

# אבטחת מידע בזמני משבר

מרץ, 2022

פעילות הסייבר סביב המשבר בין רוסיה לאוקראינה מרקיעה שחקים ולמרות שאנו לא בהכרח מעורבים בקונפליקט, כולנו בסופו של דבר מושפעים.

לכל משבר עולמי יש מימד סייבר ועלייה חדה בהודעות דוא"ל פשינג זדוניות מראות כי משבר זה אינו שונה מאחרים.

## מה קורה הלכה למעשה

כל צד בסכסוך הפעיל מתקפות סייבר על הצד השני, שכוללות הודעות זדוניות למחיקת נתונים והשבתת אתרי אינטרנט על מנת למנוע שימוש לגיטימי בהם.

מתקפות אלו אינן תמיד מרוסנות ולרוב מדביקות מכשירים ואתרי אינטרנט שאינם מעורבים בקונפליקט. אלו כוללים את הארגון שלך או מכשירים אישיים.

גם חשבונות הרשת החברתית האישיות שלך נמצאים בסיכון של פריצה, למטרת הפצת מידע שקרי או תוכנות זדוניות.



# מה אפשר לעשות על מנת להגן על הרשת הביתית

## שלך



ליידע חברים ומשפחה מה קורה ולהאיץ בהם לבצע את אותן פעולות.



הוספת אימות דו-שלבי לחשבונות הרשת החברתית שלך (Facebook, LinkedIn, Twitter וכו') ולחשבונות הדוא"ל. אם אפשרי, להוסיף גם חשבון דוא"ל גיבוי.



התקנת עדכונים של מערכת ההפעלה ושל אבטחת מידע. אם אלו זמינים, ניתן לראות התראה על כך בטלפון או במחשב שלך.

# מה אפשר לעשות על מנת להגן על הרשת שלנו



יש להמשיך לבדוק את כתובת הדוא"ל של השולח - זהו הצעד הקריטי ביותר באיתור מתקפת פשינג.



במהלך ימים אלו יש לצפות למתקפות פשינג נוספות. יש להיזהר מהודעות דוא"ל המבקשות עזרה ממך בנושאים של תמיכה טכנית או כספית.



אנו דואגים לאבטחת המידע של הרשת הפנימית שלנו, כך שאין צורך לנקוט בצעדים טכניים מהצד שלך.