4.4.2020

שלום רב,

אנו נמצאים בעיצומה של תקופה מאתגרת, אשר ההתמודדות איתה ועם העבודה/ההוראה מהבית עלולים להשפיע על תשומת הלב לכללי אבטחת המידע ופרטיותנו.

להלן מס' עדכונים ותזכורת להנחיות אבטחת מידע:

1. **תוכנת ZOOM** – השימוש העולמי הרחב באפליקציה שהפכה לכלי מרכזי בהוראה, בישיבות ומפגשים חברתיים, הביא אתגרים רבים למפתחי האפליקציה שלאחרונה פרסמו מס' אזהרות שימוש:
   א. שידורי HD - בשל העומס על שרתי החברה ורשת האינטרנט כולה, הזהירה החברה כי יתכנו שיבושים בהעברת צילום ב- HD.
   ב. אבטחת מידע – החברה דיווחה כי הפרצה המשמעותית שהתגלתה לאחרונה באפליקציה, מאפשרת "ליירט" ולנחש סיסמאות בעיקר אם הן פשוטות. לראיה למשתמשי IOS (MAC/iPhone/iPad), היא אף חסמה את אפשרות הכניסה באמצעות חשבון ה- Facebook.
   ג. לכן ההמלצה שלנו היא שימוש בסיסמה מורכבת וייחודית (שונה מהסיסמאות למערכות או אפליקציות אחרות).
   ד. פגיעה במהלך התקין של מפגש ZOOM – פרצה נוספת שעליה דווח, מאפשרת בעיקר הפרעה והצקה של גורם לא רצוי למפגש ושיבוש מהלכו התקין, כגון:
      i. הצטרפות של משתמש שלא הוזמן.
      ii. השתלטות על המיקרופון או הרמקול.
      iii. מחיקה או עדכון המצגת.

   להלן קישור למסמך המלצות של רשות התקשוב הממשלתית לשימוש מאובטח באפליקציה. רוב המלצות אלו מתאימות למפגש סגור וחסוי של ישיבות מנהלתיות ופחות להרצאות, אך משאירה לכם את הבחירה לשימוש עפ"י שיקול דעתכם. בכל מקרה, צוות IT הקשיח את החיבור דרך מערכת לי-מוד, כך שמפגשים המתוזמנים דרך לי-מוד מאובטחים יותר, אך עדיין קיימת ההתקנה המקומית של האפליקציה לכן:
   ה. עדכוני גרסאות – יש להקפיד לבצע עדכון שוטף לאפליקציה המותקנת מקומית על גבי המחשב/הציוד האישי, ניתן להיעזר בקישור זה.
2. **שימוש במחשבים האישיים** -
   א. מכוון שמחשבים אלה אינם בפיקוח אגף IT, הם לכאורה פחות מוגנים ובטוחים ולכן אנא דאגו לביצוע עדכוני מערכת הפעלה ואנטי וירוס.
   ב. להזכירכם חל איסור העברת חומרים ממחשבי המכללה למחשב הביתי, הדבר עלול להביא סיכון לדליפת מידע רגיש, פגיעה בפרטיות וחריגה מתקנות ההגנה על הפרטיות.
3. **סכנת תקיפות יזומה** – כמדי שנה במהלך חודש אפריל, "האקרים" המזוהים עם Anonymous מבצעים ניסיונות תקיפה מרוכזת על מוסדות ומחשבים בישראל לכן תזכורת להמלצותינו במטרה להקטין את סכנת הפגיעה:
   א. שימוש בסיסמאות מורכבות וייחודיות לכל אפליקציה.
   ב. ביצוע עדכוני מערכת הפעלה, אפליקציות ואנטי וירוס.
   ג. ערנות ביחס למיילים חשודים לגניבת סיסמאות (Phishing).
   ד. לא לפתוח מסמך מצורף או ללחוץ על קישור שהגיע בדוא"ל ממקור לא מוכר.
   ה. לא לתת פרטים אישיים בפניה טלפונית, בפרט של שם משתמש וסיסמה.
   ו. ביצוע גיבוי לחומרים חשובים.

   בכל ספק או עזרה יש לפנות לתמיכת מחשוב.

בברכת בריאות איתנה ועבודה בטוחה,

חג חירות שמח,

איריס בן יעיש
מנהלת מערכות מידע
סגנית מנהל אגף IT