Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss
AJSS

Cybercrimes and their Impact on Hadhrami Society: An Analytical Study on the City of Mukalla

الجرائم الإلكترونيَّة وأثرها على المجتمع الحضرمي: دراسة تحليلية على مدينة المكلا

نزيهة محمد علي العيدروس
كلية التربية، جامعة حضرموت، الجمهورية اليمنية

Naziha Mohammed Ali Al-Eidaroos
Faculty of Education, Hadhramout University, Republic of Yemen

Received 30 May 2025; accepted 13 Aug. 2025; available online 9 Dec. 2025

المستخلص

سعى هذا البحث إلى دراسة واقع الجرائم الإلكترونيَّة في مدينة المكلا بمحافظة حضرموت -اليمن، من خلال التعرف على أنواعها وأساليبها الشائعة، وتحليل أثرها على الضحايا، وتحديد العوامل التي أسهمت في حدوثها، بالإضافة إلى تقييم مستوى وعي أفراد المجتمع المحلي بمخاطرها، واستطلاع آرائهم حول الإجراءات المتخذة للحد منها، وصولًا إلى تقديم توصيات عملية قابلة للتطبيق.

وقد اعتمدت الدراسة على المنهج الوصفي التحليلي، باستخدام أداة الاستبانة لجمع البيانات من عينة مكونة من (427) مشاركًا من سكان مدينة المكلا. وتم تحليل البيانات إحصائيًّا للوصول إلى مؤشرات كمية دقيقة تدعم أهداف البحث.

وقد كشفت النتائج أن الجرائم الإلكترونيَّة منتشرة بنسب متفاوتة، وتؤثر على الضحايا نفسيًّا واجتماعيًّا وماديًّا. وبيَّنت الدراسة أن أبرز العوامل التي أسهمت في تفشي هذه الجرائم هي: ضعف الوعي، ومشاركة المعلومات الشخصية، وضعف التشريعات. كما أظهرت أن وعي المشاركين بالمخاطر يتفاوت، وأن هناك ضعفًا في الثقة بالإجراءات الأمنية والتشريعية الحاليَّة. واقترح المشاركون

الكلمات المفتاحية: الدراسات الأمنية، الجرائم الإلكترونيَّة، المجتمع الحضرمي، المكلا، الأمن السيبراني، أمن البيانات

Abstract

This study aims to examine the reality of cybercrime in the city of Mukalla, Hadhramout Governorate, in Yemen, by identifying its common types and methods, analyzing its impact on victims, and determining the contributing factors to its occurrence. Additionally, the study assesses the level of public awareness regarding cyber threats and explores participants' opinions on the measures taken to combat these crimes, ultimately providing practical and applicable recommendations.

The study adopts a descriptive-analytical approach, utilizing a questionnaire to collect data from a sample of 427 residents of Mukalla. Statistical tools were used to analyze the data and generate accurate quantitative indicators that support the study's objectives.

The findings reveal that cybercrimes are prevalent to varying degrees and have psychological, social, and financial impacts on victims. The study identified weak awareness, sharing of personal information, and inadequate legislation as key contributing factors to the spread of these crimes. It also shows that participants' awareness levels vary and that there is a general lack of confidence in current security and legal measures. Participants proposed some practical measures, most

Keywords: *security studies, cybercrime, Hadhrami society, Mukalla, cybersecurity, data security*

* Corresponding Author: *Naziha Mohammed Ali Al-Eidaroos*
Email: naz.moh@hu.edu.ye

doi: 10.26735/GSUN1347

جملة من الإجراءات العملية، من أهمها: تسهيل الإبلاغ، وتحديث القوانين، وتكثيف التوعية.

وتوصل البحث إلى أن مواجهة الجرائم الإلكترونيَّة تتطلب تدخلًا متعدد الجوانب، يشمل التوعية، والتشريع، والدعم التقني، مع ضرورة إشراك المجتمع في جهود الوقاية. وتُعدُّ هذه الدراسة إسهامًا علميًّا في فهم الظاهرة محليًّا، وتشكل قاعدة لدراسات أوسع مستقبلًا.

notably facilitating reporting procedures, updating legislation, and intensifying awareness efforts.

The study concludes that addressing cybercrime requires a multifaceted approach involving awareness, legislation, and technical support, with an emphasis on community involvement in prevention efforts. This research represents a valuable contribution to understanding cybercrime in the local context and provides a foundation for broader future studies.

1. المقدمة

يعيش العالم في الوقت الحالي تطورًا تكنولوجيًّا سريعًا غير مسبوق؛ حيث أصبحت التقنيات الرقمية جزءًا لا يتجزأ من الحياة اليومية للأفراد والمجتمعات. ومع هذا التوسع الهائل في استخدام الإنترنت ووسائل التواصل الاجتماعي، ظهرت تحديات جديدة تهدد الأمن الرقمي والسلم الاجتماعي، ومن أبرز هذه التحديات ما يُعرف بالجرائم الإلكترونيَّة.

وتُعدُّ الجرائم الإلكترونيَّة مجموعة من الأفعال غير المشروعة التي تُرتكب باستخدام الوسائط التقنية والرقمية، وتستهدف الأفراد أو المؤسسات لأغراض مالية، نفسية، أو اجتماعية، ومن أبرز صورها: الاحتيال المالي، سرقة الهوية، الابتزاز الإلكتروني، التشهير، انتهاك الخصوصية. وتمثل هذه الجرائم أحد أبرز التهديدات الأمنية في العصر الرقمي؛ حيث تمتد آثارها من الأفراد إلى المؤسسات، وقد تطول أمن الدولة واستقرارها إذا لم تُواجه بمنهجية فعَّالة.

وفي هذا السياق، يظهر المجتمع الحضرمي - كجزء من هذا العالم الرقمي المتشابك - وهو يواجه تحديات أمنية واجتماعية غير مألوفة، في ظل الانتشار المتزايد لاستخدام الإنترنت وتطبيقات التواصل الحديثة، خاصةً في مدينة المكلا التي تُعدُّ مركزًا حضريًّا متقدمًا في محافظة حضرموت. ويمتاز هذا المجتمع بطبيعته المحافظة والتزامه بمنظومة قيمية تقليدية تُولي أهمية كبرى للسمعة والأمان الاجتماعي؛ مما يجعل آثار الجرائم الإلكترونيَّة فيه أكثر حساسية وتعقيدًا.

ومن هنا تنبع أهمية هذه الدراسة التحليلية، التي تهدف إلى تسليط الضوء على واقع الجرائم الإلكترونيَّة في مدينة المكلا، من حيث أنواعها، وانتشارها، وآثارها النفسية والاجتماعية والأمنية على الأفراد، إضافة إلى قياس وعي المجتمع بمخاطرها وسبل الوقاية منها، واستكشاف الإجراءات الحاليَّة في مواجهتها. كما تُسهم في سد الفجوة البحثية؛ نظرًا لندرة الدراسات الميدانية المتخصصة التي تناولت هذه الظاهرة في المجتمع الحضرمي؛ مما يجعلها مرجعًا مهمًّا للباحثين وصُنَّاع القرار والأجهزة الأمنية المهتمة بتعزيز الأمن الرقمي في اليمن.

مشكلة الدراسة

تتزايد الجرائم الإلكترونيَّة بشكل ملحوظ على المستوى العالمي؛ مما يشكل تهديدًا للأمن والاستقرار في المجتمعات. وفي هذا السياق، يواجه المجتمع الحضرمي، الذي يتميز بقيمه وتقاليده العريقة، تحديات متزايدة نتيجة لتوسع استخدام التقنيات الرقمية. من هنا تبرز مشكلة البحث في الحاجة إلى فهم عميق لتأثير الجرائم الإلكترونيَّة، كظاهرة دخيلة، على النسيج الاجتماعي والثقافي في مدينة المكلا بمحافظة حضرموت، وتحليل العوامل المؤدية إلى ظهورها، واقتراح إستراتيجيات فعَّالة للتصدي لها، وذلك في ظل ندرة الدراسات التي تتناول هذا الموضوع في السياق المحلي.

أهمية الدراسة

تستمد هذه الدراسة أهميتها من عدة جوانب، تتمثل في:

1. توفير بيانات شاملة حول واقع الجرائم الإلكترونيَّة في مدينة المكلا، والتي يمكن أن تساعد الجهات المعنية في فهم أفضل لهذه الظاهرة وتطوير إستراتيجيات فعَّالة لمكافحتها.
2. تسليط الضوء على تأثير الجرائم الإلكترونيَّة على الضحايا؛ مما يساعد في زيادة الوعي بأهمية هذه المشكلة وضرورة تقديم الدعم للضحايا.
3. تحديد العوامل التي تسهم في وقوع الجرائم الإلكترونيَّة، ومن ثمَّ التمكن من استهداف هذه العوامل ببرامج الوقاية والتوعية.
4. تقييم مستوى الوعي بمخاطر الجرائم الإلكترونيَّة وأساليب الحماية منها؛ مما يسهم في تطوير برامج توعية أكثر فاعليَّة.
5. تقديم رؤى حول آراء أفراد المجتمع في مدينة المكلا حول الإجراءات المعمول بها لمكافحة الجرائم الإلكترونيَّة؛ مما يساعد على تحسين هذه الإجراءات وتعزيز كفاءتها.
6. الإسهام في إثراء الأدبيات العربية حول الجرائم الإلكترونيَّة، خاصةً في السياق اليمني، حيث لا تزال الدراسات حول هذا الموضوع محدودة.

أهداف الدراسة

تهدف هذه الدراسة إلى:

1. دراسة واقع الجرائم الإلكترونيَّة في مدينة المكلا، وتحديد أنواعها وأساليبها الأكثر شيوعًا.
2. تقييم تأثير الجرائم الإلكترونيَّة على الضحايا في مدينة المكلا.
3. توصيف العوامل التي أسهمت في حدوث الجرائم الإلكترونيَّة في مدينة المكلا.
4. تقييم مستوى الوعي بمخاطر الجرائم الإلكترونيَّة، وكيفية الوقاية منها لدى أفراد المجتمع.
5. تقييم آراء أفراد المجتمع حول الإجراءات المتخذة لمكافحة الجرائم الإلكترونيَّة.
6. اقتراح إستراتيجيات وتوصيات لمكافحة الجرائم الإلكترونيَّة، وتعزيز الأمن السيبراني في المجتمع الحضرمي.
7. إعداد دراسة تحليلية شاملة تسهم في إثراء المعرفة العلميَّة حول الجرائم الإلكترونيَّة في السياق المحلي.

تساؤلات الدراسة

انطلاقًا من مشكلة الدراسة وأهدافها، فقد سعت إلى الإجابة عن التساؤلات الآتية:

1. ما أنواع الجرائم الإلكترونيَّة الأكثر شيوعًا في مدينة المكلا؟
2. ما مدى تأثير الجرائم الإلكترونيَّة على الضحايا نفسيًّا، واجتماعيًّا، وماديًّا؟
3. ما العوامل التي تسهم في تفشي الجرائم الإلكترونيَّة في المجتمع الحضرمي؟
4. ما مستوى وعي أفراد المجتمع في مدينة المكلا بمخاطر الجرائم الإلكترونيَّة وسبل الوقاية منها؟
5. ما آراء المشاركين حول فاعليَّة الإجراءات المتخذة لمكافحة الجرائم الإلكترونيَّة؟
6. ما أبرز التوصيات والإجراءات المقترحة للحد من الجرائم الإلكترونيَّة وتعزيز الأمن السيبراني محليًّا؟

2. الإطار النظري

2. 1 الجرائم الإلكترونيَّة

شهد العالم في الآونة الأخيرة تطورًا هائلًا في مجال التقنية الرقمية؛ حيث أصبح الإنترنت ووسائل الاتصال الحديثة جزءًا لا يتجزأ من حياة الأفراد والمجتمعات. وعلى الرغم من الفوائد العديدة لهذه التقنيات، فإنها فتحت الباب أيضًا لظهور أشكال جديدة من الجرائم، تعرف بالجرائم الإلكترونيَّة.

2. 1. 1. تعريف الجرائم الإلكترونيَّة

تعددت الاجتهادات بشأن تعريف الجريمة الإلكترونيَّة، حيث عرفها بعض الباحثين من جوانب تقنية، وآخرون من منطلقات قانونية، بينما ركز بعضهم على وسائل ارتكابها أو دوافع مرتكبيها. ومن أبرز هذه الاجتهادات، ما ورد في تعريف شامل للجريمة الإلكترونيَّة بأنها:

«أي فعل يُخالف القانون ويُرتكب ضد الأفراد أو المُجتمعات، ويهدف إلى إيذاء الغير، أو الحُصول على منافع غير مشروعة، باستخدام الإنترنت وتقنيات الاتصال الحديثة» (أبو دية وعبد الله، 2018).

وفي سياق هذه الدراسة، تُعرّف الجرائم الإلكترونيَّة بأنها:

«كل فعل غير مشروع يُرتكب باستخدام الوسائط التقنية أو الرقمية، ويستهدف الأفراد أو المؤسسات، بهدف الإضرار النفسي أو المادي أو الاجتماعي، سواء عبر اختراق الحسابات، أو سرقة البيانات، أو الاحتيال، أو الابتزاز، أو غيرها من الأفعال التي تنتهك الخصوصية أو الأمن الرقمي للأطراف المستهدفة».

ونظرًا لارتباط الجرائم الإلكترونيَّة بمفاهيم تقنية وأمنية محورية، تقدم الدراسة التعريفات الآتية لكل من الأمن السيبراني وأمن البيانات:

الأمن السيبراني

هو «مجموعة من الوسائل التقنية والإدارية والقانونية التي تهدف إلى حماية الأنظمة الحاسوبية والشبكات الرقمية والمعلومات من الاختراق أو التخريب أو الاستخدام غير المشروع، وضمان سرية وتكامل وتوافر المعلومات» (International Organization for Standardization, 2023).

أمن البيانات

هو «مجموعة من السياسات والإجراءات والتقنيات التي تهدف إلى حماية البيانات من الوصول غير المصرح به، أو التعديل، أو الفقدان، أو التدمير، سواء أثناء التخزين أو النقل أو المعالجة، مع الحفاظ على سريتها وسلامتها وتوافرها» (International Organization for Standardization, 2022).

وتُعدُّ الجرائم الإلكترونيَّة من أبرز التحديات التي تواجه القانون والجهات المنفذة له في العصر الرقمي؛ حيث تتطلب مهارات وتقنيات متقدمة لمواجهتها والحد من آثارها المتزايدة.

2. 1. 2. أنواع الجرائم الإلكترونيَّة

تنقسم الجرائم الإلكترونيَّة وفقًا لأحكام اتفاقية بودابست (Council of Europe, 2001) إلى خمس مجموعات رئيسة تشمل:

1. الجرائم ضد سرية النزاهة وتوافر بيانات أو أنظمة الحاسب، مثل: الاختراق غير المشروع للأنظمة أو تعطيل الخدمات أو تغيير البيانات.
2. الجرائم المتعلقة باستخدام الحاسوب، مثل: الاحتيال أو التزوير الرقمي المرتكب عبر الحاسب.
3. الجرائم المرتبطة بالمحتوى، ولا سيما تلك المتعلقة بالصور الجنسية للأطفال أو الدعاية غير القانونية.
4. الجرائم المتعلقة بانتهاك حقوق النشر والحقوق ذات الصلة، مثل: توزيع محتوى محمي دون إذن.
5. الجرائم العنصرية أو الكراهية عبر الحاسوب، التي أُدرِجت ضمن البروتوكول الإضافي الأول للاتفاقية بشأن الجرائم ذات الطابع العنصري أو الكاره للأجانب.

2. 1. 3. أساليب الجرائم الإلكترونيَّة

وفقًا لمكتب الأمم المتحدة المعني بالمخدرات والجريمة (2013) فإن أبرز الأساليب المعتمدة في ارتكاب الجرائم الإلكترونيَّة تشمل:

- التصيد الاحتيالي :(Phishing) خدع تهدف إلى سرقة المعلومات من خلال روابط مزيفة أو رسائل بريدية معتدة.
- استخدام البرمجيات الخبيثة، مثل: الفيروسات، وبرامج الفدية، والبرمجيات التدميرية.
- الهندسة الاجتماعية، التي تعتمد على التلاعب النفسي والخداع للوصول إلى المعلومات.
- هجمات الحرمان من الخدمة (DoS/DDoS)، التي تعطل الوصول إلى الخدمات الرقمية أو الخوادم.
- التنصت الإلكتروني والتجسس على المحادثات أو البيانات دون إذن، بهدف سرقة أو ابتزاز الضحايا.

2. 1. 4. الفرق بين الجرائم الإلكترونيَّة والجرائم التقليدية

تتميز الجرائم الإلكترونيَّة عن الجرائم التقليدية بعدة جوانب، منها تجاوز النطاق الجغرافي للحدود الوطنية، وسرعة التنفيذ بتكلفة منخفضة نسبيًّا، بالإضافة إلى سهولة إخفاء هوية المجرمين؛ مما يصعب من عملية تعقبهم وملاحقتهم. كما تختلف طبيعة الأدلة المستخدمة؛ حيث تكون رقمية، وتتطلب مهارات فنية متخصصة في جمعها وتحليلها. علاوة على ذلك، تستدعي الجرائم الإلكترونيَّة تبني إستراتيجيات وقائية وكشفية متميزة تتناسب مع خصوصيتها مقارنة بالجرائم التقليدية.

2. 1. 5. دوافع الجرائم الإلكترونيَّة

تُعدُّ دوافع الجرائم الإلكترونيَّة متعددة ومعقدة (مهدي، 2022)، من أبرز هذه الدوافع:

1. الدوافع المادية والمالية: تحقيق مكاسب مالية سريعة؛ مثل: الاحتيال أو الفدية.
2. الدوافع الشخصية والنفسية: البحث عن التسلية، والتحدي، أو الشهرة ضمن مجتمعات الهاكرز.
3. دوافع انتقامية أو ذهنية: مثل: الرغبة في تصحيح موقف أو استهداف سمعة.
4. الدوافع السياسية: تنفيذ أعمال باسم جماعات ذات أهداف سياسية أو احتجاجية.

2. 2 الاتفاقيات الدولية المتعلقة بمكافحة الجرائم الإلكترونيَّة

تشكّل الجرائم الإلكترونيَّة تهديدًا خطيرًا ومتزايدًا في عالمنا اليوم. ففي عام 2023، كبَّدت هذه الجرائم الاقتصاد العالمي خسائر تفوق قيمتها تسعة تريليونات دولار أميركي، مقارنةً بـ 860 مليار دولار أميركي قبل ستة أعوام. ولمَّا كانت الجرائم الإلكترونيَّة، بطبيعتها، عابرة للحدود، فإنّها تتطلَّب تعاونًا بين الدول لإجراء التحقيقات فيها وملاحقة المرتكبين. وقد تم إبرام العديد من الاتفاقيات الدولية لتوفير إطار قانوني للتعاون بين الدول في هذا المجال (دورماز، 2024)، ومن أهمها:

- **اتفاقية بودابست للجرائم الإلكترونيَّة (2001) المعروفة رسميًّا باسم «الاتفاقية المتعلقة بالجريمة الإلكترونيَّة»**: وهي أول اتفاقية دولية تهدف إلى تنسيق القوانين الوطنية، وتعزيز التعاون الدول ي لمكافحة الجرائم الإلكترونيَّة. بدأت صياغتها في أواخر التسعينيات بمبادرة من مجلس أوروبا استجابةً لتزايد تهديدات الإنترنت، وتضمنت تعريفات موحدة للجرائم، وإجراءات للتحقيق والملاحقة، وآليات للتعاون بين الدول (Council of Europe, 2001).
- **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010)**: تهدف هذه الاتفاقية إلى تعزيز التعاون العربي في مجال مكافحة الجرائم الإلكترونيَّة، وتوحيد التشريعات العربية ذات الصلة، وتوفير آليات للتعاون الأمني والقضائي (جامعة الدول العربية، 2010).
- **الاتفاقية العالمية بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية (2024)**: اعتمدت الجمعية العامة للأمم المتحدة في يناير 2024 الاتفاقية العالمية الجديدة بشأن

مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، وتُعدُّ أول اتفاقية دولية شاملة تتناول الجرائم الإلكترونيَّة بطريقة موحدة على المستوى العالمي. وتهدف إلى تعزيز التعاون الدولي وتنسيق الجهود بين الدول لمكافحة التهديدات الإلكترونيَّة (United Nations General Assembly, 2024).

2. 3 قانون مكافحة الجرائم الإلكترونيَّة في اليمن

يوجد قصور تشريعي في اليمن فيما يتعلق بالجرائم الإلكترونيَّة؛ إذ لا يوجد في الجمهورية اليمنية قانون محدد ومستقل يعالج الجرائم الإلكترونيَّة حتى الآن (سبتمبر 2025)، وذلك قد يرجع إلى الفراغ التشريعي الناتج بسبب الحرب منذ سنوات، وتوقف المجلس التشريعي (مجلس النواب اليمني) عن انعقاد جلساته، ومن ثمَّ يتم التعامل مع هذه الجرائم بالاستناد إلى مواد في قانون الجرائم والعقوبات رقم (12) لسنة 1994، مثل: المواد (254)، و(256)، و(257)، و(313)، التي تتناول قضايا مثل: الاعتداء على الخصوصية، والتهديد، والابتزاز.

في السنوات الأخيرة، تم تقديم مشروع قانون لمكافحة جرائم تقنية المعلومات، وناقشته لجنة النقل والاتصالات في مجلس النواب اليمني في يونيو 2021، حيث تمت مناقشة المواد من (30) إلى (40) من المشروع. ومع ذلك، لم يتم إقرار هذا المشروع كقانون نافذ حتى الآن.

وبناءً على ذلك، لا يزال اليمن يفتقر إلى تشريع حديث ومخصص لمكافحة الجرائم الإلكترونيَّة؛ مما يبرز الحاجة الملحة لإصدار قانون يتماشى مع التطورات التكنولوجية الحديثة، ويعالج التحديات المرتبطة بها.

3. الدراسات السابقة

3. 1. عرض الدراسات السابقة

تناولت دراسات عديدة موضوع الجرائم الإلكترونيَّة من جوانب مختلفة. فقد استعرض مكتب الأمم المتحدة المعني بالمخدرات والجريمة (2013) طبيعة الجريمة السيبرانية عالميًّا، وخلص إلى أن الأطر القانونية غير كافية، وتحتاج إلى تعاون دولي وتدريب متخصص.

وفي السياق العربي، أظهرت دراسة الزبن والخرابشة (2021) أن طلاب جامعة البلقاء التطبيقية في الأردن لديهم وعي مرتفع نسبيًّا رغم ضعف التعرض للجرائم الإلكترونيَّة، فيما ركزت دراسة الشوابكة (2022) على المعوقات القانونية والفنية لمكافحة الجرائم الإلكترونيَّة في الأردن، مؤكدة الحاجة لتشريعات متطورة وتدريب المختصين، وضرورة تنمية الوعي المجتمعي حول هذه الجرائم.

أما العقيل (2022) فأكد أن الوعي المجتمعي بالجرائم الإلكترونيَّة في السعودية متوسط، مع ضعف في تطبيق إجراءات الحماية، فيما أوضحت دراسة النعامي (2023) في اليمن أن 47% من المشاركين تعرضوا لجريمة إلكترونيَّة واحدة على الأقل، وسط ضعف التوعية الرسمية. وتناولت دراسة Al-Baddai (2023) الابتزاز الإلكتروني ضد النساء اليمنيات، كاشفة عن آثاره النفسية والاجتماعية على الضحايا، وأوصت بتكاتف الجهود للحد من هذه الظاهرة وآثارها الخطيرة على الأفراد والمجتمع.

وأبرزت دراسة الخالدي وآخرين (2023) أهمية تعزيز دور الأمن العام في مكافحة الجرائم على وسائل التواصل لمواجهة التحديات المتزايدة. وأكدت دراسة الرشيدي والمهداوي (2023) تفاوت وعي طلاب الدراسات العليا في السعودية بنظام مكافحة الجرائم المعلوماتية. كما كشفت دراسة العجمي (2024) عن ارتفاع تعرض النساء الكويتيات للتنمر الإلكتروني، مشددة على ضرورة زيادة الوعي الإعلامي والبرامج التعليمية لحمايتهن ومنع هذه الجرائم.

وأظهرت دراسة العيدروس (2024) أن ضعف الوعي بالخصوصية الرقمية لدى طلاب كلية الحاسبات بجامعة حضرموت في اليمن يرتبط بزيادة تعرضهم للجرائم الإلكترونيَّة، نتيجة ممارسات غير آمنة وفجوة في أدوات الحماية. كما توصلت دراسة سعدون وعجيل (2024) في محافظة واسط بالعراق إلى تأثير العوامل الاقتصادية والاجتماعية على انتشار الجرائم، فيما ناقشت دراسة خالد (2024) ضرورة تحديث القانون الدولي الإنساني لمواكبة الحرب الإلكترونيَّة، وتعزيز التعاون الدولي لحماية البنية التحتية الحيوية.

كما تناولت دراسات حديثة أخرى القحطاني وآخرون، (2024)؛ العنوز (2024)؛ ابن داود وآخرون (2024) أدوار الإعلام الرقمي، والتباين بين الأمن السيبراني وأمن المعلومات، ومخاطر الدفع الإلكتروني، وقد خلصت جميعها إلى أهمية تعزيز الأمن الرقمي وتحديث التشريعات والتوعية المجتمعية.

3. 2. تميّز الدراسة الحاليَّة عن الدراسات السابقة

مع أن العديد من الدراسات السابقة تناولت موضوع الجرائم الإلكترونيَّة من زوايا متعددة، فإن الدراسة الحاليَّة تميزت بعدة جوانب، أبرزها:

1. التركيز المحلي المحدد: حيث تُعدُّ هذه الدراسة من أوائل الدراسات التحليلية الميدانية التي تتناول واقع الجرائم الإلكترونيَّة في مدينة المكلا بمحافظة حضرموت - اليمن، بينما أغلب الدراسات السابقة كانت ذات طابع عام، أو تناولت مدنًا أخرى أو مجتمعات غير يمنية.

2. شمولية المحاور: تضمنت الدراسة تحليلًا متكاملًا يشمل أنواع الجرائم، وآثارها النفسية والاجتماعية والمادية، ومستوى الوعي المجتمعي، وأسباب انتشارها، وتقييم فاعليَّة الإجراءات الرسمية، وهو اتساع لم تتناوله معظم الدراسات السابقة بنفس الشمول.
3. منهجية دقيقة وأداة إلكترونيَّة ذكية: استخدمت الدراسة أداة إلكترونيَّة تمنع الاستمرار دون الإجابة عن الأسئلة؛ مما قلل من الأخطاء وزاد من دقة النتائج.
4. رؤية تطبيقية موجهة للواقع المحلي: خلصت الدراسة إلى توصيات عملية قابلة للتنفيذ في البيئة اليمنية، تراعي خصوصية المجتمع المحلي وظروفه القانونية والاجتماعية والتقنية، وهو ما يجعل نتائجها ذات قيمة عملية للجهات الأمنية والمؤسسات التوعوية.

4. المنهجية

استخدمت الدراسة المنهج الوصفي باعتباره الأكثر مناسبة لتحقيق أهدافها من خلال الدراسة والتحليل والتفسير.

4. 1. مجتمع الدراسة

تكون مجتمع الدراسة من جميع الأفراد الموجودين في مدينة المكلا بمحافظة حضرموت، وهو المجتمع المستهدف في هذه الدراسة.

4. 2. عينة الدراسة

أُجريت الدراسة على عينة عشوائية من سكان مدينة المكلا في محافظة حضرموت - اليمن، وبلغ عدد أفراد العينة (427) فردًا.

تم توزيع الاستبانة إلكترونيًّا باستخدام نموذج رقمي تم تصميمه بطريقة تمنع المشارك من الانتقال إلى القسم التالي أو إرسال الاستبانة دون استكمال الإجابة عن جميع الأسئلة الإلزامية. وبناءً على ذلك، تم الحصول على عدد إجمالي من الردود بلغ (427) استبانة، جميعها صالحة للتحليل الإحصائي، دون وجود حالات مفقودة أو غير مكتملة. وقد تم اعتمادها بالكامل في تحليل النتائج.

4. 3. حدود الدراسة

الحدود المكانية: تم تنفيذ الدراسة في مدينة المكلا عاصمة محافظة حضرموت في اليمن.

الحدود الزمانية: تم تنفيذ الدراسة خلال الفترة من فبراير إلى إبريل عام 2025م.

4. 4. صعوبات الدراسة ونقاط الضعف

واجهت الدراسة عدة تحديات إجرائية قد تؤثر جزئيًّا على بعض النتائج، أبرزها: حساسية الموضوع الذي يتناول جرائم إلكترونيَّة؛ مثل: الابتزاز والتحرش والتشهير في مجتمع حضرمي محافظ؛ مما أدى إلى تحفُّظ المشاركين في الإجابة؛ والعزوف عن الإقرار بالتعرض؛ نتيجة الخوف من الوصمة الاجتماعية وفقدان الثقة؛ واستخدام الاستبانة الإلكترونيَّة التي استبعدت فئات غير متمكنة من التقنية؛ مما حدَّ من تمثيل الفئات الأقل اتصالًا بالإنترنت. مع ذلك، سعت الباحثة إلى تخفيف هذه التأثيرات عبر تبسيط لغة الاستبانة، وضمان سرية البيانات، والتأكيد على الطوعية؛ ما يعزِّز شفافية الدراسة، ويساعد في تفسير النتائج ضمن سياقها الواقعي.

4. 5. أداة الدراسة

تم استخدام الاستبانة كوسيلة من وسائل جمع البيانات من خلال قيام الباحثة بتوجيه أسئلة معينة للمستجيبين تتعلق بموضوع البحث، ويتم من خلالها الحصول على إجابات معينة يجري تحليلها لأغراض البحث.

بنيت الاستبانة على جزأين، يضمُّ الجزء الأول البيانات الديموغرافية للمستجيبين؛ مثل: العمر، الجنس، المستوى التعليمي، الوضع المهني، في حين يضمّ الجزء الثاني أربعة محاور تشمل:

- استخدام الإنترنت والتعرض للجرائم الإلكترونيَّة.
- أسباب وقوع الجرائم الإلكترونيَّة.
- الوعي بمخاطر الجرائم الإلكترونيَّة وكيفية الوقاية منها.
- آراء المستجيبين حول الإجراءات المتخذة لمكافحة هذه الجرائم.

4. 6. صدق أداة الدراسة

وهو الصدق المعتمد على آراء المحكمين، والذي يتم من خلاله التحقق من قدرة أداة الدراسة (العبارات والمجالات) على قياس ما صُممت لأجله، وقد تم التأكد من صدق الاستبانة من خلال عرضها على مجموعة من المحكمين من ذوي الاختصاص والخبرة في المجال محل الدراسة؛ حيث تم أخذ ملاحظاتهم القيمة وآرائهم بعين الاعتبار وتم تعديل بعض البنود وفقًا لذلك.

4. 7 ثبات أداة الدراسة

ويقصد به أن تعطي الاستبانة نفس النتيجة لو تم إعادة توزيعها أكثر من مرة تحت نفس الظروف والشروط؛ أو بعبارة أخرى أن ثبات الاستبانة يعني الاستقرار في نتائج الاستبانة، وعدم تغيرها بشكل كبير

جدول 1
الخصائص الديموغرافية للمشاركين في الدراسة.

Table 1
Demographic Characteristics of the Participants in the Study.

الخاصية	الفئة	العدد (n)	النسبة %
العمر	12 - 18 سنة	4	%0.9
	19 - 30 سنة	271	%63.5
	31 - 40 سنة	83	%19.4
	41 - 59 سنة	65	%15.2
	60 سنة فأكثر	4	%0.9
المستوى التعليمي	ثانوي أو أقل	43	%10
	دبلوم	24	%5.6
	بكالوريوس	294	%68.9
	دراسات عليا	66	%15.5
الوضع المهني	طالب/ة	177	%41.5
	موظف/ة	149	%34.9
	ربة منزل	20	%4.7
	أعمال حرة /خاصة	60	%14.1
	باحث/ة عن عمل	12	%2.8
	عاطل/ة عن العمل	5	%1.2
	متقاعد/ة	4	%0.9

فيما لو تم إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية معينة.

للتحقق من ثبات أداة الدراسة استُخدم أسلوب إعادة الاختبار Test-Retest على عينة عشوائية بلغ عددها حوالي 30 شخصًا، حيث طبقت الباحثة الاستمارة عليهم، ثم أعيد تطبيق الاستمارة على تلك العينة نفسها؛ وذلك بعد مرور أسبوعين من تطبيق الاختبار الأول، وقد بلغت قيمة معامل الثبات (0.88)، وهي قيمة عالية تشير إلى ثبات المقياس ودقته.

5. نتائج الدراسة وتفسيرها

التوزيع الديموغرافي لأفراد العينة

بلغ عدد أفراد العينة (427) فردًا من سكان مدينة المكلا، وقد تنوعت خصائصهم الديموغرافية من حيث الجنس، والعمر، والمستوى التعليمي، والوضع المهني (جدول 1)، بلغ عدد الذكور في العينة (203) مشاركين بنسبة (47.5%)، في حين بلغ عدد الإناث (224) مشاركة بنسبة (52.5%).

يُلاحظ أن غالبية المشاركين من الفئة العمرية (19–30 سنة)، وهي الفئة الأكثر استخدامًا للتقنيات الرقمية؛ مما يجعلها الأكثر عرضة لمخاطر الجرائم الإلكترونيَّة. كما أن العينة ذات مستوى تعليمي مرتفع نسبيًّا، حيث يشكّل حملة البكالوريوس والدراسات العليا النسبة الكبرى؛ الأمر الذي يعكس وعيًا عامًّا بطبيعة الجرائم الإلكترونيَّة. ومن حيث الوضع المهني، برزت فئة الطلاب والموظفين كالأكثر تمثيلًا، وهي الفئات الأكثر تفاعلًا مع التقنية في الحياة اليومية والمهنية؛ مما يمنح نتائج الدراسة مصداقية في رصد أثر الجرائم الإلكترونيَّة على المجتمع الحضرمي.

تحليل بيانات محور استخدام الإنترنت والتعرض للجرائم الإلكترونيَّة

أظهرت نتائج الدراسة أن الاستخدام المكثف للإنترنت يمثل عاملًا رئيسًا في رفع احتمالية التعرض للجرائم الإلكترونيَّة؛ حيث يقضي غالبية المشاركين أكثر من ست ساعات يوميًّا في أنشطة متنوعة، أبرزها التواصل الاجتماعي ومتابعة الأخبار والاستخدامات التعليمية والترفيهية. وهذا النمط من الاستخدام يعكس انخراطًا واسعًا في البيئة الرقمية، لكنه في الوقت نفسه يزيد من فرص الاستهداف بجرائم إلكترونيَّة. كما تبين أن نسبة غير قليلة من المشاركين تعرضت بالفعل لجرائم مختلفة؛ الأمر الذي يوضح وجود تهديدات حقيقية تمس الأفراد في المجتمع الحضرمي، ويؤكد ضرورة تعزيز التوعية الرقمية، وتفعيل آليات الحماية السيبرانية، إلى جانب توفير قنوات رسمية وآمنة للإبلاغ والدعم النفسي والقانوني. وتجدر الإشارة إلى أن نسب الأنشطة في الجدول قد تجاوزت 100% نظرًا لإتاحة المجال للمشاركين لاختيار أكثر من نشاط واحد في الاستبانة (جدول 2).

يوضح جدول رقم 3 أن اختراق الحسابات الشخصية يتصدر الجرائم الإلكترونيَّة بنسبة 50%؛ مما يعكس ضعف الوعي الأمني الرقمي لدى الأفراد، واستخدام إعدادات خصوصية غير كافية، وهو مدخل شائع لجرائم أخرى كالابتزاز والاحتيال. بينما تساوت جرائم الاحتيال الإلكتروني والتشهير أو السبِّ والقذف عبر الإنترنت في المرتبة الثانية بنسبة 30.3% لكل منهما؛ مما يعكس تنوع التهديدات المالية والاجتماعية. وجاء التنمر الإلكتروني والإساءة في المرتبة الثالثة بنسبة 23.7%، يليه الابتزاز الإلكتروني بنسبة 22.4%، الذي يُعدُّ من الجرائم الخطيرة بتأثيره النفسي العميق على الضحايا. أما سرقة الهوية

جدول 2

خصائص استخدام الإنترنت لدى المشاركين.

Table 2

Internet Usage Characteristics of Participants.

البند	الفئة/الخيار	العدد (n)	النسبة %
مدة الاستخدام اليومي	أقل من ساعة	7	1.6%
	1-3 ساعات	93	21.8%
	4-6 ساعات	158	37%
	أكثر من 6 ساعات	169	39.6%
الأنشطة الأكثر شيوعًا	التواصل الاجتماعي	285	66.7%
	متابعة الأخبار	272	63.7%
	الاستخدام لأغراض الدراسة	263	61.6%
	الاستخدام لأغراض العمل	207	48.5%
	الترفيه والتسوق واللعب	243	56.9%
	مشاركة المحتوى	162	37.9%
	إجراء المعاملات المالية	84	19.7%
	التعبير عن الرأي	55	12.9%
	البحث عن أصدقاء جدد	24	5.6%
التعرض للجرائم الإلكترونيَّة	نعم	76	17.8%
	لا	351	82.2%

فبلغت نسبتها 10.5%، ومع انخفاضها نسبيًّا، فإن خطورتها تكمن في استخدامها كوسيلة لجرائم أكثر تعقيدًا.

ويُلاحظ أن العدد الإجمالي لأنواع الجرائم التي أبلغ عنها المشاركون (127) يزيد على عدد الأفراد الذين تعرضوا للجرائم الإلكترونيَّة (76)، ويُعزى ذلك إلى أن بعض المشاركين تعرضوا لأكثر من نوع جريمة في الوقت نفسه، مثل: اختراق الحساب متبوعًا بالابتزاز أو الاحتيال. وبما أن الاستبانة لم تتضمن سؤالًا مستقلًّا حول عدد الجرائم التي تعرض لها الفرد (جريمة واحدة أو أكثر)، فقد تم الاكتفاء بعرض التوزيع النوعي للجرائم، كما ورد من المشاركين دون هذا التفصيل.

وتعكس هذه النتائج واقعًا مقلقًا لتنوع وانتشار الجرائم الإلكترونيَّة في المجتمع الحضرمي، خصوصًا بمدينة المكلا؛ مما يستدعي تعزيز الوعي الرقمي، وتفعيل القوانين الرادعة، ودعم برامج التثقيف الوقائي.

تُظهر النتائج أن فئة الشباب (19–30 عامًا)، التي تمثل 63.5% من العينة والأكثر استخدامًا للتقنيات الرقمية، هي الأكثر عرضة للجرائم الإلكترونيَّة، خاصةً جرائم اختراق الحسابات. كما بدا التوزيع بين الجنسين متوازنًا (47.5% ذكور، 52.5% إناث)، غير أن طبيعة الجرائم

جدول 3

توزيع أنواع الجرائم الإلكترونيَّة التي تعرض لها المشاركون.

Table 3

Distribution of Types of Cybercrimes Experienced by Participants.

نوع الجريمة الإلكترونيَّة	العدد(n)	النسبة %
اختراق الحسابات الشخصية	38	50%
الاحتيال الإلكتروني	23	30.3%
التشهير أو السبُّ والقذف عبر الإنترنت	23	30.3%
التنمر الإلكتروني والإساءة	18	23.7%
الابتزاز الإلكتروني	17	22.4%
سرقة الهوية	8	10.5%
المجموع	127	

جدول 4

التوزيع الزمني للتعرض للجرائم الإلكترونيَّة.

Table 4

Time Distribution of Exposure to Cybercrimes.

فترة التعرض	العدد (n)	النسبة %
منذ أكثر من 6 أشهر	58	76.3%
خلال الفترة من 3–6 أشهر	9	11.8%
خلال الأشهر الثلاثة الماضية	9	11.8%
المجموع	76	

اختلفت؛ إذ كانت الإناث أكثر عرضة للابتزاز والتنمر، بينما تعرض الذكور للاحتيال والتصيد الإلكتروني بدرجة أكبر.

ومع أن أكثر من 84% من المشاركين يحملون مؤهلات جامعية، فإن معدلات التعرض للجرائم ظلت مرتفعة؛ مما يشير إلى أن التعليم الأكاديمي لا يكفي وحده لتوفير وعي تقني كافٍ للحماية الرقمية.

أما من حيث الوضع المهني، فقد شكّل الطلاب (41.5%) والموظفون (34.9%) النسبة الكبرى من المتعرضين؛ نتيجة اعتمادهم المكثف على الإنترنت في الدراسة والعمل؛ مما جعلهم أكثر عرضة لأنواع متعددة من الجرائم.

كما يوضح جدول 4، فإن غالبية المشاركين الذين تعرضوا للجرائم الإلكترونيَّة (76 مشاركًا) أفادوا بوقوع الحوادث منذ أكثر من ستة أشهر بنسبة (76.3%)، في حين ذكر (11.8%) أن تعرضهم كان خلال فترة تتراوح بين ثلاثة إلى ستة أشهر، والنسبة نفسها أشارت إلى أن الحوادث وقعت خلال الثلاثة أشهر الماضية. ويُظهر ذلك أن التهديد

جدول 5

التوزيع النسبي للمشاركين المتعرضين للخسائر المالية الناتجة عن الجرائم الإلكترونيَّة.

Table 5

Distribution of participants exposed to financial losses caused by cybercrimes.

نوع الاستجابة	النسبة المئوية	تفاصيل الخسارة المالية	النسبة المئوية من المتضررين
لم يتعرض لخسائر مالية	%75	-	-
تعرض لخسائر مالية	%25	أقل من 50 ألف ريال يمني	%31.6
		من 50 ألف - 100 ألف ريال يمني	%21.1
		أكثر من 100 ألف ريال يمني	%47.4

ما يزال قائمًا، وإن تفاوتت وتيرته بين الفئات. وقد تبين أن الفئة العمرية (19-30 عامًا) هي الأكثر تعرضًا للحوادث الحديثة، نظرًا لكثافة استخدامها للتقنيات الرقمية، بينما تركزت الحوادث الأقدم بين الفئات الأكبر سنًّا بسبب محدودية أو تحفظ استخدامهم للتقنية.

وتشير هذه النتائج إلى الحاجة لتصميم برامج توعوية موجهة بحسب الفئة العمرية، مع تركيز خاص على فئة الشباب الأكثر انخراطًا في البيئة الرقمية.

أظهرت نتائج الدراسة أن معظم المشاركين الذين تعرضوا لجرائم إلكترونيَّة لم يتكبَّدوا خسائر مالية مباشرة (75%)، في حين أفاد نحو ربعهم (25%) بوقوع خسائر متفاوتة، كما هو موضح في جدول 5. وقد توزعت هذه الخسائر بين مبالغ صغيرة تقل عن 50 ألف ريال يمني (31.6%)، ومبالغ متوسطة تتراوح بين 50 ألفًا و100 ألف ريال يمني (21.1%)، بينما تكبَّد ما يقارب نصف المتضررين خسائر كبيرة تجاوزت 100 ألف ريال يمني (47.4%).

تشير هذه النتائج إلى أن الآثار الاقتصادية للجريمة الإلكترونيَّة ليست شائعة بين جميع الضحايا، لكنها قد تكون شديدة الخطورة في بعض الحالات، حيث يعكس حجم الخسائر المرتفعة أن بعض الجرائم تستهدف الأفراد مباشرة بالابتزاز أو الاحتيال المالي. وهذا يبرز الحاجة إلى تعزيز الوعي المجتمعي، ورفع مستوى الحماية الإلكترونيَّة، خصوصًا لدى الفئات الأكثر عرضة للاستهداف.

كما أظهرت نتائج الدراسة أن 57.9% من المشاركين الذين تعرضوا لجرائم إلكترونيَّة تأثروا نفسيًّا واجتماعيًّا بشكل سلبي، بينما أفاد 42.1% بعدم تعرضهم لتأثيرات تُذكر (جدول 6)، وهو ما قد يرتبط بقدرتهم

جدول 6

الآثار النفسية والاجتماعية للجرائم الإلكترونيَّة على المشاركين.

Table 6

Psychological and social impacts of cybercrimes on participants.

الحالة العامة	النسبة المئوية	نوع التأثير لدى المتضررين	النسبة المئوية
لم يتأثر نفسيًّا أو اجتماعيًّا	%42.1	-	-
تأثر نفسيًّا أو اجتماعيًّا	%57.9	فقدان الثقة بالآخرين	%77.3
		الشعور بالخوف	%50
		مشكلات في النوم	%43.2
		مشكلات في العمل أو الدراسة	%43.2
		مشكلات مع العائلة	%11.4

على التكيف أو بطبيعة الجرائم التي تعرضوا لها. وتشير هذه النتائج إلى أن آثار الجرائم الإلكترونيَّة لا تقتصر على الخسائر المالية فحسب، بل تمتد لتشمل أبعادًا نفسية واجتماعية قد تكون طويلة الأمد.

وعند تحليل طبيعة هذه التأثيرات (جدول 6)، برز فقدان الثقة بالآخرين كأكثر الآثار شيوعًا بنسبة 77.3%، يليه الشعور بالخوف (50%)، ثم مشكلات في النوم والعمل أو الدراسة (43.2%). كما أشار 11.4% من الضحايا إلى نشوء مشكلات أسرية نتيجة الحادثة. وتعكس هذه المؤشرات الحاجة إلى إدماج برامج الدعم النفسي والاجتماعي ضمن جهود التوعية والوقاية، لمساعدة الضحايا على تجاوز الصدمات والتخفيف من انعكاساتها الاجتماعية.

أظهرت نتائج الدراسة أن نسبة كبيرة من المشاركين الذين تعرضوا للجرائم الإلكترونيَّة لم يقوموا بالإبلاغ عن الحوادث لدى الجهات المختصة، حيث بلغت النسبة 76.3%، في حين أبلغ 23.7% فقط، وهو ما يعكس ضعفًا في الثقة بالإجراءات الرسمية أو فاعلية الجهات المختصة.

وعند تحليل أسباب العزوف عن الإبلاغ، كانت أبرزها:

- عدم معرفة كيفية الإبلاغ: شكَّل السبب الأكبر نسبة 46.6%؛ مما يدل على غياب واضح لقنوات توعوية فعَّالة تُرشد الضحايا إلى الإجراءات المطلوبة، أو أن الطرق المتاحة قد تكون معقَّدة أو غير معروفة لدى العامة.
- عدم الثقة بالجهات الأمنية: أفاد 12.1% من المشاركين بعدم ثقتهم في الجهات المختصة، وهو مؤشر على ضعف العلاقة بين المجتمع ومؤسسات إنفاذ القانون في هذا الجانب، وقد يكون ناتجًا عن تجارب سلبية سابقة أو بطء في الإجراءات.

جدول 7

متوسط مساهمة أهم العوامل التي تؤدي إلى الجرائم الإلكترونيَّة من وجهة نظر المجتمع.

Table 7

Average Contribution of Key Factors Leading to Cybercrimes from the Community's Perspective.

م	العامل	غير مساهم أبدًا	مساهم بشكل طفيف	مساهم	مساهم بشكل كبير	المتوسط الحسابي
1	ضعف الوعي بمخاطر الإنترنت وكيفية الحماية منها.	23	32	119	253	3.41
2	ضعف القوانين المتعلقة بالجرائم الإلكترونيَّة.	27	42	106	252	3.37
3	الإفراط في مشاركة المعلومات الشخصية على الإنترنت.	26	44	111	246	3.35
4	ضعف الرقابة الأسرية على استخدام الأبناء للإنترنت.	22	57	118	230	3.30
5	صعوبة تتبع مرتكبي الجرائم الإلكترونيَّة.	31	40	127	229	3.30
6	استخدام برامج وتطبيقات غير آمنة.	28	49	124	226	3.28
7	بطء إجراءات التقاضي.	49	70	115	193	3.06
8	الرغبة في الانتقام أو إلحاق الضرر بالآخرين.	56	89	155	127	2.83
9	الرغبة في الثراء السريع.	71	103	137	116	2.70
10	البطالة والظروف الاقتصادية الصعبة.	68	105	140	114	2.70
11	عدم تحديث أنظمة التشغيل وبرامج الحماية.	46	131	169	81	2.67

- الشعور بالإحراج والعار والخوف من الفضيحة: ظهر هذا السبب بنسبة 8.6%، خاصةً في الجرائم التي تنطوي على محتوى شخصي أو علاقات حساسة؛ مما يشير إلى وجود عبء اجتماعي وثقافي يثقل كاهل الضحية ويمنعه من طلب المساعدة.

بالإضافة إلى انخفاض نسبة الإبلاغ عن الجرائم الإلكترونيَّة، أظهرت النتائج أن تجربة الإبلاغ نفسها لم تكن مجدية في نظر غالبية من قاموا بها؛ حيث أشار 55.6% من المشاركين الذين أبلغوا عن الجريمة إلى أنهم لم يستفيدوا من الإبلاغ، في حين أفاد 16.7% فقط أنهم استفادوا فعليًّا، والبقية (27.7%) لم يستطيعوا تحديد ما إذا كانت هناك فائدة أم لا.

وهذا يُشير إلى عدة إشكالات:

- وجود تجارب سلبية أو غير واضحة بعد الإبلاغ، قد تشمل بطء الإجراءات، وغياب المتابعة، أو عدم الحصول على نتيجة مرضية.
- ضعف الشفافية والتواصل بين الجهات المختصة والمبلِّغين، مما يؤدي إلى شعور الضحية بأن بلاغه لم يكن له أثر حقيقي.
- غياب التقييم اللاحق والتغذية الراجعة؛ حيث لا يتم إبلاغ الضحايا بتطورات القضايا أو ما تم اتخاذه من إجراءات.

تحليل بيانات محور أسباب وقوع الجرائم الإلكترونيَّة

سُئل المشاركون عن مدى إسهام مجموعة من العوامل في وقوع الجرائم الإلكترونيَّة؛ وذلك باستخدام مقياس ليكرت رباعي يتراوح بين (غير مساهم أبدًا، مساهم بشكل طفيف، مساهم، مساهم بشكل كبير). وقد أظهرت النتائج تفاوتًا في درجة مساهمة هذه العوامل بحسب تقييم المشاركين، كما هو موضح في الجدول التالي (جدول 7):

نلاحظ من جدول 7 النقاط الآتية:

1. العوامل الأعلى في المتوسط الحسابي (أعلى من 3.30) التي تعني أن المشاركين يرون أنها تسهم بشكل كبير في انتشار الجرائم الإلكترونيَّة:
   - ضعف الوعي بمخاطر الإنترنت (3.41): مما يدل على الحاجة الملحَّة لتكثيف برامج التوعية.
   - ضعف القوانين المتعلقة بالجرائم الإلكترونيَّة (3.37): ويشير إلى أن المشاركين يرون القانون غير رادع؛ مما يشجع الجناة.
   - الإفراط في مشاركة المعلومات الشخصية (3.35): ويكشف عن سلوك خاطئ للمستخدمين يُسهل استغلاله.
2. العوامل المتوسطة (من 3.00 إلى 3.29)، تسهم بشكل ملحوظ ولكن أقل شدة، كما أن ضعف الرقابة الأسرية، وصعوبة

تتبع المجرمين،و استخدام برامج وتطبيقات غير آمنة، وبطء الإجراءات القضائية. هذه العوامل تشير إلى مشكلات مؤسساتية وأسرية تحتاج إلى تطوير وتعاون بين الأسرة، والجهات الأمنية، والقضاء.

3. العوامل ذات التأثير المنخفض (أقل من 3.00): وهي الأقل إسهامًا من وجهة نظر المشاركين، مثل: الرغبة في الانتقام أو الثراء، والبطالة، وعدم تحديث الأنظمة. هذه العوامل تعكس مشكلات فردية أو سلوكية أو حتى اقتصادية، ولكنها لم تُعدُّ أسبابًا رئيسة بنفس القوة.

تحليل بيانات محور الوعي بمخاطر الجرائم الإلكترونيَّة وكيفية الوقاية منها

يُعدُّ الوعي بمخاطر الجرائم الإلكترونيَّة من الركائز الأساسية التي تُمكِّن الأفراد من حماية أنفسهم من الوقوع ضحايا لتلك الجرائم، كما يمثل عنصرًا حاسمًا في منظومة الوقاية والتصدي للتهديدات الرقمية. وقد أولت هذه الدراسة أهمية خاصة لاستكشاف مستوى هذا الوعي لدى المشاركين، سواء من حيث المعرفة العامة بالمخاطر، أو السلوكيات الوقائية، أو مصادر التوعية.

عند سؤال المشاركين عن معرفتهم بمخاطر الجرائم الإلكترونيَّة، أفاد 31.6% بأن معرفتهم متوسطة، و30.9% جيدة، و20.8% جيدة جدًّا، بينما 10.8% ضعيفة و5.9% ضعيفة جدًّا. بذلك، أكثر من 80% يمتلكون معرفة بين المتوسطة والجيدة جدًّا، وهو مؤشر إيجابي على الوعي المجتمعي. ومع ذلك، يشكل 16.7% ممن لديهم معرفة ضعيفة فجوة معرفية تستدعي تعزيز التوعية، خاصة مع ارتباط ضعف الوعي بانتشار الجرائم الإلكترونيَّة.

كما تم سؤال المشاركين عن أهم المصادر الرئيسة التي يحصلون منها على المعلومات المتعلقة بالجرائم الإلكترونيَّة، وقد كانت النتائج على النحو التالي:

- 85%من المشاركين يعتمدون على وسائل الإعلام والإنترنت كمصدر أساسي للمعلومات.
- 38.4% يستقون معلوماتهم من برامج التوعية.
- 30.2% يتابعون ما تنشره الجهات الأمنية.
- 28.3% يحصلون على المعلومات من الأصدقاء والعائلة.

تشير هذه النتائج إلى أن الغالبية العظمى تعتمد على المصادر الرقمية والإعلامية العامة؛ مما يعكس أهمية الدور الذي تؤديه المنصات الإعلامية وشبكات الإنترنت في تشكيل وعي الجمهور بمخاطر الجريمة الإلكترونيَّة.

جدول 8

إجراءات الحماية المتبعة من قبل المشاركين ضد الجرائم الإلكترونيَّة

Table 8

Protective Measures Adopted by Participants against Cybercrimes.

الإجراء المتبع	النسبة المئوية
عدم مشاركة المعلومات الشخصية مع مصادر غير موثوقة	%82.2
الحذر من الروابط والرسائل المشبوهة	%80.8
استخدام كلمات مرور قوية ومعقَّدة	%76.8
استخدام التحقق الثنائي	%54.1
تحديث الأنظمة وبرامج الحماية	%36.8
استخدام برامج مكافحة الفيروسات	%36.8
تغيير إعدادات الخصوصية على شبكات التواصل	%33.3
لا يتخذ أي إجراء للحماية	%8.2

ومن جهة أخرى، فإن نسب الاعتماد على برامج التوعية، أو ما تنشره الجهات الأمنية لا تزال أقل من المتوقع، وهو ما يمكن تفسيره إما بقلة هذه المبادرات، أو بعدم وصولها بالشكل الكافي إلى الجمهور.

كما أن النسبة الملحوظة للمعلومات المتناقلة عبر الأصدقاء والعائلة قد تعني وجود نوع من المعرفة غير الرسمية، التي قد تكون أحيانًا غير دقيقة أو غير موثوقة؛ مما يستدعي تعزيز القنوات الرسمية والموثوقة لتثقيف المجتمع.

بالرغم من أن بعض المشاركين أفادوا بأنهم يعتمدون على برامج التوعية كمصدر للمعلومات، إلا أن الإجابة عن سؤال حول المشاركة الفعلية في تلك البرامج كشفت عن نتائج مقلقة؛ حيث أظهرت البيانات أن:

- 77.8% من المشاركين لم يسبق لهم المشاركة في أي برامج توعية تتعلق بالأمن السيبراني أو الجرائم الإلكترونيَّة،
- بينما أفاد الباقون (22.2%) بأنهم شاركوا في مثل هذه البرامج.

تعكس هذه النتيجة ضعف الانخراط المجتمعي في أنشطة التوعية، على الرغم من تزايد التهديدات الإلكترونيَّة. ويُحتمل أن تكون هذه النسبة نتيجة لغياب البرامج التوعوية المنهجة، أو ضعف انتشارها، أو حتى ضعف الترويج لها عبر القنوات المناسبة. ويمكن اعتبار هذه الفجوة عاملًا مفسرًا لبعض النتائج السابقة، مثل: تفاوت مستوى الوعي، واستمرار بعض السلوكيات الخطرة على الإنترنت؛ مما يدعم الحاجة إلى إعادة هيكلة برامج التوعية لتكون أكثر شمولًا وانتشارًا، مع التركيز على الفئات الأكثر عرضة للخطر.

يوضح جدول 8 أن التدابير الأكثر شيوعًا بين المشاركين كانت تجنُّب مشاركة المعلومات الشخصية (82.2%)، والحذر من الروابط المشبوهة (80.8%)، واستخدام كلمات مرور قوية (76.8%). بينما ظهر ضعف نسبي في تبنِّي بعض التدابير مثل: تحديث الأنظمة أو تغيير إعدادات الخصوصية، وهو ما يكشف الحاجة إلى حملات توعوية تستهدف رفع الوعي بهذه الجوانب.

وتشير هذه النتائج إلى أن أغلب المشاركين لديهم وعي جيد بمفاهيم الحماية الرقمية الأساسية، إلا أن هناك حاجة لتوسيع الوعي حول بعض الإجراءات الإضافية؛ مثل: أهمية تحديث الأنظمة وتفعيل إعدادات الخصوصية، وهي عوامل لا تقل أهمية في منع الاختراقات والهجمات الإلكترونيَّة.

تحليل بيانات محور آراء المستجيبين حول الإجراءات المتخذة لمكافحة هذه الجرائم

طرحت الدراسة سؤالًا لقياس «مدى ثقة المشاركين في الجهات الأمنية وقدرتها على مواجهة الجرائم الإلكترونيَّة»، فجاءت النتائج على النحو التالي:

- 34.4%من المشاركين أبدوا رأيًا محايدًا.
- 24.1%عبّروا عن أنهم غير واثقين.
- 15.9% صرّحوا بأنهم غير واثقين على الإطلاق.
- في المقابل، أفاد 19.2% بأنهم واثقون.
- بينما أعرب 6.3% فقط عن ثقة كبيرة جدًّا.

تشير هذه النتائج إلى أن ما يقارب 40% من المشاركين لا يثقون بالجهات الأمنية، وهي نسبة لا يُستهان بها، تعكس وجود فجوة في العلاقة بين المؤسسات الأمنية والمجتمع فيما يخص التعامل مع الجريمة الإلكترونيَّة.

من جهة أخرى، فإن نسبة الثقة المرتفعة نسبيًّا (25.5% مجموع «واثق» و«واثق جدًّا») تمثل شريحة ما زالت ترى أن هناك إمكانية لمواجهة هذه الظاهرة بفاعليَّة، بينما تمثل الفئة المحايدة أكبر نسبة؛ مما يدل على حالة من الترقب وعدم الحسم في تقييم الأداء الرسمي.

هذه المعطيات تؤكد ضرورة تعزيز ثقة المواطنين من خلال الشفافية، والتواصل المجتمعي، والإعلان عن النجاحات والإنجازات الأمنية في مكافحة الجرائم الإلكترونيَّة؛ لما لذلك من دور في تحفيز الإبلاغ، والمشاركة في التوعية، والتعاون مع الجهات المختصة.

كما سُئل المشاركون عن «مدى اعتقادهم بفاعليَّة القوانين الحاليَّة في ردع الجرائم الإلكترونيَّة»، فجاءت آراؤهم على النحو التالي:

- 37% أفادوا بأنهم لا يعتقدون أنها رادعة.
- 21.3% قالوا: إنهم لا يعتقدون على الإطلاق أنها رادعة.
- في المقابل، 13.8% يعتقدون أنها رادعة.
- و4% فقط يرون أن القوانين رادعة بشدة.
- بينما 23.9% كانوا محايدين في رأيهم.

تشير هذه النتائج إلى أن ما نسبته 58.3% من المشاركين لديهم قناعة بعدم فاعليَّة القوانين الحاليَّة في ردع الجرائم الإلكترونيَّة، وهي نسبة عالية تُظهر تحديًا حقيقيًّا في الثقة بالإطار التشريعي لمواجهة هذه الظاهرة.

ويبدو أن ضعف هذه القناعة قد يكون مرتبطًا بتجارب سابقة، أو بقصور في تطبيق القوانين، أو في وعي الجمهور بوجودها وآليات تفعيلها. كما أن النسبة الضعيفة لمن يعتقدون بقوة القانون تعكس حاجة ماسة إلى:

- مراجعة شاملة للتشريعات النافذة.
- توسيع نطاق التوعية القانونية.
- رفع مستوى الشفافية بشأن الحالات التي نُفذت فيها العقوبات بفاعليَّة.

ويُحتمل أن يكون هذا التصور عاملًا مساعدًا في العزوف عن الإبلاغ، كما أظهر المحور السابق؛ مما يجعل من تعزيز الإطار القانوني ونشر الوعي به ركيزة أساسية في جهود الوقاية والمكافحة.

تشير نتائج جدول 9 إلى أن المشاركين اتفقوا على مجموعة من الإجراءات المتكاملة للحد من انتشار الجرائم الإلكترونيَّة، حيث تصدَّر

جدول 9

الإجراءات المقترحة من المشاركين للحد من انتشار الجرائم الإلكترونيَّة

Table 9

Suggested Measures by Participants to Reduce the Spread of Cybercrimes.

الإجراء المقترح	نسبة التأييد
تنمية الوعي المجتمعي بأهمية الإبلاغ وعدم التستر على الجرائم الإلكترونيَّة	%76.3
تسهيل إجراءات الإبلاغ من خلال قنوات اتصال سهلة وفعَّالة	%75.4
إدراج مواد تعليمية حول الأمن السيبراني في المناهج الدراسية	%74.9
تفعيل دور الأسرة في مراقبة الأبناء وتوعيتهم	%72.6
تنظيم ورش ودورات تدريبية للجمهور حول الحماية من الجرائم الإلكترونيَّة	%72.4
تحديث وتطوير القوانين لتشمل جميع أنواع الجرائم الإلكترونيَّة وتحديد عقوبات رادعة	%71.9

تعزيز الوعي المجتمعي بأهمية الإبلاغ وعدم التستر قائمة الأولويات، تليه الحاجة إلى تسهيل قنوات الإبلاغ، ثم إدراج مفاهيم الأمن السيبراني في التعليم المبكر. كما برزت أهمية الدور الأسري والتدريب المجتمعي، إلى جانب المطالبة بتطوير التشريعات لمواكبة الأشكال المستحدثة من الجريمة.

وترى الباحثة أن هذا التوزيع المتقارب للنسب يعكس وعيًا عامًّا بضرورة الجمع بين الوقاية التوعوية والدعم القانوني والتسهيل الإداري، بما يضمن بناء بيئة رقميَّة أكثر أمانًا؛ ويعزِّز الثقة بين المجتمع والجهات الرسمية.

6. الخاتمة

يمثل هذا البحث محاولة علمية لدراسة واقع الجرائم الإلكترونيَّة في مدينة المكلا بمحافظة حضرموت - اليمن، وذلك من خلال رصد أشكالها، وتحليل العوامل المؤثرة فيها، وتقييم آثارها على الأفراد، ومستوى وعيهم بها، ومدى فاعلية الإجراءات المتخذة لمكافحتها.

أظهرت النتائج أن الجرائم الإلكترونيَّة باتت تمثل تهديدًا فعليًّا لأمن الأفراد والمجتمع، سواء من الجانب النفسي أو الاقتصادي أو الاجتماعي، كما كشفت عن وجود فجوات واضحة في منظومة الحماية الرقمية؛ سواء على مستوى الوعي المجتمعي، أو فاعليَّة القوانين، أو قنوات الإبلاغ والاستجابة.

كما تبيّن أن أغلب المشاركين يعتمدون على وسائل الإعلام والإنترنت كمصادر معرفية، مع ضعف المشاركة في البرامج التوعوية الرسمية، إضافة إلى محدودية الثقة في قدرة الجهات الأمنية على التعامل مع هذه الجرائم، وعدم القناعة بفاعليَّة التشريعات الحاليَّة. وأشار المشاركون إلى مجموعة من الإجراءات المقترحة لتعزيز الوقاية والمكافحة، شملت الجوانب القانونية، والتوعوية، والتقنية، والدور الأسري.

وتبرز هذه الدراسة الحاجة إلى تبني سياسات شاملة ومتكاملة تعزِّز من أمن المجتمع الرقمي، وتعمل على سد الثغرات الوقائية والتشريعية والتنظيمية. كما تعكس النتائج القصور الواضح في المنظومة التشريعية والتوعوية، إلى جانب الضعف في القدرات التقنية، وهو ما يجعل البيئة الرقمية في المجتمع الحضرمي عرضة لمزيد من التهديدات السيبرانية، ويستدعي تعزيز التنسيق بين الجهات الأمنية والمؤسسات التعليمية والإعلامية لمواجهتها.

وتؤكد الدراسة أن التحليل الميداني للجرائم الإلكترونيَّة يكشف عن أنماط تهديدات متنامية تستوجب تدخلات وقائية وتشريعية عاجلة. وتتمثل الإضافة العلمية للبحث في تقديم إطار تحليلي يربط بين المعطيات الميدانية والاحتياجات الأمنية الفعلية للمجتمع الحضرمي، مع اقتراح حلول عملية قابلة للتطبيق لتعزيز الحماية الرقمية.

وتختتم الدراسة بالإشارة إلى أنها تسهم في إثراء المعرفة حول هذا الموضوع الحيوي، وتمثل منطلقًا لدراسات مستقبلية أوسع نطاقًا وأكثر عمقًا، خاصة في ظل التطور السريع للتقنية وتعدد أشكال التهديدات الإلكترونيَّة.

7. النتائج العامة للدراسة

استنادًا إلى تحليل بيانات الاستبانة وتحقيقًا لأهداف البحث، توصلت الدراسة إلى مجموعة من النتائج العامة التي تعكس واقع الجرائم الإلكترونيَّة في مدينة المكلا، ويمكن تلخيصها على النحو الآتي:

1. أظهرت الدراسة أن من أكثر أنواع الجرائم الإلكترونيَّة شيوعًا في مدينة المكلا: اختراق الحسابات الشخصية، يليها الاحتيال الإلكتروني وجرائم التشهير والسب، ثم جرائم التنمر والإساءة والابتزاز الإلكتروني، إضافة إلى سرقة الهُويَّة الرقمية.
2. كشفت نتائج الدراسة أن نسبة كبيرة من المشاركين تعرضوا لأحد أشكال الجرائم الإلكترونيَّة، وأن معظمهم تعرض لها منذ أكثر من ستة أشهر؛ مما يدل على استمرار هذه الجرائم وإن كان بوتيرة متفاوتة.
3. بيَّنت النتائج أن من بين الذين تعرضوا للجرائم الإلكترونيَّة، نسبة مهمة قد تكبَّدت خسائر مادية، تجاوزت في بعض الحالات مئة ألف ريال يمني، إضافة إلى آثار نفسية واجتماعية تمثلت في فقدان الثقة، والشعور بالخوف، ومشكلات في النوم والعمل والعلاقات الأسرية.
4. كشفت الدراسة أن من أبرز العوامل التي تسهم في انتشار الجرائم الإلكترونيَّة: الإفراط في مشاركة المعلومات الشخصية، وضعف القوانين، وضعف الوعي المجتمعي، وضعف الرقابة الأسرية، وصعوبة تتبع مرتكبي هذه الجرائم.
5. أظهرت النتائج أن الغالبية العظمى من المشاركين يعتمدون على الإنترنت ووسائل الإعلام كمصدر رئيس للمعلومات، مع ضعف في المشاركة ببرامج التوعية الرسمية.
6. تباينت آراء المشاركين حول قدرة الجهات الأمنية على مكافحة هذه الجرائم، إلا أن نسبة كبيرة منهم أبدت عدم ثقة كافية، كما أن أغلبهم لا يرون أن القوانين الحاليَّة رادعة بما فيه الكفاية.
7. اقترح المشاركون عددًا من الإجراءات للحد من هذه الجرائم، كان أبرزها: تنمية الوعي، تسهيل الإبلاغ، إدراج الأمن السيبراني في التعليم، تحديث القوانين.

8. التوصيات

استنادًا إلى نتائج الدراسة، وتحقيقًا لأهدافها في تعزيز الأمن السيبراني، والحد من الجرائم الإلكترونيَّة في مدينة المكلا والمجتمع الحضرمي عامةً، تقترح الباحثة مجموعة من التوصيات العملية التي رُوعي في صياغتها أن تكون قابلة للتطبيق، مع وضوح الجهة المنفذة المحتملة وآلية التنفيذ المقترحة، بحسب طبيعة كل مجال.

وقد تم توزيع هذه التوصيات على خمسة مجالات رئيسة، بالإضافة إلى محور تقني داعم، لتعكس معالجة شاملة تشمل البعدين الوقائي والعلاجي، وتعزِّز من كفاءة الاستجابة المجتمعية والأمنية لهذه الظاهرة المتنامية.

1. التوعية الأمنية ودور المؤسسات التعليمية

توصي الباحثة بضرورة تبني برامج توعية أمنية شاملة تستهدف جميع فئات المجتمع، مع التركيز على الشباب والطلاب؛ وذلك للحد من مخاطر الجرائم الإلكترونيَّة. وتشمل هذه البرامج:

1. تنظيم حملات إعلامية على وسائل الإعلام التقليدية والمنصات الرقمية لتعريف الجمهور بأنواع الجرائم الإلكترونيَّة وأساليب الوقاية منها.
2. عقد ورش عمل ودورات تدريبية للأسر والطلاب لتعزيز مهارات الحماية الرقمية.
3. إدراج مفاهيم الأمن السيبراني والوقاية الرقمية ضمن المناهج الدراسية في المدارس والجامعات، بما يعزِّز الوعي المبكر لدى الأجيال الصاعدة.
4. تفعيل الشراكات بين المؤسسات التعليمية والجهات الأمنية لتبادل الخبرات وإطلاق مبادرات توعوية مشتركة.

تم إعداد هذه التوصية بناءً على ما كشفته نتائج الدراسة من ضعف المشاركة في البرامج التوعوية الرسمية، ومحدودية إدراج مفاهيم الأمن السيبراني في المناهج التعليمية، بما يجعلها ضرورة إستراتيجية لتعزيز الأمن المجتمعي.

2. في مجال التشريعات والأنظمة

1. الإسراع بإصدار قانون وطني خاص بمكافحة الجرائم الإلكترونيَّة في الجمهورية اليمنية، يتضمن تعريفًا دقيقًا لهذه الجرائم، وتصنيفها، وتحديد العقوبات المناسبة لها، بما يواكب التطورات الرقمية الحديثة، ويغطي الأشكال المستحدثة من الجريمة.
2. العمل على تحديد عقوبات رادعة تتناسب مع حجم الضرر الناتج عن هذه الجرائم.
3. نشر الوعي القانوني لدى أفراد المجتمع حول حقوقهم وآليات الحماية القانونية المتاحة لهم.
4. تعزيز قدرات الكوادر القضائية والأمنية في التعامل مع الجرائم الإلكترونيَّة، من خلال التدريب المستمر على القوانين الرقمية والوسائل الحديثة للتحقيق والضبط.

3. في مجال الإبلاغ والاستجابة

أظهرت نتائج الدراسة وجود فجوة في فاعليَّة قنوات الإبلاغ وضعف التفاعل المؤسسي مع بلاغات الجرائم الإلكترونيَّة؛ مما يستدعي تبني حزمة من التدخلات العملية. وتوصي الدراسة بما يلي:

1. تحسين الإجراءات المتبعة بعد تلقي البلاغات من خلال تسريع الاستجابة، وتوفير تغذية راجعة واضحة تُمكّن المبلِّغ من معرفة ما تم اتخاذه من خطوات.
2. تصميم نظام إلكتروني أو تقني يُتيح للضحايا تتبع بلاغاتهم بسهولة، سواء عبر تطبيقات أو رسائل نصية، لضمان الشفافية والمتابعة المستمرة.
3. تدريب الكوادر الأمنية المسؤولة عن استقبال البلاغات والتحقيق فيها على مهارات التواصل، والتعاطف، والتقدير النفسي لحالة الضحية، بما يُسهم في تعزيز شعور الأمان والدعم لديهم.
4. تفعيل خدمات الدعم النفسي والاجتماعي للضحايا عبر منصات إلكترونيَّة سرِّية وآمنة، تُشرف عليها جهات مختصة، وتقدّم استشارات فورية وآمنة للمتضررين.

4. في مجال الأسرة والاستخدام الشخصي

1. رفع وعي أولياء الأمور بأهمية الرقابة الأبوية على استخدام الأبناء للإنترنت، وأثر الإهمال في تعريضهم للمخاطر.
2. تقديم دورات تدريبية للأسر حول كيفية استخدام برامج الحماية وتفعيل أدوات الرقابة الرقمية.
3. تشجيع الأفراد على اتباع ممارسات حماية أساسية؛ مثل: كلمات المرور القوية، والتحقق الثنائي، وعدم مشاركة المعلومات مع مصادر غير موثوقة.

5. في مجال البحث العلمي

1. دعم الدراسات الميدانية المتخصصة في الجرائم الإلكترونيَّة على مستوى حضرموت واليمن عامةً، بهدف بناء قاعدة معرفية محلية.

2. إنشاء قاعدة بيانات وطنية لرصد أنماط الجرائم الإلكترونيَّة وتطوراتها لتكون مرجعًا للباحثين وصناع القرار.

سادسًا: في مجال التقنية والجاهزية الرقمية

1. تطوير البنية التحتية الرقمية للأمن السيبراني محليًّا، من خلال دعم أنظمة الكشف المبكر عن التهديدات وتحليلها.
2. تعزيز استخدام أدوات الذكاء الاصطناعي في تتبع الجرائم الإلكترونيَّة والتنبؤ بها.
3. بناء شراكات مع المنصات التقنية لتوفير حلول محدثة وفعَّالة تساعد في الوقاية والرصد المبكر للهجمات السيبرانية.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس لديه أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن المؤلف بأن البحث المنشور لم يتلقَ أي منحة ماليَّة، من أي جهة تمويل في القطاعات الحكوميَّة، أو التجاريَّة، أو المؤسسات غير الربحية.

المراجع

المراجع العربية

جامعة الدول العربية. (2010). الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. القاهرة.

خالد، رفيف طلال. (2024). فاعلية القانون الدولي الإنساني في تنظيم الحرب السيبرانية. مجلة قلم، 8(16)، 87-104.

الخالدي، خزيم. حماد، لجين. العمري، نسرين. البدارنة، حنين. ياسين، عرين. صبح، زين. (2023). دور الأمن العام في مكافحة الجرائم الإلكترونيَّة عبر شبكات التواصل الاجتماعي. مجلة قاف للدراسات الإعلامية والسياسية، 2(2)، 116-135. http://dx.doi.org/10.58596/qaafe/23

ابن داود، ندى منصور. محمد، الفيصل عبد الحميد. جراد، فايز علي. (2024). مخاطر خدمات الدفع الإلكتروني وعلاقتها بحدوث الجرائم الإلكترونيَّة. مجلة إدارة المخاطر والأزمات، 5(3)، 1-26. https://doi.org/10.26389/AJSRP.D190824

دورماز، ميتيهان. (2024). اتفاقية الأمم المتحدة الجديدة لمكافحة الجرائم الإلكترونيَّة: الأهداف والثغرات. منصة دعم السلامة الرقمية (smex), تم الاسترجاع في 3 أغسطس، 2025، من: https://smex.org/ar/%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9-%D8%A7%D9%84%D8%A3%D9%85%D9%85-%D8%A7%D9%84%D8%AA%D8%AD%D8%AF%D8%A9-%D8%A7%D9%84%D8%AC%D8%AF%D9%8A%D8%AF%D8%A9-%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD/

أبو دية، عبير مجلّي، وعبد الله، أسامة محمد. (2018). الجرائم الإلكترونيَّة: دراسة نظرية، الملتقى الخامس للرابطة العربية للبحث العلمي وعلوم الاتصال، بيروت، لبنان.

الرشيدي، عيده سليمان، والمهداوي، عبد الله محمد. (2023). مستوى الوعي بنظام مكافحة الجرائم المعلوماتية لدى طلاب الجامعة. المجلة العربية للدراسات الأمنية، 39(1)، 51-63.

الزبن، غدير برنس، والخرابشة، عبد الكريم عوده الله. (2021). الجرائم الإلكترونيَّة ومستوى الوعي بخطورتها. مجلة الجامعة الإسلامية للدراسات الإنسانية، 29(2)، 230-248. https://doi.org/10.33976/IUGJHR.29.2/2021/11

سعدون، طالب عبد شاطي، وعجيل، وسام عبد الحسن. (2024). التحليل الجغرافي للخصائص الاقتصادية والاجتماعية لمرتكبي الجرائم الإلكترونيَّة في محافظة واسط. مجلة كلية التربية، 56(2)، 335-356. http://dx.doi.org/10.31185/eduj.Vol56.Iss2.3983

الشوابكة، عُدي محمد علي. (2022). معوقات مكافحة الجرائم الإلكترونيَّة في المجتمع الأردني من وجهة نظر ذوي الاختصاص. المجلة العربية للنشر العلمي، 43، 331-356.

العجمي، محمد منيف. (2024). الجرائم الإلكترونيَّة الممارسة ضد المرأة الكويتية وآليات الحد منها: دراسة ميدانية. مجلة دراسات الخليج والجزيرة العربية، 50(193)، 121-163. https://doi.org/10.34120/jgaps.v50i193.311

العقيل، صالح بن عبد الله. (2022). الوعي الاجتماعي والجرائم الإلكترونيَّة. دراسة ميدانية على عينة من الأفراد بمدينة بريدة في منطقة القصيم مجلة العلوم الإنسانية والإدارية، 26(1)، 44-68. http://dx.doi.org/10.56760/IIXE1072

العنوز، سوزان محمد صالح. (2024). دور الأمن السيبراني في التقليل من أعداد الجرائم الإلكترونيَّة في محافظة العقبة باستخدام نظم المعلومات الجغرافية. مجلة العلوم الإنسانية والاجتماعية، 8(8)، 14-29. https://doi.org/10.26389/AJSRP.C180524

العيدروس، نزيهة محمد علي. (2024). تعزيز الوعي بالخصوصية الرقمية في عصر الشبكات الاجتماعية: دراسة ميدانية على طلاب كلية الحاسبات وتقنية المعلومات بجامعة حضرموت. مجلة الريان للعلوم التطبيقية، 7(13)، 185-218.

القحطاني، اللولو علي. المطيري، شقحاء محمد. الجهني، أماني صالح. (2024). دور الإعلام الرقمي السعودي في توعية المواطنين بتقنيات الجرائم الإلكترونيَّة في المملكة العربية السعودية. مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع، 104، 283-327. https://doi.org/10.33193/JALHSS.104.2024.1085

مكتب الأمم المتحدة المعني بالمخدرات والجريمة. (2013). دراسة شاملة عن الجريمة السيبرانية (مسودة). الأمم المتحدة، فيينا.

مهدي، لبنى. (2022). الجرائم الإلكترونيَّة.. أركانها وأسبابها ودوافع ارتكابها. دراسات شرطية، القيادة العامة لشرطة رأس الخيمة، تم الاسترجاع في 3 أغسطس، 2025، من:

النعامي، فهمي محمد أحمد. (2023). دور إدارات العلاقات العامة والإعلام في توعية الجمهور بمخاطر الجريمة الإلكترونيَّة. مجلة جامعة صنعاء للعلوم الإنسانية، 3(1)، 361-396.

المراجع الأجنبية

Al-Baddai, Nasser Ali. (2023). Psychological and Social Effects of Electronic Extortion of Women in the Yemeni Society. University of Science and Technology Journal for Management and Human Sciences, 1(3), 39-61. https://doi.org/10.59222/ustjmhs.1.3.3

Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Budapest.

International Organization for Standardization. (2023). ISO/IEC 27032:2023 - Cybersecurity - Guidelines for Internet security. https://www.iso.org/standard/76070.html

International Organization for Standardization. (2022). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements. https://www.iso.org/standard/27001

United Nations General Assembly. (2024). Resolution adopted on the Global Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.