

TOUCH!

עלון המודעות החודשי לביטחון עבורך

שימוש מאובטח באפליקציות לנייד

סקירה כללית

מכשירים ניידים, כמו טאבלטים, סמארטפונים ושעונים חכמים, הפכו לאחת הטכנולוגיות העיקריות בהן אנו משתמשים בחיינו האישיים והמקצועיים. מה שהופך את המכשירים האלה לכל כך חזקים הם אלפי האפליקציות שאנחנו יכולים לבחור בהן. יישומים אלה מאפשרים לנו להיות פרודוקטיביים יותר, לתקשר ולשתף עם אחרים, להתאמן וללמוד, או סתם ליהנות יותר. להלן צעדים שתוכל לנקוט בכדי להשתמש באופן מאובטח ולהפיק את המרב מהאפליקציות הניידות הזמינות.

השגת אפליקציות בטוחות לנייד

פושעי סייבר מתמחים בכישוריהם ביצירה והפצה של אפליקציות דוניות שנראות לגיטימיות. אם אתה מתקין אחת מהאפליקציות האלה, עבריינים יכולים לעתים קרובות להשתלט על המכשיר הנייד או על הנתונים שלך. זו הסיבה שאתה רוצה להבטיח שתוריד רק יישומים ניידים בטוחים ממקורות מהימנים. מה שאתה אולי לא מבין הוא שמות המכשיר הנייד שבו אתה משתמש קובע את האפשרויות שלך להורדת אפליקציות.

עבור מכשירי אפל, הורד רק יישומים ניידים מחנות האפליקציות של אפל. היתרון כאן הוא שאפל מבצעת בדיקת אבטחה של כל האפליקציות הסלולריות לפני שהן זמינות ללקוחות. אפל אמנם אינה יכולה לתפוס את כל האפליקציות הזדוניות, אך סביבה מנוהלת זו מפחיתה באופן דרמטי את הסיכון להורדה של אפליקציות. בנוסף, אפל אכן תמצא אפליקציה שלדעתה היא דונית, היא תסיר אותה במהירות.

עבור מכשירי אנדרואיד, הורידו רק אפליקציות סלולריות מ-Google Play, שמתחזקות על ידי Google. בדומה לאפל, גוגל מבצעת בדיקת אבטחה של כל האפליקציות לפני שהן זמינות ללקוחות. ההבדל עם מכשירי אנדרואיד הוא שאתה יכול גם לאפשר אפשרויות מסוימות המאפשרות לך להוריד אפליקציות מובייל ממקורות אחרים. אנו ממליצים בחום על כך שכן כל אחד, כולל פושעי סייבר, יכול ליצור ולהפיץ בקלות אפליקציות סלולריות דוניות ולהטעות אותך להדביק את המכשיר הנייד שלך.

לא משנה באיזה מותג אתה משתמש, חקור אפליקציה לפני שתוריד אותה. בדוק כמה זמן האפליקציה לנייד הייתה זמינה, כמה אנשים השתמשו בה ומי הספק.

ככל שאפליקציה הייתה זמינה לציבור זמן רב יותר, ככל שאנשים יותר השתמשו והשאירו הערות חיוביות אודותיה, וככל שספקי האפליקציות לעדכנו אותה לעתים קרובות יותר, כך ניתן יהיה לסמוך על האפליקציה. בנוסף, התקן רק אפליקציות שאתה צריך והשתמש בהן. שאל את עצמך, "האם אני באמת צריך את האפליקציה הזו?" לא רק כל אפליקציה עשויה להביא נקודות תורפה חדשות אלא גם בעיות פרטיות חדשות. אם אתה מפסיק להשתמש באפליקציה או שכבר לא מוצא אותה שימושית, הסר אותה מהמכשיר הנייד שלך (אתה תמיד יכול להוסיף אותה בחזרה מאוחר יותר אם תגלה שאתה באמת זקוק לה).

פרטיות והרשאות של אפליקציות

לאחר ההתקנה, ודא שהאפליקציה מגנה על פרטיותך. האם האפליקציה לנייד באמת צריכה לדעת את המיקום שלך או גישה לאנשי הקשר שלך? כאשר אתה מפעיל הרשאות, ייתכן שאתה מאפשר ליוצר של אותה אפליקציה לעקוב אחריך, ואפילו מאפשר לך לשתף או למכור את המידע שלך לאחרים. אם אינך מעוניין להעניק הרשאות אלה, פשוט דחה את בקשת ההרשאה, הענק לאפליקציה את ההרשאה רק כאשר משתמשים בה באופן פעיל, או חפש אפליקציה אחרת העונה על דרישותיך. זכרו, יש לכם המון אפשרויות שם בחוץ.

עדכון אפליקציות

יש לעדכן אפליקציות לנייד, ממש כמו מערכת ההפעלה של המחשב והמכשירים הניידים. עבריינים מחפשים ומוצאים כל הזמן חולשות חדשות באפליקציות ומפתחים דרכים לנצל חולשות אלה. מפתחי האפליקציה יוצרים ומשחררים עדכונים כדי לתקן חולשות אלה ולהגן על המכשירים שלך. ככל שתבדוק או התקן עדכונים לעתים קרובות יותר, כך ייטב. מרבית המכשירים מאפשרים לך להגדיר את המערכת שלך לעדכון אוטומטי של אפליקציות לנייד. אנו ממליצים בחום להפעיל הגדרה זו.

אפליקציות לנייד הן המפתח להפקת המרב מהמכשירים שלך. רק היזהר מאלה שבחרת וודא שאתה משתמש בהם בצורה בטוחה ומאובטחת.



עורך אורח

דומניקה קרוגניל היא מהנדסת אבטחת איכות ומדריכה מוסמכת במכון SANS. היא מחברת משותפת של FOR585: ניתוח סמארטפונים לעומק. להגיע לדומניקה בטוויטר [@domenicacrognal](https://twitter.com/domenicacrognal)

משאבים

כוחו של עדכון: <https://www.sans.org/security-awareness-training/resources/power-updating>

פרטיות: <https://www.sans.org/newsletters/ouch/privacy>

תורגם לקהילה על ידי: גדי מרגלית ודרור ענבר

OUCH! יוצא לאור ומפורסם על ידי חברת Awareness Security SANS, הפצתו ברישיון [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). הנך רשאי להפיץ או להשתמש בעלון זה, כל עוד אתה לא מוכר או מבצע שינויים בעלון זה. עורכי המערכת: וולט סקריבנס, פיל הופמן, אלן וגונר, לס רידוט, פרינסס יאנג.