הנחיות לגלישה בטוחה

בכדי ליהנות מחוויית גלישה נוחה ובטוחה באתר החברה, מומלץ לפעול בהתאם להנחיות הבאות:

אתר בלנדר

- וודאו כי אתם גולשים באתר מאובטח - בשורת הכתובת בדפדפן חפשו את מנעול האבטחה ואחריו האותיות https://.
- חשוב לוודא שסימן המנעול מופיע כבר בדף הראשי ולא לאחר ההתחברות לאתר.

כניסה בטוחה לאתר

- בכל כניסה למערכת יש להקליד קוד משתמש ייחודי וסיסמה אישית.
- ניסיונות כניסה שגויים ייגרמו לחסימת הסיסמה. לאחר מספר דקות של חוסר פעילות מצידכם במערכת, התקשורת תנותק כדי למנוע פעילות לא מורשית במערכת.
- בכל כניסה למערכת תוכלו לראות בראש העמוד את מועד כניסתכם האחרונה. כך תוכלו לוודא שלא נעשתה כניסה למערכת ללא ידיעתכם.

יציאה מהמערכת

- בסיום פעולתכם באתר, לחצו על כפתור יציאה/התנתקות.

התנהלות בטוחה עם קוד המשתמש והסיסמה

- בחרו סיסמה שאינה קלה לניחוש, המשלבת אותיות גדולות וקטנות באנגלית, ספרות וסימנים מיוחדים.
- הימנעו משמירת קוד המשתמש והסיסמה במקום גלוי ליד המחשב, בקובץ לא מוגן במחשב האישי, או במקום אחר שיקל על גורם לא רצוי למצוא אותם.
- החליפו את קוד המשתמש והסיסמה לאתר באופן תדיר, אחת למספר חודשים.
- קוד המשתמש והסיסמה הם אישיים ואין להעבירם לאחרים.
- **נציגי החברה לא יבקשו מכם באופן יזום לציין את סיסמתכם. אם התבקשתם לעשות זאת על ידי גורם כלשהו, סרבו ודווחו על כך מיידית למוקד שירות הלקוחות.**

אמצעי הגנה מומלצים בנוגע למחשב האישי

- וודאו שאתם משתמשים בתוכנת אנטי-וירוס מעודכנת ובמערכת הפעלה בגרסה עדכנית, הכוללות את עדכוני האבטחה האחרונים.
- הגדירו סיסמת כניסה אישית למחשב.

אמצעי הגנה מומלצים בנוגע למכשיר הטלפון הנייד

- הגדירו קוד כניסה אישי (PIN) , סיסמה ייחודית או זיהוי ביומטרי.
- התקינו יישומים (אפליקציות) רק מחנויות רשמיות (App Store, Google Play) ולא דרך קישורים שקיבלתם.
- מומלץ להגדיר באופן יזום אילו הרשאות להתיר לכל אפליקציה.
- בקבלת הודעות אימייל, SMS או WhatsApp מגורמים לא מוכרים, הימנעו מלחיצה על קישורים או מהורדה של קבצים לטלפון הנייד.

הונאה מקוונת - Phishing

- **היזהר מהודעות דוא"ל והודעות טקסט מזויפות** - הודעות מזויפות הנן הודעות הנשלחות כביכול מחברת בלנדר או מחברה מוכרת אחרת אשר מבקשות ממקבל ההודעה להיכנס לאתר בלנדר באמצעות קישור הניתן בתוך ההודעה, ולמסור או לעדכן את נתוניו האישיים תוך פירוט הסיבות בגינן נדרש העדכון: סיבות ביטחון, שדרוג מערכות וכדומה. הקישור בהודעה יכול להיות

חיקוי מדויק של האתר הרשמי של החברה ממנה כביכול נשלח המכתב. בדרך זו מנסים שלא כדין להשיג את נתוניו האישיים של הנמען לצורך גישה לחשבונותיו.

- **לידיעתך, בשום מקרה לא תפנה חברת בלנדר ללקוחותיה בהודעות דוא"ל, SMS או WhatsApp בו הם יתבקשו לעדכן את פרטיהם לצורך הזהות למערכות, ולכן אין להיענות לבקשה לביצוע עדכון פרטים המתקבלת באמצעות הודעות אלה.**

שירות ותמיכה

- אנו עומדים לשירותכם בכל שאלה במוקד שירות הלקוחות של בלנדר בדוא"ל support@blender.co.il ובטלפון: 9906*

****

כל האמור לעיל אין בו כדי לגרוע מאחריות כלשהי המוטלת על הלקוח או על החברה.