استخدام الجمهور اليمني للإنترنت وعلاقته بمستوى وعيهم بمخاطر الجريمة الإلكترونية: دراسة مسحية

فهمي محمد أحمد النعامي/ جامعة صنعاء اليمن fahmijtr3@gmail.com

تاريخ الارسال: 2023/2/18 **تاريخ التقييم**:2023/3/14 **تاريخ النشر** 2023/4/24

ملخص الدراسة

هدفت الدراسة إلى التعرف على مستوى وعي الجمهور اليمني بمخاطر الجريمة الإلكترونية، وذلك من خلال منهج المسح بالتطبيق على عينة عشوائية بلغت 400 مفردة من مستخدمي الإنترنت.
وقد توصلت الدراسة إلى زيادة حجم استخدام المبحوثين للإنترنت، وجاءت (مواقع الإنترنت ومواقع التواصل الاجتماعي) أهم المصادر التي يعتمد عليها المبحوثون في معرفتهم بالجريمة الإلكترونية، كما توصلت إلى أن ما يقارب من نصف عينة الدراسة قد تعرضوا لنوع واحد على الأقل من الجرائم الإلكترونية، كما أشارت إلى المعرفة الجيدة للمبحوثين بأساليب ارتكاب الجرائم الإلكترونية، وبالمقابل وجدت الدراسة ضعف في وعي المبحوثين بطرق الوقاية من الجريمة الإلكترونية، كما توصلت الدراسة إلى عدم وجود علاقة ارتباط ذات دلالة إحصائية بين معدل استخدام الجمهور اليمني للإنترنت ودرجة وعيهم بمفهوم الجريمة وأساليبها، بينما وجدت علاقة ارتباط ذات دلالة إحصائية بين معدل استخدام الجمهور اليمني للإنترنت ودرجة الوعي بطرق الوقاية من الجريمة الإلكترونية .

الكلمات المفتاحية: الإنترنت، الجريمة الإلكترونية، الوعي بالجرائم الإلكترونية

The Yemeni public's use of the Internet and its relationship to their level of awareness of the dangers of cybercrime - a survey study

Fahmi Mohammed Al-Naami

Abstract

The study aimed to identify the Yemeni public's level of awareness of the dangers of cybercrime, through a survey method applied to a random sample of 400 internet users.

The study found an increase in the respondents' use of the Internet, and (Internet sites and social networking sites) were the most important sources on which the respondents relied in their knowledge of cybercrime. It also concluded that nearly half of the study sample had been exposed to at least one type of cybercrime. It indicated that the respondents had good knowledge of the methods of committing cybercrime, and in contrast, the study found a weakness in the respondents' awareness of the methods of preventing cybercrime.

The study also found that there was no statistically significant correlation between the rate of the Yemeni public's use of the Internet and the degree of their awareness of the concept and methods of crime, while it found a statistically significant correlation between the rate of the Yemeni public's use of the Internet and the degree of awareness of ways to prevent cybercrime.

Keywords: Internet, cybercrime, awareness of cybercrimes

مقدمة:

أدى الاستخدام المتزايد للإنترنت ووسائل الإعلام الجديد إلى الكثير من المخاطر، وظهرت الجرائم الإلكترونية التي أصبحت ترتكب من خلال الإنترنت ومواقع التواصل الاجتماعي، وقد ترافق تزايد معدل ارتكاب الجرائم الإلكترونية على مستوى دول العالم في العقدين الأخيرين على وجه الخصوص والتي تعددت صورها وأشكالها، مع استنفار الكثير من الدول من ناحية تشريع قوانين خاصة بمكافحة هذه النوع من الجرائم واستحداثها إدارات أمنية خاصة بمكافحتها بالإضافة إلى جهود التوعية والتثقيف بمخاطر الجريمة الإلكترونية.

ويستوجب الأمر تكامل جهود المؤسسات الوطنية ذات العلاقة مع المؤسسات الأمنية والمجتمع من أجل وضع استراتيجيات إعلامية متكاملة للتوعية بمخاطر الجرائم الإلكترونية وطرق تجنبها والوقاية منها.

مشكلة الدراسة:

أصبحت الجريمة الإلكترونية في اليمن تشكل ظاهرة لها انعكاسات سلبية على أمن الأفراد واستقرار المجتمع، في ظل غياب التشريعات والقوانين المحلية المتعلقة بمكافحة الجريمة الإلكترونية، وفي ظل غياب برامج التوعية بمخاطرها، المترافق مع ندرة الدراسات المحلية التي تناولت هذه الظاهرة، وفي إحصائية شاملة للجرائم الإلكترونية المضبوطة بلغ إجمالي القضايا للجرائم الإلكترونية التي تم العمل عليها لدى الجهات ذات العلاقة خلال الأعوام 2015-2021م عدد (10.667) جريمة إلكترونية (سراج والعبالي، 2022، 16)، وهي لا تعادل 7% من حجم الجرائم الإلكترونية الفعلية الواقعة على الأفراد والمؤسسات، نظراً لإحجام الكثير من الأفراد والمؤسسات عن التقدم بالإبلاغ للخشية من الفضيحة أو لعدم الثقة في قدرة الأجهزة الأمنية على ضبط الجناة، وعليه تتبلور مشكلة الدراسة في الكشف عن استخدام الجمهور اليمني للإنترنت وعلاقته بمستوى وعيهم بمخاطر الجريمة الإلكترونية .

أهمية الدراسة:

1- أهمية معرفة واقع الجريمة الإلكترونية في اليمن في ظل ندرة الأبحاث المحلية التي تناولت هذا الشأن؛ الأمر الذي يحتم إجراء هذه الدراسة.

2- تأتي أهمية هذه الدراسة المنهجية، من أنها من الدراسات البينية لكل من الإعلام والحاسوب وعلوم الاجتماع والأمن والقانون، وعدد من الدراسات أُجريت من قبل باحثين اجتماعيين أو أمنيين خارج القطر اليمني، فاختلفت بالتالي المفاهيم وأساليب القياس واختيار العينات وكيفية أو طبيعة تناول الموضوع، ويُعتبر هذا الاختلاف مبرراً أساسياً لإجراء الدراسة الحالية.

أهداف الدراسة:

1- التعرف على مصادر معرفة المبحوثين بالجريمة الإلكترونية.
2- الكشف عن معدل تعرض المبحوثين للجريمة الإلكترونية.
3- معرفة نوع الجرائم الإلكترونية التي تعرض لها المبحوثون.
4- التعرف على مواقع الإنترنت التي تعرض من خلالها المبحوثون للجريمة الإلكترونية.
5- معرفة مستوى وعي المبحوثين بالجريمة الإلكترونية وطرق الوقاية منها.

الدراسات السابقة:

أظهرت معظم الدراسات السابقة التي تناولت استخدام الإنترنت وعلاقته بالجريمة الإلكترونية أهمية بالغة بجهود التوعية والتثقيف بمخاطر الجرائم الإلكترونية والتعريف بطرق الوقاية منها تلافياً للآثار السلبية على الفرد والمجتمع، ففي دراسة أجريت على المجتمع الأردني توصل الباحثان (الزبن والخرابشة، 2021) إلى انخفاض معدل تعرض المبحوثين للجرائم الإلكترونية، وأن مستوى الوعي بالجرائم الإلكترونية كان مرتفعاً بين عينة الدراسة، ولعل هذه النتيجة ترجع إلى الدور التوعوي السابق لشعبة البحث الجنائي لمديرية الأمن العام في الأردن في مجال التوعية الأمنية على موقع الفيسبوك.

فيما كشفت دراسة (الحزورة وحيدر، 2020م، ص ص 97- 129) عن وجود ارتباط طردي بين معدل استخدام الشباب الإنترنت ومستوى وعيهم بالشائعات الإلكترونية حول مجريات الأحداث والصراع في اليمن، وكذلك وجود ارتباط طردي بين مستوى التفكير النقدي للشائعات لدى المبحوثين ومستوى وعيهم بالشائعات، كما أكدت على أن الإنترنت وتطبيقاتها المختلفة عملت على نشر الشائعات لدى أفراد العينة، لأنها أصبحت المصدر الأسرع والمتاح بالنسبة لهم في نقل الأحداث خاصةً في أوقات الأزمات.

فيما توصلت نتائج دراسة (الدحلة، 2018) إلى أن صفحة مكافحة الجرائم الإلكترونية ركزت على التعليمات الإرشادية بنسبة (30,94%) معتمدة على المحتوى البصري في إيصال المعلومات، وأوصت بضرورة إبراز العقوبات المفروضة على الجرائم الإلكترونية في وسائل الإعلام بحيث تكون رادعاً للجمهور لتجنب ارتكابها، فيما كانت دراسة (أفروزولاخان، 2018) التي استهدفت معرفة درجة الوعي بالجريمة الإلكترونية بين طلاب كلية العمل الاجتماعي بمدينة بانجلور الهندية قد أظهرت أن (58%) من المبحوثين ليسوا على دراية بالجرائم الإلكترونية، إلى جانب أن أغلب مستخدمي مواقع التواصل الاجتماعي والإنترنت في الهند يجهلون كيفية الإبلاغ عن الجرائم الإلكترونية.

أما دراسة (ستيفن أوتر وآخرون، 2015) التي استهدفت معرفة واقع الجريمة الإلكترونية وواجبات الشرطة البريطانية حيالها، فقد توصلت إلى أن ضحايا الجرائم الإلكترونية لم يكونوا على دراية بالتهديد الذي تشكله الجرائم الإلكترونية عليهم، وقد أظهر الضحايا في الدراسة تردداً في إبلاغ جهاز الشرطة بالجرائم التي تعرضوا لها، وخلصت الدراسة إلى أهمية برامج التوعية والتثقيف بمخاطر الجريمة الإلكترونية وطرق التعامل معها لدى رجال الشرطة ولدى الضحايا.

أوجه الاستفادة من الدراسات السابقة:

1- الاستفادة في تحديد وتوصيف المشكلة البحثية، وفي وضع أهداف الدراسة وفي صياغة التساؤلات والفروض العلمية والإفادة في تحديد مصطلحات الدراسة.
2- اعتماد الدراسة على المنهج المسحي باستخدام استبيان كأداة رئيسية لجمع بيانات ومعلومات الدراسة مثل دراسة (الزبن والخرابشة 2021) ودراسة (الحزورة وحيدر، 2020م) ساعدت على تحديد المواقف والتقييم، وتعميق فهم الباحث لظاهرة الجرائم الإلكترونية، وبطبيعة وأهمية أدوار وسائل الإعلام في بث الوعي والتثقيف بخطورة الجرائم الإلكترونية.
3- استفادت الدراسة الحالية من الدراسات السابقة في التعرف على أساليب قياس وعي الجمهور بالجريمة الإلكترونية مثل دراسة (الحزورة وحيدر، 2020م) التي استهدفت

التعرف على أساليب قياس الوعي بمفهوم الشائعات وكيفية إدراك الجمهور للشائعات الإلكترونية، إلا أن الدراسة الحالية ركزت على دراسة مستوى وعي الجمهور اليمني بالجريمة الإلكترونية من خلال مقياس ثلاثي: (الوعي بمفهوم الجريمة الإلكترونية – الوعي بأساليب الجريمة الإلكترونية – الوعي بطرق الوقاية من الجريمة الإلكترونية).

تساؤلات الدراسة:

1- ما معدل استخدام الجمهور اليمني للإنترنت بشكل عام؟
2- ما هي أهم مصادر معرفة المبحوثين بالجرائم الإلكترونية؟
3- ما هي نسبة وقوع المبحوثين ضحايا لإحدى الجرائم الإلكترونية؟
4- ما نوع الجرائم الإلكترونية التي تعرض لها المبحوثون؟
5- ما المواقع بالإنترنت التي استخدمها المبحوثون وجعلتهم يتعرضون للجريمة الإلكترونية؟
6- ما مستوى وعي المبحوثين بالجرائم الإلكترونية، من حيث:
   أ- مفهوم الجريمة الإلكترونية.
   ب- أساليب الجريمة الإلكترونية.
   ت- طرق الوقاية من الجرائم الإلكترونية.

فروض الدراسة:

1- توجد علاقة ارتباط دالة إحصائياً بين معدل استخدام الجمهور اليمني للإنترنت، ودرجة وعيهم بالجريمة الإلكترونية بمستوياتها الثلاثة (مفهوم الجريمة الإلكترونية، وأساليب الجريمة الإلكترونية، وطرق الوقاية من الجريمة الإلكترونية).
2- توجد علاقة ارتباط دالة إحصائياً بين حجم استخدام الجمهور اليمني للإنترنت، وتأثيرات اعتمادهم على الإنترنت من ناحية معرفتهم بمخاطر الجريمة الإلكترونية.

التعريفات الإجرائية لمصطلحات الدراسة:

يقصد بالإنترنت في الدراسة الحالية: هو شبكة اتصالات إلكترونية تربط بين شبكات الكمبيوتر، وتربط بين ملايين الحواسيب حول العالم، وتتكون من ملايين الشبكات المنزلية، والأكاديمية،

والتجارية، والحكومية الصغيرة، ويقدم الإنترنت خدماته الفورية في التواصل المتجاوز لحدود الزمان والمكان مثل البريد الإلكتروني ومواقع التواصل الاجتماعي، والتي أصبحت أدوات بيد المجرمين الإلكترونيين سواء من داخل القطر اليمني أو من دولة أخرى لتنفيذ جرائمهم الإلكترونية، والذي يسهل عملهم التطورات الهائلة في تكنولوجيا الاتصالات والمعلومات بالإضافة إلى ضعف برامج التوعية والتثقيف بمخاطر الجرائم الإلكترونية وطرق الوقاية منها، إضافة إلى ضعف التشريعات والقوانين الوطنية الرادعة لمثل هذا النوع من الجرائم المستحدثة .

يقصد بالوعي في الدراسة الحالية: هو المعرفة التي يكتسبها الجمهور اليمني المستخدم للإنترنت، من المصادر الإعلامية التقليدية والجديدة المختلفة، والتي يترتب عليها معرفته بمخاطر التحديات التكنولوجية المعاصرة المتمثلة بالجرائم الإلكترونية، وينعكس عليه سلوكاً من ناحية معرفة مخاطرها وتجنب الوقوع فيها وطرق التعامل السليم معها حال حدوثها، وتساهم الجهود المنظمة والاحترافية للجهات المسئولة عن الجرائم الإلكترونية في أعمال التوعية والتثقيف بمخاطر الجرائم الإلكترونية في حماية المواطنين والمنظمات والمؤسسات ضد التهديدات التي تواجه سلامتهم ورفاهية مجتمعهم .

يقصد بالجريمة الإلكترونية في الدراسة الحالية: هي الجريمة التي يمكن أن يرتكبها شخص ما، باستخدام جهاز حاسوب أو هاتف محمول ذكي أو الأجهزة اللوحية، وتتم من خلال الاتصال بشبكة الإنترنت من خلال البريد الإلكتروني أو مواقع في الإنترنت أو عبر مواقع التواصل الاجتماعي، ويكون هدفه إلحاق الضرر بالمجني عليه سواء في ماله أو سمعته أو حالته النفسية والعقلية أو مكانته أو شرفه، ويشترط على مرتكب الجريمة الإلكترونية توفره على حاسب آلي أو هاتف محمول ذكي وشبكة إنترنت وتقنيات استعمالها، ويتميز مُرتكِب هذا النوع من الجرائم بالذكاء وعدة خصائص تمكنه من ارتكاب الجريمة.

منهج الدراسة:

تنتمي هذه الدراسة للبحوث الوصفية التي تعتمد على منهج المسح، حيث تم جمع البيانات باستخدام استبيان أُعد لمعرفة طبيعة استخدام الجمهور اليمني للإنترنت وعلاقته بمستوى وعيه بالجريمة الإلكترونية.

مجتمع وعينة الدراسة:

يتحدد مجتمع الدراسة المسحية في الجمهور اليمني من مستخدمي الإنترنت، والذين لا تقل أعمارهم عن ثماني عشرة سنة المتواجدين داخل العاصمة صنعاء، وقد تم اختيار العاصمة صنعاء لتطبيق الدراسة لاحتوائها على مختلف الخصائص الديموغرافية والثقافية والاجتماعية التي تتطلبها الدراسة، وقد تم اختيار العينة باستخدام العينة العشوائية البسيطة حيث بلغت 400 مفردة، (204 من الذكور و196 من الإناث).

أدوات جمع البيانات:

اعتمدت هذه الدراسة على أداة استبيان تم توزيعه يدوياً وإلكترونياً على عينة الدراسة، خلال الفترة 15 يوليو 2022م وحتى 31 أكتوبر 2022م، والذي تضمن عدداً من المحاور التي تحقق أهداف الدراسة وتجيب عن تساؤلاتها وفروضها.

إجراءات الصدق والثبات:

الصدق: تم الاعتماد على صدق المحتوى، أو ما يسمى بالصدق الظاهري في التأكد من صدق أداة الدراسة وبأنها تقيس ما صممت فعلاً لقياسه، حيث تم عرض الاستمارة مع الأهداف

والتساؤلات والفروض على مجموعة من المحكمين[1]، وتم الأخذ بآرائهم وتعديل صياغة العبارات التي اتفق المحكمون عليها.

الثبات: للتحقق من ثبات أداة الدراسة، تم استخدم أسلوب إعادة الاختبارTest-Retest على عينة عشوائية مقدارها 10% من إجمالي حجم العينة الأصلية، حيث قام الباحث بتطبيق الاستمارة على عدد (40) شخصاً من مستخدمي الإنترنت بأمانة العاصمة، ثم تم اعادة تطبيق الاستمارة على تلك المجموعة نفسها وذلك بعد مرور أسبوعين من تطبيق الاختبار الأول، وقد بلغت قيمة معامل الثبات (0.88) وهي قيمة عالية تشير إلى ثبات المقياس ودقته.

تقييم وضع أمن المعلومات الإلكتروني في اليمن:

على الرغم من التطور الذي شهدته اليمن في مجال الاتصالات وتقنية المعلومات وإدخال خدمة الإنترنت في وقت مبكر عام 1996م، إلا أن مجال أمن المعلومات الإلكتروني في اليمن لم يحظ بالاهتمام اللائق من مختلف القطاعات (الحكومية والخاصة والمجتمع المدني) والذي انعكس على

(1) السادة المحكمون، هم:

أ. د/ علي العمار- أستاذ الصحافة بكلية الإعلام – جامعة صنعاء.

أ. م. د/ علي البريهي – أستاذ الإذاعة والتلفزيون المشارك بكلية الإعلام – جامعة صنعاء.

د/ حسين جغمان – رئيس قسم الإذاعة والتلفزيون الأستاذ المساعد بكلية الإعلام – جامعة صنعاء.

د/ مهدي حيدر – رئيس قسم العلاقات العامة الأستاذ المساعد بكلية الإعلام – جامعة صنعاء.

د/ نوال الحزورة – أستاذة الإذاعة والتلفزيون المساعدة بكلية الإعلام – جامعة صنعاء.

د/ هزاع شرف – أستاذ العلاقات العامة المساعد بكلية الإعلام – جامعة صنعاء.

د/ يوسف سلمان – رئيس قسم العلوم الاجتماعية والإعلام الأستاذ المساعد جامعة العلوم والتكنولوجيا.

د/ إسماعيل حميد – أستاذ علوم الحاسوب المساعد بكلية الحاسبات جامعة العلوم والتكنولوجيا.

أ م. د/ نديم الترزي - نائب رئيس أكاديمية الشرطة للشئون التعليمية، أستاذ القانون الجنائي المشارك.

هشاشة أمن المعلومات الأمر الذي جعل البلاد هدفاً للجرائم الالكترونية بمختلف أشكالها ومصادرها.

وقد بلغ عدد مستخدمي الإنترنت في اليمن في شهر يناير 2021م حوالي 8,06 مليون مستخدم (ذمران، 2021، ص ص 1-2) ، وقد حصلت اليمن في العام 2018م على تقييم دولي متدنٍ في الأمن الإلكتروني حيث جاءت في الترتيب 172 من جملة 175 بلداً على مستوى دول العالم في مستوى الأمن الإلكتروني ، بحسب تقرير الدليل العالمي للأمن السيبراني للاتحاد الدولي للاتصالات (ITU) عام 2018م، كما تعتبر اليمن من بين أكثر 10 دول عالمياً من حيث مشاركة البرمجيات الضارة (الوصابي، 2021، ص9) ، ويرجع ضعف البنية المعلوماتية الاتصالية في اليمن وهشاشتها بدرجة أساسية إلى غياب التشريعات والقوانين المعززة للأمن الإلكتروني، خاصة في مجال مكافحة الجريمة الإلكترونية، إلى جانب غياب البرامج التوعوية والتثقيفية بمفهومها ومخاطرها، كما أن غياب برامج التوعية والتثقيف بمخاطر الجريمة الإلكترونية للجهات ذات العلاقة قد أثر أيضاً على ضعف الوعي لدى صانعي القرار السياسي والتشريعي بأهمية إقرار وإنفاذ قانون يعنى بمكافحة الجريمة الإلكترونية، حيث أن قانون مكافحة الجرائم الإلكترونية ما زال يراوح مكانه في أدراج بيروقراطية مجلس النواب اليمني منذ أواخر العام 2020م، والذي لم يقر حتى وقت إعداد هذه الدراسة.

وقد بلغ عدد الجرائم الإلكترونية المبلغ عنها بالبحث الجنائي في نطاق أمانة العاصمة صنعاء خلال عامين من تاريخ 1سبتمبر2018م حتى 1سبتمبر 2020م أكثر من (500) جريمة إلكترونية، وهي تعد نسبة بسيطة من حجم الجرائم الإلكترونية الفعلية الواقعة على الأفراد والمؤسسات (سراج، أحمد. 2021، ص ص 16-17)، نظراً لإحجام الكثير من الأفراد والمؤسسات عن التقدم بالإبلاغ لخشيتهم من الفضيحة أو لعدم ثقتهم في قدرة الأجهزة الأمنية على ضبط الجناة.

النتائج العامة للدراسة

أولاً: النتائج العامة للدراسة المسحية:

أظهرت النتائج زيادة استخدام المبحوثين للإنترنت، حيث جاء في المرتبة الأولى الاستخدام الكثيف للجمهور عينة الدراسة (أربع ساعات فأكثر) بنسبة (35.5%) من إجمالي عينة الدراسة، وجاء في المرتبة الثانية الاستخدام المتوسط من (ساعتين إلى أقل من أربع ساعات) بنسبة (35%)، تلاه الاستخدام (أقل من ساعتين) بنسبة (29.5%)، وتعكس النتائج السابقة زيادة اعتماد المبحوثين على الإنترنت كوسيلة اتصال رقمي أحدث تحولات كبيرة في المجتمع اليمني، ويعتبر الباحث أن الإنترنت أصبح يمثل قدرة الأفراد لصناعة المحتوى الشخصي والمؤسسي بعيداً عن (مقص الرقيب)، والذي انعكس على زيادة معدل الاستخدام اليومي للإنترنت، الأمر الذي يجعل الجمهور اليمني عرضة لكل تأثيرات هذه الوسيلة، بما في ذلك التأثيرات السلبية ومنها إمكانية تعرضهم للجرائم الإلكترونية .

أما فيما يتعلق بأهم المصادر التي يعتمد المبحوثون عليها في معرفتهم بالجريمة الإلكترونية، فقد أظهرت النتائج اعتماد الجمهور اليمني على (مواقع الإنترنت ومواقع التواصل الاجتماعي) التي جاءت في الترتيب الأول، فيما جاء (الأصدقاء) في الترتيب الثاني، وحل (أفراد الأسرة) في الترتيب الثالث، فيما جاء (التلفزيون) في الترتيب الرابع تلاه (الورش والمؤتمرات والندوات) في الترتيب الخامس أما (الإذاعة) فقد احتلت الترتيب السادس وأخيراً جاءت (الصحف) و(المجلات) في ترتيب متأخر.

ويعتبر الباحث أن هذه النتيجة تلفت الانتباه من ناحية تقدم (الأصدقاء والأسرة) على (الإذاعة والصحف والتلفزيون) في الترتيب كمصادر معرفة بالجريمة الإلكترونية ومخاطرها، الأمر الذي يشير بوضوح إلى ضعف الأجهزة الرسمية في توعية الجمهور اليمني بمخاطر الجريمة الإلكترونية وطرق

الوقاية منها، الأمر الذي يعرض مستخدمي الإنترنت في اليمن إلى تبعات مخاطرها السلبية على الأفراد والأسرة والمجتمع.

كما توصلت النتائج إلى تعرض (47%) من المبحوثين لنوع واحد على الأقل من الجرائم الإلكترونية، ويعتبر الباحث أن ارتفاع نسبة تعرض الجمهور للجريمة الإلكترونية مؤشر خطير يدل على تفاقم الجريمة الإلكترونية في اليمن بحيث أصبحت تشكل ظاهرة لها دلالاتها وانعكاساتها السلبية على الأفراد والمجتمع اليمني، وعلى الاقتصاد والتنمية في بلد يعاني أصلاً من شح الإمكانات والموارد المحدودة التي تضاف إلى الأوضاع الصعبة التي يعيشها اليمنيون.

جدول رقم (1) يبين توزيع المبحوثين طبقاً لنوع الجريمة التي تعرضوا لها

	درجة الموافقة	نعم				لا				الترتيب
		التكرار		النسبة		التكرار		النسبة		
	نوع الجريمة	ذكور	إناث	ذكور	إناث	ذكور	إناث	ذكور	إناث	
1	تلقي رسائل إباحية	60	48	31.9	25.5	45	35	23.9	18.6	الأول
2	تعطيل النظام المعلوماتي للجهاز بالبرامج الضارة	34	22	18.1	11.7	71	61	37.8	32.4	الثاني
3	سب وقذف وتهديد من خلال النت	32	24	17	12.8	73	59	38.8	31.4	الثاني
4	انتحال الشخصية على الإنترنت	28	25	15	13.2	77	58	41	30.9	الثالث
5	سرقة حساب الفيسبوك	29	16	15.4	8.5	75	68	39.9	36.2	الرابع
6	سرقة حساب الواتس	19	20	10.1	10.6	86	63	45.7	33.5	الخامس
7	احتيال مالي إلكتروني	12	10	6.4	5.3	92	73	48.9	38.8	السادس
8	ابتزاز وتهديد بنشر مقاطع مصورة بالجهاز	5	12	2.6	6.4	99	72	52.7	38.3	السابع
9	استغلال جنسي	6	6	3.2	3.2	99	77	52.7	41	الثامن

يحتوي الجدول السابق إحصائية بأنواع الجرائم الإلكترونية التي تعرض لها الجمهور عينة الدراسة، حيث أفاد الكثير منهم بالتعرض إلى عدة أنواع من الجرائم الإلكترونية، حيث جاء في مقدمة تلك

الجرائم (تلقي رسائل إباحية) بنسبة بلغت (57.4%)، موزعة بين (31.9%) ذكور في مقابل (25.5%) من الإناث.

تلاها في الترتيب الثاني كلاً من الجريمتين (تعطيل النظام المعلوماتي للجهاز بالبرامج الضارة) و(السب والقذف والتهديد من خلال النت) حيث جاءت كلتا العبارتين بنفس النسبة (29.8%) من إجمالي مفردات عينة الدراسة ممن تعرضوا للجرائم الإلكترونية، موزعة بين نسبة (18.1%) من الذكور مقابل (11.7%) من الإناث ممن تعرضن لتلك الجريمة بالنسبة لجريمة تعطيل النظام المعلوماتي بالبرامج الضارة، وما بين نسبة (17%) من الذكور و(12.8%) من الإناث فيما يتعلق بجريمة السب والقذف والتهديد من خلال النت، وجاءت جريمة (انتحال الشخصية على الإنترنت) في الترتيب الثالث بإجمالي نسبة (28.2%) من إجمالي الجمهور عينة الدراسة، موزعة بين نسبة (15%) ذكور بينما جاءت نسبة الإناث (13.2%).

فيما جاءت جريمة (سرقة حساب الفيسبوك) في الترتيب الرابع بنسبة (9.23%)، موزعة بين (15.4%) من إجمالى مفردات عينة الذكور مقابل (8.5%) من إجمالي عينة الإناث، تلاها بالترتيب الخامس (سرقة حساب الواتس آب) والتي جاءت بنسبة (20.7%) من إجمالي مفردات من تعرضوا للجرائم الإلكترونية من المبحوثين، موزعة بين (10.1%) من إجمالي مفردات عينة الذكور في مقابل (10.6%) من مفردات عينة الإناث.

أما جريمة (الاحتيال المالي الإلكتروني) فقد جاءت في الترتيب السادس بنسبة (11.7%)، موزعة بين (6.4%) من إجمالي عينة الذكور في مقابل (5.3%) من إجمالي عينة الإناث، تلاها جريمة (الإبتزاز والتهديد بنشر مقاطع مصورة كانت بالجهاز) في الترتيب السابع بنسبة (9%)، موزعة بين (2.6%) من إجمالي عينة الذكور في مقابل (6.4%) من إجمالي مفردات عينة الإناث،

وجاء في الترتيب الثامن والأخير جريمة (الاستغلال الجنسي) بنسبة (6.4%)، والتي تقاسمها الذكور والإناث من الجمهور عينة الدراسة بنسبة متساوية بلغت (3.2%).

ويعتبر الباحث أن انتشار أنواع الجريمة الإلكترونية في اليمن بالنسب الواردة أعلاه، أمر له انعكاسات سلبية على أمن ورفاه الأفراد والمجتمع اليمني ويستدعي استنفار الجهود الرسمية والشعبية للحد من الظاهرة.

جدول رقم (2) توزيع المبحوثين طبقاً لمواقع بالإنترنت تعرضوا من خلالها للجريمة الإلكترونية

	درجة الموافقة / المواقع أو البرامج	نعم		لا		الترتيب
		التكرار	النسبة	التكرار	النسبة	
1	الواتس آب	99	52.7	89	47.3	الأول
2	الفيسبوك	85	45.2	103	54.8	الثاني
3	غير معروف	31	16.5	157	83.5	الثالث
4	البريد الإلكتروني	26	13.8	162	86.2	الرابع
5	التيليجرام	23	12.2	165	87.8	الخامس
6	غرف الدردشة	23	12.2	165	87.8	الخامس

تكشف بيانات الجدول السابق عن (مواقع الإعلام الرقمي بالإنترنت) التي تعرض المبحوثون من خلالها للجرائم الإلكترونية، حيث جاء في مقدمة تلك المواقع (الواتس آب) بنسبة بلغت (52.7%)، تلاه بالترتيب الثاني (الفيسبوك) بنسبة (45.2%)، وجاء في الترتيب الثالث (المصادر غير المعروفة) بنسبة (16.5%) حيث لم يعلم المبحوثون كيفية الأسلوب الذي اتبعه المجرمون الإلكترونيون للإيقاع بهم كضحايا لهذا النوع من الجرائم.

وجاء بالترتيب الرابع (البريد الإلكتروني) بنسبة (13.8%)، في حين جاء كلا من تطبيقي (التيليجرام) و(مواقع الدردشة) بنفس الترتيب الخامس بنسبة (12.2%) من إجمالي مفردات عينة الدراسة ممن تعرضوا للجرائم الإلكترونية، ويعتبر الباحث ذلك نتيجة طبيعية لعدم قيام الجهات المسئولة عن الجريمة الإلكترونية في القيام بواجباتها في توعية الجمهور اليمني بطرق الوقاية من الجريمة الإلكترونية.

جدول رقم (3) توزيع المبحوثين طبقاً للعبارات المتعلقة بمفهوم الجريمة الالكترونية

	العبارات	المتوسط الحسابي	الانحراف المعياري	الوزن المئوي	الترتيب
1	الابتزاز والتهديد الإلكتروني بالتشهير بنشر مقاطع للضحية	2.82	0.542	%94	الأول
2	سرقة بيانات الحاسوب والهواتف الذكية من خلال الإنترنت	2.81	0.562	%93.6	الثاني
3	التجسس على الحاسوب والهواتف الذكية	2.80	0.565	%93.4	الثالث
4	الاحتيال المالي الإلكتروني	2.76	0.604	%91.9	الرابع
5	استغلال الأطفال جنسياً بالإنترنت	2.75	0.633	%91.5	الخامس
6	استغلال المنظمات الإرهابية للإنترنت في التمويل لتجنيد إرهابيين	2.75	0.617	%91.5	الخامس
7	الانتحال الإلكتروني للشخصية	2.74	0.631	%91.4	السادس
8	جرائم التهديد من خلال الإنترنت	2.73	0.647	%91	السابع
9	سحب بيانات الأجهزة الإلكترونية بالوصلات السلكية بدون الإذن من أصحابها	2.73	0.635	%91	السابع
10	استهداف أمن المعلومات والمرافق والاتصالات في الدولة	2.72	0.647	%90.6	الثامن
11	غسل الأموال وتجارة المخدرات عن طريق الإنترنت	2.70	0.662	%89.8	التاسع
12	جرائم السب والقذف والتهديد بالإنترنت	2.64	0.690	%88.1	العاشر
13	الترويج للمواقع والأفلام الإباحية	2.63	0.694	%87.9	حادي عشر
	المتوسط العام لجميع العبارات	2.73	0.625	%91.2	

توضح بيانات الجدول السابق موافقة أغلب المبحوثين على العبارات المتعلقة بمفاهيم الجريمة الإلكترونية، ويعكس ذلك معرفتهم (الجيدة) بمفاهيمها العامة، حيث جاء الوزن المئوي العام

للعبارات (91.2%) بمتوسط حسابي عام (2.73)، وقد جاءت في المرتبة الأولى عبارة (الإبتزاز والتهديد الإلكتروني بنشر مقاطع مصورة للضحية) بمتوسط حسابي (2.82)، فيما جاءت عبارة (سرقة بيانات الحاسوب والهواتف الذكية من خلال الإنترنت) في المرتبة الثانية بمتوسط حسابي (2.81).

كما جاء في المرتبة الثالثة العبارة (التجسس على الحاسوب والهواتف الذكية) بمتوسط حسابي (2.80)، أما المرتبة الرابعة فحلت عبارة (الاحتيال المالي الإلكتروني) كمفهوم للجريمة الكترونية لدى عينة الدراسة بمتوسط حسابي (2.76)، تلاها في المرتبة الخامسة العبارتين (استغلال الأطفال جنسياً من خلال الإنترنت) و(استغلال المنظمات الإرهابية للإنترنت في التمويل لتجنيد إرهابيين جدد) بمتوسط حسابي (2.75)، ثم في المرتبة السادسة (الانتحال الإلكتروني للشخصية) بمتوسط حسابي (2.74)، وجاء في المرتبة السابعة العبارتين (سحب بيانات الأجهزة الإلكترونية بالوصلات السلكية بدون إذن اصحابها) و(جرائم التهديد من خلال الإنترنت) بمتوسط حسابي (2.73)، تلى ذلك في المرتبة الثامنة عبارة (استهداف أمن المعلومات والمرافق والاتصالات في الدولة) بمتوسط حسابي (2.72)، كما جاءت عبارة (غسل الأموال وتجارة المخدرات عن طريق الإنترنت) في المرتبة التاسعة بمتوسط حسابي (2.70)، وفي المرتبة العاشرة جاءت العبارة (جرائم السب والقذف والتهديد بالإنترنت) بمتوسط حسابي (2.64)، وجاء في المرتبة الحادية عشرة والأخيرة العبارة (الترويج للمواقع والأفلام الإباحية) بمتوسط حسابي (2.63).

يتضح مما سبق أن وعي الجمهور بمفهوم الجريمة الالكترونية جاء جيداً، وهذا ناجم عن انتشار الجريمة الالكترونية في المجتمع اليمني، بحيث أصبح مفهومها معروفاً لدى الجمهور، على الرغم من أن أخبار الجريمة الإلكترونية لا تشكل حالياً أولوية في أجندة أخبار وسائل الإعلام الحديثة والتقليدية في اليمن.

جدول رقم (4) يبين توزيع المبحوثين طبقاً لتوصيفهم لأساليب الجريمة الالكترونية

	الأساليب	المتوسط الحسابي	الانحراف المعياري	الوزن المئوي	الترتيب
1	الاحتفاظ بالصور الشخصية غير المحتشمة في الجهاز يسهل الابتزاز الإلكتروني	2.64	0.687	%88	الأول
2	الاحتفاظ بأرقام الحسابات المصرفية في الجهاز يسهل الاحتيال المالي	2.48	0.772	%82.8	الثاني
3	القيام بالمراسلات المالية من خلال مواقع التواصل الاجتماعي يسهل الاحتيال المالي	2.44	0.786	%81.4	الثالث
4	إقامة صداقة مع غرباء في الإنترنت تسهل الجريمة الإلكترونية	2.35	0.796	%78.4	الرابع
5	فتح مرفقات بريد إلكتروني وارد من مصادر مجهولة المصدر قد يتيح انتقال فيروسات للأجهزة	2.14	0.925	%71.3	الخامس
6	فتح مرفقات بمواقع التواصل الاجتماعي دون التأكد من صحة محتواها يسهل عملية سرقة البيانات	2.11	0.934	%70.4	السادس
7	الدخول في روابط مجهولة بالإنترنت تحت إغراء الفوز بجائزة أو ربح معين من أساليب الجريمة الإلكترونية	2.10	0.935	%70.1	السابع
	المتوسط العام لجميع العبارات	2.32	0.833	%77.5	

تكشف بيانات الجدول السابق معرفة المبحوثين (المتوسطة) بأساليب ارتكاب الجرائم الإلكترونية بوزن مئوي عام (77.5%) وقد جاء ترتيب تلك العبارات على النحو التالي:

جاءت عبارة (الاحتفاظ بالصور الشخصية غير المحتشمة يسهل الابتزاز الإلكتروني) في المرتبة الأولى بمتوسط حسابي (2.64) فيما جاء في المرتبة الثانية عبارة (الاحتفاظ بأرقام الحسابات المصرفية في الجهاز يسهل الاحتيال المالي) بمتوسط حسابي (2.68)، أما في المرتبة الثالثة فقد حلت عبارة (القيام بالمراسلات المالية من خلال مواقع التواصل الاجتماعي) بمتوسط حسابي (2.44)، ويشير هذا إلى أن غالبية الجمهور موافق على هذه العبارة.

أما عبارة (إقامة علاقة صداقة مع غرباء على الإنترنت) في احتلت الترتيب الرابع بمتوسط حسابي (2.35) حلت بعدها عبارة (فتح مرفقات بريد إلكتروني وارد من مصادر مجهولة المصدر) التي حلت خامساً بمتوسط حسابي (2.14).

أما عبارتي (فتح مرفقات بمواقع التواصل الاجتماعي دون التأكد من صحة محتواها) و(الدخول في روابط مجهولة بالإنترنت تحت إغراء الفوز بجائزة أو ربح معين) فقد جاءت في ترتيب متأخر بمتوسطات حسابية المرتبة السادسة بمتوسط حسابي (2.11)، وفي المرتبة السابعة والأخيرة جاءت عبارة (الدخول في روابط مجهولة تحت إغراء الفوز بجائزة أو ربح معين) عبارة بمتوسط حسابي (2.10).

ويعتبر الباحث أن المعرفة المتوسطة للجمهور بأساليب الجريمة الإلكترونية يجعل استخدامهم للإنترنت مجازفة حقيقية بالخصوصية، وبسلامة البيانات والمعلومات التي تحتويها الأجهزة الذكية، الأمر الذي قد يشكل معه ضغطاً على موارد التنمية في بلد يعاني أصلاً من ضعف الاقتصاد.

جدول رقم (5) يبين توزيع المبحوثين طبقاً لمدى وعيهم بطرق الوقاية من الجرائم الالكترونية

	طرق الوقاية	المتوسط الحسابي	الانحراف المعياري	الوزن المئوي	الترتيب
1	التمتع بالحذر أثناء استخدام الإنترنت	2.42	0.758	%80.6	الأول
2	استخدام كلمة سر قوية للجهاز	2.32	0.684	%77.3	الثاني
3	عدم إرسال المعلومات الشخصية أو البيانات الهامةعبر البريد الإلكتروني أو مواقع التواصل	2.315	0.814	%77.2	الثالث
4	عدم فتح رسائل بريدية مجهولة المصدر	2.31	0.854	%76.9	الرابع
5	عدم استقبال ملفات في الشات من أشخاص غير موثوق بهم	2.29	0.865	%76.3	الخامس
6	عدم الاحتفاظ بمعلومات أو بيانات مهمة أو أرقام حسابات مصرفية أو صور خاصة في الجهاز	2.28	0.799	%76	السادس
7	عدم الدخول في مواقع مشبوهة مثل مواقع تعليم التجسس واختراق أجهزة الأفراد	2.35	0.874	%75	السابع
8	تجنب تحميل البرامج المهكرة مجاناً توفيراً للمال	2.21	0.848	%73.8	الثامن
9	الاحتفاظ بالمعلومات الشخصية أو البيانات الهامة أو أرقام الحسابات المصرفية في ذواكر تخزين خارج الجهاز	2.22	0.845	%74	التاسع
10	عدم الاستجابة للرسائل المغرية ورسائل الاستدراج مثل: مبروك	2.18	0.890	%72.6	العاشر

	ربحت جائزة أو ربح				
11	استخدام نظام تشغيل وبرامج مرخصة	2.07	0.850	%72.4	حادي عشر
12	عدم إقامة علاقات صداقة مع غرباء على الإنترنت	2.16	0.849	%72	ثاني عشر
13	الاحتفاظ بالملفات والمواقع على النت بكلمة سر	2.14	0.871	%71.2	ثالث عشر
14	عدم الدخول في روابط مجهولة بالإنترنت ومواقع التواصل الاجتماعي	2.11	0.917	%70.2	رابع عشر
15	عدم فتح مرفقات بمواقع التواصل أو من مصادر غير آمنة دون التأكد من صحة محتواها	2.11	0.887	%70.1	خامس عشر
16	تثقيف النفس بالفيروسات واختراق الأجهزة	2.07	0.832	%68.8	سادس عشر
17	استخدام مكافح فيروسات في الجهاز	2.03	0.854	%67.6	سابع عشر
18	القيام بتحديث نظام التشغيل للجهاز	2.03	0.810	%67.5	ثامن عشر
19	الاحتفاظ بنسخة ورقية للأعمال على الإنترنت	1.84	0.843	%61.4	تاسع عشر
20	القيام بتحديث مكافح الفيروسات بالجهاز باستمرار	1.82	0.845	%60.7	عشرون
21	تغيير كلمة السر بالجهاز بصورة دورية	1.77	0.741	%58.9	واحد وعشرون
	المتوسط العام لجميع العبارات	2.08	0.822	%69.3	

تكشف بيانات الجدول السابق عن (وعي ضعيف) للمبحوثين بالدراسة بطرق الوقاية من الجريمة الإلكترونية، حيث جاء الوزن المئوي العام (69.3%) وجاء ترتيب تلك العبارات كما يلي :

جاء (التمتع بالحذر أثناء استخدام الإنترنت) في المرتبة الأولى بمتوسط حسابي (2.42)، فيما جاءت عبارة (استخدام كلمة سر قوية للجهاز) في المرتبة الثانية بمتوسط حسابي (2.32) وقد لاحظ الباحثان أن أغلب الجمهور اليمني يعتقدون بأن استخدامهم لكلمة سر قد لا تتجاوز ستة أرقام تجعلهم في وقاية من تعرض أجهزتهم للإختراق وأعمال القرصنة ومن المعلوم في الأوساط البرمجية أن كلمة السر القوية للأجهزة تصل إلى ستة عشر رقماً تشتمل على الحروف الأبجدية والرموز، وجاء في المرتبة الثالثة (عدم إرسال معلومات شخصية أو بيانات هامة أو صور خاصة عبر البريد الإلكتروني أو مواقع التواصل) بمتوسط حسابي (2.315)، كما جاء في المرتبة الرابعة عبارة (عدم القيام بفتح رسائل بريدية مجهولة المصدر) بمتوسط حسابي (2.31)، وجاءت العبارة (عدم استقبال ملفات في الشات من أشخاص غير موثوق بهم) في المرتبة الخامسة بمتوسط حسابي (2.29)، ثم عبارة (عدم الاحتفاظ بالمعلومات أو البيانات الهامة أو أرقام الحسابات المصرفية أو

الصور الخاصة في الجهاز) فقد جاءت في المرتبة السادسة بمتوسط حسابي (2.42)، أما عبارة (عدم الدخول في المواقع المشبوهة) فقد جاءت في الترتيب الثامن بمتوسط حسابي (2.28)، بينما جاء في المرتبة السابعة عبارة (عدم الدخول في مواقع مشبوهة مثل مواقع تعليم التجسس واختراق اجهزة الأفراد) بمتوسط حسابي (2.35)، تلا ذلك عبارة (تجنب تحميل البرامج المهكرة مجاناً توفيراً للمال) في المرتبة الثامنة بمتوسط حسابي (2.21)، كما جاء بعد ذلك (الاحتفاظ بالمعلومات الشخصية أو البيانات الهامة أو أرقام الحسابات المصرفية في ذواكر تخزين خارج الجهاز) في المرتبة التاسعة بمتوسط حسابي (2.22)، وجاءت العبارة (عدم الاستجابة للرسائل المغرية ورسائل الاستدراج مثل: مبروك ربحت جائزة أو ربح معين) في المرتبة العاشرة بمتوسط حسابي (2.18)، تلاها في المرتبة الحادية عشرة (استخدام نظام تشغيل وبرامج مرخصة) بمتوسط حسابي (2.07) تلى ذلك في المرتبة الثانية عشرة (عدم إقامة علاقة صداقة مع غرباء على الإنترنت) بمتوسط حسابي (2.16)، بينما جاء (الاحتفاظ بالملفات والمواقع على النت بكلمة سر) في المرتبة الثالثة عشرة بمتوسط حسابي (2.14) وفي المرتبة الرابعة عشرة جاء (عدم الدخول في روابط مجهولة بالإنترنت ومواقع التواصل الاجتماعي) بمتوسط حسابي (2.11)، وفي المرتبة الخامسة عشرة جاء (عدم فتح مرفقات بمواقع التواصل أو من مصادر غير آمنة دون التأكد من صحة محتواها) بمتوسط حسابي (2.11)، كما جاءت عبارة (تثقيف النفس فيما يتعلق بالفيروسات واختراق الأجهزة) في المرتبة السادسة عشرة بمتوسط حسابي (2.07)، ثم جاء في المرتبة السابعة عشرة عبارة (استخدام مكافح فيروسات في الجهاز) بمتوسط حسابي (2.03)، وجاء (القيام بتحديث نظام التشغيل للجهاز) في المرتبة الثامنة عشرة بمتوسط حسابي (2.03)، كما جاءت عبارة (الاحتفاظ بنسخة ورقية للأعمال على الإنترنت) في المرتبة التاسعة عشرة بمتوسط حسابي (1.84)، ثم جاءت عبارة (القيام بتحديث مكافح الفيروسات بالجهاز باستمرار) في المرتبة العشرين بمتوسط حسابي (1.82) .

ويسترعي الانتباه مجيء عبارة (القيام بتغيير كلمة السر بالجهاز بصورة دورية) في مرتبة متأخرة هي المرتبة الحادية والعشرين بمتوسط حسابي (1.77) وهذا الأمر يجعل أجهزة المستخدمين عرضة لكشف كلمات سر المرور بأجهزتهم، ويعرض بياناتهم لأعمال القرصنة والاختراق.

ويعتبر الباحث أن ضعف وعي الجمهور اليمني بطرق الوقاية من الجريمة الإلكترونية، نتيجة طبيعية لغياب برامج التوعية والتثقيف بمخاطر الجريمة الإلكترونية من الجهات ذات العلاقة، والتي يأتي في مقدمتها وزارتي الإتصالات وتقنية المعلومات والداخلية، ونتيجة أيضاً لعدم وجود قانون لمكافحة الجريمة الإلكترونية في اليمن.

ثانياً: نتائج اختبارات الفروض:

الفرض الأول:

توجد علاقة ارتباط دالة إحصائياً بين معدل استخدام الجمهور اليمني للإنترنت، ودرجة وعيهم بالجريمة الإلكترونية بمستوياتها الثلاثة (مفهوم الجريمة الإلكترونية وأساليب الجريمة الإلكترونية وطرق الوقاية من الجريمة الإلكترونية).

جدول رقم (6) يبين العلاقة بين معدل استخدام الجمهور اليمني للإنترنت ودرجة وعيهم بالجريمة الإلكترونية

م	معدل الاستخدام	معدل الاستخدام للإنترنت		
	مستوى الوعي	قيمة معامل الارتباط	مستوى الدلالة	
1	درجة الوعي بمفهوم الجريمة	0.011	0.831	غير دال إحصائياً
2	درجة الوعي بأساليب الجريمة	0.029-	0.568	غير دال إحصائيا
3	درجة الوعي بطرق الوقاية	0.101	0.043	دال إحصائيا

تشير بيانات الجدول السابق إلى عدم وجود علاقة ارتباط ذات دلالة إحصائية بين معدل استخدام الجمهور اليمني للإنترنت ودرجة الوعي بمفهوم الجريمة، حيث بلغت قيمة معامل ارتباط بيرسون (0.011) عند مستوى معنوية (0.831)، بالإضافة إلى عدم وجود علاقة ارتباط ذات دلالة إحصائية بين معدل استخدام الجمهور اليمني للإنترنت ودرجة الوعي بأساليب الجريمة، حيث بلغت قيمة معامل ارتباط بيرسون (-0.029) عند مستوى معنوية (0.568)

فيما تشير بيانات الجدول أيضاً إلى وجود علاقة ارتباط ذات دلالة إحصائية بين معدل استخدام الجمهور اليمني للإنترنت ودرجة الوعي بطرق الوقاية من الجريمة الإلكترونية، حيث بلغت قيمة معامل ارتباط بيرسون (0.101) عند مستوى معنوية (0.043).

وعلى ضوء النتيجة السابقة يتم القبول جزئياً بصحة الفرض القائل ب (توجد علاقة ارتباط دالة إحصائياً بين معدل استخدام الجمهور اليمني للإنترنت، ودرجة وعيهم بالجريمة الإلكترونية بمستوياتها الثلاثة (مفهوم الجريمة الإلكترونية وأساليب الجريمة الإلكترونية وطرق الوقاية من الجريمة الإلكترونية)، حيث تشير هذه النتيجة إلى أن معدل استخدامات الجمهور للإنترنت بتطبيقاته المختلفة لم يكن له تأثير حقيقي في رفع مستوى وعيهم بالجريمة الإلكترونية، سواءً من ناحية مفهوم أو أساليب الجريمة الإلكترونية، بينما وجدت علاقة دالة إحصائياً بين معدل استخدام الإنترنت والوعي بطرق الوقاية منها، رغم ما تتمتع به هذه الوسيلة من إمكانيات عالية بوصفها وسيطاً للمعرفة والثقافة وتدعيم الوعي، ويعتبر الباحث أنه يمكن تفسير ذلك بضعف إحساس المستخدمين بخطورة ما أصبحت تشكله الجريمة الإلكترونية على الأمن النفسي والاقتصادي للأفراد والمجتمع، فاكتفوا باستخدامهم للإنترنت بما يحقق لهم إشباعات التواصل الاجتماعي والتسلية والترفيه والتعلم وغيرها، ويرجع ذلك إلى ضعف أداء الجهات المسئولة عن الجريمة الإلكترونية فيما يتعلق بتوعية الجمهور اليمني بمخاطر الجريمة الإلكترونية .

وقد اتفقت هذه النتيجة مع نتائج عدد من الدراسات السابقة، والتي من أهمها دراسة (الخراساني،2013، ص 138) والتي توصلت إلى أن أغلب المبحوثين في اليمن لا يعلمون مفهوم الجريمة الإلكترونية على الرغم من استخدامهم للإنترنت، كما تشابهت هذه النتيجة مع دراسة (أفروزولاخان، 2018، ص ص5-6) والتي توصلت إلى أن 58% من المبحوثين من طلاب كلية العمل الاجتماعي ومدرسة الخدمة الاجتماعية بمدينة بانجلور الهندية من مستخدمي الإنترنت ليسوا على دراية بأساليب ارتكاب الجرائم الإلكترونية.

وتتماشى هذه النتيجة مع دراسة (الأطرش وعساف، 2009، ص650) التي توصلت إلى أنه من معوقات الجريمة الإلكترونية في الضفة الغربية قلة وعي المستخدمين بخطورة الجرائم المعلوماتية وأساليب ارتكابها.

الفرض الثاني:

توجد علاقة ارتباط دالة إحصائيا بين استخدامات الجمهور اليمني للإنترنت والتأثيرات الناتجة عن هذا الاعتماد من ناحية معرفتهم بمخاطر الجريمة الإلكترونية.

جدول رقم (7) العلاقة بين استخدامات الجمهور اليمني للإنترنت وتأثيرات الاعتماد عليها من ناحية معرفتهم بمخاطر الجريمة الالكترونية

التأثيرات	استخدام الإنترنت		
	قيمة معامل الارتباط	مستوى الدلالة	
تأثير الاعتماد على الإنترنت	0.067	0.342	غير دال إحصائياً

تشير بيانات الجدول السابق إلى عدم وجود علاقة ارتباط دالة إحصائياً بين استخدام الجمهور اليمني للإنترنت وتأثيرات الاعتماد عليها من ناحية معرفتهم بمخاطر الجريمة الإلكترونية، حيث بلغت قيمة معامل ارتباط بيرسون (0.067) عند مستوى معنوية (0.342)، تم رفض الفرض القائل بوجود علاقة ارتباط دالة إحصائيا بين استخدامات الجمهور اليمني للإنترنت والتأثيرات الناتجة عن الاعتماد عليها من ناحية معرفتهم بمخاطر الجريمة الإلكترونية)، ويشير ذلك إلى أن الجمهور اليمني بشكل عام لديه معرفة محدودة بمخاطر الجريمة الإلكترونية والتأثيرات الناتجة عنها، لغياب حملات التوعية والتثقيف بخاطرها، في ظل عدم وجود التشريع الخاص بمكافحة الجريمة الإلكترونية.

وتتفق هذه النتيجة مع دراسة (الحزورة وحيدر، 2020، ص 123) والتي توصلت لعدم وجود علاقة بين درجة اعتماد المبحوثين من الشباب اليمني على الإنترنت ومستوى الوعي بمفهوم الشائعة وأسبابها.

النتائج:

1- أظهرت النتائج زيادة حجم استخدام المبحوثين اليومي للإنترنت، حيث جاء في المرتبة الأولى الاستخدام الكثيف للجمهور عينة الدراسة بنسبة (35.5%) من إجمالي عينة الدراسة، وجاء في المرتبة الثانية الاستخدام المتوسط بنسبة (35%)، تلاه الاستخدام المنخفض بنسبة (29.5%) من إجمالي عينة الدراسة، مما يجعل الجمهور اليمني عرضة لكل تأثيراتها بما في ذلك التأثيرات السلبية ومنها إمكانية تعرضهم للجرائم الإلكترونية.

2- أظهر المبحوثون اعتماداً وثقةً أكبر في (مواقع الإنترنت ومواقع التواصل الاجتماعي) التي جاءت في الترتيب الأول من مصادر معرفتهم بالجريمة الإلكترونية، كما توصلت النتائج إلى تعرض (47%) لنوع واحد على الأقل من الجرائم الإلكترونية وفي مقدمتها على الترتيب (تلقي رسائل إباحية) و(تعطيل النظام المعلوماتي للجهاز بالبرامج الضارة) و(السب والقذف والتهديد من خلال النت) و (انتحال الشخصية على الإنترنت)، بينما جاءت جريمة (الاستغلال الجنسي) في الترتيب الأخير من الجرائم الإلكترونية التي تعرض لها المبحوثون.

3- جاء مواقع (الواتس آب) و (الفيسبوك) بنسبة (45.2%) في مقدمة المواقع بالإنترنت التي تعرض المبحوثون من خلالها للجرائم الإلكترونية.

4- عكست الدراسة المعرفة المعرفة (الجيدة) للمبحوثين بمفاهيم الجريمة الإلكترونية العامة، ومعرفتهم (المتوسطة) بأساليب ارتكاب الجرائم الإلكترونية، كشفت الدراسة عن (وعي ضعيف) للمبحوثين بالدراسة بطرق الوقاية من الجريمة الإلكترونية.

5- جاءت مواقع الإنترنت ومواقع التواصل الاجتماعي في صدارة أهم المصادر التي يعتمد عليها المبحوثون في معرفتهم بالجريمة الإلكترونية، كما توصلت إلى عدم وجود علاقة ارتباط ذات دلالة إحصائية بين معدل استخدام المبحوثين للإنترنت ودرجة وعيهم بمفهوم الجريمة الإلكترونية وأساليبها، بينما وجدت علاقة ارتباط ذات دلالة إحصائية بين معدل استخدام المبحوثين للإنترنت ودرجة وعيهم بطرق الوقاية من الجريمة الإلكترونية، كما لم توجد علاقة ارتباط ذات دلالة احصائية بين استخدام المبحوثين للإنترنت وتأثيرات الاعتماد عليها من ناحية معرفتهم بمخاطر الجريمة الإلكترونية، وقد خلصت الدراسة إلى التوصيات التالية :

6- **التوصيات:**

توصي هذه الدراسة بما يلي:

1- إدراج تعليمات الوقاية من الجرائم الإلكترونية ضمن منهج دراسي (للتربية الإعلامية) لطلبة المدارس والجامعات يتناول فيه طرق الاستخدام الآمن للإنترنت وطرق الوقاية من الجرائم الإلكترونية.

2- تنفيذ حملات إعلامية للتوعية والتثقيف بمخاطر الجريمة الإلكترونية تستهدف جميع فئات الجمهور اليمني المستخدم للإنترنت، من خلال قوالب إعلامية تحتوي على عناصر الجذب والتشويق.

3- سرعة إصدار قانون مكافحة الجرائم الإلكترونية في اليمن.

قائمة المراجع

1. سراج، أحمد والعبالي، وسيم (2022، سبتمبر)، الجريمة الإلكترونية وأضرارها على الفرد والمجتمع، صنعاء، وزارة الدفاع، محاضرات بالكلية الحربية، ص 16
2. الزبن، غدير والخرابشة، عبد الكريم (2021)، الجرائم الإلكترونية ومستوى الوعي بخطورتها، الأردن، *مجلة الجامعة الإسلامية للدراسات الإنسانية*، ع 29
3. الحزورة، نوال وحيدر، مهدي (2020، سبتمبر)، استخدام الشباب اليمني للإنترنت وعلاقته بمستوى وعيهم بالشائعات الإلكترونية حول الأحداث الجارية، القاهرة، *مجلة الإعلام العربي والمجتمع*، مركز كمال أدهم للصحافة التلفزيونية والرقمية، كلية الشئون الدولية والسياسات العامة، الجامعة الأمريكية بالقاهرة، ع 29
4. الدحلة، محمود (2018)، دور صفحة وحدة مكافحة الجرائم الإلكترونية على موقع الفيسبوك في التوعية الأمنية، رسالة ماجستير، غير منشورة، الأردن، جامعة الشرق الأوسط، كلية الإعلام، قسم الصحافة والإعلام
5. Khan ,Afrozulla (May 2018), **Cybercrime Awareness among Msw Students** , School Of Social Work , Mangaluru , India : Department of Criminology and Forensic

Science , School of Social Work , Journal of Forenisic Scieences and Criminal Investigation , Research Articale , Volume 9 , Issue 2
https://juniperpublishers.com/jfsci/pdf/JFSCI.MS.ID.555757.pdf online17/6/2020

6. Otter, Stephen and Others (December 2015), **Real Lives,real crimes, study of digital crime and policing** , UK ,London ,HMIC , Inspecting Policing in the police interest https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf online17/6/2020

7. ذمران، عبد الفتاح محمد نقلاً عن GLOBAL DIGITAL HEADLINES (2021، يونيو)، الإجراءات الفنية لحماية أمن المعلومات في شبكة الاتصالات الوطنية، صنعاء، وزارة الاتصالات وتقنية المعلومات، ورقة عمل مقدمة إلى المؤتمر الوطني الأول للأمن السيبراني

8. الوصابي، علي حميد (2021، يونيو)، تحديات الأمن السيبراني على مستوى الهاتف النقال وشبكات المنظمات، صنعاء، وزارة الاتصالات وتقنية المعلومات، ورقة عمل مقدمة للمؤتمر الوطني الأول للأمن السيبراني

9. سراج، أحمد (2021، يونيو)، التحديات الأمنية في مكافحة الجريمة الإلكترونية، صنعاء، ورقة عمل وزارة الداخلية مقدمة لاجتماع لجنة الدفاع والأمن واللجان ذات العلاقة بمجلس الشورى الجمهورية اليمنية

10. الخراساني، سبأ (2013)، الأبعاد الاجتماعية للجريمة الإلكترونية، رسالة ماجستير، غير منشورة، اليمن، جامعة صنعاء، كلية الآداب والعلوم الإنسانية، قسم علم الإجتماع

11. الأطرش، عصام وعساف، محمد (2019، يونيو)، معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية، الشارقة، جامعة الشارقة، *مجلة جامعة الشارقة للعلوم القانونية*، مجلد 16، ع 1