TOP 10
לאבטחת מחשבים

הגדירו סיסמאות חזקות הכוללות שילוב של אותיות גדולות וקטנות, מספרים וסימנים מיוחדים.

הסיסמאות והקודים שלכם הם פרטיים ואין להעבירם או לשתפם עם אחרים.

בכל יציאה מעמדת העבודה, גם אם לזמן קצר, יש לנעול את המחשב. בסוף יום העבודה, אם המחשב נשאר במשרד, חובה לכבות אותו (Shut down) ולא להשאירו במצב נעול בלבד (Log off).

הקפידו לעדכן את מערכות ההפעלה, התוכנות והאפליקציות במחשב ובסלולארי שלכם. עדכונים כוללים תיקוני אבטחה חשובים שמגנים על המכשירים מפני פרצות חדשות. בצעו את העדכונים המופצים על ידי אגף ה – IT של החברה.

שמירה וגיבוי מידע יתבצע ברשת החברה. הקפידו שלא לשמור מידע על "שולחן העבודה" (Desktop) על מנת שלא יישאר מידע נגיש לתוקפים או גנבים שהמחשב עלול ליפול לידיהם.

הימנעות מקישורים חשודים: אל תלחצו על קישורים חשודים בהודעות דוא"ל או באתרים לא מוכרים. קישורים אלו יכולים להוביל לאתרים זדוניים שמטרתם לגנוב מידע או להדביק את המחשב בתוכנות זדוניות.

הגבלת גישה: ודאו שרק אנשים מורשים יכולים לגשת למחשב ולמידע הרגיש שלכם. השתמשו במערכות ניהול גישה כדי לפקח על מי יכול לגשת לאילו נתונים.

אין לחבר לרשת המחשבים של החברה רכיבים חיצוניים, ובכלל זה Disk on Key, USB, טלפון סלולארי, מצלמה וכו' גם לא לצורך טעינה או סנכרון ללא אישור.

דווחו מידית למוקד הסייבר (45055) ולממונה הביטחון על כל חשד לאירוע סייבר או ביטחון במערכות המחשבים שלכם.

אלביט מערכות
מטה החברה • ביטחון

Elbit Systems
ESOC