



הנחיות סייבר בחירום

בשל המצב הביטחוני, ישנה עלייה בניסיונות סייבר מצד גורמים עוינים - כולל פשינג, גניבת מידע ולוחמה פסיכולוגית. יש להגביר ערבות להודעות, מיילים ופניות חשודות, ולהקפיד על זהירות בפגישות מקוונות.

כיצד ניתן להתגונן?

שמירה על מידע רגיש

אין להעביר מידע משרדי ורגיש לערוצים פרטיים, כגון Gmail או WhatsApp.



הימנעו מלחיצה על קישורים

וקבצים חשודים והטילו ספק בהודעות חשודות במייל / Whatsapp / sms



איסוף מידע רגיש

איסוף מידע פרטי/רגיש יתבצע אך ורק באמצעות תשתית הטפסים המאושרת על ידי המשרד.



העברת מידע רגיש

קבצים ומסמכים רגישים יש לשמור בסביבות ענן חינוך בלבד. העברת מידע רגיש תתבצע בחשבון ענן חינוך, למורשים בלבד, באמצעות דוא"ל חינוך או קישור מאובטח.



הגדירו מנגנון אימות דו שלבי (MFA) עבור חשבונות המשתמש שלכם ברשתות החברתיות וכלי ענן, ניתן להיעזר במדריכים הבאים:



[Microsoft](#)



[Instagram](#)



[Google](#)



[TikTok](#)



[Facebook](#)



[Whatsapp](#)

אם יש ספק אין ספק! - נא לדווח על כל אירוע חשוד!