# סיסמאות חזקות - שלא יגנבו לך את המפתחות!

## נעילה של מכשירים אלקטרוניים

- מומלץ להגדיר **נעילה אוטומטית לכל המכשירים שברשותך** (טלפון, מחשב, טאבלט וכדומה).
- **פתיחת הנעילה** תתבצע באמצעות סיסמה/דפוס גרפי/זיהוי ביומטרי, בהתאם לבחירתך וליכולות המכשיר. זיהוי ביומטרי הוא המומלץ ביותר כיוון שאין צורך לזכור אותו והוא ייחודי עבורך בלבד.

## בחירת סיסמאות

- לוודא שיש לך **סיסמה שונה** לכל מכשיר, אתר וחשבון.
- להקפיד על הגדרת **סיסמאות חזקות** עבור **כל האתרים, החשבונות והמכשירים** שלך.

סיסמה חזקה היא:

**סיסמה ארוכה** בעלת 10 תווים ומעלה

**סיסמה מורכבת** שכוללת אותיות גדולות, אותיות קטנות, מספרים ותווים מיוחדים

- הדרך המומלצת ליצירת סיסמה חזקה היא באמצעות **מחולל סיסמאות**.
ואם זה לא מתאפשר - ליצור עצמאית סיסמה חזקה שמורכבת מ**רצף מילים ותווים** שקל לזכור, לדוגמה על ידי "**שיטת השיר**".

### שיטת השיר

שיטת השיר מאפשרת לך **לייצר סיסמה חזקה וקלה לזכירה**:

- לבחור **רצף מילים** משיר אהוב (או שם ספר, או כותרת חדשות...)
- להחליף את המילה האחרונה במשפט ב**שם השירות** אליו מעוניינים להתחבר
- להוסיף **מספר** לאחר המילה האחרונה שהחלפת
- להוסיף **תו מיוחד** (שאינו ספרה או אות) לאחר המספר

## ניהול סיסמאות

עם כל כך הרבה סיסמאות חזקות כדאי להשתמש ב**תוכנה לניהול סיסמאות** ולהגדיר עבור ההתחברות אליה **סיסמה חזקה**, עדיף ביומטרית.

## סיסמה לא תמיד מספיקה

- מעבר לסיסמה, כדאי **להגדיר אימות דו-שלבי** ואפילו **אימות רב-גורמי בכל חשבון מקוון שמאפשר זאת** (לדוגמה ג'ימייל, פייסבוק, אינסטגרם, ווטסאפ).
- לוודא שהאפשרות של **קבלת התראות על שימוש חריג בחשבון** פועלת בחשבונות השונים שלך.