιότητα των συνδέσεων SSL και ειδοποιεί το χρήστη σχετικά με δίκτυα που έχουν παραβιαστεί.

Προστασία εφαρμογών

Οι εφαρμογές για κινητά είναι ένας εξαιρετικά αποτελεσματικός και εύκολος τρόπος για τους εγκληματίες του κυβερνοχώρου να εξαπολύουν εξελιγμένες και στοχευμένες επιθέσεις. Οι φαινομενικά αθώες εφαρμογές μπορούν ακούσια να παραχωρήσουν απεριόριστα δικαιώματα για την εξαγωγή δεδομένων, διαπιστευτηρίων, μηνυμάτων ηλεκτρονικού ταχυδρομείου, μηνυμάτων κειμένου και τοποθεσίας. Μπορούν επίσης να δώσουν στους χάκερ πρόσβαση στο μικρόφωνο και την κάμερά σας.

Η ZoneAlarm Mobile Security εκμεταλλεύεται δεδομένα από τη μοναδική **συμπεριφορική μηχανή κινδύνου (BRE)** της Check Point, η οποία εκτελεί εφαρμογές σε περιβάλλον που βασίζεται στο cloud για σάρωση για απειλές. Το BRE χρησιμοποιεί ποικιλία τεχνικών για να καθορίσει αν μια εφαρμογή είναι κακόβουλη, όπως μηχανική μάθηση (machine learning), AI, προηγμένη ανάλυση στατικής ροής κώδικα, ανίχνευση ανωμαλιών και φήμη εφαρμογής.

Όλες οι εφαρμογές, από ένα επίσημο κατάστημα εφαρμογών ή sideloaded κατάστημα, ελέγχονται και επικυρώνονται από την ZoneAlarm Mobile Security. Εάν η εφαρμογή εντοπιστεί ως κακόβουλη, αποκλείεται και ο χρήστης ειδοποιείται να διακόψει την εγκατάσταση.

Προστασία συσκευής

Οι ρυθμίσεις στη συσκευή σας θα μπορούσαν να αποκαλύψουν σημαντικά θέματα ασφαλείας, όπως όταν μια συσκευή Android έχει ρυθμιστεί ώστε να επιτρέπει την εγκατάσταση εφαρμογών τρίτων κατασκευαστών από άγνωστες πηγές.

Η ZoneAlarm Mobile Security χρησιμοποιεί αξιολογήσεις κινδύνου σε πραγματικό χρόνο για την παρακολούθηση όλων των αλλαγών των ρυθμίσεων. Ένας μηχανισμός συμπεριφοράς εντοπίζει εάν και πώς χορηγείται πρόσβαση root στη συσκευή και ειδοποιεί εάν κάποιος έχει αποκτήσει τον έλεγχο της συσκευής σας.

Απαιτήσεις συστήματος:

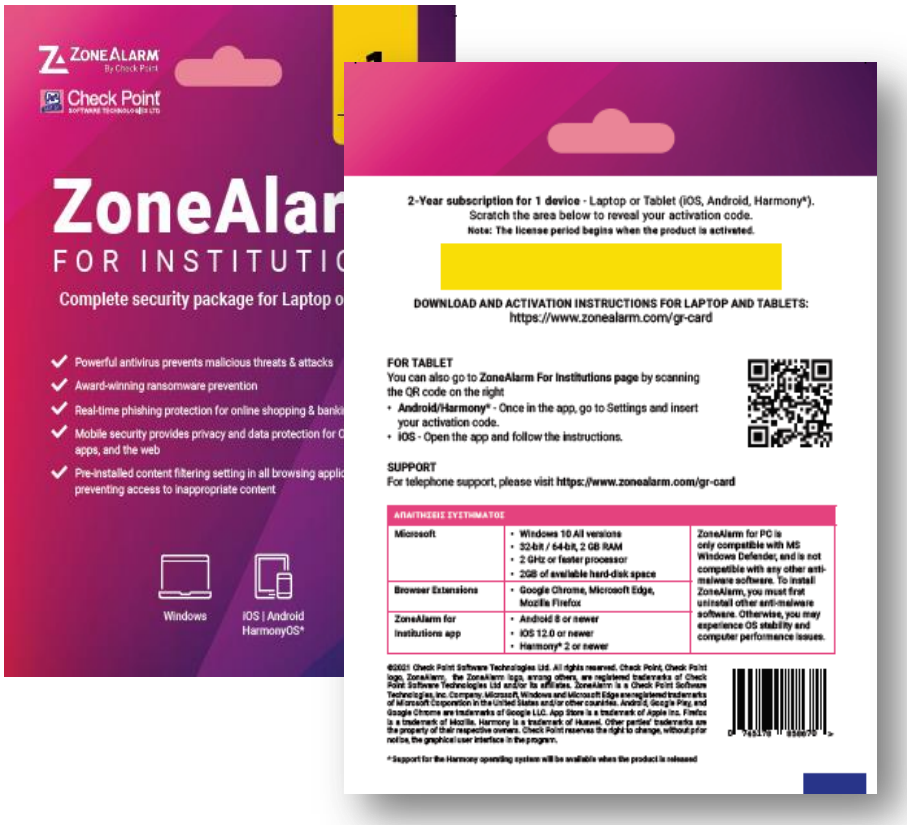
Android 8 ή νεότερη έκδοση
Harmony 2* ή μεταγενέστερο

**η υποστήριξη για το λειτουργικό Huawei HarmonyOS θα διατίθεται όταν το προϊόν κυκλοφορήσει.*

Οδηγός Εγκατάστασης και Ενεργοποίησης για Android

1. Σαρώστε τον κωδικό QR στην κάρτα ή μεταβείτε στη σελίδα λήψης ZoneAlarm For Institutions : https://www.zonealarm.com/gr-card

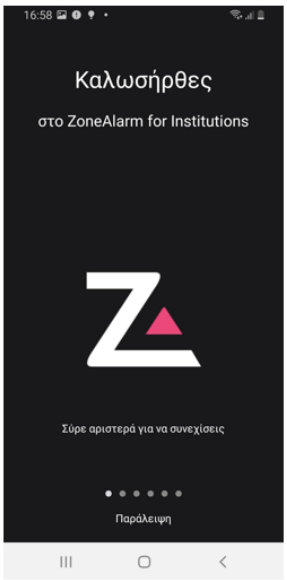
2. Κάντε κλικ στο πράσινο κουμπί λήψης. Εγκαταστείστε και ανοίξτε την εφαρμογή.



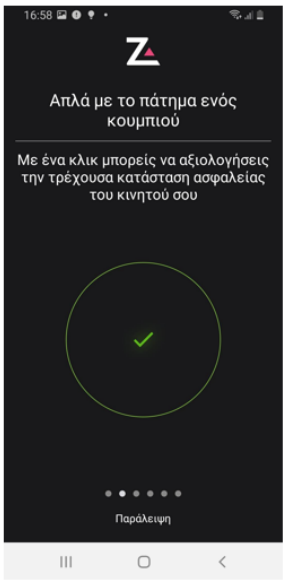
Βήματα Εγκατάστασης

Πατήστε "ΕΝΗΜΕΡΩΘΗΚΑ" για να συνεχίσετε

Σαρώστε προς τα αριστερά για να συνεχίσετε



Σαρώστε προς τα αριστερά για να συνεχίσετε



Σαρώστε προς τα αριστερά για να συνεχίσετε

Επιτρέψτε την πρόσβαση στον αποθηκευτικό χώρο

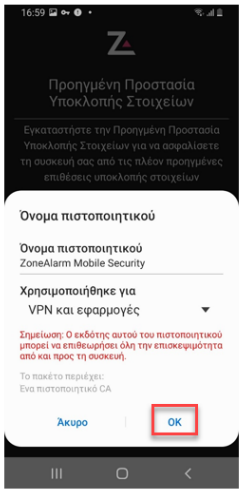
Πατήστε "Να επιτρέπεται"

Ενεργοποίηση ασφαλούς περιήγησης

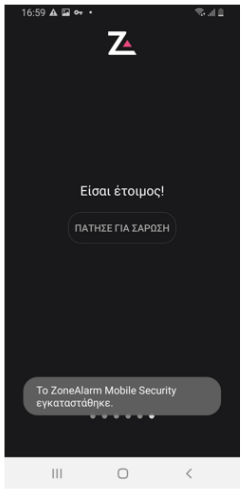
Πατήστε "Ok"

Πατήστε “Εγκατάσταση Πιστοποιητικού”

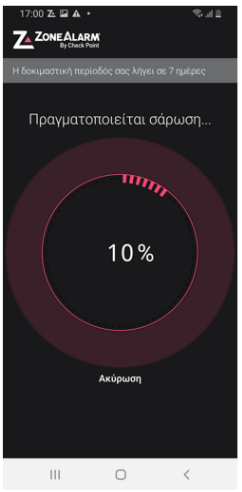
Πατήστε ”OK” για να επιτρέψετε το πιστοποιητικό από το Zonealarm



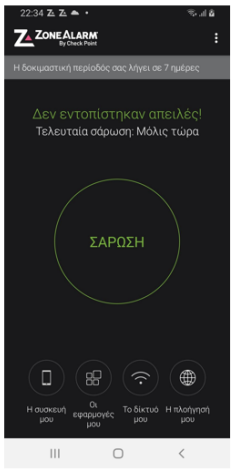
“Πατήστε για σάρωση”



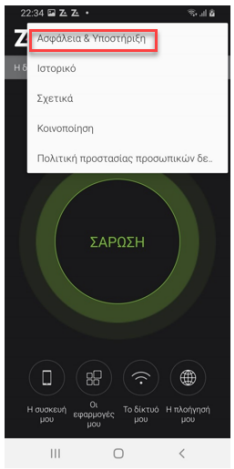
Η πρώτη σας σάρωση θα ξεκινήσει



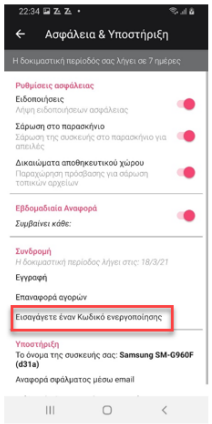
Πατήστε τις 3 κουκκίδες στην επάνω δεξιά γωνία



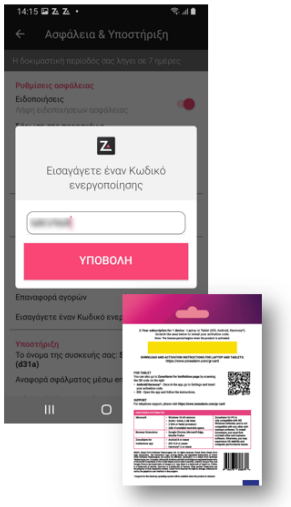
Πατήστε «Ασφάλεια & Υποστήριξη»



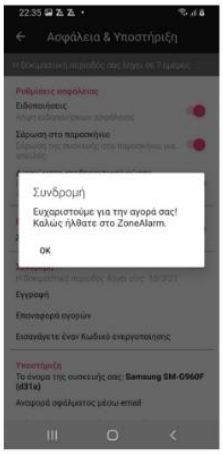
Πατήστε “Εισαγάγετε έναν κωδικό ενεργοποίησης”



Εισαγάγετε τον εξαψήφιο κωδικό ενεργοποίησης από την κάρτα



Πατήστε ”ok”.



Η συνδρομή σας είναι πλέον ενεργοποιημένη και είστε προστατευμένοι!

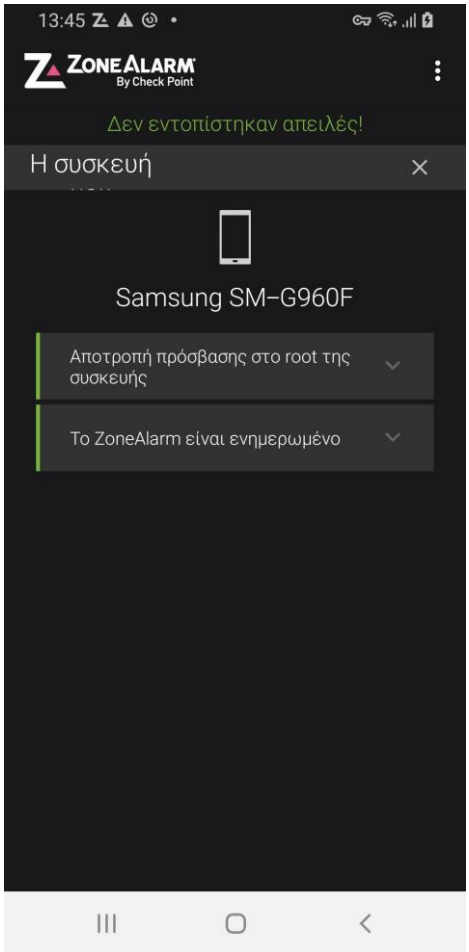
Κεντρικό Μενού

- Τα μηνύματα προβολής και η διεπαφή γίνονται κόκκινα όταν υπάρχουν προβλήματα και πράσινο όταν όλα λειτουργούν καλά και είστε πλήρως προστατευμένοι
- Κουμπί χειροκίνητης σάρωσης (ΣΑΡΩΣΗ).
- Μενού ρυθμίσεων. (3 κουκκίδες)
- Τέσσερις κατηγορίες προστασίας

Κατηγορίες Προστασίας

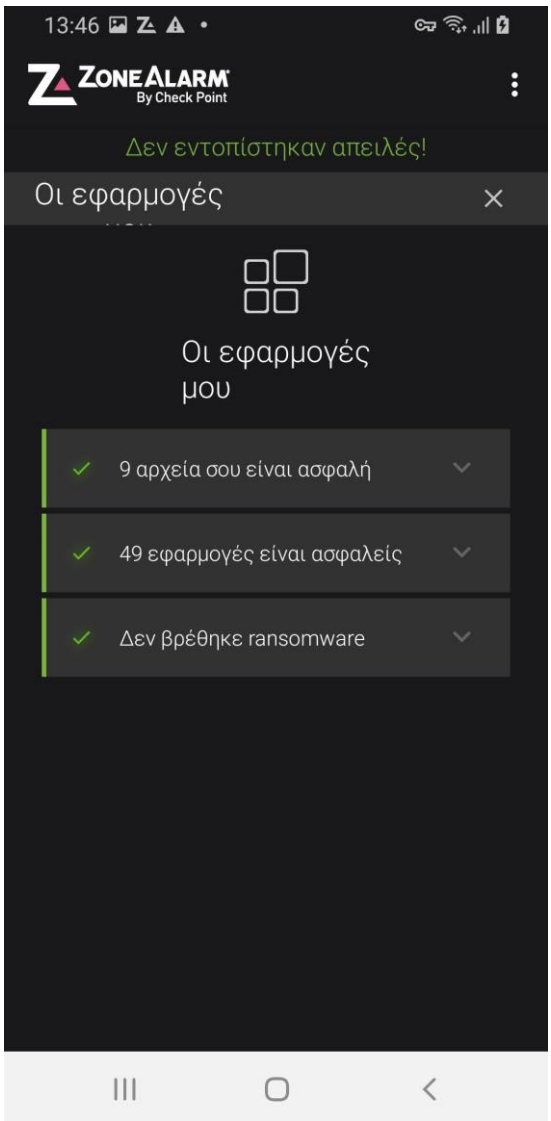
Προστασία Συσκευής

- Ασφάλεια Λειτουργικού Συστήματος Android- Σας ειδοποιεί εάν η συσκευή σας είναι rooted ή όχι.
- Έλεγχος έκδοσης ZoneAlarm - Σας ειδοποιεί εάν η έκδοση ZoneAlarm είναι ενημερωμένη.
- Ειδοποιήσεις ασφάλειας συσκευής - Ανάλογα με τις ανάγκες, διάφορες ειδοποιήσεις μπορούν να εμφανιστούν όταν η ρύθμιση της συσκευής σας ενδέχεται να σας θέσει σε κίνδυνο.



Προστασία Εφαρμογών

- Πλήθος εφαρμογών που προστέθηκαν πρόσφατα που έχουν σαρωθεί και είναι ασφαλείς για εγκατάσταση.
- Συνολικός αριθμός εφαρμογών που έχουν σαρωθεί στην κινητή συσκευή σας που είναι ασφαλείς.
- Έλεγχος για Ransomware επίθεση

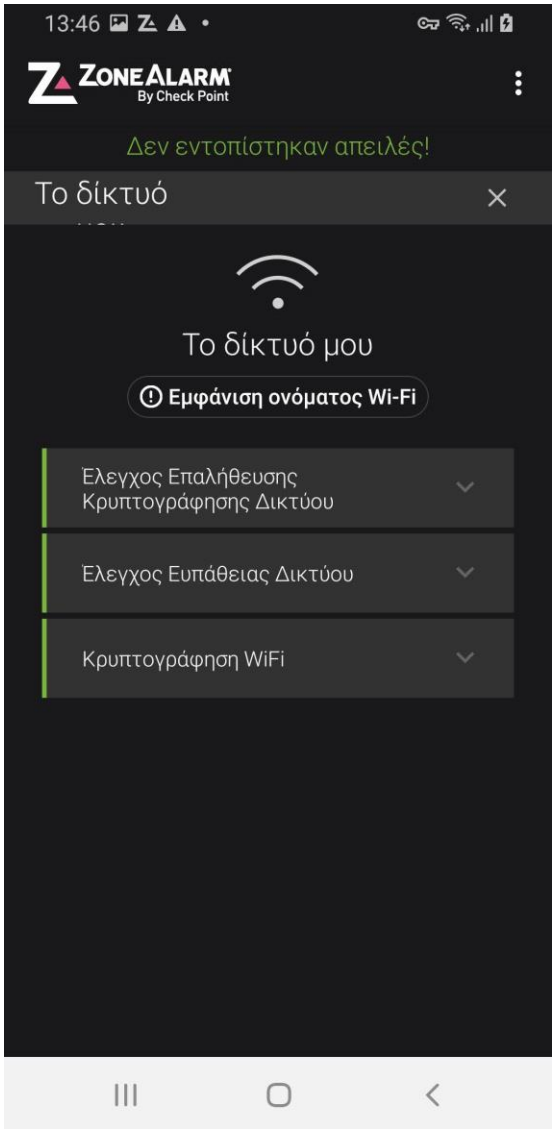


Το Δίκτυο μου

- Έλεγχος επαλήθευσης κρυπτογράφησης δικτύου - Ελέγχει την ακεραιότητα της κρυπτογραφημένης σύνδεσης SSL στο πρόγραμμα περιήγησής σας. Σας ειδοποιεί για τυχόν απόπειρες υποκλοπής δεδομένων

- Έλεγχος ευπάθειας δικτύου - Σάρωση δικτύου για διαρροή κίνησης

- Κρυπτογράφηση Wi-Fi - Ελέγχει τη σύνδεση Wi-Fi για το αν είναι ασφαλής και κρυπτογραφημένη.

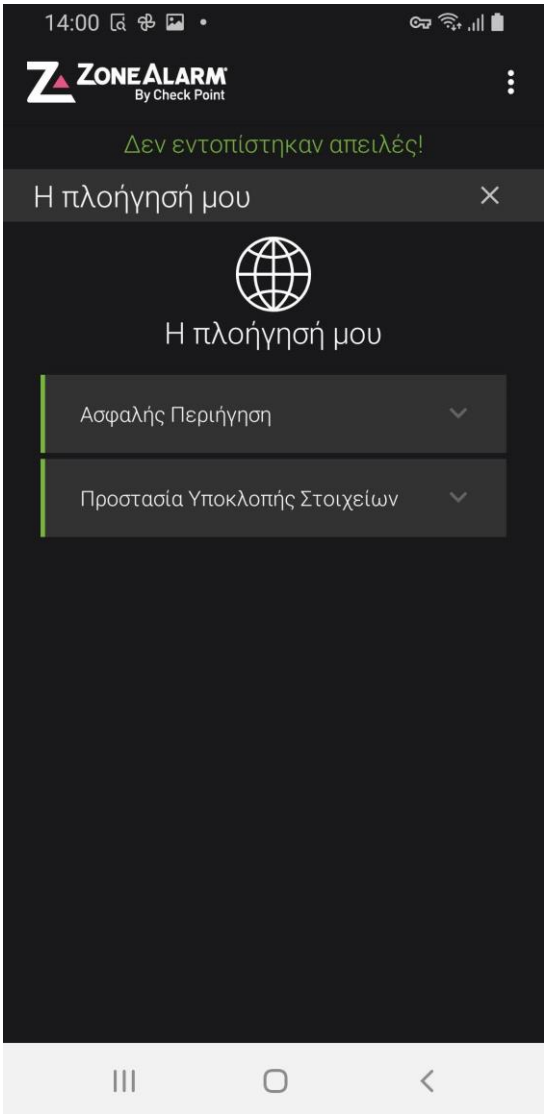


Η πλοήγησή μου

- **Ασφαλής περιήγηση** - σας προστατεύει από κακόβουλους ιστότοπους από ένα πρόγραμμα περιήγησης ιστού. Επίσης αποκλείει την πρόσβαση σε προκαθορισμένες ακατάλληλες κατηγορίες περιεχομένου σε όλα τα προγράμματα περιήγησης και τις πλατφόρμες.

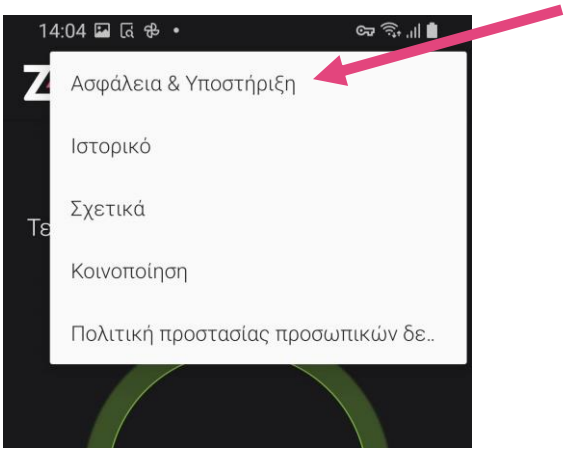
- **Προστασία Υποκλοπής Στοιχείων** (Zero-Phishing)- σας προστατεύει από νέους/άγνωστους ιστότοπους ηλεκτρονικού ψαρέματος με σάρωση πεδίων όπου μπορείτε να εισάγετε δεδομένα αυθεντικοποίησης (authentication).

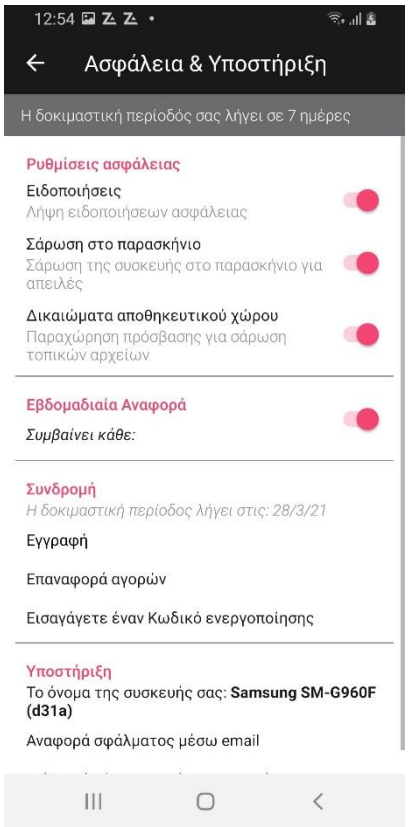
- Δεν μπορείτε να απενεργοποιήσετε επιλεκτικά αυτές τις προστασίες.



Μενού – Ρυθμίσεις

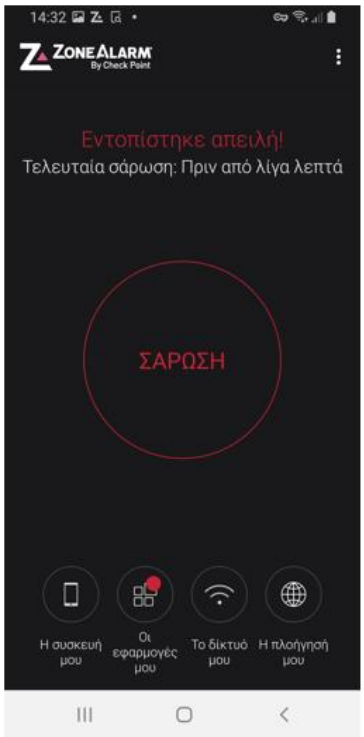
- **Ειδοποιήσεις -** Ενεργοποιήστε και απενεργοποιήστε τις ειδοποιήσεις ασφαλείας στην οθόνη.
- **Σάρωση συσκευής** – Επιλέξτε για το αν η συσκευή θα ελέγχεται από το ZoneAlarm for Institutions συνεχώς στο παρασκήνιο ή όχι . Σε ορισμένες περιπτώσεις οι χρήστες μπορεί να μην θέλουν την ασφάλεια να λειτουργεί συνεχώς ως διαδικασία παρασκηνίου.
- **Άδεια αποθήκευσης** - Ενεργοποιήστε και απενεργοποιήστε την άδεια για πρόσβαση και σάρωση των τοπικών αρχείων.
- **Εβδομαδιαία σύνοψη** - Προγραμματίστε την ημέρα και την ώρα για να λαμβάνετε μια εβδομαδιαία σύνοψη ειδοποιήσεων για συμβάντα που μπορούν να προβληθούν στη συσκευή σας.
- **Συνδρομή** - Εισαγάγετε τον κωδικό ενεργοποίησης, αγοράστε ή επαναφέρετε μια συνδρομή στο Google Play . Ενημέρωση για την κατάσταση της συνδρομής .
- **Αναφορά σφάλματος μέσω email** - Για χρήση μόνο όταν ζητηθεί από υποστήριξη. Δημιουργεί ένα email με αρχεία καταγραφής που αποστέλλονται στο Τεχνικό Τμήμα Υποστήριξης. Τα μηνύματα σφάλματος προορίζονται μόνο για αναφορά και δεν απαντώνται ποτέ.
- **Tutorial** – Σύντομος οδηγός λειτουργίας

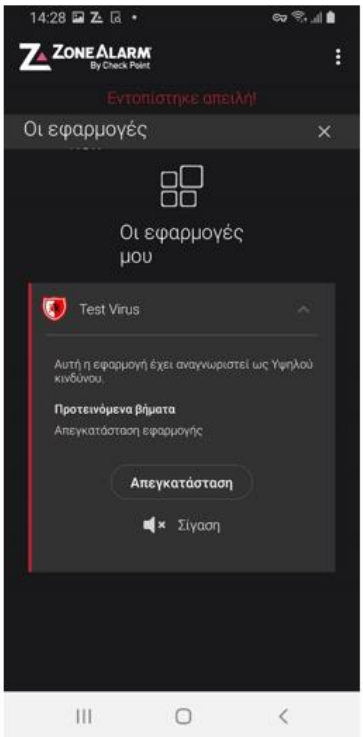


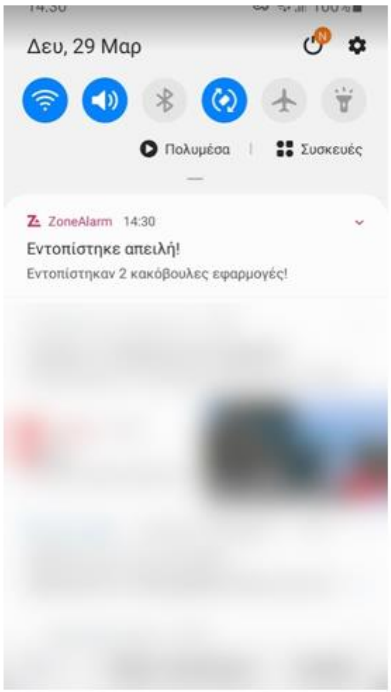


Ειδοποιήσεις Συμβάντων και Ενημερώσεις

- Στις ειδοποιήσεις εφαρμογών και συσκευής θα ενημερώνεστε αυτόματα σας για τα συμβάντα ασφαλείας.
- Η πορτοκαλί ειδοποίηση σημαίνει ότι η συσκευή κινδυνεύει.
- Η κόκκινη ειδοποίηση σημαίνει ότι έχει εντοπιστεί απειλή.








AT&T
6:59 PM
nilexd.tonohost.com
Confirmar
Si no tienes un usuario asignado ingresa con tu documento de identidad
Ingresa tu Pin
Ingresa tu e-mail
Finalizar
¿Olvidaste tu usuario?
¿Problemas para conectarte?
Demo Sucursal Virtual Personas


7:07
pbebank.cc
Check Point
SOFTWARE TECHNOLOGIES LTD
Page Blocked
Access to pbebank.cc is blocked according to the organization's security policy.
Categories: Phishing
If this classification is incorrect click here to report wrong category.


7:08
playboy.com
Check Point
SOFTWARE TECHNOLOGIES LTD
Page Blocked
Access to playboy.com is blocked according to the organization's security policy.
Categories: Sex
If this classification is incorrect click here to report wrong category.

Οδηγός χρήσης iOS Συσκευών

Οφέλη Προϊόντος

Μεταφρασμένο στα Ελληνικά
Όλα τα μενού και τα περιεχόμενα της εφαρμογής είναι πλήρως μεταφρασμένα στα Ελληνικά.

Προστασία προσωπικών δεδομένων
Η ZoneAlarm εγγυάται ότι τα δεδομένα σας παραμένουν εντελώς απόρρητα. Όλες οι αναλύσεις ασφαλείας πραγματοποιούνται στη συσκευή με ανώνυμα metadata που συλλέγονται από το λειτουργικό σύστημα,, το διαδίκτυο και τα δίκτυα.

Προστασία από υποκλοπές
Η ZoneAlarm διασφαλίζει ότι το δίκτυό σας είναι ασφαλές και δεν σας υποκλέπτει κάποιος τρίτος.

Προστασία από ηλεκτρονικές απάτες
Η ZoneAlarm Anti-Phishing τεχνολογία σας προστατεύει από τη διαρροή των διαπιστευτηρίων σας σε γνωστές και άγνωστες ψεύτικες ιστοσελίδες που προσπαθούν να διαπράξουν ηλεκτρονικό "ψάρεμα" (phishing).

Ασφαλής περιήγηση
Περιηγηθείτε στο διαδίκτυο χωρίς καμία ανησυχία – Η ZoneAlarm Mobile Security ελέγχει για κακόβουλα URL σε πραγματικό χρόνο.

Ανάλυση απειλών σε πραγματικό χρόνο
Το ZoneAlarm αξιοποιεί τη μεγαλύτερη βάση δεδομένων πληροφοριών για απειλές στον κόσμο, με το Check Point

Εξατομικευμένες εβδομαδιαίες αναφορές
Η εβδομαδιαία αναφορά συμβάντων ασφαλείας στη συσκευή σάς ενημερώνει σχετικά με τις πιο πρόσφατες απειλές από τις οποίες η ZoneAlarm προφύλαξε τη συσκευή σας.

Ασφαλής περιήγηση για παιδιά
Η ZoneAlarm συνοδεύεται από ένα ενσωματωμένο φίλτρο περιεχομένου που τα παιδιά σας δεν μπορούν να απενεργοποιήσουν ή να αλλάξουν. Επιτρέπει στα παιδιά σας να έχουν πρόσβαση στο διαδίκτυο με ασφάλεια σε όλα τα προγράμματα περιήγησης και τις πλατφόρμες.

Χωρίς διαφημίσεις
Δεν θα βλέπετε διαφημίσεις, ακόμα και κατά τη διάρκεια της δοκιμαστικής έκδοσης.

Αλληλεπιδραστικό περιβάλλον εργασίας χρήστη
Η εφαρμογή ZoneAlarm είναι απλή, γρήγορη και εύκολη στη χρήση.

Απόλυτη εμπειρία συσκευής
Ελάχιστη επίδραση στη διάρκεια ζωής της μπαταρίας και την απόδοση της συσκευής.

Δυνατότητες προϊόντος

Ασφάλεια δικτύου Wi-Fi
Προστατεύει τους χρήστες από το να παγιδευτούν σε επιθέσεις Man-in-the-Middle όταν συνδέονται με Wi-Fi

Κατάταξη ασφάλειας Wi-Fi
Κατατάσσει τα διαθέσιμα ενεργά σημεία γύρω σας με βάση το επίπεδο ασφάλειάς τους, διασφαλίζοντας ότι συνδέεστε με την πιο ασφαλή διαθέσιμη επιλογή.

Zero-Day Anti-Phishing
Αποκλείει επιθέσεις ηλεκτρονικού "ψαρέματος" τόσο από γνωστούς όσο και από άγνωστους ιστότοπους ηλεκτρονικού "ψαρέματος" και εφαρμογές.

Ασφαλής περιήγηση
Η Ελληνική έκδοση του Zone Alarm for Institutions προστατεύει από κακόβουλους ιστότοπους και διατίθεται με αυτόματα προεγκατεστημένη την ρύθμιση πρόσβασης (URL filtering) σε όλες τις εφαρμογές περιήγησης αποκλείοντας ακατάλληλο περιεχόμενο .

Φιλτράρισμα περιεχομένου
Εμποδίζει την πρόσβαση σε προκαθορισμένες κατηγορίες ακατάλληλου περιεχομένου σε όλα τα προγράμματα περιήγησης και πλατφόρμες.

Anti-Bot
Εμποδίζει τους χάκερ να πάρουν τον έλεγχο της συσκευής σας αποκλείοντας επιθέσεις bot.

Ασπίδα συσκευής
Ειδοποιεί το χρήστη για τυχόν επικίνδυνες ρυθμίσεις στη συσκευή.

Ανίχνευση jailbreak
Εντοπίζει ύποπτες συμπεριφορές συσκευής και ειδοποιεί εάν κάποιος έχει αποκτήσει τον έλεγχο του λειτουργικού σας συστήματος.

Στην προστασία δικτύου συσκευών

Η ZoneAlarm Mobile Security χρησιμοποιεί μια μοναδική υποδομή ασφάλειας δικτύου – την Προστασία δικτύου συσκευών (ONP) – για να επικυρώσει όλη την επισκεψιμότητα του χρήστη στη συσκευή χωρίς να μεταφέρει τα δεδομένα του χρήστη στο cloud. Αυτό εξασφαλίζει την προστασία των προσωπικών δεδομένων των χρηστών και επιτρέπει την απρόσκοπτη εμπειρία περιήγησης και τον ελάχιστο αντίκτυπο στην απόδοση και την μπαταρία.

Κάθε σύνδεσμος στον οποίο κάνετε κλικ, ανεξάρτητα από το αν είναι σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ένα μήνυμα σε μια εφαρμογή μέσων κοινωνικής δικτύωσης κ.λπ., επικυρώνεται σε πραγματικό χρόνο με δυναμικές πληροφορίες ασφαλείας που παρέχονται από το Check Point ThreatCloud, το μεγαλύτερο δίκτυο πληροφοριών στον κυβερνοχώρο στον κόσμο. Εάν η διεύθυνση URL εντοπιστεί ως κακόβουλη, για παράδειγμα μια τοποθεσία ηλεκτρονικού "ψαρέματος", αποκλείεται αμέσως και ο χρήστης ειδοποιείται να μην εισέλθει στην τοποθεσία.

Προστασία Eavesdrop

Μία από τις πιο κοινές επιθέσεις που βασίζονται στο δίκτυο σε κινητές συσκευές είναι **Man-in-the-Middle** (MitM), όπου ο εισβολέας ξεγελάει ανύποπτους χρήστες να συνδεθούν σε ένα ύποπτο δίκτυο Wi-Fi.

Οι χάκερ χρησιμοποιούν δύο είδη μεθόδων MitM:

- **SSL striping**: αφαίρεση του πιστοποιητικού SSL χωρίς τη γνώση του χρήστη και αποκρυπτογράφηση της κίνησης.
- **SSL bumping**: χρήση πλαστών πιστοποιητικών SSL για να ξεγελάσουν εφαρμογές και προγράμματα περιήγησης να πιστέψουν ότι χρησιμοποιούν ασφαλείς συνδέσεις.
-

Με αυτόν τον τρόπο, οι εγκληματίες του κυβερνοχώρου μπορούν να υποκλέψουν επικοινωνίες, επιτρέποντάς τους να παρακολουθούν και να κλέβουν δεδομένα κατά τη μεταφορά. Η ZoneAlarm Mobile Security επικυρώνει την ακεραιότητα των συνδέσεων SSL και ειδοποιεί το χρήστη σχετικά με δίκτυα που έχουν παραβιαστεί.

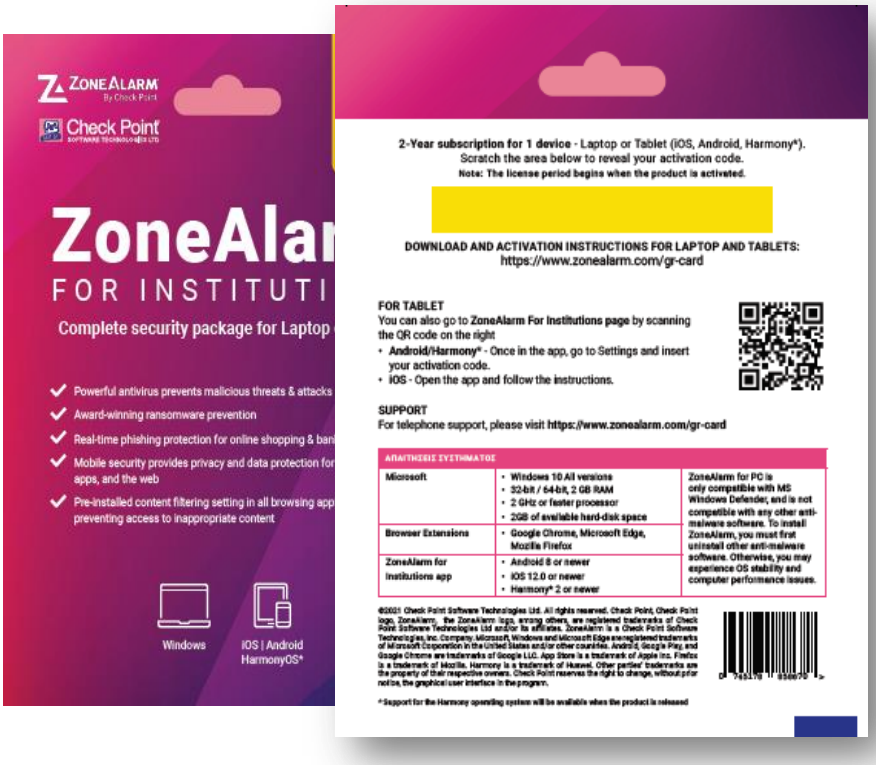
Απαιτήσεις συστήματος:

iOS 12.0 ή νεότερη έκδοση

Οδηγός Εγκατάστασης για iOS

1. Σαρώστε τον κωδικό QR στην κάρτα ή μεταβείτε στη σελίδα λήψης ZoneAlarm For Institutions: https://www.zonealarm.com/gr-card

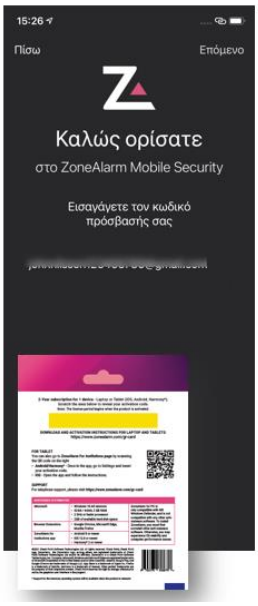
2. Κάντε κλικ στο πράσινο κουμπί λήψης. Εγκαταστείστε και ανοίξτε την εφαρμογή.



Βήματα Εγκατάστασης

Εισαγάγετε τη διεύθυνση email σας

Εισαγάγετε τον κωδικό πρόσβασης από την κάρτα



Σαρώστε προς τα αριστερά για να συνεχίσετε

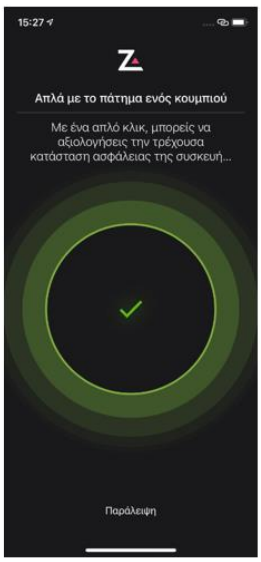
Σαρώστε προς τα αριστερά για να συνεχίσετε

Εισαγάγετε τη διεύθυνση email σας

Εισαγάγετε τον κωδικό πρόσβασης από την κάρτα

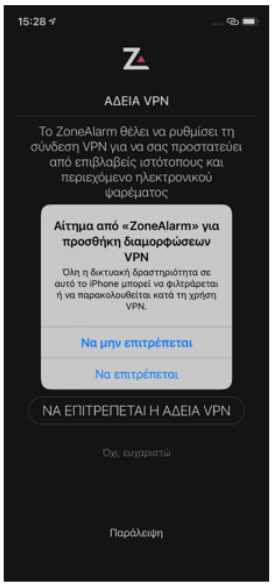
Σαρώστε προς τα αριστερά για να συνεχίσετε

Σαρώστε προς τα αριστερά για να συνεχίσετε



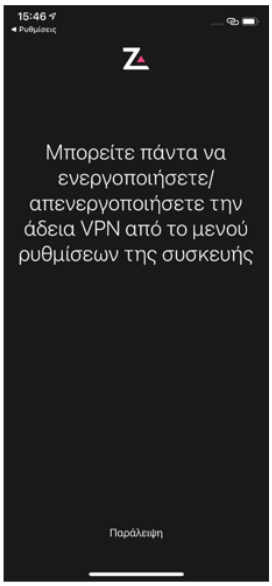
Πατήστε “ΝΑ ΕΠΙΤΡΕΠΕΤΑΙ Η ΑΔΕΙΑ VPN”

Πατήστε "Να επιτρέπεται" για να επιτρέψετε το πιστοποιητικό από το Zonealarm



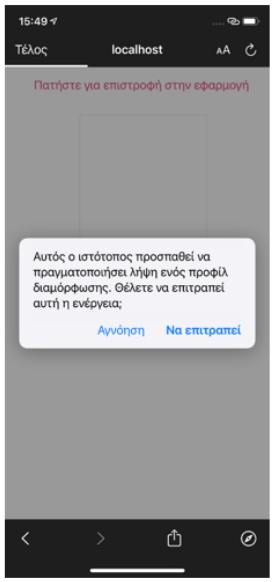
Εισαγάγετε τον κωδικό πρόσβασης της συσκευής

Σαρώστε προς τα αριστερά για να συνεχίσετε

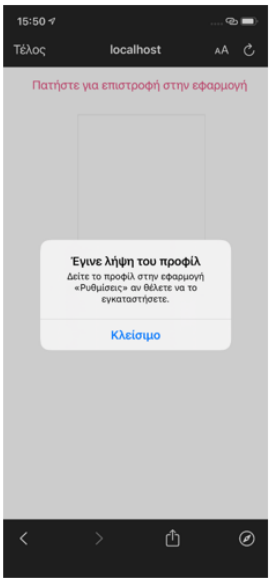


Πατήστε “Εγκατάσταση”

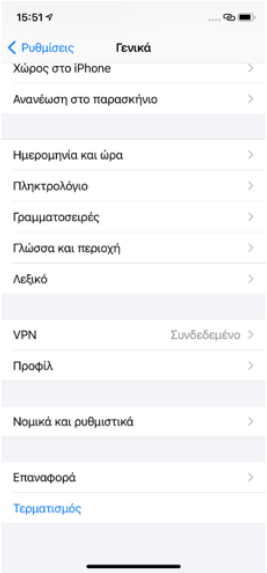
Επιτρέψτε τη λήψη του προφίλ ρύθμισης παραμέτρων



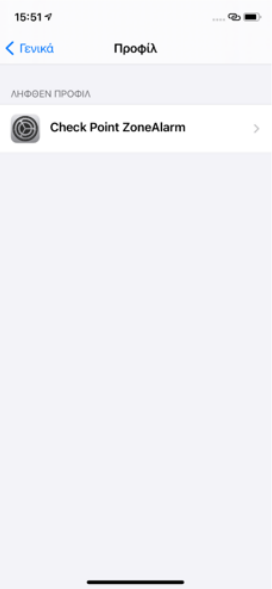
Επιβεβαίωση λήψης προφίλ. Πατήστε ”Κλείσιμο”



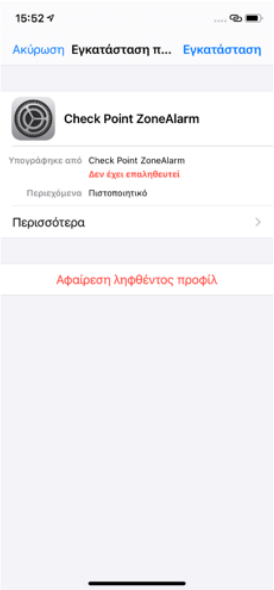
Μετάβαση στις ρυθμίσεις συσκευής/Γενικά. Κατεβείτε προς τα κάτω στην επιλογή”Προφίλ”



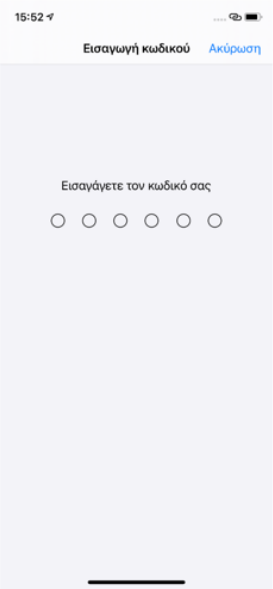
Πατήστε “Check Point ZoneAlarm” Προφίλ



Πατήστε ”Εγκατάσταση”



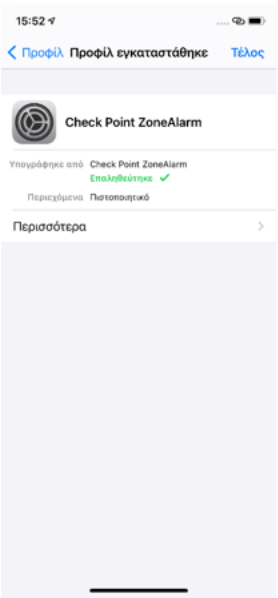
Εισαγάγετε τον κωδικό πρόσβασης της συσκευής



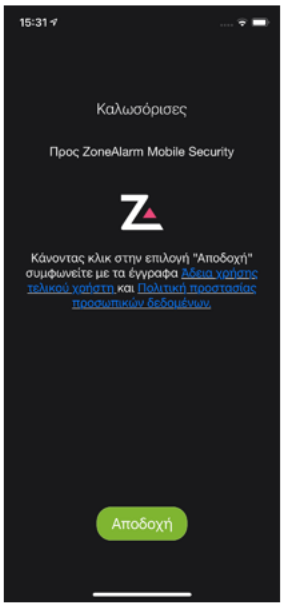
Πατήστε Εγκατάσταση

Εγακταστήστε το πιστοποιητικό Check Point ZoneAlarm

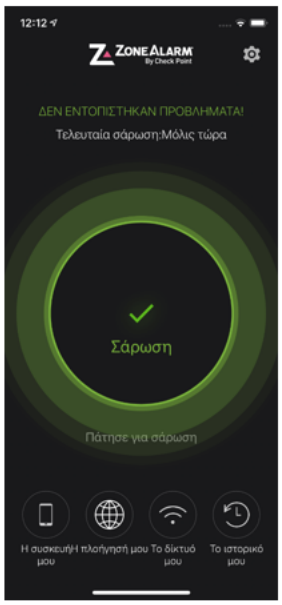
Πατήστε ”Ολοκλήρωση” και πλοηγηθείτε πίσω στην εφαρμογή ZoneAlarm For Institution



Στην εφαρμογή, πατήστε ”Αποδοχή” στο «Άδεια χρήσης τελικού χρήστη»

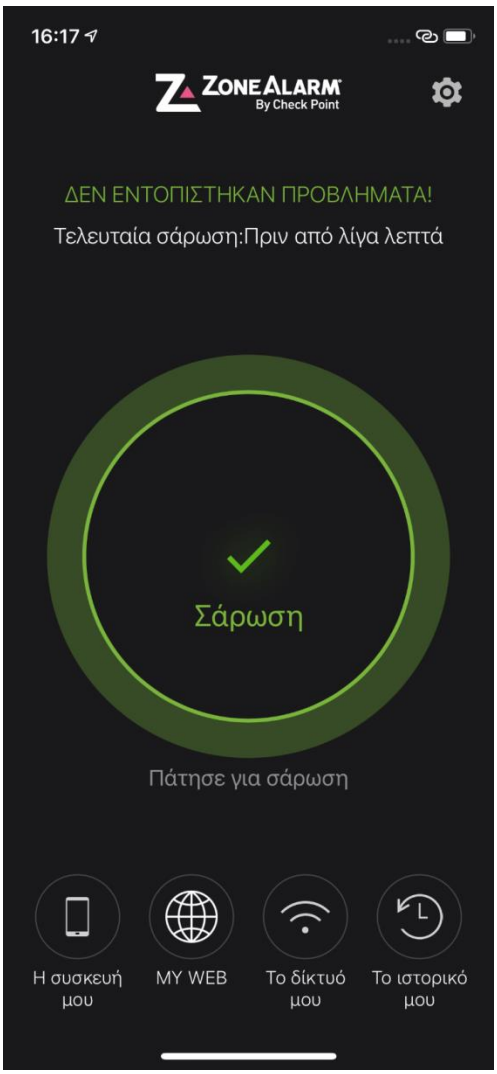


Η συνδρομή σας είναι πλέον ενεργοποιημένη και είστε προστατευμένοι!



Κεντρικό Μενού

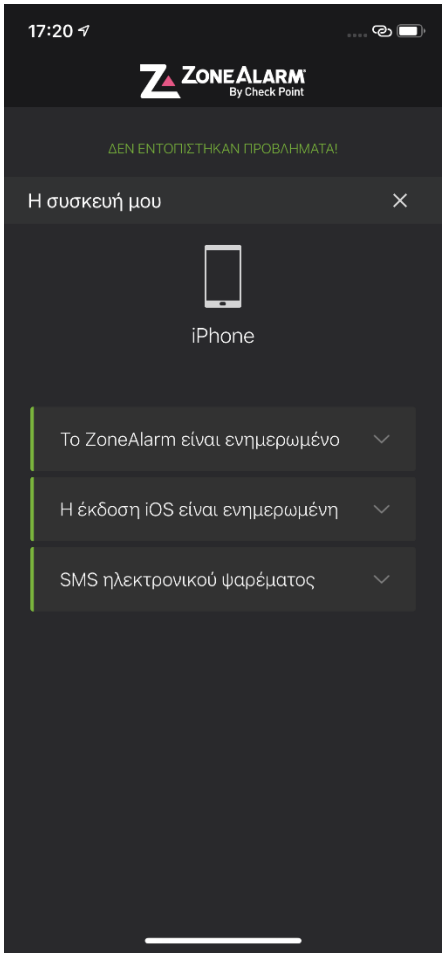
- Τα μηνύματα προβολής και η διεπαφή γίνονται κόκκινα όταν υπάρχουν προβλήματα και πράσινο όταν όλα λειτουργούν καλά και είστε πλήρως προστατευμένοι
- Κουμπί χειροκίνητης σάρωσης (ΣΑΡΩΣΗ).
- Μενού ρυθμίσεων. (Γρανάζι πάνω δεξιά)
- Τέσσερις κατηγορίες προστασίας



Κατηγορίες Προστασίας

Προστασία Συσκευής

- **Προστασία ενημέρωσης εφαρμογών** - Σας ειδοποιεί εάν η εφαρμογή είναι ενημερωμένη ή όχι.
- **Προστασία ενημέρωσης λειτουργικού συστήματος** - Σας ειδοποιεί εάν η έκδοση iOS είναι ενημερωμένη.
- **SMS Phishing** - Προσδιορίζει κακόβουλες ενδείξεις σε μηνύματα κειμένου (SMS) από δήθεν νόμιμους οργανισμούς και τις στέλνει στο φάκελο ανεπιθύμητης αλληλογραφίας της συσκευής. Σ αυτό το σημείο ειδοποιείστε για την κατάσταση και για μηνύματα SMS που εντοπίστηκαν ως ηλεκτρονικό ψάρεμα.

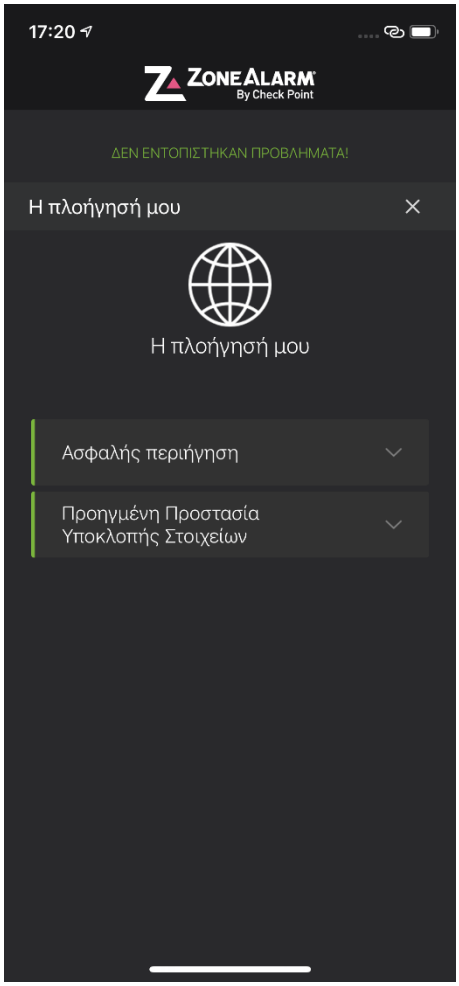


Προστασία Πλοήγησης

- **Ασφαλής περιήγηση** - σας προστατεύει από κακόβουλους ιστότοπους από ένα πρόγραμμα περιήγησης ιστού. Επίσης αποκλείει την πρόσβαση σε προκαθορισμένες ακατάλληλες κατηγορίες περιεχομένου σε όλα τα προγράμματα περιήγησης και τις πλατφόρμες.

- **Προστασία Υποκλοπής Στοιχείων** (Zero-Phishing)- σας προστατεύει από νέους/άγνωστους ιστότοπους ηλεκτρονικού ψαρέματος με σάρωση πεδίων όπου μπορείτε να εισάγετε δεδομένα αυθεντικοποίησης (authentication).

- Μπορείτε να απενεργοποιήσετε επιλεκτικά αυτές τις προστασίες.

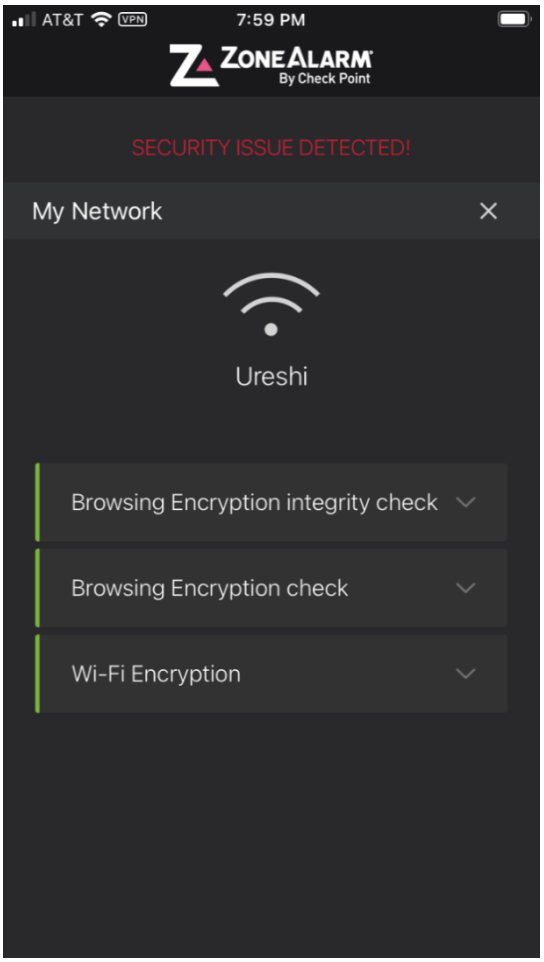


Το Δίκτυο μου

- Έλεγχος επαλήθευσης κρυπτογράφησης δικτύου - Ελέγχει την ακεραιότητα της κρυπτογραφημένης σύνδεσης SSL στο πρόγραμμα περιήγησής σας. Σας ειδοποιεί για τυχόν απόπειρες υποκλοπής δεδομένων

- Έλεγχος ευπάθειας δικτύου - Σάρωση δικτύου για διαρροή κίνησης

- Κρυπτογράφηση Wi-Fi - Ελέγχει τη σύνδεση Wi-Fi για το αν είναι ασφαλής και κρυπτογραφημένη.

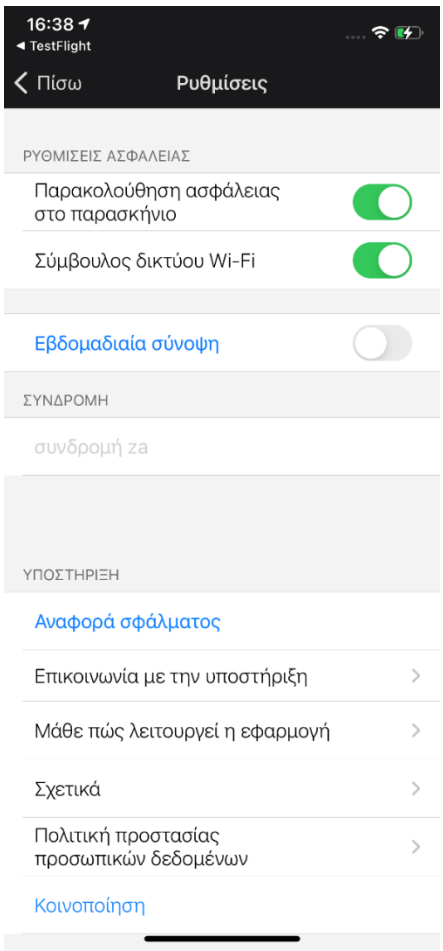


Ιστορικό

- Δείτε το ημερολόγιο συμβάντων 30 ημερών.
- Δείτε Πόσες σαρώσεις δικτύου, νέες σαρώσεις εφαρμογών, σαρώσεις ιστότοπων, απειλές δικτύου, απειλές εφαρμογών και ιστότοποι έχουν αποκλειστεί.
- Καθώς και ένα κυλιόμενο χρονοδιάγραμμα αυτών των συμβάντων με ημερομηνία και ώρες.

Μενού – Ρυθμίσεις

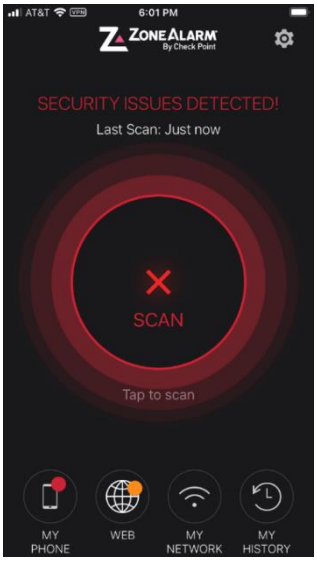
- **Ειδοποιήσεις -** Ενεργοποιήστε και απενεργοποιήστε τις ειδοποιήσεις ασφαλείας στην οθόνη.
- **Σάρωση συσκευής** – Επιλέξτε για το αν η συσκευή θα ελέγχεται από το ZoneAlarm for Institutions συνεχώς στο παρασκήνιο ή όχι . Σε ορισμένες περιπτώσεις οι χρήστες μπορεί να μην θέλουν την ασφάλεια να λειτουργεί συνεχώς ως διαδικασία παρασκηνίου.
- **Άδεια αποθήκευσης** - Ενεργοποιήστε και απενεργοποιήστε την άδεια για πρόσβαση και σάρωση των τοπικών αρχείων.
- **Εβδομαδιαία σύνοψη** - Προγραμματίστε την ημέρα και την ώρα για να λαμβάνετε μια εβδομαδιαία σύνοψη ειδοποιήσεων για συμβάντα που μπορούν να προβληθούν στη συσκευή σας.
- **Συνδρομή** - Εισαγάγετε τον κωδικό ενεργοποίησης, αγοράστε ή επαναφέρετε μια συνδρομή στο Google Play . Ενημέρωση για την κατάσταση της συνδρομής .
- **Αναφορά σφάλματος μέσω email** - Για χρήση μόνο όταν ζητηθεί από υποστήριξη. Δημιουργεί ένα email με αρχεία καταγραφής που αποστέλλονται στο Τεχνικό Τμήμα Υποστήριξης. Τα μηνύματα σφάλματος προορίζονται μόνο για αναφορά και δεν απαντώνται ποτέ.
- **Tutorial** – Σύντομος οδηγός λειτουργίας

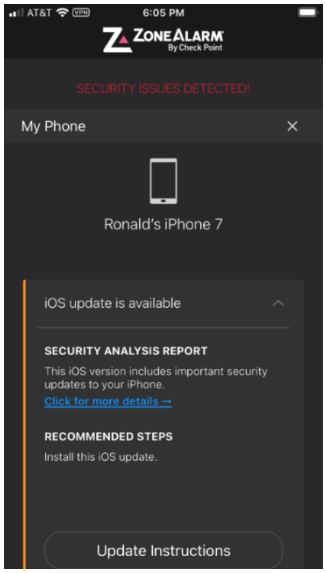


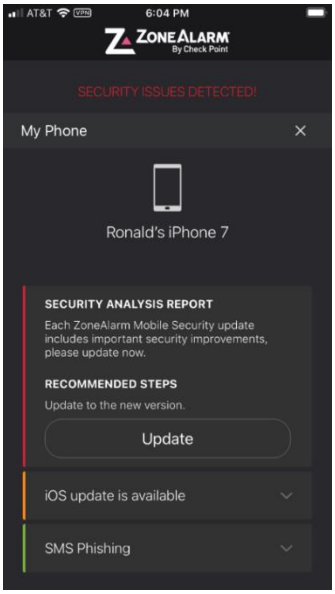
Ειδοποιήσεις Συμβάντων και Ενημερώσεις

Στις ειδοποιήσεις εφαρμογών και συσκευής θα ενημερώνεστε αυτόματα σας για τα συμβάντα ασφαλείας.

- Η πορτοκαλί ειδοποίηση σημαίνει ότι η συσκευή κινδυνεύει.
- Η κόκκινη ειδοποίηση σημαίνει ότι έχει εντοπιστεί απειλή.
- Για ορισμένες ειδοποιήσεις σας δίνεται η δυνατότητα να διορθώσετε το πρόβλημα ή να λάβετε απλώς πρόσθετες πληροφορίες. Για Ορισμένες ειδοποιήσεις επιτρέπεται να τις ορίσετε σε «Σίγαση», έτσι ώστε να μην ενημερώνεστε συνεχώς για κάτι το οποίο γνωρίζετε και έχετε αποδεχτεί. Δεν είναι δυνατή η σίγαση όλων των ειδοποιήσεων.







Ειδοποιήσεις κατά την Πλοήγηση (browsing)

Ειδοποιήσεις της Ασφαλούς Πλοήγησης στους browsers

- Ασφαλής περιήγηση - Αποκλεισμός γνωστού ιστότοπου που προσπαθεί να σας αποσπάσει προσωπικές πληροφορίες.
- Zero Phishing – Ελέγχει έναν άγνωστο ιστότοπο για δείκτες ηλεκτρονικού ψαρέματος και θα σας ειδοποιήσει εάν υπάρχουν ώστε να αποκόψει την επισφαλή πρόσβαση.
- Ασφαλής περιήγηση - Αποκλεισμός μιας προκαθορισμένης ακατάλληλης κατηγορίας περιεχομένου.