הבדלי מגדר בקשר בין מודעות לפשעי סייבר לבין מעורבות בהתנהגויות סיכון במרחב הסייבר

ענבל לם וגוסטבו מש

מחקרים המסתמכים על תאוריית הפעילות השגרתית מצביעים על דפוסי התנהגות המגדילים את הסיכוי לקורבנות לפשעי סייבר, כגון היפגעות מתוכנות זדוניות, מגנֵבת זהות ומהונאה, וממליצים להעלות את רמת המודעות החברתית כדי להקטין את מידת המעורבות בהתנהגויות סיכון במרחב הסייבר. עם זאת, מעטים המחקרים הבוחנים את הקשר בין מודעות לבין התנהגות במרחב הסייבר. המטרה המרכזית של מחקר זה היא לבחון אם קיימים הבדלי מגדר בקשר בין מודעות לפשעי סייבר לבין מעורבות בהתנהגויות סיכון במרחב הסייבר. נתוני המחקר נאספו באמצעות סקר טלפוני שנערך בשנת 2014 בקרב מדגם מייצג של משתמשי האינטרנט הפרטי בישראל ($N = 1,850$). ממצאי המחקר מצביעים על הבדלי מגדר ברמת המודעות לפשעי סייבר וברמת המעורבות בהתנהגויות סיכון במרחב הסייבר. עם זאת, לא נמצאו הבדלי מגדר בקשר בין מודעות לפשעי סייבר לבין מעורבות בהתנהגויות סיכון במרחב הסייבר. בחינת האינטראקציה בין מין הפרט לבין מודעות לפשעי סייבר מצביעה על כך שללא קשר לרמת מודעותן, נשים מעורבות בהתנהגויות סיכון פחות מגברים. ממצא זה מצביע ככל הנראה על הבדלים מובְנים בין גברים לבין נשים בדפוסי המעורבות בהתנהגויות סיכון במרחב הסייבר. ממצאים אלו עשויים לשמש לפיתוחן של תכניות חברתיות המיועדות לאפשר לכלל צרכני האינטרנט הפרטיים, ובפרט לקבוצות חברתיות מובחנות, להתמודד עם פשעי סייבר.

* **ענבל לם**, החוג לסוציולוגיה, אוניברסיטת חיפה.
דואר אלקטרוני: inval@sbcglobal.net
פרופ׳ גוסטבו מש, החוג לסוציולוגיה, אוניברסיטת חיפה.
דואר אלקטרוני: gustavo@soc.haifa.ac.il

© כל הזכויות שמורות
מגמות, 2017, נב(2), 77–108

מילות מפתח: קורבנות, פשעי מחשב, פשעי סייבר, אינטרנט, מגדר, נטילת סיכון, מודעות, הבדלי מין, תאוריה של פעילות שגרתית

נושא מרכזי בספרות הקרימינולוגית הוא חקר התפיסות החברתיות בנוגע לאיום הקורבנות מעבריינות (crime victimization). ממצאי מחקרים מורים שהציבור חושש להיות קורבן ומעריך שסיכוייו ליפול קורבן לעבֵרות שונות הם גבוהים (Farrall & Gadd, 2004; Ferraro, 1995; Warr, 1993). מחקרים ברוח זו מאירים הבדלים בתפיסות בין קבוצות חברתיות־דמוגרפיות שונות ומדגישים במיוחד את הבדלי המגדר (Hipp, 2010). נשים חוששות ומעריכות את הסיכוי שייפלו קורבן לעבריינות כגבוה יותר מהערכת הגברים את סיכוייהם לכך (ראו, לדוגמה Hirtenlehner & Farrall, 2014; Rader, May, & Goodrum, 2007). לצד עיסוק מחקרי בגורמים המסבירים את נטייתן של נשים לחשוש מאירועי עבריינות, הספרות בוחנת את השלכותיהם של הבדלי המגדר בתפיסת איום הקורבנות על דפוסי ההתנהגות היום־יומיים (Rader, Cossman, & Allison, 2009). נמצא כי החשש מהיפגעות מעבריינות ותפיסת הסיכון הגבוהה בקרב נשים מעצבים את דפוסי הפעילות היום־יומיים שלהן ומביאים אותן לכדי הימנעות ממעורבות בהתנהגויות הנתפסות כמסכנות את ביטחונן האישי (Mesch, 2000; Rader et al., 2007; Rader et al., 2009). עד כה התמקד רוב המחקר בתחום בתפיסת הסיכון ובחשש מפני אירועי פשיעה המאיימים באופן ישיר על הביטחון הפיזי של הציבור (עבֵרות גנבה המעורבות באלימות, ברצח או באונס). עבֵרות אלו מתאפיינות בקורבן שניתן לזהותו, בנזק שניתן לכמתו ובעבריין בעל זהות מוגדרת (Hollway & Jefferson, 1997). לעומת זאת, נראה כי הסוגיה המגדרית נעדרת מן הספרות העוסקת בחקר התפיסות החברתיות בנוגע לתופעת הפשיעה במרחב הסייבר ובנוגע לקשר ביניהן לבין דפוסי התנהגות במרחב זה.

מחקרנו מתמקד באוכלוסיית משתמשי האינטרנט הפרטי בישראל ומבקש לעמוד על הבדלי מגדר ברמת המודעות (awareness) ובמידת המעורבות בהתנהגויות סיכון במרחב הסייבר. נוסף על כך, הוא מבקש לבחון אם קיימים הבדלי מגדר בקשר בין מודעות לפשעי סייבר לבין מעורבות בהתנהגויות סיכון במרחב זה.

המהפכה שחולל האינטרנט בחברה האנושית חושפת את אזרחי הסביבה הדיגיטלית גם למצבים של חוסר ודאות, סכנה וקורבנות (Wall, 2007; Yar, 2013, p. 3). ספרות מדעי החברה עשירה בחקר הסכנות המקוונות הכרוכות בתקשורת בין־אישית, כגון בריונות ברשת והטרדות מיניות (Livingstone & Helsper, 2007; Mesch, 2009; Staksrud & Livingstone, 2009; Ybarra, Mitchell, Wolak, & Finkelhor, 2006), ואילו חקר הפגיעות (vulnerability) של משתמשי המחשב לעבריינות סייבר נמצא בראשיתו. עבריינות סייבר כוללת עברות ממוקדות מחשב, תוכנות זדוניות ועברות המבוצעות בסיוע מחשב (Brenner, 2007; Newman, 2009, p. 12; Wall, 2007; Yar, 2013, p. 9). עברות אלו נבדלות במאפייניהן, במטרותיהן ובהשלכותיהן, אך המשותף להן הוא ניצול תכונותיו המבניות של מרחב הסייבר ובהן אנונימיות התוקף, גלובליות המרחב החברתי

והיותו חסר גבולות גאוגרפיים ויכולת הפצת מידע במהירות להיקף גדול של צרכנים (Brenner, 2007; Clough, 2010, pp. 5-9; Savona & Mignone, 2004).

מחקרים שהסתמכו על **תאוריית הפעילות השגרתית** (routine activity theory) לחקר עבריינות וקורבנות סייבר (Cohen & Felson, 1979) מצביעים על קשר בין מידת המעורבות בהתנהגויות מסוימות במרחב הסייבר לבין הסיכוי לקורבנות, כך שמעורבות בהתנהגויות סיכון מגדילה את הסיכוי לקורבנות לעברות סייבר (Bossler & Holt, 2009; Choi, 2008). לאור ממצאים אלו נטו החוקרים להמליץ על העלאת רמת המודעות החברתית לסוגיית הפשיעה במרחב הסייבר כדי להקטין בו את מידת המעורבות בהתנהגויות סיכון (McQuade, 2006).

במחקר זה אנו בוחנים הבדלי מגדר ברמת המודעות לפשעי סייבר. הבחירה במשתנה "מודעות" אינה מקרית. פשיעה במרחב הסייבר היא תופעה חדשה יחסית הנמצאת בהתפתחות מתמדת, והשלכותיה על ציבור משתמשי המחשב טרם ידועות במלואן. תופעה זו תורמת להיותה של החברה המודרנית "חברת סיכון" (Jackson, Allum, & Gaskell, 2005; Wall, 2008, p. 9; Yar, 2005). בק (Beck, 1992, pp. 2-3) טבע את המונח "חברת סיכון" (risk society) לתיאור החברה בעידן המודרני ועמד על תפקידן המרכזי של התפתחויות מדעיות וטכנולוגיות בחשיפה לסיכונים חברתיים חדשים. חברת סיכון מתוארת כחברה במעבר: מעבר מחברה שבה מערכות חברתיות אנושיות מאורגנות סביב מרחב טריטוריאלי מוגדר, לחברה החווה תהליכי גלובליזציה, מהפכה מגדרית, אבטלה גואה והתמודדות עם סיכונים גלובליים. הפרטים בחברה המודרנית חווים תחושה גוברת של איום וסכנה (ontological insecurity) הן בשל העדר שליטה על מקורות האיום והן בשל הקושי של מערכות הפיקוח המוכרות לווסת את האיום. לפי בק, ראשיתה של ההתמודדות עם איום הכרוך ב"חברת סיכון" היא בהשגת מודעות חברתית לסכנות.

כאמור, חוקרים מכירים בהשפעה שיש למודעות לפשיעה במרחב הסייבר על המעורבות בפעילויות סיכון במרחב זה. עם זאת, מעטים המחקרים שעמדו על טיבו של קשר זה, ואלו שנעשו מצביעים על כך שמודעות לסכנות במרחב הסייבר אינה מבטיחה הימנעות ממעורבות בהתנהגויות סיכון (Davinson & Sillence, 2010). מחקר זה מבקש להוסיף לידע על הקשר בין תפיסות לבין דפוסי התנהגות במרחב הסייבר ולהשיב על שאלת מחקר מרכזית: האם יימצאו הבדלי מגדר בקשר בין מודעות לפשעי סייבר לבין מעורבות בהתנהגויות סיכון במרחב הסייבר?

הבדלי מגדר בתפיסות הנוגעות לקורבנות של עבריינות והשלכותיהן על דפוסי התנהגות

הפרט חושש להיות קורבן לעברות שונות ונוטה להעריך שסיכוייו לכך גבוהים (Ferraro, 1995). ספרות המחקר מצביעה על מאפיינים אישיים כגורמים מסבירים לתגובה לאיום הקורבנות ולמידת החשש ותפיסת הסיכון, כגון מין, גיל ומִיצב

חברתי־כלכלי (Rader et al., 2007; Rader et al., 2009). ההבדלים בתפיסת הסיכון בין פרטים מקבוצות חברתיות־דמוגרפיות שונות מוסברים לרוב על־ידי הבדלים ביניהם בתחושת הפגיעות (vulnerability). המקור לתחושת הפגיעות במרחב הפיזי (offline) מיוחס לתפיסת היחיד כי אין ברשותו משאבים פיזיים, כלכליים או חברתיים כדי להתמודד עם האיום ועם השלכותיו (Hipp, 2010; Killias & Clerici, 2000; Pantazis, 2000).

הספרות נוטה להעמיק במיוחד בסוגיית הבדלי המגדר במידת החשש מקורבנות ובתפיסת הסיכון. נשים חוששות מקורבנות ונוטות לראות את סיכוייהן להיות קורבנות כגבוהים מסיכויי הגברים (Gilchrist, Bannister, Ditton, & Farrall, 1998; May, Rader, & Goodrum, 2010; Mesch, 2000; Owens, 2015), אף על פי ששיעור קורבנות נשים בעברות שונות אינו גבוה בפועל משיעורי הגברים (Rountree & Land, 1996). תפיסת הנשים בנוגע לאיום הקורבנות מיוחסת לרוב לתחושת הפגיעות הפיזית המלווה אותן, משום שהן נוטות לתחושה סובייקטיבית שאין ביכולתן להגן על עצמן מפני אירועי עבריינות (May et al., 2010; Schafer, Huebner, & Bynum, 2006). מנקודת מבט קרימינולוגית פמיניסטית, נשים נוטות לבטא חשש רב יותר מפני קורבנות, מאחר שהן חשופות יותר מגברים לסכנות רבות, כגון אלימות ביתית, אלימות מינית והטרדות (שהדיווח עליהן לרשויות הוא פחות ולפיכך הן נעדרות מסטטיסטיקות על מצב הפשיעה), ולכן הן נוטות להפנים תפיסה עצמית חרֵדה (fearful), בשעה שגברים נוטים להפנים תפיסה עצמית חסרת מורא (fearless) (Valentine in Cops & Pleysier, 2011).

לצד עיסוק מחקרי רב בטבעה של התגובה החברתית לפשע ("פחד מפשיעה" ו"תפיסת סיכון") ובגורמים המסבירים אותה, מחקרים מעטים יחסית בחנו את השלכותיהן של תפיסות אלו על דפוסי ההתנהגות. פרו (Ferraro, 1995) קיבץ את הביטוי ההתנהגותי של תפיסת הפשע לשתי קטגוריות: השלכות על התנהגות מתגוננת, כגון התקנה של מערכות אבטחה ורכישת אקדח, והשלכות על התנהגות נמנעת, כגון הימנעות משהות בחוץ בשעות החשֵכה. מחקרים מן המרחב הפיזי מצאו קשר בין תפיסת האיום מפשיעה לבין התנהגות מתגוננת וקשר בינה לבין הימנעות ממעורבות בהתנהגויות העלולות לחשוף לסכנה. נמצא כי חשש מפני פשיעה מגביל את המעורבות בהתנהגויות שגרתיות הנתפסות כמסכנות את הביטחון האישי (Miethe, 1995; Rader et al., 2007; Rengifo & Bolton, 2012). בהקשר של הסוגיה המגדרית, במחקרים מן המרחב הפיזי נמצא כי נשים נוטות להימנע יותר מגברים ממעורבות בהתנהגויות החושפות אותן לסכנת קורבנות (May et al., 2010; Mesch, 2000).

המחקרים האמורים מצביעים על הבדלי מגדר בתפיסות הנוגעות לאיום מקורבנות במרחב הפיזי ועל הבדלי מגדר בהתנהגויות החושפות לסכנה במרחב זה. מחקר זה מבקש לבחון את הסוגיה במרחב הסייבר ולשאול אם קיימים הבדלים בין גברים לבין נשים ברמת המודעות לפשעי סייבר ובמידת מעורבותם בהתנהגויות סיכון במרחב הסייבר. החשיבות בכיוון המחקר הזה נעוצה בצורך להבין אם הקשר בין מינו של הפרט

לבין מידת מעורבותו בהתנהגויות סיכון תלוי ברמת מודעותו לסכנות במרחב הסייבר או שמא קשר זה אינו תלוי ברמת המודעות. במילים אחרות, האם הקשר בין המין לבין מידת המעורבות בהתנהגויות סיכון אינו הכרתי, אלא מובנה בהבדלים מגדריים.

פשעי סייבר: תיאור התופעה

האינטרנט הרחיב את היקף ההזדמנויות לביצוע "פשיעה נתמכת מחשב" – התנהגויות בלתי חוקיות המוכרות מן המרחב הפיזי ומבוצעות כעת על־ידי שימוש בטכנולוגיית המחשבים, כגון הטרדה מקוונת, הפצת חומר פורנוגרפי והונאת צרכנים. כך התפתחה "פשיעה ממוקדת מחשב" שהופיעה עם התפתחות הטכנולוגיה ואין באפשרותה להיות מבוצעת מחוץ למרחב המקוון, מאחר שמטרתה העיקרית היא פגיעה במערכות מחשב, כגון הפצת תוכנות זדוניות ופריצות למחשבים (Newman & Clarke, 2013, pp. 10-13; Wall, 2010).

המונח "פשעי סייבר" כולל עברות ממוקדות מחשב – הפצת תוכנות זדוניות ועברות המבוצעות בסיוע מחשב – גנבת זהות והונאה (Brenner, 2007; Newman, 2009, p. 12; Wall, 2007; Yar, 2013, p. 9). עברות אלו נבדלות במאפייניהן, במטרותיהן ובהשלכותיהן, אך המשותף להן הוא ניצול תכונותיו המבניות של מרחב הסייבר, ובהן אנונימיות יחסית של התוקף, היות האינטרנט מרחב חברתי גלובלי ללא גבולות גאוגרפיים והיכולת להפיץ מידע במהירות להיקף גדול של צרכנים (Clough, 2010, pp. 5-9; Holt & Turner, 2012; Jewkes & Yar, 2013; Savona & Mignone, 2004).

"נוזקה" (malware) היא שם כולל לסוגים שונים של תוכנות זדוניות, כגון וירוס, תולעת, סוס טרויאני ותוכנת ריגול. תוכנות אלו נבדלות זו מזו בין היתר באופן הפצתן, כגון וירוס – על־ידי מעורבות של המשתמש בהורדת קבצים מסוימים או לחיצה על קישורים המופיעים בהודעות דואר אלקטרוני (להלן דוא"ל), ותולעת – על־ידי הפצה עצמאית, ובדרך שכפולן, אך מטרתן דומה – לשבש את פעילות המחשב או לגנוב מידע אישי על המשתמש לשם ביצוע עברת הונאה וגנבת זהות (Broadhurst & Choo, 2011; Jewkes & Yar, 2013; W. Kim, Jeong, C. Kim, & So, 2011; Newman, 2009; Wall, 2007, p. 147). חשוב לציין כי בנוגע למשתמש במחשב פרטי, הנזק בגין הידבקות המחשב בתוכנה זדונית עשוי להתבטא בתסכול רב בשל הזמן הנדרש להסרת התוכנה, באיבוד מידע, בפגיעה ביעילות העבודה ובהשקעה כספית בתיקון המחשב. ואולם, האיום הממשי בעברות אלו אינו רק המשתמש היחיד, אלא החברה הרחבה. החיבור הרשתי בין מערכות המחשב הגלובליות מאפשר להפיץ את האיום, ולפיכך הנזק המצטבר עלול להיות חמור בהרבה (Kumar, Mohan, & Holowczak, 2008; Wall, 2007, p. 19).

עברות אחרות המבוצעות בסביבה הווירטואלית הן גנבת זהות והונאה, עברות שנעשה בהן שימוש בלתי חוקי בפרטים האישיים של היחיד ללא ידיעתו, כגון במספר תעודת הזהות, במספר הדרכון ובפרטי כרטיס האשראי

(Allison, Schuck, & Lersch, 2005; Pontell, 2002). עברות אלו מוכרות מן הסביבה הפיזית, אך האינטרנט הקל על נגישות העבריין למידע האישי. כמו כן הוא הרחיב את הגישה לקהלים שונים גם מחוץ למרחב גאוגרפי נתון, ולפיכך הגדיל את היקף הקורבנות לעברות אלו ואת הנזק שהן גורמות (Copes, Kerley, Huff, & Kane, 2010; Sullins, 2006; Wall, 2007). גנבות הזהות וההונאה במרחב הסייבר יכולות להתבצע בטכניקה של הנדסה חברתית המכונה "דיוג" (phishing). בפעולת הדיוג התוקף (העבריין) שולח הודעת דוא"ל המתחזה כמגיעה ממקור מוסמך או מאדם ששמו מוכר לנמען. תגובת הנמען להודעת הדוא"ל תוביל לאתר מזויף שבו יתבקש למסור פרטים אישיים, בדרך כלל פרטים הנוגעים לחשבון הבנק, במטרה לבצע לאחר מכן הונאה (Clough, 2010, pp. 192-193; Vishwanath, Herath, Chen, Wang, & Rao, 2011).

יש לציין כי ההתפתחויות הטכנולוגיות של העשור האחרון, ובייחוד ביסוסן של רשתות חברתיות כמרחב דומיננטי של אינטראקציה בחיי רבים בחברה המערבית, תורמות גם הן לשגשוג העברות, שכן רשתות חברתיות מעודדות חשיפה עצמית מעצם טבען. המשתמש נוטה לחשוף את קשריו החברתיים ואת מקום עבודתו (Stutzman, Gross, & Acquisti, 2013), ופרטים אלו עלולים להיות מנוצלים באמצעות טכניקות שונות לביצוע עברות (Fire, Goldchmidt, & Elovici, 2014; Navarro & Jasinski, 2012).

כאמור, ספרות מדעי החברה, ובכללה הספרות הקרימינולוגית, מיעטה לבחון היבטים הכרוכים בחשיפה לסכנות המוגדרות כפשעי סייבר (Holt & Bossler, 2014). כמה חוקרים נתנו את דעתם לאתגר שהמרחב הווירטואלי מציב בפני המחקר הקרימינולוגי, ובייחוד להעדר מגע פיזי בין התוקף לבין הקורבן, לאנונימיות התוקף והקורבן ולקושי לזהות את הקורבנות ואת אומדן הנזק הממשי שהעברה גורמת (Jaishankar, 2007; Yar, 2005). עם זאת, ובדומה לתפיסתו של קסטלס (Castells, 2001, p. 203) שטען כי מרחב הסייבר אינו מציאות וירטואלית (virtual reality), אלא יש וירטואליות אמתית (real virtuallity), מצאו החוקרים כי ניתן לבחון את תופעת הפשיעה והקורבנות במרחב הסייבר בכלים תאורטיים המוכרים מן הסביבה הפיזית (Grabosky, Smith, & Dempsey, 2001; Yar, 2005).

דפוסי התנהגות יום־יומיים והסיכוי לקורבנות לפשעי סייבר

הספרות הקרימינולוגית העוסקת בתופעת הקורבנות (victimization) נשענת בעיקר על תאוריית החשיפה לאורח החיים (lifestyle exposure theory) (Hindelang, Gottfredson, & Garofalo, 1978) ועל תאוריית הפעילות השגרתית (routine activity theory) (Cohen & Felson, 1979). תאוריית הפעילות השגרתית מרחיבה את רעיונותיה המרכזיים של תאוריית החשיפה לאורח החיים בנוגע להבנת המשתנים המסבירים את הסיכון לקורבנות, ולפיכך הספרות נוטה לקשור בין השתיים ולראות בהן מסגרת

תאורטית אחת (Miethe, Stafford, & Long, 1987). בבסיס הסבר תאורטי זה עומדות שתי הנחות: הזדמנות להיפגעות מעבריינות מתרחשת בהתכנסותם של שלושה רכיבים בזמן ובמקום מסוימים – קרבה לתוקף פוטנציאלי, קיומה של מטרה מתאימה והעדר אבטחה מתאימה, ושינויים מבניים בדפוסי הפעילויות היום־יומיים מייצרים מבנה הזדמנויות לפשיעה ולקורבנות (שם). כמו כן, התאוריה מניחה כי קבוצות חברתיות (על בסיס מין ביולוגי, גיל, מִיצב כלכלי, מוצא אתני וסטטוס משפחתי) נבדלות באורח חייהן, ולפיכך הן נבדלות גם בסיכוי ליפול קורבן למעשה פשע. במהלך השנים נמצאה מסגרת תאורטית זו מתאימה להסבר גורמי סיכון במרחב הפיזי לטווח רחב של סוגי קורבנות, ובעיקר להסבר של קורבנוּת לעברות רכוש ופגיעות פיזיות (לסקירה נרחבת ראו Spano & Freilich, 2009). המחקרים המעטים שעסקו בסוגיה המגדרית בהקשר של תאוריית הפעילות השגרתית עומדים על כך שגברים ונשים נבדלים בדפוסי הפעילות השגרתיים שלהם, והבדלים אלו מובְנים בסדר החברתי ומשקפים הבדלים בציפיות התרבותיות (Popp & Peguero, 2011).

בעשור האחרון מבקשים חוקרים להחיל על המרחב הווירטואלי את יסודותיהן המושגיים של התאוריות האמורות ולבחון אם בדומה למרחב הפיזי, קורבנות לפשעי סייבר קשורה להתנהגות היחיד ולהקשרהּ החברתי. בהקשר זה נמצאו הוכחות אמפיריות לקשר בין מידת המעורבות בהתנהגויות סיכון במרחב הסייבר לבין הסיכוי לקורבנות, כך שמעורבות בהתנהגויות מסוימות במרחב הסייבר מגדילה את הסיכוי להיות קורבן לעברה. באשר לחשיפה להונאה כלכלית, נמצא כי ביצוע פעולות בנקאיות מקוונות, רכישה מקוונת של מוצרים או הורדת תוכנות מגדילים את הסיכוי לקורבנות להונאה כלכלית במרחב הסייבר (Holt & Turner, 2012; Reisig, Pratt, & Holtfreter, 2009; Reyns, 2013). נגו ופטרנוסטר (Ngo & Paternoster, 2011) הוסיפו כי זמן השהות במרחב הווירטואלי אינו מגדיל את הסיכוי לקורבנות, אלא סוג הפעילות הווירטואלית והזמן המוקדש לביצועה הם שמשפיעים על הסיכוי לקורבנות סייבר, ובכללה הונאה. באשר לחשיפה לתוכנות זדוניות, נמצא קשר בין אורח חייו של המשתמש, ובייחוד פתיחת קבצים המגיעים ממקור לא ידוע והורדת תוכנות לא מורשות, לבין הסיכוי להיפגע מווירוס במחשב (Bossler & Holt, 2009; Choi, 2008).

לצד זיהוּיָם של דפוסי התנהגות מקוונת המגדילים את הסיכוי לקורבנות לתוכנות זדוניות, לגנבת זהות ולהונאה, מחקרים אלו הצביעו גם על הבדלים בין יחידים בקבוצות חברתיות־דמוגרפיות מובחנות בסיכוייהם לקורבנות. לעניינו של מחקר זה, נמצאו הבדלי מגדר במידת המעורבות בהתנהגויות סיכון במרחב הסייבר. גברים, יותר מנשים, מבצעים פעילויות מסכנות, דוגמת בנקאות מקוונת, הורדת תוכנות בלתי מורשות וצפייה בתוכני מחשב בלתי חוקיים ("פירטיים") (Bossler & Holt, 2009; Reyns, 2013).

אפשר אפוא לסכם עד כה ולומר כי מחקרים שביקשו לבחון את תקפותן של תאוריות אורח החיים על המרחב הווירטואלי הצביעו על קיומו של קשר בין מעורבות

בהתנהגויות מסוימות במרחב הסייבר לבין הסיכוי לקורבנות. עם זאת, המחקר הקיים לוקה במגבלות מסוימות, ומחקרנו מבקש להתגבר עליהן ולהרחיב את הבנת גורמי הסיכון במרחב הסייבר. ראשית, למיטב ידיעתנו, חסרה התייחסות מחקרית לגורמי סיכון לחשיפה לגנבת זהות. ריינס (Reyns, 2013) טען לבחינת גורמי סיכון לגנבת זהות, אך בפועל בחן קורבנות לעברת הונאה בלבד. בהמלצתו של פונטל (Pontell, 2002) יבחין מחקרנו בין גנבת זהות לבין הונאה ויבחן דפוסי התנהגות מסַכנים של כל אחת מהן. נוסף על כך, במחקרים רבים הורכבו המדגמים מתלמידי מכללות (ראו, לדוגמה, Bossler & Holt, 2009; Ngo & Paternoster, 2011). המדגם במחקרנו ייצג את משתמשי האינטרנט הפרטי בישראל בקרב בני 18 ומעלה.

נוסף על המוטיבציה לעמוד על מידת מעורבותם של משתמשי האינטרנט הפרטי בישראל בהתנהגויות סיכון לשלוש עברות סייבר, מחקר זה מבקש לעמוד על הקשר בין מודעות לסכנות לבין מעורבות בהתנהגויות סיכון. מחקרים ברוח תאוריית הפעילות השגרתית רואים בהעלאת רמתה של המודעות החברתית לפשעי סייבר אמצעי להפחתת מידת המעורבות בהתנהגויות סיכון במרחב זה (Choi, 2008; McQuade, 2006, p. 487).

מעורבות בהתנהגויות סיכון במרחב הסייבר ומודעות לפשעי סייבר

מחקרים מצביעים על העדר יכולתם של מערכות טכנולוגיות ושל ויסות חוקתי לספק הגנה מלאה מפשעי סייבר ועל כך שהתמודדות עם פשיעה כזאת מחייבת את מודעות המשתמש לסכנות ואת מעורבותו (LaRose, Rifon, & Enbody, 2008; Mitnick & Simon, 2011; Wall, 2008, pp. 186-206). מחקרים שהתמקדו בבחינת הקשר בין מודעות לפשעי סייבר, ובייחוד מודעות לתוכנות זדוניות, לבין דפוסי שימוש באמצעי הגנה טכנולוגיים, מצאו כי ככל שמשתמש המחשב מודע יותר לאיום ותופס אותו כחמור, כך יפעל להגן על עצמו מפניו על־ידי שימוש באמצעי האבטחה הטכנולוגיים הקיימים, כגון תוכנות נוגדות ריגול (anti-spyware) ונוגדות וירוס (anti-virus) (Bowen, Devarajan, & Stolfo, 2011; Furnell, Bryant, & Phippen, 2007; Kritzinger & von Solms, 2010; Liang & Xue, 2010). עם זאת, אין במחקרים אלו כדי להעיד על הקשר בין רמת המודעות לבין מידת המעורבות בהתנהגויות סיכון הכרוכות בדפוסי הפעילות המקוונת היום־יומית של המשתמש.

ממחקרים שנעשו בהקשר של התנהגות צרכנית מקוונת, עולה כי במרחב זה המודעות לסכנות אינה מבטיחה הימנעות ממעורבות בהתנהגויות סיכון. תופעה זו מכונה "פרדוקס האינטרנט" או "אפקט הטרייד־אוף" (the trade-off effect). נמצא כי במרחב הסייבר הציבור מניח לחששות הנוגעים לסכנות הגלומות בביצוע רכישות מקוונות ומוכן למסור פרטים אישיים בתמורה לתועלת שהוא מייחס לה חשיבות. בהקשר של האינטרנט, התמורה היא חוויית הנוחות והנגישות במשך כל שעות היממה (Davinson & Sillence, 2010; Tsai, Egelman, Cranor, & Acquisti, 2011).

עם זאת, קשר זה לא נבחן בהקשר רחב יותר של התנהגויות המבוצעות במרחב הסייבר, ולא נבחנו הבדלים בין קבוצות חברתיות־דמוגרפיות מובחנות, ובכללם בין גברים לבין נשים. על סמך ספרות המחקר מן המרחב הפיזי (המתוארת למעלה), המצביעה על הבדלי מגדר בתפיסות הנוגעות לאיום הקורבנות ועל הבדלי מגדר במעורבות בהתנהגויות סיכון, מחקר זה מבקש לבחון את השפעתו של המין הביולוגי על הקשר בין רמת המודעות לפשעי סייבר לבין מידת המעורבות בהתנהגויות סיכון במרחב הסייבר.

גורמים נוספים העשויים להשפיע על מודעות לפשעי סייבר ועל מעורבות בהתנהגויות סיכון

לפי סקירת הספרות, מצופה למצוא הבדלי מגדר ברמת המודעות לפשעי סייבר ובמידת המעורבות בהתנהגויות סיכון במרחב הסייבר. כמו כן, נצפה להבדלי מגדר בקשר בין שני המשתנים האמורים. עם זאת, קיימים משתני רקע נוספים – משתנים חברתיים־דמוגרפיים ומאפייני גלישה – העשויים להשפיע על רמת המודעות לפשעי סייבר ועל מידת המעורבות בהתנהגויות סיכון.

מאפיינים חברתיים־דמוגרפיים

לפי תאוריית הפעילות השגרתית, קבוצות חברתיות נבדלות בסיכוייהן להיות קורבן לעברה (Miethe et al., 1987; Spano & Freilich, 2009). מחקרים שבחנו סוגיה זו במרחב הסייבר מתקפים טענה זו, ולפיכך הוכנסו המשתנים האלה כמשתני פיקוח:

גיל: לעומת קבוצות הגיל הבוגרות, קבוצות הגיל הצעירות נוטות לבלות זמן רב יותר בפעילויות מקוונות ולהיות מעורבות בהתנהגויות המגדילות את הסיכוי להיות קורבן לפשעי סייבר שונים (Pratt et al., 2010). במחקר שנעשה בקרב תלמידי מכללות נמצא כי בקבוצת גיל זו יש נטייה להורדה בלתי חוקית של תוכני מחשב מן האינטרנט, פעילות המעלה את הסיכוי לקורבנות לתוכנות זדוניות (Higgins, 2007; Hinduja, 2001). כמו כן, במחקר שנערך בקרב האוכלוסייה הבוגרת בבריטניה נמצא כי עם העלייה בגיל מצטמצמת המעורבות בהתנהגויות סיכון החושפות לעברות הונאה, כגון בנקאות מקוונת וביצוע רכישות מקוונות (Reyns, 2013).

מצב משפחתי: לעומת אנשים שאינם נשואים, אנשים נשואים מבצעים יותר פעולות סיכון, כגון בנקאות מקוונת ורכישות מקוונות (Reyns, 2013). מאחר שבקרב קבוצות אוכלוסייה צעירות המתאפיינות במעורבות גבוהה בהתנהגויות סיכון בולטים הרווקים, גם הם עשויים להיות מעורבים בהתנהגויות סיכון. המחקר מבקש אפוא לפקח על משתנה זה בבואנו לאמוד את הקשר בין המין הביולוגי לבין מידת המעורבות בהתנהגויות סיכון.

מוצא אתני: בכל הנוגע לדפוסי השימוש באינטרנט בישראל, להשתייכות האתנית יש השפעה על הנגישות לאינטרנט ועל דפוסי השימוש בו. שיעור המשתמשים באינטרנט

בקרב האוכלוסייה הערבית נמוך משיעורם בקרב האוכלוסייה היהודית, ותפיסת הסיכון בחברה הערבית בנוגע לשימוש באינטרנט גבוהה מתפיסת הסיכון בחברה היהודית (מש ותלמוד, 2008). לפיכך, אפשר לצפות שתפיסות אלו עשויות לעצב דפוסי התנהגות במרחב הסייבר.

רמת השכלה: נגישותן לאינטרנט של קבוצות האוכלוסייה המשכילות גבוהה מנגישותן של קבוצות האוכלוסייה המשכילות פחות (Robinson, DiMaggio, & Hargittai, 2003). מאחר שתדירות החשיפה לאינטרנט ומִשכה עשויים להעלות את הסיכוי לקורבנות במרחב הסייבר (Ngo & Paternoster, 2011), יש צורך לפקח על משתנה זה.

מאפייני גלישה: ספרות המחקר מצביעה על ממצאים סותרים בנוגע להשפעתם של מאפייני גלישה – ותק בגלישה ותדירות גלישה – על מידת המעורבות בהתנהגויות סיכון במרחב הסייבר. מצד אחד, יש ממצאים לכך שעם העלייה בוותק השימוש באינטרנט קטֵנה מידת המעורבות בהתנהגויות סיכון במרחב הסייבר, ולפיכך קטֵנה גם החשיפה לסכנות במרחב זה (Ngo & Paternoster, 2009). לעומת זאת, ממצאים אחרים מלמדים שוותק בגלישה ותדירות שימוש גבוהה מוסיפים לתחושת השליטה במרחב הסייבר ולפיכך מביאים למעורבות גבוהה יותר בהתנהגויות סיכון (Cho, Lee, & Chung, 2010). בד בבד, הקשר בין המין הביולוגי לבין מידת המעורבות בהתנהגויות סיכון יכול להיות מושפע מהבדלים במאפייני הגלישה של קבוצות אלו. ואכן, נשים גולשות באינטרנט פחות מגברים ומדווחות על מיומנויות דיגיטליות נמוכות יותר (Hargittai & Shafer, 2006). מחקר זה יפקח אפוא על מאפייני הגלישה ועל הוותק בגלישה, שהשפעתם על מידת המעורבות בהתנהגויות סיכון מעורבת.

מטרת המחקר וההשערות

למחקר זה שתי מטרות מרכזיות: להוסיף לידע על אודות הקשר בין תפיסות לבין דפוסי התנהגות במרחב הסייבר ולבחון אם יש לו הקשר מגדרי. מן המטרות נגזרו ההשערות האלה:

1. בהתבסס על ספרות ענפה מן המרחב הפיזי המצביעה על כך שתפיסת האיום מקורבנות בקרב נשים גבוהה מזו של גברים (Rader et al., 2007), אפשר לצפות שיימצאו הבדלים בין גברים לבין נשים ברמת המודעות לסכנות סייבר, כך שנשים יגלו מודעות רבה יותר לסכנות לעומת גברים.
2. על רקע מחקרים שנעשו בקרב תלמידי מכללות ברוח תאוריית הפעילות השגרתית ומצביעים על הבדלי מגדר במידת המעורבות בהתנהגויות סיכון במרחב הסייבר (Bossler & Holt, 2009; Reyns, 2013), אפשר לצפות שדפוס זה יאפיין גם את אוכלוסיית משתמשי האינטרנט הפרטי באופן כללי, לפיכך אנו משערים שיימצאו

הבדלים בין גברים לבין נשים במידת המעורבות בהתנהגויות סיכון, כך שנשים יהיו מעורבות בהתנהגויות סיכון במרחב הסייבר פחות מגברים.

3. בהתבסס על ספרות מן המרחב הפיזי המוצאת קשר בין תפיסות בנוגע לקורבנות מעבריינות לבין מידת המעורבות בדפוסי התנהגות החושפים לסכנות (Miethe, 1995; Rader et al., 2007; Rengifo & Bolton, 2012), נשער כי יימצא קשר שלילי בין רמת המודעות לפשעי סייבר לבין מידת המעורבות בהתנהגויות סיכון במרחב הסייבר.
4. המחקר מבקש לעמוד על הבדלי מגדר בקשר בין רמת המודעות לפשעי סייבר לבין מידת המעורבות בהתנהגויות סיכון במרחב הסייבר. אנו מצפים שתהיה אינטראקציה בין המין הביולוגי לבין מודעות לפשעי סייבר, כך שהקשר השלילי שיימצא בין רמת המודעות לפשעי סייבר לבין מידת המעורבות בהתנהגויות סיכון יהיה שלילי יותר בקרב נשים לעומת גברים.

שיטה

נתוני המחקר נאספו באמצעות סקר טלפוני שבוצע במהלך חודש דצמבר 2014, על־ידי מראיינים מטעם היחידה לייעוץ סטטיסטי באוניברסיטת חיפה.

הנדגמים

הנתונים נאספו בקרב 1,850 מרואיינים, בני 18 ומעלה, שדיווחו על שימוש באינטרנט לצרכים פרטיים, 54.5% מהם היו נשים ו־45.5% היו גברים. באשר להתפלגות הגילים, 16% מן המשתתפים היו בני 18–29, 27% היו בני 30–44, 29% היו בני 45–59, ו־27% היו בני 60 או יותר. באשר להרכב המשתתפים לפי רמת ההשכלה, 35% היו בעלי 12 שנות לימוד או פחות, 22% היו בעלי 13–15 שנות לימוד ו־43% היו בעלי 16 שנות לימוד או יותר. מבין המשתתפים, 77% היו יהודים ו־23% היו ערבים. באשר למצבם המשפחתי של המשתתפים, 72% מהם היו נשואים, 19% היו רווקים ו־9% היו יחידים (פרודים, גרושים או אלמנים).

השווינו בין נתוני המדגם לבין מאפייני הגולשים באינטרנט, כפי שהם מופיעים בנתוני הלשכה המרכזית לסטטיסטיקה (2014, לוח 5, עמ׳ 90–91) (להלן הלמ״ס). ההשוואה נעשתה לפי קבוצת גיל, מין, רמת השכלה ומוצא אתני, ועלו ממנה הבדלים בהרכב הגילים במדגם לעומת מאפייניה של אוכלוסיית הגולשים באינטרנט כפי שהם מופיעים בנתוני הלמ״ס. על מנת לייצג היטב את מאפייני הגולשים באינטרנט שוקללו אפוא נתוני המדגם לפי קבוצות גיל על־פי נתוני הלמ״ס.

הליך הדגימה

בשונה ממחקרי עבר, שהתמקדו בעיקר באוכלוסיית תלמידי מכללות או במועסקים בחברות שונות, ייחודו של מחקר זה הוא בבחינת התגובה החברתית (עמדות והתנהגות) לפשעי סייבר כפי שהיא באה לידי ביטוי בקרב משתמשי האינטרנט הפרטי באוכלוסייה הכללית בישראל. אוכלוסייה זו מגוונת במאפייניה החברתיים־דמוגרפיים ובמיומנויותיה הטכנולוגיות, והיא נחשבת לחולייה החלשה בשרשרת האבטחה (S. J. Furnell, S. M. Furnell, Jusoh, & Katsabas, 2006; Mitnick & Simon, 2011; Sasse, Brostoff, & Weirich, 2001; Savona & Mignone, 2004; Wall, 2007, p. 186). בשונה ממשתמשי מחשב במקומות עבודה ובארגונים שונים, המשתמש הפרטי אחראי בעצמו לאבטחת המידע במכשיר הגלישה שלו, והוא אינו נמצא תחת עין בוחנת המגְנה על התנהלותו או מפקחת על רמת מודעותו לסכנות (Furnell et al., 2007; Kritzinger & von Solms, 2010; Liang & Xue, 2010).

כאמור, דגימת משתמשי האינטרנט הפרטי בישראל בוצעה באמצעות סקר טלפוני של היחידה לייעוץ סטטיסטי באוניברסיטת חיפה. המדגם נלקח מתוך קובץ המכיל את רשימת מנויי הטלפון הנייח והנייד בישראל. במדגם המקורי עלו 5,285 נדגמים. 1,701 מרואיינים סירבו להשיב על השאלון בפנייה הראשונה, ו־696 מרואיינים הפסיקו את ההתקשרות לאחר דחיות מרובות. 2,888 נדגמים הביעו נכונות לענות על השאלון. לנדגמים שהביעו נכונות לענות הוצגה שאלת סינון: "האם אתה משתמש/לא משתמש באינטרנט לשימושך הפרטי?". שיעור המשיבים בחיוב על שאלת הסינון שהסכימו להתראיין עמד על 35% מתוך המדגם המקורי.

המשתנים

המשתנים התלויים

מעורבות בהתנהגות סיכון. השאלון הורכב מחמש שאלות הבוחנות את מידת המעורבות בהתנהגויות העלולות לחשוף את המשתמש לקורבנות לתוכנות זדוניות, לגנבת זהות ולהונאה במרחב הסייבר. השאלות נלקחו ממחקרים קודמים שבחנו דפוסי התנהגות החושפים לסכנות במרחב הסייבר (Bossler & Holt, 2009; Choi, 2008). למרואיינים הוצגו שאלות דיכוטומיות המתייחסות למעורבות בהתנהגויות הסיכון האלה: "הקלדת נתונים אישיים, כגון מספר תעודת זהות או מספר כרטיס אשראי, במחשב שאינו שלך", "הכנסת פרטים של חשבון הבנק שלך באתר שאינך יודע אם הוא בטוח", "ענית על אימייל המודיע על זכייה בפרס", "ענית על אימייל המודיע כי פג תוקפה של סיסמה או על חסימת חשבון פעיל שלך (למשל חשבון בנק אונליין, אימייל, רשת חברתית)", "הורדת שירים, סרטים או תוכנות בלי לשלם או לרכוש רישיון עליהם". התשובות קודדו באופן הזה: 1 – מעורב בביצוע התנהגות מסוג זה, 0 – כלל לא מעורב

בביצוע התנהגות מסוג זה. משתנים אלו הוכללו משום שהיה להם תוקף נראה, שנבדק באוניברסיטת חיפה בחודש יוני 2014 בשתי קבוצות מיקוד משתי אוכלוסיות שונות.

מדד המעורבות בהתנהגויות סיכון במרחב הסייבר הוא מדד כולל, והוא חושב כסכום התשובות שהמרואיין נתן לחמש השאלות. ערכי המדד היו מ־0 – כלל לא מעורב בהתנהגויות סיכון במרחב הסייבר, עד 5 – מעורב במידה רבה בהתנהגויות סיכון במרחב הסייבר.

מודעות לסכנות סייבר. השאלון הורכב משש שאלות הבוחנות באופן ישיר את רמת המודעות לסכנות הסייבר. השאלות נאספו מסקרים וממחקרים שונים שבחנו את רמת המודעות לפשעי סייבר (לדוגמה, D'Arcy, Hovav, & Galletta, 2009; Furnell et al., 2006). למשתתפים הוצגו השאלות האלה: "באיזו מידה אתה מודע לאפשרות שייעשה שימוש בכרטיס האשראי שלך לקניות ללא רשותך?", "באיזו מידה אתה מודע לאפשרות שייעשה שימוש בפרטים אישיים שלך (המופיעים בפייסבוק או בחשבון אימייל), כגון מספר תעודת זהות, שם וכתובת מגורים, ללא רשותך, ויתחזו לך?", "באיזו מידה אתה מודע לאפשרות שישלחו לך הודעות מייל שקריות שבהן מבקשים פרטים, כגון מספר חשבון בנק או כתובת שלך, במטרה להונות אותך (לגרום לנזק כספי או לגנוב פרטים אישיים)?". באיזו מידה אתה מודע לאפשרות שתאבד מידע אישי השמור במחשב האישי שלך כתוצאה מווירוס?", "באיזו מידה אתה מודע לאפשרות שמישהו זר ישתלט על המחשב שלך כדי לבצע עברה קולקטיבית (כדי לתקוף מחשבים אחרים)?", "באיזו מידה אתה מודע לאפשרות שגורם זר יבנה חשבון פייסבוק על שמך ללא ידיעתך?". טווח התשובות היה מ־1 – כלל לא מודע, עד 5 – מודע במידה רבה מאוד. המהימנות הפנימית של שש השאלות הבוחנות רמת מודעות לפשעי סייבר הייתה גבוהה ($\alpha = .841$).

מדד המודעות לסכנות סייבר הוא מדד כולל, והוא חושב כסכום התשובות שהמרואיין השיב לשש השאלות. לפיכך, המדד קיבל ערכים מ־6 – לא מודע כלל לסכנות במרחב הסייבר, עד 30 – מודע במידה רבה לסכנות במרחב הסייבר.

המשתנים הבלתי תלויים: מאפיינים חברתיים־דמוגרפיים

מין: 1 – אישה, 0 – גבר.

קבוצת גיל: יצרנו ארבעה משתנים מדומים (dummy variables) לקבוצת הגיל: בני 18–29, בני 30–44, בני 45–59 ובני 60 או יותר.

רמת השכלה: יצרנו שלושה משתנים מדומים לרמת השכלה: 12 שנות לימוד או פחות, 13–15 שנות לימוד, 16 שנות לימוד או יותר.

השתייכות אתנית: יצרנו משתנה מדומה שבו 1 – יהודי ו־0 – אינו יהודי.

מצב משפחתי: יצרנו שלושה משתנים מדומים למצב משפחתי: רווק, נשוי ויחיד (שאינו רווק).

המשתנים הבלתי תלויים: מאפייני גלישה

תדירות גלישה: יצרנו שלושה משתנים מדומים: משתמש אינטרנט כבד (heavy user), הגולש באינטרנט לפחות שעה בכל יום; משתמש אינטרנט בינוני (mid user), הגולש באינטרנט פחות משעה בכל יום; משתמש אינטרנט קל (light user), הגולש באינטרנט פחות מפעם ביום.

ותק גלישה: 1 – משתמש אינטרנט ותיק (senior user), הגולש באינטרנט 6 שנים או יותר, 0 – משתמש אינטרנט חדש (novice user), הגולש באינטרנט פחות מ־6 שנים.

המשתנים הבלתי תלויים: אינטראקציה בין המין לבין מדד מתוקנן של מודעות לסכנות מפשעי סייבר

על מנת לצמצם את המתאם הגבוה ($r = .848$) בין המין לבין משתנה האינטראקציה, ובין רמת המודעות בערך מוחלט לבין משתנה האינטראקציה ($r = .428$), ביצענו תִקנון של מדד המודעות לסכנות במרחב הסייבר (Zscore), ומשתנה זה הוכנס לאינטראקציה עם המין. המשתנה מין, שקיבל את הערכים 0 – גבר, 1 – אישה, הוכפל במדד המתוקנן של מודעות לסכנות מפשעי סייבר.

ממצאים

הבדלי מגדר ברמת המודעות לסכנות סייבר ובמידת המעורבות בהתנהגויות סיכון במרחב הסייבר

רמת המודעות לסכנות סייבר בקרב כלל הנדגמים

לוח 1 מציג שישה פריטים המצביעים על רמת המודעות לאופני הביטוי השונים של פשעי סייבר בקרב כלל הנדגמים ובקרב גברים ונשים בנפרד. השאלות מדורגות לפי רמת המודעות, מרמת מודעות גבוהה מאוד (5) ועד רמת מודעות נמוכה מאוד (1). כמו כן, הלוח מציג את ערכי המדד הכולל של רמת המודעות בקרב כלל הנדגמים ובקרב גברים ונשים בנפרד.

לוח 1: רמת המודעות לסכנות סייבר בכלל המדגם ובקרב גברים ונשים בנפרד

	כלל המדגם $N = 1,785$		גברים $n = 809$		נשים $n = 976$		הבדלים במודעות בין גברים לבין נשים	מדד לגודל האפקט
באיזו מידה אתה מודע לסכנות האלה, מ־1 (כלל לא מודע) עד 5 (מודע במידה רבה מאוד):	*SD*	*M*	*SD*	*M*	*SD*	*M*	*t*	Cohen's *d*
1. האפשרות שישלחו לך הודעות מייל שקריות שבהן מבקשים פרטים, כגון מספר חשבון בנק או כתובת, במטרה להונות אותך (לגרום נזק כספי או לגנוב פרטים אישיים)	1.21	4.34	1.29	4.23	1.14	4.43	3.445**	0.164
2. האפשרות שייעשה שימוש בכרטיס האשראי שלך לקניות ללא רשותך	1.20	4.31	1.27	4.22	1.13	4.38	2.700**	0.133
3. האפשרות שייעשה שימוש ללא רשותך בפרטים אישיים שלך (המופיעים בפייסבוק או בחשבון דוא"ל), כגון מספר תעודת זהות, שם וכתובת, ויתחזו לך	1.28	4.15	1.34	4.06	1.24	4.23	2.802**	0.132
4. האפשרות שתאבד מידע אישי השמור במחשב שלך כתוצאה מווירוס	1.26	4.11	1.30	4.03	1.23	4.17	2.390*	0.110
5. האפשרות שמישהו זר ישתלט על המחשב שלך כדי לבצע עבֵרה קולקטיבית (כדי לתקוף מחשבים אחרים)	1.46	3.74	1.48	3.68	1.45	3.79	1.565	
6. האפשרות שגורם זר יבנה חשבון פייסבוק על שמך ללא ידיעתך	1.57	3.62	1.59	3.52	1.55	3.70	2.350*	0.114
מדד מודעות לסכנות סייבר מ־6 (אין מודעות כלל) עד 30 (מודעות גבוהה ביותר)	6.33	24.32	6.67	23.81	6.01	24.74	3.061**	0.147

* $p \leq .001$ *** $p \leq .01$ ** $p \leq .05$

מלוח 1 עולה כי בקרב כלל הנדגמים, רמת המודעות הגבוהה ביותר היא לעברות הונאה מקוונות המבוצעות באמצעות שליחת הודעות דוא"ל שקריות (*M* = 4.34, *SD* = 1.21) ובאמצעות שימוש לא מורשה בכרטיס האשראי (*M* = 4.31, *SD* = 1.20). רמת המודעות הנמוכה ביותר היא לגנבת זהות המבוצעת באמצעות פתיחת חשבון פייסבוק על שם המשתמש (*M* = 3.62, *SD* = 1.57) ולווירוסים שנועדו לבצע עברה קולקטיבית (*M* = 3.74, *SD* = 1.46).

בהמשך מוצגים ערכים המתארים את המדד של רמת המודעות הכוללת של שש השאלות הבוחנות רמת מודעות לפשעי סייבר, מרמת מודעות נמוכה מאוד (6) ועד רמת מודעות גבוהה מאוד (30). מלוח זה עולה כי רמת המודעות לכלל סכנות הסייבר שהמחקר עוסק בהן, בקרב כלל הנדגמים, היא גבוהה יחסית (*M* = 24.32, *SD* = 6.33).

רמת המודעות לסכנות סייבר בקרב גברים ובקרב נשים בנפרד

בהמשך, לוח 1 מציג תוצאות מבחן T הבוחן את ההבדלים בין גברים לבין נשים בתגובותיהם לשישה היגדים המייצגים מודעות לסכנות סייבר. מטרתם של מבחנים אלו הייתה לבחון אם בדומה למרחב הפיזי, גם במרחב הווירטואלי גברים ונשים נבדלים בתפיסותיהם בנוגע לאיום הקורבנות. מן הממצאים עולה כי בחמישה מתוך שישה אופני הביטוי השונים לביצוע פשעי סייבר, נשים מודעות לסכנות יותר מגברים באופן מובהק סטטיסטית. יוצא דופן הוא רמת המודעות להשתלטות על המחשב לשם ביצוע עברה קולקטיבית. באשר למדד הכולל של רמת המודעות לפשעי סייבר, נמצא כי נשים מודעות יותר מגברים באופן מובהק סטטיסטית.

רמת המעורבות בהתנהגויות סיכון בקרב כלל הנדגמים

לוח 2 מציג חמישה פריטים המצביעים על רמת המעורבות בהתנהגויות סיכון במרחב הסייבר, ואת ערכי המדד הכולל של מעורבות בהתנהגויות סיכון.

לוח 2: רמת המעורבות בהתנהגויות סיכון במרחב הסייבר בכלל המדגם ובקרב גברים ונשים בנפרד

	כלל המדגם $N = 1,785$		גברים $n = 842$		נשים $n = 1,008$		הבדלים בהתנהגות בין גברים לבין נשים	מדד לגודל האפקט
רמת המעורבות בהתנהגות סיכון: 0 (כלל לא מעורב), 1 (מעורב)	*SD*	*M*	*SD*	*M*	*SD*	*M*	*t*	Cohen's *d*
1. הורדת שירים, סרטים או תוכנות בלי לשלם או לרכוש רישיון עליהם	0.44	0.26	0.46	0.32	0.40	0.20	5.69**	0.274
2. הקלדת נתונים אישיים, כגון מספר תעודת זהות או מספר כרטיס אשראי, במחשב שאינו שלך	0.39	0.18	0.37	0.17	0.39	0.19		
3. ענית על דוא"ל שמודיעים בו כי פג תוקפה של סיסמה או על חסימת חשבון פעיל שלך (למשל חשבון בנק מקוון, דוא"ל, רשת חברתית)	0.34	0.13	0.34	0.13	0.33	0.12		
4. הכנסת פרטים של חשבון הבנק שלך באתר שאינך יודע אם הוא בטוח	0.22	0.05	0.24	0.06	0.19	0.04	2.28*	0.105
5. ענית על דוא"ל המודיע על זכייה בפרס	0.14	0.02	0.15	0.02	0.13	0.02		
מדד מעורבות בהתנהגות סיכון, מ־0 (אין מעורבות כלל) עד 5 (מעורבות גבוהה ביותר)	0.81	0.64	0.83	0.71	0.78	0.58	3.51**	0.166

* $p \leq .05$ ** $p \leq .01$ *** $p \leq .001$

מלוח 2 עולה כי מבין חמשת ההיגדים, רמת המעורבות הגבוהה ביותר בהתנהגות סיכון במרחב הסייבר היא ב"הורדת שירים, סרטים או תוכנות בלי לשלם או לרכוש רישיון עליהם" ($M = 0.26$, כלומר, 26% מכלל הנדגמים). רמת המעורבות הנמוכה ביותר נמצאה ב"תגובה לאימייל על אודות זכייה בפרס" ($M = 0.02$, כלומר, 2% מן הנדגמים) וכן ב"הכנסת פרטים של חשבון בנק באתר שאינך יודע אם הוא בטוח" ($M = 0.05$, 5% מכלל הנדגמים).

מדד המעורבות בהתנהגויות סיכון משקף כי בממוצע נחשפו כלל הנדגמים ל־0.64 פעילויות סיכון במרחב הסייבר בטווח הערכים 0–5, שבו 5 פירושו מעורבות בכלל התנהגויות הסיכון במרחב הסייבר.

רמת מעורבות בהתנהגויות סיכון בקרב גברים ונשים בנפרד

זאת ועוד, לוח 2 מציג תוצאות מבחן T הבוחן את ההבדלים בין גברים לבין נשים בתגובותיהם לחמישה היגדים המייצגים מעורבות בהתנהגויות סיכון במרחב הסייבר. נמצא כי באופן מובהק סטטיסטית גברים מעורבים יותר מנשים בשתיים מתוך חמש התנהגויות סיכון מקוונות: הורדת שירים, סרטים או תוכנות בלי לשלם או לרכוש רישיון עליהם; הכנסת פרטי חשבון בנק באתר שאינם יודעים אם הוא בטוח. לא נמצאו הבדלים מובהקים סטטיסטית בין גברים לבין נשים בדפוסי ההתנהגות האחרים המוצגים בשאלון.

בנוגע למדד המעורבות בהתנהגויות סיכון, הממצאים מורים שבממוצע נשים מעורבות פחות בהתנהגויות סיכון.

אפשר אפוא לסכם את ממצאי שני הלוחות ולומר כי נשים מודעות לסכנות סייבר יותר מגברים והן מעורבות בהתנהגויות סיכון פחות מגברים.

כדי לבסס ממצא זה בוצעו שני ניתוחי תסוגה שפיקחנו בהם על משתנים חברתיים־דמוגרפיים (קבוצת גיל, רמת השכלה, מוצא אתני ומצב משפחתי) וכן על תדירות הגלישה ועל ותק הגלישה באינטרנט. משתנים אלו עשויים להתערב בקשר בין המין לבין רמת המודעות ורמת המעורבות בהתנהגויות סיכון.

לוח 3 מציג את המודלים של שני ניתוחי התסוגה. במודל 1 חושבה משוואת תסוגה לניבוי רמת המודעות לסכנות סייבר באמצעות משתנים חברתיים־דמוגרפיים ומאפייני גלישה. במודל 2 חושבה רמת המעורבות בהתנהגויות סיכון במרחב הסייבר באמצעות משתנים דומים.

לוח 3: תסוגה לינארית מרובה – ניבוי מדד כולל למודעות לסכנות סייבר ומדד כולל למעורבות בהתנהגויות מסוכנות במרחב הסייבר כפונקציה של משתנים חברתיים־דמוגרפיים, תדירות השימוש באינטרנט וותק בגלישה[1]

	מודל 1			מודל 2		
	מדד כולל למודעות לסכנות סייבר			מדד כולל למעורבות בהתנהגויות סיכון		
	B	*SE*	β	*B*	*SE*	β
(קבוע)	20.221	.901**		.565	.111**	
מין: אישה	1.021	.303	.080**	–.110	.037	–.068**
קבוצת גיל 18–29	–.466	.656	–.028	.462	.081	.216**
קבוצת גיל 30–44	.905	.426	.065*	.244	.052	.135**
קבוצת גיל 45–59	.842	.412	.061*	.163	.050	.092**
לאום־אתניות יהודי	.024	.384	.002	–.025	.047	–.013
13–15 שנות לימוד	.376	.415	.024	.095	.051	.049
16 שנות לימוד או יותר	.646	.367	.051	.092	.045	.056*
מצב משפחתי נשוי	–.801	.553	–.057	–.185	.068	–.103**
יחיד (פרוד, גרוש, אלמן)	–.522	.740	–.024	–.206	.091	–.074*
משתמשי אינטרנט כבדים	.582	.423	.046	.126	.052	.077*
משתמשי אינטרנט בינוניים	.609	.441	.044	.008	.054	.005
גולשי אינטרנט ותיקים	2.451	.381	.164**	.125	.047	.065**
Adjusted R^2	.05			.09		

* $p \leq .001$ *** $p \leq .01$ ** $p \leq .05$

1 כל המשתנים המנבאים מוגדרים כמשתנים בינריים, עם הערכים 0 ו־1. הקטגוריות להשוואה במשתנים המנבאים: במין – גבר; בקבוצות הגיל – בני 60 או יותר; בלאום־אתניות – לא יהודי; בקבוצות רמת השכלה – עד 12 שנות לימוד; בקבוצות מצב משפחתי – רווק; בקבוצות משתמשי אינטרנט – משתמשי אינטרנט קלים (פחות מפעם ביום); בגלישה באינטרנט – גולשים שאינם ותיקים (פחות מ־6 שנים).

ממודל 1 בלוח 3 עולה כי גם כאשר כוללים במודל משתנים חברתיים־דמוגרפיים ומאפייני גלישה (תדירות השימוש באינטרנט ווותק הגלישה), נשים מודעות לסכנות סייבר יותר מגברים. מודל זה מעיד על כמה ממצאים נוספים. נמצא כי נדגמים מקבוצות הגיל הבוגרות (30–44, 45–59) מודעים לסכנות סייבר יותר מנדגמים מקבוצת הגיל המבוגרת (60 או יותר). כמו כן, נמצא כי בעלי ותק בגלישה באינטרנט (6 שנים או יותר) מודעים לסכנות סייבר יותר ממי שאינם ותיקים בגלישה.

ממצא זה תומך בהשערה 1 באשר להבדלים ברמת המודעות לסכנות סייבר – נשים מודעות לסכנות סייבר יותר מגברים.

בנוגע לרמת המעורבות בהתנהגויות סיכון במרחב הסייבר, ממצאי מודל 2 בלוח 3 מורים שגם כאשר כוללים במודל משתנים חברתיים־דמוגרפיים ומאפייני גלישה (תדירות השימוש באינטרנט ווותק הגלישה), נשים מעורבות בהתנהגויות סיכון פחות מגברים. עוד עולה מן המודל כי ככל שצעירים יותר, רמת המעורבות בהתנהגויות סיכון גבוהה יותר. זאת ועוד, המשכילים ביותר, בעלי 16 שנות לימוד או יותר, מעורבים בהתנהגויות סיכון יותר מבעלי 12 שנות לימוד או פחות. עוד נמצא כי נשואים ויחידים מעורבים בהתנהגויות סיכון פחות מרווקים, ומשתמשי אינטרנט כבדים וותיקים מעורבים בהתנהגויות סיכון יותר ממי שאינם משתמשים כבדים.

ממצא זה תומך בהשערה 2 באשר להבדלים במידת המעורבות בהתנהגויות סיכון במרחב הסייבר – נשים מעורבות בהתנהגויות סיכון פחות מגברים.

הקשר בין מודעות לפשעי סייבר לבין מעורבות בהתנהגויות סיכון

לוח 4 מציג תוצאות תסוגה היררכית לניבוי רמת המעורבות בהתנהגויות סיכון במרחב הסייבר. בשלב הראשון נבחן באמצעות מודל 1 את הקשר בין מודעות לפשעי סייבר לבין מעורבות בהתנהגויות סיכון בקרב כלל הנדגמים ונפקח על משתנים חברתיים־דמוגרפיים (מין, קבוצת גיל, רמת השכלה, מוצא אתני ומצב משפחתי) ועל מאפייני גלישה (תדירות הגלישה ווותק הגלישה). בשלב השני נבחן באמצעות מודל 2 את הקשר של אינטראקציה בין מין לבין מדד מתוקנן של מודעות לפשעי סייבר עם רמת המעורבות בהתנהגויות סיכון ונפקח על משתנים חברתיים־דמוגרפיים ומאפייני גלישה.

לוח 4: תסוגה היררכית לניבוי מעורבות בהתנהגויות סיכון כפונקציה של משתנים חברתיים־דמוגרפיים, מאפייני גלישה ורמת מודעות לסכנות סייבר (מודל 1) וכפונקציה של משתנים חברתיים־דמוגרפיים, מאפייני גלישה ואינטראקציה בין מין לבין רמת מודעות מתוקננת לסכנות סייבר (מודל 2)[1]

	מודל 1			מודל 2		
	B	*SE*	β	*B*	*SE*	β
(קבוע)	.694	.128**		.541	.136**	
קבוצת גיל 18–29	.476	.082	.225**	.474	.083	.224**
קבוצת גיל 30–44	.258	.054	.143**	.258	.054	.143**
קבוצת גיל 45–59	.160	.052	.090**	.159	.052	.089**
לאום־אתניות יהודי	–.032	.048	–.017	–.033	.048	–.017
13–15 שנות לימוד	.096	.052	.049	.095	.052	.048
16 שנות לימוד או יותר	.103	.046	.063*	.101	.046	.062*
מצב משפחתי נשוי	–.177	.070	–.098*	–.178	.070	–.099*
יחיד (פרוד, גרוש, אלמן)	–.192	.093	–.068*	–.193	.093	–.068*
משתמשי אינטרנט כבדים	.122	.053	.075*	.123	.053	.076*
משתמשי אינטרנט בינוניים	.018	.055	.010	.019	.055	.010
גולשי אינטרנט ותיקים	.138	.048	.072**	.139	.048	.073**
מין: אישה	–.098	.038	–.060**	–.098	.038	–.060**
מדד מודעות לסכנות סייבר	–.007	.003	–.057*	–.005	.004	–.038
אינטראקציה מין χ מדד מתוקנן (Z) של מודעות לפשעי סייבר[2]	–	–	–	–.031	.037	–.027
Adjusted R^2	.092			.093		
ΔR^2				.001		

* $p \leq .001$ *** $p \leq .01$ ** $p \leq .05$

1 כל המשתנים המנבאים, למעט מדד המודעות לסכנות סייבר, מוגדרים כמשתנים ביניריים, עם הערכים 0 ו־1. הקטגוריות להשוואה במשתנים המנבאים: במין – גבר; בקבוצות הגיל – בני 60 או יותר; בלאום־אתניות – לא יהודי; בקבוצות רמת השכלה – עד 12 שנות לימוד; בקבוצות מצב משפחתי – רווק; בקבוצות משתמשי אינטרנט – משתמשי אינטרנט קלים (פחות מפעם ביום); בגלישה באינטרנט – גולשים שאינם ותיקים (פחות מ־6 שנים).

2 התְקנון (standardization) של מדד המודעות לסכנות במרחב הסייבר בוצע כדי לצמצם את המתאמים הגבוהים בין מין לבין משתנה האינטראקציה (r = .848) ובין רמת המודעות בערך מוחלט לבין משתנה האינטראקציה (r = .428).

מלוח 4 עולה כי קיים קשר מובהק סטטיסטית בין רמת המודעות לבין רמת המעורבות בהתנהגויות סיכון ($\beta = -.057, p \leq .05$), כך שככל שרמת המודעות לפשעי סייבר גבוהה יותר, רמת המעורבות בהתנהגויות סיכון נמוכה יותר. ממצא זה תומך בהשערה 3, שלפיה יימצא קשר בין מודעות לסכנות סייבר לבין הימנעות ממעורבות בהתנהגויות סיכון במרחב הסייבר.

עוד עולה מן הממצאים כי גם כאשר כוללים במודל את רמת המודעות לפשעי סייבר, נשים מעורבות בהתנהגויות סיכון פחות מגברים. כלומר, גם כאשר לנשים ולגברים יש רמת מודעות דומה, נשים מעורבות בהתנהגויות סיכון במרחב הסייבר פחות מגברים. ממצא זה מחזק את השערה 2 בדבר הקשר בין המין לבין רמת המעורבות בהתנהגויות סיכון.

נוסף על כך, על אף הפיקוח על רמת המודעות לפשעי סייבר נמצא כי ככל שצעירים יותר, כך עולה רמת המעורבות בהתנהגויות סיכון. באשר לרמת ההשכלה, נמצא כי בעלי השכלה גבוהה (16 שנות לימוד או יותר) מעורבים יותר בהתנהגויות סיכון מבעלי השכלה נמוכה (12 שנות לימוד או פחות). כמו כן, נמצא כי נשואים ויחידים שאינם רווקים מעורבים בהתנהגויות סיכון פחות מרווקים. באשר למאפייני גלישה, נמצא כי גם כאשר פיקחנו על רמת המודעות, נמצא כי צרכני אינטרנט כבדים (שעה אחת או יותר ביום) היו מעורבים בהתנהגויות סיכון יותר ממשתמשי אינטרנט קלים (פחות מפעם ביום). ועוד, משתמשים ותיקים (6 שנים או יותר) מעורבים יותר ממשתמשים חדשים (פחות מ־6 שנים).

ממצאים אלו מנחים אותנו לצפות להשפעה (effect) של אינטראקציה בין המין לבין רמת המודעות לפשעי סייבר על רמת המעורבות בהתנהגויות סיכון, כך שהקשר בין רמת המודעות לפשעי סייבר לבין רמת המעורבות בהתנהגויות סיכון יימצא שלילי יותר בקרב נשים לעומת הקשר בקרב גברים (השערה 4). לפיכך, בשלב השני (מודל 2) חושבה רמת המעורבות בהתנהגויות סיכון כפונקציה של המין, של רמת המודעות לפשעי סייבר ושל האינטראקציה בין המין לבין משתנה המודעות המתוקנן והופעל פיקוח על מאפיינים חברתיים־דמוגרפיים נוספים ועל מאפייני גלישה. בדומה למודל 1, גם במודל זה נמצא כי נשים מעורבות בהתנהגויות סיכון פחות מגברים. עם זאת, במודל זה לא נמצא אישוש להשערה 4. למעשה, לא נמצא קשר מובהק בין משתנה האינטראקציה (בין מין לבין משתנה המודעות המתוקנן) לבין רמת המעורבות בהתנהגויות סיכון. כלומר, לא נמצא כי הקשר בין רמת המודעות לפשעי סייבר לבין רמת המעורבות בהתנהגויות סיכון הוא שלילי בקרב נשים יותר מאשר בקרב גברים. יתרה מכך, הכנסת משתנה האינטראקציה אינה תורמת לשונות המוסברת של המעורבות בהתנהגויות סיכון.

דיון

רשת התקשורת הדיגיטלית, האינטרנט, שזורה בחיי היום־יום בקרב שיעור לא מבוטל מאוכלוסיית העולם ובקרב שיעור ניכר מאוכלוסייתן של מדינות העולם המערבי, ובכללן ישראל (Internet Live Stats, 2016). אוכלוסייה זו מבצעת ברשת רבות מן הפעילויות היום־יומיות, כגון אינטראקציות חברתיות, צרכנות, תרבות פנאי ושירותי בנק (Jewkes & Yar, 2013, p. 1), וצופים כי בעשור הקרוב אף תגבר נוכחות האינטרנט בחיי המשתמש, אנשים יבלו זמן רב יותר במרחב הסייבר ויבצעו מגוון רחב יותר של פעילויות מקוונות (Pew Internet, 2014). לצד היתרונות הגלומים בתלות החברתית בטכנולוגיה, משתמשי האינטרנט חשופים למגוון רחב של סכנות, ובכללן סכנות המוגדרות במהותן כפשעי סייבר (Jewkes & Yar, 2013, pp. 1-2; Newman & Clarke, 2013, pp. 10-13).

למחקר זה היו שתי מטרות: להוסיף לידע על אודות הקשר בין תפיסות במרחב הסייבר לבין דפוסי התנהגות בו, ולבחון אם לקשר בין תפיסות לבין דפוסי התנהגות יש הקשר מגדרי.

ממצאי המחקר מצביעים על קשר מובהק סטטיסטית בין המין לבין רמת המודעות לפשעי סייבר ולבין מידת המעורבות בהתנהגויות סיכון במרחב הסייבר. בהתאם להשערת המחקר הראשונה, נמצא כי נשים מודעות לפשעי סייבר יותר מגברים, וממצא זה תקף גם כאשר מפקחים על משתנים חברתיים־דמוגרפיים (גיל, רמת השכלה, מוצא אתני ומצב משפחתי) ועל מאפייני גלישה. ממצא זה עולה בקנה אחד עם הידוע בספרות מן המרחב הפיזי על אודות הבדלי מגדר בתפיסות הנוגעות לאיום הקורבנות (May et al., 2010). נשים נוטות לבטא תפיסת איום גבוהה יותר מגברים, בייחוד בנוגע לעברות המאיימות על הביטחון הפיזי או לעברות שיש בהן סכנה לאלימות פיזית, כגון פריצה לבית (Schafer et al., 2006). הספרות מציעה כמה הסברים לנטייתן של נשים לבטא תפיסת איום גבוהה יותר, ובהם הפנמה של מודעות לסכנות המועברת מאימהות לבנותיהן בתהליכי החִברות (May et al., 2010) ותחושת הפגיעות הפיזית המלווה נשים (Killias & Clerici, 2000) ומתמקדת בתופעה המכונה "צְלה של התקיפה המינית" (Ferraro, 1996). נשים חוששות להיות קורבן לתקיפה מינית, וחשש זה מופנה גם כלפי עברות אחרות, שאינן כרוכות בתקיפה מינית (Ferraro, 1996; May et al., 2010). מאחר שההתנהגות במרחב הסייבר אינה מצריכה מפגש פנים אל פנים בין תוקף לבין משתמש שהוא קורבן פוטנציאלי ומאחר שהמשתמש מוגן מאחורי צג המחשב, יכולנו לכאורה לצפות שמרחב הסייבר יטשטש הבדלים בין המינים ברמת המודעות לסכנות. למרות זאת, ועל יסוד תימוכין מחקריים לתופעת "צלה של התקיפה המינית", שיערנו, ואף אישששנו את ההשערה, שנשים יבטאו מודעות רבה יותר לפשיעת סייבר. נראה שתחושת הפגיעות, המלווה נשים במרחב הפיזי ומביאה אותן לכדי חשש מקורבנות ולתפיסת

סיכון גבוהה בהקשר לעברות שונות, באה לידי ביטוי גם בהבדלים בין גברים לבין נשים ברמת המודעות לסכנות במרחב הסייבר.

גם להשערת המחקר השנייה נמצא אישוש. נשים מעורבות בהתנהגויות סיכון במרחב הסייבר פחות מגברים. העובדה כי גברים מעורבים בהתנהגויות סיכון יותר מנשים נתמכת בממצאי מחקרים דומים מן המרחב הפיזי. הסבר מרכזי לנטייתם של גברים להיות מעורבים בהתנהגויות סיכון החושפות לקורבנות נשען על **תאוריית השליטה העצמית הנמוכה** (Gottfredson & Hirschi, 1990). גברים נוטים להיות בעלי שליטה עצמית נמוכה המתאפיינת בנטייה לחיפוש ריגושים, בדחף לסיפוק צרכים מיָדי, בתגובתיות נמהרת (impulsivity) ובקושי להתמודד עם תסכולים, ולפיכך הם מעורבים יותר מנשים בהתנהגויות סיכון החושפות אותם לקורבנות (Schreck, Stewart, & Fisher, 2006). נציין כי בכל הנוגע למרחב הסייבר, מעטים המחקרים שבחנו אם מעורבות בהתנהגויות סיכון קשורה לשליטה עצמית נמוכה ולמאפיינים חברתיים־דמוגרפיים של משתמש האינטרנט ובכללם למין הביולוגי, והמחקרים הקיימים מתקשים לספק הוכחות חד־משמעיות לקשר זה (ראו, לדוגמה, Bossler & Holt, 2009; Holtfreter, Reisig, & Pratt, 2008). במחקר המשך נמליץ לבחון סוגיה זו מתוך התמקדות בהבדלי מגדר בנוגע לקשר בין שליטה עצמית נמוכה לבין מעורבות בהתנהגויות סיכון במרחב הסייבר.

השערת המחקר השלישית והשערת המחקר הרביעית עוסקות בקשר בין רמת המודעות לבין התנהגות במרחב הסייבר. נושא זה הוא בעל חשיבות רבה הן מן הבחינה התאורטית והן מן הבחינה המעשית. כמצוין בגוף מחקר זה, חוקרים מתחומי דעת מגוונים, ובכלל זה קרימינולוגים וחוקרים מתחום מדעי המחשב ומערכות מידע, מדגישים את חשיבותה של העלאת רמת המודעות החברתית לפשעי סייבר לשם הקטנת מידת המעורבות בהתנהגויות סיכון. לפי ממצאיו של מחקר זה, קיים קשר מובהק סטטיסטית בין מודעות גבוהה לפשעי סייבר לבין מעורבות נמוכה בהתנהגויות סיכון, וממצא זה מאשש את ההשערה השלישית. לממצא זה חשיבות רבה מאחר שמחקרים קודמים טענו להעדר קשר בין המשתנים האמורים (Acquisti & Grossklag, 2003; Berendt, Gunther, & Spiekermann, 2005). אפשר שההבדל בין מחקרנו לבין ממצאי מחקרים קודמים טמון במגוון ההתנהגויות שמחקרנו עסק בהן. מחקרים קודמים התמקדו במודעות ובמעורבות בהתנהגויות סיכון החושפות את המשתמש להונאת צרכנים (ראו, לדוגמה, Davinson & Sillence, 2010), ואילו מחקרנו בחן קשת רחבה יותר של התנהגויות החושפות אותו לתוכנות זדוניות, לגנבת זהות ולהונאה. ממצא זה נותן תוקף להמלצותיהם של חוקרים בדבר החשיבות בהעלאת רמת המודעות החברתית לפשעי סייבר.

במחקר זה לא נמצא אישוש להשערה הרביעית, שעניינה תרומת האינטראקציה בין המין לבין רמת המודעות לפשעי סייבר להסבר השונות במעורבות בהתנהגויות סיכון. לפי השערה זו, הקשר בין רמת המודעות לפשעי סייבר לבין מידת המעורבות בהתנהגויות סיכון בקרב נשים יימצא שלילי יותר מאשר בקרב גברים. למעשה, בלי קשר לרמת מודעותן, נשים מעורבות בהתנהגויות סיכון פחות מגברים. ממצא זה מצביע

כנראה על הבדלים מובְנים (אינהרנטיים) בין גברים לבין נשים בדפוסי המעורבות בהתנהגויות סיכון במרחב הסייבר. לפיכך, מומלץ שמחקר בעתיד יבחן גורמים נוספים העשויים להצביע על קשר כזה, לדוגמה האינטראקציה בין המין לבין ממדי תפיסה נוספים (פחד מפשיעה ותפיסת סיכון) לבין מידת המעורבות בהתנהגויות סיכון. משתנה נוסף העשוי להשפיע על הקשר האמור הוא היחס בין תפיסות סיכון עצמי לבין תפיסות סיכון של האחר. זו השערת ההטיה האופטימיסטית (Weinstein & Klein, 1996), סוגיה שלמיטב ידיעתנו נבחנה בעולם הסייבר רק במחקר אחד (Campbell, Greenauer, Macaluso, & End, 2007), ואנו סבורים כי יש טעם להעמיק בה כדי להבין את הקשר בין מנגנון התפיסה של המשתמש לבין מעורבותו בהתנהגויות סיכון החושפות אותו לקורבנות.

נראה אפוא כי חרף ההבדלים המבניים בין המרחב הווירטואלי לבין המרחב הפיזי, ובייחוד העדר מגע פיזי בין התוקף לבין הקורבן והאנונימיות של שניהם (Jaishankar, 2007; Yar, 2005), ממצאי מחקר זה תומכים בתפיסתו של קסטלס כי מרחב הסייבר אינו מציאות וירטואלית (virtual reality), אלא וירטואליות אמתית (real virtuallity) (Castells, 2001, p. 203). במילים אחרות, מרחב הסייבר הוא מרחב טכנולוגי־חברתי, ששורשיו נעוצים במבנה הכלכלי, החברתי, הפוליטי והתרבותי המאפיין את המרחב הפיזי. ניתן אפוא להקיש ממחקר זה כי אפשר לבחון את תופעת הפשיעה והקורבנות במרחב הסייבר בכלים תאורטיים המוכרים מן הסביבה הפיזית.

מחקר זה תורם להבנת התגובה החברתית לפשעי סייבר כפי שהיא באה לידי ביטוי ברמת המודעות ובמידת המעורבות בהתנהגויות סיכון במרחב הסייבר בקרב האוכלוסייה הבוגרת של משתמשי האינטרנט בישראל. יתרה מכך, המחקר עומד על הבדלים בין המינים בנוגע למשתנים אלו, סוגיה המעסיקה רבים מן המחקרים במרחב הפיזי, אך נעדרה עד כה מן העיסוק המחקרי במרחב הווירטואלי. יתרה מכך, מחקר זה מעיד על אופיו של הקשר בין מודעות לסכנות לבין מעורבות בהתנהגויות סיכון במרחב הסייבר, וממצאיו עשויים לשמש לפיתוחן של תכניות חברתיות להתמודדות עם איומי הסייבר, תכניות המיועדות לכלל צרכני האינטרנט הפרטיים ובפרט לקבוצות חברתיות מובחנות.

ראוי להדגיש כי מחקר זה מתבסס על דיווח סובייקטיבי של מרואיינים, כך שקרוב לוודאי שקיימות בו הטיות העלולות להשפיע על ממצאיו, כגון תעתועי זיכרון ורצייה חברתית. אם כן, במחקרי המשך מומלץ לבחון את מידת ההלימה בין הדיווח הסובייקטיבי של המרואיין בנוגע למעורבותו בהתנהגויות שונות לבין דפוסי התנהגות בפועל על בסיס נתוני גלישה במרחב הסייבר המופיעים במסדי נתונים אינטרנטיים (URL). נוסף על כך, במחקרי המשך נמליץ לעמוד על הסברים העשויים לעמוד בבסיס האינטראקציה בין המין לבין משתנים חברתיים־דמוגרפיים אחרים (גיל ורמת השכלה) בנוגע לקשר בין מודעות לפשעי סייבר לבין מעורבות בהתנהגויות סיכון במרחב זה. כמו כן, נמליץ לבחון מאפיינים סביבתיים, מבניים, העשויים לעצב את התפיסות בנוגע לקורבנות במרחב הסייבר (דפוסי פעילות יום־יומיים), סוגיה שמחקרים העוסקים בחקר תפיסות

האיום מקורבנות במרחב הפיזי מרבים לעסוק בה (Hipp, 2010; Rountree & Land, 1996).

לבסוף, ממצאי המחקר מאירים הבדלים בקשר בין רמת המודעות לפשעי סייבר לבין מידת המעורבות בהתנהגויות סיכון במרחב זה בקרב קבוצות חברתיות־דמוגרפיות שונות. במחקר המשך נמליץ לעמוד על מהותם של הבדלים אלו.

מקורות

הלשכה המרכזית לסטטיסטיקה (2014). הסקר החברתי: בני 20 ומעלה לפי השימוש במחשבים ואינטרנט ולפי תכונות נבחרות. שנתון סטטיסטי לישראל מס׳ 65. ירושלים: המחבר.

מש, ג׳ ותלמוד, א׳ (2007, 6 במאי). הבדלים תרבותיים בנגישות לטכנולוגיות תקשורת ובשימוש בהן: מתבגרים יהודים וערבים בישראל. המגזין. אוחזר מתוך https://www.isoc.org.il

Acquisti, A., & Grossklags, J. (2003, May). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *2nd Annual Workshop on Economics and Information Security – WEIS* (Vol. 3, pp. 1-27).

Allison, S. F., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice, 33*(1), 19-29.

Beck, U. (1992). *Risk society: Towards a new modernity*. London, England: Sage.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM, 48*(4), 101-106.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011, November). Measuring the human factor of cyber security. *International Conference on Technologies for Homeland Security – HST* (pp. 230-235).

Brenner, S. W. (2007). Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (Ed.), *Crime online* (pp. 12-28). Milton, England: Willan.

Broadhurst, R., & Choo, K. K. R. (2011). *Cybercrime and online safety in cyberspace.* In C. Smith, S. Zhang, & R. Barbaret (Eds.), *International handbook of criminology* (pp. 153-165). New York, NY: Routledge.

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior, 23*(3), 1273-1284.

Castells, M. (2001). *The internet galaxy: Reflections on the internet, business, and society*. Oxford, England: Oxford University Press.

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987-995.

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Clough, J. (2010). *Principles of cybercrime*. Cambridge, England: Cambridge University Press.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588-608.

Copes, H., Kerley, K. R., Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice, 38*, 1045-1052.

Cops, D., & Pleysier, S. (2011). 'Doing gender' in fear of crime: The impact of gender identity on reported levels of fear of crime in adolescents and young adults. *British Journal of Criminology, 51*(1), 58-74.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior, 26*(6), 1739-1747.

Farrall, S., & Gadd, D. (2004). Research note the frequency of the fear of crime. *British Journal of Criminology, 44*(1), 127-132.

Ferraro, K. F. (1995). *Fear of crime: Interpreting victimization risk*. New York, NY: SUNY.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: Threats and solutions. *IEEE Communications Surveys & Tutorials, 16*(4), 2019-2036.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal internet users. *Computers & Security, 26*(5), 410-417.

Furnell, S., J., Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security, 25*(1), 27-35.

Gatewood Owens, J. (2015, November). A gender-biased definition: Unintended impacts of the fear requirement in stalking victimization. *Crime & Delinquency, 63*(11), 1339-1362.

Gilchrist, E., Bannister, J., Ditton, J., & Farrall, S. (1998). Women and the 'fear of crime' challenging the accepted stereotype. *British Journal of Criminology, 38*(2), 283-298.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Grabosky, P. N., Smith, R. G., & Dempsey, G. (2001). *Electronic theft: Unlawful acquisition in cyberspace*. Cambridge, MA: Cambridge University Press.

Hargittai, E., & Shafer, S. (2006). Differences in actual and perceived online skills: The role of gender. *Social Science Quarterly, 87*(2), 432-448.

Higgins, G. E. (2007). Digital piracy, self-control theory, and rational choice: An examination of the role of value. *International Journal of Cyber Criminology, 1*(1), 33-55.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

Hinduja, S. (2001). Correlates of internet software piracy. *Journal of Contemporary Criminal Justice, 17*(4), 369-382.

Hipp, J. R. (2010). Resident perceptions of crime and disorder: How much is "bias", and how much is social environment differences? *Criminology, 48*(2), 475-508.

Hirtenlehner, H., & Farrall, S. (2014). Is the 'Shadow of Sexual Assault' responsible for women's higher fear of burglary? *British Journal of Criminology, 54*(6), 1167-1185.

Hollway, W., & Jefferson, T. (1997). The risk society in an age of anxiety: Situating fear of crime. *British Journal of Sociology, 48*(2), 255-266.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40.

Holt, T. J., & Turner, M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior, 33*(4), 308-323.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*(1), 189-220.

Internet Live Stats (2016). Internet users by country, 2016. Retrieved from http://www.internetlivestats.com/internet-users-by-country

Jackson, J., Allum, N., & Gaskell, G. (2005). Perceptions of risk in cyberspace. In R. Mansell & B. S. Collins (Eds.), *Trust and crime in information societies* (pp. 245-281). Cheltenham, England: Edward Elgar.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. *International Journal of Cyber Criminology, 1*(2), 7-9.

Jewkes, Y., & Yar, M. (Eds.). (2013). *Handbook of internet crime*. Milton, England: Routledge.

Killias, M., & Clerici, C. (2000). Different measures of vulnerability in their relation to different dimensions of fear of crime. *British Journal of Criminology, 40*(3), 437-450.

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the internet: Attacks, costs and responses. *Information Systems, 36*(3), 675-705.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847.

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems, 46*(1), 254-264.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM, 51*(3), 71-76.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Livingstone, S., & Helsper, E. J. (2007). Taking risks when communicating on the internet: The role of offline social-psychological factors in young people's vulnerability to online risks. *Information, Communication & Society, 10*(5), 619-644.

May, D. C., Rader, N. E., & Goodrum, S. (2010). A gendered assessment of the "threat of victimization": Examining gender differences in fear of crime, perceived risk, avoidance, and defensive behaviors. *Criminal Justice Review, 35*(2), 159-182.

McQuade, S. C. (2006). *Understanding and managing cybercrime*. Boston, MA: Pearson/Allyn & Bacon.

Mesch, G. S. (2000). Perceptions of risk, lifestyle activities, and fear of crime. *Deviant Behavior, 21*(1), 47-62.

Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *CyberPsychology & Behavior, 12*(4), 387-393.

Miethe, T. D. (1995). Fear and withdrawal from urban life. *The Annals of the American Academy of Political and Social Science, 539*(1), 14-27.

Miethe, T. D., Stafford, M. C., & Long, J. S. (1987). Social differentiation in criminal victimization: A test of routine activities/lifestyle theories. *American Sociological Review, 52*(2), 184-194.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. Indianapolis, IN: John Wiley & Sons.

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum, 32*(1), 81-94.

Newman, G. R. (2009). Cybercrime. In M. D. Krohn, A. J. Lizotte, & G. P. Hall (Eds.), *Handbook on crime and deviance* (pp. 551-584). New York, NY: Springer.

Newman, G. R., & Clarke, R. V. (2013). *Superhighway robbery*. Portland, OR: Willan.

Ngo, T. N., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773-793.

Pantazis, C. (2000). 'Fear of Crime', vulnerability and poverty. *British Journal of Criminology, 40*(3), 414-436.

Pew Internet (2014). Internet users by country, 2016. Digital life in 2025. Retrieved from http://www.pewinternet.org

Pontell, H. (2002, October 29). *Pleased to meet you... won't you guess my name? Reducing identity fraud in the Australian tax system*. Paper presented at the Centre for Tax System Integrity, The Australian National University, [location]. Retrieved from https://openresearch-repository.anu.edu.au

Popp, A. M., & Peguero, A. A. (2011). Routine activities and victimization at school: The significance of gender. *Journal of Interpersonal Violence, 26*(12), 2413-2436.

Pratt, T. C., Holtfreter. K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generally of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 268-296.

Rader, N. E., Cossman, J. S., & Allison, M. (2009). Considering the gendered nature of constrained behavior practices: Among male and female college students. *Journal of Contemporary Criminal Justice, 25*(3), 282-299.

Rader, N. E., May, D. C., & Goodrum, S. (2007). An empirical assessment of the "threat of victimization": Considering fear of crime, perceived risk, avoidance, and defensive behaviors. *Sociological Spectrum, 27*(5), 475-505.

Reisig, M.D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior, 36*(4), 369-384.

Rengifo, A. F., & Bolton, A. (2012). Routine activities and fear of crime: Specifying individual-level mechanisms. *European Journal of Criminology, 9*(2), 99-119.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*, 216-238.

Robinson, J. P., DiMaggio, P., & Hargittai, E. (2003). New social survey perspectives on the digital divide. *IT & Society, 1*(5), 1-22.

Rountree, P. W., & Land, K. C. (1996). Perceived risk versus fear of crime: Empirical evidence of conceptually distinct reactions in survey data. *Social Forces, 74*(4), 1353-1376.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Savona, E. U., & Mignone, M. (2004). The fox and the hunters: How IC technologies change the crime race. *European Journal on Criminal Policy and Research, 10*(1), 3-26.

Schafer, J. A., Huebner, B. M., & Bynum, T. S. (2006). Fear of crime and criminal victimization: Gender-based contrasts. *Journal of Criminal Justice, 34*(3), 285-301.

Schreck, C. J., Stewart, E. A., & Fisher, B. S. (2006). Self-control, victimization, and their influence on risky lifestyles: A longitudinal analysis using panel data. *Journal of Quantitative Criminology, 22*(4), 319-340.

Spano, R., & Freilich, J. D. (2009). An assessment of the empirical validity and conceptualization of individual level multivariate studies of lifestyle/routine activities theory published from 1995 to 2005. *Journal of Criminal Justice, 37*(3), 305-314.

Staksrud, E., & Livingstone, S. (2009). Children and online risk: Powerless victims or resourceful participants? *Information, Communication & Society, 12*(3), 364-387.

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality, 4*(2), 7-41.

Sullins, L. L. (2006). Phishing for a solution: Domestic and international approaches to decreasing online identity theft. *Emory International Law Review, 20*(1), 397-433.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254-268.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586.

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research, 8*(2), 183-205.

Wall, D. S. (2008). *Cybercrime: The transformation of crime in the information age*. Cambridge, MA: Polity.

Wall, D. S. (2010). Criminalising cyberspace: The rise of the internet as a crime problem. In Y. Jewkes & M. Yar (Eds.), *Handbook of internet crime* (pp. 88-102). Milton, England: Willan.

Warr, M. (1993). Fear of victimization. *Public Perspective, 5*, 25-28.

Warr, M. (2000). Fear of crime in the United States: Avenues for research and policy. *Criminal Justice, 4*(4), 451-489.

Weinstein, N. D., & Klein, W. M. (1996). Unrealistic optimism: Present and future. *Journal of Social and Clinical Psychology, 15*(1), 1-8.

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.

Yar, M. (2013). *Cybercrime and society*. Thousand Oaks, CA: Sage.

Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006). Examining characteristics and associated distress related to internet harassment: Findings from the Second Youth Internet Safety Survey. *Pediatrics, 118*(4), e1169-e1177.