اتجاهات اعضاء الهيئة التدريسية نحو معالجة الابتزاز الالكتروني

Faculty attitudes towards cyberbullying

دراسة تطبيقية مقدمة الى مجلس النواب العراقي ومجلس الوزراء العراقي

أ.م.د سيناء شمال مصحب أ.م.د علي الحر لازم درويش

م.د وفاء محمد كريم م.م أسماء حسين عباس

م.م بلورة عبد الكريم علون م.م جوهر محي كاظم

م. رئيس احصائيين علي جليل نعمة

كلية الآداب– الجامعة المستنصرية

Dr.alialhur@uomustansiriyah.edu.iq

المستخلص:

بالنظر للاستخدام الواسع لوسائل التواصل الاجتماعي واحتلالها حيزاً كبيراً في اكتساب المعرفة بجميع انواعها، خصوصاً بعد الاعتماد عليا بشكل اساسي خلال فترة وباء كورونا، والتوجه الحكومي بالاستخدام الواسع للتطبيقات الالكترونية في مختلف المجالات من ما ادى الى بروز ظاهرة الابتزاز الالكتروني كأحد المظاهر السلبية في المجتمع.

تهدف الدراسة بالدرجة الاساس الى بيان اتجاهات الابتزاز الالكتروني مع وضع العديد من المعالجات التي من شأنها أن تحد من ظاهرة الابتزاز الالكتروني من جهة وزيادة الروابط الاجتماعية بين شرائح المجتمع من جهة اخرى.

استخدمت الدراسة اسلوب المزاوجة بين الجانب النظري والجانب العملي من خلال استبانة معدة اساساً لهذا الغرض مكونة من (٢٠٠) من اعضاء هيئة التدريس تم توزيعها الكترونياً، واستخدام الاساليب الاحصائية في تبويب وتحليل نتائج الاستطلاع.

وتوصلت الدراسة الى مجموعة من الاستنتاجات والتوصيات التي من شأنها أن تساهم في تحديد اتجاهات الابتزاز الالكتورني ومن اهم الاستنتاجات هي (الخصوصية والسرية كانت المجال الأعلى وعيًا بين المستجيبين)، و (الإناث أظهرن مستوى وعي أعلى مقارنة بالذكور)، وايضا توصلت الدراسة الى مجموعة من التوصيات ومن أهمها (تعزيز التوعية القانونية حول حقوق الأفراد في العالم الرقمي والعواقب القانونية للتهديدات الرقمية)، وايضاً (تطوير برامج توعية موجهة لمختلف الفئات العمرية والجنسية لتعزيز الوعي الرقمي في جميع الفئات).

Abstract :

In view of the widespread use of social media and its occupation of a large space in the acquisition of knowledge of all kinds, especially after relying mainly on it during the period of the Corona epidemic, and the government's trend to use the wide range of electronic applications in various fields, which led to the emergence of the phenomenon of electronic extortion as one of the negative manifestations in society.

The study mainly aims to show the trends of electronic extortion with the development of many treatments that would reduce the phenomenon of electronic extortion on the one hand and increase social ties between segments of society on the other hand.

The study used the method of pairing the theoretical side with the practical side through a questionnaire prepared mainly for this purpose consisting of (٢٠٠) faculty members were distributed electronically, and the use of statistical methods in the classification and analysis of the results of the survey.

The study reached a set of conclusions and recommendations that would contribute to identifying trends in electronic extortion, and the most important conclusions are (privacy and confidentiality were the highest awareness area among respondents), and (females showed a higher level of awareness compared to males), and the study also

reached a set of recommendations, the most important of which are (enhancing legal awareness about the rights of individuals in the digital world and the legal consequences of digital threats), as well as (developing awareness programs directed to different age and gender groups to promote digital awareness in all categories).

المبحث الاول

المنهجية والدراسات السابقة

١.١. منهجية البحث

١.١.١ مشكلة البحث.

تعد ظاهرة الابتزاز الالكتروني من الجرائم المستحدثة داخل المجتمع العراقي في ظل التقدم التكنولوجي والثورة المعلوماتية وكثرة وسائل التواصل الاجتماعي التي انتشرت بشكل ملحوظ، الامر الذي ساهم في زيادة معدلات الاشخاص المعرضين الى الابتزاز الالكتروني، وقد اعطى تطور واتساع وسائل التواصل عن طريق شبكة الانترنيت بعض افراد المجتمع ممن لديهم الدافع الاجرامي اللجوء الى الابتزاز الالكتروني للإيقاع بالبعض واستغلالهم، وتتعقد المشكلة اكثر بتعدد صور واشكال الابتزاز على الرغم من اقتصاره في كثير من الحالات على الابتزاز المالي والمعنوي، الا انه يتعدى هذين الضررين ليشمل الضرر الجسدي عن طريق محاولة المبتز اللقاء المباشر وجها لوجه مع الضحية، من اجل الوصول الى اهداف وغايات مباشرة، وقد ارتفعت معدلات جريمة الابتزاز الالكتروني بصورة ملحوظة في المجتمع العراقي، ومما زاد في تعقيد المشكلة خشية من يتعرض الى الابتزاز من اللجوء الى القضاء خوفا من الوصم الاجتماعي.

٢.١.١ أهمية البحث.

تكمن الاهمية العملية لهذا البحث في اشراك الاساتذة الجامعيين في الراي من اجل الوصول الى حلول منطقية لمشكلة الابتزاز الالكتروني اذ ان المشرع العراقي الى الان لم يصنف هذه الجريمة تصنيفا دقيقا والمتتبع للقرارات القضائية التي تصدر في مثل هذه الدعاوى في المحاكم العراقية على الرغم من كثرتها في الواقع من جهة وقلة رفعها الى القضاء من جهة اخرى يرى ان اغلبها تستند على قرارات القاضي او عن طريق التكييف القانوني اي توظيف قانون ثابت في التشريع العراقي من اجل التعامل مع الواقعة وليس الاستناد على النصوص القانونية

الصريحة لأنها جرائم مستحدثة في الاساس وليس لها سند قانوني ثابت مما يضطر الكثير من القضاة اللجوء الى قانون قريب من الواقعة الجرمية .

ان معرفة اتجاهات النخبة من اعضاء الهيئة التدريسية تجاه هذه الجريمة والية التعامل معها والطرق المتعبة في حلها او التقليل من انتشارها سوف يمنح اصحاب القرار من المختصين ضمان الحد من انتشارها بشكل واسع، اذ ان بالابتزاز الالكتروني يمس جميع فئات المجتمع العراقي دون استثناء، ان معرفة الابعاد الاجتماعية والنفسية لهذه الجريمة عن طريق تشخيص الاساتذة الجامعيين لها يعد من المفاتيح الرئيسة للتعامل معها عن طريق رفد الجهات المختصة بالمعلومات الميدانية في تصنيف الجريمة تصنيفا دقيقا وعن طريق التحليل النظري من اجل وضع الاسس الصحيحة لمعالجتها.

٣.١.١ أهداف البحث.

انقسمت محاور الاستبيان الى خمس محاور من اجل تحقيق الاهداف الاتية:

١. تفعيل وعي المواطن بعدم التفاعل المفرط في مواقع التواصل الاجتماعي مما يقلل من احتمال وقوع جريمة الابتزاز الالكتروني
٢. تفعيل فهم المواطن للدور القانوني الرسمي الذي يحد من احتمال وقوع جريمة الابتزاز الالكتروني
٣. تفعيل وعي المواطن بالاهتمام بالخصوصية والسرية في التعامل مع مواقع التواصل الاجتماعي للحد من احتمال وقوعهم تحت جريمة الابتزاز الالكتروني
٤. تفعيل فهم المواطن حول خطورة العلاقات الانسانية غير المنضبطة في شبكات التواصل

الاجتماعي

٥. تفعيل التكافل الاجتماعي بين المواطنين للحد من انتشار جريمة الابتزاز.

١.١.٤ تسأولات البحث.

١- هل يشكل وعي المواطن دورا مهما في الحد من انتشار جريمة الابتزاز الالكتروني
٢- هل ان اللجوء الى القانون اهمية في الحد من انتشار جريمة الابتزاز الالكتروني
٣- هل ان الاهتمام بالخصوصية والسرية في التعامل مع مواقع التواصل الاجتماعي يحد من انتشار جريمة الابتزاز الالكتروني

٤- هل ان العلاقات التي تخضع للضوابط الاخلاقية تحد من انتشار جريمة الابتزاز الالكتروني
٥- هل ان اللجوء الى مساعدة المقربين في حال حدوث مشكلة على مواقع التواصل الاجتماعي يقلل من احتمال وقوع جريمة الابتزاز الالكتروني

١.١.٥ حدود البحث.

وتتمثل بالاتي:

١.الحدود الموضوعية:اقتصرت حدود البحث ضمن مجال مشكلة الابتزاز الالكتروني واهمية الحد من انتشارها والتعرف عل واقع حالها ومحاولة وضع الحلول المناسبة للحد من اتشارها ضمن مجتمع الطلبة لما يمثلة من شريحة مهمه لبناء المتمع الجديد.

٢.الحدود الزمنية:اقتصرت الحدودالزمنية للبحث للعام الدراسي ٢٠٢٤/٢٠٢٥.

٣.الحدود النوعية:تم الاعتماد عل الجانب العملي وفق مقياس معين للوصول ال نتائج البحث.

٤.الحدود اللغوية:اللغة العربية.

٦.١.١ منهج البحث.

ينتمي هذا البحث الى المنهج المسحي التحليلي الذي يعتمد على دراسة الضاهرة كما توجد في الواقع ويهتم بوصفها وصفا دقيقا ويعبر عنها كيفيا او كميا.وتم الاعتماد في هذا البحث على الجانب الكمي الذي يعطيها مقدارا رقميا الذي يبين مقدار هذة الضاهرة او حجمها او درجة ارتباطها مع الضواهر الاخرى.

٧.١.١ ادوات جمع البيانات:

1.اعتمد البحث بشكل اساسي على ادات الاستبانة التي اعدت من خلال فريق العمل للوصول الى نتائج البحث وفق مقياس معين تم اعتماده.

٢. المصادر والوثائق الخاصة بموضوع الابتزاز الالكتروني تم الاعتماد عليه لصياغة الجانب النظري.

٨.١.١ الاساليب الاحصائية المتبعة:

تم تحليل نتائج الاستبانة وفق البرنامج الاحصائي spss للاستخراج :

1.معامل الارتباط بيرسون Pearson correlation

٢. الوسط الحسابي Arithmetic mean

٣. الانحراف المعباري Standard deviation

٤.الوزن المئوي percentage weight

٥.اختبار تاي T.test

٩.١.١ المصطلحات و المفاهيم:

بما ان موضوع البحث يتطرق الى جريمة ذات ابعاد متشعبة اذ انها لها ابعادها (الاجتماعية والنفسية) ولا يخفى علينا ايضا الجانب (الاجرامي) الذي يعد الاساس في موضوع البحث لذا تحتم الدخول في المسائل القانونية، و ان توظيف المصطلحات هنا لا بد ان يأخذ بالحسبان التوسع قليلا وهو غير معتاد في البحوث التي لا يتعدى عدد صفحاتها الثلاثين لذا اقتصرت المصطلحات والمفاهيم على التعريفات الاتية: –

الاتجاه:

ازاء الكم الهائل من تعريف الاتجاه فقد اقتصر على هذا التعريف بسبب العلاقة المباشرة بينه وبين **موضوع البحث:**

(مجموع استجابات القبول أو الرفض إزاء موضوع اجتماعي جدلي).

اعضاء الهيئة التدريسية:

المقصود بهذا المصطلح هم الموظفون العاملون في الجامعة المستنصرية من الاساتذة التدريسيين في كلية الآداب من تخصص الدراستين العلمية والانسانية.

الابتزاز:

محاولة للإكراه وسلب الإرادة والحرية لإيقاع الأذى الجسدي أو المعنوي على الضحايا عن طريق وسائل يتفنن الجاني في استخدامها لتحقيق جرائمه الأخلاقية أو المادية أو كليهما معاً.

الابتزاز الالكتروني:

هي عملية تهديد وترهيب لضحية ما باستخدام وسائل إليكترونية كبرامج التواصل الاجتماعي أو أي وسيلة إلكترونية أخرى يستطيع من خلالها المبتز الوصول لمعلومات الضحايا مثل الصور، فيديوهات، وثائق... بطريقة غير مصرح بها أو حصل عليها من الضحية بطريقة مباشرة، ومن ثم يهدد بنشر تلك المحتويات إذا لم يحقق الضحية طلباته.

مكافحة:

يعد هذ المصطلح واحدا من اهم المصطلحات التي تجاوزت مداها الزماني اذ انتقل امتداد معناه الى عصرنا الحالي ووظف في الكثير من البحوث ولا سيما في البحوث الانسانية ولم يتشعب المعنى فيه وانما بقي يحتفظ بالمفاهيم العامة له دون اللجوء الى البحث عن مفردات لتفسيره، ولو القينا نظرة فاحصة لمعانيه لراينا انها جميعها تقترب من بعظها على الرغم من التغيرات الكبيرة في معاني المصطلحات التي ترافقت مع التغيرات الحديثة وجاءت معانيه في القواميس بطرق عدة نورد قسما منها جاءت في (معجم المعاني الجامع):

كَفَحَ عَدُوَّهُ : وَاجَهَهُ وَجْهاً لِوَجْهٍ

كافح الفسادَ: حاول إزالته والقضاء عليه،

مُكَافَحَةُ الْمُخَدِّرَاتِ : مُقَاوَمَتُهَا، رَدْعُهَا، القَضَاءُ عَلَيْهَا

كافَح القومُ أعداءَهم: واجهوهم وقاوموهم بقوّة وقاتلوهم

ووظفت الامم المتحدة المصطلح بالطريقة التالية:

(مُكَافَحَةُ الْمُخَدِّرَاتِ وَمَنْعُ الْجَرِيمَةِ وَمُكَافَحَةُ الْإِرْهَابِ الدَّوْلِيِّ بِجَمِيعِ أَشْكَالِهِ وَمَظَاهِرَهُ)

مكافحة الابتزاز الالكتروني:

اذن فان مصطلح مكافحة الابتزاز الالكتروني الذي وظف في هذا البحث لا يشذ عن هذه المعاني وانما هو امتداد لها فهو يمثل:

(محاربة الابتزاز الالكتروني بجميع اشكاله والعمل على القضاء على المجرمين الذين يبتزون الاخرين عن طريق شبكات الانترنيت ومقاومتهم بجميع الوسائل المتاحة)

٢.١ الدراسات السابقة.

٢.١.١. دراسة ثابت، ٢٠٢٤، (دور العروض المسرحية الطلابية في مواجهة الابتزاز الألكتروني):

سلطت هذه الدراسة الضوء حول أهمية تشخيص وكشف الاسباب الكامنة لظاهرة الأبتزاز الألكتروني من خلال العروض المسرحية وعلى مستوى طلبة الجامعات، حيث هدفت الدراسة الى مواجهة الابتزاز الالكتروني بواسطة العروض المسرحية، وتوصلت الدراسة الى مجموعة من النتائج ومن اهمها ان النساء في المجتمع العراقي اكثر عرضة للابتزاز الالكتروني، وأن الابتزاز موجود في الجامعات العراقية وان الاختلاط يعتبر من العوامل المساعدة لعملية الابتزاز، ومن اهم التوصيات هي ضرورة عمل العروض المسرحية وتشجيع الطلبة على اداءها، وزيادة التوعية للطلبة بواسطة إدارات الجامعات حول مخاطر الابتزاز الألكتروني.

٢.١.٢ دراسة سافوح، ٢٠٢٤، (الأثار الاجتماعية والنفسية للابتزاز الالكتروني ضد المرأة وأساليب مواجهتها):

استهدفت الدراسة تحديد الاثار الاجتماعية والنفسية للابتزاز الالكتروني وبالاخص المرأة، وتم استخدام عينة على الأسر الريفية المصرية ومن أبرز نتائج هذه الدراسة أن وسائل الاتصال الحديثة تعتبر من اسباب انتشار ظاهرة الابتزاز الالكتروني، وأن الابتزاز الالكتروني للمرأة سبب التفكك الاسري وفقدان الثقة في المجتمع، واصابة الضحية بالقلق والخوف اضافة الى الاكتئاب والحزن الدائم، وأن الانفتاح الثقافي يؤدي الى مساهمة معنوية في زيادة الابتزاز الالكتروني، ومن التوصيات هي تكثيف البرامج الاعلامية الهادفة يؤدي الى رفع مستوى الوعي بأثار الابتزاز الالكتروني، وان المعرفة بأسباب انتشار الابتزاز الالكتروني تؤثر في درجة الابتزاز الالكتروني للمرأة.

٢.١.٣ دراسة أبو زيد و صابر، ٢٠٢٢، (إسهامات الخدمة الأجتماعية في الحد من مخاطر الأبتزاز الالكتروني للشباب وتصور مقترح من منظور الأزمة في طريقة خدمة الفرد):

هدفت الدراسة الى التعرف على مساهمة الاختصاصيين الاجتماعيين في الحد من ظاهرة الابتزاز الالكتروني للشباب حيث ركزت على مجموعة من التساؤلات ومن اهمها ما هو واقع ممارسة اخصائي خدمة الفرد لاستخدام نموذج الازمة مع ضحايا الابتزاز الالكتروني من طلبة المرحلة الثانوية، ولعل من أهم نتائج الدراسة هي ان الاساليب الروحية لها دور بارز في تدعيم الصمود النفسي لضحايا الابتزاز الالكتروني ومنها التفاعل الاجتماعي واعادة البناء المعرفي.

٢.١.٤ دراسة الحداد و عباس، ٢٠٢٥ (الابتزاز الالكتروني في الاعلام الرقمي):

هدفت هذه الدراسة الى دور الاعلام الرقمي في انتشار الابتزاز الالكتروني داخل المجتمع العراقي، ومعرفة انماط تعرض افراد المجتمع لوسائل الاعلام الرقمي والتوصل الى انواع الابتزاز الالكتروني وتأثيره على المجتمع العراقي، واتبعت المنهج الوصفي بواسطة اجراء المسح الميداني لعينة من (٤٥٠) فرد، ومن اهم نتائج هذه الدراسة ان التطبيقات الالكترونية ساهمت في زيادة الجرائم الالكترونية.

المبحث الثاني: الجانب النظري

الابتزاز الالكتروني

١. مفهوم الابتزاز الالكتروني

يعتبر الابتزاز الالكتروني تحولاً مركباً في فهمنا للابتزاز، حيث يعتمد على استخدام التكنولوجيا لتوجيه هذه الظاهرة نحو الافراد، ويعتمد بشكل اساسي على وسائل التواصل الاجتماعي، وللابتزاز الالكتروني العديد من التعرفيات ويمكن عرضها في الجدول الأتي: –

الجدول (١) تعريفات الأبتزاز الالكتروني

ت	المصدر	التعريف
١	(ثابت، ٢٠٢٤، الصفحات ١١٧–١٣١)	"عملية اجرامية يقوم بها اشخاص محتالون يستمتعون بالحاق الاذى بالاخرين تتضمن تهديد وترهيب للضحية بنشر صور أو مواد فلمية أو تسريب

		معلومات سرية تخص الضحية، وتعرضها لمخاطر المساومة لدفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة"
2	(Ibrhim & Albatashi, 2021, pp. 54-78)	"عملية تهديد وترهيب لضحية ما بواسطة وسائل الكترونية مثل برامج التواصل الاجتماعي او اي وسيلة الكترونية اخرى من خلال وصول المبتز الى معلومات الضحية بطريقة غير مصرح بها، ومن ثم تهديده بنشر تلك المحتويات اذا لم يحقق الضحية طلباته"
3	(Gazi & Qanbar, 2024)	"عملية تهديد وترهيب للضحية بنشر صور او مواد فيلمية او تسريب معلومات سرية للضحية، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتز"
٤	(سليم & صالح، ٢٠٢٤)	"هو تلك الافعال التي تجبر الفرد على التهديد بكشف معلومات معينة عن شخص ما او على فعل شئ مؤذ للشخص المهدد، في حال عدم استجابته لبعض الطلبات المطلوبة منه"

٢. انواع الابتزاز الالكتروني.

للأبتزاز الألكتروني عدة أنواع تعتمد على الهدف المطلوب منه، ويقسم بعدة صور وأشكال ومنها: –

١– الأبتزاز العاطفي: سيتهدف هذا النوع تحقيق السيطرة العاطفية على الضحية من قبل المبتز، ويتم ذلك بواسطة استغلال مشاعر الضحية والاعتماد على الضغط بشكل عاطفي وبالتالي جعل الضحية تشعر بالذنب والخجل من خلال تهديدها بكشف المعلومات الحساسة او السلوك غير المقبول الذي يمتلكه المبتز (المطيري، ٢٠١٦).

٢- الابتزاز المادي: الغاية من هذا النوع تكمن في الحصول على مكاسب ماليه وذلك بواسطة تهديد الضحية وضعفها من قبل المبتز، ويمكن للمال أن يؤثر على الافراد بحيث يضحي الاقارب والاصدقاء المقربين ببعضهم البعض من أجل تحقيق المكسب المالي. (الدوسري، ٢٠٢٣، الصفحات ١٠١١-١٠٤٢)

٣. وسائل الابتزاز الالكتروني

يوجد العديد من الوسائل التي من الممكن ان يستخدمها الشخص المبتز على ضحيته وذلك من اجل تحقيق غايته، ومن اهم هذه الوسائل هي: -

١- الصور والمقاطع المرئية: تحصل هذه العملية من خلال عدة طرق مثل عملية تهكير حاسوب او جهاز موبايل الضحية أو الوصل اليها بطريقة غير مشروعة أو سرقة جهاز الضحية، ومن ثم المطالبة بمبالغ مالية او امور معنوية مما يؤدي الى الحاق الأذى بالضحية.

٢- التسجيل الصوتي: ويتم بواسطة تسجيل المكالمات بجميع انواعها بين المبتز والضحية ومن بعدها يتم استخدام التسجيل كوسيلة ضغط من اجل تحقيق الغاية للمبتز.

٣- الرسائل الالكترونية والغرامية: وتشمل استخدام رسائل اجهزة الموبايل و وسائل التواصل والبريد الالكتروني، من اجل ابتزاز الضحية ويمكن تحتوي هذه الرسائل على تهديدات او مطالب مادية من قبل المبتز.

٤- الابتزاز المعلوماتي: وتتم هذه العملية بواسطة سرقة المعلومات المهمة لشركة او مؤسسة ما وبالتالي تتم عملة الابتزاز لتحقيق غاية المبتز.

٥- جرائم اخرى: تشمل اعلان البغاء والتحريض على ممارسته ونشر المواد الجنسية المخلة بالاداب العامة، واستغلال حقوق المؤلف. (نقيب، ٢٠٢٣)

٤. اسباب الابتزاز الألكتروني.

يعتبر الابتزاز الالكتروني من أخطر الجرائم على مستوى المعلوماتية، حيث يشكل تهديداً لاستقرار المجتمع وامنه وذلك بسبب المشاكل السلبية التي تترتب على الفرد والمجتمع، وتعود اسباب الابتزاز الى مجموعة من العوامل لعل من أهمها هو الضعف الديني الناتج عن قصور وضعف في الخلفية الدينية للشخص المبتز الامر الذي يؤدي الى زيادة الميول الاجرامي والتوجه نحو هذه الظاهرة، ومن تلك العوامل ايضاً هي عدم قيام الافراد بواجباتهم في

الاسرة حيث قد لا يكون الاب قادراً على كسب لقمة العيش وتوجيه الابناء وزرع القدوة الحسنة داخلهم بحسن التصرف في الحياة. (سالم & السيد، ٢٠٢٤، الصفحات ٢٢٨٣-٢٢٨٥)

وتعتبر عملية انتشار وسائل التواصل الاجتماعي وشبكة الانترنيت من هام عوامل زيادة حالات الابتزاز الالكتروني، وذلك بسبب سهولة استخدام هذه الوسائل وتوفرها لجميع فئات المجتمع، اضافة الى الجهل وعدم معرفة الحقائق سبب اضافي لزيادة الابتزاز. (الحداد & عباس، ٢٠٢٥، الصفحات ٤-١٤٠)

٥. مخاطر الابتزاز الألكتروني.

هنالك العديد من المخاطر المترتبة من ظاهرة الابتزاز الألكتروني وتقسم الى : -

١- المخاطر الأجتماعية: حيث يعتبر انتشار هذه الجريمة انتهاك واضح للسلم المدني ، وذلك بسبب التهديد الذي يتعرض له الفرد والذي تتعرض له الاسرة.

٢- المخاطر النفسية: يؤثر الابتزاز الالكتروني بشكل مباشر على الامور النفسية للضحية وقد يسبب الاضطراب والخوف والقلق والاكتئاب، الامر الذي يؤدي الى التأثر المباشر للشخصية وبالتالي التفكير في الانتحار أو التخلص من الفضيحة بواسطة عمل أمور تؤدي الى زيادة هذه الظاهرة.

٣- المخاطر الأمنية: يعتبر الابتزاز الالكتروني واحداً من اخطر الجرائم المهددة للمجتمعات وامنها، وقد يؤدي الابتزاز الى استغلال الضحية من اجل تنفيذ الجرائم بجميع انواعها (كريم & خلف، ٢٠١٩).

٦. الاساليب الوقائية من الابتزاز الالكتروني.

أن من اهم الاساليب وطرق الوقاية التي يحتاج لها الفرد من اجل حماية نفسه من الابتزاز الالكتروني هي: -

١- حماية المعلومات والبيانات الشخصية، وذلك بواسطة عدم مشاركتها مع أي شخص وخصوصاً ارقام البطاقات الشخصية وبطاقات المصرف، وكلمات المرور الخاصة بالايميل ومواقع التواصل.

٢- أستخدام اعدادت الخصوصية لبرامج التواصل الاجتماعي، بهدف الحماية من المتطفلين.

٣- استخدام كلمات المرور القوية والتي تحتوي على رموز وارقام.

٤- تجنب مشاركة أي تفاصيل خاصة وشخصية (Nobles, 2014, pp. 986-1014).

٥- الحذر الدائم وعدم الرد على اي رسائل مجهولة وعدم فتح الروابط التي ترد من جهات مجهولة (البياتي، ٢٠٢٢، الصفحات ٤٨٤-٤٦٧).

المبحث الثالث:الجانب العملي

تحليل النتائج

اشارت النتائج المسترجعة من قبل الباحثين بعد عزل الإجابات الصحيحة والمكتملة الى النتائج الواردة في الجدول ادناه:

الجدول رقم (٢) يبين الأوساط الحسابية والانحرافات المعيارية والاوزان المؤية لفقرات المقياس

الفقرة	الوسط الحسابي	الانحراف المعياري	الوزن المؤي
[تجنب ارسال الصور الشخصية والخاصة او نشرها على مواقع التواصل الاجتماعي]	2.595	0.642682	85.635
[ابتعد عن قبول طلبات الصداقة العشوائية في مواقع التواصل الاجتماعي]	2.85	0.47	94.05
[ضع كلمات سر قوية وغريبة لكل حساب تمتلكه على مواقع التواصل لعدم استطاعة احدا تخمينها]	2.875	0.412585	94.875
[ابتعد عن الاتصال بشبكات الانترنت المفتوحة وخاصة في الاماكن العامة]	2.39	0.678381	78.87
[احتفظ برسائل البريد الالكتروني او نسخة من المحادثات التي تثبت تعرضك للتهديد]	2.79	0.486914	92.07
[باستمرار غير كلمات المرور الخاصة ببرامجك ولا تفصح عنها لاحد]	2.595	0.634815	85.635
[تجنب السماح لكل التطبيقات على هاتفك الوصول الى الكاميرا]	2.655	0.606477	87.615
[اتصل بالجهات المختصة في حال تعرضك لتهديد]	2.89	0.358529	95.37

[حاول ان لا تخبر احدا ليساعدك عندما تتعرض لتهديد]	1.815	0.839224	59.895
[عندما تستبدل الجهاز الخاص بك لا تكتفي بمسح الصور وأرقام الهاتف، بل سجل الخروج من جميع الحسابات المرتبطة به]	2.86	0.448784	94.38
[ابتعد عن مشاركة تاريخ ميلادك وهواياتك مع الآخرين على مواقع التواصل الاجتماعي]	2.495	0.701739	82.335
[اطلب من طلابك عدم احضار الهاتف للمدرسة لحمايتهم من سرقة معلوماتهم الشخصية]	2.42	0.70433	79.86
[اسرع بإبلاغ الجهات المعنية للتطبيق الذي تستخدمه عن اي مضايقة تتعرض لها]	2.81	0.452686	92.73
[أن استخدامك لمواقع التواصل الاجتماعي يتطلب منك الحذر والوعي]	2.91	0.320019	96.03
[ابتعد عن استخدام اي موقع مجهول المصدر او غير مشهور]	2.87	0.392262	94.71
[ضع غطاء على الكاميرا الخاصة بالكومبيوتر لجعلها غير ذات فائدة في حال تمكن احد من اختراقها وتشغيلها من دون علمك]	2.735	0.55345	90.255
[عندما يتم سرقة حسابك قم بإبلاغ شخص مقر منك ليساعدك]	2.86	0.425801	94.38
[متابعة شخصيات مؤثرة اعلاميا التي تنشر وتحث الافراد بضرورة التبليغ عن اي حالة تهديد تصادفهم]	2.575	0.60515	84.975
[قم بأغلاق جميع حساباتك عندما تشعر بوجود احد يحاول اختراقها]	2.805	0.498213	92.565
[لا ارى ان عقوبة كل شخص يحاول تهديد شخص ما السجن بمدى اقصاها سبع سنوات كافية لردعه]	2.41	0.695932	79.53
[في الفصول الدراسية يحاول الاساتذة تدريب الطلبة على عدم الخوف من اي شخص يحاول تهديدهم]	2.65	0.632058	87.45
[لا داعي لحملات التوعية التي تركز على القضايا القانونية]	1.46	0.728735	48.18
[شارك اصدقاءك صورك ويومياتك السعيدة على برامج التواصل]	1.845	0.777171	60.885

[عدم قبول استخدام اسم مستعار عند تفعيل برامج التواصل لحماية الاشخاص من تهديد الحسابات المجهولة]	2.5	0.679935	82.5

من خلال ملاحظة الجدول أعلاه يتبين ان الوعي مرتفع بين المشاركين حول أهمية الأمان في استخدام مواقع التواصل الاجتماعي، حيث حصلت العبارات المتعلقة بالحذر، مثل ضرورة استخدام كلمات مرور قوية (٢.٨٧٥)، وتجنب المواقع غير الموثوقة (٢.٨٧)، والاتصال بالجهات المختصة عند التعرض للتهديد (٢.٨٩)، على أعلى درجات التأييد، مما يدل على إدراك واضح لمخاطر الإنترنت واهتمام عام بحماية الحسابات من الاختراق والتهديدات الإلكترونية. كما يعكس التأييد الكبير للعبارة "أن استخدامك لمواقع التواصل الاجتماعي يتطلب منك الحذر والوعي" (٢.٩١) إيمان المشاركين بأن الأمان الرقمي مسؤولية فردية تتطلب اتخاذ إجراءات استباقية.

على الجانب الآخر، أظهر المشاركون رفضًا واضحًا لبعض السلوكيات غير الآمنة، مثل عدم إبلاغ الآخرين عند التعرض للتهديد (١.٨١٥) أو التقليل من أهمية حملات التوعية القانونية (١.٤٦)، ما يشير إلى تقديرهم لدور التوجيه والإرشاد في تعزيز الأمان الرقمي. يعكس هذا الرفض إدراكًا بأن مواجهة المخاطر الإلكترونية تتطلب مشاركة مجتمعية، سواء من خلال طلب المساعدة عند التعرض للتهديد أو الاستفادة من التوعية القانونية لحماية الحقوق الرقمية. كما أن رفض فكرة مشاركة المعلومات الشخصية والصور عبر وسائل التواصل الاجتماعي دون ضوابط (١.٨٤٥) يشير إلى انتشار ثقافة الخصوصية بين المشاركين، حيث أصبحوا أكثر وعيًا بالمخاطر المحتملة لنشر المعلومات الشخصية علنًا.

من ناحية أخرى، كشفت بعض العبارات ذات الانحراف المعياري المرتفع، مثل "لا داعي لحملات التوعية القانونية" (٠.٧٢٨)، عن تباين في وجهات النظر حول بعض التدابير الوقائية، مما قد يعكس اختلافًا في مستوى المعرفة أو القناعات الشخصية حول مدى أهمية القوانين في الحماية الرقمية. هذا التفاوت قد يكون ناتجًا عن تباين الخبرات السابقة بين المشاركين؛ فالبعض قد يكون تعرض لمواقف أظهرت له أهمية التشريعات في مكافحة الجرائم الإلكترونية، بينما قد يرى آخرون أن التوعية القانونية لا تؤثر بشكل مباشر على أمنهم الشخصي. أما فيما يتعلق بالممارسات الأمنية الأخرى، فإن العبارات مثل "ابتعد عن الاتصال بشبكات الإنترنت المفتوحة" (٢.٣٩) وقم بإغلاق جميع حساباتك عندما تشعر بوجود أحد يحاول اختراقها" (٢.٨٠٥) تعكس إدراكًا بضرورة اتخاذ إجراءات احترازية، رغم أن درجة التأييد لها كانت أقل من العبارات الأكثر أهمية، مما قد يشير إلى أن بعض الأشخاص لا يزالون غير مدركين تمامًا لمخاطر معينة، مثل التجسس عبر الشبكات العامة أو ترك الحسابات غير محمية.

بشكل عام، تؤكد هذه النتائج على ضرورة تكثيف الجهود التوعوية وتعزيز السلوكيات الرقمية الصحيحة، مع التركيز على أهمية الإبلاغ عن التهديدات، تجنب الشبكات المفتوحة، وعدم مشاركة المعلومات الشخصية دون وعي، حيث أصبح الأمان السيبراني مسألة أساسية تتطلب تعاونًا مجتمعيًا لضمان بيئة رقمية أكثر أمانًا للجميع.

الجدول (٣) يبين الأوسط الحسابية والانحرافات المعيارية لمجالات المقياس

المجال	الوسط الحسابي	الانحراف المعياري	الوزن المؤي
العلاقات الإنسانية	2.679	0.561	88.393
المحور القانوني	2.548	0.584	84.095
الخصوصية والسرية	2.844	0.423	93.844
الوعي	2.380	0.632	78.540
التكافل الاجتماعي	2.173	0.729	71.693

تشير نتائج التحليل إلى تباين واضح في مستويات التأييد لمجالات مختلفة تتعلق بالأمان الرقمي والمسؤولية المجتمعية، حيث تصدّر مجال الخصوصية والسرية أعلى متوسط حسابي (٢.٨٤٤) وأعلى وزن مؤيد (٩٣.٨٤٤)، مما يعكس إدراكًا واسعًا بين المشاركين لأهمية حماية البيانات الشخصية والحفاظ على سرية المعلومات في بيئة الإنترنت. كما أن الانحراف المعياري المنخفض نسبيًا (٠.٤٢٣) يدل على إجماع كبير حول هذا المجال، مما يشير إلى أنه يُنظر إليه باعتباره جانبًا أساسيًا في التعامل مع الفضاء الرقمي، وقد يكون ذلك نتيجة لتزايد المخاوف المتعلقة بسرقة البيانات والاختراقات الإلكترونية.

أما العلاقات الإنسانية فقد حظيت بدرجة تأييد مرتفعة أيضًا، بمتوسط حسابي (٢.٦٧٩) ووزن مؤيد (٨٨.٣٩٣)، مما يعكس أهمية الحفاظ على السلوك الأخلاقي والتفاعل الإيجابي في بيئات الإنترنت. الانحراف المعياري (٠.٥٦١) يشير إلى وجود تفاوت طفيف في وجهات النظر، ولكن بشكل عام، يبدو أن المشاركين يعترفون بدور العلاقات الإنسانية في تعزيز الأمان الرقمي، خاصةً في ما يتعلق بالتعامل مع الآخرين بشكل مسؤول وتجنب السلوكيات السلبية مثل التنمر الإلكتروني أو إساءة استخدام المعلومات الشخصية للآخرين.

في المحور القانوني، حصل المجال على متوسط حسابي (٢.٥٤٨) ووزن مؤيد (٨٤.٠٩٥)، مما يدل على وعي جيد بالقوانين المتعلقة بالأمان الرقمي، إلا أن هذا المستوى من التأييد لا يزال أقل نسبيًا مقارنةً بمجال الخصوصية والعلاقات الإنسانية. يشير الانحراف المعياري (٠.٥٨٤) إلى وجود اختلافات بين المشاركين في مدى إيمانهم

بأهمية الدور القانوني في الحماية الرقمية، وهو ما قد يكون ناتجًا عن تباين في مستوى المعرفة القانونية أو عدم ثقة بعض الأفراد في فعالية القوانين الحالية في التصدي للجرائم الإلكترونية. لذا، يمكن اعتبار هذه النتيجة مؤشرًا على الحاجة إلى تعزيز التوعية القانونية حول الحقوق والمسؤوليات الرقمية.

أما الوعي فقد حصل على متوسط حسابي (٢.٣٨٠) ووزن مؤيد (٧٨.٥٤٠)، مما يعكس مستوى تأييد أقل مقارنةً بالمجالات السابقة، وهو ما قد يشير إلى أن بعض المشاركين لا يزالون بحاجة إلى مزيد من الإرشاد حول أهمية الوعي الرقمي ودوره في الحماية من المخاطر الإلكترونية. الانحراف المعياري (٠.٦٣٢) هو من بين الأعلى في الجدول، مما يدل على تباين واضح في آراء المشاركين، حيث قد يكون البعض مدركًا تمامًا لأهمية الوعي الرقمي بينما لا يزال الآخرون غير مدركين لتأثيره الكبير على أمنهم وسلامتهم الإلكترونية. بناءً على هذه النتيجة، يمكن اقتراح المزيد من الحملات التوعوية التي تركز على تعزيز ثقافة الأمان الرقمي بين جميع الفئات.

أخيرًا، جاء التكافل الاجتماعي في أدنى مرتبة من حيث التأييد، بمتوسط حسابي (٢.١٧٣) ووزن مؤيد (٧١.٦٩٣)، مما يشير إلى أن المشاركين لا يعتبرونه بنفس الأهمية التي يضعونها لمجالات مثل الخصوصية والقانون. الانحراف المعياري (٠.٧٢٩) هو الأعلى في الجدول، مما يدل على وجود تباين واسع في وجهات النظر حول هذا المجال، حيث قد يرى البعض أن التكافل الاجتماعي عبر الإنترنت مسؤولية مجتمعية مهمة، بينما قد يراه آخرون أقل أهمية مقارنةً بالجوانب التقنية والقانونية للأمان الرقمي. يمكن تفسير ذلك بأن التكافل الاجتماعي في الفضاء الرقمي قد يكون أقل وضوحًا في تأثيره المباشر على الأمان الشخصي مقارنةً بالتدابير التقنية والقانونية.

وبالمجمل يتضح أن هناك إجماعًا كبيرًا على أهمية الخصوصية والسرية، مما يشير إلى وعي مرتفع بالمخاطر المرتبطة بانتهاك البيانات الشخصية. كما أن العلاقات الإنسانية والمحور القانوني يحظيان بتأييد قوي، لكنهما لا يزالان بحاجة إلى تعزيز أكبر في التوعية، خاصة فيما يتعلق بفهم القوانين الرقمية وأثرها على الحماية. أما مجالات الوعي والتكافل الاجتماعي فتحتاج إلى مزيد من الجهود لتعزيز إدراك أهميتها في تحقيق بيئة إلكترونية أكثر أمانًا وتعاونًا، لا سيما أن الوعي يعدّ عنصرًا أساسيًا في الوقاية من المخاطر الرقمية.

الجدول(٤) يبين الأوساط الحسابية والانحرافات والقيمة التائية للمقياس ككل تبعا لمتغير الجنس

الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	القيمة التائية المحسوبة	القيمة التائية الجدولية	النتيجة
ذكور	٨٩	٢.٢٦	٠.٧١	١٩٩	١.٩٧٢	١.٩٨	غير دال احصائيا
اناث	١١١	٢.٤١	٠.٦٢				

تشير نتائج التحليل الإحصائي إلى وجود تفاوت طفيف بين الذكور والإناث فيما يتعلق بالمتوسط الحسابي لمستوى الوعي، حيث حصلت الإناث على متوسط حسابي أعلى (٢.٤١) مقارنة بالذكور (٢.٢٦)، مما يشير إلى أن الإناث أكثر وعيًا أو اهتمامًا بتدابير الحماية الرقمية مقارنة بالذكور. ومع ذلك، فإن هذا الفرق لم يكن دالًا إحصائيًا، حيث بلغت القيمة التائية المحسوبة (١.٩٧٢)، وهي أقل من القيمة التائية الجدولية (١.٩٨) عند درجة حرية ١٩٩، مما يعني أن الفرق قد يكون ناتجًا عن التفاوت العشوائي وليس عن اختلاف جوهري بين الجنسين.

كذلك يكشف الانحراف المعياري أن الذكور لديهم انحراف معياري أعلى (٠.٧١) مقارنة بالإناث (٠.٦٢)، مما يشير إلى أن استجابات الذكور كانت أكثر تباينًا واختلافًا فيما بينهم، بينما كانت استجابات الإناث أكثر تقاربًا، مما قد يدل على أنهن يمتلكن تصورًا أكثر استقرارًا حول الأمان الرقمي. يمكن تفسير ذلك بعدة طرق، فقد تكون الإناث أكثر وعيًا بالمخاطر الإلكترونية نظرًا لارتفاع معدلات التعرض لمحاولات الاحتيال أو الاختراق، أو لأنهن أكثر عرضة للتركيز على الجوانب الأمنية عند استخدام وسائل التواصل الاجتماعي والمنصات الرقمية.

يتبين من خلال الكلام السابق انه على الرغم من أن الإناث سجلن متوسطًا أعلى في الوعي بالأمان الرقمي مقارنة بالذكور، إلا أن الفرق لم يكن دالًا إحصائيًا، مما يعني أنه لا يمكن الجزم بأن الجنس يؤثر بشكل حاسم على مستوى الوعي الرقمي في هذه العينة. يمكن تفسير ذلك بأن العوامل الأخرى، مثل التعليم، التجربة الشخصية، أو الاهتمام بالأمان الرقمي بشكل عام، قد تلعب دورًا أكبر من مجرد الاختلاف بين الجنسين.

الجدول (٥) يبين الأوساط الحسابية والانحرافات والقيمة التائية للمقياس ككل

العدد	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	القيمة التائية المحسوبة	القيمة التائية الجدولية	النتيجة
٢٠٠	٢.٣٣	٠.٦٧	١٩٩	٢.١١	١.٩٨	دال احصائيا

تكشف النتائج الإحصائية عن دلالة معنوية في مستوى الوعي بالأمان الرقمي لدى العينة المدروسة، حيث بلغ المتوسط الحسابي (٢.٣٣) مع انحراف معياري (٠.٦٧). الأهم من ذلك هو أن القيمة التائية المحسوبة (٢.١١) تجاوزت القيمة التائية الجدولية (١.٩٨) عند درجة حرية ١٩٩، مما يعني أن الفرق الذي تم ملاحظته ليس عشوائيًا، بل هو فرق دال إحصائيًا، أي أنه يمكن تعميمه على المجتمع الأكبر بثقة عالية.

كما يشير المتوسط الحسابي (٢.٣٣) إلى أن مستوى الوعي الرقمي لدى الأفراد في العينة كان أعلى من المتوسط النظري، مما يدل على أن هناك إدراكًا جيدًا لمبادئ الأمان الرقمي. ومع ذلك، فإن الانحراف المعياري (٠.٦٧) يعكس وجود تفاوت ملحوظ بين أفراد العينة في درجة وعيهم، مما يشير إلى أن بعض الأفراد يمتلكون معرفة قوية حول الأمان الرقمي، بينما لا يزال البعض الآخر بحاجة إلى مزيد من التوعية والتدريب.

ونظرًا لأن القيمة التائية المحسوبة (٢.١١) أكبر من القيمة التائية الجدولية (١.٩٨)، فهذا يعني أن النتائج ليست ناتجة عن الصدفة، وإنما تشير إلى وجود فرق حقيقي يمكن تفسيره بناءً على العوامل المؤثرة في العينة، مثل المستوى التعليمي، الخبرة الرقمية، أو التعرض السابق للتهديدات الإلكترونية. هذه النتيجة تؤكد أهمية الاستمرار في تعزيز البرامج التوعوية لضمان أن جميع الأفراد يتمتعون بمستوى وعي رقمي كافٍ.

وبالمجمل تشير النتائج على الوعي بالأمان الرقمي في العينة ليس مجرد ظاهرة عشوائية، بل هو فرق دال إحصائيًا يمكن تعميمه. ومع ذلك، فإن التفاوت بين الأفراد يستدعي مزيدًا من الجهود في التدريب والتوعية المستمرة لضمان أن الجميع يمتلك المعرفة اللازمة لحماية أنفسهم في العالم الرقمي.

النتائج:

١-ان مستوى الوعي بالأمان الرقمي في العينة كان أعلى من المتوسط النظري، حيث بلغ المتوسط الحسابي العام (٢.٣٣) مع انحراف معياري (٠.٦٧). وهذا يشير إلى أن الأفراد في العينة يمتلكون إدراكًا معقولًا لممارسات الأمان الرقمي، ولكن لا يزال هناك تفاوت بينهم.

٢-الإناث أظهرن مستوى وعي أعلى مقارنة بالذكور، حيث بلغ المتوسط الحسابي للإناث (٢.٤١) مقابل (٢.٢٦) للذكور، لكن الفرق لم يكن دالًا إحصائيًا (القيمة التائية المحسوبة = ١.٩٧٢ أقل من القيمة الجدولية = ١.٩٨). وهذا يعني أن الفرق قد يكون ناتجًا عن عوامل أخرى وليس عن تأثير الجنس وحده.

٣-الانحراف المعياري لدى الذكور كان (٠.٧١)، وهو أعلى من الإناث (٠.٦٢)، مما يدل على تباين أكبر في مستوى وعي الذكور مقارنة بالإناث.

٤-الخصوصية والسرية كانت المجال الأعلى وعيًا بين المستجيبين، حيث بلغ المتوسط الحسابي له (٢.٨٤٤) مع انحراف معياري (٠.٤٢٣) ووزن نسبي (٩٣.٨٤٤٪). وهذا يدل على إدراك قوي لأهمية حماية البيانات الشخصية على الإنترنت.

٥-المحور القانوني حصل على متوسط حسابي (٢.٥٤٨) مع انحراف معياري (٠.٥٨٤) ووزن نسبي (٨٤.٠٩٥٪). ورغم أن هذه النتيجة مرتفعة نسبيًا، إلا أنها تشير إلى الحاجة لمزيد من التوعية بالقوانين المتعلقة بالأمان الرقمي والجرائم الإلكترونية.

٦-أقل مستوى وعي كان في مجال التكافل الاجتماعي، حيث بلغ المتوسط الحسابي (٢.١٧٣) مع انحراف معياري (٠.٧٢٩) ووزن نسبي (٧١.٦٩٣٪).وهذه النتيجة تعكس ضعف إدراك الأفراد لأهمية التعاون المجتمعي في مواجهة التهديدات الرقمية والتبليغ عنها.

٧- كما كشفت نتائج التحليل الإحصائي وجود فرق دال إحصائيًا في مستوى الوعي الرقمي، حيث بلغت القيمة التائية المحسوبة (٢.١١) وهي أكبر من القيمة الجدولية (١.٩٨) عند درجة حرية ١٩٩. وهذا يعني أن الفروقات في مستوى الوعي ليست عشوائية، وإنما تعكس اتجاهًا حقيقيًا يمكن تعميمه.

٨-بعض الممارسات الأمنية الرقمية حظيت بمستوى وعي مرتفع، حيث حصلت العبارات التالية على أعلى الأوزان النسبية:

- "أن استخدامك لمواقع التواصل الاجتماعي يتطلب منك الحذر والوعي" حصلت على متوسط حسابي (٢.٩١) مع انحراف معياري (٠.٣٢٠٠١٩) ووزن نسبي (٩٦.٠٣٪).
- "اتصل بالجهات المختصة في حال تعرضك لتهديد" حصلت على متوسط حسابي (٢.٨٩) مع انحراف معياري (٠.٣٥٨٥٢٩) ووزن نسبي (٩٥.٣٧٪).
- "ضع كلمات سر قوية وغريبة لكل حساب تمتلكه" حصلت على متوسط حسابي (٢.٨٧٥) مع انحراف معياري (٠.٤١٢٥٨٥) ووزن نسبي (٩٤.٨٧٥٪).

٩-على الجانب الآخر، هناك بعض المفاهيم التي سجلت مستويات وعي منخفضة، ومنها:

- "لا داعي لحملات التوعية التي تركز على القضايا القانونية" حصلت على أدنى مستوى وعي، بمتوسط حسابي (١.٤٦) مع انحراف معياري (٠.٧٢٨٧٣٥) ووزن نسبي (٤٨.١٨٪)، مما يعكس عدم إدراك بعض الأفراد لأهمية التوعية القانونية في مجال الأمن الرقمي.
- "حاول أن لا تخبر أحدًا ليساعدك عندما تتعرض لتهديد" حصلت على متوسط حسابي (١.٨١٥) مع انحراف معياري (٠.٨٣٩٢٢٤) ووزن نسبي (٥٩.٨٩٥٪)، مما يشير إلى أن بعض الأفراد لا يدركون أهمية اللجوء إلى الآخرين للحصول على الدعم في المواقف الخطرة.

التوصيات:

في ضوء النتائج السابقة، يوصي الباحثون بالآتي:

١- تعزيز التوعية القانونية حول حقوق الأفراد في العالم الرقمي والعواقب القانونية للتهديدات الرقمية.
٢- تطوير برامج توعية موجهة لمختلف الفئات العمرية والجنسية لتعزيز الوعي الرقمي في جميع الفئات.
٣- إدراج مفاهيم الأمان الرقمي في المناهج الدراسية بالتعاون مع المؤسسات التعليمية.
٤- تنفيذ برامج تدريبية تركز على الاستخدام الآمن لمواقع التواصل الاجتماعي وحماية الخصوصية.
٥- توفير برامج توعية لرفع الوعي بالتكافل الاجتماعي وتعزيز التعاون والإبلاغ عن التهديدات الرقمية.
٦- تسليط الضوء على أهمية السرية وحماية المعلومات الشخصية عبر الإنترنت.
٧- إطلاق حملات توعية حول أهمية تغيير كلمات المرور بشكل دوري وعدم استخدام نفس الكلمة في أكثر من حساب.
٨- تشجيع المؤسسات الحكومية على تطوير سياسات رقابة على الأمان الرقمي.
٩- تعزيز برامج الدعم النفسي والاجتماعي للأفراد المتعرضين للتهديدات الرقمية.

١٠- مواصلة الدراسات والبحوث لفهم تأثير العوامل الاجتماعية والثقافية على الوعي الرقمي وتصميم حملات توعية فعّالة.

المصادر الانكليزية

Gazi & Qanbar. (2024). *SECURITY SERVICES EMPLOYEES AND ELECTRONIC BLACKMAIL INSTITUTIONS: A STUDY OF THE MINISTRY OF INTERIOR. AL-ADAB JOURNAL.*

Ibrhim & Albatashi. (2021). *Digital media technology and social change: a study of the phenomenon of electronic blackmail in social media in Oman.*

Nobles. (2014). *Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. Justice Quarterly.*

المصادر العربية

البياتي. (٢٠٢٢). *الابتزاز الالكتروني.*

ثابت. (٢٠٢٤). *دور العروض المسرحية الطلابية في مواجهة الابتزاز الالكتروني.* عد خاص.

ر. أ. م. س الدوسري. (٢٠٢٣). *القذف والابتزاز الالكتروني بين الشريعة الاسلامية والقانون الكويتي.* المجلة القانونية .

راكان المطيري. (٢٠١٦). *دور شبكات التواصل الاجتماعي في الابتزاز المؤدي الى الجرائم غير الاخلاقية.*

سالم & السيد. (٢٠٢٤). *مقاصد الشرعية واثرها في حماية المجتمع وصيانة افراده (الابتزاز الالكتروني) انموذجا.* مجلة البحوث الفهقية والقانونية .

سليم & صالح. (٢٠٢٤). *تأثير الابتزاز الالكتروني على الامن المجتمعي.*

ع. س الحداد & عباس. (٢٠٢٥). *الابتزاز الالكتروني في الاعلام الرقمي دراسة ميدانية.* كلية الاداب – جامعة المنوفية.

كريم & خلف. (٢٠١٩). *انتشار ظاهرة الابتزاز الالكتروني في المجتمع العراقي استطلاع اراء عينة من المجتمع العراقي حول التعامل* . مؤتمر الاداب والعلوم الانسانية والطبيعية.

نقيب. (٢٠٢٣). *الابتزاز الالكتروني على الطالبات الجامعيات عبر مواقع التواصل الاجتماعي*. جامعة مولود معمري تيزي.

الملاحق

محاور الاستبيان

كل ما جاء هنا تم على اساس فقرات الاستبيان والتي جاءت بهذه المحاوروكما يلي: –

المحور الاول: محور العلاقات الانسانية.

ابتعد عن قبول طلبات الصداقة العشوائية في مواقع التواصل الاجتماعي

ابتعد عن الاتصال بشبكات الانترنت المفتوحة وخاصة في الاماكن العامة

ابتعد عن مشاركة تاريخ ميلادك وهواياتك مع الآخرين على مواقع التواصل الاجتماعي

اطلب من طلابك عدم احضار الهاتف للمدرسة لحمايتهم من سرقة معلوماتهم الشخصية

أن استخدامك لمواقع التواصل الاجتماعي يتطلب منك الحذر والوعي

ابتعد عن استخدام اي موقع مجهول المصدر او غير مشهور

في الفصول الدراسية يحاول الاساتذة تدريب الطلبة على عدم الخوف من اي شخص يحاول تهديدهم

المحور الثاني: المحور القانوني.

احتفظ برسائل البريد الالكتروني او نسخة من المحادثات التي تثبت تعرضك للتهديد

اتصل بالجهات المختصة في حال تعرضك لتهديد

اسرع بإبلاغ الجهات المعنية للتطبيق الذي تستخدمه عن اي مضايقة تتعرض لها

متابعة شخصيات مؤثرة اعلاميا التي تنشر وتحث الافراد بضرورة التبليغ عن اي حالة تهديد تصادفهم

لا ارى ان عقوبة كل شخص يحاول تهديد شخص ما السجن بمدى اقصاها سبع سنوات كافية لردعه

لا داعي لحملات التوعية التي تركز على القضايا القانونية

المحور الثالث: محور الخصوصية والسرية.

ضع كلمات سر قوية وغريبة لكل حساب تمتلكه على مواقع التواصل لعدم استطاعة احدا تخمينها

قم بأغلاق جميع حساباتك عندما تشعر بوجود احد يحاول اختراقها

باستمرار غير كلمات المرور الخاصة ببرامجك ولا تفصح عنها لاحد

عدم قبول استخدام اسم مستعار عند تفعيل برامج التواصل لحماية الاشخاص من تهديد الحسابات المجهولة

المحور الرابع: محور الوعي.

تجنب ارسال الصور الشخصية والخاصة او نشرها على مواقع التواصل الاجتماعي

تجنب السماح لكل التطبيقات على هاتفك الوصول الى الكاميرا

عندما تستبدل الجهاز الخاص بك لا تكتفي بمسح الصور وأرقام الهاتف، بل سجل الخروج من جميع الحسابات المرتبطة به

ضع غطاء على الكاميرا الخاصة بالكومبيوتر لجعلها غير ذات فائدة في حال تمكن احد من اختراقها وتشغيلها من دون علمك

شارك اصدقاءك صورك ويومياتك السعيدة على برامج التواصل

المحور الخامس: محور التكافل الاجتماعي

عندما يتم سرقة حسابك قم بإبلاغ شخص مقرب منك ليساعدك.

حاول ان لا تخبر احدا ليساعدك عندما تتعرض للتهديد.