



שמרו על המחשבים האישיים

הקפידו לעבוד רק עם תוכנות מקוריות, תתקינו מוצרי אבטחת מידע, וודאו שיש עדכוני אבטחה תקופתיים, שימרו סיסמאות במקום בטוח, והקפידו למנוע מאנשים זרים גישה למחשב.



מצלמה חכמה? גם התוקף

התייחסו למוצרים חכמים המותקנים בבית ככאלו - המנעו מהתקנתם במקומות רגישים (שירותים, מקלחת, מקומות הלבשה).



גלישה בטוחה

השתמשו בדפדפנים של חברות ידועות. המעיטו בהורדות קבצים לא מוכרים ובמתן אישורי התקנות קוד במחשב.



הרמקול החדש מאזין

אלקסה, אקו, גוגל הום או אפל הום, לא משנה איזה רמקול חכם רכשתם לאחרונה, דעו כי הוא מאזין לכם. והוא זוכר הכול.



הקפידו לגבות חומרים אישיים

גביית נתונים, תוכנת כופר או השחתת קבצים הם חלק מהסיכונים. בצעו גיבוי מקומי ו/או בענן על מנת שתוכלו לשחזר בקלות את הקבצים האבודים.



אבטחת מידע בבית שלי

הבית הפרטי של כל אחד ואחת מאיתנו מהווה אכסניה למגוון התקני מחשוב, וככזה, הוא חשוף למתקפות סייבר. כחלק מההירתמות שלנו לחודש המודעות לסכנות במרחב הסייבר, ריכזנו עבורכם מגוון עצות ליישום אבטחת מידע בבית.

שימוש בטוח בדואר אלקטרוני

זכרו כי מתקפות הדייג (פשיינג) הכוללות קבצים או קישורים זדוניים מגיעות גם למחשב בבית. שימרו על כללי שימוש בדוא"ל גם בבית: בדקו פרטים, הקפידו לא ללחוץ על קישורים או לפתוח קבצים וכו'.



נעלו את רשת ה-WiFi

רשת ביתית פתוחה לכולם יכולה להיתפס כמעשה פילנטרופי, אך בעולם הסייבר, רשת כזו פתוחה גם לתוקפים לפריצה אליכם או לשימוש ברשת לצרכיהם. הגדירו סיסמא לכל רשת בבית.



חבר או מרגל? שמרו על הסולר

כמעט כל אחד מבני המשפחה מחזיק טלפון סלולרי הוופך אותו למטרה 24 שעות ביום. זכרו כי מדובר במכשיר שיכול להקליט ולצלם אתכם. אפשר גם לגנוב ממנו מידע.



אחלה שיתוף (תודה מראש. התוקף)

תמונות, SMS או הודעות ווטסאפ, לא משנה איך בחרתם לשתף, בסוף, ברוב המקרים, המידע נחשף. זכרו זאת כאשר אתם מצלמים או מקליטים ברחבי הבית.

