



תוכנות זדוניות? שלא ידביקו אותך!



תוכנות הגנה (אנטי-וירוס וחומת אש)

- לוודא שמותקנות תוכנות הגנה (תוכנת אנטי-וירוס ותוכנת חומת אש) של חברות מוסמכות על כל המכשירים האלקטרוניים (ואם לא - להתקין).
- להקפיד שתוכנות ההגנה מתעדכנות אוטומטית.
- אם במקום עבודתך נמצא איש/צוות IT סביר שנושא תוכנות ההגנה (אנטי-וירוס וחומת אש) מנוהל על ידו.

עדכונים אוטומטיים

- לוודא שמתבצע עדכון אוטומטי של מערכות ההפעלה של כל המכשירים האלקטרוניים שלך (טלפון נייד, מחשב, טאבלט וכדומה) וכן עבור התוכנות, הדפדפנים והאפליקציות השונות שמותקנות בהם.
- אפשר (אך פחות מומלץ) להקפיד על עדכון ידני בכל פעם שמתקבלת התראה מהיצרן.

גיבוי מידע



- לגבות את המידע בכונן חיצוני ו/או בענן, בכל פעם שחל בו שינוי או אוטומטית בפרקי זמן קבועים בהתאם לצורך (אחת ליום/לשבוע/לחודש).

קישורים וצרופות

בקבלת הודעה:

- לשאול את עצמך שאלות חשובות: האם השולח מוכר לי? האם ציפיתי להודעה?
- לחפש סימנים חשודים כמו: שגיאות כתיב (גם בכתובת), סיומת לא מוכרת של קובץ
- אם מתעורר אצלך חשד - לא ללחוץ על קישורים וקבצים חשודים!
- למנוע מהמחשב להפעיל פקודות אוטומטיות

הורדות ממקור בטוח

- להוריד אפליקציות ותוכנות מחנות הורדות רשמית בלבד!
- לבחון את ההרשאות שהאפליקציה/התוכנה מבקשת ולא לאשר אותן אוטומטית.

חיבור רכיבי חיצוני למחשב (והעברה ושיתוף של קבצים)



- לא לחבר רכיבי מדיה חיצוניים (כמו דיסק-און-קי, כרטיס זיכרון, כונן חיצוני) אלא אם ידוע בוודאות המקור שלהם או שהם עברו בדיקה ואישור על ידי מישהו מוסמך.
- לבעלי עסק מומלץ:
 - להעמיד מחשב ייעודי כדי לסרוק רכיבי מדיה חיצוניים.
 - לסמן באופן ברור רכיבים חיצוניים שמאושרים לחיבור למכשירי העובדים ולרשת הארגון.
 - להגדיר ולנהל רכיבים באמצעות מערכת Device Control.
 - להעביר קבצים באמצעות אימייל או כלים לשיתוף מידע.