|  |  |  |
| --- | --- | --- |
| **בנק ישראל**דוברות והסברה כלכלית | C:\Users\u34r\AppData\Local\Microsoft\Windows\INetCache\Content.Word\logo_70.png | ‏ירושלים, ‏ז' סיון, תשפ"ה‏3 יוני, 2025 |

إعلان للصحافة:

**مقالة من تقرير مراجعة النظام المصرفي الإسرائيلي لعام 2024 الذي سيُنشر قريباً: الجوانب الاستهلاكية لظاهرة الاحتيال وتدابير هيئة الرقابة المصرفية لحماية المستهلكين من الاحتيال المالي**

* **الاحتيال هو ظاهرة عالمية سريعة الانتشار، تؤثر على الأنظمة المالية وعلى مستهلكي الخدمات المالية والجمهور عموماً. رغم أن الاحتيال والخداع يُمارسان أحياناً باستخدام البنية التحتية والأدوات التكنولوجية التي تُتيحها المؤسسات المالية لزبائنها، إلا أنهما لا يستهدفان النظام المالي أو زبائنه فقط، بل يستهدفان الأفراد والمؤسسات والشركات والجهات الحكومية أيضاً.**
* **ترتكز أفضل الممارسات المُستخدمة في مختلف السياسات للحد من ظاهرة الاحتيال وحماية الجمهور عادةً على ثلاثة عناصر أساسية: رفع مستوى وعي الجمهور وتمكين الزبون؛ الحد من ظاهرة الاحتيال ومنعه من خلال تحسين الضوابط وملاحظة الممارسات الاحتيالية ورصدها والتصدي لها؛ وتعزيز إنفاذ القانون.**
* **في السنوات الأخيرة، شهدت إسرائيل، كغيرها من الدول، زيادة في حجم عمليات الاحتيال ضد زبائن النظام المالي. يؤثر الاحتيال على جميع أنواع الزبائن، ولكن هناك تركيز واضح على الفئات ذات الثقافة المالية والرقمية المحدودة، مثل كبار السن والمهاجرين من الاتحاد السوفيتي السابق.**
* **حددت هيئة الرقابة على البنوك أن "الحد من ظاهرة الاحتيال ومنعها" سيكون أحد أهدافها الرئيسية للسنوات القادمة، كما ستعمل على ضمان حصول المستهلكين الذين وقعوا ضحية للاحتيال على الحماية المنصوص عليها في القانون. تركز أعمال الرقابة على مرحلتين: المرحلة الوقائية - قبل وقوع الاحتيال، ومرحلة ما بعد الاحتيال - لمساعدة الزبون الذي وقع ضحية للاحتيال.**
* **تُطلق دائرة الرقابة المصرفية العديد من أنشطةً التوعية بالاحتيال. ومنها على وجه الخصوص، "أسبوع التوعية بالاحتيال الرقمي"، ضمن فعالية "منتدى التثقيف المالي" بالتعاون مع شرطة إسرائيل، وذلك بهدف توعية الجمهور بظاهرة الاحتيال المالي وتزويد الزبائن بأدواتٍ للكشف عن الاحتيال ومواجهته والوقاية منه في الوقت الحقيقي. كما خصصت هيئة الرقابة مؤتمرها المهني السنوي لعام 2024 لموضوع "الاحتيال المالي".**
* **الاحتيال هو ظاهرة معقدة وواسعة تتطلب مواجهةً وتعاوناً متعدد التخصصات بين جهات مختلفة. تعمل كل جهة ضمن نطاق مسؤوليتها ووفقاً للاحتياجات التي تحددها، على الحد من الاحتيال ومنعه. يُبرز هذا التعقيد أهمية تحديد وتعيين جهة عليا على المستوى الوطني، تُحدد استراتيجية وطنية للتعامل مع جميع جوانب هذه الظاهرة، وترصد التقدم في معالجتها. في الوقت الحالي، لم يتم تحديد جهة كهذه في إسرائيل.**
* **تشارك هيئة الرقابة على البنوك في فريق وزاري لتعزيز حلول بين القطاعات، وإزالة العوائق القائمة، وقيادة التعاون بين جميع الجهات المعنية بمكافحة الاحتيال. يضم الفريق ممثلين عن وزارة الاتصالات وشرطة إسرائيل.**
* **تعمل هيئة الرقابة على البنوك على إزالة العوائق التنظيمية لتمكين الجهات الخاضعة للرقابة من الاحتفاظ بالمعلومات ومشاركتها بغرض تحديد ومنع الاحتيال وإساءة استخدام الحسابات أو وسائل الدفع، وفقاً للقانون.**
* **يُساعد بنك إسرائيل وهيئة الرقابة على البنوك وزارة العدل في توسيع نطاق الحماية المُقدمة للزبائن في حالات الاحتيال.**
* **تُجري هيئة الرقابة على البنوك عمليات تفتيش وتنفيذ مستمرة لضمان تطوير الجهات الخاضعة للرقابة لأدوات لرصد الاحتيال والكشف المُبكر عنه، واستخلاص الدروس من حالات الاحتيال السابقة لمنع تكرارها في المستقبل، وتعويض الزبائن الذين وقعوا ضحية للاحتيال وفقاً للقانون.**

**ما هو الاحتيال المالي؟**

الاحتيال هو ظاهرة عالمية سريعة الانتشار، تؤثر على الأنظمة المالية وعلى مستهلكي الخدمات المالية والجمهور عموماً. ورغم أن الاحتيال والخداع يُمارسان أحياناً باستخدام البنية التحتية والأدوات التكنولوجية نفسها التي تتيحها المؤسسات المالية لزبائنها، إلا أنهما لا يستهدفان فقط النظام المالي أو زبائنه، بل يستهدفان الأفراد والمؤسسات والشركات والهيئات الحكومية على حد سواء.

يشير الاحتيال إلى أي عمل من أعمال الخداع أو التحايل من قبل أي طرف. يمكن أن يتخذ الاحتيال أشكالاً مختلفة ويتم تنفيذه من خلال مجموعة واسعة من الأساليب والقنوات، وبالتالي فهو مصطلح شامل لأنواع مختلفة من الجرائم التي تُرتكب عن طريق الخداع أو انتحال الشخصية، مع ممارسة أسلوب من الضغط أو التلاعب على الضحية وإخفاء الآثار. على الرغم من عدم وجود تعريف موحد ومقبول للاحتيال المالي، إلا أنه حالة خاصة من الاحتيال تهدف إلى الوصول إلى الأصول المالية للضحية (فرد أو كيان آخر) من خلال الخداع أو التحايل. الاحتيال هو أيضاً حالة خاصة من الخداع، حيث يتم إقناع الضحية بالقيام شخصياً بعمل مثل تقديم المعلومات أو تحويل الأموال معتقداً أن الكيان الذي ينفذ الفعل الاحتيالي هو كيان شرعي.

تتميز ظاهرة الاحتيال والخداع بتعقيدها الشديد وتنوعها الواسع ومستوياتها العالية من التطور، مما يُصعّب تحديدها ورصدها ومنعها. يمكن ارتكاب الاحتيال والخداع عبر مجموعة واسعة من الأساليب والقنوات، بما في ذلك التجارة الإلكترونية، ومواقع المواعدة، وشبكات التواصل الاجتماعي، ومنصات الإعلانات الرقمية، والرسائل النصية، والمكالمات الهاتفية، ومن خلال أساليب متنوعة مُعدّة لاستغلال نقاط ضعف الأفراد أو الأنظمة، مثل الجريمة العاطفية، والاحتيال الاستثماري، وانتحال شخصية كيان قانوني، وغيرها. وفي بعض الحالات، يتم ارتكاب الاحتيال على يد عناصر إجرامية من عالم الجريمة المنظمة.

من تحديات التعامل مع الاحتيال عدم الاتساق وعدم وجود منهجية موحدة لتصنيف الاحتيال والإبلاغ عنه. على سبيل المثال، في الحالات التي يُجرى فيها التصنيف من خلال المؤسسات المالية أو لحسابها، يُعطى وزن أكبر لتحديد هوية الطرف الذي بدأ الدفع (Who - الزبون نفسه أو طرف ثالث) وطريقة الدفع التي ارتُكبت من خلالها عملية الاحتيال (What - بطاقات الدفع، الحساب المصرفي، المحافظ الرقمية). أما في الحالات التي يُجرى فيها التصنيف من خلال جهات إنفاذ القانون أو شركات الإعلام أو شركات التكنولوجيا العملاقة أو لحسابها، فيُعطى وزن أكبر للمنصة التي ارتُكبت من خلالها عملية الاحتيال وتصنيفها (Module).

من الناحية المالية، من المعتاد التمييز بين:

**"الاحتيال بدفع مُصرّح به" (authorized fraud)** - وهو حالة يقوم فيها طرف مُصرّح له (الزبون) ببدء وتنفيذ معاملة الدفع. يحدث هذا النوع من الاحتيال نتيجة تلاعب المُحتال بالضحية واقناعه بإجراء دفعة أو الطلب من مُقدّم خدمة الدفع بتنفيذ الدفع. يقوم الضحية بهذا الإجراء بحسن نية، معتقداً أن الطرف الذي حُوِّلت إليه الدفعة هو طرف شرعي. يُشار إلى هذا النوع من الاحتيال أيضاً باسم "النصب" (scam). انظر أعلاه.

**"الاحتيال بدفع غير مصرح به" (unauthorized fraud)** - حالة يقوم فيها طرف غير مصرح له ببدء وتنفيذ معاملة دفع. يشمل هذا النوع من الاحتيال فقدان أو سرقة (theft) أو الاستيلاء الاحتيالي (misappropriation) على بيانات بطاقة الدفع أو معلومات الهوية ومعلومات تسجيل الدخول إلى الحساب المصرفي، حيث يتم الحصول على التفاصيل من خلال تقنيات الهندسة الاجتماعية (مثل التصيد الاحتيالي والاحتيال عبر الرسائل النصية القصيرة Phishing, Smishing) أو استخدام برمجيات خبيثة على مواقع التجارة أو بأي طريقة أخرى.

**أفضل الممارسات العالمية للحد من الاحتيال**

كشفت دراسة مقارنة أجرتها هيئة الرقابة على البنوك لدراسة أفضل الممارسات التي يتبعها صناع السياسات والجهات التنظيمية المالية والاستهلاكية حول العالم للحد من الاحتيال وحماية الجمهور وزبائن النظام المالي، أنه على الرغم من التباين الكبير في الأدوات المستخدمة في كل مكان، إلا أنه يمكن تصنيفها إلى ثلاثة مجالات واضحة:

1. **رفع مستوى وعي الجمهور وتمكين الزبائن من خلال تحسين التوعية المالية** - إدراكاً منهم أن الزبائن هم "خط الدفاع" الأول ضد هذه الظاهرة، من الضروري ضمان وعيهم بهذا الأمر وتزويدهم بالمعرفة والأدوات المناسبة للكشف الفوري عن الاحتيال وحماية أنفسهم بشكل أفضل. تُعدّ مبادرات التوعية والتدريب عادةً ثمرة تعاون بين مؤسسات القطاعين العام والخاص. على سبيل المثال، في فرنسا وإيطاليا وألمانيا، تُروّج البنوك المركزية والهيئات التنظيمية المالية لهذه المبادرات، بينما في اليابان وسنغافورة، تُروّج لها جهات إنفاذ القانون أو جهات حكومية أخرى وجهات خاصة. في دول أخرى، مثل كندا، تُروّج البنوك نفسها لهذه المسألة بالتعاون مع المؤسسات المهنية وجهات حكومية مختلفة.
2. **الحد من ظاهرة الاحتيال وايقافها من خلال تحسين الرقابة والرصد والتعرف والرصد والاستجابة من قبل جميع الجهات المعنية،** بما في ذلك شركات الاتصالات وشركات التكنولوجيا والمؤسسات المالية وسلطات إنفاذ القانون. وعادةً ما تتضمن الخطوات في هذا المجال جهة اشرافية على المستوى الوطني (وزارة حكومية أو إدارة متخصصة) مسؤولة عن بناء شراكات بين جميع الجهات المعنية داخل الدولة وخارجها. يتم إنشاء الشراكات من منطلق إدراك ضرورة وقف الاحتيال من مصدره، وأن قطاعاتٍ معينة تُمثل الحلقة الأضعف في ارتكابه. من الأمثلة على الشراكات الموجودة في هذا المجال إنشاء قواعد بيانات وتبادل المعلومات بين الجهات الفاعلة المالية والسلطات، وبين الجهات الفاعلة المالية نفسها (هونغ كونغ، اليابان). هذا التعاون سيمكن من حظر المكالمات، وتحديد الرسائل أو المواقع الإلكترونية التي تُرتكب من خلالها أعمال الاحتيال، وتسهيل الإبلاغ عن حالات الاحتيال، ومساعدة الزبون على تحديد المعاملات المشروعة. في سنغافورة على سبيل المثال، تُدير الشرطة المحلية وأكبر أربعة بنوك في البلاد "مركزاً لمكافحة الاحتيال" (Anti-Scam Center - ASC)، يستخدم تقنية الأتمتة الرقمية لتحديد الزبائن وتنبيههم فوراً إلى أي عملياتاحتيال عبر إرسال رسائل نصية قصيرة (SMS). في أستراليا أيضاً أُنشئ مركز لمكافحة الاحتيال(National Anti-Scam center (NASC)) في تموز 2023 بهدف القضاء على هذه الظاهرة من خلال تعزيز التعاون مع الجهات الحكومية، وتمكين الزبائن، وتحسين سبل التبليغ عن الاحتيال، وتحسين آلية تبادل المعلومات بين مختلف الجهات، ودعم سلطات إنفاذ القانون.
3. **تعزيز إنفاذ القانون من خلال تعزيز أجهزة إنفاذ القانون** - إنشاء نظام لجمع المعلومات وتبادلها، وتحسين نظام التبليغ، وتشديد العقوبات على مرتكبي الاحتيال. من الأمثلة الجيدة على ذلك في المملكة المتحدة، حيث أُدرجت فئة تعزيز إنفاذ القانون في الخطة الاستراتيجية للحكومة (وزارة الداخلية) للحد من الاحتيال وحماية الجمهور.[[1]](#footnote-1) تهدف التوصيات الواردة في الخطة الاستراتيجية إلى ملاحقة مرتكبي الاحتيال ومحاكمتهم، وتشمل أربع خطوات متكاملة: (أ) تعزيز أجهزة إنفاذ القانون القائمة المسؤولة عن التعامل مع الاحتيال من خلال توفير الميزانيات وبناء القدرات الرقمية، بالإضافة إلى إنشاء نظام متخصص على المستوى الوطني (National Fraud Squad) يتبع نهجاً استخباراتياً فعالاً، يركز على الاحتيال والجريمة المنظمة (ويضم أكثر من 400 متخصص وباحث)؛ (ب) إنشاء "خلية استخبارات" (UK Intelligence Community (UKIC)) للمساعدة في رصد الاحتيال وإيقافه، وتعزيز التعاون مع الوكالات الدولية؛ (ج) بناء نظام تبليغ يسهل على ضحايا الاحتيال التبليغ عن الاحتيال ويساعد سلطات إنفاذ القانون على اتخاذ الإجراءات اللازمة بعد التبليغ؛ (د) إزالة الحواجز التي تمنع مقاضاة مرتكبي الاحتيال وإدانتهم.
4. **تحديد هيئة مسؤولة على المستوى الوطني** - من النتائج المهمة التي توصلت إليها المراجعة المقارنة أهمية تحديد وتعيين هيئة مسؤولة على المستوى الوطني، تُحدد استراتيجية وطنية للتعامل مع مختلف جوانب ظاهرة الاحتيال، وترصد التقدم في معالجتها. عادةً ما تُعنى هذه الهيئة المتكاملة بتحديد الأهداف ووضع خطة عمل لتحقيقها، وهي مسؤولة عن بناء علاقات تعاون بين جميع الجهات المعنية على المستويين الوطني والدولي. في بريطانيا على سبيل المثال، تُمثل الهيئة المسؤولة وزارة حكومية (وزارة الداخلية)، وفي سنغافورة وأستراليا، تُمثل الهيئة المتكاملة مركزاً متخصصاً أُنشئ بغرض "القضاء على ظاهرة الاحتيال".

**الاحتيال المالي في إسرائيل**

شهدت إسرائيل، كغيرها من الدول، في السنوات الأخيرة زيادةً في حجم عمليات الاحتيال ضد زبائن النظام المالي. يؤثر الاحتيال على جميع فئات الزبائن، مع تركيز واضح على الفئات السكانية الضعيفة، مثل الفئات ذات الثقافة المالية والرقمية المحدودة، وكبار السن، والمهاجرين من الاتحاد السوفيتي السابق.

أظهر استطلاع أجرته هيئة الرقابة على البنوك في النظام المصرفي أن النظام المصرفي يتوقع استمرار تزايد نطاق ظاهرة الاحتيال في عام 2025، وأن مؤشرات الاحتيال المالي التي كانت في عام 2024 ستستمر خلال عام 2025. بالإضافة إلى ذلك، يتوقع النظام المصرفي أن يزداد في عام 2025 استخدام أدوات الذكاء الاصطناعي AI لانتحال الشخصية، مثل الصوت والصورة بتقنية DEEPFAKE.

في عام 2024 كانت أكثر أنواع الاحتيال شيوعاً في القطاع المالي تلك التي تستهدف زبائن ناطقين بالروسية من دول الاتحاد السوفيتي السابق، من خلال إنشاء منصات استثمارية مزيفة للعملات المشفرة وإغراء الزبائن بالاستثمار فيها وتقديم صورة زائفة عن أرباح سريعة. نُفذت عمليات الاحتيال المُكتشفة غالباً من خلال الهندسة الاجتماعية، حيث تم الحصول على معلومات شخصية أو مالية عن طريق التواصل مع الزبائن عبر رسالة نصية قصيرة (SMS) للدخول إلى موقع إلكتروني من شبكة تنتحل صفة موقع إلكتروني أو مؤسسة مالية معروفة وإجراء عملية دفع قانونية (التصيد الاحتيالي Phishing)، أو عن طريق الاتصال بالزبون عبر الهاتف وانتحال صفة جهة قانونية، مثل بنك أو ممثل حكومي (Vishing). علاوة على ذلك، ازدادت في العام الماضي حوادث الاحتيال التي تنطوي على الاستيلاء على خط الهاتف المحمول للزبون للحصول على معلومات خاصة عنه. يتم هذا الاستيلاء من خلال نسخ اشتراك الهاتف المحمول للزبون بشكل احتيالي أو من خلال استخدام برامج التحكم عن بُعد على الأجهزة المحمولة.

الاحتيال المالي هو ظاهرة معقدة وواسعة النطاق تتطلب استجابةً وتعاوناً متعدد التخصصات بين مختلف الأطراف المعنية، حيث يعمل كل طرف في نطاق مسؤولياته ووفقاً للاحتياجات التي يحددها للحد من الاحتيال ومنعه. عادةً ما تكون الأطراف المعنية هي سلطات إنفاذ القانون، والوزارات الحكومية، والجهات الفاعلة في قطاع الاتصالات، والهيئات التنظيمية المالية، ومراقبي أنظمة الدفع، وشركات التكنولوجيا العملاقة، وغيرها. في إسرائيل، لا توجد جهة شاملة محددة على المستوى الوطني للتعامل مع الاحتيال.

**أنشطة هيئة الرقابة على البنوك والجهات الخاضعة للرقابة لمنع وتقليص ظاهرة الاحتيال وحماية المستهلك**

حددت هيئة الرقابة على البنوك الحد من ظاهرة الاحتيال في النظام المصرفي ومنعها كأحد أهدافها الرئيسية للسنوات القادمة. بالإضافة إلى ذلك، تعمل الهيئة على ضمان حصول المستهلكين الذين وقعوا ضحايا للاحتيال على الحماية المنصوص عليها في القانون. تركز أنشطة الرقابة على مرحلتين: مرحلة الوقاية قبل وقوع الاحتيال، ومرحلة ما بعد وقوعه - مساعدة الزبون الذي وقع ضحية للاحتيال.

تتخذ المؤسسات المصرفية وشركات بطاقات الائتمان أيضاً خطوات استباقية لحماية زبائنها، وتقليل الأضرار، والحد من هذه الظاهرة. تشمل هذه الخطوات: استخدام أنظمة أمنية لرصد هذه الحالات وتحديدها في أقرب وقت ممكن؛ وتطبيق التحديثات والتعديلات على أنظمة التحكم؛ ووضع إجراءات وآليات عمل منتظمة؛ وإدارة العمليات لاستخلاص الدروس؛ وتدريب الموظفين؛ وزيادة وعي الزبائن.

**زيادة وعي الجمهور**

بادرت هيئة الرقابة على البنوك بأنشطة للتوعية بجرائم الاحتيال. من بين هذه الأنشطة "أسبوع التوعية بالاحتيال الرقمي"، والذي نُظم ضمن فعالية "منتدى التثقيف المالي" التي تقودها هيئة الرقابة على البنوك، وتضم في عضويتها اتحاد البنوك والبنوك وشركات بطاقات الائتمان، وبالتعاون مع شرطة إسرائيل. نُفذت هذه المبادرة على مرحلتين خلال عام 2024، بهدف توعية الجمهور بظاهرة الاحتيال المالي، وتزويد الزبائن بالأدوات اللازمة لكشف الاحتيال ومواجهته ومنعه في الوقت الحقيقي.

في إطار الأنشطة، أُلقيت حوالي 100 محاضرة في عشرات المدن والبلدات في جميع أنحاء البلاد، بالإضافة إلى خمس محاضرات عبر الانترنت (ندوات إلكترونية) باللغات العبرية والعربية والروسية. وقد شارك في هذه المحاضرات آلاف الأشخاص. رافق هذا النشاط التوعوي حملة إعلامية تدعو الجمهور للمشاركة في المحاضرات. كما أُنشئ موقع إلكتروني خاص يحتوي على مواد ذات صلة بالموضوع لخدمة الجمهور.[[2]](#footnote-2)

بالإضافة إلى ذلك، خصصت هيئة الرقابة مؤتمرها المهني السنوي لموضوع "الاحتيال المالي". في المؤتمر، عرض خبراء متخصصون جوانب متنوعة من موضوع الاحتيال، بمن فيهم محافظ بنك إسرائيل، والمراقب على البنوك، وممثلون عن الأوساط الأكاديمية، وهيئات إنفاذ القانون، والنظام السيبراني، والنظام المالي. تناول المؤتمر أهمية مواجهة الاحتيال على المستوى الوطني، والتحديات التي تواجه منع الاحتيال المالي، ومسؤولية تعويض الزبائن في حالات الاحتيال. وقد حضره مئات من كبار الشخصيات في القطاع المالي في إسرائيل، وحظي باهتمام جماهيري واسع.

**التعاون بين الوزارات للحد من الاحتيال ومنعه**

يُعد تطبيق الخطوات اللازمة للتعامل مع ظاهرة الاحتيال مهمةً معقدة تتطلب تضافر الجهود وتخصيص الموارد وإزالة العوائق التشريعية والتنظيمية والتكنولوجية. على ضوء هذه التحديات، واستمراراً للخطوات الجارية، تقرر تشكيل فريق عمل وزاري متخصص للعمل على الحد من ظاهرة الاحتيال، بما في ذلك تطبيق حلول للتحديات، مثل حظر تصفح المواقع الإلكترونية الاحتيالية (Phishing)، ومنع هجمات SIM SWAP، والتصيد الاحتيالي Smishing، و Vishing.

يضم الفريق جهات من هيئة الرقابة على البنوك، ووزارة الاتصالات، وشرطة إسرائيل، ويعمل على تعزيز الحلول المشتركة بين القطاعات، مع إزالة العوائق القائمة وتشجيع التعاون بين جميع الأطراف المعنية.[[3]](#footnote-3) إضافةً إلى ذلك، تم تشكيل لجنة توجيهية بمشاركة المراقب على البنوك، والمديرة العامة لوزارة الاتصالات، ورئيس قسم التحقيقات والاستخبارات في شرطة إسرائيل، ويرأسها نائب المراقب على البنوك ومدير قسم التكنولوجيا والابتكار والسيبرانية. تجتمع هذه اللجنة كل ثلاثة أشهر لاستعراض سير العمل وطرح القضايا للنقاش واتخاذ القرارات.

**التشريعات والتنظيمات**

تتضمن قوانين وتوجيهات الإدارة المصرفية السليمة التزامات المؤسسات المصرفية بمنع الاحتيال والحد منه وتعويض الزبائن في حالات الاحتيال. على سبيل المثال:

توجيه الإدارة المصرفية السليمة رقم 472 بشأن "إجراءات ومؤسسات تسوية معاملات بطاقات الخصم"، والذي يُحدد التزامات المؤسسات المصرفية في الحالات التي ينشأ فيها قلق حقيقي من أن أنشطة الشركة تنطوي على احتيال على الزبائن أو تضليلهم أو ممارسة تأثير غير نزيه عليهم في إطار التسويات التجارية.

قانون خدمات الدفع لعام 2019، والذي يحدد من بين أمور أخرى، الشروط التي يتعين بموجبها على المؤسسات المصرفية تعويض الزبائن عن سوء استخدام وسائل الدفع التي بحوزتهم؛ وتوجيه الإدارة المصرفية السليمة رقم 367 بشأن "الخدمات المصرفية عبر الاتصالات"، والذي ينص من بين أمور أخرى، على التزامات المؤسسات المصرفية عند رصد أي نشاط غير عادي في حساب الزبون في الوقت الفعلي لاستخلاص الدروس والتعلم من حوادث الاحتيال من أجل منع وقوع أحداث مماثلة في المستقبل.

لتمكين المؤسسات المصرفية من الاحتفاظ بالمعلومات ومشاركتها بغرض كشف ومنع الاحتيال وإساءة استخدام الحسابات أو وسائل الدفع، وفقاً للقانون، تعمل هيئة الرقابة على البنوك على تحديث توجيه الإدارة المصرفية السليمة رقم 367، والمتعلق بـ"الخدمات المصرفية عبر وسائل الاتصال". إضافةً إلى ذلك، ولمنع احتيال الشركات على الزبائن والحد منه، ساعد بنك إسرائيل وهيئة الرقابة على البنوك وزارة العدل في تعديل قانون حماية المستهلك من الشركات التي ترتكب مخالفات في ظروف مشددة. يُخول هذا التعديل مسؤول حماية المستهلك والتجارة العادلة صلاحية تحديد ما إذا كانت الشركة "مخالفة في ظروف مشددة" وإصدار أمر إلى جميع شركات الائتمان بالتوقف عن تقديم خدمات التسوية لصالحها، مما يمنع المزيد من احتيالها على زبائن آخرين.

لمساعدة الزبائن الذين وقعوا ضحية للاحتيال، يسعى بنك إسرائيل وهيئة الرقابة على البنوك على تعديل قانون خدمات الدفع لعام 2019، بحيث يُوسّع نطاق الحماية المُقدّمة للزبائن من حيث التعويض في حالات الاحتيال بانتحال صفة مؤسسة مصرفية أو سلطات حكومية، بالإضافة إلى تنظيم حدود المسؤولية بين الزبون ومُقدّم خدمة الدفع. كما تُشجّع الهيئة على وضع لوائح تُلزم المؤسسات المصرفية بإنشاء مقسم هاتفي متاح على مدار الساعة طوال أيام الأسبوع لخدمة الزبائن الذين وقعوا ضحايا للاحتيال أو الذين يشتبهون في تلقيهم اتصالات من جهات احتيالية.

**الرقابة وإنفاذ القانون**

في عام 2024، راجعت هيئة الرقابة أنشطة بعض الجهات الخاضعة للرقابة لضمان عملها وفقاً للقانون. في هذا السياق، راجعت الهيئة استعدادات المؤسسات المصرفية التي تُجري المدفوعات للشركات لمراقبة الشركات المشتبه في احتيالها على حاملي البطاقات والتعامل معها. من بين أمور أخرى، تم فحص تطبيق الأحكام التنظيمية التي تُلزم الشركات بمراقبة أنشطة الشركات وفقاً لمعايير مُختلفة، وإنهاء التعاقد مع الشركة في الحالات التي يكون فيها لدى المُشتري قلق حقيقي من أن أنشطة الشركة تنطوي على احتيال على الزبائن، أو تضليلهم، أو ممارسة تأثير غير نزيه عليهم.

تُجري هيئة الرقابة على البنوك أيضاً عمليات تدقيق على بعض المؤسسات المصرفية لضمان تطويرها لأدوات رصد الاحتيال والكشف المبكر عنه، والمتابعة المنتظمة لتطور أساليب الاحتيال في إسرائيل وحول العالم، واستخلاص الدروس من حوادث الاحتيال السابقة لمنع وقوع حوادث مماثلة في المستقبل.

بالإضافة إلى ذلك، تُساعد هيئة الرقابة على البنوك بانتظام زبائن النظام المصرفي الذين وقعوا ضحية احتيال في حساباتهم المصرفية أو وسائل الدفع الخاصة بهم ولم يتلقوا رداً مُرضياً من الجهات الخاضعة للرقابة. في بعض الحالات، وجدت هيئة الرقابة أن المؤسسات المصرفية تصرفت بشكل غير لائق، وأصدرت تعليماتها لهم بتعويض الزبائن عن الأضرار التي لحقت بهم، وفي بعض الحالات، وافقت المؤسسات المصرفية على تعويض الزبائن وفقاً للقانون. في هذا الإطار، تم تعويض زبائن النظام المصرفي في العامين الماضيين بما مجموعه حوالي 3.4 مليون شيكل.

في الختام، يُعدّ الاحتيال المالي ظاهرةً معقدةً وواسعة النطاق، تتطلب جهوداً متعددة التخصصات وتعاوناً بين مختلف الجهات، ومن المتوقع استمرارها في السنوات القادمة. وقد أدرجت هيئة الرقابة على البنوك هذه القضية في خطتها الاستراتيجية للسنوات القادمة، وستواصل العمل على تعزيز إجراءات منع الاحتيال ومساعدة الزبائن المتضررين.

**تعليمات الرقابة على البنوك وتوجيهاتها للجهات الخاضعة للرقابة**

فيما يلي أمثلة على توجيهات وإرشادات الرقابة المصرفية للجهات الخاضعة للرقابة، والمستمدة من عمليات الرقابة المُطبقة في النظام المصرفي لمكافحة الاحتيال المالي:

1. **إدارة مخاطر الاحتيال** - يجب على المؤسسات المصرفية وضع استراتيجية وسياسة للتعامل مع الاحتيال.
2. **مراقبة الأنشطة غير الطبيعية** - يجب على المؤسسات المصرفية تطبيق آلية لتحديد ومراقبة الأنشطة غير الطبيعية في حسابات الزبائن، وخاصة الأنشطة عالية المخاطر، للكشف عن أي نشاط مشبوه في الوقت الحقيقي.
3. **متابعة تطور أساليب الاحتيال** - يجب على المؤسسات المصرفية متابعة تطور أساليب الاحتيال في إسرائيل وحول العالم بانتظام، ودراسة الحاجة إلى تحديث آليات المراقبة وفقاً لذلك، واستخلاص الدروس لمنع تكرار حوادث مماثلة في المستقبل. لتحقيق ذلك، سيتم استخدام المعلومات من مصادر داخلية وخارجية، بما في ذلك شرطة إسرائيل وأجهزة أمنية أخرى.
4. **تنبيه الزبائن بشأن أي نشاط غير اعتيادي** - يجب على المؤسسات المصرفية تنبيه زبائنها بشأن أي نشاط غير اعتيادي يُكتشف في حساباتهم.
5. **زيادة وعي الزبائن** - يجب على المؤسسات المصرفية توجيه زبائنها بطريقة تُمكّنهم من كشف الاحتيال في الوقت الحقيقي وحماية أنفسهم بشكل أفضل.
6. **تعليق المعاملة أو طلب موافقة الزبون** - في حال رصد نشاط غير اعتيادي في حساب الزبون، يجب على المؤسسة المصرفية النظر في اتخاذ تدابير فورية، مثل تعليق المعاملة أو طلب موافقة الزبون عليها.
7. **تحسين إجراءات الأمن** - يجب على المؤسسة المصرفية العمل على التحسين المستمر لإجراءات أمن أدوات الدفع والحسابات المصرفية.
8. **توثيق حالات الاحتيال** - يجب على المؤسسات المصرفية تصنيف وتوثيق حالات الاحتيال لتتمكن من تتبع مسار الاحتيال، والخدمة أو المنتج المستخدم فيه، والأضرار التي لحقت بالبنك والزبون نتيجةً له.
9. **سياسة تعويض الزبائن** - يتعين على المؤسسات المصرفية وضع سياسة موحدة ومنظمة لتعويض الزبائن الذين وقعوا ضحية للاحتيال، مع مراعاة ترتيب المسؤولية المنصوص عليه في القانون.
10. **تقييم أضرار الاحتيال** - يجب على المؤسسات المصرفية تقييم الاحتيال والأضرار التي لحقت بالزبائن، وليس فقط بالمؤسسة المصرفية نفسها.



**نصائح وإرشادات للزبائن**

فيما بعض التوصيات لمساعدتك على حماية نفسك من الاحتيال:

1. **احرص على خصوصيتك** - فالبيانات المرسلة إليك عبر الرسائل النصية القصيرة SMS من البنك أو شركة بطاقة الائتمان، بما في ذلك رمز التحقق الذي يجب عليك إدخاله قبل إجراء أي معاملة أو تحويل أموال أو أي معلومات مالية حساسة أخرى، هي معلومات شخصية ولا ينبغي إفشاؤها لأي شخص. لن تبادر البنوك وشركات بطاقات الائتمان بالاتصال بك لطلب معلومات سرية منك.
2. **تجنب الضغط على الروابط** - اتبع نهجاً عاماً من الشك والحذر. تجنب الضغط على الروابط المرسلة إليك عبر الرسائل النصية القصيرة SMS أو البريد الإلكتروني. في حال الشك، لا تفعل! من الأفضل عدم الرد على الرسالة بدلاً من الضغط على رابط غير آمن.
3. **لا تُعطِ بطاقتك الائتمانية لأي شخص** - لن يُرسل البنك أو شركة بطاقات الائتمان أي شخص لاستلام بطاقتك منك.
4. **بنكك يتحدث بلغتك** - عند تلقي مكالمة هاتفية من شخص يُعرّف نفسه بأنه ممثل بنك أو شركة بطاقات ائتمان أو ضابط شرطة لا يتحدث العبرية، اطلب من الممثل التحدث باللغة العبرية. في جميع الأحوال، لا تُفصح عن أي معلومات شخصية أو مالية.
5. **استخدم كلمة مرور قوية وطرق التعريف البيومترية** - حدد كلمة مرور تتكون من مجموعة من الأحرف والأرقام والرموز الفريدة، أو استخدم التعريف البيومتري.
6. **الدخول للحساب بحذر** - لا تُسجّل الدخول إلى حسابك المصرفي من رابط مُرسَل عبر رسالة نصية أو بريد إلكتروني.
7. **لا تستخدم برامج التحكم عن بُعد** - تحدث العديد من عمليات الاحتيال بعد تثبيت برامج التحكم عن بُعد على جهاز الزبون أو هاتفه المحمول. يُنصح بتجنب تثبيت هذا النوع من البرامج.
8. **شارك المقربين منك** - في أي محادثة أو اتصال مشبوه، استشر أفراد عائلتك أو موظفي البنك أو شركة بطاقات الائتمان الذين تعرفهم.
9. **إذا ارتكبت خطأً وقدمت معلومات** - اتصل فوراً بالبنك وشركة بطاقات الائتمان، وأبلغ عن ذلك، وقدم شكوى إلى الشرطة. قدّم للبنك وشركة بطاقات الائتمان والشرطة التفاصيل الكاملة لعملية الاحتيال - كل تفصيل مهم!
10. **إذا لاحظت معاملة غير مألوفة -**
* أبلغ شركة بطاقة الائتمان والبنك فوراً!
* قد يؤدي تأخير إبلاغ البنك أو شركة بطاقة الائتمان إلى تحمل جزء من المخاسر.
* اعلم أنك تكون محمي من الأضرار التي تحدث فقط **بعد** التبليغ.
* سيتم تقديم تعويض عن الأضرار التي تحدث **قبل** التبليغ وفقاً للشروط المنصوص عليها في المادتين 24 و29 من قانون خدمات الدفع.
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. [أنشطة هيئة الرقابة على البنوك في مجال استهلاك المعاملات البنكية على موقع بنك إسرائيل](https://www.boi.org.il/information/bank-paymnts/financial-education/50256)  [↑](#footnote-ref-2)
3. [إعلان للصحافة بشأن مكتوب تعيين الفريق](https://boi.org.il/publications/pressreleases/25-9-2024)  [↑](#footnote-ref-3)