התייחסות מורים ותלמידים לאבטחת מידע - מחקר איכותני

תקציר

מטרת המחקר היא לבחון את יחסם של בני הנוער וצוותי החינוך לסוגית אבטחת המידע. המחקר התמקד בבני נוער בגילאי 15-18 ובצוותי החינוך מבתי ספר שונים ברחבי הארץ המשתייכים לאוכלוסיות מגוונות מבחינה סוציו-אקונומית וחברתית. שיטת המחקר שנבחרה היא שיטת המחקר האיכותנית. הנתונים האיכותניים נאספו באמצעות קבוצות מיקוד (Focus Groups). שיטה זו נבחרה כיוון שבאווירה של דינאמיקה קבוצתית פתוחה ובטוחה עולים רעיונות, דעות, רגשות, מעשים ומחשבות שמהם ניתן לשחזר דפוסי פעולה ואת המניעים להם. בנוסף, היות שהתוצאה המעשית הרצויה של מחקר זה היא להביא בסופו של תהליך לשינוי תרבותי בנושא אבטחת המידע, חשוב להבין את המניעים להתנהגותם של משתמשי הקצה. ממצאי המחקר הראו קשר ברור בין הערכת משאבי הידע של המורים והתלמידים לבין תחושת האיום שהם חשים כלפי הסיכונים למידע ומתוך כך למוכנותם לאבטח את המידע שברשותם. בנוסף עלה הצורך לעודד את שילובו של נושא אבטחת המידע בתוכנית הלימודים כחלק מהמיומנויות הנדרשות במאה ה-21.

מילות מפתח

התנהגות אבטחת מידע, אחריות אישית לאבטחת מידע, מניעים וגורמים לאבטחת מידע, מודעות לאבטחת המידע, כלים לאבטחת המידע

מבוא

מודעות לאבטחת המידע האינטרנטי מבוססת על היכרות עם הסכנות האורבות ברשת, ביניהן פריצות, תקשורת לא רצויה, וירוסים ותוכנות ריגול. מודעות זו גם כוללת היכרות עם התנהגויות שיכולות לגרום להתפשטות של תוכנות זדוניות ולרמייה ברשת – התחזות, דיוג, וזיוף.

בסקר שערך מרכז Pew Research (Olmstead & Smith, 2017) בארצות הברית, דיווחו 64% מהנשאלים – מבוגרים (גברים ונשים) מעל גיל 18, כי יש להם חשבון מקוון וכי פרטיהם האישיים ביותר – מידע רפואי, נתוני חשבונות בנק ונתונים רגישים אחרים – נמצאים באינטרנט. במקביל, 65% הודו כי חוו תקיפה של מידע אישי וכי אין להם אמון במוסדות השונים וברשתות החברתיות שיגנו על המידע האישי שלהם מפני גורמים עוינים שישתמשו בהם לרעה. אף שכמחצית מהנשאלים סברו שהנתונים האישיים פחות בטוחים בשנים האחרונות, הם גם הודו שלא תמיד הם משתמשים בשיטות המומלצות לאבטחת המידע בחייהם הדיגיטליים. מהסקר עולה גם כי משתמשי הקצה לא תמיד ערניים לצורך באבטחה למכשירים הניידים – 28% מבעלי הטלפונים החכמים מדווחים שהם אינם משתמשים בנעילת מסך או בתכונות אבטחה אחרות לשמירה על המידע בטלפון האישי שלהם. כמו כן, הם אינם מתקינים עדכונים ליישומונים או למערכת

ההפעלה של הטלפון החכם שלהם, וכמחציתם מדווחים כי הם משתמשים ברשתות ווי-פי ציבוריות לא מאובטחות. כלומר, חרף דאגותיהם וחוויותיהם האישיות, רוב הנשאלים – 69%, אפילו נשאלים שחוו באופן אישי פריצה לנתונים האישים – לא נוקטים אמצעי אבטחה מספיקים כדי לאבטח את הסיסמאות האישיות שלהם.

תוכניות המעודדות הגברת מודעות לאבטחת המידע הפכו להיות רכיבי מפתח בניהול אבטחת מידע ארגוני (Tsohou et al, 2015). תוכניות אלה חשובות מאוד כאשר מדברים על אוכלוסיית המורים, המשמשים כמעצבי התנהגות הבטיחות המקוונת של מתבגרים, ושל התלמידים – דור שגדל לתוך הכאוס של עולם בעיות הבטיחות המקוונות. כדי שתרבות אבטחת המידע תהפוך לטבע שני של האדם יש צורך בשינוי תרבותי, שיכול להתבצע רק באמצעות חינוך והכשרה (Chou, H. & Sun, 2017).

מכל האמור לעיל עלה הצורך במחקר הבוחן את יחסם של הנשאלים לסוגית אבטחת המידע. במסגרת מחקר זה בחרנו להתמקד באוכלוסיית התלמידים בגיל בית הספר תיכון ובצוותי החינוך שתפקידם למלא תפקיד חיוני בעיצוב התנהגות הבטיחות המקוונת של המתבגרים.

סקירת ספרות

אבטחת מידע בקרב בני הנוער

טכנולוגיות המידע והתקשורת הן חלק בלתי נפרד מעולמם של בני הנוער. התקשורת, צורת ההתבטאות, הייצוג והעברת המידע שונים לחלוטין מהמקובל בדורות הקודמים, וכך גם הרגלי ההבעה, הלמידה ואחזור המידע (Yılmaz et al., 2017). הלמידה מתבצעת היום לא רק בין כותלי הכיתה אלא גם באמצעות אתרי אינטרנט בית-ספריים, דואר אלקטרוני ורשתות חברתיות כגון פייסבוק (Facebook), אינסטגראם (Instagram) ווטסאפ (WhatsApp). כתוצאה מכך התלמידים נחשפים לאיומים רבים ברשת האינטרנט וגובר הצורך באבטחת מידע (Defranco, 2011).

אנו שבויים בתפיסה מוטעית שלפיה בני הנוער, בהיותם "ילידים" בעולם הדיגיטלי ולא "מהגרים" כהוריהם וכמוריהם (Prensky, 2001) יודעים לשמור על עצמם במרחבי הסייבר. בפועל, מתברר שעל אף שבני הנוער בקיאים יותר בשימוש בבלוגים, ברשתות חברתיות, בהורדת תכנים וכדומה, הם אינם מודעים דיים לנושא אבטחת המידע באינטרנט (Purkait & Das, 2017). צעירים נוטים לחשוף פרטים על עצמם יותר מאשר מבוגרים (Aharony, 2014, 2016), ולכן חינוך לאבטחת מידע הופך להיות אמצעי זהירות הכרחי עבור כל משתמשי הקצה. על פי דוח מקאפי (McAfee Labs, 2010), בעוד שכמעט כל בני הנוער טענו כי הם יודעים איך לשמור על בטיחותם

באינטרנט, למעשה כמחציתם מסרו מידע אישי לגורם שאינם מכירים, ויותר מרבע מבני הנוער בארה״ב אפשרו למחשב בביתם להידבק בווירוס. במחקר מאוחר יותר נמצא שלא חלו שינויים בהתנהגות בני הנוער (McAfee Labs, 2014). יתר על כן, במחקר PRACTIS (Privacy Appraising Challenges to Technologies and Ethics) שערך האיחוד האירופאי נמצא שבני נוער בגילאי תיכון מוכנים לוותר על מרכיבי פרטיות באינטרנט תמורת ההטבות שמספקת להם הסביבה הדיגיטלית (Ahituv et al., 2014).

דוגמה לאיום על אבטחת המידע בתקשורת המקוונת היא הפריצות לסיסמאות של משתמשי הקצה. במחקר משותף של המחלקה ללמידה ולתקשורת באוניברסיטת ליסטר באנגליה ושל המחלקה למדעי המחשב באוניברסיטת אוקספורד, אנגליה, מצאו וויטי ושותפיה (Whitty et al., 2015) כי צעירים נוטים לשתף את הסיסמה שלהם עם אחרים יותר ממבוגרים. למעלה מ 70% מבני הנוער משתפים את סיסמת הרשת החברתית שלהם עם חבריהם (Interdisciplinary Center for Iechnological Analysis and Forecasting, 2013). גם ולקי ושותפיו (Velki et al., 2017) מצאו שמרבית תלמידי התיכון מעידים כי הם חושפים את סיסמת הגישה שלהם למערכת הדואר האלקטרוני. בניסיון להתחקות אחר הגורם שמניע את בני הנוער לשתף את הסיסמה שלהם עם גורמים אחרים, הסיקו לי וקוזר (Lee & Kozar, 2005) שלנורמה החברתית יש משקל רב בהתנהגות האבטחה של האנשים, ואלה שאינם חושפים את הסיסמאות שלהם יכולים להיראות פרנואידים, ״חנונים״ או לא חברותיים (Lee. & Kozar, 2005). בנוסף, צעירים רבים אינם מודעים לסוגים הרבים של איומים מקוונים ולדרכים שבהן ניתן לגנוב סיסמה גם אם היא לא נחשפה. פועל יוצא מחוסר מודעות זו הוא קביעת סיסמאות חלשות, שמירת הסיסמאות במקומות לא מאובטחים ואי-הקפדה על ההנחיות הבסיסיות לשמירה על הסיסמאות (Purkait & Das, 2017). אל-ג׳רבי וג׳אלי (Al-Jerbie & Jali, 2014) הצביעו במחקרן על כך שגם תלמידי בית ספר תיכון בעלי רמת מודעות מקובלת לבעיות הקשורות לאבטחת מידע אינם מיישמים את הידע בפועל. בנוסף, בני הנוער הראו פחות מודעות לסיכונים הכרוכים בהזמנת זרים ובקבלתם כ״חברים״ ביחס למבוגרים (Al-Jerbie & Jali, 2014). מסקר שערכו צ׳אי ושותפיו (Chai et al., 2006) עולה כי החשיבות שמייחסים התלמידים לנושא אבטחת המידע משחקת תפקיד קריטי בהשפעה על התנהלותם בפועל.

מקומם של המורים בחינוך התלמידים לאבטחת מידע

מצופה מהמורים, בעלי הניסיון בהוראה בכלל ובהוראת נושאים הקשורים לבטיחות בפרט, להיות אנשי המפתח שיעזרו לדור הצעיר להתמודד עם הסכנות האורבות לפתחם בשימוש

באינטרנט (O'Keeffe & Clarke-Pearson, 2011). עם זאת, מוסדות החינוך לא מיהרו להכיר באחריותם לחנך את קהל היעד שלהם לשמירה על בטיחות וללמדו על האבטחה הקיברנטית. המורים והמחנכים אינם רואים עצמם אחראיים ללמד את תלמידיהם על אודות אבטחת מידע וטוענים שאחריות זו מוטלת על ההורים, על בני המשפחה או על המחלקה לטכנולוגית המידע במוסדות החינוך (Moreno et al., 2013).

בישראל, בהתאם לחוזר מנכ"ל "אתיקה ומוגנות ברשת" (משרד החינוך, 2011), מקדם משרד החינוך את התוכנית "חיים ברשת" שמטרתה ליצור אקלים בטוח ולמנוע אלימות מקוונת בקרב תלמידים בכל שכבות הגיל ומכל המגזרים. אף שהתוכנית מיועדת לכל באי בית הספר – תלמידים, מורים והורים – מרבית המורים אינם מתייחסים לנושא אבטחת המידע במסגרת הלימודים. במקרה הטוב הם משוחחים עם תלמידיהם על גניבה ספרותית או בריונות ברשת (Pusey & Sadera, 2012), נושאים חשובים לכשעצמם אלא שהם רק חלק מהנושאים הרבים שעמם צריכים הילדים להתמודד (Lenhart, 2010).

במסגרת מחקר שערכו קרנמר וסלווין (Cranmer &Selwyn, 2009) קראו החוקרים לשלב את נושא אבטחת המידע בתוכניות הלימודים כדי לבנות את יכולתו של התלמיד להשתמש בטכנולוגית האינטרנט באופן בטוח יותר. אולם פוסי וסדרה (Pusey & Sadera, 2012) טענו כי רמת הידע הנוכחי הנמוכה של המורים בנושא אבטחת המידע ורמת הביטחון הירודה שלהם בלמדם נושאים אלה לא מאפשרות לשלב אותם בהוראת אבטחת המידע בבתי הספר.

פוסי וסדרה (Pusey & Sadera, 2012) הוסיפו שלמורים ולמחנכים יש היסטוריה ארוכה של הקניית ערכים ונושאים חשובים בתחומי הבטיחות והביטחון, המשפיעים על תלמידים מחוץ לכיתה. בדיוק כפי שהם נרתמים לחינוך הילדים והנוער לשמירה על בטיחותם ברחוב או להתרחקות מזרים, באחריותם ללמד את התלמידים כיצד להגן על עצמם בעולם הדיגיטלי. האבטחה הקיברנטית לעולם לא תהפוך לטבע שני אצל הילדים ללא התערבות של המורים והמחנכים בבתי הספר. לשם כך על המורים לרכוש את הידע והמיומנויות של אבטחת המידע ולהגן תחילה על עצמם ועל הנתונים שלהם. על המכללות להכשרת מורים להכשיר את המורים להוראת הנושאים הקשורים באבטחת מידע. עליהן לכלול מידע טכני זה בתוכניות הלימודים, כדי לסייע למורים להשתלב בתוכנית אבטחת מידע כחלק מההוראה שלהם. יש צורך ביצירת מודלים להוראת הנושא כדי לסייע לתלמידים של היום להתגבר על הסכנות שאתן הם מתמודדים בתוך הכיתה ומחוצה לה וכדי שהדורות הבאים יידעו כיצד לשמור על עצמם בטוחים ומאובטחים באינטרנט (Pusey & Sadera, 2012). אנטונסי ושותפיה (Antonaci et al., 2017) הסכימו שניתן להכשיר את המורים להעברת ידע ואסטרטגיות כיצד להפחית סיכונים מקוונים, אלא שבפועל

הכשרה זו יוצרת קושי גדול בהתחשב בסדרי היום (האג'נדות) השונים של קהלי היעד Chou, C. & Peng, 2011). מתברר שהשגת קונצנזוס לגבי ההיבטים שיש ללמד בבית הספר ודרכי התאמתם לשכבות הגיל השונות היא משימה מאתגרת (Moreno et al., 2013).

התלמידים של היום זקוקים למורים שיקנו להם את מושגי הבטיחות המקוונת, מורים שמודעים לנושא אבטחת המידע, מבינים ויודעים איך להשתמש בטכנולוגיה בכיתה ומסוגלים לנהל עם תלמידיהם דיונים קבוצתיים ומחוברים ליישומים בעולם ה"אמיתי" (Shillair & Meng, 2017). אולם, מכיוון שהמורים בעצמם אינם יודעים הרבה על אבטחת מידע, נאלצים בני הנוער להסתמך על המדיה התקשורתית ועל חברים שיספקו להם את המידע הנדרש. חוסר הזהירות של בני הנוער וחוסר היכולת של צוותי ההוראה ללמד את נושא אבטחת המידע חוברים ליצירת בעיה גדולה (Defranco, 2011).

בהתבסס על הנאמר עד כה, שאלות המחקר תהיינה:

מה יחסם של המורים והתלמידים לסוגיית אבטחת המידע?

מה גורם או יגרום לנשאלים לאבטח את המידע שלהם?

שיטה

אוכלוסיית המחקר

אוכלוסיית המחקר כללה שש קבוצות מיקוד שבהן 70 משתתפים מאזורים שונים בישראל. ארבע קבוצות מיקוד של תלמידים: קבוצה מבית ספר בדרום שמנתה 12 תלמידי כיתות י'; קבוצה מבית ספר בצפון שמנתה 14 תלמידי כיתות י"א ו-י"ב; קבוצה מבית ספר לבנות במרכז הארץ שמנתה 9 תלמידות כיתות י' ו-י"ב וקבוצה מבית ספר לבנים במרכז הארץ שמנתה 12 תלמידי כיתות ט' עד י"ב. פרט לקבוצה הראשונה (מהדרום) בה כל התלמידים למדו במגמת מדעי המחשב, התלמידים בשאר הקבוצות למדו במגמות שונות. איתור קבוצות המיקוד כלל קבלת אישור מוועדת האתיקה של האוניברסיטה ומהמדען הראשי של משרד החינוך לקיום קבוצות המיקוד. בנוסף גובשו שתי קבוצות מיקוד של מורים: קבוצה מבית ספר בדרום שמנתה 15 מורים, וקבוצה מבית ספר במרכז הארץ שמנתה 8 מורים. בלוח 1 מוצגת התפלגות המשתתפים על פי סטטוס (מורה/תלמיד) ומגדר.

לוח 1

התפלגות המשתתפים בקבוצות המיקוד על-פי סטטוס ומגדר

		מורים		תלמידים		סה"כ	
מאפיינים	ערכים	*n*	%	*n*	%	*n*	%
מגדר	זכר	7	16%	26	84%	31	44%
	נקבה	16	46%	21	54%	39	56%
סה"כ		23	33%	47	67%	70	100%

מלוח 1 אנו למדים שבקרב התלמידים מספר הבנים גבוה ממספר הבנות ובקרב המורים מספר הנשים גבוה ממספר הגברים.

כלי המחקר

שיטת המחקר שנבחרה היא שיטת המחקר האיכותנית וזאת מכיוון שהמחקר דורש הבנה עמוקה של המאווים וההתנהגויות האנושיים. באווירה של דינאמיקה קבוצתית פתוחה ובטוחה עולים רעיונות, דעות, רגשות, מעשים ומחשבות שמהם ניתן לשחזר דפוסי פעולה ואת המניעים להם. ניתוח מקצועי של הנושאים שעולים בקבוצה עשוי לאתר את המוטיבציות הבסיסיות ואת הצרכים העמוקים ביותר של משתתפי הקבוצה ושל האוכלוסייה שהם מייצגים (Krueger & Casey, 2009). מחקר איכותני נמצא מתאים לעבודה עם בני נוער שאישיותם מבשילה ומתקבעת רק עם הפיכתם לבוגרים (Defranco, 2011), שכן הוא ייתן תובנות משלימות המתייחסות למארג הנפשי של המתבגרים. בנוסף, ילדים ובני נוער מבטאים את עצמם ביתר נוחות במסגרת דינאמיקה של קבוצות מיקוד (Krueger & Casey, 2009). מכיוון שהתוצאה המעשית הרצויה של מחקר זה היא להביא בסופו של תהליך לשינוי תרבותי בנושא אבטחת המידע (Harris et al., 2014), חשוב להבין את המניעים להתנהגותם של משתמשי הקצה. המניעים לפעולה מורכבים שכבות על גבי שכבות, ותיאור בלתי-אמצעי שלהם יחשוף רק את הרובד השטחי והעליון (Bouhnik & Deshen, 2013 ; Krueger & Casey, 2009).

תהליך המחקר

הנתונים האיכותניים נאספו באמצעות קבוצות מיקוד (focus groups). קבוצת מיקוד היא מעין ראיון שבו איסוף הנתונים האיכותניים נעשה תוך אינטראקציה קבוצתית מונחית.

שיטת איסוף הנתונים

בניית קבוצת המיקוד התבססה על הצעדים לתכנון קבוצות דיון והשימוש בהם על פי סטיוארט ושמדסני (Stewart, D. & Shamdasani, 2014), בן שאול וגיבסון (2003), קרוגר וקסי (Krueger & Casey, 2009) ושקדי (2003):

א. הגדרת הבעיה

השאלות המחקריות שנשאלו במחקר זה היו שאלות מסדר ראשון, דהיינו שאלות שמתמקדות בתיאור התופעה הנחקרת ובהסברתה והתשובה להן מתקבלת במישרין מהתיאורים ומההסברים של הנשאלים עצמם (שקדי, 2003). מטרת השיחות הייתה להבין לעומק את הסיבות והמניעים לכך שבני הנוער וצוותי החינוך מאבטחים או לא מאבטחים כראוי את המידע שלהם. שאלת המחקר הייתה: מה יחסם של הנשאלים לסוגיית אבטחת המידע? מה גורם או יגרום להם לאבטח את המידע שלהם? בנוסף, ביקשנו לבחון אם יש הבדל בין תשובותיהם של גברים ושל נשים או של מורים ושל תלמידים.

ב. קביעת זהות המשתתפים בקבוצות המיקוד

במחקר הנוכחי גובשו שש קבוצות מיקוד. ארבע קבוצות מיקוד של תלמידים ושתי קבוצות מיקוד של מורים.

ג. קביעת זהות מנחה הקבוצה

החוקרת היא מנחת קבוצות מוסמכת והיא זו שהנחתה את הקבוצות בעזרתה של מנחה נוספת, מומחית בהנחיית קבוצות. השילוב בין שתי מנחות יש בו כדי להבטיח דינאמיקה קבוצתית ונקודת מבט נוספת הן במהלך הדיון והן בניתוח המידע שנתקבל מתמלול הראיונות. המנחה הנוספת הייתה גם אחראית לרישום הנאמר לצורך ניתוח הדברים לאחר מכן.

ד. מהלך הפעילות ושאלות מנחות:

הפעילות במסגרת קבוצות המיקוד במחקר הנוכחי נפתחה בסגנון של סיעור מוחות שעל פי שקדי (2003) מתאים מאוד לסוג "השאלות המעוררות" ולדיון בעקבותיהן. בתחילת המפגש פוזרו על הרצפה כרטיסים שעליהם היגדים, כתבות, סיפורים ותמונות הקשורים לנושאים באבטחת מידע (נספח 1 בכתובת: http://katzr.net/ec3f88). כל משתתף התבקש לבחור כרטיס שהוא מתחבר אליו, מסכים אתו, מתנגד לו, חש כי הוא קרוב לליבו או שהוא מזכיר אירוע שארע לו באופן אישי או לאחד מחבריו. לאחר הבחירה נתבקש כל משתתף לענות לעצמו על השאלות הבאות: איפה האמירה/כתבה/סיפור/תמונה פוגשים אותך? האם יש קשר

בין האמירה/כתבה/סיפור/תמונה לאבטחת מידע? מה ניתן לעשות כדי למנוע פגיעה במידע? האם קרה לך או למי מחבריך מקרה של איום על אבטחת המידע? חלק מההיגדים הותאמו לאוכלוסיית התלמידים או המורים על פי הצורך. לפעילות זו הוקדשו שלוש דקות.

מטרת פעילות הפתיחה הייתה למקד את חברי הקבוצה בנושא הדיון, למשוך אותם לשיחה פתוחה ולעורר דיון בנושאים שהועלו במהלך השיחה. באמצעות הפעילות המשתתפים גירו והעשירו זה את זה, והתמונה הסופית כללה טווח רחב של משמעויות ופרשנויות של נושא אבטחת המידע. כל שיחה ארכה כשעה וכללה דיון בדילמות הקשורות לאבטחת מידע, להרגלי אבטחת המידע של המשתתפים ולעמדות המשתתפים בנושאים אלה. הדיונים כללו שאלות פתוחות והמנחות עודדו את המשתתפים להגיב על דבריהם ומעשיהם של המשתתפים האחרים ושל המנחות. הקשרים שנוצרו תוך כדי הדיון יצרו סיטואציה כמו מציאותית, והאופן שבו התמודדו המשתתפים עם הקשרים הללו סיפק חלק מן המידע שחיפשה החוקרת. ניתן לעיין בדוגמאות לשאלות שנשאלו במסגרת קבוצות המיקוד בנספח 2 בכתובת: http://katzr.net/ec3f88 בחלק מהקבוצות, השתמשה החוקרת על פי התפתחות הדיון גם בסרטונים להמחשת נקודות באבטחת מידע. דוגמאות לסרטונים ששימשו את החוקרת ניתן לראות בנספח 3 בכתובת: http://katzr.net/ec3f88.

אחת מהביקורות על קבוצות מיקוד היא שהמשתתפים פועלים מתוך רצייה חברתית, כלומר, נתונים ללחץ דעת הקהל ולכן אומרים את מה שמצופה מהם ולא את דעתם האמיתית (Stewart, D. & Shamdasani, 2014). משום כך, השתדלו המנחות להיות רגישות לסיטואציות כאלה ולעודד שיחה באווירה פתוחה ללא לחצים. בסיום הפגישה קיבלו המשתתפים מגנט שעליו כללים לאבטחת הטלפון האישי (נספח 4 בכתובת: http://katzr.net/ec3f88).

כל הדיונים בקבוצות תועדו באמצעות הקלטות שהקליטו החוקרת והמנחה הנוספת ובאמצעות רישום הערות בזמן הדיון. ההערות כללו התייחסות לתקשורת הלא-מילולית כפי שבאה לידי ביטוי במהלך הדיון – לשפת הגוף של הנשאלים, למנגינה של המילים ולאווירה הכללית בזמן הדיון.

ה. ניתוח הנתונים

ניתוח קבוצת המיקוד מתחיל למעשה ברגע שהתכנסה הקבוצה וממשיך תוך כדי איסוף הנתונים וגם לאחריו. במשך כל זמן איסוף הנתונים מתרחשת אינטראקציה בלתי פוסקת בין

איסוף הנתונים לניתוח. ניתוח המידע תוך כדי איסופו נותן לחוקרים מושג ברור יותר לגבי הכיוונים המתאימים של הראיונות – אלה שאלות לשאול או היכן ובמה להתמקד בתצפית. המנחה צריך להפעיל את שיקול דעתו מתי להרחיב את הדיון בנושא שהקבוצה מוצאת בו עניין, מתי לסיימו או מתי להציג שאלות חדשות (שקדי, 2003 ; Stewart, D. & Shamdasani, 2014). עם זאת הניתוח העיקרי מתבצע לאחר שהדיון הסתיים. ניתוח הנתונים שנבחר במחקר הנוכחי היה ניתוח לשוני, שמתייחס למילים ולתיאורים של הנשאלים כמשקפים את רגשותיהם, מחשבותיהם, את אמונותיהם וידיעותיהם (שקדי, 2003).

תמלול השיחות

השלב הראשון בניתוח הנתונים היה תמלול השיחות תוך הקפדה על האנונימיות של המשתתפים. תמלול השיחות מספק, מלבד אפשרות לניתוח תוכן השיחה, גם תיעוד רשום של השיחה שניתן לשתף עם גורמים נוספים (Stewart, D. & Shamdasani, 2014). הפריטים המקודדים היו מילים, משפטים וחילופי דברים בין המשתתפים. ניתוח תוכן של קבוצת מיקוד כולל מלבד מבעים מילוליים גם תצפיות התנהגותיות ושפת גוף, מאפיינים כמו תקשורת לא-מילולית, מחוות, תגובות התנהגותיות וכן המנגינה של המילים שנאמרו. יש משפטים שניתנים להבנה שונה לחלוטין על פי המנגינה שבה הם נאמרים. לכן, במסגרת המחקר הנוכחי תומללה כל שיחה מיד לאחר התרחשותה והוספו לתמלילי השיחות גם הערות של החוקרת מתוך התצפית שלה בקבוצה. להלן מספר הערות לדוגמה:

- ניכר שהתלמידים מרגישים בטוחים לומר את אשר על ליבם.
- השיחה הייתה חופשית ומשוחררת מאוד.
- על פי הבעות הפנים של התלמידים אמירה זו הייתה חדשה להם. הם לא חשבו על הנושא עד עתה.

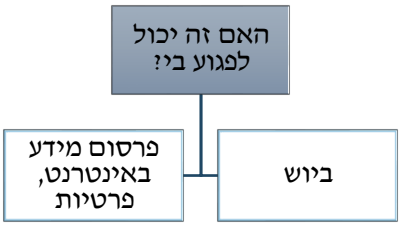
קטגוריזציה

במוקד הניתוח האיכותני קונסטרוקטיביסטי נמצא תהליך הקטגוריזציה – שיוך פיסות מידע לקטגוריות המתאימות. שלב הניתוח הראשוני, **שלב הקידוד הפתוח** (Corbin & Strauss כמובא אצל שקדי, 2003), נעשה בעזרת תוכנת MAXQDA, המסייעת באיסוף, בארגון, בניתוח ובפרסום נתונים במחקר איכותני כמו גם במחקר כמותי ומשלב. בשלב הקידוד הפתוח עברה החוקרת על כל שורה בתמליל בדקדקנות ושאלה את עצמה שאלות כמו מהו נושא השורה או מהו הרעיון העיקרי בהיגד. בהתבסס על קריאה ראשונית זו היא זיהתה את הקטעים הרלוונטיים לשאלות המחקר ויצרה מערכת ראשונית לסיווג קטגוריות עיקריות

שאליה שויכו הפריטים. יחידות הניתוח בקידוד הפתוח היו היגדים בני מילה או משפט שסיפקו את ההקשר לדברי הנשאלים. לדוגמה: "ביוש (שיימינג)", "אני לא בעניין", "פריצות", "סיסמאות", "הכול נמצא באינטרנט" ועוד. לכל קטגוריה שויך מספר שונה של פריטים, בהתאם לחשיבות הנושא כפי שבאה לידי ביטוי במספר הפעמים שהנושא עלה או בחזרה עליו פעם אחר פעם. שלב זה בניתוח פותח את תהליך החקר, כך שכל פרשנות וכל קטגוריה הן זמניות. כל דיון בקבוצת מיקוד נותח באופן עצמאי, "בראש פתוח ובמידה שווה" (שקדי, 2003, עמ' 118).

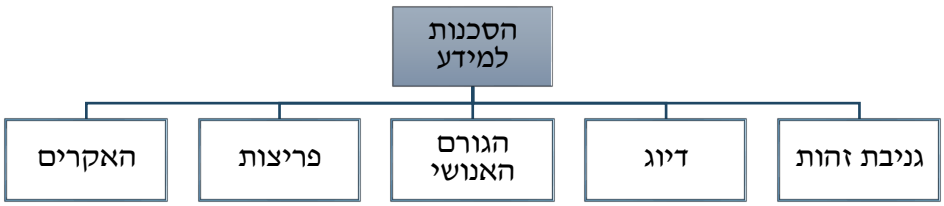
לאחר שכל הנתונים נותחו בשלב הקידוד הפתוח, אפשר היה לעבוד לשלב הבא, **ניתוח ממפה** (שקדי, 2003), שבו בוחנים ביתר דיוק ותוך הסתכלות כוללת קשרים אפשריים בין קטגוריות לבין עצמן ובין קטגוריות לבין תת-קטגוריות.

בשלב הניתוח הממפה עסקה החוקרת באותם נתונים ובניתוחם שוב ושוב, כל עוד זיהתה סוגיות חדשות שיכולות לבוא לידי ביטוי קטגוריאלי, וחילקה את הקטגוריות לרמות נפרדות. להלן דוגמה לחלוקה לרמות שונות כפי שהתבצעה בשלב זה של הניתוח: בשלב הראשוני, הקידוד הפתוח, נקבעו שלוש הקטגוריות שרמתן זהה: "ביוש", "האם זה יכול לפגוע בי" ו"פרסום מידע באינטרנט". בשלב הממפה הבינה החוקרת שהקטגוריות "ביוש" ו"פרסום מידע באינטרנט" הן למעשה תת-קטגוריות של הקטגוריה "האם זה יכול לפגוע בי" ויצרה את המבנה ההיררכי המוצג בתרשים 1.



תרשים 1 . חלוקה לתת קטגוריות – האם זה יכול לפגוע בי?

על הציר האופקי זיהתה החוקרת מספר קטגוריות ראשוניות, שמשותפת להן השתייכותן לאותה "משפחה" של קטגוריית על. לדוגמה, הקטגוריות פצחנים, פריצות, הגורם האנושי, דיוג וגניבת זהות שייכות לקטגוריית על שהחוקרת קראה לה "הסכנות למידע". ראו תרשים 2.



תרשים 2. חלוקה לתת-קטגוריות – סכנות למידע

תוך כדי מעבר על הקטגוריות השונות ועל קידוד הראיונות הבחינה החוקרת כי על אף שהקטגוריות בקבוצות המיקוד של המורים ושל התלמידים זהות, הרי שיש מקום להתייחסות נפרדת לקבוצות אלה במסגרת הניתוח. התייחסות זו תופיע בפרק הממצאים של המחקר.

שלב הניתוח השלישי הוא **השלב הממוקד** (שקדי, 2003) ובו החוקרים ממקדים את פרטי המידע להסבר קוהרנטי סביב קטגוריות מרכזיות. בהבניית הקטגוריות המרכזיות משתמשים בקטגוריות שנוצרו בניתוח הממפה ומחפשים אחר הנושא, העניין או הבעיות המרכזיות של התופעה הנחקרת. לקטגוריות המרכזיות יש תת-קטגוריות שהן למעשה התכונות שלהן.

בשלב זה זיהתה החוקרת שתי קטגוריות מרכזיות: הראשונה היא הערכת מצב הסיכונים למידע כאיום או כאתגר והשפעתה על אבטחת המידע והשנייה היא השפעת המודעות לאבטחת מידע על שימוש בכלים לאבטחה. משתי קטגוריות אלה התפצלו שש תת-קטגוריות מכוונות ומהן פוצלו קטגוריות התוכן כמתואר להלן ובתרשים 3.

1. הערכת מצב הסיכונים למידע כאיום או כאתגר והשפעתה על אבטחת המידע.
   - 1.1. האם אני מסוגל להתמודד עם האיום?
   - 1.2. האם האיום יכול לפגוע בי?
     - 1.2.1. ביוש
     - 1.2.2. פרסום מידע באינטרנט, פרטיות
   - 1.3. הסכנות למידע
     - 1.3.1. פצחנים
     - 1.3.2. פריצות
     - 1.3.3. הגורם האנושי
     - 1.3.4. דיוג
     - 1.3.5. גניבת זהות

2. השפעת המודעות לאבטחת מידע על שימוש בכלים לאבטחה

2.1. צורך בידע וכלים לאבטחת מידע

2.2. חינוך לאבטחת מידע

2.2.1. מודעות לאבטחת מידע

2.2.2. אחריות אישית

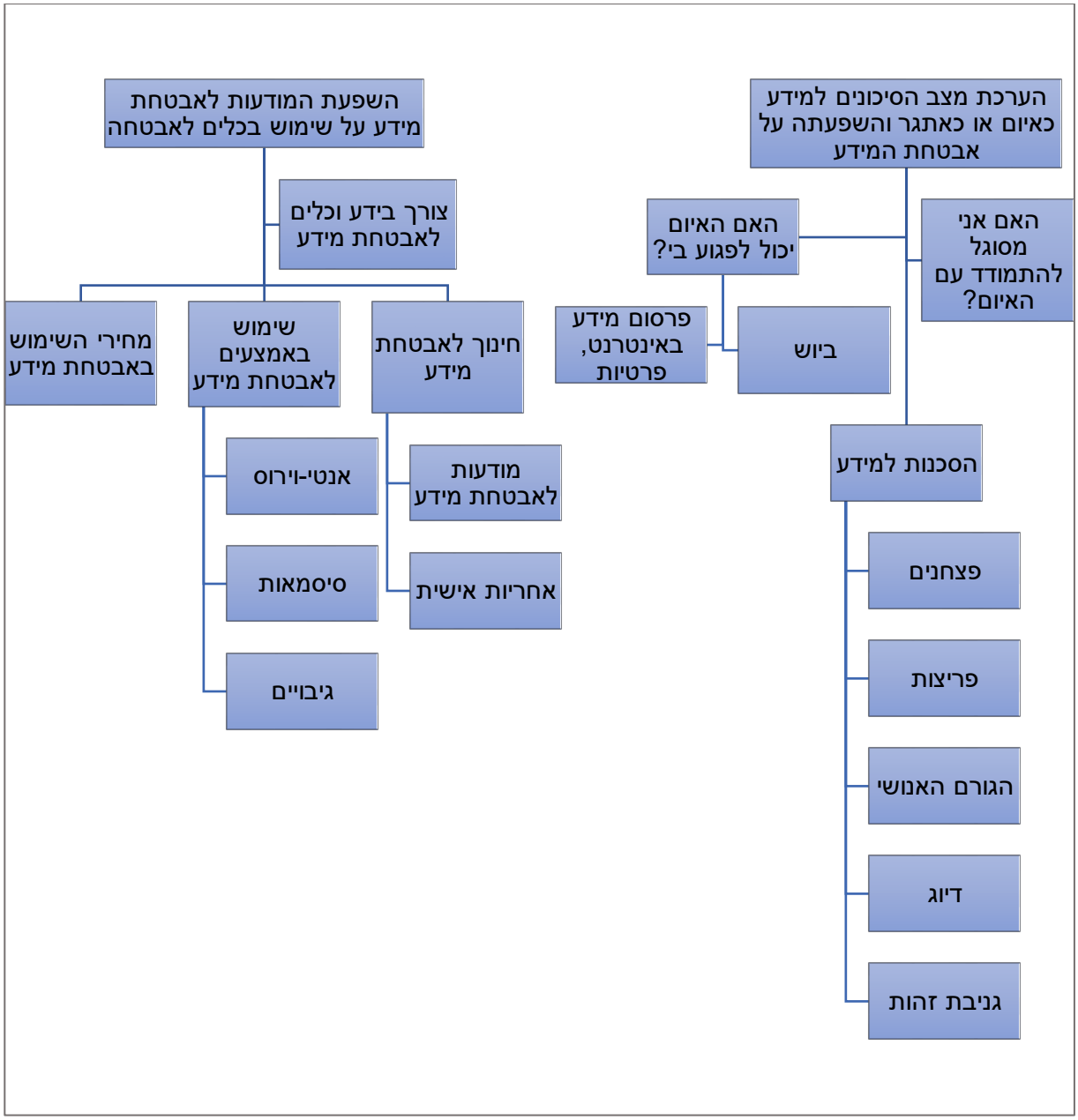
2.3. שימוש באמצעים לאבטחת מידע

2.3.1. אנטי-וירוס

2.3.2. סיסמאות

2.3.3. גיבויים

2.4. מחירי השימוש באבטחת מידע



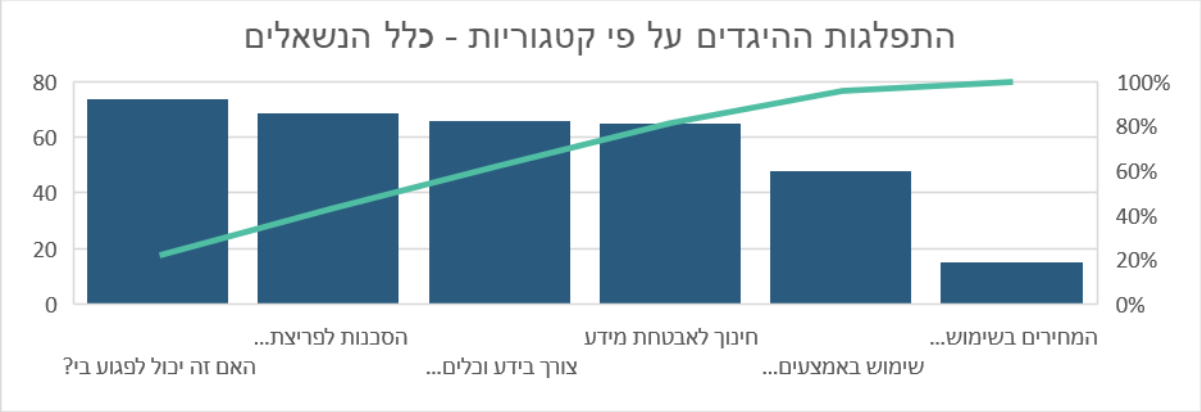
תרשים 3. עץ הניתוח: קטגוריות ותת קטגוריות

ו. מהימנות ותוקף המחקר:

כדי לתת מהימנות ותוקף לניתוח הממצאים במחקר הנוכחי, הועבר התמליל כולו לשני מעריכים נוספים. המעריך הראשון הוא פרופסור חוקר המנחה סטודנטים בעבודות מחקר והמעריכה השנייה היא מנחה בכירה בהנחיית קבוצות בחינוך הבלתי פורמלי. מעריכה זו הייתה שותפה להנחיית קבוצות המיקוד במסגרת המחקר והכירה את המחקר על כל שלביו. תמלילי השיחות הועברו לשני המעריכים תוך בקשה למיין את הנתונים לקטגוריות ולשייך אליהן את הפרטים הרלוונטיים. אחד המעריכים התבקש לקרוא את תמלילי השיחות מבלי שקיבל מידע מוקדם על הרכב הקבוצות השונות, מלבד העובדה שמדובר במחקר העוסק במוכנות של אוכלוסיית המחקר לאבטחת מידע, וזאת כדי לשמור על האובייקטיביות של ניתוח הנתונים. מעריך זה ביצע את תהליך החלוקה לקטגוריות באופן ידני בסימון המילים או המשפטים שלדעתו משמשים כקטגוריות. המעריכה השנייה הציעה אפשרות לארגון שונה של הקטגוריות, ושייכה את הפריטים השונים לקטגוריות שהציעה. הייתה הסכמה של כ- 80% בין המעריכים והחוקרת לגבי החלוקה לקטגוריות ושיוך הפריטים אליהן. ההסכמה על ניתוח 20% הנותרים התקבלה לאחר מפגש שהתקיים בין שני המעריכים הנוספים והחוקרת. לאחר דיון, תוך שקלול ההצעות השונות, נקבעו הקטגוריות, מבנה עץ הניתוח והשיוך הסופי של הפריטים לקטגוריות השונות כפי שהוצגו לעיל.

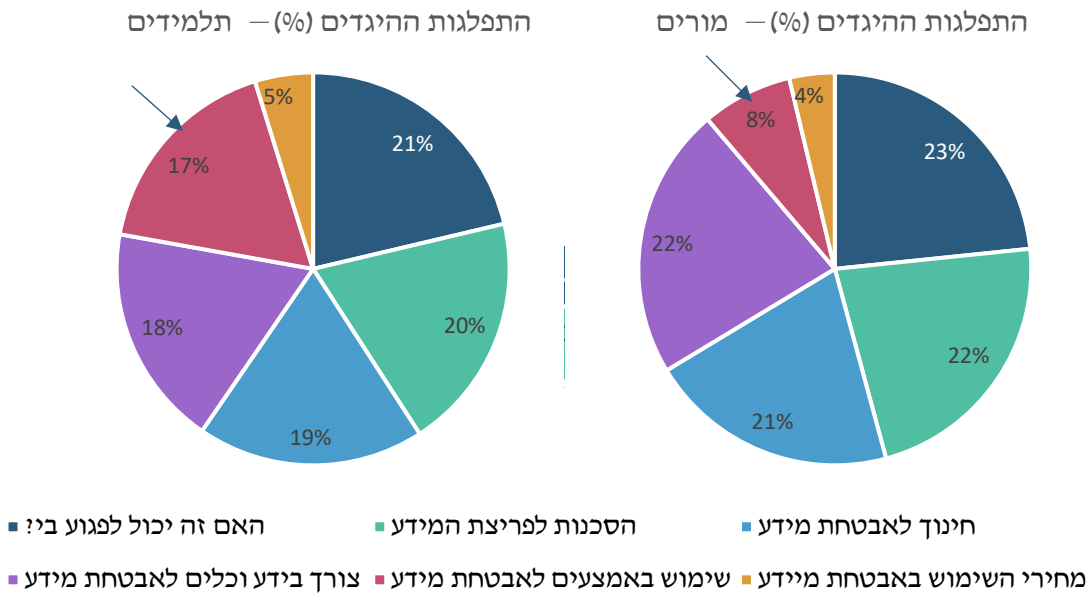
ממצאים

הממצאים מקבוצות הדיון וניתוחם שופכים אור על תפיסת הסיכונים למידע בקרב המורים והתלמידים. בתרשים 4 מוצגת התפלגות מספר ההיגדים השייכים לכל קטגוריה בסדר יורד, עבור כלל הנשאלים עם קו מצטבר בציר משני המציג אחוז מהסכום הכולל.



תרשים 4. התפלגות היגדים על פי קטגוריות – כלל הנשאלים

ניתן לראות כי הקטגוריה המשמעותית ביותר, דהיינו הקטגוריה שכללה את מספר ההיגדים הגדול ביותר, הייתה "האם זה יכול לפגוע בי". לקטגוריה זו שויכו 22% מההיגדים, והיא כוללת את ההיגדים הנוגעים לפרסום מידע אישי באינטרנט, את נושא הפרטיות באינטרנט ואת נושא הביוש. הקטגוריה השנייה בגודלה הייתה "הסכנות לפריצת המידע". קטגוריה זו כללה את התת-קטגוריות: פצחנים, פריצות, הגורם האנושי, דיוג וגניבת זהות. הקטגוריות "צורך בידע וכלים לאבטחת מידע" ו"חינוך לאבטחת מידע" תפסו את המקומות השלישי והרביעי. מיד אחריהן נמצאת הקטגוריה "שימוש באמצעי אבטחה" הכוללת את התת-קטגוריות: אנטי-וירוס, סיסמאות וגיבויים. הקטגוריה האחרונה היא "מחירי השימוש באבטחת מידע".



תרשים 5. התפלגות ההיגדים (באחוזים)

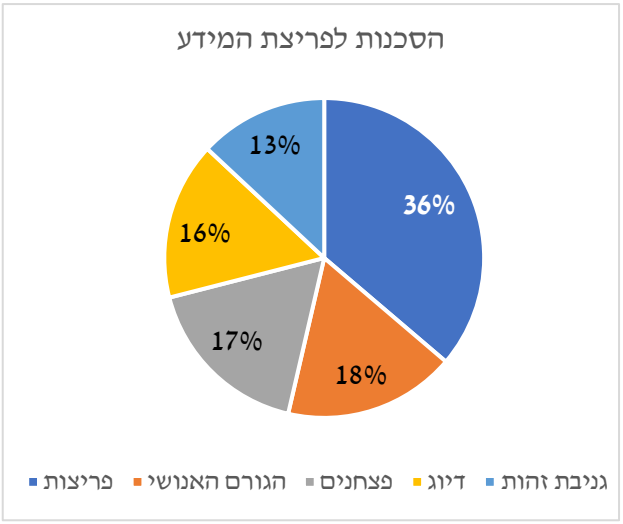
מעיון בתרשים עולה כי קיים הבדל משמעותי בין התייחסויות המורים והתלמידים לקטגוריה "השימוש באמצעי אבטחה". התלמידים העלו נושאים הקשורים לשימוש באבטחת מידע, דהיינו שימוש בסיסמאות, בגיבויים ובאנטי-וירוס, פי שניים מהמורים. יתכן כי הבדל זה נובע ממודעות גבוהה יותר של התלמידים לכל הקשור לאבטחת מידע ולהתגוננות מפני סכנות למידע כתוצאה משימוש נרחב יותר במדיה.

סכנות הפגיעה האישית ופריצת המידע

כאמור, שתי הקטגוריות העיקריות שעלו בדיונים היו נושא הפגיעה האישית והסכנות לפריצת המידע כאשר נושא הפריצות למידע האישי הוא הגורם העיקרי להערכת המצב כאיום.

בתרשימים 6 ו7 מוצגים התפלגות ההיגדים של שתי קטגוריות אלו לתת-קטגוריות.

תרשים 6. *האם זה יכול לפגוע בי?*



תרשים 7. *סכנות הפריצה למידע*

כפי שניתן לראות מהתרשימים, מרבית המשתתפים, הן המורים והן התלמידים, התייחסו לנושא הפגיעה האישית כאל הנושא המאיים והמפחיד ביותר עבורם, וחשו חוסר אונים להתגונן בפני פריצה למאגרי המידע האישיים שלהם וחוסר יכולת להתמודד עם הסכנה. תגובות להצגת סרטון בנושא האיום לפגיעה בפרטיות כללו אמירות כמו "אימאל'ה, זה מפחיד". הם הודו באזלת ידם: "אין לנו שליטה מלאה, כמו שאין לנו שליטה מלאה אם מישהו יפרוץ לנו לבית". בנספח 5 (http://katzr.net/ec3f88) מוצגים אמירות נוספות של התלמידים והמורים בנושא הפגיעה האישית. במסגרת השיחות בנושא גניבת זהות התברר שגם בקבוצת המורים וגם בקבוצת התלמידים היו שחוו על בשרם חוויה זו. אחת המורות סיפרה: "שלחו בשמי SMS שאין בוחן..." ומספר תלמידות סיפרו על פריצות לפייסבוק: "קרה לי שהשתלטו לי על הפייסבוק ושינו לי את ה- user name".

הגורם האנושי היה התת-קטגוריה השנייה בחשיבותה גם בקרב המורים וגם בקרב התלמידים. "גם אם אנשים יודעים שצריך להיזהר אנשים טועים. על זה בנויים ההאקרים. על זה בנוי לפרוץ", טען אחד התלמידים.

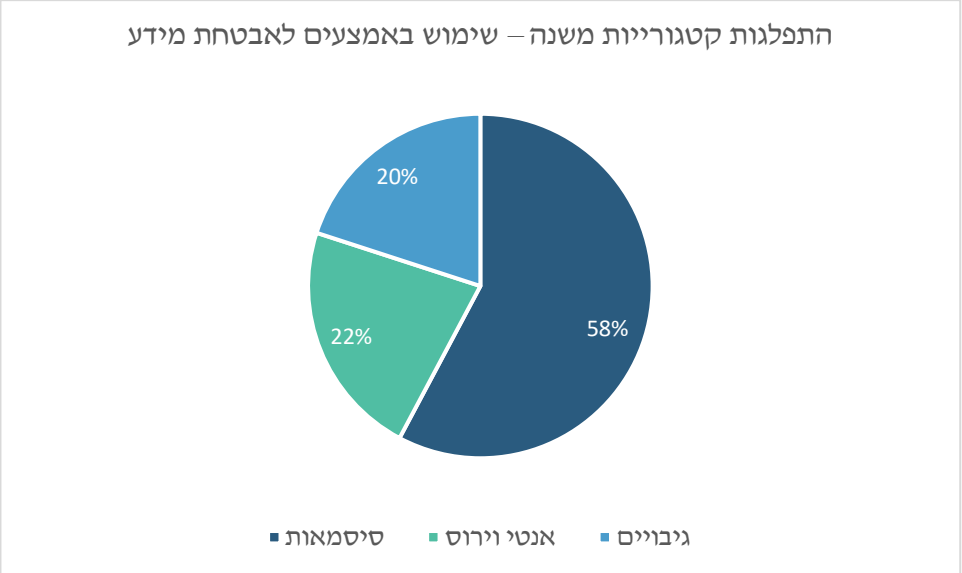
יש הבדלים רבים בין אלה החשים שאינם מסוגלים להתמודד עם נושא אבטחת המידע לבין אלה הרואים בו אתגר ומוכנים להתמודד עמו. המורים המבוגרים יותר הצהירו שמכיוון שהנושא מאיים עליהם, הם נמנעים מללמוד אותו. מורים אלה הם חסרי ידע לחלוטין בכל הנוגע לפרסום באינטרנט. הפתרון שלהם הוא להתעלם מהחדשנות: "אני רוצה להגיד רק משפט אחד. אני נולדתי במאה הקודמת. אין לי פייסבוק, אין לי מייל אני לא משתמשת בכלום, קצת בווטסאפ.

אני לא מצטלמת. אף אחד לא יכול למצוא אותי״. אמירות נוספות של התלמידים והמורים בנושא ההתמודדות עם אבטחת המידע מוצגות בנספח 6 (http://katzr.net/ec3f88). עם זאת, מדבריהם של רבים מהתלמידים ניכר היה שהם חשים כי מדובר באתגר מעורר עניין. תלמידים אלה הראו בקיאות רבה בנושאים הקשורים לאבטחת מידע ועל פי העדויות העצמיות הם מיישמים יותר כלים להגנה על המידע האישי שלהם בחיי היום-יום מעמיתיהם שנושאים אלה זרים להם. הם לומדים את הנושא ומשתמשים בטכניקות אבטחת מידע שהם מפתחים: ״אני תמיד בודק את ה-URL של האתר״. בנספח 7 (http://katzr.net/ec3f88) מוצגות אמירות נוספות של התלמידים והמורים בנושא האתגר שאבטחת המידע מציבה בפניהם.

לשאלתנו אם יש הבדל בין בנים לבנות בנוגע למודעות לאבטחת מידע ענו התלמידים שנשים פחות מתעניינות ופחות משתמשות במחשבים. לראיה, סיפר אחד התלמידים: ״בקורס אבטחת מידע יש רק אולי חמש בנות. כולן פרשו. אולי כי זה פחות מעניין אותן״.

שימוש באמצעים לאבטחת מידע

התלמידים הזכירו נושאים הקשורים לשימוש באבטחת מידע – שימוש בסיסמאות, בגיבויים ובאנטי-וירוס, בתדירות כפולה מהמורים (תרשים 5) – 17% מהתלמידים העלו את נושא השימוש באמצעים לאבטחת מידע לעומת 8% מהמורים. בתרשים 8 מוצגת התפלגות אזכורי האמצעים לאבטחת המידע.



תרשים 8. תת קטגוריות – שימוש באמצעים לאבטחת מידע

כפי שנראה, **נושא הסיסמאות** העסיק מאוד את המורים ואת התלמידים. מעל למחצית מהאמירות בנושא השימוש באמצעים לאבטחת מידע עסקו בנושא זה. במסגרת קבוצות המיקוד

התברר שמשתמשים רבים, גם בקרב המורים וגם בקרב התלמידים, משתמשים בסיסמאות קלות לפיצוח כמו 1234, שמות בני המשפחה או תאריכים משמעותיים בחייהם. חלקם אף הודו שהם מגינים על המידע באמצעות סיסמה רק כי: "כשאתה רוצה להיכנס לתוכנה אז מכריחים אותך לשים סיסמה". יש לציין כי לתלמידים רבים הייתה מודעות גבוהה יותר לצורך בסיסמה קשה לפיצוח. היו אף שהודו כי למדו שיש צורך לאבטח את המידע מתוך ניסיון אישי: "לי פרצו כמה פעמים ואז הבנתי שאני צריך לשים סיסמאות ולא 123".

ניתן לחלק את הגורמים לבחירת סיסמה קלה לפיצוח שבאו לידי ביטוי בקבוצות המיקוד לארבע קבוצות:

א. חוסר הבנה: "איך מישהו יודע שהסיסמה שלי היא השם של סבתא שלי".

ב. העדפת נוחות השימוש: "אני לא עושה סיסמאות קשות כי אני כבר לא זוכרת אותן מרוב שאני מחליפה".

ג. חוסר מודעות לנזקים האפשריים של פריצה לחשבונות: "ואם יפרצו אז מה, הם ידעו איפה אני לומדת? כל בן אדם בעולם יכול לדעת".

ד. הרגשת חוסר אונים: "לא משנה איזה סיסמה תעשי אפשר לגלות".

נושא **האנטי-וירוס** העסיק רק את התלמידים והיו חילוקי דעות אם הוא בכלל נדרש. רוב התלמידים הכריזו כי הטלפון החכם שלהם מוגן באנטי-וירוס כי "אם לטלפון אין אנטי-וירוס זה מסוכן", אלא שיש שטענו כי הוא חסר תועלת: "אנטי-וירוס כבר לא רלוונטי. אם מישהו רוצה לפרוץ לטלפון שלך הוא יצליח".

נושא הגיבויים היה מוכר למרבית המשתתפים, הן לתלמידים והן למורים, אלא שכפי שהעידה אחת המורות: "אני יודעת שזה חשוב אבל אני לא עושה את זה". לשאלה היכן צריך לגבות ידעו המשתתפים להשיב כי יש לגבות "בהתקן חיצוני". בנספח 8 (http://katzr.net/ec3f88) מוצגות אמירות נוספות בנושא הגיבויים.

מחירי השימוש באבטחת מידע

את המחירים שיש לשלם עבור השימוש בתוכנות לאבטחת מידע הזכירו בעיקר התלמידים. המחיר העיקרי שמפריע לתלמידים הוא ההאטה בגלישה שגורם האנטי-וירוס. יש שסיפרו שהסירו את תוכנת האנטי-וירוס מהמכשיר החכם שלהם מסיבה זו: "בטלפון הקודם התקנתי אנטי-וירוס אבל זה כל כך האט לי את הגלישה אז הורדתי וזה עשה לי וירוס ממש מעצבן שאי אפשר היה להיפטר מזה בשום צורה". מחיר השימוש בסיסמאות חזר ועלה בכל השיחות: "מה, כל שבועיים להחליף סיסמה זה לחיות את זה. זה להיות עבד לסיסמה".

חוסר ידע

בשיח שנוצר בקבוצות המיקוד של המורים ושל התלמידים ניכר היה שחלק מהנשאלים היו חסרי ידע בכל הנוגע לאבטחת מידע. הם אינם בקיאים במושגים בסיסיים באבטחת מידע ומצהירים על חוסר הביטחון שהם חשים בנושא. אחת המורות התלוננה: "אני יודעת איך למחוק את ההיסטוריה במחשב אבל לא יודעת איך לשנות את ה cookies וזו הבעיה שלי". בשיחה על גיבויים למידע נשמעו אמירות כגון: (מורה) "אנחנו לא יודעים לעשות את הגיבויים כמו שצריך"; חוסר הידע התבטא גם באמירות כמו (תלמידה) "חשבתי שהתפקיד של האנטי-וירוס הוא לחסום פרסומות" בדיון שהתפתח בנושא הדיוג שאלו מספר מורים: "איך יודעים אם זה אתר אמיתי או מתחזה"?

לרוב התלמידים הייתה מודעות לנושא, אך לחלקם חסר ידע בסיסי בנושא הפרטיות כפי שניתן לראות בנספח 9 (http://katzr.net/ec3f88).

אחד התלמידים הסביר את חוסר המודעות לצורך באבטחת מידע באופן מקורי ביותר: "אנשים פשוט לא מרגישים שזה סיכון כי הם לא רואים את הסכנה. למשל אם תראי בחור עם סכין את תגידי זה מסוכן. אבל אם מישהו יהיה מרחוק עם צלף את לא תדעי להגיד שאת בסכנה. תחשבי שאת בסדר. צלפים זה ההאקרים. הם רק מחכים לפגוע בנקודות התורפה שלך".

הצורך בחינוך לאבטחת מידע

הצורך בהעלאת המודעות לאבטחת מידע עלה באופן בולט מאוד הן אצל המורים והן אצל התלמידים. אלה וגם אלה העלו את הצורך בחינוך לאבטחת מידע, בהעלאת המודעות לנושא וביצירת אחריות אישית כנושאים הקריטיים שיכולים להשפיע על המשתמשים הצעירים והבוגרים ולעודדם ליישם יותר כלים לאבטחת המידע: "מה שצריך זה לחנך גם כפוגעים וגם כנפגעים". בנספח 10 (http://katzr.net/ec3f88) מוצגות אמירות נוספות בנושא הצורך בחינוך לאבטחת מידע.

לשאלתנו מי צריך להיות האחראי לחינוך למודעות לאבטחת מידע היו התשובות חלוקות. חלק מן הנשאלים, גם מורים וגם תלמידים, מאמינים שהתלמידים צריכים לחנך את חבריהם: (תלמיד) "אני חושב שהרוב המוחלט של התלמידים הם מספיק בוגרים כדי לבוא לחברים שלהם ולומר להם שיש מקרים, קרו מקרים ושלא ישלחו תמונות, יזהרו במידע שהם מעלים ומפיצים באינטרנט". לעומת זאת, חלקם טענו שיש צורך שגורמים חיצוניים יגיעו לבית הספר וישוחחו עם התלמידים על נושא אבטחת המידע: (מורה) "לא מורה צריך ללמד אלא מישהו חיצוני". אם כי אחד המורים טען: "לפני שנה או שנתיים הייתה בבית הספר הרצאה והילדים ישבו מזועזעים

ואמרו, מה באמת אפשר לזהות אותי? אבל תכלס אחרי דקה הם יצאו מהחדר ואף אחד לא באמת שינה את ההתנהגות שלו".

היו שהציעו ללמד את נושא אבטחת המידע במסגרת הלימודים. לשאלתנו: "אם יהיה שיעור שנקרא אבטחת מידע תתייחסו לזה"? התשובות היו חלוקות: לדעת התלמידים "אני חושבת שצריך להכניס לתוכנית הלימודים. לעשות סדרת שיעורים חובה לכל התלמידים כי זה באמת חשוב", "אם יהיה עליו בגרות אז כן" או אולי "בשיעורי חינוך" מנגד הועלו גם דעות שהביעו התנגדות להוראת הנושא כמקצוע בתוכנית הלימודים בטענה: "לא ללמד כמו שמלמדים מקצוע כי אז נשכח את זה רגע אחרי המבחן, כמו שקורה בכל המקצועות".

לשאלתנו לגבי תפקידם של ההורים בחינוך ובהענקת כלים לאבטחת מידע השיבו התלמידים: "ההורים לא מבינים מה קורה באינטרנט. הוא לא היה קיים כשהם היו ילדים". היו גם דעות אחרות: "אני סומך על גוגל שיש לה אינטרס לאבטח את המידע שלי, אחרת אעזוב אותה". אמירות נוספות בנושא האחריות לחינוך למודעות לאבטחת מידע מוצגות בנספח 11 (http://katzr.net/ec3f88) .

המשתתפים היו תמימי דעים באשר לאחריות האישית של המשתמש ולחובתו של כל אחד לשמור על המידע האישי שלו: (מורה) "אני חושבת שמעבר לקטע הטכני זה נוגע ברובד יותר עמוק. אנחנו צריכים לחדד את העניין של האחריות והביקורת העצמית... בגלל שהכול פרוץ זה עניין של מה שקורה אצלו בפנים".

בנוסף לצורך בחינוך לאבטחת מידע, עלה בכל קבוצות הדיון ה**צורך בהקניית ידע בנוגע לאבטחת מידע וכלים למימושה**. המורים והתלמידים הסכימו שיש צורך לצייד כל משתמש בידע ובכלים לאבטחת מידע. "צריך ללמד איך להתמודד עם זה. ללמד אמצעי מניעה". על פי דבריהם של המשתתפים נראה שלבנים בקרב התלמידים יש תחושת בקיאות בנושא, יותר מזו שיש למורים ולמורות ולתלמידות. התלמידים, בעיקר הבנים, טוענים שהם מסוגלים להשיג את הידע בעצמם ושההתגוננות שלהם "זה ניסיון שבא עם הזמן". לשאלה: "מניין אתם מקבלים את האינפורמציה שלכם על הנושא של אבטחת מידע"? התשובות היו: "אני מתעסק עם זה מגיל קטן ושמתי לב שצריך סיסמאות" וגם "מהאינטרנט כמובן וגם מהטלוויזיה. וגם אנחנו שומעים בחדשות על כל מיני מקרים, וכמובן מחברים. זה מה שהכי משפיע עלינו". הטלוויזיה כבר פחות רלוונטית לבני הנוער והרשתות החברתיות מחליפות אותה. אמירות נוספות מוצגות בנספח 12 (http://katzr.net/ec3f88)

אחת המורות סיכמה את הנושא במילים אלה:

אני חושבת שאנחנו לא יכולים להתנזר מהעולם הזה. יש בו גם המון דברים נוחים וטובים. אפשר לעשות תיאום מס ברגע ולא לעמוד שעות במס הכנסה, אפשר להזמין חופשה באילת דרך האינטרנט וזה יותר נוח ומצוין. מצד שני אין לנו שליטה מלאה, כמו שאין לנו שליטה מלאה אם מישהו יפרוץ לנו לבית. מה שצריך זה להגיד. כמו שאנחנו מדברים עם תלמידים אני לא נפגש עם זרים, אל תפיץ דברים יותר מדי אישיים על עצמך בפייסבוק, שאתה מעלה כל דבר שקורה לך, צריך לדעת לשים את האיזונים. צריך להיזהר עם זה.

דיון

מומחי אבטחת המידע מסכימים בדבר החשיבות הרבה שיש לידע, להתנהגות ולמודעות לנושאים הקשורים לאבטחת מידע (Velki et al., 2017). בפועל, לא פעם מסכנת התנהגות המשתמשים את המידע מכיוון שרוב האנשים ממעיטים בחשיבותה של אבטחת המידע (McCormac et al., 2017). שאלת המחקר הראשונה התמקדה ביחסם של אוכלוסיית תלמידים בגילאי תיכון וצוותי החינוך לסוגיית אבטחת המידע.

על פי מודל סגנונות ההתמודדות עם איום של לזרוס ופולקמן (Lazarus & Folkman, 1984), בחירת דרכי ההתמודדות של האדם נובעת מהערכתו את הסיטואציה כמאיימת ומהערכתו את המשאבים העומדים לרשותו. אדם שלדעתו המשאבים שברשותו יעילים דיים יתמקד בבעיה ויראה את המצב כאתגר, ואילו אדם המטיל ספק במשאביו וביכולתו להתמודד יתמקד ברגש או יימנע מהתמודדות, והוא עלול לראות במצב איום. בדיונים שנערכו בקבוצות המיקוד בלט מאוד הקשר שבין הערכת משאבי הידע של המורים והתלמידים לבין תחושת האיום שהם חשים כלפי הסיכונים למידע ומתוך כך למוכנותם לאבטח את המידע שברשותם. בשיח שנוצר בקבוצות המיקוד עם המורים התברר שמורים רבים אינם בקיאים במושגים בסיסיים באבטחת מידע, והם מצהירים על חוסר הביטחון שהם חשים בנושא. עוד עולה מהשיחות עם המשתתפים כי המורים רואים בסכנות למידע איום מכיוון שהם מטילים ספק במשאבים שלהם וביכולתם להתמודד, בעוד התלמידים מעריכים את המשאבים שלהם כיעילים מספיק ולכן הם רואים את המצב כאתגר. נושא הפחד עלה בקבוצות הדיון בעיקר בקרב המורים כשהפתרון של חלק מהמשתתפים להתמודדות עם הפחד היה התנתקות מהמדיה. המורים המבוגרים יותר הצהירו שמכיוון שהנושא מאיים עליהם, הם נמנעים מללמוד אותו. למורים אלה אין כלל ידע הנוגע לפרסום באינטרנט, והפתרון שלהם הוא טמינת הראש בחול והתעלמות מהחדשנות. לעומתם, ניכר כי הרבה מן התלמידים חשים שמדובר באתגר מעורר עניין. תלמידים אלה מדווחים שהם למדו שיש צורך לאבטח את המידע מתוך ניסיון והם משתמשים בטכניקות אבטחת מידע שהם מפתחים. ממצאים אלה עולים בקנה אחד עם ממצאים ממחקרים קודמים על פיהם אופן ההתמודדות של אדם עם איום כאשר המוטיבציה שלו להגנה על עצמו מושפעת מהערכת האיום ומהערכת ההתמודדות עמו. אם אדם יעריך שהסכנה אינה חמורה, שלא סביר שתתרחש או כי הוא מסוגל להתמודד עימה, תגובתו הרגשית תהיה ביטחון עצמי, והוא ייטה לאמץ את ההתנהגות המוצעת. פחד עלול להתעורר אם האדם לא מכיר דרך התמודדות יעילה. המודעות לאבטחת מידע שעולה מתוך הרגשה של איום ופחד גורמת לעיתים לפעולה ההפוכה, ובמקום לדחוף ליישום כלים

לאבטחת מידע היא גורמת להימנעות מהתמודדות אתו (D'Arcy et al., 2014; Meso et al., 2013). גם וון ושותפיה (Woon et al., 2005) הגיעו למסקנה דומה, ומצאו שככל שהסיכון נתפס כמוחשי ודרכי ההתמודדות נראות ברורות, יעילות ואפשריות לשימוש, כך עולה הנטייה של הנבדקים להשתמש באמצעי הגנה כלפי האיום, כיוון שהם חשים שהם מסוגלים להתמודד אתו. מממצאי המחקר הנוכחי עולה עוד כי נושא הפגיעה האישית הוא הנושא המאיים ביותר והמפחיד ביותר, הן עבור המורים והן עבור התלמידים. נושא זה עלה שוב ושוב, יותר מכל נושא אחר. הוא חזר ועלה גם כאשר השיחה גלשה לתחומים אחרים. גם נושא הפריצות למידע האישי גורם להערכת המצב כאיום. בשיחתם הביעו המורים וחלק גדול מהתלמידים הרגשה של חוסר אונים בכל הנוגע לסכנת הפריצות למאגרי המידע האישיים שלהם.

גם נושא הסיסמאות העסיק מאוד את המורים ואת התלמידים. מעל למחצית האמירות בנושא השימוש באמצעים לאבטחת מידע התייחסו לנושא זה. סיסמאות הן קו ההגנה הראשון מפני גישה לא מורשית לנתוני המשתמש, והרגלי הסיסמאות של המשתמשים, כגון האופן שבו הם מנהלים את הסיסמאות שלהם או בחירתם בסיסמאות פשוטות או מורכבות, משפיעים ישירות על האבטחה הכוללת שלהם (McAfee Labs, 2017). עם זאת, כפי שעולה ממחקרים ומסקרים קודמים וכפי שעלה בקבוצות המיקוד במחקר הנוכחי, משתמשים רבים עדיין משתמשים בסיסמאות קלות לפיצוח כמו 1234, שמות בני המשפחה או תאריכים משמעותיים בחייהם. שימוש זה חוצה גיל, ואמירות אלה נשמעו מפי המורים והתלמידים בהבדל אחד – יותר תלמידים היו מודעים לצורך בסיסמה קשה לפיצוח. ממצאים אלה תואמים את הממצאים שנמצאו במחקרים ובסקרים קודמים. סקר שערכו מעבדות מקאפי (McAfee Labs, 2017a) מגלה כי הרגלי אבטחת המידע של משתמשי הקצה עדיין לוקים בחסר. אנשי אבטחה רבים ממליצים על תוכנת ניהול סיסמאות כדרך הטובה ביותר ליצור סיסמאות מורכבות ולאחסן אותן, ובכל זאת 84% מהנשאלים ענו שהם בוחרים שלא להשתמש בדרך מומלצת זו. הרוב המכריע של המשתמשים עוקב אחר הסיסמאות באמצעות שיטות מסורתיות הרבה יותר, במיוחד באמצעות שינון בעל פה (86%) או כתיבה על פיסת נייר (49%). מומחי אבטחת המידע ממליצים בדרך כלל על מספר שלבים שעל המשתמשים לנקוט כדי לצמצם את החשיפה שלהם לגניבת נתונים: שימוש בסיסמה שונה ומורכבת עבור כל חשבון, הימנעות משיתוף סיסמאות עם אחרים, שימוש בתוכנות אבטחה בטלפונים החכמים והקפדה על עדכון תדיר של יישומונים בטלפונים החכמים שלהם כדי לוודא שעדכוני האבטחה האחרונים מנוצלים (McAfee Labs, 2017b). מעניין לציין שבמהלך השנים האחרונות, הכריזו החוקרים שעל סיסמה אפקטיבית לכלול 15 או 20 תווים. אולם, הרוב המכריע של המשתמשים אינם יכולים או לא רוצים להשתמש בסיסמאות כאלה באופן קבוע

במרוץ היום-יומי שלהם (Steves & Krol, 2014). אי לכך, טוענים שי ושותפיו (Shay et al., 2016) שחוזק הסיסמה אינו חייב לעמוד בהכרח ביחס הפוך לנוחות השימוש בה. קיימת היום מדיניות שמאפשרת שימוש בסיסמאות שמישות יותר ומאובטחות יותר ואינה דורשת שימוש בסיסמאות ארוכות ומסובכות כפי שדורשת המדיניות הנפוצה היום. צעירים נוטים לשתף את הסיסמה שלהם עם אחרים יותר ממבוגרים, קובעים וויטי ושותפיה במחקר משותף של המחלקה ללמידה ולתקשורת באוניברסיטת ליסטר באנגליה והמחלקה למדעי המחשב באוניברסיטת אוקספורד, אנגליה (Whitty et al., 2015). ולקי ושותפיו (Velki et al., 2017) מאשרים קביעה זו ואף מוסיפים כי גם מרבית תלמידי התיכון מודים כי הם חושפים את סיסמת הגישה שלהם למערכת הדואר האלקטרוני. ניתן לתלות זאת בנורמה החברתית המקובלת, בעיקר אצל בני נוער. לחץ חברתי עלול להקשות על משתמשים רבים לסרב לבקשה לחשוף את הסיסמה שלהם. הנורמה החברתית היא שיקול חשוב בבחירת התנהגות האבטחה של האנשים (Lee. & Kozar 2005), ולכן ניתן להעביר לאנשים בעלי רצון עז לקבלת אישור חברתי מסר שמתייחס לשיתוף סיסמאות כטעות מוסרית וכפעולה אנטי-חברתית (Kajzer et al. 2014).

שאלת המחקר השנייה התמקדה בגורמים שיגרמו לנשאלים לאבטח את המידע שלהם. גם המורים וגם התלמידים ציינו שיש צורך בתוכנית להעלאת המודעות לאבטחת מידע. אלה וגם אלה הדגישו את המודעות לאבטחת מידע, את החינוך לנושא ואת האחריות האישית כגורמים קריטיים שיכולים להשפיע על המשתמשים הצעירים והבוגרים ולעודדם ליישם יותר כלים לאבטחת המידע. "יש לחנך את המשתמשים גם כפוגעים וגם כנפגעים". למסקנה זו הגיעו גם פרסונס ושותפיה (Parsons et al., 2014) שטענו כי החינוך וההכשרה לאבטחת המידע יהיו יעילים יותר אם הם לא יתמקדו רק בשיפור הידע ובהבהרת הציפיות מהמשתמש, אלא יספקו גם הבנה מדוע חשוב לאבטח את המידע. המסקנה שעל תוכניות אבטחת המידע להסביר את הסיכונים העלולים לגרום לנזק ולאובדן נתונים ממשתמשי הקצה עולה גם מדוח מקאפי (McAfee Labs, 2017b), שבו עלה שכדי להתגונן מפני תוכנות זדוניות עלינו תחילה להבין כיצד הן פועלות ומדוע תוכנות ההגנה אינן מצליחות לעצור אותן. המשתמשים חייבים ללמוד שבמהלך גלישה הם עלולים להוריד בטעות תוכנות זדוניות, ולמידה על טכניקות התחמקות של תוכנות זדוניות היא הצעד הראשון בהגנה מפניהן. מסרים הממוקדים בהשלכות החיוביות של ההתנהגות הראויה עשויים להיות יעילים ומשכנעים יותר ממסרים המדגישים את ההשלכות השליליות שינבעו מחוסר תשומת לב לאבטחת המידע טענו אנדרסון ואגרוול (Anderson & Agarwal, 2010). ההודעות הנפוצות יותר, המתמקדות בהשלכות השליליות שינבעו מחוסר תשומת לב לאבטחת

המידע נמצאו לא מועילות. לפיכך, כדי להטמיע תרבות הכוללת מודעות לאבטחת מידע יש להתמקד ביתרונות שמהם ייהנו משתמשים שיבחרו בבטיחות במקום בהשלכות השליליות של בחירות אחרות. מסרים חיוביים משפיעים על הרגשת המסוגלות העצמית של משתמשי הקצה ומתוך כך על נכונותם להשתמש באמצעי הגנה לאבטחת המידע האישי שלהם. סטיוארט ולאסי (Stewart, G. & Lacey, 2012) אף הוסיפו שבחינוך לאבטחת המידע עבור תלמידי בתי הספר חשוב לא רק לדבר על ההשלכות של אי-הקפדה על אבטחת המידע אלא גם לתרום לתלמידים ידע חיוני על אבטחה זו. ההנחה היא שידע מוגבר יוביל בהכרח לשיפור בהתנהגות הקשורה באבטחה (Stewart, G. & Lacey, 2012). נקודה חשובה נוספת שמעלים שיליאר ופנג (Shillair & Meng, 2017) היא שבתוכניות החינוך לאבטחת מידע יש להתמקד בפרט כאינדיבידואל ולא להתייחס אליו רק כחלק מקבוצה.

הגורם האנושי הוא אחד הגורמים המשמעותיים ביותר בכל הנוגע לאבטחת מידע, טוענים טסוהו ושותפיו (Tsohou et al., 2015). גם המורים והתלמידים בקבוצות המיקוד העריכו את הגורם האנושי כאחד הגורמים המאיימים על המידע: "גם אם אנשים יודעים שצריך להיזהר, אנשים טועים, ועל זה בונים ההאקרים", טען אחד התלמידים. על פי דוח מקאפי (McAfee Labs, 2017b), ההגנה החשובה ביותר מפני זיהומים של תוכנות זדוניות היא המשתמשים עצמם. המשתמשים חייבים להיות מודעים לסיכונים הכרוכים בהורדה של יישומים שמגיעים ממקורות שעלולים להיות מסוכנים ובהתקנתם. החשיבות של העלאת המודעות לנושא אבטחת המידע עולה גם ממחקר האורך שערכו אים ובסקוויל (Im & Baskerville, 2005), שהראו שאחוז נכבד מהפרצות באבטחה נובע מטעויות אנוש ולאו דווקא מפריצה מכוונת, ולכן לא די בהגנה מפני פגיעות מכוונות. סוגיית ההגנה מפני טעויות אנוש הייתה ונותרה אחת הסוגיות המשמעותיות ביותר בכל הנוגע למערכות אבטחת מידע.

מתוך הממצאים שהועלו עד כה עולה הצורך בפיתוח מודל חינוכי-פדגוגי שמטרתו להביא לשינוי תרבותי בבית הספר, להטמעת המודעות לאבטחת המידע ולטיפוח כלים להכוונת בני הנוער לזהירות, לאבטחה ולשמירה על המידע על ידי צוותי החינוך הבית-ספריים.

חשיבות המחקר ותרומתו, מגבלות המחקר והמלצות לעתיד

חשיבותו של המחקר נעוצה בצורך בהעלאת המודעות לאבטחת מידע. המחקר מספק ערוץ נוסף להבנת השונות בין תהליכי קבלת ההחלטות של מתבגרים ומבוגרים לגבי אבטחת מידע. מהמחקר עולה הצורך לעודד את שילובו של נושא אבטחת המידע בתוכנית הלימודים כחלק מהמיומנויות

הנדרשות במאה ה-21. תוצאות המחקר ומסקנותיו משמשות בסיס תיאורטי ואמפירי לבנייתן של תוכניות חינוכיות ופדגוגיות המתחשבות בשונות של הפרטים.

מגבלות המחקר

המחקר הנוכחי נערך בקרב תלמידי בתי ספר תיכוניים, צעירים בגיל 15–18 ואת מוריהם. מכאן שלא נבדקה אבטחת המידע בקרב ילדים צעירים יותר שגם הם משתמשים באינטרנט וברשתות החברתיות (בזק, 2017).

המלצות לעתיד

א. מחקר עתידי נוסף יכול לבחון את המודעות לאבטחת מידע בחתכי גיל צעירים יותר. כיוון מחקר אפשרי נוסף הוא ביצוע המחקר בתוך מסגרת משפחתית. ניתן לבדוק את הטמעת חשיבות אבטחת המידע כבר ברובד החינוך הביתי הבסיסי לכישורי חיים שעל גביו מוסיפה מערכת החינוך להשלמת ההתנהלות התרבותית של המתבגר.

ב. מחקר עתידי יוכל לבחון את השפעת הגיל והוותק של המורים על מוכנותם לאבטחת מידע ועל יכולתם לחנך לכך את תלמידיהם.

ג. ההמלצות של מחקר זה כוללות גם הנחיות לבתי הספר ולצוותים החינוכיים כיצד להוביל שינוי תרבותי בין כל באי בית הספר: הנהלת בית הספר, צוותי ההוראה, העובדים, התלמידים וההורים, וזאת כדי שהמסר של אבטחת המידע יעמוד כל הזמן לנגד עיני קהילת המשתמשים (Harris et al., 2014), ותרבות אבטחת המידע תהפוך לתרבות הארגונית של בתי הספר.

ד. על המורים לקיים דושיח עם התלמידים בבית הספר בנושא אבטחת המידע. לשם כך על המוסדות להכשרת מורים ליצור מודלים המשלבים ידע עיוני וטכני בנושא אבטחת מידע בתוכניות הלימודים ולהכשיר את המורים להוראת נושאים אלה (Pusey & Sadera, 2012).

ה. יחד עם זאת, מכיוון שבמקרים רבים לקבוצת השווים השפעה גדולה יותר מזו של המורים והמבוגרים (van Hoorn et al., 2016), כדאי גם לבנות מנהיגות עצמית של התלמידים שתקיים דיאלוג והסברה בנושא. זהו נושא למחקר נוסף שמהמלצותיו תתגבש דרך פעולה ליישום רעיון מעין זה.

מקורות

בזק (2017). *מצב האינטרנט בישראל לשנת 2017*. אוחזר מתוך https://www.bezeq.co.il/gallerypress/27_11_2017

בן שאול, ד' וגיבסון, ע' (2003). קבוצות מיקוד. בתוך א' קפלן (עורך), *חוקרים מדברים, מחקרי שוק וייישומם בשוק הישראלי* (עמ' 41 – 47). תל-אביב: גלובוס הספרייה.

משרד החינוך (2011), . *חוזר מנכ"ל אתיקה ומוגנות ברשת*. מנהל תקשוב וטכנולוגית המידע. אוחזר מתוך http://cms.education.gov.il/EducationCMS/Applications/Mankal/EtsMedorim/9/9-4/HoraotKeva/K-2012-4-1-9-4-10.htm

שקדי, א' (2003). *מילים המנסות לגעת: מחקר איכותני – תאוריה וייישום*. תל אביב, רמות.

Aharony, N. (2016). Relationships among attachment theory, social capital perspective, personality characteristics, and Facebook self-disclosure. *Aslib Journal of Information Management*, *68*(3), 362–386. doi.org/10.1108/AJIM-01-2016-0001

Aharony, N. (2014). The effect of personal and situational factors on LIS students' and professionals' intentions to use e-books. *Library & Information Science Research*, *36*(2), 106–113. doi.org/10.1016/j.lisr.2014.01.001

Ahituv, N., Bach, N., Birnhack, M., Soffer, T., & Luoto, L. (2014). New challenges to privacy due to emerging technologies and different privacy perceptions of younger generations: The EU PRACTIS project. *Proceedings of Informing Science & IT Education conference (InSITE)*, *2014*, 1–23.

Al-Jerbie, S. I., & Jali, M. Z. (2014). A second look at the information security awareness among secondary school students. *The International Conference on Information Security and Cyber Forensics* (pp. 88–97). Retrieved from http://sdiwc.net/digital-library/a-second-look-at-the-information-security-awareness-among-secondary-school-students

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*, *34*(3), 613–643.

Antonaci, A., Klemke, R., Stracke, C. M., Specht, M., Spatafora, M., & Stefanova, K. (2017). Gamification to empower information security education. *CEUR Workshop Proceedings*, *1857*, 32–38.

Bouhnik, D., & Deshen, M. (2013). Unethical behavior of youth in the internet environment. *International Journal of Technology, Knowledge & Society, 9(2),* 109-124.

Chai, S., Bagchi-Sen, S., Morrell, C., Upadhyaya, S., & Rao, H.R. (2006). Role of perceived importance of information security: An exploratory study of middle school children's information security behavior. *Issues in Informing Science and Information Technology 3*, 127–135.

Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *Internet and Higher Education*, *14*(1), 44–53. doi.org/10.1016/j.iheduc.2010.03.006

Chou, H. L., & Sun, J. C. Y. (2017). The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers and Education*, *112*, 83–96. doi.org/10.1016/j.compedu.2017.05.003

Cranmer, S., & Selwyn, N. P. (2009). Exploring primary pupils' experiences and understandings of 'e-safety.' *Educational Informational Technology, 14*(2), 127–142. doi.org/10.1007/s10639-008-9083-7

D'Arcy, J., Herath, T., & Shoss, M. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of*

Management Information Systems, *31*(2), 285–318. doi.org/10.2753/MIS0742-1222310210

Defranco, J. F. (2011). Teaching internet security, safety in our classrooms. *Techniques: Connecting Education and Careers. May*, 52–55. Retrieved from http://files.eric.ed.gov/fulltext/EJ925444.pdf

Harris, M. A., Furnell, S., & Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy and Security*, *10*(4), 186–202. doi.org/10.1080/15536548.2014.974429

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories. *ACM SIGMIS Database*, *36*(4), 68–79. doi.org/10.1145/1104004.1104010

Interdisciplinary center for technological analysis and forecasting. (2013). *Privacy - appraising challenges to technologies and ethics*. Retrieve from https://cordis.europa.eu/result/rcn/155446_en.html.

Kajzer, M., Darcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers and Security*, *43*, 64–76. doi.org/10.1016/j.cose.2014.03.003

Krueger R. A., & Casey M. A. (2009). *Focus groups: A practical guide for applied research* (5th ed.). Sage publications.

Lazarus, R. S., & Folkman, S. (1984). *Stress, coping and appraisal.* Springer.

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM - Spyware*, *48*(8), 72–77.

Lenhart, A. (2010). *Teens and mobile phones: Exploring safety issues as mobile phones become the communication hubs for American teens*. Retrieved from Pew Internet & American Life Project at http://www.pewinternet.org/2010/11/09/teens-and-mobile-phones-exploring-safety-issues-as-mobile-phones-become-the-communications-hub-for-american-teens/

McAfee. (2010). *The secret online lives of teens*. Retrieved from http://promos.mcafee.com/en-US/PDF/lives_of_teens.pdf

McAfee. (2014), Teens' online behavior can get them in troubles. Retrieved from https://securingtomorrow.mcafee.com/consumer/family-safety/teens-and-screens

McAfee Labs. (2017a). *McAfee labs quarterly threat report April 2017.* Retrieved from https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

McAfee Labs. (2017b). McAfee labs threats report. *McAfee labs report.* 1–60. Retrieved July, 21, 2017 from https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151–156. doi.org/10.1016/j.chb.2016.11.065

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, 47–67. doi.org/10.1080/15536548.2013.10845672

Moreno, M. A., Egan, K. G., Bare, K., Young, H. N., & Cox, E. D. (2013). Internet safety education for youth: stakeholder perspectives. *BMC Public Health*, *13*(1), 543. doi.org/10.1186/1471-2458-13-543

O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, *127*(4), 800–804. doi.org/10.1542/peds.2011-0054

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center Internet, Science & Technology*. Retrieved from http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. doi.org/10.1016/j.cose.2013.12.003

Prensky, M. (2001). Digital natives, digital immigrants part one. *On the Horizon, 9*(5), 1–6.

Purkait, S., & Das, S. (2017). Exploring the password habits of youth in Asia, *IUP Journal of Information Technology, Hyderabad, 13*(3), 36–56.

Pusey, P., & Sadera, W. (2012). Preservice teacher concerns about teaching cyber ethics, cyber safety, and cyber security: A focus group study. *Society for Information Technology & Teacher Education International Conference, 2012*(1), 3415–3419.

Shay, R., Cranor, L. F., Komanduri, S., Durity, A. L., Huh, P. (Seyoung), Mazurek, M. L., Segreti, S. M., Blase, U,, Lujo, B., Christin, N. (2016). Designing password policies for strength and usability. *ACM Transactions on Information and System Security, 18*(4), 1–34. doi.org/10.1145/2891411

Shillair, R., & Meng, J. (2017). Multiple sources for security: The influence of source networks on coping self- efficacy and protection behavior habits in online safety. *Proceedings of the 50th Hawaii International Conference on System Sciences*, Retrieved from http://hdl.handle.net/10125/41766

Steves, M., & Krol, K. (2014). *Report: Authentication diary study report: authentication diary study*. doi.org/10.60028/NIST.IR.7983

Stewart, D. W., & Shamdasani, P. N. (2014). *Focus groups: Theory and practice* (3rd ed.). Sage.

Stewart, G., & Lacey, D. (2012). Death by a thousand facts. *Information Management & Computer Security*, *20*(1), 29–38. doi.org/10.1108/09685221211219182

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers and Security*, *52*, 128–141. doi.org/10.1016/j.cose.2015.04.006

Van Hoorn, J., van Dijk, E., Meuwese, R., Rieffe, C., & Crone, E. A. (2016). Peer influence on prosocial behavior in adolescence. *Journal of Research on Adolescence*, *26*(1), 90–100. doi.org/10.1111/jora.12173

Velki, T., Solic, K., Gorjanac, V., & Nenadic, K. (2017). Empirical study on the risky behavior and security awareness among secondary school pupils. validation and preliminary results. *Information and Communication Technology, Electronics and Microelectronics*. doi.org/10.23919/MIPRO.2017.7973620

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7. doi.org/10.1089/cyber.2014.0179

Woon, I. M. Y., Tan, G. W. & Low, R. T. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*. Retrieved from http://dmlab.mis.ttu.edu.tw/conference/2005-ICIS_2005/SA03.pdf

Yılmaz, R., Karaoğlan-Yılmaz, F. G., Öztürk, H. T., & Karademir, T. (2017). Examining secondary school students' safe computer and internet usage awareness: An example from Bartın province. *Pegem Eğitim ve Öğretim Dergisi, 7*(1), 83–114. doi.org/10.14527/pegegog.2017.004