|  |  |  |
| --- | --- | --- |
| **בנק ישראל**דוברות והסברה כלכלית | C:\Users\u34r\AppData\Local\Microsoft\Windows\INetCache\Content.Word\logo_70.png | ‏ירושלים, ‏ט' אייר, תשפ"ה‏7 מאי, 2025 |

הודעה לעיתונות:

**תיבה מתוך סקירת מערכת הבנקאות בישראל לשנת 2024 שתפורסם בקרוב:**

**היבטים צרכניים של תופעת ההונאות וצעדי הפיקוח על הבנקים להגנה על הצרכן מפני הונאות פיננסיות**

* **הונאות הן תופעה עולמית המתרחבת במהירות ומשפיעה על מערכות פיננסיות, צרכני שירותים פיננסיים והציבור הכללי. מעשי־ההונאה והמרמה, אף שמבוצעים לעיתים באמצעות התשתית והכלים הטכנולוגיים שהגופים הפיננסיים מעמידים לשימוש לקוחותיהם - אינם מכוונים בהכרח נגד המערכת הפיננסית או לקוחותיה אלא נגד אנשים, ארגונים, עסקים או גורמי ממשל באשר הם.**
* **פעולות מעשיות ("פרקטיקות") מיטביות שנהוגות במדיניות שונות לצמצום תופעת ההונאות והגנה על הציבור נשענות, לרוב, על שלוש רגליים: העלאת מודעות הציבור והעצמת הלקוח; צמצום התופעה וחסימת הונאות באמצעות שיפור הבקרות, הזיהוי, הניטור והתגובה למעשי־הונאה; הגברת האכיפה.**
* **בשנים האחרונות ניכרת בישראל, בדומה למדינות אחרות, עלייה בהיקפי ההונאות כלפי לקוחות המערכת הפיננסית. ההונאות פוגעות בכלל סוגי הלקוחות, אולם ניכרת התמקדות באוכלוסיות בעלות התמצאות פיננסית ודיגיטלית נמוכה, כגון קשישים ועולים ממדינות ברית־המועצות לשעבר.**
* **הפיקוח על הבנקים קבע כי "צמצום ומניעת תופעת ההונאות" יהיה אחד מיעדיו המרכזיים לשנים הקרובות, ונוסף על כך הוא פועל להבטיח שהצרכנים שנפלו קורבן למעשה־הונאה מקבלים את ההגנות הקבועות בחוק. פעילות הפיקוח מתמקדת בשני שלבים: בשלב המניעתי - טרם קרות ההונאה, ובשלב שלאחר קרות ההונאה - סיוע ללקוח שנפל קורבן להונאה.**
* **הפיקוח על הבנקים יוזם פעילויות להעלאת המודעות להונאות. בכלל־זאת יזם את "שבוע המודעות להונאות דיגיטליות", במסגרת פעילות "פורום חינוך פיננסי" בשיתוף משטרת ישראל, במטרה להעלות את מודעות הציבור הרחב לתופעת ההונאות הפיננסיות ולתת כלים ללקוח לזהות הונאות, להתמודד עימן ולמנוע אותן בזמן אמת. כמו־כן ייעד הפיקוח את הכינוס המקצועי השנתי שלו בשנת 2024 לנושא: "הונאות פיננסיות".**
* **הונאות הן תופעה מורכבת ורחבת־היקף המצריכה התמודדות רב־תחומית ושיתוף פעולה בין גורמים שונים בעלי־עניין. כל גורם, במסגרת תחומי האחריות שלו ובהתאם לצרכים שהוא מזהה, פועל לצמצום הונאות ומניעתן. מורכבות זו מחדדת את החשיבות של הגדרה ומינוי של גורם מתכלל ברמה הלאומית, אשר יקבע אסטרטגיה לאומית להתמודדות עם היבטיה השונים של התופעה ויעקוב אחר התקדמות הטיפול בנושא. כיום לא מוגדר גורם מתכלל בישראל.**
* **הפיקוח על הבנקים שותף בצוות בין־משרדי לטובת קידום פתרונות חוצי־מגזרים, הסרת חסמים קיימים והובלת שיתופי־פעולה בין כלל הגורמים הנוגעים בעניין בתחום ההונאות. בצוות חברים נציגים ממשרד התקשורת ומשטרת ישראל.**
* **הפיקוח על הבנקים פועל להסרת חסמים מאסדרים ("רגולטוריים") על־מנת לאפשר לגופים המפוקחים לשמור ולשתף מידע לשם זיהוי ומניעת הונאה ושימוש לרעה בחשבון או באמצעי־תשלום, בכפוף לדין.**
* **בנק ישראל והפיקוח על הבנקים מסייעים למשרד המשפטים להרחיב את ההגנה שניתנת ללקוחות באירועי הונאה.**
* **הפיקוח על הבנקים מקיים בקרות ובדיקות־אכיפה שוטפות כדי לוודא שהגופים המפוקחים מפתחים כלים לניטור וזיהוי מוקדם של הונאות, מפיקים לקחים מאירועי הונאה קודמים לצורך מניעת אירועים דומים בעתיד, ומפצים לקוחות שנפלו להונאה, בהתאם לדין.**

**מהן הונאות פיננסיות**

הונאות הן תופעה עולמית המתרחבת במהירות ומשפיעה על מערכות פיננסיות, צרכני שירותים פיננסיים והציבור הכללי. מעשי־ההונאה והמרמה, אף שמבוצעים לעיתים באמצעות התשתית והכלים הטכנולוגיים שמעמידים הגופים הפיננסיים לשימוש לקוחותיהם, אינם מכוונים בהכרח נגד המערכת הפיננסית או לקוחותיה אלא נגד אנשים, ארגונים, עסקים או גורמי ממשל באשר הם.

הונאה מתייחסת לכל פעולה של הולכת שולל או רמייה של גורם כלשהו. מעשה־הונאה יכול ללבוש צורות שונות ולהתבצע במגוון רחב של שיטות וערוצים ועל־כן הוא בבחינת שם כולל לסוגים שונים של עבירות שנעשות באמצעות הערמה או התחזות לאחר, תוך־כדי הפעלת מערכת לחצים או מניפולציות על הקורבן וטשטוש עקבות. הונאה פיננסית, אף שאין הגדרה אחידה ומקובלת, היא מקרה פרטי של הונאה שמטרתה השגת גישה לנכסיו הפיננסיים של הקורבן (אדם פרטי או גורם אחר) באמצעות הולכת שולל או רמיה. מרמה גם־היא מקרה פרטי של הונאה, שבו הקורבן משתכנע לעשות במו־ידיו פעולה יזומה של מסירת מידע או העברת כספים מתוך אמונה שלמה שהגורם שמבצע את פעולת ההונאה הוא גורם לגיטימי.

תופעת מעשי־ההונאה והמרמה מתאפיינת במורכבות רבה ובמנעד רחב של סוגים ורמות תחכום גבוהות. אלה מקשים על זיהויים של מעשי־המרמה, ניטורם ומניעתם. מעשי־הונאה ומרמה יכולים להיעשות במגוון רחב של שיטות וערוצים, לרבות מסחר מקוון, אתרי הכרויות, רשתות חברתיות, ‏פלטפורמות פרסום דיגיטליות, הודעות־טקסט ושיחות טלפון ובאמצעות שיטות ("טיפולוגיות") שונות שמותאמות לניצול חולשות ופגיעויות של אנשים או מערכות, דוגמת פשיעה רומנטית, הונאת השקעה, התחזות לגורם לגיטימי ועוד. בחלק מהמקרים אף מבוצעים מעשי־ההונאה באמצעות גורמים עבריינים מעולם הפשע המאורגן.

אחד האתגרים בטיפול בהונאות הוא חוסר־עקביות והעדר מתודולוגיה אחידה של סיווג ודיווח של הונאות. כך, למשל, במקרים שבהם נעשה הסיווג באמצעות או בעבור מוסדות פיננסיים, ניתן משקל גדול יותר לאפיון זהות הגורם שיזם את התשלום (Who - הלקוח עצמו או גורם שלישי) ולאמצעי־התשלום שדרכו נעשתה ההונאה (What - כרטיסי־תשלום, חשבון בנק, ארנקים דיגיטליים). במקרים שבהם נעשה הסיווג באמצעות או בעבור גורמי אכיפת־החוק, חברות תקשורת או ענקיות טכנולוגיה, ניתן משקל גדול יותר לפלטפורמה אשר דרכה נעשה מעשה־ההונאה ולטיפולוגיה שלה (Module).

מנקודת מבט פיננסית, נהוג לבצע הבחנה בין:

**"הונאה עם תשלום מורשה" (authorized fraud) -** מצב שבו גורם מורשה (הלקוח) יוזם ומבצע את פעולת התשלום. הונאה מסוג זה נעשית כתוצאה ממניפולציה שעשה מבצע ההונאה על המשלם לצורך ביצוע תשלום או מתן הנחיה לסַפָּק שירותי־התשלום להעביר את התשלום. הפעולה של המשלם נעשית בתום־לב ומתוך אמונה שהגורם שאליו הועבר התשלום הוא גורם לגיטימי. הונאות מסוג זה נהוג לכנות גם "מרמה" (scam). ראו לעיל.

**"הונאה עם תשלום שאינו מורשה" (unauthorized fraud)** - מצב שבו גורם שאינו מורשה יוזם ומבצע את פעולת התשלום. הונאות מסוג זה כוללות אובדן, גניבה (theft) או השגה במרמה misappropriation)) של נתוני כרטיס־התשלום או פרטי הזדהות והתחברות לחשבון הבנק, כאשר השגת הפרטים יכולה להיעשות באמצעות טכניקות של הנדסה חברתית (דוגמת Phishing, Smishing) או שימוש בקודים זדוניים באתרי מסחר או באמצעות כל שיטה אחרת.

**שיטות־פעולה מיטביות בעולם לצמצום תופעת ההונאות**

סקירה השוואתית שנעשתה בפיקוח על הבנקים לבחינת שיטות הפעולה (הפרקטיקות) המיטביות שנהוגות בקרב קובעי־מדיניות ומאסדרים פיננסיים וצרכניים ברחבי העולם לצמצום תופעת ההונאות והגנה על הציבור הכללי ועל לקוחות המערכת הפיננסית, העלתה כי על־אף השונות הגבוהה בכלים שמופעלים בכל מקום, אפשר לסווג אותם לשלושה תחומים מובחנים:

1. **העלאת מודעות הציבור והעצמת הלקוח בעזרת שיפור החינוך הפיננסי** - מתוך ההבנה שהלקוח הוא "קו־ההגנה" הראשון מול התופעה, יש לוודא כי הלקוחות מודעים לכך ומצוידים בידע וכלים נאותים לזהות מעשי־הונאה בזמן אמת ולהגן על עצמם טוב יותר. יוזמות של העלאת המודעות וההכשרה הן בדרך־כלל תוצר של שיתוף פעולה בין גופים מהמגזר הציבורי והפרטי. כך, למשל, בצרפת, איטליה וגרמניה יוזמות מסוג זה מקדמים הבנקים המרכזיים והמאסדרים הפיננסיים, בעוד שביפן ובסינגפור מקדמות את היוזמות רשויות אכיפת־החוק או רשויות ממשלתיות אחרות וגופים פרטיים. במדינות אחרות, דוגמת קנדה, מקדמים את הנושא הבנקים עצמם בשיתוף פעולה עם האיגודים המקצועיים ורשויות ממשלתיות שונות.
2. **צמצום התופעה וחסימת הונאות באמצעות שיפור הבקרות, הזיהוי, הניטור והתגובה למעשי־הונאה של כל בעלי העניין**, ובכלל זה של חברות־התקשרות, החברות הטכנולוגיות, המוסדות הפיננסיים ורשויות אכיפת־החוק. צעדים בתחום זה כוללים לרוב גורם מתכלל ברמה הלאומית (משרד ממשלתי או פונקציה ייעודית) שאמון על יצירת שיתופי־פעולה בין כלל הגורמים בעלי־העניין בתוך המדינה ומחוצה לה. שיתופי־הפעולה מקודמים מתוך הבנה שאת מעשה־ההונאה יש לעצור בנקודת ההתחלה ושמגזרים מסוימים הם בבחינת החולייה החלשה בביצוע מעשה־ההונאה. דוגמאות לשיתופי־פעולה שנמצאו בתחום זה כוללים הקמה של מאגרי־נתונים ושיתוף מידע בין השחקנים הפיננסיים לבין הרשויות ובין השחקנים הפיננסיים לבין עצמם (הונג־קונג, יפן). שיתוף־פעולה שכזה יאפשר חסימה של שיחות, זיהוי הודעות או אתרי מרשתת אשר באמצעותם נעשים מעשי־הונאה, הקלה על דיווח על מקרה־הונאה וסיוע ללקוח לזהות עסקאות לגיטימיות. בסינגפור למשל מפעילים המשטרה המקומית וארבעת הבנקים הגדולים במדינה "מרכז למניעת הונאות" (Anti-Scam Center - ASC), שעושה שימוש בטכנולוגיה של אוטומציה דיגיטלית לטובת זיהוי והתראת־לקוחות מפני מעשי־מרמה בזמן אמת באמצעות משלוח הודעות מסרון (SMS). דוגמה נוספת של "מרכז למניעת הונאות" אפשר למצוא גם באוסטרליה, שם הוקם ביולי 2023 מרכז (National Anti-Scam center (NASC)) במטרה למגר את התופעה באמצעות קידום שיתופי־פעולה עם גורמי ממשל, העצמת הלקוח, שיפור הדרכים לדווח על הונאות, שיפור מנגנון חילופי המידע בין הגורמים השונים ותמיכה ברשויות אכיפת־החוק.
3. **הגברת האכיפה באמצעות חיזוק רשויות אכיפת־החוק** - הקמת מערך לאיסוף ושיתוף מידע, שיפור מערך־הדיווח והחמרת הענישה נגד מבצעי מעשי־ההונאה. דוגמה טובה בהקשר זה אפשר למצוא בבריטניה, שם נכללת הקטגוריה של הגברת האכיפה בתוכנית האסטרטגית של הממשלה (משרד הפנים) לצמצום תופעת־ההונאות ולהגנה על הציבור.[[1]](#footnote-1) מטרתן של ההמלצות שמובאות בתוכנית האסטרטגית היא רדיפה אחר מבצעי־הונאות והעמדתם לדין, והן כוללות ארבעה צעדים משלימים: (א) חיזוק רשויות אכיפת־החוק הקיימות שאמונות על הטיפול במעשי־הונאה באמצעות העמדת תקציבים ובניית יכולות דיגיטליות, וכן באמצעות כוונה להקים מערך ייעודי ברמה הלאומית (National Fraud Squad) שינקוט גישה פעילה מבוססת־מודיעין, המתמקדת בהונאות ובפשיעה מאורגנת (שתכלול מעל 400 אנשי מקצוע וחוקרים); (ב) הקמה של "תא מודיעין" (UK Intelligence Community (UKIC)) שיסייע בזיהוי ובשיבוש מעשי־ההונאה ויקדם שיתופי־פעולה עם גורמים בין־לאומיים; (ג) בנייה של מערכת־דיווח שתקל על קורבנות של מעשי־הונאה לדווח על הונאות ותקל על רשויות אכיפת־החוק לנקוט פעולה בעקבות הדיווח; (ד) הסרה של חסמים שמונעים העמדה לדין והרשעה של מבצעי מעשי־הונאה.
4. **הגדרת גורם מתכלל ברמה הלאומית** - ממצא חשוב נוסף שעלה בסקירה ההשוואתית הוא החשיבות של הגדרה ומינוי של גורם מתכלל ברמה הלאומית שיקבע אסטרטגיה לאומית להתמודדות עם היבטיה השונים של תופעת ההונאות ויעקוב אחר התקדמות הטיפול בנושא. הגורם המתכלל עוסק לרוב בהגדת יעדים ובניסוח תוכנית הפעולה להשגתם והוא אמון על יצירת שיתופי־פעולה בין כל בעלי העניין הנוגעים בדבר ברמה הלאומית והבין־לאומית. כך, למשל, באנגליה הגורם המתכלל הוא משרד ממשלתי (משרד הפנים) ובסינגפור ואוסטרליה הגורם המתכלל הוא מרכז ייעודי שהוקם לטובת "מיגור תופעת ההונאות".

**הונאות פיננסיות בישראל**

גם בישראל, בדומה למדינות אחרות, ניכרת בשנים האחרונות עלייה בהיקפי ההונאות כלפי לקוחות המערכת הפיננסית. ההונאות פוגעות בכלל סוגי הלקוחות, אולם ניכרת התמקדות באוכלוסיות פגיעות, דוגמת אוכלוסיות בעלות התמצאות פיננסית ודיגיטלית נמוכה, קשישים ועולים ממדינות ברית־המועצות לשעבר.

מסקר שעשה הפיקוח על הבנקים במערכת הבנקאית עולה כי המערכת הבנקאית צופה שבשנת 2025 היקף תופעת ההונאות ימשיך ויתגבר, וכי מתווי הונאות פיננסיות שהיו שכיחים בשנת 2024 ימשיכו לאפיין גם את שנת 2025. נוסף על כך, המערכת הבנקאית צופה כי בשנת 2025 יגבר בהונאות השימוש בכלי AI לצורך התחזות כגון DEEPFAKE קולי וחזותי ועוד.

בשנת 2024 היו מתווי־ההונאה השכיחים ביותר במגזר הפיננסי הונאות שכוונו נגד לקוחות דוברי רוסית, יוצאי ברית־המועצות לשעבר, הקמת פלטפורמות מזויפות להשקעות בקריפטו ופיתוי לקוחות להשקעה בהן תוך־כדי הצגת מצג־שווא של השאת רווחים מהירים. ההונאות שזוהו התבצעו לרוב באמצעות הנדסה חברתית, ובתוך־כך קבלת מידע אישי או פיננסי באמצעות קריאה ללקוח בהודעת מסרון (SMS) לגשת לאתר מרשתת המתחזה לאתר מוכר או מוסד פיננסי ולבצע פעולת תשלום לגיטימית (פישינג-Phishing), או באמצעות בקשה בשיחה טלפונית עם הלקוח, תוך־כדי התחזות לגורם לגיטימי, כגון בנק או נציג רשויות מדינה (וישינג Vishing –). זאת ועוד, בשנה האחרונה התרבו אירועי־הונאה באמצעות השתלטות על קו הטלפון הנייד של הלקוח לצורך קבלת מידע פרטי על‏־אודותיו. השתלטות זו נעשית באמצעות ניוד הונאתי של המנוי הסלולרי של הלקוח או באמצעות שימוש בתוכנות שליטה־מרחוק על מכשירים סלולריים.

הונאות פיננסיות הן תופעה מורכבת ורחבת־היקף המצריכה התמודדות רב־תחומית ושיתוף־פעולה בין גורמים שונים הנוגעים בדבר, כאשר כל גורם פועל במסגרת תחומי האחריות שלו ובהתאם לצרכים שהוא מזהה לשם צמצום ומניעה של הונאות. הגורמים הנוגעים בדבר הם לרוב רשויות אכיפת־החוק, משרדי הממשלה, שחקנים ממגזר התקשורת, מאסדרים פיננסיים, מפקחים על מערכות התשלומים, ענקיות טכנולוגיה ועוד. בישראל לא מוגדר גורם מתכלל ברמה הלאומית להתמודדות עם הונאות.

**פעילות הפיקוח על הבנקים והגופים המפוקחים למניעה וצמצום של תופעת ההונאות והגנה על הצרכן**

הפיקוח על הבנקים קבע את הצמצום והמניעה של תופעת ההונאות במערכת הבנקאות כאחד מיעדיו המרכזיים לשנים הקרובות. נוסף על כך הוא פועל להבטיח שהצרכנים שנפלו קורבן למעשה־הונאה מקבלים את ההגנות הקבועות בחוק. פעילות הפיקוח מתמקדת בשני שלבים: בשלב המניעתי טרם קרות ההונאה, ובשלב שלאחר קרות ההונאה - סיוע ללקוח שנפל קורבן להונאה.

גם התאגידים הבנקאיים וחברות כרטיסי־האשראי נוקטים צעדים יזומים לטובת הגנה על לקוחותיהם, צמצום הנזקים וצמצום התופעה. בצעדים הנעשים: שימוש במערכות אבטחה כדי לנטר ולזהות התרחשויות אלה מוקדם ככל האפשר; יישום שדרוג והתאמה של מערכות בקרה; קביעה של נהלים ושל תהליכי עבודה סדורים; ניהול תהליכים להפקת לקחים; הכשרות עובדים; העלאת מודעות הלקוחות.

**הגברת מודעות הציבור**

הפיקוח על הבנקים יזם פעילויות להעלאת המודעות להונאות. בין פעילויות אלה ראוי לציין את "שבוע המודעות להונאות דיגיטליות", שהתקיים במסגרת פעילות "פורום חינוך פיננסי" שמוביל הפיקוח על הבנקים וחברים בו איגוד הבנקים, הבנקים והחכ"אות ובשיתוף עם משטרת ישראל. מיזם זה התקיים בשתי פעימות במהלך שנת 2024 ונועד להעלות את מודעות הציבור הרחב לתופעת ההונאות הפיננסיות ולתת ללקוח כלים לזהות הונאות, להתמודד עמן ולמנוע אותן בזמן אמת.

במסגרת הפעילויות הועברו כ-100 הרצאות בעשרות ערים ויישובים בכל רחבי הארץ, וכן חמש הרצאות מקוונות (וובינרים) - בעברית, ערבית ורוסית. בהרצאות אלה השתתפו אלפים. את פעילות ההסברה ליווה מסע־הסברה אשר הזמין את הציבור להשתתף בהרצאות. כמו־כן הוקם אתר מרשתת ייעודי ובו חומרים הנוגעים לעניין לשימוש הציבור הרחב.[[2]](#footnote-2)

נוסף על כך ייעד הפיקוח את הכינוס המקצועי השנתי שלו לנושא "הונאות פיננסיות". בכינוס הציגו מומחי תוכן שונים היבטים מגוונים בנושא ההונאות ובכלל־זאת נגיד בנק ישראל, המפקח על הבנקים ונציגים מהאקדמיה, רשויות אכיפת־החוק, מערך הסייבר ומהמערכת הפיננסית. הכינוס עסק בחשיבות הטיפול בהונאות ברמה הלאומית, באתגרים במניעת הונאות פיננסיות ובאחריות לפיצוי לקוחות באירועי הונאות. נכחו בו מאות מבכירי התעשייה הפיננסית בישראל והוא זכה לתהודה ציבורית נרחבת.

**שיתוף פעולה רב־משרדי לצמצום הונאות ומניעתן**

קידום המהלכים הנדרשים להתמודדות עם תופעת ההונאות הוא משימה מורכבת, הדורשת מאמצים משולבים, הקצאת משאבים והסרת חסמים חקיקתיים, אסדרתיים וטכנולוגיים. לנוכח אתגרים אלו, ובהמשך למהלכים שכבר מתקיימים, הוחלט להקים צוות עבודה ייעודי ורב־משרדי שיפעל לצמצום תופעת ההונאות, ובכלל זה ליישום פתרונות לאתגרים כגון חסימת גלישה לאתרים מתחזים (Phishing), מניעת SIM SWAP ומתקפות Smishing ו-Vishing.

בצוות חברים הגורמים הנוגעים בדבר מהפיקוח על הבנקים, משרד התקשורת ומשטרת ישראל, והוא פועל לקדם פתרונות חוצי־מגזרים, תוך־כדי הסרת חסמים קיימים והובלת שיתופי־פעולה בין כלל הגורמים המעורבים.[[3]](#footnote-3) נוסף על כך הוקמה ועדת־היגוי בהשתתפות המפקח על הבנקים, מנכ"לית משרד התקשורת וראש אגף חקירות ומודיעין במשטרת ישראל ובהובלת סגנית המפקח על הבנקים ומנהלת אגף טכנולוגיה, חדשנות וסייבר. ועדה זו מתכנסת בכל רבעון ובמסגרתה מוצגת התקדמות העבודה ומובאות סוגיות לדיון ולהחלטה.

**חקיקה ואסדרה**

חובות התאגידים הבנקאיים במניעה וצמצום של הונאות ופיצוי לקוחות באירועי הונאה מעוגנות בחוקים והוראות ניהול בנקאי תקין שונות. כך, למשל:

 הוראת ניהול בנקאי תקין מספר 472 בנושא: "סולקים וסליקת עסקאות בכרטיסי חיוב", אשר מעגנת חובות לתאגידים הבנקאיים בנסיבות שבהן במסגרת סליקת בית־העסק התעורר חשש ממשי כי בפעילותו של בית־עסק יש משום הונאת לקוחות, הטעיית לקוחות או הפעלת השפעה בלתי־הוגנת עליהם;

חוק שירותי תשלום, התשע"ט-2019 הקובע, בין היתר, את התנאים שבהם התאגידים הבנקאיים נדרשים לפצות לקוחות בגין שימוש לרעה באמצעי־התשלום שברשותם;

הוראת ניהול בנקאי תקין מספר 367 בנושא: "בנקאות בתקשורת" המעגנת, בין היתר, את חובות התאגידים הבנקאיים בעת ניטור פעילות חריגה בזמן אמת בחשבון לקוח לעשות הפקות־לקחים ולמידה מאירועי־הונאה לשם מניעת אירועים דומים בעתיד.

לשם מתן אפשרות לתאגידים הבנקאיים לשמור ולשתף מידע לצורך זיהוי ומניעת הונאה ושימוש לרעה בחשבון או אמצעי־תשלום, בכפוף לדין, הפיקוח על הבנקים פועל לעדכון הוראת ניהול בנקאי תקין מספר 367 שעניינה: "בנקאות בתקשורת".

נוסף על כך, לשם מניעה וצמצום הונאות־לקוחות באמצעות בתי־עסק, סייעו בנק ישראל והפיקוח על הבנקים למשרד המשפטים בקידום תיקון החוק שעניינו הגנה על הצרכן מפני בתי־עסק המבצעים הפרות בנסיבות מחמירות. התיקון מסמיך את הממונה על הגנת הצרכן והסחר ההוגן לקבוע כי בית־עסק הוא 'מפר בנסיבות מחמירות' ולהורות לכל חברות־האשראי להפסיק להעניק לו שירותי־סליקה ובכך למנוע המשך הונאה של לקוחות נוספים.

לשם סיוע ללקוחות שנפלו קורבן להונאה, בנק ישראל והפיקוח על הבנקים מסייעים בקידום תיקון חוק שירותי תשלום, התשע"ט-2019 באופן שירחיב את ההגנה הניתנת ללקוחות לפיצוי במקרים של הונאות באמצעות התחזות לתאגיד בנקאי ולרשויות מדינה, לצד הסדרת גבולות האחריות בין הלקוח לנותן שירותי־התשלום. כמו כן, הפיקוח מקדם אסדרה שתחייב את התאגידים הבנקאיים להעמיד מוקד טלפוני שיהיה זמין 24/7 לפניות לקוחות שנפלו קורבן להונאה או ללקוחות החושדים כי נעשתה אליהם פנייה מגורם הונאתי.

**פיקוח ואכיפה**

בשנת 2024 סקר הפיקוח את פעילותם של חלק מהגופים המפוקחים במטרה לוודא כי הם פועלים בהתאם לדין. במסגרת זו סקר הפיקוח את היערכות התאגידים הבנקאיים הסולקים בתי־עסק לניטור וטיפול בבתי־העסק החשודים בהונאת לקוחות מחזיקי הכרטיס. בין היתר נבדק יישום הוראות אסדרה, המחייבת את החברות לנטר את פעילות בתי־העסק על־פי תבחינים שונים ולהפסיק את ההתקשרות עם בית־העסק בנסיבות שבהן התעורר אצל סולק חשש ממשי כי בפעילותו של בית־עסק יש משום הונאת לקוחות, הטעיית לקוחות או הפעלת השפעה בלתי־הוגנת עליהם.

נוסף על כך קיים הפיקוח על הבנקים ביקורות בחלק מהתאגידים הבנקאיים כדי לוודא שהם מפתחים כלים לניטור ולזיהוי מוקדם של הונאות, עוקבים באופן שוטף אחר התפתחות שיטות־הונאה בארץ ובעולם ומפיקים לקחים מאירועי־הונאה קודמים לצורך מניעת אירועים דומים בעתיד.

מעבר לאמור, הפיקוח על הבנקים מסייע באופן שוטף ללקוחות המערכת הבנקאית אשר נפלו קורבן להונאה בחשבון הבנק או באמצעי־התשלום שבבעלותם ולא קיבלו מענה מספק מהגופים המפוקחים. בחלק מהמקרים מצא הפיקוח כי התאגידים הבנקאיים פעלו שלא כשורה והנחה אותם לפצות את הלקוחות בנזק שנגרם להם, ובחלק מהמקרים ניאותו התאגידים הבנקאיים לזכות את הלקוחות לפנים־משורת־הדין. במסגרת זו פוצו לקוחות המערכת הבנקאית בשנתיים האחרונות בסך כולל של כ-3.4 מיליוני ש"ח.

לסיכום, הונאות פיננסיות הן תופעה מורכבת ורחבת־היקף, המצריכה התמודדות רב־תחומית ושיתוף־פעולה בין גורמים שונים, והיא צפויה להימשך בשנים הקרובות. הפיקוח על הבנקים שילב את הנושא בתוכנית האסטרטגית שלו לשנים הקרובות וימשיך לפעול לקידום צעדים למניעת הונאות ולסיוע ללקוחות שנפגעו.

**הוראות הפיקוח על הבנקים והנחיות לגופים המפוקחים**

להלן דוגמאות להוראות הפיקוח על הבנקים והנחיות לגופים המפוקחים מתהליכי בקרה שנעשו במערכת הבנקאית להתמודדות עם הונאות פיננסיות:

1. **ניהול סיכון הונאות -** על התאגידים הבנקאיים לקבוע אסטרטגיה ומדיניות להתמודדות עם הונאות.
2. **ניטור פעילות חריגה** - על התאגידים הבנקאיים ליישם מנגנון אוטומטי לזיהוי וניטור של פעילות חריגה בחשבונות של לקוחות ובפרט בפעולות ברמת־סיכון גבוהה לצורך איתור של פעילות חשודה בזמן אמת.
3. **מעקב אחר התפתחות שיטות־ההונאה** - על התאגידים הבנקאיים לעקוב באופן שוטף אחר התפתחות שיטות־הונאה בארץ ובעולם ולבחון את הצורך בעדכון מנגנוני הניטור והבקרה בהתאם ולהפיק לקחים לצורך מניעת אירועים דומים בעתיד. לשם כך יעשו שימוש במידע ממקורות פנימיים וחיצוניים, לרבות משטרת ישראל ומנגנוני ביטחון נוספים.
4. **התרעה ללקוחות על פעילות חריגה** - על התאגידים הבנקאיים להתריע ללקוחותיהם על פעילות חריגה שזוהתה בחשבונותיהם.
5. **הגברת מודעות לקוחות** - על התאגידים הבנקאיים להדריך את לקוחותיהם באופן שיאפשר להם לזהות מעשי־הונאה בזמן אמת ולהגן על עצמם טוב יותר.
6. **השעיית עסקה או קבלת אישור מהלקוח** - בנסיבות שבהן זוהתה פעילות חריגה בחשבון לקוח, על התאגיד הבנקאי לשקול נקיטת אמצעים באופן מיידי כדוגמת השעיית עסקה או קבלת אשרור מהלקוח לעסקה.
7. **שיפור אמצעי הביטחון** - על התאגיד הבנקאי לפעול לשיפור מתמיד של אמצעי־הביטחון של אמצעי־התשלום וחשבונות הבנק.
8. **תיעוד אירועי־הונאה** - על התאגידים הבנקאיים לסווג ולתעד את אירועי־ההונאה על־מנת שיהיה אפשר להתחקות אחר מתווה ההונאה, השירות או המוצר שבהם נעשה שימוש במסגרת ההונאה, הנזק שנגרם לבנק והנזק שנגרם ללקוח במסגרת ההונאה.
9. **מדיניות לפיצוי לקוחות** - התאגידים הבנקאיים נדרשים לקבוע מדיניות אחידה ומוסדרת לפיצוי לקוחות שנפלו קורבן להונאה, בכפיפות להסדר האחריות בחוק.
10. **מדידת נזקי־הונאות** - על התאגידים הבנקאיים למדוד הונאות ונזקים שנגרמו ללקוחותיהם ולא רק לתאגיד הבנקאי עצמו.



**עצות וטיפים לציבור הלקוחות**

להלן מספר המלצות שיסייעו לכם להתגונן מפני הונאות:

1. **היו קנאים לפרטיותכם** - הפרטים הנשלחים אליכם בהודעת מסרוני SMS מהבנק או מחברת כרטיסי־האשראי, וכוללים קוד אימות שעליכם להזין לפני ביצוע עסקה או העברת כספים או מידע פיננסי רגיש אחר - הם מידע אישי שלכם ואין להעבירו לאיש. הבנקים וחברות כרטיסי־האשראי לעולם לא יפנו אליכם באופן יזום בבקשה לקבל מכם פרטים חסויים.
2. **הימנעו מכניסה לקישורים** - אמצו גישה כללית של חשדנות וזהירות. יש להימנע מכניסה לקישורים שנשלחים אליכם במסרוני SMS או לדואר האלקטרוני. אם יש ספק - אין ספק! מוטב שלא להיענות להודעה מאשר להיכנס לקישור לא מאובטח.
3. **לא מוסרים את כרטיס־האשראי לאף אדם** - הבנק וחברת כרטיסי־האשראי לעולם לא ישלחו שליח כדי לאסוף מכם את כרטיס־האשראי.
4. **הבנק שלכם מדבר עברית** -בעת קבלת שיחה טלפונית מגורם המזדהה כנציג בנק, חברת כרטיסי־אשראי או שוטר אשר אינו מדבר עברית, יש לבקש מהנציג לדבר עברית. ובכל מקרה לא מוסרים מידע אישי ופרטים פיננסיים.
5. **עברו לסיסמה חזקה וזיהוי ביומטרי** - הגדירו סיסמה הכוללת שילוב של אותיות, מספרים וסימנים ייחודיים, או עברו לזיהוי ביומטרי.
6. **כניסה זהירה לחשבון** - אל תתחברו לחשבון הבנק מתוך קישור הנשלח במסרון או בדואר אלקטרוני.
7. **לא מתקינים תוכנות השתלטות־מרחוק** – הונאות רבות מתרחשות לאחר התקנת תוכנת השתלטות־מרחוק על המחשב או המכשיר הסלולרי של הלקוח. יש להימנע מהתקנת תוכנות מסוג זה.
8. **שתפו את הקרובים אליכם** - בכל שיחה או פנייה חשודה התייעצו עם בני משפחה, עובדי בנק או חברת כרטיסי־אשראי שאתם מכירים.
9. **טעיתם ומסרתם מידע -** פנו מיד לבנק ולחברת כרטיסי־האשראי, דווחו על כך והגישו תלונה במשטרה.מסרו לבנק, לחברת כרטיסי־האשראי ולמשטרה את פרטי ההונאה המלאים - כל פרט חשוב!
10. **זיהיתם עסקה לא מוכרת** -
* הודיעו מיד לחברת כרטיסי־האשראי ולבנק!
* עיכוב בהודעה לבנק או לחברת כרטיסי־האשראי עלול לגרור השתתפות עצמית בנזק.
* דעו כי אתם מוגנים מפני נזק שיגרם לכם **לאחר** מסירת ההודעה.
* פיצוי על נזק שנגרם **לפני** מסירת ההודעה יינתן בהתאם לתנאי שנקבעו בסעיפים 24 ו-29 לחוק שירותי תשלום.
1. [Fraud Strategy: Stopping Scams and Protecting the Public](https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf) [↑](#footnote-ref-1)
2. [פעילות הפיקוח בתחום צרכנות בנקאית באתר בנק ישראל](https://www.boi.org.il/information/bank-paymnts/financial-education/50256) [↑](#footnote-ref-2)
3. [הודעה לעיתונות בדבר כתב המינוי של הצוות](https://boi.org.il/publications/pressreleases/25-9-2024)  [↑](#footnote-ref-3)