

כך תשמרו על מכשיר האנדרואיד שלכם

סמארטפונים המבוססים על מערכת ההפעלה אנדרואיד הולכים ונעשים נפוצים יותר ויותר **◆ עם הפופולאריות שלהם, מתרבות הסכנות האורבות למשתמשים בהם - מנוזקות, רושעות ואפילו גניבה ◆ המדריך שמסביר להם איך לשמור על המכשיר שלכם**

צבי קצבורג

נסו להשוות בין מה שהאפליקציה אמורה לעשות לעומת ההרשאות שהיא מבקשת. אם משהו נראה לכם חריג בבקשות, אם כן, וותרו. בדרך כלל תוכלו למצוא אפליקציה אחרת בחנות שמספקת שירות דומה אם לא זהה.

עוד דרך להגן על עצמכם, למקרה שאפליקציה מרושעת כן עברה את ההגנה הראשונית, היא לא לאפשר למכשיר להוריד אפליקציות שמקורן אינו בחנות של גוגל. כנסו להגדרות המכשיר, וחפשו את הכותרת 'ניהול התקנים'. אחת האפשרויות תחת הכותרת הזו מאפשרת לאשר למכשיר התקנה של יישומים לא מוכרים, כלומר התקנה של קבצי apk (קבצי ההתקנה של אנדרואיד) וכן התקנה של קבצים ממקורות אחרים ברשת. וודאו שהתיבה אינה מסומנת כדי לא לאפשר לאפליקציות להוציא כאלו שמגיעות מהחנות להיות מותקנות במכשיר שלכם. מכיוון שיישומים זדוניים יכולים לשנות הגדרות במכשיר, בדקו מדי פעם שהתיבה אכן נקייה.

במקרה של אובדן או גניבה, לחץ כאן...

אף אחד לא רוצה שזה יקרה לו, וכולנו מפחדים מהרגע הזה, אבל מה קורה אם המכשיר הולך לאיבוד או שגונבים אותו? גוגל בעצמה מספקת שירות שמאפשר במקרה הצורך לאתר את המכשיר מרחוק. קוראים לו 'ניהול מכשיר האנדרואיד'. כדי לאפשר את השירות הזה במכשיר יש לגשת למגירת האפליקציות ולחפש אפליקציה

שמכונה 'הגדרות Google' - אייקון אפור שעליו האות g וכן גלגל שיניים. אחת האפשרויות בתפריט, האחרונה בדרך כלל, היא 'ניהול מכשיר האנדרואיד'. לחיצה עליו מציגה שתי תיבות סימון: אחת שמאפשרת לאתר את המכשיר מרחוק, והשנייה מאפשרת נעילה ומחיקה מרחוק. לאחר שמאשרים את ההגדרות הללו, או רק אחת מהן, במקרה של אובדן המכשיר או גניבתו ניגשים דרך דפדפן אינטרנט כלשהו, ולא משנה אם מדובר במחשב או במכשיר נייד, לאתר הניהול שנמצא כאן. לאחר שמזדהים עם שם המשתמש והסיסמה בגוגל, מגיעים למסך שמציג במפת גוגל עד מהירה את המיקום של המכשיר שנעלם לכם, ובעצם כל מכשיר שמבוסס על אנדרואיד של גוגל שנמצא ברשותכם, בדיוק של עד כ-25 מטרים, אם המכשיר עובד כמובר. בתפריט מוצגות שתי אפשרויות. אחת מהן מאפשרת להשמיע צלצול

ל מומחה אבטחה יספר לכם שלא משנה עד כמה מערכת מוגנת באמצעות תוכנות ואפליקציות, הגורם האנושי הוא החשוב ביותר. זה נכון גם עבור מכשיר האנדרואיד שאתם מחזיקים בידכם. עוד לפני שימוש באפליקציות כאלו או אחרות, יש כמה תהליכים ודרכי התנהגות שיאפשרו לכם לשמור על המכשיר שלכם, ולמזער כמה שאפשר את ההשפעות של הסכנות שאורבות בכל פינה.

קו האבטחה הראשון, וכנראה שזה לא יפתיע אף אחד, הוא להשתמש בסיסמה כלשהי שללא הכנסתה לא ניתן יהיה פתוח את המכשיר במסך הנעילה. כדי להגדיר סיסמה חפשו את האפשרות 'מסך נעילה' בתפריט ההגדרות של המכשיר, ולאחר מכן לחצו על האפשרות 'נעילת מסך'.

במסך הבא שיופיע תמצאו רשימה ארוכה של אפשרויות נעילה, כולל רמת האבטחה שהן מספקות. כמו שתראו, הגנה באמצעות סיסמה היא

ההגנה החזקה ביותר, והגנה באמצעות PIN (מספרים בלבד) היא הבאה בתור מבחינת חוזק. שימוש בדפוס (תנועה בין נקודות על שמוצגות המסך בסדר הנכון) מספק אבטחה ברמה בינונית. בכל מקרה, בחרו אפשרות, קבעו את הסיסמה המבוקשת וזכרו אותה. בלעדיה לא תוכלו גם אתם להיכנס למכשיר.

זהירות - אפליקציה!

אין כמעט משתמש במכשיר סמארטפון או טאבלט שמבוסס על אנדרואיד שלא מוריד

לפחות כמה יישומים למכשיר שלו. עם זאת, למרות שלכאורה ניתן תמיד לסמוך על חנות האפליקציות של גוגל, Google Play, באופן מעשי זה לא כך. משתמשים ותיקים ומנוסים כבר יודעים שלמרות ההגבלות השונות הצליחו פושעי מחשב להשתיל בחנות אפליקציות שכללו סוסים טרויאנים ורושעות אחרות, והסתירו אותן מאחורי משחק חינמי או מאחורי אפליקציה שימושית כלשהי.

אמנם אי אפשר לזהות רק בזכות שימוש בעיניים אפליקציה זדונית, אך כל משתמש יכול לבצע לפחות דבר אחד: לבדוק את ההרשאות שמבקשת האפליקציה מהטלפון לפני שמתקינים אותה. אין סיבה שמשחק יבקש, לדוגמה, הרשאה לשימוש במצלמה של המכשיר, או שתוכנה שאמורה לספק לכם מאגר טפטים לדפי הבית השונים תבקש הרשאת גישה לאינטרנט ולאנשי הקשר שלכם.

