



**מצגת מודעות עובדים לאבטחת מידע ולהגנת הפרטיות**

**כחלק מהעלאת המודעות לנושא אבטחת המידע במכון וולקני, להלן  
מספר דגשים:**

## **יש מקרים בהם יכולים להיות סיכונים למערכות המידע ולמידע בארגון, דוגמאות לתרחישים מסוג זה :**

- עובד מחבר מחשב או ציוד שלא אושר ע"י מחלקת מחשוב לרשת הארגון.
- אורח לכאורה מגיע למכון ו"לוקח" מסמכים מהשולחן או מחשב נייד.
- ספק/טכנאי (או מתחזה) מכניס התקן USB או מחבר מחשב לרשת הארגון המכיל וירוס.



## כיצד נהוג להגן בפני סיכונים פיזיים?

- לנעול את דלת החדר בכל פעם שיוצאים ואין איש בחדר , במיוחד בסוף יום עבודה
- לנעול את המחשב כאשר יוצאים מהמשרד- לוחצים בו זמנית על Ctrl+Alt+Delete ובוחרים את האפשרות - Lock
- אין לחבר טלפון נייד באמצעות כבל טעינה/דאטה ישירות למחשב
- כרטיס חכם
  - אין לשמור את הקוד הסודי בצמוד לכרטיס החכם
  - בעת עזיבת עמדת העבודה, יש להוציא את הכרטיס החכם מקורא הכרטיסים

# **דיוג או פישינג הוא ניסיון לגנבת מידע רגיש על ידי התחזות ברשת האינטרנט , דוגמה לדיוג והדרך הנכונה להתמודדות איתם**

- העובד של הארגון, ראה את הדוא"ל הנכנס והיות ואינו מכיר את השולח והדוא"ל נראה לה חשוד, לא פתח את הקובץ או לחץ על LINK מצורף ומחק את ההודעה.
- יש לשים לב באופן מיוחד לכל מיני בקשות להשתלטות על מחשבים או לאספקת משוב על פעולות מחשוב כאלה או אחרות.
- מסירת מידע פיננסי, ארגוני או אישי מתבצע רק בערוצים רשמיים לאספקת מידע כפי שנקבעו בארגון.



# אינטרנט ודואר אלקטרוני

- אין להוריד/לפתוח קבצים חשודים במיוחד והגיעו ממקור לא מוכר (גם אם הגיעו ממקור מוכר)
- אין ללחוץ על קישורים (Links) לא מזוהים המצורפים להודעות דואר אלקטרוני
- בכל מקרה שיש שאלה או חשד להתקפת סייבר אפשר לפנות לתמיכה טכנית באגף טכנולוגיות דיגיטליות ומידע.

