איגוד האינטרנט הישראלי ISOC-IL

.ישראל

# העוקץ האלגוריתמי: רשתות חברתיות ובינה מלאכותית כאמצעי להונאות פיננסיות

## סקירת איומי סייבר — קו הסיוע לאינטרנט בטוח


מאי 2025

**איגוד האינטרנט הישראלי** (ע"ר) הוא ארגון ללא כוונת רווח אשר פועל מאז תחילת שנות התשעים להטמעת השימוש באינטרנט לטובת הציבור בישראל ומפעיל תשתיות אינטרנט חיוניות בישראל: מרשמי שמות המתחם (Domain Names) המדינתיים "il. "ו-".ישראל" ומחלף האינטרנט הפנים מדינתי (IIX). הידע והניסיון המקצועי של איגוד האינטרנט הישראלי במחקר, בפיתוח ובהפעלה של טכנולוגיות אינטרנט עבור הציבור הישראלי משמש בסיס לפעילות מחקר, מדיניות והעצמת הקהילה שמבצע האיגוד. בכלל זה, איגוד האינטרנט הישראלי מפעיל את קו הסיוע לאינטרנט בטוח ואת מיזם Block.org.il, המספק לציבור הרחב סיוע, ידע וכלים לשיפור המוגנות והבטיחות ברשת; מיזמים ופעילויות שונות לצמצום פערים דיגיטליים וקידום מיומנות ואוריינות רשת בחברה הישראלית; את מיזם data.isoc.org.il האוסף ומנגיש נתונים כמותיים-סטטיסטיים על האינטרנט הישראלי ומשתמשיו; ומפרסם מחקרי מדיניות מקצועיים המיועדים ליידע ולטייב את זירת האינטרנט הישראלית והגלובלית בצמתים מגוונים של משפט וטכנולוגיה.

כתיבה: ניצן יסעור ונרקיס משה
תחקיר ואיסוף נתונים: יונתן בן חורין
עריכה ופיקוח מקצועי: עידן רינג
הערות: ירדן אמיר
עיצוב: סטודיו לי ותמר
עיצוב דיגיטלי: רני עינב

קו הסיוע לאינטרנט בטוח של איגוד האינטרנט הישראלי - www.safe.org.il
איגוד האינטרנט הישראלי – www.isoc.org.il
לפרטים נוספים ויצירת קשר – info@isoc.org.il

# תוכן עניינים

# תקציר המסמך

מסמך זה מתאר גל חדש של הונאות רשת גלובליות מתוחכמות שצובר תאוצה בשנים האחרונות ופוגע גם באזרחים ישראלים רבים מכל קבוצות האוכלוסייה. הגל החדש של הונאות הרשת מתאפיין באימוץ מהיר ומתקדם של טכנולוגיות בינה מלאכותית חדשות וכלי פרסום והפצה דיגיטליים משוכללים כדי להגיע בצורה אפקטיבית יותר לקהלי יעדים ממוקדים ולהפיל אותם בפח. בניגוד להונאות רשת בסיסיות ומסורתיות יותר, הגל החדש של הונאות הרשת משתמש בטכנולוגיות בינה מלאכותית (AI) חדשות ובפלטפורמות ורשתות חברתיות כדי לייצר מיקוד והתאמה לקהלי יעד מפולחים, התחזות וניסוח זהויות, תכנים ומסרים שיווקיים מרובים ומגוונים ושימוש אפקטיבי בכלי פרסום ושיווק ממומנים בתוך פלטפורמות ורשתות חברתיות שנחשבו בעבר למרחב בטוח ומוגן יותר עבור המשתמשים. השילוב בין כלי בינה מלאכותית גנרטיבית ליצירת תמונות וסרטוני דיפ-פייק והפצתם דרך מנגנוני מודעות וקידום ממומן בפלטפורמות מגוונות, מאפשר התאמה של תכנים ומסרים של ההונאה לקהלי יעד שונים בזמן אמת והגברת האפשרות והיכולת של מבצעי ההונאות להגדיל את מספר הקורבנות ואת היקף הפגיעה בהם. מסמך זה מתעד, ממפה ומנתח את הונאות הרשת החדשות על בסיס מאות דוגמאות של מודעות ומבצעי הונאה מהסוג הזה שנאספו ותועדו בידי צוות קו הסיוע לאינטרנט בטוח של איגוד האינטרנט הישראלי בשנים 2023-2025.

## א. מבוא — הגל החדש של הונאות הרשת

הונאות ברשתות החברתיות הפכו בשנים האחרונות לתופעה גלובלית חמורה הפוגעת ביחידים, בקבוצות, בתאגידים וחברות, ובתהליכים ומוסדות דמוקרטיים ברחבי העולם. נוכלים וגורמי פשיעה מנצלים טכנולוגיות תקשורת ודיגיטל מתקדמות ליצירת תוכן מזויף, מניפולטיבי ומשכנע, תוך שימוש באפשרויות ההפצה והפרסום ממוקד של פלטפורמות ורשתות חברתיות שונות כדי לאתר ולהתמקד בקהלים וקורבנות פוטנציאליים. ההתפתחות המואצת של כלי בינה מלאכותית (AI) גנרטיבית והאפשרות ליצור תכנים ברמה גבוהה כמו תמונות או סרטוני דיפ-פייק[1] הופכות את פעולת ההונאה ברשת לנגישה, זולה ואפקטיבית מתמיד. המודל הכלכלי של הפלטפורמות החברתיות, המבוסס על מודעות ממומנות ומערכות טירגוט מתוחכמות, מאפשר להונאות לשגשג בחסות האלגוריתמים, לעיתים מבלי שיזוהו בזמן וללא מענה ופיקוח מספק של הפלטפורמות או רשויות האכיפה.

בישראל, כמו בעולם, הונאות אלו מופצות בהיקף רחב, תוך ניצול חולשות רגולטוריות והעדר מנגנוני אכיפה מספקים, מה שמאפשר לנוכלים לפעול כמעט ללא הפרעה ולהגיע להיקף משמעותי של קורבנות ורווחים. בשנים האחרונות הונאות רשת שבעבר הופצו בעיקר באמצעות הודעות סמס (כגון נסיונות פישינג לגניבת פרטי אשראי) או הודעות דואר אלקטרוניות, עוברות בהדרגה לפלטפורמות ורשתות חברתיות סגורות ואלגוריתמיות כמו פייסבוק, אינסטגרם, טיקטוק ויוטיוב, שם הן מופצות באמצעות מודעות ממומנות, תוך שימוש בטכניקות פרסום ממוקד (טירגוט) המבוססות על פילוח העדפות המשתמשים, תחומי העניין שלהם ומידע אישי שנאסף עליהם ולהתאים את ההונאה בזמן אמת להתנהגות המשתמשים. כך, הן מצליחות לפנות לקהלים ממוקדים, להתאים להם הונאות ממוקדות יותר ולנתב אותם אל ממשקים בהם הם נדרשים למסור מידע אישי, פרטי חשבונות ונכסים שונים או להפקיד כסף במצג שווא של השקעה פיננסית. מנגנוני הפרסום והקידום הממומן של הפלטפורמות החברתיות, שהם כלי טרגוט ופרסום עוצמתיים המאפשרים למפרסמים להגיע בדיוק מירבי לקהלי יעד ולייצר אינטראקציות עם המודעות שלהם - הפכו בידי נוכלים וגורמים זדוניים למכונת הונאה דיגיטלית משוכללת ואפקטיבית.

1. המונח Deepfake – דיפ-פייק (זיוף עמוק בעברית), מבוסס על חיבור בין המושגים Deep Learning ו-Fake, ומתאר טכנולוגיה מבוססת בינה-מלאכותית המאפשרת לשנות או לעבד את התוכן של תמונות או סרטונים מבלי שניתן יהיה להבחין שהתכנים זויפו. www.isoc.org.il/public-action/deepfake

קו הסיוע לאינטרנט בטוח (www.safe.org.il) של איגוד האינטרנט הישראלי פועל משנת 2013 ומספק סיוע, הכוונה, מידע וכלים למשתמשי האינטרנט והרשתות החברתיות בישראל, במטרה לתמוך בהתמודדות עם מגוון רחב של איומים מקוונים ופגיעות ברשת. כגורם מדווח רשמי (Trusted Flagger) המוכר על ידי שורה של פלטפורמות גלובליות מובילות, קו הסיוע מקבל מאות פניות חודשיות, מנתח את התופעה ומעביר דיווחים להמשך טיפול. מסמך זה מתבסס על דיווחים, נתונים ומחקר של צוות קו הסיוע לאינטרנט בטוח במהלך 2023-2025 ומציג **ניתוח מקיף של מאות מודעות ופיסות תוכן המצביע על השימוש הגובר והממוקד בטכנולוגיות AI, דיפ-פייק וקידום ממומן ברשתות חברתיות** למטרת הונאה כלכלית בישראל. המסמך מציג את היקף התופעה, מנגנוני הפעולה של הנוכלים והכשלים של הפלטפורמות והרשויות באיתור, מניעה וטיפול בהונאות AI ודיפ-פייק נגד ישראלים ברשתות החברתיות.

המסמך חושף ומנתח מגמה הולכת וגוברת שהחלה במהלך 2023 והתגברה לאחר מכן במסגרתה נוכלים מייצרים סרטוני דיפ-פייק המציגים דמויות ציבוריות מוכרות, כגון פוליטיקאים, סלבריטאים ואנשי עסקים, הממליצים בביכול על הזדמנויות השקעה מזויפות. הדמויות בסרטונים המזויפים במצבים מציאותיים ומשכנעים תוך ניצול האמון הציבורי בהן והתאמה תרבותית ושפתית. מודעות אלו מובילות משתמשים לדפי נחיתה המתחזים לשירותים פיננסיים, שם הם מתבקשים למסור מידע אישי ולהעביר כספים. בחלקו האחרון המסמך כולל גם מוצגות דרכי התמודדות אפשריות למניעה וטיפול בטרנד ההונאה הדיגיטלית הנוכחית ובתופעות דומות בעתיד, בהן פתרונות טכנולוגיים, רגולטוריים וחינוכיים, לצד שיתופי פעולה בין הפלטפורמות, רשויות האכיפה והחברה האזרחית.

## ב. תיאור שלבי ומרכיבי הונאות בינה מלאכותית ברשתות החברתיות

ההונאות המבוססות על טכנולוגיות AI לרשתות בנויות כך שהמשתמש יעבור דרך "משפך שיווקי" מותאם אישית שתוכנן בקפידה כדי לגרום לו להתעניין בהונאה, למסור את פרטיו האישיים באתר ייעודי ולבסוף גם להעביר כספים לנוכלים. המערך, הבנוי בשלבים, כולל חשיפה ראשונית למודעות שיווקיות מותאמות אישית בפלטפורמות חברתיות שונות, מעבר לאתרים חיצוניים ופלטפורמות מסחר מזויפות ולעתים גם יצירת קשר אישי עם נציג אנושי. להלן תיאור של השלבים השונים אותם עובר המשתמש עד השגת מטרת ההונאה וביצד היא מתבצעת בפועל.

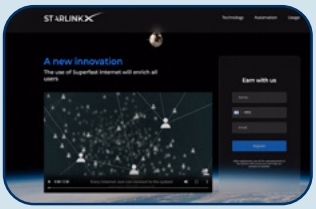
## ממודעה בפייסבוק לאיסוף פרטי אשראי

דוגמה לשלבי קמפיין הונאה אמיתי שדווח לקו הסיוע לאינטרנט בטוח

**1**

**מודעה**

(במקרה זה, מודעה מוסווה/קלוקינג)




**2**

**הפניה לדף נחיתה**

עם הלוגו של סטראלינק וסרטון תדמית

המסביר על פלטפורמת ההשקעות


**3**

**הסוכן שולח מייל לקורבן**

עם יוזר וסיסמא לאתר המסחר החדשני

ומסמכים מזויפים במטרה להרגיע

את הקורבן שהוא בידיים טובות

**4**

**הקורבן מתחיל להפקיד כספים בפלטפורמה**

ומוצגים לו רווחים פיקטיביים

אותם לא יוכל למשוך

## 1. יצירת עמוד סושיאל מזויף להונאה או השתלטות על חשבונות סושיאל קיימים

ראשית, הנובלים עושים שימוש בעמוד פייסבוק מזויף מתחזה או משתלטים על עמוד אמיתי כדי לייצר פלטפורמה להפצת ההונאה. לעתים הם יעדיפו השתלטות על נכס קיים כדי להשתמש בעמוד עם ותק בפלטפורמה, מבלי שהבעלים המקורי מודע או שאין ביכולתו לפעול להשבת הבעלות על חשבונו. תהליך יצירת עמוד מזויף או השתלטות על קיים כולל לרוב שימוש בתמונות פרופיל וכותרות שמחקות גורמים אמינים כמו גופי מדינה או כלי תקשורת באמצעות יצירה והוספה של תמונות וצילומי מסך מזויפים באמצעות כלי בינה מלאכותית גנרטיבית בסיסיים. התוכן בעמודים המקדמים את ההונאה תואם לטרנדים ומגמות אקטואליות מדוברות – למשל השקעה במיזמים של אילון מאסק ששמו ודמותו בולטים בשיח הציבורי, או במניות שקשורות בטכנולוגיות AI או באפיקי השקעה מזוייפים בפלטפורמות המדיה החברתית. לעיתים העמודים המזויפים יפרסמו בתחילה תוכן שנראה כשגרתי או לגיטימי במטרה לחזק את האמינות והנראות של הדף בעיני המשתמשים.

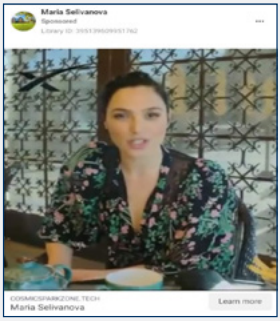

עמוד אינסטגרם המשתמש בתמונת פרופיל של ערוץ 14 ובסרטון דיפ-פייק המתחזה לראיון של פרופ' אמיר ירון, נגיד בנק ישראל, הממליץ על המוצר הפיננסי המזויף ומפנה למודעה.

## 2. יצירה ופרסום של סרטוני דיפ-פייק (AI) מותאמים אישית לפי קהלי יעד

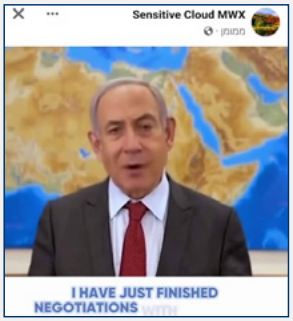
סרטוני דיפ-פייק הם כלי מרכזי לקידום הונאות אלו, שכן הם מאפשרים לנוכלים לייצר תוכן ויזואלי משכנע ועדכני במיוחד. בתהליך יצירת הסרטון, נעשה שימוש בתמונות וסרטונים קיימים של דמויות מוכרות ובעלות סמכות, כמו אנשי ציבור וממשל, מומחים, וסלבריטאים. הנוכלים משנים את הסרטון האותנטי כדי להתאים אותו לקידום ההונאה שלהם ולרתום את המוניטין של הדמויות המוכרות לטובתם. לדוגמה, הנוכלים משנים את תנועות הפנים והשפתיים של המציגים בעזרת כלי AI כדי להתאים אותם לתוכן ולמסרים השיווקיים המקדמים את ההונאה ומשכנעים את קהל היעד להשקיע בה או לרכוש אותה. המטרה היא ליצור תוכן הנראה אמיתי ואמין ככל האפשר ומעוגן במציאות, כך שיראה כאילו האדם המדובר באמת מקדם בקולו את ההשקעה או המוצר המזויף, מה שעשוי להראות עבור קהל יעד מתאים כאפשרות סבירה והגיונית.

כדי להגביר את האפקטיביות של הסרטונים המקדמים את ההונאה, מתבצעת התאמה ממוקדת של כל סרטון לקהלי היעד השונים. כך, הנוכלים מייצרים עשרות רבות של גרסאות שונות לסרטון ההונאה בכיכובם של "פרזנטורים" מפורסמים שונים, כך שהמודעות יוצגו בהתאמה אישית לקבוצות אוכלוסייה שונות בהתאם לעניין ולהעדפה שלהם. הנוכלים מבצעים התאמה מדויקת של הפרזנטורים, השפה, הסגנון הוויזואלי, והמסרים השיווקיים כך שיתאימו באופן מרבי למה ש"יתפוס" את המשתמשים. לעיתים, תכני הסרטונים מתעדכנים בהתאם למגמות, ארועים ודיונים ציבוריים עכשוויים כדי ליצור שיווק בזמן אמת (RTM – real time marketing), מה שמעצים את הרלוונטיות והאפקטיביות של הסרטונים המזויפים בעיני הקורבנות ומקשה על זיהוי הזיוף.

לדוגמה, משקיעים מתחילים ייחשפו לסרטונים המדגישים רווחים מהירים עם דמות מוכרת מהעולם העסקי (למשל מומחי השקעות המרבים להופיע בטלוויזיה) או פוליטיקאי בו הם תומכים (למשל שר האוצר), בעוד שמשתמשים מבוגרים יותר יקבלו סרטונים המתמקדים בביטחון כלכלי ויציבות פיננסית בהשתתפות דמויות המשדרות אמינות ומוכרות (למשל נשיא המדינה או נגיד בנק ישראל). קהלים צעירים יותר ייחשפו לסרטונים בהשתתפות אנשי הייטק (למשל אילון מאסק או מארק צוקרברג) או סלבריטאים וכוכבי תרבות מקומיים (למשל אייל גולן או נעה קירל). בנוסף, שימוש במגוון רחב של אלמנטים גרפיים, סטטיסטיקות מזויפות ועדויות מומצאות מחזק את האמינות המדומה של הסרטונים ומקשה על הצופים לזהות את ההונאה.





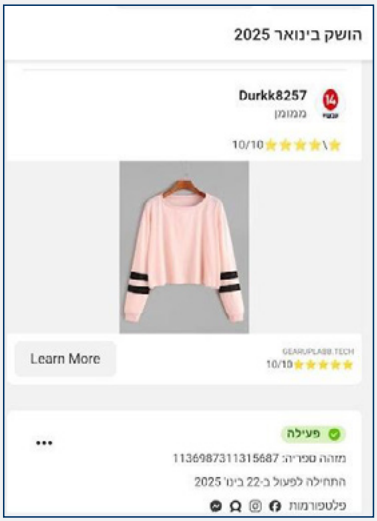



## 3. הפצת מודעות מזויפות לקידום ההונאה בפלטפורמות החברתיות

הפצת המודעות המזויפות מהעמודים המתחזים או הפרוצים מתבצעת באמצעות קידום ממומן של סרטוני הדיפ-פייק המגוונים - כאמור, כאשר לכל קהל יעד תוצג בשאיפה הגירסה המתאימו לו. מנגנוני הקידום הממומן של הפלטפורמות הם כלי טרגוט ופרסום עוצמתיים אשר מאפשרים למפרסמים להגיע בדיוק מירבי למשתמש הנכון, עם המודעה הנכונה, בזמן הנכון ביותר - כדי לגרום לו לייצר אינטראקציה עם המודעה ולפתות אותו להיכנס לאתר הייעודי שהוקם עבור ההונאה. הנוכלים יכולים לגשת בקלות ובדיוק רב למשתמשים פגיעים בהתאמה אישית עם המודעה הנכונה תוך שהם מנצלים את מנגנוני השיווק העוצמתיים של הפלטפורמות.

בנוסף, כלי הפרסום הממוקדים של הפלטפורמות מציעים אפשרויות מתקדמות נוספות אשר הנוכלים מנצלים על מנת להסוות את סרטוני ההונאות מהאלגוריתמים של הפלטפורמות. הכלים הזמינים למפרסמים, מאפשרים לנוכלים לעשות שימוש בפלטפורמות ולנצלם לרעה. למשל, כלים כמו "מודעות דינמיות" ו-"A/B testing" מאפשרים להציג בספריית המודעות מודעה עם חזות לגיטימית, ולמשתמש אותו רוצים להונות - מודעה המקדמת מוצר פיננסי מזויף. הכלים המתקדמים וההזדמנות לאנונימיות נרתמות על ידי הנוכלים על מנת להפיץ את התוכן המזויף מתחת לאפן של מערכות ומנגנוני הבטיחות והמוגנות של הפלטפורמות החברתיות.


מסך של מודעה ממומנת עם סרטון דיפ-פייק של מארק צוקרברג המפנה להונאה צילום משמאל: העמוד שמציג מודעה למשתמש עם סרטון דיפ-פייק מציג בספריית המודעות את המודעות המפנות לאותו עמוד נחיתה של ההונאה תחת תמונה גנרית ולגיטימית לבאורה של מוצר טקסטיל.

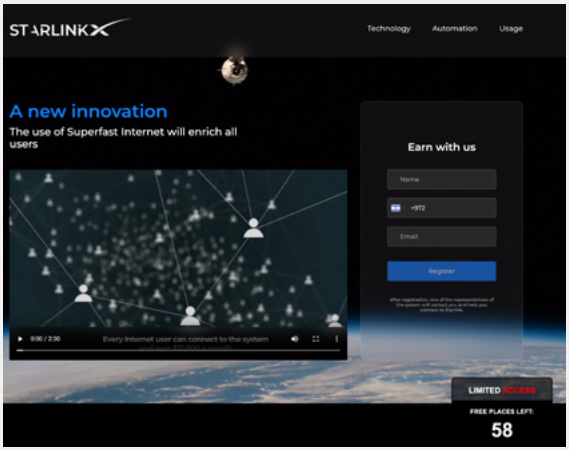



משמאל: העמוד שמציג מודעה למשתמש עם סרטון דיפ-פייק מציג בספריית המודעות את המודעות המפנות לאותו עמוד נחיתה של ההונאה תחת תמונה גנרית ולגיטימית לבאורה של מוצר טקסטיל

## 4. העברה לאתר נחיתה חיצוני של ההונאה ואיסוף פרטים אישיים

באשר המשתמש לוחץ על המודעה שהוצגה לו ברשתות החברתיות עם התוכן והסרטון המזויף, הוא מועבר לאתר או דף נחיתה חיצוני שחזותית נראה אמין, מקצועי ומושקע ומציג את אפיק ההשקעה או הרכישה המוצע לו. לרוב מדובר בשירותים או הזדמנויות פיננסיות אקטואליות וקורצות. לדוגמה, אתר המציע אפליקציית AI מזויפת שמבטיחה למשתמש ניטור חכם ומתמשך של ביצועי הבורסה והמלצה על ההשקעות המשתלמות ביותר. האתרים הרבים שהוקמו לצורך ביצוע ההונאות מציגים שלל תכנים והדמיות שנועדו

להעניק למשתמש תחושה של אמינות ומקצועיות. למשל, בדומה למודעות המזויפות שהוצגו לו בפלטפורמות החברתיות, האתרים מכילים סרטוני AI תדמיתיים מזויפים המבוססים על תמונות וקטעי וידאו אמיתיים שהוצאו מהקשרם, המלצות מזוייפות של ידוענים, מומחים או של דמויות ציבוריות על המוצר הפיננסי אשר מבטיח רווחים גבוהים והדמיות גרפיות צבעוניות ומרשימות של דאשבורדים ואפליקציות פיננסיות שונות.




## איסוף פרטים אישיים

לאחר הכניסה לאתר הנחיתה הייעודי להונאה המשתמש מתבקש להירשם לדף (או לשירות) ולהזין פרטים אישיים ופרטי יצירת קשר בגון שם, כתובת אימייל ומספר טלפון. בחלק מהמקרים נציג של הנוכלים יוזמי ההונאה יוצר קשר באופן פרטי וישיר עם המשתמש דרך שיחת טלפון או אימייל ונותן לו פרטי גישה לפלטפורמת השקעות מזויפת, על מנת לייצר מצג שווא של מוצר פיננסי לגיטימי. תועדו גם מקרים בהם נעשה שימוש זדוני בהסוואה והתחזות של מספרי טלפון זרים למספרים ישראלים מקומיים, ולמעשה כאשר מתבצע נסיון להתקשר בחזרה למספר, הוא מוביל לקו מנותק או לקו של אדם שאין לו קשר להונאה. במקרים מסוימים מנגנון ההונאה מגיע לסיומו בשלב זה – לאחר איסוף פרטי כרטיס אשראי או חשבון בנק הנוכלים מנסים לבצע העברות כספיות מהקורבן. במקרים אחרים – שיפורטו בסעיפים הבאים – יש נסיון למשוך את הקורבנות להונאות מתמשכות ומורכבות יותר, הכוללות גם קשר ישיר וליווי מתמשך.


מודעת פייסבוק מזויפת המציעה מארז יוקרתי של מוצרי פסטה ברילה. בפועל, המשתמש מתבקש להזין פרטי אשראי לצורך "תשלום דמי משלוח", אך אינו מקבל דבר – ופרטי האשראי נשלחים לנוכלים.


מודעה ממומנת מציגה כביכול גיוס לעבודה בשיתוף פעולה עם AliExpress – "לדחוף מוצרים" ולקבל עמלה. הקורבן מבצע "משימות פשוטות" באתר שנראה לגיטימי, בולל צפייה במוצרים ו"עידוד רכישה", ומקבל תצוגה של רווחים מדומים. בהמשך נדרש ממנו להפקיד כספים על מנת "ליהנות מעמלות גבוהות יותר". למעשה, מדובר באתר הונאה – הפלטפורמה מזויפת, הכסף לא ניתן למשיכה, וההכנסות אינן אמיתיות.

### 5. קבלת גישה לשימוש בפלטפורמה המזויפת

באמצעות פרטי הגישה שקיבל מנציג ההונאה, המשתמש מתחבר לפלטפורמה שנראית מקצועית ואמינה. לדוגמה, פלטפורמה המציגה דאשבורד וגרפים של פעילות בשוק ההון וממשק המתחזה לפלטפורמת מסחר לגיטימית ואף מציג כפתור משיכת כספים (Withdrawal) על מנת לתת למשתמש תחושה שהוא צפוי להרוויח כסף בזכות השימוש במוצר ויוכל למשוך את הרווחים בבוא הזמן. כדי להתחיל בתהליך המסחר וההשקעה המשתמש מתבקש להפקיד סכום התחלתי.

### 6. איסוף פרטים ומידע פיננסי רגיש

כדי "להמשיך לסחור ולהשיג רווחים נוספים" הפלטפורמה מבקשת מהמשתמש להפקיד סכומים גדולים יותר ולספק פרטי חשבון בנק, תעודת זהות ומידע פיננסי אישי נוסף. בשלבים אלו, המשתמש כבר מחויב ומושקע רגשית וכלכלית בתהליך ובפלטפורמה, מה שמקשה עליו להטיל ספק ולהבין שהוא מנוצל ונופל קורבן להונאה. הנוכלים משתמשים בטכניקות של הנדסה חברתית כדי לתמרן את המשתמש להשקיע כספים נוספים וליצור תחושת דחיפות ואמון מזויף באמצעות שיחות אישיות, הצגת גרפים ונתונים פיקטיביים.

### 7. דרישות להמשך הפקדות כספים ואיסוף מידע רגיש

המעגל חוזר על עצמו עד שהמשתמש מבקש למשוך את הכספים, או שהפלטפורמה המזויפת מציגה למשתמש כי למעשה הפסיד את כל הכסף שהפקיד. כאשר המשתמש הנפגע מנסה ליצור קשר או להתלונן, הוא נתקל בחוסר מענה מוחלט לאחר שאיבד את הונו.

## ג. התאמת מאפייני ההונאה לקהל יעד והקשר מקומי בישראל

גל ההונאות ברשתות חברתיות באמצעות טכנולוגיות דיפ-פייק ומודעות ממומנות המתואר במסמך זה הוא תופעה גלובלית רחבת היקף, שאינה מוגבלת לישראל בלבד. עם זאת, בישראל, לתופעה יש מספר מאפיינים ייחודיים המותאמים לקהל המקומי:

### ■ שימוש בדמויות וגופים ישראליים מוכרים

ההונאות בישראל מתמקדות לעיתים קרובות בדמויות ציבוריות מקומיות, כגון פוליטיקאים, אישי ציבור, אנשי תקשורת וידוענים פופולריים בישראל. השימוש בדמויות אלו נועד להעצים את תחושת האמינות ולמשוך את תשומת ליבו של קהל היעד הישראלי. לדוגמה, באחד מסרטוני ההונאה ניתן לראות את ראש הממשלה בנימין נתניהו מצהיר כי הוא ביקש מאילון מאסק לפתוח פלטפורמת השקעות לשימוש ישראלים. דוגמאות נוספות ניתן לראות בסרטונים מזויפים של חברת אל-על, חדשות i24 או ערוץ 14, הזמרת נועה קירל, רותם סלע או של ירון אמיר, נגיד בנק ישראל אשר ממליץ על השקעות כוזבות.

### ■ שימוש במטבע המקומי

הצעות הונאתיות רבות בישראל מנוסחות בהתייחסות למטבע המקומי. לדוגמה, הבטחות לרווחים גבוהים בשקלים או הצעות השקעה הנוגעות לשוק ההון המקומי. אלמנט זה מגביר את תחושת האותנטיות של התוכן בקרב קורבנות פוטנציאליים. כמו כן, ניתן לראות קמפיינים המקדמים השקעות במטבע ישראלי דיגיטלי שעדיין לא קיים במציאות. זאת, בהתאמה לאירועים אקטואליים בישראל ובמקביל, ניצול של הצהרות על פיתוח אמיתי של מטבע שכזה ועוד.

### ■ התאמה תרבותית ולשונית

בניגוד להונאות דומות בעבר, תוכן ההונאה מותאם באופן מדויק לתרבות ולשפה הישראלית. התאמות אלו, הכוללות שימוש בביטויים מקומיים ובהתייחסות לאירועים עכשוויים, מקשות על זיהוי ההונאה ומגבירות את יכולתה לשכנע את הציבור המקומי. הסרטונים עם הדמויות הישראליות המוכרות מכילים לעיתים כתוביות של שפות נפוצות בישראל כמו השפה הרוסית בהקשר המקומי, המאפשרים טירגוט מדויק ומצג שווא של אמינות של המודעות לישראלים דוברי רוסית. התאמות אלה נעשות באמצעות כלי AI חדשים שהפכו את הניסוח והיצירה של טקסטים ותוכן מקומיים לקל ונגיש יותר עבור נוכלים.

מאפיינים ייחודיים אלו מדגישים את הצורך בפתרונות מותאמים ברמה הלאומית, תוך שימת דגש על הגברת המודעות והרגולציה הישראלית, לצד שיתוף פעולה בינלאומי רחב.




## ד. נקודות תורפה וכשלים בפעולת הפלטפורמות המאפשרות את ביצוע ההונאה

בעשור האחרון, ובעיקר בשנים האחרונות, נוכלים מאמצים במהירות כלים טכנולוגיים מתקדמים ומיישמים אותם עבור שיטות הונאה מתוחכמות, מבלי שהפלטפורמות החברתיות מייצרות מנגנוני זיהוי ואכיפה אפקטיביים.

להלן מספר כשלים עיקריים שהופכים את הפלטפורמות החברתיות למנגון הפצה חכם, ידידותי ויעיל עבור נוכלים וגורמי פשע:

### 1. שימוש בכלי פרסום דיגיטליים מתקדמים

הפלטפורמות החברתיות אשר המודל הכלכלי שלהן מתבסס על מכירת כלי פרסום, מידע של משתמשים וטרגוט קהלים מפולחים, מספקות ללקוחות שלהם כלי שיווק עוצמתיים. נוכלים משתמשים בכלים הללו על מנת להסוות את ההונאות. למשל, מודעות דינמיות מאפשרות להציג גרסאות שונות של אותה מודעה. משתמש עשוי לראות מודעה למוצר פשוט כמו בגד, אך בלחיצה עליה יופנה לתוכן שונה המכיל את ההונאה. תהליכי בקרת התוכן של הפלטפורמות, שמבוססים לעיתים על דגימות אקראיות או כלים אוטומטיים, מתקשים לאתר את ההבדלים ולהגיב במהירות מספקת.

### 2. שמירה על אנונימיות הגורמים המפרסמים

רמת האנונימיות וההגנה הגבוהה שמציעות הפלטפורמות למפרסמים ושחקנים זדוניים הפועלים באמצעותן, מקשה על זיהוי ואיתור הגורמים האחראים לתוכן מטעה או מזיק, דבר שמקשה על גופי חברה אזרחית, חוקרים וגורמי אכיפה, לפעול בצורה יעילה ולאתר את מקור ההונאות. זאת במיוחד בהעדר שיתוף פעולה מצד הפלטפורמות הגלובליות, שלרוב לא מפעילות נציגות ומענה מקומי במדינות השונות ורמת שקיפות נמוכה של הפלטפורמות והמשתמשים עבור גורמי אכיפה ובדיקה מדינתיים.

### 3. אישור מודעות עם דמויות פוליטיות ללא סימון גילוי נאות

הנוכלים מפרסמים מודעות הונאה הכוללות דמויות פוליטיות מזויפות – מבלי שהמודעות יסווגו כפרסום פוליטי המחייב גילוי נאות של זהות המפרסם. באופן זה, ניתן להפעיל קמפיינים שלמים המציגים לכאורה תמיכה של דמויות פוליטיות במסרים או מוצרים מפוקפקים, מבלי שהמערכות של הפלטפורמות יזהו את התוכן כתוכן רגיש או חשוד.

### 4. קושי בניטור מודעות "קשורות"

גם כאשר מודעה מזויפת מוסרת, הפלטפורמות לא מצליחות לנטר את כל המודעות האחרות של אותו מפרסם, וכך הן ממשיכות לפעול במקביל. תוקפים משתמשים בטכניקות כמו שכפול קמפיינים, שינוי ניסוח קל ומודלים של פרסום מבוזר, שמאפשרים להם לשכפל את ההונאה שוב ושוב תוך הימנעות מזיהוי. הפלטפורמות עצמן מתעדפות שימור הכנסות מפרסום ולכן אין להן אינטרס מספק להשקיע משאבים באכיפה אקטיבית נגד מודעות הונאה.

### 5. הפניית משתמשים לאתרי הונאה חיצוניים

תהליך ההונאה בנוי מכמה שלבים שמתחילים בחשיפת הקורבנות למודעות מזויפות, ממשיכים בהפניה לאתרים לא אמינים או לשירותים מזויפים, ולעיתים כוללים יצירת קשר ישיר עם המפעילים. תגובות מזויפות וחשבונות פיקטיביים תורמים לאמינות המדומה של התוכן.

## ה. כשלים עיקריים בטיפול הפלטפורמות והרשויות בהונאות

נסיון מצטבר מהשטח מראה כי עבור פלטפורמות הרשתות החברתיות, בעיית ההונאות הפיננסיות והנזק שהן מסבות למשתמשי הרשתות אינה בראש סדר העדיפויות שלהן. יתרה מכך, הפלטפורמות גורפות רווחים מאותן מודעות ממומנות המקדמות הונאות באמצעותן. ההתמודדות הלקויה עם תופעת ההונאות ברשתות החברתיות נובעת בין היתר מהעדר כלי זיהוי וניטור מקדימים שיחסמו מודעות זדוניות ועד למחסור במנגנוני דיווח ראויים ומדיניות אפקטיבית לטיפול בדיווחי משתמשים. להלן הכשלים המרכזיים בטיפול הפלטפורמות השונות באיומי הונאה פיננסית:

### כשלים באיתור מקדים, מניעה ואכיפה של קידום הונאות בפלטפורמות

- **העדר מנגנון אפקטיבי לזיהוי ואיתור מוקדם של הונאות**

הפלטפורמות מוצפות בקמפיינים ומודעות זדוניות ומתחזות שמפילות משתמשים בפח ומוציאות מהם כספים רבים. מקרים אלה היו יכולים להמנע באמצעים טכנולוגיים שונים כדי לאתר מבעוד מועד מודעות זדוניות על פי פרמטרים שונים – למשל הפניה לאתרים זדוניים, שימוש בהתחזות למותגים וגופים לגיטימיים או קשר לתשתיות הונאה מוכרות ממקרים קודמים.

### חוסר בזיהוי מקדים ואפקטיבי של סרטוני AI דזוניים

במרבית ההונאות הנסקרות במסמך זה, מודעות הקידום עושות שימוש בסרטוני AI גנרטיביים של דמויות מוכרות. על אף זאת, אין זיהוי וסימון אפקטיבי של סרטוני AI מתחזים בפלטפורמות – גם בהקשר של הונאות וגם בהקשרים רחבים יותר.

## כשלים באכיפה וטיפול בדיווחים על הונאות המקודמות בפלטפורמות

### הסרת מודעה בודדת ללא טיפול במערכת ההונאה

ברוב המקרים, כאשר מדווחים על מודעת הונאה והסרה אפקטיבית שלה, מודעות דומות עבור אותו מבצע הונאה ימשיכו להופיע בעמודים אחרים ללא הפרעה.

### היעדר סנקציות נגד עמודים שמפעילים הונאות

גם כאשר עמוד מפרסם תוכן הונאתי, הוא אינו נחסם או מוסר, מה שמאפשר לו להמשיך להפעיל מודעות חדשות בעתיד ולשכפל את ההונאה ללא מגבלות.

### יכולת שימור התשתית הדיגיטלית של הנוכלים

ללא אכיפה מספקת, אותם גורמים יכולים להשתמש שוב ושוב באותם עמודים, פרופילים ומערכות פרסום, מבלי שיידרשו להקים תשתית חדשה.

## כשלים במנגנוני הדיווח על תכנים מתחזים ומזויפים

### מנגנוני דיווח לא אפקטיביים

למשתמשי הפלטפורמות אין כלים מתקדמים ויעילים לדיווח על תכנים מפרים, וסקרים של איגוד האינטרנט הישראלי מהשנים האחרונות מראים כי משתמשים רבים נוטים שלא לדווח על פגיעות ואיומים בפלטפורמות בגלל חוסר אמון בנכונות שלהן לטפל בדיווחים.[2] במקרים רבים גם אין מנגנון מובנה ואפשרות לדיווח על הונאות שמקודמות באופן ממומן ועל המודעות המשויכות אליהן.

2. סקר מוגנות האינטרנט הישראלי: ניתוח ומגמות של שיח אלים, פגיעות רשת והתמודדות (2024-2025) – www.isoc.org.il/sts-data/isoc-il-survey-2025-online-violence-and-safety

### היעדר טיפול ומענה מספק לדיווחי גורמים מהימנים על הונאות

הפלטפורמות מפעילות תכניות גלובליות לשיתוף פעולה עם גופי חברה אזרחית מקומיים במדינות השונות המוגדרים כגורמי דיווח מהימנים (Trusted Flaggers) המדווחים על תופעות, מגמות וארועים חמורים של פגיעה ותוכן פוגעני. עם זאת, בתכניות אלה ובמנגנוני הדיווח והמענה שהם מקבלים ניתנת חשיבות ותשומת לב נמוכה לדיווחים על הונאות ופגיעה פיננסית באמצעות הפלטפורמות.

### היעדר מנגנוני דיווח על פעילות לא אותנטית מתואמת

היעדר מנגנון המאפשר דיווח על פעילות מתואמת של קבוצות חשבונות או עמודים המפיצים תוכן הונאתי פוגע ביכולת לדווח ולאבוף פעילות של לזהות ולפרק רשתות הונאה.

## תעדוף נמוך לטיפול באיומי הונאות פיננסיות בפלטפורמות

נושא ההונאות והעוקצים הפיננסיים מקבל עדיפות נמוכה יחסית במדיניות הבטיחות והאמון (Trust and Safety) של מרבית הפלטפורמות. הפלטפורמות החברתיות מצהירות כי פעולות שלא עולות לכדי פגיעות בעולם האמיתי (Real World Harm) כמו עבירות במרחב הפיזי אינן בראש סדר העדיפות שלהן. למעשה, נראה כי המדיניות של הפלטפורמות לא מייחסות נזק משמעותי להונאות הכלכליות הללו כאשר בפועל הן עלולות להביא להרס חייהם של המשתמשים. התופעה חריפה אף יותר במדינות עם רגולציה חלשה יותר בהן האכיפה והאחריות של שיתוף הפעולה בין הפלטפורמות כלפי להמשתמשים ולרשויות האכיפה אף נמוך יותר.

## העדר רגולציה ואכיפה מדינתית

בעוד שבמדינות ואזורים אחרים כמו האיחוד האירופי, בריטניה ואוסטרליה קיימת רגולציה מתקדמת המחייבת בין היתר שקיפות ופיקוח על השימוש במודעות, במדינות רבות אחרות, לרבות בישראל, חסרים מנגנוני פיקוח ואכיפה דומים בחוק. המידע המוצג על מודעות למשתמשים בפלטפורמות אשר נמצאים בתחומי האיחוד האירופאי זוכים לפירוט נרחב בהרבה מהמשתמשים הישראלים. משתמשים בישראל חשופים להונאות ללא אפשרות לקבל מידע מספק על המודעות והמפרסמים. מעבר לכך, אין בישראל כל רגולציה או פיקוח גם על יצירה, פרסום וקידום ממומן של תכנים שיווקיים ושכנועיים סינתטיים שנוצרו באמצעות בינה מלאכותית, הנמצאים כיום בלב תעשיית ההונאות הגלובלית.

# 1. המלצות עיקריות לתיקון המצב

## המלצות לפלטפורמות — תאגידי תקשורת דיגיטלית ורשתות חברתיות

- **בקרה, אביפה ושקיפות בפרסום ממומן**

על הפלטפורמות לחייב מפרסמים הנהנים ממנגנוני הפרסום והטירגוט המתקדמים שלהן, לספק גילוי נאות ולחשוף את זהות הגורם המממן. השקעת משאבים וכסף בקידום ממומן צריכה להיות מלווה באחריות ובשקיפות מלאה כלפי הציבור.

- **שיפור מנגנוני הבקרה על הפניה לאתרים ופלטפורמות הונאה חיצוניות**

השבתת מודעות ועמודים המפנים לאתרים שמזוהים כחלק ממנגנוני הונאה פעילים.

- **הסרה שיטתית ומערכתית של תשתיות הונאה**

טיפול מקיף והסרת כפילויות של מודעות הונאה וחסימת עמודים המשויכים למפרסמי הונאות חוזרים.

- **שיפור והטמעה של מנגנוני זיהוי תוכן AI** (בדגש על אודיו וסרטוני דיפ-פייק)

איתור או סימון תכנים מטעים ומנפולטיביים טרם הפצתם בפלטפורמות ובמיוחד בשימוש במנגנונים קידום ממומן.

- **פיתוח ושיפור מנגנוני זיהוי ומניעת פעילות מתואמת ולא אותנטית**

במגוון נושאים וסוגיות לרבות הונאות ומניפולציות מסחריות בנוסף למקרים פוליטיים וקמפייני השפעה של מדינות זרות.

- **השקעת משאבים נוספים לצורך הגברת בטיחות המשתמשים בהקשר המקומי**

הקצאת כוח אדם מיומן והתאמת מערכות וכלים לשפה ולתרבות המקומית במדינות קטנות, לרבות ישראל , ומתן מענה ישיר לפגיעות במוגנות ובטיחות המשתמשים.

- **על הפלטפורמות לספק מנגנוני דיווח נוחים ומענה שוטף ויעיל למשתמשי הקצה ומענה מקיף ויעיל עבור גופי דיווח מהימני** (Trusted Flaggers).

## המלצות למדינה — מחוקקים ורשויות אכיפה

הפגיעה הכלכלית הן ברמת האינדיבידואל והן ברמה הציבורית היא משמעותית, ולכן מחייבת הקצאת משאבים ציבוריים וסדרי עדיפויות לאיתור הפוגעים, טיפול בנפגעים והתמודדות עם התופעה, באמצעות חקירה, אכיפה והגברת המודעות הציבורית. להלן מספר המלצות לפיקוח וטיפול אכיפתי של המדינה והרשויות:

- **חקיקה מחייבת לשקיפות ואחריות של פלטפורמות דיגיטליות**

קידום רגולציה בהתאם לסטנדרטים בינלאומיים (כגון ה-DSA באיחוד האירופי) של אחריות ופיקוח על התנהלות הרשתות החברתיות, לרבות קביעת סנקציות משמעותיות על הפרות הפוגעות במוגנות ובטיחות המשתמשים, לרבות שימוש בפלטפורמות לקידום הונאות, עבריינות, התחזות ופגיעה כלכלית במשתמשים בישראל.

- **שיפור יכולות האכיפה והחקירה הדיגיטליות**

חיזוק הכלים העומדים לרשות גורמי האכיפה והרשויות לצורך התמודדות עם עבירות דיגיטליות, כולל הונאות כלכליות ועוקצים ברשתות החברתיות ושיפור הממשק וזרימת המידע בין הרשויות לבין הפלטפורמות.

- **העצמת יחידות אכיפה ייעודיות**

שדרוג המשאבים והיכולות של יחידות המתמחות בטיפול בהונאות מקוונות, תוך הבשרת כוח אדם מקצועי לטיפול בעבירות רשת מורכבות ומתן מענה גם ברמת האזרח לצורך זיהוי רשתות ותופעות רחבות היקף של הונאה ופגיעה כלכלית ברשת.

- **שיתופי פעולה בינלאומיים**

קידום שיתוף פעולה בין מדינות וארגונים רלוונטיים למעקב, איתור וטיפול בהונאות דיגיטליות חוצות גבולות, לרבות מאבק בהתערבות זרה בתהליכים דמוקרטיים ובמערכות בחירות.