איגוד האינטרנט הישראלי
ISOC-IL




**כתיבה:**
יונתן בן חורין,
מנהל קו הסיוע לאינטרנט בטוח

**עריכה ופיקוח מקצועי:**
עידן רינג,
סמנכ"ל חברה וקהילה

# השתלטות עוינת וחסימת משתמשים עסקיים בפלטפורמות מטא

**קו הסיוע לאינטרנט בטוח של איגוד האינטרנט הישראלי www.safe.org.il** · סקירת איום סייבר פברואר 2023

# השתלטות עוינת וחסימת משתמשים עסקיים בפלטפורמות מטא

## רקע וכוונת המסמך

מסמך זה מתאר דפוס השתלטות והונאה חדש שבלט במיוחד במהלך שנת 2022 בפניות שהתקבלו בקו הסיוע לאינטרנט בטוח של איגוד האינטרנט הישראלי בקרב משתמשי פלטפורמות מטא (פייסבוק, אינסטגרם, וואטסאפ) ובייחוד בקרב בעלי עסקים קטנים המשתמשים בפלטפורמות אלו כדי לנהל את עסקיהם. המתואר במסמך זה מבוסס על איסוף וניתוח מאות פניות שהגיעו במהלך 2022 לקו הסיוע לאינטרנט בטוח, בנוסף לדיווחים ופרסומים רבים בקבוצות וערוצי מדיה חברתית שונים המוקדשים לסיוע והגנת סייבר עבור אזרחים ועסקים בישראל. מטרת המסמך היא להציף ולתאר את התופעה ונזקיה ואת הצורך הדחוף בפתרון ומענה מיטיבי ויעיל יותר עבור משתמשי הרשת בישראל - ובייחוד משתמשי רשתות מטא. המסמך מתאר את דפוס הפעולה שחזר על עצמו במרבית התלונות מהסוג הזה, מביא עדויות אישיות מייצגות של קורבנות התופעה ומציע דרכי טיפול והתמודדות עם התופעה עבור גורמים רלוונטיים בפלטפורמות וברשויות המדינה.

## תיאור כרוניקת התופעה

לקו הסיוע לאינטרנט בטוח של איגוד האינטרנט הישראלי הגיעו מאז ספטמבר 2021 כ-170 פניות שונות המתארות דפוס דומה של השתלטות עוינת על חשבונות פייסבוק עסקיים ושימוש מניפולטיבי זדוני בתוכן פדופילי או תוכן תומך טרור כדי להביא לחסימה אוטומטית של המשתמש המותקף משלושת פלטפורמות מטא המרכזיות - פייסבוק, אינסטגרם וואטסאפ. זאת במטרה להשיג שליטה בלעדית על נכסיו הדיגיטליים, בדגש על חשבונות המודעות המשויכים לכרטיסי האשראי שלו.

פריצה לחשבונות מטא היא תופעה מוכרת ונפוצה מאוד, אך התופעה המתוארת כאן יוצאת דופן בשל הייחודיות של שיטת התקיפה שלה, היקף הנזק שהיא גורמת וההשלכות שלה על משתמשי הפלטפורמה בישראל - ועל פי פרסומים בתקשורת הזרה, כנראה גם בעולם. כמו כן, התופעה ייחודית בשל העובדה שאין לה כרגע מענה שירותי מובנה ותמיכה טכנית שתיתן סיוע למותקפים בתוך הפלטפורמה והדרך היחידה להשתקם ממנה ולהתמודד איתה היא פנייה לגורם אנושי בתוך החברה שיכול לבחון את המקרה פרטנית - מה שקשה מאוד לעשות כיום בהעדר שירות לקוחות פעיל מטעם החברה בישראל. שיטת הפעולה המתוחכמת מנצלת לרעה מנגנון מודרציה (פיקוח תוכן) אוטומטית של הפלטפורמה שמיועד להגן על המשתמשים אך מקשה מאוד על המותקפים לדווח על הפריצה ולקבל סיוע כי בפועל הם מזוהים כמי שעברו על חוקי הפלטפורמה ונחסמים מיד.

## מרבית הפניות שהגיעו מאז ספטמבר 2021 לקו הסיוע מתארות תסריט השתלטות ופגיעה בעל מאפיינים זהים שחזרו על עצמם:

01

התוקפים משיגים גישה לחשבונות פייסבוק פרטיים של משתמשים וחודרים אליהם במטרה להשתלט על החשבון ועל הנכסים שלו ולהביא לחסימת הבעלים כדי למנוע טיפול מהיר. נראה שלרוב המניע להשתלטות הוא כלכלי.

02

אוכלוסיית היעד המועדפת על התוקפים היא משתמשי פייסבוק המחזיקים או החזיקו בעבר בחשבון מודעות בתשלום או בדף פייסבוק עסקי פעיל. התקבלו גם פניות של משתמשים שנפלו קורבן גם לאחר שהפעילו אמצעי הגנה אקטיביים, כגון אימות דו שלבי.

03

לאחר ההשתלטות על חשבון הפייסבוק של הקורבן, התוקפים מנסים להשיג גישה לחשבון המודעות ו/או לסמכויות הניהול בדף העסקי שלו/ה מבלי שבעל העמוד מודע לכך, ומוסיפים את עצמם או מישהו מטעמם כמנהל (אדמין) נוסף בחשבון המודעות המשוייך לכרטיס האשראי של הקורבן.

04

בשלב הבא התוקפים מפרסמים בעמוד הפרופיל האישי של הקורבן תוכן פדופילי או תוכן תומך טרור (לרוב בסטורי או כפוסט) על מנת להביא לזיהוי אוטומטי של התוכן על ידי מערכת המודרציה וחסימה מיידית של הפרופיל האישי שלו.

05

בשלב זה, לאחר שהפרופיל האישי נחסם, יש בבעלות התוקפים סמכויות ניהול בלעדיות על העמוד העסקי ו/או חשבון המודעות שלו. לאחר ביצוע החסימה יתחילו התוקפים לבצע הונאות אשראי תוך שימוש בחשבון המודעות ו/או דפיו העסקיים של הקרבן - לרוב על מנת לממן קמפיינים ומודעות של גופים שלישיים במקומות אחרים מחוץ לישראל באמצעות החשבון שנפרץ.

06

במידה וכרטיס האשראי או חשבון הפייפאל של הקרבנות מקושרים לחשבון הפייסבוק שנפרץ - ישתמשו בו התוקפים כדי להריץ מודעות ולפרסם מוצרים שונים - ייתכן שלטובת צדדים שלישיים שכלל לא מודעים למקור התשלום.

07

מכיוון שאין לתוקפים גישה לפרטי האשראי השמורים במערכת הם משיגים שליטה בלעדית על הפרוקסי בעל הסמכות והיכולת להפעיל את האשראי השמור בו. קורבנות רבים שפנו לקו הסיוע דיווחו כי נעשה שימוש בכרטיס האשראי שלהם למימון מודעות במקומות רחוקים כמו דרום מזרח אסיה.

08

במידה והאשראי או חשבון הפייפאל אינם מקושרים לחשבון הפייסבוק שנפרץ - התוקפים ישתמשו בכרטיסי אשראי גנובים אחרים למימוש הונאת הפרסום תוך שימוש בחשבון המודעות או דפיו העסקיים של הקורבן.

09

מהתקיפה נפגעים גם משתמשים נטולי דף פייסבוק עסקי או חשבון מודעות, אך הם מיעוט בקרב הפניות. במקרים כאלו, לרוב המטרה היא להשבית את הפרופילים האישיים שלהם כדי לפגוע בהם על רקע פוליטי, לאומי או אחר. כ-90% מהקרבנות מדווחים שהיו בבעלותם דף עסקי או חשבון מודעות פעילים או כאלה שכבר אינם פעילים.

10

בנוסף לכך, חשוב לציין כי גם כאשר הקורבנות מצליחים להחזיר לעצמם את השליטה על חשבונות הפייסבוק והאינסטגרם הפרטיים שלהם לאחר הפריצה, הם אינם מצליחים לתבוע בעלות מחודשת על חשבונות המודעות והדפים העסקיים הקשורים שהיו בבעלותם.

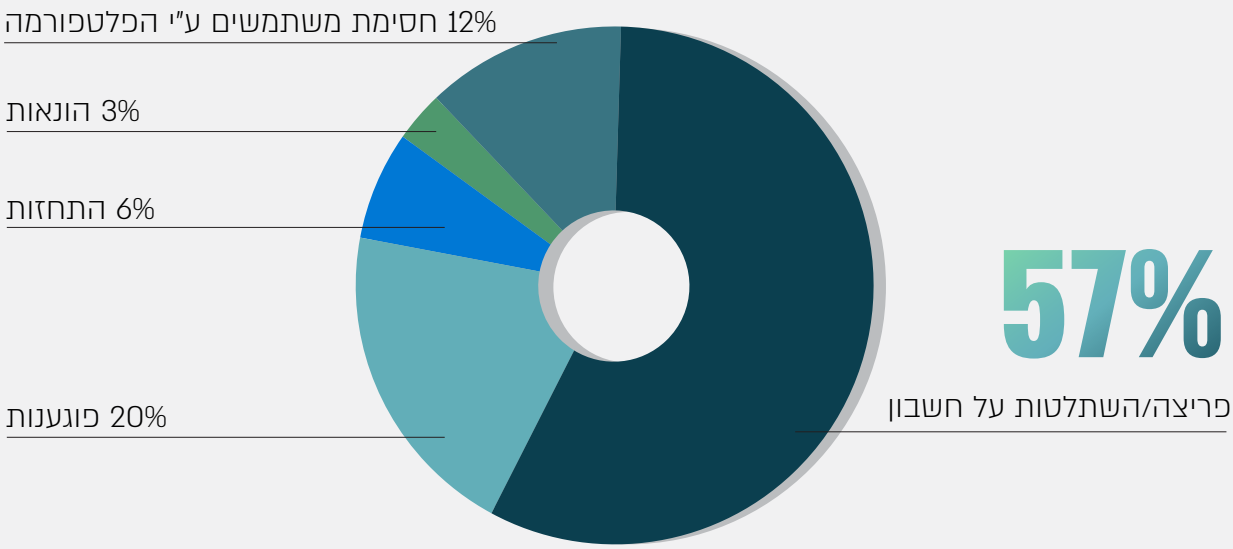
11

במידה והתקיפה השפיעה על הגישה לחשבון הWhatsApp של הקורבן, הוא עשוי להישאר חסום גם לאחר שהוחזרו לו החשבונות האחרים. ניסיונות ליצור קשר עם תמיכת WhatsApp לקבלת סיוע במקרים אלה נכשלים. המענה שניתן למשתמשי WhatsApp בישראל שואף לאפס.

12

יש לציין כי חלק מהקורבנות אשר יצרו קשר עם המחלקה המשפטית של פייסבוק ישראל והודיעו כי ינקטו בהליכים משפטיים דיווחו על פתרון מהיר יחסית של שחרור חשבונות הפייסבוק והאינסטגרם שלהם, אך לא את חשבון ה-WhatsApp.

## פניות משתמשי מטא לקו הסיוע בשנת 2022



# תיאור הנזקים הנגרמים לקורבנות מתקפת ההשתלטות

**01**

כתוצאה מהמתקפה ופרסום התוכן הפוגעני - המשתמשים מדווחים על השבתה מיידית מצד מטא של חשבונות הפייסבוק והאינסטגרם שבבעלותם. השבתות אלה משבשות בצורה קשה את יכולתם לנהל את בתי העסק שלהם, לתקשר עם לקוחות וספקים ועם המעגלים החברתיים שלהם וגורמים להם עוגמת נפש ומצוקה אישית חריפה.

**02**

פעמים רבות הם סופגים הפסדים כספיים עקב גביית אשראי שלא מוחזרת להם ונאלצים להשקיע משאבי זמן ומאמץ רבים כדי לבטל ולשחזר את כרטיסי האשראי, עמודי הסושיאל וחשבונות המודעות שלהם.

**03**

החדירה וההשתלטות על הנכסים הדיגיטליים שלהם ושיבוש הקשר והשירות ללקוחות פוגע במוניטין העסקי שלהם, בשירות שהם נותנים ללקוחות ובאמון שנותנים בהם להמשך הפעילות.

**04**

במידה והם לא מצליחים לשחזר את העמודים העסקיים ושאר הנכסים הדיגיטליים שלהם הם עשויים גם לאבד חומרים שיווקיים, פרטי לקוחות, תכתובות ותיעוד עסקאות ועוד. שחזור החומרים גובה זמן ומאמצים רבים.

**05**

למשתמשים ניתן 30 יום לערער על ההחלטה, לאחר מכן חשבונם נמחק לצמיתות. לעתים קרובות המשתמשים מערערים ללא הועיל, ומקבלים הודעה שההחלטה על ההשבתה מצד מטא - סופית.

**06**

כ-70% מהנפגעים מדווחים שגם חשבון הוואטסאפ בבעלותם נחסם - אך לא באופן מיידי אלא לאחר כשבוע-שבועיים. החסימה בוואטסאפ היא לצמיתות ואינה ניתנת לערעור.

**07**

**הנזקים לקורבנות שנותרו ללא חשבונות הפייסבוק, האינסטגרם והוואטסאפ הם כלכליים, חברתיים ואישיים כאחד.**

# עדויות אישיות של קורבנות שנפגעו ממתקפת ההשתלטות והחסימה:

"לפני מספר ימים התרחש אירוע פריצה לחשבונותיי (פייסבוק, אינסטגרם, וואטסאפ) מטא הגיבה ישירות בהשבתתם, התבקשתי לבצע אימות מולם בהגשת מסמכים כמובן ששיתפתי פעולה, אך אלה מצידם חסמו את חשבונותיי לצמיתות ללא כל אופציה לערער.

הדבר פגע בעסק שלי קשות היות וכל המלצותיי רשומות בפייסבוק, כל התוכן הפרסומי שלי שהושקעו בו משאבים וכוחות אדירים מופנה לפייסבוק לאינסטגרם ולשיחות וואטסאפ. ברמה האישית אני חסר אונים כבר מספר ימים לא ישן ומתקשה לתפקד, מפחד מההשלכות הכלכליות שהדבר יביא על משפחתי".

מ', בעל עסק לטיפול בכאב מהמרכז, דצמבר 2022

"שמי ג', גר בפתח תקווה, נשוי ואב לשלושה ילדים. בתאריך 20 בינואר בוצעה פריצה לחשבון הפייסבוק שלי ע"י האקר כלשהו, שלאחריה נחסמו חשבונות הפייסבוק והאינסטגרם (האינסטגרם מקושר דרך כניסת פייסבוק). טענתה של פייסבוק לחסימה היתה בעקבות העלאת תוכן פוגעני (שהועלה על ידי אותו האקר - אחד מחבריי שהספיק להיחשף לתוכן שהועלה בשמי בזמן אמת אמר שמדובר היה בסרטון פדופילי ושלח לי צילום מסך) והפרה של תנאי השימוש. החסימה לא שוחררה עד לרגע זה על אף העובדה שהצלחתי להעלות תמונת תעודת זהות ורשיון נהיגה וכל מה שיכולתי במסגרת בקשותיהם במידה ויש לי Objection על ההחלטה. אם לא די בכך, ביום חמישי האחרון, 3 לפברואר, שבועיים בדיוק אחרי המקרה המדובר, בשעות הצהריים קיבלתי נוטיפיקציה מווטסאפ שחשבוני מושעה. כשניסיתי להגיע לשירות של ווטסאפ קיבלתי הודעה לקונית שהחשבון שלי הפר את תנאי השימוש ויש עליו תלונות רבות. בשלב זה כבר פניתי למשטרה להגנה על שמי הטוב ולפתוח תלונה אודות המקרה.

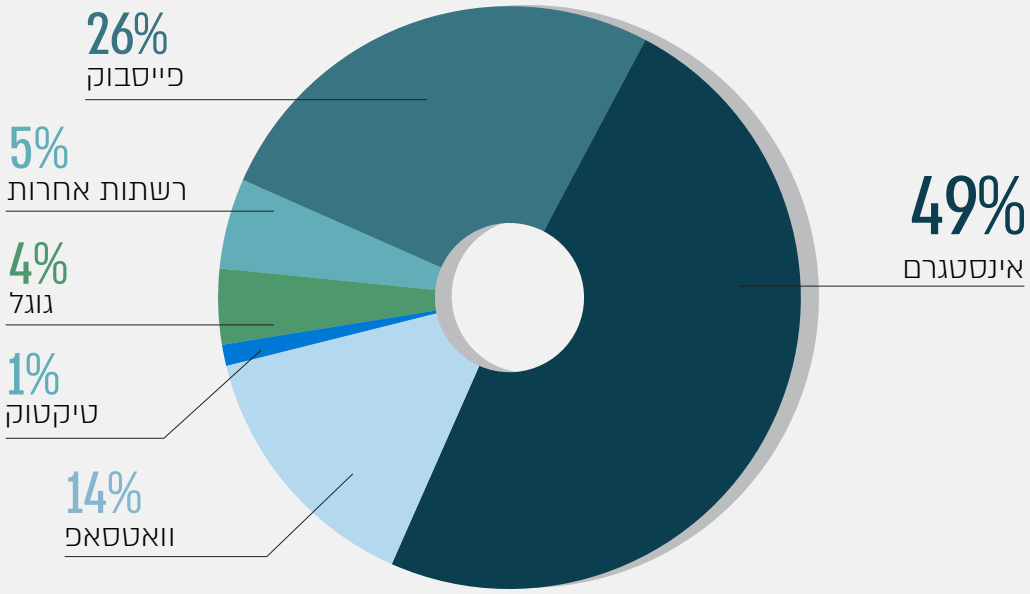
עד לרגע זה, אין לי עם מי לדבר בפייסבוק/ווסטאפ/אינסטגרם על מנת להשיב את החשבונות. הווטסאפ הוא הרגיש ביותר, עקב כמות המידע הגדולה ותיעודי השיחות שהיו לי בו (חלקם אף עם לקוחות בהם אני מטפל במסגרת העבודה שלי)".

ג', עצמאי בתחום המחשוב, פברואר 2022

"היום קיבלתי מיילים רבים מפייסבוק על כך שבוצעה כניסה לחשבוני מכתובות מיילים שונות והוגשה בקשה לאיפוס הסיסמא. הגבתי להודעות אלו על ידי לחיצה על הקישורים הרלוונטיים שלא אני ביצעתי את הבקשה הזאת. בערב קיבלתי הודעות שחשבונות פייסבוק ואינסטגרם שלי הושעו עקב אי עמידה במדיניות שלהם. כמו כן קיבלתי אימייל ש"המודעה שלך אושרה", זאת למרות שלא הקמתי אף מודעה. אין לי גישה לחשבונות וההודעה בפייסבוק ואינסטגרם אומרת שאין להם מספיק אנשים כדי לסקור את בקשתי להחזרת החשבון. מדובר על החשבון הפרטי שלי שתחתיו יש מספר דפים עסקיים שחשובים לי ולפרנסתי מאוד. כשבועיים לאחר מכן חשבון הוואטסאפ המקושר לעסק (ולאותם חשבונות פייסבוק ואינסטגרם) נחסם גם הוא".

ד', בעל עסק קטן בתחום ההפקות, אוקטובר 2022

## פניות סייבר לקו הסיוע בשנת 2022 - חלוקה לפי פלטפורמות




## מענה לקוי מצד הפלטפורמה

חרף ניסיונות רבים של הקורבנות ושל קו הסיוע של איגוד האינטרנט לערער לנציגי מטא בערוצים השונים על חסימת הפרופילים של הקורבנות - התופעה עדיין מתרחשת בהיקפים גדולים, ללא מענה הולם מצד מטא.

קו הסיוע מוגדר כ"Trusted Partner" של פייסבוק ואינסטגרם אשר מאפשרים לו לדווח על אירועי "בטיחות" (Safety) באמצעות ערוץ פנייה ייעודי. נציג הקו דיווח בערוץ זה והתריע ישירות למנהלי המדיניות בפייסבוק-אינסטגרם ובוואטסאפ (גורמים נפרדים) על התופעה במהלך שנת 2022 אך ללא מענה הולם. התופעה הוגדרה על ידי הנציגים בקטגוריית "אבטחה" (Security) שלא מקבלת מענה וטיפול על ידי ערוץ דיווח ישיר המוקדש לאירועי מוגנות חמורים (Safety) המקושרים לסכנה ממשית לחיי אדם בלבד (Real world harm). לטענת נציגי החברה אירועי סייבר על רקע כלכלי או עסקי לא נופלים תחת הגדרות הטיפול של נציגי Trust and Safety של החברה. כך נוצר מצב בו גם לקורבנות החסומים אין דרך להתלונן ולקבל סיוע מנציגי הפלטפורמה וגם ארגונים וגורמים המוגדרים כשותפים ומדווחים רשמיים (Trusted Partners) לא מורשים לדווח ולקבל מענה כדי לסייע להם במקרים מהסוג הזה. התוצאה הסופית היא הפקרה מוחלטת של הקורבנות שרובם לא רק משתמשים (Users) של הפלטפורמות אלא גם לקוחות משלמים שמשתמשים בה לצורך ניהול עסקיהם ופרסום שלהם בתשלום - אך בכל זאת לא זוכים למענה לתופעה חמורה זו שחוזרת על עצמה בהיקפים גדולים מאוד בשנה האחרונה.

# סיכום ומסקנות מניתוח התופעה

תמונת המצב שעולה מהפניות וניתוח של התופעה משקפת פגיעה קשה בבטיחות וזכויות המשתמשים ברשתות והיכולת שלהם להתנהל מבחינה עסקית ואישית בפלטפורמות מטא, שמהוות כיום ערוץ מרכזי לניהול נכסים דיגיטליים ועסקים קטנים בישראל. התוקפים מנצלים מצב בו משתמשים רבים בישראל מסתמכים על פלטפורמות מטא כזירה העיקרית לניהול עסקים קטנים ולתקשורת עם לקוחותיהם ואנשי קשר עסקיים שלהם.

במרבית הפניות שהגיעו לקו הסיוע של איגוד האינטרנט הישראלי בשנה האחרונה מצטייר מצב לפיו קיימת פגיעה כפולה במשתמשי הרשתות ובעלי עסקים - גם ביכולת התפקוד וניהול העסק שלהם מול הלקוחות שלהם וגם באמון ובמענה שלהם מול הפלטפורמה שמשמשת להם זירה פרסומית עליה הם משלמים. על כך ניתן להוסיף גם חוסר מענה וטיפול מצד הרשויות והמשטרה בישראל שלא מספקים מענה למתקפות והונאות ברשת מהסוג הזה.

התופעה המתוארת בסקירה זאת היא ביטוי למורכבות ההולכת וגוברת של פגיעות ומתקפות סייבר אזרחיות ברשת - לא מדובר רק בפגיעה כלכלית-עסקית וארוע בטיחות, אלא גם בפגיעה אישית ורגשית, המתאפיינת בחדירה חמורה לפרטיות, התחזות ונזקים אישיים ופסיכולוגיים נוספים.

מכיוון שישראל היא שוק קטן יחסית בעל מספר מצומצם של בעלי עסקים קטנים ביחס למדינות אחרות בעולם, עולה החשש כי מטא העולמית לא משקיעה מאמצים הולמים כדי לחקור את התופעה, למצוא לה פתרונות טכנולוגיים ולתת מענה ושירות לתלונות ולפגיעות אלה.

במקרים רבים המתלוננים נקטו בצעדים משפטיים בלית ברירה ומתברר כי לאחר איומים בתביעה נמצאה במטא הדרך לטפל בהם ולשחרר את החסימה שמנעה מהם את ניהול העמודים. גם פנייה לרשויות המדינה ולגורמי אכיפת חוק לא מסייעת בתיקון המצב.

# המלצות עיקריות לתיקון המצב:

## 01 בהיבט הטכנולוגי

מטא צריכה להשקיע מאמצים ומשאבים של מחקר ופיתוח כדי ללמוד את דפוס המתקפה המדוברת ולפעול לזיהוי ומניעת שימוש לרעה במנגנוני המודרציה וסינון התוכן האוטומטיים כדי שלא ישמשו ככלי תקיפה נגד המשתמשים, במקום להגן עליהם. יש לפתח כלים שיבחינו בין פרסום סיסטמי ומכוון של תוכן פוגעני ומזיק (כגון פורנו או טרור) לבין השתלטות על עמודים ופרופילים תמימים ופרסום תוכן מזיק מתוך מטרה להביא לחסימתם.

## 02 ברמת השירות והמענה ללקוחות

על מטא לפעול לחיזוק והגברת המענה והטיפול שהיא מעניקה לבעלי עמודים עסקיים שנפגעו מתופעות של מתקפה, השתלטות והונאה בתוך זמן סביר - גם בשפה העברית. זאת כדי להתמודד עם תופעות של השתלטות וחסימה בכלל - ובפרט על התופעה הזדונית המתוארת במסמך זה. יש לפעול להקמת שירות לקוחות שייתן מענה לבעלי חשבונות עסקיים שנפגעו מפריצות והונאות, מבלי שהם יצטרכו לנקוט בהליכים משפטיים כדי לקבל טיפול.

## 03 ברמת ההסברה וחינוך הציבור

תאגידי מדיה חברתית הפועלים בישראל ומהווים כלי עבודה מרכזי ומשמעותי עבור בעלי עסקים קטנים (כמו פלטפורמות מטא) צריכים לפעול בצורה פרואקטיבית, נרחבת ואפקטיבית יותר כדי לעודד לקוחות עסקיים להגן על הנכסים שלהם בצורה משמעותית ומיטבית. ניתן לעשות זאת גם באמצעים טכנולוגיים בתוך הפלטפורמה על ידי מתן מידע ותזכורות בעברית באפליקציה ועידוד משתמשים להגברת אמצעי הבטיחות - וגם באמצעות כלים ציבוריים ושיווקיים שייעלו מודעות ויעודדו שימוש באמצעי זהירות והגנה כמו אימות דו שלבי, חיזוק סיסמאות והוספת מנהלים חלופיים לחשבונות.

## 04 ברמת המדיניות

למדינה ורשויות יש תפקיד חשוב בשמירה על זכויות המשתמשים העסקיים בפלטפורמות הסושיאל וקידום פעולות הגנה ושמירה מצדם. על המדינה לפנות לפלטפורמות ולוודא שהן מבצעות פעולות הסברה ומודעות מהסוג הזה ולקדם פעולות בנושא זה גם מהצד שלה באמצעות מערך הסייבר ורשויות רלוונטיות אחרות.

## 05 ברמת האכיפה, החקירה והשיטור

יש לקדם מענה גם ברמת האכיפה, החקירה והשיטור של רשויות המדינה כדי לתת מענה הולם לבעלי עסקים קטנים שנפגעים ממתקפות, הונאות, התחזויות והטרדות בנכסים הדיגיטליים שלהם בתוך פלטפורמות הסושיאל. יש לפעול למענה וטיפול בפגיעות בנכסים הדיגיטליים של בעלי עסקים קטנים באותו האופן בו היו מטפלים בהונאות או פעולות עבריניות כלכליות אחרות כלפיהם.

איגוד האינטרנט הישראלי
ISOC-IL

סקירת איום סייבר - פברואר 2023

# השתלטות עוינת וחסימת משתמשים עסקיים בפלטפורמות מטא

פרסום של קו הסיוע לאינטרנט בטוח
של איגוד האינטרנט הישראלי

**לפניות ויצירת קשר עם קו הסיוע:**


safe@isoc.org.il

www.safe.org.il

בלוק - מרכז הגנת סייבר לאזרחים
https://block.org.il


---

**איסוף נתונים וכתיבה:**

יונתן בן חורין, מנהל הקו הסיוע לאינטרנט בטוח

**עריכה, ליווי מקצועי וניסוח המלצות:**

עידן רינג, סמנכ"ל חברה וקהילה

**ייעוץ מקצועי לקו הסיוע:**

אורנה הייילינגר, מנהלת מרכז נטיקה

**עיצוב המסמך:**

טלי גלעד

---

**איגוד האינטרנט הישראלי (ע"ר)**

www.isoc.org.il

https://www.facebook.com/ISOC.ORG.IL

https://twitter.com/ISOCIL