



שם הפרויקט		מס' פרויקט
מכשירים ושנאת סיכון בהקשר של אבטחת סייבר והתקפות התחזות		2022-01-070
מנחה שותף	מנחה אקדמי	
גב' נעמה אילני צור	פרופ' ליאור פינק	
חברי הצוות		
	אור בן זיקרי	יובל סרור
	orbenzik@post.bgu.ac.il	sroryuv@post.bgu.ac.il

## תקציר

בעשור האחרון, ישנה עלייה מתמדת בשימוש בטלפונים חכמים ("ניידים") גם מבחינת זמינות המכשירים באוכלוסיה וגם מבחינת מגוון הולך ומתרחב של שימושים. ה"ניידים" הפכו להיות המחשב האישי הנפוץ ביותר. לצד העלייה בשימוש ב"ניידים", ישנה עלייה במספר מתקפות הסייבר. הפרויקט שלנו הוא פרויקט מחקרי שמבקש לענות על השאלה האם יש הבדל בפגיעות למתקפות סייבר בין משתמשי "ניידים" למשתמשי מחשבים אישיים. הספרות של מערכות מידע מראה שיש סיבה לשער שיהיו הבדלים התנהגותיים בין משתמשי "ניידים" למשתמשי מחשבים אישיים. מבחינת התנהגות ביחס לסיכון הממצאים בספרות מעורבים.

במסגרת הפרויקט מימשנו מתודולוגיה של בניית פלטפורמה אינטרנטית לניסוי דיגיטלי, ניתחנו נתונים ובנינו מודל לחיזוי הסיכוי ללחיצה על כתובת URL לא מוכרת. כחלק מהניסוי בחנו שלושה משתנים שונים, המשתנה הראשון והמרכזי הוא סוג המכשיר, שיערנו שבשימוש בטלפון נייד הנטייה לגלישה שעלולה לסכן את המשתמש תפחת ביחס לשימוש במחשב האישי. המשתנה השני הוא רמת הקושי של המשימה שניתנה למשתמשים על מנת לסווג את רמת הריכוז שלהם והמשתנה השלישי הוא רמת מסוכנות הלינק. שיערנו שכל אחד מהמשתנים ישפיע על התנהגות המשתמשים ברשת ביחס לסיכון.

לצורך בדיקת ההשערות הקמנו פלטפורמה אינטרנטית שסייעה לנו לוודא כי המשתתפים אכן נכנסו לניסוי מהמכשיר שהתבקשו (מחשב אישי או טלפון נייד), ביצענו שני ניסויים דיגטליים תוך שימוש בפלטפורמת הניסויים של Amazon Mechanical Turk. בכל ניסוי השתתפו 256 משתתפים אשר חולקו לשמונה קבוצות בצורה אקראית כך שכל קבוצה שילבה את המשתנים הבאים: סוג המכשיר, רמת קושי המשימה ורמת מסוכנות הלינק. בניסוי הראשון הצגנו למשתתפים תמונות של עצמים לבועלי חיים לאנשים בצירוף שאלה על התמונה ברמת קושי המתאימה לקבוצה אליה משתייך המשתמש. בניסוי השני הצגנו תמונות של כלבים וחתולים כאשר המשימה הייתה לזהות מה מופיע בתמונה. תוך כדי כל אחד מהניסויים הקפצנו "פופ אפ" עם לינק בהתאם לרמת המסוכנות שסווגה לו על מנת למדוד את התנהגות המשתמשים ביחס לסיכון. בסיום כלל המשימות הצגנו למשתתפים שאלון דמוגרפי שיעזור לנו לבקר את התוצאות שהתקבלו והמודל שנבנה.

בשלב הראשוני של ניתוח תוצאות הניסויים ביצענו ניתוחי סטטיסטיקה תיאורית באקסל ומבחנים סטטיסטים כגון T-test בפלטפורמת R בכדי לבדוק האם אכן יש שוני במוצעים בין הקבוצות השונות. לאחר מכן בחנו מודלים שונים של רגרסיה לוגיסטית על מנת לבדוק את ההשפעה של הגורמים הנבדקים על נכונות הנסיינים ללחוץ על לינק במטרה ליצור מודל לחיזוי הסיכוי לגלישה מסוכנת. בחרנו במודל הלוגיסטי מכיוון שהמשתנה המוסבר שלנו (כמו גם המסבירים) הוא משתנה בינארי בעל 2 רמות בלבד (לחיצה או אי לחיצה על לינק). גילינו כי אכן לחלק מהמשתנים ישנה השפעה חיובית.

מהניתוחים שביצענו ומתוצאות המחקר עולה כי אכן מכשיר המשתמש הוא המשתנה המשפיע ביותר. משתמשי מחשב לוקחים יותר סיכון מאשר משתמשי "ניידים" (עד פי 4.43 הבדל). מסקנה נוספת מעניינת שעלתה היא שעבור לינקים ברמת סיכון נמוכה משתמשי המחשב נמצאים בסיכון גבוה יותר ליפול למתקפות פשינג מאשר משתמשי "ניידים", דבר העולה בקנה אחד עם העובדה שכיום מתקפות פשינג איכותיות מגיעות דווקא במסווה של לינקים שאינם מסוכנים ולא דווקא לינקים שנראים מסוכנים מבחינה ויזואלית.

**מילות מפתח:** פרטיות, מתקפות סייבר, מכשירים ניידים, כלכלה התנהגותית, ניסויים דיגיטלי.