



# הגברת ערנות בנושאי אבטחת מידע וסייבר

1 הגברת ערנות בנושאי אבטחת מידע וסייבר בעקבות התגברות מתקפות סייבר בארץ ובעולם

2 עדכוני אבטחת מידע

3 אימות דו-שלבי

4 סיסמאות חזקות

5 מיילים מסוג פשינג והודעות SMS

OPIsrael &





# מידעון אבטחת מידע אפריל 2023

אינטגריטי ייעוץ וניהול סיכונים

## 1 הגברת ערנות בנושאי אבטחת מידע וסייבר בעקבות התגברות מתקפות סייבר בארץ ובעולם

בעקבות התגברות של מתקפות סייבר בארץ ובעולם - הגבירו ערנות בנוגע להתנהלות ברשת האינטרנט בעבודה בבית ובמכשיר הסלולרי.

הקפידו לגלוש לרשת החברה מרחוק באמצעות חיבור מאובטח (VPN).

במיילים בדקו תמיד את שם השולח זהותו וכתובתו - לא לפתוח קישורים או קבצים אם יש חשד לגביהם, פתחו דפדפן חפשו את שם החברה במקום ללחוץ על לינק.

היו ערניים וחשדניים במיוחד להודעות SMS הכוללות קישורים.

הגדירו אימות דו-שלבי בכל שירות שניתן MFA/2FA.

## 2 עדכוני אבטחת מידע

מומלץ לבצע עדכוני אבטחת מידע לכלל המחשבים והטלפונים החכמים בהקדם האפשרי.

  
Working on updates  
20% complete  
Don't turn off your computer

ניתן לפנות לאנשי הסיסטם / IT בארגון במידה ולא תסתדרו עם עדכוני אבטחת מידע

## 3 אימות דו-שלבי

מומלץ לבחון שקיים אימות דו-שלבי על כלל הממשקים שאתם מתחברים אליהם כולל תיבות הדוא"ל הארגוניות והפרטיות. מומלץ לבצע שימוש באימות דו-שלבי בעזרת הודעת SMS או בעזרת אפליקצייה כגון: **Google Authenticator**.

2FA



Requires you to prove your identity **twice**.

V/S

MFA



Requires you to prove your identity **multiple times**.

מומלץ לבדוק שאנו משתמשים בסימאות חזקות הכוללות:

- אורך סימא של לפחות 9 תווים ויותר
- חיוב שימוש באותיות גדולות (A-Z)
- חיוב שימוש באותיות קטנות (a-z)
- חיוב שימוש במספרים (0-9)
- חיוב שימוש בסימנים מיוחדים (לדוגמא: !@#\$%^&\*(<>?"', וכד')
- חיוב הגדרת ללא רצפים ( לדוגמא: ללא 1234,1234567,98765 כחלק מהסימא).
- איסור על שימוש בשם המשתמש חלק מהסימא.



## מיילים מסוג פשינג והודעות SMS

5

מומלץ לבדוק כל מייל שמגיע אליכם ואינכם בטוחים בו:

- לבדוק שגיאות כתיב
- לבדוק מי השולח ואם אתם מכירים אותו
- לבדוק אם המייל מכין תוכן מוזר/קבצים
- לבדוק לפי הכותרת של המייל במידה ומופיע שם משהו לא מוכר
- "מייל זה הגיע מחוץ לארגון" – מומלץ להסתכל על ההודעה הזאת שמתקבלת.
- חובה לדווח על כל מייל חשוד שמגיע אליכם לצוות המחשוב בהקדם האפשרי.



מידי שנה בתחילת חודש אפריל ובפרט השנה כאשר חודש הרמדאן חל בחלקו בחודש זה, גוברת האפשרות לתקיפות סייבר של גורמים האקטיביסטים במרחב האינטרנט הישראלי.

האירוע הבולט בחודש זה הינו קמפיין תקיפה המוכר בשם #OPJerusalem וחל ב-"יום ירושלים האיראני". הקמפיין מתקיים מידי שנה ביום שישי האחרון של חודש הרמדאן, ומתאפיין בהפגנות ברחבי איראן והרשות הפלסטינית, וכן בפעילות התקפית אנטי ישראלית במרחב הסייבר.

מומלץ לשמור על ערנות מרבית ולהיצמד להנחיות השונות בנושא!

