



אבטחת המכשירים הניידים שלך

סקירה כללית

התקנים ניידים הם דרך מדהימה וקלה לתקשר עם חברים, לעשות קניות או פעולות בחשבון הבנק באינטרנט, לצפות בסרטים, לשחק במשחקים ולבצע מספר עצום של פעילויות אחרות. בגלל שהתקנים אלו הם חלק חשוב כל כך בחייך, חשוב לאבטח את המכשירים על מנת לשמור עלייך ומכשירך בטוח ומאובטח.

אבטחת המכשירים שלך

זה עשוי להפתיע אותך לדעת כי הסיכון הגדול ביותר למכשיר הנייד שלך הוא כנראה לא פושעי סייבר אלא אתה. יותר סביר שתאבד או תשכח את המכשיר הנייד מאשר שמישהו יפרוץ למכשיר. הדבר הראשון שאתה צריך לעשות כדי להגן על המכשירך הוא לאפשר נעילת מסך אוטומטית כאשר המכשיר במנוחה. משמעות הדבר היא כי כאשר אתה רוצה להשתמש במכשיר שלך, אתה צריך לפתוח את המסך עם קוד, זיהוי הפנים או טביעת האצבע שלך. אם המכשיר שלך אבד או נגנב, זה מבטיח כי יהיה הרבה יותר קשה לפתוח את המכשיר ולקבל גישה למידע. בתור בונוס, אצל רוב המכשירים הניידים, יש אפשרות לבצע הצפנה בנוסף לנעילת המסך, זה מסייע בהגנה על הנתונים המאוחסנים במכשיר.

הנה כמה טיפים נוספים כדי לסייע בהגנה על המכשירים שלך:

- עדכונים:** הפעל עדכון אוטומטי במכשירים שלך, כך שהם תמיד יפעילו את הגרסה העדכנית ביותר של מערכת ההפעלה והאפליקציות. התוקפים תמיד מחפשים חולשות חדשות בתוכנה, הספקים כל הזמן מוציאים עדכונים ותיקונים כדי לתקן את החולשות. שמירה על עדכון המכשירים שלך הופך אותם הרבה יותר מוגנים מפריצה. בעת בחירת מכשיר אנדרואיד חדש, מומלץ להסתכל על מחויבותו של הספק לעדכן את המכשיר. מוצרי אפל מתעדכנים על ידי החברה עצמה, בעוד שמכשירי אנדרואיד מתעדכנים על ידי הספק שמכר לך את ההתקן, ולא כל הספקים מעדכנים את המכשיר באופן פעיל. אם אתה משתמש בהתקן ישן שאינו נתמך עוד או לא ניתן לעדכן, יש לשקול לרכוש התקן חדש הנתמך במלואו.
- מעקב:** התקן או הפעל תוכנה ממקור מהימן כדי לעקוב מרחוק את המכשיר הנייד שלך דרך האינטרנט. בדרך זו, אתה יכול להתחבר אליו דרך האינטרנט ולמצוא את המיקום שלו אם המכשיר אבד או נגנב, ובמקרה הגרוע ביותר, ניתן למחוק מרחוק את כל המידע שלך.

3. **אפליקציות מהימנות** התקן רק יישומים שאתה באמת צריך וממקורות מהימנים. עבור מערכת הפעלה של אפל, התקנים כגון אייפד או אייפון, השתמש בחנות האפליקציות של אפל. עבור מכשירי אנדרואיד, השתמש בחנות של גוגל; עבור טאבלט של אמזון, להשתמש בחנות האפליקציות של אמזון. אמנם ייתכן שתוכל להתקין יישומים מאתרים אחרים, אלה אינם מאומתים וסביר להניח שהם עלולים להיות נגועים או דוונים, כל אחד מהם יכול לסכן את הפרטיות שלך. כמו כן, תוודא כי לאפליקציה יש הרבה ביקורות חיוביות והיא מתעדכנת באופן פעיל על ידי הספק לפני שהורדת את האפליקציה. התרחק מאפליקציות חדשות, יישומים עם מעט מאוד ביקורות, או אפליקציות אשר מתעדכנות לעתים רחוקות.

4. **אפשרויות פרטיות:** התקנים ניידים אוספים מידע נרחב אודותיך, במיוחד בגלל שאתה לוקח אותם לכל מקום שאתה הולך. יש לסקור ביוסודיות את הגדרות הפרטיות של המכשיר, כולל מעקב אחר מיקום, ולוודא הודעות רגישות (כגון קודי אימות) לא מופיעים על המסך כאשר ההתקן נעול.

5. **עבודה:** ודא שכל מכשיר נייד שבו אתה משתמש לצורך עבודה מורשה לשימוש בעבודה. במהלך העבודה, עלייך להיות זהיר במיוחד ולעולם לא לקחת תמונות או וידאו אשר עשויות בטעות להכיל מידע רגיש, כגון תמונות של לוחות או מסכי מחשב.

המכשיר הנייד שלך הוא כלי רב עוצמה - אחד שאנחנו רוצים שתהנה ותשתמש בו. לעקוב אחר כמה צעדים פשוטים אלו יכולים לשמור עלייך ועל המכשיר שלך מאובטח.



עורך אורח

ג'וראן בקרס הוא מומחה לאבטחת ניידים ב-NVISO, מחבר של קורסים OWASP MASVS ו-MSTG, מדריך של מכון SANS ומחבר של SEC575: אבטחת מכשירים ניידים וקורס האקר לבן. ניתן למצוא את ג'וראן בלינקדאין <https://www.linkedin.com/in/beckersjeroen>.

משאבים

כוחו של עדכון: <https://www.sans.org/security-awareness-training/resources/power-updating>
להשתמש באופן מאובטח באפליקציות למכשירים ניידים: <https://www.sans.org/newsletters/ouch/securely-using-mobile-apps>
התקפות מסרים / סמסטים: <https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltb46b447ff815ff84/6047f261f9638443346d63ff/201912-OUCH-December-Hebrew.pdf>
סיסמאות: <https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Hebrew.pdf>
וישינג - התקפות שיחות טלפון והונאות: <https://www.sans.org/newsletters/ouch/existing>
תורגם לקהילה על ידי: גדי מרגלית ודרור ענבר

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Awareness Security, 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 וגונו, לס רידוט, פרינסס יאנג.