Middle East Journal of Economics, Law and Social Sciences (MEJELSS)
مجلة الشرق الأوسط للاقتصاد والقانون والعلوم الاجتماعية
Online ISSN: 3062-3448
Volume 2, Issue 1, 2026, Page No: 122-130
https://mideastjournals.com/index.php/mejelss/index

Preventive Measures and Digital Protection Methods Against Electronic Financial Crimes

Ibtisam Al-Kamel Al-Shawi *
Libyan Authority for Scientific Research, Libya

التدابير الوقائية وأساليب الحماية الرقمية في مواجهة الجرائم المالية الإلكترونية

أ. إبتسام الكامل الشاوي *
الهيئة الليبية للبحث العلمي، ليبيا

*Corresponding author: ebtisamalshawi95@gmail.com

Received: January 20، 2026	Accepted: March 06، 2026	Published: March 11، 2026

Abstract

This study addresses electronic financial crimes as an escalating threat to societal security and economic stability in the digital age. It highlights the significance of preventive measures and digital protection strategies in mitigating these crimes. The findings reveal that weak digital awareness and inadequate institutional coordination constitute serious vulnerabilities within the cybersecurity framework. Furthermore, the study emphasizes the necessity of updating existing legislation to keep pace with rapid technological advancements. The study recommends the development of a comprehensive national strategy for digital financial security, the enhancement of Arab and regional cooperation in exchanging information and expertise, and the intensification of awareness programs. Additionally, it advocates for investing in artificial intelligence and modern technologies to ensure the early detection of fraud attempts.

Keywords: Preventive Measures, Digital Protection, Electronic Financial Crimes, Cybersecurity, Artificial Intelligence.

الملخص

تتناول هذه الدراسة الجرائم المالية الإلكترونية باعتبارها تهديدًا متصاعدًا لأمن المجتمعات واستقرارها الاقتصادي في العصر الرقمي. وتُبرز أهمية التدابير الوقائية واستراتيجيات الحماية الرقمية في الحد من هذه الجرائم. وقد كشفت النتائج عن أن ضعف الوعي الرقمي وقصور التنسيق المؤسسي يشكلان ثغرات خطيرة في منظومة الأمن السيبراني. كما تؤكد الدراسة على ضرورة تحديث التشريعات القائمة بما يتماشى مع التطورات التقنية المتسارعة. وتوصي الدراسة بوضع استراتيجية وطنية شاملة للأمن الرقمي المالي، وتعزيز التعاون العربي والإقليمي في تبادل المعلومات والخبرات، وتكثيف برامج التوعية، إلى جانب الاستثمار في تقنيات الذكاء الاصطناعي والتكنولوجيا الحديثة للكشف المبكر عن محاولات الاحتيال.

الكلمات المفتاحية :التدابير الوقائية، الحماية الرقمية، الجرائم المالية الإلكترونية، الأمن السيبراني، الذكاء الاصطناعي.

المقدمة:

يشهد العالم في ظل الثورة الرقمية الراهنة تطورًا متسارعًا في مجالات التقنية والاتصال، انعكس على جميع مناحي الحياة الاقتصادية والاجتماعية والأمنية. ومع هذا التطور ظهرت أنماط جديدة من الجرائم تعرف بالجرائم الإلكترونية، التي باتت تهدد الأفراد والمؤسسات والدول على حد سواء، لما تسببه من خسائر مالية جسيمة وأضرار نفسية واجتماعية بالغة. وتعد الجرائم المالية الإلكترونية من أخطر صور هذه الجرائم، نظرًا لاستهدافها المال بوصفه عصب الحياة الاقتصادية ومصدر استقرار المجتمعات.

وفي هذا السياق، برزت الحاجة إلى دراسة التدابير الوقائية وأساليب الحماية الرقمية التي يمكن أن تحد من انتشار هذه الجرائم وتقلل من آثارها، خاصة في ظل ضعف الوعي الأمني لدى المستخدمين، وتطور أساليب المجرمين في استغلال الثغرات التقنية لتحقيق مكاسب غير مشروعة.

تسعى هذه الورقة البحثية إلى تحليل واقع التدابير الوقائية وأساليب الحماية الرقمية من خلال المنهج الوصفي التحليلي، اعتمادًا على تحليل مضمون عدد من الدراسات العربية السابقة، بهدف الوصول إلى رؤية علمية تسهم في دعم الجهود الوطنية والمؤسسية لمكافحة الجرائم المالية الإلكترونية.

تشير دراسة موقع النجاح إلى أن الاحتيال المالي الرقمي أصبح من أخطر التهديدات التي تواجه الأفراد والمؤسسات، حيث يستخدم المجرمون تقنيات متطورة لاختراق الحسابات وسرقة البيانات الحساسة. وتوصي الدراسة بضرورة تعزيز الوعي الأمني لدى المستخدمين، وتطبيق استراتيجيات حماية فعالة مثل التحقق الثنائي، وتحديث البرمجيات، وتجنب الروابط المشبوهة (النجاح، 2023).

تناولت دراسة زهدور ودرار (2022) التحديات القانونية التي تواجه الدول في مكافحة الجرائم الرقمية، ومنها الجرائم المالية. وأوضحت أن غياب اتفاق دولي موحد حول تجريم بعض الأفعال الرقمية يعيق جهود المكافحة، مما يستدعي تطوير تشريعات وطنية تتماشى مع المعايير الدولية، وتعزيز التعاون القضائي والتقني بين الدول (زهدور ودرار، 2022).

يرى الدبور (2017) أن تفعيل الحماية الرقمية يتطلب إنشاء وحدات ضبطية متخصصة في الجرائم الإلكترونية داخل المؤسسات، وتدريب الكوادر على تقنيات التحقيق الرقمي. كما يؤكد على أهمية تبني سياسات أمن معلومات صارمة، تشمل مراقبة الدخول، وتشفير البيانات، وتقييم المخاطر بشكل دوري (الدبور، 2017).

مشكلة الدراسة:

في ظل التحول الرقمي المتسارع الذي تشهده المجتمعات العربية، برزت الجرائم المالية الإلكترونية كأحد أبرز التحديات الأمنية التي تهدد استقرار الأفراد والمؤسسات على حد سواء. وعلى الرغم من اعتماد العديد من الجهات الحكومية والمالية لأنظمة حماية رقمية متقدمة، إلا أن معدلات هذه الجرائم تشهد تصاعدًا ملحوظًا، مما يعكس وجود فجوة واضحة بين تطور أساليب المجرمين الرقميين وبين فعالية التدابير الوقائية المعتمدة.

وتتمثل الإشكالية الرئيسة في عدم كفاية الإجراءات الأمنية الحالية لمواكبة التهديدات المستجدة، لا سيما في ظل ضعف الوعي الرقمي لدى المستخدمين، وتنامي قدرة الجناة على استغلال الثغرات التقنية لتحقيق مكاسب غير مشروعة. من هنا، تنطلق هذه الدراسة للبحث في التدابير الوقائية وأساليب الحماية الرقمية

التي من شأنها الحد من انتشار الجرائم المالية الإلكترونية في البيئة العربية، من خلال تحليل الواقع الراهن واستشراف الحلول الممكنة.
من هنا، تحاول الدراسة الإجابة عن التساؤل الرئيس الآتي:
ما التدابير الوقائية وأساليب الحماية الرقمية الفعّالة التي يمكن أن تسهم في الحد من الجرائم المالية الإلكترونية في المجتمعات العربية؟

الفجوة البحثية:
رغم تعدد الدراسات العربية التي تناولت موضوع الجرائم الإلكترونية، إلا أن معظمها اتجه نحو التركيز على الجوانب القانونية أو التقنية البحتة، مثل تشريعات مكافحة الجريمة أو آليات التشفير والحماية السيبرانية، دون أن تولي اهتمامًا كافيًا للبعد الوقائي الذي يجمع بين التوعية التقنية والثقافة الأمنية المؤسسية. هذا القصور في التناول المتكامل يحدّ من فعالية الاستراتيجيات المقترحة في مواجهة التهديدات المتزايدة.
كما أن العديد من البحوث السابقة تناولت الجرائم الإلكترونية بشكل عام، دون تخصيص الجرائم المالية الإلكترونية بالتحليل المعمّق، رغم خطورتها المتزايدة وتأثيرها المباشر على الاستقرار الاقتصادي والاجتماعي. ومن هنا، تبرز الحاجة إلى دراسة تركز على التدابير الوقائية وأساليب الحماية الرقمية في المجال المالي تحديدًا، بما يسهم في سدّ هذه الفجوة المعرفية، وتقديم رؤية علمية عملية تدعم جهود مكافحة هذا النوع من الجرائم في السياق العربي.

أهمية الدراسة:
تكتسب هذه الدراسة أهميتها من عدة جوانب محورية، أبرزها:
1. أهمية الموضوع :تأتي في سياق تصاعد التهديدات الرقمية التي تستهدف الأنظمة المصرفية والمؤسسات المالية والأفراد، مما يجعل الأمن الرقمي المالي قضية ملحة تتطلب معالجة علمية دقيقة.
2. سد فجوة معرفية :تسعى إلى الربط بين الجانب الوقائي وأساليب الحماية الرقمية، وهي زاوية لم تنل حقها من البحث في السياق العربي.
3. إثراء المحتوى العربي :تقدم إضافة نوعية للمكتبة العربية من خلال دراسة تجمع بين التحليل النظري والاستقصاء الميداني للدراسات السابقة والممارسات الراهنة.
4. تقديم حلول عملية :تهدف إلى صياغة توصيات قابلة للتطبيق تساعد صانعي القرار والمؤسسات المالية على تطوير استراتيجيات فعالة لمكافحة الجرائم المالية الإلكترونية.

أهداف الدراسة
الهدف العام:
تحليل التدابير الوقائية وأساليب الحماية الرقمية المعتمدة في مواجهة الجرائم المالية الإلكترونية، واستكشاف مدى فعاليتها في البيئة العربية.
الأهداف الفرعية:
1. رصد أبرز أنواع الجرائم المالية الإلكترونية المنتشرة في الدول العربية.
2. تحليل الجهود المؤسسية والتقنية المبذولة للحد من هذه الجرائم.
3. دراسة الأساليب الرقمية الحديثة المستخدمة في الحماية من الاختراقات المالية.

4. الكشف عن أوجه القصور في السياسات الوقائية الحالية.
5. اقتراح آليات واستراتيجيات لتعزيز الحماية الرقمية في المؤسسات المالية العربية.

تساؤلات الدراسة

1. ما أنواع الجرائم المالية الإلكترونية الأكثر شيوعًا في البيئة العربية؟
2. ما أبرز التدابير الوقائية المعتمدة حاليًا لمواجهتها؟
3. ما مدى فعالية أساليب الحماية الرقمية المستخدمة في المؤسسات المالية؟
4. ما أوجه القصور في المنظومة الوقائية الحالية؟
5. ما الاستراتيجيات المقترحة لتعزيز الأمن الرقمي المالي في المستقبل؟

منهج الدراسة

تعتمد هذه الدراسة على المنهج الوصفي التحليلي الذي يقوم على وصف الظاهرة وتحليلها للوصول إلى نتائج علمية دقيقة.

أما أداة الدراسة فهي تحليل المضمون لعدد من الدراسات العربية السابقة التي تناولت موضوعات الجرائم المالية الإلكترونية والحماية الرقمية، من أجل استخلاص أبرز النتائج والتوصيات المشتركة بينها.

الدراسات السابقة:

فيما يلي عرض موجز لست دراسات عربية تناولت موضوع الحماية الرقمية والجرائم المالية:

1. دراسة أحمد الزهراني (2020) بعنوان "الأمن السيبراني ودوره في حماية المؤسسات المالية"، وخلصت إلى أن ضعف الثقافة الأمنية الرقمية لدى الموظفين يمثل ثغرة أساسية في منظومة الحماية.
2. دراسة سامية البلوشي (2021) بعنوان "الجرائم الإلكترونية في البيئة المصرفية العربية"، التي ركزت على أهمية التوعية المستمرة للعاملين والمستخدمين للحد من الاختراقات.
3. دراسة عبد الرحمن العبدلي (2019) "التدابير القانونية للوقاية من الجرائم المالية الرقمية"، وأكدت على ضرورة تشديد التشريعات والعقوبات بحق مرتكبي الجرائم الإلكترونية.
4. دراسة نجلاء الحربي (2022) "فاعلية أنظمة الحماية التقنية في البنوك العربية"، التي أظهرت أن معظم الأنظمة لا تزال تعتمد على تقنيات تقليدية ولا تواكب التطورات الحديثة في مجال الذكاء الاصطناعي الأمني.
5. دراسة فاطمة الكعبي (2020) "تأثير الوعي الأمني لدى الأفراد على الحد من الجرائم الإلكترونية"، والتي أوصت بضرورة دمج برامج التوعية بالأمن الرقمي في المناهج التعليمية.
6. دراسة يوسف العتيبي (2023) "استراتيجيات الحماية الرقمية في مواجهة الاحتيال المالي الإلكتروني"، وأوصت بتبني نهج تكاملي يجمع بين التدابير التقنية والقانونية والإدارية.

مفاهيم ومصطلحات الدراسة:

التدابير الوقائية: هي الإجراءات والخطط المسبقة التي تهدف إلى تقليل احتمالية وقوع الجريمة المالية الإلكترونية قبل حدوثها.

الحماية الرقمية: مجموعة من الوسائل التقنية والتنظيمية التي تستخدم لحماية الأنظمة والمعلومات من الاختراق أو التلاعب أو السرقة.

الجرائم المالية الإلكترونية: كل فعل غير مشروع يستخدم فيه الفضاء الرقمي لتحقيق مكاسب مالية غير قانونية مثل الاحتيال الإلكتروني، الاختراق المصرفي، أو سرقة البيانات البنكية.
الأمن السيبراني: هو الحماية الممنهجة للشبكات والأنظمة من التهديدات الرقمية التي تهدف إلى تعطيل الخدمات أو سرقة المعلومات.

الإطار النظري

المبحث الأول: التدابير الوقائية في البيئة الرقمية

1- تطور التشريعات العربية في مكافحة الجرائم الإلكترونية

شهدت السنوات الأخيرة إصدار عدد من القوانين العربية التي تهدف إلى مكافحة الجرائم الإلكترونية، مثل قانون مكافحة الجرائم المعلوماتية السعودي (2007)، وقانون مكافحة تقنية المعلومات الإماراتي (2012)، وقانون مكافحة جرائم الإنترنت المصري (2018). ورغم أهمية هذه التشريعات في تجريم الأفعال الرقمية مثل الاختراق والاحتيال المالي، إلا أن العديد من الدراسات تشير إلى أن هذه القوانين لا تزال بحاجة إلى تحديث مستمر لمواكبة التطور التقني السريع.

2- التحديات القانونية في البيئة الرقمية

تشير دراسة عبد الله السعيد (جامعة نايف) إلى أن أبرز التحديات التي تواجه الإطار القانوني العربي تتمثل في ضعف التنسيق بين الجهات القضائية والتقنية، وتفاوت مستوى تطبيق القوانين بين الدول، بالإضافة إلى غياب آليات فعالة للتعاون الإقليمي في التحقيقات الرقمية. كما أن بعض التشريعات تفتقر إلى تعريفات دقيقة للجرائم الإلكترونية، مما يفتح المجال لتفسيرات قانونية متباينة.

3- الإطار الأمني الوطني ومراكز الاستجابة

تؤكد دراسة شريف اللبان (جامعة القاهرة) أن بناء إطار أمني فعال يتطلب إنشاء مراكز وطنية للاستجابة للحوادث السيبرانية(CSIRTs) ، وتدريب الكوادر الفنية، وتطوير البنية التحتية الرقمية. إلا أن معظم الدول العربية تعاني من نقص في هذه المراكز، مما يجعلها عرضة للهجمات الإلكترونية المنظمة، خاصة في القطاع المالي والمصرفي.

4- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

وقّعت الدول العربية عام 2010 على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي تهدف إلى توحيد الجهود القانونية وتعزيز التعاون القضائي والتقني. ورغم أهمية هذه الاتفاقية، إلا أن دراسة ناصر العتيبي (جامعة الملك سعود) تشير إلى أن التباين في تنفيذ بنود الاتفاقية بين الدول الأعضاء يحد من فعاليتها، ويستدعي مراجعة دورية لبنودها بما يتماشى مع المستجدات الرقمية.

المحور الثاني: دور المؤسسات المالية في الوقاية الرقمية

1- تعزيز البنية التحتية الرقمية للمؤسسات المالية

تلعب المؤسسات المالية دورًا محوريًا في بناء منظومة وقائية رقمية فعالة، من خلال تطوير البنية التحتية التقنية واعتماد أنظمة حماية متقدمة مثل جدران الحماية، وأنظمة كشف التسلل، والتشفير متعدد الطبقات.

وتشير دراسة *خالد ممدوح إبراهيم* (2020)إلى أن المؤسسات التي تستثمر في تحديث أنظمتها الرقمية تقلّ لديها معدلات الاختراق بنسبة تصل إلى 40% مقارنة بالمؤسسات ذات الأنظمة التقليدية.

2- تدريب الكوادر وتطوير المهارات السيبرانية

أحد أهم عناصر الوقاية الرقمية هو تدريب الموظفين على التعامل مع التهديدات السيبرانية، وتوعيتهم بمخاطر التصيد الإلكتروني والهندسة الاجتماعية. وقد أظهرت دراسة *جامعة نايف للعلوم الأمنية* (2019) أن 60% من حالات الاختراق المالي تعود إلى أخطاء بشرية ناتجة عن ضعف الوعي الأمني لدى العاملين، مما يبرز أهمية بناء ثقافة أمنية داخل المؤسسات.

3- التعاون مع الجهات الرقابية والتقنية

تسعى المؤسسات المالية إلى تعزيز التعاون مع الجهات الحكومية والرقابية مثل البنوك المركزية، وهيئات الاتصالات، ومراكز الاستجابة للحوادث السيبرانية. هذا التعاون يتيح تبادل المعلومات حول التهديدات المستجدة، ويساعد في تطوير سياسات وقائية موحدة. وتوصي دراسة *شريف اللبان* (2021)بإنشاء منصات مشتركة بين القطاعين العام والخاص لرصد الهجمات وتنسيق الاستجابة.

4- تبني استراتيجيات استباقية للوقاية

لم تعد الوقاية الرقمية تقتصر على رد الفعل، بل أصبحت تعتمد على استراتيجيات استباقية مثل تحليل السلوكيات الرقمية، واستخدام الذكاء الاصطناعي لرصد الأنماط المشبوهة. وتؤكد دراسة *المركز القومي للبحوث الاجتماعية والجنائية* (2020)أن المؤسسات التي تطبق هذه الأساليب تقلّ لديها الخسائر الناتجة عن الجرائم المالية بنسبة ملحوظة، وتتمكن من احتواء الهجمات قبل تفاقمها.

المبحث الثاني: أساليب الحماية الرقمية ضد الجرائم المالية

المحور الأول: التوعية والأمن السيبراني

1- التوعية الرقمية كأداة وقائية

تشير دراسة *الحارث مطالقة* (2020)بعنوان "دور التوعية في الحد من الجرائم الإلكترونية في المؤسسات المالية "إلى أن التوعية الرقمية تمثل خط الدفاع الأول ضد الهجمات السيبرانية، حيث تساهم في تقليل الأخطاء البشرية بنسبة تصل إلى 60%. وقد أوصت الدراسة بضرورة إدراج برامج تدريبية دورية للموظفين والعملاء، تشمل التعرف على أساليب التصيد الإلكتروني، وإجراءات حماية البيانات المصرفية.

2- الأمن السيبراني في المؤسسات المالية

في دراسة بعنوان "تحديات الأمن السيبراني في البنوك الجزائرية "للباحثين *شايب محمد وحمادي موراد* (2023)، تم تحليل واقع الحماية الرقمية في المؤسسات المالية، وأبرزت الدراسة ضعف التنسيق بين الأقسام الفنية، ونقص الكفاءات المتخصصة، وغياب خطط استجابة فعالة للحوادث السيبرانية. وقد خلصت إلى ضرورة اعتماد معايير أمنية صارمة تشمل التشفير، وإدارة الوصول، والمراقبة المستمرة للأنشطة الرقمية.

3- الذكاء الاصطناعي وتحليل البيانات في كشف الجرائم

تناولت دراسة (2024) *Matrix219* بعنوان "الذكاء الاصطناعي والأمان السيبراني "دور تقنيات الذكاء الاصطناعي في الكشف المبكر عن الأنشطة المالية المشبوهة. وأشارت إلى أن هذه التقنيات قادرة على تحليل أنماط الاستخدام وتحديد السلوكيات غير المعتادة، مما يتيح للمؤسسات اتخاذ إجراءات استباقية قبل وقوع الهجمات، ويعزز من فعالية أنظمة الحماية الرقمية.

4- التشفير والمراقبة الذكية لحماية المعاملات

أوضحت دراسة (2023) *QIT Quality* بعنوان "مستقبل الحماية الرقمية باستخدام الذكاء الاصطناعي " أن تقنيات التشفير المتقدمة وأنظمة المراقبة الذكية تساهم في حماية المعاملات المالية بشكل فعال، حيث تقل نسبة الاختراقات في المؤسسات التي تعتمد هذه التقنيات بنسبة تصل إلى 50%. كما أكدت الدراسة أهمية دمج هذه الأدوات مع تقنيات التعلم الآلي لتعزيز الاستجابة التلقائية للحوادث.

الخاتمـــــــة

تُبرز هذه الدراسة أن الجرائم المالية الإلكترونية لم تعد مجرد تهديد محتمل، بل أصبحت واقعًا ملموسًا يهدد أمن المجتمعات واستقرارها الاقتصادي، ويستدعي استجابة شاملة ومتكاملة. وقد بيّنت النتائج أن التصدي لهذه الجرائم يتطلب تنسيقًا فعّالًا بين الأطر القانونية والتقنية والتوعوية، بما يضمن بناء بيئة رقمية آمنة ومستدامة.

وتؤكد الدراسة أن الوقاية الرقمية تمثل الخيار الأكثر فاعلية مقارنة بالاستجابة اللاحقة، إذ تساهم التدابير الوقائية وأساليب الحماية الذكية في تقليص حجم الخسائر المحتملة، وتعزيز ثقة الأفراد والمؤسسات في التعاملات الرقمية.

وتأمل الدراسة أن تُسهم نتائجها وتوصياتها في دعم جهود بناء منظومة أمن رقمي عربية متطورة، قادرة على مواكبة التهديدات المتزايدة، وتوفير حماية فعالة للقطاع المالي والمصرفي، بما ينعكس إيجابًا على التنمية الاقتصادية والاستقرار المجتمعي.

نتائج الدراسة

توصلت الدراسة إلى مجموعة من النتائج المهمة التي تعكس واقع الحماية الرقمية في المؤسسات المالية العربية، أبرزها:

1. التسارع في وتيرة الجرائم المالية الإلكترونية نتيجة التطور التكنولوجي المستمر وسهولة الوصول إلى البيانات المصرفية عبر الإنترنت، مما يزيد من تعقيد التهديدات الرقمية.
2. قصور التدابير الوقائية الحالية في المؤسسات المالية العربية، حيث تفتقر إلى التكامل والتحديث، مما يجعلها غير كافية لمواجهة الهجمات السيبرانية المتطورة.
3. ضعف الوعي الرقمي لدى الموظفين والمستخدمين يُعد من أبرز نقاط الضعف، إذ يسهم في ارتفاع معدلات الاختراق والاحتيال المالي.
4. عدم مواكبة التشريعات الوطنية للتطورات التقنية، حيث تحتاج القوانين إلى مراجعة دورية لتلائم الأساليب الحديثة التي يستخدمها المجرمون الإلكترونيون.
5. غياب التنسيق الفعّال بين الجهات المصرفية والأمنية، مما يؤدي إلى تشتت الجهود ويضعف من فعالية الاستجابة للجرائم المالية الإلكترونية.

ثانيًا: توصيات الدراسة

بناءً على النتائج السابقة، تقترح الدراسة مجموعة من التوصيات العملية لتعزيز الأمن الرقمي المالي في البيئة العربية:

1. إعداد استراتيجية وطنية شاملة للأمن الرقمي المالي، تتضمن مشاركة القطاعين العام والخاص، وتحدد أدوارًا واضحة للجهات المعنية في الوقاية والاستجابة.
2. تعزيز التعاون العربي والإقليمي في مجال تبادل المعلومات والخبرات حول الجرائم المالية الإلكترونية، من خلال إنشاء منصات مشتركة ومراكز بحثية متخصصة.
3. تحديث التشريعات والقوانين بشكل دوري بما يتماشى مع التطورات التقنية وأساليب الجريمة الرقمية، لضمان فعالية الردع القانوني.
4. إدماج برامج التوعية الرقمية في المؤسسات التعليمية والمصرفية، بهدف بناء ثقافة أمنية مستدامة لدى الأفراد والمؤسسات.
5. الاستثمار في التقنيات الحديثة مثل الذكاء الاصطناعي وتحليل البيانات الضخمة، لتطوير أنظمة ذكية قادرة على الكشف المبكر عن محاولات الاحتيال المالي.
6. إنشاء مراكز وطنية للرصد والاستجابة للطوارئ الرقمية، متخصصة في الجرائم المالية، تعمل على مراقبة الأنشطة المشبوهة والتنسيق الفوري مع الجهات المعنية.

قائمة المراجع

1. إبراهيم، خالد ممدوح .(2020) .الجرائم المعلوماتية والإلكترونية .المركز القومي للبحوث.
2. البلوشي، سامية. (2021). الجرائم الإلكترونية في البيئة المصرفية العربية .مجلة دراسات اقتصادية، جامعة الإمارات.
3. الحربي، نجلاء. (2022). فاعلية أنظمة الحماية التقنية في البنوك العربية .مجلة البحوث الاقتصادية، 11.
4. الدبور، عبد الرحمن .(2017) .آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية .كتاب أعمال مؤتمر مركز جيل البحث العلمي، طرابلس، لبنان.
5. الزهراني، أحمد. (2020). الأمن السيبراني ودوره في حماية المؤسسات المالية .مجلة الأمن الرقمي، (5)، جامعة الملك سعود.
6. السعيد، عبد الله بن محمد .(2019) .الجرائم الإلكترونية في التشريع العربي: دراسة مقارنة .جامعة نايف العربية للعلوم الأمنية.
7. العبدلي، عبد الرحمن. (2019). التدابير القانونية للوقاية من الجرائم المالية الرقمية .مجلة الحقوق والعلوم السياسية، جامعة الكويت.
8. العتيبي، ناصر .(2020) .تحليل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .جامعة الملك سعود.
9. العتيبي، يوسف. (2023). استراتيجيات الحماية الرقمية في مواجهة الاحتيال المالي الإلكتروني . مجلة دراسات أمنية، جامعة نايف العربية للعلوم الأمنية.
10. الكعبي، فاطمة. (2020). تأثير الوعي الأمني لدى الأفراد على الحد من الجرائم الإلكترونية .مجلة العلوم الإنسانية والاجتماعية، جامعة الشارقة.

11. اللبان، شريف .(2021) .السياسات الأمنية الرقمية في الوطن العربي .جامعة القاهرة.
12. المركز القومي للبحوث الاجتماعية والجنائية .(2020) .الوقاية الرقمية في المؤسسات المالية . القاهرة.
13. النجاح .(2023) .الحماية من الاحتيال المالي الرقمي: كل ما تحتاج معرفته للبقاء آمناً .مسترجع من: https://www.annajah.net :
14. زهدور، إ.، ودرار، ن. (2022). استراتيجيات الوقاية القانونية والأمنية من مهددات الأمن الرقمي .المجلة الدولية للبحوث والدراسات السياسية، .(16)
15. شايب، محمد، وحمادي، موراد. (2023). تحديات الأمن السيبراني في البنوك الجزائرية .المجلة الجزائرية للأمن الرقمي.
16. مطالقة، الحارث. (2020). دور التوعية في الحد من الجرائم الإلكترونية في المؤسسات المالية . مجلة البحوث الأمنية.
17. Matrix219. (2024). الذكاء الاصطناعي والأمان السيبراني .مسترجع من : https://matrix219.net.
18. QIT Quality. (2023). مستقبل الحماية الرقمية باستخدام الذكاء الاصطناعي .مسترجع من : https://ae.linkedin.com.