מניעת רוגלות מהטלפון הנייד

אם את מרגישה שהוא עוקב אחריך, יודע מה המיקום שלך, עם מי את מדברת ומה סימסת רק לחברה הכי קרובה - יתכן שהושתלו לך רוגלות בנייד. דרכי התמודדות:

- **רכישת מכשיר חדש -** דרך אחת להפסקת מעקב טכנולוגי באמצעות הנייד היא רכישה של סלולרי חדש וכרטיס SIM חדשים. יש לרשום אותם אצל ספק הסלולר על שמך בלבד, ללא שותפים.
- **טלפון שהתקבל במתנה -** מומלץ לא להשתמש בטלפון שהתקבל במתנה. אם את רוצה בכל זאת להשתמש בו, פרמטי אותו לפני התחלת השימוש כדי לוודא שהוא נקי ממערכות מעקב נסתרות.
- **פירמוט הטלפון הנייד האישי -** במידה וברצונך להישאר עם הסלולרי הקיים ויש חשד שמכיל רוגלה, תוכלי לאפס את הטלפון הנייד להגדרות המקוריות (כפי שהיו בעת הרכישה שלו, נקי מאפליקציות וכו'). חשוב לפני הפירמוט לוודא שיש לך גיבוי לכל השירותים הדיגיטליים והמידע החשוב לך.
- **אי מסירת מכשיר הסלולר לגורם אחר -** על מנת למנוע מצב של השתלת רוגלה במכשיר הסלולר הפרטי שלך, ללא ידיעתך, מומלץ להימנע ממסירת מכשירך לגורם אחר, כולל בני משפחה.
- **תיקון מכשיר הסלולר -** מומלץ לעשות שימוש במעבדה שהסבירות כי הצד שכנגד לא יוכל לאתרה בקלות, כמו גם לומר למעבדה שהאדם היחיד שיכול לאסוף את הטלפון מהתיקון, הוא אך ורק את. במקרים מחמירים אף יותר, פתחי את הבקשה לתיקון במעבדה על שם אחר (שאיננו שמך). כמו כן, במכשירי אנדרואיד, ניתן להגדיר בטלפון מצב "תיקון" כדי למנוע גישה לתמונות וקבצים פרטיים.

לפני החלפת מכשיר סלולארי יש לוודא:

- **"ניקוי" המכשיר** – לפני מעבר למכשיר חדש, מומלץ לבצע "איפוס להגדרות יצרן". מחיקה פשוטה של הנתונים האישיים אינה מספיקה, משום שניתן לשחזרם בקלות.
  באיפון: הגדרות « כללי « איפוס « מחק את כל התוכן וההגדרות
  באנדרואיד: הגדרות « כללי « גיבוי ואיפוס « שחזור נתוני יצרן

- **כרטיס SIM** : מידע רב נשמר גם בכרטיס ה-SIM. במידה שלא ניתן להעביר אותו למכשיר החדש, יש להשמיד פיזית/לגזור את הכרטיס הישן בכדי למנוע מאדם אחר לעשות בו שימוש.

- **מעבדה מורשית** - במידה שנדרש למסור מכשירים לתיקון מומלץ להשתמש בשירותי מעבדה מורשית בלבד.

טיפים להגנה על טלפונים ושעונים חכמים

- **נעילה אוטומטית -** יש לוודא נעילה אוטומטית בעת סיום השימוש והוספת סיסמה או זיהוי ביומטרי כגון טביעת אצבע או זיהוי פנים לפתיחת המכשיר.
- **הורדת אפליקציות מהחנות הרשמית בלבד** - מומלץ להתקין יישומים (אפליקציות) למכשיר רק מחנויות האפליקציות הרשמיות – Google Play ו-AppStore.
- **עדכוני תוכנה** - יש להקפיד על ביצוע עדכון למערכת ההפעלה מיד עם פרסומו. כמו כן, מומלץ להגדיר עדכוני תוכנה אוטומטיים לכלל המכשירים והאפליקציות.
- **סיסמאות** - מומלץ לבחור בסיסמה שונה לכל חשבון. ניתן להשתמש באפליקציה לניהול סיסמאות השומרת את כלל הסיסמאות ומצריכה לזכור רק סיסמה אחת. כמו כן, מומלץ לבצע אימות דו שלבי לכל האפליקציות המאפשרות זאת.
- **גיבויים** - מומלץ לבצע גיבוי עיתי לכל המידע שבמכשיר. ניתן לגבות על התקן חיצוני או בשרות ענן, כך במידה והמכשיר ייגנב / יפגע, ניתן יהיה לשחזר את המידע המגובה (אנשי קשר, קבצים, תמונות וכד')
- **הודעות חשודות** - יש להיזהר מהודעות המגיעות מגורמים חשודים. כמו כן, אין ללחוץ על קישורים וצרופות לא מוכרים או חשודים. בכל מקרה יש להיכנס לאתרים רק דרך חיפוש בלתי תלוי.