לחצתי, מסרתי פרטים ונלחצתי - מה עכשיו?

הנדסה חברתית מנצלת את העובדה שבני אדם עלולים ליפול למניפולציות פסיכולוגיות, לחוסר ריכוז ואף לטעויות. הודעות דיוג מכוונות לגורם האנושי הבסיסי הזה. אם זה קרה לכם, אין מה להילחץ - יש מה לעשות. לרגל שבוע הגנת הסייבר, מערך הסייבר הלאומי חיבר מדריך והמלצות למי שנפל ברשת.

- **תוכנות הגנה**- אם פתחתם קישור שנראה לכם חשוד, ואתם מתבקשים להריץ במחשב שנראה חשוד, כדאי להשתמש בתוכנות ובשירותי הגנה ייעודיים כגון אנטי וירוס, חומת אש, מערכות לגילוי/מניעת חדירות ועוד שיעזרו לזהות.

- **החלפת סיסמה**- במקרה שמסרתם את הסיסמה או קוד ייחודי בהודעת דיוג או לגורם זר, מומלץ להחליפם בכל החשבונות לסיסמה ארוכה, מורכבת וקשה לניחוש. כמו כן, תוכלו להשתמש בתוכנות ייעודיות ליצירת סיסמאות מורכבות. אם אתם לא זוכרים לאילו חשבונות ואפליקציות השם משתמש או הדוא"ל שמסרתם מקושר, ניתן להיעזר בהגדרות האבטחה של גימייל (GMAIL), שם תמצאו את רשימת האפליקציות המקושרות, וכן לחפש באתר הבא: https://namechk.com/

- **הגדרת אימות דו שלבי/רב גורמי** - אימות נוסף לסיסמה, כגון קוד ייחודי, קוד שמתקבל במסרון או בדוא"ל, או קוד שנוצר ב"מאמת החשבונות" - מומלץ להגדיר אופציה זו בכל חשבון ואפליקציה שמאפשרים זאת, זה מספק שכבת הגנה נוספת.

- **ביטול כרטיס אשראי ועדכון הבנק** - במקרה של מסירת פרטי חשבון הבנק או כרטיס האשראי באתר מתחזה, מומלץ לבצע את הפעולות הבאות: ביטול, חסימה או השהייה זמנית של כרטיס האשראי; עדכון הבנק ו/או חברת האשראי בנסיבות המקרה; ומעקב שוטף לפעולות חשודות בחשבון והאם נוצרו הוראות קבע חדשות שאינן מוכרות. במקרה של זיהוי חיוב שלא ביצעתם, דווחו מיד לחברת האשראי או לבנק וצרו קשר עם המשטרה.

- **הגדרת התראות** - מומלץ להגדיר קבלת מסרון או דוא"ל על כל רכישה המתבצעת בכרטיס האשראי באמצעות חברת האשראי או הבנק.

- **שימוש בכלי של have I been pwned** – חפשו את האתר בשם הזה שמאפשר לבדוק בקלות וביעילות אם פרטים כגון כתובת דוא"ל וסיסמה דלפו. במידה והפרטים נחשפו, מומלץ להחליף סיסמה ולהגדיר אימות דו שלבי בכל החשבונות המאפשרים זאת.

- **פנו אלינו** - אם נתקלתם בהודעת דיוג, אתר מתחזה, או מסרתם פרטים לאתר מתחזה או לגורם זר, דווחו לנו במערך הסייבר הלאומי בחיוג חינם 119.