



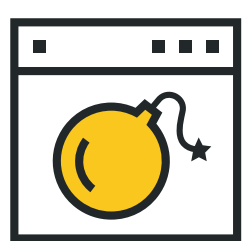
MOBILE
RANSOMWARE

ΠΕΙΤΕ ΑΝΤΙΟ ΣΤΑ ΠΡΟΣΩΠΙΚΑ ΣΑΣ ΑΡΧΕΙΑ

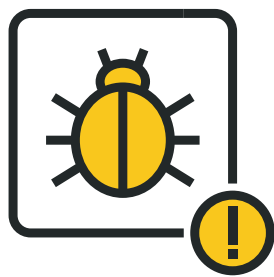
Το ransomware κρατά ομήρους τη συσκευή σας και τα δεδομένα σας, απαιτώντας ανταλλάγματα. Αυτού του είδους το κακόβουλο λογισμικό κλειδώνει την οθόνη της συσκευής σας ή δε σας επιτρέπει να έχετε πρόσβαση σε αρχεία ή λειτουργίες.



ΠΩΣ ΔΙΑΔΙΔΕΤΑΙ;



Κατά την επίσκεψη σε μολυσμένους ή κακόβουλους ιστοτόπους.

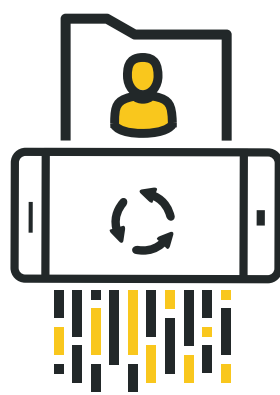


Κατεβάζοντας απομιμήσεις νόμιμων εφαρμογών.



Κάνοντας κλικ σε συνδέσμους ή επισυναπτόμενα που εμπεριέχονται σε phishing emails.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;



Ίσως χρειαστεί να επαναφέρετε τη συσκευή στις εργοστασιακές της ρυθμίσεις, χάνοντας έτσι όλα τα δεδομένα σας.



Ένας επιτιθέμενος μπορεί να έχει πλήρη πρόσβαση στη συσκευή σας και να μοιραστεί τα δεδομένα σας με τρίτους.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;



Δημιουργήστε σε τακτική βάση αντίγραφα ασφαλείας των δεδομένων σας και εγκαταστήστε όλες τις διαθέσιμες ενημερώσεις για το λειτουργικό σύστημα και τις εφαρμογές.



Αποφύγετε τις αγορές από καταστήματα εφαρμογών τρίτων.



Αν υπάρχει διαθέσιμη, εγκαταστήστε μια εφαρμογή ασφαλείας για φορητές συσκευές, που θα σας προειδοποιεί για κάθε περιστατικό ασφάλειας.



Προσέξτε τα emails και τους ιστοτόπους που φαίνονται ύποπτα ή υπερβολικά ωραία για να είναι αληθινά.



Μην παραχωρείτε σε κανέναν δικαιώματα διαχειριστή της συσκευής σας.



Μην πληρώσετε τα λύτρα. Χρηματοδοτείτε εγκληματίες και τους ενθαρρύνετε να συνεχίσουν τις έκνομες δραστηριότητές τους.