

# שנה/י את ההתנהגות שלך כדי למזער את המעקב הדיגיטלי

מעקב משפיע על כולנו, לא משנה היכן אנחנו גרים ומה אנחנו עושים. בעוד שחלקנו עשויים להיות מושפעים ישירות, אחרים עשויים פשוט לרצות לדעת אילו אמצעים הם יכולים לנקוט כדי להגן על התקשורת והנתונים שלהם מפני מעקב וריגול. להלן מספר צעדים להתחיל לחשוב אליהם לשיפור והגנה על הפרטיות בשגרת היומיום שלכם.

## עוגיות

שימו לב למה אתם מאשרים כשאתם נכנסים לאתרים. הגדירו את הדפדפן שלכם למחוק קובצי עוגיות בכל פעם שאתם סוגרים אותו. אם הפרטיות חשובה לכם במיוחד תשקלו לעבור לדפדפן מוכוון פרטיות שאיננו מאחסן עוגיות כמו Brave ו-Firefox.

## סיסמאות

כדאי ליצור סיסמאות חזקות. לא כדאי להשתמש באותה סיסמה פעמיים. אם השתמשו בסיסמה מסוימת באתר אחד, אל תשתמשו בה באתר אחר.

כדאי להשתמש ב"מנהל סיסמאות". מנהל סיסמאות יבחר לכם סיסמאות שאי אפשר לזכור, ישמור אותם אצלו וימלא אותם בלי שתצטרכו לעשות כלום, (Lastpass, bitwarden).

## אימות דו-שלבי

אבטח את החשבונות שלך באמצעות אימות דו-שלבי (two-factor authentication) - מנגנון שנועד להבטיח שאם גנבו לכם את הסיסמה - הם לא יצליחו להשתמש בה. האימות הראשון זה הסיסמה (או "שאלה סודית"), ובדרך כלל יש לאמת הזיהוי השני עם משהו שברשותך האישית - כמו הטלפון שלך.

## חסמת פרסומות

כמעט בכל אתר בו אתם גולשים יש עשרות ולעיתים גם מאות מנגנוני ניטור, שחלקם מופיעים כפרסומות ואת חלקם אנחנו בכלל לא רואים. מנגנונים אלה אוספים מידע אישי שבעזרתו ניתן לקטלג ולתייג אותנו, ולעקוב אחר כל פעולה שנעשית ברשת. חוסם הפרסומות מבטיח שמידע שלנו לא ישלח למסדי נתונים שונים ולא יימכר לחברות שסוחרות במידע האישי שלנו. (למשל, Adblock, uBlock Origin)

## הימנעות מרוגולות ורשעות

רוגולות ורשעות הינן תוכנות עם כוונה זדונית אשר יכולות לגנוב מידע אישי ורגיש ולנטר את הפעילות שלנו ברשת. רוגולות יאספו מידע על כל הקשה על המקלדת, על כל מסך שנפתח, ועל כל מידע שנכנס ויוצא מהמכשיר שלכם. הדרך לצמצם הסיכון להידבק ברוגולות ורשעות היא להתקין רק דברים נחוצים ממקורות אמינים, ולא להתפתות להתקין תוכנות או אפליקציות מיותרות ממקורות מפוקפקים, ופשוט לא ללחוץ על שום לינק ממקורות שאתם לא מכירים.

## שימוש בוי.פי.אן (VPN)

וי.פי.אן - רשת פרטית וירטואלית הוא שירות מקוון שמצפין את תעבורת האינטרנט שלך ומסתיר את כתובת ה-IP שלכם (תעודת הזהות של המחשב) היא מנתבת את הגלישה שלכם בצורה מאובטחת דרך שרתי החברה שנמצאים בד"כ במדינה אחרת. השרות מסופק על-ידי חברות מסחריות בתשלום או בחינם. צריך לשים לב ממי קונים את השרות. גם כאן ישנם חברות שמוכרות מידע אישי של המשתמשים. ה-VPN גם אינו מבטיח אנונימיות מלאה. לאנונימיות מיטבית כדאי לגלוש בדפדפן Tor בו הגלישה מתבצעת דרך שלושה שרתים שונים. (ספקי VPN ממולצים: ProtonVPN, NordVPN, Surfshark).

## גלישה וחיפוש אנונימי

שיטוט באינטרנט במצב גלישה בסתר (אינקוגניטו) היא דרך טובה לחיפושים פשוטים ודרך טובה להסתיר מאנשים נוספים המתמשים במחשב את ההיסטוריה שלכם, אבל היא איננה בטוחה. מצב "גלישה בסתר" מונע את אחסון נתוני הגלישה אך אינו מונע סוגים אחרים של מעקב, גורמים מצד-שלישי עדיין יכולים לעקוב אחריכם באמצעות כתובת ה-IP. ספק האינטרנט שלכם יכול לתעד את האתרים בהם אתם מבקרים, כמו גם את ההורדות שלכם. לחיפוש מאובטח עבורו למנוע חיפוש שלא רועם את המידע שלך (למשל DuckDuckGo).

## הצפנת מידע

מידע שאתם באמת רוצים לשמור בטוח אפשר להצפין. שימוש בהצפנה ימנע מחורשי רעה לקרוא את הנתונים המוצפנים. אפשר להתשמע בתוכנת הצפנה (כדוגמת VeraCrypt), ורוב הסמארטפונים והמחשבים מציעים הצפנה מלאה בדיסק מלא כאופציה. לאפל תכנתה הצפנה הנקראת FileVault. לוויןדוס תכנתה הצפנה בשם BitLocker.

## הגנה פיזית

כניסה למחשב מוגנת על ידי סיסמה. מצלמה מכוסה עם מדבקה או כיסוי יעודי.

המכון לטכנולוגיה חיובית



www.positive-tech.net