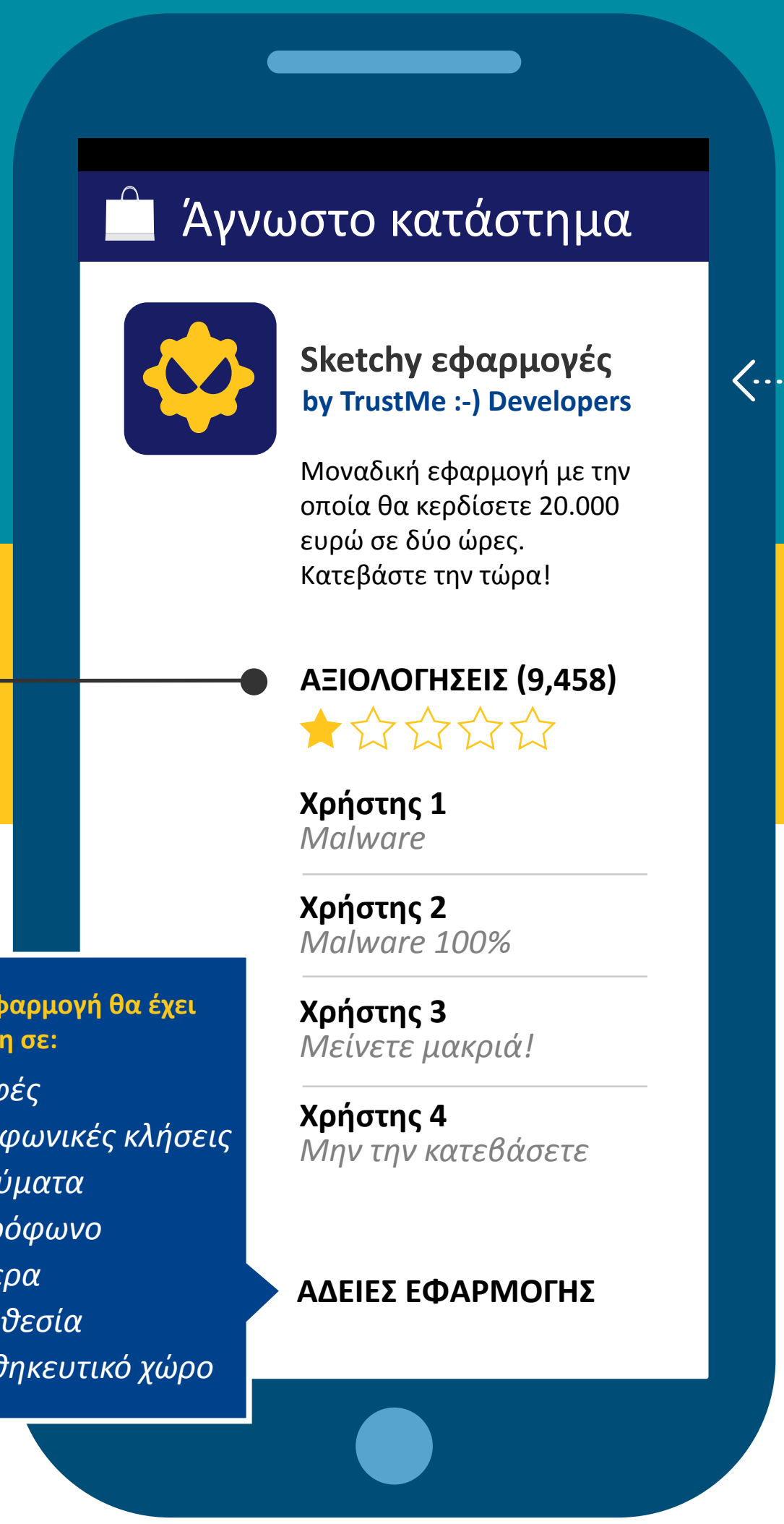
ΕΦΑΡΜΟΓΕΣ

ΔΕΝ ΕΙΝΑΙ ΠΑΙΧΝΙΔΙ!

Εγκαταστήστε εφαρμογές μόνο μέσω των επίσημων καταστημάτων εφαρμογών.

Πριν κατεβάσετε μια εφαρμογή, βρείτε πληροφορίες γι' αυτή και τους δημιουργούς της. Προσοχή στους συνδέσμους που λαμβάνετε μέσω email ή SMS, που μπορεί να σας παραπλανήσουν ώστε να εγκαταστήσετε εφαρμογές από τρίτες ή μη έμπιστες πηγές.



ΕΛΕΓΞΤΕ ΤΙΣ ΚΡΙΤΙΚΕΣ ΚΑΙ ΤΙΣ ΒΑΘΜΟΛΟΓΙΕΣ ΑΛΛΩΝ ΧΡΗΣΤΩΝ.

ΔΙΑΒΑΣΤΕ ΤΙΣ ΑΔΕΙΕΣ ΠΡΟΣΒΑΣΗΣ ΠΟΥ ΖΗΤΑ Η ΕΦΑΡΜΟΓΗ

Ελέγξτε σε ποιες κατηγορίες δεδομένων θα μπορεί να έχει πρόσβαση, καθώς και αν θα μοιράζεται πληροφορίες για εσάς με εξωτερικές οντότητες.

Χρειάζεται όλες αυτές τις άδειες; Αν όχι, τότε μην την κατεβάσετε!

ΕΓΚΑΤΑΣΤΗΣΤΕ ΜΙΑ ΕΦΑΡΜΟΓΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΦΟΡΗΤΕΣ ΣΥΣΚΕΥΕΣ.

Θα εξετάσει όλες τις εφαρμογές της συσκευής καθώς και κάθε επόμενη που θα εγκαταστήσετε και θα σας προειδοποιεί σε περίπτωση εντοπισμού κακόβουλου λογισμικού.

EUROPOL EC3 European Cybercrime Centre

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ
CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware

ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ
MOBILE BANKING

ΤΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΘΑ ΣΑΣ ΚΟΣΤΙΣΕΙ!

Το κακόβουλο λογισμικό mobile banking είναι σχεδιασμένο ώστε να υποκλέπτει τραπεζικά δεδομένα που είναι αποθηκευμένα στη συσκευή σας.

ΠΩΣ ΔΙΑΔΙΔΕΤΑΙ;

Κατά την επίσκεψη σε μολυσμένους ή κακόβουλους ιστοτόπους

Κατεβάζοντας κακόβουλες εφαρμογές

Με τη μέθοδο του phishing

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Υποκλοπή προσωπικών πληροφοριών αυθεντικοποίησης

Χωρίς δικαίωμα αναλήψεις και μεταφορές χρημάτων

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

https://

Κατεβάστε την επίσημη εφαρμογή για φορητές συσκευές της τράπεζάς σας και βεβαιωθείτε ότι επισκέπτεσθε τον επίσημο ιστότοπο της τράπεζας κάθε φορά.

Αποφύγετε την αυτόματη είσοδο (log in) στον ιστότοπο ή την εφαρμογή της τράπεζας.

Μην μοιράζεστε με κανέναν δεδομένα που αφορούν τον τραπεζικό σας λογαριασμό και ιδίως τον κωδικό πρόσβασης.

Αν υπάρχει διαθέσιμη, εγκαταστήστε μια εφαρμογή ασφαλείας που θα σας προειδοποιεί εγκαίρως για οποιαδήποτε ύποπτη δραστηριότητα.

Αν χάσετε το κινητό σας τηλέφωνο, ή αλλάξετε αριθμό, επικοινωνήστε με την τράπεζά σας, ώστε να γίνει επικαιροποίηση των στοιχείων σας.

Μην μοιράζεστε οποιαδήποτε πληροφορία για τον τραπεζικό σας λογαριασμό μέσω SMS ή email.

Χρησιμοποιήστε πάντα μια ασφαλή σύνδεση Wi-Fi για τη σύνδεσή σας στον ιστότοπο ή την εφαρμογή της τράπεζάς σας. Μην το κάνετε μέσω ελεύθερου Wi-Fi!

Ελέγχετε τακτικά τους έντυπους τραπεζικούς σας λογαριασμούς – εφόσον λαμβάνετε τέτοιους.

EUROPOL EC3 European Cybercrime Centre

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware

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.

EUROPOL EC3 European Cybercrime Centre

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware

ΑΠΕΙΛΕΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΙΣΤΟΥ

ΕΛΕΓΞΤΕ ΔΙΠΛΑ ΠΡΙΝ ΚΑΝΕΤΕ ΚΛΙΚ.

Θα μπορούσατε να χάσετε χρήματα, προσωπικά δεδομένα ή ακόμα και αποθηκευμένα αρχεία, αν η συσκευή σας σταματήσει να λειτουργεί. Μην τσιμπάτε!

ΠΩΣ ΘΑ ΜΠΟΡΟΥΣΕ ΝΑ ΣΥΜΒΕΙ;

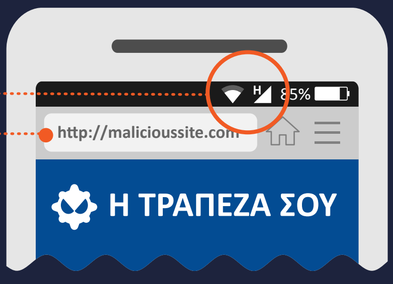
ΕΠΙΘΕΣΕΙΣ PHISHING: Εγκληματίες εξαπατούν τους χρήστες ώστε να δώσουν προσωπικές πληροφορίες, προσποιούμενοι έμπιστες οντότητες. Επιθέσεις γίνονται μέσω email, μηνυμάτων SMS ή ιστοτόπων κοινωνικής δικτύωσης.

ΠΕΡΙΗΓΗΣΗ ΣΕ ΙΣΤΟΤΟΠΟ: Η συσκευή σας μπορεί να μολυνθεί κατά τη διάρκεια μιας απλής επίσκεψης σε έναν μη ασφαλή ιστότοπο.

ΜΕΤΑΦΟΡΤΩΣΗ ΑΡΧΕΙΩΝ: Σε ένα email μπορεί να εμπεριέχονται κακόβουλοι σύνδεσμοι ή μολυσμένα επισυναπτόμενα αρχεία.

ΓΙΑΤΙ ΕΙΝΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟ;

Οι φορητές συσκευές είναι **ΔΙΑΡΚΩΣ ΣΥΝΔΕΔΕΜΕΝΕΣ** στο Διαδίκτυο.



Το **ΜΙΚΡΟ ΜΕΓΕΘΟΣ ΤΗΣ ΟΘΟΝΗΣ ΤΗΣ ΣΥΣΚΕΥΗΣ** συχνά δημιουργεί προβλήματα. Οι περιηγητές στις φορητές συσκευές προβάλλουν τα URLs σε περιορισμένο χώρο, δυσκολεύοντας έτσι τον έλεγχο για το αν ο ιστότοπος είναι ορθός.

Η ΑΝΕΠΙΦΥΛΑΚΤΗ ΕΜΠΙΣΤΟΣΥΝΗ ΤΟΥ ΧΡΗΣΤΗ στην προσωπική φύση της φορητής συσκευής.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

Θα πρέπει να σας βάλουν σε υποψίες ένα SMS ή μια τηλεφωνική κλήση από μια εταιρεία όπου σας ζητάνε προσωπικές πληροφορίες. Μπορείτε να επιβεβαιώσετε ότι το μήνυμα ή η κλήση είναι νόμιμα καλώντας απευθείας στην εταιρεία μέσω της επίσημης γραμμής επικοινωνίας της.

https://

Κατά την περιήγηση στο Διαδίκτυο από τη φορητή σας συσκευή, βεβαιωθείτε ότι η σύνδεση είναι ασφαλής (ένδειξη HTTPS). Μπορείτε πάντα να το ελέγχετε στην αρχή του URL.

Ποτέ μην κάνετε κλικ σε ένα σύνδεσμο ή ένα επισυναπτόμενο αρχείο που εμπεριέχονται σε μη ζητηθέν email ή SMS. Διαγράψτε το αμέσως.

^Bε:%}
W@RY
*)Z#$=

Θα πρέπει να σας βάλει σε υποψίες ένας ιστότοπος που περιέχει ασύντακτες προτάσεις, ορθογραφικά λάθη ή χαμηλή ανάλυση.

Αν υπάρχει διαθέσιμη, εγκαταστήστε μια εφαρμογή ασφαλείας που θα σας προειδοποιεί εγκαίρως για οποιαδήποτε ύποπτη δραστηριότητα.

EUROPOL EC3 European Cybercrime Centre

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

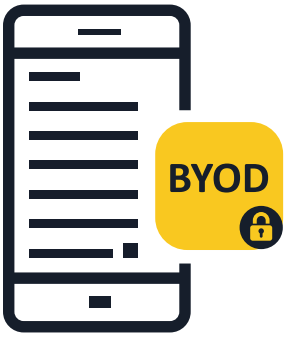
#MobileMalware

MOBILE MALWARE

ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΕΠΑΓΓΕΛΜΑΤΙΕΣ & ΕΠΙΧΕΙΡΗΣΕΙΣ

1 Ενημερώστε το προσωπικό σας για τις απειλές κατά τη χρήση φορητών συσκευών

- Η χρήση των προσωπικών φορητών συσκευών και για επαγγελματικούς σκοπούς εγκυμονεί κινδύνους. Μια επίθεση, που αρχικά έχει στόχο την προσωπική φορητή συσκευή ενός εργαζόμενου, θα μπορούσε να επηρεάσει σοβαρά και την επιχείρηση. Μια φορητή συσκευή είναι ένας υπολογιστής και θα πρέπει να προστατεύεται με όμοιες μεθόδους.



2 Εφαρμόστε εταιρική πολιτική για το bring-your-own-device (BYOD – «φέρε τη δική σου συσκευή»)

- Οι εργαζόμενοι που χρησιμοποιούν τις προσωπικές τους φορητές συσκευές για να προσπελάσουν εταιρικά δεδομένα και συστήματα (ακόμα και emails, ημερολόγια ή λίστες επαφών) οφείλουν να ακολουθούν τις πολιτικές της εταιρείας. Επιλέξτε με προσοχή τις τεχνολογίες που θα χρησιμοποιηθούν για τη διαχείριση και ασφάλεια των φορητών συσκευών και υπενθυμίστε στους εργαζομένους την ανάγκη να είναι προσεκτικοί.

3 Συμπεριλάβετε πολιτικές ασφάλειας για φορητές συσκευές στο ισχύον συνολικό πλαίσιο ασφάλειας

- Αν μια συσκευή δε ανταποκρίνεται στις πολιτικές ασφαλείας, δε θα πρέπει να επιτρέπεται η σύνδεσή της στο εταιρικό δίκτυο, ούτε η πρόσβασή της σε εταιρικά δεδομένα. Οι εταιρείες θα πρέπει να αναπτύξουν τις δικές τους λύσεις Mobile Device Management (MDM) ή Enterprise Mobility Management (EMM).
- Συμπληρωματικά, είναι εξίσου χρήσιμη η εγκατάσταση μιας λύσης Mobile Threat Defence, που θα παρέχει διευρυμένη ορατότητα και σχετική ενημέρωση για τα επίπεδα απειλών σε εφαρμογές, δίκτυα και λειτουργικά συστήματα.

4 Αποφύγετε τη χρήση δημόσιων Wi-Fi δικτύων για πρόσβαση σε εταιρικά δεδομένα

- Κατά κανόνα, τα δημόσια Wi-Fi δίκτυα δεν θεωρούνται ασφαλή. Αν ένας εργαζόμενος προσπελαύνει εταιρικά δεδομένα χρησιμοποιώντας ένα ελεύθερο Wi-Fi δίκτυο σε ένα αεροδρόμιο ή μια καφετέρια, τα δεδομένα αυτά θα μπορούσαν να εκτεθούν σε κακόβουλους χρήστες. Προτείνεται οι εταιρείες να αναπτύξουν πολιτικές «αποτελεσματικής χρήσης» προς αυτή την κατεύθυνση.

5 Ενημερώνετε τακτικά τα λειτουργικά συστήματα και τις εφαρμογές

- Τονίστε στους εργαζόμενους της εταιρείας την ανάγκη να εγκαθιστούν ενημερώσεις λογισμικού και ασφαλείας για το λειτουργικό σύστημα των φορητών τους συσκευών, αμέσως μόλις ειδοποιηθούν για τη διαθεσιμότητα αυτών. Ειδικά για τα λειτουργικά Android, αναζητήστε τις πολιτικές ενημερώσεων που ακολουθούν οι κατασκευαστές των συσκευών και οι πάροχοι υπηρεσιών κινητής τηλεφωνίας. Έχοντας εγκατεστημένες τις πιο πρόσφατες ενημερώσεις, διασφαλίζετε όχι μόνο την ασφάλεια των συσκευών, αλλά και την βέλτιστη και αποδοτικότερη λειτουργία τους.

6 Εγκαταστήστε εφαρμογές μόνο από αξιόπιστες πηγές

- Οι εταιρείες θα πρέπει να επιτρέπουν στους εργαζόμενους την εγκατάσταση εφαρμογών μόνο από επίσημες πηγές για εκείνες τις φορητές συσκευές που συνδέονται στα εταιρικά δίκτυα. Εξετάστε την επιλογή δημιουργίας ενός εταιρικού καταστήματος εφαρμογών μέσω του οποίου οι τελικοί χρήστες θα μπορούν να έχουν πρόσβαση, να μεταφορτώνουν και να εγκαθιστούν εφαρμογές εγκεκριμένες από την εταιρεία. Συμβουλευτείτε έναν προμηθευτή λύσεων ασφαλείας για έτοιμα προϊόντα ή δημιουργήστε τη δική σας πλατφόρμα ενδοεταιρικά.

7 Jailbreak: σε καμία περίπτωση!

- Με τον όρο jailbreak αναφερόμαστε στη διαδικασία αφαίρεσης των περιορισμών ασφαλείας που έχουν ορισθεί από τον πωλητή του λειτουργικού συστήματος, ώστε να μπορεί κάποιος να έχει πλήρη πρόσβαση στο λειτουργικό σύστημα και στα χαρακτηριστικά του. Το jailbreak της συσκευής εξασθενεί την ασφάλειά της, δημιουργώντας κενά ασφάλειας που ενδεχομένως δεν είναι άμεσα εμφανή. Δε θα πρέπει να επιτρέπεται η χρήση στο εταιρικό περιβάλλον συσκευών που έχουν υποστεί jailbreak.

8 Εξετάστε εναλλακτικές λύσεις αποθήκευσης στο cloud

- Οι χρήστες φορητών συσκευών συχνά επιθυμούν να έχουν πρόσβαση σε σημαντικά έγγραφα όχι μόνο μέσω του εταιρικού τους υπολογιστή, αλλά και μέσα από τα ιδιωτικά τους smartphones ή tablets, όταν βρίσκονται εκτός γραφείου. Οι εταιρείες πρέπει να εξετάσουν τη δημιουργία συστημάτων ασφαλούς cloud αποθήκευσης και συγχρονισμού αρχείων, για να ικανοποιήσουν τις ανάγκες αυτές στο πλαίσιο της μέγιστης δυνατής ασφάλειας.

9 Ενθαρρύνετε το προσωπικό σας να εγκαταστήσει λογισμικό ασφάλειας για φορητές συσκευές

- Όλα τα λειτουργικά συστήματα κινδυνεύουν να μολυνθούν. Βεβαιωθείτε ότι οι εργαζόμενοι χρησιμοποιούν, εφόσον υπάρχει διαθέσιμο, λογισμικό ασφάλειας για φορητές συσκευές, το οποίο ανιχνεύει και προστατεύει από malware, spyware και κακόβουλες εφαρμογές, αλλά και αντικλεπτικές λύσεις και λύσεις προστασίας της ιδιωτικότητας.

EUROPOL EC3 European Cybercrime Centre

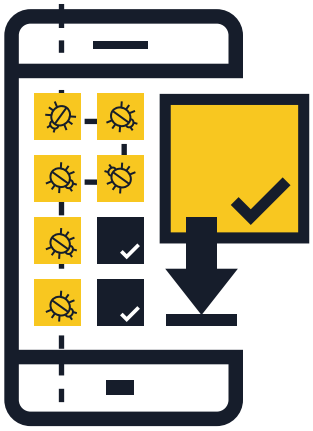
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware

MOBILE MALWARE

ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΘΕΙΤΕ

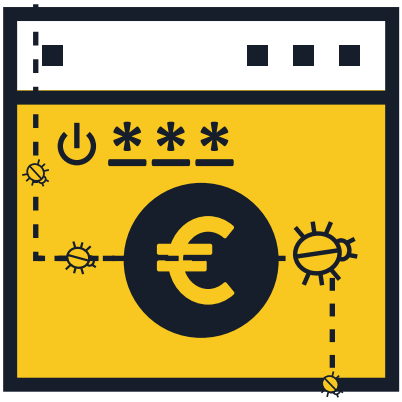


1 Εγκαταστήστε εφαρμογές μόνο από αξιόπιστες πηγές

- **Κάντε αγορές μόνο από αξιόπιστα καταστήματα εφαρμογών** — Πριν κατεβάσετε μια εφαρμογή, βρείτε πληροφορίες γι' αυτή και τους δημιουργούς της. Προσοχή στους συνδέσμους που λαμβάνετε μέσω email ή SMS, που μπορεί να σας παραπλανήσουν ώστε να εγκαταστήσετε εφαρμογές από τρίτες ή μη έμπιστες πηγές.
- **Ελέγξτε τις κριτικές και τις βαθμολογίες άλλων χρηστών,** εφόσον είναι διαθέσιμες.
- **Διαβάστε τις άδειες πρόσβασης που ζητά η εφαρμογή** — Ελέγξτε σε ποιες κατηγορίες δεδομένων θα μπορεί να έχει πρόσβαση, καθώς και αν θα μοιράζεται πληροφορίες για εσάς με εξωτερικές οντότητες. Αν πιστεύετε ότι οι όροι είναι ύποπτοι ή σας κάνουν να αισθάνεστε άβολα, μην κατεβάζετε την εφαρμογή.

2 Μην κάνετε κλικ σε συνδέσμους ή επισυναπτόμενα αρχεία που εμπεριέχονται σε μη ζητηθέντα (spam) emails ή μηνύματα SMS

- **Μην εμπιστεύεστε συνδέσμους που εμπεριέχονται σε μη ζητηθέντα (spam) emails ή γραπτά μηνύματα (SMS και MMS)** — Διαγράψτε τα αμέσως μόλις τα λάβετε.
- **Ελέγξτε προσεκτικά τυχόν συντετμημένα URLs και QR codes** — θα μπορούσαν να οδηγήσουν σε ιστοτόπους με βλαβερό περιεχόμενο ή σε απευθείας εγκατάσταση κακόβουλου λογισμικού στη συσκευή σας. Προτού κάνετε κλικ, χρησιμοποιήστε έναν ιστότοπο προεπισκόπησης του URL για να βεβαιωθείτε ότι η διεύθυνση ιστού είναι ορθή. Προτού σαρώσετε ένα QR code, επιλέξτε έναν αναγνώστη QR που δημιουργεί προεπισκόπηση του ενσωματωμένου ιστοτόπου και χρησιμοποιήστε λογισμικό προστασίας για φορητές συσκευές που σας προειδοποιεί για επικίνδυνους συνδέσμους.



3 Πραγματοποιήστε έξοδο από ιστοτόπους μετά την ολοκλήρωση μιας πληρωμής

- **Ποτέ μην αποθηκεύετε ονόματα χρηστών και κωδικούς πρόσβασης στον περιηγητή ή στις εφαρμογές της φορητής σας συσκευής** — Αν το τηλέφωνό σας ή το tablet χαθεί ή κλαπεί, οποιοσδήποτε θα μπορούσε να εισέλθει στους λογαριασμούς σας. Μετά την ολοκλήρωση της συναλλαγή σας, κάντε log out από το λογαριασμό σας αντί να κλείσετε απλά τον περιηγητή.
- **Αποφύγετε την είσοδο στους online τραπεζικούς σας λογαριασμούς και τις διαδικτυακές αγορές μέσω δημόσιων Wi-Fi δικτύων** — Χρησιμοποιήστε τις mobile banking εφαρμογές σας και πραγματοποιήστε συναλλαγές μόνο μέσα από δίκτυα που γνωρίζετε και εμπιστεύεστε.
- **Δώστε μεγάλη προσοχή στο URL του ιστοτόπου** — Βεβαιωθείτε ότι η διεύθυνση URL του ιστοτόπου είναι η σωστή, πριν κάνετε log in ή αποστείλετε ευαίσθητα δεδομένα σε αυτόν. Θα ήταν προτιμότερο να εγκαταστήσετε στη συσκευή σας την επίσημη εφαρμογή της τράπεζάς σας για να είστε σίγουροι ότι συνδέεστε πάντα στον σωστό ιστότοπο.

4 Ενημερώνετε τακτικά το λειτουργικό σύστημα και τις εφαρμογές

- **Αμέσως όταν λαμβάνετε ειδοποίηση ότι αυτές είναι διαθέσιμες, εγκαταστήστε τις ενημερώσεις του λειτουργικού συστήματος της φορητής συσκευής σας** — Έχοντας εγκατεστημένες τις πιο πρόσφατες ενημερώσεις, διασφαλίζετε όχι μόνο την ασφάλεια της συσκευής σας, αλλά και τη βέλτιστη και αποδοτικότερη λειτουργία της.

5 Απενεργοποιήστε το Wi-Fi, τις υπηρεσίες τοποθεσίας και το Bluetooth όταν δεν τα χρησιμοποιείτε

- **Απενεργοποιήστε το Wi-Fi όταν δεν το χρησιμοποιείτε** — Οι κυβερνοεγκληματίες θα μπορούσαν να προσπελάσουν τα δεδομένα σας όταν η σύνδεση που χρησιμοποιείτε δεν είναι ασφαλής. Αν είναι εφικτό, χρησιμοποιήστε 3G ή 4G σύνδεση δεδομένων αντί να συνδεθείτε σε ένα hotspot. Εξετάστε επίσης τη χρήση μιας υπηρεσίας virtual private network (VPN), ώστε τα δεδομένα σας να κρυπτογραφούνται κατά τη μετάδοσή τους.
- **Μην επιτρέπετε στις εφαρμογές να χρησιμοποιήσουν την τοποθεσία σας, παρά μόνο αν είναι αναγκαίο** — Αυτού του είδους η πληροφορία μπορεί να διαμοιραστεί ή να διαρρεύσει και τελικά να χρησιμοποιηθεί για την προβολή διαφημίσεων με βάση την τοποθεσία σας.
- **Απενεργοποιήστε το Bluetooth όταν δεν το χρειάζεστε** — Βεβαιωθείτε ότι είναι απενεργοποιημένο και όχι απλά αόρατο. Συνήθως, με βάση τις εργοστασιακές ρυθμίσεις της συσκευής σας, οποιοσδήποτε μπορεί να συνδεθεί σε αυτή χωρίς να το γνωρίζετε. Κακόβουλοι χρήστες θα μπορούσαν να αντιγράψουν τα αρχεία σας, να προσπελάσουν άλλες συνδεδεμένες συσκευές ή ακόμα και να αποκτήσουν απομακρυσμένη πρόσβαση στη συσκευή σας για να πραγματοποιήσουν κλήσεις και να στείλουν μηνύματα, κάτι που θα οδηγούσε σε αυξημένες χρεώσεις στο λογαριασμό του κινητού σας τηλεφώνου.

6 Μην αποκαλύπτετε προσωπικές πληροφορίες

- **Μην απαντάτε στέλνοντας προσωπικές πληροφορίες** σε μηνύματα SMS ή emails που ισχυρίζονται πως είναι από την τράπεζά σας ή κάποιο άλλο οργανισμό. Αντί αυτού, επικοινωνήστε απευθείας με το φορέα, για να επιβεβαιώσετε το αίτημά τους.
- **Ελέγχετε τακτικά τους λογαριασμούς κινητής τηλεφωνίας για τυχόν υπερβολικές χρεώσεις** — αν εντοπίσετε κινήσεις που δεν έχουν γίνει από εσάς, επικοινωνήστε αμέσως με τον πάροχο των υπηρεσιών.

7 Jailbreak: ξανασκεφτείτε το!

- Με τον όρο jailbreak αναφερόμαστε στη διαδικασία αφαίρεσης των περιορισμών ασφαλείας που έχουν ορισθεί από τον πωλητή του λειτουργικού συστήματος, ώστε να μπορεί κάποιος να έχει πλήρη πρόσβαση στο λειτουργικό σύστημα και στα χαρακτηριστικά του — **Το jailbreak της συσκευής εξασθενεί την ασφάλειά της,** δημιουργώντας κενά ασφάλειας που ενδεχομένως δεν είναι άμεσα εμφανή.

8 Δημιουργήστε αντίγραφα ασφαλείας των δεδομένων σας

- **Πολλά smartphones και tablets έχουν τη δυνατότητα ασύρματης δημιουργίας αντιγράφων ασφαλείας των δεδομένων** — Ελέγξτε τις διαθέσιμες επιλογές, με βάση το λειτουργικό σας σύστημα. Με τη δημιουργία αντιγράφων ασφαλείας των δεδομένων του smartphone ή του tablet σας, μπορείτε εύκολα να ανακτήσετε προσωπικά δεδομένα αν η συσκευή χαθεί, κλαπεί ή καταστραφεί.

9 Εγκαταστήστε λογισμικό ασφάλειας για φορητές συσκευές

- Όλα τα λειτουργικά συστήματα κινδυνεύουν να μολυνθούν. Αν υπάρχει διαθέσιμο, **χρησιμοποιήστε λογισμικό ασφάλειας για φορητές συσκευές,** το οποίο ανιχνεύει και σας προστατεύει από malware, spyware και κακόβουλες εφαρμογές, αλλά και αντικλεπτικές λύσεις και λύσεις προστασίας της ιδιωτικότητας.

EUROPOL EC3 European Cybercrime Centre
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware