האיום הביטחוני והנחיות ביטחון לעבודה מרחוק

עובדים מהבית? טסים לחו"ל במסגרת העבודה?
שומרים על המידע – גם מרחוק! היכולת לעבוד מרחוק באופן מאובטח הוא אחד מאבני היסוד החשובים בעבודת החברה וכלי להמשכיות עסקית איכותית. עם זאת, עדיין קיים סיכון לחשיפת מידע עסקי - ביטחוני רגיש / חסוי של החברה ולקוחותיה לגורמים שאינם מאושרים. היו ערניים לסביבת העבודה שלכם בבית ובמרחב הציבורי בארץ ובחו"ל.

כמה כללים שחשוב לזכור ולהקפיד:

הפרדת סביבות

- השתמשו במיילים נפרדים לעבודה ולשימוש פרטי.
- השתמשו בסיסמאות שונות וחזקות לכל חשבון.
- אין להשתמש בסיסמאות חשבון העבודה לחשבונות הפרטיים ולהפך.
- התנתקו מרשת המחשב בסיום השימוש בחו"ל או בעת יציאה מהבית (Shut Down).
- אין להוציא חומר מסווג מהחברה.
- אין להשאיר מחשב נייד במקום גלוי ונגיש בבית או ברכב, יש להחזיקו במקום אשר לא יהיה נגיש לפורצים/גנבים.

אבטחת רשת

- השתמשו בסיסמאות חזקות ואימות דו-שלבי.
- ודאו שכל התוכנות והמערכות מעודכנות לגרסאות האחרונות. עדכונים כוללים תיקוני אבטחה חשובים שמגנים על המכשירים מפני פרצות חדשות.
- העדיפו רשת ביתית מאובטחת או נקודה חמה בטלפון הסלולארי שלכם.
- הימנעו משימוש ברשתות Wi-Fi ציבוריות בארץ ובחו"ל (מלון, שדה תעופה וכו'). חיבור זה עלול לחשוף את המכשירים למתקפות סייבר, לגניבת מידע או להשתלטות על מכשירי הקצה.

עבודה מחו"ל

- נסיעה לחו"ל עם מחשב נייד (בלמ"ס בלבד) – באישור סמנכ"ל.
- הצטיידות במעטפות אינדיקציה למניעת גישה,
- כיבוי מלא (Shut Down) בעת השימוש ואחסנה במקום בלתי נגיש / בולט / כספת.
- העדיפו רשת ביתית מאובטחת או נקודה חמה בטלפון הסלולארי שלכם.
- הימנעו משימוש ברשתות Wi-Fi ציבוריות בארץ ובחו"ל (מלון, שדה תעופה וכו'). חיבור זה עלול לחשוף את המכשירים למתקפות סייבר, לגניבת מידע או להשתלטות על מכשירי הקצה.

עבודה נעימה ובטוחה!

אלביט מערכות
מטה החברה • ביטחון

Elbit Systems