

דוח תוצאות סקר  
סקר עסקים קטנים ובינוניים

שכיחות תקיפות סייבר בעסקים ואופני  
ההתגוננות 2023

אוקטובר 2023

לשאלות והערות על מחקר הערכה זה ניתן לפנות לעורך המחקר, ד"ר ניר בן אהרון,  
מנהל תחום מחקר, מדיניות וקשרים בין לאומיים בסוכנות לעסקים קטנים ובינוניים  
[nir.benaharon@economy.gov.il](mailto:nir.benaharon@economy.gov.il)

## תקציר מנהלים

דוח זה מבוסס על סקר שביצעה הסוכנות לעסקים קטנים ובינוניים בשנת 2023 בקרב 902 עסקים במטרה לבחון מאפיינים שונים של מצב העסקים בשנה זו. בין השאלות נשאלו העסקים האם העסק נחשף למתקפת סייבר בשנה האחרונה, מה הייתה עצמת הפגיעה, ומה אופני ההתגוננות של עסקים מפני מתקפות כאלו. 48% מהעסקים השיבו שהם משתמשים באמצעי התגוננות מתקופות סייבר, ו-5% מהעסקים השיבו שהם סבלו בשנה האחרונה ממתקפת סייבר, חמישית מהם (20%) גם נפגעו קשות ממתקפה זו.

מבין העסקים שנחשפו למתקפת סייבר, השכיחות הגבוהה ביותר היא של עסקים קטנים, בגודל 5 – 20 מועסקים (11% נחשפו למתקפה), ושל עסקים בענפי התעשייה (10% נחשפו).

מבין 48% העסקים שמשתמשים באמצעי התגוננות, 18% משתמשים באמצעי התגוננות אחד, 7% משתמשים בשני אמצעי התגוננות, ו-23% משתמשים בשלושה אמצעי התגוננות או יותר. אמצעי ההתגוננות השכיחים ביותר הם ביצוע גיבויים תקופתיים ושימוש בתוכנות הגנה מובנות.

בניתוח אשכולות שנעשה למאפייני התגוננות, נמצאו שבעה אשכולות של מאפיינים. באשכול 1 נכללים עסקים שאינם נוקטים כלל באמצעי התגוננות, באשכול 7 נכללים עסקים שעושים שימוש במגוון גדול של אמצעי התגוננות. בטווח הביניים מצויים עוד אשכולות עם מאפיינים שונים של התגוננות. השיעור הגבוהה ביותר של עסקים שהותקפו נמצא באשכול 5 (19.2%) אשכול בו אמצעי ההתגוננות הכמעט בלעדי הוא ספקים חיצוניים שמומחים להגנת סייבר. יכול להיות שאשכול זה מתאפיין בעסקים רבים שעברו תקיפת סייבר ופנו לספקים חיצוניים בעקבות התקיפה.

מנתוני המחקר עולה שכ-7,000 עסקים קטנים ובינוניים נפגעים מדי שנה פגיעה משמעותית ממתקפות סייבר. בהנחה שמתקפת סייבר ממוצעת על עסק קטן גורמת נזק של 100 אלף שקל (מבוסס על הערכה של מערך הסייבר) ומיישמים על כמות העסקים שמתקפת, יוצא שעלות המתקפות הללו למשק היא כ-700 מיליון שקל בשנה.

## תוכן העניינים

4.....	רקע
4.....	שיעור העסקים שנחשפו למתקפת סייבר בשנה האחרונה ומידת הנזק שנגרם
5.....	האמצעים בהם נוקטים עסקים כדי להתמודד עם מתקפות סייבר
6.....	האמצעים בהם נוקטים עסקים כדי להתמודד עם מתקפות סייבר לפי גודל עסק
8.....	האמצעים בהם נוקטים עסקים כדי להתמודד עם מתקפות סייבר לפי ענף
9.....	מיפוי עסקים בהתאם לרמות ההתגוננות שלהם מפני מתקפות סייבר
13.....	נספחים
13.....	נספח 1: מתודולוגיה
16.....	נספח 2: האמצעים בהם נוקטים עסקים
18.....	נספח 3 – שאלון הסקר

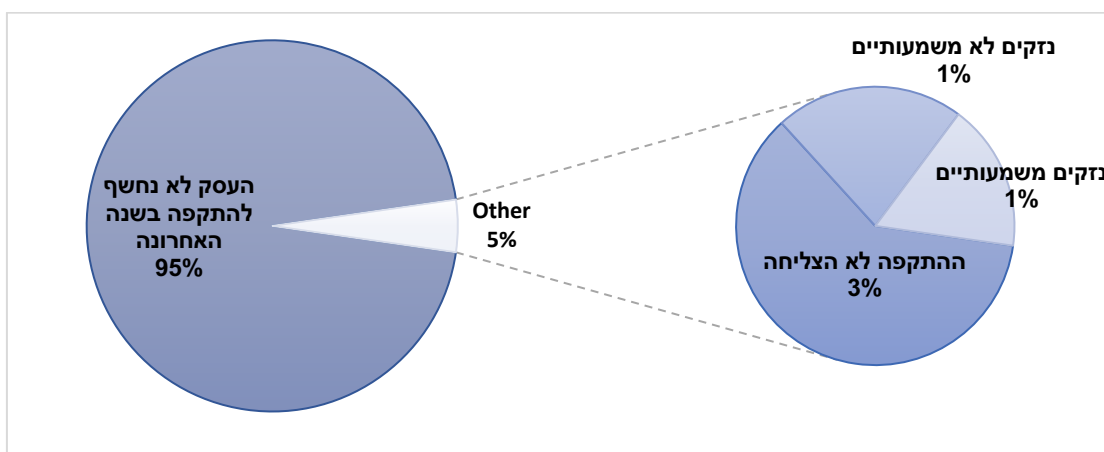
הסוכנות לעסקים קטנים ובינוניים, במשרד הכלכלה, מבצעת מדי שנה סקר כללי על מצבם של עסקים קטנים ובינוניים במטרה לדייק את המדיניות בנוגע למגזר העסקים הקטנים והבינוניים בישראל. הסקר הנו סקר טלפוני שנערך בחודשים יוני-יולי 2023 בקרב 902 עסקים בגודל של עד 100 מועסקים. ב-2023 נשאלו העסקים, בין השאר, האם העסק נחשף למתקפת סייבר בשנה האחרונה, מה הייתה עצמת הפגיעה ומה אופני ההתגוננות של עסקים מפני מתקפות כאלו.

### שיעור העסקים שנחשפו למתקפת סייבר בשנה האחרונה ומידת הנזק שנגרם.

המשיבים בסקר נשאלו האם העסק נחשף למתקפת סייבר בשנה האחרונה, 5% מכלל העסקים השיבו בחיוב. עסקים שהשיבו בחיוב נשאלו עד כמה התקיפה הזיקה להמשך פעילות העסק. 5% מהעסקים ענו שהותקפו, וחמישית מהם (20%) דיווחו שהתקיפה גרמה להם לנזקים משמעותיים.

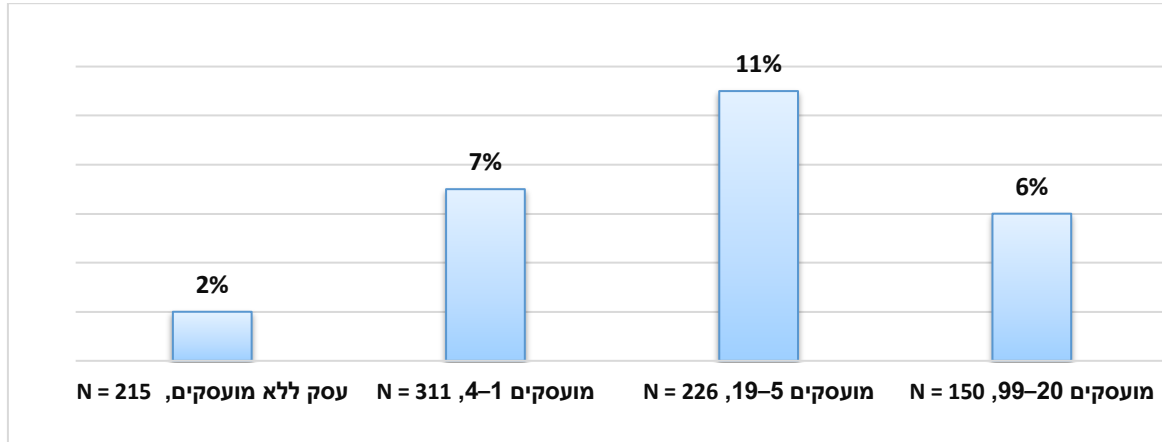
חשוב להבין שבשנת 2023 יש כ-650 אלף עסקים במגזר העסקי, והמשמעות היא שקרוב ל-33 אלף עסקים עברו תקיפה בשנה האחרונה וכ-7 אלף עסקים נפגעו פגיעה משמעותית.

תרשים 1: שיעור העסקים שנחשפו למתקפת סייבר בשנה האחרונה



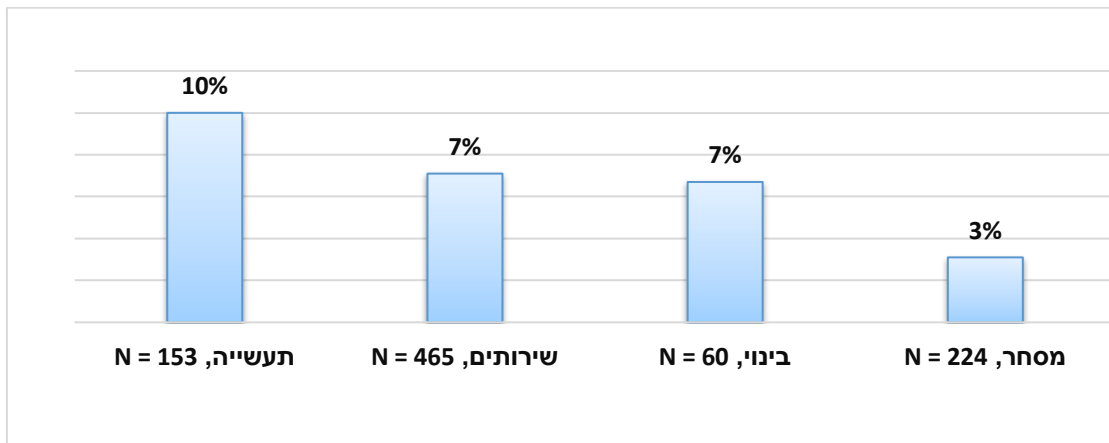
העסקים שנחשפים בשכיחות הגבוהה ביותר למתקפות סייבר הם עסקים עם 5-19 מועסקים (11% דיווחו על פגיעה), והעסקים עם שיעורי החשיפה הנמוכים ביותר למתקפות הם עסקים ללא מועסקים (2% נפגעים).

**תרשים 2 : שיעור העסקים שנחשפו למתקפת סייבר בשנה אחרונה, לפי גודל עסק**



ועסקים בתחומי התעשייה נחשפים בשיעור הגבוה ביותר למתקפות סייבר (10%) ואילו עסקים בתחום המסחר הם העסקים עם שיעורי התקיפה הנמוכה ביותר (3%).

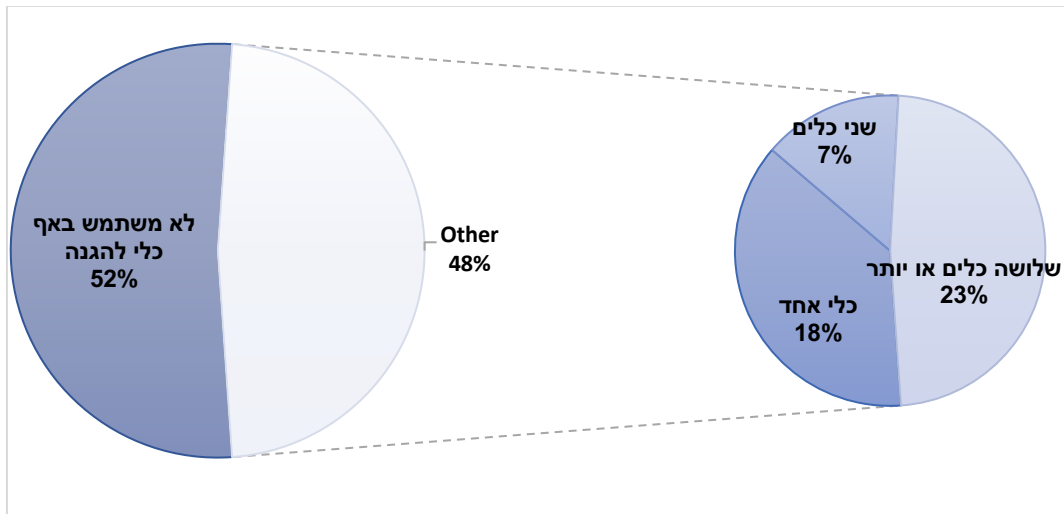
**תרשים 3 : שיעור העסקים שנחשפו למתקפת סייבר בשנה אחרונה, לפי ענף**



**האמצעים בהם נוקטים עסקים כדי להתמודד עם מתקפות סייבר**

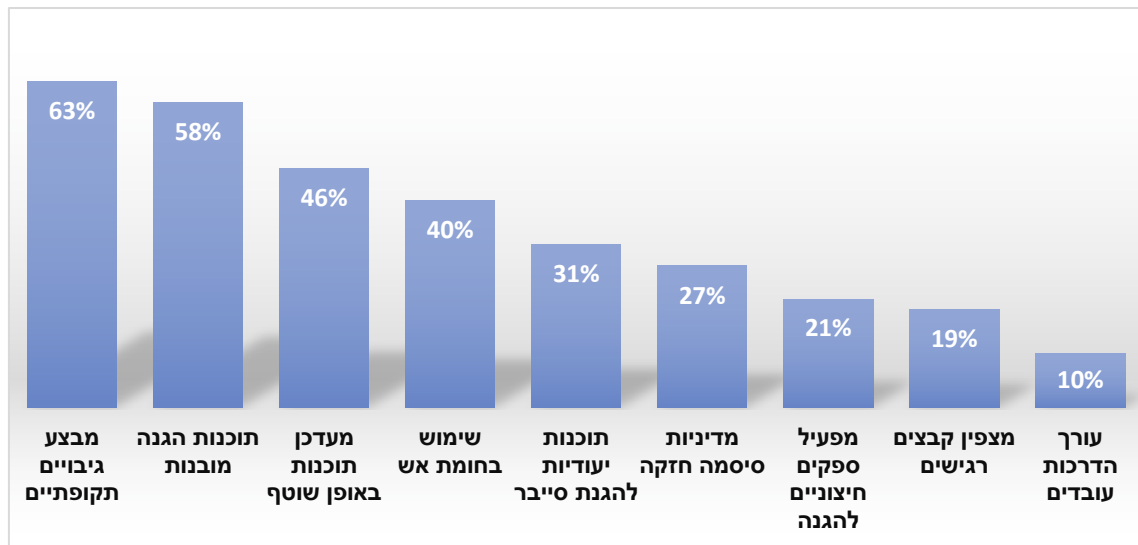
עסקים נשאלו מהם האמצעים בהם הם נוקטים כדי להתגונן ממתקפות סייבר, והתבקשו לבחור מבין תשע קבוצות של אמצעי התגוננות. כפי שניתן לראות בתרשים 4, 52% מהעסקים ציינו שאינם משתמשים באף אחד מהאמצעים כדי להתגונן ממתקפות סייבר, 18% ציינו אחד מהאמצעים בלבד, 7% ציינו שני אמצעים ו-23% ציינו שלושה אמצעים או יותר.

#### תרשים 4: מספר האמצעים בהם עסקים נוקטים כדי להתגונן ממתקפת סייבר



מבין העסקים שמשתמשים לפחות באמצעי אחד להגנה מפני מתקפות סייבר, האמצעי השכיח ביותר הוא ביצוע גיבויים תקופתיים כך שבמקרה שבו מסיבה כלשהיא המידע יחסם או ימחק ניתן יהיה לשחזר אותו (63% מהמשתמשים דיווחו על שימוש בו). אמצעי נוסף הוא שימוש בתוכנות הגנה מובנות (58%). בין האמצעים המעט פחות שכיחים: עדכון תוכנות באופן שוטף (46%) ושימוש בחומת אש (40%).

#### תרשים 5 : אחוז השימוש באמצעים שונים להגנה מפני מתקפות סייבר

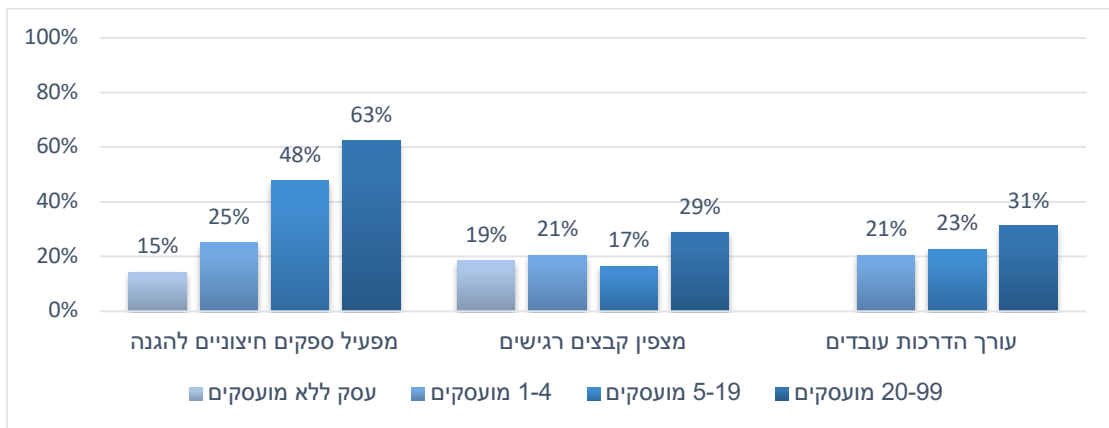
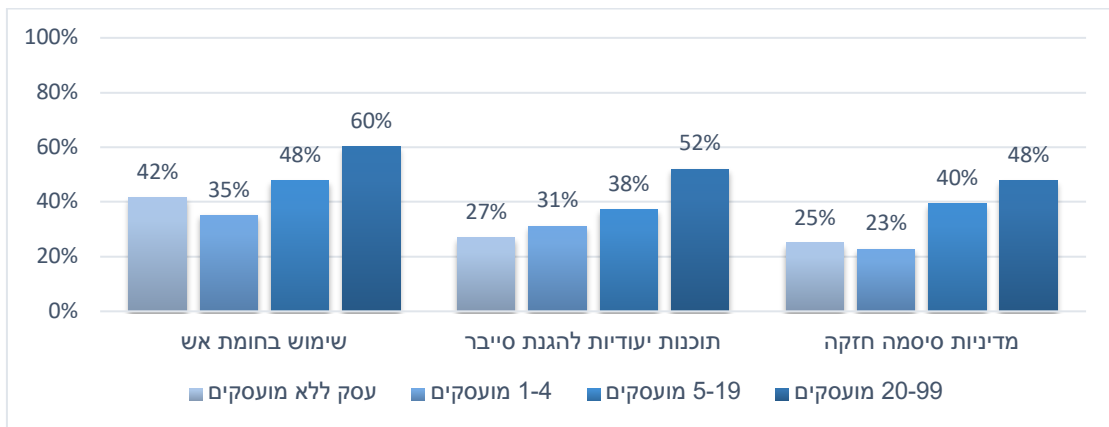
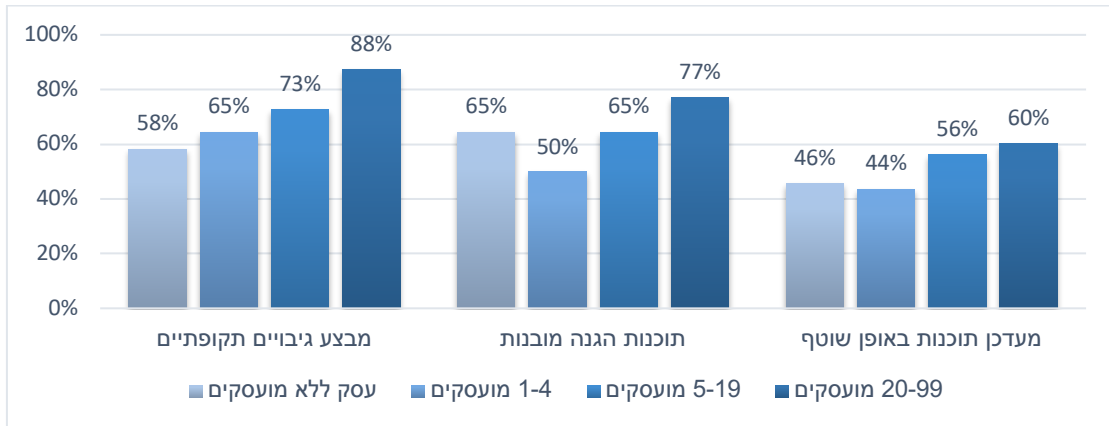


#### האמצעים בהם נוקטים עסקים כדי להתמודד עם מתקפות סייבר לפי גודל עסק

כאמור, מבין העסקים שמשתמשים לפחות באמצעי אחד להגנה מפני מתקפות סייבר, האמצעי השכיח ביותר להתמודדות עם התקפות סייבר שעסקים ציינו הוא ביצוע גיבויים תקופתיים, יש קשר חיובי בין גודל העסק לשיעור העסקים שמבצעים גיבויים תקופתיים. שימוש בחומת אש,

תוכניות יעודיות להגנת סייבר והפעלת ספקים חיצוניים להגנה הם בין האמצעים שעסקים עם עובדים רבים נוטים לעשות בהם שימוש.

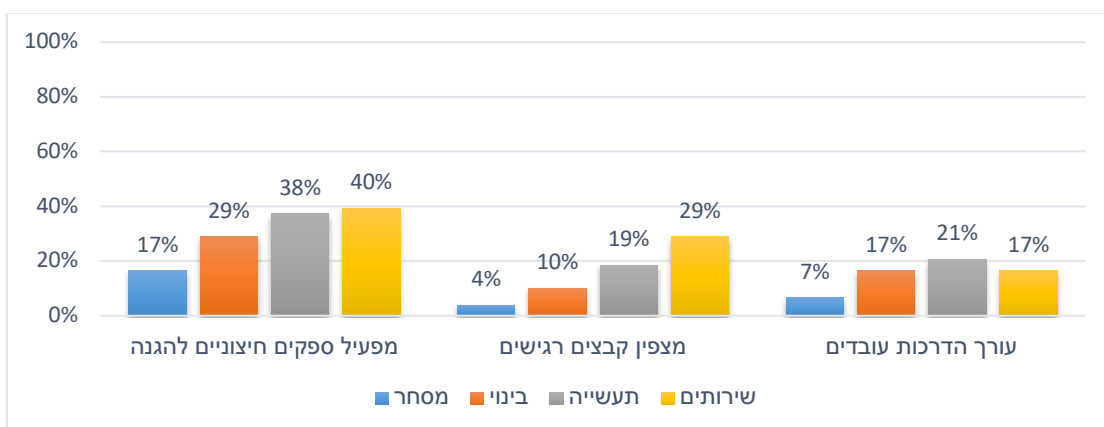
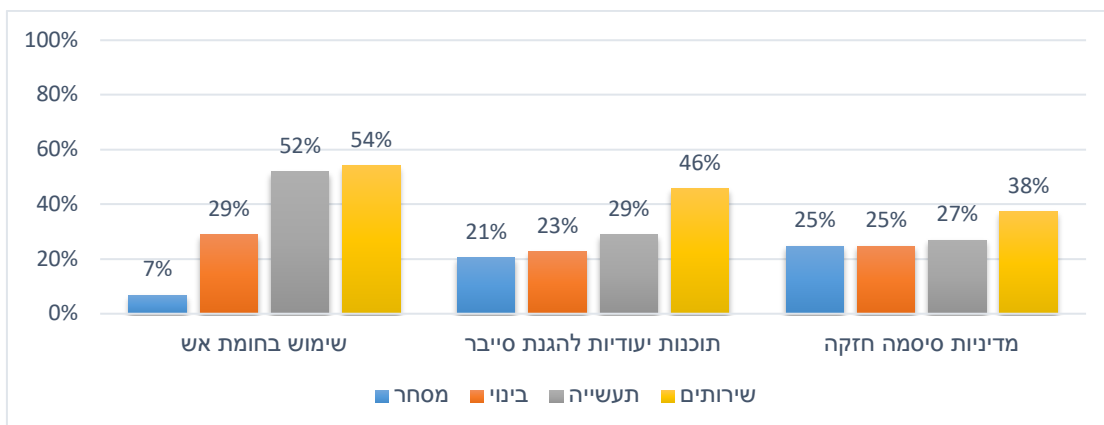
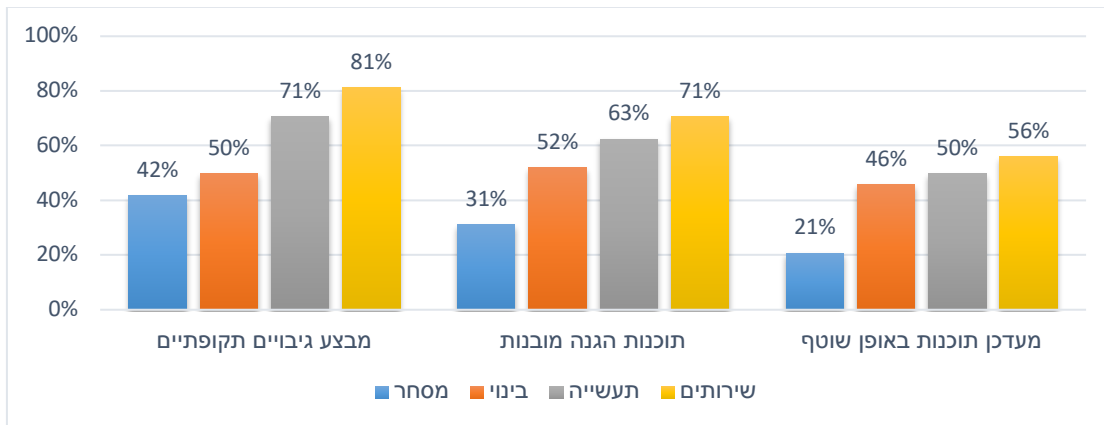
**תרשים 6: האמצעים בהם נוקטים העסקים בפילוח לפי גודל עסק**



## האמצעים בהם נוקטים עסקים כדי להתמודד עם מתקפות סייבר לפי ענף

ענף השרותים הינו הענף בו שיעור השימוש הגבוה ביותר בכל האמצעים הקיימים להתמודדות עם מתקפות הסייבר בעוד שענף המסחר הינו הענף בו שיעור השימוש הנמוך ביותר.

### תרשים 7: האמצעים בהם נוקטים העסקים בפילוח לפי ענף כלכלי





## מיפוי עסקים בהתאם לרמות ההתגוננות שלהם מפני מתקפות סייבר

בכדי לנסות למצוא מכנה משותף בין עסקים שונים בבחינת סוגי האמצעים בהם עסקים עושים שימוש כדי להתגונן ממתקפות סייבר ביצענו לתוצאות הסקר ניתוח אשכולות<sup>1</sup>. מטרת החלוקה לאשכולות הייתה למצוא דפוסים חבויים בנתוני העסקים ולבחון האם עסקים מסויימים נוהגים בדפוסים ספציפיים. התקבלו 7 אשכולות בעלי מאפיינים שונים: אשכול 1 בו כלל העסקים דיווחו שאינם עושים שימוש באף אמצעי להתגוננות במתקפות סייבר ומנגד אשכול 7 בו מצויים עסקים שעושים שימוש במגוון אמצעים להתמודדות עם מתקפות סייבר (9-4 אמצעים שונים). בטווח הביניים מצויים עוד אשכולות עם מאפיינים שונים: אשכול 4 מכיל עסקים שעושים שימוש ב-2-5 אמצעים להתגוננות כאשר 100% מהם ציינו תוכנות מובנות בצידוד המחשוב, ובנוסף לכך הם בוחרים בעיקר בחלק מהאמצעים הבאים: גיבויים תקופתיים, עדכון תוכנות שוטף וחומת אש. באשכול 6 100% מהעסקים מבצעים עדכון תוכנות באופן שוטף, באשכול 5 100% מהעסקים מעסיקים ספקים חיצוניים שמומחים להגנת סייבר וכמעט אינם פועלים בדרכים נוספות. באשכול 3 כלל העסקים משתמשים בתוכנות הגנה מובנות בלבד ובאשכול 2 עסקים שמתגוננים בעזרת אמצעי אחד בלבד במחצית המקרים מדובר על גיבויים תקופתיים ובשאר המקרים הם משתמשים בעיקר בתוכנות הגנה מובנות או בחומת אש.

מתרשים 8 ניתן ללמוד שיש מנעד של פעולות שעסקים עושים בנוגע להגנה מפני מתקפות סייבר החל מכאלו שאינם עושים אף פעולה ועד לעסקים שעושים מספר ניכר של פעולות במקביל. היקף פעולות ההגנה המבוצעות תלוי בסוג העסק, מידת הסיכון ורמת הנזק שעלול להיגרם לעסק ממתקפה.

מעניין לציין שבקבוצה הראשונה שבה עסקים אינם עושים פעולות הגנה, שיעור העסקים שנחשפו למתקפת סייבר בשנה האחרונה הוא הנמוך ביותר ועומד על פחות מ-2%. בקבוצת העסקים שעושה הכי הרבה פעולות הגנה שיעור המתקפות עמד על 7.5% בעוד שבאשכול 4 שהוא רמה אחת פחות מאשכול 7 מבחינת כמות הפעולות, שיעור המתקפות עמד על 2.6%. השיעור הגבוה ביותר של עסקים שהותקפו נמצא באשכול 5 (19.2%) בו אמצעי ההתגוננות הכמעט בלעדי הוא ספקים חיצוניים שמומחים להגנת סייבר. יכול להיות שבאשכול זה יש עסקים רבים שעברו תקיפת סייבר ופנו לספקים חיצוניים בעקבות התקיפה.

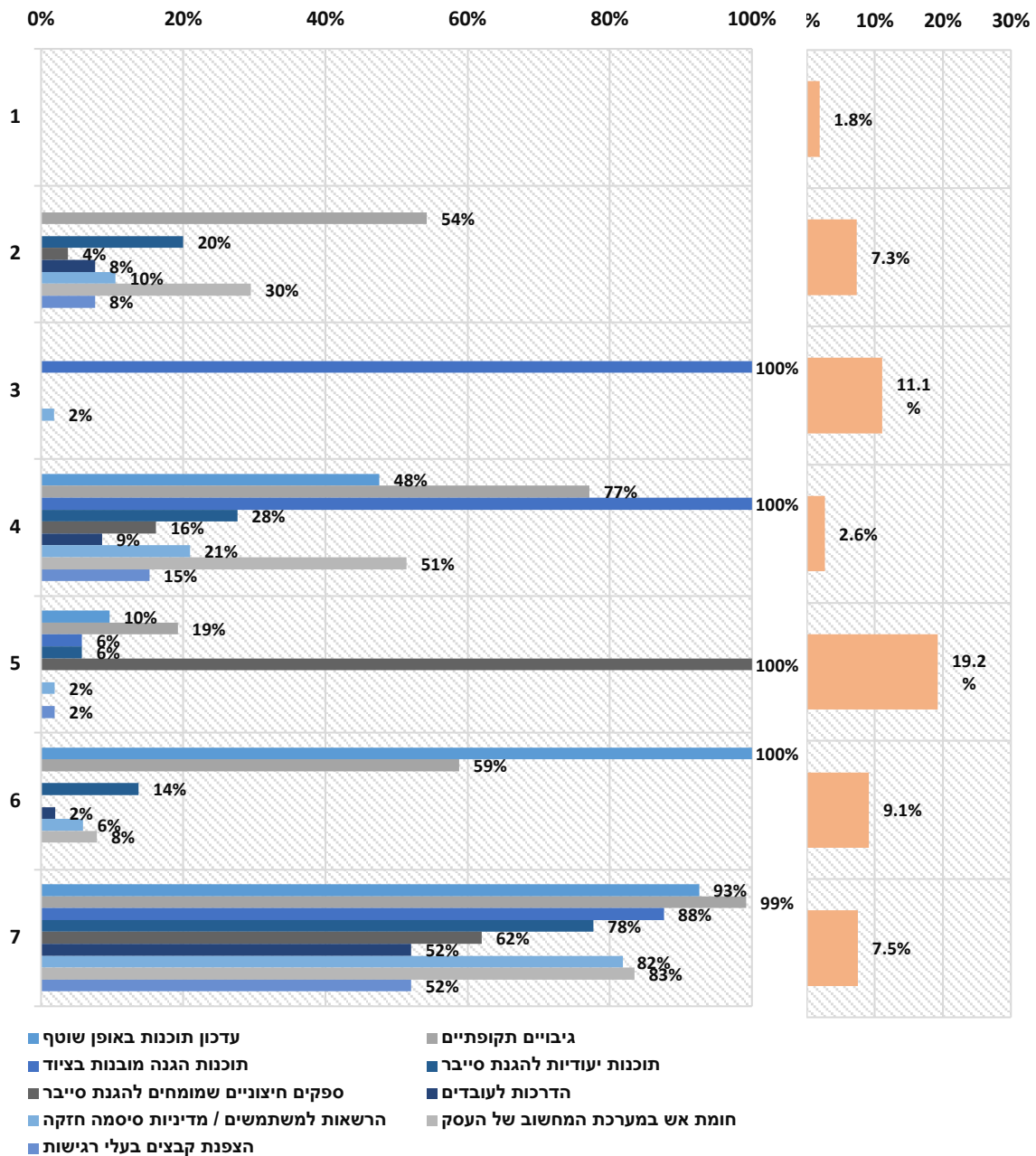
חשוב לציין שמתוך הסקר הנוכחי אי אפשר ללמוד על הקשר בין סוגי ההגנה לסיכוי לתקיפת סייבר מאחר והשאלות לא נשאלו באופן שניתן ללמוד מה קדם למה (התקיפה לאופן ההגנה או להיפך).

---

TwoStep cluster analysis <sup>1</sup>

**תרשים 8: שיעור מתקפות סייבר בשנה האחרונה ושימוש באמצעים שונים להתגוננות**

**שיעור מתקפות סייבר**      **שימוש באמצעים שונים להתגוננות**      **אשכול**



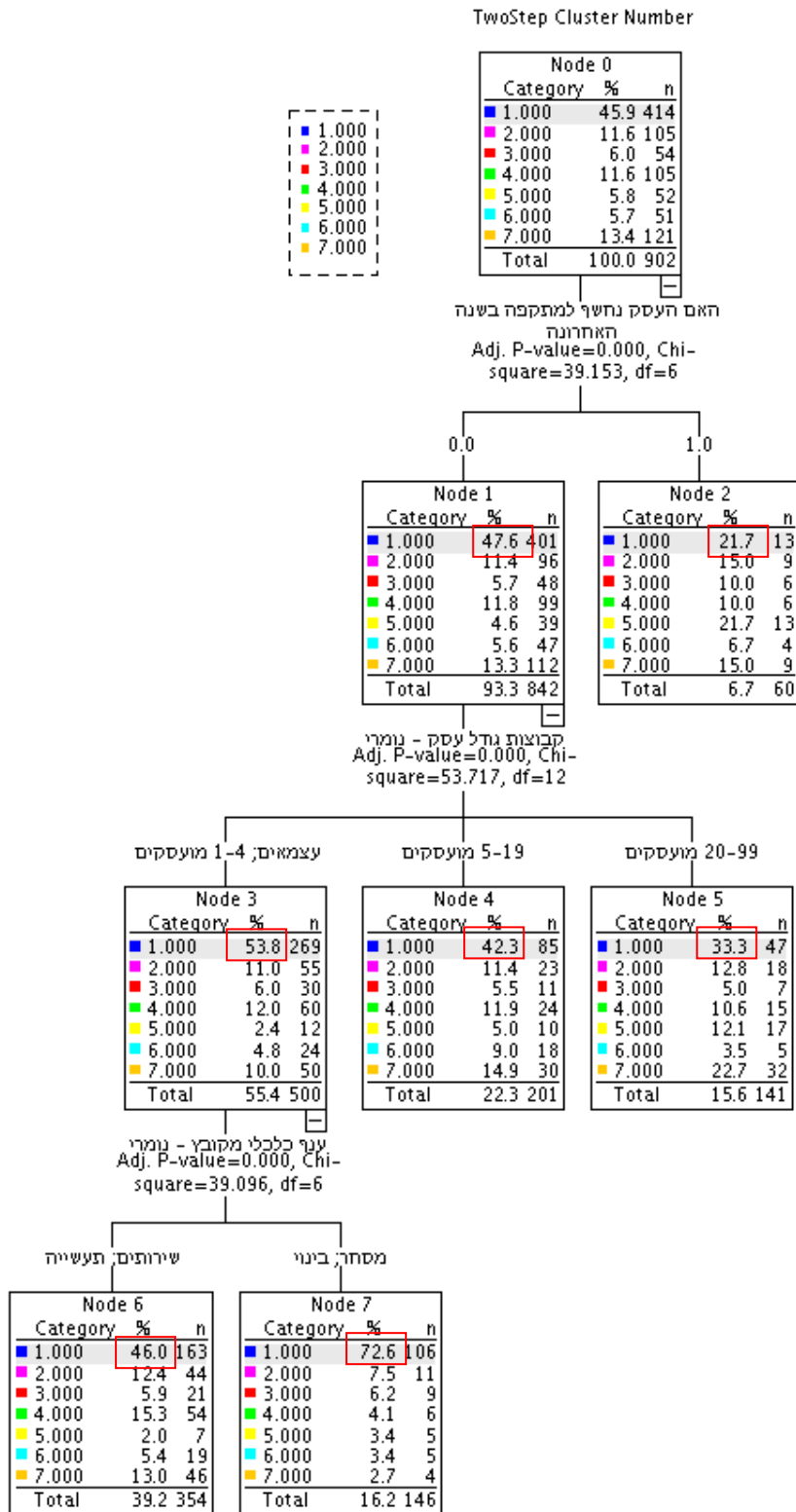
תרשים 9 מראה תוצאה של עץ החלטה לאפיון האשכולות. בתרשים זה ניתן לראות ש-842 עסקים לא נחשפו למתקפת סייבר, 500 מתוכם עסקים שלא מעסיקים עובדים, 354 מהם מתחומי השירותים והתעשייה. בכל אחת מהרמות ניתן לראות את החלוקה בין האשכולות השונים, וכן סימון (בריבוע אדום) של שיעור (%) העסקים באשכול הראשון (אלו שלא נוקטים באמצעים נגד תקיפות סייבר). בפירוט העץ המסומן בתרשים 9 מתארים הענפים שנמצאו מובהקים בנייתו הסטטיסטי של האשכולות.

ניתן לראות מהתרשים ששיעור גבוה מהעסקים אינו נוקט באמצעי זהירות מפני תקופות סייבר, אמצעים שגם מערך הסייבר יצא בהמלצות שהעסקים צריכים ליישם (לדוגמה במסמך של מערך הסייבר: "7 כללי ברזל להגנת סייבר עבור עסקים קטנים ובינוניים").

מיישום נתוני המחקר על כלל העסקים במשק עולה שכ-7,000 עסקים קטנים ובינוניים נפגעים מדי שנה פגיעה משמעותית ממתקפות סייבר. מהבדיקה שתוארה למעלה של מערך הסייבר עולה שעלות ממוצעת של פגיעה ממתקפת סייבר בעסק קטן ובינוני היא כ-800 אלף שקל. גם אם מניחים שהעסקים שנבדקו במחקר זה קטנים יותר מאלו שעליהם ניתנה ההערכה של מערך הסייבר, והפגיעה בהם בעקבות מתקפת סייבר קטנה יותר, לצורך ההנחה אנחנו לוקחים הערכה של שמינית מגובה הפגיעה שהעריכו במערך הסייבר (100 אלף שקל פגיעה לעסק במקום 800 אלף) ומיישמים על כמות העסקים שמוקפת, יוצא שעלות המתקפות הללו למשק היא כ-700 מיליון שקל בשנה.

במיוחד עולה בעיה בקרב עסקים שגודלם 5 – 19 מועסקים. כ-11% מהעסקים בגודל הזה נחשפים למתקפות סייבר. נראה שיכול להיות שהמודעות בקרב עסקים בגודל הזה לשימוש באמצעי התגוננות נמוכה יותר (ביחס לסיכון) ולכן הם נחשפים יותר למתקפות סייבר מאשר קבוצות גודל אחרות של עסקים (לדוגמה, יותר מקבוצת הגודל של 20 – 99 מועסקים, ויותר מקבוצת הגודל של 1 – 4 מועסקים).

תרשים 9 : עץ החלטה לאפיון בהמשך לניתוח האשכולות



## נספחים

### נספח 1: מתודולוגיה

בכדי שאפשר יהיה לבחון הבדלים בין עסקים בגדלים שונים, ובין ענפי כלכלה שונים, ניתן ייצוג יתר לענפי מסחר, ייצור ובנייה, וזאת על חשבון ענף השרותים. כמו כן בסקר ניתן ייצוג יתר לעסקים הקטנים (5-19) ולעסקים הבינוניים (20 – 100 מועסקים) על חשבון העסקים הזעירים (0 – 4). כך שהמדגם בסקר לא היה מייצג וכדי שאפשר יהיה להסיק ממנו בוצע תיקון לייצוגיות העסקים (בחישובים משוקללים בלבד) לפי קבוצות גודל העסק (מספר מועסקים כפי שמדווח ע"י בעלי העסקים עצמם) באופן הבא:<sup>2</sup>

---

<sup>2</sup> במקרים בהם הנסקר לא השיב על מספר מועסקים, המידע הושלם ממאגר הנתונים של הסוכנות לעסקים קטנים ובינוניים.

התפלגות המדגם ותיקון לקבלת תשובות מייצגות

סה"כ	בנוי	מסחר	שרותים	תעשייה וייצור	
					מספר משיבים במדגם
215	12	33	148	22	עצמאים
311	24	82	167	38	1-4
226	13	66	91	56	5-19
150	11	43	59	37	20+
902	60	224	465	153	סה"כ
					התפלגות במדגם
0.238	0.013	0.037	0.164	0.024	עצמאים
0.345	0.027	0.091	0.185	0.042	1-4
0.251	0.014	0.073	0.101	0.062	5-19
0.166	0.012	0.048	0.065	0.041	20+
1.000	0.067	0.248	0.516	0.170	סה"כ
					התפלגות באוכלוסייה
0.575	0.053	0.067	0.438	0.017	עצמאים
0.307	0.052	0.068	0.171	0.017	1-4
0.095	0.017	0.024	0.046	0.008	5-19
0.023	0.002	0.005	0.013	0.003	20-99
1.000	0.124	0.164	0.668	0.044	סה"כ
					מקדם תיקון
2.4125	4.0211	1.8224	2.6687	0.6965	עצמאים
0.8915	1.9433	0.7451	0.9251	0.3953	1-4
0.3787	1.1729	0.3341	0.4522	0.1277	5-19
0.1365	0.1769	0.1029	0.1951	0.0699	20-99
1.0000	1.8681	0.6594	1.2949	0.2620	סה"כ

הסקר הינו סקר טלפוני, שנערך בחודשים יוני-יולי 2023 בקרב 902 עסקים, ושיעורי ההשבה על הסקר עמדו על 11% ראיונות שהסתיימו בהצלחה. התפלגות הסטטוסים העיקריים לאי השבה:

ב- 49% מהמקרים לא הייתה תשובה או היה תפוס, 22% סרבו להשיב על הסקר, 15% היו מספרים שגויים/נתב שיחות או לא רלוונטי ו-2% ביקשו שיחזרו אליהם במועד מאוחר יותר.

#### סיכום ההשבה לסקר

רשומות	%	
7,916	100%	סך הכול
902	11%	השלים סקר
3,877	49%	תפוס/אין מענה
196	2%	ביקש שיתקשרו אליו במועד מאוחר יותר
1,765	22%	סירב
1,176	15%	מספר שגוי/ נתב שיחות. עסק נסגר וכדומה

## נספח 2: האמצעים בהם נוקטים עסקים

האמצעים בהם נוקטים העסקים, בפילוח לפי גודל עסק

p-value <sup>2</sup>	מועסקים -20 N = 150,99	מועסקים -5 N = 19,226	מועסקים -1 N = 311,4	עסק ללא מועסקים, N = 215	
0.032	88%	73%	65%	58%	מבצע גיבויים תקופתיים
0.045	77%	65%	50%	65%	תוכנות הגנה מובנות
0.15	60%	56%	44%	46%	מעדכן תוכנות באופן שוטף
0.039	60%	48%	35%	42%	שימוש בחומת אש
0.033	52%	38%	31%	27%	תוכנות יעודיות להגנת סייבר
0.003	48%	40%	23%	25%	מדיניות סיסמה חזקה
<0.001	63%	48%	25%	15%	מפעיל ספקים חיצוניים להגנה
0.3	29%	17%	21%	19%	מצפין קבצים רגישים
<0.001	31%	23%	21%	2%	עורך הדרכות עובדים



**האמצעים בהם נוקטים העסקים, בפילוח לפי ענף כלכלי**

p-value <sup>2</sup>	N בינוי, <sup>1</sup> = 60	מסחר, N = 1224	שירותים, N = 1465	תעשייה, N = 1153	
<0.001	20%	24%	39%	34%	מבצע גיבויים תקופתיים
0.007	15%	25%	34%	30%	תוכנות הגנה מובנות
0.021	10%	22%	27%	24%	מעדכן תוכנות באופן שוטף
<0.001	3.3%	14%	26%	25%	שימוש בחומת אש
<0.001	10%	11%	22%	14%	תוכנות יעודיות להגנת סייבר
0.1	12%	12%	18%	13%	מדיניות סיסמה חזקה
0.2	8%	14%	18%	19%	מפעיל ספקים חיצוניים להגנה
<0.001	2%	5%	14%	9%	מצפין קבצים רגישים
0.4	3%	8%	10%	8%	עורך הדרכות עובדים

## שאלון – סקר עסקים 2023

פתיח:

שלום, שמי \$[ 202 ]\$ ואני מתקשר/ת מטעם הסוכנות לעסקים קטנים ובינוניים במשרד הכלכלה, האחראית על סיוע לעסקים בישראל.

אפשר לדבר בבקשה עם אחד המנהלים בעסק או בעליו?

- אם העסק ולא אחד מהמנהלים או בעל העסק, יש לבקש אותו ולהקריא מחדש את הפתיח.

- אם זה לא העסק או שלא ניתן להשיג את בעל העסק או המנהל שלו >יש לסיים את השיחה ולציין זאת בנסגר/ אחר.

אנו עורכים מדי פעם סקר קצר ללמידת מצב העסקים על מנת לעזור ולשפר את מצב העסקים. חשוב לציין כי השאלון חסוי ולא יעשה שום שימוש בכל פרט מזהה שלך או של העסק.

תודה על שיתוף הפעולה.

כללי

1. כמה שנים העסק קיים? \_\_\_\_\_ (לסוקר: לענות בשנים).

א. אם העסק קיים עד שנה (סינון – יוצא מהסקר)

2. כמה מועסקים עובדים היום בעסק, **כולל בעלים ומנהלים**? (לסוקר - יש להדגיש שהמספר כולל בעלים / מנהלים, יש לקבל תשובה מספרית בלבד) (ניתן להסתפק באומדן) \_\_\_\_\_.

א. לא יודע (סינון – יוצא מהסקר).

ב. מסרב להשיב (סינון – יוצא מהסקר).

אם מעל 100 עובדים, יש להודות ולסיים את הסקר.

3. האם מצבת העובדים היום בהשוואה למצבת העובדים בשנת 2022?

א. נמוכה יותר

ב. דומה

ג. גבוהה יותר

4. בהשוואה לאותה התקופה בשנה שעברה האם רווחיות העסק:

- א. עלתה
- ב. נשארה דומה
- ג. ירדה
- ד. לא ניתן לדעת
- ה. מסרב

7. האם שקלת לסגור את העסק לצמיתות בשנה האחרונה ?

- א. כן
- ב. לא (עובר לשאלה 7)

8. מה הסיבות שגרמו לך לשקול לסגור את העסק? \_\_\_\_\_

9. מהו החסם העיקרי לדעתך להצלחת העסק שלך? (לסוקר -יש להדגיש שמדובר בחסם העיקרי - תשובה אחת. יש להקריא תשובות א-ו). **תכנות: סדר התשובות משתנה רנדומלי.**

- א. גישה למימון
- ב. מציאת לקוחות
- ג. זמינות כוח עבודה או ניהול מימון
- ד. עומס בירוקרטי (דוגמה לסוקרים: מילוי טפסים, בקשת אישורים)
- ה. עלויות ייצור, חומרי גלם או סחורות
- ו. אין חסם להצלחת העסק <לא להקריא>
- ז. אחר <לא להקריא> \_\_\_\_\_.
- ח. מסרב (לא להקריא).

מי שענה בשאלה 7 א

10. מה הקשיים של העסק בגישה למימון? (אפשר לענות על יותר מתשובה אחת)

- א. אני זקוק להלוואה לעסק, אך אף גורם אינו מאשר לי קבלת הלוואה
- ב. אני זקוק למימון אך נמנע בשל עלויות המימון הגבוהות
- ג. חסרים לי ביטחונות לצורך השגת מימון
- ד. הבנק לא מגדיל לי את מסגרת האשראי
- ה. חסם אחר \_\_\_\_\_

מי שענה בשאלה 7 ג

11. מה הקשיים של העסק מבחינת כח האדם? (אפשר לענות על יותר מתשובה אחת)

- א. תחלופת עובדים גבוהה
- ב. עלויות גבוהות להכשרה של כוח אדם חדש
- ג. קשה להשיג עובדים או מנהלים בשכר המאפשר את רווחיות העסק
- ד. עלויות השכר עלו משמעותית בשנה האחרונה

- ה. קשה להשיג עובדים מקצועיים לסוג העסק שלי  
ו. סיבה אחרת \_\_\_\_\_

מי שענה בשאלה 7 ה

12. מה החסמים של העסק מבחינת עלויות ייצור, חומרי גלם או סחורות? (אפשר לענות על יותר מתשובה אחת)  
א. חומרי הגלם או הסחורות התייקרו בשנה האחרונה באופן משמעותי  
ב. עלויות ייצור אחרות שעלו (חשמל, מים, ארנונה)  
ג. עלויות שכירות ומבנה (כולל דמי ניהול)  
ד. עלויות שילוח גבוהות  
ה. סיבה אחרת \_\_\_\_\_

דיגיטציה

13. האם אתה משתמש בחשבונית דיגיטלית המועברת ישירות לפורטל, למייל או טלפון הלקוח?  
א. כן  
ב. לא (עובר לשאלה 13)

14. מתי התחלת להשתמש בחשבונית דיגיטלית:  
א. בשנה האחרונה  
ב. אחרי תחילת משבר הקורונה  
ג. לפני שהחל משבר הקורונה

ועכשיו אשאל אותך כמה שאלות לגבי מסחר מקוון

15. האם העסק שלך פועל כיום בפלטפורמות הבאות? (להקריא תשובות 1-4. ניתן לענות יותר מתשובה אחת) חשוב להקריא את כל התשובות גם אם עונה לא על הראשונה וחושב שלא רלוונטי עבורו:  
א. חנות מקוונת או פלטפורמת מכירה (למשל, אמזון).  
ב. פעילות שיווקית באינטרנט שאינה מכירה (אתר לצורך מיתוג, דף עסקי, אינסטגרם וכו') (מי שעונה רק על שאלה זו מדלג לשאלה 16).

ג. פלטפורמת דרוג חיצונית שמפנה אלייך (דוגמת: איזי, זאפ, אתר מדרג) (מי שלא ענה תשובה א' מדלג לשאלה 16). למראיין להקריא את הדוגמאות

ד. אחר \_\_\_\_\_ (דלג לשאלה 16).

ה. לא (דלג לשאלה 16).

16. [לעסקים שמפעילים חנות מקוונת] מהו שיעור המסחר המקוון בעסק כיום, מסך המחזור הכללי? (לסוקר: שיעור הכוונה לאחוז, המחזור הכללי הכוונה להכנסה הכוללת)  
לסוקר ללא הקראת תשובות

א. עד 10%

ב. בין 11%-25%

ג. בין 26%-50%

ד. 51%-75%

ה. מעל ל 75%

ו. לא יודע (לא להקריא)

17. [לעסקים שמפעילים חנות מקוונת] שיעור המסחר המקוון של העסק כיום בהשוואה לשנה הקודמת (2022).

א. עלה במידה רבה.

ב. עלה במידה מועטה.

ג. נשאר ללא שינוי.

ד. ירד במידה מועטה.

ה. ירד במידה רבה.

ו. לא היה מסחר מקוון בשנת 2022

ז. לא יודע (לא להקריא)

18. האם בשלוש השנים האחרונות העסק עבר לשימוש באחת או יותר מהמערכות הדיגיטליות הבאות?

א. מערכת לניהול כספים

ב. מערכת לניהול לקוחות

ג. מערכת לניהול הייצור

ד. מערכת לניהול לוגיסטי

ה. מערכת אחרת

ו. לא

19. האם בשנה האחרונה העסק נחשף למתקפה של האקרים? (למשל: הצפנה של המידע על המחשב ובקשות כופר, פריצה לחשבון המייל, השתלטות על המייל, על אתר הפייסבוק וכדומה, השתלטות על הוואטסאפ) כדאי להקריא את הדוגמאות

- א. כן  
 ב. לא (עובר לשאלה 20)  
 20. מה היו הנזקים של ההתקפה?  
 א. ההתקפה לא הצליחה ולא היו נזקים  
 ב. ההתקפה הצליחה, אולם נזקים לא משמעותיים  
 ג. נזקים משמעותיים  
 ד. נזקים קריטיים שאנחנו עדיין סובלים מהם
21. באילו אמצעים אתה משתמש כדי להתגונן ממתקפה של האקרים? (ניתן לענות יותר מתשובה אחת)  
 א. מעדכן תוכנות באופן שוטף  
 ב. מבצע גיבויים תקופתיים  
 ג. משתמש בתוכנות ההגנה שבאות באופן מובנה עם ציוד המחשוב שלי  
 ד. משתמש בתוכנות ייעודיות להגנת סייבר  
 ה. מפעיל ספקים חיצוניים שמומחים להגנת סייבר  
 ו. עורך הדרכות לעובדים  
 ז. מגדיר הרשאות למשתמשים/ מדיניות סיסמה חזקה  
 ח. משתמש בחומת אש במערכת המחשוב של העסק  
 ט. מצפין קבצים בעלי רגישות
22. האם לעסק יש יועץ עסקי (מעבר לרואה חשבון או עורך דין) לעסק אין יועץ עסקי משום סוג  
 א. לעסק יש יועץ עסקי מטעם מעוף  
 ב. לעסק יש יועץ עסקי אחר  
 ג. (לא להקריא) אחר \_\_\_\_\_

לצורך ניתוח סטטיסטי בלבד:

23. מהו תחום עיסוקו העיקרי של העסק? (להקריא תשובות- אם מציין יותר מסוג אחד לכתוב באחר)  
 א. תעשייה ויצור.  
 ב. שירותים מקצועיים מדעיים וטכניים (שירותי משפטיים ושירותי חשבונאות, שירותי ייעוץ וניהול, שירותי אדריכלות והנדסה, מחקר מדעי ופיתוח, פרסום וחקר שווקים, שירותי גרפיקה, שירותי צילום וכדומה)  
 ג. שירותי ניהול ותמיכה (שירותי השכרה והחכרה, שירותי תעסוקה, סוכני נסיעות, שירותי שמירה, אבטחה וחקירה, שירותי תחזוקה לבניינים, שירותי ניהול ותמיכה למשרדים ועסקים)  
 ד. שירותים אחרים (כל השרותים שלא נכללים בב ו-ג)

ה. מסחר קמעונאי.

ו. מסחר סיטונאי

ז. בינוי.

ח. אחר \_\_\_\_\_

תודה רבה על שיתוף הפעולה!

לסוקר: למלא את מין המשיב \_\_\_\_\_